Tsinghua 2010 **Abelian Varieties** Problem Set 3

Let k be a field.

1. Let G be an abstract finite group, and $\underline{G} = \mathrm{Spec}(R)$ be the constant group scheme over k which associates to each k-scheme S the group G.

(i) Show that there exists a basis $(e_\sigma)_{\sigma\in G}$ of R over k such that the multiplication of R is given by

$$e_\sigma e_\tau = \begin{cases} e_\sigma & \text{if } \sigma = \tau, \\ 0 & \text{otherwise.} \end{cases}$$

(ii) Find the formula for the comultiplication $m^*(e_\sigma)$.

(iii) Assume G is commutative. Describe explicitly the algebra of the Cartier dual of $\underline{G}$.

2. Let G, $\underline{G}$ be as in Problem 1, $X = \mathrm{Spec}(A)$ be an affine scheme of finite type over k, and $\mu : \underline{G} \times X \to X$ be an action of $\underline{G}$ on X. So each $\sigma \in G$ gives an automorphism $\sigma : X \to X$. We denote by $\sigma^* : A \to A$ the induced automorphism on A.

(i) Show that for any $f \in A$, we have

$$\mu^*(f) = \sum_{\sigma\in G} e_\sigma \otimes \sigma^*(f) \in R \otimes A.$$

(ii) For any $f \in A$, let $P_f(T)$ denote the characteristic polynomial of the multiplication by $\mu^*(f)$, *i.e.*, $P_f(T) = N_{(R\otimes A)[T]/A[T]}(1 \otimes T - \mu^*(f))$. Show that

$$P_f(T) = \prod_{\sigma\in G} (T - \sigma^*(f)).$$

3. Let $G = \mathrm{Spec}(R)$ be a connected finite group scheme over k of order p^h (*i.e.*, R is a local Artin k-algebra with residue field k and $\dim_k(A) = p^h$), $X = \mathrm{Spec}(A)$ be an affine k-scheme of finite type equipped with an action of G: $\mu : G \times X \to X$.

(i) Show that for any $f \in A$, we have $\mu^*(f) = 1 \otimes f + g$ with $g \in \mathfrak{m}_R \otimes A$, where $\mathfrak{m}_R$ is the maximal ideal of R.

(ii) Show there exists a basis $(e_i)_{1\leq i\leq p^h}$ of R over k such that, for any $f \in A$, the matrix of the multiplication by $1 \otimes T - \mu^*(f) \in R \otimes A[T]$ under the basis $(e_i \otimes 1)_{1\leq i\leq p^h}$ is lower triangular with all the diagonal entries equal to $T - f$. (Hint: note that there is an integer $m \geq 0$ such that $\mathfrak{m}_R^{m+1} = 0$ since R is an Artin ring.)

(iii) Show that one has $P_f(T) = (T - f)^{p^h}$ for any $f \in A$.

4. Assume k is algebraically closed of characteristic 2. Let E be an elliptic curve over k defined by the affine Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and with origin at the infinity point $(0 : 1 : 0)$.

(i) Show that we can't have $a_1 = a_3 = 0$ (as E is non-singular).

(ii) Show that a point $P = (x_0, y_0) \in E(k)$ has order 2 if and only if $ax_0 + a_3 = 0$. (Hint: P has order 2 if and only if the tangent line of E at P passes through the infinity point.)

(iii) Assume $E[2](k) = 0$. Show that, up to change of variables, E is isomorphic to the elliptic curve of equation $y^2 + y = x^3$.