SYMBOLIC POWERS IN NOETHERIAN DOMAINS[1]

BY

M. HOCHSTER

0. Introduction

We say that a function v from a ring ($\equiv$ commutative ring with unit) A to the nonnegative integers $\mathbf{N}$ is a *control* if for any two nonzero elements a, b of A and each prime ideal P of A, $ab \notin P^{(n)}$, where $n = v(a) + v(b) + 1$, and $P^{(n)}$ is the n^{th} symbolic power of P, i.e.

$$P^{(n)} = \{p \in A : \text{for some } c \in A - P,\ cp \in P^n\}.$$

We also say that A is *v-controlled*. A is called *controlled* if it is v-controlled for some v. (Note that the value of $v(0)$ is quite irrelevant.)

The condition that a ring be controlled is rather strong, since the value of $v(a)$ does not depend on either b or P. However, the author knows of no Noetherian domain which is not controlled. On the other hand, it is quite difficult to prove that given domains are controlled, and many obvious conjectures (e.g. a finitely generated extension domain of a controlled Noetherian domain is controlled) remain unverified.

The object of this paper is to prove that a large class of Noetherian domains *is* controlled. In fact, we will prove the following:

THEOREM. *Let A be a Noetherian domain such that either* (a) *each element is contained in only finitely many maximal ideals*; (b) *A is finitely generated over a Dedekind domain* (*we regard fields as Dedekind domains*); *or* (c) *A is a restricted power series ring over a local domain. Then A is controlled. In particular, local and semilocal domains are controlled.*

The proofs depend in part on the fact that if (A, M) is a regular local ring and P is any prime ideal of A, then for each $n \in \mathbf{N}$, $P^{(n)} \subset M^n$. This result, which was proved independently by Zariski and Nagata, is equivalent to Theorem 1 of [3], where Zariski's proof, utilizing monoidal transformations, is presented. We include here a completely different proof for the unramified case (§4), which depends on the theory of §2 and on analyzing the relationship between symbolic powers in $A[[t]]$ and $A[t]$, where A is local and t is an analytic indeterminate. For Nagata's proof, see [6, p. 143].

At this point we ought to point out that a controlled ring *must* be a domain. For if a, b are not zero and P is any prime, $ab \notin P^{(n)}$, where

$$n = v(a) + v(b) + 1,$$

and thus $ab \neq 0$.

Received August 19, 1968.

[1] This research was partially supported by a National Science Foundation grant.

The question of whether a control exists for a given ring is a global question, since there is no dependence on P. This is one difficulty in the proofs. We note that our proofs of the existence of controls are constructive enough so that if the ring is given in an effective way, the control can be exhibited. Our main technique is to consider various kinds of homomorphisms ($\equiv$ unitary homomorphisms) $A \to B$ and find conditions under which the existence of a control for A implies the existence of one for B, or vice versa. This is a delicate matter. For example, the adjunction of indeterminates and certain kinds of integral extension can be dealt with very nicely. On the other hand, one might naturally conjecture that the adjunction of a fraction to a controlled Noetherian domain yields a controlled ring, but the author cannot prove this, even if the extension is integral to boot. Again, if A is a controlled Noetherian domain, M is contained in the Jacobson radical of A, and the completion of A with respect to M is a domain, one might well conjecture that the completion is controlled, but at the moment this can be proved only in special cases. Similarly, it is not known whether A controlled $\Rightarrow A[[t]]$ controlled, t an analytic indeterminate over A.

Residue class domains of controlled rings need not be controlled in general, but this might be true in the Noetherian case. There does not seem to be any way of approaching it.

Even the fact that regular local rings are controlled (all local domains are) is not obvious. It is well known [6, p. 203] that in a complete local domain the symbolic powers of any prime are eventually contained in higher and higher powers of the maximal ideal, and our results are related to theorems of this kind, but they are mostly in a somewhat different direction.

Most of the results of this paper are greatly improved forms of theorems in the last part of the author's doctoral thesis [4, §10], where he considered the much weaker property s-boundedness. (A ring was defined to be *s-bounded* if for each nonzero a there existed an n such that for every prime P, $a \notin P^{(n+1)}$. A controlled ring satisfies this condition trivially: take $n = v(a) + v(1)$ and apply the definition with $b = 1$.) Our results here can be specialized to obtain all the results of §10 of [4]. The rest of the thesis will appear separately [5].

Added in proof. Define a control v to be *strong* if for all $a, b \neq 0$, $v(ab) \leq v(a) + v(b)$ and for all $a \neq 0$ and for every prime P, $a \notin P^{(v(a)+1)}$. The results of this paper go through almost without exception for strong controls, with only slight modifications of the proofs. In particular, the theorem above can be strengthened to assert that A has a strong control.

With regard to the use of the terms "local", "semilocal", "quasilocal", etc. we follow [6]. An indeterminate over a ring A will frequently be regarded, tacitly, as an indeterminate over various rings associated with A, e.g. residue class rings and localizations. If P is a prime ideal of A, A_P represents, as usual, the localization $(A - P)^{-1}A$ of A at P. If A is a domain, A^* represents the field of fractions of A. Finally, if I is an ideal, $\sqrt{I}$ represents the radical of I.

1. Basic facts about controls

We observe that the function which is constantly one is a control for any given field. For a Dedekind domain A and a nonzero $a \in A$, let $P_1^{n_1} \cdots P_k^{n_k}$ be the prime factorization of aA and let $v(a) = \max_i n_i$. Let $v(0) = 0$. Then v is a control for A.

If A is v-controlled and S is a multiplicative system in A, then $S^{-1}A$ is controlled. In fact, for each $0 \neq u \in S^{-1}A$ choose $s_u \in S$ such that $s_u u \in A$ and let $v_1(u) = v(s_u u)$. Let $v_1(0) = 0$. It is trivial to verify that v_1 is a control for $S^{-1}A$. We see that by taking $s_u = 1$ whenever $u \in A$, we may assume that $v_1 |_A = v$.

We also have this useful fact.

PROPOSITION 1.1. *Let $h_i : A \to B_i$ be an injective homomorphism from the domain A into the v_i-controlled domain B_i, where i runs through a finite index set, and suppose $\bigcup_i \operatorname{Im} \operatorname{Spec} h_i = \operatorname{Spec} A$, i.e. for each prime P of A there is an i and a prime Q of B_i such that $h_i^{-1}(Q) = P$. Then A is controlled. In fact, v defined by $v(a) = \max_i v_i(h_i(a))$ for all $a \in A$ is a control. It is not even necessary to assume that the index set is finite if we know in some other way that $\max_i v_i(h_i(a)) < \infty$ for every a.*

Proof. Let a, b be nonzero elements of A and let P be a given prime of A. Choose i and a prime Q of B_i such that $h_i^{-1}(Q) = P$. Then $h_i(a), h_i(b)$ are nonzero elements of B_i, so that $h_i(a)h_i(b) = h_i(ab) \notin Q^{(n)}$, where

$$n = v_i(h_i(a)) + v_i(h_i(b)) + 1 \leq v(a) + v(b) + 1.$$

But then $ab \notin h_i^{-1}(Q^{(n)}) \supset P^{(n)}$, and the result follows.

COROLLARY 1.2. *If $h : A \to B$ is injective and $\operatorname{Spec} h$ is surjective, then if B is v-controlled, $v|_A$ is a control for A. In particular, this holds if B is an integral or a faithfully flat extension of A.*

We conclude this section with some trivial observations.

(1.3) If v is a control for A and $v_1 \geq v$ is integer-valued, then v_1 is a control for A.

(1.4) *If* $\mathfrak{V}$ is a chain of controls for A then the (pointwise) minimum of the elements of $\mathfrak{V}$ is a control for A. Hence if A is controlled it has a minimal control.

(1.5) If $\mathfrak{A}$ is a family of subrings of C directed by inclusion whose union is C and each $A \in \mathfrak{A}$ has a control v_A such that if $A, B \in \mathfrak{A}$ and $A \subset B$ then $v_A = v_B |_A$, then the function on C whose graph is the union of the graphs of the v_A is a control for C.

2. Adjunction of indeterminates

Let v be a control for A. We want to show, among other things, that if $\{t_\lambda\}_{\lambda \in \Lambda}$ is a family of indeterminates over A, then $A[t_\lambda : \lambda \in \Lambda]$ is also controlled, and we want to see the explicit relation of a control for it to v.

We first discuss the case of one indeterminate t. Let $B = A[t]$. We need to consider in detail the relation between primes of B and primes of A. Let Q be a prime of B and let $P = Q \cap A$. Let $d_Q = [(B/Q)^* : (A/P)^*]$ (possibly, $d_Q = \infty$). Then either $Q = PB$, in which case $d_Q = \infty$, or else $1 \leq d_Q < \infty$ and there is an element $H \in B$ of degree d_Q with leading coefficient not in P, unique modulo P, such that the image of H modulo P is irreducible in $(A/P)^*[t]$ and

$$Q = \{q \in B: \text{for some } a \in A - P,\ aq \in PB + HB\}.$$

Conversely, if P is a prime in A, PB is prime in B, and if $H \in B$ is of degree $d \geq 1$ with leading coefficient not in P and the image of H modulo P is irreducible in $(A/P)^*[t]$, then

$$Q(P, H) = \{q \in B: \text{for some } a \in A - P,\ aq \in PB + HB\}$$

is prime, and $d_{Q(P,H)} = d$.

PROPOSITION 2.1. *With notation as above, if $d_Q < \infty$, and J is an ideal of B such that $Q \subset \sqrt{J}$ properly, then J meets $A - P$.*

Hence, for each $n \in \mathbf{N}$,

$$Q^{(n)} = \{b \in B: \textit{for some } a \in A - P,\ ab \in (PB + HB)^n\}$$
$$= \{b \in B: \textit{for some } a \in A - P,\ ab \in \textstyle\sum_{i=0}^{n} P^i H^{n-i} B\}.$$

Proof. Reducing modulo P, we can assume $Q \cap A = (0)$. Then $QA^*[t] = HA^*[t]$, a maximal ideal, while $(\sqrt{J})A^*[t]$ is larger, so that $(\sqrt{J})A^*[t] = A^*[t]$. But this is impossible if $\sqrt{J} \cap A = (0)$, so that $\sqrt{J}$ meets $A - (0)$, and it follows at once that J meets $A - (0)$. This proves the first statement.

To prove the second part, let $b \in Q^{(n)}$ be given and let $J = Q^n : b$. Then $\sqrt{J}$ properly contains Q, so that $Q^n : b$ meets $A - P$, and the result then follows from the form of Q.

PROPOSITION 2.2. *If $d_Q = \infty$, i.e. if $Q = PB$, then for each $n \in \mathbf{N}$, $Q^n = P^n B$ and $Q^{(n)} = P^{(n)} B$.*

The proof is straightforward, and is omitted.

PROPOSITION 2.3. *If $d_Q < \infty$, $b \in B - \{0\}$, say $b = \sum_{i=0}^{m} a_i t^i$, and $a_i \in P^{(k)}$, $i > j$, but $a_j \notin P^{(k)}$, then $b \notin Q^{(k+r)}$, where r is any integer $> (j/d_Q) - 1$. In particular, if $a_m \notin P^{(k)}$ then $b \notin Q^{(k+m)}$, and if $m = 0$, i.e. $b = a_0$, and $a_0 \notin P^{(k)}$, then $a_0 \notin Q^{(k)}$. Thus $Q^{(k)} \cap A = P^{(k)}$. This last statement holds when $d_Q = \infty$ as well.*

Proof. Let $Q = Q(P, H)$. Say $b \in Q^{(k+r)}$. Then, by (2.1), for some $a \in A - P$, $ab \in (PB + HB)^{k+r} \subset P^{(k)} B + H^{r+1} B$. Modulo $P^{(k)}$ we have $ab \equiv H^{r+1} c$ for some $c \in B$. The leading coefficient of $H \notin P \Rightarrow$ the right hand side is 0 or has degree $\geq (r + 1)\, d_Q$, according as $c \equiv 0$ or $c \not\equiv 0$. But the

degree of the left hand side is j, whence $c \neq 0$ and $j \geq (r+1)\,d_Q$, contradicting the condition on r. The other statements follow trivially.

Now let ∂ be the function which assigns to each polynomial in $B[t]$ its degree ($\partial(0) = 0$ for this purpose) and let ζ be the function which assigns to each polynomial in $B[t]$ its leading coefficient ($\zeta(0) = 0$ as well).

THEOREM 2.4. *If v is a control for A, then $v\zeta + \partial$ is a control for $B = A[t]$.*

Proof. Let $b, b' \in B - \{0\}$ have leading coefficients a, a', respectively, and degrees m, m'. bb' has leading coefficient aa' and degree $m + m'$. Let

$$\begin{aligned} n &= (v\zeta + \partial)(b) + (v\zeta + \partial)(b') + 1 \\ &= v(a) + v(a') + 1 + m + m' = k + m + m', \end{aligned}$$

where $k = v(a) + v(a') + 1$. Now $aa' \notin P^{(k)}$, where $P = Q \cap A$. If $d_Q = \infty$, this implies, by (2.2), that $bb' \notin Q^{(k)} \supseteq Q^{(n)}$, and we are done. If $d_Q < \infty$ then (2.3) gives that $bb' \notin Q^{(k+m+m')} = Q^{(n)}$, as required.

COROLLARY 2.5. *Let $t_1, \cdots, t_r$ be indeterminates over the v-controlled ring A, and let $B = A[t_1, \cdots, t_r]$. Let $b = \sum_\nu a_\nu t_1^{\nu_1} \cdots t_r^{\nu_r} \in B$, where ν runs over r-tuples of nonnegative integers $(\nu_1, \cdots, \nu_r)$. Let*

$$v_1(b) = \max_\nu (v(a_\nu) + \nu_1 + \cdots + \nu_r).$$

(Let $v_1(0) = 0$.) Then v_1 is a control for B.

Proof. We may construct a control for B inductively, using (2.4) to get controls for $A[t_1]$, $A[t_1, t_2]$, $\cdots$, B successively. It is quite easy to see that the value of this control on $b \neq 0$ is one of the terms $v(a_\nu) + \nu_1 + \cdots + \nu_r$. Now apply (1.3).

COROLLARY 2.6. *Let $\{t_\lambda\}_{\lambda \in \Lambda}$ be a family of indeterminates over the controlled ring A. Then $A[t_\lambda : \lambda \in \Lambda]$ is controlled.*

Proof. For each finite subset $\{t_1, \cdots, t_r\}$ of the family of indeterminates, define a control on $A[t_1, \cdots, t_r]$ as in (2.5). Then apply (1.5).

We conclude this section with a result which we shall need in §4.

PROPOSITION 2.7. *Let $B = A[t]$, as before, let $Q = Q(P, H)$ be a prime of B, and suppose that, in addition, H is monic. Then for each $n \in \mathbf{N}$, $Q^{(n)} = \sum_{i=0}^{n} P^{(i)} H^{n-i} B$.*

Proof. It is clear that $Q^{(n)} \supseteq \sum_{i=0}^{n} P^{(i)} H^{n-i} B$. To prove the other inclusion, let $b \in Q^{(n)}$. By (2.1) we can choose $a \in A - P$ such that

$$ab \in \sum_{i=0}^{n} P^i H^{n-i} B \subset \sum_{i=0}^{n} P^{(i)} H^{n-i} B.$$

We shall now prove by induction on j that for each j, $-1 \leq j \leq n-1$, we can choose b_j such that

$$ab_j \in \sum_{i=j+1}^{n} P^{(i)} H^{n-i} B \quad \text{and} \quad b - b_j \in \sum_{i=0}^{j} P^{(i)} H^{n-i} B.$$

Once we have shown this, we can let $j = n - 1$, and we will have

$$ab_{n-1} \in P^{(n)}B \quad \Rightarrow \quad b_{n-1} \in P^{(n)}B,$$

while $b - b_{n-1} \in \sum_{i=0}^{n-1} P^{(i)}H^{n-i}B$, whence $b \in \sum_{i=0}^{n} P^{(i)}H^{n-i}B$, as required.

We take $b_{-1} = b$. Now suppose that we have b_{j-1}, $j \geq 0$, satisfying the condition and we wish to find b_j. $ab_{j-1} \in \sum_{i=j}^{n} P^{(i)}H^{n-i}B$; hence, ab_{j-1} is a multiple of H^{n-j} mod $P^{(j+1)}B$. Now, H is monic $\Rightarrow H^{n-j}$ is monic. Hence, for suitable q and $r \in B$, $b_{j-1} \equiv qH^{n-j} + r \bmod P^{(j+1)}B$ and $\deg r < \deg H^{n-j}$. Moreover, r and q are uniquely determined mod $P^{(j+1)}B$. Now, since $ab_{j-1} \equiv aqH^{n-j} + r \bmod P^{(j+1)}B$ and since ab_{j-1} is a multiple of $H^{n-j} \bmod P^{(j+1)}B$, it follows that ar is also. But $a \notin P \Rightarrow a$ is not a zero divisor mod $P^{(j+1)}B$, and we can conclude that $r \equiv 0 \bmod P^{(j+1)}B$. Thus, for suitable $q \in B$ and $r \in P^{(j+1)}B$ we have $b_{j-1} = qH^{n-j} + r$. We take $b_j = r$.

Abbreviate $J = \sum_{i=j+1}^{n} P^{(i)}H^{n-i}B$. To complete the proof, we must show that $ab_j = ar \in J$ and $b - b_j = b - r \in \sum_{i=0}^{j} P^{(i)}H^{n-i}B$. We first observe that $b - r = (b - b_{j-1}) + (b_{j-1} - r)$ and since $b - b_{j-1} \in \sum_{i=0}^{j} P^{(i)}H^{n-i}B$, it will be enough to prove, for the second part, that $b_{j-1} - r \in P^{(j)}H^{n-j}B$. Now, $b_{j-1} - r = qH^{n-j}$, so that it suffices to show that $q \in P^{(j)}B$. Now

$$r \in P^{(j+1)}B \subset P^{(j)}B \quad \text{and} \quad ab_{j-1} \in \sum_{i=j}^{n} P^{(i)}H^{n-i}B \subset P^{(j)}B.$$

Hence, $aH^{n-j}q = a(b_{j-1} - r) = ab_{j-1} - ar \in P^{(j)}B$, which is the j^{th} symbolic power of PB. Since H is monic and $a \notin P$, we have that $aH^{n-j} \notin PB$, so that $q \in P^{(j)}B$, as required.

It remains to show that $ar \in J$. Now,

$$r \in P^{(j+1)}B \quad \text{and} \quad ar = a(b_{j-1} - qH^{n-j}),$$

where $qH^{n-j} \in P^{(j)}H^{n-j}B$ and $b_{j-1} \in \sum_{i=j}^{n} P^{(i)}H^{n-i}B$, so that $ar \in \sum_{i=j}^{n} P^{(i)}H^{n-i}B$. But then

$$ar \in P^{(j+1)}B \cap (\textstyle\sum_{i=j}^{n} P^{(i)}H^{n-i}B) = P^{(j+1)}B \cap (P^{(j)}H^{n-j}B + J).$$

Since $J \subset P^{(j+1)}B$, $ar \in (P^{(j+1)}B \cap P^{(j)}H^{n-j}B) + J$. Since $H \notin PB$, it is easy to see that

$$P^{(j+1)}B \cap P^{(j)}H^{n-j}B = P^{(j+1)}H^{n-j}B \subset P^{(j+1)}H^{n-j-1}B \subset J,$$

and $ar \in J$. This completes the proof.

3. Integral extensions

We restate part of (1.2).

COROLLARY 3.1. *If B is a controlled integral extension of A, then A is controlled.*

The converse is false in general. For example, the ring of integers $\mathbf{Z}$ is controlled, but $\mathbf{Z}[2^{\varepsilon} : \varepsilon = \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \cdots]$ is not controlled, because 2 is in every power of the ideal generated by the elements $\{2^{\varepsilon} : \varepsilon = \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \cdots\}$. The author does not know whether, in general, a finitely generated integral extension domain of

a controlled domain must be controlled. However, the partial results of this section may be applied in a great many cases.

THEOREM 3.2. *Let A be a domain, and let c be an element of an algebraic closure of A^* whose monic irreducible equation over A^* actually has all of its coefficients in A. (This condition is satisfied automatically if A is normal and c is integral over A.) Then $C = A[c]$ is controlled if A is.*

The proof depends on the following result.

PROPOSITION 3.3. *With the same hypothesis as* (3.2), *let d be the degree of c over A. Then for each prime ideal R of C and each $r \in \mathbf{N}$, we have $R^{((d+1)r-1)} \cap A \subset P^{(r)}$, where $P = R \cap A$.*

Before proving (3.3), we show how to deduce (3.2) from it. Let v be a control for A. For each $c \in C$, let $v_1(c) = (d+1)v(\eta(a)) + [d/2]$ (here, $[\ ]$ is the integral part function), where $\eta(a)$ is the field norm of a from C^* to A^*, and is actually a nonzero element of $aC \cap A$. Now

$$ab \in R^{(n)} \Rightarrow \eta(a)\eta(b) \in R^{(n)} \cap A \Rightarrow \eta(a)\eta(b) \in P^{(r)}$$

for each r such that $(d+1)r - 1 \leq n$. But we must have

$$r \leq v(\eta(a)) + v(\eta(b)) \quad \Rightarrow \quad (d+1)(v(\eta(a)) + v(\eta(b)) + 1) - 1 > n,$$

i.e. $n < (d+1)v(\eta(a)) + (d+1)v(\eta(b)) + d$. But

$$v_1(a) + v_1(b) + 1 = (d+1)v(\eta(a)) + (d+1)v(\eta(b)) + 2[d/2] + 1$$

and $2[d/2] + 1 \geq d$, so that $ab \notin R^{(n)}$ when $n = v_1(a) + v_1(b) + 1$.

The following is an obvious consequence of (3.2).

COROLLARY 3.4. *Let A be a domain, K an algebraic closure of A^*, and let $\mathcal{C}(A)$ be the least class of extensions C of A in K closed under the two operations* (a) *passing to an A-subalgebra and* (b) *adjoining an element whose monic irreducible equation over the fraction field of the domain has all its coefficients in the domain.*

Then if A is controlled, so is every ring in $\mathcal{C}(A)$.

It is not difficult to show that for each $C \in \mathcal{C}(A)$, we must have $C \cap A^* = A$. The author does not know whether every finitely generated integral extension C of A in K such that $C \cap A^* = A$ must be in $\mathcal{C}(A)$, or whether, if A is normal, every finitely generated integral extension of A in K must be in $\mathcal{C}(A)$.

It remains to establish (3.3).

Proof of (3.3). Let $F \in B = A[t]$ be the monic irreducible polynomial of c over A^*. Then there is a unique A-isomorphism $\phi : B/FB \cong C$ such that $\phi(t) = c$. We identify C with B/FB, c with $\phi(t)$. Let Q be the inverse image of R under $B \to B/FB$. $Q \cap A = P$, clearly, and $F \in Q$. Hence $d_Q < \infty$, in the notation of §2. Then we can regard Q as $Q(P, H)$ for suitable $H \in B$, where

$\deg H = d_Q$, the leading coefficient of H is not in P, and the image of H modulo P is irreducible over $(A/P)^*$. Let $A_P[t] = B_1$, and let $PA_P = P_1$. $F \in Q \Rightarrow F - GH \in P_1 B_1$ for some $G \in B_1$. Choose k as large as possible such that $F - GH^k \in P_1 B_1$ for some $G \in B_1$. Let $\psi : B \to B/PB \subset (A/P)^*[t]$. Then this is the largest k such that $\psi(H)^k$ divides $\psi(F)$ in $(A/P)^*[t]$, and there is a largest such k because the leading coefficient of H is not in P and F is monic. In fact $k \leq \deg F = d$. We thus know that $1 \leq k \leq d$. We will show that $J = GB_1 + H^k B_1 + PB_1$. To prove this, we observe that $\sqrt{J}$ contains P, G, and H. Thus, we want to show that $\psi(G)$ and $\psi(H)$ generate the unit ideal in $(A/P)^*[t]$. $\psi(H)(A/P)^*[t]$ is a maximal ideal; therefore, we need only show that $\psi(G) \notin \psi(H)(A/P)^*[t]$. But this follows from the maximality of k. We can now apply Hensel's lemma (as stated in [6, (30.4), p. 104]) to B_1/P_1^r. We can do this because, in the terminology of [6], this ring is a complete local ring which may not be Noetherian.

It follows that we can choose $G_1, H_1 \in B_1$ such that $G_1 - G \in P_1 B_1$, $H^k - H_1 \in P_1 B_1$, $\deg H_1 = \deg H^k$, and $F - G_1 H_1 \in P_1^r$. Hence we can find $\gamma, \eta \in A - P$ such that $\gamma G_1, \eta H_1 \in B$ and $\gamma\eta F - (\gamma G_1)(\eta H_1) \in P^{(r)}B$. Multiplying through by η^{k-1}, we have $\gamma\eta^k F - (\gamma G_1)(\eta^k H_1) \in P^{(r)}B$. Let $\beta = \gamma\eta^k$, let $G_2 = \gamma G_1$, and let $H_2 = \eta^k H_1$. Replacing H by ηH (we have this much latitude in the choice of H) we have

$$\beta F - G_2 H_2 \in P^{(r)}B \quad \text{where } \beta \in A - P,\ G_2, H_2 \in B \text{ and } H_2 - H^k \in PB.$$

Let $s = (d+1)r - 1$. Then

$$Q^{(s)} = \{q \in B : \text{for some } a_1 \in A - P,\ a_1 q \in (PB + HB)^s\}$$
$$\subset \{q \in B : \text{for some } a_1 \in A - P,\ a_1 q \in P^r B + H^{dr}B\}.$$

Now, $H^{dr}B \subset H^{kr}B$ (since $k \leq d$) $= (H^k B)^r \subset (PB + H_2 B)^r \subset P^r B + H_2 B$ $\subset P^{(r)}B + H_2 B$. Substituting, we find that

$$Q^{(s)} \subset \{q \in B : \text{for some } a_1 \in A - P,\ a_1 q \in P^{(r)}B + H_2 B\}.$$

Now let $a \in R^{(s)} \cap A$. Then a is in the inverse image of $R^{(s)}$ under

$$B \to B/F \Rightarrow Q \supsetneq J = (Q^{(s)} + FB) : a,$$

whence, by (2.1), for some $a_1 \in A - P$, $a_1 a \in FB + Q^{(s)} \subset FB + P^{(r)}B + H_2 B$. Multiplying by β and observing that $\beta F \in P^{(r)}B + H_2 B$, we find that $\beta a_1 a \in P^{(r)}B + H_2 B$. Reducing modulo $P^{(r)}$, we have $\beta a_1 a \equiv H_2 b$ for some $b \in B$. Since $\deg \beta H_2 = \deg H_2 = \deg H^k$, since $H^k - H_2 \in PB$, and since the leading coefficient of H does not belong to P, it follows that the leading coefficient of βH_2 also does not belong P. Thus, modulo $P^{(r)}$, every nonzero multiple of βH_2 has degree greater than or equal to the degree of $\beta H_2 = \deg H_2$. Then $\beta a_1 a$ must be congruent to 0 modulo $P^{(r)}$, i.e. $\beta a_1 a \in P^{(r)}$. But $\beta a_1 \notin P$, so that $a \in P^{(r)}$. Since a was an arbitrary element of $R^{(s)} \cap A$, we have $R^{(s)} \cap A \subset P^{(r)}$, as required.

It is difficult to give an enlightening characterization of $\mathfrak{C}(A)$, and this limits the usefulness of (3.3). It is natural to ask whether the proof can be generalized to handle extensions which are not simple. This would require a generalization of Hensel's lemma to ideals and several variables. While such generalizations exist (see, for example, [2]), they are far from our needs. The following conjecture would be more to the point:

Let A be a quasilocal domain with maximal ideal M, let $K = A/M$, and let $t_1, \cdots, t_r$ be indeterminates over A. Let F be a prime ideal of $A[t_1, \cdots, t_r]$ such that $F \cap A = (0)$, and suppose that $C = A[t_1, \cdots, t_r]/F$ is a finite A-module such that $C \cap A^* = A$. Modulo M, F is contained only in maximal ideals and has a unique primary decomposition. We can write this decomposition as a product rather than an intersection, for the factors are pairwise comaximal. Let q be one of the factors and q' the product of the rest. Then (conjecturally) for each $n \in \mathbf{N}$ there is a lifting of this factorization of F modulo M into qq' to $(A/M^n)[t_1, \cdots, t_r]$ in the following sense: there exist ideals Q, Q' of $A[t_1, \cdots, t_r]$ such that Q reduced modulo M is q, $F + M^nA[t] = QQ' + M^nA[t]$, and $(Q + M^nA[t]) \cap A = M^n$, where we have abbreviated $A[t_1, \cdots, t_r]$ to $A[t]$.

This conjecture implies that if a domain C is a finite integral extension of a domain A and $C \cap A^* = A$, then C is controlled if A is. The proof mimics the proof of (3.3) and (3.2). In fact, we note that the transition from (3.3) to (3.2) can be abstracted as follows.

Call a homomorphism $\phi : A \to C$ *tight* if for each nonzero ideal I of C, $\phi^{-1}(I)$ is nonzero. If ϕ is an inclusion, this means that each nonzero $c \in C$ has a nonzero multiple in A. We also say that C is a *tight* extension of A. Thus, if A, C are domains and C is an integral extension of A, then C is a tight extension of A.

PROPOSITION 3.5. *Let v be a control for A, let C be a tight reduced extension of A, and suppose there exists an $s \in \mathbf{N}$ such that for every prime Q of C and every $n \in \mathbf{N}$, $a \in Q^{(n)} \cap A \Rightarrow a^s \in P^{(n)}$, where $P = Q \cap A$. Define v_1 on C thus: for each nonzero $c \in C$ let $a(c)$ be a nonzero element of $cC \cap A$ (let $a(0) = 0$) and let $v_1(c) = v(a(c)^s)$. Then v_1 is a control for C.*

Proof. Suppose not. Then we can find nonzero c, c' in C such that $cc' \in Q^{(n)}$, where $n = v(a(c)^s) + v(a(c')^s) + 1$. But then $a(c)a(c') \in Q^{(n)}$, and hence $a(c)^s a(c')^s \in P^{(n)}$, a contradiction.

We now approach the question of integral extensions from another direction, with much more satisfying results. The only difficulty is that the conditions we must put on the original domain are much more restrictive. We first handle the case of purely inseparable extension, which is very tractable.

PROPOSITION 3.6. *Let C be a domain integral over A, and suppose C^* is a finite purely inseparable extension of A^*, and that $C \cap A^* = A$ (this is automatic*

if A is normal). Let $d = [C^*:A^*]$. Then for each prime Q of C and $r \in \mathbf{N}$, $c \in Q^{(r)} \Rightarrow c^d \in P^{(r)}$, where $P = Q \cap A$.

Proof. Let $\phi : C \to C$ via $c \to c^d$. Then ϕ is a homomorphism and $\phi(C) \subset C \cap A^* = A$. $\phi(Q) \subset P$ and $\phi(C - Q) \subset A - P$, clearly. Now $c \in Q^{(r)} \Rightarrow$ for some c_1 in $C - Q$, $c_1 c$ can be written as a sum of terms of the form $q_1 \cdots q_r$, where the q's are in Q. Then $\phi(c_1)\phi(c)$ is a sum of terms of the form $\phi(q_1) \cdots \phi(q_r)$, and hence $\phi(c_1)\phi(c) \in P^r \Rightarrow \phi(c) \in P^{(r)}$.

COROLLARY 3.7. *With the same hypothesis as* (3.6), *suppose that v is a control for A. Define v_1 on C by $v_1(c) = v(c^d)$. Then v_1 is a control for C.*

We now consider the general case. If (A, M) is a local ($\equiv$ Noetherian quasilocal) ring, let $d(A)$ be, equivalently, the least number of generators of M or $\dim_{A/M} M/M^2$. For any Noetherian ring A, let

$$\delta(A) = \max \{d(A_p) : P \text{ prime in } A\}.$$

Quite possibly, $\delta(A) = \infty$. This is the situation we must avoid.

PROPOSITION 3.8. *Let A be a Noetherian ring. If B is a residue class ring or localization of A, then $\delta(B) \leq \delta(A)$. If B is a regular local ring, $\delta(B)$ is the dimension of B. If B is an extension of A generated by r elements, $\delta(B) \leq \delta(A) + r$, with equality if the elements are indeterminates.*

Proof. Only the last part is nontrivial. From the fact about residue class rings, the problem reduces to the case where B is obtained from A by adjoining r indeterminates. By induction, we may assume $r = 1$. Thus, we can let $B = A[t]$, t an indeterminate. We may assume $\delta(A) < \infty$, and we must show $\delta(B) = \delta(A) + 1$. If P is a prime of A such that $d(A_P) = \delta(A)$, then $Q = PB + tB$ is a prime of B such that $d(B_Q) = \delta(A) + 1$. Hence, $\delta(B) \geq \delta(A) + 1$. Now let Q be any prime of B. If $Q = PB$ for some P, $d(B_Q) = d(A_P)$. Hence, we may suppose that $Q = Q(P, H)$, with notation as in §2. Then H together with a basis for PA_P is a basis for QB_Q, and $d(B_Q) \leq d(A_P) + 1$. It follows $\delta(B) \leq \delta(A) + 1$.

With this preparation, we are ready to state a main result.

THEOREM 3.9. *Let A be a normal Noetherian domain such that $\delta(A) < \infty$, and suppose that C is an extension domain, integral over A, such that $[C^* : A^*] < \infty$. Then if A is controlled, C is controlled.*

Proof. By extending further, we may assume that C^* is a normal extension of A^*, and that C is the integral closure of A in C^*. Let K be the separable part of the extension C^*/A^*. The integral closure of A in K is a finite A-module [7, p. 264], and by vitrue of (3.1), (3.7), and (3.8), we can assume that C is the integral closure of A in a finite separable normal (i.e. finite Galois) extension field K of A^*.

By (3.5), the problem then reduces to establishing the following result.

PROPOSITION 3.10. *Let A be a normal Noetherian domain such thal $\delta(A) < \infty$, let K be a finite Galois extension field of A^*, and let C be the integrat closure of A in K. Then there is an $s \in \mathbf{N}$ such that for each prime Q of C and each $n \in \mathbf{N}$, $a \in Q^{(n)} \cap A \Rightarrow a^s \in P^{(n)}$, where $P = Q \cap A$.*

In fact, let $d = [K:A^*]$. C is a finite A-module; hence, $\delta(C) < \infty$. Let m be any integer $\geq \delta(C)$ and let r be any integer such that C can be generated as an A-module by r or fewer elements. Then we may take $s = dr(m+1)^d$.

Proof. We first reduce to the case where A is local with maximal ideal P. In making this reduction, we must, of course, be careful to keep s the same, since our result is supposed to be global in P.

Let $A' = A_P$, $P' = PA_P$, $C' = (A - P)^{-1}C$, and $Q' = QC'$. A' is normal, local, $A'^* = A^*$, and C' is the integral closure of A' in $C'^* = C^* = K$. Furthermore, Q' is prime and $Q' \cap A' = P'$. Also, $d' =]C'^*:A'^*[= K : A^*] = d$ is the same, C' can be generated as an A'-module by r or fewer elements, and $\delta(C') \leq \delta(C) \leq m$, so that d, r, and m play the same roles as before and s may be kept the same. Finally, if $a \in Q^{(n)} \cap A$ but $a^s \notin P^{(n)}$, then $a \in Q'^{(n)} \cap A'$ but $a^s \notin P'^{(n)}$, since $P'^{(n)} = P'^n$ (P' is maximal) and $P'^n \cap A = P^{(n)}$.

Thus, we may assume without loss of generality that A is local with maximal ideal P. In this case, C is semilocal, the maximal ideals $Q = Q_1, Q_2, \cdots, Q_g$ being exactly the primes of C which lie over P. Furthermore $\{Q_1, \cdots, Q_g\}$ is a complete set of conjugate ideals under the action of the Galois group $\mathcal{G}(K/A^*)$ [6, (10.12), p. 31]. In particular, $g \leq d$.

Now, $\sqrt{(PC)} = \bigcap_i Q_i = Q_1 \cdots Q_g$ (the Q_i are maximal $\Rightarrow$ pairwise comaximal). We will show that each Q_i has a basis containing $\leq 1 + d(C_i) \leq m + 1$ elements, where we have written C_i for the localization of C at Q_i. To see this, choose a basis of $\leq m$ elements for $Q_i C_i$; we can actually take these elements in C. Q_i cannot be contained in the union of the other maximal ideals of C; hence, we can pick $q \in Q_i$ not in any other maximal ideal of C. It is easy to see that q together with the basis for $Q_i C_i$ is a basis for Q_i, and our claim is established.

Now, since $\sqrt{(PC)} = Q_1 \cdots Q_g$ and $g \leq d$, it follows that $\sqrt{(PC)}$ has a basis with $\leq (m+1)^d$ elements. Let $s' = (m+1)^d$.

We next wish to show that $c \in \sqrt{(PC)} \Rightarrow c^d \in PC$. To prove this, we consider the set of all elements of C which are roots of a monic polynomial with nonleading coefficients all in P. This set is clearly a radical ideal of C and contains P, and thus it contains $\sqrt{(PC)}$. Now the irreducible monic polynomial of a given $c \in \sqrt{(PC)}$ over A^* (which actually has its coefficients in A) is then a factor of this polynomial, and it is easy to see that it also must have all of its nonleading coefficients in P. Since this polynomial is of degree $\leq d$, it follows that c^d is in PC, as claimed.

Since $I = \sqrt{(PC)}$ has a basis of s' elements, and since each element of I has its d^{th} power in PC, it follows that $I^{ds'} \subset PC$.

Now suppose $a \in Q^{(n)} \cap A$. Since Q is maximal, $Q^{(n)} = Q^n$. Since a is in-

variant under the action of $\mathcal{G}(K/A^*)$, $a \in Q_i^n$ for each i. But then $a \in \bigcap_i Q_i^n = Q_1^n \cdots Q_g^n$ (for the Q_i^n are pairwise comaximal) $= (Q_1 \cdots Q_g)^n = I^n$, and $a^{ds'} \in (I^n)^{ds'} = (I^{ds'})^n \subset (PC)^n = P^nC$.

Since $s = r\,ds'$, we can conclude the proof by showing that if a' (in our case, $a' = a^{ds'}$) is in $JC \cap A$, where J is an ideal of A (in our case, $J = P^n$), then $a'^r \in J$. This follows from the usual argument: if $c_1, \cdots, c_r$ is a basis for C over A, we can write $a'c_i = \sum_j e_{ij} c_j$ for each i, where the e's are in J, and it follows that a' is a characteristic root of an $r \times r$ matrix with entries in $J \Rightarrow a'^r \in J$.

It is well known that every ring finitely generated over a field is a finite integral extension of a polynomial ring in finitely many indeterminates over the field [6, (14.4), p. 45]. Hence

COROLLARY 3.11. *A domain finitely generated over a field is controlled.*

4. Formal power series rings

We shall eventually prove that local domains are controlled by first dealing with the case of formal power series rings.

THEOREM 4.1. *Let (B, N) be a regular local ring whose completion is a formal power series ring over a discrete valuation ring ($\equiv$ local principal ideal domain; possibly a field). Then for each prime Q of B and $n \in \mathbf{N}$, $Q^{(n)} \subset N^n$. In particular, the conclusion holds if B is unramified.*

To prove (4.1), we first reduce to the complete case; then we proceed by induction on the dimension. We need to establish some general facts about the relation between symbolic powers in the ring $A[t]$, A local, and symbolic powers in $A[[t]]$. In the following, up to (4.5), let (A, M) be local, let t be an analytic indeterminate over A and let $B = A[[t]]$. We first generalize the Weierstrass preparation theorem and its corollaries. We say that an element of B is *regular* (of *order* h (in t) if the coefficient of t^i, $i < h$, is in M, while the coefficient of t^h is not (i.e. is a unit). We say that an ideal I of B is *regular* (in t) if equivalently, the set of coefficients of elements in I is the unit ideal of A (this set is always an ideal), or if I contains some regular element. Then

PROPOSITION 4.2. *Let c be any element of B and let $b \in B$ be regular of order h. Then there exist unique elements $q \in B$ and $a_0, \cdots, a_{h-1} \in A$ such that $c = qb + \sum_{i=0}^{h-1} a_i t^i$.*

Proof. The existence proof mimics the proof for their case given in (8, p. 261]. Uniqueness may be verified by using induction on n to show $qb + \sum_{i=0}^{h-1} a_i t^i = 0 \Rightarrow$ all coefficients of q and all the a_i are in M^n for every n.

COROLLARY 4.3. *Every element of B regular of order h has a unique monic associate of degree h in $A[t]$.*

Proof. Again, one simply mimics the proof of the corresponding result in [8, pp. 145–146].

PROPOSITION 4.4. *Let Q be a regular ideal of B and let $P = Q \cap A[t]$. Then $Q = PB$, and for every $n \in \mathbf{N}$, $Q^n \cap A[t] = P^n$ ($\Rightarrow Q^n = P^nB$); moreover, if Q is prime, then for each $n \in \mathbf{N}$, $Q^{(n)} \cap A[t] = P^{(n)}$ ($\Rightarrow Q^{(n)} = P^{(n)}B$).*

Proof. Q contains an element regular in t; hence, so does P, by (4.3). Let $b \in P$ be regular. By (4.2), $B = bB + A[t]$ (as abelian groups). Hence

$$PB \subset Q = bB + P \subset PB \quad \text{and} \quad Q = PB.$$

Now,

$$\begin{aligned} Q^n = (PB)^n = P^nB &\subset P^n(bB + A[t]) \subset P^nbB + P^n \\ &\subset P^nb(bB + A[t]) + P^n \subset P^nb^2B + P^n \\ &\subset \text{(similarly) } P^nb^3B + P^n \subset \cdots \subset P^nb^nB + P^n \subset b^nB + P^n. \end{aligned}$$

Hence, $Q^n \cap A[t] \not\subset P^n \Rightarrow b^nB \cap A[t] \not\subset b^nA[t]$, a contradiction, for B is flat over $A[t]$.

Thus, $Q^n \cap A[t] = P^n$ and $Q^n = P^nB$. Now consider any $q \in Q^{(n)} \cap A[t]$. Let $J = Q^n{:}q$. $J \supset Q^n \Rightarrow J$ is regular $\Rightarrow J = J_0B$, where $J_0 = J \cap A[t]$. Then $J \not\subset Q \Rightarrow J_0 \not\subset P \Rightarrow$ for some $c \in A[t] - P$, $cq \in Q^n$. Now

$$c \in A[t],\ q \in A[t] \quad \Rightarrow \quad cq \in Q^n \cap A[t] = P^n \Rightarrow q \in P^{(n)},$$

as required.

COROLLARY 4.5. *If $b \in B$ is regular of order h, then for each prime Q of B, $b \notin Q^{(h+1)}$.*

Proof. Suppose $b \in Q^{(h+1)}$. Replace b by its monic associate in $A[t]$. Then $b \in Q^{(h+1)} \cap A[t] = P^{(h+1)}$, where $P = Q \cap A[t]$. But b is monic of degree h, and this contradicts (2.3).

The following observation is very useful.

(4.6) Let (B, N) be a regular local ring, Q a prime of B, and suppose $b \in Q - N^2$, i.e. $b \in Q$ and b is part of a regular system of parameters for B. Then $b \notin Q^{(2)}$, i.e. b is part of a regular system of parameters for B_Q. Hence, if $b^ku \in Q^{(n)}$, $u \neq 0$, then $n \geq k$ and $u \in Q^{(n-k)}$.

Proof. $B_Q/bB_Q \cong (B/bB)_{Q'}$, where Q' is the image of Q under $B \to B/bB$, and the latter is regular.

Finally, before proving (4.1), we need the following result.

PROPOSITION 4.7. *Let (A, M) be a complete local ring and let*

$$B = A[[t_1, \cdots, t_r, t]].$$

Let $b \in B$ be such that at least one of its coefficients as a power series in the t's is a unit of A. Then there is an A-automorphism of B which takes b into an element regular in t.

Proof. Let $K = A/M$, and reduce coefficients modulo M. Our hypothesis is that the image of b in $K[[t_1, \cdots, t_r, t]]$ is not zero; call it F. Choose ϕ as in the second paragraph of the proof of Lemma 3 in [8, p. 147] for this F. Then ϕ has an obvious lifting to B, and this is the required automorphism.

Proof of (4.1). Let (B, N) be as in (4.1), and let (B', N') be its completion. Let Q be any prime ideal of B. Let R be a prime of B' lying over Q. Then if for each $n \in \mathbf{N}$, $R^{(n)} \subset N'^{(n)}$, then we have $Q^{(n)} \subset R^{(n)} \cap B \subset N'^n \cap B = N^n$, and we are done. Thus, we may assume without loss of generality that B is complete, i.e. that B is a formal power series ring over a complete discrete valuation ring V. We use induction on the dimension of B. Let

$$B = V[[t_1, \cdots, t_r, t]] \cong A[[t]],$$

where $A = V[[t_1, \cdots, t_r]]$, be of smallest possible dimension such that the result supposedly fails for B. $r > 0$. Let M be the maximal ideal of A. Then the maximal ideal N of B is $MB + tB$.

We want to show that for each prime Q of B and $n \in \mathbf{N}$, $Q^{(n)} \subset N^n$. We first show that it is enough to prove this when Q is of dimension one. For otherwise choose R of dimension one containing Q. If we can show $Q^{(n)} \subset R^{(n)}$ and $R^{(n)} \subset N^n$, we will be done. The latter statement is the case to which we are trying to reduce. The former statement can be deduced from the induction hypothesis as follows. B_R and its completion C are of strictly smaller dimension than B, so that if C is a formal power series ring over a discrete valuation ring, it will follow (as in the first paragraph of this proof) that B_R has the property we are trying to establish for B, and from that it is immediate that $Q^{(n)} \subset R^{(n)}$. We still need to show that the completion C of B_R is a formal power series ring. To this end we consider two cases. Let μ be the generator of the maximal ideal of V. If $\mu \notin R$, then B_R contains the field V^* and is equicharacteristic, and the result follows. This argument also takes care of the case where V is a field. We now assume that V is not a field, and that $\mu \in R$. By (4.6), μ is part of a regular system of parameters $(\mu, \beta_1, \cdots, \beta_r)$ for B_R, and these will also be a regular system of parameters for C. (Note that $\dim B = r + 2$ and R of dimension one $\Rightarrow \dim B_R = r + 1$.) Then there is a unique V-homomorphism of $A = V[[t_1, \cdots, t_r]]$ into C such that $t_i \to \beta_i$. Since $(\mu, \beta_1, \cdots, \beta_r)$ is a regular system of parameters this homomorphism is surjective, and since $\dim A = \dim C$, it must be injective as well. This completes the proof.

We can now assume that Q is of dimension one. Let $b \in Q^{(n)}$ be given and suppose that $b \notin N^n$. We can write $b = \mu^k b'$, $b' \notin \mu B$, uniquely. If $\mu \notin Q$, we also have $b' \in Q^{(n)} - N^n$, while if $\mu \in Q$ we have $b' \in Q^{(n-k)} - N^{n-k}$, by (4.6). Thus, replacing b by b' (and n by $n - k$, if necessary) we may assume that $b \notin \mu B$.

This means that b satisfies the hypothesis of (4.7), and after applying a suitable V-homomorphism of B, we can suppose that b is regular in t. Passing to

an associate, we can also assume that b is a monic polynomial in $A[t]$. Let $Q_0 = Q \cap A[t]$, and let $P = Q \cap A = Q_0 \cap A$. Since Q_0 contains the monic polynomial b, we cannot have $Q_0 = PA[t]$, and we therefore have

$$Q_0 = \{q \in A[t] : \text{for some } a \in A - P,\ aq \in PA[t] + HA[t]\},$$

for suitable $H \in A[t]$, as described in the second paragraph of §2. Now

$$Q^{(n)} = Q_0^{(n)}B \text{ (by (4.4))} = \{q \in B : \text{for some } a \in A - P,\ aq \in (PB + HB)^n\}.$$

Since $b \in Q^{(n)}$ we know that if $J = (PB + HB)^n : b$, then $\sqrt{J}$ contains Q properly. But since Q is of dimension one in B, it follows that $\sqrt{J} = N$ or B. In either case, for some $k \in \mathbf{N}$, $t^k b \in (PB + HB)^n$. Now $t^k b$ is monic, since b is, and it follows that modulo P some multiple of H is monic. This cannot happen unless the leading coefficient of H is invertible modulo P (it is not in P), and since B is local, this implies that the leading coefficient of H is invertible in B. Passing to an associate, we may assume that H is monic. We may then apply (2.7) (which we introduced expressly for this purpose) and obtain

$$b \in Q^{(n)} \cap A[t] = Q_0^{(n)} = \textstyle\sum_{i=0}^{n} P^{(i)}H^{n-i}B \subset \sum_{i=0}^{n} M^i H^{n-i}B$$

(by the induction hypothesis $P^{(i)} \subset M^i$). Now $H \in Q_0 \subset Q \subset N$ so that $M^i H^{n-i} \subset N^n$, and we find that $b \in N^n$, as required.

COROLLARY 4.8. *Let A be a ring all of whose localizations at prime (equivalently, at maximal) ideals are unramified regular local rings. Let $P \subset Q$ be two primes of A. Then for each $n \in \mathbf{N}$, $P^{(n)} \subset Q^{(n)}$.*

5. Local and semilocal domains

THEOREM 5.1. *Every local or even semilocal domain is controlled.*

Proof. We first consider the case of a local domain (A, M). Let (A', M') be the completion and let $P_1, \cdots, P_r$ be the minimal primes of A', each of which must be disjoint from $A - \{0\}$. Let $B_i = A'/P_i$. Since each prime of A lies under a prime of A' which in turn must contain one of the P_i, it suffices to show, by (1.1), that each B_i is controlled. But each B_i is a complete local domain, and hence a finite integral extension of a formal power series ring over a discrete valuation ring [6, (31.6), p. 109]. Hence, by (3.9) and (4.1) each B_i is controlled.

Now let $(A; M_1, \cdots, M_r)$ be a semilocal domain. Let B_i be the localization of A at M_i. Each B_i is controlled, by the first part, and again we may apply (1.1).

We can generalize (5.1) slightly as follows. Call a ring *locally semilocal* if each nonzero element is contained in only finitely many maximal ideals and the localization at each maximal ideal is Noetherian. An equivalent statement is that every proper residue class ring is semilocal. By [6, (E1.1), p. 203], such a ring must be Noetherian. Dedekind domains constitute one kind of example of such rings.

COROLLARY 5.2. *A locally semilocal domain A is controlled.*

Proof. For each maximal ideal M of A, let v_M be a control for A_M which vanishes on the units of A_M and on 0. Apply (1.1), using the set of maximal ideals as the index set. The finiteness of the max follows from the fact that for each $a \neq 0$, $v_M(a) = 0$ except for the finitely many M to which a belongs.

6. Restricted power series rings

Let (A, M) be a local ring and let $t_1, \cdots, t_r$ be analytic indeterminates over A. By the *restricted power series ring* $A\{t_1, \cdots, t_r\}$ in the indeterminates t_i over A we mean the subring of $A[[t_1, \cdots, t_r]]$ consisting of those power series such that for each power of M, all but finitely many terms of series have their coefficients in that power. (See [1, §4, n° 2, pp. 79–83].) Thus, if $B = A\{t_1, \cdots, t_r\}$, $B/M^nB \cong (A/M^n)[t_1, \cdots, t_r]$ for every $n \in \mathbf{N}$. If (A, M) is complete, then B may be described as the completion of $A[t_1, \cdots, t_r]$ with respect to the ideal generated by M. Note that if (A', M') is the completion of (A, M), then the completion of $A[t_1, \cdots, t_r]$ with respect to the ideal generated by M is $A'\{t_1, \cdots, t_r\}$.

THEOREM 6.1. *Let (A, M) be a local domain, and let $B = A\{t_1, \cdots, t_r\}$ be the restricted power series ring in the indeterminates $t_1, \cdots, t_r$ over A. Then B is controlled.*

Proof. It is easy to see that MB is the Jacobson radical of B. Let A' and B' be the completions of A and B with respect to M and MB respectively. B' is a faithfully flat B-algebra so that each prime of B lifts to a prime of B'. Also, B' may be identified with $A'\{t_1, \cdots, t_r\}$. The minimal primes of B' are clearly generated by the minimal primes of A'. Hence, it suffices, by (1.1), to show that for each i, $B'/P_iB' \cong (A'/P_i)\{t_1, \cdots, t_r\}$ is controlled. Hence, we may assume without loss of generality that (A, M) is a complete local domain. Then A is a finite module over a complete unramified regular local ring (C, N) [6, (31.6), p. 109]. $\sqrt{(NA)} = M$, clearly, and for some $k \in \mathbf{N}$, $M^k \subset NA$. Hence, for each $n \in \mathbf{N}$, if $n > kr$ then $M^n \subset N^rA$. Let $a_1, \cdots, a_m$ be a basis for A over C. Then $M^n \subset \sum_i N^r a_i$ when $n > kr$, and it easily follows that

$$A \otimes_C C\{t_k, \cdots, t_r\} \cong A\{t_1, \cdots, t_r\},$$

so that $A\{t_1, \cdots, t_r\}$ is a finite module over $C\{t_1, \cdots, t_r\}$. Thus, by (3.9), we may assume without loss of generality that A is an unramified regular local ring.

We proceed by induction now on the dimension m of A. If $m = 0$, i.e. if A is a field, then $A\{t_1, \cdots, t_r\} = A[t_1, \cdots, t_r]$, and we are done. Now suppose that $m \geq 1$ and that for each unramified regular local ring A' of dimension $< m$, $A'\{t_1, \cdots, t_r\}$ is controlled. Choose $x \in M - M^2$, i.e. let x be part of a regular system of parameters for A. A/xA is then an unramified regular local

ring, and so $B/xB \cong (A/xA)\{t_1, \cdots, t_r\}$ is controlled. Let v be a control for this ring. Let $\phi : B \to B/xB$ be the canonical homomorphism. Each nonzero $b \in B$ can be written uniquely in the form $x^k b'$, where $b' \in xB$, i.e. $\phi(b') \neq 0$. Then define $v_1(b) = k + v(\phi(b'))$ when $b \neq 0, v_1(0) = 0$. We shall show that v_1 is a control for B.

Suppose, to the contrary, that $b, c \in B - \{0\}$ and that $bc \in Q^{(n)}$, where Q is a prime of B and $n = v_1(b) + v_1(c) + 1$. Let $b = x^j b'$, $c = x^k c'$, where b', $c' \notin xB$. Then $n = j + k + v_1(b') + v_1(c') + 1$. Choose a maximal ideal R of B which contains Q. Then $Q^{(n)} \subset R^{(n)} = R^n$, by (4.8), so that we may assume without loss of generality that Q is maximal.

$$bc = x^{j+k} b'c' \in Q^n \implies b'c' \in Q^{n'},$$

where $n' = v_1(b') + v_1(c') + 1$, by (4.6). Now, $x \in MB$, the Jacobson radical of B, so that $x \in Q$. Thus, the image Q_1 of Q in B/xB is also a maximal ideal, and we have $\phi(b')\phi(c') \in Q_1^{n'}$, a contradiction.

PROPOSITION 6.2. *Let V be a complete discrete valuation ring with maximal ideal (μ), let $t_1, \cdots, t_r$ be analytic indeterminates over V, and let $A = V\{t_1, \cdots, t_r\}$. Let P be an ideal of A such that $P \cap V = (0)$. Let $B = A/P$. If μ is not a zero divisor in B (in particular, if P is prime), then B is a finite module over a restricted power series ring over V.*

Proof. $B/\mu B$ is a quotient of $A/\mu A$, and hence $B/\mu B$ is a finitely generated K-algebra, where $K = V/\mu V$. We can therefore choose $b_1, \cdots, b_m \in B$ whose images $b_1', \cdots, b_m'$ in $B/\mu B$ are algebraically independent over K and such that $B/\mu B$ is a finite module over $K[b_1', \cdots, b_m']$. Let $x_1, \cdots, x_m$ be analytic indeterminates over V. We shall show that B is a finite module over the closure C in the μB-adic topology of $V[b_1, \cdots, b_m]$ in B, and that there is a V-isomorphism of $D = V\{x_1, \cdots, x_m\}$ with C such that $x \to b_i$. That B is a finite module over C follows from [8, Corollary 2 on p. 259]. Now there is certainly a unique V-homomorphism (and a necessarily surjective one besides) of $D \to C$ with $x_i \to b_i$, because C is closed in the complete ring B. We need only show that this homomorphism is injective. But if some series in D is taken to zero, we can choose one with not all its coefficients in μV, because μ is not a zero divisor in B, and we can factor out an appropriate power of μ. But the fact that the series is taken to zero then gives an algebraic relation among the b_i' when we reduce modulo (μ), a contradiction. This completes the proof.

COROLLARY 6.3. *Let V, A be as in* (6.2), *and let P be any prime ideal of A. Then A/P is controlled.*

Proof. If $P \cap V = (0)$, then A/P is a finite module over a restricted power series ring and the result follows from (3.9) and (6.1). If $P \cap V \neq (0)$, then $P \cap V = \mu V$, and A/P is a finitely generated domain over $K = V/\mu V$.

The author conjectures the following generalization of (6.3):

If A is a restricted power series ring over a local ring, then (conjecturally) every residue class domain of A is controlled.

7. Finitely generated extensions of Dedekind domains

THEOREM 7.1. *Let A be a Dedekind domain and suppose that B is a domain finitely generated over A. Then B is controlled.*

Proof. By the Noether normalization theorem [6, (14.4), p. 45] we may assume that

$$B = A[t_1, \cdots, t_r][u_1, \cdots, u_j][v_1/a, \cdots, v_k/a],$$

where t's are indeterminates, the u's and v's are integral over $A[t_1, \cdots, t_r]$, and $a \in A - \{0\}$. Let $aA = P_1^{\nu_1} \cdots P_m^{\nu_m}$ be the prime factorization of aA in A. Then by (1.1) it suffices to show that the rings $B[1/a]$, and $A_P \otimes_A B$ (i.e. $(A - P)^{-1}B$), $P = P_1, \cdots, P_m$, are all controlled. But

$$B[1/a] = A[1/a][t_1, \cdots, t_r][u_1, \cdots, u_j][v_1, \cdots, v_k],$$

and $A' = A[1/a]$ is again a Dedekind domain, so that we have an integral extension of $A'[t_1, \cdots, t_r]$, where A' is a Dedekind domain. Thus, by (3.9), $B[1/a]$ is controlled.

Each of the rings $A_P \otimes_A B$ is a finitely generated extension of a discrete valuation ring $V = A_P$, so that we have reduced to the case where $A = V$ is a discrete valuation ring, say with maximal ideal μV. Let B' be the completion of B with respect to μB, and let $B_1, \cdots, B_h$ be the quotients of B' by its various minimal primes. Those primes of B which contain μ lift to B' and hence to at least one of $B_1, \cdots, B_h$, while those which do not contain μ lift to $B[1/\mu]$. Hence, again by (1.1), it suffices to show that $B[1/\mu]$, $B_1, \cdots, B_h$ are controlled. But $B[1/\mu]$ is finitely generated over the field $V[1/\mu] = V^*$, while each of the B_i is of the type of Corollary (6.3). This completes the proof.

We conclude with another conjecture:

A domain B finitely generated over a locally semilocal domain A is (conjecturally) controlled.

This would contain two of our strongest results: (5.2) and (7.1). The proof would mimic the proof of (7.1). The conjecture following (6.3) would take the place of (6.3). If we assume that A satisfies the hypothesis of (3.9), that would be sufficient. For the general case, we would also need the conjecture following (3.3), or at least its consequence that if the domain C is a finite module over the controlled domain A and $C \cap A^* = A$, then C is controlled.

REFERENCES

1. N. BOURBAKI, "Graduations, filtrations et topologies", *Algèbre commutative*, Chapitre 3, Hermann, Paris, 1961.

2. M. GREENBERG, *Rational points in Henselian discrete valuation rings*, Publ. Math. I. H. E. S., n° 31 (1966), pp. 563–568.
3. H. HIRONAKA, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Ann. of Math., vol. 79 (1964), pp. 205–326.
4. M. HOCHSTER, *Prime ideal structure in commutative rings*, Thesis, Princeton University, 1967.
5. ———, *Prime ideal structure in commutative rings*, Trans. Amer. Math. Soc., vol. 142 (1969), pp. 43–60.
6. M. NAGATA, *Local rings*, Interscience, New York, 1962.
7. O. ZARISKI AND P. SAMUEL, *Commutative algebra*, vol. I, van Nostrand, Princeton, 1958.
8. ———, *Commutative algebra*, vol. II, van Nostrand, Princeton, 1960.

UNIVERSITY OF MINNESOTA
MINNEAPOLIS, MINNESOTA