Automorphisms of Even Unimodular Lattices and Unramified Salem Numbers

Citation
Gross, Benedict H., and Curtis T. McMullen. 2002. Automorphisms of even unimodular lattices and unramified Salem numbers. Journal of Algebra 257(2): 265-290. Revised 2008.

Published Version
doi:10.1016/S0021-8693(02)00552-5

Permanent link
http://nrs.harvard.edu/urn-3:HUL.InstRepos:3446009

Automorphisms of even unimodular lattices and unramified Salem numbers

Benedict H. Gross and Curtis T. McMullen

1 January, 2002

Abstract

In this paper we study the characteristic polynomials

$$S(x) = \det(xI - F|\,\mathrm{II}_{p,q})$$

of automorphisms of even, unimodular lattices with signature (p, q). In particular we show any Salem polynomial of degree $2n$ satisfying $S(-1)S(1) = (-1)^n$ arises from an automorphism of an indefinite lattice, a result with applications to K3 surfaces.

Contents

Research of both authors supported in part by the NSF.

2000 Mathematics Subject Classification: 11H56 (11R06, 14J50).

1 Introduction

Let $\mathrm{II}_{p,q}$ denote the even, indefinite, unimodular lattice with signature (p,q). As is well-known, such a lattice exists iff $p \equiv q \bmod 8$, in which case $\mathrm{II}_{p,q}$ is unique up to isomorphism [Ser], [MH].

Let $\mathrm{SO}(\mathrm{II}_{p,q})$ denote the group of isomorphisms $F : \mathrm{II}_{p,q} \to \mathrm{II}_{p,q}$ preserving the inner product and orientation. This paper addresses:

Question 1.1 *What are the possibilities for the characteristic polynomial $S(x) = \det(xI - F)$ of an automorphism $F \in \mathrm{SO}(\mathrm{II}_{p,q})$?*

Upon tensoring with $\mathbb{R}$, we can regard F as an element of the orthogonal group $\mathrm{SO}_{p,q}(\mathbb{R})$ of a quadratic form of signature (p,q) on $\mathbb{R}^{2n}$, $2n = p+q$. The condition $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ already implies:

- $S(x)$ is a *reciprocal* polynomial (we have $x^{2n}S(1/x) = S(x)$); and
- $(p,q) \geq (s,s)$ and $(p,q) \equiv (s,s) \bmod 2$, where $2s$ is the number of roots of $S(x)$ off the unit circle.

A subtler arithmetic condition satisfied by the characteristic polynomial of an automorphism of $\mathrm{II}_{p,q}$ is:

- The integers $|S(-1)|$, $|S(1)|$ and $(-1)^n S(1)S(-1)$ are all squares.

See §6. We speculate that these 3 conditions may be *sufficient* for a monic irreducible polynomial $S(x) \in \mathbb{Z}[x]$ to be realized as the characteristic polynomial of an automorphism of $\mathrm{II}_{p,q}$.

Unramified polynomials. The main result of this paper answers Question 1.1 in a special case. Let us say a monic reciprocal polynomial $S(x) \in \mathbb{Z}[x]$ is *unramified* if

- $|S(-1)| = |S(1)| = 1$; equivalently, if $S(-1)S(1) = (-1)^n$ (see §3).

Theorem 1.2 *Let $S(x) \in \mathbb{Z}[x]$ be an unramified, irreducible, monic reciprocal polynomial, of degree $2n$, with $2s$ roots off the unit circle. Let $\mathrm{II}_{p,q}$ be an even, indefinite unimodular lattice with signature (p,q) satisfying*

$$p+q = 2n, \quad (p,q) \geq (s,s), \quad \textit{and} \;\; (p,q) \equiv (s,s) \bmod 2.$$

Then there is an automorphism

$$F : \mathrm{II}_{p,q} \to \mathrm{II}_{p,q}$$

with characteristic polynomial $S(x)$.

The following more precise form of the theorem allows one to control the real conjugacy class of F.

Theorem 1.3 *Let $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ be an orthogonal transformation with irreducible, unramified characteristic polynomial $S(x) \in \mathbb{Z}[x]$. If $p \equiv q \bmod 8$, then there is an even unimodular lattice $L \subset \mathbb{R}^{p+q}$ preserved by F.*

To prove these results, we synthesize a lattice automorphism from its characteristic polynomial. The construction takes place in the quadratic extension of number fields K/k, where $K = \mathbb{Q}[x]/S(x)$ and $\mathrm{Gal}(K/k)$ is generated by the involution $\alpha \mapsto \overline{\alpha}$ sending x to x^{-1}. Given a fractional ideal $L \subset K$ and $\xi \in k^*$, we define an automorphism $F : L \to L$ by $F(\alpha) = x\alpha$. Then F belongs to the orthogonal group $\mathrm{SO}(L)$ for the inner product

$$\langle \alpha, \beta \rangle_L = \mathrm{Tr}_{\mathbb{Q}}^{K}(\xi \alpha \overline{\beta}).$$

Using class field theory, we show L can be chosen to be an even, unimodular lattice of any signature compatible with the condition $p \equiv q \bmod 8$; and by construction, the characteristic polynomial of F is $S(x)$. See §§2–5.

Cyclotomic polynomials. It is easy to see that the cyclotomic polynomial $\Phi_d(x) \in \mathbb{Z}[x]$ of degree $\phi(d)$ is unramified unless $d = r^e$ or $2r^e$ for some prime r (see §7). So the preceding results imply:

Corollary 1.4 *The indefinite lattice $\mathrm{II}_{p,q}$ admits a symmetry of order d whenever $p + q = \phi(d)$ and d does not have the form r^e or $2r^e$ for some prime r.*

We also recover a result first obtained in [Ba1]:

Corollary 1.5 *There exists a definite even unimodular lattice L of rank $\phi(d)$ with a symmetry of order d whenever $\phi(d) = 0 \bmod 8$ and $d \neq r^e$ or $2r^e$, r prime.*

Salem polynomials. A *Salem polynomial* $S(x) \in \mathbb{Z}[x]$ is a monic, irreducible reciprocal polynomial with exactly two roots off the unit circle, both real and positive. The unique root $\lambda > 1$ is a *Salem number.* (We permit quadratic Salem numbers.)

If a Salem polynomial of degree $2n$ is unramified, then n is odd (see Proposition 3.3). In §7 we show such polynomials are abundant in each possible degree.

Theorem 1.6 *For any odd integer $n \geq 3$, there exist infinitely many unramified Salem polynomials of degree $2n$.*

To construct these polynomials, we start with a separable polynomial $C(x) \in \mathbb{Z}[x]$ of degree $n-3$ with all its roots in the interval $(-2, 2)$. Setting

$$R(x) = C(x)(x^2 - 4)(x - a) - 1,$$

we show $S(x) = x^n R(x + x^{-1})$ is an unramified Salem polynomial for all $a \gg 0$.

Lehmer's polynomial. Inverting this construction yields interesting factorizations for certain Salem polynomials. For example, the smallest known Salem number $\lambda \approx 1.17628$ is a root of the *Lehmer polynomial*

$$S(x) = 1 + x - x^3 - x^4 - x^5 - x^6 - x^7 + x^9 + x^{10}. \tag{1.1}$$

Note that $S(x)$ is unramified. Writing $S(x) = x^5 R(x + x^{-1})$, we find

$$R(x) = (x + 1)^2(x^2 - 4)(x - 1) - 1.$$

See §7 for more details and examples.

Automorphisms of K3 surfaces. Our study of automorphisms of lattices began with K3 surfaces [Mc], and we conclude with an application to these varieties.

Let X be a complex K3 surface. With respect to the cup product, the middle-dimensional cohomology group $H^2(X, \mathbb{Z})$ is an even, unimodular lattice of signature $(3, 19)$. The characteristic polynomial $S(x) = \det(xI - f^*|H^2(X))$ of an automorphism $f : X \to X$ is a reciprocal polynomial with at most two roots off the unit circle, both positive. Thus if $S(x)$ is irreducible, it is either a Salem polynomial or a cyclotomic polynomial.

Conversely, in §8 we show:

Theorem 1.7 *Let $S(x)$ be an unramified Salem polynomial of degree 22, and let $\delta \in S^1$ be a root of $S(x)$. Then there exists:*

- *A complex analytic K3 surface X, and an automorphism $f : X \to X$, such that*
- *$S(x) = \det(xI - f^*|H^2(X))$ and*
- *f^* acts on $H^{2,0}(X)$ by multiplication by δ.*

(Remark: the surface X above is never projective.)

There are no known Salem numbers of trace less than -1, and only recently have infinitely many Salem numbers of trace -1 been constructed [Smy]. Using the fact that the Lefschetz number of f is non-negative, we show:

Corollary 1.8 *There are no unramified Salem numbers of degree 22 and trace less than -2.*

Notes. This paper elaborates the construction of lattice automorphisms in [Mc]. A similar method was used by J. G. Thompson to construct lattice automorphisms of order p [CoS, 8.7.5], and by E. Bayer-Fluckiger to characterize the cyclotomic polynomials that arise from automorphisms of definite unimodular lattices [Ba1]. For a recent survey of the construction of lattices using ideals in number fields, see [Ba2]. More examples of automorphisms of K3 surfaces via automorphisms of lattices can be found in [Bor] and the references therein.

We note that the Alexander polynomial of a knot is always a reciprocal polynomial satisfying $|S(1)| = 1$ (see e.g. [Rol, 8.C.7]), so it verifies part of the condition to be unramified. The Lehmer polynomial and other interesting Salem polynomials arise as Alexander polynomials of pretzel knots and links [Hir].

We would like to thank E. Bayer-Fluckiger for several helpful remarks.

2 Real orthogonal transformations

In this section we collect together elementary results classifying orthogonal transformations with a given characteristic polynomial over $\mathbb{R}$.

Let $\mathrm{SO}_{p,q}(\mathbb{R})$ denote the Lie group of automorphisms $F : \mathbb{R}^{p+q} \to \mathbb{R}^{p+q}$ with $\det F = 1$, preserving the quadratic form

$$x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$$

of signature (p, q). Recall that a monic polynomial $S(x) \in \mathbb{R}[x]$ of degree $2n$ is *separable* if its roots (in $\mathbb{C}$) are all simple, and *reciprocal* if $x^{2n}S(1/x) = S(x)$.

Theorem 2.1 *Let $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ be an orthogonal transformation with separable characteristic polynomial $S(x)$ of degree $2n$. Then $S(x)$ is reciprocal.*

Classification by sign invariant. For the remainder of this section we fix the following data:

- $S(x) \in \mathbb{R}[x]$, a degree $2n$ monic, separable, reciprocal polynomial with $2s$ roots off the unit circle.
- $R(x) \in \mathbb{R}[x]$, the associated monic degree n *trace polynomial*, defined by the condition
$$S(x) = x^n R(x + x^{-1}).$$
The roots of $R(x)$ have the form $\tau = \lambda + \lambda^{-1}$ as λ ranges over the roots of $S(x)$.
- $T \subset \mathbb{R}$, the $n - s$ roots τ of $R(x)$ that lie in the interval $(-2, 2)$. The roots of $R(x)$ in $(-2, 2)$ correspond to conjugate pairs of roots of $S(x)$ on S^1.

Suppose $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ has characteristic polynomial $S(x)$. For each $\tau \in T$ let
$$E_\tau = \mathrm{Ker}(F + F^{-1} - \tau I) \subset \mathbb{R}^{p+q}.$$
Then F acts on $E_\tau \cong \mathbb{R}^2$ by rotation by angle θ, where $2\cos\theta = \tau$, so E_τ has signature $(2, 0)$ or $(0, 2)$. Define the *sign invariant* $\epsilon_F : T \to \langle \pm 1 \rangle$ by
$$\epsilon_F(\tau) = \begin{cases} +1 & \text{if } E_\tau \text{ has signature } (2,0), \\ -1 & \text{if } E_\tau \text{ has signature } (0,2). \end{cases}$$

Theorem 2.2 *The sign invariant of $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ with characteristic polynomial $S(x)$ satisfies*
$$(p, q) = (s, s) + \sum_T \begin{cases} (2,0) & \text{if } \epsilon_F(\tau) = +1, \\ (0,2) & \text{if } \epsilon_F(\tau) = -1. \end{cases} \tag{2.1}$$
Conversely, any sign invariant compatible with this condition arises for some $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ with characteristic polynomial $S(x)$.

Corollary 2.3 *The polynomial $S(x)$ can be realized as $S(x) = \det(xI - F)$ for some $F \in \mathrm{SO}_{p,q}(\mathbb{R}) \iff p + q = 2n$, $(p, q) \geq (s, s)$, and $(p, q) \equiv (s, s) \bmod 2$.*

Theorem 2.4 *Let $F, G \in \mathrm{SO}_{p,q}(\mathbb{R})$ have characteristic polynomial $S(x)$. Then F and G are conjugate in $\mathrm{O}_{p,q}(\mathbb{R})$ if and only if they have the same sign invariant.*

Corollary 2.5 *The number of* $\mathrm{O}_{p,q}(\mathbb{R})$ *conjugacy classes of* $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ *with characteristic polynomial* $S(x)$ *is given by the binomial coefficient*

$$N = \binom{n-s}{(p-s)/2},$$

provided at least one such F *exists.*

Proof of Theorem 2.1. For each root $\lambda \in \mathbb{C}$ of $S(x)$, let $V_\lambda \subset \mathbb{C}^{p+q}$ denote the corresponding 1-dimensional eigenspace of F. Then for $v \in V_\alpha$ and $w \in V_\beta$ we have

$$\langle v, w\rangle = \langle Fv, Fw\rangle = \alpha\beta\langle v, w\rangle,$$

so V_α and V_β are orthogonal unless $\alpha = 1/\beta$. Since the inner product is nondegenerate, the roots of $S(x)$ must be invariant under $\lambda \mapsto \lambda^{-1}$. Moreover, ± 1 are not roots of $S(x)$ — otherwise both would be, since the number of roots is even, but then we would have $\det F < 0$. Thus $S(x)$ is a reciprocal polynomial. ■

Proof of Theorem 2.2. Consider the orthogonal, F-invariant splitting $\mathbb{C}^{p+q} = U \oplus V$, where

$$U = \oplus_{|\lambda|=1} V_\lambda \quad \text{and} \quad V = \oplus_{|\lambda|\neq 1} V_\lambda.$$

The splitting above is defined over $\mathbb{R}$, so the signatures of U and V are well-defined. Indeed, V has signature (s,s) since $\oplus_{|\lambda|>1} V_\lambda$ is an s-dimensional isotropic subspace of V. On the other hand, we can write U as an orthogonal direct sum

$$U = \bigoplus_{\tau \in T} E_\tau \otimes \mathbb{C}.$$

The signature of each summand $E_\tau \cong \mathbb{R}^2$ is recorded by the sign invariant $\epsilon_F(\tau)$. Since the signature (p,q) of $\mathbb{R}^{p+q}$ is the sum of the signatures of U and V, we obtain (2.1).

Now suppose $\epsilon : T \to \langle \pm 1\rangle$ satisfies (2.1). Partition the roots Λ of $S(x)$ into subsets of the form

$$\Lambda_i = \{\lambda, \overline{\lambda}, \lambda^{-1}, \overline{\lambda}^{-1}\}.$$

For each i define a real vector space with a quadratic form, (V_i, Q_i), and a transformation $F_i \in \mathrm{SO}(V_i, Q_i)$ with eigenvalues Λ_i, as follows.

1. For $\Lambda_i = \{\lambda, \lambda^{-1}\}$, with $\lambda \in \mathbb{R}$, take
$$V_i = \mathbb{R}^2, \ \ Q_i(x,y) = xy, \ \text{ and } \ F_i(x,y) = (\lambda x, \lambda^{-1} y).$$
2. For $\Lambda_i = \{\lambda, \overline{\lambda}\}$, with $\lambda \in S^1$, take
$$V_i = \mathbb{C} \cong \mathbb{R}^2, \ \ Q_i(z) = \epsilon(\tau)|z|^2, \ \text{ and } \ F_i(z) = \lambda z,$$
where $\tau = \lambda + \overline{\lambda}$.
3. For $\Lambda_i = \{\lambda, \overline{\lambda}, \lambda^{-1}, \overline{\lambda}^{-1}\}$ with $\lambda \not\in S^1 \cup \mathbb{R}$, take
$$V_i = \mathbb{C}^2 \cong \mathbb{R}^4, \ \ Q_i(z,w) = \operatorname{Re} zw, \ \text{ and } \ F_i(z,w) = (\lambda z, \lambda^{-1} w).$$

Let $(V,Q) = \oplus(V_i, Q_i)$ and $F = \oplus F_i$. Then F belongs to the orthogonal group $\mathrm{SO}(V,Q)$, $S(x) = \det(xI - F)$, and by construction the sign invariant satisfies $\epsilon = \epsilon_F$. The signature of (V,Q) is (p,q) by equation (2.1). Since a real orthogonal space is determined up to isomorphism by its signature, F is conjugate to a transformation in $\mathrm{SO}_{p,q}(\mathbb{R})$, completing the proof. ■

Proof of Theorem 2.4. Clearly $\epsilon_F = \epsilon_G$ if F and G are conjugate.

To prove the converse, choose a basis (e_λ) for $\mathbb{C}^{p+q}$ where λ ranges through the zeros of $S(x)$, such that $F(e_\lambda) = \lambda e_\lambda$ and
$$\overline{e_\lambda} = e_{\overline{\lambda}}. \tag{2.2}$$
Then $\langle e_\alpha, e_\beta \rangle = 0$ unless $\alpha\beta = 1$. For $\lambda \not\in S^1$ we can scale e_λ independently from $e_{1/\lambda}$ to arrange that $\langle e_\lambda, e_{1/\lambda} \rangle = 1$. But for $\lambda \in S^1$ we must preserve (2.2), so we can only arrange that
$$\langle e_\lambda, e_{1/\lambda} \rangle = \epsilon_F(\tau),$$
where $\tau = \lambda + \lambda^{-1}$.

In any case, if $\epsilon_F = \epsilon_G$ then we can choose an eigenbasis (e'_λ) for G with the same normalizations. The complex linear map defined by $H(e_\lambda) = e'_\lambda$ is then an isometry, conjugating F to G. But by (2.2) H is actually defined over $\mathbb{R}$, and therefore F and G are conjugate in $\mathrm{O}_{p,q}(\mathbb{R})$. ■

3 Ramification

In this section we relate ramification of the reciprocal polynomial $S(x)$ to ramification of an associated field extension K/k.

Continuing in the setting of the preceding section, we now specialize to the case where

- $S(x) \in \mathbb{Z}[x]$ is an *irreducible* reciprocal polynomial.

In this case we can associate to $S(x)$ a quadratic field extension K/k, where

- $K = \mathbb{Q}[x]/S(x)$ is a number field of degree $2n$ over $\mathbb{Q}$, and
- $k = \mathbb{Q}[y]/R(y) \subset K$ is the degree n subfield generated by $y = x + x^{-1}$.

Here R is the degree n trace polynomial of S.

Recall that $S(x)$ is *unramified* if $|S(\pm 1)| = 1$. (An equivalent condition is that $S(-1)S(1) = (-1)^n$; see Proposition 3.3.) We will show:

Proposition 3.1 *If the polynomial $S(x)$ is unramified, then the field extension K/k is also unramified (at all finite primes).*

Fields and traces. We start with some algebraic preliminaries; see e.g. [FT] or [La] for more background.

Let $\mathcal{O}_K \subset K$ be the ring of integers in a number field $K/\mathbb{Q}$. The *trace form* on K is defined by

$$\langle \alpha, \beta \rangle = \mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha\beta).$$

For any $\mathbb{Z}$-module $M \subset K$ generated by a basis of K over $\mathbb{Q}$, we define the *dual module* by

$$M^\vee = \{\alpha \in K \,:\, \langle \alpha, \beta \rangle \in \mathbb{Z} \text{ for all } \beta \in M\} \cong \mathrm{Hom}(M, \mathbb{Z}).$$

If $I \subset K$ is a fractional ideal, then so is $I^\vee$; in fact we have

$$I^\vee = \mathcal{O}_K^\vee \cdot I^{-1}. \tag{3.1}$$

The ideal $(\mathcal{O}_K^\vee)^{-1}$ is the *different* of K.

Quadratic extensions. A finite extension of number fields K/k is *unramified* (at all finite primes) if

$$\mathcal{O}_K^\vee = \mathcal{O}_K \cdot \mathcal{O}_k^\vee.$$

(Here $\mathcal{O}_k^\vee \subset k$ is the dual of $\mathcal{O}_k$ with respect to the trace form on k.)

Proposition 3.2 *Let $K = k[x]/(x^2 - yx + 1)$ be a quadratic extension of a number field k, where $y \in \mathcal{O}_k$. If $y^2 - 4$ is a unit in $\mathcal{O}_k$, then K/k is unramified.*

Proof. If $y^2 - 4$ is a unit, then $\mathcal{O}_k[x]^\vee = \mathcal{O}_k^\vee[x]$. Indeed, writing $\beta \in K$ as $\beta_1 + \beta_2 x$, $\beta_i \in k$, the condition $\beta \in \mathcal{O}_k[x]^\vee$ is the same as the condition $\mathrm{Tr}(\alpha\beta) \in \mathbb{Z}$ and $\mathrm{Tr}(\alpha x \beta) \in \mathbb{Z}$ for all $\alpha \in \mathcal{O}_k$. Using the fact that $x^2 = yx - 1$, this in turn translates into the condition

$$\begin{pmatrix} 2 & y \\ y & y^2 - 2 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} \in (\mathcal{O}_k^\vee)^2.$$

But the matrix on the right is invertible in $M_2(\mathcal{O}_k)$, since its determinant is the unit $y^2 - 4$. Since $\mathcal{O}_k^\vee$ is an $\mathcal{O}_k$-module, we conclude that β belongs to $\mathcal{O}_k[x]^\vee$ iff $\beta_1, \beta_2 \in \mathcal{O}_k^\vee$.

It follows that $\mathcal{O}_K = \mathcal{O}_k[x]$, since we have

$$\mathcal{O}_K^\vee \subset \mathcal{O}_k[x]^\vee = \mathcal{O}_k^\vee[x] \subset \mathcal{O}_K^\vee.$$

But then

$$\mathcal{O}_K^\vee = \mathcal{O}_k^\vee[x] = \mathcal{O}_k^\vee \cdot \mathcal{O}_k[x] = \mathcal{O}_k^\vee \cdot \mathcal{O}_K,$$

so K/k is unramified. ■

Proof of Proposition 3.1. The field $K = \mathbb{Q}[x]/S(x)$ is a quadratic extension of $k \cong \mathbb{Q}[y]/R(y)$ where $y = x + x^{-1}$. Thus we have $K \cong k[x]/(x^2 - yx + 1)$.

Now the norm of $x - a \in K = \mathbb{Q}[x]/S(x)$ is given by

$$\mathrm{N}_{\mathbb{Q}}^K(x - a) = S(a).$$

Since $S(x)$ is reciprocal and unramified, we have $|S(0)| = |S(\pm 1)| = 1$, and thus x and $x \pm 1$ are units (since they are algebraic integers of norm ± 1). Thus $y^2 - 4 = (x - x^{-1})^2 = (x-1)^2(x+1)^2/x^2$ is also a unit, and therefore K/k is unramified. ■

Parity. We conclude by pointing out some parity constraints on unramified polynomials.

Proposition 3.3 *Let $S(x)$ be an unramified monic reciprocal polynomial of degree $2n$ with $2s$ roots off the unit circle. Then $s \equiv n \bmod 2$ and $S(-1)S(1) = (-1)^n$.*

Proof. Since $S(x)$ is unramified we have $|S(\pm 1)| = |R(\pm 2)| = 1$, and clearly $R(-2) = R(2) \bmod 4$. Thus $R(2)R(-2) = 1 = (-1)^n S(-1)S(1)$.

Since $R(y)$ has the same sign at the endpoints of $[-2, 2]$, it must have an even number of zeros in this interval; but the number of zeros of R in $(-2, 2)$ is the same as the number of pairs of zeros of S on S^1, which is $n - s$. ■

4 Lattices in number fields

In this section we give a construction of automorphisms of even unimodular lattices using number theory. For a survey of related results, see [Ba2]

Lattices. A *lattice* L of rank r is an abelian group $L \cong \mathbb{Z}^r$ equipped with a non-degenerate, symmetric, bilinear form (or inner product) $\langle x, y\rangle_L \in \mathbb{Z}$.

The lattice L is *even* if $\langle x, x\rangle_L \in 2\mathbb{Z}$ for all $x \in L$; otherwise L is *odd.* If the inner product gives an isomorphism between L and $L^* = \mathrm{Hom}(L, \mathbb{Z})$, then L is *unimodular.* We say L has *signature* (p, q) if the quadratic form $\langle x, x\rangle_L$ on $L \otimes \mathbb{R} \cong \mathbb{R}^r$ is equivalent to

$$x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2.$$

If $(p, q) = (r, 0)$ or $(0, r)$, then L is *definite*; otherwise L is an *indefinite* lattice.

Any two even, indefinite, unimodular lattices with the same signature are isomorphic. There exists an even, unimodular lattice with signature (p, q) iff $p \equiv q \bmod 8$. See [Ser, §5], [MH].

Number fields. Continuing in the notation of the preceding section, let $S(x) \in \mathbb{Z}[x]$ be a monic irreducible reciprocal polynomial of even degree $2n$, with associated quadratic field extension $K = \mathbb{Q}[x]/S(x)$ over $k = \mathbb{Q}[y]/R(y)$, $y = x + x^{-1}$. The Galois group of K/k is generated by the involution ι sending x to x^{-1}. For brevity we write $\overline{\alpha} = \iota(\alpha)$. The Galois group acts on fractional ideals in K by $\overline{L} = \iota(L)$.

Theorem 4.1 *Let $L \subset K$ be a fractional ideal satisfying*

$$L \cdot \overline{L} \cdot (\xi) = \mathcal{O}_K^\vee$$

for some $\xi \in k^*$. Then L is a unimodular lattice with respect to the inner product

$$\langle \alpha, \beta\rangle_L = \mathrm{Tr}_{\mathbb{Q}}^K(\xi \alpha \overline{\beta}). \tag{4.1}$$

If K/k is unramified, then L is even.

Proof. From formula (3.1) for the dual module with respect to the trace form on K, we have

$$L^\vee = \mathcal{O}_K^\vee \cdot L^{-1} = \overline{L} \cdot (\xi). \tag{4.2}$$

The dual of L with respect to the inner product (4.1) is thus given by

$$L^* = \{\beta \in K \ : \ \xi\overline{\beta} \in L^\vee\} = L.$$

Therefore L is a unimodular lattice. For $\alpha \in L$ we have

$$\xi\alpha\overline{\alpha} \in ((\xi) \cdot L \cdot \overline{L}) \cap k = \mathcal{O}_K^\vee \cap k.$$

If K/k is unramified, then we have

$$\mathcal{O}_K^\vee \cap k = (\mathcal{O}_K \cdot \mathcal{O}_k^\vee) \cap k = \mathcal{O}_k^\vee;$$

therefore

$$\langle \alpha, \alpha \rangle_L = 2 \operatorname{Tr}_{\mathbb{Q}}^k (\xi\alpha\overline{\alpha}) \in 2\mathbb{Z},$$

so L is even. ■

Note. For L to be even it is sufficient that K/k be unramified at the primes of $\mathcal{O}_k$ dividing 2; see [Ba2, §2.6].

Isometries of L. Now define $f : K \to K$ by $f(\alpha) = x\alpha$; then $S(x)$ is the characteristic polynomial of f. Since x is a unit, f restricts to an automorphism $f : L \to L$ for any fractional ideal $L \subset K$.

Let T be the set of real places of k that become complex in K. Since the discriminant of $x^2 - yx + 1$ is $y^2 - 4$, we can identify T with the set of roots τ of $R(y)$ in the interval $(-2, 2)$. If we regard elements $\xi \in k \cong \mathbb{Q}[y]/R(y)$ as polynomials in y, then the valuation of ξ at the real place $\tau \in T$ is simply $\xi(\tau)$. We record the sign of this valuation for $\xi \in k^*$ by

$$\operatorname{sign}_\tau(\xi) = \begin{cases} +1 & \text{if } \xi(\tau) > 0, \\ -1 & \text{if } \xi(\tau) < 0. \end{cases}$$

Theorem 4.2 *The map $f : L \to L$ is an orthogonal transformation of the form $\langle \alpha, \beta \rangle_L = \operatorname{Tr}_{\mathbb{Q}}^K(\xi\alpha\overline{\beta})$, with sign invariant*

$$\epsilon_f(\tau) = \operatorname{sign}_\tau(\xi).$$

Proof. The automorphism f is an isometry because

$$\langle f(\alpha), f(\beta)\rangle_L = \mathrm{Tr}^K_{\mathbb{Q}}(\xi x\alpha\overline{x\beta}) = \mathrm{Tr}^K_{\mathbb{Q}}(\xi x\alpha x^{-1}\overline{\beta}) = \langle \alpha, \beta\rangle_L.$$

To compute its sign invariant, just observe that the inner product on $L \otimes \mathbb{R}$ restricts to the form

$$\langle \alpha, \beta\rangle_L = \xi(\tau) \cdot \mathrm{Tr}^{\mathbb{C}}_{\mathbb{R}}(\alpha\overline{\beta}) = 2\xi(\tau)\,\mathrm{Re}\,\alpha\overline{\beta}$$

on $E_\tau \cong \mathbb{C}$. ■

Example: $\mathbb{Z}^2$. Let $S(x) = x^2 + 1$. Then $\mathcal{O}_k = \mathbb{Z} \subset \mathcal{O}_K = \mathbb{Z}[i]$, and $\mathcal{O}_K^\vee = (1/2)\mathcal{O}_K$. Thus Theorem 4.1 holds for $L = \mathcal{O}_K$ and $\xi = 1/2$, yielding the automorphism $f(\alpha) = i\alpha$ of the unimodular lattice $L = \mathbb{Z}[i] \cong \mathbb{Z}^2$ with the usual positive-definite inner product

$$\langle \alpha, \beta\rangle_L \;=\; \mathrm{Tr}^K_{\mathbb{Q}}(\xi\alpha\overline{\beta}) \;=\; \mathrm{Re}\,\alpha\overline{\beta}.$$

In this case K/k is ramified (at the prime 2) and the unimodular lattice $L \cong \mathbb{Z}^2$ is odd.

Remark: completeness. In the special case where $\mathcal{O}_K = \mathbb{Z}[x]/S(x)$, all automorphisms $f : L \to L$ of lattices with characteristic polynomial $S(x)$ arise via the construction above. Indeed, any such L is an $\mathcal{O}_K$-module, hence represented by a fractional ideal in K; and any f-invariant inner product on L with values in $\mathbb{Q}$ has the form $\mathrm{Tr}^K_{\mathbb{Q}}(\xi\alpha\overline{\beta})$ for some $\xi \in k$.

For example, let $S(x) = \Phi_d(x)$ be the cyclotomic polynomial for the primitive dth roots of unity; then $\mathcal{O}_K = \mathbb{Z}[x]/S(x)$. Therefore every order d automorphism $f : L \to L$ of a lattice of rank $2n = \phi(d)$ comes from an ideal $L \subset \mathcal{O}_K$ by the construction above.

5 Class field theory

We now use class field theory to complete the proof of our main results on lattice automorphisms, Theorems 1.2 and 1.3.

In this section we specialize to the case where:

- $S(x) \in \mathbb{Z}[x]$ is a monic, irreducible, *unramified* reciprocal polynomial of degree $2n$.

As in the preceding sections, we let K/k denote the associated quadratic field extension, where $K = \mathbb{Q}[x]/S(x)$, $k = \mathbb{Q}[y]/R(y)$ and $y = x + x^{-1}$. By Proposition 3.1, the extension K/k is unramified at all finite primes.

Class groups. Let T be the set of roots of $R(y)$ in $(-2,2)$. As before we identify T with the set of real places of k which ramify (become complex) in K.

Let C_K and C_k denote the ideal class groups (fractional ideals modulo principal ideals) of K and k. Let $C_k^+(T)$ be the *restricted class group* of k at the places T; that is, the group of fractional ideals in k modulo principal ideals (α) such that $\operatorname{sign}_\tau(\alpha) = 1$ for all $\tau \in T$.

The Artin map. Let $\mathrm{A} : C_k^+(T) \to \mathrm{Gal}(K/k)$ be the *Artin homomorphism* of global class field theory. Identifying $\mathrm{Gal}(K/k)$ with the multiplicative group $\langle \pm 1 \rangle$, the value of the Artin homomorphism on the prime ideals $\mathfrak{p}$ generating $C_k^+(T)$ is given by:

$$A(\mathfrak{p}) = \begin{cases} +1 & \text{if } \mathfrak{p} \text{ splits in } K/k\text{, and} \\ -1 & \text{if } \mathfrak{p} \text{ is inert in } K/k. \end{cases}$$

(These are the only possibilities, since K/k is unramified at $\mathfrak{p}$.) On a principal ideal $(\alpha) = \alpha \cdot \mathcal{O}_k$, the Artin map assumes the value

$$\mathrm{A}((\alpha)) = \prod_{\tau \in T} \operatorname{sign}_\tau(\alpha). \tag{5.1}$$

Norms of ideals. The *norm map* from fractional ideals in K to those in k is defined by

$$\mathrm{N}(L) = \mathrm{N}_k^K(L) = (L \cdot \overline{L}) \cap k.$$

Given a principal ideal (β) in K, we have $\mathrm{N}((\beta)) = (\mathrm{N}(\beta))$, and $\operatorname{sign}_\tau(\mathrm{N}(\beta)) = 1$ for all $\tau \in T$. Thus the norm map descends to a group homomorphism

$$\mathrm{N} : C_K \to C_k^+(T).$$

As a consequence of basic results in global class field theory, we have:

Proposition 5.1 *Let K/k be an abelian extension of number fields, unramified outside the (real) places in T. Then the sequence of finite abelian groups*

$$C_K \xrightarrow{\mathrm{N}} C_k^+(T) \xrightarrow{\mathrm{A}} \mathrm{Gal}(K/k) \longrightarrow 0$$

is exact.

Proof. By [Ta, Theorem 5.1] we have an exact sequence of abelian groups,

$$I_K/K^* \xrightarrow{\mathrm{N}} I_k/k^* \xrightarrow{\mathrm{A}} \mathrm{Gal}(K/k) \longrightarrow 0,$$

where I_K and I_k are the idèles of K and k. Since K/k is ramified only at T, the subgroup

$$\prod_{v\in T}(k_v^*)_+ \times \prod_{v|\infty, v\notin T} k_v^* \times \prod_{\mathfrak{p}} \mathcal{O}_{k,\mathfrak{p}}^* \subset I_k$$

is in the kernel of the Artin homomorphism, and thus A descends to the quotient group $C_k^+(T)$ of I_k/k^*. Similarly, the induced norm map $\mathrm{N} : I_K/K^* \to C_k^+(T)$ descends to the quotient C_K of I_K/K^*. ■

Proof of Theorem 1.3. Let $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ be an orthogonal transformation with irreducible, unramified characteristic polynomial $S(x) \in \mathbb{Z}[x]$. Assume $p \equiv q \bmod 8$. Then $S(x)$ is a monic, irreducible, unramified reciprocal polynomial, of even degree $2n = p + q$, to which the discussion above applies.

As above we let T denote the roots of the reciprocal polynomial $R(x)$ in $(-2, 2)$. Since $S(x)$ is unramified, the associated quadratic extension K/k is unramified at all finite primes; it is only ramified at the infinite places in T. We now distinguish two cases.

Case 1. Assume $T = \emptyset$. (In this case the signature (p, q) is (n, n) by (2.1).)

By a result of Hecke [Wl, Theorem 13, p.291], the class $[\mathcal{O}_k^\vee]$ is equal to a square in C_k. That is, there is a fractional ideal $J \subset k$ and a $\xi \in k$ such that $J^2 \cdot (\xi) = \mathcal{O}_k^\vee$.

Let $L = \mathcal{O}_K \cdot J$. Then $L \subset K$ is a fractional ideal whose norm satisfies

$$\mathrm{N}(L) \cdot (\xi) = J^2 \cdot (\xi) = \mathcal{O}_k^\vee.$$

Since K/k is unramified at all finite places, this equation implies

$$L \cdot \overline{L} \cdot (\xi) = \mathcal{O}_K \cdot \mathcal{O}_k^\vee = \mathcal{O}_K^\vee.$$

Define $f : L \to L$ by $f(\alpha) = x\alpha$. Then Theorem 4.1 provides an f-invariant inner product making L into an even, unimodular lattice (of signature (n, n)).

By construction, the orthogonal transformations f and F share the same characteristic polynomial, $S(x)$. Moreover the sign invariants ϵ_F and ϵ_f trivially agree, since $T = \emptyset$. Therefore, by Theorem 2.4, there is an isometry

$$I : L \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}^{p+q}$$

conjugating f to F. Then F leaves invariant the even unimodular lattice $I(L) \subset \mathbb{R}^{p+q}$, completing the proof in the case $T = \emptyset$.

Case 2. Now assume $T \neq \emptyset$. Recall that $|T| = n - s$ is even by Proposition 3.3. Within the group $\langle \pm 1 \rangle^T$ of all possible sign maps $\epsilon : T \to \langle \pm 1 \rangle$, let

$$\begin{aligned} G &= \{\epsilon \, : \, \prod_T \epsilon(\tau) = A(\mathcal{O}_k^\vee)\}, \quad \text{and} \\ H &= \{\epsilon \, : \, \prod_T \epsilon(\tau) = (-1)^{|T|/2}\}. \end{aligned}$$

Clearly $|G| = |H| = 2^{|T|-1}$ (since $T \neq \emptyset$).

Let $h \in \mathrm{SO}_{u,v}(\mathbb{R})$ be an orthogonal transformation with characteristic polynomial $S(x)$. From equation (2.1), which relates the signature (u, v) of h to its sign invariant, we readily conclude that $u \equiv v \bmod 8$ iff $\epsilon_h \in H$. In particular, we have $\epsilon_F \in H$.

Now consider $\epsilon \in G$. By density of k in $k \otimes_{\mathbb{Q}} \mathbb{R}$, we can find an element $\xi \in k^*$ such that $\mathrm{sign}_\tau(\xi) = \epsilon(\tau)$ for all $\tau \in T$. By (5.1), we have $A(\mathcal{O}_k^\vee \cdot \xi^{-1}) = 1$. The exact sequence of Proposition 5.1 then implies that, after modifying ξ without changing the values of $\mathrm{sign}_\tau(\xi)$, $\tau \in T$, we can find a fractional ideal $L \subset K$ such that

$$\mathrm{N}(L) \cdot \xi = \mathcal{O}_k^\vee.$$

Define $f : L \to L$ by $f(\alpha) = x\alpha$. As in Case 1, Theorem 4.1 provides an f-invariant inner product making L into an even, unimodular lattice. By Theorem 4.2, the sign invariant of f is given by:

$$\epsilon_f(\tau) = \mathrm{sign}_\tau(\xi) = \epsilon(\tau).$$

Since the signature (u, v) of L satisfies $u \equiv v \bmod 8$ (by basic results on unimodular lattices [Ser, §5]), we have $\epsilon = \epsilon_f \in H$ for every $\epsilon \in G$.

But $|G| = |H|$, so in fact $G = H$. Therefore we can choose ξ and L such that $\epsilon_f = \epsilon_F$. Theorem 2.4 then provides an isometry I conjugating f to F, and therefore F preserves the even unimodular lattice $I(L) \subset \mathbb{R}^{p+q}$. ■

Remark. As a by-product of the proof we have shown that $A(\mathcal{O}_k^\vee) = (-1)^{|T|/2}$.

Proof of Theorem 1.2. By Corollary 2.3, under the stated conditions on (p, q) and s there is an $F \in \mathrm{SO}_{p,q}(\mathbb{R})$ with characteristic polynomial $S(x)$. By Theorem 1.3, just proved, there is an indefinite even unimodular lattice $L \subset \mathbb{R}^{p+q}$, invariant under F. Since L is determined up to isomorphism by its signature, we can regard $S(x)$ as the characteristic polynomial of an automorphism of $\mathrm{II}_{p,q}$. ■

Remark: reducible polynomials. We have restricted our attention to the problem of realizing *irreducible* polynomials via automorphisms of $\mathrm{II}_{p,q}$. The same local and global conditions are not sufficient in the reducible case, as the following example shows.

Proposition 5.2 *There is a monic unramified reciprocal polynomial $S(x) \in \mathbb{Z}[x]$ of degree 10, with $2s = 2$ roots off the unit circle, that does not arise as the characteristic polynomial of any $F \in \mathrm{SO}(\mathrm{II}_{9,1})$.*

Proof. Consider the product of a degree 4 cyclotomic polynomial and a degree 6 Salem polynomial given by

$$S(x) = C(x)D(x) = (x^4 - x^2 + 1) \cdot (x^6 - 3x^5 - x^4 + 5x^3 - x^2 - 3x + 1).$$

Clearly $S(x)$ is monic, reciprocal and unramified, with 2 roots off the unit circle. This polynomial is chosen so that C and D are relatively prime over $\mathbb{Z}$; that is, so there exist $A, B \in \mathbb{Z}[x]$ such that $AC + BD = 1$.

Now assume $F \in \mathrm{SO}(\mathrm{II}_{9,1})$ has characteristic polynomial $S(x)$. Then there is an F-invariant splitting of $\mathrm{II}_{9,1}$ into an orthogonal sum of even unimodular lattices,

$$\mathrm{II}_{9,1} = L_C \oplus L_D,$$

corresponding to the factorization of F. (Take L_C to be the image of $\mathrm{II}_{9,1}$ under the endomorphism $B(F) \circ D(F)$, and let L_D be the image under $A(F) \circ C(F)$.) The lattices L_C and L_D have ranks 4 and 6 respectively, so their signatures must be $(2, 2)$ and $(3, 3)$ by the condition $p \equiv q \bmod 8$. But then $L_C \oplus L_D$ has signature $(5, 5) \neq (9, 1)$. So no such F exists. ■

6 The spinor norm

This section establishes an arithmetic constraint on the characteristic polynomials of lattice automorphisms.

Theorem 6.1 *Let $F : L \to L$ be an automorphism of an even, unimodular lattice, with separable characteristic polynomial $S(x) \in \mathbb{Z}[x]$ of degree $2n$. Then the integers $|S(-1)|$, $|S(1)|$ and $(-1)^n S(1)S(-1)$ are squares.*

Spin. The proof is based on the relationship between the orthogonal group and its spin double-cover, which we now recall.

Let V be a finite-dimensional vector space over a field k, $\mathrm{char}(k) \neq 2$, equipped with a non-degenerate inner product $\langle v, w \rangle \in k$. Let $q : V \to k$ be the quadratic form defined by $2q(v) = \langle v, v \rangle$.

Consider the short exact sequence of algebraic groups over k,

$$1 \to \langle \pm 1 \rangle \to \mathrm{Spin}(V) \to \mathrm{SO}(V) \to 1,$$

where $\mathrm{SO}(V)$ is the special orthogonal group of (V, q), and $\mathrm{Spin}(V)$ is its double cover, constructed using the Clifford algebra of (V, q). Taking Galois cohomology gives the long exact sequence

$$1 \to \langle \pm 1 \rangle \to \mathrm{Spin}(V, k) \to \mathrm{SO}(V, k) \xrightarrow{\delta} H^1(k, \langle \pm 1 \rangle) \cong k^*/(k^*)^2. \qquad (6.1)$$

The connecting homomorphism

$$\delta : \mathrm{SO}(V, k) \to k^*/(k^*)^2$$

is the *spinor norm*; it measures the obstruction to lifting an element $F \in \mathrm{SO}(V, k)$ to $\mathrm{Spin}(V, k)$. More precisely, if $\delta(F) \equiv a \bmod (k^*)^2$, then F lifts to an element $\widetilde{F} \in \mathrm{Spin}(V, K)$ defined over the quadratic extension $K = k[\sqrt{a}]$.

The spinor norm $\delta(F)$ can be computed as follows (see [Art, Ch.5].) Write F as a product of reflections $\rho(v_i)$ through the normal hyperplanes of vectors $v_i \in V$. Then

$$\delta(F) \equiv \prod q(v_i)$$

as a class in $k^*/(k^*)^2$.

Theorem 6.2 *Let $F : V \to V$ be an automorphism of a finite-dimensional orthogonal space over $\mathbb{Q}$, preserving an even, unimodular lattice $L \subset V$. Then its spinor norm satisfies $\delta(F) \equiv \pm 1 \bmod (\mathbb{Q}^*)^2$.*

Proof. Over $\mathbb{Z}$ we have an exact sequence in flat cohomology, analogous to (6.1), of the form

$$1 \to \langle \pm 1 \rangle \to \mathrm{Spin}(L, \mathbb{Z}) \to \mathrm{SO}(L, \mathbb{Z}) \xrightarrow{\Delta} \mathbb{Z}^*/(\mathbb{Z}^*)^2 = \langle \pm 1 \rangle,$$

by [Kn, III.3.2.5 and IV.6.2.6] (using the fact that $\mathrm{Pic}(\mathbb{Z}) = 1$). Here Δ is a refinement of the spinor norm over $\mathbb{Q}$; it satisfies $\Delta(F) \equiv \delta(F) \bmod (\mathbb{Q}^*)^2$. Therefore $\delta(f) \equiv \pm 1$. ■

Proof of Theorem 6.1. Let $F : L \to L$ be an automorphism of an even, unimodular lattice of rank $2n$, with separable, reciprocal characteristic polynomial $S(x)$. Since $\delta(F) = \pm 1$, there is always a lift $\widetilde{F}$ of F to $\mathrm{Spin}(V, K)$ where $K = \mathbb{Q}[\sqrt{-1}]$. Let $t_\pm$ denote the traces of $\widetilde{F}$ on the two half-spin representations $W_\pm$ of $\mathrm{Spin}(V, K)$. By [FH, pp. 378–379] these traces satisfy

$$\begin{aligned} S(-1) &= (t_- + t_+)^2, \\ (-1)^n S(+1) &= (t_- - t_+)^2. \end{aligned}$$

Since we have $t_\pm \in \mathbb{Q}[\sqrt{-1}]$ and $S(\pm 1) \in \mathbb{Z}$, the integers $|S(\pm 1)|$ are squares.

Finally, by Proposition A.3 of the Appendix, the integer $(-1)^n S(-1) S(1)$ represents the discriminant of L in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Since L is unimodular of signature (p, q), we have

$$\mathrm{disc}(L) = (-1)^n \det(L) = (-1)^n (+1)^p (-1)^q.$$

But L is also even, so $p \equiv q \bmod 8$, and thus $q \equiv n \bmod 4$. Therefore $\mathrm{disc}(L) = 1$, and thus $(-1)^n S(-1) S(1)$ is also square. ■

7 Salem polynomials

This section gives a construction of infinitely many unramified Salem polynomials, proving Theorem 1.6.

Cyclotomic polynomials. The *cyclotomic polynomial* $\Phi_d(x) \in \mathbb{Z}[x]$ is the monic polynomial vanishing at the primitive dth roots of unity. For $d \geq 3$, $\Phi_d(x)$ is a reciprocal polynomial of even degree $2n = \phi(d)$. We begin by characterizing the unramified cyclotomic polynomials.

Theorem 7.1 *For any $d \geq 3$ we have*

$$(\Phi_d(-1), \Phi_d(+1)) = \begin{cases} (2,2) & \textit{if } d = 2^e, \textit{ some } e > 0; \\ (1,p) & \textit{if } d = p^e, \ p \textit{ an odd prime;} \\ (p,1) & \textit{if } d = 2p^e, \ p \textit{ an odd prime; and} \\ (1,1) & \textit{otherwise.} \end{cases}$$

Proof. Cyclotomic polynomials obey the recursion formula:

$$\Phi_d(x) = \frac{1 + x + \cdots + x^{d-1}}{\prod\{\Phi_e(x) \ : \ e|d \text{ and } 1 < e < d\}}.$$

Thus $\Phi_d(1) = d / \prod \Phi_e(1)$. From this expression the values of $\Phi_d(1)$ are easily determined by induction. The proof for $\Phi_d(-1)$ is similar. ■

Corollary 7.2 *The cyclotomic polynomial $\Phi_d(x)$ is unramified unless $d = p^e$ or $2p^e$ for some prime p.*

Cyclotomic trace polynomials. The associated *cyclotomic trace polynomial* $R_d(x)$ of degree $\phi(d)/2$ vanishes at the points $x = 2\cos(2\pi k/d)$, $(k, d) = 1$. Its zeros are the traces of matrices in $\mathrm{SO}(2, \mathbb{R})$ of order d. The first few cyclotomic trace polynomials are given by

$$\begin{aligned} R_3(x) &= x + 1, \\ R_4(x) &= x, \\ R_5(x) &= x^2 + x - 1, \\ R_6(x) &= x - 1, \\ R_7(x) &= x^3 + x^2 - 2x - 1. \end{aligned}$$

Among irreducible monic polynomials in $\mathbb{Z}[x]$, the cyclotomic trace polynomials are exactly those with all roots in $(-2, 2)$.

Salem numbers. A *Salem polynomial* $S(x) \in \mathbb{Z}[x]$ is a monic, irreducible reciprocal polynomial with exactly two roots outside the unit circle, both positive real numbers. The unique root $\lambda > 1$ is a *Salem number.*

A *Salem trace* is an algebraic integer $\tau > 2$ whose other conjugates all lie in the interval $[-2, 2]$; its minimal polynomial $R(x)$ is a *Salem trace polynomial.* Salem traces and Salem numbers correspond bijectively, via the relation $\tau = \lambda + \lambda^{-1}$, and $R(x)$ is the trace polynomial of $S(x)$.

Recall that a Salem polynomial of degree $2n$ is *unramified* if $|S(\pm 1)| = 1$; equivalently, if $|R(\pm 2)| = 1$. This condition implies n is odd and $R(\pm 2) = -1$ (see Proposition 3.3). Conversely, whenever n is odd, Salem polynomials of degree $2n$ can be constructed using the following result.

Theorem 7.3 *Let $C(x) \in \mathbb{Z}[x]$ be a monic separable polynomial of even degree $n - 3$, with all roots in $(-2, 2)$. Then for all $a \in \mathbb{Z}$ sufficiently large,*

$$R(x) = C(x)(x^2 - 4)(x - a) - 1$$

is an unramified Salem trace polynomial of degree n, and hence

$$S(x) = x^n R(x + x^{-1})$$

is an unramified Salem polynomial of degree $2n$.

Note that $C(x)$ must be a product of cyclotomic trace polynomials.

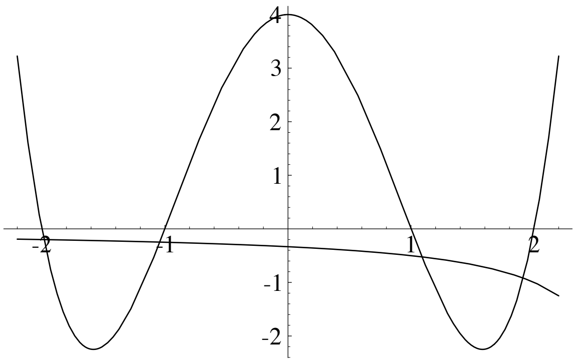

Figure 1. The graphs of $y = C(x)(x^2 - 4)$ and $y = 1/(x - a)$.

Proof. Clearly $n = \deg R(x)$. We first show $R(x)$ has $n-1$ roots in $(-2, 2)$. Indeed, for $a \gg 0$, the roots in $(-2, 2)$ are the solutions to the equation

$$C(x)(x^2 - 4) = \frac{1}{x-a} \approx -\frac{1}{a} < 0.$$

Inspecting the graphs of these functions, we see they cross at $n - 1$ points in $(-2, 2)$, near the $n - 1$ roots of $D(x) = C(x)(x^2 - 4)$ (see Figure 1). More precisely, the condition that $C(x)$ has even degree implies $D'(-2) < 0$ and $D'(2) > 0$, so the zeros of $D(x)$ at the endpoints of $[-2, 2]$ give rise to zeros of $R(x)$ inside $(-2, 2)$. The other roots of $D(x)$ are simple and lie strictly inside of $(-2, 2)$, so they also give rise to roots of $R(x)$ in $(-2, 2)$, by transversality.

Thus $R(x)$ has $n - 1$ roots in $(-2, 2)$, and the remaining root lies near $x = a \gg 0$. By construction $R(\pm 2) = -1$, so $R(x)$ is unramified. To complete the proof we need only check that $R(x)$ is irreducible.

If $R(x)$ is reducible, then one of its irreducible factors $P(x)$ has all its roots in $(-2, 2)$, and hence is a cyclotomic trace polynomial. The set of such polynomials of given degree is finite. As $a \to \infty$, the roots of $R(x)$ in $(-2, 2)$ converge to those of $D(x)$, so eventually $P(x)$ would have to divide $C(x)$. But $R(x) = 1$ at the zeros of $C(x)$, so no factor of $C(x)$ can be a factor of $R(x)$. Thus $R(x)$ is irreducible for all a sufficiently large.

It follows that $S(x) = x^n R(x + x^{-1})$ is also irreducible, and hence $S(x)$ is an unramified Salem polynomial. ∎

Remark: double roots. It is not hard to see that Theorem 7.3 continues to hold if $C(x)$ is allowed to have one or more double roots, so long as $C''(x) > 0$ at each such root.

Examples.

1. Let $C(x) = 1$. Then $R(x) = (x^2 - 4)(x - a) - 1$ is an unramified Salem trace polynomial for all $a \geq 0$. The corresponding Salem polynomials are given by:

   $$S(x) = x^6 - ax^5 - x^4 + (2a - 1)x^3 - x^2 - ax + 1, \quad a \geq 0.$$

   These are the only unramified Salem polynomials of degree 6. The case $a = 0$ corresponds to $\lambda \approx 1.40127$, the smallest Salem number of degree 6. By Theorem 1.2, these Salem polynomials all arise as characteristic polynomials of automorphisms $F \in \mathrm{SO}(\mathrm{II}_{3,3})$.

2. Let $C(x) = (x + 1)^2$. Then $R(x) = C(x)(x^2 - 4)(x - a) - 1$ is an unramified Salem trace polynomial for all $a \geq 1$. The case $a = 1$ corresponds to the smallest known Salem number, $\lambda \approx 1.17628$, a root of Lehmer's polynomial (1.1). The corresponding degree 10 Salem polynomials $S(x)$ can be realized by automorphisms of $\mathrm{II}_{9,1}$ *and* by automorphisms of $\mathrm{II}_{5,5}$.

   In fact, the six smallest known Salem numbers (which can be found in [B]) are all unramified, and the corresponding Salem trace polynomials all arise as special cases of Theorem 7.3.

3. Let $C(x) = R_{17}(x)$, where

   $$R_{17}(x) = 1 - 4x - 10x^2 + 10x^3 + 15x^4 - 6x^5 - 7x^6 + x^7 + x^8$$

   is the cyclotomic trace polynomial for the 17th roots of unity. Then $R(x) = C(x)(x^2 - 4)(x - a) - 1$ is an unramified Salem trace polynomial for all $a \geq 31$. The corresponding Salem polynomials have degree 22 and arise from K3 surface automorphisms, according to Theorem 1.7.

Proof of Theorem 1.6. Let $n \geq 3$ be an odd integer. We will show there exist infinitely many unramified Salem polynomials of degree $2n$.

Writing $n - 3$ in base 2, we obtain exponents $1 \leq k_1 < k_2 < \cdots < k_n$ such that $n - 3 = \sum_1^n 2^{k_i}$. Let $R_d(x)$ denote the cyclotomic trace polynomial for the primitive d roots of unity, let $d_i = 2^{k_i + 2}$ and let

$$C(x) = R_{d_1}(x)R_{d_2}(x) \cdots R_{d_n}(x).$$

(If $n = 3$ we take $C(x) = 1$.)

Noting that $\deg R_{2^k} = 2^{k-2}$, we find $\deg C(x) = n - 3$. Since the roots of $R_d(x)$ lie in $(-2, 2)$, the same is true of the roots of $C(x)$. Moreover the roots of $C(x)$ are simple since the d_i are distinct. Thus Theorem 7.3 provides infinitely many unramified Salem trace polynomials $R(x)$ of degree n, and hence infinitely many unramified Salem polynomials of degree $2n$. ■

8 K3 surfaces

In this section we prove Theorem 1.7, showing in particular that every unramified degree 22 Salem polynomial arises as the characteristic polynomial of $f^*|H^2(X)$ for an automorphism $f : X \to X$ of a complex K3 surface X.

The pair (X, f) is synthesized from a lattice automorphism (L, F).

Theorem 8.1 *Let $F : L \to L$ be an automorphism of an even, unimodular lattice of signature $(3, 19)$. Suppose $S(x) = \det(xI - F)$ is a Salem polynomial. Then there is:*

- *A K3 surface automorphism $f : X \to X$, and*
- *An isomorphism of lattices $\iota : L \to H^2(X, \mathbb{Z})$, making the diagram*

$$\begin{tikzcd} L \arrow[r, "F"] \arrow[d, "\iota"'] & L \arrow[d, "\iota"'] \\ H^2(X,\mathbb{Z}) \arrow[r, "f^*"] & H^2(X,\mathbb{Z}) \end{tikzcd}$$

commute.

See [Mc, Theorem 3.4]; the proof is based on the Torelli theorem and surjectivity of the period mapping.

Proof of Theorem 1.7. By Theorem 2.2, there is an $F \in \mathrm{SO}_{3,19}(\mathbb{R})$ with characteristic polynomial $S(x)$ such that for $\tau = \delta + \overline{\delta}$, the sum of eigenspaces

$$E_\tau = V_\delta \oplus V_{\overline{\delta}} \subset \mathbb{C}^{3+19}$$

has signature $(2, 0)$. By Theorem 1.3 there is an even, unimodular lattice $L \subset \mathbb{R}^{3+19}$ preserved by F. Applying Theorem 8.1 above, we obtain a K3 surface automorphism f with $S(x) = \det(xI - f^*|H^2(X))$, compatible with an isomorphism $\iota : L \to H^2(X, \mathbb{Z})$.

Since
$$Q = H^{2,0}(X) \oplus H^{0,2}(X) \subset H^2(X,\mathbb{C})$$
is the unique f^*-invariant subspace defined over $\mathbb{R}$ with signature $(2,0)$, the map $\iota \otimes \mathbb{C} : L \otimes \mathbb{C} \to H^2(X,\mathbb{C})$ sends E_τ to Q. Thus f^* acts on $H^{2,0}(X)$ by multiplication by δ or $\overline{\delta}$. In the latter case, we can replace X and f with their complex conjugates to change $\overline{\delta}$ to δ. ■

Proof of Corollary 1.8. Let $S(x)$ be an unramified degree 22 Salem number of trace t. We must show $t \geq -2$.

Let $f : X \to X$ be a K3 surface automorphism with characteristic polynomial $S(x)$, furnished by the preceding result. Then the Lefschetz number of f is given by
$$L(f) = \operatorname{Tr}\left(f^*|H^0(X) \oplus H^2(X) \oplus H^4(X)\right) = 2 + t.$$
Since $S(x)$ irreducible, $f^*|H^2(X,\mathbb{Q})$ is also irreducible and thus
$$\operatorname{Pic}(X) = H^{1,1}(X) \cap H^2(X,\mathbb{Z}) = (0).$$
Every K3 surface is Kähler, so the vanishing of $\operatorname{Pic}(X)$ implies the only proper subvarieties of X are finite sets of points. In particular, the fixed-points of f are isolated, so their total number (counted with multiplicity) is $L(f)$. Since f is holomorphic, every fixed-point has positive multiplicity, and thus $2 + t \geq 0$. ■

A Appendix: Orthogonal automorphisms over a general field

Let k_0 be any field with $\operatorname{char}(k_0) \neq 2$. This Appendix reviews the classification of automorphisms of even-dimensional orthogonal spaces over k_0, extending the results over $\mathbb{R}$ given in §2.

An *orthogonal space* V of dimension $2n$ over k_0 is a vector space equipped with a non-degenerate inner product $\langle v, w\rangle \in k_0$. Let $\operatorname{SO}(V)$ denote the group of k_0-linear maps $T : V \to V$ with $\det(T) = 1$ preserving the inner product. As in the real case, we have:

Proposition A.1 *The characteristic polynomial $S(x) = \det(xI - F) \in k_0[x]$ of any $F \in \operatorname{SO}(V)$ is a reciprocal polynomial.*

Proof. The polynomial $S(x) = \sum a_i x^i$ is reciprocal if and only if $a_i = a_{2n-i}$ for all i. To see this identity, note that

$$a_{2n-i} = (-1)^i \operatorname{Tr}(\wedge^i F).$$

The bilinear form on V gives rise to a natural isomorphism between the representations $\wedge^i V$ and $\wedge^{2n-i} V$ of $\mathrm{SO}(V)$, and thus $a_i = a_{2n-i}$. ■

Equivalent automorphisms. Our goal is to classify pairs (V, F) of orthogonal spaces equipped with automorphisms $F \in \mathrm{SO}(V)$.

Let us say (V, F) and (V', F') are *equivalent* if there is an isometry $I : V \to V'$ (a k_0-linear isomorphism preserving the inner product) such that the diagram

$$\begin{tikzcd} V \arrow[r, "F"] \arrow[d, "I"'] & V \arrow[d, "I"'] \\ V' \arrow[r, "F'"] & V' \end{tikzcd}$$

commutes. Equivalent pairs have the same characteristic polynomial.

Separable polynomials. A monic degree d polynomial $P(x) \in k_0[x]$ is *separable* if it has d distinct roots in the algebraic closure $\overline{k}_0$ of k_0. For such a polynomial, the algebra $A = k_0[x]/P(x)$ is a product of finite separable field extensions $A_1 \times \cdots \times A_m$ of k_0, one for each irreducible factor of $P(x)$. The trace map $\operatorname{Tr}^A_{k_0} : A \to k_0$ agrees with the sum of the trace maps for each factor A_i/k_0.

A key property of the algebra A, which we will use below, is that the trace form is non-degenerate; that is, we have an isomorphism

$$A \cong \operatorname{Hom}_{k_0}(A, k_0) \quad \text{by} \quad \alpha \mapsto \psi_\alpha(\beta) = \operatorname{Tr}^A_{k_0}(\alpha\beta).$$

This follows from the corresponding fact for the separable extensions A_i/k_0.

Classification. In this section we assume:

- $S(x) \in k_0[x]$ is a monic, *separable* reciprocal polynomial of degree $2n$.

As usual we can associate to $S(x)$ its degree n trace polynomial $R(x)$, satisfying $S(x) = x^n R(x + x^{-1})$; it is also separable.

Let K/k be the corresponding extension of algebras, where $K = k_0[x]/S(x)$, $k = k_0[y]/R(y)$ and $y = x + x^{-1}$. As remarked above, K and k are products of separable field extensions of k_0.

The 'Galois group' of K/k is generated by the automorphism satisfying $\iota(x) = x^{-1}$, and for $\alpha \in K$ we write $\overline{\alpha} = \iota(\alpha)$. Let $\mathrm{N} = \mathrm{N}_k^K : K \to k$ be the norm map, given by

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha}.$$

Our main result determines the structure of the space

$$\begin{aligned} \mathcal{V}(S) \quad = \quad & \{(V, F) \ : \ F : V \to V \text{ is an orthogonal automorphism over } k_0 \\ & \text{with } \det(xI - F) = S(x)\}/(\text{equivalence}). \end{aligned}$$

Theorem A.2 *Given a monic separable reciprocal polynomial $S(x) \in k_0[x]$, there is a natural bijection between $\mathcal{V}(S)$ and the 2-group*

$$\operatorname{coker}(\mathrm{N}) = k^*/\,\mathrm{N}(K^*).$$

For any (V, F) in $\mathcal{V}(S)$, the centralizer $Z(V, F)$ of F in $\mathrm{O}(V)$ is naturally isomorphic to the abelian group

$$\ker(\mathrm{N}) = \{\lambda \in K^* : \lambda\overline{\lambda} = 1\}.$$

Proof. Given $\xi \in k^*$, let $V_\xi = K$ equipped with the k_0-valued inner product

$$\langle \alpha, \beta \rangle_\xi = \mathrm{Tr}_{k_0}^K(\xi\alpha\overline{\beta}).$$

Then we have $(V_\xi, f) \in \mathcal{V}(S)$, where $f : K \to K$ is given by $f(\alpha) = x\alpha$.

If $\xi, \lambda \in k^*$ are related by $\xi = \lambda\,\mathrm{N}(\delta)$, $\delta \in K^*$, then the map $I : K \to K$ given by $I(\alpha) = \delta\alpha$ is an isometry between (V_ξ, f) and (V_λ, f). Thus we obtain a well-defined map

$$\phi : k^*/\,\mathrm{N}(K^*) \to \mathcal{V}(S),$$

given by $\phi(\xi) = (V_\xi, f)$.

Conversely, suppose $I : V_\xi \to V_\lambda$ is an isometry giving an equivalence between (V_ξ, f) and (V_λ, f). Then I is k_0-linear; moreover, $I(x\alpha) = xI(\alpha)$, and thus I is K-linear. That is, upon identifying V_ξ and V_λ with K, there exists a $\delta \in K^*$ such that $I(\alpha) = \delta\alpha$. Therefore we have:

$$\mathrm{Tr}_{k_0}^K(\xi\alpha\overline{\beta}) = \mathrm{Tr}_{k_0}^K(\lambda\delta\overline{\delta}\alpha\overline{\beta})$$

for all $\alpha, \beta \in K$. Since the trace form establishes an isomorphism between K and $\mathrm{Hom}_{k_0}(K, k_0)$, we conclude that $\xi = \lambda\,\mathrm{N}(\delta)$. Thus ϕ is *injective.*

We now show ϕ is *surjective.* Given $(V, F) \in \mathcal{V}(S)$, we can make V into a 1-dimensional vector space over $K = k_0[x]/S(x)$ by setting $\alpha(x) \cdot v =$

$\alpha(F)(v)$. Choosing a basis, we obtain an identification between V and K such that $F(\alpha) = x\alpha$. Under this identification, there is a unique element $\xi \in K^*$ such that

$$\langle 1, \beta\rangle_V = \mathrm{Tr}^K_{k_0}(\xi\overline{\beta})$$

for all $\beta \in K$. (Here again we use the fact that the trace form identifies K with $\mathrm{Hom}_{k_0}(K, k_0)$.) Since the inner product on V is F-invariant, we have

$$\langle x^i, \beta\rangle_V = \langle 1, x^{-i}\beta\rangle_V = \mathrm{Tr}^K_{k_0}(\xi x^i \overline{\beta})$$

for all i, and thus

$$\langle \alpha, \beta\rangle_V = \mathrm{Tr}^K_{k_0}(\xi\alpha\overline{\beta}) = \langle \alpha, \beta\rangle_\xi$$

for all $\alpha, \beta \in K$. Moreover we have $\xi \in k$ because $\langle \alpha, \beta\rangle_V = \langle \beta, \alpha\rangle_V$, and $\xi \in k^*$ because the inner product is non-degenerate. Thus (V, F) is equivalent to (V_ξ, f), $\xi \in k^*$, and therefore ϕ is surjective.

Finally we observe that for $(V, F) \cong (V_\xi, f)$, the centralizer of (V, F) in $\mathrm{GL}(V)$ can be identified with K^*, and thus the centralizer of (V, F) in $\mathrm{O}(V)$ can be identified with the elements $\lambda \in K^*$ such that

$$\langle \lambda\alpha, \lambda\beta\rangle_\xi = \langle \alpha, \lambda\overline{\lambda}\beta\rangle_\xi = \langle \alpha, \beta\rangle_\xi$$

for all $\alpha, \beta \in K$. But this condition holds iff $\lambda\overline{\lambda} = 1$, and thus $Z(V, F)$ is isomorphic to the kernel of the norm map $\mathrm{N} : K^* \to k^*$. ■

Real polynomials. As an example, suppose $k_0 = \mathbb{R}$. Then in $\mathbb{R}[x]$ the trace polynomial $R(x)$ factors as a product of r linear and c irreducible quadratic polynomials, where $r + 2c = n$. Let $r = t + u$ where t is the number of roots of $R(x)$ in the interval $(-2, 2)$. Then we have

$$k \cong \mathbb{R}^t \oplus \mathbb{R}^u \oplus \mathbb{C}^c \quad \text{and} \quad K \cong \mathbb{C}^t \oplus \mathbb{R}^{2u} \oplus \mathbb{C}^{2c}.$$

Therefore $k^*/\mathrm{N}(K^*) = (\mathbb{R}^*)^t/\mathrm{N}(\mathbb{C}^*)^t = \langle \pm 1\rangle^t$. This group parameterizes the possible *sign invariants* ϵ_F introduced in §2.

The discriminant. We conclude by showing that the discriminant of the quadratic space V/k_0 is determined by the characteristic polynomial of F.

The *determinant* of a non-degenerate orthogonal space V over k_0 is defined by choosing a basis $(v_1, \ldots, v_n)$ for V and setting

$$\det(V) \equiv \det(\langle v_i, v_j\rangle) \quad \text{in} \quad k_0^*/(k_0^*)^2.$$

If V has dimension $2n$, we define its *discriminant* by

$$\mathrm{disc}(V) \equiv (-1)^n \det(V)$$

as a class in $k_0^*/(k_0^*)^2$. The sign is chosen so that the discriminant of a split orthogonal space of dimension $2n$ (i.e., one with an isotropic subspace of dimension n) is a square in k_0^*.

Proposition A.3 *Let $F \in \mathrm{SO}(V)$ be an orthogonal transformation with separable, reciprocal, characteristic polynomial $S(x)$ of degree $2n$. Then the discriminant of V is given by*

$$\operatorname{disc}(V) = (-1)^n S(1) S(-1)$$

as a class in $k_0^*/(k_0^*)^2$.

Proof. We have seen that (V, F) is equivalent to (V_ξ, f) for some $\xi \in k^*$, where $V_\xi = K$ with inner product $\langle \alpha, \beta \rangle_\xi = \mathrm{Tr}_{k_0}^K(\xi \alpha \overline{\beta})$, and $f(\alpha) = x\alpha$.

As an orthogonal space over k_0, the space V_ξ is a direct sum of two n-dimensional subspaces:

$$V_\xi = K = k \oplus k^\perp = k \oplus k \cdot (x - x^{-1}).$$

Here k and $k^\perp$ are the $+1$ and -1 eigenspaces of the Galois automorphism of K/k, which acts by isometry. Therefore

$$\det(V_\xi) = \det(k)\det(k^\perp) = \det(k)^2 \cdot \mathrm{N}_{k_0}^K(x - x^{-1}) \equiv \mathrm{N}_{k_0}^K(x - x^{-1})$$

modulo $(k_0^*)^2$. But the norm of x is 1, so we have

$$\mathrm{N}_{k_0}^K(x - x^{-1}) = \mathrm{N}(x^2 - 1) = \mathrm{N}(x - 1)\,\mathrm{N}(x + 1) = S(-1)S(1).$$

Taking into account the sign convention, we obtain $\operatorname{disc}(V) = \operatorname{disc}(V_\xi) = (-1)^n S(-1)S(1)$. ■

Notes. Many of the results reviewed above are also discussed in [Mil].

References

[Art] E. Artin. *Geometric Algebra.* Wiley Interscience, 1988. Reprint of the 1957 original.

[Ba1] E. Bayer-Fluckiger. Definite unimodular lattices having an automorphism of given characteristic polynomial. *Comment. Math. Helv.* **59**(1984), 509–538.

[Ba2] E. Bayer-Fluckiger. Lattices and number fields. In *Algebraic Geometry: Hirzebruch 70 (Warsaw, 1998)*, pages 69–84. Amer. Math. Soc., 1999.

[Bor] R. E. Borcherds. Coxeter groups, Lorentzian lattices, and K3 surfaces. *Internat. Math. Res. Notices* **19**(1998), 1011–1031.

[B] D. Boyd. Small Salem numbers. *Duke Math. J.* **44**(1977), 315–328.

[CoS] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag, 1999.

[FT] A. Fröhlich and M. J. Taylor. *Algebraic Number Theory*. Cambridge University Press, 1993.

[FH] W. Fulton and J. Harris. *Representation Theory*. Springer-Verlag, 1991.

[Hir] E. Hironaka. The Lehmer polynomial and pretzel links. *Canad. Math. Bull.* **44**(2001), 440–451.

[Kn] M.-A. Knus. *Quadratic and Hermitian Forms over Rings*. Springer-Verlag, 1991.

[La] S. Lang. *Algebraic Number Theory*. Addison-Wesley, 1970.

[Mc] C. McMullen. Dynamics on K3 surfaces: Salem numbers and Siegel disks. *J. reine angew. Math.* **545**(2002), 201–233.

[Mil] J. Milnor. On isometries of inner product spaces. *Invent. math.* **8**(1969), 83–97.

[MH] J. Milnor and D. Husemoller. *Symmetric Bilinear Forms*. Springer, 1973.

[Rol] D. Rolfsen. *Knots and Links*. Publish or Perish, Inc., 1976.

[Ser] J. P. Serre. *A Course in Arithmetic*. Springer-Verlag, 1973.

[Smy] C. J. Smyth. Salem numbers of negative trace. *Math. Comp.* **69**(2000), 827–838.

[Ta] J. Tate. Global class field theory. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, pages 162–203. Academic Press Inc., 1986. Reprint of the 1967 original.

[Wl] A. Weil. *Basic Number Theory.* Springer-Verlag, 1967.

MATHEMATICS DEPARTMENT
HARVARD UNIVERSITY
1 OXFORD ST
CAMBRIDGE, MA 02138-2901