TWISTS

HUGO ZOCK

ABSTRACT. We define the notion of a "base extension", an abstract framework to axiomatize the notion of Galois descent in various contexts. We subsequently retrieve the well known principle that twisted forms of a k-object X are parametrized by the Galois cohomology set $\mathrm{H}^1(k, \mathrm{Aut}_{k^s}(X^s))$ for practically all types of objects.

1. INTRODUCTION

Mathematical objects are often defined over a base field k. Examples include vector spaces, schemes, and elliptic curves. Given an object X over k and a field extension ℓ of k, the object X can often be *extended* to an object X_ℓ over ℓ; for example, by taking a tensor product. If Y is another object over k, then Y is said to be an *ℓ/k-twist* of X if X_ℓ and Y_ℓ are isomorphic over ℓ. If Y is furthermore *not* isomorphic to X over k, then Y is said to be a *nontrivial* twist of X.

Example 1.1. Let Q be the conic defined by the equation

$$x^2 + y^2 + z^2 = 0$$

over the field of real numbers $\mathbb{R}$. The conic Q does not have a rational point over $\mathbb{R}$, and so is not isomorphic to the real projective line $\mathbb{P}^1_{\mathbb{R}}$. However, after extending the base field $\mathbb{R}$ to its algebraic closure $\mathbb{C}$, the conic $Q_{\mathbb{C}} := Q \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to the complex projective line $\mathbb{P}^1_{\mathbb{C}}$. Hence, Q is a nontrivial twist of $\mathbb{P}^1_{\mathbb{R}}$.

In particular, we are interested in twists along Galois extensions, where we can apply the theory of Galois cohomology. For the basics of (nonabelian) Galois cohomology we refer to [Ser97, Section I.5.1]. The main result of this paper is stated in Theorem 3.8, and gives a concrete parametrization of the twists of an object X over k along the maximal Galois extension k^s of k in terms of the Galois cohomology set $\mathrm{H}^1(k, \mathrm{Aut}_{k^s}(X^s))$.

The concept of twists in various contexts has been studied quite extensively. See for example [Ser97, Section III.1] and [Bru09]. Contrary to these texts, this paper is concerned with the parametrization of twists in a general setting. The general setting for twists in this paper is provided by the concept of a *base extension*, introduced in section 2. The concept should be reminiscent of that of a stack. The approach in this paper is inspired by [Poo17, Section 4.4].

2. Galois descent

We first introduce the notion of a *base extension*, which will give us an abstract framework in which to state *Galois descent*. Throughout this section we fix a field k. Denote by $\mathscr{G} = \mathscr{G}_k$ the *opposite* of the category of Galois extensions $k \subset \ell$; i.e., an arrow $L \to \ell$ in $\mathscr{G}$ is an inclusion $\ell \subset L$ of Galois extensions over k. Notice that for $k \subset \ell$ a Galois extension, there is an arrow $\ell \to \ell$ associated to any $\sigma \in \mathrm{Gal}(\ell/k)$.

Definition 2.1. A *base extension over* k is a fibered category $\mathscr{C} \to \mathscr{G}$.

If $\mathscr{C} \to \mathscr{G}$ is a base extension, then we denote by $\mathscr{C}_\ell$ the fiber over ℓ. An object of the category $\mathscr{C}_\ell$ is referred to as *an object over* ℓ. If $\ell \subset L$ is an extension of fields Galois over k, then there is an associated functor

$$(-)_{L/\ell} \colon \mathscr{C}_\ell \to \mathscr{C}_L$$

called the *base extension along* L/ℓ. It is unique up to a canonical isomorphism. Similarly, if $\sigma \in \mathrm{Gal}(\ell/k)$ is an element of the Galois group, then there is an associated functor

$$^{\sigma}(-) \colon \mathscr{C}_\ell \to \mathscr{C}_\ell.$$

For convenience, we will always take $^{\mathrm{id}}(-) = \mathrm{id}$. Sometimes we will say that $^{\sigma}X$ is the *twist of* X *by* σ.

Let $\ell \subset L$ be an extension in $\mathscr{G}$. Let $\sigma \in \mathrm{Gal}(L/k)$ be an element of the Galois group of L over k, and denote by $\overline{\sigma} \in \mathrm{Gal}(\ell/k)$ its restriction. There is a canonical isomorphism of functors

$$\eta_\sigma^{L/\ell} \colon {}^{\sigma}(-)_{L/\ell} := {}^{\sigma}(-) \circ (-)_{L/\ell} \Rightarrow (-)_{L/\ell} \circ {}^{\overline{\sigma}}(-).$$

Often the superscript L/ℓ will be omitted when it is clear from the context. Furthermore, the isomorphisms η_σ satisfy the cocycle condition: for X an object over ℓ and $\sigma, \tau \in \mathrm{Gal}(L/\ell)$ the triangle

(2.1)
$$\begin{array}{ccc} {}^{\sigma\tau}X_L & \xrightarrow{\quad \eta_{\sigma\tau} \quad} & ({}^{\overline{\sigma\tau}}X)_L \\ & {\scriptstyle {}^{\sigma}\eta_\tau} \searrow \quad \nearrow {\scriptstyle \eta_\sigma} & \\ & {}^{\sigma}({}^{\overline{\tau}}X)_L & \end{array}$$

commutes. This is often expressed simply as

$$\eta_{\sigma\tau} = \eta_\sigma \circ {}^{\sigma}\eta_\tau. \tag{2.2}$$

The isomorphisms η_σ are also compatible with the functor $(-)_{L/\ell}$ in the sense that for $\sigma \in \mathrm{Gal}(L/k)$ and X an object over k we have a commutative triangle

(2.3)
$$\begin{array}{ccc} {}^{\sigma}X_L & \xrightarrow{\quad \eta_\sigma^{L/\ell} \quad} & ({}^{\overline{\sigma}}X_\ell)_L \\ & {\scriptstyle \eta_\sigma^{L/k}} \searrow \quad \swarrow {\scriptstyle (\eta_{\overline{\sigma}}^{\ell/k})_L} & \\ & X_L. & \end{array}$$

Let X be an object over L. A collection of isomorphisms $(f_\sigma : {}^\sigma X \to X)$, with σ ranging over the elements of $\mathrm{Gal}(L/\ell)$, satisfying the *cocycle condition*

$$f_{\sigma\tau} = f_\sigma \circ {}^\sigma f_\tau \tag{2.4}$$

is called an *L/ℓ-descent datum* on X. If X and Y are objects over L with descent data (f_σ) and (g_σ) respectively, and $\varphi : X \to Y$ is a map of L-objects, then we say that φ is *compatible with descent data* if for all $\sigma \in \mathrm{Gal}(L/\ell)$ the diagram

$$\begin{array}{ccc} {}^\sigma X & \xrightarrow{{}^\sigma\varphi} & {}^\sigma Y \\ \downarrow{\scriptstyle f_\sigma} & & \downarrow{\scriptstyle g_\sigma} \\ X & \xrightarrow{\varphi} & Y \end{array}$$

commutes. The category of L-objects with L/ℓ-descent data and compatible maps is denoted $\mathscr{C}_\ell^L$. Notice that there is a natural forgetful functor $\mathscr{C}_\ell^L \to \mathscr{C}_L$. If x is an object over ℓ, then x_L is canonically equipped with a descent datium by (2.2). As a result, there is a factorization

$$\begin{array}{ccc} \mathscr{C}_\ell & \xrightarrow{(-)_{L/\ell}} & \mathscr{C}_L \\ & \searrow \quad \nearrow & \\ & \mathscr{C}_\ell^L. & \end{array}$$

Definition 2.2. (i) If $(f_\sigma : {}^\sigma X \to X)$ is an L/ℓ-descent datum on an L-object X, then we say it is *effective* if there is an object x over ℓ such that x_L and X are isomorphic in $\mathscr{C}_\ell^L$. In other words, X *descends* to x.

(ii) We say that a base extension satisfies *Galois descent* if for every *finite* Galois extension ℓ/k the induced functor $\mathscr{C}_k \to \mathscr{C}_k^\ell$ is fully faithful.

We sketch some of the most important examples of base extensions below.

Example 2.3. In all of the examples $\ell \subset L$ denotes a generic extension in $\mathscr{G}$, and F denotes a general field.

(i) Let Vect be the category of pairs (V, ℓ), where ℓ/k is a Galois extension and V is a vector space over ℓ. A morphism of pairs $(W, \ell) \to (V, L)$ consists of an arrow $L \to \ell$ in $\mathscr{G}$ and a morphism of L-vector spaces $W \to V \otimes_\ell L$. There is an obvious forgetful functor $\mathrm{Vect} \to \mathscr{G}$, which is a base extension over k.

Suppose now that ℓ/k is finite. To give a descent datum on a vector space W over ℓ is the same as defining a *semi-linear* $\mathrm{Gal}(\ell/k)$-action on W. It is then a theorem that the functor $- \otimes_k \ell$ defines an equivalence between Vect_k and the category of ℓ-vector spaces equipped with a semi-linear $\mathrm{Gal}(\ell/k)$-action. See [Poo17, Theorem 1.3.11] for more details. It follows that the base extension $\mathrm{Vect} \to \mathscr{G}$ satisfies Galois descent, and that all descent data along finite Galois extensions is effective for this base extension.

(ii) We write Alg for the category of pairs (A,ℓ), where ℓ/k is a Galois extension and A is an algebra over ℓ. Morphisms are defined analogously to the previous example. We obtain a base extension $\mathrm{Alg}\to\mathscr{G}$. This base extension then also satisfies Galois descent, and all descent data along finite extensions is effective for this base extension.

(iii) Write Sch for the category of pairs (X,ℓ), where ℓ/k is a Galois extension and X is a scheme over ℓ. A morphism of pairs $(Y,L)\to(X,\ell)$ consists of an arrow $L\to\ell$ in $\mathscr{G}$ and a morphism $Y\to X_L$ of L-schemes. Here $X_L = X\times_\ell \operatorname{Spec} L$. We obtain a base extension $\mathrm{Sch}\to\mathscr{G}$.

By fpqc-descent the base extension $\mathrm{Sch}\to\mathscr{G}$ satisfies Galois descent (see [Poo17, Theorem 4.3.5]). If Y is a quasi-projective scheme over ℓ, then all descent data on Y along ℓ/k is effective if ℓ/k is finite (see [Poo17, Corollary 4.4.6]).

(iv) For a scheme S we denote the category of sheaves over S by $\mathrm{Sh}(S)$. Fix a scheme X over k. We let Sh_X be the category consisting of pairs (F,ℓ), where ℓ/k is a Galois extension and F is a sheaf on X_ℓ. A morphism of pairs $(G,L)\to(F,\ell)$ is given by an arrow $L\to\ell$ in $\mathscr{G}$ together with a morphism $G\to F\otimes_\ell L$ of sheaves on X_L. We obtain a base extension $\mathrm{Sh}_X\to\mathscr{G}$.

Replacing sheaves by quasi-coherent sheaves, we similarly obtain a base extension $\mathrm{Qcoh}_X\to\mathscr{G}$. It is then also true that the functor $\mathrm{Qcoh}(X)\to\mathrm{Qcoh}(X_\ell)^{\ell}_{k}$ is an equivalence if ℓ/k is finite. This is the content of [Jah00, Proposition 2.6 and 2.9]. Hence, the base extension $\mathrm{Qcoh}_X\to\mathscr{G}$ satisfies Galois descent, and all descent data along finite Galois extensions is effective for this base extension.

(v) We define an *elliptic curve* over F to be a morphism $O\colon \operatorname{Spec} F\to E$ of F-schemes, where E is a smooth, projective, geometrically integral curve of genus 1 over F. An *isogeny* of elliptic curves is a map of F-schemes $\varphi: E\to E'$ fitting into a commutative triangle

$$\begin{array}{ccc} & \operatorname{Spec} F & \\ \swarrow & & \searrow \\ E & \xrightarrow{\quad\varphi\quad} & E'. \end{array}$$

If $O\colon \operatorname{Spec}\ell\to E$ is an elliptic curve over ℓ, then $O_L\colon \operatorname{Spec} L\to E_L$ is naturally an elliptic curve over L.

Let Ec be the category of pairs (E,ℓ), where ℓ/k is a Galois extension and E is an elliptic curve over ℓ. A morphism of pairs $(E',L)\to(E,\ell)$ consists of an arrow $L\to\ell$ in $\mathscr{G}$ and a morphism $E'\to E_L$ of elliptic curves. We obtain a base extension $\mathrm{Ec}\to\mathscr{G}$.

The base extension $\mathrm{Ec}\to\mathscr{G}$ satisfies Galois descent and all descent data along finite Galois extensions is effective for this base extension. This can be seen as follows. Suppose ℓ/k is finite. If $O:\operatorname{Spec}\ell\to E'$ is an elliptic curve over ℓ with descent data, then the morphism O is compatible with descent data for the base extension $\mathrm{Sch}\to\mathscr{G}$. Since O is a morphism of quasi-projective schemes, we can descend it to a morphism of schemes $o:\operatorname{Spec} k\to E$. The fact that $o:\operatorname{Spec} k\to E$ is an elliptic curve, follows from the fact that E' is (see, for instance, [Jah00, Lemma 2.12]). This provides us with a quasi-inverse to the functor $(-)_{\ell/k} : \mathrm{Ec}_k \to \mathrm{Ec}_k^{\ell}$.

(vi) We generalize the last example. An algebraic group over F is a group scheme over F of finite type. We denote by AlgGrp the category of pairs (G, ℓ), where ℓ/k is a Galois extension and G is an algebraic group over ℓ. We have a base extension AlgGrp $\to \mathscr{G}$. By [Poo17, Theorem 5.2.20] all algebraic groups over F are quasi-projective. We can use this to prove that the base extension AlgGrp $\to \mathscr{G}$ satisfies Galois descent and that all descent data along finite Galois extensions are effective.

2.1. **Some properties of base extensions.** Let $\mathscr{C} \to \mathscr{G}$ be a base extension over k.

Proposition 2.4. *For $\ell \subset L$ an extension in $\mathscr{G}$, the functor $(-)_{L/\ell} : \mathscr{C}_\ell \to \mathscr{C}_L$ restricts to a functor*

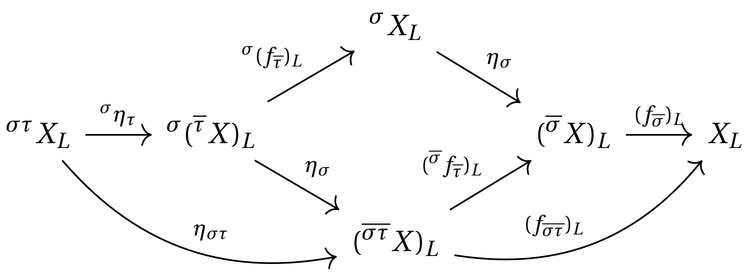
$$(-)_{L/\ell} : \mathscr{C}_k^{\ell} \to \mathscr{C}_k^{L}.$$

If X is an object over ℓ with a descent datum $(f_\sigma : {}^\sigma X \to X)$, then X_L is equipped with the L/k-descent datum

$$(F_\sigma : {}^\sigma X_L \xrightarrow{\eta_\sigma^{L/\ell}} ({}^{\overline{\sigma}} X)_L \xrightarrow{(f_{\overline{\sigma}})_L} X_L).$$

Proof. We have to prove that (F_σ) defines a descent datum on X_L and that a map $\varphi : X \to Y$ of ℓ-objects compatible with ℓ/k-descent data, induces a map $\varphi_L : X_L \to Y_L$ compatible with L/k-descent data.

For $\sigma, \tau \in \mathrm{Gal}(L/k)$ consider the diagram



The triangle on the left commutes by the cocycle condition, the middle square commutes by naturality of η_σ, and the right triangle commutes by the fact that (f_σ) defines a descent datum. Hence, the diagram is commutative. The composition of the top maps is $F_\sigma {}^\sigma F_\tau$, and the composition of the bottom maps is $F_{\sigma\tau}$.

If $\varphi : X \to Y$ is a map of ℓ-objects compatible with ℓ/k-descent data $(f_\sigma : {}^\sigma X \to X)$ and $(g_\sigma : {}^\sigma Y \to Y)$. Then we obtain a diagram

$$\begin{array}{ccc} {}^\sigma X_L & \xrightarrow{{}^\sigma \varphi_L} & {}^\sigma Y_L \\ \downarrow{\scriptstyle \eta_\sigma} & & \downarrow{\scriptstyle \eta_\sigma} \\ ({}^{\overline{\sigma}} X)_L & \xrightarrow{({}^{\overline{\sigma}}\varphi)_L} & ({}^{\overline{\sigma}} Y)_L \\ \downarrow{\scriptstyle (f_{\overline{\sigma}})_L} & & \downarrow{\scriptstyle (g_{\overline{\sigma}})_L} \\ X_L & \xrightarrow{\varphi_L} & Y_L. \end{array}$$

The top and bottom square commutes by naturality of η and the fact that φ is compatible with descent data. It follows that φ_L is compatible with descent data. ■

Proposition 2.5. *Suppose $\ell \subset L$ is an extension of fields Galois over k. Then we obtain a commutative diagram of functors*

$$\begin{array}{ccccc} \mathscr{C}_k & & \xrightarrow{(-)_{L/K}} & & \mathscr{C}_k^L \\ & \searrow{\scriptstyle (-)_{\ell/k}} & & \nearrow{\scriptstyle (-)_{L/\ell}} & \\ & & \mathscr{C}_k^\ell & & \end{array}$$

Proof. This comes down to the commutativity of the triangle (2.3). ■

The above proposition tells us that it does not matter whether we first equip a k-object X with a descent datum along ℓ/k and then with a descent datum along L/k, or directly with a descent datum along L/k.

Proposition 2.6. *If $\ell \subset L$ is an extension of fields Galois over k, then we have a commutative square of functors*

$$\begin{array}{ccc} \mathscr{C}_k & \xrightarrow{(-)_{L/k}} & \mathscr{C}_k^L \\ \downarrow{\scriptstyle (-)_{\ell/k}} & & \downarrow{\scriptstyle U} \\ \mathscr{C}_\ell & \xrightarrow{(-)L/\ell} & \mathscr{C}_\ell^L, \end{array}$$

where U denotes the natural forgetful functor.

Proof. This is by the commutativity of (2.3) and the fact that $\eta_{\mathrm{id}}^{\ell/k}$ is the identity. ■

Intuitively, for a k-object X, the L/ℓ-descent datum obtained by “forgetting a part of the L/k-descent datum”, agrees with the L/ℓ-descent datum obtained from the extension L/ℓ.

3. TWISTS

Throughout this paragraph we fix a base extension $\mathscr{C} \to \mathscr{G}_k$, over a field k. We fix a finite Galois extension ℓ/k with group G. Fix an object Z over ℓ. If (f_σ) and (g_σ) define two descent data on Z, then we say they are *equivalent*, and write $(f_\sigma) \sim (g_\sigma)$, if the two resulting objects in $\mathscr{C}_k^\ell$ are isomorphic. Define the set D_Z by

$$D_Z = \{X \in \mathscr{C}_k : X_\ell \simeq Z\}/\simeq_k .$$

Define the set E_Z to be the set of ℓ/k-descent data on Z modulo equivalence.

Given an object X over k such that there is an isomorphism $\varphi : Z \to X_\ell$, we define

$$f_\sigma^\varphi = \varphi^{-1} \circ g_\sigma \circ {}^\sigma\varphi : {}^\sigma Z \to Z$$

for $\sigma \in G$, where (g_σ) is the induced descent datum on X_ℓ. The collection of maps (f_σ^φ) defines a descent datum on Z: for $\sigma, \tau \in G$ we have

$$\begin{aligned} f_\sigma^\varphi \circ {}^\sigma f_\tau^\varphi &= \varphi^{-1} \circ g_\sigma \circ {}^\sigma\varphi \circ {}^\sigma(\varphi^{-1} \circ g_\tau \circ {}^\tau\varphi) \\ &= \varphi^{-1} \circ g_\sigma \circ {}^\sigma g_\tau \circ {}^{\sigma\tau}\varphi \\ &= \varphi^{-1} \circ g_{\sigma\tau} \circ {}^{\sigma\tau}\varphi = f_{\sigma\tau}^\varphi, \end{aligned}$$

where the last equality follows from the fact that (g_σ) is a descent datum. The descent datum (f_σ^φ) is defined precisely such that φ defines an isomorphism $Z \xrightarrow{\simeq} X_\ell$ in the category $\mathscr{C}_k^\ell$, if we equip Z with the descent datum (f_σ^φ).

Now suppose we have a second k-object Y, a k-isomorphism $Y \simeq X$, and an ℓ-isomorphism $\psi : Z \xrightarrow{\simeq} Y_\ell$. We obtain a commutative diagram

$$\begin{array}{ccccccc} {}^\sigma Z & \xrightarrow{{}^\sigma\psi} & {}^\sigma Y_\ell & \xrightarrow{\simeq} & {}^\sigma X_\ell & \xrightarrow{{}^\sigma\varphi^{-1}} & {}^\sigma Z \\ \downarrow f_\sigma^\psi & & \downarrow & & \downarrow & & \downarrow f_\sigma^\varphi \\ Z & \xrightarrow{\psi} & Y_\ell & \xrightarrow{\simeq} & X_\ell & \xrightarrow{\varphi^{-1}} & Z, \end{array}$$

for all $\sigma \in G$, which shows that the descent data (f_σ^ψ) and (f_σ^φ) on Z are equivalent. In particular, the choice of isomorphism φ is irrelevant up to equivalence of descent data. We will often write (f_σ^X), instead of (f_σ^φ), when we only care about descent data up to equivalence. We obtain a map

$$\begin{aligned} \alpha : D_Z &\to E_Z \\ X &\mapsto (f_\sigma^X). \end{aligned} \tag{3.1}$$

Proposition 3.1. *(i) If the base extension $\mathscr{C} \to \mathscr{G}$ satisfies Galois descent, then the map constructed in equation* (3.1) *is injective;*
(ii) if all descent data along ℓ/k is effective, then it is surjective.

Proof. (i) Let X and Y be objects in D_Z whose image under α agrees. Then there is an isomorphism $\varphi : X_\ell \to Y_\ell$ of objects in $\mathscr{C}_k^\ell$. Using the fact that $\mathscr{C}_k \to \mathscr{C}_k^\ell$ is fully faithful, we can descend φ to an isomorphism $X \simeq Y$ of k-objects. Hence, the classes of X and Y in D_Z agree.

(ii) This is clear.

■

3.1. **Parametrization of twists.** In the setting of the previous paragraph, we turn our attention to the case where Z is the extension of a fixed object X defined over k. Again fix a base extension $\mathscr{C} \to \mathscr{G}$ over k and a finite Galois extension ℓ/k with group G. We write (f_σ) for the induced descent datum on X_ℓ. We define the set $T_{\ell/k}(X) = T(X)$ by

$$T(X) = \{Y \in \mathscr{C}_k : Y_\ell \simeq X_\ell\}/\simeq_k,$$

the set of *ℓ/k-twists* of X. We equip the set $T(X)$ with a basepoint: the class of the object X itself. In terms of notation from the previous section, this is just the set D_{X_ℓ}. We denote the set E_{X_ℓ} from the previous section by E_X. The set E_X also has the structure of a pointed set, with basepoint the induced descent datum (f_σ) on X_ℓ.

Let A be the group $\mathrm{Aut}_\ell(X_\ell)$ of automorphisms of X_ℓ in $\mathscr{C}_\ell$. It is naturally equipped with an action of the Galois group G as follows: for $\sigma \in G$ and $\varphi \in A$ we define

$$\sigma(\varphi) = f_\sigma \circ {}^\sigma\varphi \circ f_\sigma^{-1}. \tag{3.2}$$

Let (g_σ) be a descent datum on X_ℓ. For $\sigma \in G$ we define

$$c_\sigma = g_\sigma \circ f_\sigma^{-1} \in A.$$

The collection $c = (c_\sigma)$ defines a 1-cocycle: for $\sigma, \tau \in G$ we compute

$$\begin{aligned} c_\sigma \circ \sigma(c_\tau) &= g_\sigma \circ f_\sigma^{-1} \circ \sigma(g_\tau \circ f_\tau^{-1}) \\ &= g_\sigma \circ f_\sigma^{-1} \circ f_\sigma \circ {}^\sigma(g_\tau \circ f_\tau^{-1}) \circ f_\sigma^{-1} \\ &= g_\sigma \circ {}^\sigma g_\tau \circ (f_\sigma \circ {}^\sigma f_\tau)^{-1} \\ &= g_{\sigma\tau} \circ f_{\sigma\tau}^{-1} = c_{\sigma\tau}, \end{aligned}$$

where the last equality follows from the fact that (f_σ) and (g_σ) are descent data.

Suppose (g'_σ) is another descent datum on X_ℓ, which is equivalent to (g_σ). Then there is $a \in A$ such that for all $\sigma \in G$ we have

$$g'_\sigma = a^{-1} \circ g_\sigma \circ {}^\sigma a.$$

For $c' = (g'_\sigma \circ f_\sigma^{-1})$, the cocycle associated to (g'_σ), and $\sigma \in G$, we have

$$\begin{aligned} a^{-1} \circ c_\sigma \circ {}^\sigma a &= a^{-1} \circ g_\sigma \circ f_\sigma^{-1} \circ \sigma(a) \\ &= a^{-1} \circ g_\sigma \circ f_\sigma^{-1} \circ f_\sigma \circ {}^\sigma a \circ f_\sigma^{-1} \\ &= a^{-1} \circ g_\sigma \circ {}^\sigma a \circ f_\sigma^{-1} \\ &= g'_\sigma \circ f_\sigma^{-1} = c'_\sigma. \end{aligned}$$

It follows that the cocycles c and c' are cohomologous. We conclude that we have a well-defined map

$$\begin{aligned} \beta : E_X &\to \mathrm{H}^1(G;A) \\ (g_\sigma) &\mapsto (g_\sigma \circ f_\sigma^{-1}). \end{aligned} \tag{3.3}$$

Clearly β is a map of pointed sets.

We intend to construct an inverse to the map β. Let $c = (c_\sigma)$ be a cocycle. For $\sigma \in G$, we define

$$g_\sigma = c_\sigma \circ f_\sigma : {}^\sigma X_\ell \to X_\ell.$$

The collection of maps (g_σ) defines a descent datum on X_ℓ: for $\sigma, \tau \in G$ we compute

$$\begin{aligned} g_\sigma \circ {}^\sigma g_\tau &= c_\sigma \circ f_\sigma \circ {}^\sigma (c_\tau \circ f_\tau) \\ &= c_\sigma \circ f_\sigma \circ {}^\sigma c_\tau \circ {}^\sigma f_\tau \\ &= c_\sigma \circ f_\sigma \circ {}^\sigma c_\tau \circ f_\sigma^{-1} \circ f_\sigma \circ {}^\sigma f_\tau \\ &= c_\sigma \circ \sigma(c_\tau) \circ f_{\sigma\tau} \\ &= c_{\sigma\tau} \circ f_{\sigma\tau} = g_{\sigma\tau}, \end{aligned}$$

where the last two equalities follow from the fact that (f_σ) is a descent datum and c a cocycle. Suppose that $c' = (c'_\sigma)$ is a cocycle which is equivalent to c, i.e., there exists $a \in A$ such that

$$c'_\sigma = a^{-1} \circ c_\sigma \circ \sigma(a)$$

for all $\sigma \in G$. We compute

$$\begin{aligned} c'_\sigma \circ f_\sigma &= a^{-1} \circ c_\sigma \circ \sigma(a) \circ f_\sigma \\ &= a^{-1} \circ c_\sigma \circ f_\sigma \circ {}^\sigma a \circ f_\sigma^{-1} \circ f_\sigma \\ &= a^{-1} \circ (c_\sigma \circ f_\sigma) \circ {}^\sigma a, \end{aligned}$$

and so we conclude that the descent data $(c_\sigma \circ f_\sigma)$ and $(c'_\sigma \circ f_\sigma)$ are equivalent. We have now constructed a well-defined map

$$\begin{aligned} \gamma : \mathrm{H}^1(G;A) &\to E_X \\ c = (c_\sigma) &\mapsto (c_\sigma \circ f_\sigma). \end{aligned} \tag{3.4}$$

The following lemma is now clear.

Lemma 3.2. *The maps β and γ defined in equations* (3.3) *and* (3.4) *are inverse to each other.* ■

The composition of the map α from (3.1) with the map β from (3.3) gives the map

$$\theta_{\ell/k}^{-1} = \theta^{-1} : T_{\ell/k}(X) \to \mathrm{H}^1(G; \mathrm{Aut}_\ell(X_\ell)), \tag{3.5}$$

which sends the k-isomorphism class of an ℓ/k-twist Y of X to the class of the cocycle $c = (c_\sigma)$ defined by

$$c_\sigma = \varphi^{-1} \circ g_\sigma \circ {}^\sigma\varphi \circ f_\sigma^{-1},$$

where $\varphi : X_\ell \to Y_\ell$ denotes an isomorphism, (g_σ) the induced descent datum on Y_ℓ, and (f_σ) the induced descent datum on X_ℓ.

Theorem 3.3. *(i) If the base extension* $((-)_{L/\ell} : \mathscr{C}_\ell \to \mathscr{C}_L)$ *satisfies Galois descent, then the map* θ^{-1} *from* (3.5) *is injective;*
(ii) if all ℓ/k*-descent data is effective, then* θ^{-1} *is surjective.*

Proof. Combine Proposition 3.1 and Lemma 3.2. ∎

Example 3.4. (i) Consider the elliptic curve E over $\mathbb{F}_5$ defined by the short Weierstrass equation

$$y^2 = x(x-1)(x+1).$$

It has j-invariant $3 = 1728$, and so general theory tells us that its automorphism group over $\overline{\mathbb{F}}_5$ is cyclic of order 4 (see [Sil13, III, Corollary 10.2]). It is generated by

$$(x, y) \mapsto (-x, 2y),$$

which is defined over $\mathbb{F}_5$. Consider the finite Galois extension $\ell = \mathbb{F}_5(\sqrt{3})/\mathbb{F}_5$ with Galois group G of order 2. Theorem 3.3 applied to Example 2.3(v) tells us that there is an isomorphism of pointed sets

$$T_{\ell/\mathbb{F}_5}(E) \simeq \mathrm{H}^1(G; \mathrm{Aut}_\ell(E_\ell)).$$

The Galois group G acts trivially on $\mathrm{Aut}_\ell(E_\ell)$. A basic group cohomological computation shows that $\mathrm{H}^1(G; \mathrm{Aut}_\ell(E_\ell))$ is of order 2. The only non-trivial twist of E is given by

$$E' : y^2 = 2x(x-1)(x+1).$$

Indeed, E and E' are isomorphic over ℓ via

$$E_\ell \xrightarrow{\simeq} E'_\ell$$
$$(x, y) \mapsto (x, y\sqrt{3});$$

however, the two are not isomorphic over $\mathbb{F}_5$: they don't have the same number of points over $\mathbb{F}_5$.

(ii) Let $\mathbb{G}_m$ be the multiplicative group over $\mathbb{R}$:

$$\mathbb{G}_m = \mathbb{A}^1_{\mathbb{R}} \setminus \{0\} \simeq \operatorname{Spec} \mathbb{R}[x, y]/(xy - 1).$$

Consider the base extension of algebraic groups over $\mathbb{R}$ defined in Example 2.3(vi). A $\mathbb{C}/\mathbb{R}$-twist of $\mathbb{G}_m$ is called a *torus of dimension 1* over $\mathbb{R}$. It is called *split* if it is trivial as a twist of $\mathbb{G}_m$. denote the base extension of $\mathbb{G}_m$ to $\mathbb{C}$ by $\overline{\mathbb{G}}_m$. Its automorphism group over $\mathbb{C}$ is given by $\{\pm 1\} = \langle x \mapsto y = x^{-1} \rangle$. By Theorem 3.3 there is an isomorphism of pointed sets

$$\{\text{1-dimensional tori over } \mathbb{R}\}/\simeq_{\mathbb{R}} = T_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m) \simeq \mathrm{H}^1(\mathbb{R}, \{\pm 1\}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

We conclude that there is exactly one non-split torus over $\mathbb{R}$ up to $\mathbb{R}$-isomorphism. We set out to compute it. Consider the algebraic group G over $\mathbb{R}$ defined by

$$G = \operatorname{Spec}\mathbb{R}[x, y]/(x^2 + y^2 - 1).$$

Its multiplication is defined by

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

We have an isomorphism $G_{\mathbb{C}} \simeq \overline{\mathbb{G}}_m$ of algebraic groups over $\mathbb{C}$ given by

$$\begin{aligned} G_{\mathbb{C}} &\xrightarrow{\simeq} \overline{\mathbb{G}}_m \simeq \operatorname{Spec}\mathbb{C}[x, y]/(xy - 1) \\ (x, y) &\mapsto (x + iy, x - iy). \end{aligned}$$

This isomorphism does not descend to one over $\mathbb{R}$, and we can see that none do, because the composition of this isomorphism with the only non-trivial automorphism of $\overline{\mathbb{G}}_m$ does not descend either. We conclude that G is the only non-trivial 1-dimensional torus over $\mathbb{R}$ up to isomorphism.

3.2. **Twists along a separable closure.** In practice we don't often care about whether two k-objects become isomorphic over some fixed finite Galois extension, but rather whether they become isomorphic after base extension to the separable closure. When k is perfect this is expressed by saying that two k-objects are "geometrically the same", but that they "differ arithmetically". Under some mild conditions we can parametrize k^s/k-twists using Galois cohomology.

For the rest of this paragraph we let k be a field with a fixed separable closure k^s and absolute Galois group $G = \operatorname{Gal}(k^s/k)$. All Galois extensions of k are assumed to lie in k^s. Again fix a base extension $\mathscr{C} \to \mathscr{G}_k$. Let X be an object over k. If Y is an object over k, then we denote its base extension to k^s by Y^s. We define the set $T(X)$ by

$$T(X) = \{Y \in \mathscr{C}_k : Y^s \simeq X^s\}/\simeq_k;$$

the set of k^s/k-twists, or just *twists*, of X.

The Galois group G acts on the group $\operatorname{Aut}_{k^s}(X^s)$ as in (3.2). More generally, if Y and Z denote two objects over k and ℓ/k denotes a Galois extension, then the group $\operatorname{Gal}(\ell/k)$ acts on the set $\operatorname{Isom}_\ell(Y_\ell, Z_\ell)$ of isomorphisms $Y_\ell \to Z_\ell$ in $\mathscr{C}_\ell$ by

$$\sigma(\varphi) = h_\sigma \circ {}^\sigma\varphi \circ g_\sigma^{-1}, \tag{3.6}$$

where (g_σ) denotes the ℓ/k-descent datum on Y_ℓ and (h_σ) denotes the ℓ/k-descent datum on Z_ℓ.

For any Galois extension ℓ/k, the functor $(-)_{k^s/\ell}$ induces a map

$$(-)_{k^s/\ell} : \operatorname{Isom}_\ell(Y_\ell, Z_\ell) \to \operatorname{Isom}_{k^s}(Y^s, Z^s)^{\operatorname{Gal}(k^s/\ell)},$$

by the fact that the extension of a map $\varphi : Y_\ell \to Z_\ell$ to $\mathscr{C}_{k^s}$ is compatible with the induced k^s/ℓ-descent data on Y^s and Z^s, and Proposition 2.6. In case $Y = Z$ this is a homomorphism of groups. An easy verification using Propositions 2.4 and 2.5 shows that this map is compatible with $\operatorname{Gal}(\ell/k)$-actions.

Definition 3.5. A base extension $\mathscr{C} \to \mathscr{G}$ over k is called *continuous* if

(i) for all finite Galois extensions ℓ/k and all k-objects Y and Z the map

$$(-)_{k^s/\ell} : \mathrm{Isom}_\ell(Y_\ell, Z_\ell) \to \mathrm{Isom}_{k^s}(Y^s, Z^s)^{\mathrm{Gal}(k^s/\ell)}$$

is an isomorphism of $\mathrm{Gal}(\ell/k)$-sets;

(ii) for all k-objects Y and Z we have

$$\mathrm{Isom}_{k^s}(Y^s, Z^s) = \bigcup \mathrm{Isom}_{k^s}(Y^s, Z^s)^{\mathrm{Gal}(k^s/\ell)},$$

where ℓ/k ranges over the finite Galois extensions of k.

Example 3.6. The base extensions of finite dimensional vector spaces, finite type algebras, finite type schemes, coherent sheaves on a noetherian scheme, elliptic curves and algebraic groups are all continuous.

Remark 3.7. If a base extension over k is continuous, then the group G acts continuously on the set $\mathrm{Isom}_{k^s}(Y^s, Z^s)$, for all k-objects Y and Z, when we equip it with the discrete topology. In particular this makes $\mathrm{Aut}_{k^s}(X^s)$ a *discrete G-group.*

Assume for the rest of this section that $\mathscr{C} \to \mathscr{G}$ is continuous. By the above remark and part (i) of Definition 3.5 we obtain

$$\begin{aligned} \mathrm{H}^1(G; \mathrm{Aut}_{k^s}(X_{k^s})) &= \varinjlim \mathrm{H}^1(\ell/k, \mathrm{Aut}_{k^s}(X^s)^{\mathrm{Gal}(k^s/\ell)}) \\ &\simeq \varinjlim \mathrm{H}^1(\ell/k; \mathrm{Aut}_\ell(X_\ell)), \end{aligned} \tag{3.7}$$

with the direct limit ranging over the finite Galois extension of k. The natural maps $T_{\ell/k}(X) \to T(X)$, with ℓ/k finite Galois, also give us an isomorphism

$$T(X) \simeq \varinjlim T_{\ell/k}(X), \tag{3.8}$$

because any isomorphism $X^s \simeq Y^s$ can be descended to an isomorphism $X_\ell \simeq Y_\ell$ with ℓ/k finite Galois, by continuity of the base extension. For every finite Galois extension ℓ/k we have a map of pointed sets

$$\theta^{-1}_{\ell/k} : T_{\ell/k}(X) \to \mathrm{H}^1(\ell/k; \mathrm{Aut}_\ell(X_\ell))$$

from (3.5). We prove that these maps are compatible; i.e., that the diagram

$$\begin{array}{ccc} T_{\ell/k}(X) & \xrightarrow{\theta^{-1}_{\ell/k}} & \mathrm{H}^1(\ell/k, \mathrm{Aut}_\ell(X_\ell)) \\ \downarrow & & \downarrow \\ T_{L/k}(X) & \xrightarrow{\theta^{-1}_{L/k}} & \mathrm{H}^1(L/k, \mathrm{Aut}_L(X_L)) \end{array} \tag{3.9}$$

commutes for every extension $\ell \subset L$ of finite Galois extensions over k. Let Y be an ℓ/k-twist of X. Denote the ℓ/k-descent datum on X_ℓ by (f_σ) and the ℓ/k-descent datum on Y_ℓ by (g_σ). Let $\varphi : X_\ell \to Y_\ell$ be an isomorphism over ℓ. The cocycle class of $\theta^{-1}_{\ell/k}(Y)$ in $\mathrm{H}^1(\ell/k, \mathrm{Aut}_\ell(X_\ell))$ is then given by the class of the cocycle

$$c_\sigma = \varphi^{-1} \circ g_\sigma \circ {}^\sigma\varphi \circ f_\sigma^{-1}.$$

Inflating this cocycle class to $\mathrm{H}^1(L/k, \mathrm{Aut}_L(X_L))$, we obtain the class of the cocycle

$$C_\sigma = \varphi_L^{-1} \circ (g_{\overline{\sigma}})_L \circ ({}^{\overline{\sigma}}\varphi)_L \circ (f_{\overline{\sigma}}^{-1})_L,$$

which we can expand to

$$C_\sigma = \varphi_L^{-1} \circ (g_{\overline{\sigma}})_L \circ \varepsilon_\sigma \circ {}^{\sigma}\varphi_L \circ \eta_\sigma^{-1} \circ (f_{\overline{\sigma}}^{-1})_L,$$

where ε_σ denotes the canonical isomorphism ${}^{\sigma}Y_L \to ({}^{\overline{\sigma}}Y)_L$ and η_σ denotes the canonical isomorphism ${}^{\sigma}X_L \to ({}^{\overline{\sigma}}X)_L$.

Taking the alternative route through diagram (3.9), Y is an L/k twist of X via $\varphi_L : X_L \to Y_L$. The descent datum on Y_L is given by $((g_{\overline{\sigma}})_L \circ \varepsilon_\sigma)$ and the descent datum on X_L is given by $((f_{\overline{\sigma}})_L \circ \eta_\sigma)$, by Propositions 2.4 and 2.5. The cocycle class of $\theta_{L/k}^{-1}(Y_L)$ in $\mathrm{H}^1(L/k, \mathrm{Aut}_L(X_L))$ is then given by the class of the cocycle

$$D_\sigma = \varphi_L^{-1} \circ (g_{\overline{\sigma}})_L \circ \varepsilon_\sigma \circ {}^{\sigma}\varphi_L \circ \eta_\sigma^{-1} \circ (f_{\overline{\sigma}}^{-1})_L,$$

which is precisely the cocycle C_σ from before. Hence (3.9) commutes and by taking $\varinjlim$ we obtain a map

$$\theta^{-1} : T(X) \to \mathrm{H}^1(G, \mathrm{Aut}_{k^s}(X^s)), \tag{3.10}$$

using (3.7) and (3.8). It is now not hard to see that this map is explicitly given by sending a twist Y of X to the class of the cocycle

$$c_\sigma = \varphi^{-1} \circ G_\sigma \circ {}^{\sigma}\varphi \circ F_\sigma^{-1},$$

where $\varphi : X^s \xrightarrow{\simeq} Y^s$ is an isomorphism, and (F_σ) and (G_σ) denote the the descent datum on X^s respectively Y^s.

Theorem 3.8. *Let $((-)_{L/\ell} : \mathscr{C}_\ell \to \mathscr{C}_L)$ be a continuous base extension over k.*

(i) If $((-)_{L/\ell} : \mathscr{C}_\ell \to \mathscr{C}_L)$ satisfies Galois descent, then the map θ^{-1} constructed in (3.10) *is injective;*
(ii) if all descent data along finite Galois extensions ℓ/k is effective, then θ^{-1} is surjective.

Proof. This follows from Theorem 3.3 and the fact that taking a filtered direct limit preserves injections/surjections of sets. ■

Corollary 3.9 (Hilbert Theorem 90)**.** *For $n \geq 1$ we have*

$$\mathrm{H}^1(G, \mathrm{GL}_n(k^s)) = 0.$$

Proof. Apply the Theorem above to the base extension over k of finite dimensional vector spaces, and use the fact that all twists of a vector space are trivial. ■

Example 3.10. (i) Let k be a perfect field of characteristic not 2 or 3. Consider the base extension of elliptic curves over k and fix an elliptic curve E over k. We denote its extension to $\overline{k}$ by $\overline{E}$. By [Sil13, Corollary 10.2] we have an isomorphism

$$\mathrm{Aut}_{\overline{k}}(\overline{E}) \simeq \begin{cases} \mu_2 & \text{if } j(E) \neq 0, 1728, \\ \mu_4 & \text{if } j(E) = 1728, \\ \mu_6 & \text{if } j(E) = 0, \end{cases}$$

where $\mu_n \subset \overline{k}$ denotes the group of n-th roots of unity. From the Kummer sequence

$$1 \to \mu_n \to \overline{k}^\times \xrightarrow{x \mapsto x^n} \overline{k}^\times \to 1$$

and Corollary 3.9 we obtain an isomorphism

$$\mathrm{H}^1(k, \mu_n) \simeq k^\times / (k^\times)^n.$$

By Example 3.6 and the above Theorem applied with the base extension of elliptic curves over k, we conclude that

$$T(E) \simeq \begin{cases} k^\times/(k^\times)^2 & \text{if } j(E) \neq 0, 1728, \\ k^\times/(k^\times)^4 & \text{if } j(E) = 1728, \\ k^\times/(k^\times)^6 & \text{if } j(E) = 0. \end{cases}$$

(ii) (After [Poo17, Remark 5.5.8]) Consider the base extension of algebraic groups over k from Example 2.3(vi). Let $\mathbb{G}_m^n$ be the multiplicative group over k. A *torus of dimension* n over k is a twist of $\mathbb{G}_m^n$. Denote the extension of $\mathbb{G}_m^n$ to k^s by $(\mathbb{G}_m^n)^s = (\mathbb{G}_m^s)^n$. Its automorphism group over k^s is given by $\mathrm{GL}_n(\mathbb{Z})$. The Galois group $\mathrm{Gal}(k^s/k)$ acts trivially on it. By Theorem 3.8 applied to the base extension of algebraic groups, we obtain

$$\begin{aligned} &\{n\text{-dimensional tori over } k\}/\simeq_k \\ &= T(\mathbb{G}_m^n) \\ &\simeq \mathrm{H}^1(k, \mathrm{GL}_n(\mathbb{Z})) \\ &= \mathrm{Hom}_c(\mathrm{Gal}(k^s/k), \mathrm{GL}_n(\mathbb{Z}))/\text{conjugacy} \\ &\simeq \{\mathrm{Gal}(k^s/k)\text{-modules which are free of rank } n \text{ over } \mathbb{Z}\}/\simeq. \end{aligned}$$

REFERENCES

[Bru09] Eric Brussel. *Galois descent and Severi-Brauer varieties.* 2009. URL: http://www.mathcs.emory.edu/~brussel/Papers/galoisdescent.pdf.

[Jah00] Jörg Jahnel. *The Brauer-Severi variety associated with a central simple algebra: A Survey.* 2000. URL: https://www.math.uni-bielefeld.de/LAG/man/052.pdf.

[Poo17] Bjorn Poonen. *Rational points on varieties.* Vol. 186. Graduate Studies in Mathematics. Providence, Rhode Island: American Mathematical Society, 2017.

[Ser97] Jean-Pierre Serre. *Galois cohomology.* eng. Springer Monographs in Mathematics. Berlin ; New York: Springer, 1997.

[Sil13] Joseph H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate texts in mathematics. Springer, 2013.

[Sta23] The Stacks project authors. *The Stacks project*. `https://stacks.math.columbia.edu`. 2023.

MATHEMATISCHES INSTITUT, HEINRICH-HEINE-UNIVERSITÄT DÜSSELDORF, 40225 DÜSSELDORF, GERMANY

Email address: `hugo.zock@uni-duesseldorf.de`