From sums of squares in fields to motivic cohomology and higher class field theory

Jean-Louis Colliot-Thélène

C.N.R.S., Université Paris-Sud

Kloostermanlezing, 21 april 2011

Fermat conjectured that any positive integer is a sum of four squares of integers.

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

Euler proved the statement in rationals.
L. Euler, Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum, N. Comm. Ac. Petrop. 5 (1754/5), 1760., p. 13-58.
The statement in integers was proved by Lagrange, 1770

Representation by an arbitrary form $\sum_i a_i X_i^2$.

H. Hasse, Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, J. Crelle, 1923

Hendrik Douwe Kloosterman, Over het splitsen van geheele positieve getallen in een some van kwadraten, Thesis (1924) Universiteit Leiden, published in Groningen.
Hendrik Douwe Kloosterman, On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$, Acta Mathematica 49 (1926), 407-464 (key point : 'fundamental lemma').

There are local obstructions, which show up in the "singular series". Kloosterman establishes a Hardy-Littlewood formula for the number of representations of n and then gives sufficient conditions on the a, b, c, d so that any sufficiently big integer is represented.

In this lecture I want to present a result in the spirit of Euler's and Hasse's results. Namely :

In the field $\mathbf{Q}(x_1, \ldots, x_n)$, $n \geq 2$, and more generally in a function field in n variables over $\mathbf{Q}$, any positive rational function may be written as a sum of 2^{n+1} squares.

This builds upon earlier work of Pfister over the reals. For $n = 1$, an upper bound is 8.
The universal bound 2^{n+1} was predicted by U. Jannsen and myself in 1991, building upon two conjectures which it took quite a few years to turn into theorems.
The proof of the first, purely algebraic conjecture, is the outcome on work on motivic cohomology (V. Voevodsky et al.)
The proof of the second, arithmetic, conjecture, is a chapter in higher class field theory (U. Jannsen, S. Saito).

Questions around Hilbert's 17th problem

In a field F

Characterize sums of squares

Decide if there exists an integer $n = n(F)$ such that each sum of squares in F may be written as a sum of at most n squares.

Sums of squares in a field F

$$\boxed{\text{n}} + \boxed{\text{m}} = \boxed{\text{n+m}}$$

(in any ring)

$$\boxed{\text{n}} . \boxed{\text{m}} = \boxed{\text{nm}}$$

(in any commutative ring)

$$\boxed{\text{n}} / \boxed{\text{m}} = \boxed{\text{nm}}.$$

(in any field)

$F = \mathbf{R}(x)$
$f \geq 0$ on $\mathbf{R}$ wherever defined $\Longrightarrow f = \boxed{2}$

Proof : decomposition into simple factors and identity

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2$$

hence

$$\boxed{2} . \boxed{2} = \boxed{2\ }$$

$F = \mathbf{Q}$

Characterisation of of sums of 2 squares (Fermat)

$f \geq 0 \Longrightarrow f = \boxed{4}$ (Euler, 1770)

Proof : Conics over a finite field $\mathbf{F}_p$ have a rational point (counting argument) and identity (in any commutative ring)

$$(x_1^2 + y_1^2 + z_1^2 + t_1^2)(x_2^2 + y_2^2 + z_2^2 + t_2^2) =$$
$$(x_1x_2 + y_1y_2 + z_1z_2 + t_1t_2)^2 + (x_1y_2 - y_1x_2 + t_1z_2 - z_1t_2)^2 +$$
$$(x_1z_2 - z_1x_2 + y_1t_2 - t_1y_2)^2 + (x_1t_2 - t_1x_2 + z_1y_2 - y_1z_2)^2$$

hence

$$\boxed{4}.\boxed{4} = \boxed{4\ }$$

Characterisation of sums of 3 squares (Legendre 1798, Gauß)

$F = \mathbf{R}(x,y)$
$f \in \mathbf{R}(x,y), \;\; f \geq 0 \;\text{ on }\; \mathbf{R}^2$ wherever defined $\Longrightarrow f = \boxed{4}$
(Hilbert, 1893)

Proof (very long) : A version of what is now recognized as a special case of Tsen's theorem, and identity $\boxed{4}.\boxed{4} = \boxed{4}$

1900 : Hilbert's 17th problem

Kann jede rationale Funktion, die überall, wo sie definiert ist, nichtnegative Werte annimmt, als Summe von Quadraten von rationalen Funktionen dargestellt werden ?

Analogous question for $f \in \mathbf{Q}(x_1, \ldots, x_n)$

Natural question : for a sum of squares in such a field, is there an upper bound on the number of squares required ?

$F = \mathbf{Q}(x)$

$f \in F, f \geq 0 \implies f = \boxed{8}$

(Landau, 1906)

Tools :

$\boxed{8} . \boxed{8} = \boxed{8\ }$

(in any commutative ring)

and

in a totally imaginary number field, $-1 = \boxed{4}$

E. Artin, O. Schreier, 1927

In a field, an element is a sum of squares if and only if it is positive for each total order of the field.

(Zorn type of argument)

E. Becker (1979)
Let n be an even integer. In a field F, an element f is sum of n-th powers if and only if
(1) It is a sum of squares, and
(2) for any Krull valuation v on the field F with formally real residue field (i.e. -1 not a sum of squares in the residue field), n divides the valuation of $v(f)$.

Example : For n even, $(\sum_{i=1}^{r} X_i^n)^m$ is a sum of nm-th powers in $\mathbf{Q}(X_1, \ldots, X_r)$.
Ancester : Hilbert's solution of Waring's problem

E. Artin, 1927
Solution of Hilbert's 17th problem :

If a polynomial $P(x_1, \dots, x_n) \in \mathbf{R}[x_1, \dots, x_n]$ is positive on $\mathbf{R}^n$ then it is a sum of squares in $\mathbf{R}(x_1, \dots, x_n)$

More generally, if X is an irreducible algebraic variety over the reals, and if a rational function f on X is positive on the set $X(\mathbf{R})$ of real points wherever it is defined, then f is a sum of squares in the field of functions $\mathbf{R}(X)$.
Artin shows : f positive on $X(\mathbf{R})$ implies $f \in \mathbf{R}(X)$ positive for all orderings.

Same statements with $\mathbf{Q}$ in place of $\mathbf{R}$.

E. Witt, 1934

If X is an irreductible curve over $\mathbf{R}$, then any rational function $f \in \mathbf{R}(X)$ which is positive on $X(\mathbf{R})$ is a sum of 2 squares in $\mathbf{R}(X)$.

Uses Tsen 1933 and computations of Weichold on the action of complex conjugation on periods.

Tsen, 1936

Over $\mathbf{C}(x_1, \ldots, x_n)$, and more generally over the function field $\mathbf{C}(X)$ of an n-dimensional variety X over the complex field $\mathbf{C}$, any form of degree d in at least $d^2 + 1$ variables has a nontrivial zero.

1933 for $n = 1$

1936 for arbitrary n, rediscovered by S. Lang 1953

Recent far reaching extension : rationally connected varieties over a function field (over $\mathbf{C}$) in one variable (Graber, Harris, Starr)

E. Witt, 1937

Theory of quadratic forms over an arbitrary field
Simplification theorem
An early version of the notion of Grothendieck group (legend has it that it was taught to him by his Chinese nanny) :
The Witt group $W(F)$ of nondegenerate quadratic forms over a field F modulo hyperbolics. This is actually a ring.
Fundamental ideal $IF \subset W(F)$ of even rank forms.
Powers I^nF of this ideal. Generators : n-fold Pfister forms

$$\langle\langle a_1, a_2, ..., a_n \rangle\rangle, \quad a_i \in F^\times$$

A. Pfister

1965-1966 : Theory of multiplicative quadratic forms
In a *field* F, the set of nonzero values taken by

$$\langle\langle a_1, a_2, ..., a_n\rangle\rangle = \langle 1, -a_1\rangle \otimes \langle 1, -a_2\rangle \otimes ... \otimes \langle 1, -a_mn\rangle$$

is a subgroup of the multiplicative group $F^\times$.

In particular, in a field, $\boxed{\text{m}}.\boxed{\text{m}} = \boxed{\text{m}}$ for any $m = 2^n$.

Properties of the above forms : if isotropic, then hyperbolic.

Theorem (Arason–Pfister 1971) If the class of an anisotropic form q over a field F lies in I^nF, then the dimension of q is at least 2^n.

A. Pfister

1967-1971
Let X be an irreducible $\mathbf{R}$-variety of dimension n. If $f \in \mathbf{R}(X)$ is positive on $X(\mathbf{R})$ wherever it is defined, then f is a sum of 2^n squares in $\mathbf{R}(X)$.

J. W. S. Cassels, 1964

$1 + x_1^2 + \cdots + x_n^2$ is not a sum of n squares in $\mathbf{R}(x_1, \ldots, x_n)$

Cassels-Ellison-Pfister 1971

In $\mathbf{R}(x, y)$ a sum of 4 squares need not be a sum of 3 squares.
Proof uses elliptic curves.
Quite different proof, 1993, via Lefschetz theorem.

Long standing open problem : For $n \geq 3$, is there a sum of 2^n squares in $\mathbf{R}(x_1, \ldots, x_n)$ which cannot be written as a sum of a smaller number of squares ?

Other long standing open problem : Over the function field $\mathbf{R}(X)$ of a real surface X with $X(\mathbf{R}) = \emptyset$, does any quadratic form in at least 5 variables have a nontrivial zero ?

Known for forms in at least 7 variables

(Such a field has a number of common properties with totally imaginary number fields)

Milnor, 1970

Definition of Milnor's K-theory groups of a field

$$K_0^M(F) = \mathbf{Z}$$

$$K_1^M(F) = F^\times$$

$$K_2^M(F) = F^\times \otimes_{\mathbf{Z}} F^\times / \{x \otimes y,\ x + y = 1\}$$

$$K_n^M(F) = F^\times \otimes_{\mathbf{Z}} \cdots \otimes F^\times / I$$

where I is the subgroup spanned by symbols for which two coordinates add to 1.

Milnor, 1970

Questions/conjectures on the connexions between quadratic forms, (Milnor) K-theory and Galois cohomology (Serre, Tate) of fields. Natural homomorphisms

$$h_n : K_n^M(F)/2 \to H^n_{gal}(F, \mathbf{Z}/2)$$

and

$$s_n : K_n^M(F)/2 \to I^n F / I^{n+} F$$

Basic questions : *Are these homomorphisms isomorphisms* ? Would imply existence of homomorphisms $I^n F \to H^n_{gal}(F, \mathbf{Z}/2)$ sending Pfister forms to symbols, classically known only for $n \leq 2$, and defined (Arason 1974) for $n = 3$.

Classic :

$$F^\times / F^{\times 2} \simeq H^1_{gal}(F, \mathbf{Z}/2)$$

(description of quadratic extension of fields)

$$IF/I^2F \simeq F^\times / F^{\times 2}$$

(signed determinant)

Homomorphism

$$I^2F/I^3F \to H^2_{gal}(F, \mathbf{Z}/2)$$

(Clifford, Hasse-Witt invariants)

Let F_s be a separable closure of F, for p prime distinct from $\mathrm{char} F$ let $\mu_p \subset F_s^\times$ be group of p-th roots of unity.
There is a natural homomorphism

$$K_n^M(F)/p \to H^n_{gal}(F, \mu_p^{\otimes n})$$

A conjecture of Bloch and Kato (1980/1982) predicts that this is an isomorphism.
Algebraic number theory (class field theory) enough to prove this for F a number field (Milnor).
Bloch showed stability of conjecture under $F \mapsto F(t)$.

For $n = 1$, known, this is referred to as Kummer theory :

$$F^\times/F^{\times p} \simeq H^1_{gal}(F, \mu_p)$$

This uses Hilbert's theorem 90 in the Emmy Noether version

$$H^1_{gal}(F, F_s^\times) = 0.$$

The Hilbert version says : if E/F is a finite cyclic extension, with Galois group $G =< \sigma >$, the only elements in E with norm 1 in F are those of the obvious shape $\sigma(y)/y, \ y \in E^\times$.

A consequence of Hilbert's theorem 90 is

$$H^2(F, \mu_r) \hookrightarrow H^2(F, \mu_{rs})$$

The Bloch-Kato conjectures implies

$$H^{n+1}_{gal}(F, \mu_r^{\otimes n}) \hookrightarrow H^{n+1}_{gal}(F, \mu_{rs}^{\otimes n}).$$

For E/F cyclic with Galois group $< \sigma >$, Hilbert's version of Hilbert's theorem 90 suggests exact sequences

$$K_n^M(E) \stackrel{1-\sigma}{\to} K_n^M(E) \stackrel{Norm_{E/F}}{\to} K_n^M(F)$$

Algebraic K-theory, Milnor and Bloch-Kato conjectures, and motivic cohomology

Merkur'ev, 1981
Proof of Milnor's conjecture for $n = 2$:

$$K_2^M(F)/2 \simeq H^2_{gal}(F, \mathbf{Z}/2)$$

and

$$K_2^M(F)/2 \simeq I^2F/I^3F$$

hence

$$I^2F/I^3F \simeq H^2_{gal}(F, \mathbf{Z}/2)$$

Merkur'ev and Suslin, 1982
Proof of Bloch-Kato's conjecture for $n = 2$

$$K_2^M(F)/p \simeq H^2_{gal}(F, \mu_p^{\otimes 2})$$

for any integer p prime to $\mathrm{char}\, F$.

For E/F cyclic, establish the exact sequence (Hilbert 90 for cyclic extensions)

$$K_2^M(E) \stackrel{1-\sigma}{\to} K_2^M(E) \stackrel{Norm_{E/F}}{\to} K_2^M(F)$$

Solved old problem : any central simple algebra over a field is split over a solvable extension of the ground field.

Tools :

Quillen's higher algebraic K-theory, Riemann-Roch theorem for higher algebraic K-theory (Gillet).

Algebraic varieties involved : conics, Severi-Brauer varieties (twisted form of projective space).

One variant of the proof used less algebraic K-theory, it built upon the case of number fields.

In the Merkurjev case, a key point is the exactness of the sequence

$$K_2F(C) \to \oplus_{x \in C_0} F(x)^{\times} \to F^{\times}$$

for C a conic over a field F

For x in C_0, map $\{f, g\} \in K_2F(C)$ to the class of $(-1)^{v_x(f)v_x(g)}(f^{v_x(g)}/g^{v_x(f)})$ in $F(x)^{\times}$. The map $F(x)^{\times} \to F^{\times}$ is the norm map.

After work by Rost (1986) and Merkurjev–Suslin (1990) for $n = 3$ then by Rost for $n = 4$, a proof of Milnor's conjecture

$$h_n : K_n^M(F)/2 \simeq H^n_{gal}(F, \mathbf{Z}/2)$$

for any n was announced by Voevodsky in 1996. The complete proof, which builds upon a formidable work mixing up algebraic geometry and homotopy theory appeared in 2002.
As for the isomorphism

$$s_n : K_n^M(F)/2 \simeq I^n F / I^{n+} F$$

it was published by Orlov, Vishik and Voevodsky in 2007.

The proof uses ideas and results by M. Rost.

Motivic cohomology, as envisioned in 1982/83 by A. Beilinson and by S. Lichtenbaum, and as developed by Suslin, Voevodsky and others, now replaces algebraic K-theory.

The algebraic varieties to which the theory is applied are still pretty simple varieties, namely Pfister quadrics, defined by a quadratic form

$$\langle\langle a_1, a_2, ..., a_n\rangle\rangle = \langle 1, -a_1\rangle \otimes \langle 1, -a_2\rangle \otimes ... \otimes \langle 1, -a_n\rangle$$

(more precisely, Pifster neighbours).

Things are actually not so simple, one uses the motivic cohomology of simplicial schemes associated to these varieties. The proof also involves the definition and study of Steenrod operations in the context of motivic cohomology. This builds upon the homotopy theory of schemes (Voevodsky and Morel).

Along the way, tools were developed which could be used to prove the more general Bloch–Kato conjecture

$$K_n^M(F)/p \to H^n_{gal}(F, \mu_p^{\otimes n}).$$

It was reduced to a generalized "Hilbert's theorem 90", which reads

$$\mathbf{H}^{n+1}_{\text{ét}}(F, \mathbf{Z}_{(p)}(n)) = 0,$$

This is the hypercohomology of a certain complex of sheaves $\mathbf{Z}(n)$ over (the big Zariski site of) $\mathrm{Spec}(F)$.

Connexion with Milnor K-theory :

$$\mathbf{H}^n_{Zar}(F, \mathbf{Z}(n)) \simeq K^M_n(F)$$

and with Galois cohomology :

$$\mathbf{H}^n_{\text{ét}}(F, \mathbf{Z}/p(n)) = H^n_{\text{ét}}(F, \mu_p^{\otimes n}).$$

$$\mathbf{H}^1_{\text{ét}}(F, \mathbf{Z}(0)) = H^1_{gal}(F, \mathbf{Z}) = 0$$

$$\mathbf{H}^2_{\text{ét}}(F, \mathbf{Z}(1)) = H^1_{\text{ét}}(F, F_s^\times) = 0$$

$$\mathbf{H}^3_{\text{ét}}(F, \mathbf{Z}(1)) = \mathrm{Br}(F)$$

The proof of the general case (Voevodsky 2010) involves the work of a number of people (Suslin, Rost, Weibel).
The proof involves "norm varieties", to play the rôle of Severi–Brauer varieties and of Pfister neighbours.
That such varieties with the desired properties exist is due to Markus Rost. To study them, he devised certain "degree formulas".

Fix a prime l and a symbol $\alpha = \{a_1, \dots, a_n\}$ in $K_n^M(F)/l$.
One wants a smooth projective variety X over F, of dimension d, with the following properties :
(1) $d = l^{n-1} - 1$
(2) $\deg(s_d(X)) \neq 0 \mod l^2$.
(3) The image of the symbol α vanishes in $K_n^M(F(X))/l$.

Here $s_d(X) \in CH^d(X)$ is a certain characteristic class associated to the tangent bundle of X, and which is known (Milnor) to have degree divisible by l.

These investigations have generated a whole new theory, algebraic cobordism (Levine-Morel).

Here is an old and very special case of a "degree formula" : Let $f : X \to Y$ be a morphism between conics. If the degree of f is even, then the conic Y has a rational point.

(Some) higher class field theory

Classical class field theory was brought to bear on problems concerning quadratic forms.
Hasse proved the Hasse principle for quadratic forms, both for existence of a nontrivial zero and for isomorphy of two quadratic forms.
The latter result may be rephrased as an injection

$$W(k) \hookrightarrow \prod_{v \in \Omega} W(k_v)$$

One can revisit Landau's result from this point of view.
Exact sequence based on the euclidean algorithm (Milnor, who mentions Tate's rewriting of some of Gauss' arguments)

$$0 \to W(k) \to W(k(t)) \to \oplus_{P \in k[t] \text{ monic irreducible}} W(k[t]/P) \to 0.$$

Compare this sequence over a number field k and over each completion k_v
Yields injection $W(k(t)) \hookrightarrow \prod_v W(k_v(t))$
Recall f is a sum of 2^n squares in a field F if and only if the forms $f. < 1, 1 >^{\otimes n}$ and $< 1, 1 >^{\otimes n}$ are isomorphic.
Finally, $< 1, 1 >^{\otimes 8}$ is hyperbolic over each $\mathbf{Q}_p$, and $f. < 1, 1 >^{\otimes n} \simeq < 1, 1 >^{\otimes n}$ over $\mathbf{R}$ if f is positive.

K. Kato 1986

Conjectural generalisation of class field theory of number fields : higher class field theory of function fields over number fields.

Gives a proof for the function field of curves

A consequence :
If X is an absolutely irreducible curve over $\mathbf{Q}$, if $f \in \mathbf{Q}(X)$ is positive on $X(\mathbf{R})$, then it is a sum of 8 squares in $\mathbf{Q}(X)$.
The proof uses Merkurjev 's result on the Milnor conjecture.

Which generalization of classical class field theory ?
In classical class field theory, for any number field k there is a basic exact sequence for Brauer groups

$$0 \to \mathrm{Br}(k) \to \oplus_{v \in \Omega} \mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z} \to 0$$

which contains among others Gauss' quadratic reciprocity law.
The Brauer group of a field may be viewed as the second Galois cohomology group of the field with values in the group $\mathbf{Q}/\mathbf{Z}(1)$ of roots of unity.

K. Kato (1986) had the vision that for the function field $F = k(X)$ of an n-dimensional variety X over a number field k there should exist similar but longer sequences, which would start at $H^{n+2}_{gal}(F, \mathbf{Q}/\mathbf{Z}(n+1))$ ($n+2$ being essentially the highest degree for nontrivial cohomology). Here $\mathbf{Q}/\mathbf{Z}(n+1)$ is $\mathbf{Q}/\mathbf{Z}(1)$ with a twisted action of the Galois group of F.
A special case of the conjectures predicts that the natural map

$$H^{n+2}_{gal}(k(X), \mathbf{Q}/\mathbf{Z}(n+1)) \to \prod_{v\in\Omega} H^{n+2}_{gal}(k_v(X), \mathbf{Q}/\mathbf{Z}(n+1))$$

is *injective*. For $n = 0$, this is $\mathrm{Br}(k) \hookrightarrow \prod_{v\in\Omega} \mathrm{Br}(k_v)$.

In a 1996 paper, K. Kato proved the conjectures for curves. The case of surfaces was proved by U. Jannsen in 1990. The case of varieties of arbitrary dimension was announced by him in 1991. The paper containing the proof of the entire set of Kato conjectures over a number field appeared in 2009.
Among other things the proof uses resolution of singularities and Deligne's results on the Weil conjectures (notion of weight filtration on l-adic cohomology groups of open varieties over a number field).
The case of function fields over a finite field was simutlaneously examined by U. Jannsen and S. Saito. In arbitrary dimension, the conjectures (prime to characteristic) have been established by M. Kerz and S. Saito (2010).

Back to the theorem (CT-Jannsen 1991) announced at the beginning of the lecture.

Let $F = \mathbf{Q}(x_1, \ldots, x_n)$ and $F_v = \mathbf{Q}_v(x_1, \ldots, x_n)$.
Jannsen-Saito (coefficients $\mathbf{Q}/\mathbf{Z}(n+1)$) together with Voevodsky ($H^{n+2}(F, \mathbf{Z}/2) \hookrightarrow H^{n+2}(F, \mathbf{Q}/\mathbf{Z}(n+1))$) and Orlov-Vishik-Voevodsky give an injection

$$I^{n+2}F/I^{n+3}F \to \prod_{v \in \Omega} I^{n+2}F_v/I^{n+3}F_v.$$

Assume $f \in F$ is positive on $\mathbf{R}^n$. By Pfister's result, f is a sum of 2^n squares in $\mathbf{R}(x_1, \ldots, x_n)$.
For any prime p, -1 is a sum of (at most) 4 squares in $\mathbf{Q}_p$. The basic equality $f = (\frac{f+1}{2})^2 - (\frac{f-1}{2})^2$ implies that in each F_p, f is a sum of 5 hence of 8 squares. Thus for $n \geq 2$, we have

$$f. < 1, 1 >^{\otimes n+1} \simeq < 1, 1 >^{\otimes n+1}$$

over each F_v.
This implies $< f, -1 > \otimes < 1, 1 >^{\otimes n+1} = 0$ in $I^{n+2}F/I^{n+3}F$. Then Arason–Pifster implies $< f, -1 > \otimes < 1, 1 >^{\otimes n+1} = 0 \in W(F)$, that is (Witt simplification) f is a sum of 2^{n+1} squares in F.

In the case $n = 1$, one sees that f is a sum of 8 squares (this is in substance the 1986 proof).

For arbitrary n, Arason later noticed that if one uses Milnor's conjecture in degree up to $n + 3$, then one may show that a positive rational function in $\mathbf{Q}(x_1, \ldots, x_n)$ may be written as a sum of 2^{n+2} squares without appealing to the results by Jannsen and Saito.

The arguments immediately extend to arbitrary algebraic varieties over arbitrary number fields.