A 'universal' Torsor for a Finite Group

Nitin Nitsure

Abstract

Let n be a positive integer, let $\mathbf{G}_{m,\mathbb{Z}[1/n]} = \operatorname{Spec} \mathbb{Z}[1/n][t, t^{-1}]$ be the multiplicative group scheme over $\mathbb{Z}[1/n]$, and let $(\,)^n : \mathbf{G}_{m,\mathbb{Z}[1/n]} \to \mathbf{G}_{m,\mathbb{Z}[1/n]}$ be the n th power morphism. The Hilbert theorem 90 implies that this morphism $(\,)^n : \mathbf{G}_{m,\mathbb{Z}[1/n]} \to \mathbf{G}_{m,\mathbb{Z}[1/n]}$ has the following property: Given any field K such that $char(K)$ does not divide n and K contains a primitive n th root of unity, any field extension L/K which is Galois with Galois group cyclic of order n can be obtained as a pull-back of the n th power morphism

$(\,)^n : \mathbf{G}_{m,\mathbb{Z}[1/n]} \to \mathbf{G}_{m,\mathbb{Z}[1/n]}$ via a morphism $u : \operatorname{Spec}(K) \to \mathbf{G}_{m,\mathbb{Z}[1/n]}$.

There is nothing special about the cyclic group; in fact, the following much more general result exists. For each finite group Γ, there exists a certain étale locally trivial Γ-torsor $U_{\Gamma,\mathbb{Z}} \to U_{\Gamma,\mathbb{Z}}/\Gamma$ such that for every field K, every étale locally trivial Γ-torsor over K is obtainable as a pull-back. Note that there is no restriction on the base field K, and moreover the total space of the Γ-torsor on K need not be connected (that is, L need not be a field).

When Γ is abelian, this result is a crucial step in the Lang-Rosenlicht theorem that any abelian extension of the function field of a curve is the pull-back of a covering of a generalized Jacobian of the curve (where the curve is geometrically irreducible, reduced, smooth, projective over a finite field).

What follows is an expository account of the construction and the universal property of the Γ-torsor $U_{\Gamma,\mathbb{Z}} \to U_{\Gamma,\mathbb{Z}}/\Gamma$.

1. Quotient by the free action of a finite group

The reader is assumed to be familiar with the elements of the language of schemes. In particular, we shall use the concepts of valued points, and morphisms which are of finite type, separated, finite, proper, flat, faithfully flat, unramified (separable), and étale. All of the above is nicely explained in Mumford's introductory textbook 'The Red Book of Varieties and Schemes' (an inexpensive Indian edition, published by Narosa, exists).

For a morphism $\pi : X \to S$ of schemes, $Aut_S(X)$ will denote the group of all automorphisms $\varphi : X \to X$ of the scheme X which satisfy $\pi \circ \varphi = \pi$. Let Γ be a finite group. A **right-action** of Γ on X/S is by definition a group homomorphism $\rho : \Gamma^{op} \to Aut_S(X)$ of the opposite group of Γ into $Aut_S(X)$. Unless otherwise indicated, all actions on schemes (respectively, on rings) will be right-actions (respectively, left-actions). A right-action

$\rho : \Gamma^{op} \to Aut(X)$ of Γ on an affine scheme $X = \mathrm{Spec}(A)$ corresponds to a left-action of Γ on the ring A defined as follows. Note that any $f \in A$ can be regarded as a morphism $f : X \to \mathbf{A}^1_{\mathbb{Z}}$ from X to the affine line $\mathbf{A}^1_{\mathbb{Z}}$. We put $\gamma f = f \circ \rho(\gamma) : X \to \mathbf{A}^1_{\mathbb{Z}}$, which can be seen to define a left-action of Γ on A by ring automorphisms.

By definition, if a group Γ acts on a scheme X, and if $x \in X$, then the **decomposition group** at x is the subgroup $D_x \subset \Gamma$ consisting of all γ with $\gamma(x) = x$, that is, D_x is the set-theoretic isotropy at x for the action of γ on the underlying set of the scheme X. Any element $\gamma \in D_x$ induces an automorphism $\gamma^* : \kappa(x) \to \kappa(x)$ of the residue field at x. The **inertia group** at x is the subgroup $I_x \subset D_x$ consisting of all γ such that the automorphism $\gamma^* : \kappa(x) \to \kappa(x)$ is identity. We say that Γ **acts freely** on X if for each $x \in X$ the inertia group I_x is trivial. Equivalently, Γ acts freely on X if for every field K, the action of Γ on the set $X(K)$ of K-valued points of X is free (in the usual set-theoretic sense).

Let there be given a scheme X over a base S, and let a finite group Γ act (on the right) on X over S. Let $X \times \Gamma = \coprod_\Gamma X$ be the disjoint union of copies X_γ of X, indexed by $\gamma \in \Gamma$. We define a morphism

$$\alpha : X \times \Gamma \to X \times_S X$$

as follows. If $x : T \to X_\gamma$ is a T-valued point of X_γ, we define $\alpha(x)$ to be the T-valued point $(x, x\gamma)$ of $X \times_S X$. This uniquely determines α.

We say that a given action makes $X \to S$ an **étale locally trivial Γ-torsor over the base** S (or a **Γ-torsor over S in the étale topology**) if $X \to S$ is finite, étale, surjective, and moreover the above morphism $\alpha : X \times \Gamma \to X \times_S X$ is an isomorphism.

Note that if $X \to S$ is an étale locally trivial Γ-torsor, then for any morphism $T \to S$ of schemes, the base change $X \times_S T \to T$ has a natural structure of an étale locally trivial Γ-torsor (called as the **pull back** of $X \to S$ under $T \to S$).

We say that the Γ-torsor $X \to S$ is **trivial** if there exists a Γ-equivariant isomorphism $X \to S \times \Gamma$ over the base S, where the action of Γ on $S \times \Gamma$ is by right translation (an element γ maps S_δ identically to $S_{\delta\gamma}$).

The following exercise connects the notion of a torsor with basic field theory.

Exercise. Let L/K be a field extension, and Γ a finite group acting on $\mathrm{Spec}(L)$ over $\mathrm{Spec}(K)$. Show that under this action $\mathrm{Spec}(L)$ is an étale Γ-torsor over $\mathrm{Spec}(K)$ if and only if L/K is a finite Galois extension, with Galois group $Gal(L/K)$ isomorphic to Γ via the given action.

Theorem 1. *Let k be a noetherian ring, let A be a finite type k-algebra, and let Γ be a finite group of k-automorphisms of A such that Γ acts freely*

on the scheme $\mathrm{Spec}(A)$. *Let* $A^\Gamma \subset A$ *be the invariant subring. Then the induced morphism* $\pi : \mathrm{Spec}(A) \to \mathrm{Spec}(A^\Gamma)$ *of schemes is finite étale, and together with the* Γ*-action,* π *is a* Γ*-torsor in the étale topology.*

Proof. Step 1 : A is finite over A^Γ, and A^Γ is of finite type over k. Let $a_1, \ldots, a_n$ be algebra generators for A over k. Then for each i, the element a_i satisfies the monic polynomial

$$f_i(t) = \prod_{\gamma \in \Gamma} (t - \gamma(a_i)) \in A^\Gamma[t]$$

Let $C \subset A$ be the k-subalgebra generated by the coefficients of all the f_i. Then C is of finite type over k, so C is noetherian as k is noetherian. As A is finite type and integral over C, it follows that A is finite over C. Note that $C \subset A^\Gamma \subset A$, so A^Γ is finite over C as C is noetherian. In particular, A^Γ is finite type over k. As A is finite over C, it follows that A is finite over A^Γ. We have thus proved that $\pi : \mathrm{Spec}(A) \to \mathrm{Spec}(A^\Gamma)$ is a finite morphism of affine schemes of finite type over k.

Step 2 : Flat base change and invariants. Let B be a flat A^Γ-algebra. Consider the action of Γ on $A \otimes_{A^\Gamma} B$ given by $\gamma(a \otimes b) = \gamma(a) \otimes b$. Consider the left-exact sequence of A^Γ-modules

$$0 \to A^\Gamma \to A \to \oplus_{\gamma \in \Gamma} A$$

where the last map sends a to the n-tuple $(a - \gamma_1(a), \ldots, a - \gamma_n(a))$. As B is A^Γ-flat, tensoring gives the left-exact sequence

$$0 \to B \to A \otimes_{A^\Gamma} B \to \oplus_{\gamma \in \Gamma} A \otimes_{A^\Gamma} B$$

which shows the equality $B = (A \otimes_{A^\Gamma} B)^\Gamma$.

Step 3 : Base change preserves freeness of action. Let Γ act on X/S, and let $f : S' \to S$ be any morphism. Let $X' = X \times_S S'$, and let $f' : X' \to X$ be the projection. Consider the induced action of Γ on X'/S'. For any $x' \in X'$, let $x = f'(x')$. Then it is clear that the decomposition group $D_{x'}$ is contained in D_x. Next, let $\gamma \in D_{x'}$. Note that $f' : X' \to X$ induces an inclusion $\kappa(x) \hookrightarrow \kappa(x')$, and the homomorphism $\gamma : \kappa(x') \to \kappa(x')$ restricts under this inclusion to the homomorphism $\gamma : \kappa(x) \to \kappa(x)$. Hence we get an inclusion of inertia groups $I_{x'} \subset I_x$. It follows that if the action of Γ on X is free, then the action of Γ on X' is also free.

Step 4 : Reduction to the case where A^Γ is local. For any prime $\mathbf{p} \subset A^\Gamma$, the local ring $(A^\Gamma)_{\mathbf{p}}$ is flat over A^Γ. We denote $A \otimes_{A^\Gamma} (A^\Gamma)_{\mathbf{p}}$ simply by $A_{\mathbf{p}}$ as usual (this will be a semi-local ring, as it is finite over the local

ring $(A^\Gamma)_{\mathbf{p}}$). To prove A is étale over A^Γ, we just have to prove that $A_{\mathbf{p}}$ is étale over $(A^\Gamma)_{\mathbf{p}}$ for every prime $\mathbf{p} \subset A^\Gamma$. By step 2, $(A^\Gamma)_{\mathbf{p}} = (A_{\mathbf{p}})^\Gamma$. By step 3, freeness of action holds for Γ acting on $A_{\mathbf{p}}$. Hence we are reduced to the case where A^Γ is local.

Step 5 : Reduction to the case where A^Γ is strictly henselian. Now, let B be a strict henselization of the local ring A^Γ. Note that as B is faithfully flat over A^Γ, A is étale over A^Γ if $A \otimes_{A^\Gamma} B$ is étale over B. By steps 2 and 3, we are then reduced to the case where A^Γ is strictly henselian.

Step 6 : Proof when A^Γ is strictly henselian. As already proved, A is finite over A^Γ. Hence by henselian property of A^Γ, the A^Γ-algebra A is a direct product of A^Γ-algebras $A_1 \times \ldots \times A_r$, where each A_i is a henselian local ring, finite over A^Γ. Let $\mathbf{m}_i$ denote the maximal ideal of A_i. Then

$$\mathbf{n}_i = A_1 \times \ldots A_{i-1} \times \mathbf{m}_i \times A_{i+1} \times \ldots \times A_r$$

are all the maximal ideals of A, and for each $\gamma \in \Gamma$ and each $\mathbf{n}_i$, we have $\gamma(\mathbf{n}_i) = \mathbf{n}_j$ for some j. Suppose $\gamma(\mathbf{n}_i) = \mathbf{n}_i$, in other words, γ lies in the decomposition group $D_{\mathbf{n}_i}$. Then γ induces an automorphism of the residue field $A_i/\mathbf{n}_i$ over the base $A^\Gamma/\mathbf{m}$, where $\mathbf{m}$ is the maximal ideal of A^Γ. By assumption of strict henselianness, $A^\Gamma/\mathbf{m}$ is separably closed, so the finite extension $A_i/\mathbf{n}_i$ is purely inseparable, so $\gamma \in D_{\mathbf{n}_i}$ induces identity on $A_i/\mathbf{n}_i$, hence $D_{\mathbf{n}_i}$ is the same as the inertia group $I_{\mathbf{n}_i}$. By assumption of free action, it follows that each $D_{\mathbf{n}_i}$ is trivial.

As $\mathrm{Spec}(A_i)$ are the connected components of $\mathrm{Spec}(A)$, any automorphism γ maps each A_i isomorphically onto some A_j, with $\gamma(\mathbf{n}_i) = \mathbf{n}_j$. We claim that Γ acts transitively on the set of all $\mathbf{n}_i$. Otherwise, consider the element $a = (a_1, \ldots, a_r) \in A$ where $a_i = 1 \in A_i$ if $\mathbf{n}_i$ is in the orbit of $\mathbf{n}_1$, and $a_i = 0$ otherwise. Then clearly $a \in A^\Gamma$. Now suppose $\mathbf{n}_i$ is not in the orbit of $\mathbf{n}_1$. The map $A^\Gamma/\mathbf{m} \to A_i/\mathbf{n}_i$ sends $a \mapsto 0$, so $a \in \mathbf{m}$. But then under $A^\Gamma/\mathbf{m} \to A_1/\mathbf{n}_1$ we would have $a \mapsto 0$, which is a contradiction as $a_1 = 1$. This proves transitivity.

Each $D_{\mathbf{n}_i}$ is trivial, hence for each i, j there exists a unique $\gamma \in \Gamma$ with $\gamma(\mathbf{n}_i) = \mathbf{n}_j$. In particular, for each i there is a unique γ_i with $\gamma_i(\mathbf{n}_1) = \mathbf{n}_i$. This gives an isomorphism $\varphi_i : A_1 \to A_i$. If we write $A_1 = R$ say, then it follows that A is the product $R \times \ldots \times R$ of r copies of R, and Γ acts by permuting factors in a transitive way. The invariant subring A^Γ is therefore the diagonal embedding of R into $R \times \ldots \times R$. Hence A is étale over A^Γ.

Note The hypothesis that Γ acts freely on $\mathrm{Spec}(A)$ was very important in the above. Without this hypothesis, $\pi : \mathrm{Spec}(A) \to \mathrm{Spec}(A^\Gamma)$ **may not even be flat**. For example, with base $k = \mathbb{C}$, take the action of $\Gamma = \mathbb{Z}/(2)$ on the polynomial ring $\mathbb{C}[x, y]$ sending $x \mapsto$

$-x$ and $y \mapsto -y$. Then the module $\mathbb{C}[x,y]$ is not flat over the ring $\mathbb{C}[x,y]^\Gamma = \mathbb{C}[x^2, xy, y^2]$, as its generic rank is 2, but the fiber over the point $\mathbf{m} = (x^2, xy, y^2)$ has rank 3.

Remark 2. If $\pi : Y \to X$ is a Γ-torsor in the étale topology for a finite group Γ, then in general Γ is only a subgroup of the deck transformation group $Aut_X(Y)$ of the finite étale covering $Y \to X$. For example, if X is connected, and Y is the trivial torsor $X \times \Gamma$, then the deck transformation group $Aut_X(Y)$ is the permutation group S_n, where n is the order of Γ. However, if Y is connected, then we have $\Gamma = Aut_X(Y)$, as in that case any deck transformation is determined by its effect on a single closed point.

2. The structure of Γ-torsors over a field K

Summary The first part of this section is just an exercise in so called 'Galois descent' (see for example chapter 2 of Milne's book 'Étale Cohomology' for the basics of Galois descent and its relation with Galois cohomology). Let E/K be a finite Galois field extension, let Γ be a finite group, let $\varphi : Gal(E/K) \to \Gamma$ be a group homomorphism, and let A/K be the Γ-torsor obtained by 'extension of structure group' from the $Gal(E/K)$-torsor E/K via φ. Every étale Γ-torsor over a field K arises this way, where moreover we can choose E so that φ is injective. When φ is chosen to be injective, A is isomorphic to the direct product E^r as a K-algebra, where r is the index of $image(\varphi)$ in Γ, and we explicitly write the Γ-action on $A = E^r$ which makes it a Γ-torsor.

The final result of this section (Theorem 6 below) gives the existence of an element $c \in A$ such that the determinant $\det(\gamma_i \gamma_j^{-1}(c))$ is a unit in A.

Let Γ be a finite group, K be a field, E/K a finite Galois extension field, and $\varphi : Gal(E/K) \to \Gamma$ a homomorphism of groups. The set $Maps(\Gamma, E)$ of all set maps $c : \Gamma \to E$ becomes a commutative E-algebra under pointwise operations. We denote $c(\gamma)$ by c_γ. Let $Maps_\varphi(\Gamma, E) \subset Maps(\Gamma, E)$ be the subring of φ-equivariant maps, that is, those c which satisfy

$$g(c_\gamma) = c_{\varphi(g)\gamma} \quad \text{for all } g \in Gal(E/K),\ \gamma \in \Gamma$$

The ring $Maps_\varphi(\Gamma, E)$ is a K-algebra under pointwise operations. We define a left-action of Γ on $Maps(\Gamma, E)$ by

$$(\alpha c)_\beta = c_{\alpha\beta} \quad \text{for all } \alpha, \beta \in \Gamma$$

This makes $Maps(\Gamma, E)$ a trivial Γ-torsor over E.

Note that the K-subalgebra $Maps_\varphi(\Gamma, E) \subset Maps(\Gamma, E)$ is invariant under the left-action of Γ.

We have the following structure theorem for Γ-torsors on K.

Lemma 3. *If Γ is a finite group, K is a field, E/K a finite Galois field extension, and $\varphi : Gal(E/K) \to \Gamma$ a group homomorphism, then the K-algebra $Maps_\varphi(\Gamma, E)$ with the left-action of Γ as defined above is an étale*

locally trivial Γ-torsor over K. Its pull-back to E is the trivial Γ-torsor $Maps(\Gamma, E)$ over E.

Conversely, if L is a K-algebra together with a left Γ-action which makes it an étale locally trivial Γ-torsor over K, and if E/K is a finite Galois field extension such that it pulls back to a trivial Γ-torsor over E, then there exists a group homomorphism $\varphi : Gal(E/K) \to \Gamma$ such that the given Γ-torsor is isomorphic to the Γ-torsor $Maps_\varphi(\Gamma, E)$ over K constructed above.

Proof. It is clear from its construction that $Maps_\varphi(\Gamma, E)$ indeed has the desired properties. Conversely, if a Γ-torsor over K pulls back to a trivial Γ-torsor on E where E/K is a finite Galois field extension, then it corresponds to a 1-cocycle φ in $H^1(Gal(E/K), \Gamma)$.
As Γ is a constant group, we have $H^1(Gal(E/K), \Gamma) = Hom(Gal(E/K), \Gamma)$, so we regard φ as a group homomorphism $Gal(E/K) \to \Gamma$. Now by 'descending' the trivial Γ-torsor $Maps(\Gamma, E)$ over E by the cocycle φ, we get the torsor $Maps_\varphi(\Gamma, E)$ over K constructed above.

Remark 4. With the above notation, if $N = ker(\varphi) \subset Gal(E/K)$, then we can replace E with the invariant subfield E^N, and $\varphi : Gal(E/K) \to \Gamma$ by the induced homomorphism $Gal(E/K)/N \to \Gamma$ which is injective. Hence we can always assume that $\varphi : Gal(E/K) \to \Gamma$ is injective.

We now more directly describe the structure of the Γ-torsor $Maps_\varphi(\Gamma, E)$ over K, where by the above remark, we can assume that $\varphi : Gal(E/K) \to \Gamma$ is injective without any loss of generality. Let $image(\varphi) = D \subset \Gamma$. Let $D\sigma_1, \ldots, D\sigma_r$ be the distinct right cosets of D in Γ, where $r = (\Gamma : D)$ is the index of D in Γ. Consider the r-fold direct product E^r, which is a ring under componentwise operations, and is an E-algebra (hence also a K-algebra) via the diagonal map $\Delta : E \to E^r$. For $1 \leq k \leq r$, let $p_k : E^r \to E$ be the projections, which are E-algebra homomorphisms, and let $f_k : E \to E^r$ be the inclusions (with $p_k f_k = \mathrm{id}_E$ and $p_i f_j = 0$ for $i \neq j$) which are merely E-linear maps of vector spaces. We define an E-algebra homomorphism $Maps_\varphi(\Gamma, E) \to E^r$ by sending $c \mapsto x$ where $p_k(x) = c_{\sigma_k}$, which is an isomorphism, with inverse $E^r \to Maps_\varphi(\Gamma, E)$ defined by sending $x \mapsto c$ where $c_{g\sigma_k} = g(c_{\sigma_k}) = g(p_k(x))$ where $g \in D$. These homomorphisms are inverses of each other, so define an isomorphism $Maps_\varphi(\Gamma, E) \to E^r$. Via this isomorphism, the left-action of Γ on $Maps_\varphi(\Gamma, E)$ gives the following left-action of Γ on E^r. Any element $x \in E^r$ is the sum of elements of the form $f_k(a) \in E^r$, where $a \in E$. Given any $\gamma \in \Gamma$, there exists a unique i with $1 \leq i \leq r$ and a unique $g \in D$ such that

$$\gamma = \sigma_i^{-1} g \sigma_k$$

Then we define $\gamma f_k(a) \in E^r$ by putting

$$p_j \sigma_i^{-1} g \sigma_k f_k(a) = \begin{cases} g(a) & \text{if } j = i \\ 0 & \text{otherwise.} \end{cases}$$

Trace map on Γ-torsors

For any finite K-algebra A we define the trace map

$$Trace_{A/K} : A \to K$$

as follows. For $x \in A$, consider the K linear map $A \to A$ which sends $y \mapsto xy$. Then $Trace_{A/K}(x)$ is the trace of this linear map. If E/K is a finite Galois field extension, then it is known (elementary fact) that for all $x \in E$,

$$Trace_{E/K}(x) = \sum_{g \in Gal(E/K)} g(x)$$

We now calculate trace for the Γ-torsor E^r above. For $f_k(a) \in E^r$ we have

$$\begin{aligned} p_j \left(\sum_{\gamma \in \Gamma} \gamma f_k(a) \right) &= \sum_{\gamma \in \Gamma} p_j \gamma f_k(a) \\ &= \sum_{1 \le i \le r} \sum_{g \in D} p_j \sigma_i^{-1} g \sigma_k f_k(a) \\ &= \sum_{g \in D} g(a) \\ &= Trace_{E/K}(a) \end{aligned}$$

As the above holds for all j, we get

$$\sum_{\gamma \in \Gamma} \gamma f_k(a) = \Delta(Trace_{E/K}(a))$$

For any $x \in E^r$, we have $x = \sum_k f_k p_k(x)$, hence summing the above gives the equality

$$\sum_{\gamma \in \Gamma} \gamma x = \sum_{1 \le k \le r} \Delta(Trace_{E/K}(p_k(x))) = \Delta(Trace_{E^r/K}(x))$$

Hence we have proved the following.

Proposition 5. *Let Γ be a finite group, let K be a field, and let A be an étale Γ-torsor over K. Then we have equality of K-linear maps*

$$\sum_{\gamma\in\Gamma}\gamma \;=\; Trace_{A/K} : A \to K$$

Next, suppose that A is a finite separable K-algebra. We define a symmetric K-bilinear map

$$T_{A/K} : A \times A \to K : (x, y) \mapsto Trace_{A/K}(xy)$$

If $A = L$ is a field, then by linear independence of characters, the map $Trace_{L/K} : L \to K$ is non-zero, so it follows that $T_{L/K} : L \times L \to K$ is non-degenerate. In general, $A = L_1 \times \ldots L_r$ is a direct product of such field extensions, and $(A, T_{A/K})$ is the orthogonal direct sum of the $(L_i, T_{L_i/K})$, so again $T_{A/K} : A \times A \to K$ is non degenerate.

Normal basis theorem for Γ-torsors

By the normal basis theorem for finite Galois field extensions E/K, there exists an element $a \in E$ such that $g_1(a), \ldots, g_m(a)$ is a K-linear basis for E, where $\{g_1, \ldots, g_m\} = Gal(E/K)$. Now with the previous notation, consider the Γ-torsor E^r over K. It is clear from the description of the Γ-action on E^r that the element $c = f_1(a)$ of E^r has the property that the elements $\gamma(c)$, for $\gamma \in \Gamma$, form a K-linear basis of E^r.

Existence of $c \in A$ such that $\det(\gamma_i\gamma_j^{-1}(c))$ is a unit

We are at last ready to prove the main result that we want.

Theorem 6. *Let $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ be a finite group, let K be a field, and let A be an étale Γ-torsor over K. For any $c \in A$, consider the $n \times n$ matrix $(\gamma_i\gamma_j^{-1}(c))$ over A. There exists an element $c \in A$ such that this matrix is invertible, that is,*

$$\det(\gamma_i\gamma_j^{-1}(c)) \quad \textit{is a unit in } A.$$

Proof. Let $e_1, \ldots, e_n$ be any K-linear basis for A. Consider the $n \times n$ matrix $M = (\gamma_i(e_j))$ over A. As proved above, the trace map is given by $\sum_\Gamma \gamma$. Hence we have

$$({}^tMM)_{j,k} = \sum_i \gamma_i(e_j)\gamma_i(e_k) = \sum_i \gamma_i(e_je_k) = Trace_{A/K}(e_je_k)$$

Hence ${}^tMM$ is the matrix of the bilinear form $T_{A/K} : A \times A \to K$. As this K-bilinear form is non-degenerate, $\det({}^tMM)$ is a unit in K, hence a unit in A. Hence $\det(M)$ is also a unit in A, as $(\det(M))^2 = \det({}^tMM)$.

As shown earlier (the normal basis theorem for Γ-torsors), there exists an element $c \in A$ such that $e_j = \gamma_j^{-1}(c)$ is a K-linear basis for A. For this basis, $M = (\gamma_i\gamma_j^{-1}(c))$, and so the element $\det(\gamma_i\gamma_j^{-1}(c))$ is a unit in A.

Units in a group ring

Now that adequate preparation – in particular, a careful formulation using the concept of a torsor – has been made, the rest of these notes essentially follow Serre's 1959 book 'Groupes algébriques et corps de classes'. It seems that the concept of an étale locally trivial torsor was not available then – it was formalized (by Serre himself) somewhat later.

Let Γ be a finite group. For any commutative ring k, let $k[\Gamma]$ denote the group ring of Γ with coefficients k. We define a functor

$$U_\Gamma : \mathit{Rings} \longrightarrow \mathit{Groups} : k \mapsto U_\Gamma(k) = \text{Units in } k[\Gamma]$$

Lemma 7. *The above functor U_Γ is represented by an affine group scheme $U_{\Gamma,\mathbb{Z}}$ of finite type over $\mathbb{Z}$. The underlying scheme of the group scheme $U_{\Gamma,\mathbb{Z}}$ can be embedded as an open subscheme of the affine n-space $\mathbf{A}^n_{\mathbb{Z}}$, where n is the order of Γ. In particular, $U_{\Gamma,\mathbb{Z}}$ is irreducible and smooth over* $\mathrm{Spec}(\mathbb{Z})$ *of relative dimension n. The constant group scheme $\Gamma_{\mathbb{Z}}$ is a closed subgroup scheme of $U_{\Gamma,\mathbb{Z}}$.*

Proof. Let $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$. It can be seen that an element $x = \sum x_{\gamma_i}\gamma_i \in k[\Gamma]$ is invertible if and only if the $n \times n$-matrix $M(x)$ over k with entries

$$M(x)_{i,j} = x_{\gamma_i\gamma_j^{-1}}$$

is invertible (lies in $GL_n(k)$). From this it follows that the scheme $U_{\Gamma,\mathbb{Z}}$ can be constructed as the open subscheme of the affine space $\mathbf{A}^n_{\mathbb{Z}}$, which is the inverse image of $GL_{n,\mathbb{Z}}$ under the morphism $M : \mathbf{A}^n_{\mathbb{Z}} \to \mathbf{A}^{n\times n}_{\mathbb{Z}}$ which maps the k-valued point x to the k-valued point $M(x)$. As the morphism M is affine, and as $GL_{n,\mathbb{Z}}$ is affine open in $\mathbf{A}^{n\times n}_{\mathbb{Z}}$, its inverse image $U_{\Gamma,\mathbb{Z}}$ is affine open in $\mathbf{A}^n_{\mathbb{Z}}$.

The group Γ acts on the scheme $U_{\Gamma,\mathbb{Z}}$ by right translation, and let

$$\pi : U_{\Gamma,\mathbb{Z}} \to U_{\Gamma,\mathbb{Z}}/\Gamma$$

be the quotient. The theorem 1 and Remark 2, together with the following lemma 8, imply that the morphism $\pi : U_{\Gamma,\mathbb{Z}} \to U_{\Gamma,\mathbb{Z}}/\Gamma$ is a Γ-torsor in

the étale topology (in particular π is finite étale), with deck transformation group Γ.

Lemma 8. *The right translation action of* Γ *on* $U_{\Gamma,\mathbb{Z}}$ *is free.*

Proof. Let K be a field, and consider a K-valued point $x \in U_{\Gamma,\mathbb{Z}}(K)$. This corresponds to an invertible element $x \in K[\Gamma]$. Hence for any $\gamma \neq 1$, we have $x\gamma \neq x$, so Γ acts freely on the set $U_{\Gamma,\mathbb{Z}}(K)$.

'Universal' property of $U_{\Gamma,\mathbb{Z}} \to U_{\Gamma,\mathbb{Z}}/\Gamma$

The reason for our interest in the étale Γ-torsor $U_{\Gamma,\mathbb{Z}} \to U_{\Gamma,\mathbb{Z}}/\Gamma$ is that it has the following property. I have put 'universal' in quotes, because there is no uniqueness for the morphism $u : \mathrm{Spec}(K) \to U_{\Gamma,\mathbb{Z}}/\Gamma$.

Theorem 9. *Let* K *be any field and let* L *be a* Γ*-torsor over* K *in the étale topology. Then there exists a morphism of schemes* $u : \mathrm{Spec}(K) \to U_{\Gamma,\mathbb{Z}}/\Gamma$ *and a* Γ*-equivariant morphism of schemes* $v : \mathrm{Spec}(L) \to U_{\Gamma,\mathbb{Z}}$ *such that the following diagram is cartesian.*

$$\begin{array}{ccc} \mathrm{Spec}(L) & \xrightarrow{v} & U_{\Gamma,\mathbb{Z}} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \xrightarrow{u} & U_{\Gamma,\mathbb{Z}}/\Gamma \end{array}$$

In other words, for any field K*, every étale* Γ*-torsor over* $\mathrm{Spec}(K)$ *is a pull-back of* $U_{\Gamma,\mathbb{Z}} \to U_{\Gamma,\mathbb{Z}}/\Gamma$.

Proof. Let $x_{\gamma_1}, \ldots, x_{\gamma_n}$ be indeterminates, and let $\mathbf{A}^n_{\mathbb{Z}}$ be the affine space $\mathrm{Spec}\ \mathbb{Z}[x_{\gamma_1}, \ldots, x_{\gamma_n}]$. By definition, $U_{\Gamma,\mathbb{Z}} \subset \mathbf{A}^n_{\mathbb{Z}}$ is the open subscheme which is the complement of the divisor D defined by $\det(x_{\gamma_i\gamma_j^{-1}}) = 0$, in other words, the coordinate ring of $U_{\Gamma,\mathbb{Z}}$ is

$$A = \mathbb{Z}[x_{\gamma_1}, \ldots, x_{\gamma_n}, 1/\det(x_{\gamma_i\gamma_j^{-1}})]$$

The action of the group Γ by right-translation on $U_{\Gamma,\mathbb{Z}}$ corresponds to its left-action on the polynomial ring $\mathbb{Z}[x_{\gamma_1}, \ldots, x_{\gamma_n}]$ by permuting variables, defined by

$$\alpha(x_\beta) = x_{\beta\alpha^{-1}}$$

where $\alpha, \beta \in \Gamma$. For any ring L, an L-valued point of $U_{\Gamma,\mathbb{Z}}$ is given by a ring homomorphism

$$v : \mathbb{Z}[x_{\gamma_1}, \ldots, x_{\gamma_n}, 1/\det(x_{\gamma_i\gamma_j^{-1}})] \to L$$

Let $x_\gamma \mapsto v_\gamma$ under the above homomorphism. Then note that we can choose the n elements $v_{\gamma_i} \in L$ arbitrarily, subject to the only requirement that

$$\det(v_{\gamma_i\gamma_j^{-1}}) \text{ is a unit in the ring } L.$$

If we are also given a left-action of Γ on L then the homomorphism v is Γ-equivariant if and only if the following is satisfied for all $\alpha, \beta \in \Gamma$

$$v(\alpha(x_\beta)) = \alpha(v(x_\beta))$$

Substituting $\alpha(x_\beta) = x_{\beta\alpha^{-1}}$ from above, we get $v_{\beta\alpha^{-1}} = \alpha(v_\beta)$. In particular,

$$v_\gamma = \gamma^{-1}(v_e)$$

where $e \in \Gamma$ is the identity. Hence an equivariant homomorphism $v : \mathbb{Z}[x_{\gamma_1}, \ldots, x_{\gamma_n}, 1/\det(x_{\gamma_i\gamma_j^{-1}})] \to L$ is determined by an arbitrary element $c = v_e \in L$, provided the element c satisfies the only condition that

$$\det(\gamma_j\gamma_i^{-1}(c)) \text{ is a unit in the ring } L.$$

Now assume that there exists such an element c, and let $v : H^0(U_{\Gamma,\mathbb{Z}}, \mathcal{O}_{U_{\Gamma,\mathbb{Z}}}) \to L$ be defined by $x_\gamma \mapsto \gamma^{-1}(c)$. As this ring homomorphism is Γ-equivariant, it induces a ring homomorphism

$$H^0(U_{\Gamma,\mathbb{Z}}/\Gamma, \mathcal{O}_{U_{\Gamma,\mathbb{Z}}/\Gamma}) = (H^0(U_{\Gamma,\mathbb{Z}}, \mathcal{O}_{U_{\Gamma,\mathbb{Z}}}))^\Gamma \to L^\Gamma = K$$

of the invariant subrings. Hence we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Spec}(L) & \xrightarrow{v} & U_{\Gamma,\mathbb{Z}} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \xrightarrow{u} & U_{\Gamma,\mathbb{Z}}/\Gamma \end{array}$$

As both columns are Γ-torsors and the top map is Γ-equivariant, the above rectangle is cartesian.

If L is a field, then by normal basis theorem there exists such an element c. When L is a more general étale Γ torsor over the field K, the existence of such a c is given by the theorem 6. This completes the proof of the theorem 9.

REFERENCES

1. Milne : *Étale Cohomology*, Princeton Univ Press, 1980.
2. Mumford : *The Red Book of Varieties and Schemes*, Springer-Narosa, 1995.
3. Serre : *Groupes algébriques et corps de classes*, Hermann, 1959.

Nitin Nitsure
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road, Mumbai 400 005, India.
e-mail: nitsure@math.tifr.res.in