Lecture 5

November 18, 2004
Notes by Alexander Caspar

§11 Galois descent

Let k'/k be a finite Galois extension of fields with Galois group Γ. Let $k'[\Gamma]$ denote the *twisted group ring of* Γ *over* k', that is, the set of formal linear combinations $\sum_{\gamma\in\Gamma} x'_\gamma[\gamma]$ for $x'_\gamma \in k'$, with coefficientwise addition and the multiplication $(x'[\gamma])\cdot(y'[\delta]) = (x'\cdot\gamma(y'))[\gamma\delta]$. Note that giving a left module over $k'[\Gamma]$ is the same as giving a k'-vector space together with a semilinear action by Γ, that is, an additive action satisfying $\gamma(x'v') = \gamma(x')\gamma(v')$. Extension of scalars gives us a functor

$$\mathfrak{Vec}_k = \mathfrak{Mod}_k \longrightarrow \mathfrak{Mod}_{k'[\Gamma]},\ V \mapsto V\otimes_k k', \tag{11.1}$$

where $\gamma\in\Gamma$ acts on $V\otimes_k k'$ via $\mathrm{id}\otimes\gamma$.

Theorem 11.2. This functor is an equivalence of categories.

Proof. We prove that the functor $V' \mapsto (V')^\Gamma$ is a quasi-inverse. Indeed, the natural isomorphism

$$(V\otimes_k k')^\Gamma = V\otimes_k (k')^\Gamma = V\otimes_k k \cong V$$

shows that the composite $\mathfrak{Vec}_k \to \mathfrak{Mod}_{k'[\Gamma]} \to \mathfrak{Vec}_k$ is isomorphic to the identity. For the other way around we consider the natural $k'[\Gamma]$-linear homomorphism

$$(V')^\Gamma\otimes_k k' \longrightarrow V',\ v'\otimes x' \mapsto x'v'.$$

Claim. It is injective.

Proof. Assume that it is not, and let $\sum_{i=1}^r v'_i\otimes x'_i$ be a non-zero element in the kernel with r minimal. Then $r\geq 1$ and all v'_i and all x'_i are linearly independent over k. In particular $x'_1\neq 0$, so after dividing by x'_1 we may assume that $x'_1 = 1$. Then for every $\gamma\in\Gamma$ the element

$$\sum_{i=2\ \text{(sic!)}}^r v'_i\otimes(\gamma(x'_i)-x'_i) \;=\; \gamma\Big(\sum_{i=1}^r v'_i\otimes x'_i\Big) - \sum_{i=1}^r v'_i\otimes x'_i$$

again lies in the kernel. Thus the minimality of r and the linear independence of the v'_i imply that $\gamma(x'_i) = x'_i$. Thus all $x'_i\in k$; hence $\sum_{i=1}^r v'_i\otimes x'_i = \big(\sum_{i=1}^r v'_i x'_i\big)\otimes 1 = 0$, and we get a contradiction. $\square$

Consequence. $\dim_k(V')^\Gamma \leq \dim_{k'}(V')$.

Claim. It is bijective.

Proof. It is enough to prove this when $d := \dim_{k'} V'$ is finite, because every finite dimensional k'-subspace of V' is contained in a Γ-invariant one. Choose a basis $v'_1, ..., v'_d$ of V' over k' and consider the surjective $k'[\Gamma]$-linear map

$$\varphi' : \ W' := k'[\Gamma]^{\oplus d} \to V', \ \Big(\sum_\gamma x'_{i,\gamma}[\gamma]\Big)_i \mapsto \sum_{i,\gamma} x'_{i,\gamma} \cdot \gamma(v'_i).$$

Then the short exact sequence

$$0 \to \ker(\varphi') \to W' \to V' \to 0$$

induces a left exact sequence

$$0 \to \ker(\varphi')^\Gamma \to (W')^\Gamma \to (V')^\Gamma.$$

Now observe that $k'[\Gamma]$ is a free $k[\Gamma]$-module; hence W' is one. Therefore

$$\dim_k(W')^\Gamma = \frac{\dim_k W'}{|\Gamma|} = \frac{[k'/k] \cdot |\Gamma| \cdot d}{|\Gamma|} = d|\Gamma|.$$

On the other hand, the above Consequence applied to $\ker(\varphi')$ shows that

$$\dim_k \ker(\varphi')^\Gamma \leq \dim_{k'} \ker(\varphi') = d(|\Gamma| - 1).$$

Thus the left exactness implies that $\dim_k(V')^\Gamma \geq d|\Gamma| - d(|\Gamma| - 1) = d$. This plus the injectivity shows the bijectivity. □

This finishes the proof of Theorem 11.2. □

Note. The functor (11.1), and hence the equivalence in Theorem 11.2, is compatible with the tensor product (over k, respectively over k'). Therefore, it extends to an equivalence for vector spaces with any additional multilinear structures, such as that of an algebra or a Hopf-algebra (over k, resp. k'), together with the appropriate homomorphisms. In particular we deduce:

Theorem 11.3. The base change functor $X \mapsto X \times_k k'$ induces an equivalence from the category of affine schemes over k to the category of affine schemes over k' together with a covering action by Γ. The same holds for the categories of affine group schemes, or of finite group schemes.

Note. By going to the limit over finite Galois extensions we deduce the same for any infinite Galois extension k'/k with profinite Galois group Γ, provided that the action of Γ on an affine scheme over k' is continuous, in the sense that the stabilizer of every regular function is an open subgroup of Γ.

§12 Étale group schemes

Let k^{sep} denote a separable closure of k.

Proposition 12.1. A finite group scheme G is étale iff $G_{k^{\text{sep}}}$ is constant.

Proof. By definition a morphism of schemes is étale if and only if it is smooth of relative dimension zero, i.e., if it is flat of finite type and the sheaf of relative differentials vanishes. Since k is a field, G is automatically flat over k; hence it is étale if and only if $\Omega_{G/k} = 0$. As the formation of $\Omega_{G/k}$ is invariant under base change, this is equivalent to $\Omega_{G_{k^{\text{sep}}}/k^{\text{sep}}} = 0$. This in turn means that $G_{k^{\text{sep}}}$ is reduced with all residue fields separable over k^{sep}. But k^{sep} is separably closed; hence it is equivalent to saying that $G_{k^{\text{sep}}} \cong \coprod \operatorname{Spec} k^{\text{sep}}$ as a scheme. The group structure on $G_{k^{\text{sep}}}$ then corresponds to the group structure on $G(k^{\text{sep}})$ as in §5, yielding a natural isomorphism

$$G_{k^{\text{sep}}} \cong \underline{G(k^{\text{sep}})}_{k^{\text{sep}}}.$$

□

Theorem 12.2. The functor $G \mapsto G(k^{\text{sep}})$ defines an equivalence from the category of finite étale group schemes over k to the category of continuous finite $\mathbb{Z}[\operatorname{Gal}(k^{\text{sep}}/k)]$-modules.

Proof. By the remark after Theorem 11.3 the base change functor $G \mapsto G_{k^{\text{sep}}}$ induces an equivalence from the category of étale finite group schemes over k to the category of étale finite group schemes over k^{sep} together with a continuous covering action by $\operatorname{Gal}(k^{\text{sep}}/k)$. Proposition 12.1 implies that the latter is equivalent to the category of continuous finite Galois-modules. □

§13 The tangent space

Let $G = \operatorname{Spec} A$ be a finite commutative group scheme over k, and denote by $T_{G,0}$ the tangent space at the unit element 0.

Proposition 13.1. There is a natural isomorphism of k-vector spaces

$$T_{G,0} \cong \operatorname{Hom}(G^*, \mathbb{G}_{a,k}),$$

where k acts on the right hand side through $\mathbb{G}_{a,k}$.

Proof. The tangent space $T_{G,0}$ is naturally isomorphic to the kernel of the restriction map

$$G(\operatorname{Spec}(k[t]/(t^2)) \longrightarrow G(\operatorname{Spec} k).$$

This is the set of k-algebra homomorphisms $A \to k[t]/(t^2) \cong k \oplus t\,k$ whose first component is the counit ϵ. Such a homomorphism has the form $\varphi = \epsilon + t\lambda$ for a homomorphism of k-vector spaces $\lambda\colon A \to k$, and the relations $\varphi(ab) = \varphi(a)\varphi(b)$ and $\varphi(e(1)) = 1$ making φ a homomorphism of k-algebras translate into the relations $\lambda(ab) = \lambda(a)\epsilon(b) + \epsilon(a)\lambda(b)$ and $\lambda(e(1)) = 0$. In dual terms we get the set of $\lambda \in A^*$ such that $\mu^*(\lambda) = \lambda \otimes \epsilon^*(1) + \epsilon^*(1) \otimes \lambda$ and $e^*(\lambda) = 0$. But giving an element $\lambda \in A^*$ is equivalent to giving the homomorphism of k-algebras $k[T] \to A^*$ sending T to λ, which in turn corresponds to a morphism $\ell : G^* = \operatorname{Spec} A^* \to \mathbb{A}^1_k$. The first condition on λ then amounts to saying that ℓ is a group homomorphism, and the second condition to $\ell(0) = 0$. But the latter is already a consequence of the former. This proves the bijectivity; the k-linearity is left to the reader. □

Theorem 13.2. All finite commutative group schemes over a field of characteristic zero are étale.

Proof. Without loss of generality we can assume that k is algebraically closed. Then the translation action of $G(k)$ on G is transitive. Therefore it is enough to prove étaleness at 0, that is, $T_{G,0} = 0$. By Proposition 13.1 we must show that any homomorphism $G^* \to \mathbb{G}_{a,k}$ vanishes. Since its image is a finite subgroup scheme of $\mathbb{G}_{a,k}$, it suffices to show that any finite subgroup scheme $H \subset \mathbb{G}_{a,k}$ vanishes.

For any such H, the group $H(k)$ is a finite subgroup of $\mathbb{G}_{a,k}(k)$, the additive group of k. Since this is a $\mathbb{Q}$-vector space, it contains no non-zero finite subgroup; hence $H(k) = 0$. Thus H is purely local, i.e. $H = \operatorname{Spec} k[X]/(X^n)$ for some $n \geq 1$. The fact that H is a subgroup scheme means that the comultiplication $X \mapsto X \otimes 1 + 1 \otimes X$ on $k[X]$ induces a homomorphism $k[X]/(X^n) \longrightarrow k[X]/(X^n) \otimes_k k[X]/(X^n)$. This means that

$$(X \otimes 1 + 1 \otimes X)^n \;=\; \sum_{m=1}^{n} \binom{n}{m} \cdot X^m \otimes X^{n-m} \;\in\; (X^n \otimes 1, 1 \otimes X^n).$$

Here all binomial coefficients are non-zero in k, because k has characteristic zero. Thus $n = 1$ and hence $H = 0$, as desired. □

Proposition 13.3. For any field k of characteristic $p > 0$, the finite group scheme $\boldsymbol{\alpha}_{p,k} = \operatorname{Spec} k[X]/(X^p) \subset \mathbb{G}_{a,k}$ is simple.

Proof. Any proper subgroup scheme $H \subset \boldsymbol{\alpha}_{p,k}$ has the form $\operatorname{Spec} k[X]/(X^n)$ for some $n < p$. Thus all binomial coefficients $\binom{n}{m}$ are non-zero in k for $0 < m < n$, so as in the preceding proof we deduce that $n = 1$ and $H = 0$. □