PACIFIC JOURNAL OF MATHEMATICS
Vol. 32, No. 2, 1970

FORMS OF THE AFFINE LINE AND ITS ADDITIVE GROUP

PETER RUSSELL

Let k be a field, X_0 an object (e.g., scheme, group scheme) defined over k. An object X of the same type and isomorphic to X_0 over some field $K \supset k$ is called a form of X_0. If k is not perfect, both the affine line $\mathbf{A}^1$ and its additive group $\mathbf{G}_a$ have nontrivial sets of forms, and these are investigated here. Equivalently, one is interested in k-algebras R such that $K \otimes_k R \cong K[t]$ (the polynomial ring in one variable) for some field $K \supset k$, where, in the case of forms of $\mathbf{G}_a$, R has a group (or co-algebra) structure $s: R \to R \otimes_k R$ such that $(K \otimes s)(t) = t \otimes 1 + 1 \otimes t$. A complete classification of forms of $\mathbf{G}_a$ and their principal homogeneous spaces is given and the behaviour of the set of forms under base field extension is studied.

If k is perfect, all forms of $\mathbf{A}^1$ and $\mathbf{G}_a$ are trivial, as is well known (cf. 1.1). So assume k is not perfect of characteristic $p > 0$. Then a nontrivial example (cf. [5], p. 46) of a form of $\mathbf{G}_a$ is the subgroup of $\mathbf{G}_a^2 = \operatorname{Spec} k[x, y]$ defined by $y^p = x + ax^p$ where $a \in k$, $a \notin k^p$. We show that this example is quite typical (cf. 2.1): Every form of $\mathbf{G}_a$ is isomorphic to a subgroup of $\mathbf{G}_a^2$ defined by an equation $y^{p^n} = a_0x + a_1x^p + \cdots + a_mx^{p^m}$, $a_i \in k$, $a_0 \neq 0$. Analyzing the equivalence relation induced on the right hand side polynomials by isomorphism of the groups which they define, we obtain a description of the set of forms of $\mathbf{G}_a$ split by $k^{p^{-n}}$ as, essentially, the quotient of an infinite direct sum of copies of k/k^{p^n} under a certain group action (cf. 2.5).

If G is a nontrivial form of $\mathbf{G}_a$, we show that $\operatorname{End}_k G$ is a finite field (cf. 3.1). This allows one to compute the set of k_s/k-forms of G (k_s a separable algebraic closure of k) using Golois cohomology. This set is nontrivial in general, in contrast to the same situation for $\mathbf{G}_a$.

A form X of $\mathbf{A}^1$ may fail to have a group structure for two reasons. First, and this is the serious failure, X_{k_s} may not have enough (i.e., infinitely many) automorphisms. As an example, with the identity as the only automorphism, one may take $\mathbf{P}^1 - \{q\}$, where $\mathbf{P}^1$ is the projective line and q is a purely inseparable point of degree $p^n > 2$. The general case here seems to be rather complex. Secondly, X_{k_s} may have enough automorphisms, but X may not have a rational point. We show that then X is a principal homogeneous space for a form of $\mathbf{G}_a$ (cf. 4.1). This gives a new interpretation of a result of Rosenlicht ([4], p. 10, theorem) on curves with exceptionally many automorphisms (cf. 4.2).

1. Throughout this paper k will be a fixed base field, $\bar{k}$ an algebraic closure of k, $k_i = k^{p^{-\infty}}$ ($p = \operatorname{char} k$) the perfect and k_s the separable closure of k in $\bar{k}$. Reference to k will usually be omitted.

It is well known (cf. [5], p. 34 and [6], p. 108) that a form G of $\mathbf{G}_a$ is split by k_i, that is, $G_{k_i} \cong \mathbf{G}_{a k_i}$. The same is true for forms X of $\mathbf{A}^1$. For the sake of completeness, and to establish some notation, we briefly outline the argument. The idea is to investigate the complete regular curve P determined by X. As a matter of terminology, we call a scheme Y regular if all its local rings are regular, and nonsingular if Y_K is regular for any $K \supset k$. As is well known, Y_K nonsingular implies Y nonsingular, and Y is nonsingular if and only if $Y_{k^{p^{-1}}}$ is regular. The existence of forms of $\mathbf{A}^1$ is closely connected with the divergence of these notions if k is not perfect. If Y is a curve, we denote by $\tilde{Y}_K$ the regular curve obtained by normalizing Y_K.

LEMMA 1.1. *Let X be a form of $\mathbf{A}^1$ and $P \supset X$ a complete regular curve.*

(i) *$P - X$ is a point purely inseparable over k.*

(ii) *There is a unique minimal field $k' \supset k$ such that $X_{k'} \cong \mathbf{A}^1_{k'}$, and k' is purely inseparable of finite degree over k.*

Proof. The genus of $\tilde{P}_{k_i}$ is zero since this is so after suitable base field extension and since, k_i being perfect, the genus does not change under base field extension (cf. [1], V, § 5, Th. 5). Since $\tilde{P}_{\bar{k}}$ has a rational point, $\tilde{P}_{\bar{k}} \cong \mathbf{P}^1_{\bar{k}}$. An open subscheme of $\mathbf{P}^1_K$ (K any field) is a form of $\mathbf{A}^1_K$ if and only if it is the complement of a purely in separable point. Hence $\tilde{P}_{\bar{k}} - X_{\bar{k}}$ is a point, and a fortiori $P - X$ (resp. $P_{k_i} - X_{k_i}$) is a point purely inseparable over k (resp. rational over k_i). In particular, $\tilde{P}_{k_i} \cong \mathbf{P}^1_{k_i}$ and $X_{k_i} \cong \mathbf{A}^1_{k_i}$. If $K \supset k$ is any field such that $X_K \cong \mathbf{A}^1_K$, then $\tilde{P}_K - X_K$ is a point rational over K and K contains (up to unique isomorphism) the residue field k_1 of $P - X$. Now pass to X_{k_1} and continue this process. After finitely many steps, we reach a field $k' \subset K$, $k \subset k' \subset k_i$, such that $\tilde{P}_{k'} \cong \mathbf{P}_{k'}$, and $\tilde{P}_{k'} - X_{k'}$ is rational over k'. Then $X_{k'} \cong \mathbf{A}^1_{k'}$.

$\mathbf{A}^1 = \operatorname{Spec} k[t]$ admits, up to choice of origin, a unique group structure (given by $s(t) = t \otimes 1 + 1 \otimes t$ if the origin is at $t = 0$), and any automorphism of $\mathbf{A}^1$ sending the origin to the origin is a group homomorphism. Let G and G' be groups with origins q and q' and ψ an isomorphism of the underlying schemes, supposed to be forms of $\mathbf{A}^1$, such that $\psi(q) = q'$. Then ψ is a homomorphism of groups after base field extension, which means that a certain diagram of morphisms (over k) commutes after base extension and so is commutative to begin with. Hence ψ is an isomorphism of groups. This gives:

LEMMA 1.2. *Let X be a form of $\mathbf{A}^1$. Then any group scheme G with underlying scheme X is a form of $\mathbf{G}_a$. The group structure (if it exists) is unique up to choice of origin. If $X_K \cong \mathbf{A}^1_K$, then $G_K \cong \mathbf{G}_{aK}$.*

We assume from now on that char $k = p > 0$. We denote by Θ^n the base change functor deduced from

$$\begin{aligned} \varphi^n \colon k &\longrightarrow k \\ a &\longmapsto a^{p^n} . \end{aligned}$$

For any scheme X there is a canonical morphism $F^n_X \colon X \to \Theta^n X$. If X is a group scheme, so is $\Theta^n X$ and F^n_X is a homomorphism. Referring to [3], p. I. 1–5 for more details, we remark only that if $X = \operatorname{Spec} R$ is affine, then $\Theta^n X = \operatorname{Spec}((k, \varphi^n) \otimes_k R)$ where $(k, \varphi^n) = k$ considered as a right k-algebra via φ^n and as a left k-algebra in the usual way, and that F^n_X is deduced from

$$\begin{aligned} F^n_R \colon (k, \varphi^n) \otimes_k R &\longrightarrow R \\ a \otimes x &\longmapsto a x^{p^n} . \end{aligned}$$

Θ^n accomplishes, up to isomorphism, the same as the base change $k \subset k^{p^{-n}}$. More precisely, if K is purely inseparable of exponet $\leqq n$ over k (that is, $K^{p^n} \subset k$), there is a commutative diagram

$$\begin{array}{ccc} k & \longrightarrow & K \\ {\scriptstyle \varphi^n}\big\downarrow & \swarrow{\scriptstyle \bar\varphi} & \\ k & & \end{array}$$

and we have $\Theta^n X \cong (k, \bar\varphi) \otimes_K X_K$ for any scheme X over k.

LEMMA 1.3. *Let X be a form of $\mathbf{A}^1$. For any integer $n \geqq 0$, F^n_X is a purely inseparable morphism of degree p^n. For any morphism $\psi \colon X \to Y$ of finite degree, there is a unique factorization $\psi = \bar\psi F^m_X$ where p^m is the inseparable degree of ψ and $\bar\psi$ is a separable morphism. Finally, there is an integer $n \geqq 0$ such that $\Theta^n X \cong \mathbf{A}^1$.*

Proof. The last statement follows from 1.1 and the remark above. The function field $\kappa(X)$ of X is separable of transcendence degree one over k and so has, for each n, a unique subfield $\supset k$ over which it is purely inseparable of degree p^n, namely

$$k(\kappa(X)^{p^n}) \cong (k, \varphi^n) \otimes_k \kappa(X) = \kappa(\Theta^n X)$$

(cf. [2], p. 186, Th. 19 and p. 179, corollary). This proves the first statement and the second follows in view of the fact that $\Theta^m X$ is normal.

1.4. Let X be a form of $\mathbf{A}^1$. We let $n(X)$ be the least n such that $\Theta^n X \cong \mathbf{A}^1$ or, equivalently, the least n such that X has a splitting field of exponent n over k.

The point of 1.3 is that the affine ring R of X has a unique maximal subring of the form $S = k[x]$ such that $R^{p^n} \subset S$ for som n, and that the only other subrings with this property are the rings $k[x^{p^m}]$, $m \geqq 0$. Note, however, that $n(X)$ need not be the least n such that $\kappa(\Theta^n X) \cong k(t)$ or, equivalently, that $\Theta^n X \subset \mathbf{P}^1$. $Y = \mathbf{P}^1 - \{q\}$, q purely inseparable and not rational over k, is one example and, giving Y some further twist, one can find X such that $\Theta^n X \cong Y$ and $n > 1$.

2. Since $\mathbf{G}_a$ is defined over the prime field, we may identify $\mathbf{G}_a$ and $\Theta\mathbf{G}_a$. Then $F = F_{\mathbf{G}_a} \in A = \mathrm{Hom}_k(\mathbf{G}_a, \mathbf{G}_a)$. It is well known that $A = k[F]$, a ring of noncommutative polynomials with relations $Fa = a^p F$ for $a \in k$. We define the power series ring $\hat{A} = k[[F]]$ in the same way. Let $\varepsilon: A \rightarrow k$ be the natural augmentation. We let $A^* = \varepsilon^{-1}(k^*)$ and $A^{**} = \varepsilon^{-1}(1)$ and make corresponding definitions for $\hat{A}$. As in the case of ordinary power series, $\hat{A}^*$ is the group of units of $\hat{A}$. By truncation we obtain groups $U_n = \hat{A}^*/\hat{A}F^n \cong A^*/AF^n$. $\tau = \sum_{i=0}^m a_i F^i \in A$, $a_m \neq 0$, has degree p^m as a morphism $\tau: \mathbf{G}_a \rightarrow \mathbf{G}_a$, and we also give it degree p^m in the graded ring $k[F]$. Note that $A^* \subset A$ is the subset of separable homomorphisms. An endomorphism $\lambda: k \rightarrow k$ commutes with p-th powers and so extends to an endomorphism $\lambda: A \rightarrow A$

$$\sum a_i F^i \longmapsto \sum \lambda(a_i) F^i .$$

In the particular case $\lambda = \varphi^n$ we put $\lambda(\tau) = \tau^{(n)}$ for $\tau \in A$ and $\lambda(A) = A^{(n)}$. $\tau^{(n)}$ is characterized by $F^n \tau = \tau^{(n)} F^n$.

If $G = \mathrm{Spec}\, R$ is an affine group with group operation $s: R \rightarrow R \otimes_k R$, $\mathrm{Hom}_k(G, \mathbf{G}_a)$ may be identified with

$$\{r \mid s(r) = r \otimes 1 + 1 \otimes r\} \subset R \cong \mathrm{Hom}\,(k[t], R) .$$

In particular, A is identified with the set of p-polynomials

$$f(t) = a_0 t + a_1 t^p + \cdots + a_m t^{p^m} \in k[t] .$$

THEOREM 2.1. *Let G be a form of $\mathbf{G}_a$. Then G is isomorphic to a subgroup* $\mathrm{Spec}\, k[x, y]/I$ *of* $\mathbf{G}_a^2 = \mathrm{Spec}\, k[x, y]$ *where I is generated by a polynomial $y^{p^n} - (a_0 x + a_1 x^p + \cdots + a_m x^{p^m})$, $a_0 \neq 0$. Equivalently, G is a fiber product*

$$\begin{array}{ccc} G & \xrightarrow{\xi} & \mathbf{G}_a \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\tau} \\ \mathbf{G}_a & \xrightarrow[F^n]{} & \mathbf{G}_a \end{array}$$

where $\tau = a_0 + a_1F + \cdots + a_mF^m \in A^*$. *Conversely, any* G *defined that way is a form of* $\mathbf{G}_a$.

Proof. Let $G = \operatorname{Spec} R$, $s\colon R \to R \otimes_k R$ the group operation,

$$\bar{s}\colon (k, \varphi^n) \otimes_k R \longrightarrow (k, \varphi^n) \otimes_k R \otimes_k R \cong ((k, \varphi^n) \otimes_k R) \otimes_k ((k, \varphi^n) \otimes_k R)$$

the induced group operation for $\Theta^n G$. By 1.3, we have $\Theta^n G \cong \mathbf{G}_a$ for some n, so that $(k, \varphi^n) \otimes_k R \cong k[t]$ where we can choose t such that $\bar{s}(t) = t \otimes 1 + 1 \otimes t$. Write $t = \sum a_i \otimes y_i$ with $a_i \in k$ and $y_i \in R$. Then

$$\begin{aligned} \bar{s}(t) = t \otimes 1 + 1 \otimes t &= \textstyle\sum a_i \otimes y_i \otimes 1 + \sum a_i \otimes 1 \otimes y_i \\ &= \textstyle\sum \bar{s}(a_i \otimes y_i) = \sum a_i \otimes s(y_i)\ . \end{aligned}$$

If we choose the a_i linearly independent in k considered as a vector space over k via φ^n, i.e., linearly independent over k^{p^n}, this implies $s(y_i) = y_i \otimes 1 + 1 \otimes y_i$. Hence the $y_i\,(1 \otimes y_i)$ define homomorphisms $\eta_i\colon G \to \mathbf{G}_a$ $(\Theta^n\eta_i\colon \mathbf{G}_a \to \mathbf{G}_a)$. As observed above, this implies $1 \otimes y_i = f_i(t)$ where f_i is a p-polynomial. Applying F_R^n and putting $x = F_R^n(t)$, we obtain $y_i^{p^n} = f_i(x)$. Clearly the y_i generate R over k and one of them, call it y, is a separating variable for $\kappa(G)$. Then $y^{p^n} = f(x) = a_0x + a_1x^p + \cdots + a_mx^{p^m}$, with $a_0 \neq 0$ since x is separable over $k(y)$. This shows that $k[x, y] \subset R$ is integrally closed. $\kappa(G)$ is separable and purely inseparable over $k(x, y)$, so $k(x, y) = \kappa(G)$ and $R = k[x, y]$. This proves the first statement. The next follows letting η be the homomorphism corresponding to y and $\xi = F_G^n$ the homomorphism corresponding to x. Finally, let $R = k[x, y]$ where $y^{p^n} = f(x)$. Then $s\colon R \to R \otimes_k R$, $s(x) = x \otimes 1 + 1 \otimes x$, $s(y) = y \otimes 1 + 1 \otimes y$, is well defined and gives a group structure on R. Taking $a_0 = 1$ for simplicity, we have

$$1 \otimes x = (1 \otimes y^{p^{n-1}} - (a_1^{p^{n-1}} \otimes x + \cdots + a_m^{p^{n-1}} \otimes x^{p^{m-1}}))^p = t_1^p$$

in $(k, \varphi^n) \otimes_k R$. Replacing $1 \otimes x$ by t_1^p on the right hand side and continuing that way, we find $t \in (k, \varphi^n) \otimes_k R$ such that $1 \otimes x = t^{p^n}$ and $1 \otimes y^{p^n} = (f(t))^{p^n}$. Spec R is nonsingular, so $(k, \varphi^n) \otimes_k R$ is reduced. Hence $1 \otimes y = f(t)$, showing that $(k, \varphi^n) \otimes_k R = k[t]$.

2.2. We write $G = (F^n, \tau)$ (with $\tau \in A^*$) for a fiber product as in the theorem. Note that G can be so written if and only if $\Theta^n G \cong \mathbf{G}_a$.

PROPOSITION 2.3. *Let $G = (F^n, \tau), G_1 = (F^{n_1}, \tau_1)$ and assume $n_1 \leqq n$. Then $G \cong G_1$ if and only if there exist elements $\rho \in A^*, \sigma \in A$ and $c \in k^*$ such that*

$$\tau_1^{(n-n_1)} = (\rho^{(n)}\tau + F^n\sigma)c^{-1} .$$

ρ may be chosen of degree $\leqq p^{n-1}$.

Proof. The monomorphism $(\xi, \eta): G \to \mathbf{G}_a^2$ induces an epimorphism of A-modules $A \oplus A = \operatorname{Hom}_k(\mathbf{G}_a^2, \mathbf{G}_a) \to \operatorname{Hom}_k(G, \mathbf{G}_a)$ (cf. [6], p. 102, proposition). Hence $\operatorname{Hom}_k(G, \mathbf{G}_a) = A\eta + A\xi$ with $F^n\eta = \tau\xi$ as a defining relation. Since G is reduced and irreducible, $\operatorname{Hom}_k(G, \mathbf{G}_a)$ is torsion free.

Let $\psi: G \to G_1$ be an isomorphism and consider the commutative diagram

$$\begin{tikzcd}
G \arrow[dr, "\psi"] \arrow[drr, "\xi'"] \arrow[ddr, "\eta'"'] & & \\
& G_1 \arrow[r, "\xi_1"'] \arrow[d, "\eta_1"] & \mathbf{G}_a \arrow[d, "\tau_1"] \\
& \mathbf{G}_a \arrow[r, "F^{n_1}"'] & \mathbf{G}_a
\end{tikzcd}$$

Now $\eta' = \eta_1\psi = \rho\eta + \sigma\xi$ for some $\rho, \sigma \in A$, and we must have $\rho \in A^*$ since η' is separable. Also, if $\rho = \rho_1 + \rho_2F^n$, then $\rho\eta = \rho_1\eta + \rho_2\tau\xi$. So we can choose ρ of degree $< p^n$. Assume first $n = n_1$. Then $\xi' = \xi_1\psi$ is purely inseparable of degree p^n. By 1.3, $\xi_1\psi = c\xi$ with $c \in A$ a separable and purely inseparable homomorphism, that is, $c \in k^*$. Now

$$\begin{aligned}\tau_1\xi_1\psi = F^n\eta_1\psi &= F^n\rho\eta + F^n\sigma\xi = \rho^{(n)}F^n\eta + F^n\sigma\xi \\ &= (\rho^{(n)}\tau + F^n\sigma)\xi = (\rho^{(n)}\tau + F^n\sigma)c^{-1}\xi_1\psi ,\end{aligned}$$

giving $\tau_1 = (\rho^{(n)}\tau + F^n\sigma)c^{-1}$. Conversely, define $\xi', \eta' \in \operatorname{Hom}(G, \mathbf{G}_a)$ by $\xi' = c\xi$ and $\eta' = \rho\eta + \sigma\xi$. Then $F^n\eta' = \tau_1\xi'$, and we obtain a homomor phism $\psi: G \to G_1$ such that $\xi' = \xi_1\psi$ and $\eta' = \eta_1\psi$. Now ρ is invertible in $\hat{A}$ and we can write $\rho^{-1} = \rho_1 + \sigma_2F^n$ with $\rho_1 \in A^*$. Then $\tau = (\rho_1^{(n)}\tau_1 + F^n\sigma_1)c$ with $\sigma_1 = (\sigma_2\rho^{(n)}\tau - \rho_1\sigma)c^{-1} \in A$. Reversing the roles of G and G_1 we get $\psi_1: G_1 \to G$ inverting ψ.

Suppose now $n - n_1 = n_2 \geqq 0$. In the commutative diagram

$$\begin{tikzcd}
G^1 \arrow[r, "\xi_1"] \arrow[d, "\eta_1"'] & \mathbf{G}_a \arrow[r, "F^{n_2}"] \arrow[d, "\tau_1"] & \mathbf{G}_a \arrow[d, "\tau_1^{(n_2)}"] \\
\mathbf{G}_a \arrow[r, "F^{n_1}"'] & \mathbf{G}_a \arrow[r, "F^{n_2}"'] & \mathbf{G}_a
\end{tikzcd}$$

both the left and right square are cartesian. So the big square is cartesian, and consequently $G_1 = (F^n, \tau_1^{(n_2)})$. Now the previous argument applies.

Since $(F^n, \tau) \cong (F^n, \tau\varepsilon(\tau)^{-1})$, any G can be written with $\tau \in A^{**}$. This normalizes τ to some extent:

COROLLARY 2.3.1. *Let $G = (F^n, \tau)$. Then $G \cong \mathbf{G}_a$ if and only if $\tau c \in A^{(n)}$ for some $c \in k^*$. If $\tau = 1 + a_1 F + \cdots + a_m F^m \in A^{**}$, then $k' = k(a_1^{p^{-n}}, \cdots, a_m^{p^{-n}})$ is the minimal splitting field for G.*

Proof. Since $\mathbf{G}_a = (F^n, 1)$, the proposition gives $\tau c = \rho^{(n)} + F^n\sigma \in A^{(n)}$ if $G \cong \mathbf{G}_a$. Conversely, let $\tau c = \tau_1^{(n)}$. Then $\tau_1 \in A^*$ and we can write $1 = \rho\tau_1 + \sigma F^n$. So $1 = (\rho^{(n)}\tau + F^{(n)}\sigma c^{-1})c$ and $(F^n, 1) \cong (F^n, \tau)$. This proves the first statement, and the second follows since we can take $c = 1$ above if $\tau \in A^{**}$.

COROLLARY 2.3.2. *Let $G = (F^n, \tau)$ and $0 \leqq m \leqq n$. Then*

$$\Theta^m G = (F^{n-m}, \tau) .$$

Proof. Apply Θ^m to the cartesian square defining G. Noting that $\Theta^m \tau = \tau^{(m)}$, we get $\theta^m G = (F^n, \tau^{(m)}) \cong (F^{n-m}, \tau)$.

2.4. For any field $K \supset k$, we define $E(K)$ as the set of isomorphism classes of forms of $\mathbf{G}_{aK}$ and put $E(K, n) = \{G \in E(K) \mid \Theta^n G \cong \mathbf{G}_{aK}\}$.

The rule $(\rho, \sigma, c)\cdot\tau = (\rho^{(n)}\tau + F^n\sigma)c^{-1}$ defines an action of

$$A^* \times A \times k^* ,$$

endowed with a suitable semi-direct product structure, on A^*, and 2.3 states that $E(k, n)$ may be considered as the quotient of A^* under this action. A^* is not a group, but this inconvenience can be avoided by dividing out by A first and passing to the group $U_n = A^*/AF^n$. Let $V_n = U_n \times k^*$. Then the map

$$(*) \qquad \begin{aligned} V_n \times A^*/F^nA &\longrightarrow A^*/F^nA \\ (\bar{\rho}, c) \times \bar{\tau} &\longmapsto (\rho^{(n)}\tau c^{-1})^- \end{aligned}$$

(where $^-$ denotes taking residue classes) is well defined and gives an action of V_n on A^*/F^nA. Clearly all the operations involved are compatible with base field extension. Now 2.3 implies:

THEOREM 2.5. *The map*

$$\begin{aligned} A^* &\longrightarrow E(k, n) \\ \tau &\longmapsto (F^n, \tau) \end{aligned}$$

induces a bijection between the quotient of A^*/F^nA by the action (*) defined above and $E(k, n)$. This identification is compatible with base field extension.

Similarly, we can define an action

$$U_n \times A^{**}/F^nA \longrightarrow A^{**}/F^nA \text{ by } \bar{\rho}\cdot\bar{\tau} = (\rho^{(n)}\tau\varepsilon(\rho)^{-p^n})^- .$$

Since any G can be written as $G = (F^n, \tau)$ with $\tau \in A^{**}$, the quotient may again be identified with $E(k, n)$. As an example, let us work out the case $n = 1$. Choose a complementary subspace W_0 for k^p in k and for each $i \geqq 1$ let W_i be a copy of W_0. Then $U_1 = k^*$ acts on $W = \bigoplus_{i=1}^{\infty} W_i$ by $c\cdot\sum a_i = \sum c^{p(1-p^i)}a_i$. Letting $(F, 1 + \sum a_iF^i)$ correspond to the class of $\sum a_i$, one identifies $E(k, 1)$ and W/k^*.

Let $A^*/F^{n+1}A \to A^*/F^nA$ be the natural map and define $V_{n+1} \to V_n$ by $\overline{(\rho, c)} \mapsto \overline{(\rho^{(1)}, c)}$. Then

$$\begin{array}{ccc} V_{n+1} \times A^*/F^{n+1}A & \longrightarrow & A^*/F^{n+1}A \\ \downarrow & & \downarrow \\ V_n \times A^*/F^nA & \longrightarrow & A^*/F^nA \end{array}$$

commutes and it follows from 2.3.2 that the induced map on the quotients is $\Theta\colon E(k, n + 1) \to E(k, n)$. Unfortunately there does not seem to be a coherent way to reverse the vertical arrows in order to obtain the inclusion $E(k, n) \subset E(k, n + 1)$.

PROPOSITION 2.6. *Let $K \supset k$ be a field and*

$$\begin{aligned} \Psi\colon E(k) &\longrightarrow E(K) \\ G &\longmapsto G_K \end{aligned}$$

the natural map.

(i) *If K is purely inseparable over k, then Ψ is surjective.*

(ii) *If k is algebraically closed in K and K is separable over k, then Ψ is injective.*

Proof. (i) Let $G = (F^n, \tau) \in E(K)$, $\tau = 1 + a_1F + \cdots + a_mF^m$. There is an integer $r \geqq 0$ such that $a_i^{p^r} = \alpha_i \in k$, $i = 1, \cdots, m$. Let $\tau' = 1 + \alpha_1F + \cdots + \alpha_mF^m$ and $G' = (F^{n+r}, \tau') \in E(k)$. Then $\tau' = \tau^{(r)}$ over K and 2.3 implies $G'_K = (F^{n+r}, \tau^{(r)}) \cong (F^n, \tau) = G$.

(ii) Let $G = (F^n, \tau)$, $\tau = 1 + \sum a_iF^i \in A$, $\rho = \sum x_iF^i \in A_K^*$ with $x_i = 0$ for $i \geqq n$, *and* $\sigma = \sum y_iF^i \in A_K$. Suppose $(\rho^{(n)}\tau + F^n\sigma)x_0^{-p^n} = 1 + \sum b_iF^i = \tau' \in A$, that is,

$$(*) \qquad \Big(\sum_{j=0}^{i-1} x_j^{p^n} a_{i-j}^{p^j} + x_i^{p^n} + y_{i-n}^{p^n}\Big)x_0^{-p^{n+i}} = b_i \in k$$

for $i \geqq 1$. (Set $y_i = 0$ for $i < 0$). We have to show that the same can be done with $x_i, y_i \in k$. We may clearly assume $G \not\cong \mathbf{G}_a$. Then not all $a_i \in k^{p^n}$ and there is an $r \geqq 1$ such that $a_1, \cdots, a_{r-1} \in k^{p^n}$ but $a_r \notin k^{p^n}$. If $r > 1$, we can replace τ by $(1 - a_1 F)\tau$ (since $a_1 \in k^{p^n}$) which has a zero linear term. By an obvious induction argument, we can assume $a_1 = \cdots = a_{r-1} = 0$. Then $(*)$ gives (for $i = r$)

$$a_r x_0^{p^n - p^{n+r}} + x_r^{p^n} x_0^{-p^{n+r}} + y_{r-n}^{p^n} x_0^{-p^{n+r}} = b_r \, .$$

Put $u = x_0^{-1}$, $v = x_r x_0^{-p^r}$ if $r < n$ (and so $y_{r-n} = 0$), and $v = y_{n-r} x_0^{-p^r}$ if $r \geqq n$ (and so $x_r = 0$). In both cases $a_r u^{(p^r - 1)p^n} + v^{p^n} = b_r$. Extracting p-th roots in k from a_r and b_r as far as possible, we can write $a u^{(p^r-1)p^{n_1}} + v^{p^{n_1}} = b$ where not both a and b are in k^p and $n_1 \geqq 1$ (since $a_r \notin k^{p^n}$). If $u \notin k$, then u is transcendental over k, $a u^{(p^r-1)p^{n_1}} - b + v^{p^{n_1}}$ is irreducible in $k(u)[v]$, but becomes reducible upon adjoining $a^{p^{-1}}$ and $b^{p^{-1}}$ to k. This shows that $k(u, v) \subset K$ is not separable, contradicting the separability of K. Hence $x_0 = u^{-1} \in k$. Taking $(*)$ first with $i = 1, \cdots, n-1$, we see that $x_i \in k$, and then $y_{i-n} \in k$ follows for $i \geqq n$.

The proof above suggests examples showing that the assumptions in (ii) cannot be weakened. First, let $k = k_0(a, b)$ with a, b algebraically independent over k_0. Then $G = (F, 1 + aF)$ and $G' = (F, 1 + bF)$ are not isomorphic over k. On the other hand, we can define $K = k(u, v)$ by $a u^{p(p-1)} - b + v^p = 0$. One checks that k is algebraically closed in K. But now $1 + bF = u^{-p}(1 + aF)u^p + Fv$, so that $G_K \cong G'_K$. Next, suspose k contains elements a and c such that $a \notin k^p$ and $c \notin k^{q-1}$ where $q = p^m > 2$. Let $G = (F^m, 1 + aF^m)$, $G' = (F^m, 1 + c^q a F^m)$. If $K \supset k$, then $G_K \cong G'_K$ if and only if $a u^{q(q-1)} + v^q = c^q a$ has a solution with u, $v \in K$. If K is separable over k, then $a \notin K^p$, so necessarily $v = 0$ and $u^{q-1} = c$. This is possible over a finite separable extension of k but not over k. We will see below that this example is typical (cf. 3.1.1.).

3. Let G and G_1 be forms of $\mathbf{G}_a$ written as fiber products

$$\begin{array}{ccc} G & \xrightarrow{\xi} & \mathbf{G}_a \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\tau} \\ \mathbf{G}_a & \xrightarrow[F^n]{} & \mathbf{G}_a \end{array} \qquad \text{and} \qquad \begin{array}{ccc} G_1 & \xrightarrow{\xi_1} & \mathbf{G}_a \\ {\scriptstyle\eta_1}\downarrow & & \downarrow{\scriptstyle\tau_1} \\ \mathbf{G}_a & \xrightarrow[F^{n_1}]{} & \mathbf{G}_a \end{array}$$

with $n = n(G)$ and $n_1 = n(G_1)$ (cf. 1.4). Suppose $\psi \in \mathrm{Hom}_k(G, G_1)$ is nonzero. Then $\Theta^n\psi\colon \mathbf{G}_a \to \Theta^n G_1$ is nonzero, and since a nonzero homomorphic image of $\mathbf{G}_a$ is isomorphic with $\mathbf{G}_a$ (cf. [6], p. 101, lemma), we must have $n_2 = n - n_1 \geqq 0$. Now $F^{n_2}\xi_1\psi$ has inseparable degree $\geqq p^n$ and therefore factors through ξ. This gives a commutative diagram

$$\begin{tikzcd}
G \arrow[rr, "\xi"] \arrow[d, "\psi"'] & & \mathbf{G}_a \arrow[d, "\tau_2 = \Theta^n \psi"] \\
G_1 \arrow[r, "\xi_1"] \arrow[d, "\eta_1"'] & \mathbf{G}_a \arrow[r, "F^{n_2}"] \arrow[d, "\tau_1"] & \mathbf{G}_a \arrow[d, "\tau_1^{(n_2)}"] \\
\mathbf{G}_a \arrow[r, "F^{n_1}"'] & \mathbf{G}_a \arrow[r, "F^{n_2}"'] & \mathbf{G}_a .
\end{tikzcd}$$

If ψ is separable, so are τ_2 and $\tau_1^{(n_2)}\tau_2$. This shows that one can use the big square to define G as a fiber product, that is, $G \cong (F^n, \tau_1^{(n_2)}\tau_2)$. By 2.3 there exist $\rho \in A^*$ and $\sigma \in A$ such that

$$(*) \qquad \tau_1^{(n_2)}\tau_2 = \rho^{(n)}\tau + F^n\sigma .$$

(No c appears since ξ is left unchanged.) Conversely, if τ_2 satisfies $(*)$, there is a unique ψ making the diagram commutative. So separable homomorphisms $\psi: G \to G_1$ are in one-to-one correspondence with those $\tau_2 \in A^*$ for which a solution to $(*)$ exists.

THEOREM 3.1. *Let G be a form of $\mathbf{G}_a$, $G \not\cong \mathbf{G}_a$. Then $\mathrm{End}_k G$ may be identified with a finite subfield of k. If $\mathrm{End}_{k_s} G_{k_s} = \mathbf{F}_q$ and $k \subset K \subset k_s$, then $\mathrm{End}_K G_K = K \cap \mathbf{F}_q$.*

Proof. Let $G = (F^n, \tau)$, $n = n(G)$, and suppose $\psi: G \to G$ is nonzero. If ψ is not separable, there is a nonzero homomorphism $\Theta G \to G$. Since $n(\Theta G) < n(G)$, this is impossible, as we have seen. So ψ is separable and $\tau_2 = \Theta^n\psi$ satisfies a relation

$$(*) \qquad \tau\tau_2 = \rho^{(n)}\tau + F^n\sigma , \qquad \rho \in A^*, \sigma \in A .$$

We will assume, as we may, that $\deg \rho < p^n$. Since Θ^r, $r \geqq 0$, is a faithfully flat base change functor, $\Theta^r: \mathrm{End}_k \mathrm{G} \to \mathrm{End}_k \Theta^r G$ is injective and moreover $\Theta^r\psi$ is a monomorphism (epimorphism) if and only if ψ is. Taking $r = n - 1$, we see that it is enough to prove the first statement in case $n = 1$. We can then choose $\rho = a \in k^*$ and $\tau = 1 + a_1F^{m_1} + \cdots + a_sF^{m_s}$ with $1 \leqq m_1 < m_2 < \cdots < m_s$ and $a_i \notin k^p$. Let $\tau_2 = c_0 + c_1F + \cdots + c_rF^r$, $c_0 \neq 0$ and $c_r \neq 0$. Comparing coefficients in $(*)$, we get $a_sc_r^{p^{m_s}} \in k^p$ unless $r = 0$. Since $m_s \geqq 1$ and $a_s \notin k^p$, we actually have $r = 0$ and $\tau_2 = c_0 = c \in k^*$. $(*)$ now reduces to $a^p\tau - \tau c \in FA$, and this gives $a^p - c = 0$ and $(c - c^{p^{m_i}})a_i \in k^p$, $i = 1, \cdots, s$. Since $a_i \notin k^p$, this implies $c - c^{p^{m_i}} = 0$. Or, equivalently, $c - c^{p^m} = 0$ where m is the greatest common divisor of $m_1, \cdots, m_s$. Conversely $\tau c = c\tau$ for such c and if $c \neq 0$, it lifts to an automorphism of G. Hence $\mathrm{End}_k G = k \cap \mathbf{F}_{p^m}$ in this case.

Now let $n \geqq 1$, $\mathbf{F}_q = \mathrm{End}_{k_s} G_{k_s}$, $k \subset K \subset k_s$ and $\tau_2 = c \in K \cap \mathbf{F}_q^*$. To show that $c \in \mathrm{End}_K G_K$, we have to solve $(*)$ with $\rho, \sigma \in A_K$. However there exists a solution over k_s, and applying to it a K-automorphism λ of k_s, we get $\tau c = \lambda(\tau c) = \lambda(\rho^{(n)}) + F^n\lambda(\sigma)$ and $0 = (\rho^{(n)} - \lambda(\rho^{(n)}))\tau + F^n(\sigma - \lambda(\sigma))$. Multiplying by τ^{-1} (in $\hat{A}_K$), we have $0 = (\rho^{(n)} - \lambda(\rho^{(n)})) + F^n(\sigma - \lambda(\sigma))\tau^{-1}$, giving $\rho^{(n)} = \lambda(\rho^{(n)})$ and $\sigma = \lambda(\sigma)$ since $\deg \rho < p^n$. Hence $\rho, \sigma \in A_K$.

The theorem states that the automorphism functor of G coincides with the functor μ_r (r-th roots of unity, $r = q - 1$ prime to p) on separable algebraic extensions of k. Galois cohomology therefore gives (for details we refer to [8], in particular I, § 5, II, § 1 and III, § 1):

COROLLARY 3.1.1. *Let $E(k_s/k, G)$ be the set of k_s/k-forms of G. Then $E(k_s/k, G) = H^1(k, \mathbf{F}_q^*) \cong k^*/k^{*q-1}$.*

4. We turn now to forms of $\mathbf{A}^1$ that fail to be groups by just the absence of a rational point.

PROPOSITION 4.1. *Let X be a form of $\mathbf{A}^1$ and suppose that X_{k_s} admits a group structure. Then X is a principal homogeneous space for a form G of $\mathbf{G}_a$ determined uniquely by X. Moreover, $X = \mathrm{Spec}\, k[x, y]/I$, $G = \mathrm{Spec}\, k[u, v]/J$ where I and J are generated respectively by $y^{p^n} - b - f(x)$ and $v^{p^n} - f(u)$ with $b \in k$ and f a separable p-polynomial. Conversely, if X and G are defined as above, then X is a principal homogeneous space for G.*

Proof. Let $X = \mathrm{Spec}\, R$. As in the proof of 2.1, we have $(k, \varphi^n) \otimes_k R \cong k[t]$ for some n, $t = \sum a_i \otimes y_i$ with $a_i \in k$ linearly independent over k^{p^n}, and $y_i^{p^n} = g_i(x) \in k[x]$ with $x = F_R^n(t)$. Let $q \in X_{k_s}$ be rational over k_s and let $c_i \in k_s$ be the residue of y_i at q. Put $y'_i = y_i - c_i$, $t' = t - \sum a_i c_i^{p^n} = t - c$ and $x' = x - c$. Then $t' = \sum a_i \otimes y'_i$, q lies above the point $t' = 0$ of $\mathbf{A}^1_{k_s} \cong \Theta^n X_{k_s}$ and we can choose q as the origin of the group structure supposed to exist on X_{k_s}. The a_i remain linearly independent over $k_s^{p^n}$ and we have $y'^{p^n} = f_i(x')$ with f_i a p-polynomial as in the proof of 2.1. Hence $g_i(x) = y_i^{p^n} = b_i + f_i(x)$ with $b_i = c_i^{p^n} - f_i(c)$, and $g_i(x) \in k[x]$ implies $b_i \in k$ and $f_i(x) \in k[x]$. If y is a separating variable for $\kappa(X)$ picked from the y_i, we get $y^{p^n} = b + f(x)$ where f has nonzero linear term. As before, this implies $R = k[x, y]$. Let $G = \mathrm{Spec}\, S$, $S = k[u, v]$ with $v^{p^n} = f(u)$. Then $\alpha\colon R \to R \otimes_k S$, $\alpha(x) = x \otimes 1 + 1 \otimes u$ and $\alpha(y) = y \otimes 1 + 1 \otimes v$, defines an action of G on X. $\bar{\alpha}\colon R \otimes_k R \to R \otimes_k S$ defined by $\bar{\alpha}(w \otimes z) = (w \otimes 1)\alpha(z)$ is an isomorphism and gives an isomorphism (over X) $G \times_k X \xrightarrow{\sim} X \times_k X$. Hence X is a principal homogeneous space for G. If this is also true for G_1, we get an isomorphism (over X) $G \times_k X \xrightarrow{\sim} G_1 \times_k X$. Applying 2.6 (ii) to the fiber over the generic point of X, we see that $G \cong G_1$.

Principal homogeneous spaces for G are clasified by $H^1(k, G)$ (cf. [8], I, Proposition 33). Let $G = (F^n, \tau)$. Then there is a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker \eta & \longrightarrow & G & \xrightarrow{\eta} & \mathbf{G}_a & \longrightarrow & 0 \\ & & \wr\downarrow & & \xi\downarrow & & F^n\downarrow & & \\ 0 & \longrightarrow & \ker \tau & \longrightarrow & \mathbf{G}_a & \xrightarrow[\tau]{} & \mathbf{G}_a & \longrightarrow & 0\,. \end{array}$$

The exact cohomology sequence and $H^1(k, \mathbf{G}_a) = 0$ give $H^1(k, G) = k/f(k) + k^{p^n}$, where f is the p-polynomial corresponding to τ. The Galois group of the spliting field of $0 = b + f(x) = b + a_0x + \cdots + a_m x^{p^m}$, $a_0 \neq 0$, is isomorphic to a subgroup of $f^{-1}(0) \subset k_s$. Hence $f(k) = k$ if k has no normal extension of degree p, and $H^1(k, G) = 0$ for all forms G of $\mathbf{G}_a$ in that case. The author does not know whether the converse of this statement is true if k is not perfect.

In [4] Rosenlicht characterized curves that are "exceptional" in the sense that the genus g is $\geqq 1$ and the group of automorphisms (leaving a point fixed if $g = 1$) is infinite. We give another characterization, already implicit in [4], p. 10, theorem, assuming the exceptional case over k_s only.

THEOREM 4.2. *Let P be a complete regular curve such that P_{k_s} is exceptional. Then P has exactly one singular point q, q is purely inseparable over k, and $X = P - \{q\}$ is a principal homogeneous space for a form of $\mathbf{G}_a$.*

Proof. It is enough to prove the first statement in case $k = k_s$. It is then taken directly from [4], p. 5, lemma. It is also shown there that $\tilde{P}_{k_i}$ has genus zero. Hence $X = P - \{q\}$ is a form of $\mathbf{A}^1$ and we have $F_X^n\colon X \rightarrow \Theta^n X \cong \mathbf{A}^1 = \operatorname{Spec} k[t]$ for some n. This gives an injection $\Theta^n\colon \operatorname{Aut}_k X \rightarrow \operatorname{Aut}_k \mathbf{A}^1$. Now let $k = k_s$. It then follows from [4], loc. cit., that $\operatorname{Aut}_k X$ has an infinite subset of automorphisms operating without fixed point. Hence $\Theta^n(\operatorname{Aut}_k X)$ contains infinitely many translations $t \mapsto t + b$. With notations as in the proof of 4.1, write $t = \sum a_i \otimes y_i$, $1 \otimes y_i = f_i(t)$, with t so chosen that the point $q_0 \in X$ above $t = 0$ is rational. If c_i is the residue of y_i at q_0, we have $f_i(0) = c_i^{p^n} \in k^{p^n}$. Since $0 = \sum a_i f_i(0)$, we get $f_i(0) = 0$. If T_b is the automorphism of X inducing $t \mapsto t + b$, we have $t + b = \sum a_i \otimes T_b^*(y_i)$. Let $b_i \in k$ be the residue of y_i at $T_b(q_0)$. Then $b = \sum a_i b_i^{p^n}$ and $t + b = \sum a_i \otimes (y_i + b_i)$. Hence $T_b^*(y_i) = y_i + b_i$ and $f_i(t + b) = 1 \otimes T_b^*(y_i) = f_i(t) + b_i^{p^n}$. With $t = 0$, this shows $b_i^{p^n} = f_i(b)$. Since this holds for infinitely many b, each f_i is a p-polynomial. Hene X has a group structure (over k_s) and 4.1 applies.

If X is a principal homogeneous space for a form G of $\mathbf{G}_a$ and $P \supset X$ a complete regular curve, then $G(k_s) \subset \mathrm{Aut}_{k_s} P_{k_s}$ is infinite. So P_{k_s} is exceptional if the genus g of P is positive. The cases $g = 0$ as well as $g = 1$ can be settled completely. Excluding the trivial case $X = \mathbf{A}^1$, we have: If $g = 0$, then $\operatorname{char} k = 2$. If $g = 1$, then $\operatorname{char} k = 3$. Moreover, $X = \operatorname{Spec} k[\mathrm{x}, y]/I$ where I is generated by $y^p - b - x - ax^p$ with $p = 2$ or 3 respectively and $a, b \in k$.

It is enough to prove the corresponding statement for the groups G that are involved, that is, we may assume $X = G$ has a rational point. Now, by a theorem of Tate ([9], Corollary 2), the genus changes by a multiple of $1/2(p-1)$ on passage from X to θX. On the other hand, if $\mathcal{O}$ is the local ring of $P - X$, the genus change is $\dim_k \mathcal{O}_1/\mathcal{O}'$ where $\mathcal{O}' = (k, \varphi) \otimes_k \mathcal{O}$ and $\mathcal{O}_1$ is the normalization of $\mathcal{O}'$ (cf. [7], p. 73, example). So a drop in genus occurs unless $\mathcal{O}$ is nonsingular. But then P is nonsingular, so $g = 0$ and $P \cong \mathbf{P}^1$. Excluding the case $G = \mathbf{G}_a$ we must have $\mathbf{P}^1 - G$ of degree 2 (cf. [5], p. 35 or the remark in the introduction). Hence $p = 2$ and $n(G) = 1$. If $p > 2$, we see that $g \geqq 1/2n(G)(p-1)$. So $g = 1$ implies $n(G) = 1$ and $p = 3$. In both cases ($g = 0$ or 1) $G = \operatorname{Spec} k[x, y]$ with $y^p = x + a_1x^p + \cdots + a_m x^{p^m}$ and $a_m \notin k^p$ (cf. 2.1). Using [9], proposition, one checks that then $g = 1/2(p-1)(p^m - 2)$. So necessarily $m = 1$.

References

1. C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Math. Surv. VI, New York, 1951.

2. N. Jacobson, *Lectures in abstract algebra*, vol. III, D. Van Nostrand Co., Princeton, 1964.

3. F. Oort, *Commutative group schemes*, Lecture Notes in Mathematics 15, Springer, Berlin, 1965.

4. M. Rosenlicht, *Automorphisms of function fields*, Trans. Amer. Math. Soc. **79** (1955), 1-11.

5. ———, *Some rationality questions on algebraic groups*, Annali di Mat. (IV) **43** (1957), 25-50.

6. ———, Questions of rationality for solvable algebraic groups over nonperfect fields, Annali di mat., (IV) **61** (1963), 97-120.

7. J. P. Serre, *Groupes Algébriques et Corps de Classes*, Hermann, Paris, 1959.

8. ———, *Cohomologie Galoisienne*, Lecture Notes in Mathematics 5, Springer, Berlin, 1964.

9. J. Tate, *Genus change in inseparable extensions of function fields*, Proc. Amer. Math. Soc. **3** (1952), 400-406.

Received May 16, 1969. This research was supported in part by the U. S. Army Research Office (Durham).

HARVARD UNIVERSITY