Unramified reciprocal polynomials and Coxeter decompositions

Benedict H. Gross

Let $f(x)$ be a monic, integral polynomial of degree $2n$, which is irreducible over $\mathbf{Q}$. We say $f(x)$ is reciprocal provided $x^{2n}f(1/x) = f(x)$, and unramified provided $f(-1) \cdot f(1) = (-1)^n$. In an earlier paper [G-M], we realized such unramified, reciprocal, irreducible polynomials as the characteristic polynomials of automorphisms t of certain even, unimodular lattices L of rank $2n$.

A natural question which then arises is to classify the pairs (L, t) with characteristic polynomial $f(x)$, up to isomorphism. One invariant of an even, unimodular L is its signature (p, q) over the reals; here we will assume that $(p - q)$ is maximal, equal to the number of complex roots of $f(x)$ which lie on the unit circle. An invariant of the pair (L, t) is the ring of endomorphism of the abelian group L which commute with t. This is an order A in the number field $K = \mathbf{Q}[x]/f(x)$ which contains the order $\mathbf{Z}[x]/f(x)$, and we will classify those pairs where A is equal to the full ring of integers A_K of K. In particular, we show that the number of equivalence classes with this property is equal to a power of 2 times the minus class number of K; a precise statement is given in Proposition 1.7.

We then turn to the classification of those pairs (L, t) where t is conjugate to t^{-1} in the orthogonal group $O(L)$. This is a natural condition to impose, as it is true in the orthogonal group over $\mathbf{Q}$. To this end, we develop the notion of a Coxeter decomposition of L over $\mathbf{Z}$. A Coxeter decomposition is, among other things, a pair (L_1, L_2) of positive definite scaled unimodular sublattices of L, such that $L = L_1 + L_2$ as an abelian group. From this decomposition, we obtain two involutions σ_1 and σ_2 in $O(L)$, whose -1 eigenspaces are L_1 and L_2, and we require that the product $\sigma_1\sigma_2 = t$ has characteristic polynomial $f(x)$. Such decompositions occur in the theory of simply-laced Coxeter groups, when the Coxeter graph can be 2-colored. There t is a Coxeter element, and each σ_i is the product of simple reflections.

We end with some examples of Coxeter decompositions, for unramified cyclotomic and Salem polynomials. Here the lattices constructed are positive definite and hyperbolic respectively. Our hope is that by attaching a rich algebraic stucture, such as an even, unimodular lattice L with a Coxeter decomposition, to an unramified, reciprocal polynomial $f(x)$, we will obtain a new tool to investigate some of the deeper questions (like the Lehmer conjecture for Salem numbers) on the location of the real roots of $f(x)$. As a by-product, we also get candiates for the "Coxeter element" of lattices L (such as the Leech lattice) which have no simple reflections in their orthogonal group.

It is a pleasure to thank Daniel Allcock, Curt McMullen, and William Stein for their help.

Table of Contents

1. A classification (cf. [G-M])

We fix an unramified, reciprocal, irreducible polynomial $f(x)$, of degree $2n$ over $\mathbf{Z}$. Let K be the number field $\mathbf{Q}[x]/(f(x))$, of degree $2n$, and let k be the subfield fixed by the involution $\alpha \mapsto \overline{\alpha}$ of K, where $\overline{x} = x^{-1}$.

We will assume that all of the complex roots λ of $f(x)$ lie on the union of the unit circle and the positive real line. Then $\lambda + \lambda^{-1}$ is a real number greater than -2, and the field k is totally real. We will further assume that the number s of roots $\lambda > 1$ satisfies the congruence

$$s \equiv n \pmod 4. \tag{1.1}$$

This implies that the set T of real places of k which ramify in K satisfies

$$\#T = n - s \equiv 0 \pmod 4. \tag{1.2}$$

Some examples of polynomials $f(x)$ which satisfy our hypotheses are unramified cyclotomic polynomials (when $s = 0$) of degree $8k = 8, 16, 24, \ldots$ and unramified Salem polynomials (when $s = 1$) of degree $8k + 2 = 10, 18, 26, \ldots$. As specific examples, there is the cyclotomic polynomial

$$f(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1\ , \tag{1.3}$$

satisfied by the primitive 30-th roots of 1, and the Salem polynomial

$$f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1\ , \tag{1.4}$$

satisfied by Lehmer's number $\lambda = 1.17628\ldots$

Given such a polynomial $f(x)$, we wish to classify the even, unimodular lattices L of signature $(2n - s, s)$, together with the isometries $t : L \to L$ which have characteristic polynomial $f(x)$. We consider the pairs (L, t) and (L', t') equivalent if there is an isometry $i : L \to L'$ such that $t' \circ i = i \circ t$.

Since t satisfies its own characteristic polynomial in $\mathrm{End}(L)$, L is a $\mathbf{Z}[x]/f(x)$-module. Let A_K be in integral closure of $\mathbf{Z}[x]/f(x)$ in the field K. We will classify those lattices which are full A_K-modules.

Let $E_K = A_K^*$ be the unit group of K, and let $C_K = \mathrm{Pic}(A_K)$ be the ideal class group. The norm from K to k induces homomorphisms

$$\mathbf{N} : E_K \to E_{k,T}^+ \tag{1.5}$$

$$\mathbf{N} : C_K \to C_{k,T}^+. \tag{1.6}$$

Here $E_{k,T}^+$ is the subgroup of the units of k which are positive at the real places in T, and $C_{k,T}^+$ is the quotient of the ideal group of k by the principal ideals which have a positive generator at T.

Proposition 1.7. *The set of equivalence classes of even, unimodular, A_K-lattices of signature $(2n-s,s)$ is finite and non-empty, of cardinality*

$$\#\ \mathrm{coker}\left(E_K \underset{\mathbf{N}}{\to} E_{k,T}^+\right) \cdot \#\ \ker\left(C_K \underset{\mathbf{N}}{\to} C_{k,T}^+\right).$$

Proof. Let $A_K^\vee$ be the dual module of A_K with respect to the trace form. In [G-M] we show that the even, unimodular, A_K-lattices of signature $(2n-s,s)$ are all given by pairs (L,c), where L is a fractional ideal of K, c is an element of k^* which is positive at the real places of T, and the pair satisfies the ideal equation

$$L \cdot \overline{L} \cdot (c) = A_K^\vee. \tag{1.8}$$

The pairing on L is given by the formula

$$\langle \alpha, \beta \rangle = \mathrm{Tr}(c\alpha\overline{\beta}). \tag{1.9}$$

In [G-M] we also show such pairs *exist*. Here we need the hypothesis that $s \equiv n (\mathrm{mod} 4)$, so that the signature (p, q) of L has difference $p - q = 2n - 2s$ divisible by 8.

The pair (L, c) is equivalent to the pair (L', c') if there is an element γ in K^* with

$$L' = (\gamma) \cdot L$$
$$c' = c/\gamma\overline{\gamma}. \tag{1.10}$$

The group of pairs (I, a), where $I \cdot \overline{I} = (a)$ and $a > 0$ at T, acts simply-transitively on the solutions of (1.8) by the formula $(L, c) \mapsto (I \cdot L, c/a)$. The quotient group $\{(I, a)\}/\{((\gamma), \gamma\overline{\gamma})\}$ acts simply-transitively on the equivalence classes of lattices.

This quotient group maps surjectively to the group $\ker(\mathbf{N} : C_K \to C_{k,T}^+)$ by the map $(I, a) \mapsto$ class of I in C_K.

The kernel of this map is isomorphic to the group $\mathrm{coker}(\mathbf{N} : E_K \to E_{k,T}^+)$ via the map

$$((\gamma), a) \mapsto \gamma\overline{\gamma}/a \pmod{\mathbf{N}E_K}.$$

This completes the proof of Proposition 1.7.

To calculate the number of equivalence classes, let h_K and h_k denote the class numbers of K and k. Then

$$\# C_{k,T}^+ = h_k \cdot 2^{n-s} / \#(E_k/E_{k,T}^+).$$

By class-field theory, the cokernel of $\mathbf{N} : C_K \to C_{k,T}^+$ is isomorphic to $\mathrm{Gal}(K/k)$, so has order 2. Hence

$$\#\ker(\mathbf{N} : C_K \to C_{k,T}^+) = 2^{s+1-n} \cdot \#(E_k/E_{k,T}^+) \cdot (h_K/h_k)$$

$$\#\mathrm{coker}(\mathbf{N} : E_K \to E_{k,T}^+) = \#(E_{k,T}^+/\mathbf{N}E_K)$$

and the total cardinality is

$$2^{s+1-n} \cdot \#(E_k/\mathbf{N}E_K) \cdot (h_K/h_k).$$

Since $\#(E_k/E_k^2) = 2^n$ by the unit theorem, this cardinality is also given by the formula:

$$2^{s+1} \cdot h_K / \#(\mathbf{N}E_K : E_k^2) \cdot h_k.$$

2. When is t conjugate to t^{-1}?

To motivate the theory of Coxeter decompositions, we will consider the following problem, in the notation of §1. Let (L, c) be a solution of the ideal equation (1.8), giving us an A_K-even, unimodular lattice. Then $(\overline{L}, c)$ is another solution. When are these two solutions equivalent?

An equivalence is given by an element γ in K^*, with $L = (\gamma)\overline{L}$ and $\gamma\overline{\gamma} = 1$. Writing $\gamma = \overline{\beta}/\beta$ by Hilbert's Theorem 90, and putting $M = (\beta)L = (\overline{\beta})\overline{L}$ and $c_M = c/\beta\overline{\beta}$, we find an A_K-even unimodular lattice (M, c_M) in the same equivalence class with

$$M = \overline{M}. \tag{2.1}$$

Then the map $\alpha \mapsto \overline{\alpha}$ gives an involution σ in $O(M)$, which satisfies

$$\sigma t \sigma^{-1} = t^{-1}. \tag{2.2}$$

Hence t is conjugate to t^{-1} in $O(M)$.

There is a non-trivial condition which is necessary for such lattices to exist. Since $M = \overline{M}$ and the extension K/k is unramified at all finite primes [GM,§3], we have

$$M = M_k \otimes A_K \tag{2.3}$$

with M_k a fractional ideal of k. Similarly,

$$A_K^\vee = A_k^\vee \otimes A_K. \tag{2.4}$$

The ideal equation $M \cdot \overline{M} \cdot (c_M) = A_K^\vee$ in K then yields the ideal equation

$$M_k^2 \cdot (c_M) = A_k^\vee \tag{2.5}$$

in k.

Since $c_M > 0$ at all real places T which ramify in K/k, we deduce from (2.5) that the class of $A_k^\vee$ in $C_{k,T}^+$ is a *square*. This is a nontrivial condition, which is equivalent to the hypothesis that for every quadratic extension of k which is unramified outside of T, the number of real places which ramify is divisible by 4 (cf. [G]). Conversely, if it is satisfied, we let M_k be a solution of (2.5) and $M = M_k \otimes A_K$. Then (M, c_M) gives an even, unimodular A_K-lattice, and t is conjugate to t^{-1} in $O(M)$.

The theory of Coxeter decompositions will give this conjugacy, and a bit more. We digress for a section, to review the general theory of Coxeter groups.

3. The Coxeter element (cf. [B, Ch. IV])

Let (W, S) be a Coxeter group, with finite set S of generating reflections s. For $s \neq s'$ in S, let $m(s, s') = 2, 3, \ldots, \infty$ be the order of the product ss' in W. Since $s's = (ss')^{-1}$, we have $m(s, s') = m(s', s)$. We let V be the real vector space with basis e_s indexed by S, and define a symmetric, bilinear form on V by:

$$\begin{aligned} \langle e_s, e_s \rangle &= 2 \\ \langle e_s, e_{s'} \rangle &= -2 \cos \frac{\pi}{m(s, s')} \qquad s \neq s'. \end{aligned}$$

Then $-2 \leq \langle e_s, e_{s'} \rangle \leq 0$, whenever $s \neq s'$. The group W acts faithfully on V, preserving the bilinear form, via the reflections $sv = v - \langle v, e_s \rangle \cdot e_s$.

The Coxeter graph of (W, S) has vertices indexed by the elements of S. Two vertices are connected by an edge if $\langle e_s, e_{s'} \rangle < 0$, in which case the edge is labelled by the integer $m(s, s') \geq 3$. When the Coxeter graph is a tree, the element

$$t = \prod_S s \tag{3.1}$$

is well-defined up to conjugacy in W, independent of the order of the product. This is the Coxeter conjugacy class. Let $f(x)$ be its characteristic polynomial. Since $\langle tv, tw \rangle = \langle v, w \rangle$ and $\det(t/V) = (-1)^{\#S} = (-1)^{\dim V}$, the polynomial $f(x)$ is reciprocal: $f(x) = x^{\dim V} \cdot f(1/x)$.

More generally, when the Coxeter graph is bipartite, with opposing sets of vertices S_1 and S_2, we define the following elements in W:

$$\begin{cases} \sigma_1 = \prod_{S_1} s \\ \sigma_2 = \prod_{S_2} s \\ t = \sigma_1 \sigma_2 \end{cases} \tag{3.2}$$

Since σ_1 and σ_2 are products of *commuting* simple reflections, they have order 2 in W, and

$$t^{-1} = \sigma_2 \sigma_1 = \sigma_2 t \sigma_2^{-1} = \sigma_1 t \sigma_1^{-1}. \tag{3.3}$$

Let V_1 and V_2 be the -1 eigenspaces of σ_1 and σ_2 on V. Each V_i is a Euclidean space, with basis the orthogonal roots e_s, $s \in S_i$, and $V = V_1 + V_2$ as a real vector space (although the direct sum is not orthogonal). Both t and t^{-1} represent the Coxeter class, when that class is well-defined.

Proposition 3.4. *In the bipartite case, the complex roots of the characteristic polynomial $f(x)$ of $t = \sigma_1\sigma_2$ lie on the union of the unit circle and the positive real line.*

The bilinear form on V is non-degenerate if and only if $f(1) \neq 0$. In this case, V has signature $(n - s, s)$, where $n = \dim\ V$ and s is the number of real roots λ of $f(x)$ with $\lambda > 1$.

This result is due to A'Campo [A] and Berman-Lee-Moody [B-L-M]. We sketch the argument. The Gram matrix of the bilinear form $\langle , \rangle$ on $V = V_1 + V_2$, with respect to the basis of simple roots, is

$$A = \begin{pmatrix} 2I & B \\ {}^tB & 2I \end{pmatrix}.$$

Similarly, the involutions σ_1 and σ_2 have matrices

$$\sigma_1 = \begin{pmatrix} -I & -B \\ 0 & I \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} I & 0 \\ -{}^tB & -I \end{pmatrix}$$

with respect to the root bases. Hence

$$\sigma_1 + \sigma_2 = \begin{pmatrix} 0 & -B \\ -{}^tB & 0 \end{pmatrix}.$$

The latter operator is self-adjoint, with respect to the inner product on V where the basic roots have length 2 and are all orthogonal. Hence its eigenvalues κ are all real numbers. They are stable under the involution $\kappa \mapsto -\kappa$, for if $v = v_1 + v_2$ is an eigenvector with eigenvalue $\kappa \neq 0$, then v_1 and v_2 are nonzero, and $v' = v_1 - v_2$ has eigenvalue $-\kappa$.

We have the identity

$$(\sigma_1 + \sigma_2)^2 = 2 + t + t^{-1} \qquad \text{in} \quad \mathrm{End}(V).$$

Hence the eigenvalues of $2 + t + t^{-1}$ are nonnegative real numbers, and the eigenvalues λ of t satisfy $\lambda + \lambda^{-1} \geq -2$. This implies that they lie on the union of the unit circle and the positive real line.

The eigenvalues μ of the matrix

$$A = 2I - (\sigma_1 + \sigma_2)$$

are of the form $\mu = 2 - \kappa$, so are stable under the involution $\mu \mapsto 4 - \mu$. The bilinear form is degenerate if $\mu = 0$ occurs as an eigenvalue of A, so $\kappa = 2$ occurs as an eigenvalue of $\sigma_1 + \sigma_2$, so $\kappa^2 = 4$ occurs as an eigenvalue of $t + t^{-1} + 2$. This occurs when $f(1) = 0$. If $f(1) \neq 0$, the number s of negative eigenvalues for A is equal to the number of $\kappa > 2$, so $\kappa^2 > 4$ and $\lambda + \lambda^{-1} > 2$. This is equal to the number s of roots λ of $f(x)$ with $\lambda > 1$.

4. Coxeter decompositions

We now return to the situation in §1. Let L be even, unimodular of signature $(2n-s, s)$, and let $t : L \to L$ be an orthogonal transformation with characteristic polynomial $f(x)$.

A Coxeter decomposition for (L, t) is a decomposition of L as the direct sum of two abelian groups (not necessarily orthogonal)

$$L = L_1 + L_2. \tag{4.1}$$

Both of the sublattices L_1 and L_2 of L are required to be positive-definite, with dual lattices satisfying:

$$2 \cdot L_i^\vee = L_i. \tag{4.2}$$

In other words, the bilinear form $\langle , \rangle$ should take even values on each L_i, and $\frac{1}{2}\langle , \rangle$ should be a unimodular pairing on each L_i.

Let $pr_i : L \to \frac{1}{2}L_i$ be the projection operator, taking λ in L to the unique element λ_i in $\frac{1}{2}L_i$ which satisfies

$$\langle \lambda, m_i \rangle = \langle \lambda_i, m_i \rangle \tag{4.3}$$

for all m_i in L_i. From the projections pr_i, we obtain two involutions in $O(L)$:

$$\begin{cases} \sigma_1(\lambda) = \lambda - 2pr_1(\lambda) \\ \sigma_2(\lambda) = \lambda - 2pr_2(\lambda) \end{cases} \tag{4.4}$$

The -1 eigenspace of σ_i on L is L_i, and the final requirement on the Coxeter decomposition is that

$$t = \sigma_1\sigma_2 \qquad \text{in } O(L). \tag{4.5}$$

Then $t^{-1} = \sigma_2\sigma_1$ is conjugate to t, so we are in the situation of §2 (with the additional hypothesis that the -1 eigenspaces are positive definite).

If we have a Coxeter decomposition $L = L_1 + L_2$, then extending scalars to $\mathbf{R}$, we may choose orthogonal root bases for $V_1 = L_1 \otimes \mathbf{R}$ and $V_2 = L_2 \otimes \mathbf{R}$. In $O(V)$, the involutions are the product of simple reflections, as for a Coxeter group. However, it may not be possible to choose the root bases e_s so that every inner product $\langle e_s, e_{s'} \rangle$ lies in the interval $[-2, 0]$.

We consider two Coxeter decompositions equivalent if there is an isometry $i : L \to L'$ mapping L_1 to L'_1 and L_2 to L'_2. Then $i \circ \sigma_1 = \sigma'_1 \circ i$ and $i \circ \sigma_2 = \sigma'_2 \circ i$, so $i \circ t = t' \circ i$ and the pairs (L, t) and (L', t') are equivalent in the sense of §1.

Proposition 4.5. *There is a Coxeter decomposition $L = L_1 + L_2$, with L an A_K-module and $t = \sigma_1 \sigma_2$ having characteristic polynomial $f(x)$, if and only if $A_k^\vee$ is a square in C_k^+, the strict class group of k.*

If such a Coxeter decomposition exists, the equivalence classes of Coxeter decompositions form a principal homogeneous space for the finite 2-group $k_+^{*(2)}/k^{*^2}$, where $k_+^{*(2)}$ is the subgroup of k^* consisting of totally positive α with $(\alpha) = I^2$, as ideals of k.

5. A proof of Proposition 4.5

Before giving the proof, we identify some units of A_K. Since $f(x)$ is unramified and reciprocal, we have

$$
\begin{aligned}
f(0) &= 1 \\
f(-1) &= 1 \\
f(1) &= (-1)^n.
\end{aligned}
$$

Lemma 5.1. *The elements x, $\delta = (x - x^{-1})$, $\gamma = (1 + x^{-1})$, and $\mu = (1 - x^{-1})$ are all units of A_K. They satisfy:*

$$
\begin{aligned}
\overline{\delta}/\delta &= -1 \\
\overline{\gamma}/\gamma &= x \\
\overline{\mu}/\mu &= -x \\
\delta &= x\gamma\mu.
\end{aligned}
$$

If $y = x + x^{-1}$ in k, then

$$\gamma + \overline{\gamma} = \gamma\overline{\gamma} = y + 2$$

is a totally positive unit, and the units

$$\epsilon = \delta\overline{\delta} = 4 - y^2$$

$$\mu\overline{\mu} = 2 - y$$

are positive at T, and negative at the real places which split in K/k.

Proof. This follows from: $\mathbf{N}(\gamma) = f(-1)$ and $\mathbf{N}(\mu) = f(1)$, and the fact that $f(x)$ is unramified.

Now assume that A_K–module L has a Coxeter decomposition $L = L_1 + L_2$, with $\sigma_1\sigma_2 = t$. The bilinear form on L has the form $\langle \alpha, \beta \rangle = \mathrm{Tr}(c\alpha\overline{\beta})$, with $c > 0$ at the places in T, and $L \cdot \overline{L} \cdot (c) = A_K^\vee$.

View $V = L \otimes \mathbf{Q} = K$ as a $k = \mathbf{Q}(t + t^{-1})$ module of rank 2, with bilinear form $\{\alpha, \beta\} = c(\alpha\overline{\beta} + \beta\overline{\alpha})$. Since $t + t^{-1} = (\sigma_1 + \sigma_2)^2 - 2$ preserves the spaces $V_1 = L_1 \otimes \mathbf{Q}$ and $V_2 = L_2 \otimes \mathbf{Q}$, they are both k-modules of rank 1. Moreover, the involutions σ_1 and σ_2 commute with $t + t^{-1}$, so give reflections in $O(V/k) = O(K/k)$, with -1 eigenspaces V_1 and V_2.

All reflections in $O(K/k)$ have the form $\sigma(\alpha) = e \cdot \overline{\alpha}$ with e in K^* satisfying $e\overline{e} = 1$. Write $e = \overline{\beta}/\beta$ by Hilbert's theorem 90. Then the -1 eigenspace for σ is positive definite if and only if $d = \epsilon c/\beta\overline{\beta}$ is totally positive in k. Recall that the unit $\epsilon = \delta\overline{\delta}$ is positive precisely at the places in T.

But $\sigma = \sigma_1$ stabilizes L, so $L = (e)\overline{L} = (\overline{\beta}/\beta)\overline{L}$. Then $M = (\beta)L$ is stable under conjugation in K. The pair (M, d) satisfies the ideal equation

$$M \cdot \overline{M} \cdot (d) = A_K^\vee$$

in K, so the underlying ideal M_k of k satisfies

$$M_k^2 \cdot (d) = A_k^\vee. \tag{5.2}$$

Hence $A_k^\vee$ is a square in the strict class group.

Conversely, assume we have a solution to (5.2) with $d > 0$, and put $M = M_k \otimes A_K$ and $c = d/\epsilon$. Then (M, c) gives an even, unimodular A_K-lattice of signature $(2n - s, s)$. Let

$$\sigma_1(\alpha) = \overline{\alpha} \qquad \text{in } O(M) \tag{5.3}$$

$$\sigma_2 = \sigma_1 t. \tag{5.4}$$

Then $\sigma_2(\alpha) = x^{-1}\overline{\alpha}$ is also in involution of M. We claim σ_1 and σ_2 give rise to a Coxeter decomposition.

To verify this, we let L_1 and L_2 be the -1 eigenspace of σ_1 and σ_2. We find

$$L_1 = M_k \cdot \delta \qquad \text{with } \langle m\delta, m'\delta \rangle = 2\mathrm{Tr}(dmm')$$

$$L_2 = M_k \cdot \mu \qquad \text{with } \langle m\mu, m'\mu \rangle = 2\mathrm{Tr}(d^* mm')$$

Both $d = c\epsilon$ and $d^* = c\mu\overline{\mu}$ are totally positive, so L_1 and L_2 are positive definite. Since

$$(M_k)^2(d) = (M_k)^2(d^*) = A_k^\vee,$$

they have dual lattices $\frac{1}{2}L_1$ and $\frac{1}{2}L_2$, respectively. Finally, $L_1 + L_2$ is an $A_k[x] = A_K$-submodule of L containing $M_k = L_1 \cdot \delta^{-1}$. It must then equal $L = A_K \otimes M_k$.

The above argument shows that the Coxeter decompositions correspond to pairs (M_k, d) with $d > 0$ and $M_k^2 \cdot (d) = A_k^\vee$. The group $k_+^{*(2)}$ acts simply-transitively on these pairs: if $(\alpha) = I^2$ then

$$\alpha(M_k, d) = (M_k \cdot I, d/\alpha).$$

The subgroup k^{*^2} preserves the equivalence classes: if $\alpha = \gamma^2$, then multiplication by γ gives an isometry from M_k to $M_k(\gamma)$, preserving the Coxeter decomposition. Hence the equivalence classes form a principal homogeneous space for $k_+^{*(2)}/k^{*^2}$.

6. Euclidean lattices

Some interesting invariants of a Coxeter decomposition are the classes of the unimodular, A_k-Euclidean lattices L_1 and L_2. Such lattices are given by pairs (M_k, d) satisfying (5.2), with form $\langle m, m' \rangle = \mathrm{Tr}(dmm')$. The group $k_+^{*(2)}/k^{*^2}$ permutes these classes simply-transitively.

Proposition 6.1. *The lattice L_2 is the translate of L_1 by the element $\gamma\overline{\gamma} = y + 2$ in E_k^+/E_k^2.*

This is clear, as both L_1 and L_2 are based on the same ideal M_k, and $d_2 = \gamma\overline{\gamma} d_1$.

Proposition 6.2. *The restriction of the operator $2pr_1 : L \to L_1$ to the subgroup L_2 is given by multiplication by the unit $(1+x)$ on L. It gives an isomorphism of abelian groups $L_2 \to L_1$.*

Proof. Since $L_2 = M_k \cdot \mu$, we have

$$\begin{aligned}(1+x)L_2 &= M_k(1+x)(1-x^{-1}) \\ &= M_k(x - x^{-1}) \\ &= M_k \cdot \delta = L_1.\end{aligned}$$

To see that this map is $2pr_1$, let $\lambda_1 = m\delta$ be in L_1 and $\lambda_2 = m'\mu$ be in L_2. Then

$$\begin{aligned}\langle \lambda_1, (1+x)\lambda_2 \rangle &= \mathrm{Tr}(c \cdot m\delta \cdot \overline{(1+x)m'\mu}) \\ &= \mathrm{Tr}(cm\delta m'\overline{\delta}) \\ &= \mathrm{Tr}(c\epsilon mm') \qquad \epsilon = \delta\overline{\delta}\end{aligned}$$

Since $\frac{1}{\gamma} + \frac{1}{\overline{\gamma}} = \frac{\gamma+\overline{\gamma}}{\gamma\overline{\gamma}} = 1$, we have

$$\begin{aligned}\mathrm{Tr}(c\epsilon mm') &= 2\mathrm{Tr}\left(c\epsilon mm' \cdot \frac{1}{\gamma}\right) \\ &= 2\mathrm{Tr}(c \cdot m\delta \cdot m'\overline{\mu}) \qquad \epsilon = \delta\gamma\overline{\mu}\end{aligned}$$

Hence $\langle \lambda_1, (1+x)\lambda_2 \rangle = 2\langle \lambda_1, \lambda_2 \rangle$.

7. On the group $(k_+^{*(2)}/k^{*^2})$

Let $C_{k,+} \to C_k$ be the usual surjection, and let $D_k[2]$ be the image of the 2-torsion subgroup $C_{k,+}[2]$ in C_k. Then we have an exact sequence

$$1 \to E_k^+/E_k^2 \to k_+^{*(2)}/k^{*^2} \xrightarrow{g} D_k[2] \to 1 \tag{7.1}$$

where $g(\alpha)$ is the class of the ideal I in C_k, $I^2 = (\alpha)$. If $g(\alpha) = 1$, then $(\alpha) = (\beta^2)$ and $\epsilon = \alpha/\beta^2$ is totally positive in E_k.

Since the kernel of the map

$$C_{k,+}[2] \to C_k$$

has order $2^n/\#(E_k/E_k^+)$, we find

$$\#D_k[2] = \#C_{k,+}[2] \cdot \#(E_k/E_k^+)/2^n$$

$$\#(k_+^{*(2)}/k^{*^2}) = \#C_{k,+}[2] \cdot \#(E_k/E_k^2)/2^n.$$

But $(E_k/E_k^2) \simeq (\mathbf{Z}/2)^n$ by the unit theorem, so we have:

Proposition 7.2. *The group $k_+^{*(2)}/k^{*^2}$ is isomorphic, as a finite 2-group, to $C_{k,+}/2C_{k,+}$.*

Indeed, both are killed by 2 and have the same order as $C_{k,+}[2]$.

Here is a useful criterion for the existence of a "unique" Coxeter decomposition for $f(x)$.

Proposition 7.3. *The following two conditions are equivalent:*

a) The strict class number h_K^+ of K is odd.

b) The strict class number h_k^+ of k is congruent to 2 (mod 4).

When a) and b) are satisfied, the class of $A_k^\vee$ is a square in C_k^+, and a Coxeter decomposition $L = L_1 + L_2$ with characteristic polynomial $f(x)$ exists and is unique, up to a permutation of the Euclidean lattices L_1 and L_2.

Proof. Class-field theory (cf. [GM, §5]) gives an exact sequence

$$C_K^+ \underset{\mathbf{N}}{\to} C_k^+ \to \mathrm{Gal}(K/k) \to 1.$$

Hence, if h_K^+ is odd, $h_k^+ \equiv 2 \pmod 4$.

If conversely $h_k^+ \equiv 2 \pmod 4$, then K is the unique quadratic extension of k ramified only at infinity. Since $\mathrm{Ram}(K/k) = T$ has cardinality divisible by 4, $A_k^\vee$ is a square in C_k^+. If C_K^+ had even order, then the $\mathrm{Gal}(K/k)$-invariants in $C_K^+/2C_K^+$ would be nontrivial. Hence there would be a quadratic extension L of K, ramified only at infinity, with L Galois over k. Since $\mathrm{Gal}(L/k)$ has order 4, it would be abelian, and by class field theory this would imply that $h_k^+ \equiv 0 \pmod 4$. This contradiction shows that h_K^+ is odd.

When a) and b) hold, the group

$$k_+^{*(2)}/k^{*^2} = E_k^+/E_k^2$$

has order 2, and is represented by the positive unit $\gamma\overline{\gamma} = y + 2$. This gives the unicity of the Coxeter decomposition, up to permutation of the factors.

Note 7.4. When $s \leq 1$, conditions a) and b) of Proposition 7.3 are equivalent to the simpler assertion that the class number h_K of K is odd. Indeed,

when $s = 0$, K is totally complex and $C_K^+ = C_K$,

when $s = 1$, K has two real places, and there is an exact sequence

$$\langle \pm 1 \rangle^2 / (\text{signs of } E_K) \to C_K^+ \to C_K \to 1.$$

Since the units $\langle 1, -1, x - x^{-1}, x^{-1} - x \rangle$ exhaust the possible signs at real places, we again find that $C_K^+ = C_K$.

8. Examples

We end with six examples, to illustrate various aspects of Coxeter decompositions. We will consider three cyclotomic polynomials, where $s = 0$, and three Salem polynomials, where $s = 1$.

The three cyclotomic examples are the polynomials satisfied by the primitive 30-th, 24-th, and 84-th roots of 1. They are:

$$f_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$$

$$f_{24}(x) = x^8 - x^4 + 1$$

$$f_{84}(x) = x^{24} + x^{22} - x^{18} - x^{16} + x^{12} - x^8 - x^6 + x^2 + 1.$$

In all cyclotomic cases, $\mathbf{Z}[x]/f(x)$ is the full ring A_K of integers of K. In these three cases $h_K = 1$. So in each case, there is a unique Coxeter decomposition

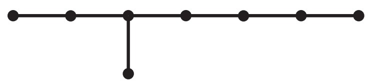
$$L = L_1 + L_2$$

with L even, unimodular of rank $2n = 8, 8$, and 24, and the sublattices L_i scaled unimodular lattices of rank $n = 4, 4$, and 12.

For $f_{30}(x)$ and $f_{24}(x)$, the even unimodular lattice L must be the E_8-lattice, and the scaled unimodular sublattices L_i must be $\mathbf{Z}^4$. In the first case, one can choose root bases for the L_i with inner products

$$B = \begin{pmatrix} -1 & 0 & 0 & 0 \\ -1 & -1 & -1 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

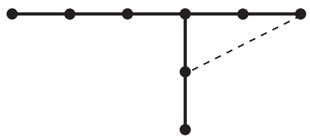
The associated 8 simple reflections of L generate the Weyl group of E_8, with Coxeter diagram:



and t is the Coxeter element (of order 30) in this finite Coxeter group. In the second case, one can choose root bases of the L_i with inner product matrix

$$B = \begin{pmatrix} -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & -1 \\ 0 & -1 & -1 & +1 \end{pmatrix}.$$

The associated diagram looks like this:



where the dotted edge indicates that $\langle e_s, e_{s'} \rangle = 1$. Here t has order 24; it lies in the Coxeter group of type E_8, but is *not* the Coxeter element.

In the final case, L is the Leech lattice, which is the only even unimodular lattice of rank 24, having an automorphism of order 84. The sublattices L_i are scaled D_{12}^+ lattices.

The three Salem polynomials we will consider, and their unique roots $\lambda > 1$, are:

$$f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

$$\lambda = 1.17628...$$

$$f(x) = x^{10} - x^6 - x^5 - x^4 + 1$$

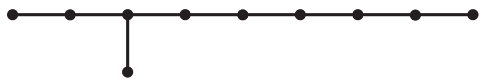
$$\lambda = 1.21639...$$

$$f(x) = x^{18} - x^{17} + x^{16} - x^{15} - x^{12} + x^{11} - x^{10} + x^9 - x^8 + x^7 - x^6 - x^3 + x^2 - x + 1$$

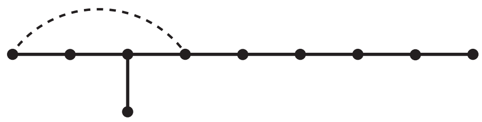
$$\lambda = 1.18837...$$

In all three cases, $A_K = \mathbf{Z}[x]/f(x)$ and $h_K = 1$. The Coxeter decomposition $L = L_1 + L_2$ is unique. In the first two cases $L = \mathrm{II}_{9,1}$, and in the third, $L = \mathrm{II}_{17,1}$.

In the first case, $L_1 = L_2 = \mathbf{Z}^5$ and the matrix of inner products has diagram



In this case, t is the Coxeter element in the hyperbolic Coxeter group E_{10}. In the second case, $L_1 = L_2 = \mathbf{Z}^5$ and the matrix of inner products has diagram



Here t lies in the Coxeter group E_{10}, but is *not* the Coxeter element.

In the last case, $L_1 = \mathbf{Z}^9$ but $L_2 = \mathbf{Z} + E_8$. In this case one can show, t does *not* lie in the subgroup of $O(\mathbb{I}_{17,1})$ generated by reflections in the root vectors [M, Cor 7.11].

9. Bibliography

[A] A'Campo, N. Sur les valeurs propres de la transformation de Coxeter. Invent. math. 33 (1976), 61–67.

[B] Bourbaki, N. Groupes et algèbres de Lie. Masson, 1981.

[B-L-M] Berman, S., Lee, Y.S., and Moody, R.V. The spectrum of a Coxeter transformation, affine Coxeter transformations, and the defect map. J. Algebra 121 (1989), 339–357.

[G] Gross, B.H. Some remarks on signs in functional equations. Preprint (2001).

[G-M] Gross, B.H. and McMullen, C.T. Automorphisms of even unimodular lattices and unramified Salem numbers. Preprint (2001).

[M] McMullen, C.T. Coxeter groups, Salem numbers, and the Hilbert metric. Preprint (2001).