COMPOSITIO MATHEMATICA

PETER RUSSELL

Simple Galois extensions of two-dimensional affine rational domains

Compositio Mathematica, tome 38, nº 3 (1979), p. 253-276
<http://www.numdam.org/item?id=CM_1979__38_3_253_0>

COMPOSITIO MATHEMATICA, Vol. 38, Fasc. 3, 1979, pag. 253–276

SIMPLE GALOIS EXTENSIONS OF TWO-DIMENSIONAL AFFINE RATIONAL DOMAINS

Peter Russell

Introduction

Let k be a field and $B = k^{[2]}$. (If R is a ring, we write $R^{[n]}$ for the polynomial ring in n variables over R.) Let $A \subset B$, where A is an affine factorial k-algebra. It was shown in [5] (under some mild additional restrictions on A) that if $B = A[t]$ with $t \in \mathrm{qt}(A)$ (the field of quotients of A), then $A \simeq k^{[2]}$. D. Wright [9] proved that this is true also if $t^n \in \mathrm{qt}(A)$ with t lying in some extension field of $\mathrm{qt}(A)$ and $n > 1$. We in turn extend the ideas of [5] and [9] to show: *Suppose $B = A[t]$ is a simple extension of A and Galois over A in the sense that $G = \mathrm{Aut}_A B$ is finite and $\mathrm{qt}(B^G) = \mathrm{qt}(A)$. Then $A \simeq k^{[2]}$.* (The restrictions on A mentioned above are again needed. See 2.4 for a precise statement.) Let us note that the results of [5] and [9] as well as [7] have been generalized in another direction in [6].

The proof of the above result breaks up naturally into two steps:

(i) Classification of actions by a finite group G on B such that B is a simple extension of B^G. It turns out that G fixes a variable in B and $B^G \simeq k^{[2]}$. This we show in section 1. (The argument is quite brief if card G is prime to char k and somewhat involved otherwise.)

(ii) Analysis of $A \subset B^G \subset B$ with $\mathrm{qt}(A) = \mathrm{qt}(B^G)$. One finds $A \simeq k^{[2]}$ by an argument very close to the one used to settle the birational case in [5]. This is done in section 2.

As in [5], [6], [7] and [9] one derives, in a by now familiar way, consequences concerning the *cancellation problem* for $k^{[2]}$ and the *problem of embedded planes* from our main result. This is the content of section 3.

Using techniques from [6] we prove the following results in section

0010-437X/79/03/0253-24 $00.20/0

4: *Let K be a locally factorial Krull domain and $F \in B \simeq K^{[2]}$ such that for each prime $P \subset K$ the canonical image of F in $K_P \otimes_K B/P(K_P \otimes_K B) \simeq (K_P/PK_P)^{[2]}$ is a variable. Then F is a variable in B.* As a consequence of this and the results of section 1 we can settle a further special case of cancellation for $k^{[2]}$: *Let k be a locally factorial Krull domain and A a k-algebra such that $A^{[1]} \simeq A[T] = k[X, Y, Z] \simeq k^{[3]}$ with $Z \in A[T^n]$ for some $n > 1$ invertible in k. Then $A \simeq k^{[2]}$.*

As a matter of notation, by a statement $A \simeq K^{[n]}$ we always mean that K is (in an obvious way) a subring of A and A is K-isomorphic with $K^{[n]}$.

I would like to acknowledge the hospitality and lively mathematical environment of Bhaskaracharya Pratishtana of Poona, India, which I enjoyed during the preparation of this paper.

1.

Let k be a commutative ring, B a k-algebra and $G \subset \mathrm{Aut}_k B$ a finite subgroup. Put

$$A = B^G = \{b \in B \mid \varphi(b) = b \quad \text{for all } \varphi \in G\}.$$

Suppose B is a simple extension of A, say $B = A[t]$ with $t \in B$. Then any $b \in B$ can be written

$$b = a_0 + a_1 t + \cdots + a_m t^m$$

with $a_i \in A$. Let $\varphi \in G$. Then

$$\psi(b) - b = a_1(\varphi(t) - t) + \cdots + a_m(\varphi(t^m) - t^m)$$

and we deduce the following basic fact:

(1.1) For all $b \in B$ and $\varphi \in G$,

$$\varphi(b) - b \in (\varphi(t) - t)B.$$

The next point is an immediate consequence of (1.1). The situation described will arise numerous times in the sequel.

(1.2) Let $K \subset B$ be a subring such that $B = K[t']$ for some $t' \in B$.

Let $\psi \in G$ such that $K \subset B^{\psi}$ and $t' \notin B^{\psi}$. Then $B^{\psi}[t'] = B = B^{\psi}[t]$ and $\psi(t) - t = u(\psi(t') - t')$ with $u \in B^*$.

REMARK: If R is a ring, we denote by R^* the group of units and by R^+ the additive group of R.

(1.3) Let $G_c = \{\varphi \in G \mid \varphi(t) - t \in k\}$. Then

(i) G_c is a subgroup of G.

(ii) The map $\varphi \mapsto \varphi(t) - t$ identifies G_c with a subgroup of k^+. Hence $G_c = \{1\}$ if char $k = 0$ and $G_c \simeq (Z/pZ)^n$ for some n if char k is a prime $p > 0$.

(1.4) If $\varphi \in G$ and $\varphi(b) - b \in k^*$ for some $b \in B$, then $\varphi(t) - t \in k^*$ and $\varphi \in G_c$.

In 1.5 and 1.6 we collect some more or less well known facts about additive polynomials. The proofs are included for the convenience of the reader.

(1.5) Let K be a domain of characteristic exponent p and $H \subset K^+$ a finite subgroup. Put

$$f_H(T) = \prod_{h \in H} (T - h).$$

Then $f_H(T)$ is a monic p-polynomial in T, that is

$$f_H(T) = T^{p^n} + a_{n-1}T^{p^{n-1}} + \cdots + a_0 T$$

with $a_i \in K$ and $p^n = \text{card } H$. In particular, $f_H(T)$ is *additive* i.e., if R is any K-algebra and $T_1, T_2 \in R$, then

$$f_H(T_1 + T_2) = f_H(T_1) + f_H(T_2).$$

(Note $f_H(T) = T$ if char $k = 0$.)

PROOF: We may assume $p > 1$. Let $h \in H$. Then $\Pi_{0 \le i \le p-1} (T - ih) = T^p - Th^{p-1}$. This proves the result in case card $H = p$. If card $H > p$, we can write $H = H_1 \oplus H_2$ with card $H_i <$ card H, $i = 1, 2$.

One finds

$$f_H(T) = f_{H'}(f_{H_2}(T)),$$

with $H' = f_{H_2}(H_1)$. By induction on card H, $f_{H'}$ and f_{H_2} are p-polynomials. Hence, so is f_H.

(1.6) LEMMA: *Let K be a field of characteristic $p > 0$, $H \subset K^+$ a finite subgroup and*

$$\rho \colon H \to K^+$$

a homomorphism. Then there exists a unique additive polynomial $f(T) \in K[T]$ such that

$$\deg f < \operatorname{card} H \quad \textit{and} \quad f(h) = \rho(h) \quad \textit{for all } h \in H.$$

PROOF: Let $H' \subsetneq H$ and suppose $f'(T)$ is additive of degree $<$ card H' such that $f(h) = \rho(h)$ for $h \in H'$. Let $h_0 \in H - H'$, $c = \rho(h_0) - f'(h_0)$ and $d = f_{H'}(h_0)$. Note $d \neq 0$. Put $f = f' + (c/d)f_{H'}$. Then $f(h) = \rho(h)$ for $h \in H'' = H' \oplus \langle h_0 \rangle$ and $\deg f \leq \deg f_{H'} = \operatorname{card} H' <$ card H''. Induction on card H now establishes the existence of f. Uniqueness is obvious.

(1.7.1) LEMMA: *Let K be a domain, $B \simeq K^{[1]}$ and $G \subset \operatorname{Aut}_K B$ a finite subgroup. Then there exists a finite cyclic subgroup $W \subset K^*$, a finite subgroup $H \subset K^+$ stable under multiplication by elements of W and $T \in B$ with $B = K[T]$ such that*

$$G = \{\varphi \in \operatorname{Aut}_K B \mid \varphi(T) = wT + h, \quad w \in W, h \in H\}.$$

PROOF: Let $B = K[X]$ and $\varphi \in G$. Then $\varphi(X) = a_\varphi X + b_\varphi$ with $a_\varphi \in K^*$ and $b_\varphi \in K$. The map

$$\pi \colon G \to K^*$$
$$\varphi \mapsto a_\varphi$$

is a homomorphism and $W = \pi(G)$ is a finite, hence cyclic, subgroup of K^*. If $W = \{1\}$, set $T = X$. Otherwise, choose $\psi \in G$ such that $w = a_\psi$ generates W and put $T = X + (w-1)^{-1}b_\psi$. Then $\psi(T) = wT$ and clearly G is the semi-direct product of $\langle \psi \rangle \simeq W$ and Ker $\pi \simeq H = \{a_\varphi \mid \varphi \in \operatorname{Ker} \pi\} \subset K^+$ with W operating on H by multiplication.

(1.7.2) COROLLARY: *Put $r = \operatorname{card} W$. Then $B^G = K[v]$ with $v = f_H(T)^r$.*

PROOF: Let $q = \operatorname{card} H$. Since W operates on H by multiplication, we have $q - 1 \equiv 0 \bmod r$ and $w^q = w$ for any $w \in W$. Also,

$$\prod_{\varphi \in G} \varphi(T) = \prod_{w \in W} \prod_{h \in H} w(T + w^{-1}h) = \prod_{w \in W} w f_H(T) = \pm f_H(T)^r.$$

Hence $v \in B^G$. Now $B = K[T]$ is integral of degree rq over both $K[v]$ and B^G. Hence $B^G \subset R = \tilde{K}[v] \cap K[T]$ where $\tilde{K}$ is the integral closure of K, and it is easy to see that $R = K[v]$ since v is monic in T (see also lemma 2.6.1 of [6]).

Let k be a field, $p = \operatorname{char} k$ and $B \simeq k^{[2]}$ for the remainder of this section. We fix (for the moment) a system (x, y) of variables for B. If $\varphi \in \operatorname{Aut}_k B = GA_2$, we write

$$\varphi = (f_1, f_2)$$

to mean that φ is the k-homomorphism with $\varphi(x) = f_1 \in B$ and $\varphi(y) = f_2 \in B$. Put

$$AF_2 = \{\varphi \in GA_2 \mid \varphi = (f, g), \deg f = \deg g = 1\}$$

and

$$E_2 = \{\varphi \in GA_2 \mid \varphi = (ax + h(y), by + c), a, b \in k^*, c \in k, \quad h(y) \in k[y]\}.$$

(1.8) Let $G \subset GA_2$ be a finite subgroup. As is well known (see [4], theorem 3.3, for instance), GA_2 is the amalgamated product of its subgroups AF_2 and E_2. It follows that G is conjugate to a subgroup of AF_2 or E_2 (see [8]) or, which is the same, is a subgroup of AF_2 or E_2 after suitable choice of (x, y).

(1.9) LEMMA: *Let $B = [x, y]$ and suppose each $\varphi \in G$ is of the form*

$$\varphi = (x + a, y + b)$$

with $a, b \in k$. Then G fixes a variable in B, i.e., there exist x_1, y_1 such that $B = k[x_1, y_1]$ and $\varphi(x_1) = x_1$ for all $\varphi \in G$, if and only if $\operatorname{card} G \leq \operatorname{card} k$.

PROOF: Clearly $G \simeq G' = \{(a, b) \mid (x + a, y + b) \in G\} \subset k^+ \times k^+$. If, say, G fixes y, then $G' \subset k^+ \times \{0\}$ and $\operatorname{card} G \leq \operatorname{card} k$. We have to prove the converse.

Put $G_1 = \{\varphi \in G \mid \varphi(x) = x\}$. We can find $G_2 \subset G$ such that $G = G_1 \oplus G_2$. For $\varphi = (x + a, y + b) \in G_2$, b is uniquely determined by a and the map sending a to b is a homomorphism from G_2 to k^+. By 1.6 we can find an additive polynomial $f_1(x) \in k[x]$ such that $f_1(a) = b$ whenever $(x + a, y + b) \in G_2$. Let $y' = y - f_1(x)$. Then $\varphi(y') = y'$ for $\varphi \in G_2$ and $\psi(y') - y' \in k$ for any $\psi \in G$. Hence replacing y by y' we may assume $G_2 = \{\varphi \in G \mid \varphi(y) = y\}$.

We claim that there exists $d \in k$ such that $a - bd \neq 0$ for all $1 \neq \varphi = (x + a, y + b) \in G$. In fact, it is enough to choose $d \notin L = \{a/b \mid (x + a, y + b) \in G,\ b \neq 0\}$, and this is possible since $\operatorname{card} L \leq (\operatorname{card} G_1)\ (\operatorname{card} G_2 - 1) < \operatorname{card} G \leq \operatorname{card} k$. Replace x by $x' = x - dy$. Then b is determined by a whenever $\varphi = (x + a, y + b) \in G$ and we can find an additive polynomial $f_2(x)$ such that $f_2(a) = b$ as φ ranges over G. Now $y - f_2(x)$ is a variable fixed by G.

(1.10) LEMMA: *Let $B = k[x, y]$ and suppose $\epsilon, \eta \in G$, where*

$$\epsilon = (x, wy), \quad \eta = (x + g(y), y)$$

with $1 \neq w \in k^*$ and $0 \neq g(y) \in k[y]$. Then B is not a simple extension of $A = B^G$.

PROOF: We may assume that G is generated by ϵ and η. Suppose $B = A[t]$ with $t \in B$. Then it follows from 1.2 that $\eta(t) - t = d_1(\eta(x) - x) = d_1 g(y)$ for some $d_1 \in k^*$. Note order $\epsilon \neq p$ and hence $\epsilon(t) - t \notin k^*$ by 1.3. By 1.1, $\epsilon(t) - t \mid (w - 1)y$ and hence $\epsilon(t) - t = d_2 y$ with $d_2 \in k^*$. Now $\eta\epsilon(t) - t = \eta(\epsilon(t) - t) + \eta(t) - t = d_2 y + d_1 g(y)$, and $\eta\epsilon(t) - t \mid (w - 1)y$ by 1.1. Hence $g(y) = d_3 y$ with $d_3 \in k^*$. After replacing x by x/d_3 we may assume $d_3 = 1$. Then $G = \{(x + ay, wy) \mid w \in W,\ a \in H\}$, where $W \subset k^*$ and $H \subset k^+$ are finite subgroups with H stable under multiplication by elements of W.

Let $1 \neq \varphi = (x + ay, wy) \in G$. Then $\varphi(t) - t \notin k^*$ since $(0, 0)$ is a fixpoint for φ. By 1.1, $\varphi(t) - t$ divides $(w - 1)y$ and ay. Since $w \neq 1$ or $a \neq 0$, $\varphi(t) = t + d_\varphi y$ with $d_\varphi \in k$. Write $t = F_0 + F_1 + \cdots + F_m$ with $F_i \in k[x, y]$ homogeneous of degree i. Since φ is homogeneous, we have $\varphi(F_i) = F_i$ for $i \neq 1$ and $\varphi(F_1) = F_1 + d_\varphi y$. Since we are free to replace t by $t + c$ with $c \in B^G$, we may assume $t = F_1$, say $t = b_1 x + b_2 y$ with $b_1, b_2 \in k$. Then clearly $b_1 \neq 0$ and we may assume $b_1 = 1$. We put $b_2 = b$.

Let $G' = \{(x + ay, y) \mid a \in H\}$. G' is normal in G and $G/G' \simeq W$. Put

$$f(T, y) = \prod_{a \in H} (T + ay). \tag{1}$$

Then $f(T, y)$ *is homogeneous in* (T, y) *and* $f(T, y) = f_{Hy}(T)$ *in the terminology of* 1.5. Hence

$$f(T, y) = T^{p^n} + a_{n-1}T^{p^{n-1}}y^{p^n - p^{n-1}} + \cdots + a_0 T y^{p^n - 1} \tag{2}$$

with $a_i \in k$ and $p^n = \text{card } H$. Since H is stable under multiplication by elements of W,

$$\begin{aligned} f(T, wy) &= f(T, y) \quad \text{and} \\ f(wT, y) &= wf(T, y) \quad \text{for any } w \in W. \end{aligned} \tag{3}$$

In particular,

$$f(T, y) = g(T, y^r) \in k[T, y^r], \quad \text{where } r = \text{card } W. \tag{4}$$

Put $u = f(x, y)$ and $v = y^r$. Then $B^{G'} = k[u, y]$ and $B^G = k[u, v]$. (Both steps follow from 1.7.2 modulo some confusion in the notation.) The conjugates of t over $A = B^G$ are $\varphi(t) = x + (wb + a)y$, $w \in W$, $a \in H$. Making use of (2) and (3) we find

$$\begin{aligned} f(T - x - wby, y) &= f(T, y) - f(x, y) - f(wby, y) \\ &= g(T, v) - u - wy^{p^n}f(b, 1). \end{aligned}$$

Hence,

$$\begin{aligned} \Theta(u, v, T) &= \prod_{\varphi \in G} (T - \varphi(t)) \\ &= \prod_{w \in W} \prod_{a \in H} ((T - x - wby) - ay) \\ &= \prod_{w \in W} f(T - x - wby, y) \\ &= \prod_{w \in W} (g(T, v) - u - wy^{p^n}f(b, 1)). \end{aligned}$$

The constant term w.r.t. T of Θ is

$$\prod_{w \in W} ((-u) - wy^{p^n}f(b, 1)) = (-u)^r - f(b, 1)^r v^{p^n}$$

and the linear term is

$$\begin{aligned} a_0 T v^{(p^n - 1)/r} &\sum_{w \in W} \prod_{w' \neq w} ((-u) - w'f(b, 1)y^{p^n}) \\ &= r a_0 T v^{(p^n - 1)/r}(-u)^{r-1}. \end{aligned}$$

Clearly $k[u, v, t] \simeq k[u, v, T]/\Theta$. Hence, since $\min\{r, p^n\} > 1$ and $1 + ((p^n - 1)/r) + r - 1 > 1$, $u = v = t = 0$ is a singular point of $k[u, v, t] = B$, and we have reached a contradiction.

(1.11) THEOREM: *Let k be a field, $B = k^{[2]}$, G a finite subgroup of* $\mathrm{Aut}_k B$ *and $A = B^G$. Then $B = A[t]$ for some $t \in B$ if and only if G fixes a variable in B.*

PROOF: The "if" part of the theorem is obvious and we proceed to prove the "only if" part. By 1.8 we may assume $G \subset E_2$ or $G \subset AF_2$.

Case I: $G \subset E_2$.

Let $\varphi \in G$ and write

(1) $\varphi = (v_\varphi x + h_\varphi(y),\ w_\varphi y + a_\varphi)$ with $v_\varphi, w_\varphi \in k^*$, $a_\varphi \in k$ and $h_\varphi(y) \in k[y]$.

Then

(2) $v_\varphi \neq 1$ or $w_\varphi \neq 1$ implies order $\varphi \neq \operatorname{char} k = p$.

Let G_c be as in 1.3 and

(3) $$L = \{\varphi \in G \mid v_\varphi = w_\varphi = 1\}.$$

Then L is normal in G and $G_c \subset L$ by (2) and 1.3. If $\varphi = (x + h(y), y + a) \in L$, then $a \neq 0$ implies $\varphi \in G_c$ by 1.4. Hence $L = G_c \cup \{\varphi \in L \mid a_\varphi = 0\}$ and we have

(4) $G_c \subset L$ and either (i) $G_c = L$ or (ii) $a_\varphi = 0$ for all $\varphi \in L$.

(5) Let $\varphi \in G - L$. Then $\varphi(t) - t \notin k^*$ by (2) and 1.3 and $\varphi(t) - t$ divides both $(v_\varphi - 1)x + h_\varphi(y)$ and $(w_\varphi - 1)y + a_\varphi$ by 1.1.

Hence

(6) $v_\varphi \neq 1$ implies $w_\varphi = 1$ and $a_\varphi = 0$, $w_\varphi \neq 1$ implies $v_\varphi = 1$ and $(w_\varphi - 1)y + a_\varphi \mid h_\varphi(y)$.

Hence $G = \{\varphi \mid w_\varphi = 1\} \cup \{\varphi \mid v_\varphi = 1\}$ and it follows that

$$
(7) \qquad \begin{aligned} &w_\varphi \neq 1 \text{ for some } \varphi \in G \text{ implies } v_\psi = 1 \text{ for all } \psi \in G, \\ &v_\varphi \neq 1 \text{ for some } \varphi \in G \text{ implies } w_\psi = 1 \text{ for all } \psi \in G. \end{aligned}
$$

(I.1) Assume $v_\varphi \neq 1$ for some $\varphi \in G$. It follows from (6) and (7) that $w_\psi = 1$ and $a_\psi = 0$ for all $\psi \in G$. Hence G fixes y.

(I.2) Assume $v_\varphi = 1$ for all $\varphi \in G$. Suppose $\eta = (x + h(y),\ y + a) \in L$ with $a \neq 0$. We may then assume $a = 1$. Note that $L = G_c$ by (4). Suppose $a_m y^m$ appears in $h(y)$ with $m + 1 \not\equiv 0 \bmod p$. Replacing x by $x - (a_m/m + 1)y^{m+1}$ we eliminate the y^m-term from $h(y)$ without disturbing terms of higher degree or changing L. It is clear, therefore, that we may assume

$$\eta = (x + y^{p-1}h_1(y^p),\ y + 1)$$

with $h_1(y^p) \in k[y^p]$. Then

$$
\begin{aligned}
\eta^p &= \Big(x + \sum_{0 \le i \le p-1} (y + i)^{p-1} h_1(y^p + i),\ y\Big) \\
&= (x - h_1(y^p) + h_2(y),\ y)
\end{aligned}
$$

where only terms $b_j y^j$ with $j \not\equiv 0 \bmod p$ appear in $h_2(y)$. Since $\eta \in G_c$, $\eta^p = 1$ and we must have $h_1(y^p) = 0$, that is

$$\eta = (x,\ y + 1).$$

Let

$$G'_c = \{\psi \in G_c \mid h_\psi \in k\}$$

and

$$H = \{a_\psi \mid \psi \in G'_c\} \subset k^+.$$

Suppose $\epsilon = (x + h(y),\ y + a) \in G_c$ and $\epsilon \notin G'_c$. Then

$$(8) \qquad a \notin H.$$

In fact, suppose $\psi = (x + b,\ y - a) \in G'_c$ with $b \in k$. Then $\psi' = \psi\epsilon = (x + h_1(y),\ y) \in G_c$ with $h_1(y) = b + h(y - a)$ of positive degree. But $h_1 \mid \psi'(t) - t$ by 1.2, and this contradicts $\psi' \in G_c$.

Now $\psi\epsilon = \epsilon\psi$ for all $\psi \in G'_c$ and hence

$$h(y + a') = h(y) \quad \text{for all } a' \in H. \tag{9}$$

By 1.7.2, $h \in k[v]$ where $v = f_H(y)$ is an additive polynomial. We have $\epsilon(v) = f_H(y + a) = v + b$ with $b = f_H(a) \neq 0$ by (8). Replacing x by $x + g(v)$ with $g(v) \in k[v]$ we do not alter the representation of elements of G'_c since $f_H(a') = 0$ and hence $g(f_H(y + a')) = g(v)$ for $a' \in H$. Repeating the argument given above we may assume, therefore, that $h = 0$. Proceeding this way we obtain $L = G_c = G'_c$.

This discussion can be summarized as follows:

(10) After a suitable choice of variables L is of one of the following two types.
L1: There exists $\eta = (x, y + 1) \in L$ and every $\psi \in L$ is of the form $\psi = (x + h_\psi, y + a_\psi)$ with $a_\psi, h_\psi \in k$.
L2: $a_\psi = 0$ for all $\psi \in L$, that is L fixes y.

(I.2.1) Suppose $G = L$. If L is of type L1, then $G = G_c$ by (4) and G is isomorphic to a subgroup of k^+ by 1.3. Hence G fixes a variable by 1.9. If L is of type L2, then G fixes y.

(I.2.2) Suppose $G \supsetneqq L$. Let $W = \{w_\varphi \mid \varphi \in G\}$. W is a finite, hence cyclic, subgroup of k^* and $r = \text{card } W > 1$. Let

$$\varphi = (x + h(y), wy + a) \in G$$

such that w generates W. Replacing y by $y + (w-1)^{-1}a$ we may assume $a = 0$. Then $\varphi(t) = t + cy$ with $c \in k^*$ by (5) and $\varphi^r(t) = t + (1 + w + \cdots + w^{r-1})cy = t$, that is $\varphi^r = 1$. Since $\varphi^r = (x + \Sigma_{0 \le i \le r-1} h(w^i y), y)$, we have

$$\sum_{0 \le i \le r-1} h(w^i y) = 0. \tag{11}$$

(a) Assume L is of type L2.
Let $h = \Sigma\, b_j y^j$. Then by (11)

$$b_j \sum_{0 \le i \le r-1} w^{ij} = 0 \quad \text{for all } j. \tag{12}$$

If $g(y) = \Sigma\, c_j y^j$ and $x' = x + g(y)$, then $\varphi(x') = x' + \Sigma\, ((1 - w^j)c_j + b_j)y^j$. It follows from (12) that we can determine c_j such that $(1 - w^j)c_j + b_j = 0$ for all j. Replacing x by x' (this does not change the type of L) we may assume, therefore, that $\varphi = (x, wy)$. Then $L = \{1\}$ by 1.10 and G fixes x.

(b) Suppose L is of type L1.

Let $\psi = (x+b, y+a) \in L$. Then $\varphi\psi\varphi^{-1} = (x + b + h(y) - h(y + w^{-1}a), y + w^{-1}a) \in L$ and $h(y) - h(y + w^{-1}a) = c_1 \in k$. By induction on i,

$$\varphi^i\psi\varphi^{-i} = (x + b + c_1 + \cdots + c_i, y + w^{-i}a) \quad \text{with}$$

$$c_i = h(y) - h(y + w^{-i}a) \in k.$$

Let H be the subgroup of k^+ generated by $\{a_\psi w^i \mid i = 1, \ldots, r, \psi \in L\}$. It follows from the above that $h(y) - h(y+d) = c_d \in k$ for any $d \in H$, and clearly the map $d \mapsto c_d$ is a homomorphism on H. By 1.6 there exists an additive polynomial $f(y)$ such that $f(d) = c_d$ for $d \in H$. Let $h'(y) = h(y) - f(y)$. Then $h'(y+d) = h'(y)$ for $d \in H$ and $h'(y) = h_1(v) \in k[v]$ with $v = f_H(y)$ by 1.7.2. Since H is stable under multiplication by $w \in W$,

$$f_H(wy) = wf_H(y), \tag{13}$$

and since no term $b_m y^m$ with $m \equiv 0 \bmod r$ appears in f,

$$\sum_{0 \le i \le r-1} f(w^i y) = 0. \tag{14}$$

By (11), (13), and (14),

$$0 = \sum_{0 \le i \le r-1} h'(w^i y) = \sum_{0 \le i \le r-1} h_1(w^i v).$$

Arguing as in (a) we may assume, after replacing x by $x' = x + g_1(v)$ with suitable $g_1(v) \in k[v]$, that $h_1(v) = h'(y) = 0$. Again, this substitution does not change the type of L. In fact, if $\psi \in L$, then $a_\psi \in H$, so $f_H(a_\psi) = 0$ and $\psi(x') = x + b_\psi + g_1(f_H(y + a_\psi)) = x' + b_\psi$.

Since now h is an additive polynomial we can next change x to $x' = x + g_2(y)$, where $g_2(y)$ is additive, with the effect of making h vanish. Again this does not affect the type of L, for now $\psi(x') = x' + b'_\psi$ with $b'_\psi = b_\psi + g_2(a_\psi) \in k$.

Hence again $\varphi = (x, wy) \in G$. If $\psi = (x+b, y+a) \in L$ and $\varphi' = \varphi\psi = (x+b, wy+a)$, then order $\varphi' \neq p$, $\varphi'(t) - t \notin k^*$ and $\varphi'(t) - t \mid b$. Hence $b = 0$. So G fixes x.

Case II: $G \subset AF_2$.

Let $\varphi = (a_1x + b_1y + c_1,\ a_2x + b_2y + c_2) \in G$. If some eigenvalue of $M_\varphi = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}$ is not 1, then order $\varphi \neq p$ and $\varphi(t) - t \notin k^*$ by 1.3. On the other hand, $\varphi(t)-t$ divides both $l_1=(a_1-1)x+b_1y+c_1$ and $l_2=a_2x+(b_2-1)y+c_2$ by 1.1. Hence l_1 and l_2 are linearly dependent.

We conclude that for each $\varphi\in G$ one eigenvalue of M_φ is 1. Then the other is $\det M_\varphi\in k^*$, and one finds by a straightforward calculation that all M_φ can be simultaneously brought into lower triangular form by a linear change of variables. This brings us back to case I.

(1.11.1) COROLLARY: *Let the assumptions be as in* 1.11 *and let* $x_1\in B$ *be a variable fixed by* G. *Then there exists* $y_1\in B$ *such that* $B=k[x_1,y_1]$ *and* $G=G_1G_2$ *is a semi-direct product, where*

$$G_1=\{(x_1,y_1+h)\mid h\in H\}\simeq H,$$

$$G_2=\{(x_1,xy_1)\mid w\in W\}\simeq W$$

with W *and* H *subgroups of* k^* *and* $k[x_1]^+$ *respectively and* W *acting on* H *by multiplication. Moreover,*

$$B^G=k[x_1,f_H(y_1)^r]$$

where $r=\operatorname{card} W$ *and* $f_H(y_1)\in k[x_1,y_1]$ *is monic and additive in* y *of degree card* H.

PROOF: This follows from 1.11, 1.7.1 and 1.7.2.

(1.11.2) REMARK: If $\operatorname{card} G$ is prime to $\operatorname{char} k$ then $G=G_2\simeq W$ is cyclic. It is clear that the proof of 1.11 simplifies considerably under this assumption.

(1.11.3) REMARK: If $\operatorname{char} k=p>0$ and $\varphi\in\operatorname{Aut}_k k^{[2]}$ is of order p, then $\varphi=(x+h(y),y)$ w.r.t. suitable variables (x,y) for $k^{[2]}$.

In fact, by 1.8 we may assume $\varphi\in AF_2$ or $\varphi\in E_2$. In the latter case $\varphi=(x+h(y),\ y+b)$ with $h(y)\in k[y]$ and $b\in k$. In the first case this form can be achieved by a linear change of variables. If $b\neq 0$ then h can be made to vanish by changing x to $x'=x+g(y)$ with suitable $g(y)\in k[y]$ as we have seen in I.2 of the proof of 1.11.

REMARK: It would be highly desirable to find a proof of 1.11 that does not make explicit use of the structure theorem for $\operatorname{Aut}_k k^{[2]}$ hidden in 1.8, particularly with a view of extending the result to polynomial rings in three (or more) variables. If the latter were possible, one would have established, in conjunction with 4.3 below, the cancellation property for $k^{[2]}$.

2.

(2.1) LEMMA: *Let A and A' be noetherian domains with $A \subset A'$ such that* $\mathrm{qt}(A) = \mathrm{qt}(A')$. *Suppose A is normal prefactorial, every height* 1 *prime of A' contracts to a hight* 1 *prime of A and $A^* = A'^*$. Then $A = A'$.*

PROOF: Let Q and Q' be the set of height 1 primes of A and A' respectively. If $P \in Q$, then P is the radical of fA for some $f \in A$ (since A is prefactorial) and $f \notin A^* = A'^*$. If P' is a minimal, hence height 1, prime of fA', then $P' \cap A \supset fA$ and $P' \cap A \in Q$ by assumption. Hence $P' \cap A = P$. Now $A'_{P'} \supset A_P$ and $\mathrm{qt}(A'_{P'}) = \mathrm{qt}(A)$. Hence $A'_{P'} = A_P$ since A is normal. It follows that $A' \subset \bigcap_{P' \in Q'} A'_{P'} \subset \bigcap_{P \in Q} A_P = A$.

For the remainder of this section we assume

(2.2) k is a field, A a finitely generated k-domain such that $\mathrm{qt}(A) \simeq \mathrm{qt}(k^{[2]})$ and in addition one of the following holds:

(i) A is factorial and contains a field generator, i.e., there exists $f \in A$ such that $\mathrm{qt}(A) = k(f, g)$ for some $g \in \mathrm{qt}(A)$;
(ii) char $k = 0$ and A is factorial;
(iii) k is perfect and A is regular prefactorial.

(2.3) PROPOSITION: *Let A be as in* 2.2. *Suppose*

$$A \subset B' \subset B$$

where $B \simeq k^{[2]}$, $B' \simeq k^{[2]}$, $\mathrm{qt}(A) = \mathrm{qt}(A')$, *$B = A[t]$ for some $t \in B$, and every height* 1 *prime of B contracts to a height* 1 *prime of B'. Then*

$$A \simeq k^{[2]}.$$

PROOF: We may assume $A \underset{\neq}{\subset} B'$. Let $S = \{P_1, \ldots, P_r\}$ be the (finite) set of height 1 primes P_i of B' such that $A \cap P_i = M_i$ is maximal. Note $S \neq \phi$ by 2.1. Write $P_i = f_i B'$ with $f_i \in B'$ and let P'_i be a minimal prime of $f_i B$. Then $P'_i \cap A = M_i$, $M_i B \subset f_i B \subset P'_i$ and $B/M_i B \simeq$

$(A/M_i)[\bar{t}]$, where $\bar{t}$ is the image of t mod M_iB. It follows that

(1) $$M_iB = P'_i = f_iB;$$

(2) $$(f_i, f_j)B = B \quad \text{for } i \neq j.$$

Now $P'_i \cap B'$ is a height 1 prime containing $f_iB' = P_i$, hence $P'_i \cap B' = P_i$ and we have

(3) $$M_iB' = P_i = f_iB';$$

(4) $$(f_i, f_j)B' = B' \quad \text{for } i \neq j;$$

(5) $$B'/P_i \subset B/P'_i \simeq A/M_i^{[1]}.$$

It follows from (5) that B/P'_i is integral over B'/P_i (since B/P'_i has only one valuation at infinity). Hence

(6) if $M \subset B'$ is a maximal ideal and $f_i \in M$, then there is a maximal ideal $N \subset B$ such that $N \cap B' = M$.

Now $f_iB = P'_i$ is regular and hence if M, N are as in (6) we have: $f_i \notin N^2$, hence $f_i \notin M^2$, hence $f_iB' = P_i$ is regular. By (5) and the affine lemma of Lüroth (see [1], 2.7, for instance)

(7) $$B'/P_i \simeq A/M_i^{[1]}.$$

Making use of (3), (4) and (7) we now proceed exactly as in the proof of 1.3 of [5] to find $x, v \in B'$ such that

(8) $$B' = k[x, v] \quad \text{and} \quad f_i \in k[x], \quad i = 1, \ldots, r.$$

We claim:

(9) Suppose A is factorial, Then $x \in A$.

In fact, let $g \in k[x]$ be irreducible such that $g \nmid f_i$, $i = 1, \ldots, r$. Then $gB' \cap A$ is a height 1 prime, say $gB' \cap A = aA$ with $a \in A$, and

$$A/aA \subset B'/gB' \simeq k[x]/g^{[1]}.$$

If $aB' \neq gB'$, then some f_i is a factor of a in B' and $a \in M_i$ (recall that $\mathrm{qt}(A) = \mathrm{qt}(B')$). Suppose this is the case. Arguing as in (6) we find a maximal ideal N of B' such that $g \in N$ and $N \cap A = M_i$. But then $f_i \in N$, and this is impossible since $(f_i, g)B' = B'$. It follows that $aB' = gB'$. Hence $g \in A$ and x is integral over A, so $x \in A$ since A is normal.

Suppose (i) or (ii) of 2.2 holds. In view of (8) and (9) we find, as in the proof of 1.3 in [5], that $A = k[x, uv]$ where $u \in k[x]$ is of minimal degree such that $uv \in A$.

Suppose (iii) of 2.2 holds. Using theorem 3.1 of [5] we find $u \in k[x]$ such that $A \subset k[x, uv] = A'$ and every height 1 prime of A' contracts to a height 1 prime of A. Then $A = A'$ by 2.1.

We record the following more precise version of 2.3 established during the proof.

(2.3.1) COROLLARY: *There exists $x \in A$ such that $A \simeq k[x]^{[1]}$, $B' \simeq k[x]^{[1]}$ and either $A = B'$ or there exists an irreducible $f \in k[x]$ such that $fB' \cap A$ is maximal and $B/fB \simeq k[x]/f^{[1]}$. Moreover, if x has this property and $B' = k[x, v]$, then $A = k[x, uv]$ for some $u \in k[x]$.*

REMARK: Let the notation be as in 2.3.1. It seems highly likely that $B \simeq k[x]^{[1]}$ as well. We will show this under special circumstances in the next section.

(2.4) THEOREM: *Let A be as in 2.2. Assume*
(i) *$A \subset B \simeq k^{[2]}$ such that $B = A[t]$ for some $t \in A$,*
(ii) *if $G = \mathrm{Aut}_A B$ and $B' = B^G$, then $\mathrm{qt}(A) = \mathrm{qt}(B')$.*
Then

$$A \simeq k^{[2]}.$$

More precisely, variables for A can be chosen as in 2.3.1.

PROOF: B is a simple extension of $B' = B^G$. By 1.11.1, $B' \simeq k^{[2]}$. Also, B is integral over B^G. Hence all assumptions of 2.3 are satisfied.

3.

Let A be a k-algebra and $F \in A[T] \simeq A^{[1]}$, $F \notin A$. Put $B = A[T]/FA[T]$. The canonical map from A to B is injective. We identify A with its image and write $B = A[t]$, where t is the image of T.

(3.1) DEFINITION.

(i) *F is a Galois equation over A if*
 (α) *F is prime;*
 (β) *if $G = \mathrm{Aut}_A B$ and $B' = B^G$, then $\mathrm{qt}(B') = \mathrm{qt}(A)$.*
(ii) *G is of constant type if $\varphi(t) - t \in k$ for all $\varphi \in G$.*

(3.2) THEOREM: *Let k be a perfect field and A a k-algebra such that*

$$A^{[1]} \simeq A[T] = k[X, Y, Z] \simeq k^{[3]}.$$

Suppose Z is a Galois equation over A. Then $A \simeq k^{[2]}$.

PROOF: Clearly A is finitely generated over k, regular and factorial, so 2.2(iii) holds. Also $B = A[T]/ZA[T] \simeq k^{[2]}$. Hence the theorem follows from 2.4.

(3.3) THEOREM: *Let k be a field, $A \simeq k^{[2]}$ and $F \in A[T]$ a Galois equation over A such that $B = A[T]/FA[t] \simeq k^{[2]}$. If G is of constant type, assume also that k is perfect. Then $A[T] \simeq k[F]^{[2]}$.*

A more precise description of F from which 3.3 will follow is given in 3.8.4. We start by collecting some preliminary results. The first, a substitute of sorts in positive characteristic for the epimorphism theorem of Abhyankar and Moh [2], was obtained recently by R. Ganong [3].

(3.4) PROPOSITION: *Let k be a field and $x \in k[x_1, y_1] \simeq k^{[2]}$ such that $k[x_1, y_1]/x \simeq k^{[1]}$. Then there is a unique $k(x)$-valuation V of $k(x_1, y_1)$ not containing $k(x)[x_1, y_1]$, and the residue field L of V is purely inseparable over $k(x)$. Moreover, $k[x_1, y_1] \simeq k[x]^{[1]}$ if and only if $L = k(x)$.*

(3.5) LEMMA: *Let k be a field of characteristic exponent p. Suppose $k^{[2]} \simeq A = k[x, y] \subset k[x_1, y_1] = B \simeq k^{[2]}$ such that*

$$B/xB \simeq k^{[1]}$$

and either

(i) *$[\mathrm{qt}(B) : \mathrm{qt}(A)] = r < \infty$ with $(r, p) = 1$,* *or*

(ii) $p > 1$ *and* $A = B^G$, *where* $G \subset \mathrm{Aut}_k B$ *is a finite* p-*group.*

Then $B \simeq k[x]^{[1]}$.

PROOF: Consider

$$A' = k(x)[y] \subset k(x)[x_1, y_1] = B'$$

By 3.4 the valuation at infinity V_1 of $\mathrm{qt}(A')$ (given by $-\deg_y$) has a unique extension V to $\mathrm{qt}(B')$. Let L_1 and L be the residue fields of V_1 and V respectively and $f = [L : L_1]$. Then $f = p^m$ for some m by 3.4. Moreover, $[\mathrm{qt}(B') : \mathrm{qt}(A')] = ef$, where e is the ramification index of V over V_1. By 3.4 it is enough to show $f = 1$.

If (i) holds, then $[\mathrm{qt}(B') : \mathrm{qt}(A')] = r$ is prime to p, hence $f = 1$. So assume (ii) holds. Then G has a normal subgroup G_1 of order p. Let φ generate G_1. By 1.11.3 we can assume that x_1, y_1 have been chosen so that $\varphi = (x_1, y_1 + h(x_1))$ with $h(x_1) \in k[x_1]$. Then $B^{G_1} \simeq k^{[2]}$. Moreover, $B^{G_1}/x \simeq k^{[1]}$ by the argument used to establish (7) in the proof of 2.3. By induction on card G, $B^{G_1} = k[x]^{[1]}$ and it is enough to prove the lemma in case $G = G_1$. Let $\bar{}$ denote images mod x and write $B/xB = k[t]$. Then $\bar{\varphi}(t) - t \in k$ and $\bar{\varphi}(\bar{y}_1) - \bar{y}_1 = h(\bar{x}_1)$. If $\bar{\varphi} \neq 1$, then $h(x_1) \in k$ by 1.2, and $\bar{\varphi} = 1$ implies $h(\bar{x}_1) = 0$. Hence $x \mid h(x_1) - c$ with $c \in k$. If $h(x_1) - c \neq 0$, this implies $x = ax_1 + b$ with $a \in k^*$ and $b \in k$ and we are done. Otherwise $h(x_1) = c \in k^*$ and B' is unramified over A'. Then V is ramified over V_1, that is $e > 1$, and since $ef = p$ we have $f = 1$.

The next result was mentioned without proof in [5], 3.6. We need it now and briefly indicate a proof.

(3.6) LEMMA: *Let* k *be a field,* $\bar{k}$ *an algebraic closure of* k *and* $F \in k[T, S] \simeq k^{[2]}$ *such that*

(i) $k[T, S]/F \simeq k^{[1]}$;
(ii) $\bar{k}[T, S] \simeq \bar{k}[F]^{[1]}$.

Then $k[T, S] \simeq k[F]^{[1]}$.

PROOF: Let Λ be the pencil of curves $C_\lambda = \{F = \lambda \mid \lambda \in \bar{k}\}$ and $p_1, \ldots, p_s$ the base points of Λ (they are all at infinity). Then, as is well known, it follows from (ii) that all members of Λ, including the generic member, "go through each other" in the sense that the multiplicity of (the proper transform of) C_λ at p_i is independent of λ. Moreover, the generic member is a rational curve over $\bar{k}(F)$. On the other hand, by (i) all base points of Λ are rational over k (they are on C_0 which has one place at infinity rational over k), so the generic member in fact is a rational curve over $k(F)$, and this implies $k[S, T] \simeq k[F]^{[1]}$, as is again well known.

(3.7) LEMMA: *Let k be a field of characteristic $p > 0$ and $F = f(T) - g(S) \in k[T, S] \simeq k^{[2]}$, where f and g are additive polynomials over k. Suppose $k[T, S]/F \simeq k^{[1]}$. Then $k[T, S] = k[F]^{[1]}$.*

PROOF: By 3.6 we may assume that k is perfect. If $\deg f = p^n$ and $\deg g = p^m$ with, say, $m \leq n$, and if a (resp. b) is the leading coefficient of f (resp. g), the substitution $S = S' + (a/b)^{p^{-m}} T^{p^{n-m}}$ changes F to $F' = f'(T) - g(S')$ where $f'(T) = f(T) - g((a/b)^{p^{-m}} T^{p^{n-m}})$ is additive and $\deg f' < p^n$. The lemma follows by induction on $\min(\deg f, \deg g)$.

We now turn to the proof of 3.3. Clearly B is a simple extension of $B^G \supset A$ and we can choose variables x_1, y_1 for B as in 1.11.1. We use the notation established there and let $p = \operatorname{char} k$.

(3.8.1) There exists $x \in A$ such that $A \simeq k[x]^{[1]}$ and $B \simeq k[x]^{[1]}$.

PROOF: (i) If $A = B^G$, our claim follows from 1.11.1.

(ii) Suppose $A \subsetneq B^G$. Clearly 2.2 (i) holds for $A \simeq k^{[2]}$ and hence the assumptions of 2.4 are satisfied. We choose x as in 2.3.1. Let $\bar{k}$ be an algebraic closure of k and put $B_1 = \bar{k} \otimes_k B$. Clearly if f_1 is an irreducible factor of f over $\bar{k}$, then $f_1 = \alpha x + \beta$ with $\alpha \in \bar{k}^*$ and $\beta \in \bar{k}$, $B_1^G \simeq \bar{k}[f_1]^{[1]}$ and $B_1/f_1 \simeq \bar{k}^{[1]}$. Noting $B_1^{G_1} \simeq \bar{k}^{[2]}$ we find $B_1^{G_1}/f_1 \simeq \bar{k}^{[1]}$ by the argument for (7) in the proof of 2.3. Since $[qt(B_1^{G_1})\colon \mathrm{qt}(B^G)] = \operatorname{card} G_2 = r$ with $(r, p) = 1$, we have $B_1^{G_1} \simeq \bar{k}[f_1]^{[1]} = \bar{k}[x]^{[1]}$ by 3.5(i). Similarly $B_1 \simeq \bar{k}[x]^{[1]}$ now follows from 3.5(ii).

(α) If G is of constant type, then $\bar{k}$ is separable over k by assumption and $B \simeq k[x]^{[1]}$ by [5], lemma 1.5.

(β) Suppose G is not of constant type. Then either there exists $\varphi = (x_1, wy_1) \in G$ with $w \neq 1$ or there exists $\psi = (x_1, y_1 + h_1(x_1))$ with $h_1(x_1) \in k[x_1] - k$. Choose $y \in B_1$ such that $B_1 = \bar{k}[x, y]$. In the first case, $\varphi(y) = wy + \delta(x)$ with $\delta(x) \in \bar{k}[x]$ and $d((w-1)y + \delta(x)) = (w-1)y_1$ for some $d \in \bar{k}^*$ by 1.2. Hence $B_1 = \bar{k}[x, y_1]$ and $B = k[x, y_1]$. In the second case, $\psi(y) = y + h(x)$ with $h(x) \in \bar{k}[x]$ and $h(x) = dh_1(x_1)$ with $d \in \bar{k}^*$ by 1.2. Hence $x = ax_1 + b$ with $a \in \bar{k}^*$ and $b \in \bar{k}$. Since $x, x_1 \in B$, we have a, $b \in k$ and $B \simeq k[x_1]^{[1]} = k[x]^{[1]}$.

REMARK: If char $k = 0$, we can finish the proof of 3.3 by referring to [6], theorem 2.6.2. The remainder of the proof is devoted mainly to establishing that F is a variable in $k(x) \otimes_{k[x]} A[T]$ in case char $k = p > 0$. Even in characteristic 0, though, we have the bonus of finding an explicit form for F.

(3.8.2) Let x be as in 3.8.1 and $B = k[x, y]$ where y is chosen so that $G = G_1G_2$ as in 1.11.1 (with (x, y) in place of (x_1, y_1)). Then $B^G = k[x, v]$ with $v = f_H(y)^r$ and $A = k[x, w]$ where $w = uv$ with $u \in k[x]$.

PROOF: This is clear from 1.11.1 and 2.3.1.

(3.8.3) Let x, y, v, u, w be as in 3.8.2. Let F' be the minimal equation of t over $k[x, v]$. Then either

(i) $F' = f(T + c)^r - v$, where $f(T) \in k[x, T]$ is monic additive of degree $p^n = \text{card } H$ in T and $c \in k[x, v] = B^G$,

or

(ii) $F' = f(T + c) - g(v)$, where $f(T) \in k[T]$ and $g(v) \in k[v]$ are additive with $\deg f = p^n = \text{card } H$, $1 < \deg g = p^{n_1} < p^n$, and $c \in k[x, v]$.

PROOF: Let $\psi = (x, wy + h) \in G$. Then by 1.2

$$(1) \qquad \psi(t) - t = a_\psi((w - 1)y + h) \quad \text{with } a_\psi \in k^*.$$

(α) Assume $W \neq \{1\}$. Let $\varphi = (x, wy)$ with $1 \neq \mathrm{w} \in \mathrm{W}$, and $\eta = (x, y + h)$ with $h \in H$. Then $\psi = \varphi\eta$ and

$$t + a_\psi((w - 1)y + h) = \psi(t) = t + a_\varphi(w - 1)y + a_\eta h.$$

Hence $a_\psi = a_\varphi = a_\eta$ and it follows that a_ψ is constant for $\psi \in G$. Hence

$$(2) \qquad \text{there exist } d \in k^* \text{ and } c \in k[x, v] \text{ such that } y = d(t + c).$$

(β) Assume $W = \{1\}$ and there exist $h_1, h_2 \in H$ such that $h_i \neq 0$, $i = 1, 2$ and $h_1 \notin kh_2$. Given any such pair put $\psi_i = (x, y + h_i)$.

Then

$$t + a_{\psi_1\psi_2}(h_1 + h_2) = \psi_1\psi_2(t) = t + a_{\psi_1}h_1 + a_{\psi_2}h_2$$

and hence $a_{\psi_1} = a_{\psi_1\psi_2} = a_{\psi_2}$. Again a_ψ is independent of ψ and (2) holds.

(γ) Suppose $W = \{1\}$ and $H = H'h$ with fixed $h \in k[x]$ and $H' \subset k^+$.

If $\psi = (x, y + ah) \in G$, then $\psi(t) = t + bh$ with $b \in k$ by 1.2 and the map $a \mapsto b$ is a homomorphism on H'. Let $g_1(y) \in k[y]$ be the unique additive polynomial of degree $< p^n = \text{card } H'$ such that $g_1(a) = b$ for $a \in H'$ (see 1.6). Let $\tilde{g}_1(y) = hg_1(y/h) \in k(x)[y]$. Then $\tilde{g}_1(y)$ is additive and $\tilde{g}_1(ah) = bh$ for $ah \in H$. Hence $\psi(t - \tilde{g}_1(y)) = t - \tilde{g}_1(y)$ for $\psi \in G$ and $t = \tilde{g}_1(y) + \tilde{c}$ with $\tilde{c} \in k(x)[v]$. Now $\deg_y \tilde{g}_1 < p^n$, $\deg_y v = p^n$ and $t \in k[x, y]$. Hence $\tilde{g}_1(y) \in k[x, y]$ and $\tilde{c} \in k[x, v]$. This is possible only if either $\deg_y \tilde{g}_1 = 1$, in which case (2) holds, or $\deg_y \tilde{g}_1 > 1$ and $h \in k^*$. In the latter case we may take $h = 1$ and $g_1 = \tilde{g}_1$. Then

(3) $H \subset k^+$ and $t = g_1(y) - c$, where $g_1(y) \in k[y]$ is additive of degree p^{n_1} with $1 < p^{n_1} < p^n$ and $c \in k[x, v]$. Moreover, the conjugates of t are $\{t + g_1(a) \mid a \in H\}$.

If (3) holds, let $H_1 = g_1(H)$ and put $f(T) = f_{H_1}(T)$. Then $f(g_1(y)) = g(v) \in k[v]$ and $f(g_1(y))$ is additive in y, hence additive in v. Moreover, $\deg_y v = \deg_T f = p^n$ and $\deg_v g = \deg_y g_1 = p^{n_1}$. Clearly the minimal equation of t over $k[x, v]$ is $f(T + c) - g(v)$, so F' is as in (ii).

Now suppose (2) holds. Since $f_H(y)^r - v$ is the minimal equation of y over $k[x, v]$ (see 1.7.2), the minimal equation for t is $f(T + c)^r - v$ where $f(T) = f_H(dT)$. Hence F' is as in (i) (after multiplication by $d^{-rp^n} \in k^*$).

3.8.4 (i) Suppose 3.8.3(i) holds. Let $u' \in k[x]$ such that $u'c = c' \in k[x, w]$ and $GCD(u', c') = 1$. Then $u_1 = u/u'^{rp^n} \in k[x]$ and

$$F = u_1(u'^{p^n}f(T) + u'^{p^n}f(c'/u'))^r - w.$$

Moreover, if π is an irreducible factor of u', then

$$u_1c'^{rp^n} - w \equiv a + bw \bmod \pi$$

with $a, b \in k[x]$ and $b \not\equiv 0 \bmod \pi$.

(ii) If 3.8.3(ii) holds, then $u = 1$, $c \in k[x, w]$ and

$$F = f(T + c) - g(v).$$

PROOF:

(i) Let $u/u'^{rp^n} = u_1/u_2$ with $u_1, u_2 \in k[x]$ and $GCD(u_1, u_2) = 1$. Let

$$\begin{aligned} F'' &= u_2 u F' \\ &= u_1(u'^{p^n} f(T) + u'^{p^n} f(c'/u'))^r - u_2 w. \end{aligned}$$

Since $f(T)$ is monic of degree p^n in T, $u'^{p^n} f(c'/u') = c'^{p^n} + u'\alpha$ with $\alpha \in k[x, w]$. So clearly $u_2 u$ is a polynomial $\tilde{u}$ of minimal degree in $k[x]$ such that $\tilde{u}F' \in k[x, w, T]$ and it follows that $F = F''$. Let π be an irreducible factor of u_2. Then F reduces to $u_1 c'^{rp^n} \equiv 0 \bmod \pi$, and this is not possible since

(1) $$k[x, w, T]/(F, \pi) \simeq k[x]/\pi^{[1]} \text{ is a domain.}$$

Hence $u_2 = 1$. Now let π be an irreducible factor of u'. Then $F \equiv u_1 c'^{rp^n} - w \bmod \pi$, and since (1) again holds, F is congruent to a polynomial of degree 1 in $w \bmod \pi$.

(ii) Let $u'c = c'$ as in (i) and put $u^{p^{n_1}}/u'^{p^n} = u_1/u_2$ with $u_1, u_2 \in k[x]$ and $GCD(u_1, u_2) = 1$. One sees as before that $u_2 = 1$ and $F = u^{p^{n_1}} F' = u_1 u'^{p^n} f(T) + u_1 u'^{p^n} f(c'/u') - u^{p^{n_1}} g(w/u)$. Let π be an irreducible factor of u. Then F reduces to $u_1 c'^{p^n} - a_{n_1} w^{p^{n_1}} \equiv 0 \bmod \pi$ where a_{n_1} is the leading coefficient of g. Since $p^n > p^{n_1} > 1$ this is again incompatible with (1), so $u = 1$ as claimed.

(3.8.5) Let F be as in 3.8.4 (i) or (ii). Then $k[x, w, T] = k[x, F]^{[1]}$.

PROOF:

(i) It follows from 3.8.3(i) that $k(x)[w, T] = k(x)[v, T] = k(x)[v, T + c] = k(x)[F', T + c] = k(x)[F, T + c]$. One sees in the same way that F_π, the canonical image of F in $(k[x]/\pi)[w, T]$, is a variable if $\pi \in k[x]$ is irreducible and $\pi \nmid u$. If, on the other hand, $\pi \mid u$, this follows from the considerations in 3.8.4(i). The conclusion now follows from theorem 4.1 below applied to $K = k[x] \subset k[x, w, T]$.

(ii) Suppose 3.8.4(ii) holds. Let $T' = T + c$. Then $k[x, w, T] = k[x, w, T']$ and $k[x, w, T']/f(T') - g(w) = k[x, y]$. By the cancellation property for $k[x]$ (see [1], 2.8), $k[w, T']/f(T') - g(w) \simeq k^{[1]}$ and hence $k[w, T'] = k[F]^{[1]}$ by 3.7. So clearly $k[x, w, T] = k[x, F]^{[1]}$.

(3.8.6) REMARK: Clearly if F is as in (3.8.4) and $f = f_H$ for some $H \subset k[x]^+$ stable under multiplication by elements of $W = \{w \in k^* \mid w^r = 1\}$, then F is a Galois equation over $k[x, w]$ with group G isomorphic to the semidirect product HW.

Let us note that if $u \neq 1$, then the examples of "embedded planes" obtained this way are all of the type described in [6], (3.8.2). Let us point out also that if F is a Galois equation, then $F + c$ with $c \in k^*$ in general is not Galois.

4.

(4.1) THEOREM: *Let K be a locally factorial Krull domain and $F \in K[X, Y] \simeq K^{[2]}$. For each prime $P \subset K$ let $L_P = \mathrm{qt}(K/P)$, denote by F_P the canonical image of F in $L_P[X, Y]$ and assume $L_P[X, Y] = L_P[F_P]^{[1]}$. Then $K[X, Y] = K[F]^{[1]}$.*

PROOF: If $P \subset K$ is a prime, then

(1) $K[X, Y]/PK[X, Y] \simeq (K/P)[X, Y]$ is a domain,
(2) $L_P(F_P)$ is algebraically closed in $L_P(X, Y)$,
(3) $L_P(F_P) \cap (K/P)[X, Y] \subset L_P[F_P]$.

((2) and (3) are immediate consequences of $L_P[X, Y] = L_P[F_P]^{[1]}$.) Also, since F is a variable, hence transcendental, modulo each maximal ideal of K, the content of $F - F(0)$ is (1) and

(4) $L_P[F_P] \cap (K/P)[X, Y] = (K/P)[F_P]$ by [6], (2.6.1)

Hence

(5) $L_P(F_P) \cap (K/P)[X, Y] = (K/P)[F_P]$.

We have established (by (1), (2) and (5)) that $K(F)$ is S-inert in $K[X, Y]$ relative to K, where $S = K - \{0\}$ (see [6], 2.1.2), and by [6], corollary 2.5.3, $K[X, Y] \simeq \mathrm{Sym}_K(Q) \otimes_K K[F]$, where Q is a finitely generated rank 1 projective K-module. Hence $K[X, Y] \simeq \mathrm{Sym}_K(Q \oplus K)$, so $Q \oplus K$ is free, so Q is free (since Q is of rank 1) and $K[X, Y] \simeq K[F]^{[1]}$.

(4.2) REMARK: Let $F = (F_1, \ldots, F_r)$ and $X = (X_1, \ldots, X_r)$. Otherwise keep the notation of 4.1, and assume $F_1, \ldots, F_r$ are part of a system of variables in $L_P[X, Y]$ for each prime $P \subset K$. (1), (2) and (3) in the above proof then hold. Moreover (4) is easy to establish if $P = (0)$ since K is normal. Clearly (4) is trivial for $P \neq 0$ in case K is a principal ideal domain. Hence the conclusion of the theorm holds in that case.

(4.3) THEOREM: *Let k be a locally factorial Krull domain and A* a *k-algebra such that*

$$A^{[1]} \simeq A[T] = k[X, Y, Z] \simeq k^{[3]}.$$

Suppose $Z \in A[T^n]$ with $n > 1$ and invertible in k. Then

$$A \simeq k^{[2]}.$$

PROOF: Suppose first that k contains a primitive n-th root of unity w. Then $Z \in A[T^n]$ if and only if Z is fixed by the A-automorphism φ of $A[T]$ such that $\varphi(T) = wT$. Put $B = A[T]$ and $C = B^{\varphi} = A[T^n]$. Let $K = k[Z]$ and $P \subset K$ a prime. We define: $L_P = \mathrm{qt}(K/P)$; T_P (resp. C_P) = canonical image of T (resp. C) in $(K/P)[X, Y] \subset L_P[X, Y]$; φ_P = automorphism induced by φ on $(K/P)[X, Y]$ or $L_P[X, Y]$; $P' = P \cap k$.

We claim:

(1) $T_P \neq 0$.

Clearly $T \notin P'B$ and replacing, for the moment, k by k/P' we may assume $P' = (0)$. Let $L = \mathrm{qt}(k)$. If $P = (0)$ we are done. Otherwise $M = PL[Z]$ is maximal and $L_P \simeq L[Z]/M$. Write $M = aL[Z]$ with $a \in L[Z]$. Now T is prime in $L[X, Y, Z] \simeq (L \otimes_k A)[T]$ and $T_P = 0$, i.e., $T \in PB \subset aL[X, Y, Z]$, implies $T = ab$ with $b \in L$. This, however, is impossible since $\varphi(T) = wT \neq T$ whereas $\varphi(ab) = ab$. Hence $T_P \neq 0$.

Note $(K/P)[X, Y] = C_P[T_P]$ and

(2) $L_P[X, Y] = S^{-1}C_P[T_P]$ with $S = (K/P - \{0\}) \subset C_P$.

It follows from (1) and (2) that order $\varphi_P = n$ and $L_P[X, Y] = L_P[X, Y]^{\varphi_P}[T_P]$. By (1.11.1) we can find $X_1, Y_1 \in L_P[X, Y]$ such that $L_P[X, Y] = L_P[X_1, Y_1]$ with $\varphi_p(X_1) = X_1$ and $\varphi_P(Y_1) = wY_1$. By 1.1, $(w-1)T_P \mid (w-1)Y_1$ and hence T_p is a variable in $L_P[X, Y]$.

If k does not contain a primitive n-th root of unity, we adjoin one, again calling it w. Then $k[w] \supset k$ is an integral extension, and so is $K[w] \supset K$. If P is a prime of K, let P' be a prime of $K[w]$ such that $P' \cap K = P$. Then $L_{P'} \supset L_P$ is a separable extension. By what we have shown, $T_P \in L_P[X, Y]$ is a variable in $L_{P'}[X, Y]$, and by [5], lemma 1.5, T_P is a variable in $L_P[X, Y]$. It follows from 4.1 that $B = k[Z, U, T]$ for some $U \in B$. Hence $A = B/TB \simeq k^{[2]}$.

REFERENCES

[1] S.S. ABHYANKAR, P. EAKIN and W. HEINZER: On the uniqueness of the coefficient ring in a polynomial ring. *J. Algebra 23* (1972) 310–342.

[2] S.S. ABHYANKAR and T.-T. MOH: "Embeddings of the line in the plane". *J. Reine Angew. Math. 276* (1975), 148–166.

[3] R. GANONG: *On plane curves with one place at infinity. Thesis.* McGill University, 1978.

[4] M. NAGATA: "On automorphism group of $k[X, Y]$". *Lectures in Mathematics 5*, Kyoto University, Kinokuniya Bookstore, Tokyo.

[5] P. RUSSELL: "Simple birational extensions of two-dimensional affine rational domains". *Compositio Math. 33* (1976), 197–208.

[6] P. RUSSELL and A. SATHAYE: "On finding and cancelling variables in $k[X, Y, Z]$". (To appear in *J. Algebra*).

[7] A. SATHAYE: On linear planes. *Proc. Amer. Math. Soc. 56* (1976), 1–7.

[8] J.-P. Serre, Arbres, amalgames et SL_2. *Collège de France*, 1968/69.

[9] D. WRIGHT: Cancellation of variables of the form $bT^n - a$. (To appear).

(Oblatum 15-VIII-1977)

Department of Mathematics
McGill University
Montreal Quebec
Canada