AN ABSTRACT OF THE THESIS OF

Gary Robert Greenfield for the degree of DOCTOR OF PHILOSOPHY

in Mathematics presented on April 22, 1976

Title: EVEN ORDER SUBGROUPS OF FINITE DIMENSIONAL DIVISION RINGS

Redacted for privacy

Abstract approved: ______________________

Burton I. Fein

Let K be a field, and G a finite group. G is said to be K-adequate if there exists a division ring D, finite dimensional over K, and with center K, such that G is contained in the multiplicative group of nonzero elements of D.

In this dissertation we investigate the notion of K-adequacy under the assumptions that K is an algebraic number field or p-local field and G is a noncyclic group of even-order. Results in this area depend upon the classification of K-division rings by means of Hasse invariants, and Amitsur's classification of those finite groups which can be embedded in the multiplicative group of some division ring.

It is shown that if K is an algebraic number field then there exists a noncyclic group of even-order which is K-adequate.

We show this is not true if K is a p-local field and determine necessary and sufficient conditions on K for there to exist a noncyclic group of even-order which is K-adequate. Combining this with previous work on noncyclic odd-order subgroups we determine when the restriction that the noncyclic group be of even-order may be dropped.

Even Order Subgroups of Finite Dimensional Division Rings

by

Gary Robert Greenfield

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

June 1976

APPROVED:

Redacted for privacy

Associate Professor of Mathematics
in charge of major

Redacted for privacy

Chairman of Department of Mathematics

Redacted for privacy

Dean of Graduate School

Date thesis is presented April 22, 1976

Typed by Clover Redfern for Gary Robert Greenfield

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EVEN ORDER SUBGROUPS OF FINITE DIMENSIONAL DIVISION RINGS

I. INTRODUCTION

1. Historical Background

The existence of (finite) noncyclic subgroups which can be embedded in the multiplicative group of nonzero elements of a division ring was established coincident with the discovery of the division ring of real quaternions by Hamilton in 1878. The question of which finite groups can be so embedded was first studied by I. N. Herstein in [12], who conjectured that the finite odd-order subgroups of a division ring are cyclic. He proved this conjecture for division rings of nonzero characteristic and the real quaternions. Herstein's conjecture was proved false in general by S. Amitsur [2] who determined all possible finite subgroups of division rings. In particular, Amitsur showed that the minimal possible odd-order group was one of order 63.

In view of Amitsur's results, B. Fein and M. Schacher posed a question related to Herstein's conjecture. They asked, "For which fields K, does there exist at least one division ring, finite dimensional over K and with center K, which contains a noncyclic odd-order subgroup?" That is, for which fields K does Herstein's conjecture fail. In [6] they showed that $\mathbb{Q}$, the field of rational numbers, and any quadratic extension of $\mathbb{Q}$ except $\mathbb{Q}(\sqrt{-3})$ satisfied Herstein's conjecture. In [7] they completely settled the question for K a p-local field, in [8] for K an algebraic number field, and in [9] under the assumption that D is a division ring with center K having exponent and index equal, for K an arbitrary field.

In this thesis we shall study a question related to the one given above by dropping the restriction that the group be of odd-order. Since [9, Theorem 9] there is an infinite dimensional division ring with center $\mathbb{Q}$ which contains all possible finite subgroups of division rings, we shall work only with division rings which are finite dimensional over their centers. Thus we ask for which fields K does there exist a division ring, finite dimensional over K and with center K, which contains an even-order noncyclic group?

2. Central Simple Algebras

The elementary properties of division rings arise from the theory of central simple algebras. Here we summarize some of these results. For a complete discussion the reader is referred to [13] or [14].

A ring A is an <u>algebra over K</u> (or <u>K-algebra</u>) if there exists an isomorphism $\sigma : K \rightarrow A$ such that $\sigma(K)$ is contained in the center of A. Moreover, A is called <u>central simple</u> if $\sigma(K)$

is the center of A, and A, as a ring, is simple. A is a vector space over K, and the vector space dimension is denoted $[A:K]$. We assume all K-algebras are finite dimensional over K.

From the Wedderburn Theorems it follows that if A is a central simple K-algebra, then $A \cong (D)_n$, the ring of $n \times n$ matrices with entries in a division ring with center K, for some n. Moreover n and D are unique up to isomorphism.

The class of central simple K-algebras is closed under the operation of the tensor product. A morphism from K-algebras to L-algebras where L is an extension field of K is given by

$$A \rightsquigarrow A \otimes_K L.$$

This morphism preserves dimensions (i.e., $[A:K] = [A \otimes_K L:L]$). L is called a <u>splitting field</u> for A if $A \otimes_K L \cong (L)_m$. The algebraic closure of K, denoted $\widetilde{K}$, is a splitting field for A, and if $A \cong (D)_n$ then any maximal subfield of D is a splitting field.

If A is finite dimensional over K then $[A:K] = n^2$. The <u>index of A,</u> denoted $\text{ind}(A)$, is defined to be n. In particular, if D is a division ring with center K and index m, then all maximal subfields of D are of degree m over K.

If A and B are finite dimensional central simple K-algebras, then A is <u>similar</u> to B, denoted $A \sim B$, if

$(A)_m \cong (B)_n$ for some m and n.[1] The relation $\sim$ is an equivalence relation and the equivalence class of A is denoted by $[A]$. The set of equivalence classes forms an abelian group $B(K)$, called the Brauer group of K, under the operation $[A] \cdot [B] = [A \otimes_K B]$.[2] $B(K)$ is a torsion group and the exponent of A, denoted $\exp(A)$, is defined to be the order of $[A]$ in this group. If $A \cong (D)_n$ and $[D:K] = m^2$ then $[A]^m = [K]$ so $\exp(A) \mid \operatorname{ind}(A)$.

The morphism $A \rightsquigarrow A \otimes_K L$ respects the equivalence relation, and hence induces a homomorphism from $B(K)$ to $B(L)$ whose kernel consists of all classes $[A]$ which are split by L.

If A is a K-algebra and B is a subalgebra of A, the centralizer of B in A is $C_A(B) = \{a \in A \mid ab = ba \text{ for all } b \in B\}$

Definition. A division ring D with center K is called a K-division ring.

Lemma 1.1. If D is a K-division ring, and $L \supset K$ is a subfield of D, then $C_D(L) \sim D \otimes_K L$.

Proof. See [6, Lemma 1].

[1] An equivalent definition is that if $A \cong (D)_r$ and $B \cong (D')_s$, then $A \sim B$ if and only if $D \cong D'$.

[2] The identity is $[K]$ and the inverse of $[A]$ is $[A^\circ]$ where $A^\circ = (A, +, \circ)$ has multiplication defined by $a \circ b = b \cdot a$.

3. Cyclic Crossed Products

Suppose K is a field and L is a cyclic extension of K with $<\sigma> = \mathrm{Gal}(L/K)$ and $n = [L:K]$. Let u be a symbol and consider the left K-module

$$V = \left\{ \sum_{i=0}^{n-1} \ell_i u^i \,\middle|\, \ell_i \in L \right\}.$$

Let $\gamma \in K^*$ and define a multiplication on V by

$$u \cdot \ell = \sigma(\ell) u$$
$$u^n = \gamma .$$

Then V is a finite dimensional central simple K-algebra called the <u>cyclic crossed product</u> of L by K with respect to σ, and is denoted (L, σ, γ).[3]

If for $1 \leq i < n$, γ^i is not a norm from K to L then (L, σ, γ) is a K-division ring. If γ is a norm from K to L then $(L, \sigma, \gamma) \sim K$.

Conversely, if D is a K-division ring which contains a maximal subfield L, and L is a cyclic extension of K, then $D \cong (L, \sigma, \gamma)$ for some $\gamma \in K^*$.

[3] A more general crossed product construction (L, G, ρ) allows a Galois extension L of K with $\mathrm{Gal}(L/K) = G$ and defines multiplication with respect to a <u>factor set</u> $\rho \in H^2(G, L^*)$.

With this construction in mind we examine more closely K-division rings where K is a local field or an algebraic number field.

4. Hasse Invariants

Suppose K is a local field. By this we mean a finite dimensional extension of the field of p-adic numbers $\mathbb{Q}_p$ for some prime p. We denote the residue field of K by $\overline{K}$, and the fundamental prime of K by π. Thus any $k \in K$ can be written in the form $k = u\pi^s$ where u is a unit of K and $s \in \mathbb{Z}$, the ring of integers.

If $|\overline{K}| = q$ then K has a unique unramified extension L of degree n. In fact $L = K(\varepsilon)$ where ε is a primitive $q^n - 1^{st}$ root of unity. L is a cyclic extension of K and the Galois group of L over K is generated by the Frobenius automorphism Frob: $\varepsilon \mapsto \varepsilon^q$. In general, we denote a primitive mth root of unity by ε_m.

Any K-division ring D of index n, contains a maximal subfield L which is unramified over K. Since any element of K of the form $u\pi^{sn}$ is a norm from K to L it follows that

$$D \cong (K(\varepsilon_{q^{n-1}}), \text{Frob}, \pi^r) \qquad \text{where} \qquad (r, n) = 1$$

Definition. Let D be a K-division ring of index n. Thus $D \cong (K(\varepsilon_{q^{n-1}}), \mathrm{Frob}, \pi^r)$. The Hasse invariant of D is defined to be $r/n \in \mathbb{Q}/\mathbb{Z}$.

Let A be a finite dimensional central simple K-algebra. Write $A \cong (D)_m$ with $D \cong (K(\varepsilon_{q^{n-1}}), \mathrm{Frob}, \pi^r)$. We define the map

$$\mathrm{inv} : B(K) \to \mathbb{Q}/\mathbb{Z}$$

by

$$\mathrm{inv}[A] = \frac{r}{n} \pmod 1.$$

By [5, p. 113 Satz 3] if $r/n \equiv s/m \pmod 1$ then $(K(\varepsilon_{q^{n-1}}), \mathrm{Frob}, \pi^r) \cong (K(\varepsilon_{q^{m-1}}), \mathrm{Frob}, \pi^s)$ so inv is well-defined. In fact inv is an additive isomorphism.

Now, suppose K is an algebraic number field. We consider a prime of K as either a prime ideal in the ring of algebraic integers of K or as one of the equivalence classes of valuations of K. A prime is finite or nonarchimedean if it extends the p-adic valuation of $\mathbb{Q}_p$, and is infinite or archimedean if it extends the usual absolute value of the rationals.

Let $\mathfrak{p}$ be a finite prime of K. We denote the completion of K at $\mathfrak{p}$ by $K_{\mathfrak{p}}$. Let A be a finite dimensional central simple K-algebra. We define $\mathrm{inv}_{\mathfrak{p}}[A]$ to be the composition of the maps

$$\begin{tikzcd}
B(K) \arrow[r, "\otimes_K K_{\mathfrak{p}}"] & B(K_{\mathfrak{p}}) \arrow[r, "\mathrm{inv}"] & \mathbb{Q}/\mathbb{Z} \\
{[A]} \arrow[r, mapsto] & {[A \otimes_K K_{\mathfrak{p}}]} \arrow[r, mapsto] & \mathrm{inv}[A \otimes_K K_{\mathfrak{p}}] .
\end{tikzcd}$$

Definition. Let K be an algebraic number field, A a finite dimensional central simple K-algebra, and $\mathfrak{p}$ a prime of K (finite or infinite). The Hasse invariant of A at $\mathfrak{p}$, $\mathrm{inv}_{\mathfrak{p}} A$, is defined to be

i) 0, if $\mathfrak{p}$ is complex

ii) $\mathrm{inv}_{\mathfrak{p}} [A]$, if $\mathfrak{p}$ is finite

iii) $1/2$, if $\mathfrak{p}$ is real archimedean and $A \otimes_K K_{\mathfrak{p}} \sim \mathcal{U}_{\mathbb{R}}$

iv) 0, if $\mathfrak{p}$ is real archimedean and $A \otimes_K K_{\mathfrak{p}} \sim \mathbb{R}$

where $\mathcal{U}_{\mathbb{R}}$ denotes the division ring of real quaternions.

Definition. If $\mathfrak{p}$ is a prime of K, the local index of A at $\mathfrak{p}$, $\ell.i._{\mathfrak{p}} A$, is defined to be the denominator of $\mathrm{inv}_{\mathfrak{p}} A$ as a fraction reduced to lowest terms.[4]

Let S be the set of primes of K, and let A and B be finite dimensional central simple K-algebras. The following properties of Hasse invariants are found in [5, Chapter VII]:

[4] If $\mathrm{inv}_{\mathfrak{p}} A = 0$, we set $l.i._{\mathfrak{p}} A = 1$.

(1.2) $\operatorname{inv}_{\mathfrak{p}} A = 0$ for all but finitely many $\mathfrak{p}$

(1.3) $\displaystyle\sum_{\mathfrak{p} \in S} \operatorname{inv}_{\mathfrak{p}} A \equiv 0 \pmod 1$

(1.4) $A \sim K$ iff $\operatorname{inv}_{\mathfrak{p}} A = 0$ for all $\mathfrak{p} \in S$

(1.5) $A \sim B$ iff $\operatorname{inv}_{\mathfrak{p}} A \equiv \operatorname{inv}_{\mathfrak{p}} B$ for all $\mathfrak{p} \in S$

(1.6) $\exp(A) = \underset{\mathfrak{p} \in S}{\mathrm{l.c.m.}} \{\mathrm{l.i.}_{\mathfrak{p}} A\}$

We have seen that Hasse invariants distinguish between the classes in the Brauer group of K. By Wedderburn's theorem each class is determined by a unique K-division ring. The following existence theorem gives an indication of how many K-division rings are available.

Theorem 1.7. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be a given set of primes (finite or infinite) of K; $u_1, \ldots, u_n$ rational numbers in lowest terms such that $0 \leq u_i < 1$, $\displaystyle\sum_{i=1}^{n} u_i \equiv 0 \pmod 1$, $u_j = 0$ or $1/2$ if $\mathfrak{p}_j$ is real, and $u_j = 0$ if $\mathfrak{p}_j$ is complex. Then there exists a K-division ring D with $\operatorname{inv}_{\mathfrak{p}_j} D = u_j$ for all j and $\operatorname{inv}_{\mathfrak{p}} D = 0$ for all other primes $\mathfrak{p}$ of K.

Proof. See [5, Satz 9 p. 119].

The next result allows us to tell when a division ring decays after tensoring.

Theorem 1.8. Let L be a field extension of K, $\mathfrak{p}$ a prime of K, and $\mathfrak{P}$ a prime of L dividing $\mathfrak{p}$. Then for any K-division ring D,

$$\mathrm{inv}_{\mathfrak{P}}\, D \otimes_K L \equiv \mathrm{inv}_{\mathfrak{p}}\, D \cdot [L_{\mathfrak{P}} : K_{\mathfrak{p}}] \pmod{1}.$$

Proof. See [5, Satz 4 p. 113].

If D is a K-division ring, our final result, tests maximal subfields.

Theorem 1.9. If L is a field extension of K, with $[L:K] = \mathrm{ind}(D)$ then L is isomorphic to a maximal subfield of D if and only if $\mathrm{l.i.}_{\mathfrak{p}}\, D \mid [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ for all primes $\mathfrak{p}$ of K and all extensions $\mathfrak{P}$ of $\mathfrak{p}$ to L.

Proof. This follows from [1, Theorem 27, p. 61] and [5, Satz 2, p. 118].

5. Amitsur's Classification

In this section we describe briefly those finite subgroups which can occur as subgroups of division rings. A complete discussion of this material is given in [2].

If G is a finite subgroup of the multiplicative group of a division ring we set

$$v(G) = \{\Sigma \alpha_i A_i \mid \alpha_i \in \mathbb{Q},\ A_i \in G\} .$$

$v(G)$ is a finite dimensional central division algebra over its center and is the minimal division algebra containing G.

A finite subgroup G of a division ring is a group acting without fixed points and hence must satisfy one of the following conditions:

A) All Sylow subgroups of G are cyclic

B) All odd order Sylow subgroups are cyclic, and the even Sylow subgroup is a generalized quaternion group of order 2^{a+1}, $a \geq 2$.

Definition. If m, r are relatively prime integers with $m > 0$, then $[r, m]$ is the order of r (mod m). That is $[r, m]$ is the least positive integer f such that $m \mid r^f - 1$. If u, v are integers with $u \mid v$ then $\beta(u, v)$ is the highest power of u dividing v. That is $u^{\beta(u, v)} \| v$.

Let $m, r \in \mathbb{Z}$ with $(m, r) = 1$. If $r = 1$, set $n = s = 1$. Otherwise we set

$$s = (r-1, m)$$

$$t = m/s$$

$$n = [r, m] .$$

Denote by $G_{m,r}$ the group

$$G_{m,r} = <A, B \mid A^m = 1,\ B^n = A^t,\ BAB^{-1} = A^r> .$$ [5/]

Then $|G_{m,r}| = mn$, the commutator is $G'_{m,r} = <A^s>$, and the center is $Z(G_{m,r}) = <A^t>$.

We call (r, m, t, s, n) as above an <u>Amitsur quintuple</u> if these integers satisfy

C) $(n, t) = (s, t) = 1$

or D) $\beta(2, n) = \beta(2, s) = 1$, $\beta(2, m) \geq 2$, $(n, t) = (s, t) = 2$, and

$r \equiv -1 \pmod{2^{\beta(2, m)}}$.

The motivation for this construction is that a $G_{m,r}$ group satisfies condition A) if and only if it satisfies C), and condition B) if and only if it satisfies D).

Now, for an Amitsur quintuple (r, m, t, s, n) we denote by $U_{m,r}$ the cyclic crossed product $(\mathbb{Q}(\varepsilon_m), \sigma_r, \varepsilon_s)$ where $\sigma_r : \varepsilon_m \mapsto \varepsilon_m^r$. $U_{m,r}$ has dimension n^2 over its center $Z_{m,r}$. If $G_{m,r}$ is a subgroup of the multiplicative group of a division ring then $v(G_{m,r}) \cong U_{m,r}$ under the correspondence $A \longleftrightarrow \varepsilon_m$, $B \longleftrightarrow \sigma_r$. Thus it suffices to determine which of the $U_{m,r}$ are division algebras.

[5/] If $r = 1$, then $G_{m,1}$ is a cyclic group of order m.

Let p and q be primes dividing m. Write $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} p^{\alpha} q^{\beta}$ and set

$$n_p = [p, mp^{-\alpha}]$$

$$\gamma_0 = [p, q^{\beta}]$$

$$\gamma_i = [p, p_i] .$$

Theorem 1.10. A necessary and sufficient condition that $U_{m,r}$ be a division algebra is that (r, m, t, s, n) is an Amitsur quintuple and either:

1) $n = s = 2$ and $r \equiv -1 \pmod m$

or 2) For every prime $q | n$ there exists a prime $p | m$ such that $q \nmid n_p$, and one of the following holds:

a) $p \equiv 1 \pmod 4$ or $q \neq 2$, and

$$\beta(q, s) \geq \beta(q, p-1) + \max_i\{\beta(q, \gamma_i)\}$$

b) $p \equiv 1 + 2 + \ldots + 2^i \pmod{2^{i+2}}$ for $i \geq 1$, $q = 2$, condition C) holds, and

i) $\beta(2, s) \geq i+1 + \max(1, \beta(2, \gamma_i))$, if $s \equiv 0 \pmod 4$

ii) $\beta(2, \gamma_i) = 0$ (i.e. all γ_i are odd integers) if $s \not\equiv 0 \pmod 4$.

c) $p = q = 2$, condition D) holds, and all γ_i are odd integers.

Proof. See [2, Theorem 5].

A complete determination of the subgroups of division rings requires the introduction of the binary tetrahedral, octahedral, and icosahedral groups denoted T^*, O^*, and I^* respectively. These groups are described in terms of generators and relations in [2, pp. 374-377].

Theorem 1.11. A group G can be embedded in a division ring if and only if G is one of the following types:

1) A cyclic group.

2) A $G_{m,r}$ group as described in the previous theorem.

3) $T^* \times G_{m,r}$ where $G_{m,r}$ is cyclic, or of the preceding type, and in either case for all primes $p|m$, $[2, p]$ is odd.

4) The groups O^* and I^*.

Proof. See [2, Theorem 7].

II. THE SPECIAL GROUPS Q*, T*, O*, AND I*

1. Invariants of the Special Groups

In studying the subgroups of division rings we wish to restrict ourselves to $G_{m,r}$ groups which satisfy condition C). To accomplish this we first present a detailed study of the special groups. The groups T*, O*, and I* have already been introduced, so only Q* remains.

Set $m = 4$ and $r = 3$. A direct computation shows that $n = s = t = 2$, and thus (r, m, t, s, n) is an Amitsur quintuple satisfying condition D). By Theorem 1.10 $G_{4,3}$ is a subgroup of a division ring of type 1). In terms of generators and relations

$$G_{4,3} = <A, B | A^4 = 1, B^2 = A^2, BAB^{-1} = A^3> .$$

This is the well-known quaternion group of order eight which we denote by Q*.

The remainder of this section is devoted to computing the invariants of the minimal division rings of the special groups. We first present some tools to aid in these computations.

Proposition 2.1. If K is an algebraic number field and $A = (L, \sigma, \gamma)$ is a cyclic crossed product with center K, then the only finite primes of K for which A may have nonzero invariants are those which ramify from K to L.

Proof. This follows immediately from [1, Theorem 14, p. 75] and [1, Theorem 19, p. 141].

Lemma 2.2. Let K be an algebraic number field, and D a K-division ring of index two. Then the nonzero invariants of D all have value $1/2$.

Proof. Let S be the set of primes of K. By [5, Satz 7, p. 119], $\mathrm{ind}(D) = \exp(D)$ and thus by Property 1.6,

$$2 = \underset{\mathfrak{p} \in S}{\mathrm{l.c.m.}} \{\mathrm{l.i.}_{\mathfrak{p}} D\}$$

Suppose $\mathrm{inv}_{\mathfrak{p}} D \neq 0$ for $\mathfrak{p} \in S$. By definition $\mathrm{l.i}_{\mathfrak{p}} D \neq 1$, and so $\mathrm{l.i.}_{\mathfrak{p}} D = 2$. Since the latter is the denominator of $\mathrm{inv}_{\mathfrak{p}} D$ and the invariants are defined (mod 1) we must have $\mathrm{inv}_{\mathfrak{p}} D = 1/2$.

From the construction given in Section 5 of Chapter I, we know that

$$v(Q^*) \cong (\mathbb{Q}(\varepsilon_4), \sigma_3, -1).$$

Since $v(Q^*)$ has index $n = 2$, and the only subfield of degree two in $\mathbb{Q}(\varepsilon_4)$ is the rationals, $v(Q^*)$ has center $\mathbb{Q}$. By [15, Theorem 9.1, p. 39], the prime (2) is the only prime which ramifies from $\mathbb{Q}$ to $\mathbb{Q}(\varepsilon_4)$. Thus the infinite prime of $\mathbb{Q}$, denoted ∞, and the prime (2) are the only primes for which $v(Q^*)$ may have nonzero invariants. Since $v(Q^*)$ is a division ring it must have at least one nonzero invariant, and by Lemma 2.2 this invariant has the value $1/2$. By applying Property 1.2 we conclude

$$(2.3) \qquad \operatorname{inv}_{\mathfrak{p}} v(Q^*) = \begin{cases} 1/2 & \text{if } \mathfrak{p} = (2) \text{ or } \infty \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathcal{U}$ denote the division ring of rational quaternions, and $\mathcal{U}_{\mathbb{R}}$ the division ring of real quaternions. As $\mathcal{U}$ is a $\mathbb{Q}$-division ring of index two containing Q^*, $v(Q^*) \cong \mathcal{U}$.

In [2, pp. 375-377], it is shown that

$$\begin{aligned} v(T^*) &\cong \mathcal{U} \\ v(O^*) &\cong \mathcal{U} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \\ v(I^*) &\cong \mathcal{U} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{5}). \end{aligned}$$

As $v(T^*) \cong v(Q^*)$, the invariants of $v(T^*)$ are determined by (2.3). Thus only $v(O^*)$ and $v(I^*)$ remain. By Theorem 1.8 we need only consider the primes of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ which extend (2) and ∞.

Let K be an algebraic number field. By [15, Theorem 4.4, p. 87] if $\tau_1, \ldots, \tau_r$ are the real embeddings of K and

$\tau_{r+1}, \ldots, \tau_{r+s}$ are one member of each conjugate pair of complex embeddings of K, then the infinite primes of K are in one-to-one correspondence with the archimedean valuations defined by $|x|_i = |\tau_i(x)|$.

Briefly we shall let G be the group O^* or I^* and a be $\sqrt{2}$ on $\sqrt{5}$ respectively. Then $\mathbb{Q}(a)$ has two real infinite primes ∞_1 and ∞_2 corresponding to the embeddings $\tau_1, \tau_2 : \mathbb{Q}(a) \to \mathbb{R}$ defined by

$$\tau_1 : a \mapsto a$$
$$\tau_2 : a \mapsto -a.$$

Using Theorem 1.8, we have

$$\begin{aligned} \mathrm{inv}_{\infty_i} v(G) &\equiv \mathrm{inv}_{\infty} \mho [\mathbb{Q}(a)_{\infty_i} : \mathbb{Q}_{\infty}] \\ &\equiv \frac{1}{2} \cdot 1 \\ &\equiv \frac{1}{2} \pmod 1. \end{aligned}$$

By [18, Corollary 6-2-3], the prime (2) is inertial in $\mathbb{Q}(\sqrt{5})$ and is ramified in $Q(\sqrt{2})$. Let $\mathfrak{B}$ denote the prime of $\mathbb{Q}(a)$ extending (2). Then

$$e(\mathfrak{B}/(2)) = 1, \quad f(\mathfrak{B}/(2)) = 2 \quad \text{if} \quad a = \sqrt{5}$$
$$e(\mathfrak{B}/(2)) = 2, \quad f(\mathfrak{B}/(2)) = 1 \quad \text{if} \quad a = \sqrt{2}$$

where e and f are the ramification and relative degrees respectively. In either case,

$$\begin{aligned}[\mathcal{Q}(\alpha)_{\mathfrak{B}} : \mathcal{Q}_{(2)}] &= ef \\ &= 2.\end{aligned}$$

Computation gives

$$\begin{aligned}\mathrm{inv}_{\mathfrak{B}}\ v(G) &= \mathrm{inv}_{(2)}\mathcal{U}\,[\mathcal{Q}(\alpha)_{\mathfrak{B}} : \mathcal{Q}_{(2)}] \\ &\equiv \frac{1}{2}\cdot 2 \\ &\equiv 0 \pmod 1,\end{aligned}$$

and thus,

$$\mathrm{inv}_{\mathfrak{y}}\ v(G) = \begin{cases} 1/2 & \text{if } \mathfrak{y} = \infty_1 \text{ or } \infty_2 \\ 0 & \text{otherwise.} \end{cases} \tag{2.4}$$

The invariants of the minimal algebras for the special groups are summarized in Table 1.

2. K-Adequacy of Q^* and T^*

Definition. A group G is K-adequate if there exists a K-division ring D such that G is contained in the multiplicative group of nonzero elements of D.

If G is K-adequate then $v(G)$, the minimal division ring containing G, is contained in some K-division ring. Thus the

Table 1. Invariants for v(G) where G is a special group.

$$\left.\begin{array}{l}\operatorname{inv}_{\mathfrak{p}}\ v(Q^*)\\[2em] \operatorname{inv}_{\mathfrak{p}}\ v(T^*)\end{array}\right\} = \begin{cases} 1/2 & \text{if } \mathfrak{p} = (2) \text{ or } \infty \\[2em] 0 & \text{otherwise}\end{cases}$$

$$\left.\begin{array}{l}\operatorname{inv}_{\mathfrak{p}}\ v(O^*)\\[2em] \operatorname{inv}_{\mathfrak{p}}\ v(I^*)\end{array}\right\} = \begin{cases} 1/2 & \text{if } \mathfrak{p} = \infty_1 \text{ or } \infty_2 \\[2em] 0 & \text{otherwise}\end{cases}$$

where ∞_1, ∞_2 correspond to the embeddings

$$\tau_1, \tau_2 : \mathbb{Q}(\alpha) \to \mathbb{R}$$

defined by

$$\tau_1 : \alpha \mapsto \alpha$$

$$\tau_2 : \alpha \mapsto -\alpha$$

and

$$\alpha = \begin{cases} \sqrt{2} & \text{for } O^* \\ \sqrt{5} & \text{for } I^* \end{cases}$$

Q^* = quaternion group of order 8

T^* = binary tetrahedral group of order 24

O^* = binary octahedral group of order 48

I^* = binary icosahedral group of order 120 problem of embedding a group G in a K-division ring is equivalent to embedding $v(G)$ in a K-division ring. Since $v(Q^*) \cong v(T^*)$ we need only consider the group Q^*.

Lemma 2.5. Let K be a field. Then $\mathfrak{U} \otimes_{\mathbb{Q}} K \sim K$ if and only if $-1 = a^2 + b^2$ in K.

Proof. Suppose $-1 = a^2 + b^2$ in K. If a or $b = 0$, then $\varepsilon_4 \in K$. Thus $\mathfrak{U} \otimes_{\mathbb{Q}} K \cong (\mathfrak{U} \otimes_{\mathbb{Q}} \mathbb{Q}(\varepsilon_4)) \otimes_{\mathbb{Q}(\varepsilon_4)} K$. But $\mathfrak{U} \cong (\mathbb{Q}(\varepsilon_4), \sigma_3, -1)$ where $\sigma_3 : \varepsilon_4 \mapsto -\varepsilon_4$, so $\mathbb{Q}(\varepsilon_4)$ is a maximal subfield of $\mathfrak{U}$ and hence splits $\mathfrak{U}$. Therefore

$$\begin{aligned} \mathfrak{U} \otimes_{\mathbb{Q}} K &\sim \mathbb{Q}(\varepsilon_4) \otimes_{\mathbb{Q}} K \\ &\sim K. \end{aligned}$$

If $\varepsilon_4 \notin K$, then $K(\varepsilon_4)$ is a quadratic extension of K. We extend $\sigma = \sigma_3$ to $K(\varepsilon_4)$ by defining $\sigma(k) = k$ for all $k \in K$. Then

$$\begin{aligned} \mathfrak{U} \otimes_{\mathbb{Q}} K &\cong (\mathbb{Q}(\varepsilon_4), \sigma, -1) \otimes_{\mathbb{Q}} K \\ &\cong (K(\varepsilon_4), \sigma, -1) . \end{aligned}$$

The latter is a K-algebra of index two and so by Wedderburn's Theorem is either split by K or is a K-division ring.[6] It is split

[6] $\mathfrak{U} \otimes_{\mathbb{Q}} K \cong (D)_r$ where $r \cdot \operatorname{ind}(D) = 2$. Thus either $\operatorname{ind}(D) = 1$, in which case $D = K$, or $r = 1$ and $\mathfrak{U} \otimes_{\mathbb{Q}} K$ is a K-division ring.

by K if and only if $-1 = N_{K(\varepsilon_4)/K}(\alpha)$ for some $\alpha \in K(\varepsilon_4)$. Let $\beta = a + b\varepsilon_4$. Then

$$\begin{aligned} N_{K(\varepsilon_4)/K}(\beta) &= (a+b\varepsilon_4)(a-b\varepsilon_4) \\ &= a^2 + b^2 \\ &= -1. \end{aligned}$$

Conversely, if $\mathcal{U} \otimes_{\mathbb{Q}} K \sim K$ and $\varepsilon_4 \in K$, then $-1 = (\varepsilon_4)^2$ as required. If $\varepsilon_4 \notin K$, then $-1 = N_{K(\varepsilon_4)/K}(\alpha)$ for α. Writing $\alpha = a + b\varepsilon_4$ gives $-1 = a^2 + b^2$.

<u>Proposition 2.6</u>. If K is a field, then Q^* is K-adequate if and only if $-1 \neq a^2 + b^2$ for all $a, b \in K$.

<u>Proof</u>. Suppose $-1 \neq a^2 + b^2$ for all $a, b \in K$. Then by the previous lemma $D = \mathcal{U} \otimes_Q K$ is not split by K and hence must be a K-division ring. But $v(Q^*) \cong \mathcal{U}$ so Q^* is K-adequate.

If Q^* is contained in D for some K-division ring D, then $v(Q^*) \subseteq D$. Since K is the center of D it commutes with $v(Q^*)$ and thus the algebra generated by K and $v(Q^*)$ is contained in D. This is $v(Q^*) \otimes_{\mathbb{Q}} K$ and must be a subdivision ring of D. Since $v(Q^*) \otimes_{\mathbb{Q}} K$ is either split by K or a K-division ring the previous lemma shows $-1 \neq a^2 + b^2$ for all $a, b \in K$.

We will be particularly interested in this last result when K is an algebraic number field or p-local field. The result is sufficient for K an algebraic number field but we require a better description for p-local fields.

By [18, Corollary 2-2-8] if $p \equiv 1 \pmod 4$ then -1 is a square in $\mathbb{Q}_p$, so if K is a p-local field with $p \equiv 1 \pmod 4$ Q^* is not K-adequate. We extend this result to a larger class of fields.

Proposition 2.7. If K is a p-local field with p an odd prime then Q^* is not K-adequate.

Proof. By [7, Proposition 2] a necessary condition that Q^* be K-adequate is that there exists a prime $\mathfrak{P}$ of $\mathbb{Q}$ such that $\operatorname{inv}_{\mathfrak{P}} v(Q^*) = e/n$, $(e, n) = 1$, $\mathfrak{P} \mid p$, and $p \mid |Q^*|$. Since p is an odd prime $p \nmid |Q^*|$ and thus Q^* is not K-adequate.

The situation for 2-local fields is a bit more complicated. We first note that Q^* is $\mathbb{Q}_2$-adequate since

$$\begin{aligned}\operatorname{inv}_{(2)} v(Q^*) &= \operatorname{inv} v(Q^*) \otimes_{\mathbb{Q}} \mathbb{Q}_2 \\ &= \frac{1}{2}\end{aligned}$$

and thus $v(Q^*) \otimes_{\mathbb{Q}} \mathbb{Q}_2$ is not split so must be a $\mathbb{Q}_2$-division ring.

Proposition 2.8. Let K be a 2-local field. Then Q^* is K-adequate if and only if $2 \nmid [K:\mathbb{Q}_2]$.

Proof. Let $w(Q^*) = v(Q^*) \otimes_{\mathbb{Q}} \mathbb{Q}_2$. As noted above $w(Q^*)$ is a $\mathbb{Q}_2$-division ring. As in the proof of Proposition 2.6 we need only determine when

$$\begin{aligned} D &= v(Q^*) \otimes_{\mathbb{Q}} K \\ &\cong (v(Q^*) \otimes_{\mathbb{Q}} \mathbb{Q}_2) \otimes_{\mathbb{Q}_2} K \\ &\cong w(G) \otimes_{\mathbb{Q}_2} K \end{aligned}$$

is a K-division ring. Since D has index two this occurs when D has nonzero invariant.

$$\begin{aligned} \text{inv } D &\cong \text{inv } w(G)\,[K:\mathbb{Q}_2] \\ &\equiv \frac{1}{2}\cdot[K:\mathbb{Q}_2] \pmod 1) \end{aligned}$$

Thus $\text{inv } D \not\equiv 0 \pmod 1$ if and only if $2 \nmid [K:\mathbb{Q}_2]$.

3. K-Adequacy of O^* and I^*

In this section we determine the K-adequacy of the special groups O^* and I^*. It is interesting to note that even though I^* is the only finite group of a division ring which is nonsolvable,[7/] in

[7/] Its center, $Z(I^*)$ has order two, and $I^*/Z(I^*) \cong A_5$, the alternating group of order 60, which is simple.

terms of K-adequacy it is quite similar to O^*.

Though we will not use the following result in its full generality it is of independent interest.

Theorem 2.9. Let K be an algebraic number field and D a K-division ring of index $n = p_1^{a_1} \dots p_r^{a_r}$. Let L be a finite extension of K. Then $D \otimes_K L$ is an L-division ring if and only if for each p_i $i = 1, \dots, r$ there is a prime $\mathfrak{P}_i$ of K with

$$\operatorname{inv}_{\mathfrak{P}_i} D = \frac{b_i}{p_i^{a_i} u_i},$$

$p_i \nmid u_i$ and a prime $\mathcal{Y}_i$ of L extending $\mathfrak{P}_i$ such that $p_i \nmid [L_{\mathcal{Y}_i} : K_{\mathfrak{P}_i}]$.

Proof. Let S be the set of primes of K. We note that $D \otimes_K L$ is an L-algebra of index n. Since K is an algebraic number field, $\operatorname{ind}(D) = \exp(D)$. By Property 1.6,

$$\exp(D) = \underset{\mathfrak{P} \in S}{\text{l.c.m.}} \{\text{l.i.}_{\mathfrak{P}} D\}.$$

By definition, $\text{l.i.}_{\mathfrak{P}} D$ is the denominator of $\operatorname{inv}_{\mathfrak{P}} (D)$. Since $p_i^{a_i} | n$ there exists a prime $\mathfrak{P}_i \in S$ with

$$\mathrm{inv}_{\mathcal{B}_i} D = \frac{b_i}{p_i^{a_i} u_i}, \quad p_i \nmid u_i .$$

If $D \otimes_K L$ is an L-division ring then $\exp(D \otimes_K L) = n$ and so

$$n = \underset{\mathcal{Y} \text{ a prime of } L}{\mathrm{l.c.m}} \{\mathrm{l.i.}_{\mathcal{Y}} D \otimes_K L\} .$$

If $\mathcal{Y}_{ij}$ extends $\mathcal{B}_i$, then

$$\mathrm{inv}_{\mathcal{Y}_{ij}} D \otimes_K L \equiv \mathrm{inv}_{\mathcal{B}_i} D \, [L_{\mathcal{Y}_{ij}} : K_{\mathcal{B}_i}]$$

$$\equiv \frac{b_i}{p_i^{a_i} u_i} [L_{\mathcal{Y}_{ij}} : K_{\mathcal{B}_i}] \pmod 1$$

Considering all $\mathcal{B}_i$ with $p_i^{a_i} | \mathrm{l.i.}_{\mathcal{B}_i} D$ we have

$$p_i^{a_i} | \underset{i,j}{\mathrm{l.c.m}} \{\mathrm{l.i.}_{\mathcal{Y}_{ij}} D \otimes_K L\}$$

only if $p_i \nmid [L_{\mathcal{Y}_{ij}} : K_{\mathcal{B}_i}]$ for some i and j.

Conversely, if such $\mathcal{Y}_i$ and $\mathcal{B}_i$ exist then $p_i^{a_i} | \exp(D \otimes_K L)$ for all i so $n | \exp(D \otimes_K L)$. Since $\exp(D \otimes_K L) | \mathrm{ind}(D \otimes_K L) = n$, $\exp(D \otimes_K L) = n$. Writing $D \otimes_K L = (D')_r$, we have $\exp(D \otimes_K L) = \exp(D') = n$ and taking dimensions over L gives $n^2 = n^2 r^2$, so $r = 1$ and $D \otimes_K L$

is an L-division ring.

As in Section 1, we let G be O^* or I^* and $\alpha = \sqrt{2}$ or $\sqrt{5}$ accordingly. We now determine the K-adequacy of G for K an algebraic number field.

Lemma 2.10. If G is K-adequate with K an algebraic number field, then $\alpha \in K$.

Proof. Suppose G is K-adequate. Then $v(G)$ is contained in D, a K-division ring. Since $v(G) \cong \mathcal{U} \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha)$, $\alpha \in D$. Thus $K(\alpha)$ is a subfield of D. Since K, the center of D, commutes with $v(G)$; and $\mathbb{Q}(\alpha)$, the center of $v(G)$, commutes with $v(G)$, $v(G) \subseteq C_D(K(\alpha))$. Thus $D' = v(G) \otimes_{\mathbb{Q}(\alpha)} K(\alpha)$ is a subdivision ring of D. Now,

$$\begin{aligned}[D' : \mathbb{Q}(\alpha)] &= [v(G) : \mathbb{Q}(\alpha)][K(\alpha) : \mathbb{Q}(\alpha)] \\ &= 4[K(\alpha) : \mathbb{Q}(\alpha)] ,\end{aligned}$$

and

$$[D' : \mathbb{Q}(\alpha)] = [D' : K(\alpha)][K(\alpha) : \mathbb{Q}(\alpha)]$$

so

$$[D' : K(\alpha)] = 4 .$$

Also,

$$[K(\alpha) : K] = \begin{cases} 1 & \text{if } \alpha \in K \\ 2 & \text{if } \alpha \notin K . \end{cases}$$

If $\alpha \notin K$, then

$$([K(\alpha): K], [D': K(\alpha)]) \neq 1$$

which contradicts [6, Theorem 1]. Thus $\alpha \in K$.

Proposition 2.11. G is K-adequate if and only if $\alpha \in K$ and K has at least one real infinite prime.

Proof. By the previous lemma we know $\alpha \in K$. As in the proof of Proposition 2.6, we have G is K-adequate if and only if $v(G) \otimes_{\mathbb{Q}(\alpha)} K$ is a K-division ring. By Theorem 2.9 this occurs if and only if there is a prime $\mathfrak{P}$ of K extending ∞_i, $i = 1$ or 2, such that $2 \nmid [K_{\mathfrak{P}}: \mathbb{Q}(\alpha)_{\infty_i}]$. Since extensions of ∞_i are archimedean primes, by Ostrowski's Theorem [18, Theorem 1-8-3] these completions are isomorphic to $\mathbb{R}$ on $\mathbb{C}$. Since $\mathbb{Q}(\alpha)_{\infty_i} \cong \mathbb{R}$, we require a prime $\mathfrak{P}$ such that $[K_{\mathfrak{P}} : \mathbb{R}] = 1$. Equivalently $\mathfrak{P}$ is a real infinite prime of K.

Since a real infinite prime of K corresponds to a real embedding, G is K-adequate if and only if $\alpha \in K$ and K has at least one real embedding. Fortunately, the K-adequacy for p-local fields is much simpler.

Proposition 2.12. If K is a p-local field then G is not K-adequate.

Proof. Suppose not. Since K is p-local by [7, Proposition 2] there exists a prime $\mathfrak{p}$ of $\mathbb{Q}(\alpha)$, $\mathfrak{p} \mid p$ and $p \mid |G|$ such that $\mathrm{inv}_{\mathfrak{p}}\, v(G) = e/n$ with $(e, n) = 1$. Since $|O^*| = 48$ and $|T^*| = 120$ we must have $p = 2, 3$, or 5. Thus $\mathfrak{p}$ is a finite prime of $\mathbb{Q}(\alpha)$. But this contradicts 2.4 which says $\mathrm{inv}_{\mathfrak{p}}\, v(G) = 0$ for all finite primes of $\mathbb{Q}(\alpha)$.

We note that G is $\mathbb{R}$-adequate since

$$\begin{aligned} v(G) \otimes_{\mathbb{Q}(\alpha)} \mathbb{Q}(\alpha)_{\infty_i} &\cong (\mathcal{U} \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha)) \otimes_{\mathbb{Q}(\alpha)} \mathbb{R} \\ &\cong \mathcal{U} \otimes_{\mathbb{Q}} \mathbb{R} \\ &\cong \mathcal{U}_{\mathbb{R}}\ , \end{aligned}$$

the division ring of real quaternions. Moreover $\mathcal{U} \subseteq \mathcal{U}_{\mathbb{R}}$ so all the special groups are $\mathbb{R}$-adequate.

4. A Result for Arbitrary Fields

If K is an arbitrary field then it is not true in general that for any K-division ring D, $\mathrm{ind}(D) = \exp(D)$. This makes the general problem of K-adequacy quite difficult. By Proposition 2.6 the K-adequacy of Q^* is completely determined. We shall attempt to prove K-adequacy for $G = O^*$ or I^*.

By [2, Lemmas 12 and 13],

$$v(O^*) \cong (\mathbb{Q}(\varepsilon_8), \sigma_{-1}, -1)$$

$$v(I^*) \cong (\mathbb{Q}(\varepsilon_5), \sigma_{-1}, -1).$$

Thus we set $u = 8$ or 5 according as G is O^* or I^*. Let K be an arbitrary field of characteristic zero and D a K-division ring of index n containing G.

<u>Lemma 2.13</u>. $D \cong \mathfrak{U} \otimes_{\mathbb{Q}} A$ where A is a K-algebra of degree $(n/2)^2$ over K.

<u>Proof</u>. G contains the quaternion group Q^*. Thus $D \supseteq v(Q^*) \cong \mathfrak{U}$, and $\mathfrak{U} \otimes_{\mathbb{Q}} K$ is a central simple subalgebra of D. Thus $D \cong (\mathfrak{U} \otimes_{\mathbb{Q}} K) \otimes_K A$ where $A = C_D(\mathfrak{U} \otimes_{\mathbb{Q}} K)$.

$$[D:K] = [(\mathfrak{U} \otimes_{\mathbb{Q}} K) \otimes_K A:K]$$
$$n^2 = [U \otimes_{\mathbb{Q}} K:K][A:K]$$
$$n^2 = 4[A:K]$$
$$\left(\frac{n}{2}\right)^2 = [A:K] .$$

<u>Lemma 2.14</u>. If $\operatorname{ind}(D) = \exp(D)$, then $n/2$ is odd.

<u>Proof</u>. Since A has index $n/2$ and $\exp(A) \mid \operatorname{ind}(A)$,

$$[A]^{n/2} = [K].$$

Suppose $n/2 = n'$ is even. Then $[\mathfrak{U}] \in B(\mathbb{Q})$ satisfies $[\mathfrak{U}]^{n'} = [\mathbb{Q}]$. Using the homomorphism from $B(\mathbb{Q})$ to $B(K)$ we have $[\mathfrak{U}] \mapsto [\mathfrak{U} \otimes_{\mathbb{Q}} K]$, and thus $[\mathfrak{U} \otimes_{\mathbb{Q}} K]^{n'} = [K]$. Now

$$\begin{aligned} [D]^{n'} &= [\mathfrak{U} \otimes_{\mathbb{Q}} K]^{n'} \cdot [A]^{n'} \\ &= [K] \cdot [K] \\ &= [K]. \end{aligned}$$

Thus $\exp(D) \leq n' < n$ contrary to assumption. Therefore $n/2$ is odd.

Lemma 2.15. If $\operatorname{ind}(D) = \exp(D)$ then $\alpha \in K$.

Proof.
$$\begin{aligned} D &\supseteq v(G) \\ &\cong (\mathbb{Q}(\varepsilon_u), \sigma_{-1}, -1). \end{aligned}$$

Thus $\varepsilon_u \in D$. We recall that if L is a field, $L \subseteq D$, then $[L:K] \mid \operatorname{ind}(D)$.

Suppose $[K(\varepsilon_u):K] = 4$. Then $4 \mid n$, so $n/2$ is even which contradicts the previous lemma. Thus $[K(\varepsilon_u):K] = 1$ or 2. If it is one then we are done, so we assume $[K(\varepsilon_u):K] = 2$.

If $u = 5$, then K contains *the* quadratic extension of $\mathbb{Q}(\varepsilon_u)$ which is $\mathbb{Q}(\alpha)$.

If $u = 8$, then K must contain one of three quadratic extensions of $\mathbb{Q}(\varepsilon_u)$ which are $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\varepsilon_4)$, and $\mathbb{Q}(\sqrt{-2})$. But if K contains one of the latter two then either

$$-1 = (\varepsilon_4)^2$$

or

$$-1 = (\sqrt{-2})^2 + (1)^2$$

so

$$\mathbb{U} \otimes_{\mathbb{Q}} K \cong (K)_2$$

and thus

$$\begin{aligned} D &\cong (K)_2 \otimes_K A \\ &\cong (A)_2 \end{aligned}$$

and so is not a division ring. Thus K contains $\mathbb{Q}(\alpha)$.

If K is an algebraic number field then $\operatorname{ind}(D) = \exp(D)$ for every K-division ring so the previous result is an extension of Lemma 2.10. We complete this section with:

<u>Proposition 2.16</u>. If K is a field of characteristic zero for which index equals exponent then G is K-adequate if and only if $\alpha \in K$ and $-1 \neq a^2 + b^2$ for all $a, b \in K$.

<u>Proof</u>. By the previous lemma we may assume $\alpha \in K$. Then G is K-adequate if and only if

$$v(G) \otimes_{\mathbb{Q}(a)} K \cong (\mathbb{U} \otimes_{\mathbb{Q}} \mathbb{Q}(a)) \otimes_{\mathbb{Q}(a)} K$$

$$\cong \mathbb{U} \otimes_{\mathbb{Q}} K$$

is a division ring. The proof is completed by an application of Proposition 2.6.

III. INVARIANTS OF CERTAIN $G_{m,r}$ GROUPS

1. The Schur Subgroup

In this chapter we shall determine the invariants of the minimal division algebra $v(G)$ for certain groups G satisfying the conditions of Theorem 1.10.

If a $G_{m,r}$ group is a subgroup of a division ring then

$$v(G_{m,r}) \cong (\mathbb{Q}(\varepsilon_m), \sigma_r, \varepsilon_s)$$

is of a special type. The center $Z_{m,r}$ of $v(G_{m,r})$ is the fixed field of σ_r, which has index n in $\mathbb{Q}(\varepsilon_m)$ and contains $\mathbb{Q}(\varepsilon_s)$ [2, p. 364]. Thus $Z_{m,r}$ is a subfield of a cyclotomic field.

Definition. The Schur subgroup $S(K)$ of the Brauer group $B(K)$ consists of those classes which contain a simple component of the group algebra $K(G)$ for some finite group G.

Evidently $[v(G_{m,r})] \in S(Z_{m,r})$. By [3, Theorem 1], if p is a rational prime (finite or infinite) and $\mathfrak{y}_1, \mathfrak{y}_2$ are primes of $Z_{m,r}$ dividing p, then

$$\text{l.i.}_{\mathfrak{y}_1} v(G_{m,r}) = \text{l.i.}_{\mathfrak{y}_2} v(G_{m,r}) .$$

This common index is called the p-local index of $v(G_{m,r})$. The following result shows that the invariants of $v(G_{m,r})$ are "uniformly distributed".

Proposition 3.1. If $v(G_{m,r})$ has p-local index v, then each of the values u/v where $0 < u < v$ and $(u, v) = 1$ occurs equally often as Hasse invariants of $v(G_{m,r})$ at primes over p. Moreover if $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are primes of $Z_{m,r}$ dividing p, then

$$\operatorname{inv}_{\mathfrak{P}_1} v(G_{m,r}) = \operatorname{inv}_{\mathfrak{P}_2} v(G_{m,r})$$

if and only if

$$\mathfrak{P}_1 \cap \mathbb{Q}(\varepsilon_v) = \mathfrak{P}_2 \cap \mathbb{Q}(\varepsilon_v).$$

Proof. This is just a restatement of [4, Corollaries 1 and 2] for the special case of $v(G_{m,r})$.

We will see that these tools along with the well known fact that the only primes which ramify from $\mathbb{Q}$ to $\mathbb{Q}(\varepsilon_m)$ occur at primes p dividing m [15, Theorem 9.2, p. 42] allow us to compute explicitly the invariants of $v(G_{m,r})$ for certain of the $G_{m,r}$ groups.

2. $G_{2p,-1}$ Where p is an Odd Prime

Let p be an odd prime. Setting $m = 2p$ and $r = -1$ gives $n = s = 2$ and $t = p$. Thus (r, m, t, s, n) is an Amitsur quintuple satisfying condition C). By Theorem 1.10 $G_{2p,-1}$ is a subgroup of a division ring of type 1). Since $\mathcal{Q}(\varepsilon_{2p}) = \mathcal{Q}(\varepsilon_p)$ the center of $v(G_{2p,-1})$ is the fixed field of index two in $\mathcal{Q}(\varepsilon_p)$. This is easily seen to be $\mathcal{Q}(\varepsilon_p + \varepsilon_p^{-1})$ which is totally real.

The index of $v(G_{2p,-1})$ is two, hence its exponent is two, and as we have seen previously the nonzero invariants all have value $1/2$.

The prime (p) is the only finite prime which ramifies from $\mathcal{Q}$ to $\mathcal{Q}(\varepsilon_p)$, and it is totally ramified. Let $\mathfrak{P}$ be the prime of $Z_{2p,-1}$ extending (p). Let ∞_i $i = 1, \ldots, p-1/2$ be the (real) infinite primes of $Z_{2p,-1}$. By Proposition 2.1 the nonzero invariants occur at $\mathfrak{P}$ or ∞_i. Since $v(G_{2p,-1})$ has nonzero invariants Property 1.3 implies $\mathrm{inv}_{\infty_i} v(G_{2p,-1}) = 1/2$ for some j. But then by Proposition 3.1, $\mathrm{inv}_{\infty_i} v(G_{2p,-1}) = 1/2$ for all i. Finally Property 1.3 determines the invariants of $v(G_{2p,-1})$ according as $(p-1)/2$ is odd or even. In summary we have

$$\mathrm{inv}_{\mathfrak{p}}\, v(G_{2p,-1}) = \begin{cases} 1/2 & \text{if } \mathfrak{p} = \infty_i \\ 0 & \text{otherwise} \end{cases} \tag{3.2}$$

if $p \equiv 1 \pmod 4$; and

$$(3.3) \qquad \operatorname{inv}_{\mathfrak{y}} v(G_{2p,-1}) = \begin{cases} 1/2 & \text{if } \mathfrak{y} = \mathfrak{B} \text{ or } \infty_i \\ 0 & \text{otherwise} \end{cases}$$

if $p \equiv 3 \pmod 4$.

3. $G_{2^{\lambda+i}p,r}$ Where $p \equiv 1 \pmod 4$

Let p be an odd prime with $p \equiv 1 \pmod 4$. Let $\lambda = \beta(2, p-1)$ so $2^{\lambda} || p-1$. We note that since $4|p-1$, $\lambda \geq 2$. Let i be a non-negative integer and set

$$m = 2^{\lambda+i}p$$

$$s = 2^{\lambda+i}$$

$$t = p$$

$$n = 2^j \quad \text{where} \quad 1 \leq j \leq \lambda$$

Lemma 3.4. There exists an integer r such that

i) $r \equiv 1 \pmod{2^{\lambda+i}}$

and ii) $[r, p] = 2^j$.

Proof. Since $2^j | p-1$, there exists an integer x with $1 < x < p$ such that x has order $2^j \pmod p$.[8]

[8] Since $a^{p-1/2^j}$, where a is a generator of the cyclic group $\mathbb{Z}_p^{\bullet}$, has order 2^j in $\mathbb{Z}_p^{\bullet}$, $x = a^{p-1/2^j} \pmod p$ will do.

Let $r_k = x + kp$, $k \in \mathbb{Z}$. Then r_k has order $2^j \pmod p$ for all k. Since $(2, p) = 1$ there exist integers u, v such that

$$up + v2^{\lambda+i} = 1 .$$

$$(x-1)up + (x-1)v2^{\lambda+i} = x - 1$$

$$(x-1)v2^{\lambda+i} = (x-(x-1)up) - 1$$

$$(x-1)v2^{\lambda+i} = r_{(1-x)u} - 1$$

$$r_{(1-x)u} \equiv 1 \pmod{2^{\lambda+i}}$$

Thus $r = r_{(1-x)u}$ fulfills the requirements.

Since

$$r \equiv 1 \pmod{2^{\lambda+i}}$$

$$r^{2^j} \equiv 1 \pmod{2^{\lambda+i}} .$$

Also

$$r^{2^j} \equiv 1 \pmod p,$$

so

$$r^{2^j} \equiv 1 \pmod m.$$

If

$$r^c \equiv 1 \pmod m,$$

then

$$r^c \equiv 1 \pmod p,$$

so $2^j \mid c$ since r has order $2^j \pmod p$. This shows r has order $2^j \pmod m$. Thus (r, m, t, s, n) is an Amitsur quintuple satisfying condition C). We will show $G_{m, r}$ satisfies Theorem

1.10 by showing it is of type 2a).

We have $\alpha = 1$. So $mp^{-\alpha} = 2^{\lambda+i}$. Since $r \equiv 1 \pmod{2^{\lambda+i}}$, $n_p = 1$. Since $q = 2$, $q \nmid n_p$ as required. It remains to show that

$$\beta(2, s) \geq \beta(2, p-1) + \beta(2, \gamma_0)$$

where $\gamma_0 = [p, 2^{\lambda+i}]$. We begin with the following number theoretic result.

Lemma 3.5. Let p be a prime such that $p \nmid q$, $p^t || q-1$ and $p^t \geq 3$. Then $p^{t+f} || q^{p^f} - 1$ for any $f \geq 0$.

Proof. The proof is by induction on f. If $f = 0$ this is trivial, so we assume the result holds for $f > 0$.

$$\frac{q^{p^{f+1}} - 1}{q^{p^f} - 1} = \frac{(q^{p^f})^p - 1}{q^{p^f} - 1}$$

Let

$$g(x) = \frac{x^p - 1}{x - 1}$$

$$= x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Substituting $x = q^{p^f}$ gives

$$q^{p^{f+1}} - 1 = (q^{p^f} - 1)g(q^{p^f})$$

By induction $p^{t+f} || q^{p^f} - 1$, so it suffices to show $p || g(q^{p^f})$.

Since $p^t \geq 3$ and p is prime, $t \geq 1$.

$$p | q-1$$

$$q \equiv 1 \pmod p$$

$$q^{p^f} \equiv 1 \pmod p.$$

$$\begin{aligned} g(q^{p^f}) &= (q^{p^f})^{p-1} + (q^{p^f})^{p-2} + \ldots + (q^{p^f}) + 1 \\ &\equiv \underbrace{1 + 1 + \ldots + 1 + 1}_{p \text{ times}} \pmod p \\ &\equiv 0 \pmod p \end{aligned}$$

Thus $p | g(q^{p^f})$. We must show $p^2 \nmid g(q^{p^f})$.

Case 1. $t > 1$. Then $p^2 | q - 1$, so $q \equiv 1 \pmod{p^2}$. Using the above argument gives

$$g(q^{p^f}) \equiv p \pmod{p^2}$$

$$g(q^{p^f}) \not\equiv 0 \pmod{p^2}$$

$$p^2 \nmid g(q^{p^f}).$$

Case 2. $t = 1$. Then $p | q - 1$, $p^2 \nmid q - 1$. So $q = 1 + kp$ where $p \nmid k$.

$$q^{p^f} = (1+kp)^{p^f}$$

$$= \sum_{n=0}^{p^f} \binom{p^f}{n}(kp)^n$$

$$= 1 + \binom{p^f}{1}kp + \sum_{n=2}^{p^f-1} \binom{p^f}{n}(kp)^n + (kp)^{p^f} .$$

$$q^{p^f} - 1 = p^f kp + p^{f+2}[\cdot] + (kp)^{p^f} .$$

Since $p^t \geq 3$ for all t, $p \geq 3$. By assumption $f \geq 1$, so $f + 2 \leq p^f$, and thus $p^{f+2} | p^{p^f}$. [9/]

$$q^{p^f} - 1 = p^{f+1}k + p^{f+2}[\cdot] .$$

If $p^{f+2} | q^{p^f} - 1$, then $p^{f+2} | p^{f+1}k$ and so $p|k$ contrary to assumption. Thus $p^{f+2} = p^{t+f+1} \nmid q^{p^f} - 1$. This completes the proof of the lemma.

By definition, γ_0 is the least positive integer f such that $p^f \equiv 1 \pmod{2^{\lambda+i}}$. By hypothesis, $2^\lambda || p-1$ and $2^\lambda \geq 3$. Thus from

[9/] Consider $h(x) = p^x - (x+2)$ defined on $[1, \infty)$. Then $h'(x) = p^x \ln p - 1$. Since $p \geq 3$, $p > e$, so $\ln p > 1$. Since $x \geq 1$, $p^x \geq 1$, so $h'(x) > 0$. Thus $h(x) \geq 0$ for all $x \geq 1$. In particular $p^f \geq f + 2$ for all positive integers f.

the previous lemma, $2^{\lambda+i}||p^{2^i}-1$. This shows $1 \leq f \leq 2^i$. We show by induction on i, that $f = 2^i$:

If $i = 0$, then since $2^{\lambda}||p-1$, we have $f = 2^0 = 1$.

If $i = 1$, then since $2^{\lambda+1}\nmid p-1$ and $2^{\lambda+1}|p^2-1$, $f = 2^1 = 2$.

Now suppose $i > 1$. Since $2^{\lambda+i}\nmid p-1$, $f > 1$. Thus $1 < f \leq 2^i$. Suppose $f < 2^i$. Then $2^{\lambda+i}|p^f-1$. But $2^{\lambda+i}|p^{2^i}-1$, so $2^{\lambda+i}|(p^{2^i}-1) - (p^f-1)$.

$$2^{\lambda+i}|p^{2^i} - p^f$$

$$2^{\lambda+i}|p^f(p^{2^i-f}-1)$$

$$2^{\lambda+i}|p^{2^i-f}-1\ .$$

By the definition of f,

$$f \leq 2^i-f$$

$$2f \leq 2^i$$

$$f \leq 2^{i-1}\ .$$

Since $2^{\lambda+i}|p^f-1$, $2^{\lambda+i-1}|p^f-1$ and so by induction $f \geq 2^{i-1}$. But $f|2^i$ so $f = 2^{i-1}$. But this gives $2^{\lambda+i}|p^{2^{i-1}}-1$ which contradicts the previous lemma.[10] Thus $f = 2^i$, as claimed.

[10] Since $\lambda > 1$ and $i > 1$, $\lambda + i > 2$. Thus $\lambda + i - 1 > 1$ and so $2^{\lambda+i-1} \geq 3$. By the lemma $2^{\lambda+i-1}||p^{2^{i-1}}-1$.

Now,

$$\begin{aligned}\beta(2, s) &= \lambda + i \\ &= \beta(2, p-1) + \beta(2, \gamma_0)\end{aligned}$$

and so $G_{m,r}$ is a subgroup of a division ring. Actually, the following result shows we have done much more than determine that $G_{m,r}$ is a subgroup of a division ring.

Theorem 3.6. If $m = p^s n$ with $(p, n) = 1$, then the factorization of (p) in $\mathcal{Q}(\varepsilon_m)$ is $(\mathcal{B}_1 \cdots \mathcal{B}_r)^{\phi(p^s)}$ where $\mathcal{B}_1, \ldots, \mathcal{B}_r$ are the distinct primes extending (p) of relative degree f and $fr = \phi(n)$ with f the smallest positive integer such that $p^f \equiv 1 \pmod{n}$.

Proof. See [18, Theorem 7-2-4 and 7-4-3].

For our purposes $m = 2^{\lambda+i}p$, and so we must find the least positive integer f such that $p^f \equiv 1 \pmod{2^{\lambda+i}}$. But this is γ_0! So $f = 2^i$. Now,

$$\begin{aligned} fr &= \phi(2^{\lambda+i}) \\ 2^i r &= 2^{\lambda+i-1} \\ r &= 2^{\lambda-1} \quad (\text{or} \quad \phi(2^\lambda)).\end{aligned}$$

Recalling that $Z_{m,r}$ is the field of index $n = 2^j$ containing $\mathcal{Q}(\varepsilon_{2^{\lambda+i}})$ we have determined the factorization of (p) in $Z_{m,r}$

(see Figure 1). Let $\mathfrak{N}_1, \ldots, \mathfrak{N}_{\phi(2^\lambda)}$ be the primes of $\mathbb{Q}(\varepsilon_{2^{\lambda+i}})$ dividing (p). Since each $\mathfrak{N}_k$ ramifies completely from $\mathbb{Q}(\varepsilon_{2^{\lambda+i}})$ to $\mathbb{Q}(\varepsilon_m)$ its unique extension $\mathfrak{B}_k$ of $Z_{m,r}$ ramifies from $Z_{m,r}$ to $\mathbb{Q}(\varepsilon_m)$. Since $Z_{m,r} \subseteq \mathbb{Q}(\varepsilon_{2^{\lambda+i}})$ and $\lambda \geq 2$, $Z_{m,r}$ is totally complex. Thus $v(G_{m,r})$ has invariant zero at the infinite primes of $Z_{m,r}$. Since (2) is the only prime other than (p) which ramifies from $\mathbb{Q}$ to $\mathbb{Q}(\varepsilon_m)$ the only primes for which $v(G_{m,r})$ may have nonzero invariants are $\mathfrak{B}_k$ and those extending (2). We now show they occur only at $\mathfrak{B}_k$.

$$\begin{tikzcd}
 & \mathbb{Q}(\varepsilon_{2^{\lambda+i}p}) \arrow[d, dash, "2^j"] & (p) = (\mathfrak{Y}_1 \cdots \mathfrak{Y}_{\phi(2^\lambda)})^{p-1} \\
\text{totally ramified} & Z_{m,r} \arrow[d, dash, "p-1/2^j"] & (p) = (\mathfrak{B}_1 \cdots \mathfrak{B}_{\phi(2^\lambda)})^{p-1/2^j} \\
 & \mathbb{Q}(\varepsilon_{2^{\lambda+i}}) \arrow[d, dash, "2^i"] & (p) = \mathfrak{N}_1 \cdots \mathfrak{N}_{\phi(2^\lambda)} \\
\text{inertial} & & \\
 & \mathbb{Q}(\varepsilon_{2^\lambda}) \arrow[d, dash, "2^{\lambda-1}"] & (p) = \mathfrak{P}_1 \cdots \mathfrak{P}_{\phi(2^\lambda)} \\
\text{splits completely} & & \\
 & \mathbb{Q} & (p)
\end{tikzcd}$$

$p \equiv 1 \pmod 4, \quad \lambda = \beta(2, p-1)$

Figure 1. Factorization of (p) in $\mathbb{Q}(\varepsilon_{p2^{\lambda+i}})$, $p \equiv 1 \pmod 4$.

Lemma 3.7. If p and q are primes, then any prime of $\mathbb{Q}(\varepsilon_{q^a})$ extending (q) is unramified from $\mathbb{Q}(\varepsilon_{q^a})$ to $\mathbb{Q}(\varepsilon_{q^a p})$.

Proof. Since $(q, p) = 1$ we have $\mathbb{Q}(\varepsilon_{q^a p}) = \mathbb{Q}(\varepsilon_{q^a})(\varepsilon_p)$. Let $f(x) = \mathrm{Irr}(\varepsilon_p, \mathbb{Q}(\varepsilon_{q^a}))$. Then $f(x) \mid x^p - 1$. Let $\mathfrak{P}$ be a prime of $\mathbb{Q}(\varepsilon_{q^a})$ extending (q). Since $\mathfrak{P}$ is totally ramified from $\mathbb{Q}$ to $\mathbb{Q}(\varepsilon_{q^a})$, $f(\mathfrak{P}/(q)) = 1$, and thus $\overline{\mathbb{Q}(\varepsilon_{q^a})}_{\mathfrak{P}} \cong \mathbb{Z}_q$ the field of q elements. Since $x^p - 1$ has no multiple roots in $\tilde{\mathbb{Z}}_q$, neither does $f(x)$. By [15, Theorem 7.6, p. 32] $\mathfrak{P}$ is unramified from $\mathbb{Q}(\varepsilon_{q^a})$ to $\mathbb{Q}(\varepsilon_{q^a})(\varepsilon_p)$.

Let $\mathfrak{a}$ be a prime of $Z_{m,r}$ extending (2). If $\mathfrak{a}$ ramifies from $Z_{m,r}$ to $\mathbb{Q}(\varepsilon_m)$, then $\mathfrak{P} = \mathfrak{a} \cap \mathbb{Q}(\varepsilon_{2^{\lambda+i}})$ ramifies from $\mathbb{Q}(\varepsilon_{2^{\lambda+i}})$ to $\mathbb{Q}(\varepsilon_m)$ which contradicts the lemma. Thus $\mathfrak{a}$ is unramified from $Z_{m,r}$ to $\mathbb{Q}(\varepsilon_m)$. This shows that the nonzero invariants of $v(G_{m,r})$ occur only at $\mathfrak{B}_k$. We give an explicit description of the invariants for the cases $n = 2$ and $n = 2^\lambda$.

If $n = 2$, by Lemma 2.2, all invariants have value $1/2$. By Proposition 3.1,

$$(3.8) \qquad \mathrm{inv}_{\mathfrak{P}}\, v(G_{m,r}) = \begin{cases} 1/2 & \text{if } \mathfrak{P} = \mathfrak{B}_1, \ldots, \mathfrak{B}_{\phi(2^\lambda)} \\ 0 & \text{otherwise.} \end{cases}$$

Let $n = 2^\lambda$. Since the exponent of $v(G_{m,r})$ is 2^λ, it must have p-local index 2^λ. By Proposition 3.1 the invariants must be of the form $\mathrm{inv}_{\mathfrak{B}_k} v(G_{m,r}) = u/2^\lambda$ with $0 < u < 2^\lambda$, and $(u, 2^\lambda) = 1$. Since there are $\phi(2^\lambda)$ such primes and $\phi(2^\lambda)$ choices for u this determines the invariants. Since invariants are defined (mod 1) we alter this as follows: Let $\{a, -a_1, a_2, -a_2, \ldots\}$ be a complete set of representatives for units modulo 2^λ. Then, without loss of generality,

(3.9)
$$\mathrm{inv}_{\mathfrak{B}_{2k}} v(G_{m,r}) = -\frac{a_k}{2^\lambda}$$

$$\mathrm{inv}_{\mathfrak{B}_{2k-1}} v(G_{m,r}) = \frac{a_k}{2^\lambda}$$

$$k = 1, \ldots, \phi(2^\lambda)/2$$

$$\mathrm{inv}_{\mathfrak{y}} v(G_{m,r}) = 0 \quad \text{if} \quad \mathfrak{y} \neq \mathfrak{B}_k \quad \text{for some} \quad k .$$

4. $G_{2^{\lambda+i}p, r}$ Where $p \equiv 3 \pmod 4$

Let p be a prime, $p \equiv 3 \pmod 4$, with $p \equiv 1 + 2 + \ldots + 2^j \pmod{2^{j+2}}$, $j \geq 1$.[11] Let $\lambda = j+2$, and set

[11] We will show in Chapter V that every prime p with $p \equiv 3 (\mathrm{mod}\ 4)$ can be expressed uniquely in this form.

$$m = 2^{\lambda+i}p$$

$$s = 2^{\lambda+i}$$

$$t = p$$

$$n = 2,$$

where i is a non-negative integer. By Lemma 3.4 there exists r such that $r \equiv 1 \pmod{2^{\lambda+i}}$ and $[r, p] = 2$, and by the argument which follows that lemma, $[r, m] = 2$. Thus (r, m, t, s, n) is an Amitsur quintuple satisfying condition C). We will show $G_{m,r}$ satisfies Theorem 1.10 by showing it is of type 2b).

As in the previous section $n_p = 1$ so $q \nmid n_p$ for $q = 2$. Thus we need only verify (since $s \equiv 0 \pmod 4$) that

$$\beta(2, s) \geq j + 1 + \max(1, \beta(2, \gamma_0))$$

where $\gamma_0 = [p, 2^{\lambda+i}]$. Simultaneously, by Theorem 3.6, this will determine the factorization of (p) in $\mathbb{Q}(\varepsilon_m)$. It is more convenient to solve this problem via the latter approach.

We know $(p) = (\mathfrak{y}_1 \cdots \mathfrak{y}_r)^{p-1}$ in $\mathbb{Q}(\varepsilon_{2^{\lambda+i}p})$ where $f = f(\mathfrak{y}_i/p)$ is $[p, 2^{\lambda+i}]$ and $fr = \phi(2^{\lambda+i})$. We show by induction on i, that $f = 2^{i+1}$. The proof relies on a result from algebraic number theory.

Theorem 3.10. If $m = 2^s$ $(s \geq 3)$, then $\mathrm{Gal}(\mathbb{Q}(\varepsilon_m)/\mathbb{Q})$ is isomorphic to the direct product of two cyclic groups; the first of order two with $\rho: \varepsilon_m \mapsto \varepsilon_m^{-1}$ as generator, and the second of order 2^{s-2} with $\tau: \varepsilon_m \mapsto \varepsilon_m^5$ as generator.

Proof. See [10, Corollary 7-1-2].

By [16, p. 205], $\mathrm{Gal}(Q(\varepsilon_m)/Q) \cong \mathbb{Z}_m^{\bullet}$ under the isomorphism which takes $\sigma \mapsto r$ where $\sigma: \varepsilon_m \mapsto \varepsilon_m^r$. This fact and the previous theorem show that $\mathbb{Z}_{2^s}^{\bullet} \cong \langle -1 \rangle \times \langle 5 \rangle$ for $s \geq 3$. We are now able to accomplish the induction.

Induction Hypothesis. $f = 2^{i+1}$ (i.e. $2^{\lambda+i} \mid p^{2^{i+1}} - 1$) and $2^{\lambda+i+1} \nmid p^{2^{i+1}} - 1$.

Proof. Since $\lambda \geq 3$ and $p \equiv 3 \pmod 4$, $p \not\equiv 1 \pmod{2^{\lambda}}$. For $i = 0$, this shows $f > 1$.

$$
\begin{aligned}
p &\equiv 1 + 2 + \ldots + 2^j \pmod{2^{j+2}} \\
p &\equiv 2^{j+1} - 1 \pmod{2^{j+2}} \\
p^2 &\equiv (2^{j+1} - 1)^2 \pmod{2^{j+2}} \\
p^2 &\equiv 2^{2j+2} - 2(2^{j+1}) + 1 \pmod{2^{j+2}} \\
&\equiv 2^j 2^{j+2} - 2^{j+2} + 1 \\
&\equiv 1 \pmod{2^{j+2}}
\end{aligned}
$$

Thus

$$f = 2 = 2^{i+1}.$$

If $2^{\lambda+1} | p^2-1$, then $\overline{p}$ has order two in $\mathbb{Z}^{\bullet}_{2^{\lambda+1}}$. Thus $\overline{p} = 1, -1, 5^{2^j}$, or -5^{2^j} in $\mathbb{Z}^{\bullet}_{2^{\lambda+1}}$. So $\overline{p} = 1$ or -1 in $\mathbb{Z}^{\bullet}_{2^{\lambda}}$. If

$$\overline{p} = -1 \text{ in } \mathbb{Z}^{\bullet}_{2^{\lambda}},$$

then

$$p \equiv -1 \pmod{2^{\lambda}}$$

$$p+1 \equiv 0 \pmod{2^{\lambda}}$$

But

$$p \equiv 1 + 2 + \ldots + 2^j \pmod{2^{\lambda}},$$

so

$$p \equiv 2^{j+1} - 1 \pmod{2^{\lambda}},$$

and

$$p+1 \equiv 2^{j+1} \pmod{2^{\lambda}},$$

a contradiction. If $\overline{p} = 1$ in $\mathbb{Z}^{\bullet}_{2^{\lambda}}$, then

$$p \equiv 1 \pmod{2^{\lambda}},$$

and so

$$p \equiv 1 \pmod{4},$$

contrary to assumption. Thus we conclude $2^{\lambda+1} \nmid p^2-1$.

Now, suppose the induction hypothesis holds for $i \geq 1$. If $2^{\lambda+i+1} | p^f-1$, then $2^{\lambda+i} | p^f-1$, so $f \geq 2^{i+1}$. Since $2^{\lambda+i+1} \nmid p^{2^{i+1}}-1$, $f > 2^{i+1}$.

$$\begin{aligned} fr &= \phi(2^{\lambda+i+1}) \\ &= 2^{\lambda+i}. \end{aligned}$$

Since $r \geq 2^j$ and $f > 2^{i+1}$ (recall $\lambda = j+2$) we must have $r = 2^j$ and $f = 2^{i+2}$. Thus $f = 2^{(i+1)+1}$. Finally we show $2^{\lambda+i+2} \nmid p^{2^{i+2}} - 1$.

Suppose not. Then $\bar{p}^{2^{i+2}} = 1$ in $\mathbb{Z}^{\cdot}_{2^{\lambda+i+2}}$. Write $\bar{p} = \pm 5^k$, $1 \leq k \leq 2^{\lambda+i}$.

$$(\pm 5^k)^{2^{i+2}} = 1$$

$$(5^{2^{i+1}})^k = 1.$$

Since 5 has order $2^{\lambda+i}$, $2^j | k$. Thus

$$\bar{p} = \pm 5^{2^j \ell} \quad \text{in} \quad \mathbb{Z}^{\cdot}_{2^{\lambda+i+2}}$$

so

$$p \equiv \pm 5^{2^j \ell} \pmod{2^{\lambda+i+2}},$$

and

$$p \equiv \pm 5^{2^j \ell} \pmod{2^{\lambda}}.$$

But 5 has order 2^j in $\mathbb{Z}^{\cdot}_{2^\lambda}$, so $p \equiv \pm 1 \pmod{2^\lambda}$. As in the $i = 0$ case this gives a contradiction. Thus the induction hypothesis holds for $i+1$ and the proof is complete.

By definition $\gamma_0 = [p, 2^{\lambda+i}]$, which we have seen is 2^{i+1}.

Now,

$$\begin{aligned}\beta(2, s) &= \lambda + i \\ &= j + 2 + i \\ &= j + 1 + \beta(2, \gamma_0) \\ &\geq j + 1 + \max(1, \beta(2, \gamma_0))\end{aligned}$$

so $G_{m,r}$ is a subgroup of a division ring.

The induction hypothesis and Theorem 3.6 give the factorization of (p) in $Z_{m,r}$, the field of index two containing $\mathbb{Q}(\varepsilon_{2^{\lambda+i}})$ (see Figure 2). As $\lambda \geq 2$, $Z_{m,r}$ is totally complex so the invariants are zero at all infinite primes. By Lemma 3.7 any prime extending (2) is unramified from $Z_{m,r}$ to $\mathbb{Q}(\varepsilon_m)$. By Lemma 2.2 and Proposition 3.1 we have

$$(3.11) \qquad \operatorname{inv}_{\mathfrak{y}} v(G_{m,r}) = \begin{cases} 1/2 & \text{if } \mathfrak{y} = \mathfrak{B}_i \quad i = 1, \ldots, 2^j \\ 0 & \text{otherwise.} \end{cases}$$

The invariants of the $G_{m,r}$ groups presented in this chapter are summarized in Table 2.

$$\begin{tikzcd}
\mathbb{Q}(\varepsilon_{2^{\lambda+i}p}) \arrow[d, dash, "2"] & (p) = (\mathfrak{Y}_1 \cdots \mathfrak{Y}_{2^j})^{p-1} \\
Z_{m,r} \arrow[d, dash, "p-1/2"] & (p) = (\mathfrak{B}_1 \cdots \mathfrak{B}_{2^j})^{p-1/2} \\
\mathbb{Q}(\varepsilon_{2^{\lambda+i}}) \arrow[d, dash, "2^{j+1+i}"] & (p) = \mathfrak{n}_1 \cdots \mathfrak{n}_{2^j} \\
\mathbb{Q} & (p)
\end{tikzcd}$$

$p \equiv 3 \pmod 4$, $\lambda = j + 2$

$p \equiv 1 + 2 + \ldots + 2^j \pmod{2^{j+2}}$, $j \geq 1$.

Figure 2. Factorization of (p) in $\mathbb{Q}(\varepsilon_{p2^{\lambda+i}})$, $p \equiv 3 \pmod 4$.

Table 2. Invariants of $v(G_{m,r})$ for $G = G_{m,r}$ groups with $m = 2^a p$.

1) $p \equiv 1 \pmod 4$

i) $a = 1$

$$\mathrm{inv}_{\mathcal{Y}}\, v(G) = \begin{cases} 1/2 & \text{if } \mathcal{Y} \text{ is infinite} \\ 0 & \text{otherwise} \end{cases}$$

ii) $a > 1$, $\lambda = \beta(2, p-1)$

$a = \lambda + i$

$$\mathrm{inv}_{\mathcal{Y}}\, v(G) = \begin{cases} -a_k/2^{\lambda} & \text{if } \mathcal{Y} = \mathcal{B}_{2k} \\ a_k/2^{\lambda} & \text{if } \mathcal{Y} = \mathcal{B}_{2k-1} \\ 0 & \text{otherwise} \end{cases}$$

for $n = 2^{\lambda}$; $k = 1, \ldots, \phi(2^{\lambda})/2$

$$\mathrm{inv}_{\mathcal{Y}}\, v(G) = \begin{cases} 1/2 & \text{if } \mathcal{Y} = \mathcal{B}_j \\ 0 & \text{otherwise} \end{cases}$$

for $n = 2$ where $\mathcal{B}_1, \ldots, \mathcal{B}_{\phi(2^{\lambda})}$ are the primes of $Z_{m,r}$ dividing (p).

2) $p \equiv 3 \pmod 4$

i) $a = 1$

$$\mathrm{inv}_{\mathcal{Y}}\, v(G) = \begin{cases} 1/2 & \text{if } \mathcal{Y} \text{ is infinite or } \mathcal{Y} \text{ divides } (p) \\ 0 & \text{otherwise} \end{cases}$$

ii) $a > 1$, $\lambda = j + 2$

$p \equiv 1 + 2 + \ldots + 2^j \pmod{2^{j+2}}$

$a = \lambda + i$

$$\mathrm{inv}_{\mathcal{Y}}\, v(G) = \begin{cases} 1/2 & \text{if } \mathcal{Y} \text{ divides } (p) \\ 0 & \text{otherwise} \end{cases}$$

for $n = 2$.

IV. EXISTENCE THEOREMS OVER ALGEBRAIC NUMBER FIELDS

1. Factorization of Primes in Composites

In this chapter we assume that K is an algebraic number field. Our goal is to prove that for every such K there exists a noncyclic group which is K-adequate. Much of the preliminary work has been completed in Chapters II and III.

If G is K-adequate then $v(G)$ is contained in a K-division ring D, and so $w(G) = v(G) \otimes_Z KZ$, where Z is the center of $v(G)$, is a subdivision ring of D. To determine the invariants of $w(G)$ we require information on the factorization of primes of Z in KZ.

Suppose K and L are algebraic number fields, and $\mathfrak{P}$ is a (finite) prime of $K \cap L$.

Lemma 4.1. If $\mathfrak{P}$ splits completely in L and $\mathfrak{n}$ is a prime of K extending $\mathfrak{P}$, then $\mathfrak{n}$ splits completely in KL.

Proof. Clearly we may assume $L, K \neq K \cap L$. By the Primitive Element Theorem [16, Theorem 14, p. 185], $L = (K \cap L)(\alpha)$ and so $KL = K(\alpha)$. Let $f(x) = \mathrm{Irr}(\alpha, K \cap L)$. By [15, Exercise 1, p. 92] since $\mathfrak{P}$ splits completely in L, $f(x)$ splits completely in $(K \cap L)_{\mathfrak{P}}$. Thus $f(x)$ splits completely in $K_{\mathfrak{n}}$ and so splits completely in KL.

We next drop the restriction that $\mathfrak{B}$ split completely in L.

Lemma 4.2. If $\mathfrak{q}$ is a prime of L extending $\mathfrak{B}$ then there exists a prime $\mathfrak{P}$ of KL extending $\mathfrak{n}$ such that $\mathfrak{P} \cap L = \mathfrak{q}$.

Proof. Let $(p) = \mathfrak{B} \cap \mathbb{Q}$, and let $\widetilde{\mathbb{Q}}_p$ be a fixed algebraic closure of $\mathbb{Q}_p$. Then $(K \cap L)_{\mathfrak{B}} \subset \widetilde{\mathbb{Q}}_p$. Let $\psi: L \to \widetilde{\mathbb{Q}}_p$ be the valuation corresponding to $\mathfrak{q}$ which extends the $\mathfrak{B}$-adic valuation of $K \cap L$. Let $\phi: K \to \widetilde{\mathbb{Q}}_p$ be the $\mathfrak{n}$-adic valuation of K. We must show that $\psi = \hat{\phi}|_L$ for some extension $\hat{\phi}: KL \to \widetilde{\mathbb{Q}}_p$ of ϕ. Let $\psi(\alpha) = \beta \in \widetilde{\mathbb{Q}}_p$. Since $\psi|_{K\cap L} = \phi|_{K \cap L}$ $\phi(f(x)) = \psi(f(x))$. Now,

$$\begin{aligned} 0 &= \phi(f(\alpha)) \\ &= \psi(f(\alpha)) \\ &= \psi(f(\psi(\alpha)) \\ &= \psi(f(\beta)), \end{aligned}$$

so β is a root of $\phi(f(x))$. We let $\hat{\phi}$ be the valuation of $KL = K(\alpha)$ defined by

$$\hat{\phi}|_K = \phi$$

and

$$\hat{\phi}(\alpha) = \beta .$$

2. The Main Theorem

Let K be an algebraic number field. Let $b \geq 1$ satisfy $K \supseteq Q(\varepsilon_{2^b})$, $K \not\supseteq \mathbb{Q}(\varepsilon_{2^{b+1}})$.

Lemma 4.3. There exists an odd prime p such that

1) $p \equiv 1 \pmod{2^b}$ but $p \not\equiv 1 \pmod{2^{b+1}}$.

2) p is unramified in K.

3) If π is a prime of K extending p then $[K_\pi : \mathbb{Q}_p]$ is a power of two.

4) There exists a prime π of K extending p such that $K_\pi = \mathbb{Q}_p$.

5) a) If $b = 1$, then $K \cap \mathbb{Q}(\varepsilon_p) = \mathbb{Q}$.

b) If $b > 1$, and d is maximal with $[K_\pi : \mathbb{Q}_p] = 2^d$ for π a prime of K extending p; and Z is the subfield of index 2^b in $\mathbb{Q}(\varepsilon_{p2^{b+d}})$, $Z \supseteq \mathbb{Q}(\varepsilon_{2^{b+d}})$, then $K \cap Z = \mathbb{Q}(\varepsilon_{2^b})$.

Proof. Let E be the normal closure of K over $\mathbb{Q}$, and let $L = \mathbb{Q}(\varepsilon_{2^{b+1}})$.

Case 1. $L \not\subseteq E$.

By Bauer's Theorem [10, Theorem 9.1.3] there exist infinitely many primes which split completely in E but not in EL. Let p be such an odd prime with $\mathbb{Q}(\varepsilon_p) \cap E = \mathbb{Q}$. Since p splits completely in $\mathbb{Q}(\varepsilon_{2^b})$ but not in L,

$$p \equiv 1 \pmod{2^b} ,$$

but

$$p \not\equiv 1 \pmod{2^{b+1}} .$$

Since p splits completely, 2), 3) and 4) hold. Also $[K_\pi : \mathbb{Q}_p] = 1$ for all π, so $d = 0$. Thus

a) $K \cap \mathbb{Q}(\varepsilon_p) = \mathbb{Q}$

b) $K \cap \mathbb{Q}(\varepsilon_{p2^{b+d}}) = K \cap \mathbb{Q}(\varepsilon_{2^b})$
$= \mathbb{Q}(\varepsilon_{2^b})$.

Case 2. $L \subset E$ (see Figure 3).

Since $L \not\subset K$,

$$\begin{aligned}[KL:K] &= [L:K \cap L] \\ &= [L:\mathbb{Q}(\varepsilon_{2^b})] \\ &= 2\end{aligned}$$

Since KL/K is Galois, there exists $\sigma \in \mathrm{Gal}(KL/K)$ of order two. Let τ be an automorphism of E extending σ. Say τ has order $2^c t$ with $(2,t) = 1$ and $c \geq 1$. Thus there exists $u, v \in \mathbb{Z}$ with $u2^c + vt = 1$.

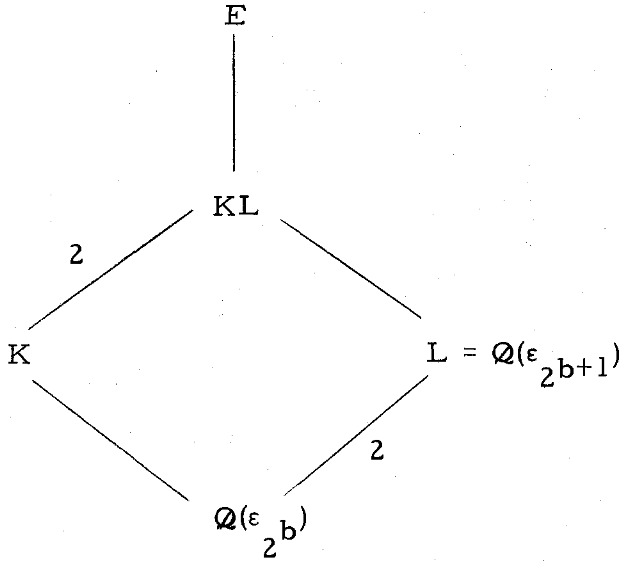
E
KL
2
K
L = $\mathbb{Q}(\varepsilon_{2^{b+1}})$
2
$\mathbb{Q}(\varepsilon_{2^b})$

Figure 3. Subfields of E.

$$\begin{aligned} \tau^{vt}|_{KL} &= (\tau|_{KL})^{vt} \\ &= \sigma^{vt} \\ &= \sigma^{1-u2^c} \\ &= \sigma \circ (\sigma^{2^c})^t \\ &= \sigma \circ 1 \\ &= \sigma \end{aligned}$$

Thus τ^{vt} extends σ. Also

$$\begin{aligned} (\tau^{vt})^{2^c} &= (\tau^{2^c t})^v \\ &= 1 . \end{aligned}$$

Replacing τ by τ^{vt} we may assume τ has order 2^c, $c \geq 1$.

Let $K = \mathbb{Q}(\theta)$ and $f(x) = \mathrm{Irr}(\theta, \mathbb{Q})$. We view $\mathrm{Gal}(E/\mathbb{Q})$ as a group of permutations of the roots of $f(x)$. By the Tchebotarev Density Theorem [15, Theorem 10.4, p. 182] there are infinitely many primes p of $\mathbb{Q}$ for which τ determines the Frobenius automorphism at p of E over $\mathbb{Q}$.

Choose one such p. If τ has cycle type $[n_1, \ldots, n_r]$ then in $\mathbb{Q}_p[x]$ $f(x)$ factors into irreducible factors of degrees $n_1, \ldots, n_r$. Now, since τ has order 2^c, each n_i is a power of two. Since τ extends σ, and σ fixes K, $\sigma(\theta) = \theta$. Thus some $n_i = 1$. Since the local degrees of the completions of K over $\mathbb{Q}_p$ are precisely $n_1, \ldots, n_r$ 2), 3) and 4) hold. Since there is a prime of local degree one over p and $K \supset \mathbb{Q}(\varepsilon_{2^b})$, p splits completely in $\mathbb{Q}(\varepsilon_{2^b})$.[12] Let π be a prime of K with $K_\pi = \mathbb{Q}_p$, and let $\mathfrak{P}$ be the prime of E dividing (p) which determines the Frobenius automorphism τ. Thus

$$\tau = \left[\frac{E/\mathbb{Q}}{\mathfrak{P}}\right].$$

Let $\mathfrak{N}$ be a prime of KL extending π and $\mathfrak{Y}$ a prime of E extending $\mathfrak{N}$. By [15, Proposition 6.8, p. 29] there exists

[12] If π satisfies $K_\pi = \mathbb{Q}_p$, then $\varepsilon_{2^b} \in K \subseteq K_\pi = \mathbb{Q}_p$. Since $\mathbb{Q}_p$ contains the $(p-1)$st roots of unity, $2^b | p-1$, and thus p splits completely in $\mathbb{Q}(\varepsilon_{2^b})$.

$\rho \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\rho(\mathfrak{B}) = \mathfrak{y}$. By [15, Property 2.2., p. 98]

$$\tau = \rho\left[\frac{E/\mathbb{Q}}{\mathfrak{y}}\right]\rho^{-1}.$$

Let $\mathfrak{P} = \mathfrak{B} \cap KL$. Then by [15, Property 2.4, p. 99] since $\tau|_{KL} = \sigma$,

$$\begin{aligned}\sigma &= \left[\frac{KL/\mathbb{Q}}{\mathfrak{P}}\right] \\ &= \rho\left[\frac{KL/\mathbb{Q}}{\mathfrak{n}}\right]\rho^{-1}.\end{aligned}$$

Since $f(\pi/p) = 1$ by [15, Property 2.3, p. 99]

$$\left[\frac{KL/\mathbb{Q}}{\mathfrak{n}}\right] = \left[\frac{KL/K}{\mathfrak{n}}\right].$$

Since σ has order two, $\left[\frac{KL/K}{\mathfrak{n}}\right]$ has order two, and thus by [15, Property 2.6, p. 100] π does not split completely in KL. By Lemma 4.1, p does not split completely in L, and thus $p \not\equiv 1 \pmod{2^{b+1}}$. This shows 1) holds.

Again choosing p such that $E \cap \mathbb{Q}(\varepsilon_p) = \mathbb{Q}$, we see 5a) holds. Finally, let d be maximal with $[K_\pi : \mathbb{Q}_p] = 2^d$. Since d depends only on τ[13] and not on p, we may choose p so that 5b) holds. This completes the proof of the lemma.

[13] $d = \max_i \beta(2, n_i)$.

We are now ready to prove a "best possible" result.

Theorem 4.5. If K is an algebraic number field then there exists a noncyclic K-adequate group of even-order.

Proof. Let b and p be as in the previous lemma.

Case 1. $b = 1$.

If $-1 \neq a^2 + c^2$ for all $a, c \in K$ then by Proposition 2.6 the quaternions Q^* are K-adequate. In particular the quaternions are $\mathbb{Q}$-adequate. Thus we may assume $-1 = a^2 + c^2$ in K and hence K is totally complex with $2 | [K: \mathbb{Q}]$.[14]

Let $m = 2p$, $n = s = 2$, and $r = -1$. By (3.3) $G = G_{m,r}$ is a subgroup of a division ring and by 1) of the previous lemma, $p \not\equiv 1 \pmod 4$ so

$$\mathrm{inv}_{\mathfrak{B}}\, v(G) = \frac{1}{2}$$

$$\mathrm{inv}_{\infty_i}\, v(G) = \frac{1}{2} \quad i = 1, \ldots, p-1/2$$

$$\mathrm{inv}_{\mathfrak{y}}\, v(G) = 0 \quad \text{otherwise,}$$

where $\mathfrak{B}$ is the prime of $Z = Z_{m,r}$ extending p.

[14] $[K: \mathbb{Q}] > 1$. If $2 \nmid [K: \mathbb{Q}]$, then $[K: \mathbb{Q}]$ is odd so K has a real embedding, σ. But then $-1 = \sigma(a)^2 + \sigma(c)^2$ in $\mathbb{R}$.

Let $\pi_1, \ldots, \pi_\ell$ be the primes of K extending p. Then

$$(4.6) \qquad [K: \mathbb{Q}] = \sum_{i=1}^{\ell} e(\pi_i/p) f(\pi_i/p)$$

$$= \sum_{i=1}^{\ell} f(\pi_i/p) \ ,$$

since p is unramified in K. By 4) of the lemma we assume without loss of generality $[K_{\pi_1} : \mathbb{Q}_p] = 1$. Then

$$[K: \mathbb{Q}] = 1 + \sum_{i=2}^{\ell} [K_{\pi_i} : \mathbb{Q}_p].$$

Since $[K_{\pi_i} : \mathbb{Q}_p]$ is a power of two for all i and $[K:\mathbb{Q}]$ is even there must exist $u > 1$ for which $[K_{\pi_u} : \mathbb{Q}_p] = 1$. Without loss of generality $\pi_1, \ldots, \pi_v$ satisfy $[K_{\pi_j} : \mathbb{Q}_p] = 1$. Then by (4.6) v is even.

Let $\mathfrak{P}_i$ be a prime of KZ extending π_i for $1 \leq i \leq v$ (see Figure 4).

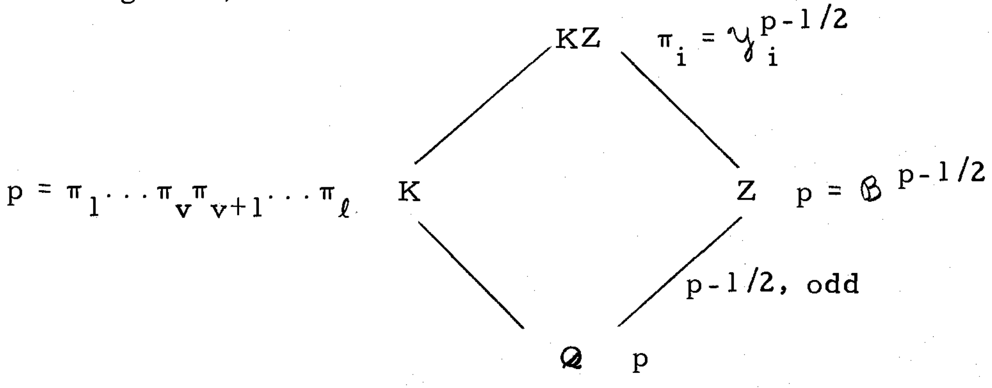
KZ
$\pi_i = \mathfrak{P}_i^{p-1/2}$
$p = \pi_1 \cdots \pi_v \pi_{v+1} \cdots \pi_\ell$
K
Z
$p = \mathfrak{B}^{p-1/2}$
p-1/2, odd
$\mathbb{Q}$ p

Figure 4. Factorization of p in KZ.

Since KZ/K is Galois

$$
\begin{aligned}
e(\mathfrak{P}_i/\pi_i)f(\mathfrak{P}_i/\pi_i) \mid [KZ:K] & \\
&= [Z:Q]\ {}^{15/} \\
&= \frac{p-1}{2}\,.
\end{aligned}
$$

Thus $e(\mathfrak{P}_i/\pi_i)$, $f(\mathfrak{P}_i/\pi_i)$ are odd.

$$[KZ_{\mathfrak{P}_i}:\mathbb{Q}_p] = [KZ_{\mathfrak{P}_i}:K_{\pi_i}][K_{\pi_i}:\mathbb{Q}_p]$$

$$[KZ_{\mathfrak{P}_i}:Z_{\mathfrak{B}}][Z_{\mathfrak{B}}:\mathbb{Q}_p] = e(\mathfrak{P}_i/\pi_i)f(\mathfrak{P}_i/\pi_i)$$

$$[KZ_{\mathfrak{P}_i}:Z_{\mathfrak{B}}]\underbrace{\frac{p-1}{2}}_{\text{odd}} = \underbrace{e(\mathfrak{P}_i/\pi_i)f(\mathfrak{P}_i/\pi_i)}_{\text{odd}}\,.$$

This shows $[KZ_{\mathfrak{P}_i}:Z_{\mathfrak{B}}]$ is odd.[16] Let $w(G) = v(G) \otimes_Z KZ$

$$
\begin{aligned}
\operatorname{inv}_{\mathfrak{P}_i} w(G) &\equiv \operatorname{inv}_{\mathfrak{B}} V(G)\,[KZ_{\mathfrak{P}_i}:Z_{\mathfrak{B}}] \\
&\equiv \frac{1}{2}\,[KZ_{\mathfrak{P}_i}:Z_{\mathfrak{B}}] \\
&\equiv \frac{1}{2} \pmod 1,
\end{aligned}
$$

for $i = 1, \ldots, v$.

[15] Recall $Z \subseteq \mathbb{Q}(\varepsilon_p)$ and $\mathbb{Q}(\varepsilon_p) \cap K = \mathbb{Q}$.

[16] In fact it equals one for $1 \leq i \leq v$.

By Theorem 2.9, $w(G)$ is a KZ-division ring.

$$e(\mathfrak{P}_j/\pi_j) \leq [KZ:K], \qquad \text{for all} \quad j$$

$$e(\mathfrak{P}_j/\pi_j)e(\pi_j/p) = e(\mathfrak{P}_j/\mathfrak{B})e(\mathfrak{B}/p)$$

$$e(\mathfrak{P}_j/\pi_j) = e(\mathfrak{P}_j/\mathfrak{B})\frac{p-1}{2} \quad .$$

So

$$e(\mathfrak{P}_j/\pi_j) \geq \frac{p-1}{2} \ ,$$

and hence

$$e(\mathfrak{P}_j/\pi_j) = \frac{p-1}{2} \qquad \text{for all} \quad j.$$

An easy calculation shows

$$[KZ_{\mathfrak{P}_j}:Z_{\mathfrak{B}}] = f(\pi_j/p) \qquad \text{for all} \quad j,$$

and since KZ is totally complex and Z is totally real,

$$\text{inv}_{\mathfrak{P}_j} w(G) = \frac{1}{2}\ , \qquad 1 \leq j \leq v$$

$$\text{inv}_{\mathfrak{n}} w(G) = 0\ , \qquad \text{for all other primes.}$$

Let D be the K-division ring with

$$\text{inv}_{\pi_i} D = \frac{(-1)^i}{p-1}\ , \qquad 1 \leq i \leq v$$

and

$$\text{inv}_{\wp} D = 0 \qquad \text{otherwise.}$$

Since v is even, (1.3) holds and the existence of D is guaranteed by Theorem 1.7.

Consider $K(\varepsilon_p)$. Since $K \cap \mathbb{Q}(\varepsilon_p) = \mathbb{Q}$,

$$[K(\varepsilon_p) : K] = [\mathbb{Q}(\varepsilon_p) : \mathbb{Q}]$$

$$= p-1 .$$

Since π_i is completely ramified from K to $K(\varepsilon_p)$, for $1 \leq i \leq v$ we have

$$\begin{aligned}
\mathrm{inv}_{\mathcal{P}_i} D \otimes_K K(\varepsilon_p) &\equiv \mathrm{inv}_{\pi_i} D\, [K(\varepsilon_p)_{\mathcal{P}_i} : K_{\pi_i}] \\
&\equiv \frac{(-1)^i}{p-1}\ e(\mathcal{P}_i/\pi_i) \\
&\equiv \frac{(-1)^i}{p-1} \cdot p-1 \\
&\equiv 0 \pmod 1,
\end{aligned}$$

where $\mathcal{P}_i$ extends π_i. Theorem 1.9 shows $K(\varepsilon_p)$ is a maximal subfield of D. Thus $D \supseteq \mathbb{Q}(\varepsilon_p) \supseteq Z$, and so $D \supseteq KZ$, hence $D \supset C_D(KZ)$. By Lemma 1.1, $C_D(KZ) \sim D \otimes_K KZ$. Thus

$$\begin{aligned}
\mathrm{inv}_{\mathcal{Y}_i} C_D(KZ) &\equiv \mathrm{inv}_{\mathcal{Y}_i} D \otimes_K KZ \\
&\equiv \mathrm{inv}_{\pi_i} D\, [KZ_{\mathcal{Y}_i} : K_{\pi_i}] \\
&\equiv \frac{(-1)^i}{p-1}\ \frac{p-1}{2}
\end{aligned}$$

$$\equiv \frac{1}{2} \pmod 1$$

$$\equiv \mathrm{inv}_{\mathcal{Y}_i} w(G)$$

for $1 \leq i \leq v$. By (1.5), $C_D(KZ) \cong w(G)$ and thus G is K adequate.

Case 2. $b > 1$.

Let d be as in 5b) of the lemma. Set $m = 2^{b+d}p$, $s = 2^{b+d}$, and $n = 2^b$. By 1) of the lemma $b = \beta(2, p-1)$. By Section 3 of Chapter III we know there exists r such that $G = G_{m,r}$ is a subgroup of a division ring and moreover

$$\mathrm{inv}_{\mathfrak{B}_{2w}} v(G) = \frac{-a_w}{2^b},$$

$$\mathrm{inv}_{\mathfrak{B}_{2w-1}} v(G) = \frac{a_w}{2^b}$$

with

$$w = 1, \ldots, \phi(2^b)/2.$$

We note that the field Z of 5) of the lemma is precisely $Z_{m,r}$ since $Z_{m,r}$ is the fixed field of $\sigma_r : \varepsilon_m \mapsto \varepsilon_m^r$ containing $\mathbb{Q}(\varepsilon_s)$, and r has order $n \pmod m$, so $|< \sigma_r >| = n$ (see Figure 5).

Now,

$$[Z_{\mathfrak{P}_i} : \mathbb{Q}_p] = f(\mathfrak{P}_i/p)e(\mathfrak{P}_i/p)$$

$$= 2^d \, \frac{p-1}{2^b}.$$

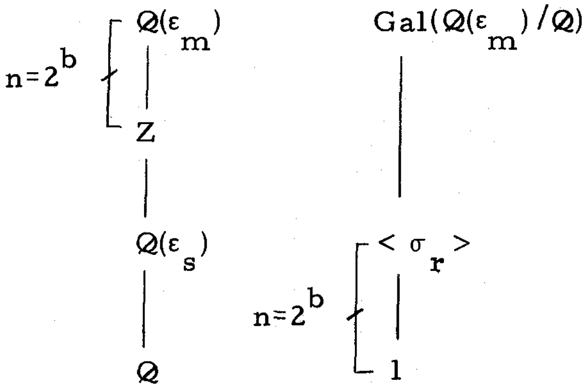
$\mathbb{Q}(\varepsilon_m)$
$n=2^b$
Z
$\mathbb{Q}(\varepsilon_s)$
$\mathbb{Q}$
$\mathrm{Gal}(\mathbb{Q}(\varepsilon_m)/\mathbb{Q})$
$< \sigma_r >$
$n=2^b$
1

Figure 5. Fixed field of σ_r.

If π is a prime of K extending p, then $Z_{\mathfrak{P}_i} \supseteq K_\pi$ since the unramified extensions of $\mathbb{Q}_p$ are unique and $\beta(2, f(\pi/p)) \leq d$ (see Figure 6).

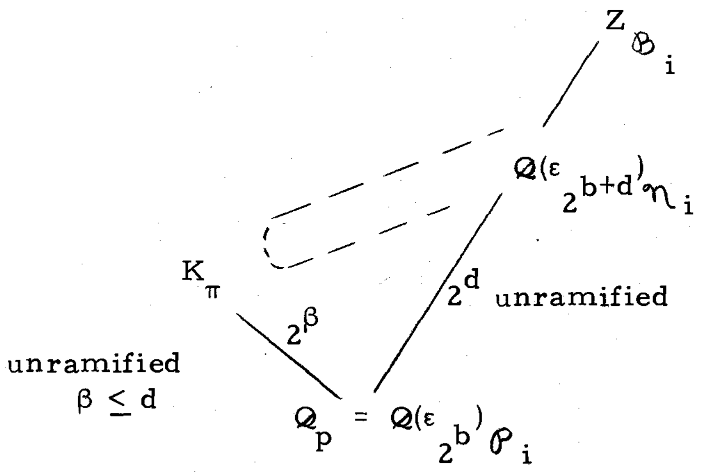
$Z_{\mathfrak{P}_i}$
$\mathbb{Q}(\varepsilon_{2^{b+d}})_{\mathfrak{n}_i}$
K_π
2^β
2^d unramified
unramified
$\beta \leq d$
$\mathbb{Q}_p = \mathbb{Q}(\varepsilon_{2^b})_{\mathcal{P}_i}$

Figure 6. Completions at primes extending p.

Thus if $\mathfrak{A}_i$ is a prime of KZ extending $\mathfrak{B}_i$, we have

$$[KZ_{\mathfrak{A}_i} : Z_{\mathfrak{B}_i}] = 1.$$

Therefore $\mathfrak{B}_i$ splits completely in KZ. Let $u = [KZ: Z]$ and let $\mathfrak{B}_{i1}, \ldots, \mathfrak{B}_{iu}$ be the complete set of primes of KZ over $\mathfrak{B}_i$ $i = 1, \ldots, \phi(2^b)$.

We now show $w(G) = v(G) \otimes_K KZ$ is a division ring.

$$\operatorname{inv}_{\mathfrak{B}_{cj}} w(G) \equiv \operatorname{inv}_{\mathfrak{B}_c} v(G) \; [KZ_{\mathfrak{B}_{cj}} : Z_{\mathfrak{B}_c}]$$

$$\equiv \operatorname{inv}_{\mathfrak{B}_c} v(G) .$$

Thus $w(G)$ has exponent and index equal 2^b, and so by Theorem 2.9, $w(G)$ is a KZ-division ring. We note that

$$\operatorname{inv}_{\mathfrak{B}_{cj}} w(G) = \operatorname{inv}_{\mathfrak{B}_c} v(G)$$

for $c = 1, \ldots, \phi(2^b)$ and $j = 1, \ldots, u$ and $\operatorname{inv}_{\mathcal{Y}} w(G) = 0$ otherwise.

Let $\pi_{ij} = \mathfrak{B}_{ij} \cap K$ (the π_{ij} are not necessarily distinct). Then by Lemma 4.2, $\{\pi_{ij}\}$ is a complete set of primes of K extending the primes $\mathcal{P}_i$ of $\mathbb{Q}(\varepsilon_{2^b})$. We denote π_{ij} by $\pi(i, j)$ and $K_{\pi_{ij}}$ by $K(i, j)$. Set $q(i, j) = [K(i, j): \mathbb{Q}_p]$. By 3) of the lemma

$q(i,j) = 2^{\beta_{ij}} \leq 2^d$. Define $\rho: \{\pi(i,j)\} \to \mathbb{Q}/\mathbb{Z}$ by

$$\rho(\pi(2w,j)) = \frac{-a_w q(2w,j)}{(p-1)2^d}$$

$$\rho(\pi(2w-1,j)) = \frac{a_w q(2w-1,j)}{(p-1)2^d} .$$

Claim: ρ is well-defined.

Proof: If $\pi_{ij} \neq \pi_{kj}$,

$$\mathcal{B}_{ij} \cap K \neq \mathcal{B}_{kj} \cap K$$

$$\mathbb{Q}(\varepsilon_s) \cap (\mathcal{B}_{ij} \cap K) \neq \mathbb{Q}(\varepsilon_s) \cap (\mathcal{B}_{kj} \cap K)$$

$$\mathbb{Q}(\varepsilon_s) \cap \mathcal{B}_{ij} \neq Q(\varepsilon_s) \cap \mathcal{B}_{kj}$$

$$\mathcal{P}_i \neq \mathcal{P}_k$$

so $i \neq k$, and thus

$$\rho(\pi_{ij}) \neq \rho(\pi_{kj}).$$

If

$$\pi_{ij} = \pi_{ik} ,$$

then

$$q(i,j) = q(i,k)$$

so

$$\rho(i,j) = \rho(i,k).$$

Claim: $\sum_{i,j} \rho(\pi(i,j)) \equiv 0 \pmod 1$.

Proof: Let $g(x) = \mathrm{Irr}(\theta, \mathbb{Q}(\varepsilon_{2^b}))$ where $K = \mathbb{Q}(\theta)$. Since $\mathbb{Q}(\varepsilon_{2^b})_{\mathcal{P}_i} = \mathbb{Q}_p$, for fixed i, the values of $q(i,j)$ correspond to the degrees of the irreducible factors of $g(x)$ in $\mathbb{Q}_p[x]$. Thus for $i \neq k$ the set of $q(i,j)$ counting multiplicities is the same as the set of values of $q(k,j)$ counting multiplicities. Letting $i = 2w$ and $k = 2w-1$ gives

$$\sum_{i,j} \rho(\pi(i,j)) \equiv 0 \pmod 1 .$$

Let D be the K-division ring with $\mathrm{inv}_{\mathfrak{y}} D = 0$ if $\mathfrak{y} \nmid \mathfrak{B}$ and $\mathrm{inv}_{\pi(i,j)} D = \rho(\pi(i,j))$ for all i and j. The existence of D is guaranteed by the previous claim and Theorem 1.7.

Since $\{-a_1, a_1, \ldots\}$ is a complete set of representatives of units modulo 2^b, we may choose i so that $i = 2w$ and $a_w = 1$. Let π_ℓ satisfy 4) of the lemma so $[K_{\pi_\ell} : \mathbb{Q}_p] = 1$. By Lemma 4.2 one of the primes $\mathfrak{B}_{ij}$ of KZ extending $\mathfrak{B}_i$ extends π_ℓ. Thus $q(i,j) = 1$ and

$$\rho(\pi(i,j)) = \frac{1}{(p-1)2^d}$$

for some i,j. By (1.6) $\exp(D) = (p-1)2^d$.

Consider $F = KZ(\varepsilon_{2^{2b+d}})$. We will show F is a maximal subfield of D. We first show it has the proper dimension over K (see Figure 7).

$$[KZ(\varepsilon_{2^{2b+d}}): K] = [Z(\varepsilon_{2^{2b+d}}): \mathbb{Q}(\varepsilon_{2^b})]$$
$$= (p-1)2^d .$$

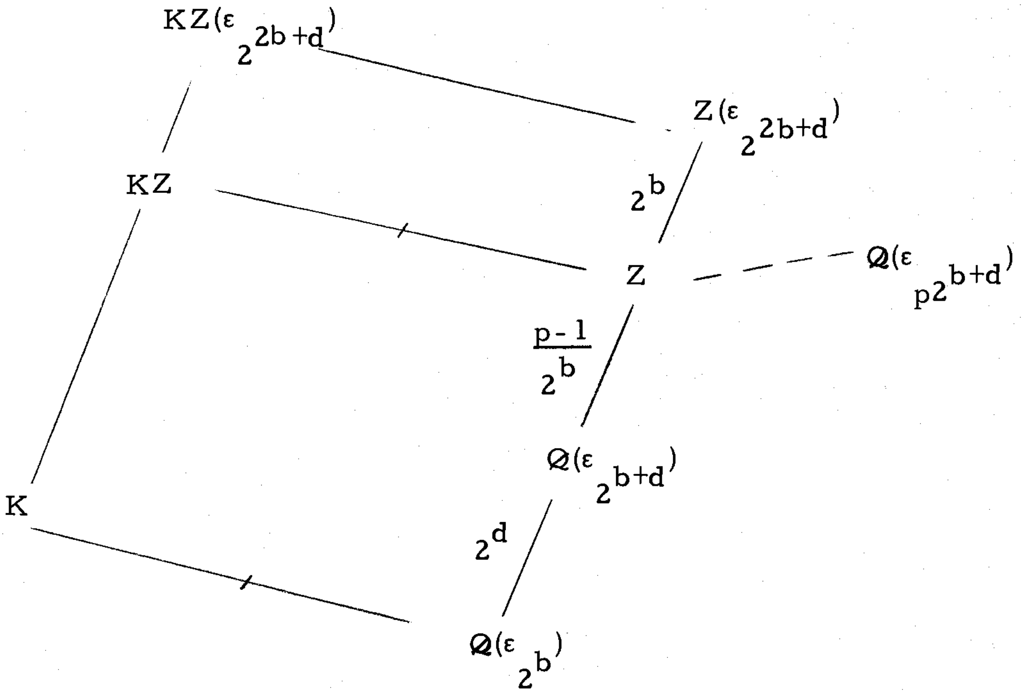
$KZ(\varepsilon_{2^{2b+d}})$
$Z(\varepsilon_{2^{2b+d}})$
KZ
2^b
Z
$\mathbb{Q}(\varepsilon_{p2^{b+d}})$
$\frac{p-1}{2^b}$
$\mathbb{Q}(\varepsilon_{2^{b+d}})$
K
2^d
$\mathbb{Q}(\varepsilon_{2^b})$

Figure 7. Subfields from $\mathbb{Q}(\varepsilon_{2^b})$ to F.

By Theorem 1.9 we need only show F splits D. Figure 8 gives a diagram that will aid in the computation of local degrees. Inspection shows it is just Figure 1 with λ replaced by b and i by $b+d$.

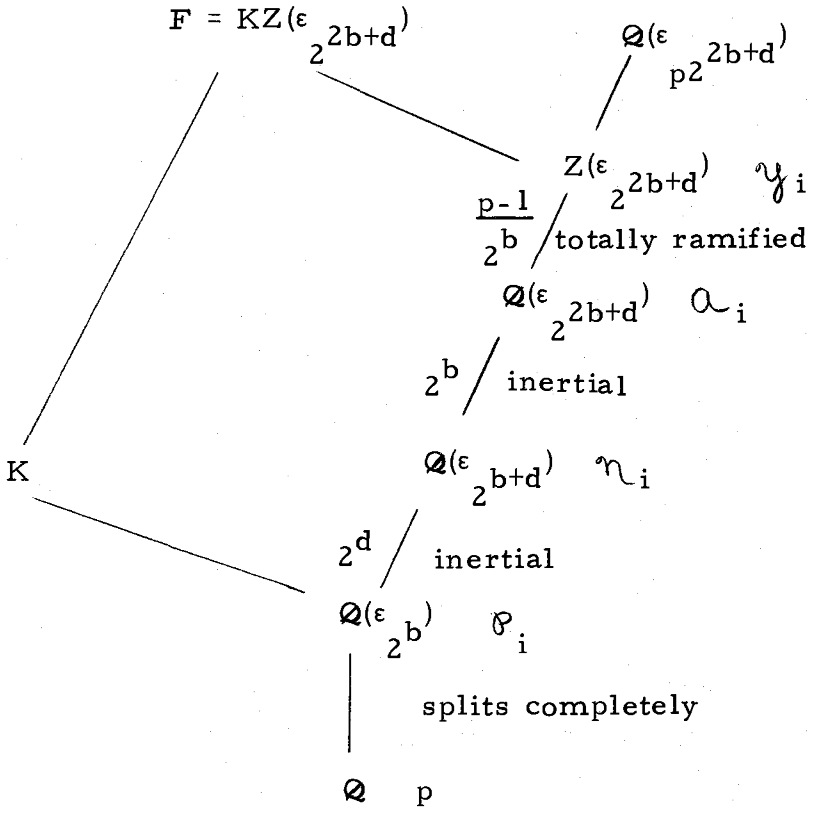
$F = KZ(\varepsilon_{2^{2b+d}})$
$\mathbb{Q}(\varepsilon_{p2^{2b+d}})$
$Z(\varepsilon_{2^{2b+d}})$ $\mathfrak{y}_i$
$\frac{p-1}{2^b}$
totally ramified
$\mathbb{Q}(\varepsilon_{2^{2b+d}})$ $\mathfrak{a}_i$
2^b
inertial
K
$\mathbb{Q}(\varepsilon_{2^{b+d}})$ $\mathfrak{n}_i$
2^d
inertial
$\mathbb{Q}(\varepsilon_{2^b})$ $\mathfrak{p}_i$
splits completely
$\mathbb{Q}$ p

Figure 8. Subfields from $\mathbb{Q}$ to F.

Claim: F splits D.

Proof: If γ extends π_{ij} then

$$\operatorname{inv}_\gamma D \otimes_K F \equiv \operatorname{inv}_{\pi_{ij}} D\,[F_\gamma : K_{\pi_{ij}}]$$

$$\equiv \rho(i,j)[F_\gamma : K_{\pi_{ij}}]\,.$$

$$[F_\gamma : K_{\pi_{ij}}][K_{\pi_{ij}} : \mathbb{Q}_p] = [F_\gamma : Z(\varepsilon_{2^{2b+d}})_{\mathfrak{y}_i}](p-1)2^d$$

Since

$$[K_{\pi_{ij}} : \mathbb{Q}_p] = q(i,j) ,$$

$$[F_\gamma : K_{\pi_{ij}}] = [F_\gamma : Z(\varepsilon_{2^{2b+d}})_{\mathfrak{Y}_i}] \frac{(p-1)2^d}{q(i,j)}$$

Thus

$$\begin{aligned} \mathrm{inv}_\gamma D \otimes_K F &\equiv \pm \frac{a_w q(i,j)}{(p-1)2^d} [F_\gamma : K_{\pi_{ij}}] \\ &\equiv \pm a_w [F_\gamma : Z(\varepsilon_{2^{2b+d}})_{\mathfrak{Y}_i}] \\ &\equiv 0 \pmod 1). \end{aligned}$$

Thus F splits D.

Since F is a maximal subfield of D, $F \supset KZ$, and hence $D \supset KZ$. Therefore $D \supset C_D(KZ)$ and by Lemma 1.1, $C_D(KZ) \sim D \otimes_K KZ$. Computing local degrees, gives

$$[KZ_{\mathfrak{B}_{ij}} : K_{\pi_{ij}}][K_{\pi_{ij}} : \mathbb{Q}_p] = [KZ_{\mathfrak{B}_{ij}} : Z_{\mathfrak{B}_i}][Z_{\mathfrak{B}_i} : \mathbb{Q}(\varepsilon_{2^b})_{\mathfrak{P}_i}] .$$

$$[KZ_{\mathfrak{B}_{ij}} : K_{\pi_{ij}}]q(i,j) = 1 \ (\frac{2^d(p-1)}{2^b})$$

Thus

$$[KZ_{\mathfrak{B}_{ij}} : K_{\pi_{ij}}] = \frac{2^d(p-1)}{q(i,j)2^b}$$

$$\begin{aligned}
\mathrm{inv}_{\mathcal{B}_{ij}} C_D(KZ) &\equiv \mathrm{inv}_{\mathcal{B}_{ij}} D \otimes_K KZ \\
&\equiv \mathrm{inv}_{\pi_{ij}} D\,[KZ_{\mathcal{B}_{ij}} : K_{\pi_{ij}}] \\
&\equiv \rho(\pi(i,j))\,\frac{2^d(p-1)}{q(i,j)2^b} \\
&\equiv \frac{-a_w q(i,j)}{(p-1)2^d}\,\frac{2^d(p-1)}{q(i,j)2^b} \\
&\equiv \frac{-a_w}{2^b} \pmod 1 \\
&\equiv \mathrm{inv}_{\mathcal{B}_{2w,j}} w(G), \quad \text{for} \quad i = 2w.
\end{aligned}$$

A similar calculation holds for $i = 2w-1$. Since $C_D(KZ)$ has nonzero invariants and is contained in D it is a division ring. Further since $C_D(KZ) \sim w(G)$ we have $C_D(KZ) \cong w(G)$ and thus $w(G)$ is contained in D and so G is K-adequate. This completes the proof of the theorem.

It is of interest to note that in the case where $b = 1$ and K is complex the prime p of the lemma satisfied $p \equiv 3 \pmod 4$. This is in fact a necessary condition since if $p \equiv 1 \pmod 4$ then by (3.2) the nonzero invariants of $v(G)$ occur at infinite primes. But then $v(G)$ is split by KZ, so $w(G)$ is not a division ring--a necessary condition for K-adequacy.

Also of note is the fact that examples exist for all cases covered in the lemma and theorem. They are:

1) $\mathbb{Q}(\sqrt{-15})$: Here $b = 1$ and since $-15 \equiv 1 \pmod 8$ the quaternions are K-adequate

2) $\mathbb{Q}(\sqrt{-5})$: Here $b = 1$ and since $-5 \not\equiv 1 \pmod 8$ Q^* is not K-adequate. Since $K/\mathbb{Q}$ is Galois $E = K$, and $\varepsilon_4 \notin E$

3) $\mathbb{Q}(\varepsilon_8 \sqrt[4]{2})$: Here $b = 1$ and $(\varepsilon_4 \sqrt{2})^2 + 1^2 = -1$ so Q^* is not K-adequate. Also $\varepsilon_4 \in E = \mathbb{Q}(\varepsilon_8, \sqrt[4]{2})$

4) $\mathbb{Q}(\varepsilon_4)$: Here $b > 1$, and since K is Galois, $\varepsilon_8 \notin E = K$

5) $\mathbb{Q}(\varepsilon_4, \varepsilon_8 \sqrt[4]{2})$: Here $b > 1$ and $\varepsilon_8 \in E = \mathbb{Q}(\varepsilon_8, \sqrt[4]{2})$.

The conclusion of the theorem itself is somewhat surprising in view of [8, Theorem 6] which states that a noncyclic odd-order group is K-adequate if and only if K contains a primitive odd-order root of unity. As was shown there this result is not true if K is a p-local field. We will obtain a similar result in the next chapter. Before doing so we present a result which puts the notion of K-adequacy in perspective.

3. A Contrasting Result

We have seen that for every algebraic number field K there exists a K-division ring D containing a noncyclic group. This does not say that every K-division ring has this property. In fact that is far from the truth.

Lemma 4.7. The Euler ϕ-function is bounded from below. That is; given N there exists M such that $\phi(m) > N$ whenever $m \geq M$.

Proof. Let $\pi(m)$ be the number of primes less than m, so $\pi(m) \to \infty$ as $m \to \infty$. Given N, choose M such that $\pi(M) > N$. By definition, $\phi(m)$ is the number of integers less than or equal to m which are relatively prime to m. Thus if $m \geq M$, $\phi(m) \geq \pi(M) > N$.

Theorem 4.8. Let K be an algebraic number field. Then for every $n > 1$, there exists a K-division ring D of index n such that the only finite subgroups contained in D are those contained in K.

Proof. Fix $n > 1$. Consider $\{K(\varepsilon_m) \mid m \in \mathbb{Z}^+\}$. By the previous lemma, since $[K:\mathbb{Q}] < \infty$, there exist only finitely many m_i, say $m_1, \ldots, m_r$ such that $[K(\varepsilon_{m_i}):K] \mid n$. Without loss of generality $m_1, \ldots, m_s$ satisfy $[K(\varepsilon_{m_i}):K] > 1$ (i.e., $\varepsilon_{m_i} \notin K$) and $[K(\varepsilon_{m_i}):K] \mid n$.

Claim: There exists a prime $\mathfrak{P}_i$ of K such that $\mathfrak{P}_i$ splits completely in $K(\varepsilon_{m_i})$.

Proof: It suffices to show there exists a prime p of $\mathbb{Q}$ which splits completely in $\mathbb{Q}(\varepsilon_{m_i})$. Since then any prime $\mathfrak{q}_i$ of

$K \cap \mathbb{Q}(\varepsilon_{m_i}) \subsetneqq \mathbb{Q}(\varepsilon_{m_i})$ splits completely in $\mathbb{Q}(\varepsilon_{m_i})$ and so by Lemma 4.1 any prime $\mathcal{B}_i$ of K extending $\mathcal{Y}_i$ will do.

By Dirichlet's theorem on primes in an arithmetic progression [15, Theorem 5.9, p. 138] there exist infinitely many primes of the form $1 + m_i t$. Choose one such p. Then $p \equiv 1 \pmod{m_i}$ so by Theorem 3.6, p splits completely in $\mathbb{Q}(\varepsilon_{m_i})$.

Let $\mathcal{B}_1, \ldots, \mathcal{B}_t$ $(t \leq s)$ be a distinct set of primes such that: for any j there exists i such that $\mathcal{B}_i$ splits completely in $K(\varepsilon_{m_j})$. Let ℓ be the smallest integer $(\ell \geq t)$ such that $n | \ell$. Choose finite primes $\mathcal{B}_{t+1}, \ldots, \mathcal{B}_\ell$ of K distinct from $\mathcal{B}_1, \ldots, \mathcal{B}_t$.

Let D be the K-division ring with invariants $\operatorname{inv}_{\mathcal{B}_j} D = 1/n$, $1 \leq j \leq \ell$ and zero at all other primes of K. Since (1.3) holds, the existence of D is guaranteed by Theorem 1.7. By (1.6), D has exponent n.

Suppose $G \subset D^*$, $G \not\subset K$, with $|G| < \infty$. Let $\alpha \in G$, $\alpha \notin K$. Then α has finite order and $[K(\alpha): K] | \operatorname{ind}(D) = n$, so $K(\alpha) \cong K(\varepsilon_{m_i})$ and thus $K(\varepsilon_{m_i})$ is a subfield of D. We will show this is impossible.

Extend $K(\varepsilon_{m_i})$ to a maximal subfield $L \subset D$, so $[L: K] = n$. Since L is maximal, L is a splitting field for D. Thus

$$D \otimes_K L \sim L.$$

By construction there exists j, $1 \leq j \leq t$, such that $\mathfrak{B}_j$ splits completely from K to $K(\varepsilon_{m_i})$. Let $\mathfrak{Q}_j$ be a prime of L extending $\mathfrak{B}_j$. Then

$$\operatorname{inv}_{\mathfrak{Q}_j} D \otimes_K L \equiv \operatorname{inv}_{\mathfrak{B}_j} D\,[L_{\mathfrak{Q}_j} : K_{\mathfrak{B}_j}]\,.$$

Let

$$\mathfrak{N}_j = \mathfrak{Q}_j \cap K(\varepsilon_{m_i})\,.$$

$$\begin{aligned}
[L_{\mathfrak{Q}_j} : K_{\mathfrak{B}_j}] &= [L_{\mathfrak{Q}_j} : K(\varepsilon_{m_i})_{\mathfrak{N}_j}][K(\varepsilon_{m_i})_{\mathfrak{N}_j} : K_{\mathfrak{B}_j}] \\
&= [L_{\mathfrak{Q}_j} : K(\varepsilon_{m_i})_{\mathfrak{N}_j}] \\
&\leq [L : K(\varepsilon_{m_i})] \\
&< [L : K(\varepsilon_{m_i})][K(\varepsilon_{m_i}) : K] \\
&= [L : K] \\
&= n
\end{aligned}$$

So

$$\begin{aligned}
\operatorname{inv}_{\mathfrak{Q}_j} D \otimes_K L &\equiv \frac{c}{n}\,, \qquad 1 \leq c < n \\
&\not\equiv 0 \pmod{1}.
\end{aligned}$$

This contradicts (1.4), and the proof is complete.

By 1) of Theorem 1.11 the cyclic group of order m, C_m, is K-adequate for some K. If K is an algebraic number field then in general C_m is not K-adequate. In [17, Theorem 4.2] it is shown that not every C_m is $\mathbb{Q}$-adequate. It is shown there, however, that there are infinitely many cyclic groups which are $\mathbb{Q}$-adequate.

In contrast, the previous theorem shows that there is a $\mathbb{Q}$-division ring which contains no cyclic groups other than C_2. Moreover the proof shows that up to isomorphism a K-division ring contains only finitely many cyclic groups. The phrase "up to isomorphism" is crucial as the following example shows.

The quaternions are $\mathbb{Q}$-adequate. They are contained in $\mathfrak{U}$. Thus $x^2 + 1$ has at least six solutions in $\mathfrak{U}$. By [11, Corollary 2] $x^2 + 1$ has an infinite number of solutions in $\mathfrak{U}$. Since any root $\alpha \in \mathfrak{U}$ of $x^2 + 1$ generates a group isomorphic to C_4, $\mathfrak{U}$ contains an infinite number of cyclic groups. Yet "up to isomorphism" $\mathfrak{U}$ contains only C_2, C_3, C_4 and C_6.

Again, all of the above is false for local fields. The real quaternions $\mathfrak{U}_{\mathbb{R}}$ contain the complex numbers $\mathbb{C}$ as a maximal subfield and thus $\varepsilon_m \in \mathbb{C}$ generates a group isomorphic to C_m. As noted earlier if K is p-local and D is a K-division ring of index n, then D contains a unique unramified extension of degree n, say $K(\alpha)$, and α generates a cyclic group "outside" K. We now turn to a more detailed study of p-local fields.

V. EXISTENCE THEOREMS OVER LOCAL FIELDS

1. Reductions

In this chapter we shall assume K is a p-local field, $p \neq \infty$. Our goal is to show that for every p there exist infinitely many fields K for which no noncyclic group is K-adequate. By Propositions 2.7 and 2.12, we know that if p is an odd prime, the special groups Q^*, T^*, O^*, and I^* are not K-adequate. Thus by Theorem 1.11 the only groups which can be K-adequate are those $G_{m,r}$ groups which satisfy the conditions of Theorem 1.10. But in view of [7, Theorem 1] which gives necessary and sufficient conditions for an odd-order noncyclic group to be K-adequate we may restrict our attention to the (nonempty) class of p-local fields for which no odd-order noncyclic group is K-adequate. Under these assumptions we make a reduction of the even-order groups to the cases we may handle.

Lemma 5.1. Suppose G is a noncyclic even-order group which is K-adequate. Then there exists a noncyclic subgroup $H \subset G$ with $|H| = 2^a q^b$.

Proof. From the discussion above we know that G is a $G_{m,r}$ group. Since $|G|$ is even G has a nontrivial 2-Sylow subgroup. By [2, Theorem 2] the 2-Sylow subgroup of G is either cyclic or generalized quaternion. If it is the latter then G contains the quaternion group Q^*. Since G is K-adequate, Q^* is K-adequate. This contradicts Proposition 2.7, and thus we conclude the 2-Sylow subgroup is cyclic.

Since G is solvable, G has Hall $\{p, q\}$-subgroups for every pair of primes p, q dividing $|G|$. We claim that one of these subgroups is noncyclic.

If not, then every Hall $\{p, q\}$-subgroup is cyclic. Let P be a p-Sylow subgroup of G. Then for any $q \mid |G|$, there is a q-Sylow subgroup of G contained in the centralizer in G of P, and so P is central in G. Thus every Sylow subgroup is both cyclic and normal and so G is cyclic, a contradiction.

Let H be a noncyclic Hall $\{p, q\}$-subgroup, so $|H| = p^a q^b$. If p and q are odd, then by assumption H is not K-adequate so, without loss of generality, $|H| = 2^a q^b$.

Replacing G by H we assume, $|G| = 2^a q^b$. Since the 2-Sylow subgroup of G is cyclic, G is a $G_{m,r}$ group satisfying condition C). We analyze the Amitsur quintuple on this basis.

By [2, Lemma 1] t is odd. Since $st = m$, $t \mid m$. If $t = 1$, then $s = m$, so $m = (r-1, m)$, and thus $m \mid r-1$. But then $n = 1$, so $v(G)$ is a field and so G is cyclic, a contradiction. Thus $t = q^c$, $c > 0$.

Since $(n,t) = 1$, $n = 2^d$, $d > 0$. Since $mn = |G|$, $m = 2^{a-d}q^b$. Since $t = m/s$ and $(s,t) = 1$, we must have $s = 2^{a-d}$ and $t = q^b$. Since $n|s$, $a-d \geq d$.

In summary, we have shown for $|G| = 2^a q^b$,

$$\begin{aligned} t &= q^b \\ n &= 2^d, \quad d > 0 \\ s &= 2^{a-d}, \quad a-d \geq d \\ m &= 2^{a-d}q^b . \end{aligned}$$

We replace $a-d$ by c, so $c \geq d$. We now make a further reduction.

Lemma 5.2. There exists a noncyclic subgroup H of G, H a K-adequate group, where H is a $G_{m,r}$ group with $m = 2^c q$, $s = 2^c$, $n = 2$.

Proof. From the above we know G is a $G_{m,r}$ group with $m = 2^c q^b$, $s = 2^c$, and $n = 2^d$. By definition,

$$G = \langle A, B \,|\, A^m = 1, B^n = A^{q^b}, BAB^{-1} = A^r \rangle,$$

$s = (r-1, m)$ and $n = [r, m]$.

We first show that we can reduce to the case $b = 1$. Suppose $b > 1$. Let $H_0 = \langle A^{q^{b-1}}, B\rangle$. Then $q \,|\, |H_0|$ but $q^2 \nmid |H_0|$. H_0 is noncyclic since if $B \epsilon C_{H_0}(A^{q^{b-1}})$ then

$$BA^{q^{b-1}} = A^{q^{b-1}}B$$

$$BA^{q^{b-1}}B^{-1} = A^{q^{b-1}}$$

$$(BAB^{-1})^{q^{b-1}} = A^{q^{b-1}}$$

$$(A^r)^{q^{b-1}} = A^{q^{b-1}}$$

$$rq^{b-1} \equiv q^{b-1} \pmod m$$

$$q^b | q^{b-1}(r-1)$$

$$q | r-1$$

$$q | (r-1, m)$$

$$q | s \ , \quad \text{a contradiction.}$$

H_0 is K-adequate, so H_0 is a $G_{m,r}$ group. Replacing G by H_0, we assume $G = G_{m,r}$ with $m = q2^c$, $s = 2^c$, and $n = 2^d$, where $c \geq d \geq 1$. If $d = 1$ there is nothing to prove, so we suppose $d > 1$.

Let $H = <A, B^{2^{d-1}}>$. We first show H is noncyclic. If $B^{2^{d-1}} \epsilon C_H(A)$, then $B^{2^{d-1}}A = AB^{2^{d-1}}$. By induction $B^iA = A^{r^i}B$. Applying this to $B^{2^{d-1}}A = AB^{2^{d-1}}$ gives $A^{r^{2^{d-1}}}B^{2^{d-1}} = AB^{2^{d-1}}$, so

$$A^{r^{2^{d-1}}} = A,$$

and thus

$$r^{2^{d-1}} \equiv 1 \pmod{m}.$$

So $[r, m] \leq 2^{d-1} < n$, a contradiction.

Let $\overline{B} = B^{2^{d-1}}$. This gives

$$H = <A, \overline{B} | A^{2^c q} = 1, \overline{B}^2 = A^q, \overline{B}A\overline{B}^{-1} = A^u>$$

where $u = r^{2^{d-1}}$. Now,

$$r \equiv 1 \pmod{2^c}$$

so

$$s = 2^c = (u-1, q2^c)$$

since if $q|u-1$, then

$$r^{2^{d-1}} \equiv 1 \pmod{q}$$

and $[r, m] = 2^{d-1}$, a contradiction. Since two equals the order of $u \pmod{m}$, we have $H = G_{m, r}$ with $m = q2^c$, $s = 2^c$, and $n = 2$. This completes the proof of the lemma.

Replacing G be the group H of the previous lemma, we may assume G is a $G_{m, r}$ group with those values of m, s, and n. Moreover since G is K-adequate G satisfies Theorem 1.10, and is of type 1), 2a), or 2b).[17/] The invariants of the minimal algebras for certain groups of these types were classified in Chapter III.

We must show G is one of those which were classified.

Recall $m = 2^c q$. If $c = 1$, then

$$r^2 \equiv 1 \pmod{2q},$$
$$r \not\equiv 1 \pmod{2q}.$$

Since $(m, r) = 1$, r is odd so $2 | r-1$. If $q | r-1$, then $2q | r-1$, so $r \equiv 1 \pmod{2q}$, a contradiction. Now,

$$r^2 \equiv 1 \pmod{2q}$$
$$r^2 \equiv 1 \pmod{q}$$
$$q | r^2 - 1$$
$$q | (r+1)(r-1),$$

and by the above $q | r+1$. Since r is odd, $2 | r+1$ and thus $2q | r+1$. Thus $r \equiv -1 \pmod{2q}$ and G is of type 1). Moreover v(G) satisfies either (3.2) or (3.3).

[17/] G is not of type 2c) since groups of this type satisfy condition D) and hence their 2-Sylow subgroup is generalized quaternion.

If $c > 1$, then G is of type 2a) if $q \equiv 1 \pmod 4$ and of type 2b) if $q \equiv 3 \pmod 4$.

Suppose G is of type 2a). Then $\beta(2,s) \geq \beta(2,p-1)$. Letting $\lambda = \beta(2,p-1)$ this means $c \geq \lambda$ and hence $c = \lambda + i$. Moreover as r does not effect the invariants, $v(G)$ satisfies (3.8).

The case where G is of type 2b) is more difficult to handle.

Lemma 5.3. A prime q satisfies $q \equiv 3 \pmod 4$ if and only if q has a unique expression of the form

$$q \equiv 1 + 2 + \ldots + 2^i \pmod{2^{i+2}} \quad \text{with} \quad i \geq 1.$$

Proof. We first show if q is a prime with

$$q \equiv 1 + 2 + \ldots + 2^i \pmod{2^{i+2}}, \quad i \geq 1$$

then

$$q \equiv 3 \pmod 4.$$

If $i = 1$, then $q \equiv 3 \pmod 8$ so $q \equiv 3 \pmod 4$. Suppose $i > 1$.

$$q \equiv 3 + 2^2 + \ldots + 2^i \pmod{2^{i+2}}$$

$$q \equiv 3 + 2^2 + \ldots + 2^i \pmod 4$$

$$q \equiv 3 \pmod 4.$$

Now, suppose q is a prime with $q \equiv 3 \pmod 4$.

$$q - 3 \equiv 0 \pmod 4$$

$$q + 1 \equiv 0 \pmod 4$$

Thus $q + 1 = 2^j k$ with $(2, k) = 1$ and $j \geq 2$.

Case 1. $k = 1$.

Then $q + 1 = 2^j$, $j \geq 2$.

$$q = 2^j - 1$$

$$q \equiv 2^j - 1 \pmod{m} \quad \text{for all} \quad m$$

$$q \equiv 2^j - 1 \pmod{2^{j+1}}$$

$$q \equiv 1 + 2 + \ldots + 2^{j-1} \pmod{2^{j+1}}$$

Since $j \geq 2$, $j-1 \geq 1$.

Case 2. $k > 1$.

Since k is odd, $k = 2\ell + 1$ with $\ell > 1$.

$$q + 1 = 2^j(2\ell+1)$$

$$q + 1 = 2^{j+1}\ell + 2^j$$

$$q \equiv 2^j - 1 \pmod{2^{j+1}}$$

$$q \equiv 1 + 2 + \ldots + 2^{j-1} \pmod{2^{j+1}}$$

Again since $j \geq 2$, $j-1 \geq 1$.

Finally, suppose that

$$q \equiv 1 + 2 + \ldots + 2^i \pmod{2^{i+2}}$$

$$q \equiv 1 + 2 + \ldots + 2^j \pmod{2^{j+2}}$$

where $i, j \geq 1$. We must show $i = j$.

Suppose not. Then, without loss of generality, $i < j$.

Case 1. $j = 1 + i$.

Then

$$q \equiv 1 + 2 + \ldots + 2^{i+1} \pmod{2^{i+3}},$$

so

$$q \equiv 1 + 2 + \ldots + 2^{i+1} \pmod{2^{i+2}}.$$

As

$$q \equiv 1 + 2 + \ldots + 2^{i} \pmod{2^{i+2}},$$

subtraction gives

$$2^{i+1} \equiv 0 \pmod{2^{i+2}},$$

a contradiction.

Case 2. $j \geq i + 2$.

Here we write q as

$$q = 1 + 2 + \ldots + 2^{i} + k2^{i+2},$$

and

$$q = 1 + 2 + \ldots + 2^{j} + n2^{j+2}.$$

So

$$2q = 2(1+2+\ldots+2^{i}) + 2^{i+1} + \ldots + 2^{j} + k2^{i+2} + n2^{j+2}.$$

$$q = (1+2+\ldots+2^{i}) + 2^{i} + \ldots + 2^{j-1} + k2^{i+1} + n2^{j+1}$$

$$= (1+2+\ldots+2^{i-1}) + 2^{i+1} + 2^{i+1} + \ldots + 2^{j-1} + 2^{i+1}(k+n2^{j-i}).$$

Thus

$$q \equiv 1 + 2 + \ldots + 2^{i-1} \pmod{2^{i+1}}. \qquad (*)$$

Since

$$q \equiv 1 + 2 + \ldots + 2^i \pmod{2^{i+2}},$$

$$q \equiv 1 + 2 + \ldots + 2^i \pmod{2^{i+1}}.$$

Subtraction from (*) gives $2^i \equiv 0 \pmod{2^{i+1}}$, a contradiction. This completes the proof.

Now, suppose G is K-adequate of type 2b). We write $q \equiv 1 + 2 + \ldots + 2^j \pmod{2^{j+2}}$ and set $\lambda = j + 2$. Since $\beta(2, s) \geq j + 2$, $c = \lambda + i$ and so $v(G)$ has invariants as in (3.11).

2. The Main Theorem

We begin with a "keystone" lemma which is the analog of Lemma 4.3 for local fields. Recall p is an odd prime.

Lemma 5.4. Let K be a p-local field, and let L be the subfield of index two in $\mathbb{Q}_p(\varepsilon_p)$.

a) If $p \equiv 1 \pmod 4$, set $\lambda = \beta(2, p-1)$.

b) If $p \equiv 3 \pmod 4$, we write $p \equiv 1 + 2 + \ldots + 2^j \pmod{2^{j+2}}$ where $j \geq 1$; set $\lambda = j + 2$, and assume $2 | [KL: L]$.

Set $L_i = L(\varepsilon_{2^{\lambda+i}})$ for $i \geq 0$ and let $w = \beta(2, [KL_0: L_0])$. Then the following are equivalent;

1) $\varepsilon_{2^{\lambda+w}} \in K$

2) $2 \nmid e[KL_0: L_0]$

3) There exists $b > 0$ such that $2 \nmid [KL_b: L_b]$

4) $KL_w = KL_0$

5) $2 \nmid [KL_i : L_i]$ for all $i \geq w$.

Proof. There is a unique unramified extension of $\mathbb{Q}_p$ of every degree. We note that $\mathbb{Q}_p(\varepsilon_{2^{\lambda+i}})$ is unramified. By [18, Proposition 3-2-12], $[\mathbb{Q}_p(\varepsilon_{2^{\lambda+i}}) : \mathbb{Q}_p] = f$ where f is the smallest positive integer such that $p^f \equiv 1 \pmod{2^{\lambda+i}}$. With this fact in mind we show 1) and 2) are equivalent.

i) $p \equiv 1 \pmod 4$.

In this case $\lambda \geq 2$, so $2^\lambda > 3$ and we have seen previously that $f = 2^i$. Thus $\mathbb{Q}_p(\varepsilon_{2^{\lambda+w}})$ is the unique unramified extension of $\mathbb{Q}_p$ of degree 2^w.

Claim: $L = L_0$.

Proof: Since $2^\lambda \| p-1$, $\varepsilon_{2^\lambda} \in \mathbb{Q}_p$. Thus

$$L_0 = L(\varepsilon_{2^\lambda}) = L.$$

Now, $\varepsilon_{2^{\lambda+w}} \in K$ is equivalent to $2^w | f(K/\mathbb{Q}_p)$. Since $L/\mathbb{Q}_p$ is completely ramified, $\varepsilon_{2^{\lambda+w}} \in K$ is equivalent to $2^w | f(KL/L)$. But

$$\begin{aligned} 2^w \| [KL_0 : L_0] &= [KL : L] \\ &= f(KL/L)e(KL/L). \end{aligned}$$

Thus by definition of w, $2^w | f(KL/L)$ if and only if

$2 \nmid e(KL/L)$. Since $e(KL/L) = e(KL_0/L_0)$ 1) and 2) are equivalent.

ii) $p \equiv 3 \pmod 4$ (see Figure 9).

$$\begin{tikzcd}
& KL_0 \arrow[dl, dash] \arrow[dr, dash, "2^w \| [KL_0 : L_0]"] & \\
KL \arrow[dr, dash, "2 |"'] & & L_0 = L(\varepsilon_{2^\lambda}) \arrow[dl, dash, "\text{unramified of degree 2}"] \\
& L &
\end{tikzcd}$$

Figure 9. Subfields of KL_0.

We have seen previously $f = 2^{i+1}$. Thus $\mathbb{Q}_p(\varepsilon_{2^{\lambda+w}})$ is the unique unramified extension of $\mathbb{Q}_p$ of degree 2^{w+1}. $\varepsilon_{2^{\lambda+w}} \in K$ is equivalent to $2^{w+1} | f(KL/L)$. We know $2^{w+1} \| [KL_0 : L]$. So

$$2^{w+1} \| f(KL_0/L)e(KL_0/L) \qquad (*)$$

Since $KL \subsetneq KL_0$,

$$f(KL_0/KL)f(KL/L) = f(KL_0/L) .$$

Now,

$$2^{w+1} | f(KL/K) \quad \Rightarrow$$

$$2^{w+1} | f(KL_0/L) \Leftrightarrow$$

by (*)

$$2 \nmid e(KL_0/L) \iff$$
$$2 \nmid e(KL_0/L_0) ,$$

since L_0 over L is unramified. Thus 1) implies 2).

Finally, suppose $2 \nmid e(KL_0/L_0)$. We have

$$\begin{aligned} e(KL_0/L_0) &= e(KL_0/L) \\ &= e(KL_0/KL)e(KL/L). \end{aligned}$$

Thus $2 \nmid e(KL/L)$. Since $2 \mid [KL:L]$, $2 \mid f(KL/L)$ and thus $KL \supseteq L_0$. So $KL_0 = KL$. Therefore $f(KL_0/L) = f(KL/L)$. From (*) we have

$$2 \nmid e(KL_0/L_0) \Rightarrow 2^{w+1} \mid f(KL/L).$$

Thus 2) implies 1).

Since $L \subseteq \mathbb{Q}_p(\varepsilon_p)$, $\overline{L} = \mathbb{Z}_p$ the field of p elements. $[\overline{L}_i : \mathbb{Z}_p]$ is the smallest integer f such that $p^f \equiv 1 \pmod{2^{\lambda+i}}$. Thus

$$[\overline{L}_i : \mathbb{Z}_p] = \begin{cases} 2^i & p \equiv 1 \pmod 4 \\ 2^{i+1} & p \equiv 3 \pmod 4). \end{cases}$$

Thus

$$L_{i+1} \neq L_i .$$

So

$$[L_{i+1}:L_i] = 2 \qquad \text{for all} \quad i \geq 0,$$

hence

$$[KL_{i+1}:KL_i] = 1 \text{ or } 2.$$

Suppose for some r, $[KL_{r+1}:KL_r] = 2$. Since KL_{r+1} is unramified over KL_r, $[\overline{K}\overline{L}_{r+1}:\overline{K}\overline{L}_r] = 2$.

If $[\overline{K}\overline{L}_{r+2}:\overline{K}\overline{L}_{r+1}] = 1$, then $[\overline{K}\overline{L}_{r+2}:\overline{K}\overline{L}_r] = 2$. Let σ be an automorphism of $\overline{K}\overline{L}_{r+2}$ over $\overline{K}\overline{L}_r$ of order two. σ fixes $\overline{K}$ and so σ can be identified with an automorphism of $\mathbb{Z}_p(\overline{\varepsilon}_{2^{\lambda+r+2}})$ over $\mathbb{Z}_p(\overline{\varepsilon}_{2^{\lambda+r}})$. Since σ has order two, σ fixes $\overline{\varepsilon}_{2^{\lambda+r+1}}$. Thus σ fixes $\overline{K}\overline{L}_{r+1}$, contrary to assumption.

This proves $KL_{r+2} \neq KL_{r+1}$, and so if $[KL_{r+1}:KL_r] = 2$ then $[KL_{r+s+1}:KL_{r+s}] = 2$ for all $s \geq 0$.

Now, assume 3) holds.

$$\begin{aligned}[KL_t:KL_0][KL_0:L_0] &= [KL_t:L_t][L_t:L_0] \\ &= [KL_t:L_t]2^t .\end{aligned}$$

If $t < w$, then since $2^w \mid [KL_0:L_0]$ we must have $2 \mid [KL_t:L_t]$. This shows $b \geq w$.

If $b = w$, then $2 \nmid [KL_w:L_w]$.

$$[KL_w:KL_0][KL_0:L_0] = [KL_w:L_w][L_w:L_0]$$
$$= [KL_w:L_w]2^w .$$

Since $2^w || [KL_0:L_0]$ we conclude $2 \nmid [KL_w:KL_0]$. Then from the above discussion we conclude

$$[KL_w:KL_{w-1}] = \ldots = [KL_1:KL_0] = 1.$$

Then $[KL_w:KL_0] = 1$.

Thus we may assume there exists $b > w$ such that $2 \nmid [KL_b:K_b]$ and $2 | [KL_i:L_i]$ for $w \leq i < b$. But then from

$$\underbrace{[KL_b:L_b]}_{2\nmid}\ \underbrace{[L_b:L_{b-1}]}_{=2} = [KL_b:KL_{b-1}]\ \underbrace{[KL_{b-1}:L_{b-1}]}_{2|}$$

we have $2 \nmid [KL_b:KL_{b-1}]$. So as above $KL_w = KL_0$.

Conversely, if 4) holds then $KL_w = KL_0$ and so

$$[KL_0:L_0] = [KL_w:L_0]$$
$$= [KL_w:L_w][L_w:L_0]$$
$$= [KL_w:L_w]2^w .$$

Thus

$$2 \nmid [KL_w:L_w] \qquad (**).$$

Then $[KL_{w+1}:KL_w] = 2$ and $2 \nmid [KL_{w+1}:L_{w+1}]$ (see Figure 10).

Thus we may take $b = w+1 > 0$, and so 3) holds. Hence 3) and 4) are equivalent.

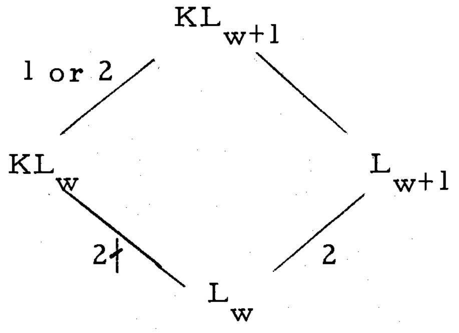

Figure 10. Subfields of KL_{w+1}.

Suppose 4) holds. Then from (**) $2\nmid[KL_w:L_w]$. Suppose we have shown $2\nmid[KL_i:L_i]$ for all i, $w \le i \le t$. Then

$$\underbrace{[KL_{t+1}:KL_t]}_{=\,1 \text{ or } 2}\;\underbrace{[KL_t:L_t]}_{2\nmid} = [KL_{t+1}:L_{t+1}]\;\underbrace{[L_{t+1}:L_t]}_{=\,2}$$

Since the contribution from two which divides the left hand side is at most two, and two divides the right hand side we must have $2\nmid[KL_{t+1}:L_{t+1}]$. By induction $2\nmid[KL_b:L_b]$ for all $b \ge w$. Thus 4) implies 5).

If 5) holds, then $2\nmid[KL_w:L_w]$.

$$\underbrace{[KL_w:L_w]}_{2\nmid}\;\underbrace{[L_w:L_0]}_{=\,2^w} = [KL_w:KL_0]\;\underbrace{[KL_0:L_0]}_{2^w\,||}$$

So $2 \nmid [KL_w : KL_0]$. And as done previously, we have $KL_w = KL_0$, so 4) holds. Thus 3), 4), and 5) are equivalent.

By definition, $KL_w = KL(\varepsilon_{2^{\lambda+w}})$, and $KL_0 = KL(\varepsilon_{2^\lambda})$.

If $\varepsilon_{2^{\lambda+w}} \in K$, then $KL_w = KL$. Since $KL_w \supseteq KL_0 \supseteq KL$, we conclude $KL_w = KL_0$ so 1) implies 4).

Suppose 4) holds, so $KL_w = KL_0$.

i) $p \equiv 1 \pmod 4$.

Since $L_0 = L$, $KL_w = KL$. Thus $\overline{K}\,\overline{L}(\overline{\varepsilon}_{2^{\lambda+w}}) = \overline{K}\,\overline{L} = \overline{K}$. Therefore $\overline{\varepsilon}_{2^{\lambda+w}} \in \overline{K}$ and by Hensel's Lemma [18, Theorem 2-2-1] we conclude $\varepsilon_{2^{\lambda+w}} \in K$.

ii) $p \equiv 3 \pmod 4$.

If $w = \beta(2, [KL_0 : L_0]) = 0$, then since $2 | [KL : L]$ we have $[KL_0 : KL] = 1$ (see Figure 9) and so $KL_0 = KL$. Thus

$$\begin{aligned}\overline{K}\,\overline{L}(\overline{\varepsilon}_{2^\lambda}) &= \overline{K}\,\overline{L}\\ &= \overline{K}.\end{aligned}$$

If $w > 0$, then $KL_w = KL_0$ so $\overline{K}\,\overline{L}(\overline{\varepsilon}_{2^{\lambda+w}}) = \overline{K}\,\overline{L}(\overline{\varepsilon}_{2^\lambda})$ and since $\overline{L} = \mathbb{Z}_p$, $\overline{K}(\overline{\varepsilon}_{2^{\lambda+w}}) = \overline{K}(\overline{\varepsilon}_{2^\lambda})$. Since $w > 1$, this is possible only if $\overline{\varepsilon}_{2^{\lambda+w}} \in \overline{K}$.

So for all w, $\overline{\varepsilon}_{2^{\lambda+w}} \in \overline{K}$ and by Hensel's Lemma $\varepsilon_{2^{\lambda+w}} \in K$. Thus 4) implies 1) and the proof of the lemma is complete.

We will show that 2) of the lemma can be replaced by $2 \nmid e(KL/L)$.

Claim: $2 \nmid e(KL_0/L_0)$ if and only if $2 \nmid e(KL/L)$.

Proof: If $p \equiv 1 \pmod 4$ then $L = L_0$ and there is nothing to prove.

Thus we may assume $p \equiv 3 \pmod 4$. Since L_0/L and KL_0/KL are unramified, $e(L_0/L) = e(KL_0/KL) = 1$. Since $e(KL_0/L_0)e(L_0/L) = e(KL_0/KL)e(KL/L)$, $e(KL_0/L_0) = e(KL/L)$.

We now present the main theorem of this chapter.

Theorem 5.5. Let K be a p-local field, p an odd prime. Then there exists a noncyclic K-adequate group if and only if there is a prime divisor q of $p-1$ such that $q \nmid e(KL^q/L^q)$ where L^q is the subfield of index q in $\mathbb{Q}_p(\varepsilon_p)$.

Proof. From [7, Theorem 1] we know there exists a noncyclic odd-order group which is K-adequate if and only if $q \nmid e(KL^q/L^q)$ where q is an odd prime divisor of $p-1$.

Thus we need only show there exists an even-order noncyclic group which is K-adequate if and only if $2 \nmid e(KL^2/L^2)$, and $q | e(KL^q/L^q)$ for all odd prime divisors q of $p-1$.

Suppose G is a noncyclic even-order group which is K-adequate. Then by Lemma 5.2 we may assume G is a $G_{m,r}$

group with $m = p_0 2^c$, $s = 2^c$, and $n = 2$. By [7, Proposition 2] we must have $p = p_0$.

Case 1. $c = 1$.

We know G is of type 1) and has invariants as in (3.2) or (3.3).

If $p \equiv 1 \pmod 4$, then $v(G)$ has nonzero invariants only at the infinite primes of Z, the center of $v(G)$. So by [7, Proposition 2] G is not K-adequate. This shows if $p \equiv 1 \pmod 4$ we cannot have $c = 1$.

If $p \equiv 3 \pmod 4$, let D be a K-division ring containing $v(G)$. Then $D \supseteq v(G) \otimes_Z Z_{\mathfrak{P}}$ where Z is the subfield of index two in $\mathbb{Q}(\varepsilon_p)$ and $\mathfrak{P}$ is a prime of Z extending p. Thus $D \supseteq KZ_{\mathfrak{P}} \otimes_{Z_{\mathfrak{P}}} (Z_{\mathfrak{P}} \otimes_Z v(G)) = D_0$, and D_0 must be a division ring. Since the invariant of D_0 is

$$\begin{aligned}[KZ_{\mathfrak{P}} : Z_{\mathfrak{P}}]\mathrm{inv}(Z_{\mathfrak{P}} \otimes_Z v(G)) &\equiv [KZ_{\mathfrak{P}} : Z_{\mathfrak{P}}]\mathrm{inv}_{\mathfrak{P}}\, v(G) \\ &\equiv [KZ_{\mathfrak{P}} : Z_{\mathfrak{P}}]\tfrac{1}{2} \pmod 1,\end{aligned}$$

we must have $2 \nmid [KZ_{\mathfrak{P}} : Z_{\mathfrak{P}}]$. Since $Z_{\mathfrak{P}}$ is precisely the field L^2 we have

$$2 \nmid [KL^2 : L^2]$$
$$2 \nmid f(KL^2/L^2)e(KL^2/L^2).$$

Thus

$$2 \nmid e(KL^2/L^2).$$

Case 2. $c > 1$.

We know G is of type 2a) or 2b) and $v(G)$ satisfies (3.8) or (3.11). Again let D be a K-division ring, $D \supseteq v(G)$. Then $D \supseteq v(G) \otimes_Z Z_{\mathfrak{P}}$ for some prime $\mathfrak{P}$ of Z extending p. Letting D_0 be as above, the same computation shows $2\nmid[KZ_{\mathfrak{P}} : Z_{\mathfrak{P}}]$. Let λ be as in the previous lemma, and set $L_i = L^2(\varepsilon_{2^{\lambda+i}})$, where $c = \lambda + i$. Then $L_i \cong Z_{\mathfrak{P}}$. Thus $2\nmid[KL_i : L_i]$. By the previous lemma, $2\nmid e(KL^2/L^2)$. [18]

Conversely suppose $2\nmid e(KL^2/L^2)$. Suppose first that $p \equiv 3 \pmod 4$ and $2\nmid[KL^2:L^2]$. We set $m = 2p$, $n = s = 2$, and $r = -1$. By (3.3) $G_{m,r}$ is a subgroup of a division ring and $\mathrm{inv}_{\mathfrak{P}}\, v(G) = 1/2$ where $\mathfrak{P}$ is the prime of Z extending p. Moreover $Z_{\mathfrak{P}} \cong L^2$. The invariant of $D_0 = (v(G) \otimes_Z Z_{\mathfrak{P}}) \otimes_{Z_{\mathfrak{P}}} KZ_{\mathfrak{P}}$ is

$$\begin{aligned} &\equiv \mathrm{inv}_{\mathfrak{P}} v(G)\, [KL^2:L^2] \\ &\equiv \frac{1}{2}\, [KL^2:L^2] \\ &\equiv \frac{1}{2} \pmod 1, \end{aligned}$$

and so D_0 is a KL^2-division ring. Let D be the K-division ring

[18] If $p \equiv 3 \pmod 4$ we may assume $2 | [KL^2 : L^2]$ or there is nothing to prove. The lemma then shows $2\nmid e(KL_0/L_0)$ and from the remark which follows that lemma $2\nmid e(KL^2/L^2)$. For $p \equiv 1 (\mathrm{mod} 4)$, $L^2 = L_0$ so if $2\nmid e(KL_0/L_0)$ then $2\nmid e(KL^2/L^2)$.

with invariant $1/2u$ where $u = [KL^2 : K]$.

If $\varepsilon_p \in K$, then

$$[KL^2 : L^2] = [KL^2 : \mathbb{Q}_p(\varepsilon_p)][\mathbb{Q}_p(\varepsilon_p) : L^2]$$

$$= 2[KL^2 : \mathbb{Q}_p(\varepsilon_p)] ,$$

contrary to assumption.

Thus $\varepsilon_p \notin K$, and so

$$[K(\varepsilon_p) : K] = [K(\varepsilon_p) : KL^2][KL^2 : K]$$

$$= 2u ,$$

so $K(\varepsilon_p)$ is a maximal subfield of D. Thus $D \supset KL^2$ so $C_D(KL^2) \subseteqq D$ and $C_D(KL^2) \sim D \otimes_K KL^2$ has invariant

$$\equiv \frac{1}{2u} [KL^2 : K]$$

$$\equiv \frac{1}{2} \pmod 1$$

$$\sim D_0 ,$$

so $D_0 \subseteqq D$ and hence so is G.

Now we will complete the proof by choosing a G for $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.

Suppose $2 | [KL^2 : L^2]$ and $p \equiv 3 \pmod 4$. Write $p \equiv 1 + 2 + \ldots + 2^j \pmod{2^{j+2}}$ and set $\lambda = j + 2$, $w = \beta(2, [KL^2 : L^2]$.

Then we let G be the $G_{m,r}$ group of (3.11) with $m = p2^{\lambda+w}$, $s = 2^{\lambda+w}$, and $n = 2$.

Let $p \equiv 1 \pmod 4$. Set $\lambda = \beta(2, p-1)$, so $\lambda > 1$, and let $w = \beta(2, [KL^2 : L^2])$. Then we let G be the $G_{m,r}$ group of (3.8) with $m = p2^{\lambda+w}$, $s = 2^{\lambda+w}$, and $n = 2$.

We will show that G, according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ is K-adequate.

Since Z, the center of $v(G)$ is normal over $\mathcal{Q}$, all completions of Z at primes $\mathcal{B}$ extending p are isomorphic. Thus $Z_{\mathcal{B}} = L_w$. Let $b = [KZ_{\mathcal{B}} : Z_{\mathcal{B}}]$. By the previous lemma, $2 \nmid b$. $\mathrm{inv}_{\mathcal{B}}\, v(G) = 1/2$ so the invariant of $v(G) \otimes_Z Z_{\mathcal{B}}$ is $1/2$, and the invariant of $D_0 = (v(G) \otimes_Z Z_{\mathcal{B}}) \otimes_{Z_{\mathcal{B}}} KZ_{\mathcal{B}}$ is $1/2$. Let $u = [KZ_{\mathcal{B}} : K]$ and let D be the K-division ring with invariant $1/2u$. Now, $[K(\varepsilon_m) : KZ_{\mathcal{B}}] = [K(\varepsilon_m) : KL_w]$.

If $K(\varepsilon_m) = KZ_{\mathcal{B}}$ then $K(\varepsilon_m) = KL_w$. But $2 \mid e(K(\varepsilon_m)/L_w)$ and so $2 \mid e(KL_w/L_w)$, a contradiction.

Thus $[K(\varepsilon_m) : KZ_{\mathcal{B}}] = 2$, and so

$$\begin{aligned} [K(\varepsilon_m) : K] &= [K(\varepsilon_m) : KZ_{\mathcal{B}}][KZ_{\mathcal{B}} : K] \\ &= 2u. \end{aligned}$$

Hence $K(\varepsilon_m)$ is a maximal subfield of D and so

$$\begin{aligned} D &\supseteq C_D(KZ_{\mathcal{B}}) \\ &\sim D \otimes_K KZ_{\mathcal{B}} . \end{aligned}$$

$C_D(KZ_{\mathcal{B}})$ has invariant

$$\begin{aligned} &\equiv \operatorname{inv} D\, [KZ_{\mathcal{B}} : K] \\ &\equiv \frac{1}{2u}\, u \\ &\equiv \frac{1}{2} \\ &\sim D_0 . \end{aligned}$$

Thus $C_D(KZ_{\mathcal{B}}) \cong D_0$ and so $v(G) \subseteq D$, and G is K-adequate. This completes the proof.

Corollary 5.6. Let p be an odd prime. Then there exist infinitely many p-local fields K for which no noncyclic group is K-adequate.

Proof. Let K be any p-local field containing $\mathbb{Q}_p(\varepsilon_p)$. Then

$$e(K/L^q) = e(K/\mathbb{Q}_p(\varepsilon_p))e(\mathbb{Q}_p(\varepsilon_p)/L^q) .$$

Since $\mathbb{Q}_p(\varepsilon_p)$ is totally ramified

$$\begin{aligned} e(\mathbb{Q}_p(\varepsilon_p)/L^q) &= [\mathbb{Q}_p(\varepsilon_p) : L^q] \\ &= q . \end{aligned}$$

Thus $q \mid e(K/L^q)$ for all primes $q \mid p-1$. Since $KL^q = K$ the result follows from the previous theorem.

Finally we shall show that the previous theorem can be strengthened so as to handle the K-adequacy of even-order noncyclic groups.

Proposition 5.7. If K is a p-local field then there exists a noncyclic even-order group which is K-adequate if and only if $q \nmid e(KL^q/L^q)$ for some prime $q \mid p-1$.

Proof. Assume there exists a prime $q \mid p-1$ such that $q \nmid e(KL^q/L^q)$. If $q = 2$, and for all prime divisors r of $p-1$, $r \mid e(KL^r/L^r)$, then the proof of the preceding theorem shows there exists a noncyclic even-order group which is K-adequate.

If there exists an odd prime q with $q \mid p-1$ and $q \nmid e(KL^q/L^q)$ then by [7, Theorem 1] there exists a noncyclic group H of odd-order which is K-adequate. Since $K \supseteq \mathbb{Q}_p$, $-1 \in K$ generates a group of order two. If $-1 \in H$, then $2 \mid |H|$, a contradiction. Thus $-1 \notin H$, and since -1 commutes with H, the group $G = C_2 \times H$ is K-adequate. It is noncyclic since H is, and has order $2 \cdot |H|$.

For the converse, we suppose G is an even-order K-adequate group. Let S be the (nonempty) set of even-order noncyclic groups which are K-adequate. We consider the set A of noncyclic Hall $\{p, q\}$-subgroups of these groups. If A contains an odd-order group then by [7, Theorem 1] $q \nmid e(KL^q/L^q)$ for some prime q, $q | p-1$. Thus we assume A contains only even-order noncyclic groups. This means $q \nmid e(KL^q/L^q)$ for all odd primes q, $q | p-1$; since if not we have an odd-order group which then has a group extension which is of even-order and hence in S. Then by the previous theorem, $2 \nmid e(KL^2/L^2)$.

3. The Exceptional Case, $p = 2$

In this section we assume K is a 2-local field. By [7, Corollary 1] no noncyclic odd-order groups are K-adequate. Thus "noncyclic" and "noncyclic of even-order" are equivalent. This fact determines K-adequacy for noncyclic groups.

Proposition 5.8. There exists a noncyclic group which is K-adequate if and only if $2 \nmid [K: \mathbb{Q}_2]$.

Proof. By Proposition 2.8, the quaternions Q^*, are K-adequate if and only if $2 \nmid [K: \mathbb{Q}_2]$.

Thus if $2 \nmid [K: \mathbb{Q}_2]$ then Q^* is K-adequate.

To prove the converse we will show that if $2 | [K: \mathbb{Q}_2]$ then there is no noncyclic K-adequate group.

Suppose not. Let G be a noncyclic group which is K-adequate. Then the above discussion shows G is of even-order and the 2-Sylow subgroup of G is cyclic. Since the odd-order Hall-$\{p, q\}$ subgroups of G must be cyclic, Lemma 5.1 shows there exists a noncyclic subgroup H of order $2^a q^b$. But then Lemma 5.2 shows we may refine H to a $G_{m, r}$ group with $m = 2^c q$, $s = 2^c$, and $n = 2$. The discussion following that lemma shows $v(G)$ has invariants satisfying (3.2), (3.3), (3.8), or (3.11). In any case, this contradicts [7, Proposition 2] and thus the proof is complete.

BIBLIOGRAPHY

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

2. S. Amitsur, Finite subgroups of division rings, Trans. Amer. Math. Soc. 80 (1955), pp. 361-386.

3. M. Benard, The Schur Subgroup I, J. Algebra 22 (1972), pp. 374-377.

4. M. Benard and M. Schacher, The Schur Subgroup II, J. Algebra 22 (1972), pp. 378-385.

5. M. Deuring, "Algebra," Springer-Verlag, New York/Berlin, 1968.

6. B. Fein and M. Schacher, Embedding finite groups in rational division algebras I, J. Algebra 17 (1971), pp. 412-418.

7. B. Fein and M. Schacher, Embedding finite groups in rational division algebras II, J. Algebra 19 (1971), pp. 131-139.

8. B. Fein and M. Schacher, Embedding finite groups in rational division algebras III, J. Algebra 28 (1974), pp. 304-310.

9. B. Fein and M. Schacher, Finite subgroups occurring in finite-dimensional division algebras, J. Algebra 32 (1974), pp. 332-338.

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

11. I.N. Herstein, Conjugates in division rings, Proceedings of the Amer. Math. Soc. v.2 (1956), pp. 1021-1022.

12. I.N. Herstein, Finite multiplicative subgroups in division rings, Pacific J. Math. 1 (1953), pp. 121-126.

13. I.N. Herstein, "Noncommutative Rings," Carus Monograph, 1968.

14. N. Jacobson, "P.I.-Algebras," Springer-Verlag, Berlin-Heidelberg - New York, 1975.

15. J. Janusz, "Algebraic Number Fields," Academic Press, New York, 1973.

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

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

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