CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

1

Introduction

A fundamental fact about Diophantine equations is that there can be no algorithm determining whether a given equation is soluble in integers $\mathbf{Z}$ or not. This is the famous negative solution of Hilbert's tenth problem by M. Davies, H. Putnam, J. Robinson, Ju. Matijąsevič and G. Čudnovskiĭ. More precisely, there exists a polynomial $f(t; x_1, \dots, x_n)$ with integer coefficients such that there is no algorithm that would tell us whether for an integer t the equation $f(t; x_1, \dots, x_n) = 0$ is soluble in integers or not. The polynomial $f(t; x_1, \dots, x_n)$ can be made explicit, for instance, we can have $n = 13$ (see, for example, [Manin, L], VI).

In this book, however, we are mostly interested in the solubility of Diophantine equations in the field of rational numbers $\mathbf{Q}$ and more general number fields. In this case the analogue of Hilbert's tenth problem is still open. For homogeneous equations the existence of solutions in $\mathbf{Z}$ and in $\mathbf{Q}$ is, of course, equivalent provided one does not count the all-zero solution.

For certain classes of equations an algorithm deciding the solubility over $\mathbf{Q}$ can be found. Such is the case when a class of projective varieties defined over $\mathbf{Q}$ satisfies *the Hasse principle*. This principle consists in requiring that the obvious necessary conditions for the solubility of a system of homogeneous polynomial equations with integer coefficients $F_i(x_1, \dots, x_n) = 0, i = 1, \dots, m$, that is, the solubility of congruences modulo all the powers of prime numbers, and the solubility in the field of real numbers $\mathbf{R}$, be also sufficient. (The solubility of congruences modulo all powers of a prime number p is equivalent to the solubility in p-adic integers $\mathbf{Z}_p$.) If the Hasse principle holds, the problem of the existence of a rational point reduces to a purely local problem at finitely many critical places of $\mathbf{Q}$. The first non-trivial example when the Hasse principle holds is when we have one quadratic equation; this is the famous Minkowski–Hasse

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

theorem. However, very soon one encounters rather simple equations which are *counter-examples to the Hasse principle*: these are equations soluble in all completions of $\mathbf{Q}$, that is, $\mathbf{R}$ and the fields of p-adic numbers $\mathbf{Q}_p$ for all primes p, but not in $\mathbf{Q}$. Such are the homogeneous cubic equations $3x^3+4y^3+5z^3=0$ (Selmer) and $5x^3+9y^3+10z^3+12t^3=0$ (Cassels and Guy), where one of course excludes the all-zero solution. The first of these equations defines a smooth projective curve of genus 1, and the second one defines a smooth cubic surface. Despite the failure of the Hasse principle there are reasons to believe that for cubic equations in any number of variables there does exist an algorithm telling us whether a given equation is soluble or not.

In the middle of the twentieth century, the Minkowski–Hasse theorem motivated Mordell, Selmer, Châtelet and others in their search for other cases of the Hasse principle and similar local-to-global principles, and in the analysis of the cases when it fails. In the course of this were discovered concepts of particular significance such as the Selmer group of an elliptic curve, the Tate–Shafarevich group, and the Cassels–Tate form on it, and finally, its vast generalization, the Manin obstruction to the Hasse principle.

It was Manin who found a first general obstruction to the Hasse principle, and a good substitute to the Hasse principle when it does not hold is the statement that *the Manin obstruction to the Hasse principle is the only obstruction*. This means that as long as a collection consisting of a real solution and p-adic solutions for all primes p satisfies certain conditions, there also exists a solution in $\mathbf{Q}$. These conditions, provided by the Brauer-Grothendieck group of the variety, are based on the global reciprocity law. To verify each condition requires finitely many elementary operations, and, in the ideal cases, there are only finitely many such conditions. The Manin obstruction to the Hasse principle is known to be the only obstruction for many types of homogeneous spaces of linear algebraic groups (Sansuc, Borovoi, building on the results of Kneser, Harder, Chernousov; the first counter-example to the Hasse principle for a principal homogeneous space of a semisimple group was found by Serre). This is one possible generalization of the Minkowski–Hasse theorem for quadrics. In another direction, computer calculations along with various partial or conditional results provide ample evidence that the Manin obstruction to the Hasse principle is the only obstruction for varieties given by one cubic or two quadratic equations. Most of these results were obtained using a generalization of the classical descent on cubic curves by Colliot-Thélène and Sansuc, who were

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

motivated by some pioneering computations of Swinnerton-Dyer. They introduced an important notion of universal torsors which encompasses descent on projective varieties with finitely generated geometric Picard group.

What happens next? Can we still hope for the existence of an algorithm when the Manin obstruction fails to be the only obstruction to the Hasse principle? The first counter-example to the Hasse principle not accounted for by the Manin obstruction was recently found by the author. It is a bielliptic surface over $\mathbf{Q}$, and can be given by two homogeneous quartic equations in five variables. Here again, but for a different reason, we believe that for such systems of equations a solubility algorithm should exist. To explain why we need to introduce *torsors*.

Suppose that we have a variety X over a field k, and an algebraic k-group G which can be finite or not. An X-torsor under G is a pair consisting of a morphism $Y \to X$ and an action of G on Y preserving f, which is locally (in an appropriate topology) a direct product. From the point of view of the geometric invariant theory a torsor is simply a variety Y equipped with a free (in the scheme-theoretic sense) action of G such that X is the quotient of Y by this action. One extreme case is when X is a point, $X = Spec(k)$, and G is a connected algebraic group, say an abelian variety or a linear group. Then k-torsors Y under G are also known under the classical name of *principal homogeneous spaces* of G. Another classical situation is when a finite group G acts freely on Y; then Y is an unramified Galois covering of $X = Y/G$ with group G.

Suppose that Y is a principal homogeneous space of an elliptic curve E defined over k, G is a finite subgroup of E, and $X = Y/G$. Assume that X has rational points over all completions of k. Then the classical procedure of *descent* sometimes tells us that X contains no k-rational point[1].

The descent method can be described for general torsors. One associates to an X-torsor Y under G and a k-torsor P under G a *twist* of Y by P, denoted by ${}_PY$. In practice a k-torsor P under G is represented by a 1-cocycle of the Galois group of k with coefficients in G. The twist ${}_PY$ is an X-torsor under a certain twisted form of G, which is G itself when G is abelian. Suppose now that X has points everywhere locally, that is, in all completions of k. Given a torsor $Y \to X$ the following descent method

[1] There are other applications of descent: when $Y = E$ the descent can be used to bound the number of generators of the group of k-rational points of E. In the weak Mordell–Weil theorem this is used to prove that the quotient of the group of rational points $E(k)$ of an elliptic curve E over a number field k by $mE(k)$ is finite for any $m \in \mathbf{Z}$.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

can sometimes tell us that X has no k-rational point. It is possible to determine a finite set of k-torsors P under G such that if ${}_PY$ has points everywhere locally, then P is isomorphic to a k-torsor in this set. For example, if G is finite, and $Y \to X$ is an isogeny of elliptic curves, then this set is none other than the Selmer group associated to this isogeny. If no twist ${}_PY$ has points everywhere locally, this is an obstruction to the Hasse principle. Indeed, if X has a k-point M, then twisting Y by the k-torsor given by the fibre Y_M we arrive at a twisted torsor with a k-point in the fibre over M, hence in particular with points everywhere locally. We call this obstruction *the descent obstruction*. It was introduced by Colliot-Thélène and Sansuc in the case when G is a torus, but was already widely used in the classical descent theory on elliptic curves, where G is finite abelian. This was extended to the case of non-commutative groups by D. Harari and the author.

The point is that, at least in principle, this 'neo-classical' descent obstruction is computable in finitely many elementary operations: we only have to check the local solubility of a finite family of torsors in finitely many critical places. Another important feature is that the Manin obstruction can be recovered as a particular case of the descent obstruction. There are natural torsors attached to the varieties we discussed above: for cubic curves G is finite and abelian, for cubic surfaces G is a torus, and for bielliptic surfaces G is a finite nilpotent group of class 2. The counter-example to the Hasse principle not explained by the Manin obstruction, which we mentioned above, is explained by the descent obstruction related to a torsor under such a finite nilpotent group.

This book consists of two parts. The first part concerns the theory of torsors in general, and the second part is devoted to applications of torsors to the arithmetic of varieties over number fields. The general theory is given in Chapter 2. It is not surprising that a satisfactory classification is available in the abelian case, more precisely, for torsors under groups of multiplicative type (these are extensions of finite abelian group schemes by tori). We illustrate the general concepts by considering in detail some important examples of torsors in Chapter 3. These are quotients by 'generically free' torus actions and homogeneous spaces of algebraic groups. We consider the quotient of the Grassmannian $G(2,5)$ by the action of a maximal torus of $PGL(5)$, explicit 2- and 4-coverings of elliptic curves, the universal covering of a semisimple group. Chapter 4 deals with specific properties of torsors under groups of multiplicative type. The main result here is a description of certain torsors by explicit equations, which is a gen-

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

eral set-up of 'explicit descent'. This is illustrated on the example of some natural torsors on hyperelliptic curves and conic bundle surfaces. In Chapter 5 we define the number-theoretic obstructions to the Hasse principle and to various approximation properties. The main theorem in Chapter 6 describes an important particular case of the Manin obstruction (the so called 'algebraic' Manin obstruction) in terms of the descent obstruction associated with torsors under groups of multiplicative type.

For this book we selected three recent applications of these general methods. In Chapter 7 we prove that the Manin obstruction to the Hasse principle is the only obstruction on some surfaces fibred into conics over the projective line, including some cases with six degenerate fibres. In Chapter 8 we study a surface of a different kind, which is a counter-example to the Hasse principle not explained by the Manin obstruction but explained by the non-abelian descent obstruction. In Chapter 9 using the language of gerbs we prove that the homogeneous spaces of (simply connected) semi-simple groups with connected stabilizers also have the property that the Manin obstruction is the only obstruction to the Hasse principle. These last three chapters illustrate different methods one uses, besides the theory of torsors, in studying the arithmetic of rational points in three main cases where some understanding of the Hasse principle is available. Roughly speaking, these are varieties which are either (1) close to rational varieties (quadrics, families or intersections of such, cubics, etc.), or (2) close to abelian varieties, or (3) close to affine algebraic groups (with methods using the group structure).

Note that the descent method has other important applications: the study of the R-equivalence classes of rational points, of the group of 0-cycles; descent provides an obstruction to weak approximation, etc. The scope of this book did not permit us to treat these and other important subjects closely related to the descent techniques. Some of this material is covered in the survey articles [C86], [C87], [C92], [C95], [C98], [MT], [Sansuc 82], [Sansuc 87], [SD96]. Another noticeable omission is the theory of the Brauer group.

Acknowledgements. The subject of this book owes its existence to the pioneering ideas of Yuri Ivanovich Manin and Sir Peter Swinnerton-Dyer, and the conceptual framework laid out by Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. I would like to thank Jean-Louis Colliot-Thélène for his generosity and openness. I am grateful to David Harari for permission to include here parts of our yet unpublished work, and for his comments. Thanks are due to M. Borovoi, B. Kunyavskiĭ and T. Szamuely for their

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

comments, and to S. Siksek for his help with 4-descent. A large part of this book was written at I.H.E.S. (Bures-sur-Yvette) whose hospitality is gratefully acknowledged. I thank my wife Anna for suggesting the epigraph.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

Part one

TORSORS

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

Notation and conventions. In this part k is a field of characteristic 0 (unless otherwise stated, often a less restrictive condition would be enough); $\overline{k}$ denotes a separable closure of k, $\Gamma_k = Gal(\overline{k}/k)$. By a *variety* over k we mean a separable scheme of finite type $p : X \to Spec(k)$. If X is a k-variety we write the action of Γ_k on the set of $\overline{k}$-points $X(\overline{k})$ by $(g, x) \mapsto {}^g x$, where $g \in \Gamma_k, x \in X(\overline{k})$. For a k-variety X we write $\overline{X} = X \times_k \overline{k}$.

We employ the notation $k[X] = \Gamma(X, \mathcal{O})$, $k[X]^* = \Gamma(X, \mathcal{O}^*)$. The set of Z-morphisms of Z-schemes $Y \to Y'$ is denoted by $Mor_Z(Y, Y')$, in particular, $Mor_k(X, \mathbf{A}^1_k) = k[X]$.

Let $\mathbf{G}_m = \mathbf{G}_{m,\mathbf{Z}} = Spec(\mathbf{Z}[t, t^{-1}])$, this is a group scheme over $Spec(\mathbf{Z})$, which as a scheme is isomorphic to $\mathbf{A}^1_{\mathbf{Z}} \setminus \{0\}$. We have $Mor_k(X, \mathbf{G}_{m,k}) = k[X]^*$.

Unless otherwise stated all cohomology and sheaves are understood in the sense of the étale topology. The sheaf $\mathbf{G}_m$ over a scheme X is defined by $\mathbf{G}_m(U) = \Gamma(U, \mathcal{O}^*) = Mor_X(U, \mathbf{G}_{m,X})$ for $U \to X$ étale. A group scheme G over Z is called a *Z-group of multiplicative type* if it is locally (for the étale topology) a group subscheme of $\mathbf{G}^n_{m,Z}$ for some n. Torsors under groups of multiplicative type will be sometimes referred to as *abelian torsors*. A group scheme G over Z is called a *Z-torus* if it is locally isomorphic to $\mathbf{G}^n_{m,Z}$ for some n.

The *Brauer group* $\mathrm{Br}(X)$ throughout this book is understood as the cohomological Brauer–Grothendieck group $H^2(X, \mathbf{G}_m)$. Let $\mathrm{Br}_0(X)$ (resp. $\mathrm{Br}_1(X)$) be the image of the natural map $p^* : \mathrm{Br}(k) \to \mathrm{Br}(X)$ (resp. the kernel of the natural map $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})^{\Gamma_k}$).

By $M[n]$ we denote the n-torsion subgroup of an abelian group M. If M is a discrete Γ_k-module we shall write $H^i(k, M)$ for the Galois cohomology groups $H^i(\Gamma_k, M)$. If R is a commutative ring, and $\mathcal{F}$ is a sheaf over $Spec(R)$ we write $H^i(R, \mathcal{F})$ for $H^i(Spec(R), \mathcal{F})$.

The notation $Ext^n_k(\cdot, \cdot)$ (resp. $Ext^n_X(\cdot, \cdot)$, resp. $Ext^n_{k\text{-groups}}(\cdot, \cdot)$) stands for the group of n-fold extensions in the category of Γ_k-modules (resp. of sheaves over X, resp. of commutative algebraic k-groups). We write $\mathcal{H}om_X$ for the internal Hom of sheaves on X, and $\mathcal{H}om_k$ for the internal Hom of sheaves on $Spec(k)$.

An *algebraic k-group* is a k-group scheme which is a smooth variety over k (hence of finite type). Recall that any algebraic group is quasi-projective as an algebraic variety. An algebraic k-group S such that $\overline{S}$ is a group subscheme of $\mathbf{G}^n_{m,\overline{k}}$ for some n is a k-group of multiplicative type. A connected k-group of multiplicative type is a k-torus. The *module of characters* of S is $Hom_{k\text{-groups}}(S, \mathbf{G}_m)$; it is denoted by $\hat{S}$. Associating $\hat{S}$ to S defines an anti-equivalence of the category of k-groups of multiplicative

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

type with the category of discrete Γ_k-modules which are of finite type as abelian groups. If $\tau : S_1 \to S_2$ is a homomorphism of k-groups of multiplicative type, then we denote by $\hat{\tau} : \hat{S}_2 \to \hat{S}_1$ the dual map of Γ_k-modules, and vice versa. A k-group S of multiplicative type is a torus if and only if $\hat{S}$ is torsion free. A k-torus is called *quasi-trivial* if its module of characters is a *permutation* Γ_k*-module*, which means by definition that it has a Γ_k-invariant basis.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-80237-6 - Torsors and Rational Points
Alexei Skorobogatov
Excerpt
More information

2

Torsors: general theory

The aim of the first two sections of this chapter is to review the general theory of torsors with its useful tools, like twisting by Galois, *fppf* or étale descent, Čech cohomology, contracted product. We included only the concepts relevant for our purposes in this book, and the reader who needs to know more is referred to [Milne, EC], [BLR] and [Giraud]. The reader interested in applications of torsors can skip most of Section 2.2 in the first reading.

Section 2.3 contains the theory of torsors under groups of multiplicative type which is due to Colliot-Thélène and Sansuc. This theory is much more precise than the general case. Here belongs the notion of *the type* of the torsor, and that of *universal torsors*, which leads to the so called *elementary obstruction* to the existence of rational points (defined over arbitrary fields).

In the final section we relate this elementary obstruction to another one, earlier defined by Grothendieck. It is the class of the well known natural extension of the absolute Galois group of k by the (geometric) fundamental group of $\overline{X}$, given by the algebraic fundamental group of X. The significance of this obstruction for the study of rational points remains to be explored.

2.1 Torsors over a field

Let us start by recalling the definition of torsors under an algebraic (possibly non-abelian) group defined over a field k. An unsurpassed exposition of the first non-abelian cohomology set is found in [Serre, CG], I.5, and the reader is expected to be to a certain extent familiar with it. Torsors (in other terminology, principal homogeneous spaces) are discussed in [Serre, GA], V.4.21 and [Serre, CG], III.1.

Let G be an algebraic group defined over k. Its left action on itself

© Cambridge University Press www.cambridge.org