Raymond and Beverly Sackler
Distinguished Lectures in Mathematics

Tel Aviv University

November 10, 2003

# The local-global principle for rational points and zero-cycles

J.-L. Colliot-Thélène

C. N. R. S. et Université Paris-Sud
(France)

*Diophantine equation*: a system of equations

$$f_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$$

where the $f_i$ are polynomials in $n$ variables with coefficients in $\mathbf{Q}$.

*Questions*

*Existence*

Does there exist at least one solution with coordinates in $\mathbf{Q}$ ?

*Weak approximation* (in a special case)

Are such solutions dense (for the real topology) in the set of solutions with coordinates in $\mathbf{R}$ ?

*Zariski density*

For any polynomial $g(x_1, \ldots, x_n)$ which does not vanish identically on the set of complex solutions of the above system, can one find at least one solution $(a_1, \cdots, a_n)$ of the system with coordinates in $\mathbf{Q}$, such that moreover $g(a_1, \ldots, a_n) \neq 0$?

*The language of algebraic geometry*

A system of equations

$$f_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r$$

where the $f_i$ are polynomials in $n$ variables with coefficients in a field $k$, defines an (affine) algebraic variety $X$ over the field $k$.

For any field $F$ containing $k$ one denotes by $X(F)$ the set of solutions of the system with coordinates in $F$. This is the set of $F$-rational points of the $k$-variety $X$. One often refers to $X(k)$ simply as the set of rational points of the $k$-variety $X$.

For most purposes, it makes more sense to reduce oneself to the search of rational points on *nonsingular* varieties (locally, the jacobian matrix is of maximal rank).

It is also useful to consider *projective* varieties (defined by a system of homogeneous equations) rather than affine varieties.

Finally, a $k$-variety $X$ is called *geometrically irreducible* if for any field $F$ containing $k$, the variety $X_F$ (same variety as $X$, but considered over the field $F$) is irreducible (not the union of two proper, closed subvarieties).

*First necessary conditions for the existence of* $\mathbf{Q}$*-rational points*

There is no $\mathbf{Q}$-rational point on the affine conic

$$1 + x_1^2 + x_2^2 = 0,$$

because there is no solution over $\mathbf{R}$.

Given any variety $X/\mathbf{R}$, one may decide in a finite amount of time whether $X(\mathbf{R}) \neq \emptyset$.

There is no $\mathbf{Q}$-rational point on the affine conic

$$x_1^2 + x_3^2 - 3 = 0.$$

Proof : congruences modulo suitable powers of 3 (or powers of 2). More abstract version, parallel to case of reals : there is no solution in the 3-adic field $\mathbf{Q}_3$ (and there is no solution in $\mathbf{Q}_2$).

For each prime $p$, one defines the nonarchimedean $p$-adic valuation $v_p$ and its associated absolute value on $\mathbf{Q}$, the completion is the $p$-adic field $\mathbf{Q}_p$, which is equipped with a natural topology.

Hensel's lemma implies that given a variety over $\mathbf{Q}_p$, one can in a finite amount of time decide whether it has a $\mathbf{Q}_p$-point. Given a diophantine equation, one may in a finite amount of time decide if it has $\mathbf{Q}_p$-solutions for all $p$ (Lang-Weil estimates for the number of rational points of a variety over a finite field).

*The space of adèles*

Given an absolute value $v$ on $\mathbf{Q}$ one denotes by $\mathbf{Q}_v$ the completion (it is either $\mathbf{R}$ or $\mathbf{Q}_p$). Let $\Omega$ denote the set of (inequivalent) absolute values on $\mathbf{Q}$.

Given a nonsugular, projective, absolutely irreducible $\mathbf{Q}$-variety $X$, the product

$$X(\mathbb{A}_{\mathbf{Q}}) := \prod_{v \in \Omega} X(\mathbf{Q}_v)$$

is called the set of adèles of $X$. Each $X(\mathbf{Q}_v)$ may be equipped with the topology induced by that of $\mathbf{Q}_v$. We equip $X(\mathbb{A}_{\mathbf{Q}})$ with the product topology.

The obvious diagonal inclusion

$$X(\mathbf{Q}) \subset X(\mathbb{A}_{\mathbf{Q}})$$

encapsulates the obstructions to existence of $\mathbf{Q}$-rational points on $X$ discussed on the previous transparency.

*Weak approximation*

One says that *weak approximation* holds for $X/\mathbf{Q}$ if the closure of $X(\mathbf{Q})$ under the above embedding is the whole of $X(\mathbb{A}_{\mathbf{Q}})$. This is equivalent to requiring density of the diagonal embedding $X(\mathbf{Q}) \subset \prod_{v \in S} X(\mathbf{Q}_v)$ for any finite set $S \subset \Omega$.

One says that a class of algebraic varieties over $\mathbf{Q}$ satisfies *weak approximation* if any variety in the class satisfies it. This is a distinctly stronger requirement than the

*Local-global "principle"* ("Hasse principle")

One says that a class $\mathcal{C}$ of projective varieties over $\mathbf{Q}$ satisfies the local-global principle, or Hasse principle, if for any $X$ in $\mathcal{C}$, $X(\mathbb{A}_{\mathbf{Q}}) \neq \emptyset \Rightarrow X(\mathbf{Q}) \neq \emptyset$.

For nonsingular, projective, absolutely irreducible varieties, the validity of each of these two properties only depends on the function field of the variety: these properties are "birationally invariant".

Weak approximation trivially holds for projective space $\mathbf{P}^d_{\mathbf{Q}}$.

**Theorem**

*If $X/\mathbf{Q}$ is a projective variety which is a homogeneous space of a connected linear algebraic group over $\mathbf{Q}$, then weak approximation holds for $X$.*

(Legendre, Minkowski, Hasse, Eichler, Landherr, Kneser, Harder, Tchernousov)

The hard part is the Hasse principle. If such a variety has a $\mathbf{Q}$-rational point, it is $\mathbf{Q}$-birational to projective space over $\mathbf{Q}$, hence weak approximation holds.

Examples
*Conics* (Legendre, Hilbert); more generally
*Quadrics* (H. Minkowski, H. Hasse)
*Severi-Brauer varieties* (F. Châtelet)

Birational invariance of the local-global principle (and weak approximation) leads to the proof of these properties for seemingly different looking vareties.

*Norm equations*

$$N_{K/\mathbf{Q}}(\Xi) = c$$

when $K/\mathbf{Q}$ is a *cyclic extension* (Hasse).

Nonsingular *cubic surfaces* over $\mathbf{Q}$ *with a special Galois action on the 27 lines* (Selmer, Cassels, Swinnerton-Dyer, Châtelet). Example:

$$ax^3 + by^3 + cz^3 + dt^3 = 0$$

when $\frac{ab}{cd}$ is a cube in $\mathbf{Q}$.

*Quadrics: proofs*

Let $q(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i^2$ be a quadratic form in $n \geq 3$ variables over $\mathbf{Q}$. We want to show that if there is a nontrivial zero for $q$ in each $\mathbf{Q}_v$, then there is one in $\mathbf{Q}$. We may assume all $a_i \in \mathbf{Z}$.

The case $n = 3$ was handled by Legendre using the geometry of numbers. Let us mention an important *fact* (a special case of a recriprocity law): for a conic $C/\mathbf{Q}$, the (finite) number of $v \in \Omega$ with $C(\mathbf{Q}_v) = \emptyset$ is *even*.

Case $n = 4$ (Hasse's proof). If the quadratic form has nontrivial solutions in all $\mathbf{Q}_v$, then for each $v \in \Omega$ one may find $c_v \in \mathbf{Q}_v^*$ such that the system

$$a_1 x^2 + a_2 x_2^2 = c_v = -a_3 x_3^2 - a_4 x_4^2$$

has a solution in $\mathbf{Q}_v$. Let $S \subset \Omega$ be a finite set containing the real absolute value and all the $v_p$ for with $p \mid 2a_1a_2a_3a_4$. Using *Dirichlet's theorem on primes in an arithmetic progression*, one finds a rational number $c \in \mathbf{Q}^*$ which is very close to $c_v$ for each $v \in S_{\text{finite}}$, has the sign of $c_\infty$, and has absolute value 1 at all other $v$ except *one*, say $v_l$. Then each of the conics $a_1 x_1^2 + a_2 x_2^2 - c = 0$ and $c + a_3 x_3^2 + a_4 x_4^2 = 0$ has solutions in all $\mathbf{Q}_v$ except possibly $\mathbf{Q}_l$, hence also in this last one by the above mentionned *fact*, hence in $\mathbf{Q}$ by the 3 variables case.

Hence $q = 0$ has a nontrivial solution over $\mathbf{Q}$.

The case $n \geq 5$ is easier. Here is a more general statement ([CT/Sansuc, 1982]).

**Theorem**

*Let $P(t) \neq 0 \in \mathbf{Q}[t]$ be a polynomial, and $\sum_{i=1}^{3} a_i x_i^2$ a nondegenerate quadratic form with coefficients in $\mathbf{Q}$. Then the local-global principle holds for the equation*

$$P(t) = \sum_{i=1}^{3} a_i x_i^2 \neq 0.$$

One may assume that all $a_i$ are in $\mathbf{Z}$. Let $S$ be the union of the real absolute values and the absolute value $v_p$ for $p \mid 2a_1a_2a_3$. Over $\mathbf{Q}_p$ for $p$ not in $S$, the form $\sum_{i=1}^{3} a_i x_i^2$ represents *any* element in $\mathbf{Q}_p^*$. For $v \in S$, one chooses $t_v \in \mathbf{Q}_v$ such that $P(t_v) \neq 0$ is represented by $\sum_{i=1}^{3} a_i x_i^2$ over $\mathbf{Q}_v$.

*Weak approximation* in $\mathbf{Q}$ at the places in $S$ now produces $t_0 \in \mathbf{Q}$ such that $P(t_0)$ is represented by $\sum_{i=1}^{3} a_i x_i^2$ over each $\mathbf{Q}_v$, hence over $\mathbf{Q}$ by the theorem for quadratic forms in 4 variables.

The proof yields weak approximation for the variety considered in the theorem.

Here is a general statement.

**Theorem** *Let $X/\mathbf{Q}$ be a nonsingular, projective, absolutely irreducible variety and let $p : X \to \mathbf{P}^1_{\mathbf{Q}}$ be a dominant morphism with absolutely irreducible generic fibre.*

*Assume :*

*(i) The nonsingular fibres of $p$ above points of $\mathbf{P}^1(\mathbf{Q})$ satisfy the Hasse principle (resp. weak approximation).*

*(ii) The fibres of $p$ above points of $\mathbf{P}^1(\mathbf{C})$ are irreducible and of multiplicity one.*

*Then $X$ satisfies the Hasse principle (resp. weak approximation).*

The proof is essentially the same as Hasse's proof for quadratic forms in 5 variables starting from the 4 variables case – except that instead of elementary facts on quadrics one uses the Lang-Weil estimates for the number of points of absolutely irreducible varieties over a finite field.

One can relax the second condition sligthly.

**Theorem**

*Let $X/\mathbf{Q}$ be a nonsingular, projective, absolutely irreducible variety and let $p : X \to \mathbf{P}^1_{\mathbf{Q}}$ be a dominant morphism with absolutely irreducible generic fibre.*

*Assume :*

*(i) The nonsingular fibres of $p$ above points of $\mathbf{P}^1(\mathbf{Q})$ satisfy the Hasse principle (resp. weak approximation).*

*(ii) The fibres of $p$ above points of $\mathbf{A}^1(\mathbf{C})$ are irreducible and of multiplicity one.*

*(iii) The fibre of $p$ above $\infty \in \mathbf{P}^1(\mathbf{C})$ contains a component of multiplicity one.*

*Then $X$ satisfies the Hasse principle (resp. weak approximation).*

In the proof, one replaces *weak approximation* in $\mathbf{Q}$ by *strong approximation* (a special case of which is the Chinese remainder theorem). Roughly speaking, one replaces the projective line $\mathbf{P}^1_{\mathbf{Z}}$ by the affine line $\mathbf{A}^1_{\mathbf{Z}}$. Freedom (lack of control in the approximation) at one prime is required; this is afforded by a conjunction of hypothesis (iii) and the Chebotarev theorem.

*The circle method*

Hardy, Littlewood, Davenport, Birch, Skinner, ...

**Theorem**
*Let $F(x_0, \cdots, x_n) = 0$ define a nonsingular hypersurface $X$ of degree $d$ in $\mathbf{P}^n_{\mathbf{Q}}$. Assume $n \geq (d-1).2^d$. Then $X(\mathbf{Q})$ is dense in $X(\mathbb{A}_{\mathbf{Q}})$.*

The theorems are actually more precise: they evaluate how the number of solutions in a "box" varies as the size of the box goes to infinity. In short, one counts the number of solutions.

There are such theorems for a system of forms, and also over a number field. However, the circle method generally requires that the number of variables be fairly large with respect to the degree.

For instance, under the hypothesis of the above theorem, for $n \geq 4$, one could dream of a local-global principle as soon as $n \geq d$.

For nonsingular cubic hypersurfaces in $\mathbf{P}^n_{\mathbf{Q}}$, there are good results: for $n \geq 9$ there is always a $\mathbf{Q}$-rational point (Heath-Brown), and for $n = 8$ the local-global principle holds (Hooley). The latter is however widely conjectured to hold for $n \geq 4$.

*There are many counterexamples to the Hasse principle (and weak approximation)*

*Homogeneous spaces of connected linear algebraic groups* (nonprojective)

– Norm equations

$$N_{K/\mathbf{Q}}(\Xi) = c$$

for $K/\mathbf{Q}$ Galois with group $\mathbf{Z}/2 \times \mathbf{Z}/2$ (Hasse, Witt)

– Principal homogeneous spaces under (nonsimply-connected) semisimple groups (Serre)

*Homogeneous spaces of abelian varieties* (projective)

– Curves of genus one (Reichardt, Lind)

$$3x^3 + 4y^3 + 5z^3 = 0 \quad \text{(Selmer)}$$

*Cubic surfaces* (Swinnerton-Dyer)

$$5x^3 + 9y^3 + 10z^3 + 12t^3 = 0 \quad (\text{Cassels} - \text{Guy})$$

*One-parameter families of conics*

$$y^2 + z^2 = (3 - x^2)(x^2 - 2) \quad \text{(Iskovskikh)}$$

*Reciprocity*

In all previous examples, the set of adèles $X(\mathbb{A}_{\mathbf{Q}})$ is not empty, but $X(\mathbf{Q})$ is. There are also examples where $X(\mathbf{Q})$ is not empty but not dense in $X(\mathbb{A}_{\mathbf{Q}})$.

In the proofs, reciprocity laws such as Gauß's quadratic *reciprocity law* are used.

Let $F$ be a field. The Brauer group of $F$ was defined by R. Brauer as the group of isomorphism classes of central simple algebras of finite dimension over $F$, when one decrees that matrix algebras be trivial, and addition in $\mathrm{Br}(F)$ is induced by tensor product of algebras.

Let more generally $k$ be a number field, $\Omega$ the set of its places (inequivalent absolute valuations).

For each $v \in \Omega$, there is a natural embedding

$$\mathrm{inv}_v : \mathrm{Br}(k_v) \subset \mathbf{Q}/\mathbf{Z}$$

which is an isomorphism if $v$ is nonarchimedean.

There are many aspects of the *reciprocity law* in class field theory. One version of it, in commutative class field theory, is the following fundamental exact sequence:

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

There is a general formalism, due to Manin (1970), which subsumes the technique employed in the counterexamples listed in the last but one transparency.

This uses the Brauer group $\mathrm{Br}(X)$ of a scheme $X$, as defined by Grothendieck. This is a generalization of the Brauer group of a field. This notion is "functorial", given an algebraic variety $X$ over a field $F$, there is a natural pairing

$$X(F) \times \mathrm{Br}(X) \to \mathrm{Br}(F)$$

$$(M, A) \mapsto A(M)$$

Let $X$ be a nonsingular, projective, geometrically irreducible variety over a number field $k$. The above pairing induces a pairing

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbf{Q}/\mathbf{Z}$$

$$(\{M_v\}_{v\in\Omega}, A) \mapsto \sum_{v\in\Omega} \mathrm{inv}_v(A(M_v)).$$

Let $X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)$ denote the left kernel of this pairing.

Manin's basic observation (1970) is that the diagonal inclusion $X(k) \subset X(\mathbb{A}_k)$ factorizes as

$$X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k).$$

This is an immediate consequence of the reciprocity sequence for the Brauer group of $k$.

More precisely, the topological closure of $X(k)^{\mathrm{cl}}$ of $X(k)$ in $X(\mathbb{A}_k)$ is contained in $X(\mathbb{A}_k)^{\mathrm{Br}}$.

One gets a counterexample to the Hasse principle if $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ and $X(\mathbb{A}_k) \neq \emptyset$.

One gets counterexamples to weak approximation as soon as $X(\mathbb{A}_k)^{\mathrm{Br}}$ is a proper subset of $X(\mathbb{A}_k)$.

*Can one effectively determine the set $X(\mathbb{A}_k)^{\mathrm{Br}}$ ?*

This depends on the complexity of the quotient group $\mathrm{Br}(X)/\mathrm{Br}(k)$. This group need not be finite, for general $X$ we do not know if there is a finite procedure to decide whether or not $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.

If $X$ is geometrically unirational, or more generally if $X$ is geometrically rationally connected, then $\mathrm{Br}(X)/\mathrm{Br}(k)$ is finite.

**Basic problem**

*To produce classes $\mathcal{C}$ of varieties such that for any $X$ in $\mathcal{C}$*

$$X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}$$

*or at least*

$$X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset \quad \text{implies} \quad X(k) \neq \emptyset$$

**Warning**

We never hoped that this could be true for all (nonsingular, projective) varieties.

The first unconditional example with $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ and $X(k) = \emptyset$ is due to Skorobogatov (1999).

(More on this later)

There is however a substitute with zero-cycles of degree one which might hold for all (nonsingular, projective) varieties.

(More on this later)

*Classes of varieties $X$ for which one has proved*

$$X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}.$$

Nonsingular projective models of homogeneous spaces of connected linear algebraic groups, when the geometric stabilizer is either connected or finite and commutative (Sansuc when the stabilizer is trivial; Borovoi under these more general hypotheses).

Conic bundles over the projective line $\mathbf{P}^1_k$ with at most 5 geometric degenerate fibres
(CT/Sansuc/Coray, CT/Sansuc/Swinnerton-Dyer, Salberger, CT, Salberger, Salberger/Skorobogatov)

Nonsingular projective models of irreducible complete intersections of two quadrics in $\mathbf{P}^n_k$ if $n \geq 8$ (CT/Sansuc/Swinnerton-Dyer)

Cubic hypersurfaces with three singular points in $\mathbf{P}^n_k$ ($n \geq 3$) (CT/Salberger)

Nonsingular cubic hypersurfaces in $\mathbf{P}^n_k$ ($n \geq 3$) containing a $k$-rational line (Salberger/Skorobogatov; Harari)

**Theorem** (D. Harari)

*Let $X/k$ be a nonsingular, projective, geometrically integral variety and let $p : X \to \mathbf{P}^1_k$ be a dominant $k$-morphism with geometrically irreducible generic fibre.*

*Assume*

*(i) All geometric fibres of $p$ above $\mathbf{A}^1_k$ are irreducible and of multiplicity one.*

*(ii) The geometric generic fibre is rationally connected (e.g. unirational).*

*(iii) For $P \in \mathbf{P}^1(k)$ with nonsingular fibre $X_P$, we have $X_P(k)^{\mathrm{cl}} = X_P(\mathbb{A}_k)^{\mathrm{Br}}$.*

*Then $X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}$.*

Tools used in the proof are Hilbert's irreducibility theorem, strong approximation, Tchebotarev's density theorem, and a *formal lemma* relative to ramified central simple algebras over the function field of $X$ (more on this later).

There is a similar theorem over $\mathbf{P}^n_k, n \geq 1$. When the fibration admits a section, an easy application of the result gives a proof of Sansuc's result : For a smooth compactification $X$ of a connected linear algebraic group, $X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}$. The idea here goes back to a paper of Kunyavskiĭ and Skorobogatov.

*Classes of varieties $X$ for which one has conditional proofs of*

$$X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}.$$

**Theorem**

*Let $X/k$ be a nonsingular, projective, geometrically integral variety and let $p : X \to \mathbf{P}^1_k$ be a dominant $k$-morphism with geometrically irreducible generic fibre.*

*Assume*

*(i) For each closed point $P \in \mathbf{P}^1_k$, the fibre $X_P$ over the residue field $k(P)$ contains a multiplicity one component whose field of definition is an abelian extension of $k(P)$*

*(ii) Weak approximation holds for the nonsingular fibres of $p$ above points in $\mathbf{P}^1(k)$.*

*(iii) Schinzel's hypothesis is true.*

*Then $X(k)^{\mathrm{cl}} = X(\mathbb{A}_k))^{\mathrm{Br}}$.*

(CT/Sansuc, Serre, Swinnerton-Dyer, CT/Swinnerton-Dyer, CT/Skorobogatov/Swinnerton-Dyer)

We do not know whether the abelianity condition in (i) can be gotten rid of.

*Schinzel's hypothesis*

(H) *Let* $f_i(X) \in \mathbf{Z}[X], i = 1, \cdots, m$ *be irreducible polynomials. Assume their leading coefficients are positive, and assume that the g.c.d. of all* $\prod_i f_i(n)$ *for* $n \in \mathbf{Z}$ *is equal to 1. Then there exist infinitely many integers* $n$ *such that each* $f_i(n)$, $i = 1, \cdots, m$ *is a prime.*

It is the natural generalization of the conjecture on twin primes. Special cases of the conjecture were put forward by Bouniakowsky and by Dickson.

The only known case is that of one polynomial of degree one: this is Dirichlet's theorem on primes in an arithmetic progression.

Dirichlet's theorem was used by Hasse in his proof of the local-global principle for quadrics of dimension 2. The starting point for the proof of the theorem is to use Schinzel's hypothesis in place of Dirichlet's theorem.

**Conjecture**

*Let $X/k$ be a nonsingular, projective, geometrically integral variety and let $p : X \to \mathbf{P}^1_k$ be a dominant $k$-morphism. Assume that the generic fibre of $p$ is irreducible, and contains an open set which is a homogeneous space of a connected linear algebraic group (over the function field $k(\mathbf{P}^1)$). Assume that the geometric stabilizer for this action is connected. Then*

$$X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}.$$

One would like to combine

(a) Borovoi's theorem on homogeneous spaces over a number field

(b) the proof of Harari's theorem

(c) the proof of the theorem depending on Schinzel's hypothesis

to get a conditional proof of the conjecture, i.e. one depending on Schinzel's hypothesis.

Unfortunately the abelianity condition in the previous theorem prevents us from achieving this.

*A simple class of equations, a hard problem*

Let $K/\mathbf{Q}$ be a finite field extension of degree $m$, $K = \oplus_{i=1}^{m} k e_i$, and let $P(t) \in \mathbf{Q}[t]$ be a nonzero polynomial of degree $d$.

One would like to be able to describe the existence and density properties of the rational solutions of

$$P(t) = \mathrm{Norm}_{K/\mathbf{Q}}(x_1 e_1 + \cdots + x_m e_m) \neq 0.$$

For a nonsingular projective model $X$ of this variety, does one have $X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}$ ?

For $d = 0$, the answer is yes (class field theory, Tate-Nakayma).

For $d = 1$, the answer is trivially yes.

For $d = 2$, when $P$ has two distinct rational roots, the answer is yes (Heath-Brown/Skorobogatov; a result coming from the circle method is used).

For $d = 3$, and $[K : \mathbf{Q}] = 3$, the answer is yes (CT/Salberger 1989).

For $d \leq 4$ and $[K : \mathbf{Q}] = 2$, the answer is yes (CT/Sansuc/Swinnerton-Dyer 1987).

For $d$ arbitrary and $K/\mathbf{Q}$ cyclic, if one accepts Schinzel's hypothesis, then the answer is yes.

If $K/\mathbf{Q}$ is Galois with group $\mathbf{Z}/2 \times \mathbf{Z}/2$ and $P$ is of degree 3, the answer is unclear (abelianity problem).

*Homogeneous spaces of abelian varieties*

**Theorem** (Manin, L. Wang)
*Let $X$ be a principal homogeneous space under an abelian variety $A$. Let us assume that the Tate-Shafarevich group of $A$ is a finite group. Then*
*(i) If $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$, then $X(k) \neq \emptyset$*
*(ii) Assume that $k$-rational points of $A$ are dense in the neutral component of the product of the $A(k_v)$ for all archimedean places $v$ of $k$. Then $X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}$.*

The proof is an algebraic computation which reduces this statement to arithmetic duality theorems of Cassels and Tate.

That Tate-Shafarevich groups of abelian varieties should be finite is a well-known conjecture.

In dimension one, the varieties $X$ in the theorem are exactly the (nonsingular, projective) curves of genus one.

One may then go on and investigate one-parameter families of curves of genus one. This will be the topic of the second lecture.

*Classes of varieties $X$ for which it is very unlikely that $X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)^{\mathrm{Br}}$.*

Let $X \subset \mathbf{P}^n_k$ be a nonsingular hypersurface of dimension at least 3 and of degree $d$.

Then $\mathrm{Br}(X)/\mathrm{Br}(k) = 0$. The above hypothesis would thus imply $X(k)^{\mathrm{cl}} = X(\mathbb{A}_k)$. In particular, if $X(k) \neq \emptyset$, the $k$-points would be dense in the $k_v$-points for any place $v$, hence they would be dense for the Zariski topology. But for $d > n$ this would contradict the higher dimensional analogue of Mordell's conjecture.

One can show by examples (Lang-Sarnak, Poonen) that the implication $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset \Rightarrow X(k) \neq \emptyset$ would also contradict the higher dimensional analogue of Mordell's conjecture.

Note: such hypersurfaces have a trivial geometric fundamental group.

*Classes of varieties $X$ for which one can show $X(k)^{\mathrm{cl}} \neq X(\mathbb{A}_k)^{\mathrm{Br}}$.*

*Skorobogatov's unconditional example*

This is a surface over $\mathbf{Q}$ with affine model given by the system

$$y^2 = g(t)(x^2+1), \qquad z^2 = g(t)(x^2+2)$$

with $g(t) = 3(t^4 - 54t^2 - 117t - 243)$.

Here $X(\mathbb{A}_{\mathbf{Q}})^{\mathrm{Br}} \neq \emptyset$ but $X(\mathbf{Q}) = \emptyset$.

The associated nonsingular projective surface is a hyperelliptic surface $X$, the quotient of a product $C \times E$, where $C$ ($y^2 = g(t)$) and $E$ ($y^2 = x^2+1, z^2 = x^2+2$) are two curves of genus one, by a fixed point free involution $\tau = (\rho, \sigma)$, where $\rho$ is the hyperelliptic involution on $C$ and $\sigma$ is the translation by a rational 2-torsion point on the elliptic curve $E$.

A key point here is that the geometric fundamental group of $X$ is not trivial. But even more to the point is the fact that *the geometric fundamental group of $X$ is not abelian.* This was stressed by Harari, who showed that under this hypothesis one may in a systematic fashion produce counterexamples to weak approximation which cannot be accounted for by the Brauer group – i.e. by Manin's scheme.

*Technique I : The descent method*

This in essence goes back to Fermat. It was particularly developed for curves of genus one (Weil, Selmer, Cassels ...). One starts with a curve $C$ of genus (at least) one. Using factorization arguments one produces a finite set of curves $C_i$ together with morphisms $f_i : C_i \to C$ such that any $k$-point of $C$ comes from a $k$-point of one of the $C_i$'s. There is a commutative finite $k$-group scheme $\mu$ such that each $f_i : C_i \to C$ is a principal homogeneous space over $C$ under $\mu$. One then iterates the process with the $C_i$'s.

What Sansuc and I systematically developed is a similar procedure when $C$ is replaced by a higher dimensional variety $X$ and the finite $k$-group scheme $\mu$ is replaced by a $k$-torus $S$ (a $k$-group which over an algebraic closure becomes isomorphic to a product of multiplicative groups).

When the geometric Picard group is free of finite type (example: the variety $X$ is geometrically unirational) there is no need to iterate the process, there is a best $S$, whose character group is the Picard group. The question then arises whether the corresponding $X_i$'s satisfy the local-global principle and weak approximation.

The hypothesis $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ ensures that there is such an $X_i$ with points in all completions (this is the *main theorem* of descent theory).

*Technique II : The fibration method*

We saw it at work in Hasse's proof for quadratic forms in 4 and 5 variables.

To prove Harari's theorem, or to prove the theorem conditional on the Schinzel hypothesis, one needs more elaborate versions which exploit the hypothesis $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$.

A crucial technical tool is Harari's

**Formal lemma**

*Let $X/k$ be a nonsingular, projective, geometrically irreducible variety and let $\emptyset \neq U \subset X$ be an open set. Let $B \subset \mathrm{Br}(U)$ be a finite subgroup. Let $\{P_v\} \in U(\mathbb{A}_k)$. If for all $\alpha \in B \cap \mathrm{Br}(X)$*

$$\sum_{v \in \Omega} \alpha(P_v) = 0$$

*then for any finite set $S$ of places of $k$ there exists $\{M_v\} \in U(\mathbb{A}_k)$ such that $M_v = P_v$ for $v \in S$ and*

$$\sum_{v \in \Omega} \beta(M_v) = 0$$

*for each $\beta \in B$.*

One may naturally *combine* the two techniques. This is indeed how we (CT/Sansuc/Swinnerton-Dyer) proved: *A positive rational number may be written as a sum* $a^2 + b^2 + c^4$ *with* $a, b, c \in \mathbf{Q}$ *if and only if it can be written as such a sum over* $\mathbf{Q}_2$.

*Other technique : Zero-cycles of degree one*

In extremely favourable circumstances, the existence of a zero-cycle of degree one implies the existence of a rational point. One may then apply theorems concerning zero-cycles of degree one (more on this last topic later) (Salberger and Skorobogatov).

*Other technique : The circle method*

This method does prove the local-global principle and weak approximation when the number of variables is big with respect to the degree. In one special case, one has managed to combine this with the descent method: the number of variables is not big enough in the diophantine equation of interest, but descent reduces the problem to a situation where the circle method applies (Heath-Brown and Skorobogatov)

*Other technique: Descent using torsors under non-commutative group schemes* (Skorobogatov, Harari)

*A very general conjecture on algebraic cycles*

Let $X/k$ be a nonsingular, projective, geom. irreducible variety over a number field $k$, let $d = \dim(X)$, let $i$ be an integer, $1 \leq i \leq d$, and $j = d + 1 - i$.

Let $CH^i(X)$ be the Chow group of cycles of codimension $i$ on $X$ modulo rational equivalence.

Over any field $F$ containing $k$ there are *cycle maps* $\mathrm{cl}_n : CH^i(X_F) \to H^{2i}_{\text{ét}}(X_F, \mu_n^{\otimes i})$ for each $n \geq 1$.

Class field theory (Poitou-Tate) combined with (geometric) Poincaré duality leads to exact sequences

$$\ldots H^{2i}_{\text{ét}}(X, \mu_n^{\otimes i}) \to \prod_{v\in\Omega} H^{2i}_{\text{ét}}(X_{k_v}, \mu_n^{\otimes i}) \to$$
$$\to \mathrm{Hom}(H^{2j}_{\text{ét}}(X, \mu_n^{\otimes j}), \mathbf{Q}/\mathbf{Z}) \to \ldots$$

(S. Saito)

One thus obtains a pairing

$$\prod_{v\in\Omega} CH^i(X_{k_v}) \times H^{2j}_{\text{ét}}(X, \mathbf{Q}/\mathbf{Z}(j))) \to \mathbf{Q}/\mathbf{Z}$$

and the diagonal image of $CH^i(X)$ in the product $\prod_{v\in\Omega} CH^i(X_{k_v})$ is in the left kernel of this pairing.

For $i = d$, this is a statement on zero-cycles which is a direct extension of Manin's observation on the pairing between rational points and the Brauer group.

**Conjecture**

*Let* $\{z_v\} \in \prod_{v\in\Omega} CH^i(X_{k_v})$. *Assume that for each* $\xi \in H^{2j}_{\text{ét}}(X, \mathbf{Q}/\mathbf{Z}(j))$ *one has*

$$\sum_{v\in\Omega}(z_v, \xi) = 0.$$

*Then for each* $n > 0$ *there exists* $z_n \in CH^i(X)$ *such that for each finite place* $v$

$$\mathrm{cl}_n(z_n)_{|v} = \mathrm{cl}_n(z_v) \in H^{2i}_{\text{ét}}(X_{k_v}, \mu_n^{\otimes i}).$$

For $i = 1$, this is a conjecture on classes of divisors. *If the Tate-Shafarevich group of the Picard variety of* $X$ *is finite, then the conjecture holds.*

For $i = d$, this conjecture implies: if there is a family of zero-cycles $z_v, v \in \Omega$, each of degree 1, such that for each $\alpha \in \mathrm{Br}(X)$ one has $\sum_{v\in\Omega} \alpha(z_v) = 0$, then there exists a zero-cycle of degree 1 on $X$.

If $X$ is a curve, the result for $i = 1$ is just a reinterpretation by Manin of results of Cassels and Tate.

For rational surfaces and $i = 2$, the conjecture was put forward by CT/Sansuc in 1981. Some general, related conjectures were then suggested by Kato and Saito in 1986. For $i = d$ a closely related question was raised by S. Saito in 1989.

For conic bundles over the projective line and $i = 2$, the conjecture was proved by Salberger in 1988. Salberger's result has been extended in two directions.

**Theorem**

*Let $X/k$ be a nonsingular, projective, geometrically integral variety and let $p : X \to \mathbf{P}^1_k$ be a dominant $k$-morphism with geometrically irreducible generic fibre.*

*Assume*

*(i) For each closed point $P \in \mathbf{P}^1_k$, the fibre $X_P$ over the residue field $k(P)$ contains a multiplicity one component whose field of definition is an abelian extension of $k(P)$.*

*(ii) The Hasse principle holds for the nonsingular fibres of $p$ above closed points of $\mathbf{P}^1_k$.*

*(iii) There is a family of zero-cycles $z_v, v \in \Omega$, each of degree 1, such that for each $\alpha \in \mathrm{Br}(X)$ one has $\sum_{v\in\Omega} \alpha(z_v) = 0$.*

*Then there exists a zero-cycle of degree 1 on $X$.*

(CT/Swinnerton-Dyer 1994, CT, Skorobogatov and Swinnerton-Dyer 1997)

When the generic fibre is a Severi-Brauer variety of prime index, the whole conjecture for $i = \dim(X)$ is proved.

Note: No Schinzel !

**Theorem**

*Let $k$ be a number field, $C/k$ a geom. irreducible, nonsingular curve, $X/k$ an absolutely irreducible, nonsingular variety which is a conic bundle over $C$: there exists a dominant $k$-morphism $p : X \to C$ whose generic fibre is a conic.*

*Assume that the Tate-Shafarevich group of the jacobian of $C$ is finite.*

*Then the conjecture holds for zero-cycles on $X$.*

(CT 2000, Frossard 2002, van Hamel 2003)

For $C = \mathbf{P}^1_k$, this is Salberger's 1988 result.

The theorem more generally holds for $X \to C$ whose generic fibre is a Severi-Brauer of square-free index.

*Key ingredient: Salberger's device*

This is a clever but elementary substitute for Schinzel's hypothesis. Ideally, one would wish that any "theorem" which one proves for rational points upon use of Schinzel's hypothesis yield an actual theorem for zero-cycles of degree one.

*The twin primes case*

**Proposition**

*For any integer $N \geq 2$, there exist a field extension $K/\mathbf{Q}$ of degree $N$ and an integer $\theta \in K$ such that one has prime ideal decompositions*

$(\theta) = \mathfrak{p}\mathfrak{p}_2$

$(\theta + 2) = \mathfrak{q}\mathfrak{q}_2$

*with $\mathfrak{p}_2$ and $\mathfrak{q}_2$ above 2.*

*Proof* For general $p, q$ primes and $R(t) \in \mathbf{Z}[t]$ monic polynomial of degree $N - 2$, the polynomial $P(t) := R(t)t(t+2) + qt + p(t+2)$ is irreducible. Let $K = \mathbf{Q}[t]/P(t)$. Then $N_{K/\mathbf{Q}}(\theta) = \pm 2p$ and $N_{K/\mathbf{Q}}(\theta + 2) = \pm 2q$.