# FACTORIZATION OF MONIC POLYNOMIALS

WILLIAM J. HEINZER AND DAVID C. LANTZ

(Communicated by Wolmer Vasconcelos)

ABSTRACT. We prove a uniqueness result about the factorization of a monic polynomial over a general commutative ring into comaximal factors. We apply this result to address several questions raised by Steve McAdam. These questions, inspired by Hensel's Lemma, concern properties of prime ideals and the factoring of monic polynomials modulo prime ideals.

## 0. INTRODUCTION

There is an interesting relationship between the factorization of monic polynomials and the behavior of prime ideals in integral extensions. This is illustrated for example by the well-known result of Nagata [7, (43.12)] that asserts that a quasilocal integral domain $R$ satisfies Hensel's Lemma if and only if every extension domain integral over $R$ is quasilocal. Other references that deal with this relationship include the papers [2] and [4]. Recent work of Steve McAdam [4], [5], [6] on this topic is the motivation for our interest in the matters considered here. For a prime ideal contained in the Jacobson radical of an integral domain, McAdam [4] introduces the concepts of H-prime, weak-H-prime and quasi-H-prime. The H-primes are precisely those for which a version of Hensel's Lemma holds. The other definitions reflect a careful analysis of the comaximal factorization of monic polynomials.

In Theorem 1.2 we make use of a famous theorem of Quillen-Suslin, a key ingredient in their resolution of the Serre Conjecture, to prove a uniqueness result concerning comaximal factors of a monic polynomial over a general commutative ring. We apply this result to prove in Theorems 2.2 and 2.3 that the concepts of H-prime, weak H-prime and quasi-H-prime are equivalent.

All rings considered here are commutative with unity. Two general references for our notation and terminology are [7] and [3].

## 1. Comaximal factors of monic polynomials

**Remark 1.1.** Let $I, J$ be ideals in a ring $S$ for which $IJ = fS$ where $f$ is a nonzerodivisor in $S$. Then $I, J$ are invertible ideals, i.e., rank-1 projective $S$-modules. Moreover, using subscript $f$ to denote passing to the ring of fractions with respect to the multiplicatively closed system generated by $f$, we have $I_f = S_f = J_f$. Suppose in particular that $S = R[X]$, where $R$ is a ring and $X$ is an indeterminate over $R$, and that $f$ is monic in $R[X]$. Then by the Quillen–Suslin theorem ([9]; [8]; [3, Chapter IV, Theorem 3.14]), $I, J$ are free $R[X]$-modules, i.e., principal ideals generated by nonzerodivisors, and there are generators $p, q$ of $I, J$ respectively for which $f = pq$.

**Theorem 1.2.** *Let $R$ be a ring and $X$ be an indeterminate over $R$. Let $g, h$ be comaximal monic polynomials in $R[X]$, and suppose that the monic polynomial $f$ in $R[X]$ is such that $gh \in fR[X]$. Then $f$ has a factorization of the form $f = pq$ where $g \in pR[X]$ and $h \in qR[X]$. In particular, if $f$ is irreducible in $R[X]$, then either $g \in fR[X]$ or $h \in fR[X]$.*

*Proof.* Let $R[X]_g$ and $R[X]_h$ denote the localizations of $R[X]$ at the multiplicatively closed systems generated by $g$ and $h$ respectively, and let $I := fR[X]_g \cap R[X]$ and $J := fR[X]_h \cap R[X]$. Suppose $g(X)h(X) = f(X)k(X)$, where $k(X) \in R[X]$. Then because

$$h(X) = f(X)k(X)/g(X) \in I \ \text{ and } \ g(X) = f(X)k(X)/h(X) \in J \ ,$$

the ideals $I$ and $J$ are comaximal in $R[X]$; so their intersection, which is

$$fR[X]_g \cap fR[X]_h \cap R[X] = fR[X] \ ,$$

is their product. By Remark 1.1, there are generators $q(X), p(X)$ of $I, J$ respectively for which $f = pq$, $g \in pR[X]$ and $h \in qR[X]$. $\qquad\qquad\square$

**Remark 1.3.** With the notation of Theorem 1.2, if $R$ is an integral domain, the polynomials $p(X), q(X) \in R[X]$ such that $f = pq$ can clearly be chosen to be monic. More generally, if $\operatorname{Spec} R$ is connected, then $p(X)$ and $q(X)$ can be chosen to be monic. To see this, we use the fact that for any ring $S$ and nonconstant polynomial $a(X) \in S[X]$, if $S[X]/(a)$ is a free $S$-module of rank $n$, then there exists a monic polynomial $b$ of degree $n$ in the ideal $(a)$ [3, Prop. 2.2, page 44]; and because $S[X]/(b)$ is also a free $S$-module of rank $n$ of which $S[X]/(a)$ is a homomorphic image, $b$ is a generator of $(a)$. Now in our present context, we have $R[X]/(f) \cong R[X]/(p) \oplus R[X]/(q)$, so $R[X]/(p)$ and $R[X]/(q)$ are locally free $R$-modules. Thus, $\operatorname{Spec} R$ is covered by neighborhoods $\operatorname{Spec} R_i$ on which the extension

of $(p)$ is generated by monic polynomials. Because $\operatorname{Spec} R$ is connected, $R[X]/(p)$ has constant rank and these monic polynomials all have the same degree $n$ and up to units of $R_i$ are extensions of polynomials in $(p)$ of degree $n$. An appropriate $R$-linear combination of these polynomials in $(p)$ gives a monic polynomial of degree $n$ in the ideal $(p)$, and this monic polynomial generates $(p)$. Similarly, the ideal $(q)$ is generated by a monic polynomial if $\operatorname{Spec} R$ is connected.

**Example 1.4.** The hypotheses in Theorem 1.2 that we are working with monic polynomials is necessary: Indeed, let $D$ be a Dedekind domain that is not a principal ideal domain. Let $P$ be a maximal ideal of $D$ that is not principal. Then there exists an irreducible element $f$ in $P - P^2$. Write $fD = PQ_1^{e_1} \cdots Q_n^{e_n}$, where the $Q_i$'s are distinct maximal ideals; because $P$ is not principal, $n > 0$. Let $g \in PQ_1^{e_1} \cdots Q_{n-1}^{e_{n-1}} - Q_n$, and choose $h \in Q_n^{e_n}$ but not in any of the maximal ideals containing $g$. Then $gD + hD = D$ and $gh \in fD$, but $g, h \notin fD$. For a specific example, consider the Dedekind domain $D = \mathbb{Z}[\sqrt{-5}]$ ([1, page 417]). We have $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in this $D$, and 2 and 3 are comaximal, but neither of the irreducible factors on the right side of the equation divides either 2 or 3.

**Example 1.5.** The hypothesis that $g, h$ are comaximal is very necessary: Let $R$ be any integral domain that is not integrally closed, let $a$ be an element of the field of fractions of $R$ that is integral over $R$ but not in $R$, and let $f \in R[X]$ be a monic polynomial of minimal degree of which $a$ is a root. Then $f(X) = (X - a)g(X)$ for some polynomial $g(X)$ over the integral closure of $R$. Let $b, c$ be nonzero elements of $R$ for which $ba \in R$ and $cg(X) \in R[X]$. Then $f$ is irreducible in $R[X]$ and

$$f(X)(f(X) + b(X - a) + cg(X) + bc)$$
$$= (f(X) + b(X - a))(f(X) + cg(X)) \ ,$$

but $f(X)$ divides neither of the factors on the right side of the equation.

Thus over any domain $R$ that is not integrally closed, there exist monic polynomials $f, g, h \in R[X]$ such that $f$ is irreducible and $gh \in fR[X]$, but $g, h \notin fR[X]$. For $R$ an integrally closed domain this phenomenon is not possible; for in this case a monic irreducible in $R[X]$ generates a prime ideal.

## 2. HENSELIAN-LIKE CONDITIONS

In [4], McAdam uses the following definitions:

**Definition 2.1.** Let $P$ be a prime contained in the Jacobson radical of an integral domain $R$. Then $P$ is

(a) an *H-prime* if, for every list of nonconstant monic polynomials $f, g, h$ in $R[X]$ such that $gR[X] + hR[X] = R[X]$ and $f - gh \in PR[X]$, there exist monic $p, q$ in $R[X]$ for which $f = pq$, and $g - p, h - q \in PR[X]$;

(b) a *weak-H-prime* if, for every list of nonconstant monic polynomials $f, g, h$ in $R[X]$ such that $gR[X] + hR[X] = R[X]$ and $f - gh \in PR[X]$, $f$ is reducible; and

(c) a *quasi-H-prime* if, for every list of nonconstant monic polynomials $f, g, h$ in $R[X]$ such that $gR[X] + hR[X] = R[X]$ and $f - gh \in PR[X]$, and for every prime ideal $K$ in $R[X]$ lying over 0 in $R$ and having $f \in K$, either $K + gR[X] = R[X]$ or $K + hR[X] = R[X]$.

**Theorem 2.2.** *A weak-H-prime is an H-prime (and of course conversely).*

*Proof.* Let $P$ be a weak-H-prime in the domain $R$, and let $f, g, h$ be nonconstant monic polynomials in $R[X]$ for which $f - gh \in PR[X]$ and $g, h$ generate the unit ideal in $R[X]$. Denote by overbars images mod $PR[X]$, let $\overline{R} := R/P$ and identify $R[X]/PR[X] \cong \overline{R}[X]$. For each monic irreducible factor $p$ of $f$, we show that either $\overline{g}$ or $\overline{h}$ is in $\overline{p}\,\overline{R}[X]$:

We have $\overline{g}\overline{h} \in \overline{p}\,\overline{R}[X]$ and $\overline{g}$ and $\overline{h}$ are comaximal in $\overline{R}[X]$. Hence by Theorem 1.2, $\overline{p}$ factors into a monic factor of $\overline{g}$ and a monic factor of $\overline{h}$. The latter factors are comaximal because $\overline{g}$ and $\overline{h}$ are comaximal. If both factors were nonconstant, then because $P$ is a weak-H-prime, $p$ would be reducible; so one of the factors is a constant, i.e., 1, and hence either $\overline{g} \in \overline{p}\,\overline{R}[X]$ or $\overline{h} \in \overline{p}\,\overline{R}[X]$.

We proceed by induction on the number $n$ of irreducible factors of $f$. The case where $n = 1$ is clear. Assume the theorem holds for monic polynomials $f$ having $n$ irreducible factors. Suppose $f' = pf$, where $p$ is irreducible and monic, and that $\overline{f'} = \overline{g'h'}$, where $g', h'$ are nonconstant, monic and comaximal. Then by the last paragraph we may assume $\overline{g'} \in \overline{p}\,\overline{R}[X]$. Let $g$ in $R[X]$ be such that $\overline{g'} = \overline{pg}$, and set $h = h'$. Then $\overline{f} = \overline{gh}$ and

$$R[X] = g'R[X] + h'R[X] \subseteq gR[X] + hR[X] + PR[X] \subseteq R[X] .$$

Suppose there is a maximal ideal $M$ of $R[X]$ that contains both $g$ and $h$. Then because $M$ contains monic polynomials, it meets $R$ in a maximal ideal and so contains $P$, a contradiction. Therefore $g, h$ are comaximal. By the induction hypothesis, there exist monic polynomials $g_1, h_1$ in $R[X]$ for which $f = g_1 h_1$, $\overline{g_1} = \overline{g}$, and $\overline{h_1} = \overline{h}$; so $f' = pf = pg_1 h_1$, $\overline{pg_1} = \overline{pg} = \overline{g'}$ and $\overline{h_1} = \overline{h} = \overline{h'}$. This completes the induction and the proof. $\square$

Much of the work needed to prove Theorem 2.3 is done by McAdam in [4]; it merely remains for us to make a few observations and apply the Quillen-Suslin Theorem.

**Theorem 2.3.** *A quasi-H-prime is an H-prime, and conversely.*

*Proof.* McAdam proves in [4, Proposition (2.1)] that an H-prime is a quasi-H-prime; so it remains to prove that a quasi-H-prime is an H-prime. Let $P$ be a quasi-H-prime in the domain $R$, and let $f, g, h$ be nonconstant monic polynomials in $R[X]$ such that $f - gh \in PR[X]$ and $gR[X] + hR[X] = R[X]$. Then by [4, Proposition (2.7)], there are ideals $I, J$ properly containing $fR[X]$ for which

$$\frac{I}{fR[X]} \oplus \frac{J}{fR[X]} = \frac{R[X]}{fR[X]}.$$

It follows that $I$ and $J$ are comaximal in $R[X]$ and intersect in $fR[X]$. Thus as in the proof of Theorem 1.2, $IJ = fR[X]$, so by Remark 1.1, $f$ is the product of generators of the principal ideals $I, J$. Neither generator can be a unit, because $I, J$ both properly contain $fR[X]$ and their product is $fR[X]$. Thus, $f$ is reducible; so $P$ is a weak-H-prime and hence by Theorem 2.2 an H-prime. $\qquad\square$

## References

1. M. Artin, *Algebra*, Prentice Hall, Englewood Cliffs (1991).
2. W. Heinzer and S. Wiegand, *Prime ideals in two-dimensional polynomial rings*, Proc. Amer. Math. Soc. **107** (1989), 577–586.
3. E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston (1985).
4. S. McAdam, *Strongly Comaximizable Primes*, J. Algebra **170** (1994), 206–228.
5. S. McAdam, *Unique factorization of monic polynomials*, Comm. in Algebra (to appear).
6. S. McAdam, *Henselian-like prime ideas*, Abstracts of Papers Presented to the American Mathematical Society **22(2)** (2001), Abstract 964-13-51, 318.
7. M Nagata, *Local Rings*, Interscience, New York (1962).
8. D. Quillen, *Projective modules over polynomial rings*, Inv. Math. **36** (1976), 167–171.
9. A. Suslin, *Projective modules over polynomial rings* (Russian), Dokl. Akad. Nauk S. S. S. R. **26** (1978).

MATHEMATICS DEPARTMENT, PURDUE UNIVERSITY, WEST LAFAYETTE, IN 47907-1395
*E-mail address*: `heinzer@math.purdue.edu`

MATHEMATICS DEPARTMENT, COLGATE UNIVERSITY, HAMILTON, NY 13346-1398
*E-mail address*: `dlantz@mail.colgate.edu`