TORSORS AND THE BRAUER GROUP IN NUMBER THEORY

ALEXEI SKOROBOGATOV

Talks[1] at the Independent University Moscow, 2005, Imperial College London, 2007

1. What is the fundamental group?

1.1. **Definition.** Let k be a field of characteristic 0, and let $\overline{k}$ denote an algebraic closure of k, Γ =Gal$(\overline{k}/k)$. Let X be a k-scheme. A base point $\bar{x} \in X(\overline{k})$ defines the functor $F_{\bar{x}}$ from the category of finite étale coverings of X to the category of sets: $F_{\bar{x}}(Y/X) = Y_{\bar{x}}$. Grothendieck defined the fundamental group $\pi_1(X, \bar{x})$ as the automorphism group of this fibre functor,

$$\pi_1(X, \bar{x}) = \mathrm{Aut}\, F_{\bar{x}}.$$

This says that $\pi_1(X, \bar{x})$ acts by permutations of the points of the finite set $Y_{\bar{x}}$, and if Y'/X is a finite étale covering that factors through Y/X, then the natural map $Y'_{\bar{x}} \to Y_{\bar{x}}$ is $\pi_1(X, \bar{x})$-equivariant.

The fundamental group $\pi_1(X, \bar{x})$ is a covariant functor on the category of schemes over $\overline{k}$ with a marked $\overline{k}$-point. Indeed, if $(X', \bar{x}')$ maps to $(X, \bar{x})$, then the fibre of $Y \times_X X'$ over $\bar{x}'$ is the same as the fibre of Y over $\bar{x}$, so that $\mathrm{Aut}\, F_{\bar{x}'}$ acts on it.

In particular, we obtain homomorphisms $\pi_1(\overline{X}, \bar{x}) \to \pi_1(X, \bar{x})$, where $\overline{X} = X \times_k \overline{k}$, and $\pi_1(X, \bar{x}) \to \Gamma$. If X is a geometrically connected variety over k, then we actually have the fundamental exact sequence

$$1 \to \pi_1(\overline{X}, \bar{x}) \to \pi_1(X, \bar{x}) \to \Gamma \to 1. \tag{1}$$

By functoriality, any k-point defines a section of the map $\pi_1(X, \bar{x}) \to \Gamma$. This gives a necessary condition for the existence of k-points.

Another approach to (1) is via Galois theory. Fix an algebraic closure of $k(X)$, and let K be its maximal unramified subfield, that is, unramified with respect to all the discrete valuation rings in $k(X)$ whose valuation is trivial on k. Define $\pi_1(X)$ =Gal$(K/k(X))$; then (1) becomes the exact sequence of Galois groups corresponding to $k(X) \subset \overline{k}(X) \subset K$. (The field K is the filtered union of the function fields $k(Y)$, for all connected finite étale coverings Y/X.)

1.2. **Finite torsors.** Let Y/X be a finite étale Galois covering with group G, that is, $k(Y)$ is a Galois extension of $k(X)$ with Galois group G. Then G acts on Y preserving the fibres of Y/X in such a way that $G = \mathrm{Aut}\,(Y/X)$. This property shows that G has a natural

[1] Email your comments and questions to `a.skorobogatov@imperial.ac.uk`

action of Γ turning it into a finite k-group scheme. The action of G on Y defines a canonical isomorphism of k-schemes

$$Y \times_X Y = Y \times_k G. \tag{2}$$

By definition (see below) Y/X is an X-torsor under G. Thus the notion of a finite torsor can be used as a shorthand for that of a finite étale Galois covering.

1.3. **Sections and pro-coverings.** A projective system (Y_i) of finite X-torsors is called a *pro-covering* (M. Stoll) if for any finite $\overline{X}$-torsor $\overline{Y}$ there exists i and a morphism of $\overline{X}$-torsors $\overline{Y}_i \to \overline{Y}$. This means that there is a morphism of structure groups $\overline{G}_i \to \overline{G}$ such that the natural diagram commutes

$$\begin{tikzcd}
\overline{Y}_i \arrow[d] & \times & \overline{G}_i \arrow[r] \arrow[d] & \overline{Y}_i \arrow[d] \\
\overline{Y} & \times & \overline{G} \arrow[r] & \overline{Y}
\end{tikzcd}$$

Proposition 1.1. *There is a natural bijective correspondence between the isomorphism classes of pro-coverings and sections of* (1) *considered up to conjugation in* $\pi_1(\overline{X}, \bar{x})$*. Under this correspondence the section defined by* $P \in X(k)$ *corresponds to a pro-covering that lifts* P *(there is a compatible system of* k*-points in each* Y_i *over* P*).*

A section $\sigma : \Gamma \to \pi_1(X, \bar{x})$ defines the invariant subfield $K^{\sigma(\Gamma)}$ such that k is algebraically closed in $K^{\sigma(\Gamma)}$, and $\bar{k}K^{\sigma(\Gamma)} = K$. This field is a filtered union of finite Galois extensions $K_i/k(X)$. Define Y_i as the normalization of X in K_i. Then (Y_i) is a pro-covering.

In general, Γ acts on $\pi_1(\overline{X}, \bar{x})$ by outer automorphisms, but a section defines a Γ-action on $\pi_1(\overline{X}, \bar{x})$. A pro-covering is morally an X-torsor under $\pi_1(\overline{X}, \bar{x})$. So we get a map

$$X(k) \to \mathrm{H}^1_{cont}(\Gamma, \pi_1(\overline{X}, \bar{x})).$$

The following statement was pointed out to us by A. Pal. We let Aut $(\overline{Y}/X)$ denote the group of semi-linear automorphisms of $\overline{Y}$, i.e. the automorphisms that are allowed to act non-trivially on $\bar{k}$.

Proposition 1.2. *Let* X *be a geometrically connected and reduced variety over* k*. If the fundamental exact sequence* (1) *has no section, then there exists a finite étale Galois covering* $\overline{Y}/\overline{X}$ *whose Galois group* $G = \mathrm{Aut}\,(\overline{Y}/\overline{X})$ *is a characteristic subgroup of* $\pi_1(\overline{X}, \bar{x})$*, such that the push-out sequence*

$$1 \to G \to \mathrm{Aut}\,(\overline{Y}/X) \to \mathrm{Gal}(\bar{k}/k) \to 1$$

has no section.

The last sequence defines a gerb; the gerb is neutral if and only if the sequence is split.

2. What is a torsor?

2.1. **The definitions of a torsor.** Let G be an algebraic group over k, and let X be a smooth k-variety. Here is a naïve geometric definition of a torsor.

Definition 2.1. An X-*torsor* under the group G is a surjective morphism $f : Y \to X$, where Y is equipped with an action of G which preserves the fibres of f, and which is simply transitive on the geometric fibres.

Equivalently, G acts freely on Y, and X is the space of orbits Y/G. Note however that 'freely' should be understood in the scheme-theoretic sense, see Mumford's "Geometric Invariant Theory". An obvious example of a torsor is the "trivial torsor" $Y = X \times_k G$.

The *action* of G on Y is a morphism $\sigma : G \times_k Y \to Y$ satisfying the obvious properties which say that $g_1 g_2$ acts as g_2 followed by g_1, and that the neutral element of G acts as the identity morphism $Y \to Y$. Consider the morphism

$$\Psi = (p_1, \sigma) : Y \times_k G \to Y \times_k Y,$$

where p_1 is the first projection. To make Definition 2.1 precise we need a more conceptual definition of freeness. The action σ is *free* if Ψ is a closed embedding. In particular, the orbit Gy of any $\overline{k}$-point y is closed and isomorphic to G, so that the action is free in the set-theoretic sense (all stabilizers are trivial). (Definition 2.1 is valid as stated if G is finite, or if G is affine and f is an affine morphism. The first statement is not very hard, but the second one is much harder – it is a consequence of Luna's étale slice theorem.)

More often, however, one defines torsors topologically:

Definition 2.2. A *torsor* is a morphism $f : Y \to X$ together with a group action of G on Y such that "locally in étale topology", Y is isomorphic as a scheme over X to the "trivial torsor" $X \times_k G$. More precisely, this means that there exists a family of étale (quasi-finite, unramified) maps $\pi_i : U_i \to X$ whose images cover X, such that

$$U_i \times_X Y \cong U_i \times_k G\,,$$

where each isomorphism respects the action of G.

When G is finite, Definition 2.2 amounts to saying that the map

$$Y \times_k G \to Y \times_X Y, \quad (y, g) \mapsto (y, gy)$$

is an isomorphism. Indeed, if $Y \to X$ is a torsor under a finite k-group, then Definition 2.2 implies that Y is étale over X (it is a local property). Thus we can choose an étale open covering of X consisting of a single "open set" Y.

2.2. **Examples of torsors.** 1) Let X be a point, $X = \mathrm{Spec}(k)$. "Y is a k-torsor (or $\mathrm{Spec}(k)$-torsor) under G" means that G acts on Y in such a way that over $\overline{k}$, this is isomorphic to G acting on itself by translations. For instance, Y is a curve of genus 1 and G the Jacobian of Y. Or, G is the 1-dimensional torus given by $x^2 - ay^2 = 1$ (called the *norm torus*) and Y is given by $x^2 - ay^2 = c$, for $a, c \in k^\times$. In general we have a natural bijection

$$\{k\text{-torsors under } G\}/\mathrm{iso} \quad \longleftrightarrow \quad \mathrm{H}^1(k, G) := \mathrm{H}^1_{cont}(\mathrm{Gal}(\overline{k}/k), G(\overline{k}))\,,$$

where $G(\overline{k})$ is given discrete topology. Note that if G is not commutative, then $\mathrm{H}^1(k,G)$ is a set (in general it does not have a natural group structure) with a distinguished element, the class of a trivial torsor.

2) The natural morphism $\mathbf{A}_k^{n+1}\setminus\{0\}\to\mathbf{P}_k^n$ is a torsor under the multiplicative group $\mathbf{G}_m$.

3) Let G be a connected reductive algebraic k-group, for example, a semisimple group like $\mathrm{SL}(n)$, $\mathrm{PGL}(n)$, $\mathrm{SO}(n)$, a torus like $\mathbf{G}_m^n$, or an extension of a torus by a semisimple group, like $\mathrm{GL}(n)$. Suppose that Y is a smooth, projective and geometrically irreducible variety with an action of G, such that there exists a G-linearized ample invertible sheaf L on Y. (This means that the action of G extends to a linear action on L; if L is very ample this means that the action of G on Y comes from a representation of G in $\mathrm{H}^0(Y,L)$.) Let Y^s denote the stable points of Y, in the sense of the Geometric Invariant Theory. This is an open (possibly empty) subset of Y. There is a morphism $Y^s\to X$ whose fibres are the orbits of G. In the language of GIT X is a "geometric quotient" of Y^s. If some quotient of G acts freely on Y^s, then $Y^s\to X$ is an X-torsor. Interesting examples are obtained when Y is the Grassmannian variety $\mathrm{G}(m,n)$ and G is a maximal torus in $\mathrm{GL}(n)$, or when $Y=(\mathbf{P}_k^n)^m$ and $G=$PGL$(n+1)$. For instance, the natural action of $\mathbf{G}_m^5$ on the affine cone over $\mathrm{G}(2,5)$ (re-scaling the coordinates of the 5-dimensional vector space) gives rise to the universal torsor on the blowing-up of four points in general position on $\mathbf{P}^2$ (the del Pezzo surface of degree 5).

4) Let $1\to G\to H\to F\to 1$ be an extension of algebraic groups. Definition 2.1 implies that $H\to F$ is an F-torsor under G. If G is semisimple, and G^{sc} is a semisimple group which is a simply connected covering of G, then the isogeny $G^{sc}\to G$ is a universal torsor.

5) Let E be an elliptic curve. An n-covering $C\to E$ is a map which over $\overline{k}$ becomes the multiplication by n. (In other words, C is a twisted form of E by the action of $E[n]$ on E by translations.) Any n-covering is an E-torsor under $G=E[n]$. Further, if D is an mn-covering of E and the covering map factors as $D\to C\to E$, then $D\to C$ is a C-torsor under $G=E[m]$ (and $C=D/E[m]$).

6) Let $p_1(x)$ and $p_2(x)$ be co-prime separable polynomials, and let X and Y be the affine curves defined by

$$X: y^2=p_1(x)p_2(x)$$

$$Y:\begin{cases} y_1^2=\alpha p_1(x) \\ y_2^2=\dfrac{1}{\alpha}p_2(x)\end{cases}\qquad \text{for } \alpha\in k^\times.$$

Then the degree 2 map $Y\to X:(y_1,y_2,x)\mapsto(y_1y_2,x)$ is a torsor under $G=\mathbb{Z}/2$. Actually, any unramified double covering has a unique structure of a torsor under $\mathbb{Z}/2$.

7) Similarly, if X and Y are the affine varieties given by

$$X: y^2-az^2=p_1(x)p_2(x)$$

$$Y:\begin{cases} y_1^2-az_1^2=\alpha p_1(x) \\ y_2^2-az_2^2=\dfrac{1}{\alpha}p_2(x)\end{cases}$$

then the map $Y\to X$ given by $(y_1+\sqrt{a}z_1)(y_2+\sqrt{a}z_2)=y+\sqrt{a}z$ is a torsor under the norm torus $y^2-az^2=1$.

2.3. **Torsors under groups of multiplicative type.** We write $\overline{X} = X \times_k \overline{k}$, and denote by $\overline{k}[X]^*$ the group of invertible regular functions on $\overline{X}$. Such a function is the same thing as a morphism $\overline{X} \to \mathbf{G}_{m,\overline{k}}$.

A commutative algebraic k-group G *of multiplicative type* is an extension of a finite commutative k-group by a k-torus. The *module of characters* $\widehat{G}$ =Hom$(\overline{G}, \mathbf{G}_{m,\overline{k}})$ of G is an abelian group of finite type acted on by Γ. (We take the Hom in the category of commutative $\overline{k}$-groups.) G is a torus if and only if $\widehat{G}$ is torsion-free. One proves that the category of k-groups of multiplicative type is anti-equivalent to the category of continuous Γ-modules, which are of finite type as abelian groups. The tori are the groups which over $\overline{k}$ become isomorphic to $\mathbf{G}_m^n$ for some n. We have encountered tori in the examples 1, 2, 3, 4 and 7.

Torsors under groups of multiplicative type are the nicest of all torsors. First of all, an X-torsor under the multiplicative group $\mathbf{G}_m$ is a line bundle over X with the zero section removed. So these objects are parameterized by the elements of the Picard group $\mathrm{Pic}\, X = \mathrm{H}^1(X, \mathbf{G}_m)$. (Here we mean étale topology, but the same result is obtained if one uses Zariski topology.) It is a general fact that torsors under a commutative group G are classified by the étale cohomology group $\mathrm{H}^1(X, G)$. We shall not need a definition of this group, but we shall amply use its various functoriality properties.

The canonical $\cup$-paring

$$\mathrm{H}^1(\overline{X}, \overline{G}) \times \hat{G} \to \mathrm{H}^1(\overline{X}, \mathbf{G}_m) = \mathrm{Pic}\, \overline{X}$$

gives rise to the map $\mathrm{H}^1(\overline{X}, \overline{G}) \to \mathrm{Hom}(\hat{G}, \mathrm{Pic}\, \overline{X})$. Combining it with the canonical map $\mathrm{H}^1(X, G) \to \mathrm{H}^1(\overline{X}, \overline{G})$ we obtain the map $\mathrm{H}^1(X, G) \to \mathrm{Hom}_\Gamma(\hat{G}, \mathrm{Pic}\, \overline{X})$. The image of the class of a torsor Y/X with structure group G under this map is called the *type* of Y/X.

An elegant and useful description of $\mathrm{H}^1(X, G)$, where G is a k-group of multiplicative type, is provided by the following exact sequence of Colliot-Thélène and Sansuc:

$$(3) \quad 0 \to \mathrm{Ext}^1_k(\widehat{G}, \overline{k}[X]^*) \to \mathrm{H}^1(X, G) \to \mathrm{Hom}_\Gamma(\widehat{G}, \mathrm{Pic}\, \overline{X}) \to \mathrm{Ext}^2_k(\widehat{G}, \overline{k}[X]^*) \to \mathrm{H}^2(X, G).$$

If X is such that $\overline{k}[X]^* = \overline{k}^*$, then this looks a bit simpler:

$$(4) \qquad 0 \to \mathrm{H}^1(k, G) \to \mathrm{H}^1(X, G) \xrightarrow{\chi} \mathrm{Hom}_\Gamma(\widehat{G}, \mathrm{Pic}\, \overline{X}) \xrightarrow{\partial} \mathrm{H}^2(k, G) \to \mathrm{H}^2(X, G).$$

The map χ sends the class of torsor to its type (up to sign). When k is algebraically closed, then (4) shows that a torsor is determined by its type up to isomorphism (more generally, the same is true for split tori $T \simeq \mathbf{G}_m^n$ by Hilbert's theorem 90).

Remark. The maps $\mathrm{H}^i(k, G) \to \mathrm{H}^i(X, G)$ in (4) are induced by the structure morphism $p : X \to \mathrm{Spec}(k)$. Consequently, these maps are injective if $X(k) \neq \emptyset$, since a k-point is a section of p. Thus *torsors of any given type exist if X has a k-point.*

Definition 2.3 (Colliot-Thélène–Sansuc)**.** An X-torsor under a group of multiplicative type is *universal* if its type is an isomorphism.

The universal torsors make sense only for varieties X such that $\mathrm{Pic}\, \overline{X}$ is finitely generated as an abelian group. If X is projective, this is equivalent to the condition $\mathrm{H}^1(X, \mathcal{O}_X) = 0$.

It follows from the exact sequence (4) that universal torsors have a universal property similar to the universal property of pro-coverings: if Y/X is a universal torsor and $\overline{Y}'/\overline{X}$ a torsor under a group of multiplicative type, then there is a morphism of $\overline{X}$-torsors $\overline{Y} \to \overline{Y}'$.

When do universal torsors exist? Let X be a smooth variety over k such that $\operatorname{Pic}\overline{X}$ is finitely generated and $\overline{k}[X]^* = \overline{k}^*$. Colliot-Thélène and Sansuc proved that universal torsors on X exist if and only if the natural sequence of discrete Γ-modules

$$1 \to \overline{k}^* \to \overline{k}(X)^* \to \overline{k}(X)^*/\overline{k}^* \to 1$$

is split. They also proved that this occurs if and only if the natural sequence of discrete Γ-modules

$$1 \to \overline{k}^* \to \overline{k}[U]^* \to \overline{k}[U]^*/\overline{k}^* \to 1$$

is split, where $U \subset X$ is a dense open subset such that $\operatorname{Pic}\overline{U} = 0$. Note that the abelian group $\overline{k}[U]^*/\overline{k}^*$ is free of finite rank. Indeed, it fits into the exact sequence

$$1 \to \overline{k}[U]^*/\overline{k}^* \to \operatorname{Div}_{\overline{X}\setminus\overline{U}}\overline{X} \to \operatorname{Pic}\overline{X} \to \operatorname{Pic}\overline{U} = 0,$$

where $\operatorname{Div}_{\overline{X}\setminus\overline{U}}\overline{X}$ is freely generated by the 'components at infinity', that is, by the irreducible components of $\overline{X} \setminus \overline{U}$.

Example Let X be a smooth compactification of the affine surface $U \subset \mathbf{A}^3$ given by the equation $y^2 - bz^2 = af(x)$, where a, $b \in k^*$, and $f(x)$ is a separable monic polynomial. The universal torsors on X exist if and only if a is a product of a norm from $k(\sqrt{b})$ and a norm from $k[x]/(f(x))$. For instance, this condition is satisfied if $f(x)$ has a root $\alpha \in k$, but then $(\alpha, 0, 0)$ is a k-point in X.

There are classes of varieties over arithmetically interesting fields for which the existence of universal torsors implies the existence of k-points. Such are forms of projective spaces, quadrics, and more generally, homogeneous spaces of algebraic groups with connected stabilizers over p-adic fields. (The same is true for number fields if the group is linear.)

2.4. **Relation to the fundamental group.** Let $\pi_1^{ab}(\overline{X})$ be the abelianization of $\pi_1(\overline{X}, \overline{x})$ in the category of profinite groups. We can omit the base point since the abelianized fundamental groups for different choices of the base point are canonically isomorphic. Consider the push-out of the fundamental sequence (1) in the case of the open set $U \subset X$ as above, with respect to the abelianization map $\pi_1(\overline{U}, \overline{u}) \to \pi_1^{ab}(\overline{U})$:

$$1 \to \pi_1^{ab}(\overline{U}) \to P \to \Gamma \to 1. \tag{5}$$

The abelianized fundamental group $\pi_1^{ab}(\overline{U})$ is easy to compute. The geometric class field theory produces canonical isomorphisms of Γ-modules:

$$\pi_1^{ab}(\overline{U}) = \lim_{\leftarrow} \pi_1^{ab}(\overline{U})/n, \quad \text{where} \quad \pi_1^{ab}(\overline{U})/n = Hom(H^1(\overline{U}, \mu_n), \overline{k}^*),$$

and the Kummer sequence gives an exact sequence of Γ-modules

$$0 \to (\overline{k}[U]^*/\overline{k}^*)/n \to H^1(\overline{U}, \mu_n) \to Pic(\overline{U})[n] \to 0.$$

Proposition 2.4. *Let X be a smooth and geometrically integral variety over k such that $\overline{k}[X]^* = \overline{k}^*$, and $Pic(\overline{X})$ is a finitely generated abelian group. Let $U \subset X$ be a dense open subset such that $Pic(\overline{U}) = 0$. Then the universal torsors on X exist if and only if* (5) *is split.*

Indeed, D. Harari and the author proved that the universal torsors on X exist if only if the pushed-out of (5) by the mod n map is split for all n. The proof of the following lemma was kindly provided to us by A. Pal.

Lemma 2.5. *Let $1 \to A \to B \to C \to 1$ be an exact sequence of profinite groups and continuous homomorphisms, where A is abelian. This sequence is split if and only if its push-out by the mod n map $A \to A/n$ is split for all n.*

Let $S(n)$ be the set of homomorphisms of profinite groups $C \to B/nA$ which are sections of the map $B/nA \to C$. This set if finite. (The choice of one section identifies $S(n)$ with $\mathrm{Hom}(C, A/n)$. Since A/n is a finite abelian group, $S(n)$ identifies with the finite set $\mathrm{Hom}(C^{ab}/n, A/n)$.) Since the inverse limit of a projective system of finite non-empty sets is non-empty (a consequence of Tikhonov's theorem), and the canonical map $A \to \lim_{\leftarrow} A/n$ is an isomorphism, we obtain the desired splitting.

2.5. **More on the type of a torsor.** Let T be a k-torus over k.

Exercise. a) (Rosenlicht's lemma) Prove that $\overline{k}[T]^*$ is generated by $\overline{k}^*$ and the characters of $\overline{T}$. (Hint: First prove this for $T = \mathbf{G}_m$.)

b) Let Z be a k-torsor under T. Then there is an exact sequence of Γ-modules

$$1 \to \overline{k}^* \to \overline{k}[Z]^* \to \widehat{T} \to 0.$$

Moreover, we have $\mathrm{Ext}^1_k(\hat{T}, \overline{k}^*) = \mathrm{H}^1(k, T)$, and the class of this extension is the class of the k-torsor Z in $\mathrm{H}^1(k, T)$ (up to sign).

Now let $Z \to Y$ be a torsor under T, where both Y and Z are geometrically integral, and $\overline{k}[Y]^* = \overline{k}^*$. The following exact sequence of Γ-modules, due to Colliot-Thélène and Sansuc, is a generalization of (b):

$$1 \to \overline{k}^* \to \overline{k}[Z]^* \to \widehat{T} \to \mathrm{Pic}\,\overline{Y} \to \mathrm{Pic}\,\overline{Z} \to 0. \tag{6}$$

Moreover, up to sign the map $\widehat{T} \to \mathrm{Pic}\,\overline{Y}$ coincides with the type of $Z \to Y$. It is clear from (6) that when the type is injective we have $\overline{k}[Z]^* = \overline{k}^*$. It is also clear that the torsor Z/Y is universal if and only if $\overline{k}[Z]^* = \overline{k}^*$ and $\mathrm{Pic}\,\overline{Z} = 0$.

In the case when $Z \to Y$ is a torsor under a k-group F of multiplicative type (for instance, a finite commutative k-group scheme), and the condition $\overline{k}[Z]^* = \overline{k}^*$ is satisfied, we still have an exact sequence

$$0 \to \widehat{F} \to \mathrm{Pic}\,\overline{Y} \to \mathrm{Pic}\,\overline{Z}. \tag{7}$$

Here again, $\widehat{F} \to \mathrm{Pic}\,\overline{Y}$ is the type of the torsor $Z \to Y$.

Let's use (7) to find the type of the torsor $[n] : E \to E$ (the multiplication by n map) from Example 5. Recall that the Galois module $E[n]$ is auto-dual because of the Weil pairing. The map $[n]^* : \mathrm{Pic}\,\overline{E} \to \mathrm{Pic}\,\overline{E}$ sends the class of a point $[x]$ to the sum of the classes $[y]$, where $ny = x$, $x, y \in E(\overline{k})$. This sum equals the sum of $[y] + [\varepsilon]$, where $\varepsilon \in E[n]$, and this equals $n^2[y] = n[ny] = n[x]$. Thus $[n]^*$ is the multiplication by n, and the type of the torsor $[n] : E \to E$ is the composition of an automorphism of $E[n]$ and the natural injection $E[n] \subset \mathrm{Pic}\,\overline{E}$. It can be shown, at least up to sign, that the type is indeed this natural injection.

Exercises. **1** Assume that X is geometrically integral, i.e. $\overline{X}$ is reduced and irreducible. Prove that the torsor Y is geometrically connected, i.e. $\overline{Y}$ is connected, if and only if the kernel of $\chi([Y])$ has no torsion, for example when the type is injective. Hint: use (6).
2 Check that the torsor in Example 2 is universal.
3 Find the type of torsors in Examples 6 and 7.

3. What is the Brauer group?

3.1. **The Brauer group of a field.** The Brauer group of a field k is the group $\mathrm{Br}\, k$ of equivalence classes of central simple algebras over k. Recall that a k-algebra A is *central* if the centre of A is k, and A is *simple* if it has no nontrivial two-sided ideals. The set of such algebras is closed under taking the tensor product. The basic example of a c.s.a. is the matrix algebra $M_n(k)$. If A is a c.s.a. over k, and $k \subset K$ is a field extension, then $A \otimes_k K$ is a c.s.a. over K. For any c.s.a. A the algebra $A \otimes_k \overline{k}$ is isomorphic to $M_n(\overline{k})$. Thus the central simple algebras are precisely those algebras over k which over $\overline{k}$ become isomorphic to a full matrix algebra.

Two algebras A_1 and A_2 are called *equivalent* if $A_1 \otimes_k M_n(k)$ is isomorphic to $A_2 \otimes_k M_m(k)$ for some positive integers n and m. To a c.s.a. A we can associate its opposite algebra A^{op}, that is, A with the reversed order of multiplication. One checks that $A \otimes_k A^{op}$ is isomorphic to a matrix algebra. Thus the set of equivalence classes of central simple algebras is a group under the tensor product.

There is a cohomological interpretation of the Brauer group. The Skolem–Noether theorem says that every automorphism of $M_n(k)$ comes from the conjugation by an invertible matrix, in other words, $\mathrm{Aut}\, M_n = \mathrm{PGL}(n)$. Hence the isomorphism classes of the central simple algebras A such that $A \otimes_k \overline{k} \simeq M_n(\overline{k})$ are in a natural bijection with the elements of the cohomology set $\mathrm{H}^1(k, \mathrm{PGL}(n))$. The exact sequence of algebraic groups

$$1 \to \mathbf{G}_m \to \mathrm{GL}(n) \to \mathrm{PGL}(n) \to 1 \tag{8}$$

gives a map $\mathrm{H}^1(k, \mathrm{PGL}(n)) \to \mathrm{H}^2(k, \overline{k}^*)$. Using this map one establishes a natural isomorphism $\mathrm{Br}\, k = \mathrm{H}^2(k, \overline{k}^*)$ (to a c.s.a. one associate a "system of factors", which is a 2-cocycle with coefficients in $\overline{k}^*$).

The map $x \mapsto x^n$ gives rise to the exact sequence

$$1 \to \mu_n \to \overline{k}^* \to \overline{k}^* \to 1. \tag{9}$$

By Hilbert's theorem 90 we deduce that $(\mathrm{Br}\, k)[n] = \mathrm{H}^2(k, \mu_n)$. Consider the pairing of Galois modules

$$\mu_n \times \mathbb{Z}/n \quad \to \quad \mu_n.$$

This gives a pairing

$$\mathrm{H}^1(k, \mu_n) \times \mathrm{H}^1(k, \mathbb{Z}/n) \quad \to \quad (\mathrm{Br}\, k)[n].$$

On the one hand, it follows from (9) that $\mathrm{H}^1(k, \mu_n) = k^*/k^{*n}$. On the other hand, $\mathrm{H}^1(k, \mathbb{Z}/n) = \mathrm{Hom}_{cont}(\Gamma, \mathbb{Z}/n)$. Thus, if $a \in k^*$, $\chi \in \mathrm{Hom}_{cont}(\Gamma, \mathbb{Z}/n)$, we have an element of order dividing n in the Brauer group, written as (a, χ). One can construct explicitly a c.s.a. whose class in $\mathrm{Br}\, k$ is (a, χ); it is called a *cyclic* algebra. From our construction it is clear that (a, χ) is multiplicative in each argument. Sometimes it is more convenient to write (a, K) instead of (a, χ), where $K \subset \overline{k}$ is the invariant subfield of the kernel of χ.

If $n = 2$ there is no difference between $\mathbb{Z}/2$ and μ_2 (the characteristic of k is zero), so that we can write the corresponding class as (a, b), where $a, b \in k^*$ are defined up to squares. (The same can be done for any cyclic algebra if k contains the n-th roots of 1.) The cyclic algebra in this case is the quaternion algebra with generators i and j subject to relations

$i^2 = a$, $j^2 = b$, $ij = -ji$. (It may not be a division algebra, though.) It is an important fact that $(a, b) = 0$ if and only if the plane projective conic $ax^2 + by^2 = z^2$ has a k-point. This implies the relations $(a, -a) = (a, 1 - a) = 0$ whenever these symbols are defined. In algebraic terms, we have $(a, b) = 0$ if and only if a is a norm of the quadratic extension $k(\sqrt{b})/k$.

Examples. 1) $\mathrm{Br}\,\mathbb{C} = 0$. The same is true for any algebraically closed field.

2) $\mathrm{Br}\,\overline{k}(t) = 0$ (Tsen's theorem).

2) $\mathrm{Br}\,\mathbb{R} \simeq \mathbb{Z}/2$. The non-trivial element is the class of Hamilton's quaternions. Let $\mathrm{inv} : \mathrm{Br}\,\mathbb{R} \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ be the corresponding isomorphism.

3) Let k be a non-archimedean local field of characteristic 0. The local class field theory provides a local invariant map $\mathrm{inv} : \mathrm{Br}\,k \to \mathbb{Q}/\mathbb{Z}$, which is an isomorphism. Suppose that p is prime to the residual characteristic of k, and consider $\mathrm{inv} : (\mathrm{Br}\,k)[p] \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$. Assume that a is a unit. If K/k is unramified, then $\mathrm{inv}((a, K)) = 0$. If K/k is ramified, then $\mathrm{inv}((a, K))$ is the class of the reduction of a modulo the maximal ideal of $\mathcal{O}_K$, considered up to n-th powers in the residue field.

4) Let k be a number field. The sum of local invariants of a class in $\mathrm{Br}\,k$ is zero; moreover, any collection of values with the zero sum comes from a unique element of $\mathrm{Br}\,k$. This powerful consequence of the global class field theory can be written as the exact sequence

$$0 \to \mathrm{Br}\,k \to \oplus_v \mathrm{Br}\,k_v \to \mathbb{Q}/\mathbb{Z} \to 0.$$

5) Let $F = k(t)$. Somewhat similarly, we have an exact sequence (D.K. Faddeev):

$$0 \to \mathrm{Br}\,k \to \mathrm{Br}\,k(t) \to \oplus_P \mathrm{H}^1(k[t]/P(t), \mathbb{Q}/\mathbb{Z}) \to 0,$$

where $P(t)$ ranges through all the irreducible monic polynomials. (These polynomials bijectively correspond to the closed points of the affine line over k.)

3.2. **The Brauer group of a scheme.** Grothendieck generalized the Brauer group to any scheme X using étale cohomology, namely he defined $\mathrm{Br}\,X = \mathrm{H}^2(X, \mathbf{G}_m)$. In particular, the Brauer group of any ring R is defined by $\mathrm{Br}\,R = \mathrm{H}^2(\mathrm{Spec}\,R, \mathbf{G}_m)$.

Let $\mathcal{O}$ be a discrete valuation ring (DVR) with the fraction field K and the residue field κ. Assume that κ has characteristic 0. Then (using some general properties of étale cohomology) one defines the *residue* map

$$\mathrm{res} : \mathrm{Br}\,K \to \mathrm{H}^1(\kappa, \mathbb{Q}/\mathbb{Z}),$$

whose kernel is $\mathrm{Br}\,\mathcal{O}$. The maps $\mathrm{Br}\,k(t) \to \mathrm{H}^1(k[t]/P(t), \mathbb{Q}/\mathbb{Z})$ from Faddeev's exact sequence are examples of the residue map. The local invariant from Example 3 is also a residue map (but note that the residue field has characteristic p now). Indeed, the Galois group of a finite field is procyclic, so that $\mathrm{H}^1(\kappa, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$, where the map sends χ to its value on the topological generator of $\mathrm{Gal}(\overline{\kappa}/\kappa)$.

Let X be a smooth integral variety over k. Then we have an exact sequence (Grothendieck's purity theorem for the Brauer group):

$$0 \to \mathrm{Br}\,X \to \mathrm{Br}\,k(X) \to \oplus_Y \mathrm{H}^1(k(Y), \mathbb{Q}/\mathbb{Z}),$$

where Y ranges through all the integral subvarieties of X of codimension 1. The map $\mathrm{Br}\, k(X) \to \mathrm{H}^1(k(Y), \mathbb{Q}/\mathbb{Z})$ here is the residue map. This can be seen as a vast generalization of Example 5; Faddeev's exact sequence shows that $\mathrm{Br}\, \mathbf{A}^1_k = \mathrm{Br}\, k$.

The elements of the intersection of the residue maps defined by all possible DVR's in $k(X)$ such that the restriction of the valuation to k is zero, are called *unramified*. If X is projective and smooth, then the Brauer group of X can be interpreted as the group of unramified elements of $\mathrm{Br}\, k(X)$. This has an important consequence that the Brauer group of a smooth and projective variety is a birational invariant.

Examples. 1) $\mathrm{Br}\, \mathbf{A}^n_k = \mathrm{Br}\, \mathbf{P}^n_k = \mathrm{Br}\, k$.

2) Let C be the conic $ax^2 + by^2 = z^2$. Then $\mathrm{Br}\, C$ is the quotient of $\mathrm{Br}\, k$ modulo the subgroup generated by (a, b).

3) (Open problem.) Let K/k be a biquadratic extension. Choose coordinates x_1, x_2, x_3, x_4 in K as a vector space over k. Let $N : K \to k$ be the norm. Let X be any smooth compactification of the affine variety $N(x_1, x_2, x_3, x_4) = c$, for $c \in k^*$. It is known that $\mathrm{Br}\, X/\mathrm{Br}\, k \simeq \mathbb{Z}/2$. Find explicitly a non-constant element in $\mathrm{Br}\, X$, i.e. an unramified element in $\mathrm{Br}\, k(X)$ which is not in $\mathrm{Br}\, k$.

3.3. **Computing the Brauer group.** In many cases the Brauer group of X can be computed from the Hochschild–Serre spectral sequence

$$\mathrm{H}^p(k, \mathrm{H}^q(\overline{X}, \mathbf{G}_m)) \Rightarrow \mathrm{H}^{p+q}(X, \mathbf{G}_m).$$

This spectral sequence is a particular case of the general Grothendieck spectral sequence of composed functors. Write $p : X \to \mathrm{Spec}(k)$ for the structure morphism. Here we have three abelian categories

$$\{\text{Étale sheaves on } X\} \longrightarrow \{\text{Continuous } \Gamma\text{-modules}\} \longrightarrow \{\text{Abelian groups}\}$$

and the functors between them: $p_* : \mathcal{F} \mapsto \mathrm{H}^1(\overline{X}, \mathcal{F})$ and $M \mapsto M^\Gamma$. The composition of these functors sends $\mathcal{F}$ to $\mathrm{H}^1(X, \mathcal{F})$. It is a general theorem that once some fairly mild conditions are satisfied (which they are in this case) we get a spectral sequence as above.

Note that if X is projective, then $\mathrm{H}^0(\overline{X}, \mathbf{G}_m) = \overline{k}^*$. To use the Hochschild–Serre spectral sequence we need to know how Γ acts on $\mathrm{Pic}\, \overline{X} = \mathrm{H}^1(\overline{X}, \mathbf{G}_m)$ and $\mathrm{Br}\, \overline{X} = \mathrm{H}^2(\overline{X}, \mathbf{G}_m)$, as well as the differentials $d_2^{1,1} : \mathrm{H}^1(k, \mathrm{Pic}\, \overline{X}) \to \mathrm{H}^3(k, \overline{k}^*)$ and $d_2^{0,2} : (\mathrm{Br}\, \overline{X})^\Gamma \to \mathrm{H}^2(k, \mathrm{Pic}\, \overline{X})$. Of course, things become easier

when $\mathrm{Br}\, \overline{X} = 0$ (This is equivalent to the absence of transcendental cycles in $\mathrm{H}^2(X \times \mathbb{C}, \mathbb{Q})$ and $\mathrm{H}^3(X \times \mathbb{C}, \mathbb{Z})_{tors} = 0$ – this holds for the smooth projective curves for dimension reasons, and also for the rational varieties since $\mathrm{Br}\, \overline{X}$ is a birational invariant of smooth projective varieties and $\mathrm{Br}\, \mathbf{P}^n_{\overline{k}} = 0$),

when X has a zero-cycle of degree one, for example, a rational point (then $d_2^{0,1}$ and $d_2^{1,1}$ are the zero maps, since a k-point gives a section of the structure morphism p),

or when $\mathrm{H}^3(k, \overline{k}^*) = 0$ (this holds for number fields and local fields by class field theory, and also for $k(t)$, where k is a number field or its completion).

If X is projective, then the above spectral sequence gives an exact sequence

(10)
$$0 \to \operatorname{Pic} X \to (\operatorname{Pic} \overline{X})^{\Gamma} \to^{\star} \operatorname{Br} k \to \operatorname{Br}_1 X \to \mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \to^{\star} \mathrm{H}^3(k, \overline{k}^*) \to \mathrm{H}^3(X, \mathbf{G}_m),$$

where the starred maps are zero if X has a k-point, and $\operatorname{Br}_1 X = \operatorname{Ker}[\operatorname{Br} X \to \operatorname{Br} \overline{X}]$ is the *algebraic* Brauer group of X. In good cases this sequence reduces the computation of the structure of the group $\operatorname{Br}_1 X$ modulo the image of $\operatorname{Br} k$ to the easier question of computing the first Galois cohomology group of $\operatorname{Pic} \overline{X}$. When $\operatorname{Pic} \overline{X}$ is finitely generated and torsion free, such a computation can be done by a computer once we find a system of generators and relations of $\operatorname{Pic} \overline{X}$.

In the general case, the starred map up to sign are the Yoneda cup-products with the class of the 2-extension

$$0 \to \overline{k}^* \to \overline{k}(X)^* \to \mathrm{Div}\overline{\mathrm{X}} \to \operatorname{Pic} \overline{X} \to 0.$$

It is a difficult problem to lift a class in the kernel of $\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \to \mathrm{H}^3(k, \overline{k}^*)$ to $\operatorname{Br}_1 X$ (cf. Example 3 above). However, if T is a group of multiplicative type, and *we are given* a torsor $Y \to X$ under T of type $\lambda : \hat{T} \to \operatorname{Pic} \overline{X}$, then lifting the elements of $\operatorname{Im}(\lambda_*) \subset \mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ is easy. Let us now describe this important link between torsors and the Brauer group.

3.4. **From torsors to the Brauer group.** Suppose $Y \to X$ is a torsor under a k-group of multiplicative type T, and let $[Y/X]$ be its class in $\mathrm{H}^1(X, T)$. The structure morphism $p : X \to \operatorname{Spec}(k)$ gives rise to the map $\mathrm{H}^1(k, \hat{T}) \to \mathrm{H}^1(X, \hat{T})$ (actually, an isomorphism). Hence for each $c \in \mathrm{H}^1(k, \hat{T})$ we obtain an element of $\operatorname{Br} X$ via the cup product

$$\mathrm{H}^1(X, T) \times \mathrm{H}^1(k, \hat{T}) \longrightarrow \mathrm{H}^1(X, T) \times \mathrm{H}^1(X, \hat{T}) \longrightarrow \mathrm{H}^2(X, \mathbb{G}_m) = \operatorname{Br} X\,.$$

The cup product is an element of $\operatorname{Br}_1 X$ since c is killed by extending the ground field to $\overline{k}$.

Theorem 3.1. *Let $\lambda : \hat{T} \to \operatorname{Pic} \overline{X}$ be the type of the torsor $Y \to X$ under a k-group of multiplicative type T. Then the following diagram commutes:*

$$\begin{tikzcd}
\mathrm{H}^1(k, \hat{T}) \arrow[r] \arrow[d, equal] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \\
\mathrm{H}^1(X, \hat{T}) \arrow[r] & \operatorname{Br}_1 X \arrow[u]
\end{tikzcd}$$

where the upper arrow is λ_*, the right hand arrow is the map from (10)*, and the bottom arrow is the cup-product with the class* $[Y/X]$.

Examples. 1) Assume that $\operatorname{Pic} \overline{X}$ has no divisible part, e.g. is torsion free. Let T be the group dual to $\operatorname{Pic} \overline{X}$, i.e. $\hat{T} = \operatorname{Pic} \overline{X}$, and let Y/X be a universal torsor. The cup product with the class $[Y/X]$ defines a homomorphism $\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \to \operatorname{Br}_1 X$, which is a splitting of the exact sequence

$$0 \to \operatorname{Br} k \to \operatorname{Br}_1 X \to \mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \to 0.$$

2) Let Y/X be the multiplication by 2 on an elliptic curve $E : y^2 = (x - c_1)(x - c_2)(x - c_3)$, so that $k(Y) = k(X)(\sqrt{x - c_1}, \sqrt{x - c_2})$. Here $T = \hat{T} = E[2]$. Note that the degree map $\operatorname{Pic} E \to \mathbb{Z}$ has a section $1 \mapsto [0]$, where $0 \in E(k)$ is the origin of the group law. Hence $\operatorname{Pic} E \simeq E(\overline{k}) \oplus \mathbb{Z}$ as Galois modules. This implies that $\mathrm{H}^1(k, \operatorname{Pic} \overline{E}) = \mathrm{H}^1(k, E)$ since

$\mathrm{H}^1(k,\mathbb{Z}) = \mathrm{Hom}_{cont}(\Gamma,\mathbb{Z}) = 0$ because Γ is a profinite group. On the other hand, $\mathrm{Br}\,E = \mathrm{Br}_1 E$ is the direct sum of $\mathrm{Br}\,k$ and the subgroup $\mathrm{Br}^0 E \subset \mathrm{Br}\,E$ consisting of the elements with trivial value at 0. Then (10) shows that $\mathrm{Br}^0 E$ is naturally isomorphic to $\mathrm{H}^1(k,E)$. We computed the type λ of $Y \to X$ above. This calculation implies that $\lambda_* : \mathrm{H}^1(k,E[2]) \to \mathrm{H}^1(k,E)$ is the natural map. By Theorem 3.1 this map can be interpreted as sending

$$(a_1,a_2) \in \mathrm{H}^1(k,E[2]) \cong (k^*/k^{*2})^2\,,$$

to the element $(x-c_1,a_1)+(x-c_2,a_2) \in \mathrm{Br}^0 E$. (The value of this element at $0 \in E(k)$ is 0 because the fibre of $Y \to X$ at 0 contains the k-point $0 \in Y(k)$, and so is a trivial torsor under $E[2]$.) Since $\mathrm{Im}(\lambda_*) = \mathrm{H}^1(k,E)[2]$, every element of $(\mathrm{Br}^0 E)[2]$ can be obtained in this way.

3) Let $Y \to X$ be the torsor from Example 7; its structure group is the norm torus T given by $y^2 - az^2 = 1$. Assume that $a \in k^*$ is not a square in $k[x]/(p_i(x))$, $i = 1,2$, and that $p_1(x)$ and $p_2(x)$ are coprime, irreducible and of even degree. Then $Y \to X$ extends to the torsor $Y_c \to X_c$ between the natural compactifications. (The fibre of $X_c \to \mathbf{P}^1_k$ at infinity is smooth.) It is easy to see that $\hat{T}$ is the abelian group $\mathbb{Z}$ on which Γ acts through $\mathrm{Gal}(k(\sqrt{a})/k) \simeq \mathbb{Z}/2$, whose generator sends 1 to -1. Representing $\hat{T}$ as the kernel of the summation map $\mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$, where $\mathrm{Gal}(k(\sqrt{a})/k) \simeq \mathbb{Z}/2$ swaps the coordinates of $\mathbb{Z} \oplus \mathbb{Z}$, one shows that $\mathrm{H}^1(k,\hat{T}) \simeq \mathbb{Z}/2$. The commutative diagram of Theorem 3.1 gives rise to the commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1(k,\hat{T}) \arrow[r] \arrow[d, equal] & \mathrm{H}^1(k,\mathrm{Pic}\,\overline{X}_c) \\
\mathrm{H}^1(X_c,\hat{T}) \arrow[r] & \mathrm{Br}_1 X_c/\mathrm{Br}\,k \arrow[u]
\end{tikzcd}$$

In fact, all the arrows in this diagram are isomorphisms between the groups of order 2 (see Chapter 7 of my book). The element $(a,p_1(x)) \in \mathrm{Br}\,X = \mathrm{Br}_1 X$ generates $\mathrm{Br}_1 X_c/\mathrm{Br}\,k$ (ibidem).

4) (P. Swinnerton-Dyer + A.S.) Consider (the unique minimal smooth projective model of) the surface

$$X : z^2 = (x-c_1)(x-c_2)(x-c_3)(y-d_1)(y-d_2)(y-d_3)\,.$$

X a K3 surface, more precisely the Kummer surface obtained from the product of two elliptic curves

$$u^2 = (x-c_1)(x-c_2)(x-c_3) \quad \text{and} \quad v^2 = (y-d_1)(y-d_2)(y-d_3)\,.$$

Assume that these curves are not isogenous over $\overline{k}$. Then $\mathrm{Br}_1 X = \mathrm{Br}\,k$. Using Example 2 one shows that $(\mathrm{Br}\,\overline{X})[2] \simeq (\mathbb{Z}/2)^4$ is generated by the elements $((x-c_i)(x-c_3),(y-d_j)(y-d_3))$ for $i,j \in \{1,2\}$.

If X is a variety with $\mathrm{Br}\,\overline{X} \neq 0$, then the computation of the whole Brauer group $\mathrm{Br}\,X$ is much harder. For example, what is $\mathrm{Br}\,X$ when X is an abelian variety? The same question for a K3 surface. Zarhin and the author proved that if k is finitely generated over $\mathbb{Q}$, then $\mathrm{Br}\,X/\mathrm{Br}\,k$ is finite if X is a K3 surface, and $\mathrm{Br}\,X/\mathrm{Br}_1 X$ is finite is X is an abelian variety.

It is an interesting question whether the order of this group can be computed arithmetically. If X is defined over a number field, is there a connection to the L-function of X?

Exercises. 1. Write down the elements of the Brauer group that can be obtained from the torsor in Example 6.

2. With notation of the previous example, prove directly that $(a, p_1(x)) \in \operatorname{Br} k(X)$ is unramified.

4. What is descent?

4.1. **Torsors and descent.** Torsors are useful in number theory for doing descent.

Let $f : Y \to X$ be a left torsor under an algebraic k-group G. Recall that there is a natural bijection

$$\{\text{left } k\text{-torsors under } G\}/\text{iso} \quad \longleftrightarrow \quad \mathrm{H}^1(k,G).$$

To a k-point P on X we can associate the class of the fibre $[Y_P] = [f^{-1}(P)] \in \mathrm{H}^1(k,G)$. This defines an important map $X(k) \to \mathrm{H}^1(k,G)$, which can be used to study the set $X(k)$.

Let α be a continuous cocycle of Γ with coefficients in $G(\overline{k})$, and let $[\alpha]$ be its class in $\mathrm{H}^1(k,G)$. Then we can form the *twist* of Y by α, denoted $f_\alpha : Y_\alpha \to X$, which can be described as follows. Note that to give a quasi-projective variety over k is the same as to give a variety over $\overline{k}$ together with an action of $\mathrm{Gal}(\overline{k}/k)$ on it such that the stabilizer of every point is open. (For affine varieties going down to k is easy: just take the Galois invariant subring of the coordinate ring.) For Y_α, we have $\overline{Y_\alpha} = \overline{Y}$, and the twisted Galois action is $y \mapsto \alpha(\gamma)\gamma y$ for $\gamma \in \mathrm{Gal}(\overline{k}/k)$. The fact that this is a group action amounts to the cocycle condition:

$$\alpha(\gamma_2\gamma_1)\gamma_2\gamma_1 = \alpha(\gamma_2)\gamma_2 \cdot \alpha(\gamma_1)\gamma_1 \quad \Leftrightarrow \quad \alpha(\gamma_2\gamma_1) = \alpha(\gamma_2) \cdot {}^{\gamma_2}\alpha(\gamma_1).$$

Lemma 4.1. *Let $f : Y \to X$ be a torsor under G. Then*

$$X(k) = \coprod_{[\alpha]\in \mathrm{H}^1(k,G)} f_\alpha(Y_\alpha(k)).$$

Proof. Suppose $P \in X(k)$. Then $Y_P = f^{-1}(P) \to P$ is a k-torsor under G. Take the corresponding class $[\alpha] := [f^{-1}(P)] \in \mathrm{H}^1(k,G)$. Then $f_\alpha^{-1}(P)$ contains a k-rational point. The idea is that the twisting by α "untwists" Y_P by turning it into a trivial torsor. □

Warning. If G is not abelian, then in general Y_α is not a left torsor under G. In fact Y_α is a left torsor under a certain twisted form of G, namely the inner form G_α of G twisted by the cocycle α. In this case $\mathrm{H}^1(k,G)$ and $\mathrm{H}^1(k,G_\alpha)$ can be identified as sets, but the distinguished point of $\mathrm{H}^1(k,G_\alpha)$ corresponds to the class of α in $\mathrm{H}^1(k,G)$.

From now on we assume that X is projective and k is a number field. Then there are only finitely many classes $[\alpha]$ such that $Y_\alpha(k) \neq \emptyset$.

Consider the topological space $\prod X(k_v)$, where the product is taken over all the places of k. We have $\prod X(k_v) = X(\mathbb{A}_k)$, where $\mathbb{A}_k$ is the ring of adèles of k. Because of this we shall refer to the points of $\prod X(k_v)$ as 'adelic' points. We assume that there is at least one adelic point, or, in the terminology of Diophantine equations, that X is everywhere locally soluble. Define

$$\left(\prod X(k_v)\right)^f := \bigcup_{[\alpha]\in \mathrm{H}^1(k,G)} f_\alpha\left(\prod Y_\alpha(k_v)\right) \subseteq \prod X(k_v), \tag{11}$$

where all our products are taken over all the places v of k. This set is sometimes called 'the set of adelic points that survive the descent with respect to $Y \to X$'. By Lemma 4.1 $(\prod X(k_v))^f$ contains $X(k)$. This set consists of the families of points $P_v \in X(k_v)$, for all v, such that the classes $[Y_{P_v}] \in \mathrm{H}^1(k_v,G)$ are the restrictions of one global class in $\mathrm{H}^1(k,G)$.

The process of descent can be seen as consisting of two steps:
(1) determining the set of elements $\alpha \in \mathrm{H}^1(k, G)$ such that $\prod Y_\alpha(k_v)$ is not empty;
(2) computing $(\prod X(k_v))^f$.
If the set in (1) is empty, then $X(k)$ is empty.

Example. The most famous example of descent is the 2-descent on the elliptic curve $E : y^2 = (x - c_1)(x - c_2)(x - c_3)$. We keep the notation of Example 2 of Section 2, in particular $f : Y \to X = E$ is the multiplication by 2. We obtain the exact sequence

$$0 \to E[2] \to E(k) \to E(k) \to \mathrm{H}^1(k, E[2]).$$

The right hand map here is the map $E(k) \to \mathrm{H}^1(k, E[2])$ sending a point $P = (x, y)$ to the class $[Y_P]$. (Its explicit expression is well known: choose $(c_1, 0)$ and $(c_2, 0)$ for a basis of $E[2]$, then this map sends a point $P = (x, y)$ to $(x - c_1, x - c_2)$. If either expression is not defined at P, it must be multiplied by a square in $k(E)$ to make it regular and invertible at P.) The set of classes $[\alpha] \in \mathrm{H}^1(k, E[2])$ such that $Y_\alpha(k_v) \neq \emptyset$ for all v is none other than the 2-Selmer group. This is task (1). To solve it one looks at all the 2-coverings of E in order to decide which have points everywhere locally; such coverings form the Selmer group. (The process is in fact finite because it is enough to consider only the classes that are unramified away from finitely many places. For each covering there are only finitely many places to test.) Finally, $(\prod E(k_v))^f$ is the subset of $(\prod E(k_v))$ consisting of the elements whose image in $\prod \mathrm{H}^1(k_v, E[2])$ comes from $\mathrm{H}^1(k, E[2])$.

4.2. **The Manin obstruction.** The Brauer–Manin set $(\prod X(k_v))^{\mathrm{Br}}$ is the set of families of points $P_v \in X(k_v)$, for all v, such that

$$\sum_v \mathrm{inv}_v\, \mathcal{A}(P_v) = 0 \quad \text{for all } \mathcal{A} \in \mathrm{Br}\, X. \tag{12}$$

Here $\mathcal{A} \mapsto \mathcal{A}(P_v) \in \mathrm{Br}\, k_v$ is the "value" of $\mathcal{A}$ at P_v, defined because of the functoriality of the Brauer group. The sum is finite since for almost all places $\mathcal{A}(P_v)$ is not just an element of $\mathrm{Br}\, k_v$, but an element of its subgroup $\mathrm{Br}\, \mathcal{O}_v$ consisting of the unramified elements of $\mathrm{Br}\, k_v$. But $\mathrm{Br}\, \mathcal{O}_v = 0$. Finally, $X(k) \subset (\prod X(k_v))^{\mathrm{Br}}$ by the global reciprocity.

The pairing in (12) is called the Brauer–Manin pairing. A subgroup of $\mathrm{Br}\, X$ does not obstruct the Hasse principle if X contains an adelic point Brauer–Manin orthogonal to it. The Brauer–Manin obstruction is the only obstruction to the Hasse principle for a class of varieties if for every variety in the class the emptiness of $X(k)$ is equivalent to the emptyness of $(\prod X(k_v))^{\mathrm{Br}}$.

For an explicitly given $\mathcal{A} \in \mathrm{Br}\, X$ the obstruction is easy to compute.

Example (V.A. Iskovskih). This example continues Example 7 of Section 1 and Example 3 of Section 2. Let $k = \mathbb{Q}$, $a = -1$, $p_1(x) = 3 - x^2$, $p_2(x) = x^2 - 2$. The class $\mathcal{A} = (-1, 3 - x^2)$ is unramified. It is not hard to check that $\mathrm{inv}_v\, \mathcal{A}(P_v) = 0$ for any P_v, $v \neq 2$. (Note that $(-1, 3 - x^2) = (-1, x^2 - 2)$, because $(-1, y^2 + z^2) = 0$. Since $(3 - x^2) + (x^2 - 2) = 1$, one of these must be a unit (resp. positive), but since $v \neq 2$ the invariant of the quaternion algebra of the form (unit,unit) (resp. (-1,positive)) is 0.) It is more involved to prove that

$\mathrm{inv}_2\,\mathcal{A}(P_2)=\frac{1}{2}$ for any 2-adic point P_2. It follows that the Brauer–Manin pairing never takes the value 0, so there are no $\mathbb{Q}$-points on our surface.

4.3. **Descent and the Manin obstruction.** Thus we have two "competing approaches" to bounding $X(k)$: descent using torsors (the more classical approach), and the Brauer–Manin obstruction. Colliot-Thélène and Sansuc proved that the information that can be obtained from torsors under groups of multiplicative type can also be obtained via the Brauer–Manin obstruction. Their main result is the following theorem.

Theorem 4.2. *Let X be a projective variety over a number field k; then we have*

$$(\prod X(k_v))^{\mathrm{Br}_1 X}=\bigcap_{\lambda:M\hookrightarrow \mathrm{Pic}\,\overline{X}}\ \bigcup_{\mathtt{type}(Y,f)=\lambda} f(\prod Y(k_v)),$$

where $\lambda: M\hookrightarrow \mathrm{Pic}\,(\overline{X})$ runs over the Γ-submodules of $\mathrm{Pic}\,\overline{X}$ of finite type.

The condition on the global points provided by the algebraic Brauer group $\mathrm{Br}\,_1X$ is called the algebraic Manin obstruction. The theorem shows that it is equivalent to the combination of obstructions of two different kinds: the obstruction for the existence of torsors $f: Y\to X$ of a given type λ, and the descent obstruction defined by torsors of type λ, for all possible λ's. Note that by (4) all torsors of given type can be obtained from one such torsor by twisting as described above.

This theorem is a consequence of the following more detailed result.

Let $r: \mathrm{Br}\,_1X\to \mathrm{H}^1(k,\mathrm{Pic}\,\overline{X})$ be the canonical map from the Hochschild–Serre spectral sequence (10). Let M be a Γ-module of finite type, and $\lambda: M\to \mathrm{Pic}\,(\overline{X})$ a homomorphism of Γ-modules. Let S be the k-group of multiplicative type such that $M=\hat{S}$. Let

$$\mathrm{Br}\,_\lambda X := r^{-1}\lambda_*(\mathrm{H}^1(k,M))\subset \mathrm{Br}\,_1X.$$

We define $(\prod X(k_v))^{\mathrm{Br}\,_\lambda}\subset \prod X(k_v)$ as the set of adelic points orthogonal to $\mathrm{Br}\,_\lambda X$ with respect to the Brauer–Manin pairing.

Theorem 4.3. *Let X be a projective variety over a number field k, M be a Γ-module of finite type, S its dual group of multiplicative type, and $\lambda\in \mathrm{Hom}_k(M,\mathrm{Pic}\,(\overline{X}))$. Then*

(a) *we have*

$$(\prod X(k_v))^{\mathrm{Br}\,_\lambda}=(\prod Y(k_v))^f, \tag{13}$$

where $f: Y\to X$ is an X-torsor under S of type λ,

(b) *there are only finitely many isomorphism classes of torsors $f: Y\to X$ of type λ such that $\prod Y(k_v)\neq\emptyset$.*

To derive Theorem 4.2 note that for any $\alpha\in \mathrm{Br}\,_1X$ there exists a Γ-submodule $\lambda: M\hookrightarrow \mathrm{Pic}\,\overline{X}$ of finite type such that $r(\alpha)\in\lambda_*(\mathrm{H}^1(k,M))$ ([Serre, Cohomologie galoisienne], I.2.2, Cor. 2). Thus $(\prod X(k_v))^{\mathrm{Br}\,_1X}=\bigcap_\lambda(\prod X(k_v))^{\mathrm{Br}\,_\lambda}$.

Let us point out some of the many corollaries of this theorem.

Corollary 4.4. (1) $\mathrm{Br}_\lambda X$ *does not obstruct the Hasse principle if and only if there exists an X-torsor Y of type λ such that $\prod Y(k_v) \neq \emptyset$. In particular, when* $\mathrm{Pic}\,\overline{X}$ *is of finite type, the vanishing of the algebraic Manin obstruction is equivalent to the existence of universal torsors with an adelic point.*

(2) *If the X-torsors of type λ satisfy the Hasse principle, then the Manin obstruction to the Hasse principle on X related to* $\mathrm{Br}_\lambda X$ *is the only obstruction.*

The proof of Theorem 4.3 (a) breaks into three statements:

(1) If there exists an adelic point which is Brauer–Manin orthogonal to the elements of $\mathrm{Br}_\lambda X$ coming from the everywhere locally trivial elements of $\mathrm{H}^1(k, M)$, then there exists a torsor $f : Y \to X$ of type λ. (This is the hardest part.)

(2) Suppose there exists a torsor $f : Y \to X$ of type λ. If an adelic point is Brauer–Manin orthogonal to $\mathrm{Br}_\lambda X$, then there exists $\sigma \in \mathrm{H}^1(k, S)$ such that this point lifts to an adelic point on Y^σ.

(3) If there exists a torsor $f : Y \to X$ of type λ such that $Y(\mathbb{A}_k) \neq \emptyset$, then $f(\prod Y(k_v)) \subset (\prod X(k_v))^{\mathrm{Br}_\lambda}$.

The proof is in Chapter 6 of my book. The proof of (2) and (3) is based on Theorem 3.1 (proved in Chapter 4).

4.4. **Non-abelian torsors and beyond.** The previous discussion gives a satisfactory theory of the algebraic Manin obstruction. Two questions though are left unanswered:

Question 1. Can the non-algebraic (also known as *transcendental*) Manin obstruction be given in terms of torsors?

Question 2. If the Manin obstruction fails to explain a counter-example to the Hasse principle, can it be done using torsors? If not, what other obstructions can be there?

Let $\mathcal{F}$ be a contravariant functor from the category of k-schemes to the category of sets or abelian groups. For example, $\mathcal{F} = \mathrm{H}^i(X, G)$, where G is a commutative k-group scheme, or $\mathcal{F} = \mathrm{H}^1(X, G)$, where G is any k-group scheme. For $\phi \in \mathcal{F}(X)$ define $X(\mathbb{A}_k)^\phi$ as the the set of adelic points (P_v) such that $(\phi(P_v))$ belongs to the image of the diagonal map $\mathcal{F}(k) \to \prod_{all\ v} \mathcal{F}(k_v)$. Define $X(\mathbb{A}_k)^\mathcal{F}$ as the intersection of $X(\mathbb{A}_k)^\phi$ for all $\phi \in \mathcal{F}(X)$. We have obvious inclusions

$$X(k) \subset X(\mathbb{A}_k)^\mathcal{F} \subset X(\mathbb{A}_k)^\phi.$$

In the case of $\mathrm{H}^2(X, \mathbf{G}_m) = \mathrm{Br}\, X$ the set $X(\mathbb{A}_k)^\mathcal{F}$ is the Brauer–Manin set. In the case when G is a k-group scheme, and $\phi \in \mathrm{H}^1(X, G)$ is the class of a torsor $f : Y \to X$ under G, the set $X(\mathbb{A}_k)^\phi$ is the set $X(\mathbb{A}_k)^f$ defined earlier in (11).

Theorem 4.5 (Harari 2002). *Let X be a smooth geometrically integral variety over k.*

(i) $X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)^\phi$ *for any $\phi \in \mathrm{H}^2(X, G)$, where G is a* **commutative** *k-group.*

(ii) $X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)^\phi$ *for any $\phi \in \mathrm{H}^1(X, G)$, where G is a* **connected linear** *k-group.*

(iii) *if $\overline{k}[X]^* = \overline{k}^*$ and X is smooth, then $X(\mathbb{A}_k)^{\mathrm{Br}_1} \subset X(\mathbb{A}_k)^\phi$ for any $\phi \in \mathrm{H}^1(X, G)$, where G is a* **commutative** *k-group.*

Harari points out that the case of commutative G and $i \geq 3$ is of no interest because the corresponding diagonal map is an isomorphism (moreover, only the real places can give rise to non-zero cohomology groups).

Answer to Question 1. (iii) and Theorem 4.2 show that the algebraic Brauer–Manin obstruction is equivalent to the intersection of all the obstructions given by torsors under commutative groups (including the obstruction coming from the existence of such torsors). However, if $\mathrm{Br}\,\overline{X} \neq 0$ we need torsors under $\mathrm{PGL}(n)$ to account for the full Brauer–Manin obstruction.

Let X be a smooth and projective variety. By a theorem of Gabber (see de Jong's paper) $\mathrm{Br}\,X = \mathrm{Br}_{\,A}(X)$, where the latter is the group of similarity classes of Azumaya algebras ($\mathcal{O}_X$-sheaves of central simple algebras). The exact sequence of étale sheaves of groups defined by the exact sequence of algebraic groups (8) gives rise to the exact sequence of pointed (Čech cohomology) sets

$$\mathrm{H}^1(X, \mathbf{G}_m) \to \mathrm{H}^1(X, \mathrm{GL}(n)) \to \mathrm{H}^1(X, \mathrm{PGL}(n)) \xrightarrow{d_n} \mathrm{Br}\,X.$$

The group $\mathrm{Br}_{\,A}(X)$ is the union of images of $d_n(\mathrm{H}^1(X, \mathrm{PGL}(n)))$ for all n. It is known that $d_n(\mathrm{H}^1(X, \mathrm{PGL}(n))) \subset \mathrm{Br}_{\,A}(X)[n]$ ([Milne, EC], IV.2.7). In the case X =Spec(k), where k is a number field or a local field, it is well known that the map

$$d_n : \mathrm{H}^1(k, \mathrm{PGL}(n)) \to \mathrm{Br}\,(k)[n]$$

is surjective. (The order of the class of a central simple algebra in the Brauer group of k equals its index.) This map is also injective (see [Serre, CL], X.5), and hence is bijective.

Let **PGL** be the disjoint union of sets $\mathrm{H}^1(X, \mathrm{PGL}(n))$ for all $n = 2, 3, \ldots$. Using the facts we mentioned above, it is easy to show that

$$X(\mathbb{A}_k)^{\mathrm{Br}_{\,A}(X)} = \bigcap_{f \in \mathbf{PGL}} X(\mathbb{A}_k)^f.$$

The conclusion is that all Manin obstruction can be given in terms of torsors.

Answer to Question 2. In the late 90's examples were found of descents involving torsors under nonabelian G, which go beyond the Brauer–Manin obstruction.

(a) There is a bielliptic surface X over $\mathbb{Q}$ (constructed by the author) such that $X(\mathbb{Q})$ is empty, but the Brauer–Manin set is not. This counter-example can be explained by descent using a torsor under a finite nilpotent group G. This G is the semi-direct product of $E[4]$ by $\mathbb{Z}/2$, where E is an elliptic curve, and the non-trivial element of $\mathbb{Z}/2$ acts on $E[4]$ as multiplication by -1. (See Chapter 8 of my book.)

(b) Harari gives a geometric condition which guarantees that the closure of $X(k)$ in the space of adelic points is smaller than the Brauer–Manin set. This is always the case for smooth projective varieties X such that

(i) $\pi_1(\overline{X}, \bar{x})$ is non-abelian;

(ii) $\mathrm{H}^2(X, \mathcal{O}_X) = 0$;

(iii) $\mathrm{H}^1(X, \mathcal{O}_X) = 0$, or $\dim \mathrm{H}^1(X, \mathcal{O}_X) = 1$ and $\dim X \geq 2$.

These conditions are satisfied for all bielliptic surfaces as well as for some elliptic surfaces and for some surfaces of general type.

(c) The theorem in (b) does not apply to Enriques surfaces for which $\pi_1(\overline{X}, \bar{x}) \simeq \mathbb{Z}/2$ (the universal covering is a K3 surface). However, Harari and the author produced an example of such a surface $X/\mathbb{Q}$ for which the closure of $X(\mathbb{Q})$ in the space of adelic points is smaller than the Brauer–Manin set. This counter-example can be explained by descent using a torsor under a group G, which is an extension of $\mathbb{Z}/2$ by a 1-dimensional torus. In fact, G is a k-form of the orthogonal group $\mathrm{O}(2)$

However, it is unlikely that the counter-example to the Hasse principle constructed by Sarnak and Wang (conditionally on Lang's conjecture) can be explained in terms of torsors. In this case $\mathrm{Br}\, X = \mathrm{Br}\, k$ so the torsors under connected linear groups give no obstruction, and, on the other hand, $\overline{X}$ is simply connected, so no obstruction comes from torsors under finite groups either. In this example $\dim X = 4$, so this does not rule out the possibility that some theory may still exist for curves and surfaces.

In his thesis S. Cunnane constructed an Enriques surface $X/\mathbb{Q}$ such that the closure of $X(\mathbb{Q})$ is smaller than the Brauer–Manin set, but for which no torsor-theoretic argument is known. His proof uses the Manin obstruction on the K3 cover Y/X that does not come from an Azumaya algebra on X. This idea was already used in Example (c) above, but in that example the obstruction comes from an algebraic element of $\mathrm{Br}\, Y$; it is this that makes it possible to relate it to torsors. When the obstruction comes from a transcendental element, as in Cunnane's example, no such relation is known.