CONSTRUCTION OF 2-ADIC GALOIS EXTENSION WITH WILD INERTIA GIVEN BY AN EXTRA SPECIAL 2-GROUP

by

Christopher Kocs

A dissertation submitted to the faculty of
The University of Utah
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

The University of Utah

August 2012

The University of Utah Graduate School

STATEMENT OF DISSERTATION APPROVAL

The dissertation of **Christopher Kocs**

has been approved by the following supervisory committee members:

Gordan Savin	, Chair	**4/23/2012** Date Approved
Dan Ciubotaru	, Member	**4/23/2012** Date Approved
Dragan Milicic	, Member	**4/23/2012** Date Approved
Martin Weissman	, Member	**4/23/2012** Date Approved
Peter Trapa	, Member	**4/23/2012** Date Approved

and by **Peter Trapa**, Chair of the Department of **Mathematics**

and by Charles A. Wight, Dean of The Graduate School.

ABSTRACT

Given any field F and an odd integer n, suppose K be a degree 2^{n-1} multiquadratic extension of F. We consider the conditions under which there is a Galois extension E of F such that $\mathrm{Gal}(E/F)$ is a particular extra special 2-group Γ_0 – namely, the multiplicative group generated by basis elements of the even Clifford algebra associated with the quadratic form $X_1^2 + ... + X_n^2$. These conditions can be restated in terms of the Weil index, which can be computed explicitly as a Gauss sum when $F = \mathbb{Q}_{2^n}$. We prove an equidistribution of Gauss sums for quadratic characters on $\mathbb{Q}_{2^n}$ of conductor $4\mathbb{Z}_{2^n}$. As a consequence, we prove that, when n is an odd prime greater than 3, there exists a Galois extension K of $\mathbb{Q}_2$ such that K is a multiquadratic extension of $\mathbb{Q}_{2^n}$ that admits a quadratic extension E such that $\mathrm{Gal}(E/F) \cong \Gamma_0$.

CONTENTS

ACKNOWLEDGEMENTS

I would like to thank my parents and my sister for all of their support and encouragement. Also, I am greatly indebted to my advisor, Gordan Savin, for his constant and patient guidance.

CHAPTER 1

QUADRATIC FORMS

In this chapter, we will generalize a theorem due to Witt that constructs a Galois extension E of a field F such that $\mathrm{Gal}(E/F)$ is the quaternion group [12]. To best describe the conditions under which such an extension exists (see Theorem 1.5.2 for the precise statement), we will first need to recall some of the theory of quadratic forms.

1.1 Preliminaries

We say that a polynomial q in n variables is an n-ary *quadratic form* over a field[1] F if

$$q(X) = q(X_1, X_2, ..., X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$$

for some $a_{ij} \in F$. For q as above, we can define a symmetric matrix M_q, in the group $M(n, F)$ of $n \times n$ matrices with entries in F, such that

$$(M_q)_{ij} = \frac{1}{2}(a_{ij} + a_{ji}).$$

Observe that M_q is the unique symmetric matrix in $M(n, F)$ with the property that

$$q(X) = X^\top M_q X. \tag{1.1}$$

(Here X is treated as a column vector, and $X^\top$ denotes the transpose of X.) Two n-ary quadratic forms q_1 and q_2 are said to be *equivalent* over F if there exists a matrix $P = (p_{ij}) \in GL(n, F)$ such that $q_1(Y) = q_2(X)$ where

$$Y_i = \sum_{j=1}^{n} p_{ij} X_j.$$

In other words, $q_1(PX) = q_2(X)$. From (1.1), we see that an invertible $n \times n$ matrix P satisfies this condition if and only if $P^\top M_{q_1} P = M_{q_2}$. We leave it to the reader to verify that this does indeed define an equivalence relation on the set of quadratic forms over F.

---

[1] For the entirety of this paper, we will use "field" to mean a field of characteristic not 2.

Let V be an n-dimensional vector space over a field f and B, a symmetric bilinear form $V \times V \longrightarrow F$. We call the pair (V, B) a *quadratic space*. We can define a *quadratic map* Q on V by defining $Q(x) = B(x, x)$ for all $x \in V$. We can recover B from Q since

$$\frac{1}{2}(Q(x+y) - Q(x) - Q(y)) = B(x+y, x+y) - B(x,x) - B(y,y) = B(x,y).$$

Thus, it makes sense to use the notation (V, Q) and (V, B) interchangeably. Given a particular basis $\{e_1, ..., e_n\}$ of V, B determines a quadratic form q –

$$q(X) = \sum_{i,j=1}^{n} B(e_i, e_j) X_i X_j.$$

This correspondence is unique up to change of basis; that is, (V, B) uniquely determines the equivalence class of q.

From linear algebra, we know that every quadratic space (V, Q) has an orthogonal basis with respect to the bilinear form B ([6, pp.575-6]). Hence, every quadratic form q can be *diagonalized* – i.e., q is equivalent to some quadratic form whose associated matrix is diagonal. We will use $<a_1, a_2, ..., a_n>$ to denote the quadratic form with the associated diagonal matrix $\text{diag}(a_1, a_2, ..., a_n)$.

1.2 Clifford Algebras

Let (V, Q) be a quadratic space over a field F. A linear map L from V to an F-algebra[2] A is said to be Q-*compatible* if $L(v)^2 = Q(v) \cdot 1$ for all $v \in V$. (1 here is the unit element of A.)

An F-algebra C together with a Q-compatible linear map $\psi : V \longrightarrow C$ is called a *Clifford algebra* if, for every F-algebra A, every Q-compatible linear map $\phi : V \longrightarrow A$ factors through ψ – i.e., there exists a unique algebra homomorphism $\phi' : C \longrightarrow A$ such that $\phi = \phi' \circ \psi$.

It is easy to verify from this definition that, for C and ψ as above, $\psi(V)$ generates C as an F-algebra and, moreover, that C must be unique up to isomorphism. Provided that it exists, we shall write $C(V, Q)$ – or just $C(V)$ if Q is clear from the context – for the Clifford algebra of (V, Q).

We will now show that the Clifford algebra $C(V)$ exists by explictly constructing such an algebra.

---

[2]We will always use "algebra" to mean a unital associative algebra.

Consider the tensor algebra $T(V) = \bigoplus_{i=0}^{\infty} T^m(V)$, where

$$T^0(V) = K \text{ and } T^m(V) = \bigotimes_{i=1}^{m} V.$$

Multiplication in $T(V)$ is induced by the bilinear map

$$T^m(V) \times T^l(V) \longrightarrow T^{m+l}(V)$$
$$(v_1 \otimes v_2 \otimes \cdots \otimes v_m, u_1 \otimes u_2 \otimes \cdots \otimes u_l) \longmapsto v_1 \otimes \cdots \otimes v_m \otimes u_1 \otimes \cdots \otimes u_l,$$

for $v_i, u_j \in V$. Take I_Q to be the two-sided ideal of $T(V)$ generated by all elements of the form

$$v \otimes v - Q(v) \cdot 1$$

for v in V. Let C be $T(V)/I_Q$ and ψ, the composition of the natural embedding of $T^1(V) = V$ into $T(V)$ and the canonical homomorphism $T(V) \longrightarrow T(V)/I_Q$. Clearly, this construction statisfies our definition of a Clifford algebra for (V, Q).

Since $T(V)$ is a graded algebra (in which the tensors of rank n directly correspond with the elements homogeneous of degree n) and

$$v \otimes v - Q(v) \cdot 1 \in \bigoplus_{m \text{ even}} T^m(V),$$

$C(V, Q)$ inherits a $\mathbb{Z}/2\mathbb{Z}$-graded structure. We will call the image of $\bigoplus_{m \text{ even}} T^m(V)$ under the quotient map the *even Clifford algebra* of (V, Q) and denote it by $C_0(V, Q)$.

Suppose a quadratic space (V, Q) of odd dimension $n > 1$ over F has an orthogonal basis $\{e_1, e_2, ..., e_n\}$. By abuse of notation, we will use e_i to refer to the image of $e_i \in V$ under the map ψ associated to $C(V)$. Also, for notational simplicity, we will drop the tensor symbol when expressing multiplication in $C(V)$.

We claim that the center of $C_0(V)$ is F. For all i different from j,

$$e_i e_j + e_j e_i = (e_i + e_j)^2 - e_i^2 - e_j^2 = Q(e_i + e_j) - Q(e_i) - Q(e_j) = 0,$$

so e_i and e_j anticommute if $i \neq j$. In particular, this means that if $y = e_1^{p_1} e_2^{p_2} \cdots e_n^{p_n} \in C_0(V)$, then the element $\prod_{i \neq k} e_i$ commutes with y if and only if $p_k = 0$. The claims follows.

Proposition 1.2.1 *If (V, Q) is a quadratic space of odd dimension over a field F, the even Clifford algebra $C_0(V)$ is a central simple algebra over F.*

We have just seen that such a quadratic space must be central over F; to see a proof that $C_0(V)$ is simple consult [5].

1.3 The Spinor Norm

Define an anti-automorphism θ of $T(V)$ such that θ fixes $a \cdot 1$ for all $a \in K$ and that, for $m > 0$,

$$\theta(v_1 \otimes v_2 \otimes \cdots \otimes v_m) = v_m \otimes v_{m-1} \otimes \cdots \otimes v_1,$$

where $v_i \in V$. Observe that θ is an involution on $T(V)$ since $\theta \circ \theta$ is just the identity map on $T(V)$. Because θ preserves the graded structure of $T(V)$ and

$$\theta(v \otimes v - Q(v) \cdot 1) = v \otimes v - Q(v) \cdot 1,$$

θ induces an anti-automorphism on $C(V)$ which preserves the graded structure of $C(V)$. Let $\bar{x}$ denote the image of $x \in C(V)$ under this induced map. Then we define the *spinor norm* of x to be $N(x) = x\bar{x}$.

1.4 The Extra Special 2-group Γ_0

Given a field F, let (V, Q) be a quadratic space of odd dimension $n > 1$. Suppose that $Q(e_i) = 1$ for all $1 \leq i \leq n$ – that is, the matrix associated with the quadratic form determined by Q with respect to $\{e_1, e_2, ..., e_n\}$ is the identity matrix. Let $(C_0(V))^\times$ be the multiplicative group consisiting of all the invertible elements of $C_0(V)$. Define Γ_0 to be the subgroup of $(C_0(V))^\times$ generated by the e_i. Observe that every element of $C_0(V)$ is a finite sum of elements of Γ_0 with coefficients in F. Let $\mu_2 = \{-1, 1\} \subset (C_0(V))^\times$; then we have the following short exact sequence of groups:

$$1 \longrightarrow \mu_2 \hookrightarrow \Gamma_0 \xrightarrow{g} (\mathbb{Z}/2\mathbb{Z})^n,$$

where

$$g(e_i) = (x_1, x_2, ..., x_n) \text{ where } x_k = \begin{cases} 1 & \text{if } k = i \\ 0 & \text{otherwise} \end{cases}.$$

Observe that g gives us an identification of elements of Γ_0 with the elements of $(\mathbb{Z}/2\mathbb{Z})^n$ up to sign. Accordingly, we may reindex the elements of Γ_0 using g and $(\mathbb{Z}/2\mathbb{Z})^n$. That is, if an element $\gamma \in \Gamma_0$ can be written as $e_{i_1} e_{i_2} \cdots e_{i_k}$ $(1 \leq k \leq n)$ where $i_1 < i_2 < ... < i_k$, then

$$\gamma = e_{g(\gamma)}.$$

(Otherwise, $\gamma = -e_{g(\gamma)}$.) To keep track of signs when multiplying these reindexed elements, we will define

$$\zeta_{\sigma,\tau} = e_\sigma e_\tau e_{\sigma\tau}^{-1}, \text{ for } \sigma, \tau \in (\mathbb{Z}/2\mathbb{Z})^n.$$

Let $\rho(\sigma)$ be the number (modulo 2) of coordinates of σ equal to 1 – i.e.,

$$\rho(\sigma) = \sum_{i=1}^{n} \rho_i(\sigma),$$

where $\rho_i(\sigma)$ is the ith coordinate of σ. So the image of Γ_0 under g is the subgroup

$$G_0 = \{\sigma \in (\mathbb{Z}/2\mathbb{Z})^n : \rho(\sigma) = 0\} \subset (\mathbb{Z}/2\mathbb{Z})^n.$$

For $\sigma, \tau \in G_0$, let $\rho(\sigma, \tau)$ be the number of i such that $\rho_i(\sigma)$ and $\rho_i(\tau)$ are both 1. From the simple observation that two elements e_σ and e_τ of $C_0(V)$ commute if they have an even number of e_i in common and anticommute otherwise, we have that

$$\zeta_{\sigma,\tau}\zeta_{\tau,\sigma} = \zeta_{\sigma,\tau}\zeta_{\tau,\sigma}^{-1} = e_\sigma e_\tau e_\sigma^{-1} e_\tau^{-1} = (-1)^{\rho(\sigma,\tau)}.$$

1.5 Construction of Galois Extension

Define a field extension $K = F(\xi_1, \xi_2, \xi_3, ..., \xi_n)$ of F, where

$$a_i = \xi_i^2 \text{ is an element of } F \text{ and } \xi_1\xi_2 \cdots \xi_n = 1.$$

For the purposes of this section, we will restrict our attention to fields F and K as above such that $\mathrm{Gal}(K/F) = G_0$; this means that the $\xi_\tau = \prod_{i=1}^n \xi_i^{-\rho_i(\tau)}$ $(\tau \in G_0)$ are linearly independent over F. Given $\sigma \in G_0$, we will also denote by σ the automorphism of K in $\mathrm{Gal}(K/F)$ which sends ξ_i to $-\xi_i$ if $\rho_i(\sigma) = 1$ and fixes ξ_i if $\rho_i(\sigma) = 0$. Thus,

$$\sigma(\xi_\tau) = (-1)^{\rho(\sigma,\tau)}\xi_\tau = \zeta_{\sigma,\tau}\zeta_{\tau,\sigma}\xi_\tau. \tag{1.2}$$

Our construction to this point leads us to consider the conditions under which there is an extension E of F with Galois group isomorphic to Γ_0.

For $n = 3$, this is the same as requiring that $\mathrm{Gal}(E/F)$ be isomorphic to the usual quaternions, and in this case, Witt used the structure of the quaternions to explicitly construct such an extention E when the quadratic forms

$$q_1(X) = \sum_{i=1}^{n} X_i^2 \text{ and } q_2(Y) = \sum_{j=1}^{n} a_i Y_j^2$$

are equivalent over F (see [12]).[3] Witt's proof can be generalized by recognizing that Γ_0 performs the same role as the quaternions for $n \geq 3$.

[3] In fact, Witt showed that such an extension exists only if these two quadratic forms are equivalent.

Theorem 1.5.2 *There exists a quadratic extension E of K such that E is Galois over F and Gal(E/F) is isomorphic to the extra special 2-group Γ_0, if the quadratic forms*

$$q_1(X) = \sum_{i=1}^{n} X_i^2 \text{ and } q_2(Y) = \sum_{j=1}^{n} a_j Y_j^2$$

over F are equivalent. In particular, suppose $q_1(PX) = q_2(X)$ for some matrix $P = (p_{ij})$ in $GL(n, F)$. If $\rho_i(\sigma) = 0$ for all i, let p_σ be 1; otherwise, let p_σ the determinant of the submatrix of P consisting of all entries p_{ij} such that $\rho_i(\sigma)$ and $\rho_j(\sigma)$ are both nonzero. Then such a field extention E of K is $K\left(\sqrt{r(\sum_{\sigma\in G_0} p_\sigma \xi_\sigma)}\right)$ for any fixed, nonzero $r \in F$.

Proof. Let $\{e'_1, e'_2, ...e'_n\}$ be an orthogonal basis for for the quadratic space (V, Q) such that, for all $1 \leq i \leq n$,

$$e'_i = \sum_{j=1}^{n} p_{ij} e_j.$$

Denote the element $\xi_\sigma e'_\sigma$ in the K-algebra $C_0(V \otimes_F K) \cong C_0(V) \otimes_F K$ by f_σ. It is clear that

$$f_\sigma f_\tau f_{\sigma\tau}^{-1} = \zeta_{\sigma,\tau}.$$

Now, define $c = \dfrac{1}{2^{(n-1)/2}} \displaystyle\sum_{\sigma\in G_0} e_\sigma^{-1} f_\sigma \in C_0(V \otimes_F K)$. We claim that $N(c) \in K^\times$.

Lemma 1.5.3 *$N(c)$ is an element of K.*

Proof. Since $C_0(V \otimes_F K)$ is central over K, it suffices to show that $N(c)$ commutes with all elements of $C_0(V \otimes_F K)$. We first notice that

$$\begin{aligned} 2^{(n-1)/2} e_\tau^{-1} c f_\tau &= \sum_{\sigma\in G_0} e_\tau^{-1} e_\sigma^{-1} f_\sigma f_\tau \\ &= \sum_{\sigma\in G_0} \zeta_{\sigma,\tau} e_{\sigma\tau}^{-1} \zeta_{\sigma,\tau} f_{\sigma\tau} \\ &= \sum_{\sigma\in G_0} e_{\sigma\tau}^{-1} f_{\sigma\tau} \\ &= 2^{(n-1)/2} c. \end{aligned}$$

It follows immediately from the definition of the involution θ (cf. 2.2) that $\overline{e_\sigma} = e_\sigma^{-1}$ and $\overline{f_\sigma} = f_\sigma^{-1}$. Hence,

$$2^{(n-1)/2}\overline{c} = \overline{\sum_{\sigma\in G_0} e_\sigma^{-1} f_\sigma} = \sum_{\sigma\in G_0} \overline{f_\sigma} \cdot \overline{e_\sigma^{-1}} = \sum_{\sigma\in G_0} f_\sigma^{-1} e_\sigma,$$

so we have that

$$\begin{aligned} 2^{(n-1)/2} f_\tau \overline{c} e_\tau^{-1} &= \sum_{\sigma \in G_0} f_\tau f_\sigma^{-1} e_\sigma e_\tau^{-1} \\ &= \sum_{\sigma \in G_0} \zeta_{\tau,\tau}\zeta_{\sigma,\tau} f_{\sigma\tau}^{-1} \zeta_{\tau,\tau}\zeta_{\sigma,\tau} e_{\sigma\tau} \\ &= \sum_{\sigma \in G_0} \overline{f_{\sigma\tau}} e_{\sigma\tau} \\ &= 2^{(n-1)/2} \overline{c}. \end{aligned}$$

This implies that $N(c)$ commutes with all e_τ (and hence all elements of $C_0(V) \otimes_F K$) as

$$e_\tau c\overline{c} = c f_\tau \overline{c} = c\overline{c} e_\tau$$

for all $\tau \in G_0$. ■

To show that $N(c)$ is nonzero and thus invertible, we will explicitly calculate $N(c)$. It is enough to consider the constant term of

$$\frac{1}{2^{n-1}} \sum_{\sigma \in G_0} e_\sigma^{-1} f_\sigma \sum_{\tau \in G_0} f_\tau^{-1} e_\tau = \frac{1}{2^{n-1}} \sum_{\sigma,\tau} e_\sigma^{-1} \zeta_{\sigma,\tau} f_{\sigma\tau} e_\tau^{-1} = \frac{1}{2^{n-1}} \sum_{\sigma,\tau} e_\sigma^{-1} \zeta_{\sigma,\tau} \xi_{\sigma\tau} e'_{\sigma\tau} e_\tau^{-1}. \quad (1.3)$$

We claim that the constant term of $e_\sigma^{-1} e'_\sigma \in C_0(V \otimes_F K)$ is precisely p_σ. If $\rho(\sigma) = 0$, the statement is obvious. Suppose $m = \rho(\sigma) > 0$. Then there exist $1 \le i_1 < i_2 < ... < i_m \le n$ such that $\rho_{i_j}(\sigma) \neq 0$, and the constant term of $e_\sigma^{-1} e'_\sigma$ is

$$e_\sigma^{-1} \sum_{s \in S_m} \prod_{j=1}^{m} p_{i_j, i_{s(j)}} e_{i_{s(j)}} = \sum_{s \in S_m} \operatorname{sgn}(s) \prod_{j=1}^{m} p_{i_j, i_{s(j)}} = p_\sigma$$

where S_m is the group of all permutations of m numbers and $\operatorname{sgn}(s)$ is the signature of the permutation $s \in S_m$. Thus, the constant term of equation (1.3) is just

$$\frac{1}{2^{n-1}} \sum_{\sigma,\tau} e_\sigma^{-1} \zeta_{\sigma,\tau} \xi_{\sigma\tau} p_{\sigma\tau} e_{\sigma\tau} e_\tau^{-1} = \frac{1}{2^{n-1}} \sum_{\sigma,\tau} p_{\sigma\tau} \xi_{\sigma\tau} = \sum_{\sigma \in G_0} p_\sigma \xi_\sigma$$

(as $|G_0| = 2^{n-1}$). Because the ξ_σ are linearly independent over F and the p_σ are not all zero (if σ is the identity in G_0, for instance, $p_\sigma = 1$), $N(c)$ cannot be 0. Because $N(c) \in K^\times$, c is also invertible in $C_0(V \otimes_F K)$

Let $\tau \in G_0$. Then τ induces a map τ (by abuse of notation) on $C_0(V \otimes_F K)$ corresponding to the automorphism $\mathrm{id}_{C_0(V)} \otimes \tau$ of $C_0(V) \otimes_F K$. By equation (1.2), $\tau(f_\sigma) = \zeta_{\sigma,\tau}\zeta_{\tau,\sigma}f_\sigma$, so using the identity $e_\tau^{-1}cf_\tau = c$ from the proof of Lemma 1.5.3, we have that

$$\zeta_{\sigma,\tau}\zeta_{\tau,\sigma}\tau(c^{-1}e_\sigma c) = \zeta_{\sigma,\tau}\zeta_{\tau,\sigma}\tau(f_\sigma) = f_\sigma = c^{-1}e_\sigma c. \tag{1.4}$$

Following the usual convention, we will adopt the notation

$$x^{\sum_\tau a(\tau)\tau} = \prod_{\tau \in G_0} \tau(x)^{a(\tau)},$$

where $a(\tau) \in \mathbb{Z}$ and $x \in C_0(V \otimes_F K)$. In this notation, (1.4) implies that

$$\begin{aligned}
\zeta_{\sigma,\tau}\zeta_{\tau,\sigma}c^{-\tau}e_\sigma c^\tau &= c^{-1}e_\sigma c \\
c^{-\tau}\zeta_{\sigma,\tau}\zeta_{\tau,\sigma}e_\sigma e_\tau e_\tau^{-1}c^\tau &= c^{-1}e_\sigma c \\
c^{-\tau}e_\tau e_\sigma e_\tau^{-1}c^\tau &= c^{-1}e_\sigma c \\
(e_\tau^{-1}c^\tau c^{-1})^{-1}e_\sigma(e_\tau^{-1}c^\tau c^{-1}) &= e_\sigma.
\end{aligned}$$

Thus, $e_\tau^{-1}c^\tau c^{-1}$ commutes with all e_σ, so

$$e_\tau^{-1}c^\tau = \delta_\tau c$$

for some element δ_τ of K. Taking the spinor norm of both sides gives

$$N(c)^\tau = \delta_\tau^2 N(c).$$

Observe that $\delta_\tau\delta_\sigma^\tau = \zeta_{\sigma,\tau}\delta_{\tau\sigma}$ as

$$\begin{aligned}
\delta_\tau\delta_\sigma^\tau &= (c^{-1}e_\tau^{-1}c^\tau)\tau(c^{-1}e_\sigma^{-1}c^\sigma) \\
&= c^{-1}e_\tau^{-1}c^\tau c^{-\tau}e_\sigma^{-1}c^{\tau\sigma} \\
&= c^{-1}\zeta_{\sigma,\tau}e_{\tau\sigma}^{-1}c^{\tau\sigma} \\
&= \zeta_{\sigma,\tau}\delta_{\tau\sigma}.
\end{aligned}$$

Suppose that $\sqrt{rN(c)}$ is an element of K for some nonzero $r \in F$. We have that $\delta_\sigma = \epsilon_\sigma(\sqrt{rN(c)})^{\sigma-1}$ for some $\epsilon_\sigma \in \mu_2$, so

$$\begin{aligned}
\zeta_{\sigma,\tau}\zeta_{\tau,\sigma}\delta_{\tau\sigma}\delta_{\sigma\tau} &= \delta_\tau\delta_\sigma^\tau\delta_\sigma\delta_\tau^\sigma \\
&= \epsilon_\tau\left(\sqrt{rN(c)}\right)^{\tau-1}\epsilon_\sigma\left(\sqrt{rN(c)}\right)^{\tau\sigma-\tau}\epsilon_\sigma\left(\sqrt{rN(c)}\right)^{\sigma-1}\epsilon_\tau\left(\sqrt{rN(c)}\right)^{\sigma\tau-\sigma} \\
&= \delta_{\tau\sigma}\delta_{\sigma\tau}.
\end{aligned}$$

Since $\zeta_{\sigma,\tau}\zeta_{\tau,\sigma}$ is not equal to 1 for all $\sigma, \tau \in G_0$, we have a contradiction, and $\sqrt{rN(c)}$ is not in K.

Let $E = K(\sqrt{rN(c)})$ for any given nonzero $r \in F$. For every $\sigma \in G_0$, we can define an automorphism $\tilde{\sigma}$ of E over F by

$$\tilde{\sigma}(x + y\sqrt{rN(c)}) = x^\sigma + y^\sigma \delta_\sigma \sqrt{rN(c)}$$

for $x, y \in K$, and similarly, we can define $-\tilde{\sigma} \in \mathrm{Aut}(E/F)$ by

$$-\tilde{\sigma}(x + y\sqrt{rN(c)}) = x^\sigma - y^\sigma \delta_\sigma \sqrt{rN(c)}.$$

The group of automorphisms of E over F consists entirely of all these maps $\tilde{\sigma}, -\tilde{\sigma}$. Hence, $|\mathrm{Aut}(E/F)| = 2|G_0| = [E : F]$, so the field extension E/F is Galois. We have a bijective map f from $\mathrm{Gal}(E/F)$ to Γ_0 such that $f((-1)^i\tilde{\sigma}) = (-1)^i e_\sigma$ $(i \in \{0, 1\})$. Observe that

$$\begin{aligned}(\tilde{\tau})(\tilde{\sigma})(\sqrt{rN(c)}) &= \delta_\tau \delta_\sigma^\tau \sqrt{rN(c)} \\ &= \zeta_{\sigma,\tau}\delta_{\tau\sigma}\sqrt{rN(c)} \\ &= \zeta_{\sigma,\tau}(\widetilde{\sigma\tau})(\sqrt{rN(c)}).\end{aligned}$$

From this observation it follows easily that f is an isomorphism, and therefore,

$$\mathrm{Gal}(E/F) \cong \Gamma_0.$$

■

While the converse implication of Theorem 1 need not hold in general, we can say more in the case that F is a p-adic field. First though, we will need to recall the definition of the Hilbert symbol of two elements of F.

1.6 The Hilbert Symbol

For the rest of this chapter, let us restrict our attention to the case when F is a local, non-Archimedean field. For two nonzero elements $a, b \in F$, set $K = F(\sqrt{a})$ and define the *Hilbert symbol*

$$(a, b)_F = \begin{cases} 1, & \text{if } b \in N_{F/K}(K^\times) \\ -1, & \text{otherwise} \end{cases}.$$

Some of the useful properties of the Hilbert symbol are listed in following lemma.

Lemma 1.6.4 *For all nonzero $a, b, c \in F$, the following properties hold for the Hilbert symbol:*

(a) $(a,b)_F = (b,a)_F$

(b) $(a,bc^2)_F = (b,a)_F$

(c) $(a,b)_F(a,c)_F = (a,bc)_F$

(d) $(a,a^{-1})_F = (a,a)_F = (a,-1)$

For a proof of this lemma, see Chapter III of [5].

1.7 The Hasse Invariant

To distinguish between quadratic forms, we will need to introduce some invariants on quadratic spaces. Let (V,Q) and (V',Q') be two quadratic spaces over F. Let q and q' be quadratic forms determined by (V,Q) and (V',Q'), respectively.

Define the *determinant* $\det(q)$ of a quadratic form q to be the determinant of the matrix M_q associated with q modulo $\dot{F}^2$, the subgroup generated by the squares of $F^\times$. This gives us an invariant on (V,Q) since, for any $P \in \mathrm{GL}(n,F)$

$$\det(PM_qP^\top) \equiv \det(M_q)(\bmod \dot{F}^2).$$

The *Hasse invariant* $S(q)$ of a quadratic form $q = <a_1,...,a_n>$ (for $a_i \in F$) is the product

$$\prod_{i<j}(a_i,a_j)_F.$$

(When $\dim(V) = 1$, we set $S(q)$ equal to 1.) One can show (see, for example, [5]) that that this product does not depend on the choice of diagonalization for q, so this is indeed an invariant on (V,Q).

In the case that F is a p-adic field, we have the following well-known theorem for quadratic forms:

Theorem 1.7.5 *Two quadratic forms q and q' over a p-adic field F are equivalent if and only if $dim(V) = dim(V')$, $S(q) = S(q')$, and $det(q) = det(q')$.*

A proof of this theorem can be found in [5]. Note that, for $\dim(V)$ odd, we could replace the condition that $S(q) = S(q')$ above with the condition that $C_0(V)$ and $C_0(V')$ belong to the same class in the Brauer group $B(F)$ of F, since the Hasse invariant of an odd dimensional quadratic space is determined by the even Clifford algebra of that space; see [5, Chapter 5] for a discussion of the details.

CHAPTER 2

WEIL INDEX

In this chapter, we will relate the Hilbert symbol to the Weil index of a quadratic field extension. This will allow us to reduce the conditions of Theorem 1.5.2 to a Gauss sum computation.

Before getting started, let us set up some notation which we will use throughout the rest of the chapter.

Unless stated otherwise, F will denote a local, non-Archimedean field, with characteristic different than 2. Let K be a finite, separable field extension of F. Then there are non-trivial, complete discrete valuations val_F and val_K on F and K, respectively. Let $\mathbb{O}_F$ be the discrete valuation ring corresponding to F and val_F – that is, the set of all elements x in F such that $\mathrm{val}_F(x) \geq 0$. Denote by π_F an element of F such that $\mathrm{val}_F(\pi_F) = 1$; π_F generates the maximal ideal $\mathfrak{p}_F$ of $\mathbb{O}_F$. The ramification index $e_{K/F} = \mathrm{val}_K(\pi_F)$, and the residue degree $f_{K/F} = [\mathcal{K} : \mathcal{F}]$, where $\mathcal{K} = \mathbb{O}_K/\mathfrak{p}_K$ is a separable field extension of $\mathcal{F} = \mathbb{O}_F/\mathfrak{p}_F$. Recall that $e_{K/F} \cdot f_{K/F}$ is equal to $n = [K : F]$.

2.1 Lattices

Let V be an n-dimensional vector space over F. A *lattice* L in V is a sub-$\mathbb{O}_F$-module of V that is free of rank n. Equivalently, a lattice L is an $\mathbb{O}_F$-module for which every generating set of n elements is a F-basis for V.

Suppose $<,>: V \otimes V \longrightarrow F$ is a nondegenerate, symmetric bilinear form. If M is any sub-$\mathbb{O}_F$-module M of V, then we define the *dual* module M^* (with respect to $<,>$) to be the set of all elements v in V such that $<v, x>$ is in $\mathbb{O}_F$ for all x in M. It is easy to see that the dual L^* of a lattice L is also a lattice. Indeed, if $\{x_1, ..., x_n\}$ is a basis for L, then $\{x_1^*, ..., x_n^*\}$ is a basis for L^* where $<x_i, x_j^*>$ is equal to the Kronecker delta of i, j.

When $V = K$, a finite, separable field extension of F, one can define a nondegenerate, symmetric F-bilinear form $<,>$ on K by setting $<x, y> = \mathrm{Tr}(xy)$ ([8, pp.204-5]). Whenever we speak of the dual of an $\mathbb{O}_F$-module in K, we will always assume that the dual is taken with respect to this form.

Proposition 2.1.6 *$\mathbb{O}_K$ is a lattice in K.*

Proof. Let $\{e_1, e_2, ..., e_n\}$ be a basis for K over F such that $e_i \in \mathbb{O}_K$. The $\mathbb{O}_F$-span L of this basis is a lattice in K. By our earlier discussion, L^* is also a lattice in K. Since $L \subset \mathbb{O}_K$, $(\mathbb{O}_K)^* \subset L^*$, so the statement that $(\mathbb{O}_K)^*$–and hence, $\mathbb{O}_K$–is a free $\mathbb{O}_F$-module of rank n follows from the fact that $\mathbb{O}_F$ is a principal ideal domain. ■

Given a basis $\{x_1, .., x_n\}$ for a lattice L, the *discriminant* $\Delta(L)$ of L is the ideal generated by the determinant of the matrix $(<x_i, x_j>)$ in $\mathbb{O}_F$. If $A \in \mathrm{GL}_n(\mathbb{O}_F)$, then

$$\det(A^t(<x_i, x_j>)A)\mathbb{O}_F = \det(A)^2\det((<x_i, x_j>))\mathbb{O}_F = \det((<x_i, x_j>))\mathbb{O}_F = \Delta(L).$$

In other words, the definition of the discriminant is independent of the choice of basis for L.

Proposition 2.1.7 *Suppose $L \subset L^*$. Let $q = |\mathcal{F}|$ and $a = \log_q([L^* : L])$. Then the discriminant $\Delta(L) = \mathfrak{p}_F^a$.*

Proof. By the stucture theory for finitely-generated modules over a PID (see, for example, [6, p.153]), we know that there is a basis for L^* – say, $\{x_1^*, .., x_n^*\}$ – such that $\{\alpha_1 x_1^*, .., \alpha_n x_n^*\}$ is a basis for L for some $\alpha_i \in \mathbb{O}_F$. Let $\{x_1, .., x_n\}$ be the basis of L corresponding to this choice of basis for L^*. On one hand, $L^*/L \cong \bigoplus \mathbb{O}_F/\alpha_i\mathbb{O}_F$ and, hence,

$$a = \log_q([L^* : L]) = \sum_{i=1}^{n} \mathrm{val}_F(\alpha_i).$$

On the other hand, there must be a matrix $A \in \mathrm{GL}_n(\mathbb{O}_F)$, corresponding to this change of basis of L, so that $(<x_i, x_j>)A = (<x_i, \alpha_j x_j^*>)$. Clearly, $(<x_i, \alpha_j x_j^*>)$ is just equal to the diagonal matrix $\mathrm{diag}(\alpha_1, ..., \alpha_n)$, so the discriminant

$$\Delta(L) = \det((<x_i, x_j>))\mathbb{O}_F = \det((<x_i, x_j>)A)\mathbb{O}_F = \alpha_1 \cdots \alpha_n\mathbb{O}_F = \mathfrak{p}_F^a.$$

■

Let us return now to the case when $V = K$. We call the lattice in K dual to $\mathbb{O}_K$ the *codifferent* of the extension K/F. The inverse of the codifferent (as a fractional ideal of K with respect to $\mathbb{O}_K$) is called the *different*, denoted by $\mathcal{D}$, of K/F and is a nonzero ideal of $\mathbb{O}_K$.

Define the discriminant Δ of the field extension K/F to be the discriminant $\Delta(\mathbb{O}_K)$. The relationship between the different and the disciminant is described in the following corollary to Proposition 2.1.7:

Corollary 2.1.8 $\mathrm{N}(\mathcal{D}) = \Delta$.

Proof. For some nonnegative integer b, $\mathcal{D} = \mathfrak{p}_K^b$. As an $\mathbb{O}_F$-module, $\mathbb{O}_K$ has index $q^a = q^{b \cdot f_{K/F}}$ (where $q = |\mathcal{F}|$) in $\mathbb{O}_K^* = \mathcal{D}^{-1} = \mathfrak{p}_K^{-b}$. Thus, $\mathrm{N}(\mathcal{D}) = \mathfrak{p}_F^a = \Delta$. ■

2.2 The Different

In this section, we will restrict our attention to lattices – specifically, $\mathbb{O}_K$ and its dual $\mathbb{O}_K^*$ – in K. We will begin by showing how to construct a basis for $\mathbb{O}_K$ as an $\mathbb{O}_F$-module.

Now, there exists an $x \in \mathbb{O}_K$ such that $\bar{x}$, the class of x modulo $\mathfrak{p}_K$, is a primitive element for $\mathcal{K}/\bar{F}$. Let $f(X)$ be a polynomial in $\mathbb{O}_F[X]$ such that, modulo $\mathfrak{p}_K$, $f(X)$ is the minimal polynomial for $\bar{x}$ over F. Hence, $f(x) \equiv 0 \bmod \mathfrak{p}_K$ and, since $\mathcal{K}$ is a separable extension of $\bar{F}$, the derivative $f'(x) \not\equiv 0 \bmod \mathfrak{p}_K$. The Taylor series expansion of f about x gives

$$f(x + \pi_K) \equiv f(x) + f'(x)\pi_K \bmod \mathfrak{p}_K^2.$$

Thus, either $f(x)$ or $f(x + \pi_K)$ is nonzero modulo $\mathfrak{p}_K^2$, so after possibly replacing x by $x + \pi_K$, we have that $f(x)$ is a uniformizer of $\mathbb{O}_K$.

By construction, $1, \bar{x}, ..., \bar{x}^{f_{K/F}-1}$ form a basis for $\mathcal{K}$ as a vector space over $\bar{F}$, so given $y \in \mathbb{O}_K$, we can inductively define y_m in the $\mathbb{O}_F$-span of

$$B = \{x^i f(x)^j \ : \ 0 \le i < f_{K/F}, 0 \le j < e_{K/F}\}$$

such that $y \equiv y_m \bmod \mathfrak{p}_K^m$. Hence, the elements of B generate $\mathbb{O}_K$, and since B contains $f_{K/F} \cdot e_{K/F} = n$ elements, B is an $\mathbb{O}_F$-basis for $\mathbb{O}_K$. Now, x is a root of a monic, degree-n polynomial $g(X) \in \mathbb{O}_F[X]$, so we have proved the following proposition:

Proposition 2.2.9 *There exists an element $x \in \mathbb{O}_K$ such that $\{1, x, ..., x^{n-1}\}$ is a basis for $\mathbb{O}_K$ as a lattice in K.*

This proposition leads us to the following useful characterization of $\mathcal{D}$:

Proposition 2.2.10 *For x and $g(X)$ as before, the different $\mathcal{D} = g'(x)\mathbb{O}_K$.*

For a proof of this proposition, see [4, pp.30-31] or [9, pp.55-57].

2.3 Ramification Groups

Suppose that the extension K of F is Galois. Let G be the Galois group $\mathrm{Gal}(K/F)$. By the previous section, there is an $x \in \mathbb{O}_K$ that generates $\mathbb{O}_K$ as an $\mathbb{O}_F$-algebra. Just as before, we will denote by $g(X)$ the minimal polynomial of x for K/F. In this case,[1]

$$\mathrm{val}_K(\mathcal{D}) = \mathrm{val}_K(g'(x)) = \mathrm{val}_K\Big(\prod_{\substack{\sigma\in G\\ \sigma\neq 1}}(x-\sigma(x))\Big) = \sum_{\substack{\sigma\in G\\ \sigma\neq 1}}\mathrm{val}_K(x-\sigma(x)). \tag{2.1}$$

Set $i_G(\sigma) = \mathrm{val}_K(x-\sigma(x))$. Since every element in $\mathbb{O}_K$ is a linear combination of $1,x,...,x^{n-1}$ over $\mathbb{O}_F$, the next lemma follows from the properties of valuations:

Lemma 2.3.11 *For all nonnegative integer i, $i_G(\sigma) \geq i$ if and only if $val_K(y-\sigma(y)) \geq i$ for every y in $\mathbb{O}_K$.*

Remark 2.3.12 *There are two immediate consequences of Lemma 2.3.11. First, the number $i_G(\sigma)$ does not depend on a choice of x. Second, specifying that $i_G(\sigma) \geq i > 0$ is equivalent to requiring that σ act trivially on $\mathbb{O}_K/\mathfrak{p}^i$.*

For each integer $i \geq -1$, let $G_i = \{\sigma \in G : i_G(\sigma) \geq i+1\}$. The groups G_i are called the *ramification groups* of G (with lower numbering) and form a decreasing sequence

$$G = G_{-1} \supset G_0 \supset G_1 ... \supset G_i \supset ...$$

where $G_i = \{1\}$ for all i large enough. For example, when K is an unramified extension of F, $G_i = \{1\}$ for all $i \geq 0$. From Lemma 2.3.11, we see that the ramification groups "behave well" with respect to subgroups – that is, for a subgroup H of G,

$$H_i = G_i \cap H,$$

where H_i is the ramification group of the subextension of K fixed by H. However, for a normal subgroup H of G, $(G/H)_i$ is not in general equal to $(G_iH)/H$. To get the ramification groups compatible with passage to quotients, we can reindex the ramification groups as follows:

---

[1] Here $\mathrm{val}_K(\mathcal{D})$ is just the valuation of a generator of $\mathcal{D}$ in K.

First, extend the domain of the function $i \longmapsto G_i$ from $\mathbb{Z}_{\geq -1}$ to $[-1, \infty) \subset \mathbb{R}$ by defining G_r to be the ramification group whose index is the largest integer less than or equal to r. Let ν be the inverse of the increasing homeomorphsim $\eta_{K/F} : [-1, \infty) \longrightarrow [-1, \infty)$ where

$$\eta_{K/F}(s) = \int_0^s \frac{dt}{[G_0 : G_t]}. \tag{2.2}$$

Then we can define the ramification groups of G *with upper numbering* to be the groups

$$G^r = G_{\nu(r)} \quad (r \geq -1).$$

With this modified numbering, the ramification groups of G now satisfy the desired property ([9, pp.74-75]):

Theorem 2.3.13 *For any normal subgroup H of G and $r \in [-1, \infty)$,*

$$(G/H)^r = G^r H/H.$$

2.4 The Norm

We will begin this section by recalling two of the main theorems in local class field theory:

Theorem 2.4.14 *[7, Theorem 1, p.243] For any abelian extension K of a non-Archimedian local field F, there exists a canonical isomorphism*

$$\phi_{K/F} : F^\times / N(K^\times) \longrightarrow Gal(K/F).$$

Theorem 2.4.15 *[7, Theorem 2, p.249] Let F be a local, non-Archimedean field. Then there is a one-to-one correspondence between open subgroups of finite index in $F^\times$ and subgroups of the form $N(K^\times)$ for some finite abelian extension K of F.*

Let χ be a quadratic character on $F^\times$. The kernel of χ is an open subgroup in $F^\times$ of index 2, so by Theorem 2.4.15, there exists an abelian extension K such that $\ker(\chi) = N(K^\times)$. By Theorem 2.4.14, K/F is a quadratic extension since

$$[K : F] = [F : \mathrm{N}(K^\times)] = 2.$$

Denote by U_i the multiplicative subgroup $1+\pi_F^i\mathcal{O}_F$ of $F^\times$ ($i \in \mathbb{Z}_{\geq 0}$). If c is the smallest integer such that $U_i \subset \ker(\chi) = \mathrm{N}(K^\times)$, then the ideal $\mathfrak{p}_F^c$ is called the *conductor*, denoted $\mathfrak{f}(\chi)$, of χ. One can show (see [4, Chapter 7, §4]) that

$$\phi_{K/F}(U_i) = \mathrm{Gal}(K/F)^i \qquad (i \in \mathbb{Z}_{\geq 0}),$$

so $U_i \subset \mathrm{N}(K^\times)$ precisely when $\mathrm{Gal}(K/F)^i = 1$.

Let σ be the nontrivial element of $G = \mathrm{Gal}(K/F)$. From (2.2), we see that $\eta_{K/F}(r) = r$ for $-1 \leq r < i_G(\sigma)$ and $\eta_{K/F}(2r + i_G(\sigma) - 1) = r + i_G(\sigma) - 1$ for $r > 0$, so $G_i = G^i$ for all integers $i \geq -1$. This implies that $G^i = 1$ if and only if $i_G(\sigma) \leq i$. Hence, by (2.1), the valuation of the different

$$\mathrm{val}_K(\mathcal{D}) = i_G(\sigma) = \mathrm{val}_F(\mathfrak{f}(\chi)). \tag{2.3}$$

Notice that this is simply a specific example of the *conductor-discriminant theorem* ([4, pp.113-4]):

Theorem 2.4.16 *If Δ is the discriminant of a finite, abelian extension of local fields K/F,*

$$\Delta = \prod_{\chi} \mathfrak{f}(\chi),$$

where this product is taken over all characters[2] *χ whose kernel contains $N(K^\times)$.*

2.5 The Weil Index

Let F be a local field with characteristic different than 2, and let $K = F[\sqrt{d}]$ for some $d \in F$. Fix an additive character ψ on F.

There is an isomorphism from K to its dual K^* (as a vector space over F) given by the map[3]

$$\rho : x \longmapsto (x^* : y \longmapsto \mathrm{Tr}(y\bar{x})).$$

Now K admits a Haar measure[4] dx (unique up to scalar), and for f in $\mathcal{S}(K)$, the Bruhat-Schwartz space of functions on K, denote the Fourier transform

$$\mathcal{F}(f) : y^* \longmapsto \int_K \psi(y^*(x))f(x)dx.$$

---

[2] Via $\phi_{K/F}$, we can think of these characters as those on G.

[3] Of course, when $K = F$, x^* is just the map given by multiplication by x.

[4] Throughout this discussion, we treat K as a F-vector space, so we are implicitly using the additive group structure on K and K^*.

There exists a Haar measure dx^* on K^* dual to dx with respect to this Fourier transform–i.e., such that

$$f(-x) = \mathcal{F}(\mathcal{F}(f))(x) = \int_{K^*} \psi(y^*(x))\mathcal{F}(f)(y^*)dy^*.$$

Recall that a continuous linear functional from $\mathcal{S}(K)$ to $\mathbb{C}$ is called a *tempered distribution* on (the additve group underlying) K. For example, the map

$$fdx : \phi \longmapsto \int_K \phi(x)f(x)dx, \quad \phi \in \mathcal{S}(K),$$

is a tempered distribution for any given continuous, bounded, complex-valued function f on K. The Fourier transform of a tempered distribution u on K is a tempered distribution $\mathcal{F}(u)$ on K^* such that, for $\phi^* \in \mathcal{S}(K^*)$,

$$\mathcal{F}(u)(\phi^*) = u(\mathcal{F}(\phi^*)).$$

The following theorem relates the two tempered distributions $\psi \circ \mathrm{N}\ dx$ and $\frac{1}{\psi \circ \mathrm{N} \circ \rho^{-1}} dx^*$ and leads us to the definition of the Weil index.

Theorem 2.5.17 *There exists a complex constant $\gamma(K/F)$ such that*

$$\mathcal{F}(\psi \circ N\ dx) = \gamma(K/F)|c_\rho|^{-1/2} \frac{1}{\psi \circ N \circ \rho^{-1}} dx^*, \tag{2.4}$$

where $|c_\rho|$ is the modulus defined such that $dx^* = |c_\rho|dx$. The constant $\gamma(K/F)$ is independent of the choice of dual Haar measures dx and dx^*.

We call $\gamma(K/F)$ the *Weil index* of the field extension K/F. Note that the definition here is actually a special case of the usual Weil index for a character of second degree. In fact, observe that, when K is a nontrivial extension of F,

$$\mathrm{N}(a+b) = a\bar{a} + a\bar{b} + b\bar{a} + b\bar{b} = \mathrm{N}(a) + \mathrm{Tr}(a\bar{b}) + \mathrm{N}(b), \tag{2.5}$$

so $\psi(\mathrm{N}(x+y))\psi(\mathrm{N}(x))^{-1}\psi(\mathrm{N}(y))^{-1} = \psi(\mathrm{Tr}(x\bar{y})) = \psi(\mathrm{Tr}(y\bar{x}))$ is a bicharacter in x and y–i.e., $\psi \circ \mathrm{N}$ is a nondegenerate character of second degree.

We will sometimes denote $\gamma(F[\sqrt{d}]/F)$ by $\gamma(\chi)$, where χ is the quadratic character of F such that $N(F[\sqrt{d}]^\times) = \ker(\chi)$, or (when F is clear from context) just by $\gamma(d)$. The following theorem, proved by Weil, shows that the failure of the Weil index to be multiplicative is captured by the Hilbert symbol $(\cdot,\cdot)_F$ on F.

Theorem 2.5.18 *For $a, b \in F$,*

$$\gamma(ab) = (a,b)_F \gamma(a)\gamma(b).$$

Corollary 2.5.19 *The following identities hold for all $a, b \in F$.*

(a) $\gamma(ab^2) = \gamma(a)$

(b) $\gamma(1) = 1$

(c) $\gamma(a)$ *is a fourth root of unity.*

Proof. Part (a) is immediate from the definition of the Weil index. Since $(1,1)_F = 1$, (b) follows from Theorem 2.5.18 (using $a = b = 1$). Finally, (c) follows from the observation that

$$\gamma(a)^4 = [(a,b)_K \gamma(a)^2]^2 = \gamma(a^2)^2 = 1.$$

■

A simple inductive argument using Theorem 2.5.18 together with the bi-multiplicativity of the Hilbert symbol gives the next corollary.

Corollary 2.5.20 *For $a_1, a_2, ..., a_n \in F$,*

$$\gamma\left(\prod_{i=1}^{n} a_i\right) = \prod_{i<j} (a_i, a_j)_F \prod_{i=1}^{n} \gamma(a_i).$$

Observe that $\prod_{i<j}(a_i, a_j)_F$ is precisely the Hasse invariant of the quadratic form

$$Q(x) = \sum_{i=1}^{n} a_i x_i^2.$$

2.6 Computing the Weil Index over $\mathbb{Q}_{2^n}$

Let us restrict our attention to the case when $F = \mathbb{Q}_{2^n}$. Let χ be a quadratic character on F of conductor $\mathfrak{p}_F^2$, and let K be the quadratic extension of F associated with χ. Because χ has conductor $\mathfrak{p}_F^2$, K is a (totally) ramified extension of F, and by (2.3), we have that the codifferent $\mathcal{D}^{-1} = \mathfrak{p}_K^{-2}$.

Let $\psi(x)$ be an additive character on F whose kernel is $\mathcal{O}_F$. If $\phi_{\mathcal{O}_K}$ denotes the characteristic function of $\mathcal{O}_K$, then

$$\mathcal{F}(\phi_{\mathcal{O}_K})(y^*) = \int_K \psi(\mathrm{Tr}(x\bar{y}))\phi_{\mathcal{O}_K}(x)dx$$

Since $\psi \circ y^*$ is an additive character on $\mathcal{O}_K$, the above integral is nonzero if and only if $\psi \circ y^*$ is trivial on $\mathcal{O}_K$ – i.e., y is contained in the codifferent $\mathcal{D}^{-1}$. We may assume that the measure dx is normalized so that the volume of $\mathcal{O}_K$ is $\frac{1}{2^n}$. Hence,

$$\mathcal{F}(\phi_{\mathcal{O}_K})(y^*) = \int_{\mathcal{O}_K} dx \cdot \phi_{\mathcal{D}^{-1}}(y) = \frac{1}{2^n}\phi_{\mathcal{D}^{-1}}(y).$$

Consequently,

$$\int_K \psi(\mathrm{Tr}(\bar{y}x))\mathcal{F}(\phi_{\mathcal{O}_K})(y^*)dy = \frac{1}{2^n}\int_K \psi(\mathrm{Tr}(\bar{y}x))\phi_{\mathcal{D}^{-1}}(y)dy = \frac{1}{2^n}\int_{\mathcal{D}^{-1}} dx\cdot\phi_{\mathcal{O}_K}(x) = \phi_{\mathcal{O}_K}(-x).$$

This implies that, in this case, $dx^* = dx$ and $|c_\rho| = 1$.

Theorem 2.6.21 *For F, K, ψ, and χ as above, χ induces a quadratic character $\overline{\chi}$ on $(\mathcal{O}_K/\mathfrak{p}_K^2)^\times$, and the Weil index*

$$\gamma(K/F) = \frac{1}{2^n}\sum_{x\in(\mathcal{O}_F/\mathfrak{p}_F^2)^\times} \overline{\chi}(x)\psi(x/\pi_F^2),$$

where $\pi_F = N(\pi_K)$ for some uniformizer π_K of K.

Proof. Apply both sides of (2.4) to the function $\phi_{\mathcal{O}_K} \circ \rho^{-1}$. Considering the right-hand side applied to $\phi_{\mathcal{O}_K} \circ \rho^{-1}$, we have that

$$\begin{aligned}
\gamma(K/F)|c_\rho|^{-1/2}\int_{K^*} \frac{1}{\psi(\mathrm{N}(\rho^{-1}(x^*)))}\phi_{\mathcal{O}_K}(\rho^{-1}(x^*))dx^* &= \gamma(K/F)\int_K \frac{1}{\psi(\mathrm{N}(x))}\phi_{\mathcal{O}_K}(x)dx \\
&= \gamma(K/F)\int_{\mathcal{O}_K} \frac{1}{\psi(\mathrm{N}(x))}dx \\
&= \gamma(K/F)\int_{\mathcal{O}_K} dx \\
&= \frac{1}{2^n}\gamma(K/F).
\end{aligned}$$

Turning our attention now to the left-hand side, we first compute

$$\mathcal{F}(\phi_{\mathcal{O}_K}\circ\rho^{-1})(x) = \int_{K^*}\psi(\mathrm{Tr}(\bar{x}y))\phi_{\mathcal{O}_K}(\rho^{-1}(y^*))dy^* = \int_{\mathcal{O}_K}\psi(\mathrm{Tr}(\bar{x}y))dy = \frac{1}{2^n}\phi_{\mathcal{D}^{-1}}(x).$$

Thus, we have that

$$\gamma(K/F) = \int_K \phi_{\mathcal{D}^{-1}}(x)\psi(\mathrm{N}(x))dx.$$

By (2.5), $\psi \circ \mathrm{N}$ is constant on each coset of $\mathcal{O}_K$ in $\mathcal{D}^{-1}$, so we have that

$$\int_{\mathcal{D}^{-1}} \psi(\mathrm{N}(x))dx = \sum_{x \in \mathcal{D}^{-1}/\mathcal{O}_K} \psi(\mathrm{N}(x)) \cdot \frac{1}{2^n} = \frac{1}{2^n} \sum_{x \in \mathcal{O}_K/\mathfrak{p}_K^2} \psi(\mathrm{N}(x/\pi_K^2)) = \frac{1}{2^n} \sum_{x \in \mathcal{O}_K/\mathfrak{p}_K^2} \psi(\mathrm{N}(x)/\pi_F^2).$$

The norm map induces a isomorphism from $\mathfrak{p}_K/\mathfrak{p}_K^2$ to $\mathfrak{p}_F/\mathfrak{p}_F^2$. Indeed, under the identification of $\alpha\pi_K + \mathfrak{p}_K^2$ and $\beta\pi_F + \mathfrak{p}_F^2$ with $\alpha, \beta \in \mathbb{F}_{2^n}$ respectively, this is just the Frobenius automorphism on $\mathbb{F}_{2^n}$. Since the map $x \longmapsto \psi(x/\pi_F^2)$ is a nontrivial additive character on the group $\mathfrak{p}_F/\mathfrak{p}_F^2$, $\gamma(K/F)$ is equal to

$$\frac{1}{2^n} \sum_{x \in (\mathcal{O}_K/\mathfrak{p}_K^2)^\times} \psi(\mathrm{N}(x)/\pi_F^2).$$

Since χ has conductor $\mathfrak{p}_F^2$, $1 + \mathfrak{p}_F^2$ is contained in $\mathrm{N}(\mathcal{O}_F)$, so χ induces a quadratic character $\overline{\chi}$ on $(\mathcal{O}_F/\mathfrak{p}_F^2)^\times$. Hence,

$$\begin{aligned}
\gamma(K/F) &= \frac{1}{2^n} \sum_{x \in (\mathcal{O}_K/\mathfrak{p}_K^2)^\times} \psi(\mathrm{N}(x)/\pi_F^2) = \frac{1}{2^n} \cdot 2 \sum_{x \in \ker \overline{\chi}} \psi(x/\pi_F^2) \\
&= \frac{1}{2^n} \cdot 2 \sum_{x \in \ker \overline{\chi}} \psi(x/\pi_F^2) - \frac{1}{2^n} \sum_{x \in (\mathcal{O}_F/\mathfrak{p}_F^2)^\times} \psi(x/\pi_F^2) \\
&= \frac{1}{2^n} \sum_{x \in (\mathcal{O}_F/\mathfrak{p}_F^2)^\times} \overline{\chi}(x)\psi(x/\pi_F^2).
\end{aligned}$$

The third equality follows from the simple observation below. ■

Remark 2.6.22 *Observe that*

$$\sum_{x \in (\mathcal{O}_F/\mathfrak{p}_F^2)^\times} \psi(x/\pi_F^2) = \sum_{x \in (\mathcal{O}_F/\mathfrak{p}_F^2)} \psi(x/\pi_F^2) - \sum_{x \in (\mathfrak{p}_F/\mathfrak{p}_F^2)} \psi(x/\pi_F^2).$$

Since both sums on the right-hand side are obviously 0, we conclude the left-hand side must be 0 as well.

Note that $\gamma(K/F)$ gives us Tate's epsilon factor associated with the character χ (assuming χ is trivial on 2) [11], so we can express this factor explicitly using the Gauss sum in Theorem 2.6.21. We will discuss this in more detail in Chapter 4.

CHAPTER 3

GAUSS SUM COMPUTATION

The Gauss sum of Theorem 2.6.21 is difficult to calculate for general quadratic characters on $\mathbb{Q}_{2^n}$, so instead, we will show that the number of quadratic characters whose Gauss sum is equal to a given fourth root of unity corresponds with the number of points in $\mathbb{F}_{2^n}$ on the elliptic curve

$$Y^2 + Y = X^3 - X.$$

This will allow us to prove an equidistribution of Gauss sums for quadratic characters on $\mathbb{Q}_{2^n}$.

3.1 Sum of All Gauss Sums

Let $n = 2m + 1$ for some integer m greater than 0, and for every postive integer l, let R_{2^n} denote the quotient $\mathbb{Z}_{2^n}/4\mathbb{Z}_{2^n}$. An element of R_{2^n} can be uniquely represented as the pair (a, b) for some $a, b \in \mathbb{F}_{2^n}$ with addition and multiplication defined as follows:

$$(a_0, b_0) + (a_1, b_1) = (a_0 + a_1, b_0 + b_1 + a_0 a_1),$$
$$(a_0, b_0)(a_1, b_1) = (a_0 a_1, a_0^2 b_1 + a_1^2 b_0),$$

for $a_i, b_i \in \mathbb{F}_{2^n}$ (see Chapter II, §6, of [9]). Fr induces a homomorphism $\overline{\mathrm{Fr}} : R_{2^n} \longrightarrow R_{2^n}$, and $\mathrm{Tr}_{\mathbb{Q}_{2^n}/\mathbb{Q}_2}$ induces an R_2-linear map $T : R_{2^n} \longrightarrow R_2$, which, for $(a, b) \in R_{2^n}$, can be explicitly expressed as

$$\begin{aligned}(a,b) + \overline{\mathrm{Fr}}((a,b)) + ... + \overline{\mathrm{Fr}}^{n-1}((a,b)) &= (a,b) + (a^2, b^2) + ... + (a^{2^{n-1}}, b^{2^{n-1}}) \\ &= (a + a^2, b + b^2 + a^3) + (a^4, b^4) + ... + (a^{2^{n-1}}, b^{2^{n-1}}) \\ &= (\mathrm{tr}(a), \mathrm{tr}(b) + \sum_{i=1}^{n-1} \sum_{j=0}^{i-1} a^{2^i + 2^j}),\end{aligned}$$

where tr here denotes the field trace of the extension $\mathbb{F}_{2^n}/\mathbb{F}_2$. If $n = 3$, we have that

$$\sum_{i=1}^{n-1} \sum_{j=0}^{i-1} a^{2^i + 2^j} = a^3 + a^5 + a^6 = \mathrm{tr}(a^3).$$

We leave it as an exercise for the reader to verify that, if $n = 5$,

$$\sum_{i=1}^{n-1}\sum_{j=0}^{i-1} a^{2^i+2^j} = \mathrm{tr}(a^3) + \mathrm{tr}(a^5).$$

These examples suggest that we may be able to express the double sum $\sum_{i=1}^{n-1}\sum_{j=0}^{i-1} a^{2^i+2^j}$ in terms of trace for general (odd) n. This relationship is made clearer in the proceeding lemma.

Lemma 3.1.23 *For an odd integer $n > 1$ and $a \in \mathbb{F}_{2^n}$,*

$$\sum_{i=1}^{n-1}\sum_{j=0}^{i-1} a^{2^i+2^j} = \sum_{t=1}^{m} \mathrm{tr}(a^{2^t+1}).$$

Proof. Let $S_1 = \{2^i + 2^j : 1 \le i \le n-1,\ 0 \le j \le i-1\}$ and $S_2 = \{(2^s+1)2^t : 0 \le s < n,\ 1 \le t \le m\}$, where both sets are thought of as subsets of $\mathbb{Z}/(2^n-1)\mathbb{Z}$. First of all, it is clear that $S_2 \subset S_1$. Second, suppose $2^i + 2^j \in S_1$ $(1 \le i \le n-1,\ 0 \le j \le i-1)$. If $i - j \le m$, then

$$2^i + 2^j = (2^{i-j}+1)2^j \in S_2.$$

If $i - j > m$, then $n - 1 - i + j < m$, so

$$2^i + 2^j = (2^{n-i-j}+1)2^{i-n} \equiv (2^{n-i-j}+1)2^i \bmod (2^n - 1)$$

is an element of S_2. Hence, $S_1 \subset S_2$. Therefore, we have that

$$\sum_{i=1}^{n-1}\sum_{j=0}^{i-1} a^{2^i+2^j} = \sum_{x\in S_1} a^x = \sum_{y\in S_2} a^y = \sum_{t=1}^{m}\sum_{s=0}^{n-1} a^{(2^s+1)2^t} = \sum_{t=1}^{m} \mathrm{tr}(a^{2^t+1}).$$

■

By abuse of notation, we will treat T as a map from R_{2^n} to $\mathbb{Z}/4\mathbb{Z}$ where elements of R_2 have been identified with those of $\mathbb{Z}/4\mathbb{Z}$ via the isomorphism $\mathbb{Z}/4\mathbb{Z} \longrightarrow R_2$ (induced canonically by the homomorphism $\mathbb{Z} \longrightarrow R_2$ sending n to $n(1,0)$). Accordingly, we define an additive map $\psi : R_{2^n} \longrightarrow \{\pm 1, \pm i\} \subset \mathbb{C}^*$ by setting $\psi(x) = e^{\pi i T(x)/2}$ for all $x \in R_{2^n}$.

Given a quadratic character χ on the multiplicative group G underlying R_{2^n}, use ψ to define the Gauss sum

$$g(\chi) = \sum_{x \in G} \chi(x)\psi(x).$$

Suppose χ is a quadratic character of G. If χ is trivial on G, we have already seen that $g(\chi) = 0$ by Remark 2.6.22. Otherwise,

$$g(\chi)^2 = \chi(-1)2^{2n}.$$

We claim that $\chi(-1)$ is -1 for half of the quadratic characters χ of G and 1 for the other half. To show this, we will use the next lemma, which follows easily from the orthogonality relations on characters (c.f. [6, Chapter XVIII, §5]):

Lemma 3.1.24 *Let G be any finite, abelian group. Denote by $G\hat{}$ the group of quadratic characters of G. If A is $\bigcap_{\chi \in G\hat{}} \ker(\chi)$, then*

$$\sum_{\chi \in G\hat{}} \chi(x) = \begin{cases} 0 & x \notin A \\ |G/A| & x \in A \end{cases}.$$

In our case, let A be the subgroup $\{(a, 0) : a \in \mathbb{F}_{2^n}^*\}$ of G.

Remark 3.1.25 *It is easy to see that $A = \bigcap_{\chi \in G\hat{}} \ker(\chi)$ and that G/A is isomorphic to $\mathbb{F}_{2^n}$ (where the latter is considered as an additive group).*

Since $-1 = (1, 1) \notin A$, the claim follows from Lemma 3.1.24.

By all of the above work, the number of distinct $\chi \in G\hat{}$ for which $g(\chi)$ equals a particular value can be determined from the sum

$$\frac{1}{2^n} \sum_{\chi \in G\hat{}} g(\chi) = \frac{1}{2^n} \sum_{\chi \in G\hat{}} \sum_{x \in G} \chi(x)\psi(x) = \frac{1}{2^n} \sum_{x \in G} \psi(x) \sum_{\chi \in G\hat{}} \chi(x) = \sum_{x \in A} \psi(x),$$

where, in particular, the last equality follows from Lemma 3.1.24 and the remarks proceeding it.

From the definition of ψ, one is led at this point to ask for what $z \in \mathbb{F}_{2^n}$ does

$$\sum_{i=1}^{m} \mathrm{tr}(z^{2^i+1}) = \mathrm{tr}(z).$$

We will see that the answer to this question depends on whether the trace of z is 0 or 1.

3.2 Equidistribution of Gauss Sums

To help us answer the question asked in the previous section, we will prove the following lemma and its corollary.

Lemma 3.2.26 *If n is an odd integer, there is a two-to-one correspondence between the set of $x \in \mathbb{F}_{2^n}$ such that $\mathrm{tr}(x) = \mathrm{tr}(x^3)$ and the set of $z \in \mathbb{F}_{2^n}$ such that*

$$\sum_{i=1}^{m} \mathrm{tr}(z^{2^i+1}) = \mathrm{tr}(z) = 0.$$

Proof. Consider the linear map $L : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ given by $L(x) = x^2 + x$. Obviously, $\mathrm{tr}(x^2 + x) = 0$ for all $x \in \mathbb{F}_{2^n}$, so $L(\mathbb{F}_{2^n})$ is exactly the set of all traceless elements of $\mathbb{F}_{2^n}$.

Given $x \in \mathbb{F}_{2^n}$, evaluate the sum

$$\sum_{i=1}^{m} L(x)^{2^i+1} = \sum_{i=1}^{m} (x + x^2)^{2^i+1}.$$

Each summand can be expanded as follows:

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

Hence, after cancellation, our sum becomes

$$\sum_{i=1}^{m} L(x)^{2^i+1} = x^3 + x^4 + x^{2^{(n+1)/2}+1} + x^{2^{(n+1)/2}+2}.$$

Take the trace of both sides. Since

$$(2^{(n+1)/2} + 2)2^m = 2^n + 2^{(n+1)/2} \equiv 2^{(n+1)/2} + 1 \bmod (2^n - 1),$$

$\mathrm{tr}(x^{2^{(n+1)/2}+1})$ is equal to $\mathrm{tr}(x^{2^{(n+1)/2}+2})$, so $\mathrm{tr}(x) = \mathrm{tr}(x^3)$ if and only if $\sum_{i=1}^{m} \mathrm{tr}(L(x)^{2^i+1}) = 0$. That L defines a 2-to-1 correspondence on the given sets follows from the observation that $\mathrm{tr}((x+1)^3) = \mathrm{tr}(x+1)$ if and only if $\mathrm{tr}(x^3) = \mathrm{tr}(x)$. ■

Corollary 3.2.27 *If $n = 2m + 1$ for a positive integer m, there is a two-to-one correspondence between the set of $x \in \mathbb{F}_{2^n}$ such that $\mathrm{tr}(x) = \mathrm{tr}(x^3)$ and the set of $z \in \mathbb{F}_{2^n}$ such that $\mathrm{tr}(z) = 1$ and*

$$\sum_{i=1}^{m} \mathrm{tr}(z^{2^i+1}) = m.$$

Proof. Define a linear map $L' : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ by $L'(x) = x^2 + x + 1$. Proceed by an argument very similar to that for Lemma 3.2.26, using L' instead of L. ■

Remark 3.2.28 *In the proofs of Lemma 3.2.26 and its corollary, we also showed that every traceless element of $\mathbb{F}_{2^n}$ is equal to $y+y^2$ for precisely two $y \in \mathbb{F}_{2^n}$ and, similarly, that every trace 1 element of $\mathbb{F}_{2^n}$ equals $y + y^2 + 1$ for precisely two $y \in \mathbb{F}_{2^n}$.*

By the above remark, $\mathrm{tr}(x^3) = \mathrm{tr}(x)$ $(x \in \mathbb{F}_{2^n})$ only when $x^3 + x = y^2 + y$ for some $y \in \mathbb{F}_{2^n}$, so our sum of Gauss sums can be computed from the number of points of $\mathbb{F}_{2^n}$ lying on the curve $E : y^2 + y = x^3 - x$. Before turning the machinery of elliptic curves to bear upon this problem, we need to verify that E is actually nonsingular over $\mathbb{F}_2$.

Recall that, for a curve E given by a Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

the discriminant Δ of E is defined as the sum

$$-(a_1^2 + 4a_2)^2(a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2) - 8(2a_4 + a_1a_3)^3 - 27(a_3^2 + 4a_6)^2 + 9(a_1^2 + 4a_2)(2a_4 + a_1a_3)(a_3^2 + 4a_6).$$

In the case of the curve $E : y^2 + y = x^3 - x$ (in nonhomogeneous coordinates $x = X/Z$ and $y = Y/Z$), Δ is 37, so the discriminant of E is nonzero over $\mathbb{F}_2$.

Proposition 3.2.29 *[10, Proposition 1.4, p.45] A curve given by a Weierstrass equation is nonsingular if and only if its discriminant is nonzero.*

Having verified that our curve is indeed an elliptic curve over $\mathbb{F}_2$, we may now apply the following proposition:

Proposition 3.2.30 *[10, Theorem 2.3.1, p.142] For an elliptic curve E defined over $\mathbb{F}_q$, the number $\#E(\mathbb{F}_{q^n})$ of points on E over the finite field $\mathbb{F}_{q^n}$ is*

$$q^n + 1 - \alpha^n - \beta^n,$$

where α and β are complex conjugates with norm $\sqrt{q}$.

Clearly, there are 5 points on the elliptic curve $E : y^2 + y = x^3 - x$ over $\mathbb{F}_2$, including the point at infinity, $[0 : 1 : 0]$ (written in homogeneous coordinates $[X : Y : Z]$), so $2\mathrm{Re}(\alpha) = \alpha + \beta = 2$. Because $|\alpha| = |\beta| = \sqrt{2}$, α and β must the conjugates $-1 \pm i$, and if $n = 2m + 1$,

$$\begin{aligned}\#E(\mathbb{F}_{2^n}) &= 2^n + 1 - (-1-i)^n - (1+i)^n = 2^n + 1 - (2i)^m(-1-i) - (-2i)^m(-1+i) \\ &= \begin{cases} 2^n + 1 + 2^{m+1} & \text{if } m \equiv 0, 3 \bmod (4) \\ 2^n + 1 - 2^{m+1} & \text{if } m \equiv 1, 2 \bmod (4) \end{cases}\end{aligned}$$

If, for example, m is congruent to 0 modulo 4, the number of $a \in \mathbb{F}_{2^n}^*$ such that $\psi((a, 0)) = 1$ is $\frac{1}{4}(2^n + 2^{m+1}) - 1$ by Lemma 3.2.26 and Remark 3.2.28. By Corollary 3.2.27, the number of $b \in \mathbb{F}_{2^n}^*$ such that $\psi((b, 0)) = i$ is $\frac{1}{4}(2^n + 2^{m+1})$. Since ψ is either 1 or -1 for $2^{n-1} - 1$ elements of A and is either i or $-i$ for the other 2^{n-1} elements of A,

$$\frac{1}{2^n} \sum_{\chi \in G\hat{}} g(\chi) = 2^m - 1 + 2^m i$$

in this case. More generally, we have

$$\frac{1}{2^n} \sum_{\chi \in G\hat{}} g(\chi) = \begin{cases} 2^m - 1 + 2^m i & \text{if } m \equiv 0 \bmod (4) \\ -2^m - 1 + 2^m i & \text{if } m \equiv 1 \bmod (4) \\ -2^m - 1 - 2^m i & \text{if } m \equiv 2 \bmod (4) \\ 2^m - 1 - 2^m i & \text{if } m \equiv 3 \bmod (4) \end{cases}.$$

For $\alpha \in \{0, \pm 1, \pm i\}$, Let $\theta_n(\alpha)$ denote the number of χ in $(R_{2^n}^\times)\hat{}$ such that $2^{-n} g(\chi) = \alpha$. We summarize our results in Table 3.1.

From this table, we immediately obtain a proof for a sort of equidistribution of the values of all the nontrivial Gauss sums $g(\chi)$:

Theorem 3.2.31 *Let α be either 1, -1, i, or $-i$. If $\theta_n(\alpha)$ is defined as before, then*

$$\lim_{n \longrightarrow \infty} \frac{\theta_n(\alpha)}{|(R_{2^n}^\times)\hat{}|} = \lim_{n \longrightarrow \infty} \frac{\theta_n(\alpha)}{2^n} = \frac{1}{4}.$$

Table 3.1. Values of θ_n

$m \bmod (4)$	$\theta_{2m+1}(0)$	$\theta_{2m+1}(1)$	$\theta_{2m+1}(-1)$	$\theta_{2m+1}(i)$	$\theta_{2m+1}(-i)$
0	1	$2^{n-2} + 2^{m-1} - 1$	$2^{n-2} - 2^{m-1}$	$2^{n-2} + 2^{m-1}$	$2^{n-2} - 2^{m-1}$
1	1	$2^{n-2} - 2^{m-1} - 1$	$2^{n-2} + 2^{m-1}$	$2^{n-2} + 2^{m-1}$	$2^{n-2} - 2^{m-1}$
2	1	$2^{n-2} - 2^{m-1} - 1$	$2^{n-2} + 2^{m-1}$	$2^{n-2} - 2^{m-1}$	$2^{n-2} + 2^{m-1}$
3	1	$2^{n-2} + 2^{m-1} - 1$	$2^{n-2} - 2^{m-1}$	$2^{n-2} - 2^{m-1}$	$2^{n-2} + 2^{m-1}$

3.3 Quadratic Characters of Conductor $4\mathbb{Z}_{2^n}$

Let χ be any nontrivial quadratic character on $F = \mathbb{Q}_{2^n}$, and let a be an element of the set

$$S_\chi = \{d \in \mathbb{Q}_{p^n}^\times : \mathrm{N}(F[\sqrt{d}]^\times) = \ker(\chi)\}.$$

We have already seen in Section 2.4 that S_χ is nonempty.

Lemma 3.3.32 *Let $d \in S_\chi$, and let $K = F[\sqrt{d}]$. Then*

$$val_F(d) \equiv val_F(\mathfrak{f}(\chi)) \ mod\ 2.$$

Proof. Let σ denote the nontrivial element of $\mathrm{Gal}(K/F)$. There exist $x, y \in K$ such that $\mathbb{O}_K = \mathbb{O}_F[x + y\sqrt{d}]$. By (2.3),

$$\begin{aligned}\mathrm{val}_F(\mathfrak{f}(\chi)) &= i_\sigma(x + y\sqrt{d}) = \mathrm{val}_K(x + y\sqrt{d} - \sigma(x + y\sqrt{d})) \\ &= \mathrm{val}_K(2y\sqrt{d}) = \mathrm{val}_K(2) + \frac{1}{2}\mathrm{val}_K(d) + \mathrm{val}_K(y).\end{aligned}$$

If K is a ramified extension of F, $\frac{1}{2}\mathrm{val}_K(d) = \mathrm{val}_F(d)$ and $\mathrm{val}_K(2), \mathrm{val}_K(y) \equiv 0 \bmod 2$. If K is an unramified extension of F, $\mathrm{val}_F(\mathfrak{f}(\chi)) = 0$ and

$$\mathrm{val}_F(d) = \mathrm{val}_K(d) = 2\mathrm{val}_F(\mathfrak{f}(\chi)) - 2\mathrm{val}_K(2) - 2\mathrm{val}_K(y) \equiv 0 \bmod 2.$$

In either case, the lemma holds. ■

Remark 3.3.33 *From Lemma 3.3.32, we observe that a quadratic character χ of F has conductor $4\mathbb{Z}_{2^n}$ if and only if there is a $d \in S_\chi$ such that d is a unit and $F[\sqrt{d}]$ is a ramified extension of F.*

We can define a new character χ_1 on F by composing χ with the Frobenius automorphism Fr of $F/\mathbb{Q}_2$. Notice that

$$\ker(\chi \circ \mathrm{Fr}) = \mathrm{Fr}^{-1}(\ker(\chi)) = \{x^2 + \mathrm{Fr}^{-1}(a)y^2 : x, y \in F\}.$$

That is, χ_1 corresponds with the extension $F[\sqrt{\mathrm{Fr}^{-1}(a)}]$ of F (in the sense of Section 2.4). More generally, set $\chi_i = \chi \circ \mathrm{Fr}^i$ $(0 \le i \le p-1)$, so $\mathrm{Fr}^{-i}(a)$ is in S_{χ_i}. Here we use the usual convention that Fr^0 just denotes the identity map on F.

We will spend the remainder of this chapter proving the following theorem:

Theorem 3.3.34 *Let n be an odd number greater than 3. For any integer $d > 1$, let $c(d)$ denote the order of 2 in $(\mathbb{Z}/d\mathbb{Z})^\times$, and let $\phi(d)$ denote $|(\mathbb{Z}/d\mathbb{Z})^\times|$. If*

$$\theta_n(-1) < \prod_{\substack{d|n \\ d\neq 1}} (2^{c(d)} - 1)^{\phi(d)/c(d)},$$

then there exists a quadratic character χ on $\mathbb{Q}_{2^n}^\times$ of conductor $4\mathbb{Z}_{2^n}$ and a unit $a \in S_\chi$ satisfying the following conditions:

(i) $(N_{F/\mathbb{Q}_2}(a), 2)_{\mathbb{Q}_2} = 1$.

(ii) $\prod_{i=0}^{n-1} \overline{\chi}_i^{c_i}$ *is trivial,*[1] *for $c_i \in \{0,1\}$ if and only if $c_i = c_j$ for all $0 \leq i, j \leq n-1$.*

(iii) The Hasse invariant of the quadratic form $\sum_{i=0}^{n-1} Fr^j(a)x_i^2$ is trivial.

The χ given by the above theorem will allow us to construct a multiquadratic field extension of $\mathbb{Q}_{2^n}$ that is a Galois over $\mathbb{Q}_2$ and which satisfies the hypotheses of Theorem 1.5.2. This construction will be handled in detail in the next chapter.

Remark 3.3.35 *Condition (i) of Theorem 3.3.34 implies that $(a,2)_{\mathbb{Q}_{2^n}} = (N_{F/\mathbb{Q}_2}(a), 2)_{\mathbb{Q}_{2^n}} = 1$, so (i) and (ii) give us that*

$$\prod_{i=0}^{n-1} \chi_i^{c_i} \text{ is trivial, for } c_i \in \{0,1\} \iff c_i = c_j \text{ for all } 0 \leq i, j \leq n-1.$$

Suppose χ satisfies condition (ii) of Theorem 3.3.34. By Corollary 2.5.20 and Theorem 2.6.21, condition (iii) is equivalent to requiring that

$$\begin{aligned} 1 &= \gamma\left(\prod_{i=0}^{n-1} \mathrm{Fr}^i(a)\right) \prod_{i=0}^{n-1} \gamma(\mathrm{Fr}^i(a))^{-1} = \gamma(N_{F/\mathbb{Q}_2}(a)) \prod_{i=0}^{n-1} \left[\frac{1}{2^n} \sum_{x \in (\mathbb{Z}_{2^n}/\mathfrak{p}_F^2)^\times} \overline{\chi}_i(x)\psi(x/\pi_F^2)\right]^{-1} \\ &= \gamma(\mathrm{N}_{F/\mathbb{Q}_2}(a)) \left[\frac{1}{2^n} \sum_{x \in (\mathbb{Z}_{2^n}/\mathfrak{p}_F^2)^\times} \overline{\chi}_0(x)\psi(x/\pi_F^2)\right]^{-n} = \gamma(\mathrm{N}_{F/\mathbb{Q}_2}(a))\gamma(a)^{-n} \\ &= \gamma(\mathrm{N}_{F/\mathbb{Q}_2}(a))\gamma(a), \end{aligned}$$

where the last equality follows from the next lemma.

---

[1] Just as in Theorem2.6.21, we use $\overline{\chi}$ to mean the character induced on $(\mathbb{Z}_{2^n}/4\mathbb{Z}_{2^n})^\times$ by χ.

Lemma 3.3.36 *Suppose that χ is a quadratic character of conductor $4\mathbb{Z}_{2^n}$ on F and that $a \in S_\chi$. Then the following hold:*

(a) The Weil index $\gamma(a)^2 = \chi(-1) = \prod_{i=0}^{n-1} \overline{\chi}_i(-1)$.

(b) If $\gamma(a) = 1$ *and* $(N_{F/\mathbb{Q}_2}(a), 2)_{\mathbb{Q}_2} = 1$, *then* $N_{F/\mathbb{Q}_2}(b)$ *is a square in* $\mathbb{Q}_2^\times$ *for all* $b \in S_\chi$.

Proof. By Lemma 3.3.32, we may assume that $a \in \mathbb{Z}_{2^n}^\times$.

For part (a), observe that

$$1 = \gamma(a \cdot a^{-1}) = (a, a^{-1})_F \gamma(a)\gamma(a^{-1}) = (a, -1)_F \gamma(a)\gamma(a^2 \cdot a^{-1}) = \chi(-1)\gamma(a)^2.$$

Of course, the claim that $\chi(-1) = \prod_{i=0}^{p-1} \overline{\chi}_i(-1)$ is obvious since n is odd and -1 is fixed by the Frobenius Fr.

Now suppose that $\gamma(a) = 1$. Then by what we have just shown, $\chi(-1) = 1$ or, equivalently,

$$(-1, \mathrm{N}_{F/\mathbb{Q}_2}(a))_F = \prod_{i=0}^{p-1} \overline{\chi}_i(-1) = 1.$$

We know (see, for instance, ([1, p.56]) that, for $a, b \in (\mathbb{Z}_2)^\times$,

$$(2, a)_{\mathbb{Z}_2} = (-1)^{(a^2-1)/8} \text{ and } (a, b)_{\mathbb{Z}_2} = (-1)^{(a-1)(b-1)/4}.$$

This implies that $\mathrm{N}_{F/\mathbb{Q}_2}(a)$ is 1 modulo $4\mathbb{Z}_{2^n}$ since $(-1, -1)_F = -1 = -(-1, 1)_F$. Recall that the the subgroup of squares in $\mathbb{Z}_2^\times$ is precisely the subgroup $1 + 8\mathbb{Z}_2$ ([1, p.49]), so in this case, $\mathrm{N}_{F/\mathbb{Q}_2}(a)$ is in either $1 + 8\mathbb{Z}_2$ or $5 + 8\mathbb{Z}_2$. Since $(2, 5)_{\mathbb{Z}_2} = -1$, we conclude part (b) of the lemma must hold. ■

Notice that the fields $\mathbb{Q}_{2^n}[\sqrt{a}]$ and $\mathbb{Q}_{2^n}[\sqrt{5a}]$ have the same discriminant over $\mathbb{Q}_{2^n}$, so the quadratic characters χ and χ' associated with these two extensions, respectively, have the same conductor. Since $\overline{\chi} = \overline{\chi'}$, χ satisfies condition (ii) if and only if χ' does as well.

Hence, to prove Theorem 3.3.34, it suffices to show that the number of χ such that $\gamma(\chi) = -1$ is less than the number of χ satisfying condition (ii), so we just need to show that the second of these numbers is equal to

$$\prod_{\substack{d|n \\ d \neq 1}} (2^{c(d)} - 1)^{\phi(d)/c(d)}.$$

3.4 f-invariant Subspaces of $\mathbb{F}_{2^n}$

Let n be an odd number greater than 3. For $a \in \mathbb{F}_{2^n}$ define a group homomorphism $\psi_a : (R_{2^n}^{\times})^{\wedge} \longrightarrow \mathbb{F}_2$ by setting

$$\psi_a(\chi) = \begin{cases} 0, & \chi(1,a) = 1 \\ 1, & \chi(1,a) = -1 \end{cases}, \qquad \chi \in (R_{2^n}^{\times})^{\wedge}.$$

The Frobenius automorphism f defines an $\mathbb{F}_2$-linear transformation of $\mathbb{F}_{2^n}$ with minimal polynomial $X^n - 1$. There exists an $x \in \mathbb{F}_{2^n}$ not contained in any nontrivial f-invariant subspace of $\mathbb{F}_{2^n}$; that is, $\{x, f(x), ..., f^{n-1}(x)\}$ provides a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. By Remark 3.1.25, the map $\Psi : (R_{2^2}^{\times})^{\wedge} \longrightarrow \mathbb{F}_2^n$ such that

$$\Psi(\chi) = \sum_{i=0}^{n-1} \psi_{f^i(x)}(\chi) f^{-i}(x) = \sum_{i=0}^{n-1} \psi_x(\chi \circ \mathrm{Fr}^i) f^{-i}(x)$$

is a group isomorphism. Observe that $f(\Psi(\chi)) = \Psi(\chi \circ \mathrm{Fr})$. Hence, for $c_i \in \{0, 1\}$ such that $c = \sum_{i=0}^{n-1} c_i$ is nonzero, $\prod_{i=0}^{n-1} \chi_i^{c_i}$ is trivial if and only if $\Psi(\chi)$ is contained in a c-dimensional, f-invariant subspace of $\mathbb{F}_{2^n}$. Every c-dimensional, f-invariant subspace of $\mathbb{F}_{2^n}$ corresponds uniquely (assuming that $c > 0$) with a monic, degree-c polynomial factor of $X^n - 1$ in $\mathbb{F}_2[X]$.

Lemma 3.4.37 *Let q be a prime number and r, a positive integer relatively prime to q. If c is the order of q in $(\mathbb{Z}/r\mathbb{Z})^{\times}$, then the r-th cyclotomic polynomial $\Phi_r(X)$ decomposes into a product of irreducible polynomials each of degree c in $\mathbb{F}_q[x]$.*

Proof. Let s be a positive integer. Then $q^s \equiv 1 \bmod r$ if and only if every r-th root of unity satisfies the equation $x^{q^s - 1} - 1 = 0$ or, equivalently, lies in $\mathbb{F}_{q^s}$. Because c is the order of q in $(\mathbb{Z}/r\mathbb{Z})^{\times}$ by assumption, the splitting field of Φ_r is $\mathbb{F}_{q^c}$. Any field extension of $\mathbb{F}_q$ which contains a root of any irreducible factor $g(x)$ of Φ_p in $\mathbb{F}_q[x]$ must contain all r-th roots of unity. In particular, the splitting field of such $g(x)$ must be $\mathbb{F}_{q^c}$, and $g(x)$ has degree c. ■

There is a unique $(n-1)$-dimensional, f-invariant subspace V of $\mathbb{F}_{2^n}$ (considered as a vector space over $\mathbb{F}_2$). By Lemma 3.4.37, we have that the number of vectors contained in V but not contained in any other proper f-invariant subspace is precisely

$$\prod_{\substack{d|n \\ d \neq 1}} (2^{c(d)} - 1)^{\phi(d)/c(d)},$$

where $c(d)$ is the order of 2 in $(\mathbb{Z}/d\mathbb{Z})^{\times}$. Combining this with our previous work, we conclude that the statement of Theorem 3.3.34 must hold.

Now, let us consider the specific case when n is an odd prime greater than 3.

Lemma 3.4.38 *For V as above and n, an odd prime greater than 3, the number of vectors contained in V but not contained in any other proper f-invariant subspace is strictly greater than $2^{n-1}\left(\frac{11}{15}\right)$.*

Proof. The existence and uniqueness of $V \subset \mathbb{F}_{2^n}$ is clear from our earlier comments. For the cyclotomic polynomial $\Phi_{2^n} \in \mathbb{F}_2[x]$, let c be as in Lemma 3.4.37. Then $c \geq \lceil \log_2(n) \rceil$ (the ceiling function of $\log_2(n)$) and the number of vectors contained in V but not contained in any other proper f-invariant subspace is greater than or equal to

$$2^{n-1} - \left(\frac{n-1}{c}\right) 2^{n-1-c} = 2^{n-1}\left(1 - \frac{n-1}{c2^c}\right) > 2^{n-1}\left(1 - \frac{n-1}{n\lceil \log_2(n) \rceil}\right)$$
$$\geq 2^{n-1}\left(1 - \frac{4}{15}\right) = 2^{n-1}\left(\frac{11}{15}\right).$$

■

Let $m = (n-1)/2$. By the previous section, the number of quadratic characters χ on $\mathbb{Q}_{2^n}$ of conductor $4\mathbb{Z}_{2^n}$ such that $\gamma(\chi) = -1$ is less than or equal to

$$2^{n-2} + 2^{m-1} = 2^{n-1}\left(\frac{1}{2} + 2^{-m-1}\right) \leq 2^{n-1}\left(\frac{1}{2} + \frac{1}{8}\right) = 2^{n-1}\left(\frac{5}{8}\right) < 2^{n-1}\left(\frac{11}{15}\right).$$

Hence, all odd primes $n > 3$ satisfy the hypotheses of Theorem 3.3.34.

Finally, we note that the hypotheses of Theorem 3.3.34 are not true for every odd number $n > 3$. When $n = 63$ for example, we have that

$$\prod_{\substack{d|63 \\ d \neq 1}} (2^{c(d)} - 1)^{\phi(d)/c(d)} = (2^2 - 1)(2^3 - 1)^{6/3}(2^6 - 1)(2^6 - 1)^{12/6}(2^6 - 1)^{36/6}$$
$$< 2^{63-2} - 2^{\frac{63-1}{2}-1},$$

so in this case, our work is insufficient to generalize Theorem 3.3.34.

CHAPTER 4

GALOIS EXTENSIONS OF $\mathbb{Q}_2$

In this final chapter, we will prove that there is a Galois extension of $\mathbb{Q}_2$ whose wild inertia group is isomorphic to the extra special 2-group Γ_0.

4.1 Group Cohomology

Let G be a group and H, a subgroup of G with index n. Suppose that A is a (left) G-module. We would like to recall two homomorphisms between cohomology groups which will be useful in the next section.

First of all, let the *restriction homomorphism* Res denote the map $\mathrm{H}^m(G,A) \longrightarrow \mathrm{H}^m(H,A)$ (for all $m \geq 0$) induced by the inclusion map $H \hookrightarrow G$.

Now, define the *co-induced $G-$module* $M_H^G(A)$ to be the set

$$\{f : G \longrightarrow A : f(hg) = hf(g) \text{ for all } g \in G, h \in H\}.$$

Let $g_1, ..., g_n$ be representatives of the left cosets of H in G. We can construct a homomorphism $\psi : M_H^G(A) \longrightarrow A$ by

$$f \in M_H^G(A) \longmapsto \sum_{i=1}^{n} g_i f(g_i^{-1}),$$

and it is easy to check that this homomorphism does not depend on a choice of coset representatives. The map ψ gives us a homomorphism $\mathrm{H}^m(G, M_H^G(A)) \longrightarrow \mathrm{H}^m(G,A)$. This allows us to define the *corestriction homomorphism* $\mathrm{Cor} : \mathrm{H}^m(H,A) \longrightarrow \mathrm{H}^m(G,A)$ since, by Shapiro's Lemma ([3, p.804]),

$$\mathrm{H}^m(G, M_H^G(A)) \cong \mathrm{H}^m(H,A).$$

Proposition 4.1.39 *For all $m \geq 0$ and any cohomology class $C \in H^m(G,A)$,*

$$Cor(Res(C)) = nC.$$

The above statements are proved in [3, p.807]. For a more functorial approach, consult [9, Chapter VII].

4.2 Inverse Galois Problem

Let K be a quadratic extension of a local, non-Archimedean field F. Then the Galois group of the algebraic closure $\overline{F}$ (of F) over K is an index 2 subgroup of $\mathrm{Gal}(\overline{F}/F)$. For readability, we will use the notation $\mathrm{G}(F)$ from now on to mean $\mathrm{Gal}(\overline{F}/F)$. Thus, we can define a quadratic character on $\mathrm{G}(F)$ via the canonical map

$$\mathrm{G}(F) \longrightarrow \mathrm{G}(F)/\mathrm{G}(K) \xrightarrow{\cong} \mu_2.$$

This allows us to uniquely identify each quadratic character χ on $F^\times$ with a quadratic character $\widetilde{\chi}$ on $G(F)$ by local class field theory.

Let n be an odd integer. We will now construct representations of $G(\mathbb{Q}_{2^n})$ using a quadratic character χ on $\mathbb{Q}_{2^n}^\times$ and also the choice σ of a map in $G(\mathbb{Q}_2)$ whose restriction to $\mathbb{Q}_{2^n}$ is the Frobenius automorphism of $\mathbb{Q}_{2^n}$ over $\mathbb{Q}_2$.

Let $\widetilde{\chi}_i = \widetilde{(\chi_i)}$ so that $\widetilde{\chi}_i(h) = \widetilde{\chi}(\sigma^{-i}h\sigma^i)$ for all $h \in G(\mathbb{Q}_{2^n})$. Define the representations (π_i, V_i) $(0 \leq i < n)$ of $G(\mathbb{Q}_{2^n})$ by letting V_i a complex, one-dimensional vector space and setting

$$\pi_i(h)(v_i) = \widetilde{\chi}_i(h)v_i$$

for all $h \in G(\mathbb{Q}_{2^n})$, $v_i \in V_i$. Hence, the restriction of the induced representation $(\mathrm{Ind}_{G(\mathbb{Q}_{2^n})}^{G(\mathbb{Q}_2)}\pi_0, V)$ to $G(\mathbb{Q}_{2^n})$ is isomorphic to the representation $\bigoplus_{i=0}^{n-1} V_i$.

Proposition 4.2.40 *Via* $\mathrm{Ind}_{G(\mathbb{Q}_{2^n})}^{G(\mathbb{Q}_2)}\pi_0$, $G(\mathbb{Q}_2)$ *acts on* V *by special orthogonal transformations if the following two conditions hold:*

(i) π_0 *is not isomorphic to* π_i *for all* $0 \leq i \leq n-1$ *and*

(ii) $\displaystyle\prod_{i=0}^{n} \widetilde{\chi}_i = 1.$

Proof. Assume that condition (i) of the theorem is true. We claim that this assumption implies that V is irreducible and self-dual. By Frobenius reciprocity,

$$\mathrm{Hom}_{G(\mathbb{Q}_2)}(V, V) = \mathrm{Hom}_{G(\mathbb{Q}_{2^n})}(V_0, V|_H) = \mathrm{Hom}_{G(\mathbb{Q}_{2^n})}(V_0, \bigoplus_{i=0}^{n-1} V_i),$$

so by (i), $\dim(\mathrm{Hom}_{G(\mathbb{Q}_2)}(V, V)) = 1$ and V is irreducible.

Similarly, if the contragredient representation of V denoted V^*, we have that

$$\begin{aligned}\mathrm{Hom}_{G(\mathbb{Q}_2)}(V, V^*) &= \mathrm{Hom}_{G(\mathbb{Q}_{2^n})}(V_0, (V^*)|_H) = \mathrm{Hom}_{G(\mathbb{Q}_{2^n})}(V_0, (V|_H)^*) \\ &= \mathrm{Hom}_{G(\mathbb{Q}_{2^n})}(V_0, \bigoplus_{i=0}^{n-1} V_i^*) = \mathrm{Hom}_{G(\mathbb{Q}_{2^n})}(V_0, \bigoplus_{i=0}^{n-1} V_i),\end{aligned}$$

where the last equality follows from the observation that $\pi_i(h)(v_i) = \pi_i(h^{-1})(v_i)$ for all $h \in G(\mathbb{Q}_{2^n})$, $v_i \in V_i$. Just as before, we have that $\dim(\mathrm{Hom}_{G(\mathbb{Q}_2)}(V, V^*)) = 1$ and, since V and V^* are irreducible, $V \cong V^*$.

Since V is self-dual, there exists a bilinear, $G(\mathbb{Q}_2)$-invariant form B on V. Moreover, this form is nondegenerate and unique (up to scalar) because V is irreducible. Every bilinear form can be written as the sum of a symmetric and skew-symmetric form, so the uniqueness of B implies that B is either symmetric or skew-symmetric. However, $\dim(V) = n$ an odd integer, and there are no nondegenerate, skew-symmetric, bilinear forms of odd dimension. Hence, $G(\mathbb{Q}_{2^n})$ acts on V by orthogonal transformations.

Identify each $g \in G(\mathbb{Q}_2)$ with the linear transformation given by the action of g on V. To finish the proof of the theorem, we only have left to show that the determinant $\det(g)$ of g is 1 for all $g \in G(\mathbb{Q}_2)$. Define a homomorphism $\phi : G(\mathbb{Q}_2) \longrightarrow \mu_2$ such that $\phi(g) = \det(g)$. If we assume (ii) holds, $G(\mathbb{Q}_{2^n}) \subset \ker(\phi)$ since, as noted earlier, $V|_H \cong \oplus_{i=0}^{n-1} V_i$. Because $[G(\mathbb{Q}_2) : \ker(\phi)]$ divides both $|\mu_2| = 2$ and $[G(\mathbb{Q}_2) : G(\mathbb{Q}_{2^n})] = n$, we conclude that $[G(\mathbb{Q}_2) : \ker(\phi)] = 1$ – i.e., ϕ is trivial on $G(\mathbb{Q}_2)$–and $\mathrm{Ind}_{G(\mathbb{Q}_2)}^{G(\mathbb{Q}_{2^n})}\pi_0$ maps $G(\mathbb{Q}_2)$ into $\mathrm{SO}(V)$. ■

Let K be a Galois extension of $\mathbb{Q}_2$ such that

$$\ker(\mathrm{Ind}_{G(\mathbb{Q}_{2^n})}^{G(\mathbb{Q}_2)}\pi_0) = \mathrm{G}(K). \tag{4.1}$$

Denote the Galois groups $\mathrm{Gal}(K/\mathbb{Q}_{2^n})$ and $\mathrm{Gal}(K/\mathbb{Q}_2)$ by G_0 and G, respectively. Notice that G_0 is the inertia subgroup of G. Suppose conditions (i) and (ii) of Proposition 4.2.40 hold; then $G \cong \mathrm{G}(\mathbb{Q}_2)/\mathrm{G}(K)$ injects into $\mathrm{SO}(V)$.

There exists a (Lie) group homomorphism $\phi : \mathrm{Spin}(V) \longrightarrow \mathrm{SO}(V)$ such that

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(V) \xrightarrow{\phi} \mathrm{SO}(V) \longrightarrow 1$$

is a short exact sequence, and thinking of G as a subgroup of $\mathrm{SO}(V)$, we can define Γ to be $\phi^{-1}(G)$ and Γ_0 to be $\phi^{-1}(G_0)$.

Remark 4.2.41 *Notice that $\Gamma/\Gamma_0 \cong Gal(\mathbb{Q}_{2^n}/\mathbb{Q}_2) \cong \mathbb{Z}/n\mathbb{Z}$. For χ as in Theorem 3.3.34, we have that Γ_0 is the extra special 2-group Γ_0 defined in Chapter 1.*

If r is the homomorphism $\mathrm{G}(\mathbb{Q}_2) \longrightarrow G$ that restricts the domain of an element in $G(\mathbb{Q}_2)$ to K, we attain the following commutative diagram of short exact sequences:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{G}(\mathbb{Q}_2) \times_G \Gamma & \xrightarrow{p_1} & \mathrm{G}(\mathbb{Q}_2) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle p_2} & & \downarrow{\scriptstyle r} & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \Gamma & \xrightarrow{\phi|_\Gamma} & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{Spin}(V) & \xrightarrow{\phi} & \mathrm{SO}(V) & \longrightarrow & 1,
\end{array}$$

using the fibered product $\mathrm{G}(\mathbb{Q}_2) \times_G \Gamma$ together with its associated homomorphisms p_1 and p_2.

Recall that, for any group G and abelian group A, the elements (or "factor sets") of $\mathrm{H}^2(G, A)$ correspond precisely with the isomorphism classes of the extentions of A by G. We will use this correspondence to show that the isomorphism class of $\mathrm{G}(\mathbb{Q}_2) \times_G \Gamma$ is trivial (so that the top exact sequence in the above diagram splits), but first, we need more facts from local class field theory.

Theorem 4.2.42 *[7, Theorem 4, p.233] Let K be a local, non-archimedean field, then*

$$H^2(Gal(\overline{K}/K), \overline{K}^\times) \cong \mathbb{Q}/\mathbb{Z}.$$

Corollary 4.2.43 *For all positive integers n, $H^2(G(\mathbb{Q}_{2^n}), \mu_2)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

Proof. The *Kummer sequence*

$$0 \longrightarrow \mu_2 \longrightarrow \overline{\mathbb{Q}}_2^\times \xrightarrow{\times 2} \overline{\mathbb{Q}}_2^\times \longrightarrow 0$$

induces a long exact sequence in group cohomology

$$\begin{aligned}
\ldots \longrightarrow \mathrm{H}^1(\mathrm{G}(\mathbb{Q}_{2^n}), \overline{\mathbb{Q}}_2^\times) \longrightarrow \mathrm{H}^2(\mathrm{G}(\mathbb{Q}_{2^n}), \mu_2) & \\
\longrightarrow \mathrm{H}^2(\mathrm{G}(\mathbb{Q}_{2^n}), \overline{\mathbb{Q}}_2^\times) \xrightarrow{\times 2} \mathrm{H}^2(\mathrm{G}(\mathbb{Q}_{2^n}), \overline{\mathbb{Q}}_2^\times) \longrightarrow \ldots &
\end{aligned}$$

By Hilbert's Theorem 90 [7, p.220], $\mathrm{H}^1(\mathrm{G}(\mathbb{Q}_{2^n}), \overline{\mathbb{Q}}_2^\times) = 0$, and hence, by Theorem 4.2.42, $\mathrm{H}^2(\mathrm{G}(\mathbb{Q}_{2^n})$,

$$0 \longrightarrow \mathrm{H}^2(\mathrm{G}(\mathbb{Q}_{2^n}), \mu_2) \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{\times 2} \mathbb{Q}/\mathbb{Z}$$

is exact, and the statement of the corollary follows. ∎

Theorem 4.2.44 *Let n be an odd number greater than 3. Define $\theta_n(-1)$ as in section 3.2. For any integer $d > 1$, let $c(d)$ denote the order of 2 in $(\mathbb{Z}/d\mathbb{Z})^\times$, and let $\phi(d)$ denote $|(\mathbb{Z}/d\mathbb{Z})^\times|$. If*

$$\theta_n(-1) < \prod_{\substack{d|n \\ d\neq 1}} (2^{c(d)} - 1)^{\phi(d)/c(d)},$$

then for V as above, there exists a homomorphism

$$G(\mathbb{Q}_2) \longrightarrow Spin(V)$$

such that the image of $G(\mathbb{Q}_2)$ under this map is Γ and the image of $G(\mathbb{Q}_{2^n})$ under this map is the extra special 2-group Γ_0.

Proof. Let χ and a be as in Theorem 3.3.34. Then there is a Galois extension K of $\mathbb{Q}_2$ satisfying (4.1), so

$$\mathrm{G}(K) = \bigcap_{i=0}^{n-1} \ker(\widetilde{\chi}_i).$$

That is, $K = \mathbb{Q}_{2^n}(\xi_0, .., \xi_{n-1})$ where $\xi_i^2 = \mathrm{Fr}^i(a)$. We chose a so that the Hasse invariant $S(<a, \mathrm{Fr}(a), ..., \mathrm{Fr}^{n-1}(a)>) = 1$, so by Theorem 1.5.2, there is a Galois extension E of $\mathbb{Q}_{2^n}$ such that $\mathrm{Gal}(E/\mathbb{Q}_{2^n}) = \Gamma_0$. Thus, the canonical surjection $\mathrm{G}(\mathbb{Q}_{2^n}) \longrightarrow \mathrm{G}(\mathbb{Q}_{2^n})/\mathrm{G}(E) \cong \mathrm{Gal}(E/\mathbb{Q}_{2^n})$ gives us a homomorphism from $\mathrm{G}(\mathbb{Q}_{2^n})$ to Γ_0. By the universal property of fibered products, the top sequence in the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{G}(\mathbb{Q}_{2^n}) \times_{G_0} \Gamma_0 & \longrightarrow & \mathrm{G}(\mathbb{Q}_{2^n}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{G}(\mathbb{Q}_2) \times_G \Gamma & \xrightarrow{p_1} & \mathrm{G}(\mathbb{Q}_2) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle p_2} & & \downarrow{\scriptstyle r} & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \Gamma & \xrightarrow{\phi|_\Gamma} & G & \longrightarrow & 1
\end{array}$$

splits, and $\mathrm{G}(\mathbb{Q}_{2^n}) \times_{G_0} \Gamma$ is trivial in $\mathrm{H}^2(\mathrm{G}(\mathbb{Q}_{2^n}), \mu_2)$. Observe that the image of $\mathrm{G}(\mathbb{Q}_2) \times_G \Gamma$ under $\mathrm{Res} : \mathrm{H}^2(\mathrm{G}(\mathbb{Q}_2), \mu_2) \longrightarrow \mathrm{H}^2(\mathrm{G}(\mathbb{Q}_{2^n}), \mu_2)$ is the cohomology class of $\mathrm{G}(\mathbb{Q}_{2^n}) \times_{G_0} \Gamma_0$. Composition of $\mathrm{Cor} : \mathrm{H}^2(\mathrm{G}(\mathbb{Q}_{2^n}), \mu_2) \longrightarrow \mathrm{H}^2(\mathrm{G}(\mathbb{Q}_2), \mu_2)$ with Res is just multiplication by n on classes of $\mathrm{H}^2(\mathrm{G}(\mathbb{Q}_2), \mu_2)$, and since n is odd, $\mathrm{G}(\mathbb{Q}_2) \times_G \Gamma$ must be trivial in $\mathrm{H}^2(G(\mathbb{Q}_2), \mu_2)$. Thus, there is a homomorphism $\psi : \mathrm{G}(\mathbb{Q}_2) \longrightarrow \mathrm{G}(\mathbb{Q}_2) \times_G \Gamma$ such that $p_1 \circ \psi$ is the identity map on $\mathrm{G}(\mathbb{Q}_2)$.

We claim that the homomorphism $p_2 \circ \psi : \mathrm{G}(\mathbb{Q}_2) \longrightarrow \Gamma$ is surjective. Observe that, for any $\sigma \in G_0$, $\phi(p_2(\psi(\sigma))) = r(p_1(\psi(\sigma))) = r(\sigma)$, so $\phi \circ p_2 \circ \psi$ is surjective. Because $|\Gamma| = 2|G|$,

this implies that either $p_2(\psi(\mathrm{G}(\mathbb{Q}_2))) = \Gamma$ or $p_2(\psi(\mathrm{G}(\mathbb{Q}_2))) \cong G$. Suppose the latter case holds. Observe that $[p_2(\psi(\mathrm{G}(\mathbb{Q}_2))) : p_2(\psi(\mathrm{G}(\mathbb{Q}_{2^n})))] = [G : G_0]$, so $|p_2(\psi(\mathrm{G}(\mathbb{Q}_{2^n})))| = |G_0|$. That is, $p_2(\psi(\mathrm{G}(\mathbb{Q}_{2^n}))) \cong G_0$, and we have that the sequence

$$1 \longrightarrow \mu_2 \longrightarrow \Gamma_0 \xrightarrow{\phi|_{\Gamma_0}} G_0 \longrightarrow 1$$

splits, which clearly cannot be true. Thus, $p_2 \circ \psi$ defines a surjection from $\mathrm{G}(\mathbb{Q}_2)$ onto Γ_0. ■

If we let ω be the root number associated with the representation $\mathrm{G}(\mathbb{Q}_2) \longrightarrow \mathrm{SO}(V)$, then as a consequence of Deligne's formula for orthogonal root numbers [2], we have know that $\mathrm{G}(\mathbb{Q}_2) \longrightarrow \mathrm{SO}(V)$ lifts to a homomorphism $\mathrm{G}(\mathbb{Q}_2) \longrightarrow \mathrm{Spin}(V)$ if and only if $\omega = 1$, that is, ω corresponds with the trivial cohomology class in $\mathrm{H}^2(\mathbb{Q}_2, \mu_2)$. As we showed in the above theorem, this second condition is equivalent to requiring that the root number ω' associated with the representation $(\mathrm{Ind}_{\mathrm{G}(\mathbb{Q}_{2^n})}^{\mathrm{G}(\mathbb{Q}_2)} \pi_0)|_{\mathrm{G}(\mathbb{Q}_{2^n})}$ is 1. In this case, $(\mathrm{Ind}_{\mathrm{G}(\mathbb{Q}_{2^n})}^{\mathrm{G}(\mathbb{Q}_2)} \pi_0)|_{\mathrm{G}(\mathbb{Q}_{2^n})}$ decomposes a direct sum of one-dimensional representations V_i, so ω' is just the product of Tate's epsilon factors [11] associated with the V_i. Theorem 3.3.34 assures us that there is a quadratic character for which this product is 1. However, under our construction, we also know that exactly what the image of $\mathrm{G}(\mathbb{Q}_2) \longrightarrow \mathrm{Spin}(V)$ must be, and moreover, we can explicitly write down the Galois extension E of $\mathbb{Q}_2$ satisfying (4.1) in terms of $a \in S_\chi$.

REFERENCES

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[2] P. Deligne, *Les constantes locales de léquation fonctionnelle de la fonction l d'Artin d'une representation orthogonale*, Invent. Math., 35 (1976), pp. 299–316.

[3] D. S. Dummit and R. M. Foote, *Abstract Algebra*, John Wiley & Sons, third ed., 2004.

[4] K. Iwasawa, *Local Class Field Theory*, Oxford University Press, New York, 1986.

[5] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, 1973.

[6] S. Lang, *Algebra*, Springer, New York, revised third ed., 2002.

[7] F. Lorenz, *Algebra II: Fields with Structure, Algebras and Advanced Topics*, Springer, New York, 2008.

[8] S. Roman, *Field Theory*, Springer, New York, second ed., 2006.

[9] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 2009.

[11] J. Tate, *Fourier analysis in number fields and Hecke's zeta-functions*, in Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich, eds., Academic Press, London, 1967, pp. 305–347.

[12] E. Witt, *Konstruktion von galoisschen körpern der charakteristik p zu vorgegebener gruppe der ordnungpf*, J. Reine Angew. Math., 174 (1936), pp. 237–245.