Title

Contents

1 Wednesday April 22nd **2**

1 Wednesday April 22nd

Remarks:

1. In the category of G-sets, we have $\mathrm{Aut}_{G\text{-set}}(G) = G$ where G acts on itself by translation.
2. For k a field, G/k a smooth algebraic group, X/k a variety, $\mu : G \times X \to X$ is a torsor iff the map

$$\begin{aligned} \varphi : G \times X &\to X \times X \\ (g, x) &\mapsto (\mu(g, x), x) \end{aligned}$$

is an isomorphism. Letting $G_X := G \times X, X_X := X \times X$ be the base changes, this asks for a commuting diagram

$$\begin{tikzcd} G_X \times_X G_X \arrow[r, "\mu_{G_X}"] & G_X \arrow[d, "1\times\varphi"] \\ G_X \times_X X_X \arrow[r, "\mu_{X_X}"] & X_X \end{tikzcd}$$

thus the base change to X is the trivial G-torsor on X.

Suppose G is commutative and recall we have a Weil-Chevalley group $WC(k, G)$. Question: What is the difference between a twisted form X/k of G/k and a torsor under fG/k?

Better question: Suppose $(X, \mu) \in WC(k, G)$. How many other elements of $WC(k, G) \ni (X', \mu)$ have $X' \cong_k X$?

Recall that $\cdot [(X, \mu)] = (X, \mu([-1] \circ \cdot, \cdot))$. Letting $G = E$ an elliptic curve, we can consider the subtraction map

$$\begin{aligned} v : X \times X &\to E \\ (p, g) &\mapsto g \end{aligned}$$

with $p = g + q$ iff

$$\begin{tikzcd} \underline{\mathrm{Pic}}^1 X \times \underline{\mathrm{Pic}}^1 X \arrow[rr, "v"] \arrow[dr, "v"'] & & E \\ & \underline{\mathrm{Pic}}^0 X \arrow[ur, dotted] & \end{tikzcd}$$

For X/k a nice genus one curve, E/k an elliptic curve, $\mu : E \times X \to X$ is a torsor iff the map $\underline{\mathrm{Pic}}^0 X \to E$ is an isomorphism. Therefore two elements $X_1, X_2 \in WC(k, E)$ are isomorphic iff X_1, X_2 lie in the same $\mathrm{Aut}(E)$-orbit of $WC(k, E)$.

Remarks: Thus the torsors over E aren't much more interesting than E itself. E.g. characteristic zero, $j \neq 0, 1728$, you just mod out by ± 1. There is a version of this for abelian varieties.

- $WC(k,E) = (0) \iff$ every genus 1 curve with Jacobian E has a k-rational point.
- $\forall E/k WC(k,E) = (0) \iff$ every genus 1 C/k has $C(k) \neq \emptyset$.

Example For $k = \bar{k}$, all nonempty V/k have $V(k) \neq \emptyset$.

Example Say a k is *pseudo algebraically closed* iff every geometrically integral V/k has a k-rational point, i.e. $V(k) \neq \emptyset$. E.g., if k is *separably closed* it is pseudo algebraically closed.

Example For $k = \mathbb{F}_q$ a finite field, if X/k is nice of genus g, then

$$|\#X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

Thus for $g = 1$, for elliptic curves, we get

$$q + 1 - 2\sqrt{q} \leq \#X(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

and since $q > 2$, the number of points is strictly positive.

Example (Non-Example) Take $C : y^2 = P_4(x) \in k[x]$ for P_4 a separable degree 4 polynomial. Look at $C \xrightarrow{x} \mathbb{P}^1$, and define the *index* $I(C)$ of a genus 1 curve C/k to be the least positive degree of a k-rational divisor on C, equivalently the gcd of degrees of closed points on C.

Exercise If C is a genus 1 curve, then C is given by $y^2 = P_4(x)$ iff C has a k-rational divisor of degree 2 iff $I(C) \in \{1, 2\}$.

Exercise If $C : y^2 = ax^4 + bx^3 + cx^2 + dx + e$, then $C(k)$ is ? iff there exists $x, y \in k$ such that $y^2 = P_4(x)$ or $a \in k^\times$ is a square.

Example Take $k = \mathbb{R}$ and $C : y^2 = -\left(x^4 + 1\right)$. The leading term is negative, and not a square, and the point at ∞ doesn't need to be check (this would yield exactly 2 real points, thus not a 1-dimensional real manifold). Thus C is a nontrivial element of $WC(\mathbb{P}, \underline{\mathrm{Pic}}^0 C)$.

Exercise Let p be a prime number and find $P_4(x) \in \mathbb{Q}_p[x]$ such that $y^2 = P_4(x)$ has no $\mathbb{Q}_p$-points.

Try not choosing $p = 2$, and try polynomials in $\mathbb{Z}[x]$ and apply Hensel's lemma.

Exercise If $C : F(x, y, z) = 0$ is a nice plane cubic curve over k

a. Show that C/k admits such a defining equation iff it has a rational divisor of degree 3 iff $I(c) \in \{1, 3\}$.

b. Take $k = \mathbb{Q}_p$ and find C/k with no k-rational points.

For G/k a smooth (commutative, but not necessary) group, X/k a G-torso, choose $p \in k^{\mathrm{sep}}$. Then defining $g \coloneqq \mathrm{Aut}(k^{\mathrm{sep}}/k)$, then $X(k^{\mathrm{sep}})$ has two actions: a galois action $g \curvearrowright$ the left, and a $G(k^{\mathrm{sep}})$ action on the right. For all $\sigma \in g$, there exists a unique $a_\sigma \in G(k^{\mathrm{sep}})$ such that $\sigma p = p a_\sigma$.

This defines a map $a_\bullet : g \to G(k^{\mathrm{sep}})$ – however, this is not a group morphism, it is a "twisted" version. For $\sigma, \tau \in g$, by definition we have $p_{a_{\sigma\tau}} = \sigma\tau p = \sigma(\tau p) = \sigma(P a_\tau) = \cdots$ and we can conclude

$$a_{\sigma\tau} = a_\sigma^\sigma a_\tau,$$

which is in fact a 1-cocycle.