AUTOMORPHISMS OF ANALYTIC LOCAL RINGS

by SHREERAM SHANKAR ABHYANKAR (1)

§ 1. Introduction.

Let K be any valued field. Let $X_1, X_2, \ldots$ be indeterminates. For every non-negative integer d let A_d be the ring of convergent power series in $X_1, \ldots, X_d$ with coefficients in K, and let A'_d be the ring of formal power series in $X_1, \ldots, X_d$ with coefficients in K. By an analytic local ring over K we mean an overring A^* of K such that there exists a K-epimorphism $A_d \to A^*$ for some d. (Note that K is allowed to be discrete, and in that case: K is simply an arbitrary field; $A'_d = A_d$; and an analytic local ring over K is exactly a complete local ring with coefficient field K).

The group $G_K(A_d)$ of all K-automorphisms of the convergent power series ring A_d, for $d > 0$, is quite large. Namely, $g \mapsto (g(X_1), \ldots, g(X_d))$ gives a bijection of $G_K(A_d)$ onto the set of all ordered d-tuples of elements of A_d which constitute a basis of the maximal ideal $M(A_d)$ in A_d.

The group $G(A'_d)$ of all automorphisms of the formal power series ring A'_d is even richer. Namely, any isomorphism of K onto any coefficient field of A'_d can be extended, in many ways, to an automorphism of A'_d. In fact, let H′ be the set of all ordered d-tuples of elements of A'_d which constitute a basis of $M(A'_d)$, let H^* be the set of all monomorphisms $W : K \to A'_d$ such that W(K) is a coefficient field of A'_d, and let $H = \{(Y, W) : Y \in H' \text{ and } W \in H^*\}$. Then $g \to ((g(X_1), \ldots, g(X_d)), g \mid K)$ gives a bijection of $G(A'_d)$ onto H.

The genesis of the present investigation (including our forthcoming joint papers [3] and [4] with Moh and van der Put) was Zariski's discovery [10] that, like formal power series rings, saturated rings are also very rich in automorphisms.

Namely, let K′ be an algebraically closed field of characteristic zero, and let B be a one-dimensional complete local domain with coefficient field K′ such that B is saturated in the sense of [10]. Then:

I) B *has infinitely many* K′*-automorphisms.*

More precisely, given any transversal parameters Z and Z′ of B (i.e., Z and Z′ are elements in B such that, upon letting D to be the integral closure of B in its quotient

(1) This work was supported by the National Science Foundation under N.S.F.-GP-6388 at Purdue University.

field, we have $\mathrm{ord}_D Z = \mathrm{ord}_D Z' = \min\{\mathrm{ord}_D r : r \in M(B)\}$) there exists $g \in G_{K'}(B)$ such that $g(Z) = Z'$ [10, Theorem (1.11)].

And:

II) *Any isomorphism of* K′ *onto any coefficient field of* B *can be extended to an automorphism of* B.

More precisely, given any transversal parameter Z of B and any monomorphism $w : K' \to B$ such that $w(K')$ is a coefficient field of B, there exists $g \in G(B)$ such that $g(Z) = Z$ and $g(k) = w(k)$ for all $k \in K'$ [10, Theorem (1.16)].

Now II) is all the more striking in view of the following two well-known facts:

(′) For every algebraically closed field K^* we have that $G(K^*)$ is infinite and Inv $G(K^*)$ = the prime subfield of K^*, where Inv $G(K^*)$ denotes

$$\{k \in K^* : g(k) = k \text{ for all } g \in G(K^*)\};$$

(see (2.8)).

(″) If the characteristic of K is zero, K is not algebraic over its prime subfield, and R is any analytic local ring over K with $R \neq K$, then R has infinitely many coefficient fields (see (2.20)).

We want to find out as to how far I) and II) can be generalized to analytic local rings.

The results to be reported are positive in the direction of I), and negative in the direction of II).

First consider II).

In § 5 we shall prove

Theorem 1. — *Let* L *be any subfield of* K *such that* L *is finitely generated over the prime subfield of* K. *Then there exists a one-dimensional analytic local domain* R *over* K *with* emdim $R = 2$ *such that for every* $g \in G(R)$ *we have* $g(k) - k \in M(R)$ *for all* $k \in L$; *whence, in particular, if* $g(K) = K$ *then* $g(k) = k$ *for all* $k \in L$.

In our forthcoming joint paper [4] with van der Put, the following theorem will be proved:

Theorem 1′. — *If* R *is any analytic local ring over the complex number field* **C** *such that* R *has a nonunit nonzerodivisor, then for any* $g \in G(R)$ *we have:* $g(\mathbf{C}) = \mathbf{C}$ *and* $g(r) = r$ *for every real number r. More generally, if* $t : R^* \to R$ *is any local homomorphism of analytic local rings over* **C** *such that* $t(M(R^*))$ *contains a nonzerodivisor of* R, *then:* $t(\mathbf{C}) = \mathbf{C}$ *and* $t(r) = r$ *for every real number r.*

Theorems 1 and 1′ relate to II) in view of (′) and (″).

Now we turn to I).

We start off by proving

Theorem 2. — *Let* R *be any complete local domain such that* dim $R > 0$ *and* R *has the same characteristic as* $R/M(R)$. *Let* J *be any nonzero ideal in* R. *Let* R′ *be the integral closure of* R *in its quotient field*; (it is known that then R′ is a complete local domain and R′ is a finite R-module). *Assume that* R′ *is regular*; (note that this assumption is automatically

satisfied if $\dim R=1$). *Then* $G(R, J)$ *is infinite* (where $G(R, J)$ denotes the " inertia group " $\{g\in G(R) : g(r)-r\in J$ for all $r\in R\}$). *If, moreover,* F *is a coefficient field of* R *which can be extended to a coefficient field of* R′ *then* $G_F(R, J)$ *is infinite* (where $G_F(R, J)$ denotes $G_F(R)\cap G(R, J)$; note that if $R'/M(R')$ is separable over $R/M(R)$ then, by Hensel's lemma, every coefficient field of R can be extended to a coefficient field of R′).

Proof. — By Cohen's theorem R′ has a coefficient field E; in case F is a given coefficient field of R which can be extended to a coefficient field of R′ then we take E to be such an extension. Let C be the conductor of R in R′, i.e., $C=\{c\in R : cr'\in R$ for all $r'\in R'\}$. Since R′ is a finite R-module, we know that C contains a nonzero element. Now CJ is a nonzero ideal in R and it remains an ideal in R′. Since CJ is an ideal in R′, we have that $G_E(R', CJ)$ is a subgroup of $G_E(R')$ (see (2.1)). Given any $g\in G_E(R', CJ)$, we have $g(r')-r'\in CJ$ for all $r'\in R'$; since $CJ\subset R$, it follows that $g(r)\in R$ for all $r\in R$, i.e., $g(R)\subset R$; since $G_E(R', CJ)$ is a subgroup of $G_E(R')$, we have $g^{-1}\in G_E(R', CJ)$ and hence also $g^{-1}(R)\subset R$; therefore $g(R)=R$. Thus $g(R)=R$ for all $g\in G_E(R', CJ)$; since $CJ\subset J$, it now suffices to show that $G_E(R', CJ)$ is infinite. By assumption R′ is regular, and hence we may regard R′ to be the ring of formal power series in $X_1, \ldots, X_n$ with coefficients in E, where $n=\dim R'$. For every $y\in(CJ)\cap M(R')^2$ we have a unique $g_y\in G_E(R')$ such that $g_y(X_i)=X_i+y$ for $1\leq i\leq n$; moreover, $g_y\in G_E(R', CJ)$ (see (2.9)). Now $(CJ)\cap M(R')^2$ is clearly infinite, and hence $G_E(R', CJ)$ is infinite.

In (4.2), (4.3) and (4.4) we shall prove, respectively, Theorems 3, 4 and 5 stated below; the actual versions of these theorems which we shall prove there will be more detailed than as stated below.

Theorem 3. — *Let* R *be an analytic local ring over* K *such that* $\dim R=0$ *and* $R\neq K$. *Let* J *be any nonzero ideal in* R. *Then we have the following.*

1) *If* K *is infinite then* $G_K(R, J)$ *is infinite.*

2) $G_K(R, J)=\{1\}\Leftrightarrow G(R)=\{1\}\Leftrightarrow$ R *consists of four elements.*

Theorem 4. — *Let* R *be an analytic local ring over* K *such that* $\dim R>0$. *Assume that the zero ideal in* R *has an isolated primary component* Q *such that upon letting* $P=\mathrm{rad}_R Q$ *we have that* $Q\neq P$ *and*:

(*) *there exists a* K*-epimorphism* $u : A_d\to R$, *for some d, such that* $u^{-1}(Q)$ *is contained in the second symbolic power* $(u^{-1}(P))^{(2)}$ *of* $u^{-1}(P)$.

Let J *be any ideal in* R *with* $J\not\subset Q$. *Then* $G_K(R, J\cap P)\cap G_K[R, Q]$ *is infinite* (where $G_K[R, Q]$ denotes the " splitting group " $\{g\in G_K(R) : g(Q)=Q\}$).

Theorem 5. — *Let* R *be an analytic local ring over* K. *Let* $J, Q_1, \ldots, Q_a$, $(a>0)$, *be ideals in* R *such that* $Q_1, \ldots, Q_a$ *are primary and* $J\cap Q_1\cap\ldots\cap Q_a=\{0\}$. *Let* $P_i=\mathrm{rad}_R Q_i$. *Let* $v : R\to S$ *be a* K*-epimorphism where* S *is an analytic local ring over* K *and* $\mathrm{Ker}\, v=P_1\cap\ldots\cap P_a$. *Assume that*:

(**) *there exists a* K*-epimorphism* $u : A_d\to R$, *for some d, such that* $u^{-1}(Q_i)$ *is a symbolic power of* $u^{-1}(P_i)$ *for* $1\leq i\leq a$.

Then v induces an epimorphism of

$$G_K(R, J) \cap \bigcap_{i=1}^{a} G_K[R, P_i] \cap \bigcap_{i=1}^{a} G_K[R, Q_i]$$

onto

$$G_K(S, v(J)) \cap \bigcap_{i=1}^{a} G_K[S, v(P_i)].$$

In (3.4) and (3.6) we shall give intrinsic formulations of the above conditions (*) and (**) respectively.

In our forthcoming joint paper [3] with Moh and van der Put, we shall prove several other results about automorphisms of analytic local rings. There, in addition to the methods of the present paper, we shall use Samuel's [7] technique by which he proved the algebraicity of an algebroid hypersurface with an isolated singularity. The following two theorems are a sample of the results which are proved in [3]:

Theorem 2'. — Let R *be an analytic local ring over* K *such that* $\dim R > 0$. *Assume that there exists an isolated primary component* P *of* $\{0\}$ *in* R *such that* P *is prime and* R/P *is analytically separably generated over* K (for definition see (2.21)). *Then* $G_K(R)$ *is infinite.*

Theorem 3'. — Assume that K *is perfect* (the characteristic of K may or may not be zero), *and let* R *be any analytic local ring over* K *such that* $\mathrm{rad}_R\{0\}=\{0\}$. *Then* $\mathrm{Inv}\, G_K(R)=K$.

§ 2. Terminology and preliminaries.

I) *Splitting and inertia groups.* — For a ring (commutative with identity) R and a subring K of R we *set*:

$$\begin{aligned} G(R) &= \text{the group of all automorphisms of } R;\\ G_K(R) &= \text{the group of all K-automorphisms of } R\\ &= \{g \in G(R) : g(k)=k \text{ for all } k \in K\}. \end{aligned}$$

By analogy with Hilbert's ramification theory, for any ideal Q in R we *set*:

$$\begin{aligned} G[R, Q] &= \text{the } \textit{splitting group} \text{ of Q in R}\\ &= \{g \in G(R) : g(Q)=Q\};\\ G_K[R, Q] &= \text{the } \textit{splitting group} \text{ of Q in R over K}\\ &= G_K(R) \cap G[R, Q];\\ G(R, Q) &= \text{the } \textit{inertia group} \text{ of Q in R}\\ &= \{g \in G(R) : g(r)-r \in Q \text{ for all } r \in R\};\\ G_K(R, Q) &= \text{the } \textit{inertia group} \text{ of Q in R over K}\\ &= G_K(R) \cap G(R, Q). \end{aligned}$$

Clearly $G[R, Q]$ and $G_K[R, Q]$ are subgroups of $G(R)$ and $G_K(R)$ respectively. We claim that also

(2.1) $G(R, Q)$ *is a subgroup of* $G[R, Q]$.

Namely, for any $g \in G(R, Q)$ we have $g(r)-r \in Q$ for all $r \in R$, and hence $g(r) \in Q$ for all $r \in Q$. Thus $g(Q) \subset Q$ for all $g \in G(R, Q)$. For any $g \in G(R, Q)$ and any $r \in R$,

upon letting $s=g^{-1}(r)$, we have $s\in R$ and $g^{-1}(r)-r=g^{-1}(r)-g(g^{-1}(r))=s-g(s)\in Q$; consequently $g^{-1}\in G(R, Q)$, and hence $g^{-1}(Q)\subset Q$; since $g(Q)\subset Q$ and $g^{-1}(Q)\subset Q$, we get $g(Q)=Q$. For any g and h in $G(R, Q)$ and any $r\in R$, we have $(gh)(r)-r=(g(h(r))-h(r))+(h(r)-r)$ and $g(h(r))-h(r)\in Q$ and $h(r)-r\in Q$, and hence $(gh)(r)-r\in Q$; consequently $gh\in G(R, Q)$. Thus $G(R, Q)$ is a subgroup of $G(R)$, and $G(R, Q)\subset G[R, Q]$.

It follows that also $G_K(R, Q)$ is a subgroup of $G_K[R, Q]$. Also note that:

(2.2) *If* Q^* *is any ideal in* R *with* $Q^*\subset Q$ *then clearly* $G(R, Q^*)\subset G(R, Q)$ *and* $G_K(R, Q^*)\subset G_K(R, Q)$.

We remark that the splitting groups and inertia groups of the galois theory of local rings [1, § 7] are special cases of $G_K[R, Q]$ and $G_K(R, Q)$ respectively; also, Hilbert's higher ramification groups [8, chapter V, § 10] are special cases of $G_K(R, Q)$.

We may now restrict our attention to $G_K(R)$, $G_K[R, Q]$, $G_K(R, Q)$, because the case of $G(R)$, $G[R, Q]$, $G(R, Q)$ would then follow by taking K to be the prime subring (i.e., the smallest subring) of R.

Let $v: R\to S'$ be a ring homomorphism, let $S=v(R)$, and let $L=v(K)$ (note that if K is the prime subring of R then L is the prime subring of S). For any $g\in G_K[R, \operatorname{Ker} v]$ we have a unique $g'\in G_L(S)$ such that: $g'(v(r))=v(g(r))$ for all $r\in R$; we say that g' is *induced* by g. Thus we have a unique map $w: G_K[R, \operatorname{Ker} v]\to G_L(S)$ such that: $w(g)(v(r))=v(g(r))$ for all $g\in G_K[R, \operatorname{Ker} v]$ and all $r\in R$; we again say that w is *induced* by v.

(2.3) *Clearly* $w: G_K[R, \operatorname{Ker} v]\to G_L(S)$ *is a group homomorphism,*

and
$$\operatorname{Ker} w=G_K(R, \operatorname{Ker} v).$$

(2.4) *Let* P *be any ideal in* R. *Then*
$$w(G_K[R, \operatorname{Ker} v]\cap G_K(R, P))\subset G_L(S, v(P)),$$
and
$$w(G_K[R, \operatorname{Ker} v]\cap G_K[R, P])\subset G_L[S, v(P)].$$

If moreover $\operatorname{Ker} v\subset P$ *then*
$$w^{-1}(G_L(S, v(P)))\subset G_K(R, P),$$
and
$$w^{-1}(G_L[S, v(P)])\subset G_K[R, P].$$

Namely, everything except the last inclusion is obvious. The last inclusion follows by noting that for any $g\in G_K[R, \operatorname{Ker} v]$, assuming $\operatorname{Ker} v\subset P$, we have the following: 1) if $w(g)(v(P))\subset v(P)$ then clearly $g(P)\subset P$; 2) if $w(g)\in G_L[S, v(P)]$ then, since w is a homomorphism, also $w(g)^{-1}=w(g^{-1})\in G_L[S, v(P)]$.

(2.5) Let J be any ideal in R with $\operatorname{Ker} v\subset J$, and let G be any subset of $G_K[R, \operatorname{Ker} v]$ such that for each $g\neq h$ in G we have $g(x_{gh})-h(x_{gh})\notin J$ for some $x_{gh}\in R$. *Then upon letting* $y_{gh}=v(x_{gh})$, *for every* $g\neq h$ *in* G *we clearly have* $y_{gh}\in S$ *and* $w(g)(y_{gh})-w(h)(y_{gh})=v(g(x_{gh})-h(x_{gh}))\notin v(J)$. *Whence, in particular, w induces an injection of* G.

(2.6) Let $u : A \to R$ be a ring epimorphism and let K' be a subring of A such that $u(K') = K$. Let $t : G_{K'}[A, \operatorname{Ker} u] \to G_K(R)$ be the homomorphism induced by u. Let $v' = vu$ and let $w' : G_K[A, \operatorname{Ker} v'] \to G_L(S)$ be the homomorphism induced by v'. *Then for any* $h \in G_{K'}[A, \operatorname{Ker} u] \cap G_{K'}[A, \operatorname{Ker} v']$ *we clearly have* $t(h) \in G_K[R, \operatorname{Ker} v]$, *and* $w(t(h)) = w'(h)$.

For any subset H of G(R) we *set*:

$$\operatorname{Inv} H = \{r \in R : g(r) = r \text{ for all } g \in H\};$$

note that then

(2.7) Inv H *is a subring of* R; *moreover, if* T *is any subfield of* R *then* (Inv H) $\cap$ T *is a subfield of* R.

Namely, for any $0 \neq x \in (\operatorname{Inv} H) \cap T$ and any $g \in H$ we have:

$$1/x = (1/x)g(1) = (1/x)g((x)(1/x)) = (1/x)g(x)g(1/x) = (1/x)(x)g(1/x) = g(1/x),$$

and hence $1/x \in (\operatorname{Inv} H) \cap T$.

(2.8) Let E be an algebraically closed field, let F be a subfield of E, and let F^* be the algebraic closure of F in E. Then we have the following:

1) $\operatorname{Inv} G_F(E) \subset F^*$, and if F^* is separable over F then $\operatorname{Inv} G_F(E) = F$.

2) If $F^* \neq E$ then $G_F(E)$ is infinite. If F^* is separable over F and $[F^* : F] = \infty$ then $G_F(E)$ is infinite.

[*Note that it follows that if* F *is the prime subfield of* E *then* $\operatorname{Inv} G_F(E) = F$ *and* $G_F(E)$ *is infinite.*]

To prove 1) and 2), take any transcendence basis $\{x_b\}_{b \in B}$ of E over F^*. Let g be any element in $G_F(F^*)$ (for instance $g =$ the identity). Given any $0 \neq f \in F^*$, there exists a unique $h_f \in G_F(F^*(\{x_b\}_{b \in B}))$ such that $h_f(r) = g(r)$ for all $r \in F^*$ and $h_f(x_b) = fx_b$ for all $b \in B$. Since E is an algebraic closure of $F^*(\{x_b\}_{b \in B})$, there exists $g_f \in G_F(E)$ such that $g_f(r) = h_f(r)$ for all $r \in F^*(\{x_b\}_{b \in B})$. Now F^* is infinite, and hence we see that if $F^* \neq E$ (i.e., if B is nonempty) then $G_F(E)$ is infinite; since we may assume that the transcendence basis $\{x_b\}_{b \in B}$ includes any given element in E which is not in F^*, it also follows that $\operatorname{Inv} G_F(E) \subset F^*$. We have just seen that given any $g \in G_F(F^*)$ there exists $g_1 \in G_F(E)$ such that $g_1(r) = g(r)$ for all $r \in F^*$; therefore the proof is now completed by noting that by ordinary galois theory we have the following: if F^* is separable over F then $\operatorname{Inv} G_F(F^*) = F$; if F^* is separable over F and $[F^* : F] = \infty$ then $G_F(F^*)$ is infinite.

For any ideal Q in a ring R, by $\operatorname{rad}_R Q$ we shall *denote* the radical of Q in R.

II) *Local rings.* — For a (noetherian) local ring R we *set*: dim R = max n such that there exists a chain $P_0 \subset P_1 \subset \ldots \subset P_n$ of distinct prime ideals in R; M(R) = the maximal ideal in R; endim R = the vector space dimension of $M(R)/M(R)^2$ as a vector space over $R/M(R)$. Recall that for any $N \subset M(R)$ we have: $NR = M(R) \Leftrightarrow NR + M(R)^2 = M(R)$; whence, in particular, emdim R = the number of elements in any irredundant basis

of $M(R)$. For any $x\in R$ we *set*: $\operatorname{ord}_R x=\max j$ such that $x\in M(R)^j$; recall that: $\operatorname{ord}_R x=\infty \Leftrightarrow x=0$. Recall that: $\dim R=\min d$ such that there exist d elements in R which generate an ideal which is primary for $M(R)$; whence, in particular, $\operatorname{emdim} R\geq\dim R$; recall that by definition, R is *regular* $\Leftrightarrow \operatorname{emdim} R=\dim R$. By a *system of parameters* of R we mean a sequence $(x_1, \ldots, x_d)$ of elements in $M(R)$ such that $d=\dim R$ and $(x_1, \ldots, x_d)R$ is primary for $M(R)$. Given a homomorphism v of R into another local ring S, we say that v is *local* if $v(M(R))\subset M(S)$.

Note that clearly $G(R)=G[R, M(R)^i]$ for all i; whence, in particular, the canonical epimorphism $R\to R/M(R)$ induces a homomorphism $G(R)\to G(R/M(R))$.

By a *coefficient field* of R we mean a subfield K of R such that K gets mapped onto $R/M(R)$ by the canonical epimorphism $R\to R/M(R)$.

(2.9) *Assume that* R *has a coefficient field* K. *Let* $N\subset R$ *be such that* $NR=M(R)$, *let* J *be an ideal in* R, *and let* $g\in G_K(R)$ *be such that* $g(x)-x\in J$ *for all* $x\in N$. *Then* $g\in G_K(R, J)$.

Proof. — By induction on m (m any positive integer) we shall show that if $x_1, \ldots, x_m$ are any elements in N then $g(x_1\ldots x_m)-x_1\ldots x_m\in J$; by assumption this is true for $m=1$; so now let $m>1$ and suppose true for $m-1$; upon letting $x'=x_2\ldots x_m$ we have $g(x_1)-x_1\in J$ by assumption, and $g(x')-x'\in J$ by the induction hypothesis; now

$$\begin{aligned} g(x_1\ldots x_m)-x_1\ldots x_m &= g(x_1)g(x')-x_1x' \\ &= g(x_1)g(x')-g(x_1)x'+g(x_1)x'-x_1x' \\ &= g(x_1)(g(x')-x')+x'(g(x_1)-x_1), \end{aligned}$$

and hence $g(x_1\ldots x_m)-x_1\ldots x_m\in J$. Since g is a K-automorphism, it now follows that $g(y)-y\in J$ for all $y\in K[N]$. Let any $z\in R$ be given. Given any nonnegative integer i we can find $y_i\in K[N]$ with $z-y_i\in M(R)^i$; now $g(y_i)-y_i\in J$ and $g(M(R)^i)=M(R)^i$; whence $g(z)-z\in J+M(R)^i$. Thus $g(z)-z\in\bigcap_{i=0}^{\infty}(J+M(R)^i)=J$.

(2.10) *Assume that* R *has a coefficient field* K. *Then* $K+\operatorname{rad}_R\{0\}=$ *the integral closure of* K *in* R (where, as usual, $K+\operatorname{rad}_R\{0\}$ denotes $\{k+x : k\in K, x\in\operatorname{rad}_R\{0\}\}$). *Whence in particular*: K *is integrally closed in* $R\Leftrightarrow R$ *has no nonzero nilpotent element.*

Proof. — For any $z\in\operatorname{rad}_R\{0\}$ we have $z^d=0$ for some positive integer d, and hence z is integral over K; since every element in K is certainly integral over K, it follows that every element in $K+\operatorname{rad}_R\{0\}$ is integral over K. Conversely, let any $y\in R$ be given such that y is integral over K. Since $y\in R$ and K is a coefficient field of R, we can write $y=k+x$ with $k\in K$ and $x\in M(R)$. Now k is certainly integral over K and by assumption y is integral over K; consequently x is integral over K. Therefore there exists a positive integer n and elements $k_0, k_1, \ldots, k_n$ in K with $k_0=1$ such that $k_0x^n+k_1x^{n-1}+\ldots+k_n=0$. Let e be the largest nonnegative integer $\leq n$ such that $k_e\neq 0$. Now $0\neq k_e\in K$ and

$$\begin{aligned} k_0x^e+k_1x^{e-1}+\ldots+k_e &= k_e+\text{an element in } xR \\ &= k_e+\text{an element in } M(R) \end{aligned}$$

and hence $k_0x^e+k_1x^{e-1}+\ldots+k_e$ is a unit in R; since $k_0x^n+k_1x^{n-1}+\ldots+k_n=0$, we must have $e\neq n$, i.e., $n-e>0$. Now

$$x^{n-e}(k_0x^e+k_1x^{e-1}+\ldots+k_e)=k_0x^n+k_1x^{n-1}+\ldots+k_n$$
$$=0$$

and $k_0x^e+k_1x^{e-1}+\ldots+k_e$ is a unit in R, and hence $x^{n-e}=0$. Therefore $x\in\mathrm{rad}_R\{0\}$, and hence $y\in K+\mathrm{rad}_R\{0\}$.

(2.11) *Assume that* R *has a coefficient field* K. *Let* N *be any subset of* R *with* $NR=M(R)$. *Let* S *be any other local ring with coefficient field* K. *Let* $u:R\to S$ *and* $v:R\to S$ *be any local* K*-homomorphisms such that* $u(x)=v(x)$ *for all* $x\in N$. *Then* $u=v$.

Proof. — Now $u(x)=v(x)$ for all $x\in K[N]$; also $u(M(R)^i)\subset M(S)^i$ and $v(M(R))^i\subset M(S)^i$ for all i. Let any $y\in R$ be given. Since K is a coefficient field of R, given any nonnegative integer i we can find $x_i\in K[N]$ with $y-x_i\in M(R)^i$; by what we have just said we now get $u(y)-v(y)\in M(S)^i$. Thus $u(y)-v(y)\in\bigcap_{i=0}^{\infty}M(S)^i$, and hence $u(y)=v(y)$.

In the following two Remarks we recall some known facts about the uniqueness of coefficient fields.

Remark **(2.12)**. — Assume that $R/M(R)$ is a perfect field of characteristic $p\neq 0$, and R is of characteristic p. *Then* R *has at most one coefficient field.*

Namely let $w:R\to R/M(R)$ be the canonical epimorphism, and let K and K′ be any coefficient fields of R. Given any $z\in R/M(R)$, let $x\in K$ and $x'\in K'$ be the unique elements such that $w(x)=z=w(x')$. For any positive integer n we have $x^{p^{-n}}\in K$, $x'^{p^{-n}}\in K'$, and $w(x^{p^{-n}})=z^{p^{-n}}=w(x'^{p^{-n}})$; consequently, $x^{p^{-n}}-x'^{p^{-n}}\in M(R)$; now $x-x'=(x^{p^{-n}}-x'^{p^{-n}})^{p^n}$, and hence $x-x'\in M(R)^{p^n}$. This being so for all n, we must have $x-x'=0$, i.e., $x=x'$. Thus $K=K'$.

On the other hand:

Remark **(2.13)**. — Assume that R is henselian (for definition see [2, § 12 A]), $M(R)\neq\{0\}$, R has the same characteristic as $R/M(R)$, $R/M(R)$ is not algebraic over its prime subfield, and $R/M(R)$ possesses a separating transcendence basis over its prime subfield (note that the last assumption is automatically satisfied if $R/M(R)$ is of characteristic zero). *Then* R *has infinitely many coefficient fields.* In fact, let $w:R\to R/M(R)$ be the canonical epimorphism, and take any subfield L of R and any nonempty family $\{x_a\}_{a\in A}$ of elements in R such that the elements $\{w(x_a)\}_{a\in A}$ are algebraically independent over $w(L)$ and $R/M(R)$ possesses a separating transcendence basis $\{z_b\}_{b\in B}$ over $w(L)(\{w(x_a)_{a\in A}\})$. Let $D=\{r_a\}_{a\in A}$ be any family of elements in M(R) (with the same indexing set A). *Then there exists a coefficient field* K_D *of* R *such that* $L[\{x_a+r_a\}_{a\in A}]\subset K_D$. (Namely, take $y_b\in w^{-1}(z_b)$, and let $L'=L[\{x_a+r_a\}_{a\in A},\{y_b\}_{b\in B}]$; then for every $0\neq s\in L'$ we clearly have $w(s)\neq 0$ and hence s is a unit in R; consequently R contains the quotient field L^* of L′; by Zorn's lemma, L^* is contained in a maximal subfield K_D of R; now $R/M(R)$ is separable algebraic over $w(L^*)$ and hence, since R is henselian, by a standard argument (see the proof of [9, Corollary 2 on page 280]) we see that K_D

is a coefficient field of R.) Now M(R) is infinite and hence there are infinitely many distinct families $D=\{r_a\}_{a\in A}$ of elements in M(R). Moreover, if $D=\{r_a\}_{a\in A}$ and $D'=\{r'_a\}_{a\in A}$ are any two families of elements in M(R) then for any $a\in A$ we clearly have that: $x_a+r'_a\in K_D \Leftrightarrow r'_a=r_a$.

III) *Analytic local rings.* — Let K be a valued field, and let $X_1, X_2, \ldots$ be indeterminates. For every nonnegative integer m we *set*:

$K[[X_1, \ldots, X_m]]$ = the ring of formal power series in $X_1, \ldots, X_m$ with coefficients in K;
$K((X_1, \ldots, X_m))$ = the quotient field of $K[[X_1, \ldots, X_m]]$;
$K[\langle X_1, \ldots, X_m\rangle]$ = the ring of convergent power series in $X_1, \ldots, X_m$ with coefficients in K;
$K(\langle X_1, \ldots, X_m\rangle)$ = the quotient field of $K[\langle X_1, \ldots, X_m\rangle]$.

Note that if K is discrete then $K[\langle X_1, \ldots, X_m\rangle]=K[[X_1, \ldots, X_m]]$.

By an *analytic local ring* over K we mean an overring R of K such that there exists a K-epimorphism of $K[\langle X_1, \ldots, X_q\rangle]$ onto R for some q.

For properties of analytic local rings see [2]. It should be remarked that although in [2] we assumed K to be complete, in all the relevant (algebraic as opposed to the function theoretic) material this assumption was never used; alternatively it suffices to note that, upon letting K^* to be the completion of K, we have $K[\langle X_1, \ldots, X_m\rangle]=K^*[\langle X_1, \ldots, X_m\rangle]\cap K[[X_1, \ldots, X_m]]$. In particular then $K[\langle X_1, \ldots, X_m\rangle]$ is an m-dimensional regular local ring with coefficient field K. We also remark that in case K is discrete, an analytic local ring over K is exactly a complete local ring with coefficient field K.

Now let R be an analytic local ring over K. Clearly then R is a local ring with coefficient field K.

For every nonnegative integer m let $A_m=K[\langle X_1, \ldots, X_m\rangle]$.

We observe that given any finite number of elements $x_1, \ldots, x_n$ in M(R) there exists a unique local K-homomorphism $v: A_n\to R$ with $v(X_i)=x_i$ for $1\leq i\leq n$. Namely, the uniqueness follows by (2.11). To see the existence, note that by definition there exists a K-epimorphism $s: A_q\to R$ for some q; take $f_i(X_1, \ldots, X_q)\in s^{-1}(x_i)$ for $1\leq i\leq n$; now define v by taking

$$v(f(X_1, \ldots, X_n))=s(f(f_1(X_1, \ldots, X_q), \ldots, f_n(X_1, \ldots, X_q)))$$

for all $f(X_1, \ldots, X_n)\in A_n$. For any $f(X_1, \ldots, X_n)\in A_n$ we *define* $f(x_1, \ldots, x_n)$ to be $v(f(X_1, \ldots, X_n))$; also we *set*: $K[\langle x_1, \ldots, x_n\rangle]=v(A_n)$ and $K(\langle x_1, \ldots, x_n\rangle)$ = the total quotient ring of $K[\langle x_1, \ldots, x_n\rangle]$. For the case of a complete local ring with coefficient field K we may denote the corresponding objects by $f(x_1, \ldots, x_n)$, $K[[x_1, \ldots, x_n]]$, and $K((x_1, \ldots, x_n))$ respectively.

Note that given any finite number of elements $x_1, \ldots, x_n$ in M(R) and any nonnegative integer $e\leq n$, upon letting $v: A_n\to R$ and $t: A_e\to R$ to be the unique

local K-homomorphisms with $v(X_i)=x_i$ for $1\leq i\leq n$ and $t(X_i)=x_i$ for $1\leq i\leq e$, we clearly have $t(f)=v(f)$ for all $f\in A_e$.

The following lemma is quite useful.

(2.14) *Given any finite number of elements* $x_1, \ldots, x_e$ *in* $M(R)$, *let* $t : A_e\to R$ *be the unique local* K*-homomorphism with* $t(X_i)=x_i$ *for* $1\leq i\leq e$. *Then we have the following*:

1) $(x_1, \ldots, x_e)R$ *is primary for* $M(R)\Leftrightarrow R$ *is integral over* $K[\langle x_1, \ldots, x_e\rangle]\Leftrightarrow R$ *is a finite* $K[\langle x_1, \ldots, x_e\rangle]$*-module.*

2) *If* $(x_1, \ldots, x_e)R$ *is primary for* $M(R)$ *then*: $\dim R=e\Leftrightarrow t$ *is injective.*

3) $(x_1, \ldots, x_e)R=M(R)\Leftrightarrow t$ *is surjective.*

4) *If* R *is a domain and* $(x_1, \ldots, x_e)$ *is a system of parameters of* R, *then, for any* $z\in M(R)$, *upon letting* $F(X)$ *to be the minimal monic polynomial of* z *over* $K(\langle x_1, \ldots, x_e\rangle)$ (where X is an indeterminate) *and* D *to be the degree of* $F(X)$, *we have* $F(X)-X^D\in M(K[\langle x_1, \ldots, x_e\rangle])[X]$. (Note that by 1) we know that if R is a domain and $(x_1, \ldots, x_e)$ is a system of parameters of R, then the quotient field of R is a finite algebraic extension of $K(\langle x_1, \ldots, x_e\rangle)$.)

Proof. — Take a basis $(x_{e+1}, \ldots, x_n)$ of $M(R)$ and let $v : A_n\to R$ be the unique local K-homomorphism with $v(X_i)=x_i$ for $1\leq i\leq n$. Now 1), 2) and 4) follow by applying [2, (23.3) and (23.10)] to the ideal $\operatorname{Ker} v$ in A_n. To prove 3), note that if $(x_1, \ldots, x_e)R=M(R)$, then, upon letting $R'=K[\langle x_1, \ldots, x_e\rangle]$ we clearly have $R=R'+M(R')R$ as R'-modules and by 1) we have that R is a finite R'-module, and hence $R=R'$ by Nakayama's lemma. Q.E.D.

(2.15) *Given any nonnegative integer* n *and any basis* $(Y_1, \ldots, Y_n)$ *of* $M(A_n)$, *upon letting* $h : A_n\to A_n$ *to be the unique local* K*-homomorphism with* $h(X_i)=Y_i$ *for* $1\leq i\leq n$, *by* (2.14) *we have that* $h\in G_K(A_n)$. *Thus we have a bijection of* $G_K(A_n)$ *onto the set of all ordered* n*-tuples* $(Y_1, \ldots, Y_n)$ *of elements in* $M(A_n)$ *with* $(Y_1, \ldots, Y_n)A_n=M(A_n)$.

It may be remarked that the Implicit Function Theorem [2, (10.8)] and the Inversion Theorem [2, (10.10)] can be deduced directly from (2.15).

Another immediate consequence of (2.14) is that:

(2.16) *There exists a* K*-epimorphism* $A_n\to R\Leftrightarrow n\geq \operatorname{emdim} R$.

Moreover, all these epimorphisms can be derived from one of them in the following manner:

(2.17) *Let* $v : A_n\to R$ *and* $t : A_e\to R$ *be any* K*-epimorphisms where* n *is any nonnegative integer and* $e=\operatorname{emdim} R$. *Let* $b : A_n\to A_e$ *be the* K*-epimorphism defined by taking* $b(f(X_1, \ldots, X_n))=f(X_1, \ldots, X_e, 0, \ldots, 0)$ *for all* $f(X_1, \ldots, X_n)\in A_n$. *Then there exists* $h\in G_K(A_n)$ *such that* $tbh=v$. (Note that if $n=e$ then we get $th=v$.)

Actually, we shall prove the following slightly stronger version of (2.17):

(2.18) *Let* $v : A_n\to R$ *and* $u : A_m\to R$ *be any* K*-epimorphisms where* n *and* m *are any nonnegative integers with* $n\geq m$. *Let* $b : A_n\to A_m$ *be the* K*-epimorphism defined by taking* $b(f(X_1, \ldots, X_n))=f(X_1, \ldots, X_m, 0, \ldots, 0)$ *for all* $f(X_1, \ldots, X_n)\in A_n$. *Then there exists* $h\in G_K(A_n)$ *such that* $ubh=v$. (Note that if $n=m$ then we get $uh=v$.)

Proof. — Let $x_i = u(X_i)$ for $1 \leq i \leq m$, and let $e = \operatorname{emdim} R$. Since $u : A_m \to R$ is an epimorphism, we have $(x_1, \ldots, x_m)R = M(R)$ and hence there exists a permutation $(a(1), \ldots, a(m))$ of $(1, \ldots, m)$ such that $(x_{a(1)}, \ldots, x_{a(e)})R = M(R)$. Since $v : A_n \to R$ is an epimorphism, we can take $Z'_{a(i)} \in M(A_n)$ with $v(Z'_{a(i)}) = x_{a(i)}$ for $1 \leq i \leq e$; now the elements $x_{a(1)}, \ldots, x_{a(e)}$ are K-independent modulo $M(R)^2$, and hence the elements $Z'_{a(1)}, \ldots, Z'_{a(e)}$ are K-independent modulo $M(A_n)^2$; consequently there exists a basis $(Z_1, \ldots, Z_n)$ of $M(A_n)$ such that $Z_{a(i)} = Z'_{a(i)}$ for $1 \leq i \leq e$. By (2.15) we can now take $h' \in G_K(A_n)$ such that $h'(X_i) = Z_i$ for $1 \leq i \leq n$. Now $vh' : A_n \to R$ is a K-epimorphism and $vh'(X_{a(i)}) = x_{a(i)}$ for $1 \leq i \leq e$. Let $t : A_e \to R$ be the unique local K-homomorphism with $t(X_i) = x_{a(i)}$ for $1 \leq i \leq e$. By (2.14) we know that t is surjective, and hence there exist

$$F_i(X_1, \ldots, X_e) \in M(A_e) \quad \text{and} \quad f_i(X_1, \ldots, X_e) \in M(A_e)$$

such that

$$F_i(x_{a(1)}, \ldots, x_{a(e)}) = vh'(X_i) \qquad \text{for } 1 \leq i \leq n,$$

and

$$f_i(x_{a(1)}, \ldots, x_{a(e)}) = x_i \qquad \text{for } 1 \leq i \leq m.$$

Let

$$Y_i = \begin{cases} X_i - F_i(X_{a(1)}, \ldots, X_{a(e)}) & \text{for } m < i \leq n, \\ X_i \quad \text{for } i \in \{a(1), \ldots, a(e)\}, \\ X_i - F_i(X_{a(1)}, \ldots, X_{a(e)}) + f_i(X_{a(1)}, \ldots, X_{a(e)}) & \text{for } 1 \leq i \leq m \text{ with } i \notin \{a(1), \ldots, a(e)\}. \end{cases}$$

Then clearly $(Y_1, \ldots, Y_n)$ is a basis of $M(A_n)$, and

$$vh'(Y_i) = x_i \quad \text{for } 1 \leq i \leq m, \text{ and } vh'(Y_i) = 0 \text{ for } m < i \leq n.$$

Since $(Y_1, \ldots, Y_n)$ is a basis of $M(A_n)$, by (2.15) we can take $h^* \in G_K(A_n)$ with $h^*(X_i) = Y$ for $1 \leq i \leq n$, and then we have

$$vh'h^*(X_i) = x_i \quad \text{for } 1 \leq i \leq m, \text{ and } vh'h^*(X_i) = 0 \text{ for } m < i \leq n.$$

Let $h = h^{*-1}h'^{-1}$, and let $X'_i = h'h^*(X_i)$ for $1 \leq i \leq n$. Then $h \in G_K(A_n)$, $(X'_1, \ldots, X'_n)$ is a basis of $M(A_n)$,

$$v(X'_i) = vh'h^*(X_i) = x_i = u(X_i) = ubh(X'_i) \qquad \text{for } 1 \leq i \leq m,$$

and

$$v(X'_i) = vh'h^*(X_i) = 0 = ubh(X'_i) \qquad \text{for } m < i \leq n.$$

Thus $ubh : A_n \to R$ and $v : A_n \to R$ are both local K-homomorphisms,

$$(X'_1, \ldots, X'_n)A_n = M(A_n),$$

and $ubh(X'_i) = v(X'_i)$ for $1 \leq i \leq n$; consequently by (2.11) we get $ubh = v$.

Using (2.17) we shall now prove

(2.19) *Let $v : A_n \to R$ be any K-epimorphism where n is any nonnegative integer, let J be any ideal in A_n, and let $w : G_K[A_n, \operatorname{Ker} v] \to G_K(R)$ be the homomorphism induced by v. Then*

$$w(G_K[A_n, \operatorname{Ker} v] \cap G_K(A_n, J)) = G_K(R, v(J)).$$

Proof. — Let $e = \operatorname{emdim} R$, and take a basis $(x_1, \ldots, x_e)$ of $M(R)$. Let $t : A_e \to R$ be the unique local K-homomorphism with $t(X_i) = x_i$ for $1 \leq i \leq e$; by (2.14) we know that t is surjective. Let $b : A_n \to A_e$ be the K-epimorphism defined by taking $b(f(X_1, \ldots, X_n)) = f(X_1, \ldots, X_e, 0, \ldots, 0)$ for all $f(X_1, \ldots, X_n) \in A_n$. By (2.17) we can find $h \in G_K(A_n)$ such that $tbh = v$.

Let any $g' \in G_K(R, v(J))$ be given. Then $g'(x_i) - x_i \in v(J) = tbh(J)$ for $1 \leq i \leq e$, and hence there exists

$$Z_i^* \in J \quad \text{for} \quad 1 \leq i \leq e \tag{1}$$

such that upon letting

$$Z_i = h(Z_i^*) \quad \text{for} \quad 1 \leq i \leq e \tag{2}$$

we have $g'(x_i) - x_i = tb(Z_i)$ for $1 \leq i \leq e$. Now

$$t(X_i + b(Z_i)) = g'(x_i) \quad \text{for} \quad 1 \leq i \leq e; \tag{3}$$

since g' is an automorphism of R, we have $(g'(x_1), \ldots, g'(x_e))R = M(R)$ and hence the elements $g'(x_1), \ldots, g'(x_e)$ are K-independent modulo $M(R)^2$; since $t : A_e \to R$ is an epimorphism, in view of (3) we deduce that the elements $X_1 + b(Z_1), \ldots, X_e + b(Z_e)$ are in $M(A_e)$ and they are K-independent modulo $M(A_e)^2$. Therefore $(X_1 + b(Z_1), \ldots, X_e + b(Z_e))A_e = M(A_e)$; now $b : A_n \to A_e$ is an epimorphism with $\operatorname{Ker} b = (X_{e+1}, \ldots, X_n)A_n$ and $b(X_i + Z_i) = X_i + b(Z_i)$ for $1 \leq i \leq e$; consequently, we must have $(X_1 + Z_1, \ldots, X_e + Z_e, X_{e+1}, \ldots, X_n)A_n = M(A_n)$. By (2.15) we now get $h' \in G_K(A_n)$ such that

$$h'(X_i) = X_i + Z_i \text{ for } 1 \leq i \leq e, \quad \text{and} \quad h'(X_i) = X_i \text{ for } e < i \leq n. \tag{4}$$

Since $t(X_i) = x_i$ for $1 \leq i \leq e$, by (3) and (4) we see that

$$\text{for } 1 \leq i \leq e\text{: } tbh'(X_i) = g'(x_i) = g't(X_i) = g'tb(X_i),$$

and

$$\text{for } e < i \leq n\text{: } tbh'(X_i) = 0 = g'tb(X_i);$$

thus

$$tbh'(X_i) = g'tb(X_i) \quad \text{for} \quad 1 \leq i \leq n. \tag{5}$$

Let

$$g = h^{-1}h'h, \quad \text{and} \quad X_i^* = h^{-1}(X_i) \quad \text{for} \quad 1 \leq i \leq n. \tag{6}$$

Then $g \in G_K(A_n)$, and

$$(X_1^*, \ldots, X_n^*)A_n = M(A_n). \tag{7}$$

By (2), (4), and (6) we get

$$g(X_i^*) = X_i^* + Z_i^* \text{ for } 1 \leq e \leq i, \quad \text{and} \quad g(X_i^*) = X_i^* \text{ for } e < i \leq n;$$

consequently, in view of (1) and (7), by (2.9) we see that $g \in G_K(A_n, J)$. Since $tbh = v$, by (5) and (6) we get that for $1 \leq i \leq n$:

$$\begin{aligned} vg(X_i^*) = (tbh)(h^{-1}h'h)h^{-1}(X_i) &= tbh'(X_i) \\ &= g'tb(X_i) = g'(tbh)h^{-1}(X_i) = g'v(X_i^*). \end{aligned}$$

Thus $vg(X_i^*)=g'v(X_i^*)$ for $1\leq i\leq n$; now $vg : A_n\to R$ and $g'v : A_n\to R$ are both local K-homomorphisms, and by (7) we have $(X_1^*, \ldots, X_n^*)A_n=M(A_n)$; therefore by (2.11) we get

$$vg=g'v.$$

From this it follows that $g\in G_K[A_n, \operatorname{Ker} v]$ and $g'=w(g)$.

Since, in view of (2.4), we have

$$w(G_K[A_n, \operatorname{Ker} v]\cap G_K(A_n, J))\subset G_K(R, v(J)),$$

we now conclude that

$$w(G_K[A_n, \operatorname{Ker} v]\cap G_K(A_n, J))=G_K(R, v(J)).$$

Remark **(2.20)**. — *By* [2, (20.6)] *we know that* R *is henselian.* Whence, in particular, Remark (2.13) is applicable to R.

Definition **(2.21)**. — *An analytic local domain* S *over* K *is said to be* analytically separably generated over K *if there exists a system of parameters* $(y_1, \ldots, y_d)$ *of* S *such that the quotient field of* S *is separable over* $K(\langle y_1, \ldots, y_d\rangle)$. *Given a prime ideal* P *in* R, R/P *can be considered to be an analytic local domain over* K *by identifying* K *with its image under the canonical epimorphism* $R\to R/P$, *and hence the above definition applies to* R/P.

Equivalently, upon regarding R/P to be a K-algebra, in view of (2.14) we have that: R/P is analytically separably generated over K$\Leftrightarrow$there exists a local K-monomorphism $u : A_m\to R/P$, for some m, such that R/P is integral over $u(A_m)$ and the quotient field of R/P is separable over the quotient field of $u(A_m)$ (note that we must then have $m=\dim R/P$).

It is known that if K is perfect then every analytic local domain over K is analytically separably generated over K. For the case when K is an infinite perfect field see for instance [2, (24.5)]. In [3] we shall give an elementary proof of this which applies also when K is finite.

It may be noted that in case of characteristic zero, by definition every field is considered to be perfect and every algebraic extension is considered to be separable.

For some other criteria of analytic separable generation reference may be made to [5] and [6, Exercises 1 to 4 on page 202].

§ 3. Symbolic powers.

Recall that for a primary ideal Q in a noetherian ring R: $\operatorname{exponent}_R Q=\min n$ for which $(\operatorname{rad}_R Q)^n\subset Q$; and $\operatorname{length}_R Q=\max n$ for which there exists a chain of distinct ideals $Q_1\subset Q_2\subset\ldots\subset Q_n$ in R such that $Q_1, \ldots, Q_n$ are primary for $\operatorname{rad}_R Q$ and $Q_1=Q$. Also recall that for a prime ideal P in a noetherian domain R, the n-th symbolic power of P is denoted by $P^{(n)}$, i.e., $P^{(n)}=M(R_P)^n\cap R$; also note that if Q is an ideal in R which is primary for P, then upon letting $e=\operatorname{exponent}_R Q$ we have that: Q is a symbolic power of $P\Leftrightarrow Q=P^{(e)}$. As usual, by $\binom{i}{j}$ we denote binomial coefficients.

(3.1) *Let* A *and* R *be noetherian rings, let* $u : A \to R$ *be an epimorphism, and let* Q *be a primary ideal in* R. *Then* $\text{exponent}_R Q = \text{exponent}_A u^{-1}(Q)$, *and* $\text{length}_R Q = \text{length}_A u^{-1}(Q)$.

Proof. — The assertion about length is obvious. The assertion about exponent follows by checking that if Q′ and Q* are any ideals in R and n is any positive integer then: $Q^{*n} \subset Q' \Leftrightarrow (u^{-1}(Q^*))^n \subset u^{-1}(Q')$.

(3.2) *Let* P *and* Q *be ideals in a regular local ring* A *such that* P *is prime and* $Q \subset P^{(2)}$. *Then* $Q \subset M(A)^2$ *and* $\text{emdim } A/Q = \dim A$.

Proof. — Suppose if possible that there exists $x \in P^{(2)}$ with $x \notin M(A)^2$. Now A_P is a regular local ring with $\dim A_P = \dim A - \dim A/P$, A/xA is a regular local ring with $\dim A/xA = \dim A - 1$; P/xA is a prime ideal in A/xA, and $(A/xA)_{P/xA}$ is a regular local ring with $\dim(A/xA)_{P/xA} = \dim A/xA - \dim(A/xA)/(P/xA)$; consequently

$$\begin{aligned}\text{emdim}(A/xA)_{P/xA} &= \dim(A/xA)_{P/xA} \\ &= \dim A/xA - \dim(A/xA)/(P/xA) \\ &= \dim A/xA - \dim A/P \\ &= (\dim A - 1) - \dim A/P \\ &= (\dim A - \dim A/P) - 1 \\ &= \dim A_P - 1 \\ &= \text{emdim } A_P - 1.\end{aligned}$$

Also, by the permutability of residue class ring and quotient ring formations we know that $(A/xA)_{P/xA}$ is isomorphic to A_P/xA_P; whence we get that

$$\text{emdim } A_P/xA_P = \text{emdim } A_P - 1.$$

However, $x \in P^{(2)} \subset M(A_P)^2$ and hence

$$\text{emdim } A_P/xA_P = \text{emdim } A_P$$

which is a contradiction.

Thus we must have $P^{(2)} \subset M(A)^2$. Therefore $Q \subset M(A)^2$ and hence

$$\text{emdim } A/Q = \text{emdim } A = \dim A.$$

(3.3) *Let* P *and* Q *be ideals in a regular local ring* A *such that* P *is prime and* Q *is primary for* P. *Then*:

$$Q \subset P^{(2)} \Leftrightarrow \dim A = \text{emdim } A/Q = \text{emdim } (A/Q)_{P/Q} + \dim A/Q.$$

Proof. — Since Q is primary for P, we have $\dim A/Q = \dim A/P$; also $\text{emdim } A_P = \dim A_P = \dim A - \dim A/P$; consequently,

$$\text{emdim } A_P = \dim A - \dim A/Q.$$

Also, by the permutability of residue class ring and quotient ring formations we know that A_P/QA_P is isomorphic to $(A/Q)_{P/Q}$, and hence

$$\text{emdim } A_P/QA_P = \text{emdim}(A/Q)_{P/Q}.$$

Clearly : $\dim A = \operatorname{emdim}(A/Q)_{P/Q} + \dim A/Q \Leftrightarrow \dim A - \dim A/Q = \operatorname{emdim}(A/Q)_{P/Q}$, and hence by the above two displayed equations we get that

$$\dim A = \operatorname{emdim}(A/Q)_{P/Q} + \dim A/Q \Leftrightarrow \operatorname{emdim} A_P = \operatorname{emdim} A_P/QA_P.$$

Clearly: $Q \subset P^{(2)} \Leftrightarrow QA_P \subset M(A_P)^2 \Leftrightarrow \operatorname{emdim} A_P = \operatorname{emdim} A_P/QA_P$, and hence by the above displayed implication we get that

$$Q \subset P^{(2)} \Leftrightarrow \dim A = \operatorname{emdim}(A/Q)_{P/Q} + \dim A/Q.$$

Our assertion follows from this in view of (3.2).

Proposition **(3.4)**. — *Let* P *and* Q *be ideals in a local ring* R *such that* P *is prime and* Q *is primary for* P. *Then we have the following.*

1) *If* $u : A \to R$ *is any epimorphism such that* A *is a regular local ring and* $u^{-1}(Q) \subset (u^{-1}(P))^{(2)}$, *then* $\dim A = \operatorname{emdim} R$.

2) *Now assume that there exists an epimorphism* $B \to R$ *such that* B *is a regular local ring with* $\dim B = \operatorname{emdim} R$ (note that by (2.16) we know that this assumption is satisfied if R is an analytic local ring over a valued field K). *Then the following three conditions are equivalent*:

(*) *There exists an epimorphism* $u : A \to R$ *such that* A *is a regular local ring and* $u^{-1}(Q) \subset (u^{-1}(P))^{(2)}$.

(**) *If* $u : A \to R$ *is any epimorphism such that* A *is a regular local ring with* $\dim A = \operatorname{emdim} R$, *then* $u^{-1}(Q) \subset (u^{-1}(P))^{(2)}$.

(***) $\operatorname{emdim} R = \operatorname{emdim} R/Q = \operatorname{emdim}(R/Q)_{P/Q} + \dim R/Q$.

Proof. — Follows from (3.3) by noting that if $A \to R$ is any epimorphism such that A is a regular local ring, then

$$\dim A \geq \operatorname{emdim} R \geq \operatorname{emdim} R/Q.$$

(3.5) *Let* P *and* Q *be ideals in a regular local ring* A *such that* P *is prime,* Q *is primary for* P, *and* $Q \neq P$. *Then the following two conditions are equivalent*:

(*) Q *is a symbolic power of* P.

(**) $$\dim A = \operatorname{emdim} A/Q$$

and $$\operatorname{length}_{A/Q}\{0\} = \binom{\operatorname{emdim} A/Q - \dim A/Q + \operatorname{exponent}_{A/Q}\{0\} - 1}{\operatorname{exponent}_{A/Q}\{0\}}.$$

Proof. — Since Q is primary for P, we have $\dim A/Q = \dim A/P$; also $\dim A_P = \dim A - \dim A/P$; consequently: if $\dim A = \operatorname{emdim} A/Q$ then

$$\operatorname{emdim} A/Q - \dim A/Q = \dim A_P.$$

Therefore, in view of (3.1) and (3.2), we see that our assertion would follow from the following:

(1) Q is a symbolic power of $P \Leftrightarrow \operatorname{length}_A Q = \binom{\dim A_P + \operatorname{exponent}_A Q - 1}{\operatorname{exponent}_A Q}$.

To prove (1), let $e = \text{exponent}_A Q$. Then $P^{(e)} \subset Q$ and hence

$$Q = P^{(e)} \Leftrightarrow \text{length}_A Q = \text{length}_A P^{(e)}. \tag{2}$$

Also:

$$Q \text{ is a symbolic power of } P \Leftrightarrow Q = P^{(e)}. \tag{3}$$

Now A_P is a regular local ring, and hence

$$\text{length}_A P^{(e)} = \binom{\dim A_P + e - 1}{e}. \tag{4}$$

Now (1) follows from (2), (3) and (4).

Proposition **(3.6).** — *Let* P *and* Q *be ideals in a local ring* R *such that* P *is prime,* Q *is primary for* P, *and* $Q \neq P$. *Then we have the following*:

1) *If* $u : A \to R$ *is any epimorphism such that* A *is a regular local ring and* $u^{-1}(Q)$ *is a symbolic power of* $u^{-1}(P)$, *then* $\dim A = \text{emdim } R$.

2) *Now assume that there exists an epimorphism* $B \to R$ *such that* B *is a regular local ring with* $\dim B = \text{emdim } R$ (note that by (2.16) we know that this assumption is satisfied if R is an analytic local ring over a valued field K). *Then the following three conditions are equivalent*:

(*) *There exists an epimorphism* $u : A \to R$ *such that* A *is a regular local ring and* $u^{-1}(Q)$ *is a symbolic power of* $u^{-1}(P)$.

(**) *If* $u : A \to R$ *is any epimorphism such that* A *is a regular local ring with* $\dim A = \text{emdim } R$, *then* $u^{-1}(Q)$ *is a symbolic power of* $u^{-1}(P)$.

(***) $$\text{emdim } R = \text{emdim } R/Q$$

and

$$\text{length}_{R/Q}\{0\} = \binom{\text{emdim } R/Q - \dim R/Q + \text{exponent}_{R/Q}\{0\} - 1}{\text{exponent}_{R/Q}\{0\}}.$$

Proof. — Follows from (3.5) by noting that if $A \to R$ is any epimorphism such that A is a regular local ring, then

$$\dim A \geq \text{emdim } R \geq \text{emdim } R/Q.$$

§ 4. Proof of Theorems 3, 4 and 5.

Let K be a valued field. Let R be an analytic local ring over K. Let $X_1, X_2, \ldots$ be indeterminates, and for every nonnegative integer d let $A_d = K[\langle X_1, \ldots, X_d \rangle]$. By card we shall denote cardinal number; note that for any infinite set N, $\text{card}(N) = \text{card}(N) - 1$.

(4.1) *Let* d *be a positive integer. Let* P *be a nonzero prime ideal in* A_d. *Let* Q *be an ideal in* A_d *such that* Q *is primary for* P, *and* $Q \subset P^{(2)}$. *Let* J *be an ideal in* A_d *such that* $J \not\subset Q$. *Let* $G_0 = G_K(A_d, J \cap P) \cap G_K[A_d, Q]$. *Then we have the following*:

1) *There exists* $G' \subset G_0$ *with* $\mathrm{card}(G') \geq \mathrm{card}(K) - 1$ *such that* $g(X_1) - h(X_1) \notin Q$ *for all* $g \neq h$ *in* G'.

2) *If there exists* $Z \in J \cap M(A_d)$ *with* $Z \notin Q$ *such that either* $Z \in M(A_d)^2$ *or* $Z \notin X_1 A_d + M(A_d)^2$, *then there exists* $G^* \subset G_0$ *with* $\mathrm{card}(G^*) \geq \mathrm{card}(K)$ *such that* $g(X_1) - h(X_1) \notin Q$ *for all* $g \neq h$ *in* G^*.

3) $G_0 \subset G_K(A_d, Q) \Leftrightarrow d = 1$, $\mathrm{card}(K) = 2$, *and* $Q = P^{(2)}$.

4) *If* $P \neq M(A_d)$ *then there exists an infinite subset* G *of* G_0 *such that* $g(X_1) - h(X_1) \notin Q$ *for all* $g \neq h$ *in* G.

Proof. — Since $J \not\subset Q$, there exists $Z \in J$ with $Z \notin Q$; in the general case we fix any such Z, and in case of 2) we take $Z \in J \cap M(A_d)$ with $Z \notin Q$ such that either $Z \in M(A_d)^2$ or $Z \notin X_1 A_d + M(A_d)^2$. Since Q is primary for P, there exists a positive integer m such that $P^m \subset Q$, and then $ZP^m \subset Q$; now $ZP^0 \not\subset Q$; therefore there exists a unique nonnegative integer n such that upon letting $B = ZP^n$ we have $B \not\subset Q$ and $BP \subset Q$. Since P is a nonzero prime ideal, we must have $M((A_d)_P) \neq 0$; consequently $M((A_d)_P) \neq M((A_d)_P)^2$, and hence $P \neq P^{(2)}$; since $Q \subset P^{(2)}$, we get $P \not\subset Q$. Now Q is primary for P, $BP \subset Q$, and $P \not\subset Q$; therefore $B \subset P$. Since $B = ZP^n$, it follows that $B \subset J \cap P$.

Let any $H \in G_K(A_d, B)$ and any $q \in Q$ be given. Since $B \subset P$ and $H \in G_K(A_d, B)$, by (2.1) and (2.2) we see that $H(P) = P$. Since $q \in Q \subset P^{(2)}$, we can write

$$rq = \sum_{i=1}^{e} y_i z_i \quad \text{with} \quad r \in A_d, \quad r \notin P, \quad y_i \in P, \quad z_i \in P.$$

Now
$$\begin{aligned} H(r)(H(q) - q) &= q(r - H(r)) + H(rq) - rq \\ &= q(r - H(r)) + \sum_{i=1}^{e} (H(y_i z_i) - y_i z_i) \\ &= q(r - H(r)) + \sum_{i=1}^{e} (H(y_i)(H(z_i) - z_i) + z_i(H(y_i) - y_i)); \end{aligned}$$

also
$$H(z_i) - z_i \in B \quad \text{and} \quad H(y_i) - y_i \in B \quad \text{for} \quad 1 \leq i \leq e$$

because $H \in G_K(A_d, B)$, and

$$H(y_i) \in P \quad \text{and} \quad z_i \in P \quad \text{for} \quad 1 \leq i \leq e$$

because $H(P) = P$; therefore

$$H(r)(H(q) - q) \in Q + BP.$$

Since $BP \subset Q$, we thus get $H(r)(H(q) - q) \in Q$; since $r \notin P$ and $H(P) = P$, we must also have $H(r) \notin P$; since Q is primary for P, we conclude that $H(q) - q \in Q$, and hence $H(q) \in Q$.

Thus we have shown that $H(Q) \subset Q$ for all $H \in G_K(A_d, B)$. Given any $H \in G_K(A_d, B)$, since $G_K(A_d, B)$ is a subgroup of $G_K(A_d)$ by (2.1), we have $H^{-1} \in G_K(A_d, B)$; consequently by what we have just shown we get that $H(Q) \subset Q$ and $H^{-1}(Q) \subset Q$;

therefore $H(Q)=Q$. Thus $G_K(A_d, B) \subset G_K[A_d, Q]$; since $B \subset J \cap P$, by (2.2) we also have $G_K(A_d, B) \subset G_K(A_d, J \cap P)$. Therefore

$$G(A_d, B) \subset G_0. \tag{5}$$

If $d=1$ and $\mathrm{card}(K)=2$ then for any basis (X_1') of $M(A_d)$ we would have $X_1'-X_1 \in M(A_d)^2=P^{(2)}$. Therefore, in view of (2.9) we get the following:

(6) If $d=1$ and $\mathrm{card}(K)=2$ then $G_K(A_d)=G_K(A_d, P^{(2)})$.

Since $B \not\subset Q$, we can take $Y \in B$ with $Y \notin Q$. Since $Y \in B$ and $B \subset P \subset M(A_d)$, we have $Y \in M(A_d)$.

For a moment suppose that $P \neq M(A_d)$. Then $X_j \notin P$ for some j. For every positive integer t we have $M(A_d)=(X_1+X_j^t Y, X_2, \ldots, X_d)A_d$ and hence by (2.15) we get $h_t \in G_K(A_d)$ with $h_t(X_1)=X_1+X_j^t Y$ and $h_t(X_i)=X_i$ for $2 \leq i \leq d$; now $X_j^t Y \in B$ and hence by (2.9) we see that $h_t \in G_K(A_d, B)$. For any integers $0<t<s$ we have $h_t(X_1)-h_s(X_1)=X_j^t Y(1-X_j^{s-t})$; since $X_j \notin P$, $Y \notin Q$, and Q is primary for P, we get that $X_j^t Y \notin Q$; also $1-X_j^{s-t}$ is a unit in A_d, and hence $h_t(X_1)-h_s(X_1) \notin Q$. In view of (5), this completes the proof of 4).

Now, reverting back to the general case (i.e., without assuming $P \neq M(A_d)$), in view of (5) and (6) we see that 1), 2) and 3) would follow from 1'), 2') and 3') respectively:

1') There exists $G' \subset G_K(A_d, B)$ with $\mathrm{card}(G') \geq \mathrm{card}(K)-1$ such that

$$g(X_1)-h(X_1) \notin Q$$

for all $g \neq h$ in G'.

2') If $Z \in M(A_d)$ and either $Z \in M(A_d)^2$ or $Z \notin X_1 A_d + M(A_d)^2$, then there exists $G^* \subset G_K(A_d, B)$ with $\mathrm{card}(G^*) \geq \mathrm{card}(K)$ such that $g(X_1)-h(X_1) \notin Q$ for all $g \neq h$ in G^*.

3') If either $d \geq 2$ or $\mathrm{card}(K)>2$ or $Q \neq P^{(2)}$, then $G_K(A_d, B) \not\subset G_K(A_d, Q)$.

We now proceed to prove 1'), 2') and 3').

Since $Y \in M(A_d)$, there exist unique elements $k_1, \ldots, k_d$ in K such that

$$Y+k_1X_1+\ldots+k_dX_d \in M(A_d)^2. \tag{7}$$

Let

$$K_0=\begin{cases} \{k \in K : k \neq 1/k_1\} & \text{if } k_1 \neq 0=k_2=\ldots=k_d, \\ K & \text{otherwise.} \end{cases} \tag{8}$$

If $k_2=\ldots=k_d=0$ then let $(X_2', \ldots, X_d')=(X_2, \ldots, X_d)$; and if $k_j \neq 0$ for some j with $2 \leq j \leq d$ then let $(X_2', \ldots, X_d')=(X_2, \ldots, X_{j-1}, Y, X_{j+1}, \ldots, X_d)$. Now $M(A_d)=(X_1, X_2', \ldots, X_d')A_d$ and hence by (2.15) we get $g^* \in G_K(A_d)$ with $g^*(X_1)=X_1$ and $g^*(X_i)=X_i'$ for $2 \leq i \leq d$. For any $k \in K_0$ we have $M(A_d)=(X_1+kY, X_2', \ldots, X_d')A_d$ and hence by (2.15) we get $g_k^* \in G_K(A_d)$ with $g_k^*(X_1)=X_1+kY$ and $g_k^*(X_i)=X_i'$ for

$2 \leq i \leq d$; let $g_k = g_k^* g^{*-1}$; then $g_k \in G_K(A_d)$ with $g_k(X_1) = X_1 + kY$ and $g_k(X_i') = X_i'$ for $2 \leq i \leq d$; since $kY \in B$, by (2.9) we see that $g_k \in G_K(A_d, B)$. Thus we have found

(9) $$g_k \in G_K(A_d, B) \quad \text{for all } k \in K_0.$$

For any $k \neq k'$ in K_0 we have $g_k(X_1) - g_{k'}(X_1) = (k-k')Y$; now $Y \notin Q$ and $k-k'$ is a unit in A_d; consequently $g_k(X_1) - g_{k'}(X_1) \notin Q$. Thus

(10) $$\text{for all } k \neq k' \text{ in } K_0 \text{ we have } g_k(X_1) - g_{k'}(X_1) \notin Q.$$

By (8) we have $\operatorname{card}(K_0) \geq \operatorname{card}(K) - 1$, and hence 1') follows from (9) and (10). Now $Y \in ZA_d$; consequently by (7) and (8) we see that if $Z \in M(A_d)$ and either $Z \in M(A_d)^2$ or $Z \notin X_1 A_d + M(A_d)^2$ then $K_0 = K$; therefore 2') also follows from (9) and (10).

Now only 3') remains to be proved.

By (9) and (10) we see that if $\operatorname{card}(K_0) > 1$ then $G_K(A_d, B) \not\subset G_K(A_d, Q)$; since always $\operatorname{card}(K) \geq 2$, by (8) we see that $\operatorname{card}(K_0) \geq 1$; therefore we get the following:

(11) $$\text{If } \operatorname{card}(K_0) \neq 1 \quad \text{then} \quad G_K(A_d, B) \not\subset G_K(A, Q).$$

By (8) we get (12) and (13):

(12) $$\text{If } \operatorname{card}(K) \neq 2 \quad \text{then} \quad \operatorname{card}(K_0) \neq 1.$$

(13) $$\text{If } \operatorname{card}(K_0) = 1 \quad \text{then} \quad k_1 \neq 0 = k_2 = \ldots = k_d.$$

If $d \geq 2$ and $k_2 = 0$ then $M(A_d) = (X_1, X_2 + Y, X_3, \ldots, X_d)A_d$ and hence by (2.15) we get $g' \in G_K(A_d)$ such that $g'(X_1) = X_1$, $g'(X_2) = X_2 + Y$, and $g'(X_i) = X$ for $3 \leq i \leq d$; since $Y \in B$, by (2.9) we have $g' \in G_K(A_d, B)$; since $Y \notin Q$, we also have $g' \notin G_K(A_d, Q)$. Thus we have proved the following:

(14) $$\text{If } d \geq 2 \quad \text{and} \quad k_2 = 0 \quad \text{then} \quad G_K(A_d, B) \not\subset G_K(A_d, Q).$$

If $d = 1$ and $k_1 \neq 0$ then clearly $YA_d = X_1 A_d = M(A_d) = P$; since $Y \in B$ and $BP \subset Q \subset P^{(2)}$, we then must have $Q = P^{(2)}$. Thus we have proved the following:

(15) $$\text{If } d = 1 \quad \text{and} \quad k_1 \neq 0 \quad \text{then} \quad Q = P^{(2)}.$$

Now 3') follows from (11), (12), (13), (14) and (15).

Theorem (**4.2**). — *Assume that* $\dim R = 0$ *and* $R \neq K$ (i.e., equivalently, $\dim R = 0$ and $M(R) \neq M(R)^2$). *Let* x *be any element in* $M(R)$ *with* $x \notin M(R)^2$. *Let* J *be any nonzero ideal in* R. *Then we have the following.*

1) $G_K(R, J) = \{1\}$
$\Leftrightarrow \operatorname{emdim} R = 1$, $\operatorname{card}(K) = 2$, *and* $M(R)^2 = \{0\}$
$\Leftrightarrow \operatorname{card}(K) = 2$ *and* R *is* K*-isomorphic to* $A_1/(X_1^2 A_1)$
$\Leftrightarrow \operatorname{card}(K) = 2$ *and* R *is isomorphic to* $A_1/(X_1^2 A_1)$
$\Leftrightarrow \operatorname{card}(R) = 4$
$\Leftrightarrow G(R) = \{1\}$
$\Leftrightarrow G_K(R) = \{1\}$

2) *There exists* $G' \subset G_K(R, J)$ *with* $\text{card}(G') \geq \text{card}(K) - 1$ *such that* $g(x) \neq h(x)$ *for all* $g \neq h$ *in* G'.

3) *If there exists* $0 \neq z \in J \cap M(R)$ *such that either* $z \in M(R)^2$ *or* $z \notin xR + M(R)^2$, *then there exists* $G^* \subset G_K(R, J)$ *with* $\text{card}(G^*) \geq \text{card}(K)$ *such that* $g(x) \neq h(x)$ *for all* $g \neq h$ *in* G^*.

4) *If either* $\text{emdim } R \neq 1$ *or* $M(R)^2 \neq \{0\}$, *then there exists* $G \subset G_K(R)$ *with* $\text{card}(G) \geq \text{card}(K)$ *such that* $g(x) \neq h(x)$ *for all* $g \neq h$ *in* G.

5) *If* $\text{card}(R) \neq 4$ *then there exists* $g \in G_K(R)$ *such that* $g(x) \neq x$.

Proof. — Upon letting $d = \text{emdim } R$, we can take $x_2, \ldots, x_d$ in R such that $M(R) = (x, x_2, \ldots, x_d)R$. Let $v : A_d \to R$ be the unique local K-homomorphism with $v(X_1) = x$ and $v(X_i) = x_i$ for $2 \leq i \leq d$; by (2.14) we know that v is surjective. Let $Q = \text{Ker } v$. Now Q is primary for $M(A_d)$, $Q \subset M(A_d)^2 = M(A_d)^{(2)}$, $v^{-1}(J) \not\subset Q$, and $G_K(A_d, v^{-1}(J) \cap M(A_d)) = G_K(A_d, v^{-1}(J))$. Also, we have the following:

6) If z is any nonzero element in $J \cap M(R)$ such that either $z \in M(R)^2$ or $z \notin xR + M(R)^2$, then upon taking any $Z \in v^{-1}(z)$ we have that $Z \in v^{-1}(J) \cap M(A_d)$, $Z \notin Q$, and either $Z \in M(A_d)^2$ or $Z \notin X_1 A_d + M(A_d)^2$.

Let $G_0 = G_K(A_d, v^{-1}(J)) \cap G_K[A_d, Q]$. By (4.1) we get 1'), 2') and 3'):

1') $G_0 \subset G_K(A_d, Q) \Leftrightarrow d = 1$, $\text{card}(K) = 2$, and $Q = M(A_d)^2$.

2') There exists $G_0' \subset G_0$ with $\text{card}(G_0') \geq \text{card}(K) - 1$ such that $g(X_1) - h(X_1) \notin Q$ for all $g \neq h$ in G_0'.

3') If there exists $Z \in v^{-1}(J) \cap M(A_d)$ with $Z \notin Q$ such that either $Z \in M(A_d)^2$ or $Z \notin X_1 A_d + M(A_d)^2$, then there exists $G_0^* \subset G_0$ with $\text{card}(G_0^*) \geq \text{card}(K)$ such that $g(X_1) - h(X_1) \notin Q$ for all $g \neq h$ in G_0^*.

Let $w : G_K[A_d, \text{Ker } v] \to G_K(R)$ be the homomorphism induced by v. Then by (2.3) and (2.4) we have $\text{Ker } w = G_K(A_d, Q)$ and $w(G_0) \subset G_K(R, J)$. In view of (2.5), 2) now follows from 2') by taking G' to be $w(G_0')$. In view of (2.5) and 6), 3) follows from 3') by taking G^* to be $w(G_0^*)$.

Since $\text{Ker } w = G_K(A_d, Q)$ and $w(G_0) \subset G_K(R, J)$, by 1') we get that:

$$G_K(R, J) = \{1\} \Rightarrow d = 1, \text{ card}(K) = 2, \text{ and } M(R)^2 = \{0\}.$$

Clearly: $d = 1$, $\text{card}(K) = 2$, and $M(R)^2 = \{0\}$
$\Rightarrow \text{card}(K) = 2$ and R is K-isomorphic to $A_1/(X_1^2 A_1)$
$\Rightarrow \text{card}(K) = 2$ and R is isomorphic to $A_1(X_1^2 A_1)$
$\Rightarrow \text{card}(R) = 4$;

and: $$G(R) = \{1\} \Rightarrow G_K(R) = \{1\} \Rightarrow G_K(R, J) = \{1\}.$$

For a moment suppose that $\text{card}(R) = 4$; now $\text{card}(K) \geq 2$, $x \notin K$, $1 + x \notin K$, and $x \neq 1 + x$; therefore we must have $\text{card}(K) = 2$ and $R = \{0, 1, x, 1 + x\}$; for any $g \in G(R)$ we must have $g(0) = 0$ and $g(1) = 1$; also $g(x) = x$ because $M(R) = \{x\}$; hence also $g(1 + x) = 1 + x$; therefore g is the identity automorphism. Thus: $\text{card}(R) = 4 \Rightarrow G(R) = \{1\}$. This completes the proof of 1).

To prove 4) assume that either $d \neq 1$ or $M(R)^2 \neq \{0\}$. If $d \neq 1$ then let $z = x_2$; if $d = 1$ and $M(R)^2 \neq \{0\}$ then let z be any nonzero element in $M(R)^2$. Now in both cases $0 \neq z \in M(R)$ and either $z \in M(R)^2$ or $z \notin xR + M(R)^2$. So take J to be zR and apply 3).

Finally, 5) follows from 1), 2), and 4).

Theorem **(4.3).** — *Assume that* $\dim R \neq 0$. *Let* Q *be an isolated primary component of* $\{0\}$ *in* R, *and let* $P = \mathrm{rad}_R Q$. *Let* $Q' = Q'_1 \cap \ldots \cap Q'_b$ *where* $Q'_1, \ldots, Q'_b$ *are any finite number of primary ideals in* R *with* $Q'_i \not\subset P$ *for* $1 \leq i \leq b$. *Let* J *be any ideal in* R *with* $J \not\subset Q$. *Let* x *be any element in* $M(R)$ *with* $x \notin M(R)^2$. *Assume that* $Q \neq P$ *and*:

(*) *there exists a* K-*epimorphism* $u : A_d \to R$, *for some* d, *such that* $u^{-1}(Q) \subset (u^{-1}(P))^{(2)}$.

Then there exists an infinite subset G *of* $G_K(R, J \cap P \cap Q') \cap G_K[R, Q]$ *with* $\mathrm{card}(G) \geq \mathrm{card}(K)$ *such that* $g(x) - h(x) \notin Q$ *for all* $g \neq h$ *in* G.

(Note that by (2.1) and (2.2) we then have $G \subset G_K[R, P]$ and $G \subset G_K[R, Q'_i]$ for $1 \leq i \leq b$.)

(For an intrinsic formulation of (*) see (3.4).)

(Note that if we assume $Q = P$ but keep all the other assumptions unchanged, then: $P = Q = \{0\} \neq J \cap Q' \cap M(R)^2$, $d > 0$, and u is an isomorphism. In view of (2.15) we can now identify R with A_d so that x gets identified with X_1. We can take $0 \neq y \in J \cap Q' \cap M(R)^2$. For every positive integer n and every $k \in K$, in view of (2.9) and (2.15), we get $g_{k,n} \in G_K(R, J \cap Q')$ with $g_{k,n}(x) = x + ky^n$ and $g_{k,n}(X_i) = X_i$ for $2 \leq i \leq d$. Clearly $g_{k,n}(x) \neq g_{k',n'}(x)$ whenever $(k, n) \neq (k', n')$.)

Proof. — By (3.4) we know that $d = \mathrm{emdim}\, R$, and hence we can take $x_2, \ldots, x_d$ in R such that $M(R) = (x, x_2, \ldots, x_d)R$. Let $v : A_d \to R$ be the unique local K-homomorphism with $v(X_1) = x$ and $v(X_i) = x_i$ for $2 \leq i \leq d$. By (2.14) we see that v is surjective, and then by (3.4) we see that $v^{-1}(Q) \subset (v^{-1}(P))^{(2)}$. Now $d > 0$, $v^{-1}(P)$ is a nonzero prime ideal in A_d with $v^{-1}(P) \neq M(A_d)$, and $v^{-1}(Q)$ is primary for $v^{-1}(P)$. Since Q is an isolated primary component of $\{0\}$ in R, we have $\{0\} = Q \cap Q^*$ with $Q^* = Q^*_1 \cap \ldots \cap Q^*_a$ where $Q^*_1, \ldots, Q^*_a$ are primary ideals in R with $Q^*_i \not\subset P$ for $1 \leq i \leq a$. Let $J_0 = J \cap Q^* \cap Q'$. Then $J_0 \not\subset Q$ and hence $v^{-1}(J_0) \not\subset v^{-1}(Q)$. Let

$$G_0 = G_K(A_d, v^{-1}(Q^*)) \cap G_K(A_d, v^{-1}(J \cap P \cap Q')) \cap G_K[A_d, v^{-1}(Q)].$$

Now $$G_K(A_d, v^{-1}(Q^*)) \cap G_K(A_d, v^{-1}(J \cap P \cap Q')) = G_K(A_d, v^{-1}(Q^*) \cap v^{-1}(J \cap P \cap Q'))$$

and $$v^{-1}(Q^*) \cap v^{-1}(J \cap P \cap Q') = v^{-1}(J_0) \cap v^{-1}(P).$$

Therefore by (4.1) there exists an infinite subset G′ of G_0 with $\mathrm{card}(G') \geq \mathrm{card}(K)$ such that $g(X_1) - h(X_1) \notin v^{-1}(Q)$ for all $g \neq h$ in G′.

By (2.1) we have

$$G_K(A_d, v^{-1}(Q^*)) \subset G_K[A_d, v^{-1}(Q^*)],$$

and clearly $$G_K[A_d, v^{-1}(Q^*)] \cap G_K[A_d, v^{-1}(Q)] \subset G_K[A_d, v^{-1}(Q^*) \cap v^{-1}(Q)]$$

and $$v^{-1}(Q^*) \cap v^{-1}(Q) = \mathrm{Ker}\, v.$$

Therefore $G_0 \subset G_K[A_d, \operatorname{Ker} v]$. Let $w : G_K[A_d, \operatorname{Ker} v] \to G_K(R)$ be the homomorphism induced by v. Now, in view of (2.4), we see that

$$w(G_0) \subset G_K(R, J \cap P \cap Q') \cap G_K[R, Q].$$

In view of (2.5) we see that w induces an injection of G', and $g(x) - h(x) \notin Q$ for all $g \neq h$ in $w(G')$. Therefore it suffices to take G to be $w(G')$.

Theorem **(4.4)**. — *Let* $J, Q_1, \ldots, Q_a$ $(a > 0)$ *be any ideals in* R *such that* $Q_1, \ldots, Q_a$ *are primary and* $J \cap Q_1 \cap \ldots \cap Q_a = \{0\}$. *Let* $P_i = \operatorname{rad}_R Q_i$. *Let* $v : R \to S$ *be a* K*-epimorphism where* S *is an analytic local ring over* K *and* $\operatorname{Ker} v = P_1 \cap \ldots \cap P_a$. *Let* $w : G_K[R, \operatorname{Ker} v] \to G_K(S)$ *be the homomorphism induced by* v. *Let*

$$G = G_K(R, J) \cap \bigcap_{i=1}^{a} G_K[R, P_i] \cap \bigcap_{i=1}^{a} G_K[R, Q_i],$$

and

$$G' = G_K(S, v(J)) \cap \bigcap_{i=1}^{a} G_K[S, v(P_i)].$$

Assume that:

(*) *there exists a* K*-epimorphism* $u : A_d \to R$, *for some* d, *such that* $u^{-1}(Q_i)$ *is a symbolic power of* $u^{-1}(P_i)$ *for* $1 \leq i \leq a$.

Then $w(G) = G'$.

(Note that clearly $G_K[R, P_1] \cap \ldots \cap G_K[R, P_a] \subset G_K[R, \operatorname{Ker} v]$, and hence it makes sense to talk about $w(G)$.)

(Note that (*) is automatically satisfied if $Q_i = P_i$ for $1 \leq i \leq a$, because then we can take u to be any K-epimorphism $A_d \to R$. For the case when $Q_i \neq P_i$ for some i, for an intrinsic formulation of (*) see (3.6).)

Proof. — Let $t : G_K[A_d, \operatorname{Ker} u] \to G_K(R)$ be the homomorphism induced by u. Let $v' = vu$ and let $w' : G_K[A_d, \operatorname{Ker} v'] \to G_K(S)$ be the homomorphism induced by v'. Let any $g' \in G'$ be given.

Clearly $v'(u^{-1}(J)) = v(J)$, and hence by (2.19) there exists $h \in G_K[A_d, \operatorname{Ker} v']$ such that $h \in G_K(A_d, u^{-1}(J))$ and $w'(h) = g'$. By (2.1) we see that $h(u^{-1}(J)) = u^{-1}(J)$.

Now $\operatorname{Ker} v' \subset u^{-1}(P_i)$ and $v'(u^{-1}(P_i)) = v(P_i)$, and hence by (2.4) we get that $h \in G_K[A_d, u^{-1}(P_i)]$, i.e., $h(u^{-1}(P_i)) = u^{-1}(P_i)$. Therefore there exists a unique automorphism of the quotient ring B_i of A_d with respect to $u^{-1}(P_i)$ such that $h_i(x) = h(x)$ for all $x \in A_d$. For every positive integer n we now have

$$h(M(B_i)^n \cap A_d) = h_i(M(B_i)^n \cap A_d) = h_i(M(B_i)^n) \cap h_i(A_d) = M(B_i)^n \cap A_d;$$

since $u^{-1}(Q_i)$ is a symbolic power of $u^{-1}(P_i)$, we conclude that $h(u^{-1}(Q_i)) = u^{-1}(Q_i)$.

Thus $h(u^{-1}(J)) = u^{-1}(J)$ and $h(u^{-1}(Q_i)) = u^{-1}(Q_i)$ for $1 \leq i \leq a$; clearly

$$\operatorname{Ker} u = u^{-1}(J) \cap u^{-1}(Q_1) \cap \ldots \cap u^{-1}(Q_a),$$

and hence $h(\operatorname{Ker} u) = \operatorname{Ker} u$. Thus $h \in G_K[A_d, \operatorname{Ker} u]$ and upon letting $g = t(h)$, in view of (2.6), we see that $g \in G_K[R, \operatorname{Ker} v]$ and $w(g) = w(t(h)) = w'(h) = g'$. Now

$h \in G_K(A_d, u^{-1}(J))$, $h \in G_K[A_d, u^{-1}(P_i)]$ for $1 \leq i \leq a$, and $h \in G_K[A_d, u^{-1}(Q_i)]$ for $1 \leq i \leq a$; consequently, in view of (2.4), we have $g \in G$.

Thus we have shown that, given any $g' \in G'$ there exists $g \in G$ with $w(g) = g'$. Now, in view of (2.4), $w(G) \subset G'$, and hence we conclude that $w(G) = G'$.

§ 5. Rigid subfields.

Let K be a valued field. Let $A = K[\langle X \rangle]$ where X is an indeterminate.

Let $z_1, \ldots, z_e$ be any given finite number of elements in K. Let L be the field generated by $z_1, \ldots, z_e$ over the prime subfield of K.

Take $z_0 = 1$. We can take positive integers m, n, q, d such that: $q + qe < m$; $m + q + qe < n$; n is not divisible by the characteristic of K; $n + m \leq d$; and n and d are coprime. Now we can take $Y = Y(X) \in A$ such that the coefficient of X^d in $Y(X)$ is nonzero and

$$Y = X^{n+m} + \sum_{i=0}^{e} z_i X^{n+m+q+qi} + Y' \quad \text{with} \quad Y' \in X^{n+m+q+qe+1}A.$$

Let $R = K[\langle X^n, Y \rangle]$. Then clearly R is a one-dimensional analytic local domain over K, with $\operatorname{emdim} R = 2$.

(5.1) A *is the integral closure of* R *in the quotient field of* R.

Proof. — Clearly A is the integral closure of R in $K(\langle X \rangle]$, $K(\langle X^n \rangle)$ is contained in the quotient field of R, and $[K(\langle X \rangle) : K(\langle X^n \rangle)] = n$; consequently it suffices to show that $[K(\langle X^n \rangle)(Y) : K(\langle X^n \rangle)] \geq n$. Let K′ be an algebraic closure of K. Let v be a primitive n-th root of 1 in K′. We have a unique K′-automorphism h_j of $K'[[X]]$ such that $h_j(X) = v^j X$; h_j extends uniquely to an automorphism of $K'((X))$ which we continue to denote by h_j; clearly h_j is then a $K'((X^n))$-automorphism of $K'((X))$. Now $Y = \sum_i y_i X^i$ with $y_i \in K$ for $i = 0, 1, 2, \ldots$, and $y_d \neq 0$; we have $h_j(Y) = \sum_i y_i v^{ij} X^i$; since n is not divisible by the characteristic of K, and n and d are coprime, we see that $v^{d1}, \ldots, v^{dn}$ are pairwise distinct; since $y_d \neq 0$, we get that $h_1(Y), \ldots, h_n(Y)$ are pairwise distinct. Thus Y has n distinct $K'((X^n))$-conjugates in $K'((X))$, and hence $[K'((X^n))(Y) : K'((X^n))] \geq n$. Since $K(\langle X^n \rangle) \subset K'((X^n))$, we must also have $[K(\langle X^n \rangle)(Y) : K(\langle X^n \rangle)] \geq n$.

(5.2) *Let* $r \in R$ *be such that* $0 < \operatorname{ord}_A r < 2n$. *Then* $\operatorname{ord}_A r =$ *either* n *or* $n + m$.

Proof. — Since $r \in R$ and $\operatorname{ord}_A r > 0$, we can write $r = aX^n + bY + r'$ where $a \in K$, $b \in K$, and $r' = sX^{2n} + tX^nY + uY^2$ with $s \in R$, $t \in R$, $u \in R$. Since $\operatorname{ord}_A Y = n + m > n$, we have $\operatorname{ord}_A r' \geq 2n$. Since $\operatorname{ord}_A r < 2n$, we see that $\operatorname{ord}_A r = \operatorname{ord}_A(aX^n + bY) =$ either n or $n + m$.

(5.3) *Let* g *be any automorphism of* R. *Then* $g(z) - z \in M(R)$ *for all* $z \in L$. *Whence, in particular, if* $g(K) = K$ *then* $g(z) = z$ *for all* $z \in L$.

(Note that by (2.12) we know that if K is a perfect field of nonzero characteristic then $g(K) = K$ for all $g \in G(R)$.)

Proof. — In view of (5.1), we can uniquely extend g to an automorphism of A which we continue to denote by g. Now $\mathrm{ord}_A g(X)=1$ and hence there exists $0\neq k\in K$ with $\mathrm{ord}_A(g(X)-kX)>1$.

Suppose if possible that $\mathrm{ord}_A(g(X)-kX)\leq m$. Then $g(X)=kX(1+EX^u)$ where u is an integer with $0<u<m$ and E is a unit in A. Now

$$g(X^n)=k^nX^n(1+nEX^u+\text{an element in } X^{u+1}A);$$

since n is not divisible by the characteristic of K, we get that $\mathrm{ord}_A(g(X^n)-k^nX^n)=n+u$; since $n<n+u<n+m<2n$ and $g(X^n)-k^nX^n\in R$, we have a contradiction by (5.2).

Therefore $g(X)=kX(1+DX^m)$ with $D\in A$. Now

$$k^{-n-m}g(Y)=k^{-n-m}g(Y')+X^{n+m}(1+DX^m)^{n+m}$$
$$+\sum_{i=0}^{e}g(z_i)k^{q+qi}X^{n+m+q+qi}(1+DX^m)^{n+m+q+qi};$$

since $Y'\in X^{n+m+q+qe+1}A$, we have

$$g(Y')\in X^{n+m+q+qe+1}A;$$

also, for all $j\geq 0$ we have

$$X^{n+m+j}(1+DX^m)^{n+m+j}=X^{n+m+j}+\text{an element in } X^{n+2m+j}A$$
$$=X^{n+m+j}+\text{an element in } X^{n+m+q+qe+1}A \quad \text{because } q+qe<m.$$

Consequently $k^{-n-m}g(Y)-Y=\sum_{i=0}^{e}(g(z_i)k^{q+qi}-z_i)X^{n+m+q+qi}$
$$+\text{an element in } X^{n+m+q+qe+1}A.$$

Since $k^{-n-m}g(Y)-Y\in R$ and $n+m+q+qe<2n$, in view of (5.2) we now conclude that

$$g(z_i)k^{q+qi}-z_i\in M(A) \quad \text{for } 0\leq i\leq e.$$

Since $z_0=1$, we have $g(z_0)=1$; consequently $k^q-1\in M(R)$ and hence $k^q=1$. Therefore $k^{q+qi}=1$ for all i, and hence

$$g(z_i)-z_i\in M(A) \quad \text{for } 1\leq i\leq e.$$

Let $w: A\to A/M(A)$ be the canonical epimorphism. Now $g(M(A))=M(A)$ and hence g induces $g'\in G(w(A))$. Since $g(z_i)-z_i\in M(A)$, we get that $w(z_i)\in \mathrm{Inv}\{g'\}$; by (2.7) we know that $\mathrm{Inv}\{g'\}$ is a subfield of $w(A)$, and hence we must have $w(L)\subset \mathrm{Inv}\{g'\}$. Therefore

$$g(z)-z\in M(A)\cap R=M(R) \quad \text{for all } z\in L.$$

Purdue University, Lafayette, Indiana, U.S.A.

REFERENCES

[1] S. S. Abhyankar, *Ramification theoretic methods in algebraic geometry*, Princeton, Princeton University Press, 1959.

[2] S. S. Abhyankar, *Local analytic geometry*, New York, Academic Press, 1964.

[3] S. S. Abhyankar, T. T. Moh and M. Van der Put, Invariants of analytic local rings, *Publ. math. I.H.E.S.*, n° 36 (1969), p. 165-193.

[4] S. S. ABHYANKAR and M. VAN DER PUT, Homomorphisms of analytic local rings, forthcoming in *J. für die reine und angew. Math.*

[5] M. NAGATA, Note on complete local integrity domains, *Memoirs of the College of Science, University of Kyoto*, vol. 28 (1953-1954), pp. 271-278.

[6] M. NAGATA, *Local rings*, New York, John Wiley and Sons, 1962.

[7] P. SAMUEL, Algébraïcité de certains points singuliers algébroïdes, *Journal de Mathématiques*, vol. 35 (1956), pp. 1-6.

[8] O. ZARISKI and P. SAMUEL, *Commutative algebra*, vol. I, Princeton, Van Nostrand, 1958.

[9] O. ZARISKI and P. SAMUEL, *Commutative algebra*, vol. II, Princeton, Van Nostrand, 1960.

[10] O. ZARISKI, Studies in equisingularity: III. Saturation of local rings and equisingularity, *American Journal of Mathematics*, vol. 90 (1968), pp. 961-1023.

Manuscrit reçu le 14 février 1969.