Torsors and Galois cohomology

Kolchin Seminar in Differential Algebra

Graduate Center Series

May 05, 2006

Acknowledgement. We are grateful to Arne Ledet for letting us use his notes on torsors in the preparation of this talk.

Easy type of torsors

Let G be a group, X a set. X is called a G-set if G acts on X, that is, if there is a map

$$\begin{array}{ccc} G \times X & \to & X \\ (\sigma, x) & \mapsto & \sigma x \end{array}$$

such that $1x = x$ and $(\sigma\tau)x = \sigma(\tau x)$.

Note that for every fixed σ we have a bijection on X, thus we have a map from G to the group of bijective transformations of X.

The group G is itself a G-set.

Example

Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function and $D^{-1}(f) = \{\text{antiderivatives of } f\}$. Then $G = \mathbb{R}^+$ acts on $D^{-1}(f)$ in an obvious way.

Let X and Y be G-sets. We say that a map $f : X \to Y$ is a G-map if it respects the group action:

$$f(\sigma x) = \sigma f(x), \qquad \sigma \in G.$$

A *G-torsor* is a G-set that is isomorphic to G (as a set).

The following are equivalent:

(i) X is a G-torsor.

(ii) For all $x, y \in X$ there is a unique $\sigma \in G$ such that $\sigma x = y$.

(iii) For all $x \in X$, $\sigma \mapsto \sigma x$ gives an isomorphism $G \cong X$.

(iv) The map $G \times X \to X \times X$ given by $(\sigma, x) \mapsto (\sigma x, x)$ is a bijection.

The torsors we are interested in

Let K be a field. A *linear algebraic group* over K is a subgroup G of $\mathsf{GL}_n(K)$ defined by a set of polynomials $f_1(X), \ldots, f_n(X)$ where $X = (X_{ij})$. That is, an invertible matrix $A \in \mathsf{GL}_n(K)$ is an element of G if and only if

$$f_1(A) = \cdots = f_n(A) = 0.$$

Some classical examples

1. The general linear group $\mathsf{GL}_n(K)$ (take $f = 0$).

2. The special linear group $\mathsf{SL}_n(K)$ (let $f = \det(X) - 1$).

3. The orthogonal group

$$\mathsf{O}_n(K) = \{A \in \mathsf{GL}_n(K) | A^T A = I\}$$

(take the entries of $X^T X - I$).

4. The group $\mathsf{UT}_n(K)$ of upper triangular matrices (let x_{ij}, $i > j$, be the defining polynomials).

The *coordinate ring* of $\mathsf{GL}_n(K)$ is

$$H_n = K[X, 1/\det(X)].$$

It has the following property: A K-homomorphism $f : H_n \to K$ sends X to an invertible matrix A and, conversely, every $A \in \mathsf{GL}_n(K)$ determines a K-homomorphism by $X \mapsto A$.

If G is a linear algebraic subgroup of $\mathsf{GL}_n(K)$, its coordinate ring is the factor ring $H = H_n/\mathfrak{a}(G)$, where $\mathfrak{a}(G)$ is the ideal of polynomials in H_n that vanish on G.

The image of the matrix X in H is a *generic element* of G.

The ring H also encodes the group operation via $\mu : H \to H \otimes_k H$ with

$$\mu(X) = (X \otimes 1)(1 \otimes X).$$

Then, if $f, g : H \to K$ are given by $f : X \mapsto A$ and $g : X \mapsto B$ we have that $(f \otimes g) \circ \mu : H \to K$ is given by $X \mapsto AB$.

Let L/K be a field extension. Then a K-homomorphism $f : H \to L$ determines a subgroup of $\mathrm{GL}_n(L)$ denoted by $G(L)$. We redefine the linear algebraic group G as the functor obtained in this way and let $G(K)$ denote the original group.

For example, GL_n, SL_n, O_n, UT_n now become linear algebraic groups in this sense.

An *algebraic set* is defined in a similar fashion: If $\mathfrak{a}$ is a radical ideal in $K[\mathbf{x}] = K[x_1, \ldots, x_n]$, we form the *coordinate ring*

$$R = K[\mathbf{x}]/\mathfrak{a}(X),$$

and the points in the algebraic set $X \subseteq K^m$ are given as the image of the *generic point* $\mathbf{x}$ under K-homomorphisms $R \to L$, and let the *algebraic set* X be this functor, with the original set now denoted $X(K)$.

Note that $X(K)$ may be empty.

If $X$and Y are algebraic sets, with coordinate rings R and S, the product $X \times_K Y$ is given by $R \otimes_K S$. This ensures that

$$(X \times_K Y)(L) = X(L) \times Y(L).$$

A *morphism* $X \to Y$ of algebraic sets is a K-homomorphism $S \to R$. This will give an actual map $X(L) \to Y(L)$. In the case of μ, we denote the corresponding morphism $G \times_K G \to G$ by m.

A *group action* can then be defined in terms of a morphism $a : G \times_K X \to X$ (i.e., a K-homomorphism $\alpha : R \to H \otimes_K R$) such that the diagrams

$$\begin{array}{ccc} G \times_K G \times_K X & \xrightarrow{m \times 1_X} & G \times_K X \\ {\scriptstyle 1_G \times a}\downarrow & & \downarrow{\scriptstyle a} \\ G \times_K X & \xrightarrow[a]{} & X \end{array}$$

and

$$\begin{array}{ccc} K \times_K X & & \\ {\scriptstyle e \times 1_X}\downarrow & \searrow^{\rho} & \\ G \times_K X & \xrightarrow[a]{} & X \end{array}$$

commute. A trivial example is $X = G$ and $a = m$.

We then have that $G(L)$ acts on $X(L)$ for all $L \supseteq K$.

X is then a G-torsor if $r \otimes s \mapsto \alpha(r) \cdot (1 \otimes s)$ is an isomorphism $R \otimes_K R \cong H \otimes_K R$.

If $X(K) \neq \emptyset$ then X is trivial, *i.e.*, isomorphic to G.

Crossed homomorphisms and G-torsors

A *crossed homomorphism* is a continuous map $e\colon \mathrm{Gal}(K) \to G(\bar{K})$, where $\mathrm{Gal}(K)$ is the absolute Galois group of K, satisfying

$$e_{\sigma\tau} = e_\sigma \, \sigma e_\tau,$$

and two crossed homomorphisms e and e' are *equivalent* if

$$e'_\sigma = f \, e_\sigma \, \sigma f^{-1}$$

for some $f \in G(\bar{K})$.

A crossed homomorphism e gives rise to a torsor as follows:

Let H be the coordinate ring of G. On the scalar extension $\bar{H} = H \otimes_K \bar{K}$, we then have an obvious $\mathrm{Gal}(K)$-action, and we define an e-twisted action by

$$^{\sigma}x = e_\sigma(\sigma x), \quad \sigma \in \mathrm{Gal}(K).$$

The fixed ring $R = \bar{H}^{\mathrm{Gal}(K)}$ under this action is then the coordinate ring for a G-torsor, with the G-action induced by the restriction

$$\alpha \colon R \to H \otimes_K R$$

of the co-multiplication on $\bar{H}$.

Theorem. *The isomorphism classes of G-torsors correspond bijectively to the equivalence classes of crossed homomorphisms in $H^1(K, G)$.*

Review of quadratic forms

Let K be a field of characteristic $\neq 2$. A *quadratic* form over K is a map $q\colon V \to K$, where V is a finite-dimensional K-vector space, such that $q(\mathbf{x}) = B(\mathbf{x}, \mathbf{x})$ for some symmetric bilinear form $B\colon V \times V \to K$. Thus, if we pick a basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ for V, we get

$$q(\mathbf{x}) = (x_1, \ldots, x_n) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

where $\mathbf{x} = x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n$, and $A = (B(\mathbf{e}_i, \mathbf{e}_j))_{i,j}$. We say that the quadratic form is *represented* by A in the given basis.

If we choose another basis for V, the matrix B representing q in the new basis will have the form $B = P^T AP$, where $P \in \mathsf{GL}_n(K)$ is the coordinate transformation matrix for the two bases.

In particular: If q is represented by an invertible matrix in one basis, any matrix representing it will be invertible. We then refer to the quadratic form as *regular*. In this case, the determinant of a matrix representing q is called the *discriminant* of q.

Since $\det(B) = \det(P)^2 \det(A)$, the discriminant is only determined up to a quadratic factor.

Two quadratic forms $q\colon V \to K$ and $q'\colon V' \to K$ are *equivalent*, if there exists a vector space isomorphism $f\colon V \to V'$ such that $q(\mathbf{x}) = q'(f(\mathbf{x}))$ for all $\mathbf{x} \in V$. In terms of matrices, this means: If A represents q, and B represents q', there should exists an invertible matrix P with $P^T AP = B$.

An equivalence of q with itself is called an *isometry*. The isometries of q form a group, called the *orthogonal group* for q, denoted $\mathrm{O}(q)$. If we pick a basis for V, in which q is represented by A, the orthogonal group consists of all matrices P with $P^T AP = A$. In particular, an isometry must have determinant ± 1. The isometries with determinant 1 form a subgroup of $\mathrm{O}(q)$, called the *special orthogonal group* and denoted $\mathrm{SO}(q)$.

In the special case of the quadratic form

$$\mathbf{1}_n \colon K^n \to K$$

given by $\mathbf{1}_n(\mathbf{x}) = x_1^2 + \cdots + x_n^2$, the orthogonal and special orthogonal groups are denoted by $\mathrm{O}_n(K)$ and $\mathrm{SO}_n(K)$, respectively.

Every regular quadratic form is *diagonalizable*, i.e., representable by a diagonal matrix.

Theorem. *The elements of $H^1(K, \mathrm{SO}_n)$ correspond bijectively to the equivalence classes of n-dimensional quadratic forms over K of discriminant 1.*

The correspondence between the cohomology classes in $H^1(K, \mathrm{SO}_n)$ and the isomorphism classes of regular n-dimensional quadratic forms of discriminant 1 can be realized as follows:

Given a crossed homomorphism $e\colon \mathrm{Gal}(K) \to \mathrm{O}_n(\bar{K}_{\mathrm{sep}})$, we define the e-twisted Galois action on $\bar{K}^n_{\mathrm{sep}}$ by

$$^{\sigma}\mathbf{x} = e_\sigma(\sigma\mathbf{x}), \quad \mathbf{x} \in \bar{K}^n_{\mathrm{sep}}, \quad \sigma \in \mathrm{Gal}(K),$$

and get the twisted quadratic space by restricting the quadratic form $\mathbf{1}_n$ to the K-vector space V_e of fixed points under this action. This defines a quadratic form $q\colon V_e \to K$, since e_σ is an isometry, so that $\mathbf{1}_n(^{\sigma}\mathbf{x}) = \mathbf{1}_n(\sigma\mathbf{x}) = \sigma\mathbf{1}_n(\mathbf{x})$, making the image of a fixed point a fixed point, i.e., an element in K. If e maps into $\mathrm{SO}_n(\bar{K}_{\mathrm{sep}})$, this space will have discriminant 1.

Thus, since the elements in $H^1(K, \mathrm{SO}_n)$ correspond to isomorphism classes of quadratic forms of discriminant 1 on one hand, and to torsors for the special orthogonal group on the other, we have that the torsors correspond to quadratic forms. In particular, that a quadratic form not equivalent to the unit form $\mathbf{1}_n$ will correspond to a non-trivial torsor.

Picard-Vessiot Extension

Let F be a differential field of characteristic zero with algebraically closed field of constants $\mathcal{C}$ and

$$L = Y^{(n)} + a_1 Y^{(n-1)} + \cdots + a_n Y^{(0)}$$

be a monic homogeneous linear differential operator over F. A differential field extension $E \supset F$ is said to be a Picard-Vessiot extension for L if:

1. E is generated over F as a differential field by the set V of solutions of $L = 0$ in E ($E = F\langle V \rangle$);

2. E contains a full set of solutions of $L = 0$ (there are $y_i \in V$, $1 \leq i \leq n$ with the wronskian $w(y_1, \ldots, y_n) \neq 0$);

3. Every constant of E lies in F.

A *Picard-Vessiot ring* over F for the equation $y' = Ay$, with $A \in \mathsf{M}_n(F)$, is a differential ring R over F satisfying:

1. R is a simple differential ring.

2. There is a fundamental matrix S for $y' = Ay$ with coefficients in R, i.e., the matrix $S \in \mathsf{GL}_n(R)$ satisfies $S' = AS$.

3. R is generated as a ring by F, the entries of S and the inverse of the determinant of S.

Theorem (Kolchin's Main Structure Theorem)**.** *Let R be a Picard-Vessiot ring with differential Galois group G. Then $Z = max(R)$ is a G-torsor over K.*