CONSTRUCTION OF THE INTEGRAL CLOSURE OF A
FINITE INTEGRAL DOMAIN. II

A. SEIDENBERG

ABSTRACT. In a previous paper the problem of constructing the integral
closure of a finite integral domain $k[x_1, \ldots, x_n] = k[x]$ was considered. A reduc-
tion to the case $\text{deg } k(x)/k = 1$, $k(x)/k$ separable, and $n = 2$ was made. A subsidiary
problem was: if $k[x]$ is not integrally closed, to find a $y$ in $k(x)$ integral over $k[x]$ but not in it. This was done for $n = 2$, but should have been done for arbi-
trary $n$. The extra details are here given. For the convenience of the reader,
the full argument is sketched.

In [2] we proposed to construct the integral closure of a finite integral
domain $k[x_1, \ldots, x_n] = k[x]$ in its quotient field $k(x_1, \ldots, x_n)$. Three
subsidiary problems were formulated, of which the first two were:

1. to give a method for deciding whether $k[x]$ is integrally closed;
2. in the case $k[x]$ is not integrally closed, to give a method for finding
an element in $k(x)$ integral over $k[x]$ but not in it.

We dealt first with the case that $k(x)/k$ is separable, and a reduction
to the case degree of transcendency of $k(x)/k = 1$ was made. It is then easy
to reduce the original problem to the case $n = 2$, but on p. 7 it was stated,
though incorrectly, that the subsidiary problem 2 was thus reduced. The
slip was (in effect) noted in [1]. This is a note of correction. Basically we
assume a familiarity with [2], but, for the convenience of the reader, try to
rely on [2] as little as possible.

For another treatment (not quite complete) of the problems here con-
sidered see [5].

1. Preliminaries. Reference [3] considers some basic construction prob-
lems in a polynomial ring $k[X_1, \ldots, X_n] = k[X]$. If $A$ is an ideal in $k[X]$, given via a finite basis, and $b \in k[X]$ is given, one can decide whether $b \in A$ ($\S 5$), find the dimension of $A$ ($\S 6$), and construct $A \cap k[X_1, \ldots, X_{n-1}]$ ($\S 23$; Note 4; see also [2, p. 17]). Hence if dim $A = 0$, by contracting $A$ to
$k[X_1]$, one can find a polynomial whose roots are precisely the $i$th coordinates
of the points annihilating $A$. If dim $A = r$ and $A = Q_1 \cap \cdots \cap Q_s$ is a nor-
mal decomposition of $A$ into primary ideals, one can construct the intersec-
tion of the $r$-dimensional $Q_i$ ($\S 17$). Given ideals $A$ and $B$, one can construct

Received by the editors November 13, 1973.


Key words and phrases. Constructive mathematics, finite integral domain, inte-
gral closure.

1 Supported in part by an NSF grant.
A \cap B, A : B (§S2, 3) and an integer p such that $A : B^p = A : B^{p+1}$ (§20). These constructions hold for any explicitly given field $k$.

The ring $k[x_1, \ldots, x_n] = k[x]$ (whose integral closure $k[x]^*$ is sought) is given as $k[X]$ mod the ideal $P$ of relations satisfied by $x/k$. Contracting $A = P$ to $k[X_1, \ldots, X_n]$, one can test the algebraic independence of $x_1, \ldots, x_r$ over $k$, and in this way find a transcedency basis of $k(x)/k$ amongst the $x_i$; say this is $(x_1, \ldots, x_r)$. If $y = f(x)/g(x)$ with $f, g \in k[X]$, then $\bigcup_P y \in k(x)$, and contracting this to $k[x_1, \ldots, x_r, Y]$ one finds the defining equation of $y$ over $k(x_1, \ldots, x_r)$. If $y$ is integral over $k[x_1, \ldots, x_r]$, then (since this ring is integrally closed) the equation will be an equation of integral dependence. Hence, though we omit some details, for $y \in k(x)$, we can test the integral dependence of $y/k[x]$ and, if $y$ is integral, construct an equation showing this.

In [2] (cf. also [3]) we introduced a condition (P) for explicitly given fields $k$ that in effect allows us to check for $p$-independence in $k$ (i.e., if $a_1, \ldots, a_s \in k$, whether $[k^p(a_1, \ldots, a_s) : k^p] = p^s$). Our problems are to be solved for $k$ satisfying (P), a condition void for explicitly given $k$ of characteristic 0. (For the role of (P) see [2] and reference 6 in [3].)

Let $u$ be an indeterminate and $K = k(u)$. If $y_1, \ldots, y_m$ are $k(u)[x]$-module generators for the integral closure $k(u)[x]^*$ of $k(u)[x]$, we may, multiplying the $y_i$ by a denominator $a(u) \in k[u]$, suppose the $y_i$ integral over $k(x, u)$, hence in $k(x)[u]$. Writing the $y_i$ as polynomials in $u$, the coefficients are in $k[u]$ (since $k[u]$ is integrally closed) and yield a $k[x]$-module basis of $k[x]^*$. Thus in solving our main problem we may freely adjoin indeterminates to $k$; in particular, we may assume $k$ infinite. By [2, p. 9] a similar technique is available for $K/k$ finite and $K$ linearly disjoint from $k(x)/k$, a result we use only for $d(k(x)/k) = 1$ and $K = k(u)$ with $a \in k$.

2. The construction. Let $V$ be the variety having $(x_1, \ldots, x_n)$ as generic point over $k$; $k[x]$ is integrally closed if and only if $V$ is normal.

Let $r = \dim V$; we may as well suppose $r \geq 1$. Using the mixed-Jacobian of Zariski (cf. [4, p. 360]) and (P), we can write down an ideal $A$ in $k[X]$ for the singularities of $V/k$ and find its dimension. If $V$ has a singularity of codimension 1, it is certainly not normal (cf. [4]). Assume $V$ has no singularity of codimension 1. By [2, p. 10] or the reference to F. K. Schmidt in [4, p. 376], one can construct an element $c \neq 0$ in the conductor of $k[x]$; for $k(x)/k$ separable, see [4, p. 365]. If $(c) = (1)$, which we can decide, then $V$ is normal, and if $(c) \neq (1)$, then by [2, p. 1] or [4, p. 363], $V$ is normal if and only if $(c)$ is unmixed. Let $(c) = Q_1 \cap \cdots \cap Q_s \cap \cdots \cap Q_t$ be a normal decomposition of $(c)$ into primary
ideals with $Q_1, \ldots, Q_s$ the primaries belonging to the minimal primes of (c). We can construct $Q_1 \cap \cdots \cap Q_s$ and compare it with (c); assume (c) is mixed. Let $d \in Q_1 \cap \cdots \cap Q_s$ not in (c). Taking note that the local rings of $k[x]$ with respect to its minimal primes are the same as the local rings of $k[x]^*$ with respect to its minimal primes, we see that $d/c$ is integral over $k[x]$ but not in it. The same reasoning shows that $Q_i \cap \cdots \cap Q_s/c$ is the full integral closure of $k[x]$. Thus problem 1 is solved and so is the main problem if $V$ has no singularity of codimension 1.

Assuming $r > 1$, we cut $V$ by a generic hyperplane $H$. Let $u_1, \ldots, u_n$ be indeterminates and place $z = u_1 x_1 + \cdots + u_n x_n$. Then by [4, p. 367], the ring of this section is $k(u, z)[x]$. Now let $u_{i1}, \ldots, u_{in}$, $i = 1, \ldots, r - 1$, be indeterminates and place $z_i = u_{i1} x_1 + \cdots + u_{in} x_n$, $i = 1, \ldots, r - 1$. Then $k(u, z)[x]$ is 1-dimensional. Assuming the main problem solved for $r = 1$, let $y_1, \ldots, y_m$ be a $k(u, z)[x]$-module basis of $k(u, z)[x]^*$; we may suppose $y_1, \ldots, y_m$ are integral over $k(u)[z, x] = k(u)[x]$. Further, by an argument given above, we may suppose $y_1, \ldots, y_m$ to be in $k(x)$; they are, then, integral over $k[x]$. It is not to be expected that the variety $V'$ having $(x, y)$ as generic point over $k$ is normal; however, it is free of singularities of codimension 1. In fact, suppose $p$ is an $(r - 1)$-dimensional prime in $k[x, y]$ such that its local ring $k[x, y]_p$ is not regular. Then also the local ring $k(u)[x, y]_p$ is not regular; but (since the $z_i$ are algebraically independent over $k(u)$ mod $p$) this is the same as the local ring of $k(u, z)[x, y]_p$ in $k(u, z)[x, y]$, a contradiction. Hence, by the preceding paragraph, we can construct $k[x, y]^* = k[x]^*$. Thus the main problem is reduced to $r = 1$. (Cf. [2, p. 6f].)

Let, then, $(x_1, \ldots, x_n)$ be a generic point for a curve $V/k$. We (first) assume $k(x)/k$ separable. By our condition (P), which allows us to check for $p$-independence, we can decide whether a given element $a$ of $k$ has a $p$th root in $k$ ($p = \text{characteristic}$); and if it does not, then adjoining $a^{1/p}$ to $k$ we get an extension of $k$ linearly disjoint from $k(x)/k$. As mentioned, if we can solve our (main) problem over $k(a^{1/p})$ we can work back to get a solution over $k$. Hence we can freely adjoin $p$th roots to our base field. We are given the ideal $P$ of relations of $(x_1, \ldots, x_n)/k$, via a basis, and we adjoin the $p$th roots of the coefficients of the basis elements to $k$ and may thus suppose they are in $k$. The result is that the singularities of $V$ (over the new $k$) become absolute (in effect, given by the Jacobian rather than the mixed-Jacobian of the basis). $V$ may lose its singularities and thus become normal in the process, but this makes no difference.

Assume for a moment that $k$ is algebraically closed. Let $P$ be a point on $V$, say the origin. If no branch of $V$ centered at $P$ has its tangent in $X_1 = 0$ (equivalently: if $X_1 = 0$ is not tangent to $V$ at $P$), then $\nu(x_1) \leq$
\( v(x_i) \) in every branch centered at \( P, \ i = 2, \ldots, n \), and hence \( x_i/x_1 \) is integral over the local ring at \( P \). Even if \( V \) is tangent to \( X_1 = 0 \) at \( P \), but assuming \( V \) is not in \( X_1 = 0 \), one can compute a \( \rho \) such that \( x_i^\rho/x_1 \) is integral over the local ring at \( P \); in fact obviously \( \rho = \text{order of } V \) will do.

Let \( (x_1, \ldots, x_n) \) be a generic point of \( V/k, k(x)/k \) separable, and, as above, with the singularities of \( V \) absolute. We subject \( V \) to a generic homogeneous nonsingular linear transformation. Here we adjoin \( n^2 \) indeterminates \( u_{ij} \) to \( k \), but, as explained, we can later remove them, so we write \( k \) for \( k(u); \) and \( x_1, \ldots, x_n \) for the "transformed" variables. As mentioned, we can compute a polynomial \( g_i^*(X) \in k[X] \) whose roots are precisely the \( i \)th coordinates of the singularities of \( V \). Then, as in [2, p. 20], after extending \( k \) by some \( p \)th roots, we get a polynomial \( g_i(X) \in k[X] \) having these coordinates as roots with multiplicity 1. Let \( \overline{V} \) be the variety having \( (x_1, \ldots, x_n) \) as generic point over \( \overline{k} \), the algebraic closure of \( k \). Because of the nonspecial position of \( V \), by an argument given above, \( g_i(x_i)/g_1(x_1) \) will be integral over the local ring of \( \overline{V}/\overline{k} \) of each point of \( \overline{V} \) that is singular for \( V/k \); it will also be in the local ring of any point \( P \) for which \( g_1(P) \neq 0 \). There remain the simple points of \( V \) on \( g_i(X_i) = 0 \). Because of the generic direction of \( X_i = 0 \), no two points of \( V \cap (g_i(X_i) = 0) \) have the same \( i \)th coordinates \( (i > 1) \). We can compute a polynomial \( P_i(X) \) having these \( i \)th coordinates as roots, and, as before, with multiplicity 1. Then \( P_i = P_i^*/g_1 \) will be a polynomial over \( k \) having as roots the \( i \)th coordinates of the simple points (of \( V \)) on \( g_1(X_1) = 0 \); and G.C.D. \( (g_i, P_i) = 1 \). As above, we can compute a \( \rho \) such that \( z_i = g_i(x_i)(P_i(x_i))^\rho/g_1(x_1) \) is integral over every local ring of \( \overline{V}/\overline{k} \), hence integral over \( \overline{k}[x] \), and over \( k[X] \). If \( V \) has singularities, the \( z_i \) will not all be in \( k[x] \), for if \( P \) is one such singularity and \( z_i \in Q(P/V), \) the local ring, then from \( g_i(x_i)(P_i(x_i))^\rho/g_1(x_1) \in Q(P/V) \) we get a polynomial in \( \overline{k}[X_1 - X_1(P), \ldots, X_n - X_n(P)] \) vanishing over \( V \) and having for linear terms a linear term in \( X_i - X_i(P) \); if this happens for all \( i \), then \( P \) is simple on \( Y \) by the Jacobian criterion. Hence at least one \( z_i \) is not in \( k[x] \); it is easy to decide which \( z_i \) are in \( k[x] \), after converting this question into one on polynomials. This solves problem 2 (for \( \dim V = 1, k(x)/k \) separable, and for an augmented \( k \)).

After a nonspecial homogeneous linear transformation on \( (x_1, \ldots, x_n) \) over \( k \), we may suppose \( k[x] \) is integral over \( k[x_1] \). Let \( w_1, \ldots, w_m \) be a linear basis of \( k(x)/k(x_1) \). Place \( \text{Tr } w_i w_j = \Sigma w_i^{(k)} w_j^{(k)} \), where the superscript indicates conjugation/\( k(x_1) \). Then \( d(w) = \det(\text{Tr } w_i w_j) \) is the discriminant of the basis \( w_1, \ldots, w_m \) and is \( \neq 0 \). If \( w'_i = \Sigma a_{ij} w_j \), with \( a_{ij} \in k(x_1) \), is another basis of \( k(x)/k(x_1) \), then \( d(w'_i) = (\det A)^2 d(w) \); here \( A = \| a_{ij} \| \). Now let \( w_1, \ldots, w_m \) be integral over \( k[x_1] \), whence \( d(w) \in k[x_1] \), and let \( w'_i \) be integral over \( k[x_1, w_1, \ldots, w_m] \) but not in it. Write \( w'_1 = \ldots \)
\[(a_1w_1 + \cdots + a_mw_m)/c,\] with \(a_i, c \in k[x_1].\) We may assume \(a_i = 0\) or \(\deg a_i < \deg c, i = 1, \cdots, m;\) and at least one \(a_i \neq 0,\) say \(a_1 \neq 0.\) Place \(w'_2 = w_2, \cdots, w'_m = w_m.\) Then \(d(w') = (a_1^2/c^2)d(w),\) whence \(\deg d(w') < \deg d(w).\) Starting with \(w_1, \cdots, w_m\) in \(k[x],\) the process can be applied at most \(d(w)\) times, a bound that does not change even upon successive adjunctions to \(k\) of indeterminates and \(p\)th roots. Hence we soon get to the integral closure of \(k[x]\) and the main problem is solved, over an augmented \(k.\) As mentioned earlier, we can work back to the original \(k.\) Now the main problem (and with it problem 2) is solved for any explicitly given \(k\) satisfying (P) and \(k(x)/k\) separable.

The above construction does not use our condition (F), the condition that one should be able to factor a polynomial effectively over \(k.\) Cf. \([2, pp. 8, 16].\)

Finally, there is the problem (for \(r = 1\)) of reducing to the separable case; this is done on pp. 9–10 of \([2]\) and involves successive adjunctions of \(p\)th roots to the base field: any such extension is either inner, i.e., for a \(p\)th root \(a^{1/p}, a^{1/p} \in k(x),\) or outer, i.e., \(a^{1/p} \notin k(x);\) and assuming condition (P) for \(k,\) we can decide which by \([2, p. 12]\) or \([3, \S 40].\) An outer extension yields a field \(k(a^{1/p})\) linearly disjoint from \(k(x)/k;\) and we have said above how to meet this. If the extension is inner, the ring to be constructed does not change, but we have to compute the ideal of relations for \((x_1, \cdots, x_n)\) over the (new) base field \(k(a^{1/p});\) if \(a^{1/p} = f(x)/g(x)\) with \(f, g \in k[X],\) then this is \((P, a^{1/p}g(x) - f(x)); g(x)^{p-1},\) as one easily checks.

The third subsidiary problem was to count the number of steps. The above considerations involve no new difficulty in this regard.

**BIBLIOGRAPHY**


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720