SUMS OF SQUARES

OLGA TAUSSKY, California Institute of Technology

1. Introduction. Sums of squares is a major concept in mathematics going back to ancient days and yet of great current interest. It is a subject which links many different branches of mathematics and produces results which have a certain similarity but whose complete connection is still not understood. In recent years logicians have been much interested in the subject too. There are applications to and from logic to sums of squares. Statistics from its beginnings has been involved in sums of squares.

This article describes some of these ideas, but is by no means comprehensive. In particular the chapter on number theory is very incomplete. The presentation is a spotlight treatment, sometimes putting very deep results next to easier ones, although the latter may have a particular appeal and even importance. Proofs are included only when they are very brief. Some new ideas are incorporated.

This account is devoted to algebra and number theory on the whole, apart from describing facts which link up with analysis and topology and ought not to be separated. But sums of squares also occur in the very definition of the Hilbert space and all its consequences, e.g. in Parseval's theorem, in the definition of L^2-convergence, in normed algebras and such like. The composition of infinite quadratic forms will not be discussed. Not even the theory of finite euclidean and unitary space will be included, nor facts concerning orthonormal vectors, nor the theory of norms of finite matrices. Hence orthogonal and unitary matrices are not treated, nor automorphs of quadratic forms.

2. Pythagorean triangles and Fermat's last theorem. The first sum of squares we meet in our life is in Pythagoras' theorem

$$a^2 + b^2 = c^2, \tag{1}$$

where a, b are the sides of a right angled triangle with hypotenuse c. Later we meet in elementary trigonometry

$$\cos^2 \alpha + \sin^2 \alpha = 1 \tag{2}$$

and much later we meet

$$\cos^2 z + \sin^2 z \equiv 1 \tag{3}$$

The author received her training under P. Furtwängler at the University of Vienna, held assistantships at Göttingen and Vienna, and a fellowship at Girton College, Cambridge, and was a lecturer at London University. She was Scientific Officer with the British Aircraft Production Ministry and served with the Department of Scientific and Industrial Research, London. After many years with the National Bureau of Standards, she transferred to Cal Tech where she is Research Associate (equivalent rank of Full Professor). Leaves of absence were spent at NYU, Bryn Mawr College, Vienna (as Fulbright Professor), and UCLA.

Olga Taussky's prolific research centers on algebraic number theory, quaternions, and matrix theory. She was co-editor of Hilbert's *Gesammelte Abhandlungen* and edited several volumes of the Nat. Bur. Stand. Applied Math. Series. *Editor.*

for all complex values z. The Pythagorean triangles too turn up at an early stage in our education. They are right angled triangles whose sides have integral ratios like

$$3, 4, 5;\ 5, 12, 13;\ \cdots.$$

They are already mentioned in an old-Babylonian text discovered by Neugebauer and Sachs. It is known that there are infinitely many such triangles and that they are obtained from a parametric formula

$$\lambda(m^2 - n^2), \quad \lambda 2mn, \quad \lambda(m^2 + n^2) \tag{4}$$

with λ, m, n any integers. Sometimes the same triangle can be obtained several times by this formula, e.g. the triangle 6, 8, 10 is given by $\lambda=1$, $m=3$, $n=1$, and by $\lambda=2$, $m=2$, $n=1$. That every expression (4) leads to a Pythagorean triangle is clear. The converse will now be proved. We start with some general remarks.

At least one of a, b is even. For, if $a=2n+1$, $b=2m+1$, n, m integers, then $c^2=4N+2$, N an integer. This is impossible, for the square of an odd number is always of the form $4r+1$, r an integer, and that of an even number is divisible by 4. We shall assume that b is even. If a and b have a common factor $d\neq 2$, then $d \mid c$. Hence a/d, b/d also define a Pythagorean triangle. If, however, $d=2$ and $b/2$ is odd then we cannot remove it, unless $a/2$ is even, in which case we interchange the role of a and b. If, however, both $a/2$ and $b/2$ are odd then $(c/2)^2$ would again be of the form $(4M+2)$, M an integer, which is impossible.

The following elementary proof for the converse uses the fact that the expressions (4) suggest the formulas for $\cos 2\alpha$, $\sin 2\alpha$. Let

$$a^2 + b^2 = c^2.$$

Define the angle $\alpha (0<2\alpha<\pi/2)$ by

$$\frac{a}{c} = \cos 2\alpha, \quad \frac{b}{c} = \sin 2\alpha.$$

Since $\cos 2\alpha=\cos^2\alpha-\sin^2\alpha$ and $\cos^2\alpha+\sin^2\alpha=1$ we have

$$\cos^2 \alpha = \frac{1}{2}\left(1 + \frac{a}{c}\right) = r_1, \text{ a rational,}$$

$$\sin^2 \alpha = \frac{1}{2}\left(1 - \frac{a}{c}\right) = r_2, \text{ a rational.}$$

Since $\sin 2\alpha = 2 \sin \alpha \cos \alpha$ we have

$$\sin \alpha \cos \alpha = \frac{1}{2} \frac{b}{c} = r, \text{ a rational.}$$

Hence

$$r = \sqrt{r_1 r_2}.$$

Hence

$$\sin \alpha = \frac{r}{r_1} \cos \alpha = \frac{n}{m} \cos \alpha,$$

where n, m are integers which we may suppose without a common factor. Put

$$\frac{\cos^2 \alpha}{m^2} = \lambda_0 \quad \text{(a rational) so that } \sin^2 \alpha = \lambda_0 n^2.$$

This gives

$$a = \lambda(m^2 - n^2), \qquad b = \lambda \cdot 2mn,$$

where $\lambda = \lambda_0 c$. We claim that λ is necessarily integral. For, if λ were fractional with p, a prime, dividing the denominator, then $p \mid (m^2 - n^2)$, $p \mid 2mn$. If $p \neq 2$, then $p \mid m$ or $p \mid n$. Since $p \mid (m+n)$ or $p \mid (m-n)$ it follows that $p \mid m$ and $p \mid n$ which is a contradiction. If $p = 2$ and $p \nmid m$, $p \nmid n$ then b is not even as was assumed.

In contrast to the various elementary proofs of (4) a proof using Galois theory will now be given. It is based on Hilbert's Theorem 90 which concerns algebraic extension fields with a cyclic Galois group. This theorem is obtained nowadays as a special case of a theorem in Galois cohomology (see e.g. Jacobson, Algebra III.)

Let F be a cyclic extension of a field K of relative degree l. Let S be a generator of the Galois group of F over K. For any $\alpha \in F$ we write α^S for the automorphism defined by S. We then have

$$\operatorname{norm}_{F/K}(\alpha) = \operatorname{norm}_{F/K}(\alpha^S).$$

Hence by the multiplicativity of the norm we have

$$\operatorname{norm}_{F/K}(\alpha/\alpha^S) = 1.$$

Hilbert's theorem states that, conversely, any element $\beta \in F$ with norm $\beta = 1$, is of the form $\beta = \alpha/\alpha^S$ for a suitable $\alpha \in F$.

Apply the theorem to the situation where F is the extension obtained from the rational number field Q by adjoining $\sqrt{-1}$, i.e., the set of elements $m + in$, $m, n \in Q$. This field is cyclic with respect to Q and of degree 2. Further

$$(m + in)^S = m - in \quad \text{and} \quad \operatorname{norm}(m + in) = m^2 + n^2.$$

Let then $a^2 + b^2 = c^2$ hold with a, b and c in Z, the ring of integers. This implies

$$\operatorname{norm}\left(\frac{a}{c} + i \frac{b}{c}\right) = 1.$$

By Hilbert's theorem

$$\frac{a}{c} + i \frac{b}{c} = \frac{m + in}{m - in} = \frac{(m + in)^2}{m^2 + n^2}$$

for some $m, n \in Z$. Comparing the real and imaginary parts (4) emerges.

We add three further comments to the study of Pythagorean triangles:

(1) The expressions (4) can be given another interpretation: It is clear that Pythagorean triangles have much in common with complex numbers. The product of two complex numbers m_1+in_1, m_2+in_2 is $m_1m_2-n_1n_2+i(m_1n_2+m_2n_1)$. This associates two bilinear forms $m_1m_2-n_1n_2$, $m_1n_2+m_2n_1$ with the field of complex numbers. The corresponding quadratic forms

$$m^2 - n^2,\ 2mn$$

are exactly the expressions (4).

Similarly, one can associate a set of n bilinear (respectively quadratic) forms with any basis of an algebra. This idea is being investigated separately, particularly for algebraic number fields.

(2) The Pythagorean triangles form a group under a certain composition law: more precisely to every triangle a, b, c consider the whole set λa, λb, λc, with $\lambda=1, 2, \cdots$, as an element of the group under consideration. Further identify all the four pairs $\pm a$, $\pm b$. We may therefore assume a, b as coprime positive integers. Exactly one of these two integers is then even, because $a^2+b^2=c^2$ is a square, hence cannot be $\equiv 2(4)$. We will assume that b is an even number.

Let a_i, b_i, $i=1, 2$, be a pair which generate a Pythagorean triangle. Then it follows at once that

$$A = a_1a_2 + b_1b_2, \qquad B = a_1b_2 - a_2b_1$$

again generate a Pythagorean triangle. The set of triangles generated by A, B is the "product" of a_1, b_1 and a_2, b_2. If $a_1=a_2$, $b_1=b_2$, we obtain

$$A = a_1^2 + b_1^2, \qquad B = 0$$

which is equivalent with $A=1$, $B=0$. We consider this as the unit element in our group. For, this element when composed with a, b gives a, $-b$ which is equivalent with a, b. The associative law too follows for our composition if we again allow the above identification.

(3) The two quadratic forms $f=x^2-y^2$, $g=2xy$ associated with Pythagorean triangles, have a special property. Let

$$f_i = x_i^2 - y_i^2, \quad g_i = 2x_iy_i, \qquad i = 1, 2.$$

Then the pair of forms

$$f_1f_2 - g_1g_2, \qquad f_1g_2 + f_2g_1$$

are again the same forms f, g, but applied to the indeterminates:

$$x_1x_2 - y_1y_2, \qquad x_1y_2 + x_2y_1.$$

For $x_1=x_2$, $y_1=-y_2$ this gives the well-known relation $(x^2-y^2)^2+4x^2y^2 =(x^2+y^2)^2$.

The existence of these triangles made it desirable to know whether the equation

$$x^n + y^n = z^n \tag{5}$$

can be solved in integers x, y, z for $n > 2$, apart from trivial cases. The not yet established statement that this is impossible is referred to as Fermat's last theorem. A similar question was raised concerning the relation (3) namely, do there exist two entire functions $f(z)$, $g(z)$, neither of them a constant, such that for some $n > 2$

$$(f(z))^n + (g(z))^n \equiv 1. \tag{6}$$

A very brief proof was given by Iyer showing that such a pair does not exist. The equation (6) above is identical with

$$\prod(f(z) + \zeta g(z)) \equiv 1$$

when the product is taken over all solutions ζ of the equation $x^n + 1 = 0$. Since none of the n factors can vanish the meromorphic function $f(z)/g(z)$ cannot assume any of the n values of ζ which would be in contradiction with the 'big' Picard theorem.

3. Sums of squares in number theory. This is an enormous subject which can only be touched briefly here. Again a very old theorem comes to our mind immediately: every positive integer is a sum of four squares of integers. Then we have the characterizations of integers which are sums of three squares and the well-known fact that an integer is a sum of two squares if and only if its square-free part is the product of primes $\equiv 1(4)$.

The quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is not the only form $\sum a_i x_i^2$, a_i positive integers, which represents all positive integers. Forms of this nature are called universal and have been studied, e.g. by L. E. Dickson, Kloosterman, Linnik, Pall, and Ramanujan. Forms which represent all but one positive integer were examined by Halmos. Heilbronn showed that there exist four continuous functions $f_i(x)$ such that every rational x is represented by $\sum f_i(x)^2$. To represent positive integers by more than four, in particular by many, squares has been studied too and the function giving the number of representations of the fixed integer n as the sum of exactly s squares has been of much interest for a long time. Recently Bateman pointed out that the function $f_s(n) = (2s)^{-1} r_s(n)$ is multiplicative precisely for $s = 1, 2, 4, 8$, where $r_s(n)$ is the number of representations of n as a sum of s integral squares.

The problem of representing algebraic integers as sums of squares in the same field has been much studied, but will not be discussed here.

Next we look at *integral* symmetric matrices, a subject not fully investigated so far.

(The fact that a *real* symmetric matrix has real characteristic roots links their study with sums of squares, but this aspect will be discussed in Chapter 6.)

Even the subject of rational symmetric matrices is not fully explored. For 2×2 matrices the characteristic roots of such a matrix must lie in a field $Q(\sqrt{m})$, m a sum of two squares. This can be checked easily from the formula for the zeros of the (quadratic) characteristic polynomial. However, it can also be obtained as a special case of the following fact: Let F be an extension of degree n of the rationals and let it have a symmetric $n\times n$ Q-representation. Then this is equivalent with the existence of n elements $\alpha_1, \cdots, \alpha_n$ in F such that $\sum_i \alpha_i^{(r)}\alpha_i^{(s)}=0$, $r, s=1, \cdots, n$, $r\neq s$, where the upper suffices denote the conjugate elements with respect to Q. First we show that this is necessary: Let A be the Q-matrix which represents the primitive element α. Since A is symmetric its characteristic vectors are orthogonal. Since A is a Q-matrix these vectors can be chosen in $Q(\alpha^{(i)})$, $i=1, \cdots, n$, and as the conjugates of the vector corresponding to the characteristic root α. Hence the components of this vector are of the form of the above $\alpha_1, \cdots, \alpha_n$. Next we show sufficiency: the matrix

$$(\alpha_i^{(j)}) \begin{pmatrix} \alpha & & & \\ & \alpha^2 & & \\ & & \ddots & \\ & & & \alpha^{(n)} \end{pmatrix} (\alpha_i^{(j)})'$$

is rational and symmetric; here and later the prime indicates the transpose. Hence we have obtained a rational symmetric representation of $Q(\alpha)$.

From the orthogonality it also follows that F is totally real.

The case $n=2$ gives an alternative proof for a fact mentioned above, for the two elements α_1, α_2 are expressible as

$$\alpha_1 = a + b\sqrt{m}, \qquad \alpha_2 = c + d\sqrt{m},$$

where a, b, c, d, m are in Q and m is not a square in Q. Then

$$a^2 - mb^2 + c^2 - md^2 = 0.$$

Hence

$$a^2 + c^2 = m(b^2 + d^2).$$

Symmetric $n\times n$ matrices over the integers with a given characteristic polynomial of degree n, with integer coefficients and 1 as coefficient of x^n can sometimes best be studied by looking first for general matrices, i.e. not necessarily symmetric ones. Such matrices fall into classes: two matrices being considered equivalent if they belong to the same integral unimodular similarity class. For irreducible polynomials this leads to an integral $n\times n$ representation of the ring generated by a zero of the polynomial and hence to a rational $n\times n$ representation for the algebraic number field generated by it. Let A be a suitable matrix. Then A', the transpose, is a matrix-zero of the same polynomial. Under special circumstances it can belong to the class of A. We then have

$$A' = S^{-1}AS$$

when S is integral and unimodular. If in addition S is p.d. (positive definite) and even of the form $S=TT'$ with T integral (this follows from p.d. for $n\leqq 7$, (see Chapter 4)), then

$$T^{-1}AT = (T^{-1}AT)'$$

Hence the class of T contains a symmetric matrix and conversely. Faddeev, Shapiro, Bender studied symmetric matrices over algebraic number fields with given characteristic polynomials. However, not all polynomials which can turn up for symmetric matrices have been characterized so far.

This whole chapter belongs partly to the theory of positive definite matrices. They are treated in the next chapter which also includes further number theoretic results. Also the similarity between a matrix and its transpose and the connection with symmetric matrices will turn up there again for the case of the real number field.

4. Positive definite (p.d.) matrices. These are real symmetric matrices with positive characteristic roots. Again a very old fact is our starting point: a positive definite quadratic form with real coefficients is a sum of squares of linear forms. Positive definite hermitian forms are expressible as $\sum l_i(x)\bar{l}_i(\bar{x})$, where $l_i(x)$ is a linear form and $\bar{l}_i(x)$ is the form with the conjugate coefficients.

For the matrix itself this means in the real case that it can be factorized as AA' where A' is the transpose of A and in the complex case as BB^* where $B^*=\bar{B}'$ is the transposed complex conjugate.

One of the most important uses of p.d. matrices is to generalize facts in many different branches of mathematics, by replacing the identity matrix by a given p.d. matrix. We begin with two specific examples.

(1) *The orthogonal matrices.* They leave $\sum x_i^2$ unchanged. This was generalized in the study of the 'automorphs' of p.d. quadratic forms.

(2) *The field of values of a complex $n\times n$ matrix A.* It is the set of numbers in the complex plane given by x^*Ax/x^*x, where $x\neq 0$ is an arbitrary complex n-vector. Givens introduced the generalized field of values x^*AHx/x^*Hx when H is a p.d. form. This was recently even extended to operators.

In differential geometry Riemannian geometry extends Euclidean geometry. In the subject of partial differential equations the theory of elliptic equations extends that of the Laplace equation. There are many examples in the calculus of variations. There are examples in number theory on all levels.

We begin with the discussion of products of real symmetric matrices. It can be shown that every real matrix is the product of two symmetric matrices—more generally a matrix with elements in an arbitrary field F can be expressed as the product of two symmetric matrices in the same field. In the case of the reals: if one of the two symmetric factors is positive definite then the product is similar to a real diagonal. If both factors are p.d. then the product is similar to a p.d. diagonal. Connected with this is the following fact: while every matrix with elements in a field F is similar to its transpose via a symmetric matrix over F, the latter can be chosen in the form AA' (and therefore p.d. for the reals) if the original matrix is similar to a symmetric matrix, (i.e. has real characteristic roots and is diagonalizable in the case of the reals). Real matrices with positive determinant can always be expressed as products of p.d. matrices, in fact only four factors are needed, unless the matrix is a negative scalar in which case five factors are required, in general. This was shown by Ballantine who also characterized products of three p.d. factors. Products of two p.d. matrices had been characterized by Taussky.

Positive definite matrices can be employed to determine the signs of the real parts of the characteristic roots of a general matrix. This is an important practical problem. By a theorem of D. C. Lewis, Jr., one can find for any matrix A with simple elementary divisors a p.d. hermitian G such that the roots λ of $\det(GA+A^*G-2\lambda G)=0$ are the real parts of the characteristic roots of A. Also there is the matrix version of Lyapunov's stability criterion:

A matrix A is stable if and only if a p.d. G exists such that $AG+GA^*$ is negative definite.

This was generalized to give statements concerning the signs of the real parts of the characteristic roots.

The fact that every real symmetric matrix can be transformed to diagonal form by an orthogonal matrix can be generalized by saying that a pair of symmetric matrices, one of which is p.d., can be transformed to diagonal form simultaneously. This again is generalized by saying that a pair of symmetric matrices S_1, S_2 which generate a pencil $\lambda S_1+\mu S_2$ which contains a p.d. matrix can be simultaneously diagonalized. Such pencils have been studied recently and were linked up with the convex cone formed by the p.d. $n\times n$ matrices in the $n(n+1)/2$ dimensional space.

The cone of p.d. matrices H is invariant under the transformation

$$AHA'$$

when A is any non-singular matrix of the same dimension. Thus they form a 'positivity domain' like the positive vectors which are invariant under transformation by a positive matrix (in this case even a non-negative ($\neq 0$) matrix). The transformation defined by A on the linear space of symmetric matrices can be regarded as a 'positive operator' and the finite version of the Krein-Rutman theorem concerning such operators can be applied to it. From this it follows that the matrix which corresponds to the operator has a positive dominant characteristic root. The matrices H which are 'characteristic vectors' are of interest too.

We now turn to consideration of number theory and we mention some facts concerning the factorization XX' and the problem of representing integers by p.d. forms.

Positive definite matrices play a big role in number theory. In particular, unimodular integral matrices A have been studied by Hermite and Minkowski who showed that for $n\leqq 7$ every such matrix is of the form BB', with B an integral $n \times n$ matrix. For $n=8$ this is not any longer true as an example by Korkine and Zolotareff shows. Mordell showed that there are two classes in this case if we count two matrices A, B as belonging to the same class if $B=SAS'$ where S is an integral and unimodular matrix. The number of classes is finite in all cases.

A special case of p.d. unimodular matrices arises from the set of group matrices for the finite group G (a ring isomorphic with the integral group ring of G). These matrices are of the form $(a_{rs^{-1}})$, where r, s range over the elements of G in a fixed order. The unimodular ones correspond to the units in the group ring. A factorization of the above type is possible only if B is a group matrix for the same group, times an integral matrix P with $PP'=I$. For $n \leqq 7$ such a factorization is possible always, for $n=8$ there are again two classes. For $n=9$, however, there is only one class. These results were obtained by Taussky, M. Newman, R. C. Thompson, M. Kneser, some still unpublished.

The results concerning the factorization of positive definite unimodular matrices have been extended to hermitian matrices and to matrices over quadratic number fields. For instance, any matrix

$$A = \begin{pmatrix} a & \alpha \\ \bar{\alpha} & b \end{pmatrix}$$

with a, b positive integers, $\alpha = x+iy$ a Gaussian integer and $ab-\alpha\bar{\alpha}=1$ can be factorized into BB^* with B a square matrix of Gaussian integers. This result leads to an alternative proof for Lagrange's theorem on expressing a positive integer a as a sum of four squares. The following fact is needed: Given a number a, integers $b>0$, x, y can be found such that

$$x^2 + y^2 = -1 + ab.$$

Starting with the positive integer a the matrix A is now determined. The factorization $A=BB^*$ then expresses a as a sum of four squares. (This was pointed out by M. Newman during a discussion with the author.)

Even if the p.d. integral matrix is not of the form XX', X an integral square matrix, it may still be expressible in this form with X a rectangular matrix with more columns than rows. For the corresponding quadratic form this means that it is still expressible as a sum of squares of integral linear forms, but with more than n terms. However, even this is not always possible. This was studied by Mordell, Erdös, Chao Ko, Pall and Taussky.

Alternatively, the problem of expressing a matrix A in the form XBX' has been studied in full generality by Siegel, where now A and B do not need to have the same dimension. Hence this includes the representation of numbers by p.d. quadratic forms.

The extension of the problems to algebraic number fields led Siegel to a conjecture which was established quite recently. It concerns 'classes' and 'genera' of forms. It is known that over the rationals the forms

$$\sum_1^4 x_i^2, \qquad \sum_1^8 x_i^2$$

are in a genus of one class. Over totally real fields the form $\sum_1^4 x_i^2$ lies in a genus of one class only for $Q(\sqrt{2})$, $Q(\sqrt{5})$. This is what Siegel had conjectured. After some initial progress by Dzewas it was established by Barner.

5. Formally real fields. The congruence

$$x^2 + y^2 \equiv -1(p), \qquad p \text{ any prime},$$

used in Chapter 4, can be used as a link with this theory since the integers modulo a prime p form a field. A formally real field is characterized by the fact that -1 cannot be expressed as a sum of squares in that field. The fact that the above congruence can be solved for any p not only shows that the residues mod p do not form a formally real field (a fact obvious from the finite characteristic), but it gives the actual expression for -1.

If the field is not formally real and if its characteristic $\neq 2$ then every element in the field is a sum of squares.

If -1 is a sum of squares then it is of interest to study the minimum number of terms in the representation of -1 for various fields F. It is easy to see that 3 cannot occur as a minimum. For, assume that 3 is the minimum and let

$$-1 = x_1^2 + x_2^2 + x_3^2, \qquad x_i \in F, \quad x_i \neq 0.$$

This implies

$$0 = x_0^2 + x_1^2 + x_2^2 + x_3^2, \qquad x_i \in F.$$

Hence

$$\begin{aligned} 0 &= (x_0^2 + x_1^2)^2 + (x_0^2 + x_1^2)(x_2^2 + x_3^2) \\ &= (x_0^2 + x_1^2)^2 + (x_0x_2 - x_1x_3)^2 + (x_0x_3 + x_1x_2)^2, \end{aligned}$$

so that transferring $(x_0^2+x_1^2)^2$ to one side and dividing across by it (using the fact that $x_0^2+x_1^2=0$ by assumption) we get a representation of -1 as a sum of two squares. This contradicts our assertion. This proof depends on the multiplication of complex numbers and their norms. A similar proof using the multiplication of quaternions and the multiplicativity of their norms shows that 5, 6, 7 cannot occur as a minimum. The same idea, using Cayley numbers, shows that the numbers 9, $\cdots$, 15 cannot occur as a minimum. The question concerning the possible minima had been raised by van der Waerden in 1932 and was settled only quite recently by Pfister. He showed that only powers of 2 can occur as a minimum and that every such power does occur for some field. Pfister uses results of Cassels on quadratic forms for his proof. The relevant theorems are:

Let F be a field of characteristic $\neq 2$. Let $d \in F$ and x be an indeterminate. Necessary and sufficient for x^2+d to be a sum of $n>1$ squares in $F(x)$ is that either -1 or d is a sum of $n-1$ squares in F.

Let R be the field of real numbers and let $x_1, \cdots, x_n$ be indeterminates over R. Then $x_1^2+ \cdots +x_n^2$ is not a sum of $n-1$ squares in $R(x_1, \cdots, x_n)$.

As the cases 1, 2, 4, 8 show, the result is connected with the composition of sums of squares which will be discussed in the next chapter.

By defining 'positive' in real fields as 'sums of squares' an ordering can be introduced in such fields.

Symmetric matrices over formally real fields have been studied. The set of all their characteristic roots form a field which is real closed. Krakowski and recently also Bender studied symmetric matrices over arbitrary fields with given minimum polynomial.

An application of formally real fields appeared in a very unexpected connection: R. C. Thompson proved (generalizing a theorem by Shoda obtained for algebraically closed fields) that, with the exception of certain 2×2 matrices over GF(2), every unimodular matrix A with elements in a field F is a commutator $B^{-1}C^{-1}BC$ in F. He also studied the question: when can the factors B, C themselves be chosen unimodular? For the case that A is a scalar matrix, this depends, among other things, on whether -1 is a sum of two squares in F. Later Thompson examined the case when the factors B, C have given determinants b, c and then the representation of -1 in the form bx^2+cy^2 becomes critical.

6. Composition of sums of squares, anticommuting matrices, composition algebras. Hurwitz showed that $n=1$, 2, 4, 8 are the only values of n for which identities of the following type hold:

$$\sum_1^n x_j^2 \sum_1^n y_k^2 = \sum_1^n [l_i(x, y)]^2,$$

where l_i are bilinear forms in the x_j, y_k. Pfister's results concerning -1 as a sum of squares are linked with an extension of this problem: he allows the $l_i(x, y)$ to be *rational* functions. In this way he obtains an identity for any n which is a power of 2. For $n=8$ such an identity had been obtained independently by Taussky by a different method and this result was extended to $n=16$ by Eichhorn and Zassenhaus:

The usual way to obtain the above mentioned identities is from the product $\alpha\beta$ of two complex numbers, respectively quaternions, or Cayley numbers, and using the fact that norm $\alpha\beta=$norm α norm β in all these cases. The identities found by Taussky and Eichhorn and Zassenhaus were, however, derived for $n=2$ from the reals, for $n=4$ from the complex field, for $n=8$ from quaternions, for $n=16$ from Cayley numbers. The method is based on the generalization of the relation $\det X \overline{\det X} = \det XX^*$ when X^* means the transpose conjugate.

The identities are special cases of Gauss' concept of composition of quadratic forms: two n-ary quadratic forms $f(x_i)$, $g(x_i)$ are said to permit composition if the product fg can again be expressed as a quadratic form under a bilinear transformation of the indeterminates.

Hurwitz' proof is based on matrix theory and leads to the enumeration of skew symmetric $n\times n$ matrix pairs which are anticommuting. Such pairs are of interest in many connections and will be mentioned again in Chapter 7. Using an idea of Jordan, von Neumann, and Wigner the theory of group representations was employed by Eckmann (after he replaced Hurwitz' matrices by abstract elements and -1 by an element of order 2) to give a proof of Hurwitz' theorem.

Freudenthal uses a projective geometry over the field of two elements and Desargues' theorem to prove Hurwitz' theorem and Chevalley uses Clifford algebras. An account of this and connected ideas are in a paper by van der Blij.

Later Albert, Kaplansky, and Jacobson imbedded the problem into the study of composition algebras. We start by defining a normed algebra. Let $e_1, \cdots, e_n$ be a basis for the algebra. Let

$$a = a_1e_1 + \cdots + a_ne_n$$

be an element of the algebra. Define

$$\text{norm } a = |a| = \sum a_i^2.$$

The algebra will be called normed, if

$$|ab| = |a||b|.$$

If the algebra is over the reals, has an identity and is normed then it can be shown that it is either the reals, the complex field, the quaternions or the Cayley numbers. This gives a proof for the Hurwitz theorem. Jacobson treated a more general situation. He starts with a quadratic form $N(x)$ defined on a vector space V over a field of characteristic $\neq 2$. He assumes that $N(x)$ permits composition, i.e., there exists a bilinear composition xy in V such that

$$N(x)N(y) = N(xy), \qquad x, y \in V.$$

The product xy makes an algebra out of V which is then called a composition algebra. However, Albert had shown that forms of dimension 2^n permit composition even for fields of characteristic 2.

The Hilbert identities

$$\left(\sum_1^r x_i^2\right)^m = \sum \rho_k(a_{1k}x_1 + \cdots + a_{rk}x_k)^{2m}$$

with ρ_k positive rationals and a_{ik} integers were used in Hilbert's original solution of the Waring problem, i.e., the proof of the following assertion: every positive integer is a sum of n-th powers of integers and the number of these is determined solely by n. A simpler proof of the identities goes back to Hausdorff. They have the flavour of a composition identity and could possibly be generalized for products

$$\sum x_i^2 \sum y_i^2 \cdots .$$

The associative algebras among the above-mentioned four algebras over the reals are characterized by other properties, e.g., Pontryjagin obtains them from topological properties of fields in which addition and multiplication are continuous functions under some topology. The Gelfand-Mazur theorem states that they are the only normed algebras which are also fields. They will be discussed further in the next chapter.

7. Division algebras over the reals, n-dimensional spheres, n-dimensional Laplace differential equations. Frobenius proved that the reals, the complex numbers and the quaternions are the only division algebras over the reals if commutativity is not required, but associativity retained. In spite of arduous attempts there is still no algebraic proof available for the fact that $n=1, 2, 4, 8$ are the only numbers of base elements for which real division algebras exist, if associativity is not required any longer. The only proofs available so far rely heavily on deep algebraic topology. This approach was initiated by H. Hopf and continued by Stiefel and others with a final break-through by Bott, Kervaire, Milnor, Adams.

The norm in the case of the best known division algebras, the complex numbers, quaternions, Cayley numbers, is the sum of the squares of the coordinates.

The role of these hypercomplex systems in almost any part of mathematics is well known. Quaternions have applications in most abstract parts of mathematics, but also in concrete ones from where they stem. They were introduced by Hamilton and are of great use in theoretical physics, as well as in ring theory, group theory and number theory. If the coordinates are permitted to be complex then the system is no longer a division algebra, but it has other applications. Generalized quaternions are in much use too, they are again algebras with four base elements, but the role of -1 in the products is taken over by other scalars.

In abstract group theory the quaternions are linked with the quaternion group which is the hamiltonian group of lowest order. A hamiltonian group is a non-abelian group, all of whose subgroups are normal. The real group algebra of the quaternion group is homomorphic with the real quaternions.

The norms of these hypercomplex systems link them immediately with the n-dimensional spheres. In particular the fact that no division algebra over the reals with three base elements exists is connected with the fact that the 3-dimensional sphere, the set of triples x_1, x_2, x_3 with $x_1^2+x_2^2+x_3^2=1$, cannot be made into a topological group. The latter result follows easily from Brouwer's fixed point theorem. E. Cartan proved that the n-dimensional sphere is a group space only for $n=1, 2, 4$. It was the study of the topological properties of the higher dimensional spheres which led to the success in the investigation of the real division algebras. That the associative case follows easily from Cartan's result was noticed by Taussky. Recently a new proof of Cartan's result was given by M. Curtis and Dugundji. An earlier proof came from Samelson.

The ring $R[x_1, \cdots, x_n]$ of polynomials in n variables with real coefficients 'modulo the unit sphere', i.e. the ring

$$R[x_1, \cdots, x_n]/(x_1^2 + \cdots + x_n^2 - 1)$$

has been studied in several connections:

Swan showed that a 'unimodular' vector $(x_1, \cdots, x_n)$ over this ring cannot always be completed to a unimodular matrix, unless $n=1, 2, 4$, or 8.

Estes and Butts showed that for $n=3$ composition of quadratic forms is not possible in this ring.

Another subject connected with the classical division algebras is the Laplace differential equation

$$\left(\frac{\partial^2}{\partial x_1^2} + \frac{\partial^2}{\partial x_2^2} + \cdots + \frac{\partial^2}{\partial x_n^2}\right) u = 0.$$

For $n=2$ the Laplace equations for two functions of two real variables are a consequence of the Cauchy-Riemann equations. The question was raised (and answered) by Taussky as to whether an analogous situation exists for other values of n. It turns out this can happen only for $n=2, 4, 8$ and in fact it is a rather simple consequence of the result concerning the division algebras over the reals. However, a purely algebraic proof was obtained by Stiefel subsequently. The 4-dimensional case leads to a set of generalized Cauchy-Riemann equations which were much studied by Fueter and his school for the purpose of generalizing complex function theory. In slightly changed form they appear in theoretical physics as the Dirac equations.

Eichhorn, who had previously contributed to the study of generalized Cauchy-Riemann equations, considered the following more general problem recently: Let X be a vector space over a field F of characteristic $\neq 2$. Let $x \in X$. Consider linear mappings $L(x)$ of X into $\mathrm{Hom}(X, X)$ such that another such mapping exists so that

$$M(x)L(x) = \mu(x)I$$

when I is the identity mapping and $\mu(x) \not\equiv 0$ is a mapping of X into F. The function $\mu(x)$ can be interpreted as a quadratic form and if this form is positive definite and of rank n and X an n-dimensional vector space we are back in the problem of the generalized Cauchy-Riemann equations. However, it is now shown that for any form, whether p.d. or not, as long as it has full rank n, the only possible values of n are 1, 2, 4, 8. But also the case of lower rank $r < n$ is considered. For $n = p2^g$, p odd, Eichhorn obtains $r \leqq 2g+2$. The results are based on the following result: Let $n=p2^g$, p odd. Let F be an arbitrary field of characteristic $\neq 2$. Let A_i, $i=1, \cdots, r-1$, be a set of $n\times n$ matrices with elements in F with the properties: $A_i^2=\alpha_i I$, $\alpha_i\in F$, $\alpha_i\neq 0$ and $A_iA_k+A_kA_i=0$, $i\neq k$. Then $r\leqq 2g+2$.

Connected with this fact is a result by Adams, Lax and Phillips: Let $A_1, \cdots, A_k$ be a set of real $n\times n$ matrices such that $\sum\lambda_iA_i$ is non-singular for all real λ_i, except $\lambda_1=\cdots=\lambda_n=0$. Let $n=2^{b+4c}(2a+1)$, $0\leqq b\leqq 3$. Then $k\leqq 2^b+8c$.

Anticommuting matrices are much connected with the various problems studied in this and the preceding chapter.

Dieudonné studied the following generalization of results by Eddington and by M. H. A. Newman. Let F be a not necessarily commutative field of characteristic $\neq 2$, V an n-dimensional right vector space over F, let σ be an automorphism of F and γ an element of F such that $\gamma^\sigma=\gamma$ and $\xi^\sigma=\gamma^{-1}\xi\gamma$ for $\xi\in F$. Determine the maximal number of semi-linear transformations u_k of V, relative to the automorphism σ, satisfying the relations

$$u_k^2(x) = x\gamma \quad \text{for } x\in V,\ \forall k$$
$$u_hu_k = -u_ku_h \qquad h\neq k.$$

Quaternions and Cayley numbers have many applications in number theory. Lipschitz had studied the ring of quaternions with rational integral coordinates, but Hurwitz later noticed that they do not form a maximal order. By order we understand a subring containing 1 and a basis for the algebra. He constructed the following basis for the maximal order: $(1+i+j+k)/2$, i, j, k. He then studied the factorization of rational primes in this ring. Similar problems have been studied for Cayley numbers by various authors, e.g. Coxeter, Lamont, Linnik, Mahler, Pall, Pall and Taussky, and Rankin.

If $e_1, \cdots, e_n$ ($n=4$, respectively 8) is a basis for an order and $x_1, \cdots, x_n$ indeterminates then

$$(x_1e_1+\cdots+x_ne_n)(x_1\bar{e}_1+\cdots+x_n\bar{e}_n)$$

is the norm form of the order if $\bar{e}_i$ is the conjugate of e_i. The problems associated with these forms can then be studied via the associated orders. Here the work of Brandt was basic and recently Kaplansky, Estes and Pall have made contributions.

8. Positive definite polynomials. This chapter is closely linked with the earlier chapters on number theory and on formally real fields. A positive rational number can be expressed as a sum of squares and Hilbert asked whether a real positive definite polynomial, i.e., one which assumes positive values only, can be expressed as a sum of squares of polynomials or, failing this, whether it can be expressed as a sum of squares of rational functions. He gave an example of a positive definite polynomial which cannot be expressed as a sum of squares of polynomials. Recently Motzkin gave a rather simple example of such a polynomial, namely $(x_1^2+x_2^2-3x_3^2)x_1^2x_2^2+x_3^6$. He found this in connection with a study of inequalities in which he expresses the difference of the two sides as sums of squares. Other examples were found recently by R. Robinson:

$$x^2(x^2-1)^2+y^2(y^2-1)^2-(x^2-1)(y^2-1)(x^2+y^2-1)$$
$$x^2(x-1)^2+y^2(y-1)^2+z^2(z^2-1)^2+2xyz(x+y+z-2).$$

Artin solved Hilbert's question completely, showing that an expression by rational functions does indeed exist. Recently the subject was reactivated by asking for a quantitative result, namely the minimum number of terms and explicit representations. It was shown by Pfister that a definite rational function of n variables in a real closed field is a sum of 2^n squares in this field. This is only an upper bound, but for $n=2$ a smaller number will not suffice. Quite recently Cassels, Ellison and Pfister showed that the Motzkin polynomial is not a sum of 3 squares. The lower bound $n+1$ follows from Cassels' Theorem showing that $1+x_1^2+\cdots+x_n^2$ is not a sum of n squares. Ax had shown earlier that Artin's own work can be used to imply the bound 2^n if a further condition is fulfilled which he showed was in fact true for $n=3$.

For polynomials with integral coefficients the following facts have been studied: If the polynomial assumes square values for all integral arguments then $f(x)$ is itself the square of an integral polynomial. A much deeper result was obtained in a diophantine formulation by Siegel: An integral polynomial, not a square, can attain a square value for a finite number of integral values only. Recently LeVeque generalized the question: if $f(x)$ assumes only values which are sums of two squares, is $f(x)$ a sum of two squared polynomials? This was answered affirmatively by several authors.

9. Sums of squares in Galois theory. The converse problem of Galois theory, namely to find a normal algebraic extension with a given Galois group, leads in some special cases connected with the number 2 to sums of squares. The two following cases will be discussed:

(i) The cyclic group of order 4.

(ii) The quaternion group.

Let k be a given field and F a separable normal extension. In case (i) there exists exactly one quadratic field F_0 between k and F. This field is generated by the square root of an element $\mu\in k$. It can be shown that μ is a sum of two squares in k. Conversely, any sum of two squares occurs in this connection. There are various proofs for this. If μ is a sum of squares in k, say $\mu=\mu_1^2+\mu_2^2$, $\mu_i\in k$, then $F_0=k(\sqrt{\mu_1^2+\mu_2^2})$ has the property that $-1=\text{norm}_{F_0/k}(\rho)$ where $\rho\in F_0$. For, every element in F_0 is of the form $\alpha+\beta\sqrt{\mu_1^2+\mu_2^2}$, α, $\beta\in k$ and the norm of this element is $\alpha^2-\beta^2(\mu_1^2+\mu_2^2)$. This can be made equal to -1 for $\alpha^2=\mu_1^2/\mu_2^2$ and $\beta^2=1/\mu_2^2$. Conversely, if $-1=\text{norm}_{F_0/k}(\rho)$, $\rho\in F_0$, then F_0 is generated by the square root of a sum of two squares. For $k=Q$ it can happen that -1 is even the norm of a unit.

In case (ii) the field F contains three quadratic fields F_1, F_2, F_3 between k

and F. Let F_i be generated by $\sqrt{\mu_i}$, $\mu_i \in k$. Then $\mu_1\mu_2 = \mu^2\mu_3$ where $\mu \in k$. It can be shown by elementary field theory that each μ_i can be represented as a sum of three squares in k. However, two expressions which are sums of three squares do not in general have a product with the same property. Hence μ_1, μ_2 cannot be arbitrary sums of three squares. Pairs of sums of three integers whose product is of the same type can be characterized easily from the known characterization of such integers. Not all such pairs, however, qualify for quaternion fields. A parametric representation for μ_1, μ_2 was given by G. Bucht. The 'sum of three squares' character of such a representation will now be explained (The following treatment is due to Cassels arising out of a discussion with the author.):

The elements μ_1, μ_2 can be obtained as:

$$\mu_1 = \frac{u^2l^2 + s^2u^2 + s^2m^2}{l^2r^2 + l^2v^2 + s^2v^2} = \frac{u^2(l^2 + s^2) + s^2m^2}{v^2(l^2 + s^2) + l^2r^2}$$

$$\mu_2 = \frac{u^2r^2 + m^2r^2 + m^2v^2}{l^2r^2 + l^2v^2 + s^2v^2} = \frac{m^2(r^2 + v^2) + u^2r^2}{l^2(r^2 + v^2) + s^2v^2}.$$

It can be shown, conversely, that any pair of elements μ_1, $\mu_2 \in K$ for which these relations hold have the property that $k(\sqrt{\mu_1}, \sqrt{\mu_2})$ can be extended to a quaternion field. That μ_1 is a sum of three squares follows from the fact that both denominator and numerator are norms in the field generated by $i\sqrt{l^2+s^2}$, hence their quotient is again such a norm, hence clearly a sum of 3-squares. An analogous fact is true for μ_2. Next we show that $\mu_1\mu_2$ is a sum of three squares. Since μ_1, μ_2 have the same denominator we need only worry about the numerators. Both of them are norms of the field generated by $i\sqrt{u^2+m^2}$; hence their product is a norm in this field. Finally, we give an example showing that not every set μ_1, μ_2, $\mu_1\mu_2$, all sums of three squares, comes in question. Take $\mu_1 = 3\cdot 73$, $\mu_2 = 3\cdot 37$. Then

$$\mu_1v^2 + \mu_2l^2 = u^2 + m^2,$$

hence

$$3(73v^2 + 37l^2) = u^2 + m^2. \tag{*}$$

This implies that $u \equiv m = 0(3)$, hence $v^2 + l^2 \equiv 0(3)$, hence $v \equiv l \equiv 0(3)$. Remove a factor 3 from u, m, v, l in (*) and repeat the process. This will finally lead to a contradiction.

A proof for the fact that the μ_i are sums of three squares by non-elementary methods was given by Reichardt.

10. Rational arctangents.*

We now return to a problem concerning the sums of two squares, which, in principle, goes back to Gauss.

* This chapter was written by John Todd.

In elementary trigonometry one encounters relations of the following form:

$$\arctan 239 = 4 \arctan 5 - 5\pi/4$$
$$\arctan 99 = \arctan 12 - 2 \arctan 5 - \arctan 2 + 5\pi/4.$$

We take up the question of generating all such relations or rather a basis for them. (One of the reasons for the study of those relations is to find convenient methods of calculating π.)

We shall write (x) for that value of arctan x between 0 and $\frac{1}{2}\pi$, so that, in particular, $(1) = \pi/4$. We ask, to begin with, can we have relations of the form

$$(2) = r(1)$$
$$(3) = s(1) + t(2),$$

where r, s, t are integers?

Suppose the first relation holds. Then the complex numbers $1+2i$ and $(1+i)^r$ necessarily have the same argument so that their ratio

$$(1 + 2i)/(1 + i)^r$$

is necessarily real. Since the real part of the denominator is an integer, m say, it follows that this ratio must be $1/m$. If we take the squares of the absolute values of each side of the equation

$$m(1 + 2i) = (1 + i)^r$$

we obtain the equation

$$5m^2 = 2^r$$

which manifestly has no solutions.

Similar considerations applied to the second relation lead to the equation

$$10\, m^2 = 2^s 5^t$$

which has a solution $s=3$, $t=1$, $m=2$. This gives us the relation

$$(3) = 3(1) - (2).$$

We now introduce the formal definition: (n) is called reducible if it can be expressed in the form

$$(n) = \sum f_r \cdot (n_r),$$

where the n_r are positive integers less than n and the f_r are integers (it can be shown that no change occurs if we allow the f_r to be rational); if no such relation exists we call (n) irreducible. Thus (2) is irreducible, while (3) is reducible. We find that (4), (5), (6) are irreducible but that

$$(7) = -(1) + 2(2)$$
$$(8) = 5(1) - (2) - (5).$$

Consideration of these examples suggested the following theorem:

THEOREM. *A condition necessary and sufficient for the reducibility of* (m) *is that the largest prime factor* $l(m)$ *of* $1+m^2$ *should be less than* $2m$.

We can verify this in the early cases quoted:

n	$1+n^2$	$l(n)$		$2n$
2	5	5	$>$	4
3	10	5	$<$	6
4	17	17	$>$	8
5	26	13	$>$	10
6	37	37	$>$	12
7	50	5	$<$	14
8	65	13	$<$	16
9	82	41	$>$	18

This theorem can be established constructively by elementary methods: an algorithm for carrying out the reduction of (n) when it is possible can be given, granted that the factorization of $1+r^2$ is known for $r \leqq n$. A listing of the reductions of (n) for $n \leqq 2089$ is available.

The irreducible (n) are analogous to the ordinary prime numbers and it is possible to ask whether there are theorems about them similar to theorems about prime numbers. In the first place there is an analog of Euclid's theorem: there *is* an infinite number of irreducible arctangents. We can also ask whether there is an infinite number of reducible arctangents—this is also true. Both these results are elementary. Gauss conjectured that the number of ordinary prime numbers $<n$ is approximately $n/\log n$ and this "Prime Number Theorem" was proved much later. Observation of the density of the irreducible arctangents suggests that their density is $\log 2 = .6931$—some theoretical evidence in support of this is available, but the result seems very difficult to prove.

It can also be shown that the arctangent of any rational number can be expressed in terms of the irreducible integral arctangents. For instance

$$(100/17) = (6) + (290) - (4836).$$

This work was carried out (in part) under NSF grant 3909 and 11236. The author is indebted for some references to A. A. Albert, D. Estes, I. Kaplansky, G. Pall, J. Robinson.

This is an account of part of a course with the same title given at California Institute of Technology in 1966. It is an extended version of a lecture given at University of California at Santa Barbara and Riverside, at University of Miami and Rice University.

References to 1

1. L. Henkin, Sums of squares, in Summer Institute for symbolic logic, Cornell University 1957, 2nd edition, IDA, (1962) 284–291.

2. I. Kaplansky, Theory of fields, unpublished manuscript, 1970.

3. G. Kreisel, Sums of squares, in Summer Institute for symbolic logic, Cornell University 1957, 2nd edition, IDA, (1962) 313–320.

4. A. Robinson, On ordered fields and definite functions, Math. Ann., 130 (1955) 257–271; 405–409.

5. ———, Introduction to model theory and to the metamathematics of algebra, North Holland, Amsterdam, 1965.

6. J. Robinson, Existential definiability in arithmetic Trans. Amer. Math. Soc. 72, (1952) 437–444.

7. ———, The decision problem for fields, in Symposium on the theory of models, North Holland, Amsterdam, 1965.

8. R. M. Robinson, The undecidability of pure transcendental extensions of real fields, Z. Math. Logik Gunrdlagen Math., 10 (1964) 275–282.

9. A. Tarski and J. C. C. McKinsey, A decision method for elementary algebra and geometry, University of Calif. Press, Berkeley, 1951.

10. O. Taussky, Sums of Squares, Matematička Biblioteka, Beograd, 41 (1969) 19–27.

11. F. van der Blij, History of the octaves, Simon Stevin, 34 (1960/61) 106–125.

References to 2

1. J. P. Ballantine and D. E. Brown, Pythagorean sets of numbers, this MONTHLY, 45 (1938) 298–301.

2. F. J. M. Barning, On Pythagorean and quasi-Pythagorean triangles and a generation process with the help of unimodular matrices, Math. Centrum Amsterdam, 1963.

3. F. Gross, On the equation $f^n+g^n=h^n$, this MONTHLY, 73 (1966) 1093–1096.

4. G. Iyer, On certain functional equations, J. Indian Math. Soc., 3 (1939) 312–315.

5. J. Mariani, The group of the Pythagorean numbers, this MONTHLY, 69 (1962) 125–128.

6. O. Neugebauer and A. Sachs, Mathematical cuneiform texts, New Haven, 1945.

7. N. E. Sexauer, Pythagorean triples over Gaussian domains, this MONTHLY, 73 (1966) 829–834.

8. W. Sierpiński, Pythagorean triangles, Yeshiva University, New York, 1962.

9. O. Taussky, A generalization of the Pythagorean forms, to be published.

10. H. Zassenhaus, What is an angle?, this MONTHLY, 61 (1954) 369–378.

References to 3

1. P. Bateman, Problem E2051, this MONTHLY, 76 (1969) 190–191.

2. E. Bender, Classes of matrices over an integral domain, Illinois J. Math., 11 (1967) 697–702.

3. ———, Classes of matrices and quadratic fields, Linear Algebra and Appl., 1 (1968) 195–201.

4. ———, Characteristic polynomials of symmetric matrices, Pacific J. Math., 25 (1968) 433–441.

5. H. Cohn, Decomposition into four integral squares in the fields of $\sqrt{2}$, $\sqrt{3}$, Amer. J. Math., 82 (1960) 301–322.

6. C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, New York, 1962.

7. L. E. Dickson, Integers represented by positive ternary quadratic forms, Bull. Amer. Math. Soc., 33 (1927) 63–70.

8. J. D. Dixon, Another proof of Lagrange's four square theorem, this MONTHLY, 71 (1964) 286–88.

9. J. Dzewas, Quadratsummen in reell-quadratischen Zahlkörpern, Math. Nachr., 21 (1960) 233–284.

10. D. K. Faddeev, On the characteristic equations of rational symmetric matrices, Doklady Akad. Nauk. SSSR, 58 (1947) 753–754.

11. O. Fraser and B. Gordon, On representing a square as the sum of three squares, this MONTHLY, 76 (1969) 922–923.

12. P. R. Halmos, Note on almost-universal forms, Bull. Amer. Math. Soc., 44 (1938) 141–144.

13. H. Heilbronn, On the representation of a rational as a sum of four squares by means of regular functions, J. London Math. Soc., 39 (1964) 72–76.

14. H. Maass, Über die Darstellung totalpositiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten, Abh. Math. Sem. Univ. Hamburg, 14 (1941) 185–191.

15. ———, Modulformen und quadratische Formen über dem quadratischen Zahlkörper $R(\sqrt{5})$, Math. Ann., 118 (1941) 65–84.

16. M. Newman, Subgroups of the modular group and sums of squares, Amer. J. Math., 82 (1960) 761–778.

17. G. Pall, On sums of squares, this MONTHLY, 40 (1933) 10–18.

18. S. Ramanujan, On the expression of a number in the form $ax^2+by^2+cz^2+du^2$, Proc. Cambridge Phil. Soc., 19 (1917) 11–21.

19. R. A. Rankin, On the representation of a number as the sum of any number of squares, and in particular of twenty, Acta Arith., 7 (1962) 399–407.

20. A. P. Sapiro, Characteristic polynomials of symmetric matrices, Sibirsk Mat. Z., 3 (1962) 280–291.

21. C. L. Siegel, Darstellung total positiver Zahlen durch Quadrate, Math. Z., 11 (1921) 246–275.

22. O. Taussky, On matrix classes corresponding to an ideal and its inverse, Illinois J. Math., 1 (1957) 108–113.

23. ———, Classes of matrices and quadratic fields, Pacific J. Math., 1 (1951) 127–132.

24. ———, Classes of matrices and quadratic fields II, J. London Math. Soc., 27 (1952) 237–239.

25. R. C. Thompson, Problem E1814, this Monthly, 72 (1965) 782; (1967) 200.

References to 4

1. C. S. Ballantine, Products of positive definite matrices III, J. Algebra, 10 (1968) 174–182.

2. ———, A note on the matrix equation $H=AP+PA^*$, Linear Algebra and Appl., 2 (1969) 37–47.

3. ———, Products of positive definite matrices II, to appear.

4. K. Barner, Über die quaternäre Einheitsform in total reellen algebraischen Zahlkörpern, J. Reine Angew. Math., 229 (1968) 194–208.

5. G. Birkhoff, Linear transformations and invariant cones, this MONTHLY, 74 (1967) 274–276.

6. E. Calabi, Linear systems of real quadratic forms, Proc. Amer. Math. Soc., 15 (1964) 844–846.

7. D. H. Carlson, On real eigenvalues of complex matrices, Pacific J. Math., 15 (1965) 1119–1129.

8. P. Erdös and Ch. Ko, On definite quadratic forms, which are not the sum of two definite or semidefinite forms, Acta Arith., 3 (1939) 102–122.

9. D. Estes and G. Pall, The definite octonary quadratic forms of determinant 1, Illinois J. Math., 14(1970) 159–163.

10. M. Fiedler and V. Pták, Some generalizations of positive definiteness and monotonicity, Numer. Math., 9 (1966) 163–172.

11. W. Givens, Fields of values of a matrix, Proc. Amer. Math. Soc., 3 (1952) 206–209.

12. C. Hermite, Lettres de M. Hermite à M. Jacobi, 2nd letter, in Oeuvres 1, Gauthier-Villars, Paris, 1905, 122–135.

13. M. R. Hestenes, Pairs of quadratic forms, Linear Algebra and Appl., 1(1968) 397–407.

14. M. Kneser, Klassenzahlen definiter quadratischer Formen, Archiv Math., 8 (1957) 241–250.

15. ———, unpublished.

16. Ch. Ko, On the representation of a quadratic form as a sum of squares of linear forms, Quart. J. Math. Oxford, 8 (1937) 81–98.

17. ———, Determination of the class number of positive quadratic forms in nine variables with determinant unity, J. London Math. Soc., 13 (1938) 102–110.

18. ———, On the positive definite quadratic forms with determinant unity, Acta Arith., 3 (1939) 75–85.

19. M. Koecher, Positivitätsbereiche im R^n, Amer. J. Math., 53 (1957) 575–596.

20. A. Korkine and G. Zolotareff, Sur les formes quadratiques positives, Math. Ann., 11 (1877) 242–292.

21. A. Lyapunov, Problème général de la stabilité du mouvement, Commun. Soc. Math., Kharkov, (1892), (1893).

22. W. Magnus, Über die Anzahl der in einem Geschlecht enthaltenen Klassen von positiv definiten quadratischen Formen, Math. Ann., 114 (1937) 465–475; Berichtigung, Math. Ann., 115 (1938) 643–644.

23. J. Milnor, in W. H. Greub, Linear Algebra, Academic Press, New York, 1965.

24. H. Minkowski, Mémoire sur la théorie des formes quadratiques à coefficients entiers, Ges. Abh. 1, Chelsea, New York, 1967. 1–144.

25. L. J. Mordell, A new Waring problem with squares of linear forms, Quart. J. Math. Oxford, 4 (1930) 276–280.

26. ———, The definite quadratic forms in eight variables with determinant unity, J. Math. Pure Appl., 17 (1938) 41–46.

27. M. Newman and O. Taussky, On a generalization of the normal basis in abelian algebraic number fields, Commun. Pure Appl. Math., 9 (1956) 85–91.

28. ——— and ———, Classes of definite unimodular circulants, Canadian Math. J., 9 (1956) 71–73.

29. D. G. Quillen, On the representation of hermitian forms as sums of squares, Invent. Math., 5 (1968) 237–242.

30. R. Redheffer, Remarks on a paper of Taussky, J. Algebra, 2 (1965) 42–47.

31. H. Schneider, Positive operators and an inertia theorem, Numer. Math., 7 (1965) 11–15.

32. P. Stein, Some general theorems on iterants, J. Res. Nat. Bur. Standards, 48 (1952) 82–83.

33. ———, On the range of two functions of positive definite matrices, J. Algebra, 2 (1965) 350–353.

34. ——— and A. Pfeffer, On the ranges of two functions II, ICC Bull., 6 (1967) 81–86.

35. O. Taussky, Automorphs and generalized automorphs of quadratic forms treated as characteristic value relations, Linear Algebra and Appl., 1 (1968) 349–356.

36. ———, Unimodular integral circulants, Math. Z., 63 (1955) 286–289.

37. ———, Problem 4846, this MONTHLY, 66 (1959) 427.

38. ———, Positive definite matrices and their role in the study of the characteristic roots of general matrices, Advances in Math., 2 (1968) 175–186.

39. ———, Matrices C with $C^n \to 0$, J. Algebra, 1 (1964) 5–10.

40. ———, Matrix Theory Research Problem, Bull. Amer. Math. Soc., 71 (1965) 711.

41. ———, Positive definite matrices in 'Inequalities', O. Shisha, Ed., Academic Press, 1967.

42. ———, Stable Matrices in 'Programmation en Analyse Numérique,' J. L. Rigal, Ed., Cahiers Centre Math. Rech. Sci. 1968.

43. R. C. Thompson, Unimodular group matrices with rational integers as elements, Pacific J. Math., 14 (1964) 719–726.

44. ———, Classes of definite group matrices, Pacific J. Math., 17 (1966) 175–190.

45. B. L. van der Waerden, Die Reduktionstheorie der positiven quadratischen Formen, Acta Math., 96 (1956) 265–309.

46. E. P. Wigner, On weakly positive matrices, Canadian J. Math., 15 (1965) 313–317.

47. ——— and M. M. Yanase, On the positive semidefinite nature of a certain matrix expression, Canadian J. Math., 16 (1964) 397–406.

48. M. Wonenburger, Simultaneous diagonalization of symmetric bilinear forms, J. Math. Mech., 15 (1966) 617–622.

49. Yik-Hoi Au Yeung, A theorem on a mapping from a sphere to the circle and the simultaneous diagonalization of two hermitian matrices, Proc. Amer. Math. Soc., 20 (1969) 545–548.

50. ———, Some theorems on the real pencil and diagonalization of two hermitian bilinear functions, Proc. Amer. Math. Soc., 23 (1969) 246–254.

References to 5

1. E. Artin and O. Schreier, Algebraische Konstruktion reeller Körper, Abh. Math. Sem. Univ. Hamburg, 5 (1926) 83–115.

2. E. Bender, The dimensions of symmetric matrices with a given minimum polynomial, Linear Algebra and Appl. To appear.

3. J. W. S. Cassels, On the representation of rational functions as sums of squares, Acta Arith., 9 (1964) 79–82.

4. ———, Représentations comme somme de carrés, Les tendances géométriques en algèbre et théorie des nombres, 55–65, Paris, 1966.

5. P. Chowla, On the representation of -1 as a sum of squares in a cyclotomic field, J. Number Theory, 1 (1969) 208–210.

6. B. Fein and B. Gordon, On the representation of -1 as a sum of two squares in an algebraic number field, J. Number Theory, to appear.

7. H. Kneser, Verschwindende Quadratsummen in Körpern, Jber. Deutsch. Math.-Verein, 44 (1934) 143–146.

8. F. Krakowski, Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern, Comment. Math. Helv., 32 (1958) 224–240.

9. A. Pfister, Zur Darstellung von -1 als Summe von Quadraten in einem Körper, J. London Math. Soc., 40 (1965) 159–165.

10. J.-P. Serre, Extension de corps ordonnes, C. R. Acad. Sci. Paris, 229 (1949) 576–577.

11. J. Smith, The equation $-1=x^2+y^2$ in certain number fields, J. Number Theory, to appear.

12. R. C. Thompson, Commutators in the special and general linear groups, Trans. Amer. Math. Soc., 101 (1961) 16–33.

13. B. L. van der Waerden, Problem, Jber. Deutsch. Math-Verein, 42 (1932) 71.

14. ———, Modern Algebra I, Frederick Ungar, New York, 1966.

References to 6

1. A. A. Albert, Quadratic forms permitting composition, Ann. Math. (2), 43 (1942) 161–177.

2. ———, Quadratic forms permitting composition, unpublished manuscript, 1962.

3. H. Brandt, Der Kompositionsbegriff bei den quaternären quadratischen Formen, Math. Ann., 91 (1924) 300–315.

4. C. Chevalley, The algebraic theory of spinors, Columbia University Press, New York, 1954.

5. C. W. Curtis, The four and eight square problem and division algebras, in Studies in Modern Algebra 2, A. A. Albert, ed., (1963) 100–125.

6. J. Dieudonné, A problem of Hurwitz and Newman, Duke Math. J., 20 (1953) 381–389.

7. B. Eckman, Gruppentheoretischer Beweis der Satzes von Hurwitz-Radon über die Komposition der quadratischen Formen, Comment. Math. Helv., 15 (1942/3), 358–366.

8. H. Freudenthal, Oktaven, Ausnahmegruppen und Oktavengeometrie, Utrecht, 1951.

9. M. Gerstenhaber, On semicommuting matrices, Math. Z., 83 (1964) 250–260.

10. F. Hausdorff, Zur Hilbertschen Lösung des Waringschen Problems, Math. Ann., 67 (1909) 301–305.

11. A. Hurwitz, Über die Komposition der quadratischen Formen, Math. Ann., 88 (1923) 1–25.

12. N. Jacobson, Composition algebras and their automorphisms, Rend. Circ. Mat. Palermo 7, (1958) 55–80.

13. P. Jordan, J. von Neumann and E. Wigner, On an algebraic generalization of the quantum mechanical formalism, Ann. Math., 2 (1934) 29–64.

14. I. Kaplansky, Composition of binary quadratic forms, Studia Math., 31 (1968) 85–92.

15. ———, Infinite-dimensional quadratic forms permitting composition, Proc. Amer. Math. Soc., 4 (1953) 956–96.

16. P. Kustaanheimo and E. Stiefel, Perturbation theory of Kepler motion based on spinor regularization, J. Reine Angew. Math., 218 (1965) 204–219.

17. K. McCrimmon, A proof of Schafer's conjecture for infinite dimensional forms admitting composition, J. Algebra, 5 (1967) 72–83.

18. M. H. A. Newman, Note on an algebraic theorem of Eddington, J. London Math. Soc., 7 (1932) 93–99.

19. A. Pfister, Multiplikative quadratische Formen, Archiv Math., 16 (1965) 363–370.

20. J. Putter, Maximal sets of anti-commuting skew-symmetric matrices, J. London Math. Soc., 42 (1967) 303–308.

21. R. D. Schafer, Forms permitting composition, Advances in Math., 4 (1970) 127–148.

22. W. Scharlau, Quadratische Formen und Galois-Cohomologie, Invent. Math., 4 (1967) 238–264.

23. O. Taussky, A determinantal identity for quaternions and a new eight square identity, J. Math. Anal. Appl., 15 (1966) 162–164.

24. B. Walsh, The scarcity of cross products on euclidean spaces, this MONTHLY, 74 (1967) 188–194.

25. H. Zassenhaus and W. Eichhorn, Herleitung von acht- und sechzehn-Quadrate–Identitäten mit Hilfe von Eigenschaften der verallgemeinerten Quaternionen und der Cayley-Dicksonschen Zahlen, Archiv Math., 17 (1966) 492–496.

References to 7

1. J. F. Adams, Vector fields on spheres, Ann. Math., 75 (1962) 603–632.

2. ———, P. D. Lax and R. S. Phillips, On matrices whose real linear combinations are non-singular, Proc. Amer. Math. Soc., 16 (1965) 318–322; Proc. Amer. Math. Soc., 17 (1966) 945–947.

3. A. A. Albert, Absolute-valued real algebras, Ann. Math., 48 (1947) 495–501.

4. ———, Absolute-valued real algebras, Bull. Amer. Math. Soc., 55 (1949) 763–768.

5. R. Arens, Linear topological division algebras, Bull. Amer. Math. Soc., 53 (1947) 623–630.

6. M. F. Atiyah, The role of algebraic topology in mathematics, J. London Math. Soc., 41 (1966) 63–69.

7. F. A. Behrens, Über Systeme reeller algebraischer Gleichungen, Composito Math., 7 (1939) 1–19.

8. G. Benneton, Sur l'arithmétique des quaternions et des biquaternions, Ann. Sci. École Norm. Sup., (3), 60 (1943) 173–214.

9. R. Bott and J. Milnor, On the parallelizability of the spheres, Bull. Amer. Math. Soc., 64 (1958) 87–89.

10. H. Butts and D. Estes, Modules and binary quadratic forms over integral domains, Linear Algebra and Appl., 1 (1968) 153–180.

11. H. Cohn and G. Pall, Sums of four squares in a quadratic ring, Trans. Amer. Math. Soc., 105 (1962) 536–556.

12. H. S. M. Coxeter, Integral Cayley numbers, Duke Math. J., 13 (1946) 561–578.

13. M. L. Curtis and J. Dugundji, Groups which are cogroups, manuscript.

14. L. E. Dickson, On quaternions and their generalizations and the history of the eight square theorem, Ann. Math., 20 (1919) 155–171.

15. W. Eichhorn, Funktionalgleichungen in Vektorräumen, Kompositionsalgebren und Systeme partieller Differentialgleichungen, Aequationes Math., 2(1969) 287–303.

16. D. Estes and G. Pall, Modules and rings in the Cayley algebra, J. Number Theory, 1 (1969) 163–178.

17. R. Fueter, Die Theorie der regulären Funktionen einer Quaternionenvariablen, Comptes Rendus du congrès int. des mathématiciens, Oslo, 1936, 75–91.

18. I. Gelfand. Normierte Ringe, Mat. Sbornik N. S. 9 (51) (1941) 3–24.

19. J. W. Givens, Tensor coordinates of linear spaces, Ann. Math., 38 (1937) 355–385.

20. W. R. Hamilton, Mathematical papers, Vol. III, Algebra, Cambridge, 1967.

21. H. Hopf, Ein topologischer Beitrag zur reellen Algebra, Comm. Math. Helv., 13 (1941) 219–239.

22. A. Hurwitz, Über die Zahlentheorie der Quaternionen, Ges. Abh., 2, Birkhäuser, 1933, 303–330.

23. N. Jacobson and O. Taussky, Locally compact rings, Proc. Nat. Acad. Sci. USA, 21 (1935) 106–108.

24. I. Kaplansky, Submodules of quaternion algebras, Proc. London Math. Soc., 19 (1969) 219–232.

25. M. Kervaire, Non-parallelizability of the n-sphere for $n>7$, Proc. Nat. Acad. Sci. USA, 14 (1958) 280–283.

26. H. Kestelman, Anticommuting linear transformations, Canadian J. Math., 13 (1961) 614–624.

27. P. J. C. Lamont, Arithmetics in Cayley's algebra, Proc. Glasgow Math. Assoc., 6 (1963) 99–106.

28. Yu. U. Linnik, Quaternions and Cayley numbers; some applications of the arithmetic of quaternions, Uspehi Mat. Nauk (N.S.) 4 (33) (1949) 49–98.

29. ———, Quaternions and Cayley numbers, Math. Centrum Amsterdam, Rapport ZW-1951-002, 1951.

30. R. Lipschitz, Recherches sur les transformations, par des substitutions réelles d'une somme de deux ou de trois carrés en elle-même, J. Math. Pures Appl., 4, 2 (1886) 373–439.

31. D. Lissner, Outer product rings, Trans. Amer. Math. Soc., 116 (1965) 526–535.

32. K. Mahler, On ideals in the Cayley-Dickson algebra, Proc. Roy. Irish Acad. (A), 48 (1943) 123–133.

33. S. Mazur, Sur les anneaux linéaires, C. R. Acad. Sci. Paris, 207 (1938) 1025–1027.

34. G. Pall, On generalized quaternions, Trans. Amer. Math. Soc., 59 (1946) 280–332.

35. G. Pall and O. Taussky, Applications of quaternions to the representations of binary quadratic form as a sum of four squares, Proc. Roy. Irish Acad. (A), 58 (1957), 23–38.

36. ——— and O. Taussky, Factorization of Cayley numbers, J. Number theory, 2 (1970) 74–90.

37. L. S. Pontryagin, Topological groups; Topological groups, Transl. by A. Brown, Gordon and Breach, New York, 1966.

38. J. Radon, Lineare Schären orthogonaler Matrizen, Abh. Math. Sem. Univ. Hamburg, 1 (1922) 1–14.

39. R. A. Rankin, A certain class of multiplicative functions, Duke Math. J., 13 (1946) 281–306.

40. H. Samelson, Über die Sphären, die als Gruppenräume auftreten, Comm. Math. Helv., 13 (1940/41) 149–155.

41. E. Stiefel, Richtungsfelder und Fernparallelismus in n-dimensionalen Mannigfaltigkeiten, Comm. Math. Helv., 8 (1935/6) 3–51.

42. ———, On Cauchy-Riemann equations in higher dimensions, J. Res. Nat. Bur. Standards, 48 (1952) 395–398.

43. M. H. Stone, On the theorem of Gelfand-Mazur, Ann. Polon. Math., 24 (1952) 238–240.

44. R. G. Swan, Vector bundles and projective modules, Trans. Amer. Math. Soc., 105 (1962) 264–277.

45. O. Taussky, Analytical methods in hypercomplex systems, Compositio Math., 3 (1936) 399–407.

46. ———, An algebraic property of Laplace's differential equation, Quart. J. Math. Oxford, 10 (1939) 99–103.

47. ———, (1, 2, 4, 8)-sums of squares and Hadamard matrices, Proc. Symp. on Combinatorics, Los Angeles, 1968, to appear.

48. L. Tornheim, Normed fields over the real and complex numbers, Michigan Math. J., 1 (1952) 61–68.

49. F. van der Blij and T. A. Springer, The arithmetics of octaves of the group G_2, Nederl. Akad. Wetensch. Proc., 62A (1959) 406–418.

50. F. Wright, Absolute valued algebras, Proc. Nat. Acad. Sci. USA, 39 (1953) 330–332.

51. ———, Absolute valued algebras, Proc. Amer. Math. Soc., 11 (1960) 861–866.

References to 8

1. E. Artin, Über die Zerlegung definiter Funktionen in Quadrate, Abh. Math. Sem. Univ. Hamburg, 5 (1926) 100–115.

2. J. Ax, On ternary definite rational functions, Proc. London Math. Soc., to appear.

3. L. Carlitz, Sums of squares of polynomials, Duke Math. J., 3 (1937), 1–7.

4. D. W. Dubois, Note on Artin's solution of Hilbert's 17th problem, Bull. Amer. Math. Soc., 73 (1967) 540–541.

5. W. Habicht, Über die Zerlegung strikt definiter Formen in Quadrate, Comment. Math. Helv., 12 (1946) 317–322.

6. ———, Zerlegung strikte definiter Formen in Quadrate, Comment. Math. Helv., 12 (1940) 317–322.

7. D. Hilbert, Über die Darstellung definiter Formen als Summe von Formenquadraten, Ges. Abh. 2, Springer, Berlin, 1933, 154–161.

8. ———, Mathematische Probleme, in particular problem 17, Ges. Abhandlungen III, Springer, Berlin, 1935, 290–329.

9. E. Landau, Über die Darstellung definiter Funktionen als Summe von Quadraten, Math. Ann., 62 (1906) 272–285.

10. T. S. Motzkin, Algebraic inequalities, in Inequalities, Ed. O. Shisha, Academic Press, New York, 1967, 199–203.

11. A. Pfister, Zur Darstellung definiter Funktionen als Summe von Quadraten, Invent. Math., 4 (1967), 229–237.

12. R. M. Robinson, Some definite polynomials which are not sums of squares of real polynomials (abstract), Notices, Amer. Math. Soc., 16 (1969) 554.

References to 9

1. Gösta Bucht, Arkiv. Math. Astron. and Physik. 6, No. 30.

2. H. Reichardt, Über Normalkörper mit Quaternionengruppe, Math. Z., 41 (1936) 218–221.

3. B. L. van der Waerden, Problem, Jber. Deutsch. Math.-Verein., 43 (1933) 61.

References to 10

1. S. D. Chowla and John Todd, The density of reducible integers, Canadian J. Math., 1 (1949) 297–299.

2. D. H. Lehmer, On arccotangent relations for π, this MONTHLY, 45 (1938) 657–664.

3. John Todd, A problem on arctangent relations, this MONTHLY, 56 (1949) 517–528.

4. ———, Table of arctangents of rational numbers, National Bureau of Standards, Applied Math. Series, No. 11 (1951–1965), U. S. Government Printing Office, Washington, D. C.

This list is not intended to be complete in any respect.