AN ABSTRACT OF THE THESIS OF

MARY JEANNE PE NG for the degree of DOCTOR OF PHILOSOPHY

in MATHEMATICS presented on August 10, 1976

Title: THE $Z_p(t)$-ADEQUACY OF PURE POLYNOMIALS

Signature redacted for privacy.

Abstract approved: _____
Burton I. Fein

Let k be a field and $f(x)$ a polynomial in $k[x]$. $f(x)$ is said to be k-adequate if there exists a division ring D, finite dimensional over k and with center k, and $A \in D$ such that $f(A) = 0$.

In this dissertation we investigate the notion of k-adequacy under the assumption that k is $Z_p(t)$ and $f(x)$ is a pure polynomial, $x^m - a$. Necessary and sufficient conditions on m and a are given. Our results depend upon the classification of k-division rings by Hasse invariants.

The $Z_p(t)$-Adequacy of Pure Polynomials

by

Mary Jeanne Pe Ng

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Completed August 1976

Commencement June 1977

APPROVED:

Signature redacted for privacy.

Associate Professor of Mathematics

in charge of major

Signature redacted for privacy.

Chairman of Department of Mathematics

Signature redacted for privacy.

Dean of Graduate School

Date thesis is presented August 10, 1976

Typed by Clover Redfern for Mary Jeanne Pe Ng

ACKNOWLEDGMENT

I would like to thank my major professor, Dr. Burton I. Fein, for his constant encouragement, patience and consideration. Many thanks also go to my family, Fr. Bienvenido F. Nebres, S.J. and Martin J. Stynes without whose inspiration and enthusiasm this thesis would never have been written. Finally, I am grateful to many friends for making my stay in Corvallis a happy one.

TABLE OF CONTENTS

THE $Z_p(t)$-ADEQUACY OF PURE POLYNOMIALS

I. INTRODUCTION

At the Brighton Class Field Theory Conference held in September, 1965 at the University of Sussex, Brighton, J.P. Serre observed that if k is a local field and $f(x)$ is an irreducible polynomial of degree n in $k[x]$, then there exists a division ring D, finite dimensional over k and with center k, such that $f(x)$ has a root in D. M. Schacher considered the same question for k a global field, i.e., an algebraic number field or a function field in one variable over a finite field, and showed that an analogous result is not true. In his thesis, Schacher also attempted to determine the k-adequacy of polynomials in terms of their Galois groups. The results, however, did not yield any sort of classification and indeed, it proved to be easy to give examples of two polynomials having the same Galois group, one of which is k-adequate, the other not [12].

In [5] and [6], Fein and Schacher considered the question of the k-adequacy of pure polynomials x^m-a where k is a number field. In this thesis, we completely classify the k-adequacy of pure polynomials for $k = Z_p(t)$.

A division ring D which is finite dimensional over its center k will be called a <u>k-division ring</u>. By Weddeburn's theorem,

$[D:k] = n^2$. n is called the index of D. If k is a global field, then the exponent of D, i.e., the order of D as an element in the Brauer group $B(k)$ of k, is equal to n.

Let k be a field and $f(x)$ an irreducible polynomial of degree n in $k[x]$. Let α be any root of $f(x)$. Schacher defined $f(x)$ to be k-adequate if there is a k-division ring D containing $k(\alpha)$ as a maximal subfield. In [12], he proved that $f(x)$ is k-adequate $<=>$ there is a k-division ring of index n in which f has a root. We shall take the latter as the definition of k-adequacy in this dissertation.

II. BACKGROUND MATERIAL

1. Valuations, Completions

Definition. A valuation of a field k is a map $|\ |$ from k to the positive reals satisfying

(i) $|x| = 0 \iff x = 0$

(ii) $|xy| = |x||y|$

(iii) $|x+y| \leq |x| + |y|$ where $x, y \in k$.

If $|x+y| \leq \max\{|x|, |y|\}$, then $|\ |$ is said to be non-archimedean.

The value group $V(k)$ of $|\ |$ is the multiplicative group $\{|x| \mid x \in k,\ x \neq 0\}$. $|\ |$ is discrete if the value group of $|\ |$ is infinite cyclic. Necessarily, $|\ |$ is non-archimedean.

Henceforth, we shall deal with discrete valuations.

Let $\mathcal{O} = \{x \in k \mid |x| \leq 1\}$, $\mathcal{P} = \{x \in k \mid |x| < 1\}$. Then $\mathcal{O}$ is a discrete valuation ring (i.e., a principal ideal domain with exactly one maximal ideal) with $\mathcal{P}$ as its maximal ideal and k its quotient field.

Definition. Two valuations $|\ |, |\ |'$ are equivalent if for all $x \in k$, $|x| \leq 1$ if and only if $|x|' \leq 1$.

A prime in k will denote either an equivalence class of valuations of k or a prime ideal in the valuation ring of k.

Each valuation $|\ |$ on k defines a topology on k by taking the sets $\{x \in k \mid |x-a| < \epsilon\}$ as the basis for the neighborhoods of $a \in k$. Equivalent valuations define the same topology on k. Let K denote the completion of k relative to this topology. Then K is a field consisting of equivalence classes of Cauchy sequences of elements of k, with two sequences being equivalent if their difference forms a null sequence. K contains an isomorphic copy of k and the valuation $|\ |$ on k is extended to K by defining

$$|\{a_n\}^*|^K = \lim |a_n|$$

where $\{a_n\}$ is a Cauchy sequence in k. Note that K is complete relative to the topology induced by the valuation $|\ |^K$. The two valuations have the same value group and the same residue class field up to isomorphism.

More generally, let R be a discrete valuation ring with quotient field k and unique maximal ideal $(\eta) = R\eta$. Every non-zero element x in k can be expressed as $x = u\eta^n$ for some unit $u \in R$ and some integer n. Then

$$\nu_\eta(x) = \nu(x) = \begin{cases} n, & x \neq 0 \\ +\infty, & x = 0 \end{cases}$$

is an <u>exponential valuation</u> on k. If p is any prime number, then

$|x| = p^{-\nu(x)}$ defines a non-archimedean valuation on k, called the η-adic valuation on k. Let k_η be the η-adic completion of k and let S be a set of representatives of the cosets of (η) in R. Then every non-zero element a in k_η has a unique representation as a power series

$$a = \eta^q(s_0+s_1\eta+\dots)$$

with $s_0 \neq 0$ and $s_i \in S$.

Let η be a monic irreducible polynomial in $Z_p[t]$ and let R be the localization of $Z_p[t]$ at (η). Then R is a discrete valuation ring with quotient field k and maximal ideal $(\eta)R$. Thus, there is a prime in $k = Z_p(t)$ containing the valuation

$$|x|_\eta = p^{-\nu(x)}$$

where $\nu(x) = \nu(\eta(t)^n \frac{a(t)}{b(t)}) = n \deg \eta$ if $a(t)$, $b(t)$ are not divisible by $\eta(t)$. Now, if $a \in k_\eta$, then $a = \eta^q(s_0+s_1\eta+\dots)$ where $s_i \in R/(\eta)R \cong GF(p^{\deg \eta})$. Hence, k_η is isomorphic to the Laurent series field

$$GF(p^{\deg \eta})((t)) = \left\{ \sum_{i \geq i_0} d_i t^i \,\middle|\, d_i \in GF(p^{\deg \eta}) \right\}.$$

Consider the map from the valuation ring $\mathcal{O}_\eta$ in k_η

$$\mathcal{O}_\eta = \left\{ \sum_{i \geq 0} d_i t^i \,|\, d_i \in GF(p^{\deg \eta}) \right\},$$

to $GF(p^{\deg \eta})$ given by $\sum_{i \geq 0} d_i t^i \longmapsto d_0$. The kernel is the maximal ideal $\mathcal{P}_\eta = t \cdot \mathcal{O}_\eta$ and so the residue class field $\bar{k}_\eta = \mathcal{O}_\eta / \mathcal{P}_\eta \cong GF(p^{\deg \eta})$.

These primes are mutually inequivalent and every prime of k, except for one, is equivalent to one of these. The remaining prime, ∞, contains the valuation

$$|x|_\infty = \left| \frac{a(t)}{b(t)} \right|_\infty = p^{\deg a - \deg b}.$$

Observe that every element in k can be thought of as a rational function in $1/t$, namely,

$$\frac{a(t)}{b(t)} = \left(\frac{1}{t}\right)^{\deg b - \deg a} \frac{t^{-\deg a} a(t)}{t^{-\deg b} b(t)}$$

where $t^{-\deg a} a(t)$ and $t^{-\deg b} b(t)$ are not divisible by $1/t$. Let $t' = 1/t$, then $k = Z_p(t') = Z_p(t)$ and a t'-valuation is defined by

$$\left| \frac{a(t)}{b(t)} \right|_{t'} = p^{\deg a - \deg b}$$

We denote this by $|\ |_\infty$ and we now have all the inequivalent primes of k.

k_∞ is then the completion of $k = Z_p(t')$ with respect to the monic irreducible polynomial $f(t') = t'$. Thus, $k_\infty = (Z_p(t'))_{(t')}$ is isomorphic to the Laurent series field $GF(p^{\deg t'})((t')) = Z_p((t')) = Z_p((1/t))$.

Lemma 2.1. Let k be complete with respect to a non-archimedean valuation $|\ |_\eta$ and let L be a finite dimensional extension field of k. Then there is a unique extension of the valuation on k to L given by $|y| = \sqrt[n]{|N_{L/k}(y)|_\eta}$ for all $y \in L$ where $[L:k] = n$.

Proof. See [11, p. 71].

Lemma 2.2. (Hensel's Lemma) Let k be a field complete with respect to a non-archimedean valuation, $\mathcal{O}$ its ring of integers, $\mathcal{P}$ the unique maximal ideal of $\mathcal{O}$, $\bar{k} = \mathcal{O}/\mathcal{P}$ the residue class field of k. Let $f(x)$ be a polynomial in $\mathcal{O}[x]$, $f(x) \notin \mathcal{P}[x]$. Assume $\bar{f}(x) = G(x)H(x)$ in $\bar{k}[x]$. If $G(x)$ and $H(x)$ are relatively prime, then $f(x) = g(x)h(x)$ in $\mathcal{O}[x]$ where $\bar{g}(x) = G(x)$, $\bar{h}(x) = H(x)$ and $\deg g = \deg G$.

Proof. See [9, Proposition 3.5, p. 83].

2. Ramification Index, Residue Class Degree

Definition. A Dedekind ring R is a noetherian integral domain such that the localization $R_{\mathfrak{p}}$ is a discrete valuation ring for every non-zero prime ideal $\mathfrak{p}$ of R.

Let R, R' be two Dedekind rings with quotient fields F, E respectively. Assume E/F is finite-dimensional separable. Let $\mathfrak{p}$ be a non-zero prime ideal of R. Then

$$R'\mathfrak{p} = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$$

where the $\mathfrak{B}_i$'s are distinct prime ideals in R' and $\mathfrak{p} = R \cap \mathfrak{B}_i$.

The integer $e_i = e(\mathfrak{B}_i/R) = e(\mathfrak{B}_i/\mathfrak{p})$ is called the ramification index if $\mathfrak{B}_i$ over R and $f_i = f(\mathfrak{B}_i/R) = f(\mathfrak{B}_i/\mathfrak{p}) = [R'/\mathfrak{B}_i : R/\mathfrak{p}]$ is the residue class degree of $\mathfrak{B}_i$ over $\mathfrak{p}$. We say that $\mathfrak{B}_i$ is unramified in E/F if $e_i = 1$ and $R'/\mathfrak{B}_i$ is separable over $R/\mathfrak{p}$. Likewise, we say that $\mathfrak{p}$ is unramified from F to E if each $\mathfrak{B}_i$ is unramified in E/F. Under our assumption, we have $\sum e_i f_i = [E:F]$.

Let K be complete with respect to a discrete valuation $|\ |$. Let $\mathfrak{o}_K$ be its valuation ring and $\mathfrak{p}_K$ the maximal ideal of $\mathfrak{o}_K$, i.e., $\mathfrak{p}_K = \pi_K \mathfrak{o}_K$ where π_K is a prime in $\mathfrak{o}_K$. Let $\bar{K} = \mathfrak{o}_K/\mathfrak{p}_K$ be the residue class field. Let ν_K be the

exponential valuation on K defined by

$$xR = \begin{cases} (\mathfrak{P}_K)^{\nu_K(x)}, & x \neq 0 \\ +\infty, & x = 0 . \end{cases}$$

Let L/K be finite. Then ν_K extends to an exponential valuation ν_L for L. We define $e(L/K) = e = \nu_L(\pi_K)$ to be the ramification index and $f(L/K) = f = [\bar{L}:\bar{K}]$ the residue class degree.

Since $R'\mathfrak{P} = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$, then there are g inequivalent valuations $\varphi_1, \ldots, \varphi_g$ on E which extend the $\mathfrak{P}$-adic valuation $|\ |_{\mathfrak{P}}$ on F obtained by choosing φ_i to be the $\mathfrak{B}_i$-adic valuation on E. Let K be the $\mathfrak{P}$-adic completion of F and L_i the $\mathfrak{B}_i$-adic completion of E, we have

$$e_i = e(\mathfrak{B}_i/\mathfrak{P}) = e(L_i/K)$$

$$f_i = f(\mathfrak{B}_i/\mathfrak{P}) = f(L_i/K)$$

$$[L_i:K] = e_i f_i \qquad i = 1, 2, \ldots, g.$$

3. Hasse Invariants

Let $K = k_\eta$ be the completion of $k = Z_p(t)$ with respect to some prime η. We showed that $\bar{K}$, the residue class field, is a finite field.

If $|\bar{K}| = q$, then for every positive integer f, there exists a unique unramified extension L of K such that $[L:K] = [\bar{L}:\bar{K}] = f$, namely $L = K(\epsilon)$ where ϵ is a primitive $(q^f - 1)$st root of unity. Moreover, L/K is Galois and the Galois group $G(L/K)$ is cyclic, generated by the Frobenius automorphism of L/K $\sigma : \epsilon \longmapsto \epsilon^q$.

Any K-division ring D of index n contains a maximal subfield L which is unramified over K. Let π be the fundamental prime of K. If u is a unit in K and $r \in Z$, then $u\pi^{rn} \in K$ is a norm from L to K. Thus,

$$D \cong (L, \text{Frob}, u\pi^{rn}) \cong (K(\epsilon_{q^n-1}), \text{Frob}, \pi^r)$$

where $(r, n) = 1$. The Hasse invariant of D, inv D, is defined to be $r/n \in Q/Z$.

Let A be a finite dimensional central simple K-algebra, say $A = (D)_m$ with $D = (K(\epsilon_{q^n-1}), \text{Frob}, \pi^r)$, then the map

$$\text{inv}: B(K) \longrightarrow \frac{Q}{Z}$$

$$[A] \longmapsto \frac{r}{n} \pmod 1$$

is an additive isomorphism.

Now, let A be a finite dimensional central simple k-algebra. Let $A_\eta = k_\eta \otimes_k A = K \otimes_k A$ be the η-adic completion of A. Then A_η is a central simple k_η-algebra and so the map $[A] \longmapsto [A_\eta]$ yields a homomorphism between the Brauer groups $B(k)$, $B(K)$.

Definition. The Hasse invariant of A at η, $\mathrm{inv}_\eta A$ is defined to be the composition of the maps

$$B(k) \xrightarrow{k_\eta \otimes_k} B(K) = B(k_\eta) \xrightarrow{\mathrm{inv}} \frac{\mathbb{Q}}{\mathbb{Z}}$$

$$[A] \longmapsto [k_\eta \otimes_k A] = [A_\eta] \longmapsto \mathrm{inv}[A_\eta].$$

The following properties are listed in [3, Chapter VII].

(2.3) $A \sim k$ iff $\mathrm{inv}_\eta A = 0$ for all primes η.

(2.4) $\sum_\eta \mathrm{inv}_\eta A = 0 \pmod 1$.

(2.5) $A \sim B$ iff $\mathrm{inv}_\eta A = \mathrm{inv}_\eta B$ for all primes η.

(2.6) $\exp[A] = \text{l.c.m.}\{m_\eta\}$ where m_η, the local index of A at η, is the denominator of $\mathrm{inv}_\eta A$ as a fraction reduced to lowest terms.[1/]

[1/] If $\mathrm{inv}_\eta A = 0$, we set $m_\eta = 1$.

We have the following existence theorem.

Theorem 2.7. Let $\eta_1, \ldots, \eta_g$ be a given set of primes of k; $u_1, \ldots, u_g$ rational numbers in lowest terms such that $0 \leq u_i < 1$, $\sum_{i=1}^{g} u_i \equiv 0 \pmod 1$, then there exists a k-division ring D with $\operatorname{inv}_{\eta_i} A = u_i$, $i = 1, \ldots, g$ and $\operatorname{inv}_{\eta} A = 0$ for all other primes η of k.

Proof. See [3, Satz 9, p. 119].

4. Useful Results

In this section we list down results that will be constantly referred to in the next chapter.

Theorem 2.8. Let k be a field and n an integer ≥ 2. Let $a \in k$, $a \neq 0$. Assume that for all prime numbers p such that $p \mid n$, we have $a \notin k^p$ and if $4 \mid n$, then $a \notin -4k^4$. Then $x^n - a$ is irreducible in $K[x]$.

Proof. See [10, Theorem 16, p. 221].

Lemma 2.9. Let $f(x) = x^m + b = f_1(x) \ldots f_r(x)$ where $f_i(x)$ is an irreducible polynomial in $(Z_p[t])[x]$ of degree n_i. $f(x)$ is $Z_p(t)$-adequate iff there exists a j, $1 \leq j \leq r$, and two distinct

primes η_1, η_2 such that $f_j(x)$ is irreducible over both k_{η_1}, k_{η_2} where $k = Z_p(t)$. A sufficient condition for this to occur is for the Galois group G_j of $f_j(x)$ to contain a cycle of length n_j when G_j is viewed as a group of permutations on the n_j distinct roots of $f_j(x)$.

Proof. (<=) Replace $\mathbb{Q}$ by k, Z by $Z_p[t]$ and the Frobenius density theorem by the Tchebotarev Density Theorem [13, Theorem 12, p. 289] in the proof of Lemma 1 of [5].

(=>) follows from Lemma 1 of [6].

Lemma 2.10. Let $f_1(x)$, $f_2(x)$ be k-adequate irreducible polynomials in $k[x] = Z_p(t)[x]$ of degree n_1, n_2 respectively, $(n_1, n_2) = 1$. Let $f(x)$ be the monic irreducible polynomial for a primitive element of $k(\alpha_1, \alpha_2)$ where α_i is a root of $f_i(x)$, $i = 1, 2$. Then $f(x)$ is k-adequate. In particular, let $f(x) = x^{mr} + b$, $(m, r) = 1$, $f_1(x) = x^m + b$, $f_2(x) = x^r + b$ and suppose $f_1(x)$, $f_2(x)$ and $f(x)$ are irreducible. If $f_1(x)$ and $f_2(x)$ are k-adequate then so is $f(x)$.

Proof. See Lemma 4 of [5] and replace $\mathbb{Q}$ by k.

III. DETERMINATION OF $Z_p(t)$-ADEQUATE POLYNOMIALS

Throughout this chapter, k denotes the function field $Z_p(t)$; K denotes the polynomial ring $Z_p[t]$ and ϵ_j denotes a primitive jth root of unity. Every element a in K is expressed in the form $a = a_0 + a_1 t + \ldots + a_r t^r$ with $a_i \in \{0, 1, \ldots, p-1\}$. We shall characterize the k-adequate polynomials of the form x^m+a, $a \in k$.

It suffices to consider x^m+a, $a \in K$ because $x^m + u/v$ is k-adequate if and only if $x^m + v^{m-1}u$ is k-adequate, where $u, v \in K$, $uv \neq 0$ and $(u, v) = 1$. The proof of the latter can be found in [5, p. 92] by replacing $\mathbb{Q}$ by k and Z by K. Note that x^m-b can be written in the form x^m+a by a suitable change in the coefficients of b modulo p.

Lemma 3.1. If m is odd, then x^m+a is k-adequate.

Proof. Suppose x^m+a is reducible, then by Lemma 2.8, $-a = b^n$ where $m = n\ell$. Thus, $x^m+a = (x^\ell-b)(x^{(n-1)\ell}+\ldots+b^{n-1})$ and x^m+a is k-adequate if $x^\ell-b$ is. Reducing iteratively, we may then assume that x^m+a is irreducible over k. Let $m = q^s r$, $(q, r) = 1$. By Lemma 2.8, $x^{q^s}+a$, x^r+a are irreducible. In view of Lemma 2.10, we need only prove that $x^{q^s}+a$, x^r+a are k-adequate. Proceeding by induction on the number of primes dividing r, we see that to prove the k-adequacy of x^m+a, it suffices to prove that $x^{q^s}+a$ is k-adequate where q is an odd

prime and $x^{q^s}+a$ is irreducible over k.

By Lemma 2.9, we need to show that $x^{q^s}+a$ is irreducible over k_η for two distinct primes η of k. Suppose not, then $-a \in k_\eta^q$ for almost all primes η of k. It follows from [2, p. 82] that $-a \in k^q$. But then, $x^{q^s}+a$ would be reducible over k, a contradiction.

Lemma 3.2. If $k = Z_p(t)$, then $x^{p^s}+a$ is k-adequate.

Proof. If $x^{p^s}+a$ is not irreducible, then by Lemma 2.8, $-a = b^p$ for some $b \in k$. We have $x^{p^s}+a = x^{p^s}-b^p = (x^{p^{s-1}}-b)^p$. Reducing iteratively, we end up having to deal with $x^{p^s}+a$, an irreducible polynomial over k.

If p is an odd prime, then $x^{p^s}+a$ is k-adequate by Lemma 3.1. If $x^{2^s}+a$, $s \geq 1$, is not irreducible in $k_\eta[x]$ for at least two primes $\eta \in k$, then, in view of Lemma 2.8, $-a \in k_\eta^2$ or $a \in 4k_\eta^4 = k_\eta^2$. In $Z_2(t)$, $-1 = 1$; so $-a \in k_\eta^2$ if and only if $a \in (\sqrt{-1}\, k_\eta^2) = k_\eta^2$. Hence, $-a \in k_\eta^2$ for almost all primes η in k. By [2, p. 82], $-a \in k^2$ and so $x^{p^s}+a$ is reducible over k, a contradiction.

Lemma 3.3. If $a \in Z_p$, then $x^{2^s}+a$ is k-adequate.

Proof. The case $p = 2$ is handled in the preceding lemma.

Suppose $f(x) = x^{2^s} + a = g_1(x)g_2(x)\dots g_r(x)$ where $g_i(x)$ is an irreducible polynomial of degree n_i in $Z_p[x]$. Take $g(x) = g_1(x)$ and $n = n_1$. Let α be any root of $g(x)$, then $F = Z_p(\alpha) \cong Z_p[x]/(g(x))$ is a field with p^n elements.

Let $F^* = \langle\omega\rangle$, then $\omega^p, \omega^{p^2}, \dots, \omega^{p^n} = \omega$ are all different and so $\varphi^j: \omega \longmapsto \omega^{p^j}$, $j = 1, 2, \dots, n$ are distinct automorphisms. But $[F: Z_p] = n$. Hence, these must be all the elements of the Galois group $G(F/Z_p)$. Thus, $G(k(\alpha)/k) \cong G(F/Z_p)$ is cyclic of order n. By Lemma 2.9, $f(x)$ is k-adequate.

Henceforth, we assume that $a \in Z_p[t]$, $a \notin Z_p$.

Lemma 3.4. If $p \equiv 1 \pmod 4$, then $x^{2^s} + a$ is k-adequate.

Proof. Case 1. Suppose $f(x) = x^{2^s} + a$ is irreducible over k and suppose $f(x)$ is not irreducible in $k_\eta[x]$ for at least two primes η of k, then for almost all $\eta \in k$, $-a \in k_\eta^2$ or $a \in 4k_\eta^4 = k_\eta^2$.

By [14, p. 252], $p \equiv 1 \pmod 4$ implies that $\sqrt{-1} \in k$. Hence, $a \in -k_\eta^2$ if and only if $a \in (\sqrt{-1}\, k_\eta)^2 = k_\eta^2$. For almost all primes $\eta \in k$, we have $a \in -k_\eta^2$. By [2, p. 82], $a \in -k^2$, a contradiction.

$f(x)$ is k-adequate by Lemma 2.9.

Case 2. Suppose $f(x)$ is not irreducible over k, then either $-a = b^2$ or $a = 4c^4$.

(i) $f(x) = x^{2^s}+a = x^{2^s}-b^2 = (x^{2^{s-1}}+b)(x^{2^{s-1}}-b)$. This reduces iteratively to either the case $x^{2^s}+d$ irreducible over k which is k-adequate by Case 1, or the case $x^{2^s}+4d^4$.

(ii) $f(x) = x^{2^s}+a = x^{2^s}+4c^4$

$$= (x^{2^{s-2}}-(-c+\sqrt{-1}\,c))(x^{2^{s-2}}-(-c-\sqrt{-1}\,c)$$

$$\times (x^{2^{s-2}}-(c+\sqrt{-1}\,c)(x^{2^{s-2}}-(c-\sqrt{-1}\,c))$$

$p \equiv 1 \pmod 4 \Rightarrow \sqrt{-1} \in k \Rightarrow \pm c \pm\sqrt{-1}\, c \in k$. Hence, to determine the k-adequacy of $f(x)$, it suffices to consider $x^{2^{s-2}}+b$, $b \in k$. An iterative reduction leads to either the case $x^{2^s}+d$ irreducible over k or the case x^4+4d^4. But

$$x^4+4d^4 = (x-(-d+\sqrt{-1}\,d))(x-(-d-\sqrt{-1}\,d))(x-(d+\sqrt{-1}\,d))(x-(d-\sqrt{-1}\,d))$$

and this splits completely in $k[x]$, so $f(x)$ is k-adequate.

Lemma 3.5. If $p \equiv 3 \pmod 8$, then $x^{2^s}+4a^4$ is k-adequate.

Proof. $s = 1$: $f(x) = x^2+4a^4$ is k-adequate because the Galois group of $f(x)$ has a 2-cycle if $f(x)$ is irreducible over k.

$s = 2$: $f(x) = x^4+4a^4 = (x^2+2ax+2a^2)(x^2-2ax+2a^2)$.

Suppose there exists an $\alpha \in k$ such that $\alpha^4+4a^4 = 0$, then either $\alpha^2+2a\alpha+2a^2 = 0$ or $\alpha^2-2a\alpha+2a^2 = 0$. Thus, $\alpha = \pm a(1\pm\sqrt{-1})$; so $\sqrt{-1} \in k$ and $p \equiv 1 \pmod 4$, a contradiction. Hence,

$x^2+2ax+2a^2$, $x^2-2ax+2a^2$ are irreducible over k. By a similar argument as above, $f(x)$ is k-adequate.

$s \geq 3$: $f(x) = x^{2^s}+4a^4 = (x^{2^{s-1}}+2ax^{2^{s-2}}+2a^2)(x^{2^{2-1}}-2ax^{2^{s-2}}+2a^2)$.

Let the first factor be $f_1(x)$ and the second factor be $f_2(x)$. Let G be the Galois group of $f(x)$ over k. Then G is a permutation group on the roots of $f(x)$ and any element of G sends roots of an irreducible factor of $f(x)$ into roots of that same factor.

Let $\epsilon = \epsilon_{2^s}$ and let α be any root of $f_1(x)$. Then $L = k(\epsilon, \alpha)$ is the splitting field of $x^{2^s}+4a^4$ over k. Since $k = Z_p(t)$, then the Galois group of $k(\epsilon_8)/k$ is generated by the Frobenius automorphism sending ϵ_8 to ϵ_8^p. But $p \equiv 3 \pmod 8$. Thus, ϵ_8 maps into ϵ_8^3. Let σ be any extension to L of this Frobenius automorphism. Necessarily, $\sigma(\alpha) = \epsilon^r\alpha$. But $\alpha^{2^{s-1}} = \pm 2a^2\sqrt{-1}$ and $\sigma(\sqrt{-1}) = -\sqrt{-1}$. Now,

$$(\sigma(\alpha))^{2^{s-1}} = \epsilon^{2^{s-1}r}\alpha^{2^{s-1}} = \sigma(\alpha^{2^{s-1}}) = \sigma(\pm 2a^2\sqrt{-1}) = \mp 2a^2\sqrt{-1} = -\alpha^{2^{s-1}}.$$

Thus, $\epsilon^{2^{s-1}r} = -1$ and so r is odd. Observe that $\sigma^{2^{s-2}}(\alpha) = \epsilon^n\alpha$ where

$$n = r(1+3+3^2+\ldots+3^{2^{s-2}-1})$$

$$= r\left(\frac{3^{2^{s-1}}-1}{2}\right).$$

By induction it can easily be shown that $3^{2^{s-2}} \not\equiv 1 \pmod{2^{s+1}}$, so $\sigma^{2^{s-2}}(\alpha) \neq \alpha$. A similar argument shows that $\sigma^{2^{s-2}}(\epsilon^2\alpha) \neq \epsilon^2\alpha$ and that $\sigma^{2^{s-1}}$ is the identity automorphism of L. Thus σ has order 2^{s-1}. Since the order of σ is the least common multiple of the lengths of the cycles in the cycle structure of σ, we see that σ is the product of cycles at least one of which has length 2^{s-1}. α is in a cycle of length 2^{s-1}, so $f_1(x)$ is irreducible. Note that $\epsilon^2\alpha$ is a root of $f_2(x)$ and $\epsilon^2\alpha$ is in a cycle of length 2^{s-1} so $f_2(x)$ is also irreducible. In particular, σ is the product of two 2^{s-1}-cycles and so the Galois group of each $f_i(x)$, $i = 1, 2$, contains a 2^{s-1}-cycle. By Lemma 2.9, $f(x)$ is k-adequate.

Lemma 3.6. $x^{mr}+a$ k-adequate $\Rightarrow$ x^m+a k-adequate.

Proof. By assumption, there is a k-division ring D and an element $A \in D$ such that $A^{mr} = -a$. Now, $B = A^r \in D$ and $B^m = -a$. Hence, x^m+a is k-adequate.

Lemma 3.7. Let $k = Z_p(t)$, $p \equiv 7 \pmod 8$, then $\sqrt[2^r]{2} \in k$ for all r.

Proof. Let $F = Z_p$. By [14, p. 252], $p \equiv 7 \pmod 8$ $\Rightarrow$ $\sqrt{2} \in Z_p$ and for all $a \in F$, either $a \in F^2$ or $-a \in F^2$.

Thus $|F^{*2}|$ is odd. The map σ sending a to $a^{2^{r-1}}$ is clearly a homomorphism from F^{*2} onto F^{*2^r}. Suppose $\sigma(a) = 1$, then $a^{2^{r-1}} - 1 \equiv 0 \pmod{p}$, i.e.,

$$(a^{2^{r-2}}+1)(a^{2^{r-3}}+1)\ldots(a^2+1)(a+1)(a-1) \equiv 0 \pmod{p}.$$

Since $p \equiv 7 \pmod 8$, $a^{2^m}+1 \not\equiv 0 \pmod{p}$, $m \geq 1$. Thus either $a = 1$ or $a = p-1$. If $\ker \sigma = \{1, p-1\}$, then we get an even-order subgroup of an odd group, a contradiction.

$$\therefore \quad F^{*2} \cong F^{*2^r} \quad \text{and} \quad \sqrt[2^r]{2} \in F \subset k.$$

Lemma 3.8. If $p \equiv 3 \pmod 4$ and η is a prime of k with odd degree, then $[k_\eta(\sqrt{-1}): k_\eta] = 2$.

Proof. By Hensel's lemma, x^2+1 has a solution in k_η if x^2+1 has a solution in $\bar{k}_\eta = GF(p^{\deg \eta})$. Let $\deg \eta = r$. Observe that $\sqrt{-1}$ is a root of $g(x) = x^4-1$. Let E be the splitting field of x^4-1 over $F = GF(p^r)$.

Suppose $4 \mid p^r-1$, then $(\sqrt{-1})^{p^r-1} = 1$. Since $a \in F \iff a^{p^r-1} = 1$, then $\sqrt{-1} \in F$. Conversely, suppose $E = F$, then $(\sqrt{-1})^4 = 1$ and $(\sqrt{-1})^{p^r-1} = 1$, so $4 \mid p^r-1$.

Hence, $\sqrt{-1} \in F = GF(p^r)$ if and only if $p^r \equiv 1 \pmod 4$. But $p \equiv 3 \pmod 4$. Thus, if r is odd, then $p^r \not\equiv 1 \pmod 4$ and

so $\sqrt{-1} \notin F$ and $\sqrt{-1} \notin k_\eta$. $\therefore [k_\eta(\sqrt{-1}): k_\eta] = 2$.

Remarks. If $p \equiv 3 \pmod 4$ and $k = Z_p(t)$, then any polynomial in $k[x]$ of degree 2 is k-adequate. This follows immediately from Lemma 2.9 and the fact that the Galois group of $f(x)$ has a 2-cycle if $f(x)$ is k-adequate.

Consider $f(x) = x^4+4a^4 = (x^2+2ax+2a^2)(x^2-2ax+2a^2)$. $f(x)$ is then k-adequate. We have to check $x^{2^r}+4a^4$, $r \geq 3$.

Lemma 3.9. Let $b \in Z_p[t]$, $p \equiv 7 \pmod 8$, $b \notin k^{2^{s-2}}$; $b \in k^{2^{s-3}}$, $s \geq 3$. Then $x^{2^s}+4b^4$ is k-adequate if and only if $x^{2^r}+4b^4$ is k-adequate, $\forall\ r \geq s$.

Proof. (<=) follows from Lemma 3.6.

(=>) Let $b = c^{2^{s-3}}$, $c \notin k^2$. Suppose β is a root of $x^{2^s}+4b^4$, then $\beta^{2^s} = -4b^4 = -4c^{2^{s-1}}$ and so $\beta^2 = \epsilon_{2^s} dc$ where $d = \sqrt{2}^{2^{s-2}} \in k$. Hence $k(\beta) \supseteq k(\epsilon_{2^s}) \supseteq k$ and $k(\beta)/k$ is Galois.

$$\begin{array}{c} k(\beta) \\ | \quad 2 \\ k(\epsilon_{2^s}) \\ | \quad 2^m \\ k \end{array}$$

Suppose $[k(\epsilon_{2^s}):k] = 2^m$, $m \geq 2$. Let λ be any extension to $k(\beta)$ of the Frobenius automorphism sending ϵ_{2^s} to $\epsilon_{2^s}^p$. Necessarily,

$\lambda(\beta) = \epsilon_{2^s}^{u}\beta$. Write $\epsilon_{2^s} = \epsilon$.

Since

$$-\beta^{2^{s-1}} = \lambda(\beta^{2^{s-1}}) = (\lambda(\beta))^{2^{s-1}} = \epsilon^{u2^{s-1}}\beta^{2^{s-1}},$$

then $\epsilon^{u2^{s-1}} = -1$ and so u is odd. Since $\lambda \in G(k(\beta)/k)$, λ must have order a power of 2. Now

$$\lambda^{2^m}(\beta) = \epsilon^{u(p^{2^m-1}+\ldots+p+1)}\beta$$

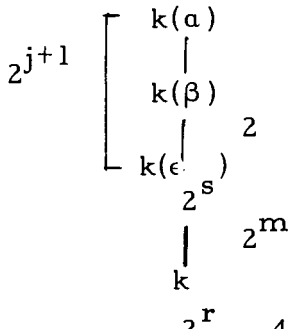
$$= \epsilon^{(u(p^{2^m}-1))/(p-1)}\beta$$

$$= \epsilon^{(u(p^{2^{m-1}}-1)(p^{2^{m-1}}+1))/(p-1)}\beta,$$

Since $p \equiv 7 \pmod 8$, then $p-1 \not\equiv 0 \pmod 4$ and $p^{2^{m-1}}+1 \not\equiv 0 \pmod 4$ for $m \geq 2$. By assumption, $p^{2^m}-1 \equiv 0 \pmod{2^s}$ while $p^{2^m}-1 \not\equiv 0 \pmod{2^{s+1}}$. If $2^s \mid p^{2^{m-1}}-1$, then $2^{s+1} \mid (p^{2^{m-1}}-1)(p^{2^{m-1}}+1) = p^{2^m}-1$, a contradiction. Thus $\lambda^{2^m}(\beta) \neq \beta$ while $\lambda^{2^{m+1}}$ is the identity automorphism. Since $[k(\beta):k] = 2^{m+1}$, then $G(k(\beta)/k)$ is cyclic and is generated by λ. In particular, $x^{2^s}+4b^4$ is k-adequate.

Let $r = s+j$, $j = 0, 1, 2, \ldots$. Since $(\beta^{2^{-j}})^{2^r} = -4b^4$, then

$\alpha = \beta^{2^{-j}}$ is a root of $x^{2^r}+4b^4$. Observe that $\alpha^{2^{r-s+1}} = \alpha^{2^{j+1}} = \epsilon_{2^s} dc\ \epsilon\ k(\epsilon_{2^s})$. We have



Let L be the splitting field of $x^{2^r}+4b^4$ over k, $L = k(\epsilon_{2^r}, \alpha)$. Let $\lambda \in G(L/k)$ where λ is any extension to L of the Frobenius automorphism sending $\theta = \epsilon_{2^r}$ to θ^p. Necessarily, $\sigma(\alpha) = \theta^u\alpha$. Since $-\alpha^{2^{r-1}} = \lambda(\alpha^{2^{r-1}}) = (\lambda(\alpha))^{2^{r-1}} = \theta^{u2^{r-1}}\alpha^{2^{r-1}}$, then $\theta^{u2^{r-1}} = -1$ and so u is odd. Since $[L:k]$ is a power of 2, then λ must have order a power of 2.

$$\lambda^{2^{m+j}}(\alpha) = \theta^{u(p^{2^{m+j}-1}+\ldots+p+1)}\alpha$$

$$= \theta^{(u(p^{2^{m+j}}-1))/(p-1)}\alpha$$

$$= \theta^{(u(p^{2^{m+j-1}}-1)(p^{2^{m+j-1}}+1))/(p-1)}\alpha$$

Since $p \equiv 7 \pmod 8$, then $p-1 \not\equiv 0 \pmod 4$ and

$p^{2^{m+j-1}} + 1 \not\equiv 0 \pmod 4$ for $j \geq 0$, $m \geq 2$.

Claim. $p^{2^{m+j-1}} - 1 \not\equiv 0 \pmod{2^{s+j}}$ while $p^{2^{m+j}} - 1 \equiv 0 \pmod{2^{s+j}}$.

Proof. Induct on j.

$j = 0$ has been verified already.

Suppose the result holds for all integers less than j, since $p^{2^{m+j-1}} - 1 \equiv 0 \pmod{2^{s+j-1}}$ and $p^{2^{m+j-1}} + 1 \equiv 0 \pmod 2$, then $p^{2^{m+j}} - 1 = (p^{2^{m+j-1}} - 1)(p^{2^{m+j-1}} + 1) \equiv 0 \pmod{2^{s+j}}$. On the other hand, $p^{2^{m+j-1}} - 1 \equiv 0 \pmod{2^{s+j}} \Rightarrow p^{2^{m+j-2}} - 1 \equiv 0 \pmod{2^{s+j-1}}$, a contradiction. Thus $p^{2^{m+j-1}} - 1 \not\equiv 0 \pmod{2^{s+j}}$ as required.

We have therefore shown that $\lambda^{2^{m+j}}(\alpha) \neq \alpha$ and that $\lambda^{2^{m+j+1}}$ is the identity homomorphism. Now, $G(L/k)$ is a permutation group on the roots of $x^{2^r} + 4b^4$. Since the order of λ, 2^{m+j+1}, is the least common multiple of the lengths of the cycles in the cycle structure of λ, we see that λ is a product of cycles, at least one of which is of length 2^{m+j+1}. From our proof we see that α is in a cycle of length $2^{m+j+1} = [k(\alpha):k]$ and so the Galois group of $\mathrm{Irr}(\alpha, k)$ contains a 2^{m+j+1}-cycle. By Lemma 2.9, $x^{2^r} + 4b^4$ is k-adequate.

Suppose $[k(\epsilon_{2^s}):k] = 2$, we have the following diagram:

$$\begin{array}{c} k(\beta) \\ | \quad 2 \\ k(\epsilon_{2^s}) \\ | \quad 2 \\ k \end{array} \qquad k(\beta)/k \text{ Galois.}$$

Let $\sigma \in G(k(\beta)/k)$, then σ must be an extension of $k(\beta)$ of either the automorphism sending $\epsilon_{2^s} = \epsilon$ to ϵ or the Frobenius automosphism sending ϵ to ϵ^p. Necessarily, $\sigma(\beta) = \epsilon^u \beta$.

(1) Suppose $\sigma(\epsilon) = \epsilon$, then $\beta^2 = \sigma(\beta^2) = (\sigma(\beta))^2 = \epsilon^{2u}\beta^2$. Thus $\epsilon^{2u} = 1$ and so $2^{s-1} | u$. The possibilities are

$$\sigma_1 : \begin{cases} \epsilon \longmapsto \epsilon \\ \beta \longmapsto \epsilon^{2^{s-1}}\beta \end{cases} \qquad \sigma_2 : \begin{cases} \epsilon \longmapsto \epsilon \\ \beta \longmapsto \beta \end{cases}$$

Observe that σ_1, σ_2 are of orders 2, 1 respectively.

(2) Suppose $\sigma(\epsilon) = \epsilon^p$.

If $p \equiv -1 \pmod{2^s}$, then $\sigma(\epsilon) = \epsilon^{-1}$. Also, $\sigma^2(\beta) = \epsilon^{-u}\epsilon^u\beta = \beta$. Hence, $G(k(\beta)/k)$ is not cyclic. In fact $G(k(\beta)/k) \tilde{=} Z_2 \oplus Z_2$.

Let $p \not\equiv -1 \pmod{2^s}$. Since $\epsilon^{p-1}\beta^2 = \sigma(\beta^2) = (\sigma(\beta))^2 = \epsilon^{2u}\beta^2$, then $\epsilon^{2u} = \epsilon^{p-1}$ and so $p-1 | 2u$. But $p \equiv 7 \pmod 8$, so u is odd. Note that the order of σ must either be 2 or 4. By assumption, $p+1 \not\equiv 0 \pmod{2^s}$, so $\sigma^2(\beta) = \epsilon^{u(p+1)}\beta \neq \beta$. On the

other hand, $\sigma^4(\beta) = \epsilon^{u(p^3+p^2+p+1)}\beta = \epsilon^{(u(p^2-1)(p^2+1))/(p-1)}\beta = \beta$ because $p^2+1 \not\equiv 0 \pmod 4$, $(p-1) \not\equiv 0 \pmod 4$ and $p^2-1 \equiv 0 \pmod{2^s}$. Hence, every extension of the Frobenius automorphism $\epsilon \longmapsto \epsilon^p$ is of order 4. In fact, $G(k(\beta)/k) = \langle\sigma\rangle$ is cyclic of order 4. By Lemma 2.9, $x^{2^s}+4b^4$ is k-adequate. The same computation as before shows that if λ is any extension to $L = k(\epsilon_{2^r}, a)$ of the Frobenius automorphism sending ϵ_{2^r} to $\epsilon_{2^r}^p$, then λ is of order 2^{j+2} and $x^{2^r}+4b^4$ is k-adequate.

Assume now that $G(k(\beta)/k) \cong Z_2 \oplus Z_2$. Suppose η is a prime in k which does not ramify from k to $k(\beta)$. Since $G(k_\eta(\beta)/k_\eta) \subseteq G(k(\beta)/k)$, and the Galois group of an unramified extension is cyclic, then $[k_\eta(\beta):k_\eta] = 1$ or 2 and so $Irr(\beta, k)$ can not remain irreducible over k_η.

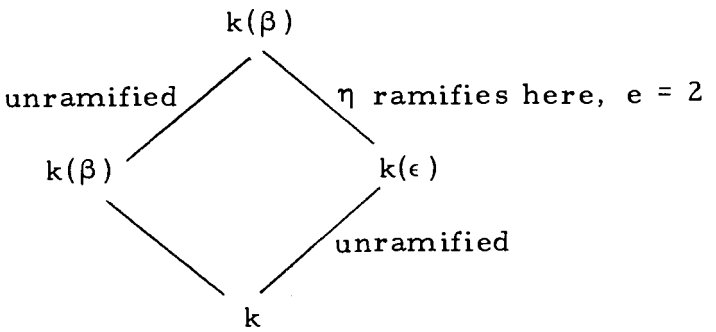
$$4 \left[\begin{array}{c} k(\beta) \\ | \ 2 \\ k(\epsilon_{2^s}) = k(\epsilon) \\ | \quad \text{unramified } f = 2 \\ k \end{array}\right.$$

Note that $\beta^2 = \epsilon dc \in k(\epsilon)$. If η is a prime of odd degree in k such that $\eta^w | c$, $\eta^{w+1} \nmid c$, w odd, then

$$|\beta|_\eta = \sqrt{|N_{k(\beta)/k(\epsilon)}(\beta)|_\eta} = \sqrt{|\epsilon dc|_\eta} = p^{-w/2}.$$

We have $2 \leq e \leq [k(\beta):k(\epsilon)] = 2$. Thus, η ramifies from $k(\epsilon)$

to $k(\beta)$ with $e = 2$. But



Thus, η ramifies from k to $k(\beta)$ with $e = 2$. We have $k_\eta(\sqrt{\epsilon dc})/k_\eta$ is ramified with $e = 2$ while $k_\eta(\epsilon)/k_\eta$ is unramified with $f = 2$. Hence, $[k_\eta(\beta):k_\eta] = 4$.

Suppose two primes of odd degree divide c, then $x^{2^s}+4b^4$ is k-adequate. Suppose exactly one prime of odd degree divides c, consider $|\ |_\infty$. We only have to look at $Z_p((t'))(\Delta)/Z_p((t'))$ where Δ is a root of $y^{2^s}+4(t')^{2^s q}b(1/t')^4$ and q is the smallest integer such that $(t')^{2^s q}b(1/t')^4 \in Z_p[t']$.

We want the smallest q satisfying $2^s q \geq 4 \deg b = 2^{s-1}\deg c$, i.e., $q \geq \deg c/2$. Since c has exactly one prime factor of odd degree and $c \notin k^2$, then $\deg c$ is odd. Let ν be the exponential valuation in $Z_p(t')(\Delta)$ extending the t'-valuation in $Z_p(t')$, then

$$2^s \nu(\Delta) = 2^s q - 2^{s-1}\deg c$$

and so $\nu(\Delta) = q - \deg c/2 = z/2$, z odd. $|\ |_\infty$ ramifies from k

to $k(\beta)$ with $e = 2$ since $|Z_p((t'))(\Delta)/Z_p((t'))| \leq 4$ with $Z_p((t'))(\epsilon)/Z_p((t'))$ an unramified extension of degree 2. Thus $[k_\infty(\beta):k] = 4$. By Lemma 2.9, $x^{2^s}+4b^4$ is k-adequate. It remains to prove that $x^{2^s}+4b^4$ k-adequate $\Rightarrow$ $x^{2^r}+4b^4$ k-adequate $\forall\ r \geq s$.

$$\begin{array}{c} k(a) \\ | \quad 2^{j+1} \\ k(\epsilon^{2^s}) = k(\epsilon) \\ | \quad 2 \\ k \end{array}$$

Note that $a^{2^{j+1}} = \epsilon dc\ \epsilon\ k(\epsilon)$.

(i) Suppose there exists two primes η in k of odd degree which divide c, let ν be the exponential valuation in $k(a)$ extending the η-valuation in k.

$$\therefore \quad |a|_\eta = \sqrt[2^{j+1}]{N_{k(a)/k(\epsilon)}(a)|_\eta} = \sqrt[2^{j+1}]{|\epsilon dc|_\eta} = p^{-w/2^{j+1}}$$

$\therefore \quad \nu(a) \geq 2^{j+1}$. But $[k(a):k(\epsilon)] = 2^{j+1}$, so $e = \nu(a) = 2^{j+1}$. As before, if η divides c, then η ramifies from k to $k(a)$ with $e = 2^{j+1}$. Since $k_\eta(\epsilon)/k_\eta$ is unramified with $f = 2$ while $k_\eta(\sqrt[2^{j+1}]{\epsilon dc})/k_\eta$ is ramified with $e = 2^{j+1}$, then $[k_\eta(a):k_\eta] = ef = 2^{j+2}$ and so $Irr(a,k)$ remains irreducible over

k_η for the same two η's.

(ii) Suppose there exists exactly one prime η in k of odd degree which divides c. We shall show that $|\ |_\infty$ ramifies from k to $k(a)$ with $e = 2^{j+1}$.

Let Δ be any root of $y^{2^r q} + 4(t')^{2^r q} b(1/t')^4$, where q is the smallest integer such that $(t')^{2^r q} b(1/t')^4 \in Z_p[s]$. A similar calculation as before shows that $q \gneq \deg c/2^{r-s+1} = \deg c/2^{j+1}$. Let ν be the exponential valuation in $Z_p(t')(\Delta)$ extending the t'-valuation in $Z_p(t')$, then

$$2^r \nu(\Delta) = 2^r q - 2^{s-1} \deg c$$

i.e.,

$$\nu(\Delta) = q - \frac{\deg c}{2^{j+1}} = \frac{w}{2^{j+1}}, \quad w \text{ odd.}$$

Since $Z_p((t'))(\epsilon)/Z_p((t'))$ is unramified with $f = 2$, then $2^{j+1} \leq \nu(\Delta) = e \leq 2^{j+1}$. Thus $|\ |_\infty$ ramifies with $e = 2^{j+1}$ and $[k_\infty(a):k_\infty] = 2^{j+2}$ making $x^{2^r} + 4b^4$ k-adequate.

Remarks. We have also shown that if $b \notin k^{2^{s-2}}$, $b \in k^{2^{s-3}}$, then $x^{2^s} + 4b^4$ is k-adequate if any one of the following conditions holds:

(i) $[k(\epsilon_{2^s}):k] \geq 4$.

(ii) $[k(\epsilon_{2^s}):k] = 2$ and $p \not\equiv -1 \pmod{2^s}$.

Let $[k(\epsilon_{2^s}):k] = 2$ and $p \equiv -1 \pmod{2^s}$. A necessary and sufficient condition then is the existence of at least one prime of odd degree which divides c where $b = c^{2^{s-3}}$, $c \notin k^2$.

Lemma 3.10. Let $b \in Z_p[t]$, $b \in k^{2^{s-2}}$, $s \geq 3$. Then $x^{2^s}+4b^4$ is k-adequate.

Proof. Let $b = c^{2^{s-2}}$. If β is any root of $x^{2^s}+4b^4$, then $\beta^{2^s} = -4b^4 = -4c^{2^s}$ and $\beta = \epsilon_{2^{s+1}} dc$ where $d = \sqrt[2^{s-1}]{2} \in k$. Thus, $k(\beta) = k(\epsilon_{2^{s+1}})/k$ is an unramified extension with cyclic Galois group. By Lemma 2.9, $x^{2^s}+4b^4$ is k-adequate.

From hereon, we take $a \in Z_p[t]$, $k = Z_p(t)$, $p \equiv 3 \pmod 4$.

Lemma 3.11. Let $f(x) = x^{2^r}+a$, where $a \in -k^2$ and $a \notin 4k^4$, then $f(x)$ is k-adequate.

Proof. Assume $a = -b^2$.

$r = 2$: $f(x) = x^4-b^2 = (x^2+b)(x^2-b)$. k-adequacy follows from the remarks preceding Lemma 3.9.

$r \geq 3$: $f(x) = x^{2^r}-b^2 = (x^{2^{r-1}}+b)(x^{2^{r-1}}-b)$. If $x^{2^{r-1}}+b$ is not irreducible in $k[x]$, then by Lemma 2.8, $b = -u^2$ or $b = 4v^4 = w^2$. We only need consider either

$x^{2^{r-1}}+b = x^{2^{r-1}}-u^2 = (x^{2^{r-2}}+u)(x^{2^{r-2}}-u)$ or

$x^{2^{r-1}} - b = x^{2^{r-1}} - w^2 = (x^{2^{r-2}} + w)(x^{2^{r-2}} - w)$. By continued reduction, we see that it suffices to consider $f(x) = x^{2^r} + a$, $r \geq 3$, $a \notin \pm k^2$. In fact, $f(x)$ is irreducible in $k[x]$.

Let $a = cd^2$, c square-free. Let α be any root of $f(x) = x^{2^r} + a$ and $\epsilon = \epsilon_{2^s}$.

Claim. If η is a prime in k dividing c, then η ramifies totally in $k(\alpha)$.

Proof. Let ν be the exponential valuation of $k(\alpha)$ extending the η-valuation of k. Suppose $\eta^q | d$, $\eta^{q+1} \nmid d$, since $\alpha^{2^r} = -a = -cd^2$, then

$$2^r \nu(\alpha) = \nu(\eta) + 2q\nu(\eta) = (1+2q)\nu(\eta).$$

$(1+2q)$ is odd, so $2^r | \nu(\eta)$. But $f(x)$ is irreducible. Thus, $\nu(\eta)$ is an integer less than or equal to 2^r. Hence,

$$e = \nu(\eta) = 2^r .$$

Note that η must be totally ramified in every subfield of $k(\alpha)$; in particular, η is totally ramified in every subfield of $k(\alpha) \cap k(\epsilon)$. But $k(\epsilon)/k$ is unramified, so $k(\alpha) \cap k(\epsilon) = k$. Now, the map σ given by $\sigma(\epsilon) = \epsilon$, $\sigma(\alpha) = \epsilon\alpha$ defines a 2^r-cycle in the Galois

group of $f(x)$. By Lemma 2.9 $f(x)$ is k-adequate.

Lemma 3.12. Let $f(x) = x^{2^r} + a$ where $a \notin 4k^4$. Then $f(x)$ is k-adequate.

Proof. Consider $f(x) = x^4 + a$. By Lemma 2.8, $f(x)$ is irreducible in $k[x]$. Moreover, by [10, Proposition 9, p. 178], $f(x)$ has four distinct roots, namely a_1, a_2, a_3, a_4.

Let $\alpha = a_1a_2 + a_3a_4$, $\beta = a_1a_3 + a_2a_4$, $\gamma = a_1a_4 + a_2a_3$. Let E be the splitting field of $f(x)$ over k. Then the Galois group of $f(x)$ over k, $G(E/k) = G$ is contained in S_4. Let $V = \{(1), (12)(34), (13)(24), (14)(23)\}$. We have

$$\begin{array}{ccc} E & & \{1\} \\ | & & | \\ k(\alpha, \beta, \gamma) & & G \cap V \\ | & & | \\ k & & G \end{array}$$

Note that $(y-\alpha)(y-\beta)(y-\gamma) = y^3 - 4ay = y(y^2-4a)$ so $k(\alpha, \beta, \gamma) = k(\sqrt{a})$ and $|G/G \cap V| = 2$. Since G acts transitively on the roots a_i, G must be cyclic of order 4. By Lemma 2.9, $f(x)$ is k-adequate.

By Lemma 2.8 and Lemma 2.9, $x^4 + a$ is irreducible over k_η for at least two primes η in k, i.e., $a \notin -k_\eta^2$, $a \notin 4k_\eta^4$ for at least two primes η in k. At these same primes,

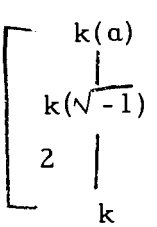
$x^{2^r}+a$ is irreducible for all r. By Lemma 2.9, $x^{2^r}+a$ is k-adequate.

Lemma 3.13. Let $f(x) = x^4+b^2$, $b = cd^2$, c square-free, then $f(x)$ is k-adequate if and only if there exists at least one prime η of odd degree in k which divides c.

Proof. By Lemma 2.8, $f(x)$ is irreducible over k. Let α be any root of $f(x)$, then $\alpha^2 = \pm\sqrt{-1}\, b$, so $k(\alpha) \supset k(\sqrt{-1})$. Without loss of generality, take $\alpha^2 = \sqrt{-1}\, b$. We have $b+\sqrt{-1}\, b/\alpha \in k(\alpha)$ and $2b = (b+\sqrt{-1}\, b/\alpha)^2$. Thus $\sqrt{2b} \in k(\alpha)$ and $k(\alpha) = k(\sqrt{-1}, \sqrt{2b}) = k(\sqrt{-1}, \sqrt{2c})$.

As in Lemma 3.9, $f(x)$ can not be irreducible in $k_\eta[x]$ unless η ramifies from k to $k(\alpha)$. Suppose η is a prime in k dividing c, then $|\sqrt{2c}|_\eta = |\sqrt{c}|_\eta = \sqrt{|N(\sqrt{c})|_\eta} = \sqrt{|c|_\eta} = p^{-1/2}$.

4 since $f(x)$ is irreducible over k.



Thus $2 \le e = \nu(\eta) \le [k(\alpha):k(\sqrt{-1})] = 2$, and so if $\eta \mid c$, then $k_\eta(\sqrt{2c})/k_\eta$ is ramified with $e = 2$. By Lemma 3.8, if η is of odd degree, then $k_\eta(\sqrt{-1})/k_\eta$ is unramified with $f = 2$. Hence, if there exist two primes η of odd degree dividing c, then in each

case, $[k_\eta(\alpha):k_\eta] = 4$ and x^4+b^2 where $b = cd^2$, c square-free, is k-adequate.

Suppose exactly one prime of odd degree divides c, then we check $|\ |_\infty$. Let $\gamma = \deg c$, $\delta = \deg d$. As in Lemma 3.9, it suffices to check $|Z_p((s))(\beta)/Z_p((s))|$ where $s = 1/t$, β is a root of $y^4 + g(s)$ and $g(s) = s^{4q}[c(1/s)d(1/s)^2]^2$, q is the minimal integer such that $s^{4q}[c(1/s)d(1/s)^2]^2 \in Z_p[s]$.

γ is odd, say $\gamma = 2m+1$. Then $q = m + \delta + 1$. We see that $s^2 | g(s)$, $s^3 \nmid g(s)$. Since $\beta^4 = -g(s)$, then $4\nu_s(\beta) = 2$ and $\nu_s(\beta) = 1/2$. Note that $Z_p((s))(\sqrt{-1})/Z_p((s))$ is unramified with $f = 2$. Hence, $[k_\infty(\alpha):k_\infty] = 4$ and $f(x)$ is k-adequate.

Lemma 3.14. If x^4+b^2 where $b = cd^2$, c square-free, is k-adequate, then $x^{2^r}+b^2$ is k-adequate, $r \geq 3$.

Proof. By Lemma 2.8, x^4+b^2, $x^{2^r}+b^2$ are irreducible in $k[x]$. If x^4+b^2 is k-adequate, then by Lemma 2.9 x^4+b^2 is irreducible over k_η for at least two primes η in k. Observe that $x^4+b^2 = (x^2+b\sqrt{-1})(x^2-b\sqrt{-1})$, and

$$4 \left[\begin{array}{c} k_\eta(\alpha) \\ | \quad 2 \\ k_\eta(\sqrt{-1}) \\ | \\ k_\eta \end{array} \right.$$

where α is any root of x^4+b^2 over k_η. Since x^4+b^2 is irreducible over k_η, $x^2 \pm b\sqrt{-1}$ must be irreducible over $k_\eta(\sqrt{-1})$. By Lemma 2.8 $b\sqrt{-1} \notin \pm(k_\eta(\sqrt{-1}))^2$. Thus, $\pm b\sqrt{-1} \notin 4(k_\eta(\sqrt{-1}))^4$ and $x^{2^{r-1}} \pm b\sqrt{-1}$ are irreducible over $k_\eta(\sqrt{-1})$; $[k_\eta(\sqrt{-1}):k_\eta] = 2$.

But $x^{2^r}+b^2 = (x^{2^{r-1}}+b\sqrt{-1})(x^{2^{r-1}}-b\sqrt{-1})$, so if α is any root of $x^{2^{r-1}}+b\sqrt{-1}$, then $[k_\eta(\alpha):k_\eta] = 2^r$ and $x^{2^r}+b^2$ is irreducible in $k_\eta[x]$ for the same η.

Thus, $x^{2^r}+b^2$ is k-adequate.

Lemma 3.15. $x^{2^r m}+a$, m odd, is k-adequate if $x^{2^r}+a$ is k-adequate.

Proof. Suppose $x^{2^r m}+a$ is irreducible, then $x^{2^r}+a$ and x^m+a are irreducible by Lemma 2.8. x^m+a is k-adequate [Lemma 3.1]. Assume $x^{2^r}+a$ is k-adequate. Let α be any root of $x^{2^r m}+a$. Then $\alpha_1 = \alpha^m$ and $\alpha_2 = \alpha^{2^r}$ are roots of $x^{2^r}+a$, x^m+a respectively. $[k(\alpha):k] = 2^r m = [k(\alpha_1):k][k(\alpha_2):k]$ so $k(\alpha) = k(\alpha_1, \alpha_2)$ with $([k(\alpha_1):k], [k(\alpha_2):k]) = 1$. By Lemma 2.10, $x^{2^r m}+a$ is k-adequate.

Assume $x^{2^r m}+a$ is reducible:

Case 1. x^m+a irreducible, $x^{2^r}+a$ reducible. By Lemma 2.8, $-a = b^2$ or $a = 4b^4$.

(i) $x^{2^r m}+a = x^{2^r m}-b^2 = (x^{2^{r-1} m}+b)(x^{2^{r-1} m}-b)$.

(Induct on r:) $r = 0$; x^m-b^2 is k-adequate since m is odd.

$r = 1$; $x^{2m}-b^2 = (x^m+b)(x^m-b)$ is k-adequate since $x^m \pm b$ is.

Now, x^m+a irreducible $\Rightarrow$ $x^m \pm b$ irreducible; $x^{2^r}+a$ k-adequate $\Rightarrow$ $x^{2^{r-1}}+b$ or $x^{2^{r-1}}-b$ k-adequate. By inductive hypothesis, $x^{2^{r-1} m}+b$ or $x^{2^{r-1} m}-b$ is k-adequate. Thus $x^{2^r m}+a$ is k-adequate.

(ii) $f(x) = x^{2^r m}+a = x^{2^r m}+4b^4$. Suppose $x^{2^r}+4b^4 = g_1(x)g_2(x)$ where $g_1(x)$ is irreducible over k of degree 2^u. Let $f(\alpha) = 0$. WLOG, $g_1(\alpha^m) = 0$. Since x^m+a is irreducible and $(\alpha^{2^r})^m+a = 0$, then $[k(\alpha^{2^r}):k] = m$. Observe that $f(x) = g_1(x^m)g_2(x^m)$ and degree $g_1(x^m)$ is $2^u m$. Hence, $k(\alpha) = k(\alpha^{2^r}, \alpha^m)$ and $g_1(x^m)$ is the minimal polynomial for α. By Lemma 3.1, x^m+a is k-adequate. Since $x^{2^r}+a$ is k-adequate, then by Lemma 2.10, $f(x)$ is k-adequate.

Case 2. x^m+a reducible. Then for some $n \mid m$, $a = b^n$ and x^u+b is irreducible over k where $m = nu$. Now $x^{2^r m}+a = x^{2^r nu}+b^n = (x^{2^r u}+b)(x^{(n-1)2^r u}+\ldots)$. From Case 1, $x^{2^r u}+b$ is k-adequate if $x^{2^r}+b$ is. Observe that $a \neq \pm k^2 \Rightarrow b \neq \pm k^2$ and $a = 4c^4 \Rightarrow b$ is of the same form. In fact, $a = cd^2 \Rightarrow b = ch^2$.

Thus $x^{2^r}+a$ k-adequate => $x^{2^r}+b$ k-adequate. By Case 1, $x^{2^r u}+b$ is k-adequate.

Theorem. Let $k = Z_p(t)$, the field of rational functions over Z_p, and $a \in k$. Let m be a positive integer.

(i) x^m+a is k-adequate if any one of the following conditions is satisfied:

(1) $m = p^s$

(2) $4 \nmid m$

(3) $a \in Z_p$

(4) $p \equiv 1 \pmod 4$

(5) $p \equiv 3 \pmod 8$ and $a \in 4(Z_p[t])^4$

(6) $a \notin (Z_p[t])^2$

(ii) $x^{2^r m}+a$, m odd, is k-adequate iff $x^{2^r}+a$ is k-adequate.

(iii) Let $a \in (Z_p[t])^2$, $a \notin 4(Z_p[t])^4$ and suppose $a = b^2$ where $b = cd^2$, c square-free. Then $x^{2^r}+a$ is k-adequate iff there exists at least one prime η of odd degree in k which divides c.

(iv) Let $p \equiv 7 \pmod 8$ and $a = 4b^4 \in Z_p[t]$. Let $b \notin k^{2^{s-2}}$, $b \in k^{2^{s-3}}$. Then

(1) $x^{2^r}+4b^4$ is k-adequate if $r \leq s-1$.

(2) $x^{2^r}+4b^4$ is k-adequate $\forall$ $r \geq s$ iff $x^{2^s}+4b^4$ is k-adequate.

(3) $x^{2^s}+4b^4$ is k-adequate if $[k(\epsilon_{2^s}):k] \geq 4$ or $[k(\epsilon_{2^s}):k] = 2$ and $p \not\equiv -1 \pmod{2^s}$.

(4) If $[k(\epsilon_{2^s}):k] = 2$ and $p \equiv -1 \pmod{2^s}$, then $x^{2^s}+4b^4$ is k-adequate iff there exists at least one prime η of odd degree in k which divides c where $b = c^{2^{s-3}}$ and $c \nmid k^2$.

(v) Let $u, v \in Z_p[t]$, $uv \neq 0$ and $(u, v) = 1$. $x^m + u/v$ is k-adequate iff $x^m+v^{m-1}u$ is k-adequate.

Proof. (i) follows from Lemmas 3.1, 3.2, 3.3, 3.4, 3.5, 3, 11, 3.12, 3.15 and the remarks following Lemma 3.8.

(ii) follows from Lemmas 3.6 and 3.15.

(iii) follows from Lemmas 3.13 and 3.14.

(iv) follows from Lemmas 3.9 and 3.10.

(v) is explained at the beginning of Chapter III.

BIBLIOGRAPHY

1. A. Albert, "Structure of Algebras", American Mathematical Society, New York 1939.

2. E. Artin and J. Tate, "Class Field Theory", Harvard University Press, Cambridge, Mass. 1961.

3. M. Deuring, "Algebra", Springer-Verlag, New York 1968.

4. M. Eichler, "Introduction to the Theory of Algebraic Numbers and Functions", Academic Press, New York 1966.

5. B. Fein and M. Schacher, Solutions of pure equations in rational division algebras I, J. Algebra 17 (1971) pp. 83-93.

6. B. Fein and M. Schacher, Solutions of pure equations in rational division algebras II, J. Algebra 21 (1972) pp. 518-522.

7. L. Goldstein, "Analytic Number Theory", Prentice-Hall, New Jersey, 1971.

8. I. Herstein, "Noncommutative Rings", Carus Monograph 15, 1968.

9. G. Janusz, "Algebraic Number Fields", Academic Press, New York 1973.

10. S. Lang, "Algebra", Addison-Wesley, Reading, Mass. 1965.

11. I. Reiner, "Maximal Orders", Academic Press, New York 1975.

12. M. Schacher, Subfields of division rings I, J. Algebra 9 (1968), pp. 451-477.

13. A Weil, "Basic Number Theory", Springer-Verlag, Berlin, 1974.

14. E. Weiss, "Algebraic Number Theory", McGraw-Hill, New York, 1963.

15. O. Zariski and P. Samuel, "Commutative Algebra" Vol I, van Nostrand, Princeton, 1958.