Prime Ideals That Satisfy Hensel's Lemma

Stephen McAdam

Abstract Nagata proved that (R, P) is a Henselian domain if and only if every integral extension domain of R is quasi-local. We explore, with partial success, how to generalize that result.

Keywords Henselian • Prime ideals • Integral extensions • Integral domains

Subject Classifications: 13A15, 13B22, 13G05, 13J15

1 Introduction

Notation. Throughout, R will be a commutative domain with integral closure R' and Jacobson radical $J(R)$. P will be a nonzero prime ideal of R.

Definition 1. We call P an H-prime if the following holds. For any non-constant monic polynomial $f(X) \in R[X]$, if there exist non-constant monic polynomials $g(X)$ and $h(X)$ in $R[X]$ such that $f(X) = g(X)h(X) \bmod P$ and such that $g(X)$ and $h(X)$ are comaximal (i.e., $g(X)R[X] + h(X)R[X] = R[X]$), then $f(X)$ is reducible in $R[X]$.

The following crucial result is proven in [1, (2.2)].

S. McAdam (✉)
Mathematics Department, RLM 8.100, The University of Texas at Austin,
2515 Speedway - Stop C1200, Austin, TX 78712-1202, USA
e-mail: mcadam@math.utexas.edu

M. Fontana et al. (eds.), *Commutative Algebra: Recent Advances in Commutative Rings, Integer-Valued Polynomials, and Polynomial Functions*, DOI 10.1007/978-1-4939-0925-4_15,

Theorem 1. *Let $P \subseteq J(R)$. The following are equivalent.*

(i) *P is an H-prime.*
(ii) *For all non-constant monic polynomials $f(X) \in R[X]$, if there exist non-constant monic polynomials $g(X)$ and $h(X)$ in $R[X]$ such that $f(X) \equiv g(X)h(X) \bmod P$ and such that $g(X)$ and $h(X)$ are comaximal, then there are monic polynomials $g'(X)$ and $h'(X)$ in $R[X]$ such that $f(X) = g'(X)h'(X)$ and $g(X) \equiv g'(X) \bmod P$ and $h(X) \equiv h'(X) \bmod P$.*

Remark 1. 1. We do not know whether some version of Theorem 1 (i) ⇒ (ii) holds when P is not contained in $J(R)$, although (ii) ⇒ (i) is trivially true.

2. Hensel's lemma says that if R is complete in the P-adic topology, then P satisfies condition (ii) of Theorem 1 and so is an H-prime. (Hence, H-primes do exist.)
3. We will see that when P is not contained in $J(R)$, it is in some sense unlikely for P to be an H-prime. In particular, we will see that if R is Noetherian, and P is an H-prime, then $P \subseteq J(R)$.
4. In the above, when we wrote $g(X)$ and $h(X)$, we assumed they were comaximal. In some references, that is modified to say, $PR[X] + g(X)R[X] + h(X)R[X] = R[X]$. However, the bulk of our interest here will be in the case that $P \subseteq J(R)$, and when that is true, the two conditions are equivalent. This is easily seen, using the fact that if M is a maximal ideal of $R[X]$ and M contains a monic polynomial $k(X)$, then $M \cap R$ is maximal in R. That fact, [5, Lemma 1.1(v)], is an easy consequence of the fact that the integral extension $R \subseteq R[X]/k(X)R[X]$ satisfies going up.

Lemma 1. *Let $P \subseteq Q$ be prime ideals of R. If Q is an H-prime, then so is P.*

Proof. Suppose P is not an H-prime. Then there is an irreducible non-constant monic $f(X) \in R[X]$ and non-constant monic polynomials $g(X)$ and $h(X)$ in $R[X]$ such that $f(X) \equiv g(X)h(X) \bmod P$ and such that $g(X)$ and $h(X)$ are comaximal. However, we also have $f(X) \equiv g(X)h(X) \bmod Q$, and that implies Q is not an H-prime. □

The inspiration for this paper is the following well-known result of Nagata [6, (43.12)].

Theorem 2. *Let (R, P) be a quasi-local domain. Then, P satisfies condition (ii) of Theorem 1 (i.e., an H-prime) if and only if every integral extension domain of R is quasi-local. (When those equivalent conditions hold, (R, P) is called a Henselian domain.)*

The goal of this paper is to try to globalize that and to see if some similar result holds for H-primes that are not the sole maximal ideal their ring R. The first guess might be that P is an H-prime if and only if for every integral extension domain T of R, there is a unique prime of T lying over P. However, when R is Noetherian, that guess is hopelessly wrong, as we now show.

By [2, Theorem 1.1(ii)], if R is Noetherian and if in every integral extension domain of R only one prime ideal lies over P, then R is local and P is its maximal ideal. Hence, if our above guess were correct, it would imply that if P is an H-prime (with R Noetherian), then P would be maximal. However, Lemma 1 shows that is not always the case for H-primes. As our first guess is wrong, we need a more appropriate (possible) extension of Nagata's result. That leads us to our next definition.

Definition 2. We call P a K-prime if there does not exist an integral extension domain T of R such that exactly two primes of T lie over P and those two primes are comaximal in T.

Question 1. How closely related are H-primes and K-primes? Specifically, if $P \subseteq J(R)$, are the concepts of H-prime and K-prime equivalent?

We will prove the following two propositions.

Proposition 1. *If R is integrally closed, then P is an H-prime if and only if it is a K-prime.*

Proposition 2. *Suppose that for all nonzero non-units $y \in R'$, there is a prime ideal Q' of R' containing y such that either $Q' \neq Q'^2$, or R'/Q' is not integrally closed, or the quotient field of R'/Q' is not algebraically closed. If P is a K-prime of R, then $P \subseteq J(R)$ and P is an H-prime.*

Proposition 2 shows that in a very large class of domains, K-primes are H-primes, considerably strengthening the work in [5], in which R' was the integral closure of Noetherian domain. Much less is known about the converse of Proposition 2, Proposition 1 being the most significant case in which it is known to hold.

Example 1. If P is a prime in a Henselian domain (R, Q), then P is both an H-prime and a K-prime. Since every integral extension of R is quasi-local, P must be a K-prime. Since Q is an H-prime, Lemma 1 shows P is an H-prime.

Example 2 (Heitmann). Let T is Noetherian integrally closed non-Henselian domain, and (with Y an indeterminate) let $R = T[[Y]]$ and $P = YR$. Hensel's lemma shows that P is an H-prime. Also, Proposition 1 shows that since R is integrally closed, P is also a K-prime. Finally, [6, (43.4)] shows R is not Henselian.

The present paper constitutes a streamlining and extension of Sects. 2 and 3 of [5]. The improvement of this work over the earlier work is due to the availability of Theorems 1 (above) and 4 (below), both proved in [1] (as well as a new construction given in Sect. 5 below). Section 1 of [5] contains some related facts of interest. Specifically, [5, (1.5(i) $\Leftrightarrow$ (ii)] shows that if R is Noetherian and if P is not a K-prime, then for any $m \geq 1$, there is an integral extension domain T of R in which there are exactly m primes lying over P and those m primes are pairwise comaximal.

2 Proposition 1

Definition 3. Recall that if Q is a prime ideal in a ring R, then a prime q in the polynomial ring $R[X]$ is called an upper to Q if $q \cap R = Q$, but $q \neq QR[X]$. Furthermore, if q is an upper to Q and q contains a monic polynomial, then q is called an integral upper to Q. (All of the facts we use about uppers and integral uppers are easily proven and can be found in [5, Lemma 1.1].)

Lemma 2. *Let $R \subseteq T$ be rings, and let P be a prime ideal of R. Let Q be a prime ideal of T with $Q \cap R = P$, and let $t \in Q$. Then $Q \cap R[t] = (P, t)R[t]$.*

Proof. One inclusion is obvious. For the other, assume that $f(t) \in Q \cap R[t]$ (with f a polynomial with coefficients in R). Since $t \in Q$, we must have the constant coefficient of f in $Q \cap R = P$. Hence $f(t) \in (P, t)R[t]$. □

Lemma 3. *Let P be a prime ideal in a domain R. The following are equivalent.*

(a) P is not a K-prime.
(b) There is an integral extension domain T of R in which the set V of prime ideals lying over P can be partitioned into two nonempty subsets, say $V = V_1 \cup V_2$, such that $\cap\{p \mid p \in V_1\}$ and $\cap\{q \mid q \in V_2\}$ are comaximal in T.
(c) There is an integral upper K to 0 in $R[X]$ such that K is contained in the uppers $(P, X)R[X]$ and $(P, X+1)R[X]$, but in no other uppers to P except those two.
(d) There is an integral extension domain $R[t]$ of R such that the only prime ideals of $R[t]$ that lie over P are $(P, t)R[t]$ and $(P, t+1)R[t]$.

Proof. (d) ⇒ (a) ⇒ (b): These are obvious from the definition of a K-prime.
(b) ⇒ (d): Assuming (b) and using comaximality, pick $t \in T$ with $t \equiv 0 \bmod \cap \{p \mid p \in V_1\}$ and $t \equiv -1 \bmod \cap \{q \mid q \in V_2\}$. As t is contained in each prime in V_1, Lemma 2 shows that every prime ideal in V_1 intersects $R[t]$ at $(P, t)R[t]$. Similarly, since $t + 1 \in \cap\{q \mid q \in V_2\}$, we see that every prime in V_2 intersects $R[t+1] = R[t]$ at $(P, t+1)R[t+1] = (P, t+1)R[t]$. Finally, since all primes in V contract to one of these two primes, lying over in $R[t] \subseteq T$ shows they are the only primes of $R[t]$ lying over P.
(c) ⇔ (d): For an integral extension of domains $R \subseteq R[t]$, let K be the kernel of the map $R[X] \to R[t]$. Thus K is an integral upper to 0 and $R[X]/K$ is isomorphic to $R[t]$. The prime ideals of $R[X]/K$ that lie over P all have the form L/K where L is an upper to P in $R[X]$ with L containing K. The equivalence of (c) and (d) follows easily. □

Lemma 4. *(a) Let R' be an integrally closed domain, and let L be an ideal of $R'[X]$. Then L is an integral upper to 0 if and only if $L = f(X)R'[X]$ for some non-constant monic irreducible polynomial $f(X) \in R'[X]$.*
(b) Let R be an arbitrary domain. If $f(X)$ is a non-constant monic polynomial in $R[X]$ which is irreducible in $R'[X]$, then $f(X)R[X]$ is an integral upper to 0 in $R[X]$.
(c) Let R be an arbitrary domain. If $g(X)$ is a non-constant polynomial, then some upper to 0 in $R[X]$ contains $g(X)$.

Proof. (a) This is well known. (A proof is recorded in [5, Lemma 2.4].)

(b) Suppose R and $f(X)$ are as in (b). By part (a), $f(X)R'[X]$ is an integral upper to 0 in $R'[X]$, and so $f(X)R'[X] \cap R[X]$ is an integral upper to 0 in $R[X]$. However, since $f(X)$ is monic in $R[X]$, an easy exercise shows $f(X)R'[X] \cap R[X] = f(X)R[X]$.

(c) Let F be the quotient field of R. Since $g(X)$ is not a unit of $F[X]$, it is contained in some prime ideal H of $F[X]$. Let $L = H \cap R[X]$. We have $L \cap R = (H \cap R[X]) \cap (F \cap R) = (H \cap F) \cap R = 0 \cap R = 0$. Thus, L is an upper to 0 in $R[X]$, and $g(X) \in L$. □

Proposition 1. *Let R be integrally closed. Then P is an H-prime if and only if it is a K-prime.*

Proof. Suppose P is not an H-prime. Then there exists a non-constant monic irreducible $f(X) \in R[X]$ and comaximal non-constant monic polynomials $g(X)$ and $h(X)$ in $R[X]$ such that $f(X) \equiv g(X)h(X) \bmod P$. By part (a) of the previous lemma, $R \subseteq R[X]/f(X)R[X]$ is an integral extension of domains. The primes of the larger domain that lie over P in R all have the form $L/f(X)R[X]$, with L an upper to P in $R[X]$ that contains $f(X)$. In other words, they are the images in $R[X]/f(X)R[X]$ of those uppers L to P that contain $f(X)$. As $f(X) \equiv g(X)h(X) \bmod P$ with $g(X)$ and $h(X)$ comaximal, that set of L can be partitioned into those L that contain $g(X)$ and those L that contain $h(X)$. Thus, the set of primes lying over P is $V = V_1 \cup V_2$, with $V_1 = \{L/f(X)R[X] \mid L$ is an upper to P containing $f(X)$ and $g(X)\}$ and $V_2 = \{L/f(X)R[X] \mid L$ is an upper to P containing $f(X)$ and $h(X)\}$. The comaximality of $g(X)$ and $h(X)$ shows that union is disjoint and also shows that the comaximality of $\cap\{q \mid q \in V_1\}$ and $\cap\{q \mid q \in V_2\}$. We claim that neither set in that union is empty. For that, it will suffice (by symmetry) to show that there does exist an upper L to P in $R[X]$ with $f(X) \in L$, such that $g(X) \in L$. Letting g' represent $g(X) \bmod P$, part (c) of the previous lemma shows there is an upper L' to 0 in $(R/P)[X]$ with $g'(X) \in L'$. Now it is easily seen that L' has the form $L/PR[X]$ for some upper L to P in $R[X]$, with $g(X) \in L$. Since $f(X) - g(X)h(X) \in PR[X] \subseteq L$, we also have $f(X) \in L$. That proves the claim. Finally, using Lemma 3((b) ⇒ (a)), P is not a K-prime.

Conversely, suppose P is not a K-prime. By Lemma 3((a) ⇒ (c)), there is an integral upper K to 0 in $R[X]$ such that K is contained in the uppers $(P, X)R[X]$ and $(P, X + 1)R[X]$, but in no other uppers to P except those two. By Lemma 4(a), $K = f(X)R[X]$ for some non-constant monic irreducible polynomial $f(X) \in R[X]$. Thus, the only uppers to P in $R[X]$ that contain $f(X)$ are (P, X) and $(P, X + 1)$. It easily follows that the factorization of $f(X) \bmod P$ has the form $X^n(X + 1)^m$ (since if there was another factor, Lemma 4(c) applied to R/P would show that a third upper to P also contains $f(X)$). That shows P is not an H-prime. □

3 Concerning K-Primes P Not Contained in $J(R)$

Lemma 5. *Let D be a domain between R and its quotient field, and let $C = \{r \in R \mid rd \in R$ for all $d \in D\}$ (the conductor of D to R). Suppose Q is a prime ideal in R comaximal to C, and let q be a prime ideal of D lying over Q. Then the following are true.*

(a) *For all $n \geq 1$, $q^n \cap R = Q^n$.*
(b) *For all $n \geq 1$, the following are equivalent:*

  (i) $Q^n \neq Q^{n+1}$;
  (ii) $q^n \neq q^{n+1}$;
  (iii) $Q^n \not\subseteq q^{n+1}$.

(c) $R/Q = D/q$.

Proof. (a) Suppose $q^n \cap R$ properly contains Q^n. Then there exist $s_{ij} \in q$ with $r = \sum_{j=1}^{m} \prod_{i=1}^{n} s_{ij} \in (q^n \cap R) - Q^n$. Now $(Q^n : r) = \{x \in R \mid xr \in Q^n\}$ is a proper ideal of R and consists of zero divisors modulo Q^n. By Zorn's lemma, it can be enlarged to an ideal N maximal with respect to consisting of zero divisors modulo Q^n, and by a standard argument [3, Theorem 1], N is a prime ideal of R. As $Q^n \subseteq (Q^n : r) \subseteq N$, we have $Q \subseteq N$, so that C is not contained in N. Pick $c \in C - N$. Now $c^n r = \sum_{j=1}^{m} \prod_{i=1} (cs_{ij}) \in Q^n$, since each $cs_{ij} \in q \cap R = Q$. Thus $c^n \in (Q^n : r) \subseteq N$. That contradicts that c is not in N. Thus $q^n \cap R = Q^n$.

(b) Obviously (iii) implies (ii). Suppose (ii) holds, and let $y \in q^n - q^{n+1}$. As C and Q are comaximal, write $1 = c + z$ with $c \in C$ and $z \in Q$. Raising both sides to the nth power, we can write $1 = c^n + w$ with $w \in Q$. We have $y = c^n y + wy$. Now $wy \in Qq^n \subseteq q^{n+1}$, and since y is not in q^{n+1} we must have $c^n y \notin q^{n+1}$. Thus, $c^n y \notin Q^{n+1}$. However, since $y \in q^n$ and $Cq \subseteq Q$, we have $c^n y \in Q^n$. Thus (i) holds. Finally, suppose (i) holds. Then (iii) follows, since part (a) shows $q^{n+1} \cap R = Q^{n+1}$.

(c) We have the natural embedding $R/Q \subseteq D/q$. In order to show equality, it will suffice to show that for all $y \in D$, there is a $t \in R$ with $t - y \in q$. By comaximality, there is a $c \in C$ with $c - 1 \in Q \subseteq q$. We have $yc - y \in q$, and so we let $t = yc$, which is in R. □

Lemma 6. *The following are equivalent for a domain D.*

(i) *D is integrally closed, and its quotient field is algebraically closed.*
(ii) *Every non-constant monic polynomial in $D[X]$ can be factored into a product of monic linear polynomials in $D[X]$.*

Proof. Suppose (i) is true, and let $f(X)$ be a non-constant monic polynomial in $D[X]$. With Ω the algebraically closed quotient field of D, in $\Omega[X]$ we see that $f(X)$ factors into a product of linear polynomials. Let $X - b$ be one of them. Since $f(b) = 0$, b is integral over D, and so $X - b$ is in $D[X]$. Thus (ii) holds.

Now suppose (ii) holds. Let Ω be an algebraic closure of the quotient field of D, and let T be the integral closure of D in Ω. Since Ω is algebraic over the quotient field of D, a standard argument shows Ω is the quotient field of T. Therefore, it will suffice to show $D = T$. Pick any $t \in T$. There is a monic polynomial in $D[X]$ having t as a root. By (ii), that monic polynomial factors into a product of monic linear factors in $D[X]$. Clearly one of those factors must be $X - t$, showing $t \in D$. Thus $D = T$. □

We come to the main result of this section.

Theorem 3. *Suppose P is not contained in the Jacobson radical of R, and let Q be a prime of R comaximal to P. Consider the following three statements.*

(i) $Q \neq Q^2$;
(ii) R/Q *is not integrally closed;*
(iii) the quotient field of R/Q *is not algebraically closed.*

(a) If any of (i), (ii), or (iii) is true, then P is not an H-prime.
(b) If the conductor C of R' to R is comaximal to Q, and if any of (i), (ii), or (iii) is true, then P is not a K-prime.

Proof. (a) Suppose first that $Q \neq Q^2$. Pick $d \in Q - Q^2$. Since P is comaximal to Q and also to Q^2, by the Chinese remainder theorem, pick $b \in R$ with $b \equiv d \bmod Q$ and $b \equiv 1 \bmod P$, and pick $c \in R$ with $c \equiv d \bmod Q^2$ and $c \equiv 0 \bmod P$. Let $f(X) = X^2 + bX + c$. Clearly $f(X) \equiv X(X+1) \bmod P$. Thus, to show P is not an H-prime, it will suffice to show $f(X)$ is irreducible in $R[X]$. That follows from Eisenstein's criterion, since $d \in Q - Q^2$, implies $b \in Q$ and $c \in Q - Q^2$.

Next, suppose either (ii) or (iii) is true. Then Lemma 6 shows there is some monic irreducible polynomial $\alpha(X) \in (R/Q)[X]$ of degree $n \geq 2$. Let $k(X)$ be a monic pre-image of $\alpha(X)$ in $R[X]$. As P and Q are comaximal, by the Chinese remainder theorem, there is a monic polynomial $f(X) \in R[X]$ with $f(X) \equiv k(X) \bmod Q$ and $f(X) \equiv X^{n-1}(X+1) \bmod P$. The image of $f(X)$ in $(R/Q)[X]$ is $\alpha(X)$ which is irreducible in $(R/Q)[X]$, and so $f(X)$ is irreducible in $R[X]$. The factorization of $f(X) \bmod P$ therefore shows that P is not an H-prime.

(b) The proof is similar to that of (a), except we must move matters from R up to R', since the $f(X) \in R[X]$ mentioned in the proof of (a) will now need to be irreducible in $R'[X]$.

First suppose that $Q \neq Q^2$. Let Q' be a prime ideal of R' lying over Q. Using Lemma 5(b)((i) $\Rightarrow$ (iii)), we see that Q is not contained in Q'^2. Pick $d \in Q - Q'^2$, and pick b and c as in the proof of (a). Let $f(X) = X^2 + bX + c$. We have $b \in Q \subseteq Q'$ and (since $c - d \in Q^2 \subseteq Q'^2$)$c \in Q' - Q'^2$. Eisenstein's criterion shows $f(X)$ is irreducible in $R'[X]$. By Lemma 4(b), $K = f(X)R[X]$ is an integral upper to 0 in $R[X]$. However, we also have $f(X) \equiv X(X+1) \bmod P$, showing that K is contained in $(P, X)R[X]$ and $(P, X+1)R[X]$, but in no other uppers to P in $R[X]$. By Lemma 3((c) $\Rightarrow$ (a)), P is not a K-prime.

Now suppose that either R/Q is not integrally closed or its quotient field is not algebraically closed. Let $\alpha(X)$, $k(X)$, and $f(X)$ be as in the second half of the proof of part (a). Let Q' be a prime ideal of R' lying over Q. Using Lemma 5(c), the image of $f(X)$ in $(R/Q)[X] = (R'/Q')[X]$ is $\alpha(X)$, which is irreducible, and so $f(X)$ is irreducible in $R'[X]$. Thus $K = f(X)R[X]$ is an integral upper to 0 in $R[X]$. Since $f(X) \equiv X^{n-1}(X+1) \bmod P$, Lemma 3((c) $\Rightarrow$ (a)) shows P is not a K-prime. □

Heuristic Remark: If P is an H-prime not contained in $J(R)$, then for every ideal Q comaximal to P, we must have (i), (ii), and (iii) of Theorem 3 all be false. We feel that justifies saying that H-primes not contained in the Jacobson radical are rather rare. In particular, since the Krull intersection theorem shows that for any prime $Q \neq 0$ in a Noetherian domain we have $Q \neq Q^2$, we see that in a Noetherian domain, P can only be an H-prime if $P \subseteq J(R)$. Similarly, K-primes not contained in the Jacobson radical are somewhat rare. However, Example 3 below shows both H-primes and K-primes not contained in $J(R)$ do exist.

The next corollary is the first of three key pieces in the proof of Proposition 2.

Corollary 1. *Suppose P is not contained in the Jacobson radical of R, and suppose P is also an ideal of R'. Let Q be a prime of R comaximal to P, and let Q' be a prime ideal of R' lying over Q. If any one of the following three conditions holds, then P is neither an H-prime nor a K-prime.*

(i) $Q' \neq Q'^2$;
(ii) *R'/Q' is not integrally closed;*
(iii) *the quotient field of R'/Q' is not algebraically closed.*

Proof. Since P is an ideal in R', we have $PR' \subseteq P \subseteq R$, so that $P \subseteq C$, the conductor of R' to R. Therefore, Q is also comaximal to C. Using Lemma 5, we see that $Q' \neq Q'^2$ if and only if $Q \neq Q^2$, and also $R/Q = R'/Q'$. The corollary now follows from the theorem.

The hitch in the corollary is the need to have P be an ideal in R'. In Sect. 5, we deal with that problem by mimicking P with a prime we will call $P^{\#}$. □

Example 3. Suppose R is the integral closure of the integers in the algebraic closure of the rationals. If $P \neq 0$ is a prime ideal of R, then P is an H-prime and a K-prime.

Proof. Suppose P is not an H-prime. Then there is a monic irreducible $f(X) \in R[X]$ such that $f(X)$ is reducible modulo P. That last implies the degree of $f(X)$ is at least 2. However, as $f(X)$ is irreducible, Lemma 6 shows the degree of $f(X)$ is 1, a contradiction. Thus P is an H-prime, and so by Proposition 1, it is also a K-prime. □

4 Going Down from Maximals

We begin with another crucial result proven in [1, (2.3)]. (As in Theorem 1, we do not know if the assumption $P \subseteq J(R)$ is required.)

Theorem 4. *Let $P \subseteq J(R)$. The following are equivalent.*

(i) P is an H-prime.
(ii) For all non-constant monic polynomials $f(X) \in R[X]$, if there exist non-constant monic polynomials $g(X)$ and $h(X)$ in $R[X]$ such that $f(X) \equiv g(X)h(X) \bmod P$ and such that $g(X)$ and $h(X)$ are comaximal, then for any upper K to 0 in $R[X]$ with $f(X) \in K$, either K and $g(X)$ are comaximal or K and $h(X)$ are comaximal.

Definition 4. We say that P is a GDM prime if for all integral extension domains T of R and all maximal ideals N of T, there is a prime ideal Q of T such that $Q \subseteq N$ and $Q \cap R = P$. (By letting $T = R$, we see that a GDM prime must be contained in $J(R)$.)

Remark 2. GDM stands for "going down from maximals." In [5], GDM was defined in terms of finitely generated integral extensions. However, by Lemma 8, it is easily seen that it does not matter if we allow T to be arbitrary, or insist that it be finitely generated, or even insist that it be generated by a single element over R. All are equivalent.

In this section, we will show that if P is both a K-prime and a GDM prime, then P is an H-prime. (Later, we will see that in many domains, K-primes are GDM primes and so are H-primes.) The next result is the second key piece in the proof of Proposition 2.

Theorem 5. *If P is a K-prime and a GDM prime, then P is an H-prime.*

Proof. It will suffice for us to assume that P is a GDM prime but not an H-prime and to prove that P is not a K-prime. Since we know GDM primes are contained in the Jacobson radical, Theorem 4 shows there are non-constant monic polynomials $f(X)$, $g(X)$, and $h(X)$ in $R[X]$ and an upper, K, to 0 in $R[X]$ such that $f(X) \equiv g(X)h(X) \bmod P$, with $g(X)$ and $h(X)$ comaximal and with $f(X) \in K$, such that K is not comaximal to either $g(X)$ or $h(X)$.

Let $V = \{p \in \operatorname{Spec} R[X] \mid p \text{ is an upper to } P \text{ and } K \subseteq p\}$. If $p \in V$, then $f(X) \in K \subseteq p$, and since $f(X) \equiv g(X)h(X) \bmod P$ (and $P \subseteq p$), we see that either $g(X) \in p$ or $h(X) \in p$. Thus if $V_g = \{p \in V \mid g(X) \in p\}$ and $V_h = \{p \in V \mid h(X) \in p\}$, then $V = V_g \cup V_h$. Since $g(X)$ and $h(X)$ are comaximal in $R[X]$, clearly V_g and V_h partition V.

We claim neither V_g nor V_h is empty. (The argument used in the analogous claim in the proof of Proposition 1 will not work here, since we only have $f(X) \in K$ instead of $K = f(X)R[X]$.) Since K is not comaximal to $g(X)$, there is a maximal ideal N of $R[X]$ that contains both K and $g(X)$. Now N/K is a maximal ideal in $R[X]/K$, and this last ring is an integral extension domain of R. Since P is assumed to be a GDM prime, there must be a prime ideal p'/K of $R[X]/K$ with $p'/K \subseteq N/K$ and with $(p'/K) \cap R = P$. We easily see that p' is an upper to P in $R[X]$ such that $K \subseteq p' \subseteq N$. Thus $p' \in V = V_g \cup V_h$. Suppose $p' \in V_h$. Then by definition, $h(X) \in p' \subseteq N$. However, N also contains $g(X)$, which contradicts that $g(X)$ and $h(X)$ are comaximal. Therefore, p' is not contained in V_h and so must be contained in V_g, which is therefore not empty. Similarly, V_h is not empty.

We easily see that in the integral extension domain $R[X]/K$ of R, the set of primes lying over P is $\{p/K \mid p \in V\} = \{p/K \mid p \in V_g\} \cup \{p/K \mid p \in V_h\}$. Neither subset in this partition is empty (by the preceding paragraph). Also, if g' and h' represent $g(X)$ and $h(X)$ taken modulo K, then since $g(X)$ and $h(X)$ are comaximal in $R[X]$, g' and h' are comaximal in $R[X]/K$. It follows that $\cap\{p/K \mid p \in V_g\}$ and $\cap\{p/K \mid p \in V_h\}$ are comaximal. It now follows from Lemma 3((b) $\Rightarrow$ (a)) that P is not a K-prime. □

Although we do not need it, the following is perhaps worth recording.

Lemma 7. *Let $R \subseteq T$ be an integral extension of domains. Let Q be prime in T with $Q \subseteq J(T)$, and let $P = Q \cap R$. If Q is an H-prime, then P is an H-prime.*

Proof. Since $Q \subseteq J(T)$, we have $P \subseteq J(R)$. Assuming Q is an H-prime, we will use Theorem 4 to show P is an H-prime. Let $f(X)$, $g(X)$, and $h(X)$ be non-constant monic polynomials in $R[X]$ with $f \equiv g(X)h(X) \bmod P$ and with $g(X)$ and $h(X)$ comaximal. Let K be an upper to 0 in $R[X]$ with $f(X) \in K$. (We must show K is comaximal to either $g(X)$ or $h(X)$.) There is an upper L to 0 in $T[X]$ with $L \cap R[X] = K$. In $T[X]$, we have $f(X) \equiv g(X)h(X) \bmod Q$, and $f(X) \in L$. Since Q is an H-prime contained in $J(T)$, Theorem 4 shows L is comaximal to one of $g(X)$ or $h(X)$. We may suppose L and $g(X)$ are comaximal in $T[X]$. An easy exercise (using going up) shows K and $g(X)$ are comaximal in $R[X]$. □

5 A Useful Construction

Lemma 8. *Let $R \subseteq T$ be rings, and let P be a prime ideal of R and M be a prime ideal of T. Let W be the set of all prime ideals of T that lie over P. If W is not empty, then there is a $p \in W$ such that $p \subseteq M$ if and only if $\cap\{p' \mid p' \in W\} \subseteq M$.*

Proof. One direction is trivial. For the other, assume $\cap\{p' \mid p' \in W\} \subseteq M$. We will show there is some $p \in W$ with $p \subseteq M$. (This task is simple if W happens to be finite.) Let p be a prime of T contained in M and minimal over $\cap\{p' \mid p' \in W\}$. It is well known that p consists of zero divisors modulo that intersection [3, Theorem 84]. That is, if $x \in p$, then there is a y not contained in $\cap\{p' \mid p' \in W\}$ such that $xy \in \cap\{p' \mid p' \in W\}$. Therefore, for some $p' \in W$, we have $y \notin p'$ but $xy \in p'$. It follows that $x \in p'$. This shows that $p \subseteq \cup\{p' \mid p' \in W\}$. Now consider any $x \in p \cap R$. For some $p' \in W$ we have $x \in p' \cap R = P$. Thus, $p \cap R \subseteq P$, and obviously $P \subseteq \cap\{p' \mid p' \in W]\} \subseteq p$, so that $P \subseteq p \cap R$. We now have $p \cap R = P$, showing $p \in W$. Since $p \subseteq M$, that completes the argument. □

Remark 3. Let $R \subseteq T$ be an integral extension of rings. In [4, Proposition 2], it is shown that $R \subseteq T$ satisfies going down if and only if $R \subseteq R[t]$ satisfies going down for all $t \in T$. We leave to the reader the exercise of giving a second proof of that fact, using Lemma 8. Although the two approaches have much in common, we feel that Lemma 8 throws a bit more light on the subject.

Notation. Let $P^\# = \cap\{p' \in \text{Spec } R' \mid p' \cap R = P\}$. Also let $R^\# = R + P^\# = \{r + x \mid r \in R \text{ and } x \in P^\#\}$.

Lemma 9. *$R^\#$ is a domain between R and R'. $P^\#$ is a prime ideal in $R^\#$ (and an ideal in R') and is the only prime ideal of $R^\#$ lying over P in R.*

Proof. Obviously $R \subseteq R^\# \subseteq R'$, and using that $P^\#$ is obviously an ideal in R', it is easily verified that $R^\#$ is a domain. The definition of $P^\#$ easily implies $P^\# \cap R = P$. Suppose $r + x$ and $s + y$ are two elements of $R^\#$, with $r, s \in R$ and $x, y \in P^\#$, such that $(r + x)(s + y) \in P^\#$. Since $sx + ry + xy \in P^\#$, we see $rs \in P^\# \cap R = P$, and so we may assume $r \in P \subseteq P^\#$, showing $r + x \in P^\#$. Thus $P^\#$ is a prime ideal of $R^\#$. Finally, suppose Q is any prime ideal of $R^\#$ lying over P in R. Then there is a prime ideal p' in R' with $p' \cap R^\# = Q$, so that $p' \cap R = P$. By definition, we have $P^\# \subseteq p'$, and so $P^\# \subseteq p' \cap R^\# = Q$. As $P^\#$ and Q are both in $R^\#$ and both lie over P, incomparability shows that $Q = P^\#$. Thus $P^\#$ is the unique prime of $R^\#$ lying over P. □

We come to the third and final key piece in our puzzle.

Lemma 10. *(a) P a K-prime if and only if $P^\#$ is a K-prime.*
(b) The following are equivalent.

- *(i) P is a GDM prime.*
- *(ii) $P^\#$ is a GDM prime.*
- *(iii) $P^\# \subseteq J(R^\#)$.*
- *(iv) $P^\# \subseteq J(R')$.*

Proof. (a) Suppose $P^\#$ not a K-prime, so that there is an integral extension T of $R^\#$ in which exactly two primes, say p_1 and p_2, lie over $P^\#$, and p_1 and p_2 are comaximal. Obviously p_1 and p_2 lie over P, and since $P^\#$ is the unique prime of $R^\#$ lying over P, there are no other primes of T lying over P. Thus we see P is not a K-prime.

Conversely, if P is not a K-prime, then by Lemma 3((a) $\Rightarrow$ (c)) there is an integral upper K to 0 in $R[X]$ with K contained in $(P, X)R[X]$ and in $(P, X + 1)R[X]$, but in no other uppers to P. K can be lifted to an integral upper L to 0 in $R^\#[X]$. Since $K \subseteq (P, X)R[X]$ and L lies over K, by going up there is a prime ideal q of $R^\#[X]$ containing L and lying over $(P, X)R[X]$. It is easy to verify that q must be an upper to some prime of $R^\#$ lying over P. The only such prime is $P^\#$, and so q is an upper to $P^\#$. Since $X \in (P, X)R[X] \subseteq q$, we see that q must equal $(P^\#, X)R^\#[X]$. Thus $L \subseteq (P^\#, X)R^\#[X]$. Similarly, $L \subseteq (P^\#, X + 1)R^\#[X]$. Now any upper q' to $P^\#$ containing L contracts to an upper to P containing K. Thus $q' \cap R[X]$ is either $(P, X)R[X]$ or $(P, X+1)R[X]$. Since q' contains either X or $X+1$, it equals either $(P^\#, X)R^\#[X]$ or $(P^\#, X+1)R^\#[X]$. Now Lemma 3((c) ⇒ (a)) shows $P^\#$ is not a K-prime.

(b) (i) ⇒ (iii): Suppose (i) holds. Let M be a maximal ideal of $R^\#$. As $R \subseteq R^\#$ is an integral extension, the definition of GDM prime shows that M contains a prime of $R^\#$ lying over P. The only possibility is that M contains $P^\#$. Thus $P^\# \subseteq J(R^\#)$, and so (i) ⇒ (iii).

(iii) ⇒ (iv): Use that maximal ideals of R' contract to maximal ideals of $R^\#$.

(iv) ⇒ (i): Suppose $P^\# \subseteq J(R')$. We will show P is a GDM prime. Let T be an integral extension domain of R, and let M be a maximal ideal of T. (We must show some prime of T contained in M lies over P.) Let S be the domain gotten by adjoining all the elements of R' to T. Thus $T \subseteq S$ is an integral extension, and so we can lift M to a maximal ideal N of S. As $R' \subseteq S$, $N \cap R'$ is a maximal ideal of R'.

Since (iv) shows $\cap\{p' \in \operatorname{Spec} R' \mid p' \cap R = P\} = P^\# \subseteq N \cap R'$, Lemma 8 shows there is a $p \in \operatorname{Spec} R'$ lying over P, with $p \subseteq N \cap R'$. Since R' (being integrally closed) satisfies the famous going down theorem, there is a prime q of S with $q \cap R' = p$ and $q \subseteq N$. Contracting to T, we see that $q \cap T$ is contained in $N \cap T = M$ and lies over P, showing P is a GDM prime.

(ii) ⇔ (iii): We iterate, now finding $(R^\#)^\#$ and $(P^\#)^\#$. Since $P^\#$ is the unique prime ideal of $R^\#$ lying over P in R, we see that a prime ideal p' in R' lies over $P^\#$ in $R^\#$ if and only if it lies over P in R. Therefore, the definition shows $P^{\#\#} = P^\#$. Also, $R^{\#\#} = R^\# + P^{\#\#} = R^\# + P^\# = R^\#$. Using the equivalence of (i) and (iii) applied to $P^\#$, we now see $P^\#$ is a GDM prime if and only if $P^{\#\#} \subseteq J(R^{\#\#})$ if and only if $P^\# \subseteq J(R^\#)$. □

Corollary 2. *Suppose P is a K-prime. If $P^\# \subseteq J(R^\#)$, then P is an H-prime and a GDM prime (so that $P \subseteq J(R)$).*

Proof. If $P^\# \subseteq J(R^\#)$, by Lemma 10(b), P is a GDM prime. By Theorem 5, P is an H-prime. □

6 Proposition 2 (Slightly Augmented)

Proposition 2. *Suppose that for all nonzero non-units $y \in R'$, there is a prime ideal Q' of R' containing y such that at least one of the following is true: $Q' \neq Q'^2$, or R'/Q' is not integrally closed, or the quotient field of R'/Q' is not algebraically closed. If P is a K-prime of R, then $P \subseteq J(R)$, and P is an H-prime and a GDM prime.*

Proof. Assume P is a K-prime of R. By Corollary 2, it will suffice to show that $P^\# \subseteq J(R^\#)$. If not, let M be a maximal ideal of $R^\#$ not containing $P^\#$, and write $x + y = 1$ with $x \in P^\#$ and $y \in M$. Obviously y is a nonzero non-unit in $R^\#$ and so also in the integral extension R'. By hypothesis, there is a prime ideal Q' of R'

containing y such that either $Q' \neq Q'^2$, or R'/Q' is not integrally closed, or the quotient field of R'/Q' is not algebraically closed. Let $Q = Q' \cap R^{\#}$. Since $y \in Q$, we see that $P^{\#}$ and Q are comaximal. By Corollary 1 applied to $R^{\#}$, and its primes $P^{\#}$ and Q, we see that $P^{\#}$ is not a K-prime. That contradicts Lemma 10(a). □

The next corollary shows that Proposition 2 applies to a large class of domains.

Corollary 3. *Suppose R' satisfies any one of conditions (i) through (iv) below. If P is a K-prime of R, then $P \subseteq J(R)$, and P is an H-prime and a GDM prime.*

(i) There is a subset S of SpecR' *such that $R' = \cap\{R'_{Q'} \mid Q' \in S\}$ and such that for each $Q' \in S$, at least one of the following holds: (i) $Q'^2 \neq Q'$; (ii) R'/Q' is not integrally closed; or (iii) the quotient field of R'/Q' is not algebraically closed.*

(ii) For every maximal ideal M of R', either $M \neq M^2$ or R/M is not algebraically closed.

(iii) R' is an intersection of some set W of quasi-local domains (D_α, N_α), each between R' and its quotient field, such that for each α, $\cap\{N_\alpha^n \mid n \geq 1\} = 0$.

(iv) R' is the intersection of a set of DVRs between R' and its quotient field. (This case includes Krull domains and so includes the case that R is Noetherian.)

Proof. It will suffice to show that in each case, R' satisfies the hypothesis of Proposition 2.

(i) It will suffice to show that if y is a nonzero non-unit in R', then one of the Q' in S contains y. If not, then we would have $y^{-1} \in \cap\{R'_{Q'} \mid Q' \in S\} = R'$, a contradiction.

(ii) This follows from (i), since R equals the intersection of all of its maximal localizations.

(iii) If $N_\alpha = 0$, then (D_α, N_α) must be the quotient field of R' and can be ignored. Thus, we may assume $N_\alpha \neq 0$. Let $Q_\alpha = N_\alpha \cap R'$. For some $0 \neq z \in N_\alpha$, write $z = r/s$ with r and s nonzero in R'. Thus $r = sz \in N_\alpha \cap R = Q_\alpha$, showing $Q_\alpha \neq 0$. Therefore, $Q_\alpha \not\subseteq \cap\{N_\alpha^n \mid n \geq 1\}$. It follows that $Q_\alpha \neq Q_\alpha^2$. By (i), it will suffice to show that every nonzero non-unit y of R' is contained in some Q_α. Were that false, then y would be a unit in each D_α and so a unit in R', which is a contradiction.

(iv) This follows easily from (iii). □

Question 2. Modifying our earlier question, we ask if the concepts of H-prime and K-prime are equivalent for GDM primes?

References

1. W. Heinzer, D. Lantz, Factorization of Monic polynomials. Proc. Am. Math. Soc. **131**, 1049–1052 (2003)
2. W. Heinzer, S. Wiegand, Prime ideals in two-dimensional polynomial rings. Proc. Am. Math. Soc. **107**, 577–586 (1989)
3. I. Kaplansky, *Commutative Rings* (University of Chicago Press, Chicago, 1974)
4. S. McAdam, Going down and open extensions. Can. J. Math **27**, 111–114 (1975)
5. S. McAdam, Strongly comaximizable primes. J. Algebra **170**, 206–228 (1994)
6. N. Nagata, *Local Rings* (Interscience, New York, 1962)