ANNALES SCIENTIFIQUES
DE L'UNIVERSITÉ DE CLERMONT-FERRAND 2
Série Mathématiques

DAVID F. ANDERSON
DAVID E. DOBBS
MOSHE ROITMAN

Root closure in commutative rings

Annales scientifiques de l'Université de Clermont-Ferrand 2, tome 95, série *Mathématiques*, nº 26 (1990), p. 1-11
<http://www.numdam.org/item?id=ASCFM_1990__95_26_1_0>

Ann. Sci. Univ. "Blaise Pascal", Clermont II, Sér. Math., Fasc. 26ème, pp. 1-11

ROOT CLOSURE IN COMMUTATIVE RINGS

David F. Anderson* and David E. Dobbs
University of Tennessee
Knoxville, Tennessee 37996-1300, U.S.A.

Moshe Roitman**
University of Haifa
Mount Carmel, Haifa 31999, ISRAEL

0. Introduction.

When solving polynomial equations by radicals over a field K, one generally cannot express the solutions as rational functions of roots of elements in K. For example, to express the radical $\sqrt{1+\sqrt{1+\sqrt{2}}}$ over $\mathbb{Q}$, one has to extract roots in 3 steps and no fewer: $\mathbb{Q} \underset{\neq}{\subset} \mathbb{Q}(\sqrt{2}) \underset{\neq}{\subset} \mathbb{Q}(\sqrt{1+\sqrt{2}}) \underset{\neq}{\subset} \mathbb{Q}(\sqrt{1+\sqrt{1+\sqrt{2}}})$ (Example 2.1(b) below). More generally, this paper deals with the question of how many steps are needed to obtain the "total root closure" of a given domain. Often the number of steps is infinite (Example 2.1(a)). Even though the number of steps is finite for any affine domain, it is

*D.F. Anderson was supported in part by a National Security Agency grant.
**M. Roitman thanks the University of Tennessee at Knoxville for its hospitality during his visit in August 1989.

unbounded in the class of affine domains (Theorem 2.2 and Example 2.1(b)).

For background and related work, see [BCM], [An], and especially [A], [AII], and the references in all these papers.

1. Preliminaries.

We first present some basic conventions, definitions and facts. Throughout this paper, we denote by S a nonempty subset of $\mathbb{N} = \{1, 2, 3, \ldots\}$. All rings in this paper are commutative with identity.

We assume in this section that $A \subseteq B$ are rings. The ring A is called S-root closed in B if whenever $b \in B$ and $b^n \in A$ for *some* n in S, then $b \in A$. The ring A is called S-closed in B if whenever $b \in B$ and $b^n \in A$ for *all* n in S, then $b \in A$. (See [A, §3, especially Theorem 3.2]). These two definitions coincide in case S contains just one element n; we say in this case that A is n-root closed in B. In this paper, we will use mainly the first definition.

The smallest subring of B which contains A and is S-root closed in B is called the total S-root closure of A in B and is denoted by $\mathfrak{R}^S_\infty(A, B)$. Thus $\mathfrak{R}^S_\infty(A, B)$ is the intersection of all the subrings of B which contain A and are S-root closed in B. For $0 \le m < \infty$, define $\mathfrak{R}^S_m(A, B)$ inductively as follows: $\mathfrak{R}^S_0(A, B) = A$; and for $m > 0$, $\mathfrak{R}^S_m(A, B)$ is the subring of B generated by $\mathfrak{R}^S_{m-1}(A, B)$ and the elements $b \in B$ such that $b^n \in \mathfrak{R}^S_{m-1}(A, B)$ for some $n \in S$. Thus for $0 < m < \infty$, $\mathfrak{R}^S_m(A, B) = \mathfrak{R}^S_1(\mathfrak{R}^S_{m-1}(A, B), B)$. Note that if $S \subseteq T$, then $R^S_m(A, B) \subseteq R^T_m(A, B)$ for all $0 \le m \le \infty$. In case $S = \mathbb{N}$, we delete reference to S; so the total root closure means the total $\mathbb{N}$-root closure. If

$S = \{n\}$, we write $\mathfrak{R}^n_m(A, B)$ rather than $\mathfrak{R}^{\{n\}}_m(A, B)$.

Rather than representing the total S-root closure as an intersection, the following proposition represents it more explicitly as an ascending union.

PROPOSITION 1.1. Let $A \subseteq B$ be rings. Then $\mathfrak{R}^S_\infty(A, B) = \bigcup_{0 \le m < \infty} \mathfrak{R}^S_m(A, B)$.

PROOF. Since $\mathfrak{R}^S_\infty(A, B)$ is S-root closed in B, we obtain by induction on m that $\mathfrak{R}^S_m(A, B) \subseteq \mathfrak{R}^S_\infty(A, B)$ for all $0 \le m < \infty$; so $D := \bigcup_{0 \le m < \infty} \mathfrak{R}^S_m(A, B) \subseteq \mathfrak{R}^S_\infty(A, B)$. On the other hand, let $b \in B$ and $n \in S$ such that $b^n \in D$. There is an integer m such that $b^n \in \mathfrak{R}^S_m(A, B)$, so $b \in \mathfrak{R}^S_{m+1}(A, B)$. It follows that the ring D is S-root closed in B, so $\mathfrak{R}^S_\infty(A, B) \subseteq D$, and we have equality. □

Let S be a subset of $\mathbb{N}$. We denote by $D(S)$ the set of all divisors of integers in S. The set S will be called divisorially closed if $S = D(S)$. Of course, $D(S)$ is always divisorially closed. Moreover, it is easy to show that for all $0 \le m \le \infty$, $\mathfrak{R}^S_m(A, B) = \mathfrak{R}^{D(S)}_m(A, B)$. However, on the other hand, we have

EXAMPLE 1.2. Let S and T be two distinct divisorially closed subsets of $\mathbb{N}$. We can assume that $S \nsubseteq T$, and let $r \in S \setminus T$. Let F be a field of characteristic 0, and X an indeterminate over F. Let $A = F[X^r]$ and $B = F[X]$. Clearly $\mathfrak{R}^S_1(A, B) = B$. However, $X \notin \mathfrak{R}^T_1(A, B)$. Otherwise, there exists $g \in B$ and $t \in T$ such that $g^t \in A$ and the coefficient of X in g is nonzero. If the constant coefficient of g is nonzero, then X has a nonzero coefficient in g^t (since char(F) = 0) , whence $X \in A$ and $r = 1$, a contradiction. So we can assume that the constant coefficient of g is zero, whence $X^t \in A$. Hence r is a divisor of t and $r \in D(T) = T$, a contradiction. It follows that $\mathfrak{R}_1^S(A, B) \neq \mathfrak{R}_1^T(A, B)$. □

Let $\langle S \rangle$ be the multiplicative submonoid of $\mathbb{N}$ generated by S (by definition, $1 \in \langle S \rangle$) . It is easy to see that $\mathfrak{R}_\infty^S(A, B) = \mathfrak{R}_\infty^{\langle S \rangle}(A, B)$. Thus, A is S-root closed in B if and only if A is $\langle S \rangle$-root closed in B .

PROPOSITION 1.3. Let P be the set of primes which divide some integer in S. Then $\mathfrak{R}_\infty^S(A, B) = \mathfrak{R}_\infty^P(A, B)$.

PROOF. Evidently, $\langle D(S) \rangle = \langle P \rangle$. Hence $R_\infty^S(A, B) = R_\infty^{D(S)}(A, B) = R_\infty^{\langle D(S) \rangle}(A, B) = R_\infty^{\langle P \rangle}(A, B) = R_\infty^P(A, B)$. □

EXAMPLE 1.4. Let P and Q be two distinct sets of primes in $\mathbb{N}$. Assume that $P \not\subseteq Q$. In Example 1.2 above, take $S = P$ and $T = Q$. We have, for all $0 \leq m \leq \infty$, $B = \mathfrak{R}_\infty^P(A, B) \neq \mathfrak{R}_\infty^Q(A, B)$. □

If A is a domain with quotient field $Q(A)$, the <u>S-total root closure of</u> A is defined as $\mathfrak{R}_\infty^S(A, Q(A))$, and denoted by $\mathfrak{R}_\infty^S(A)$. Similarly, define $\mathfrak{R}_m^S(A)$ for all $0 \leq m \leq \infty$. Also, $\mathfrak{R}_m(A)$ means $\mathfrak{R}_m^{\mathbb{N}}(A, Q(A))$; and a root closed domain means as usual a domain which is root closed in its quotient field.

We now return to the general case of rings. The transitivity of the S-root closure is straightforward. More precisely, we have the following easy

PROPOSITION 1.5. Let $A \subseteq B \subseteq C$ be rings such that B is S-root closed in C. Then A is S-root closed in B if and only if A is S-root closed in C.

Similarly, we have

PROPOSITION 1.6. Let $A \subseteq B \subseteq C$ be rings such that B is S-closed in C. Then A is S-closed in B if and only if A is S-closed in C.

THEOREM 1.7. Let A and B be rings with a common ideal I. Then A is S-root closed in B if and only if A/I is S-root closed in B/I. Moreover, if $\nu : B \to B/I$ is the canonical homomorphism and $0 \leq m \leq \infty$, then

$$\mathfrak{R}_m^S(A, B) = \nu^{-1}(\mathfrak{R}_m^S(A/I, B/I)) .$$

PROOF. The theorem follows from the fact that for $b \in B$ and $n \in \mathbb{N}$, $b^n \in A$ if and only if $(b + I)^n \in A/I$. □

In particular, let F be a field, D a subring of F, B a ring containing F, and I a proper ideal of B. Then $D + I$ is S-root closed in $F + I$ if and only if D is S-root closed in F. (This follows from Theorem 1.7 since we have canonical isomorphisms $(F + I)/I \cong F$ and $(D + I)/I \cong D$.) If we assume in addition that $I \neq 0$ and $F + I$ is an S-root closed domain, then $D + I$ is S-root closed if and only if D is S-root closed in F. Indeed, let K be the quotient field of $F + I$ (and also of $D + I$, since $I \neq 0$). Then by Proposition 1.5 and Theorem 1.7, $D + I$ is S-root closed (in K) $\Leftrightarrow D + I$ is S-root closed in $F + I$ $\Leftrightarrow D$ is S-root closed in

F. This generalizes [A, Lemma 2.1(c)].

For further applications of Theorem 1.7, let $A \subseteq B$ be given rings. Then by Theorem 1.7, for all $0 \le m \le \infty$, we have $\mathfrak{R}^S_m(A + XB[X], B[X]) = \mathfrak{R}^S_m(A, B) + XB[X]$. In particular, let $A = F$ and $B = K$ be fields. Thus by Proposition 1.5 and Theorem 1.7, $\mathfrak{R}^S_m(F + XK[X]) = \mathfrak{R}^S_m(F + XK[X], K(X)) = \mathfrak{R}^S_m(F + XK[X], K[X]) = \mathfrak{R}^S_m(F, K) + XK[X]$. This enables us to obtain examples regarding $\mathfrak{R}^S_m(D)$ for a domain D using constructions of the type $\mathfrak{R}^S_m(F, K)$, where F and K are fields. (Instead of the polynomial extension $B[X]$, one can also use the power series extension $B[[X]]$.)

As a further illustration of Theorem 1.7, applying the previously described method to Example 1.2, one obtains a domain D such that $\mathfrak{R}^S_1(D) \neq \mathfrak{R}^T_1(D)$. A similar remark holds for Example 1.4.

By analogy with Theorem 1.7, we have

THEOREM 1.8. Let A and B be rings with a common ideal I. Then A is S-closed in B if and only if A/I is S-closed in B/I.

We recall (cf. Swan [S]) that a domain A is <u>seminormal</u> if and only if it is $\{2, 3\}$-closed in its quotient field. Note that if x is an element in an extension domain of A such that x^2 and x^3 are in A, then $x \in Q(A)$. (Indeed, if $x \neq 0$, then $x = x^3/x^2 \in Q(A)$.)

Using Theorem 1.8 and Proposition 1.6, we obtain:

COROLLARY 1.9. Let $A \subseteq B$ be domains with a common nonzero ideal $I \neq B$. If A/I is $\{2,3\}$-closed in B/I and B is seminormal, then A is seminormal.

COROLLARY 1.10. If $D_1 \subseteq D_2$ are seminormal domains, then the domains $D_1 + XD_2[X]$ and $D_1 + XD_2[[X]]$ are also seminormal.

PROOF. D_1 is seminormal in (i.e., {2, 3}-closed in) D_2, by the above remarks. For the first assertion, apply Corollary 1.9, with $A = D_1 + XD_2[X]$, $B = D_2[X]$ and $I = XD_2[X]$. (One also needs the fact that the polynomial ring and the power series ring over a seminormal domain are seminormal: cf. [BCM], [BN].) Similarly, use $A = D_1 + XD_2[[X]]$ for the second remark.□

The preceding corollary can be generalized to any number of variables.

2. <u>The number of steps for the total root closure</u>.

EXAMPLE 2.1. (a) *A quasilocal one-dimensional seminormal domain* A *such that for all* $0 \leq m < \infty$, $\mathfrak{R}_m(A) \subsetneq \mathfrak{R}_{m+1}(A)$. *Moreover, for every finite* m, $\mathfrak{R}_m(A)$ *is generated as an* A*-algebra by one element.*

(b) *For each positive integer* m, *a quasilocal (resp., affine) one-dimensional seminormal domain* A *such that* $A = R_0(A) \subsetneq R_1(A) \subsetneq \dots \subsetneq R_m(A) = R_\infty(A)$; *i.e., the total root closure of* A *is obtained in exactly* m *steps. Moreover,* $R_\infty(A)$ *is generated as an* A*-algebra by one element.*

(a) Define inductively a sequence (v_n) of positive real numbers: $v_0 = 1$

and for $n > 0$, $v_n = \sqrt{1 + v_{n-1}}$. Clearly $v_n > 1$ for $n \geq 1$ and $\mathbb{Q}(v_0) \subseteq \mathbb{Q}(v_1) \subseteq \ldots$. Set $K = \mathbb{Q}(v_0, v_1, \ldots)$.

We prove by induction on $n \geq 1$ that $v_n \notin \mathbb{Q}(v_{n-1})$. This is evident for $n = 1$ since $\sqrt{2}$ is irrational. Now suppose, as induction hypothesis, that $v_n \notin \mathbb{Q}(v_{n-1})$ for some $n \geq 1$. Then $N_{\mathbb{Q}(v_n)/\mathbb{Q}(v_{n-1})}(v_{n+1}^2)$ $= N_{\mathbb{Q}(v_n)/\mathbb{Q}(v_{n-1})}(1 + v_n) = (1 + v_n)(1 - v_n) = -v_{n-1}$ is negative, and so cannot be a square of an element in $\mathbb{Q}(v_n) \subset \mathbb{R}$. Thus $v_{n+1} \notin \mathbb{Q}(v_n)$, completing the induction step.

Next, we show for $n \geq 1$ that if $y \in \mathbb{Q}(v_n) \backslash \mathbb{Q}(v_{n-1})$ has some power in $\mathbb{Q}(v_{n-1})$, then $v = b\, v_n$ with $b \in \mathbb{Q}(v_{n-1})$. Put $F = \mathbb{Q}(v_{n-1})$ and $v = v_n$. Write $y = a + bv$ for suitable $a, b \in F$, with $b \neq 0$. Without loss of generality, $a \neq 0$; put $c = ba^{-1}$. By hypothesis, $(1 + cv)^k \in F$ for some integer $k \geq 1$. Since $v^2 \in F$, the binomial expansion leads to $\sum_{\substack{i \text{ odd} \\ 1 \leq i \leq k}} \binom{k}{i} (cv)^i \in F$. As v factors out of each term in the sum, and we know (by the previous paragraph) that $v \notin F$, we have $\sum_{\substack{i \text{ odd} \\ 1 \leq i \leq k}} \binom{k}{i} c^i v^{i-1} = 0$. As each $v^{i-1} > 0$ (since $i - 1$ is even) and all the odd powers of c have the same sign, we have $c^i = 0$, and so $c = 0$, the desired contradicton.

Next, we prove by induction on $n \geq 1$ that $v_{n-1} v_n^2$ is not the square of an element in $\mathbb{Q}(v_{n-1})$. This is immediate in case $n = 1$. If $v_n v_{n+1}^2 = r^2$ for some $r \in \mathbb{Q}(v_n)$, then $N_{\mathbb{Q}(v_n)/\mathbb{Q}(v_{n-1})}(v_n v_{n+1}^2) = (-v_n^2)(-v_{n-1}) = v_{n-1} v_n^2$ $= (N_{\mathbb{Q}(v_n)/\mathbb{Q}(v_{n-1})}(r))^2$, contrary to induction hypothesis.

Finally, we proceed to show that $\mathbb{R}_m(\mathbb{Q}, K) = \mathbb{Q}(v_m)$ for all $0 \le m < \infty$. This is clear for $m = 0$. Proceed by induction on m, supposing that $\mathbb{R}_m(\mathbb{Q}, K) = \mathbb{Q}(v_m)$. As $v_{m+1}^2 \in \mathbb{Q}(v_m)$, we have $\mathbb{Q}(v_{m+1}) \subset \mathbb{R}_{m+1}(\mathbb{Q}, K)$. Conversely, suppose $y \in K$ has some power in $\mathbb{R}_m(\mathbb{Q}, K) = \mathbb{Q}(v_m)$. Choose n minimal so that $y \in \mathbb{Q}(v_n)$ and, without loss of generality, $n > m + 1$. Since $m \le n - 2$, some power of y is in $\mathbb{Q}(v_{n-2})$. As shown two paragraphs earlier, this leads to $y = bv_n$ for some $b \in \mathbb{Q}(v_{n-1})$. Thus some power of $b^2 v_n^2$ is in $\mathbb{Q}(v_{n-2})$. It is easy to show that $b^2 v_n^2 \notin \mathbb{Q}(v_{n-2})$ unless $b = 0$. So we can assume that $b^2 v_n^2 = c\, v_{n-1}$ for some $c \in \mathbb{Q}(v_{n-2})$. Applying $N = N_{\mathbb{Q}(v_{n-1})/\mathbb{Q}(v_{n-2})}$, we have $N(v_n^2 v_{n-1}) = N(cb^{-2} v_{n-1}^2)$ is the square of an element in $\mathbb{Q}(v_{n-2})$. However, $N(v_n^2 v_{n-1}) = v_{n-2} v_{n-1}^2$, which we showed above is <u>not</u> the square of an element in $\mathbb{Q}(v_{n-2})$. This (desired) contradiction completes the induction step, and completes the proof that $\mathbb{R}_m(\mathbb{Q}, K) = \mathbb{Q}(v_m)$ for all $0 \le m < \infty$.

Define $A = \mathbb{Q} + XK[[X]]$. By Theorem 1.7 we have for all $0 \le m < \infty$, $\mathfrak{R}_m(A) = \mathbb{Q}(v_m) + XK[[X]]$; so $\mathfrak{R}_m(A) \subsetneq \mathfrak{R}_{m+1}(A)$, as claimed. By Corollary 1.10, A is seminormal. Clearly A satisfies all the stated requirements.

(b) Modify the proof of (a), using $K = \mathbb{Q}(v_m)$ and $A = \mathbb{Q} + X\mathbb{Q}(v_m)[[X]]$ (resp., $A = \mathbb{Q} + X\mathbb{Q}(v_m)[X]$) . □

For any given integer $d \ge 2$, let $Y_1,\dots, Y_{d-1}$ be independent indeterminates over a field K. Let T (resp., T') be the complement of the ideal $(Y_1,\dots, Y_{d-1})$ in $\mathbb{Q}[Y_1,\dots, Y_{d-1}]$ (resp., $K[Y_1,\dots, Y_{d-1}]$). In the preceding example, we may replace A by $\mathbb{Q}[Y_1,\ldots, Y_{d-1}]_T + XK[X, Y_1,\ldots, Y_{d-1}]_T$ in order to obtain an example with Krull dimension d.

We next show that no ring of the kind in Example 2.1(a) can be affine. More precisely, the total root closure of any Noetherian domain with finite normalization is attained in finitely many steps.

THEOREM 2.2. Let A be a Noetherian domain such that $\mathfrak{R}^S_\infty(A)$ is a finitely generated A-module. Then $\mathfrak{R}^S_\infty(A) = \mathfrak{R}^S_m(A)$ for some finite m.

PROOF. $\mathfrak{R}^S_\infty(A)$ is a Noetherian A-module. Hence the chain of submodules $A = \mathfrak{R}^S_0(A, B) \subseteq \mathfrak{R}^S_1(A, B) \subseteq \mathfrak{R}^S_2(A, B) \subseteq \ldots$ stabilizes. Apply Proposition 1.1. □

Let A be a Noetherian domain. The A-module $\mathfrak{R}^S_\infty(A)$ is finitely generated in case the integral closure of A (in its quotient field) is finitely generated. This holds for a large class of domains; see e.g. [M, Ch. 12]. In particular, this holds for affine domains.

The case in which the Noetherian domain A is local and one-dimensional is of special interest. If such A is seminormal, then its integral closure is A-finite. (See [BGR] for more general results.) Thus, by Theorem 2.2, the total root closure of A is obtainable in finitely many steps.

In general, the integral closure of a Noetherian domain need not be finitely generated; the first example of this is due to Y. Akizuki. (See also the examples in [GL] and the references there.) In view of these examples, we conjecture that the total root closure of a Noetherian domain A need not be obtainable in finitely many steps, even if A is local and one-dimensional.

REFERENCES

[A] D.F. ANDERSON, Root closure in integral domains, *J. Algebra* 79(1982), 51-59.

[AII] D.F. ANDERSON, Root closure in integral domains II, *Glasgow Math. J.* 31 (1989), 127-130.

[An] G. ANGERMULLER, Root closure, *J. Algebra* 90(1984), 189-197.

[BGR] V. BARUCCI, S. GABELLI, AND M. ROITMAN, On semi-Krull domains, in preparation.

[BCM] J.W. BREWER, D.L. COSTA AND K. McCRIMMON, Seminormality and root closure in polynomial rings and algebraic curves, *J. Algebra* 58(1979), 217-226.

[BN] J.W. BREWER AND W.D. NICHOLS, Seminormality in power series rings, J. Algebra 82(1983), 282-284.

[GL] K.R. GOODEARL AND T.H. LENAGAN, Constructing bad noetherian local domains using derivations, *J. Algebra* 123 (1989), 478-495.

[M] H. MATSUMURA, *Commutative Algebra* (second edition), Benjamin, New York, 1980.

[S] R.G. SWAN, On seminormality, *J. Algebra* 67(1980), 210-229.

Manuscrit reçu en Février 1990