Math. J. Okayama Univ. 38(1996), 47–51

WEAKLY HENSELIAN RINGS

THOMAS MCKENZIE

1. Introduction.

Throughout this paper we will assume that all rings are commutative rings with identity, that ring homomorphisms preserve identities, and that a ring and its subrings have the same identity. We say that a ring is connected if it has exactly two idempotents. By a local ring we mean a (not necessarily Noetherian) ring with a unique maximal ideal. For the remainder of this paper we assume that R is a local ring with maximal ideal M.

In this paper we give a definition of a weakly Henselian ring. The main result of this paper is Theorem 1.5. In this theorem we give a characterization of weakly Henselian rings. A version of this Theorem appears as Theorem 4.15 on page 176 of [5]. But in [5] the author assumes that the residue class field of R is infinite. In this paper we have no such restriction.

2. Weakly Henselian Rings.

If S is a connected ring and $f \in S[x]$ then f is said to be a separable polynomial if f is monic and there exist $u, v \in S[x]$ such that $uf + vf' = 1$ where f' is the formal derivative of f.

Definition 1.1. We say that R is a weakly Henselian ring if whenever $f \in R[x]$ is a separable polynomial and there exist monic polynomials $g_0, h_0 \in (R/M)[x]$ with $\overline{f} = g_0 h_0$ then there exist monic polynomials $g, h \in R[x]$ such that $f = gh, \overline{g} = g_0$, and $\overline{h} = h_0$

Note that since f is separable the polynomials g, h, g_0, and h_0 in Definition 1.1 are also separable by Lemma 1.2 on page 22 of [2]. By the same lemma there exist $u, v \in R[x]$ and $u_0, v_0 \in (R/M)[x]$ such that $ug + vh = 1$ and $u_0 g_0 + v_0 h_0 = 1$.

If S is a ring and $f \in S[x]$ we write $deg(f)$ for the degree of f. If f is a monic polynomial then we say that f is indecomposable if whenever there exist monic polynomials $g, h \in S[x]$ such that $f = gh$ it follows that

$g = 1$ or $h = 1$. If T is a finite projective separable extension of S and P is a maximal ideal of T then $Q = P \cap S$ is a maximal ideal of S since T is an integral extension of S. We call the degree of the field T/P over S/Q the inertial degree of P over Q.

The next lemma is Theorem 3.5 on page 172 of [5]. We include it for the convenience of the reader.

Lemma 1.2. *If S is a connected ring , f is an indecomposable separable polynomial in $S[x]$, Q is a maximal ideal of S, and $f_1, \ldots, f_n$ are monic polynomials in $S[x]$ such that $\overline{f} = \overline{f}_1 \cdot \ldots \cdot \overline{f}_n$ is the unique factorization of $\overline{f}$ in S/Q, and $T = S[x]/(f)$ then:*

(i) *The maximal ideals in T which lie over Q are precisely the ideals of the form $P_i = Q \cdot T + (f_i + (f)) \cdot T$;*

(ii) *The inertial degree of P_i over Q equals the $deg(f_i)$.*

If $F \subseteq L$ is an extension of fields we let $deg(L : F)$ denote the degree of L over F. In order to prove the main result in this section we need the following technical lemma regarding the existence of irreducible polynomials over finite fields.

Lemma 1.3. *Let F be a finite field with q elements, $F \subseteq L$ be an extension of finite fields, and M be a positive integer. There exists a monic polynomial $g \in F[x]$ such that:*

(i) *g is irreducible in $L[x]$;*

(ii) *there exist at least M distinct monic irreducible polynomials in $F[x]$ of degree $deg(g) \cdot deg(L : F)$.*

Proof : Let n be a positive integer, and let $N_q(n)$ denote the number of irreducible polynomials in $F[x]$ of degree n. By Example 3.26 on page 86 of [4]

$$N_q(i) \geq (1/i)(q^i - q^{i-1} - q^{i-2} - \ldots - q).$$

Thus

$$\lim_{i \to \infty} N_q(i) = \infty.$$

So we may choose a positive integer M_0 such that whenever $i > M_0$ it follows that $N_q(i) > M$.

Let j be positive integer such that $j > M_0$ and j is relatively prime to $deg(L : F)$. Since $j > M_0$ there exists a monic irreducible polynomial g in

$F[x]$ of degree j. By Corollary 3.47 on page 100 of [4], the fact that j and $deg(L : F)$ are relatively prime implies g is irreducible over L. Also, since $j \cdot deg(L : F) > M_0$ it follows that $N_q(j \cdot deg(L : F)) > M$. This completes the proof.

If S is a connected ring we let Ω_S denote the separable closure of R. If T is a ring extension of R we say that T has a primitive element over S if there exists $\alpha \in T$ such that $T = R[\alpha]$

Lemma 1.4. *Assume that R/M is a finite field and Ω_R is not a local ring. Then there exists a separable indecomposable polynomial $f \in R[x]$ such that $\overline{f}$ is not irreducible in $(R/M)[x]$.*

Proof : Since Ω_R is not local there exists a finite projective connected Galois extension S of R such that S is not a local ring. Let $Q_1, \ldots, Q_n$ be the distinct maximal ideals of S. By Lemma 1.3 there exists a monic irreducible polynomial $g_0 \in (R/M)[x]$ such that:

(i) g_0 is irreducible in S/Q_1;

(ii) There exist at least n distinct irreducible polynomials in $(R/M)[x]$ of degree $deg(g_0) \cdot deg(S/Q_1 : R/M)$.

Let $g \in R[x]$ be monic such that $\overline{g} = g_0$ in $(R/M)[x]$. Note that g is separable in R[x] since $\overline{g}$ is separable in $(R/M)[x]$. Also, g is indecomposable in $S[x]$ since g is irreducible in $(S/Q_1)[x]$. Thus $T = S[x]/(g)$ is a finite projective separable connected extension of S.

Since S is Galois over R, Lemma 2.2 on page 167 of [5] implies that

$$deg(S/Q_1 : R/M) = deg(S/Q_j : R/M), \forall j \in \{1, \ldots, n\}.$$

So by Corollary 3.47 on page 100 of [4], $\overline{g}$ is irreducible in $(S/Q_j)[x]$ for all $j \in \{1, \ldots, n\}$. Thus by Lemma 1.2, T has exactly one maximal ideal P_j which lies over Q_j for all $j \in \{1, \ldots, n\}$. Further the inertial degree of P_j over Q_j equals $deg(g)$ for all $j \in \{1, \ldots, n\}$. Hence

$$T/(MT) \simeq T/P_1 \times \ldots \times T/P_n,$$

the inertial degree of Q_j over M equals $deg(g_0) \cdot deg(S/Q_1 : R/M)$ for all $j \in \{1, \ldots, n\}$, and there are at least n irreducible polynomials of degree $deg(g_0) \cdot deg(S/Q_1 : R/M)$ in $(R/M)[x]$. Let $h_1, \ldots, h_n$ be n distinct polynomials in $(R/M)[x]$ each of degree equal to the inertial degree of Q_1 over

M. Then

$$T/P_1 \times \ldots \times T/P_n \simeq (R/M)[x]/(h_1) \times \ldots \times (R/M)[x]/(h_n).$$

Also,

$$(R/M)[x]/(h_1) \times \ldots \times (R/M)[x]/(h_n) \simeq (R/M)[x]/(h_1 \cdot \ldots \cdot h_n)$$

since $h_1 \ldots h_n$ are pairwise relatively prime. A standard argument now shows that $T/(M \cdot T)$ has a primitive element over R. Using this fact and an application of Nakayama's Lemma one can show that T has a primitive element over R. So by Theorem 3.3 page 171 of [5] there exists an indecomposable separable polynomial $h \in R[x]$ such that $T \simeq R[x]/(h)$ and by Lemma 1.2 h is not irreducible in $(R/M)[x]$. This completes the proof.

We can now prove the main result in this paper.

Theorem 1.5. *R is weakly Henselian if and only if Ω_R is a local ring.*

Proof : If R/M is an infinite field then the theorem follows from Theorem 4.15 on page 176 of [5]. Thus we assume that R/M is finite. If Ω_R is not local then by Lemma 1.4 R is not weakly Henselian. If R is not weakly Henselian then by Lemma 1.2 there exists a finite projective separable extension of R which is not local. Thus Ω_R is not local. This completes the proof.

Corollary 1.6. Henselian local rings have local separable closures.

Proof : This is clear.

REFERENCES

[1] F. DEMEYER and E. INGRAHM, *Separable algebras over commutative rings*, Lecture Notes in Math. vol. 181, Springer-Verlag, New York, 1971.

[2] D. K. HARRISON and T. MCKENZIE, *Toward an arithmetic of polynomials*, Aequationes Math. **43**(1992), 21–37.

[3] G. JANUSZ, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122**(1966), 461–479.

[4] R. LIDL and H. NIEDERREITER, *Introduction to Finite Fields and their applications*,

revised edition, Cambridge University Press, Cambridge, 1994.

[5] T. McKenzie, *Separable Polynomials and Weak Henselizations,* Rings, extensions, and cohomology (Evenston, IL, 1993), 165-179, Lecture Notes in Pure and Appl. Math., 159, Marcel Dekker, New York, 1994.

T. McKenzie
Department of Mathematics
Bradley University
Peoria, Illinois

(Received August 26, 1996)