AUTOMORPHISM GROUP SCHEMES OF FINITE FIELD EXTENSIONS

Ke-Zheng Li

Graduate School of Academia Sinica/Max-Planck-Institut für Mathematik

0. Introduction.

Let S be a noetherian scheme and $X \to S$ be a flat projective morphism. The automorphism group scheme $\mathcal{A}ut(X/S)$ represents the following functor

$$\begin{aligned} \mathfrak{Aut}_{X/S}\colon ((S\text{-schemes})) &\to ((\text{sets})) \\ T &\mapsto \{T\text{-automorphisms of } T \times_S X\} \end{aligned}$$

We study $\mathcal{A}ut(X/S)$ because of two reasons. First, $\mathcal{A}ut(X/S)$ is an important invariant of the S-scheme X, which often gives useful information about X; second, the structure of $\mathcal{A}ut(X/S)$ and its action on X are also interesting objects to study. The situation is usually non-trivial even when $S = \mathrm{Spec}(K)$ for a field K.

In this paper we mainly discuss the case when $X \to S$ is finite, especially when $X = \mathrm{Spec}(L)$, $S = \mathrm{Spec}(K)$ for a finite field extension $L \supset K$, in this case $\mathcal{A}ut(X/S)$ may play a role of a stronger tool than the Galois group $\mathrm{Gal}(L/K)$, and its structure is by no means trivial. This is also the necessary first step toward the calculation of $\mathcal{A}ut(X/S)$ in general case.

In §1 we give the definition and basic properties of automorphism group schemes, and then give some examples. This will show the non-triviality of the calculation of $\mathcal{A}ut(X/S)$, even when $S = \mathrm{Spec}(K)$ for a field K. In §2 we discuss the automorphism group schemes of finite field extensions. We first give a canonical decomposition for inseparable case and explain the calculation for the purely inseparable case. This almost reduces the general calculation to separable case. Finally we discuss the separable case and give more examples in §3.

1. Automorphism group schemes.

Let X be a flat relatively projective scheme over a noetherian scheme S, then the following functor

$$\begin{aligned} \mathfrak{Aut}_{X/S}\colon ((S\text{-schemes})) &\to ((\text{sets})) \\ T &\mapsto \{T\text{-automorphisms of } T\times_S X\} \end{aligned}$$

is represented by a locally quasi-projective S-scheme $\mathcal{A}ut(X/S)$, called the *automorphism group scheme* of X over S (if $S = \mathrm{Spec}(K)$ for a field K, then we also denote $\mathcal{A}ut(X/S)$ by $\mathcal{A}ut(X/K)$). Explicitly, let $\Phi_{X/S} : \mathcal{A}ut(X/S)\times_S X \to \mathcal{A}ut(X/S)\times_S X$ be the universal $\mathcal{A}ut(X/S)$-automorphism, then an S-morphism $f : T \to \mathcal{A}ut(X/S)$ corresponds to the base change of $\Phi_{X/S}$ via f.

The following are some basic properties of automorphism group schemes.

Lemma 1. *Let S be a noetherian scheme and X be a flat relatively projective scheme over S.*

i) *$\mathcal{A}ut(X/S)$ commutes with base change, i.e. if T is a noetherian S-scheme we have $\mathcal{A}ut(X\times_S T/T)\cong \mathcal{A}ut(X/S)\times_S T$.*
ii) *$\mathcal{A}ut(X/S)$ is an S-group scheme with a canonical action on X representing the following functor:*

$$\begin{aligned} \mathfrak{Act}_{X/S}\colon ((S\text{-group schemes})) &\to ((\text{sets})) \\ G &\mapsto \{\text{actions of } G \text{ on } X\} \end{aligned}$$

Explicitly, $\rho_{X/S} = pr_1\circ\Phi_{X/S} : \mathcal{A}ut(X/S)\times_S X \to X$ is the canonical action, and each homomorphism $h : G \to \mathcal{A}ut(X/S)$ corresponds to the action $\rho_{X/S}\circ(h\times_S id_X) : G\times_S X \to X$.

These are just abstract nonsense.

Lemma 2. *Let S be a noetherian scheme and $X \to S$ be a flat finite morphism. Then $\mathcal{A}ut(X/S)$ is linear, i.e. locally over S, $\mathcal{A}ut(X/S)$ can be embedded into* $\mathrm{GL}(n,S)$ *as a closed subgroup scheme, where n is the local degree of $X\to S$.*

This is easy to check directly.

Remark 1. The assumption of relative projectivity is quite essential in the definition of $\mathcal{A}ut(X/S)$, in fact, if $X\to S$ is flat and quasi-projevtive but not projective, then $\mathfrak{Aut}_{X/S}$ is usually not representable, not even when $X = \mathbb{A}^1_S$. Note that the two concepts "representation" and "action" (of S-group schemes on X) are equivalent only when $\mathfrak{Act}_{X/S}$ is representable. When $S = \mathrm{Spec}(K)$ for a field K and $X = \mathbb{A}^1_K$, $\mathfrak{Act}_{X/S}$ is representable only when $\mathrm{ch}(K) = 0$.

Example 1. Let $S = \mathrm{Spec}(\mathbb{Z})$, $X = \mathbb{P}^n_{\mathbb{Z}}$. Then for any S-scheme T, every T-automorphism of $T \times_S X$ preserves $O(1)$. Hence $\mathcal{A}ut(X/S)$ is isomorphic to a closed subgroup scheme of $\mathrm{PGL}(n+1, S)$. On the other hand, $\mathrm{PGL}(n+1, S)$ really acts on X. Hence $\mathcal{A}ut(X/S) \cong \mathrm{PGL}(n+1, S)$.

Example 2. Let X be an abelian variety over an algebraically closed field k. Then by [L2, Lemma 2.3], one sees easily that $\mathcal{A}ut(X/k) \cong X \rtimes \mathrm{Aut}(X)$, where $\mathrm{Aut}(X)$ is the automorphism group of X endowed the discrete group scheme structure, and X acts on X by translation.

Example 3. Let C be a complete non-singular curve over a field K. Using the method of §2 and Lemma 3.1 below, one can calculate $\mathcal{A}ut(C/K)$ as follows: first calculate $\mathcal{A}ut(C \otimes_K \bar{K}/\bar{K})$ (where $\bar{K}$ is the algebraic closure of K), then by taking the quotient of an action of a finite group scheme one can get $\mathcal{A}ut(C/K)$. Therefore it reduces to consider the case when K is algebraically closed. If $g(C) = 0$ or 1, we can apply Example 1 or Example 2 to calculate $\mathcal{A}ut(C/K)$. If $g(C) > 1$, then $\mathcal{A}ut(C/K)$ is finite étale (cf. [L2]).

If X is a smooth projective variety of dimension > 1 over K, then $\mathcal{A}ut(X/K)$ need not to be reduced when $\mathrm{ch}(K) > 0$ (see [L2, Example 2.8]).

Terminology. A morphism of schemes $f : X \to Y$ is called an *epimorphism* if f is set-theoretically onto and $f^* : O_Y \to f_* O_X$ is a monomorphism.

Let S be a noetherian scheme, X be an S-scheme of finite type and G be a group scheme of finite type over S. An action $\rho : G \times_S X \to X$ of G on X is called *transitive* if $(\rho, \mathrm{pr}_2) : G \times_S X \to X \times_S X$ (intuitively $(g, x) \mapsto (gx, x)$) is an epimorphism. If ρ has a geometric quotient X/G which is a locally closed subscheme of S, then ρ is transitive; on the other hand, if $X \to S$ is f.f. and ρ is transitive, then there is a geometric quotient $X/G \cong S$.

Corollary 1. *If $X \to S$ is finite étale of degree n, then $\mathcal{A}ut(X/S)$ is finite étale of degree $n!$ over S, and the universal action $\rho_{X/S}$ is transitive. In fact, $(\rho, \mathrm{pr}_2) : G \times_S X \to X \times_S X$ is f.f. and there is a universal geometric quotient $X/\mathcal{A}ut(X/S) \cong S$.*

Proof. Take an étale cover $S' \to S$ such that $X \times_S S'$ is a disjoint union of n copies of S'. It is clear that $(X \times_S S'/S')$ is the discrete group scheme structure of the permutation group of the n copies of S' ($\cong \mathfrak{S}_n$), in particular it acts transitively on $X \times_S S'$. Therefore $\mathcal{A}ut(X/S) \to S$ is étale of degree $n!$ because it is so after an étale base change, and $\rho_{X/S}$ is transitive also because it is so after an étale base change. Q.E.D.

2. The case of finite field extensions.

In the following we study a special case: $S = \mathrm{Spec}(K)$, $X = \mathrm{Spec}(L)$, where $L \supset K$ is a finite field extension. For simplicity we will denote $G_{L/K} = \mathcal{A}ut(X/S)$ in this case. We are interested with this case because of two reasons: First, the calculation of $G_{L/K}$ can be a first step toward the general calculations of $\mathcal{A}ut(X/S)$, which is by no means trivial as we will see; Second, in any case $L^{G_{L/K}} = K$ (see Proposition 1 below), while $L^{\mathrm{Gal}(L/K)} = K$ only when $L \supset K$ is Galois, hence $G_{L/K}$ is a useful tool which can take over the job of $\mathrm{Gal}(L/K)$ when $L \supset K$ is not a Galois extension (especially when $L \supset K$ is inseparable). For example, in many constructions one can make use of an arbitrary base field extension, and after the construction one can go back to the original base field whenever the construction commutes with the action of $G_{L/K}$.

Note that by definition there is a canonical isomorphism $\mathrm{Gal}(L/K) \cong G_{L/K}(K)$ (the group of K-points of $G_{L/K}$). However, we will see $G_{L/K}$ is larger than $\mathrm{Gal}(L/K)$ (i.e. it has points which are not K-points) unless $L = K$ or $L \supset K$ is a separable extension of degree 2.

For a group scheme G over K we will denote by $m : G \times_K G \to G$ the multiplication, $\iota : G \to G$ the inverse and $o : \mathrm{Spec}(K) \to G$ the unit section. When G is affine, we will only give m^*, ι^* and o^* for the group scheme structure of G.

Example 1. Let $K = \mathbb{Q}$, $L = \mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}[\sqrt[3]{2}]$. Then $G_{L/K}$ is an étale group scheme of degree 6 over $\mathbb{Q}$ (see Corollary 1.1). By direct calculation we can get $G_{L/K} = \mathrm{Spec}(R)$, where

$$R = \mathbb{Q}[r, s, t]/(r - s^2 - s + t^3/2 - 1, rs, rt, st) \cong \mathbb{Q} \times \mathbb{Q}[\sqrt{-3}] \times \mathbb{Q}[\sqrt[3]{2}] \qquad (1)$$

with group scheme structure given by

$$\begin{aligned}
&m^*(r) = r \otimes r + \tfrac{1}{3}(s \otimes s + s^2 \otimes s^2 + s^3 \otimes s^3) + \tfrac{1}{12}(2t^2 \otimes t + 2t \otimes t^2 + t^3 \otimes t^3),\\
&m^*(s) = r \otimes s + s \otimes r + \tfrac{1}{3}(2s \otimes s - s^2 \otimes s^2 - s^3 \otimes s^3) + \tfrac{1}{12}(4t^2 \otimes t - 2t \otimes t^2 - t^3 \otimes t^3),\\
&m^*(t) = r \otimes t + t \otimes r + s^2 \otimes t + t \otimes s,\\
&\iota^*(r) = r, \iota^*(s) = s^2, \iota^*(t) = t, o^*(r) = 1, o^*(s) = o^*(t) = 0
\end{aligned}$$

and the universal action ρ is given by

$$\rho^*(x) = r \otimes x + s \otimes x + \tfrac{1}{2}t^2 \otimes x^2.$$

One observes that 2 and 3 appear in the denominators, this is because that L has bad reduction at 2 and 3 (but good reductions at the other places). One also see that L appears in the structure of $G_{L/K}$, and we will see this is a pretty general situation.

Example 2. Let K be a field of characteristic $p > 0$, and $L = K[t^{\frac{1}{p}}] \cong K[x]/(x^p - t)$ for some $t \in K - K^p$. By direct calculation we can get $G_{L/K} = \mathrm{Spec}(R)$, where

$$R = K[y_0, y_1, ..., y_{p-1}, y_1^{-1}]/(y_0^p + (y_1^p - 1)t + y_2^p t^2 + ... + y_{p-1}^p t^{p-1}) \qquad (2)$$

and the universal action ρ is given by

$$\rho^*(x) = y_0 \otimes_K 1 + y_1 \otimes_K x + \cdots + y_{p-1} \otimes_K x^{p-1}$$

(for simplicity we omit the group scheme structure, e.g. when $p = 2$, the group scheme structure of $G_{L/K}$ is given by $m^*(y_0) = y_0 \otimes 1 + y_1 \otimes y_0$, $m^*(y_1) = y_1 \otimes y_1$, $\iota^*(y_0) = y_0 y_1^{-1}$, $\iota^*(y_1) = y_1^{-1}$, $o^*(y_0) = 0$, $o^*(y_1) = 1$). We see that $\dim(G_{L/K}) = p - 1 > 0$ and $G_{L/K}$ is non-commutative. Furthermore, $G_{L/K}$ is integral and geometrically irreducible, but not normal, and not geometrically reduced.

For the general case we use the following decomposition method.

Proposition 1. *Let $L \supset K$ be a finite field extension. Denote by L' the largest separable extension of K in L.*

- i) *If $ch(K) = p > 0$, then the inclusion $L' \hookrightarrow L$ induces an epimorphism $G_{L/K} \to G_{L'/K}$. Let $H = ker(G_{L/K} \to G_{L'/K})$, then $L^H = L'$. Furthermore, for any finite extension $\Lambda \supset L$ which is normal over K, $H \otimes_K \Lambda \cong \prod_{i=1}^n G_{L/L'} \otimes_{L'} \Lambda$.*
- ii) *$G_{L/K}$ acts transitively on $Spec(L)$, i.e. $(\rho, pr_2) : G_{L/K} \times_K Spec(L) \to Spec(L) \times_K Spec(L)$ is f.f., where $\rho : G_{L/K} \times_K Spec(L) \to Spec(L)$ is the universal action of $G_{L/K}$ on $Spec(L)$. Therefore we have $Spec(L)/G_{L/K} \cong Spec(K)$, or in other words $L^{G_{L/K}} = K$.*

Proof. When $L \supset K$ is separable, ii) holds by Corollary 1.1, so in the following we assume $\mathrm{ch}(K) = p > 0$.

For any K-algebra A, any A-automorphism of $A \otimes_K L$ induces an A-automorphism of $A \otimes_K L'$, because $L' = K[L^{p^m}]$ for some m. Hence there is an induces homomorphism $G_{L/K} \to G_{L'/K}$. If $\Lambda \supset L$ is a finite extension which is normal over K, then $L \otimes_K \Lambda \cong \prod_{i=1}^n R$, where $R = L \otimes_{L'} \Lambda \cong \Lambda[x_1, ..., x_r]/(x_1^{p^{m_1}}, ..., x_r^{p^{m_r}})$ for some $r \geq 0$, $m_1, ..., m_r > 0$. By Lemma 1.1.i), $G_{L/K} \otimes_K \Lambda \cong \mathcal{A}ut(\mathrm{Spec}(L \otimes_K$

$\Lambda)/\Lambda)$. Obviously any Λ-automorphism of $\mathrm{Spec}(L' \otimes_K \Lambda)$ can be lifted to an Λ-automorphism of $\mathrm{Spec}(L \otimes_K \Lambda)$, hence $G_{L/K} \to G_{L'/K}$ is an epimorphism (because it is an epimorphism after an f.f. base change). Furthermore, it is easy to see that $H \otimes_K \Lambda \cong \prod_{i=1}^n \mathcal{A}ut(\mathrm{Spec}(R)/\Lambda)$, and $\mathrm{Spec}(R)/\mathcal{A}ut(\mathrm{Spec}(R)/\Lambda) \cong \mathrm{Spec}(\Lambda)$. Thus ii) holds because $\mathcal{A}ut(\mathrm{Spec}(R)/\Lambda) \cong G_{L/L'} \otimes_{L'} \Lambda$. Finally, it is it is easy to see that $\mathcal{A}ut(\mathrm{Spec}(R)/\Lambda)$ acts transitively on $\mathrm{Spec}(R)$, hence $\mathcal{A}ut(\mathrm{Spec}(L \otimes_K \Lambda)/\Lambda)$ acts transitively on $\mathrm{Spec}(L \otimes_K \Lambda)$, so $G_{L/K}$ acts transitively on $\mathrm{Spec}(L)$. Q.E.D.

When $\mathrm{ch}(K) = p > 0$, let $H_m = \ker(F^m_{G_{L/K}/K})$, where m satisfies $L^{p^m} \subset L'$. Then H_m is a finite normal subgroup scheme of $G_{L/K}$, $H_m \subset H$, and $L^{H_m} = L'$. Therefore to get down from L to K we need only divide by finite group schemes. If $L \supset K$ is normal, there exists an intermediate field L'' of $K \subset L$ such that $L'' \supset K$ is purely inseparable (or trivial) and $L \supset L''$ is separable. In this case $L \cong L' \otimes_K L''$, hence for any K-algebra A, an A-automorphism of $A \otimes_K L''$ is equivalent to an $A \otimes_K L'$-automorphism of $A \otimes_K L$. Therefore $G_{L''/K} \otimes_K L' \cong G_{L/L'}$. Imitating Example 2, the calculation of $G_{L''/K}$ is not hard, though the results are rather complicated. Furthermore, the semidirect product $G = H_m \rtimes \mathrm{Gal}(L/K)$ is a finite subgroup scheme of $G_{L/K}$ such that $L^G = K$.

With the decomposition method in Proposition 1 and the above way to calculate the purely inseparable case, it remains to study the calculation of separable case for the general calculation of $G_{L/K}$.

3. Separable case.

In the following we consider the case when $L \supset K$ is separable. The following lemma is a general method to study schemes using flat base change (see [Ra]).

Lemma 1. *Let $T \to S$ be a finite f.f. morphism of locally noetherian schemes, and $G \subset \mathcal{A}ut(T/S)$ be a flat finite subgroup scheme acting freely and transitively on T. Then there is an equivalence of categories*

$$((S\text{-schemes}))/\sim \ \leftrightarrow \ \left(\left(\begin{matrix} T\text{-schemes together with an action of } G \\ \text{compatible with the action of } G \text{ on } T \end{matrix}\right)\right)\Big/\sim$$
$$Y \mapsto Y \times_S T$$
$$X/G \leftarrow\!\shortmid X$$

(*where the S-schemes are all assumed to be separated, and an action of G on X is assumed to have a geometric quotient X/G such that $X \to X/G$ is flat, these all hold if we only consider locally quasi-projective schemes*).

Proof. By assumption we have $T/G \cong S$ and $T \times_S T \cong G \times_S T$. We need to show that for any separated T-scheme X together with an action of G compatible with the action of G on T, we have $X \cong T \times_S (X/G)$.

Denolte by ρ the action of G on X, $Y = X/G$ and $\pi : X \to T$ the projection. We claim that G acts freely on X. By the assumptions on G we have an isomorphism

$$\theta : \; G \times_S X \cong (G \times_S T) \times_T X \xrightarrow{\cong} (T \times_S T) \times_T X \cong T \times_S X \tag{5}$$

By the compatibility of the actions of G on X and T, we have a commutative diagram

$$\begin{array}{ccc} G \times_S X & \xrightarrow{(\rho, \mathrm{pr}_2)} & X \times_S X \\ \big\downarrow \theta & & \big\downarrow \pi \times_S \mathrm{id}_X \\ T \times_S X & \xrightarrow{\mathrm{id}} & T \times_S X \end{array} \tag{6}$$

Hence $G \times_S X \to X \times_S X$ is a closed immersion because it is a section of the separated morphism $\pi \times_S \mathrm{id}_X$. Therefore $X \times_Y X \cong G \times_S X$. We get

$$\begin{aligned} &(T \times_S Y) \times_Y X \cong T \times_S X \cong (T \times_S T) \times_T X \\ \cong &(G \times_S T) \times_T X \cong G \times_S X \cong X \times_Y X \end{aligned} \tag{7}$$

Since $X \to Y$ is f.f., we see $X \to T \times_S Y$ is an isomorphism. Q.E.D.

Corollary 1. *Let $\Lambda \supset K$ be a finite Galois extension. Then there is an equivalence of categories*

$$\{K\text{-schemes}\}/\sim \;\leftrightarrow \left\{ \begin{array}{c} \Lambda\text{-schemes together with an action of } \mathrm{Gal}(\Lambda/K) \\ \text{compatible with the action of } \mathrm{Gal}(\Lambda/K) \text{ on } \Lambda \end{array} \right\} \Big/ \sim$$

$$\begin{aligned} Y &\mapsto Y \otimes_K \Lambda \\ X/\mathrm{Gal}(\Lambda/K) &\leftarrow\!\shortmid X \end{aligned}$$

(*where the schemes are all assumed to be separated, and an action of* $\mathrm{Gal}(\Lambda/K)$ *on X is assumed to have a geometric quotient Y such that $X \to Y$ is flat). In particular, we have an equivalence of categories*

$$\left\{ \begin{array}{c} \text{étale } K\text{-schemes of degree } n \\ \text{which are split over } \Lambda \end{array} \right\} \Big/ \sim \;\leftrightarrow\; \mathrm{Hom}(\mathrm{Gal}(\Lambda/K), \mathfrak{S}_n)/\mathrm{Aut}(\mathfrak{S}_n)$$

where $\mathrm{Gal}(\Lambda/K)$ *acts on* $\mathrm{Spec}(\Lambda\times \overset{n}{\cdots} \times\Lambda)$ *by* $\sigma(a_1,...,a_n) = (\sigma a_{\sigma 1},...,\sigma a_{\sigma n})$ $(\forall\sigma \in \mathrm{Gal}(\Lambda/K))$ *via the* Λ*-algebra structure* $\Lambda \to \Lambda\times\cdots\times\Lambda$.

Let $X = \mathrm{Spec}(\Lambda\times \overset{n}{\cdots} \times\Lambda)$ with a permutatione action ρ of $H = \mathrm{Gal}(\Lambda/K)$. Then ρ gives a homomorphism $\eta : \mathrm{Gal}(\Lambda/K) \to \mathrm{Per}(X) \cong \mathfrak{S}_n$. Let Y be the K-scheme corresponding to X in Lemma 2. Then we have a one-to-one correspondence

$\mu_X : \{H\text{-orbits of } X\} \to \{\text{points of } Y\}$

where for any $x \in X$, the H-orbit C_x of x satisfies $\mu_X(C_x) = \mathrm{Spec}(K_x)$ for a field $K_x \supset K$, with $\#(C_x) = [K_x : K]$ (= the degree of $\mu_X(C_x)$ over K). Furthermore, if $H_x \subset \mathrm{Gal}(\Lambda/K)$ is the stabilizer of x under ρ, then K_x is isomorphic to the intermediate field of $\Lambda \supset K$ corresponding to H_x. (Note that for different choices of representatives x of an orbit, the stabilizers H_x just form a conjugacy class of subgroups of $\mathrm{Gal}(\Lambda/K)$, which corresponds to just one K-isomorphism class of intermediate fields.) Thus $|H_x| = [\Lambda : K_x]$.

In particular, if $Y = \mathrm{Spec}(L)$, where L is a separable field extension of K, we can take Λ to be a Galois closure of $L \supset K$ (and $X = Y \otimes_K \Lambda$), in this case η is a monomorphism.

Let $\Lambda \supset K$ be a finite Galois extension. Let $Y = \mathrm{Spec}(A)$ be an étale K-scheme of degree n which splits over Λ, and $X = Y \otimes_K \Lambda$. Denote $G = \mathcal{A}ut(Y/K)$, $G' = G \otimes_K \Lambda$. Then by Lemma 1.1.i), G' is isomorphic to $\mathrm{Per}(X) \cong \mathfrak{S}_n$ with the discrete group scheme structure over Λ. By Corollary 1 we see that H acts on both $X(\Lambda)$ and $G'(\Lambda) \cong \mathfrak{S}_n$, and it is easy to see that $\sigma(g(x)) = \sigma(g)(\sigma(x))$ $(\forall\sigma \in H$, $g \in G'$, $x \in X)$, hence

$$\sigma(g) = \eta(\sigma) \circ g \circ \eta(\sigma)^{-1} \quad \forall\sigma \in H,\ g \in \mathfrak{S}_n \tag{8}$$

Therefore we have a one-to-one correspondence

$\mu : \{\eta(H)\text{-conjugacy classes of } \mathfrak{S}_n\} \to \{\text{points of } G\}$

where for any $g \in \mathfrak{S}_n$, the $\mu(H)$-conjugacy class C_g of g satisfies $\mu(C_g) = \mathrm{Spec}(K')$ for a field $K' \supset K$, with $\#(C_g) = [K' : K]$ (= the degree of $\mu(C_g)$ over K). Furthermore, if $H_g \subset H$ is the stabilizer of g under action (8), then K' is isomorphic to the intermediate field of $\Lambda \supset K$ corresponding to H_g. In particular $|H_g| = [\Lambda : K']$. Summarizing we get

Proposition 1. *Let* $\Lambda \supset K$ *be a finite Galois extension,* Y *be an étale scheme of degree* n *over* K *which splits completely over* Λ*,* $X = Y \otimes_K \Lambda$*,* $G = \mathcal{A}ut(Y/K)$*,* $H = \mathrm{Gal}(\Lambda/K)$*, and* $\eta : H \to \mathfrak{S}_n$ *be the induced permutative representation of* H *on* $X \cong Spec(\Lambda\times \overset{n}{\cdots} \times\Lambda)$*. Then*

i) *Under the equivalence of categories in Corollary 1 (with $n!$ instead of n), G corresponds to the conjugation action of H on $\mathfrak{S}_n$ given by (8).*

ii) *There is a one-to-one correspondence*

$\mu : \{\eta(H)\text{-conjugacy classes of } \mathfrak{S}_n\} \to \{\text{points of } G\}$

where for any $g \in \mathfrak{S}_n$, the $\eta(H)$-conjugacy class C_g of g satisfies $\mu(C_g) = \mathrm{Spec}(K')$ for the intermediate field K' of $\Lambda \supset K$ corresponding to the stabilizer H_g of g in H under action (7), and $\#(C_g) = [K' : K]$, $|H_g| = [\Lambda : K']$. Hence $G \cong \mathrm{Spec}(\prod_{i=1}^{r} K_i)$ for some intermediate fields K_i of $\Lambda \supset K$, and $\sum_{i=1}^{r}[K_i : K] = n!$.

In particular, if $Y = \mathrm{Spec}(L)$ for a separable extension $L \supset K$ and Λ is a Galois closure of $L \supset K$, then H can be viewed as a subgroup of $\mathfrak{S}_n$, and H_g is just the centralizer of g in H.

It is natural to ask: For a given extension $L \supset K$, what intermediate fiels appear as some K_i? The following example answers this in the case when $L \supset K$ is Galois.

Example 1 (The case $L = \Lambda$). We use the notation in Proposition 1. Let $L \supset K$ be a Galois extension. Then X is in one-to-one correspondence with $\mathrm{Gal}(L/K)$, hence we can identify X as H with the action of H by left multiplication. We show that when $n \neq 2$, any subgroup $H' \subset H$ is equal to H_g for some $g \in G'$.

We may assume $H' \neq H$. Let $r = i_H(H')$. Take $u_1 = e$, $u_2, ..., u_r$ such that $H = H'u_1 \cup \cdots \cup H'u_r$. If $r > 2$, let $g \in \mathfrak{S}_n$ be defined by $g(hu_1) = hu_1$, $g(hu_i) = hu_{i+1}$ $(2 \leq i < r)$, $g(hu_r) = hu_2$ $(\forall h \in H')$. Clearly $g \circ \phi_h = \phi_h \circ g$ $\forall h \in H'$, where $\phi_h : H' \to H'$ is the left multiplication by h. But for $u \in H - H'$ we have $g \circ \phi_u \neq \phi_u \circ g$, because $g(u \cdot e) \neq u \cdot e$. If $r = 2$, then $|H'| > 1$. Take $a \neq e \in H'$ and define $g \in \mathfrak{S}_n$ by $g(hu_i) = hau_i$ $(\forall i > 1)$, $g(hu_1) = hu_1$ $(\forall h \in H')$. Again we have $g \circ \phi_h = \phi_h \circ g$ $(\forall h \in H')$ but $g \circ \phi_u \neq \phi_u \circ g$ $(\forall u \in H - H')$, because $g(u \cdot e) \neq u$. In any case we have $H_g = H'$.

By Proposition 1, we see that every intermediate field of $L \supset K$ is isomorphic to some K_i over K.

Example 2.1 shows that when $L \supset K$ is not Galois, there may be a K_i which is not isomorphic to an intermediate field of $L \supset K$ over K. On the other hand, if $L \neq \Lambda$, there may be an intermediate field K' of $\Lambda \supset K$ which is not isomorphic to any K_i over K, for example when $n > 4$ and $\mathrm{Gal}(\Lambda/K) \cong \mathfrak{S}_n$, we can identify $\mathrm{Gal}(\Lambda/K)$ with $\mathrm{Per}(X) \cong \mathfrak{S}_n$, there is no element of $\mathfrak{S}_n$ whose centralizer is A_n, hence there is no K_i such that $[K_i : K] = 2$. Furthermore, in general case there may not be a subgroup scheme of G (of degree n) which acts freely and transitively on $\mathrm{Spec}(L)$, for example if $[L:K]=5$ and $\mathrm{Gal}(\Lambda/K)\cong\mathfrak{S}_5$, then since all of the elements of order 5 in $\mathfrak{S}_5$ are in one and the same conjugacy class, they correspond to a K_i with $[K_i:K]=24$, hence there is no subgroup scheme of G of degree 5.

References

[F] W. Fulton: *Intersection Theory*, Springer-Verlag, Berlin-Heidelberg-N.Y.-Tokyo (1984)

[H] R. Hartshorne: *Algebraic Geometry*, GTM52, Springer-Verlag, NY-Heidelberg-Berlin (1977)

[La] S. Lang: *Abelian Varieties*, Interscience Pub. Inc., New York (1959)

[LN] S. Lang & A. Néron: Rational points of abelian varieties over function fields, Amer. J. Math. 81 (1959), 95-118

[L1] K. Li: *Commutative Algebra and Homological Algebra* (in Chinese), Sci. Press (1999)

[L2] K. Li: Actions of group schemes (I), Compsitio Math. 80 (1991), 55-74

[L3] K. Li: Actions of group schemes (II), to appear

[L4] K. Li: *Lectures on Group Schemes and Their Actions* (in Chinese), preprint (1996)

[L5] K. Li: Push-out of schemes and some applications, preprint (1997)

[Ma] H. Matsumura: *Commutative Algebra*, W.A.Benjamin Co., New York (1970)

[Mi] M. Miyanishi: Some remarks on a covering of an abelian variety, J. Math. Kyoto Univ. 7-1 (1967), 77-92

[M1] D. Mumford: *Lectures on Curves on an Algebraic Surface*, Annals of Math. Studies 59, Princeton University Press, Princeton (1966)

[M2] D. Mumford - *Abelian varieties*, 2nd print, reprinted, Tata Inst. Fund. Res. & Oxford Univ. Press (1985)

[M3] D. Mumford: *Geometric Invariant Theory*, 2nd ed., Ergebnisse, Springer-Verlag, Berlin-Heidelberg-New York (1982)

[M4] D. Mumford - The structure of the moduli spaces of curves and abelian varieties. In: Actes, Congrès international math. 1970, tome 1, 457-465. Paris: Gauthier-Villars 1971

[O1] F. Oort - *Commutative group schemes*, LNM 15, Springer-Verlag (1966)

[O2] F. Oort - Some questions in algebraic geometry, preprint

[Ra] M. Raynaud: Schémas en groupes de type $(p,...,p)$, Bull. Soc. math. France 102 (1974), 241-280

[Ro] M. Rosenlicht: Some basic theorems on algebraic groups, Amer. J. Math. 78 (1956), 401-443

[TO] J. Tate & F. Oort: Group schemes of prime order, Ann. Sc. Ecole Norm. Sup. 3 (1970), 1-21