ROOTS OF GENERALIZED SCHÖNEMANN POLYNOMIALS IN HENSELIAN EXTENSION FIELDS

Ron Brown

Abstract. We study generalized Schönemann polynomials over a valued field F. If such a polynomial f is tame (i.e., a root of f generates a tamely ramified extension of F), we give a best-possible criterion for when the existence in a Henselian extension field K of an approximate root of f guarantees the existence of an exact root of f in the extension field K.

Let (F, v) be a valued field with residue class field $\overline{F}$, value group vF, and valuation ring A. For any $a \in A$ and polynomial $h \in A[x]$ we let $\overline{a}$ and $\overline{h}$ denote the canonical image of a and h in $\overline{F}$ and $\overline{F}[x]$, respectively. Using notation as in [5, pp. 82–83], we call a polynomial $k \in A[x]$ a *generalized Schönemann polynomial* over (F, v) if it can be written in the form

$$k = p^e + th$$

where $e \geq 1$; $p \in A[x]$ is monic with $\overline{p}$ irreducible over $\overline{F}$; $h \in A[x]$ has degree less than $e \deg p$; $\overline{p}$ does not divide $\overline{h}$; and, finally, $t \in A$ and $v(t) \notin svF$ for any divisor $s > 1$ of e.

If vF is discrete rank one, then the above condition on t is satisfied when $v(t)$ is positive and generates vF; thus the Schönemann polynomials of [5, pp. 82–83] are indeed generalized Schönemann polynomials in the above sense. We allow the case $p = x$, in which case we obtain generalized Eisenstein polynomials. We use the above notation in the statement of our first theorem.

Theorem 1. *Suppose $k = p^e + th$ is a generalized Schönemann polynomial over (F, v) with $\overline{p}$ separable over $\overline{F}$ and e not divisible by the characteristic of $\overline{F}$. If a Henselian extension (K, u) of (F, v) has an element α with $u(k(\alpha)) > v(t)$, then k has a root in K.*

In Remark 6B below we will see that when $e \neq 1$, the value $v(t)$ is best possible in Theorem 1.

Remarks 2. (A) The hypotheses of the first sentence of Theorem 1 guarantee that an extension of F by a root of k is tamely ramified (cf. the proof of Lemma 4). One would like a generalization of Theorem 1 allowing wild ramification. The Eisenstein polynomial $x^2 - 2$ over the valued field of 2–adic numbers $(\mathbb{Q}_2, v_2)$ has no root in $\mathbb{Q}_2\big[\sqrt{-6}\,\big]$ even though $v_2\big((\sqrt{-6})^2 - 2\big) > v_2(2)$. Thus *as stated* Theorem 1 is not valid without the hypotheses of its first sentence.

(B) We will see below in the proof of Theorem 5 that the hypotheses of Theorem 1 imply that $v(k'(\alpha)) = \big(1 - \frac{1}{e}\big)v(t)$. Thus if $e \leq 2$, then we have $v(k(\alpha)) > 2v(k'(\alpha))$, and hence the existence of a root of k in K follows from a standard version of Hensel's Lemma [2, Theorem 4.1.3(5), p. 88]. When $e > 2$ the application of Theorem 1 gives a stronger result than the application of this version of Hensel's Lemma. Similar remarks hold for versions of Hensel's Lemma involving the discriminant of f. For example the Eisenstein polynomial $x^3 - 2$ over $(\mathbb{Q}_2, v_2)$ has discriminant -108; applying the Hensel-Rychlik Theorem of [4, Theorem 10.8, p. 263] to it gives a weaker result than applying Theorem 1 since $v_2(-108) = v_2(4) > v_2(-2)$.

We will prove a modest generalization of Theorem 1 with an eye toward a more sweeping generalization (cf. Remark 8). We extend v to $F[x]$ with the Gaussian valuation, so

$$v\left(\sum a_i x^i\right) = \min_i v(a_i) \quad \text{for all } a_i \in F\,.$$

Notation 3. For the remainder of this paper $k \in F[x]$ will be assumed to have the form $k = p^e + \sum_{i<e} A_i p^i$ where $e \geq 1$ and

(a) $p \in A[x]$ is monic with $\overline{p}$ irreducible over $\overline{F}$;

(b) for all $i < e$, $A_i \in A[x]$, $\deg A_i < \deg p$, and $A_0 \neq 0$;

(c) $v(A_0) \notin svF$ for any divisor $s > 1$ of e;

(d) $ev(A_i) \geq (e-i)v(A_0) > 0$ whenever $i < e$.

We also set $f = \deg p$. Condition (c) above says that in the divisible hull of vF we have $(vF + \mathbb{Z}\frac{1}{e}v(A_0) : vF) = e$ and that when $i \neq 0$, the inequalities of (d) are strict.

Any generalized Schönemann polynomial $k = p^e + th$ is easily seen to satisfy the conditions in Notation 3 above. (Since p is monic, there exist $B_i \in A[x]$ of degree less than deg p with $h = \sum_{i<e} B_i p^i$; the fact that $\overline{p} \nmid \overline{h}$ tells us that $v(tB_0) = v(t)$.) Polynomials satisfying the conditions of Notation 3 with $\overline{p}$ separable over $\overline{F}$ are also considered by Khanduja and Saha; in the next lemma we expand on their Theorem 1.1 [3, p. 38].

Lemma 4. *(A) The polynomial k is irreducible over F, and if α is a root of k in some algebraic extension of F, then v has a unique extension, say v', to $F[\alpha]$ and the ramification degree and ramification index of v'/v are f and e, respectively.*

(B) If α is an element of some valued field extension (K, u) of (F, v) with $u(k(\alpha)) > v(A_0)$, then $u(\alpha) \geq 0$, $\overline{p}(\overline{\alpha}) = 0$, $u(p(\alpha)^e) = v(A_0) = u(A_0(\alpha)) = u(\sum_{i<e} A_i(\alpha)p(\alpha)^i)$, and $\overline{p(\alpha)^e / \sum_{i<e} A_i(\alpha)p(\alpha)^i} = -1$.

Proof. We begin by proving (B). Pick any $b \in F$ with $v(b) = v(A_0)$. Since valuation rings are integrally closed, we have $u(\alpha) \geq 0$ (note that α is a root of $k - k(\alpha)$). Since all the coefficients of the polynomials A_i are in the maximal ideal of v, we have $u(p(\alpha)^e) > 0$, so $\overline{p}(\overline{\alpha}) = 0$. Because $v(b) = v(A_0) \neq \infty$, thus $\overline{b^{-1}A_0}$ is a nonzero polynomial of degree less than that of $\overline{p}$, the irreducible polynomial of $\overline{\alpha}$ over $\overline{F}$. Thus $b^{-1}A_0(\alpha)$ is a unit, so $v(A_0) = v(b) = u(A_0(\alpha))$. If $u(p(\alpha)^e) > v(A_0)$, then whenever $0 < i < e$ we have $u(A_i(\alpha)) \geq v(A_i)$ and hence

$$u(A_i(\alpha)p(\alpha)^i) > \frac{e-i}{e}u(A_0(\alpha)) + \frac{i}{e}v(A_0) = u(A_0(\alpha))\,,$$

so $u(k(\alpha)) = v(A_0)$, a contradiction. On the other hand, if $u(p(\alpha)^e) < v(A_0)$, then for all $i < e$ we have

$$\begin{aligned} u(A_i(\alpha)p(\alpha)^i) &\geq \frac{e-i}{e}v(A_0) + iu(p(\alpha)) \\ &> (e-i)u(p(\alpha)) + iu(p(\alpha)) = u(p(\alpha)^e)\,, \end{aligned}$$

so $u(k(\alpha)) = u(p(\alpha)^e) < v(A_0)$, another contradiction. Thus $u(p(\alpha)^e) = v(A_0)$. The last assertions of (B) follow easily since $u(p(\alpha)^e b^{-1}) = 0$ and by hypothesis

$$u\Big((p(\alpha)^e + \sum A_i(\alpha)p(\alpha)^i)b^{-1}\Big) = u(k(\alpha)) - v(A_0) > 0\,.$$

We now apply the results of (B) to prove (A). Let v' denote any extension of v to $F[\alpha]$. We denote by $f_{v'/v}$ and $e_{v'/v}$ the ramification degree and index of v'/v, respectively. Part B applied with $u = v'$ tells us that $\overline{p}(\overline{\alpha}) = 0$, so $f_{v'/v} \geq f$. That $(vF + \mathbb{Z}\frac{1}{e}v(A_0) : vF) = e$ shows that $e_{v'/v} \geq e$. But $ef = \deg k \geq [F[\alpha] : F] \geq e_{v'/v}f_{v'/v} \geq ef$ so that $e = e_{v'/v}$

and $f = f_{v'/v}$ and $\deg k = [F[\alpha] : F]$. Thus k is irreducible over F and v has a unique extension to $F[\alpha]$. $\square$

Theorem 1 will be a corollary of:

Theorem 5. *Suppose that $\overline{p}$ is separable over $\overline{F}$ and that e is not divisible by the characteristic of $\overline{F}$. Further suppose that there is an integer $d > 0$ with*

$$edv(A_i) > (e-i)(d+1)v(A_0) > 0 \tag{1}$$

whenever $0 < i < e$. If $u(k(\alpha)) > v(A_0)$ for some element α of a Henselian extension (K, u) of (F, v), then k has a root in K.

Remarks 6. (A) Working in the divisible hull of vF we can rewrite condition (1) in the form

$$\frac{1}{e-i}v(A_i) > \left(1 + \frac{1}{d}\right)\left(\frac{1}{e}\right)v(A_0) > 0\,.$$

The existence of such an integer d is automatic when vF is rank one (as we observed earlier, the inequalities of Notation 3(d) are strict when $i > 0$). The existence is also clear if k is a generalized Schönemann polynomial (just set $d = e$), so that Theorem 1 is indeed a corollary of Theorem 5.

(B) We now show that if $e \neq 1$, then the value $v(A_0)$ in Theorem 5 is best possible, so that in particular the value $v(t)$ in Theorem 1 is best possible. Let α be a root of p in an algebraic extension (K, u) of a Henselization (F', v') of (F, v). Since (F', v') is an immediate extension of (F, v), the conditions of Notation 3 hold with (F, v) replaced by (F', v'), so k is irreducible over F' by Lemma 4. We have $u(\alpha) \geq 0$ since $p \in A[x]$, and hence $u(k(\alpha)) = u(A_0(\alpha)) \geq v(A_0)$. However the Henselian extension $F'[\alpha]$ of F cannot have a root of k since k has degree ef, but α generates an extension of F' of degree only f.

Proof of Theorem 5. We will use Lemma 4B repeatedly, and usually only implicitly. Observe that $p'(\alpha)$ is a unit since $\overline{p}$ is irreducible and separable over $\overline{F}$ with root $\overline{\alpha}$. We now show that $u(k'(\alpha)) = \big(1 - \frac{1}{e}\big)v(A_0)$. We may write

$$k'(\alpha) = ep(\alpha)^{e-1}p'(\alpha) + \sum_{i<e}(A_i(\alpha)ip(\alpha)^{i-1}p'(\alpha) + A_i'(\alpha)p(\alpha)^i)\,. \tag{2}$$

Since $\operatorname{char}\overline{F} \nmid e$ and $p'(\alpha)$ is a unit, we have $u\big(ep^{e-1}(\alpha)p'(\alpha)\big) = \big(1 - \frac{1}{e}\big)v(A_0)$. It suffices to show that the other terms of (2) have larger values. If $0 < i < e$ we have

$$\begin{aligned} u(A_i(\alpha)ip(\alpha)^{i-1}p'(\alpha)) &\geq v(A_i) + (i-1)\frac{1}{e}v(A_0) \\ &> (\frac{e-i}{e})v(A_0) + (\frac{i-1}{e})v(A_0) = \big(1 - \frac{1}{e}\big)v(A_0)\,, \end{aligned}$$

and since the coefficients of A_i' are integer multiples of those of A_i, we have

$$u(A_i'(\alpha)p^i(\alpha)) \geq v(A_i) + iu(p(\alpha)) \geq v(A_0) > \big(1 - \frac{1}{e}\big)v(A_0).$$

Finally, $u(A_0'(\alpha)) \geq v(A_0) > \big(1 - \frac{1}{e}\big)v(A_0)$. Thus indeed $u(k'(\alpha)) = \big(1 - \frac{1}{e}\big)v(A_0)$.

Let us write $r = -\sum_{i<e} A_i p^i$, so $k = p^e - r$. By the Lemma $p(\alpha) \neq 0$ and $\overline{r(\alpha)/p(\alpha)^e} = 1$. Since $\operatorname{char}\overline{F} \nmid e$, we may apply Hensel's Lemma to $X^e - r(\alpha)/p(\alpha)^e$ to show the existence of $\eta \in K$ with $\overline{\eta} = 1$ and $\eta^e = r(\alpha)/p(\alpha)^e$, i.e., $r(\alpha) = (\eta p(\alpha))^e$. Applying Hensel's Lemma to $p - \eta p(\alpha)$ we deduce the existence of $\delta \in K$ with $\overline{\delta} = \overline{\alpha}$ and $p(\delta) = \eta p(\alpha)$ (recall that $u(p(\alpha)) > 0$). Then $p(\delta)^e - r(\alpha) = 0$. We may assume without loss of generality that

$p(\alpha) \neq p(\delta)$ (and hence that $\alpha \neq \delta$) since otherwise

$$k(\alpha) = p(\alpha)^e - r(\alpha) = p(\delta)^e - r(\alpha) = 0\,,$$

proving the theorem in this case.

We claim that $u(p(\alpha) - p(\delta)) = u(\alpha - \delta)$. If α is not a unit, then p is monic and linear (since $\overline{p}(\overline{\alpha}) = 0$), and hence $p(\alpha) - p(\delta) = \alpha - \delta$. Suppose that α is a unit. Write $p = \sum b_i x^i$, and set

$$\xi = \sum b_i \alpha^{i-1} \left(1 + \left(\frac{\delta}{\alpha}\right) + \cdots + \left(\frac{\delta}{\alpha}\right)^{i-1}\right).$$

Since $\overline{\delta/\alpha} = 1$, the separability of $\overline{p}$ implies that $\overline{\xi} = \overline{p}\,'(\overline{\alpha}) \neq 0$. But $p(\alpha) - p(\delta) = (\alpha - \delta)\xi$, so that in this case we also have $u(p(\alpha) - p(\delta)) = u(\alpha - \delta)$.

Now note that

$$\begin{aligned} k(\alpha) &= p(\alpha)^e - p(\delta)^e + p(\delta)^e - r(\alpha) \\ &= p(\alpha)^e - p(\delta)^e = p(\alpha)^e(1 - \eta^e) \\ &= p(\alpha)^{e-1}(p(\alpha) - p(\delta))(1 + \eta + \cdots \eta^{e-1})\,. \end{aligned}$$

Since $\overline{\eta} = 1$ and the characteristic of $\overline{F}$ does not divide e, therefore $1 + \eta + \cdots + \eta^{e-1}$ is a unit and hence

$$u(k(\alpha)) = (e-1)u(p(\alpha)) + u(\alpha - \delta) = \left(1 - \frac{1}{e}\right) v(A_0) + u(\alpha - \delta)\,. \tag{3}$$

We next estimate $u(k(\delta))$. Note that

$$\begin{aligned} k(\delta) &= p^e(\delta) - r(\delta) + r(\alpha) - r(\alpha) \\ &= r(\alpha) - r(\delta) = \sum_{i<e} A_i(\delta)p(\delta)^i - A_i(\alpha)p(\alpha)^i\,. \end{aligned}$$

Each A_i is a sum of terms of the form cx^j where $0 \le j < f$, $c \in F$, and

$$v(c) \ge v(A_i) \ge \left(1 - \frac{i}{e}\right)\left(1 + \frac{1}{d}\right) v(A_0)\,,$$

so $k(\delta)$ is a sum of terms of the form

$$c\delta^j p(\delta)^i - c\alpha^j p(\alpha)^i = c\big(\delta^j (p(\delta)^i - p(\alpha)^i\big) + p(\alpha)^i\big(\delta^j - \alpha^j)\big)\,.$$

Arguing as above and using equation (3) we calculate that if $e > i > 0$, then

$$\begin{aligned} & u\big(c\delta^j (p(\delta)^i - p(\alpha)^i)\big) \\ & \qquad \ge v(c) + u\big(p(\alpha)^{i-1}(p(\alpha) - p(\delta))(1 + \eta + \cdots + \eta^{i-1})\big) \\ & \qquad \ge \left(\left(1 - \frac{i}{e}\right)\left(1 + \frac{1}{d}\right) + \frac{i-1}{e}\right) v(A_0) + u(\alpha - \delta) \\ & \qquad = u(k(\alpha)) + \left(\left(1 - \frac{i}{e}\right)\left(1 + \frac{1}{d}\right) + \frac{i-1}{e} - \left(1 - \frac{1}{e}\right)\right) v(A_0) \\ & \qquad = u(k(\alpha)) + \frac{e-i}{de} v(A_0) \ge u(k(\alpha)) + \frac{1}{de} v(A_0)\,, \end{aligned}$$

and similarly that if $j > 0$ then

$$\begin{aligned} & u\big(c(p(\alpha)^i(\delta^j - \alpha^j))\big) \\ & \qquad \ge \left(\left(1 - \frac{i}{e}\right)\left(1 + \frac{1}{d}\right)\right) v(A_0) + \frac{i}{e} v(A_0) + u(\alpha - \delta) \\ & \qquad \ge u(k(\alpha)) + \frac{1}{de} v(A_0)\,. \end{aligned}$$

Combining these inequalities we have

$$u(k(\delta)) \ge u(k(\alpha)) + \frac{1}{de} v(A_0)\,.$$

To summarize, we have shown that for any α in K with $u(k(\alpha)) > v(A_0)$ we have $u(k'(\alpha)) = \big(1 - \frac{1}{e}\big) v(A_0)$ and we can find an α' in K with $u(k(\alpha')) \ge u(k(\alpha)) + \frac{1}{de} v(A_0) >$

$v(A_0)$ (so that $u(k'(\alpha')) = \big(1 - \frac{1}{e}\big)v(A_0)$). Thus we can find α'' in K with $u(k(\alpha'')) \geq u(k(\alpha')) + \frac{1}{de}v(A_0) \geq u(k(\alpha)) + \frac{2}{de}v(A_0)$ and $u(k'(\alpha'')) = \big(1 - \frac{1}{e}\big)v(A_0)$. Continuing in this manner we can find an element $\alpha^* \in K$ with

$$u(k(\alpha^*)) > 2\left(1 - \frac{1}{e}\right)v(A_0) = 2u(k'(\alpha^*))\,,$$

so that by a standard version of Hensel's Lemma [2, Theorem 4.1.3(5), p. 88], k has a root in K. □

We record a corollary to Theorem 5. We continue the hypotheses of Notation 3.

Corollary 7. *Suppose that (F, v) is Henselian and that a finite degree tamely ramified extension (K, u) of (F, v) has an element α satisfying $u(k(\alpha)) > v(A_0)$. Then k has a zero in K.*

Proof. The "tame" hypothesis means that $[K : F] = \big[\overline{K} : \overline{F}\big](vK : vF)$, that $\overline{K}/\overline{F}$ is separable, and that the characteristic of $\overline{F}$ does not divide $(uK : vF)$. Then by Lemma 4, $\overline{p}$ must be separable over $\overline{F}$ and the characteristic of $\overline{F}$ cannot divide e (a divisor of $(uK : vF)$). Theorem 5 then implies our result. □

Remark 8. We plan to generalize the above Corollary (but not Theorem 5 itself) to a class of irreducible polynomials over F which when (F, v) is a maximal field is precisely the class of monic irreducible polynomials. In this generalization the role of the values $v(A_0)$ would be essentially played by the invariants "γ_f" of [1, p. 466].

Acknowledgements. Part of the work on this paper was done while the author was visiting the University of Saskatchewan. I acknowledge with pleasure the stimulating atmosphere of the University's Algebra and Logic Group, and the generosity with which Professor Franz-Viktor Kuhlmann shared his knowledge of the literature of valuation theory.

References

[1] R. Brown, Valuations, primes and irreducibility in polynomial rings and rational function fields, *Trans. Amer. Math. Soc.,* **174** (1972), 451–488.
[2] A. J. Engler and A. Prestel, *Valued Fields*, Springer–Verlag, Berlin (2005).
[3] F.-V. Kuhlmann, *Valuation Theory*, 2007 draft available at http://math.usask.ca/∼fvk/Fvkbook.htm.
[4] S. Khanduja and J. Saha, On a generalization of Eisenstein's irreducibility criterion, *Mathematika,* **44** (1997), 37–41.
[5] P. Ribenboim, *The Theory of Classical Valuations*, Springer–Verlag, New York (1999).

Keywords: Henselian fields, Schönemann polynomials, irreducible polynomials, roots

MSC (2000): Primary 12J10; Secondary 12E05.

Department of Mathematics, 2565 McCarthy Mall, University of Hawaii, Honolulu, HI 96822, USA
E-mail address: ron@math.hawaii.edu