Aspects of Mathematics

Jean-Pierre Serre

Lectures on the Mordell-Weil Theorem

Third Edition

Jean-Pierre Serre

Lectures on the Mordell-Weil Theorem

Aspects of Mathematics

Edited by Klas Diederich

Vol. E 3: G. Hector/U. Hirsch: Introduction to the Geometry of Foliations, Part B

Vol. E 5: P. Stiller: Automorphic Forms and the Picard Number of an Elliptic Surface

Vol. E 6: G. Faltings/G. Wüstholz et al.: Rational Points*

Vol. E 9: A. Howard/P.-M. Wong (Eds.): Contribution to Several Complex Variables

Vol. E 10: A. J. Tromba (Ed.): Seminar of New Results in Nonlinear Partial Differential Equations*

Vol. E 15: J.-P. Serre: Lectures on the Mordell-Weil Theorem

Vol. E 16: K. Iwasaki/H. Kimura/S. Shimomura/M. Yoshida: From Gauss to Painlevé

Vol. E 17: K. Diederich (Ed.): Complex Analysis

Vol. E 18: W. W. J. Hulsbergen: Conjectures in Arithmetic Algebraic Geometry

Vol. E 19: R. Racke: Lectures on Nonlinear Evolution Equations

Vol. E 20: F. Hirzebruch, Th. Berger, R. Jung: Manifolds and Modular Forms*

Vol. E 21: H. Fujimoto: Value Distribution Theory of the Gauss Map of Minimal Surfaces in $\mathbf{R}^m$

Vol. E 22: D. V. Anosov/A. A. Bolibruch: The Riemann-Hilbert Problem

Vol. E 23: A. P. Fordy/J. C. Wood (Eds.): Harmonic Maps and Integrable Systems

Vol. E 24: D. S. Alexander: A History of Complex Dynamics

Vol. E 25: A. Tikhomirov/A. Tyurin (Eds.): Algebraic Geometry and its Applications

Vol. E 26: H. Skoda/J.-M. Trépreau (Eds.): Contributions to Complex Analysis and Analytic Geometry

Vol. E 27: D. N. Akhiezer: Lie Group Actions in Complex Analysis

Vol. E 28: R. Gérard, H. Tahara: Singular Nonlinear Partial Differential Equations

Vol. E 29: R.-P. Holzapfel: Ball and Surface Arithmetics

Vol. E 30: R. Huber: Étale Cohomology of Rigid Analytic Varieties and Adic Spaces

*A Publication of the Max-Planck-Institut für Mathematik, Bonn

Jean-Pierre Serre

Lectures on the Mordell-Weil Theorem

Translated and edited by Martin Brown
from notes by Michel Waldschmidt

3rd edition

Springer Fachmedien Wiesbaden GmbH

vieweg

Prof. *Jean-Pierre Serre*
Collège de France
Chaire d'Algèbre et Géométrie
75005 Paris

AMS Subject Classification: 14 G 13, 14 K 10, 14 K 15

1st edition 1989
2nd edition 1990
3rd edition 1997

Originally published by Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1997

Cover design: Wolfgang Nieger, Wiesbaden

Printed on acid-free paper

ISSN 0179-2156
ISBN 978-3-663-10634-0 ISBN 978-3-663-10632-6 (eBook)
DOI 10.1007/978-3-663-10632-6

Foreword

This is a translation of "Autour du théorème de Mordell-Weil", a course given by J.-P. Serre at the Collège de France in 1980 and 1981.
These notes were originally written weekly by Michel Waldschmidt and have been reproduced by Publications Mathématiques de l'Université de Paris VI, by photocopying the handwritten manuscript.
The present translation follows roughly the French text, with many modifications and rearrangements. We have not tried to give a detailed account of the new results due to Faltings, Raynaud, Gross-Zagier ...; we have just mentioned them in notes at the appropriate places, and given bibliographical references.

Paris, Fall 1988

M. L. Brown
J.-P. Serre

CONTENTS

1. SUMMARY

The aim of this course is the study of rational and integral points on algebraic varieties, especially on curves or abelian varieties. Before the end of the last century only special cases had been considered. The first general results are found, around 1890, in the work of Hurwitz and Hilbert [HH] where they introduced the, nowadays natural, viewpoint of algebraic geometry: if X and X' are two birationally equivalent algebraic curves over $\mathbf{Q}$ in $\mathbf{P_2}$, their rational points correspond. Hence the importance of birational invariants, in particular the genus. They studied especially the case of genus zero:

Theorem. *A curve of genus zero is isomorphic to a conic. If it has a rational point over* $\mathbf{Q}$*, then it is isomorphic to* $\mathbf{P}_1$*, and thus has an infinite number of rational points over* $\mathbf{Q}$*.*

The principle of the proof is the following. As the genus is zero, the canonical divisor has degree -2. Changing the sign, one obtains a divisor of degree 2. The correspondence between divisors and morphisms to projective space provides a morphism $X \to \mathbf{P_2}$ whose image is of degree 2, hence is a conic.

Around 1901, Poincaré [P] took up this question again, apparently unaware of the work of Hurwitz and Hilbert. He gave another treatment of the case $g = 0$. When $g = 1$ (elliptic case), he made use of the affine structure of the set of rational points. His paper is not very clear. Still, one can credit him with descent arguments (3-descents, while his successors used mostly 2-descents), and with the following conjecture (proved by Mordell [M] in 1922):

Theorem. *The group of rational points on an elliptic curve is finitely generated.*

In the same paper Mordell stated his famous conjecture [now proved by Faltings]:

Mordell's Conjecture. *A curve of genus* ≥ 2 *has only finitely many rational points.*

In his thesis (1928), Weil [W1] considered a curve of genus $g \geq 1$ over a number field K, with jacobian J. Weil's theorem concerns the group $J(K)$ of points of J rational over K:

Theorem. (Mordell-Weil.) *The group $J(K)$ is finitely generated.*

One of the main themes of this course is the proof of this theorem (with J replaced by an arbitrary abelian variety).

Here is a brief sketch of the contents of each section:

1.1. Heights.

For simplicity, let us assume that K is $\mathbf{Q}$. Let $\mathbf{P}_n$ be projective n-space and $P \in \mathbf{P}_n(\mathbf{Q})$ a rational point of $\mathbf{P}_n$. We may write P uniquely (up to sign) as

$$P = (x_0, \ldots, x_n),$$

where $x_0, \ldots, x_n$ are rational integers with no common factor. Define the height of P to be

$$H(P) = \sup |x_i| .$$

The number of points of $\mathbf{P}_n(\mathbf{Q})$ of height $\leq N$ is asymptotically

$$\frac{2^n}{\zeta(n+1)} N^{n+1}.$$

The logarithmic height of P is $h(P) = \log H(P)$ (which is approximately the number of digits required to write the coordinates of P). If $\phi : X \to \mathbf{P}_n$ is a morphism, we define on $X(\mathbf{Q})$: $H_\phi(x) = H(\phi(x))$, $h_\phi(x) = h(\phi(x))$. If X is a projective variety, one associates to $\phi : X \to \mathbf{P}_n$ the divisor class $c_\phi \in \mathrm{Pic}(X)$ of the inverse image of a hyperplane section of $\mathbf{P}_n$. Then h_ϕ depends only on c_ϕ up to $O(1)$ (where $O(1)$ denotes a bounded function). Let $c \in \mathrm{Pic}(X)$; there are two morphisms ϕ and ψ such that $c = c_\phi - c_\psi$. We put $h_c = h_\phi - h_\psi$, which is defined up to $O(1)$. Then there are properties of the type $h_{c+c'} = h_c + h_{c'} + O(1)$. If moreover X is an abelian variety, there is the Néron normalisation of the height h_c: to every $c \in \mathrm{Pic}(X)$ is associated a well-defined function $\tilde{h}_c$. For simplicity, suppose that c is symmetric, that is to say $[-1]c = c$, where $[-1]$ is the morphism $x \mapsto -x$ on X. The Néron function is characterised by

$$\tilde{h}_c(nx) = n^2 \tilde{h}_c(x), \quad \text{for} \quad x \in X(\mathbf{Q}) \quad \text{and} \quad n \in \mathbf{Z}.$$

(In fact, this holds over $X(\bar{\mathbf{Q}})$.) This function $\tilde{h}_c$ is a quadratic form. There is also a decomposition of $\tilde{h}_c$ into local components.

1.2. The Mordell-Weil theorem and Mordell's conjecture.

The proof of the Mordell-Weil theorem divides into two steps.

The weak Mordell-Weil Theorem. Let A be an abelian variety defined over $\mathbf{Q}$, $\Gamma = A(\mathbf{Q})$ the group of rational points on A, and n an integer ≥ 1. *Then* $\Gamma/n\Gamma$ *is a finite group.*

The proof goes as follows. Suppose that $Y \to X$ is a finite étale covering of a projective variety X, where Y and X are defined over $\mathbf{Q}$. Let m be the degree of the covering. For each $x \in X(\mathbf{Q})$ we choose a lifting $y \in Y$. Let K_y be the field of rationality of y. Evidently, $[K_y : \mathbf{Q}] \leq m$. Further, one can show (Chevalley-Weil [CW]) that K_y is unramified outside a finite set of prime numbers $p_1, \ldots, p_h$, (depending only on X, Y and the covering map). But, by a theorem of Hermite, there are up to isomorphism only finitely many number fields of given discriminant and given degree. Thus the fields K_y are finite in number, and there is a number field K for which all rational points of X can be lifted to points of $Y(K)$ (that is to say, the image of $Y(K)$ contains $X(\mathbf{Q})$). One applies this to $Y = X = A$ and to the morphism $A \to A$ of multiplication by n. The finiteness of $\Gamma/n\Gamma$ follows easily.

The second part of the proof of the Mordell-Weil theorem is a descent argument using heights. Select an integer $n \geq 2$. Let x_i be representatives of the classes of Γ modulo $n\Gamma$. One shows that there is an integer r such that the points of Γ satisfying $h(x) \leq r$ generate Γ: choosing r large, if $h(x) > r$ one has that $x = ny + x_i$ with $y \in \Gamma$ and $h(y) < h(x)/2$; the proof then proceeds by induction.

As for Mordell's conjecture, it has been the subject of work of (a) Chabauty [Ch], (b) Demjanenko [D], and Manin [Ma1], (c) Mumford [Mu1], [and (d) Faltings [F]].

(a) Let X be an algebraic curve of genus ≥ 1 and J its jacobian. Suppose that the genus of X is strictly larger than the rank of $J(\mathbf{Q})$. Then $X(\mathbf{Q})$ is finite (Chabauty [Ch]).

(b) Let $x_0 \in X$. Let A be an abelian variety over $\mathbf{Q}$. Suppose that

$$\text{rank Hom}(X, A) > \text{rank } A(\mathbf{Q}),$$

where $\text{Hom}(X, A)$ denotes the group of morphisms from X to A which send x_0 to the neutral element of A. Then Demjanenko and Manin showed that $X(\mathbf{Q})$ is finite. This result has applications to modular curves.

(c) Let X be a curve of genus ≥ 2 over $\mathbf{Q}$. Suppose that it has an infinite number of rational points $P_1, P_2, \ldots$ ordered by increasing height. Then

Mumford proved,

$$h(P_n) \geq c_1 c_2^n, \text{ with } c_1 > 0, c_2 > 1.$$

[(d) Finally, Faltings proved Mordell's conjecture: if X is a curve of genus ≥ 2 over $\mathbf{Q}$, then $X(\mathbf{Q})$ is finite.]

1.3. Integral points on algebraic curves. Siegel's theorem.

Let X be an affine curve over $\mathbf{Q}$. and $\bar{X}$ its projective completion. The algebra Λ of regular functions on X is of finite type over $\mathbf{Q}$; let $x_1, \ldots, x_n \in \Lambda$ be a set of generators. A subset S of $X(\mathbf{Q})$ is *quasi-integral* if there is $\lambda \neq 0$ such that $x_i(S) \in (1/\lambda)\mathbf{Z} (1 \leq i \leq n)$; in other words, the $x_i(S)$ have bounded denominators. One checks that this condition is independent of the choice of generators.

Theorem (Siegel [Si]). *If $g \geq 1$, or if $g = 0$ and $\bar{X} - X$ has at least 3 elements, then all quasi-integral subsets are finite.*

The hypotheses of this theorem are necessary: if $g = 0$, the case of just one point at infinity corresponds to the affine line $\mathbf{A}_1$ (which has an infinite number of $\mathbf{Z}$-integral points), and the case where there are two points at infinity corresponds to the Pell-Fermat equation $X^2 - DY^2 = 1$.

Siegel's proof uses on the one hand, the weak Mordell-Weil theorem, and on the other hand a theorem on Diophantine approximation (Thue-Siegel-Roth theorem).

The idea consists of approximating the slope of an asymptote by rational numbers. For example, if the curve $X^3 - 3Y^3 = \text{const.}$ had an infinite number of integral points, one would immediately obtain better approximations of $3^{1/3}$ than are permitted by Roth's theorem. In the general case, one uses a theorem of bad approximation on abelian varieties:

Theorem. *Let A be an abelian variety defined over $\mathbf{Q}$, and let $x_1, x_2, \ldots$ be a sequence of distinct points of $A(\bar{\mathbf{Q}})$ converging to a point $x \in A(\mathbf{Q})$. Then*

$$\lim_{n \to \infty} \frac{\log 1/d(x, x_n)}{h(x_n)} = 0.$$

The proof uses Roth's theorem combined with the Mordell-Weil theorem.

The application to curves can be made in the following way:

Theorem. *Let X be a curve of genus ≥ 1 over $\mathbf{Q}$, f a non-constant rational function on X, and $x_1, x_2, \ldots$ an infinite number of distinct rational points. Put $f(x_i) = a_i/b_i, i = 1, 2 \ldots$, where, for $i \geq 1$, a_i and b_i are coprime integers. Then,*

$$\frac{\log |a_i|}{\log |b_i|} \to 1, \quad as \quad i \to \infty \quad .$$

For the proof, one embeds X in its jacobian and applies the theorem above.

1.4. Baker's Method.

For this method, the fundamental case is $g = 0$ with 3 points at infinity. The affine algebra of $\mathbf{P}_1 - \{0, 1, \infty\}$ is generated by 4 elements x, y, z, t with the relations

$$xy = 1, zt = 1, x + z = 1.$$

Therefore, associated to an integral point over K is a pair of units x, z of K with $x + z = 1$. More generally, the search for quasi-integral points reduces to the determination of pairs (x, z) of units of K satisfying some equation

$$Ax + Bz = C.$$

Expressing x, z in terms of a base of the group of units, one then uses Baker's theorem on lower bounds for linear forms in logarithms and obtains a finiteness result.

Other cases can be reduced to this by means of coverings; for example curves of genus 1 or curves of genus 2 with a pair of points invariant by the involution removed. Moreover the proof is *effective* (whereas Siegel's is not).

1.5. Hilbert's Irreducibility Theorem. Sieves.

Let C be an irreducible algebraic curve over $\mathbf{Q}$, and let $C \to \mathbf{P}_1$ be a morphism of degree $n \geq 2$. Then "few" rational points of $\mathbf{P}_1$ lift to rational points of C, and indeed, "most" points give extensions of degree n.

Equivalently, if X is the variable of $\mathbf{P}_1$ and $F(T, X) = 0$ is the equation of C, of degree n in T and irreducible over $\mathbf{Q}(X)$, there are "many" $x \in \mathbf{Q}$ for which $F(T, x)$ is irreducible over $\mathbf{Q}$.

The *rational* points of $\mathbf{P}_1$ with $H(P) \leq N$ which lift to rational points on C may be counted. Out of a total number $\sim cN^2$ rational points of height $\leq N$, the number of those which lift is