Diss. ETH No. 13506

Symplectic characteristic classes and the Farrell cohomology of $\mathrm{Sp}(p-1,\mathbb{Z})$

A dissertation submitted to the

SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of

DOCTOR OF MATHEMATICS

presented by

CORNELIA MINETTE BUSCH

Dipl. Math. ETH
born November 13, 1968
citizen of Germany

accepted on the recommendation of

Prof. Dr. Guido Mislin, examiner
Prof. Dr. Urs Stammbach, co-examiner

2000

Meinen Eltern

Contents

Abstract

This thesis contains two main results. The first one is a new proof of the fact that the universal symplectic classes $d_j(\mathbb{Z}) \in \mathrm{H}^{2j}(\mathrm{Sp}(\mathbb{Z}), \mathbb{Z})$ have infinite order (Theorem 3.3). This proof uses only techniques from group cohomology. The second result is that for odd primes p with odd relative class number h^- the p-period of the Farrell cohomology of $\mathrm{Sp}(p-1, \mathbb{Z})$ is $2y$ where y is an odd integer with $p - 1 = 2^r y$ (Theorem 4.6). In order to prove these two results, the conjugacy classes of elements and subgroups of odd prime order p in $\mathrm{Sp}(p-1, \mathbb{Z})$ are studied. In particular, we determine the representations $\mathbb{Z}/p\mathbb{Z} \to \mathrm{U}((p-1)/2)$ whose associated representation $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1, \mathbb{R})$ factors, up to conjugation, through a representation $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1, \mathbb{Z})$. We also compute the p-primary component of the Farrell cohomology of $\mathrm{Sp}(p-1, \mathbb{Z})$ for small primes p with $h^- = 1$.

Zusammenfassung

Diese Arbeit enthält zwei Hauptresultate. Das erste Resultat (Theorem 3.3) ist ein neuer Beweis der Tatsache, daß die universellen symplektischen Klassen $d_j(\mathbb{Z}) \in \mathrm{H}^{2j}(\mathrm{Sp}(\mathbb{Z}), \mathbb{Z})$ unendliche Ordnung haben. In diesem Beweis werden nur Methoden aus der Gruppenkohomologie gebraucht. Das zweite Resultat (Theorem 4.6) besagt, daß für ungerade Primzahlen p, deren relative Klassenzahl h^- ungerade ist, die p-Periode der Farrell-Kohomologie von $\mathrm{Sp}(p-1, \mathbb{Z})$ gleich $2y$ ist, wobei y eine ungerade ganze Zahl ist mit $p - 1 = 2^r y$. Um diese beiden Resultate zu beweisen, werden die Konjugationsklassen von Elementen und Untergruppen der Ordnung p in $\mathrm{Sp}(p-1, \mathbb{Z})$ untersucht. Insbesondere werden die Darstellungen $\mathbb{Z}/p\mathbb{Z} \to \mathrm{U}((p-1)/2)$ bestimmt, deren induzierte Darstellung $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1, \mathbb{R})$ bis auf Konjugation durch eine Darstellung $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1, \mathbb{Z})$ faktorisiert. Für kleine Primzahlen p mit $h^- = 1$ werden wir auch den p-primären Teil der Farrell-Kohomologie von $\mathrm{Sp}(p-1, \mathbb{Z})$ berechnen.

Danksagung

Für das interessante Thema dieser Dissertation und die hervorragende Betreuung danke ich Herrn Prof. Dr. Guido Mislin von ganzem Herzen. Sein Verständnis, sein Rat und seine Ruhe, welche er mir auch in den schwierigen Momenten vermittelte, haben wesentlich zum Erfolg beigetragen.

Herrn Prof. Dr. Urs Stammbach danke ich dafür, daß er so bereitwillig das Korreferat übernommen hat.

Mit vielen Ratschlägen und Freundlichkeiten haben mir meine Kollegen das Leben während der Arbeit erleichtert.

Es ist ein ganz besonderes Glück, wenn man so liebe Eltern hat, wie ich sie habe. Es war sicher nicht immer leicht für sie, mir die Unterstützung zu geben, die so kostbar für mich war.

Introduction

Let $\mathrm{U}(n)$ be the group of unitary $n\times n$-matrices and let $\mathrm{Sp}(2n,\mathbb{R})$ denote the group of symplectic $2n\times 2n$-matrices. We will define a homomorphism

$$\phi : \mathrm{U}(n) \longrightarrow \mathrm{Sp}(2n,\mathbb{R})$$

such that the induced homomorphism

$$\phi^* : \mathrm{H}^*(B\mathrm{Sp}(2n,\mathbb{R}),\mathbb{Z}) \xrightarrow{\cong} \mathrm{H}^*(B\mathrm{U}(n),\mathbb{Z})$$

is an isomorphism that maps the symplectic class $d_j \in \mathrm{H}^{2j}(B\mathrm{Sp}(2n,\mathbb{R}),\mathbb{Z})$ to the universal Chern class $c_j \in \mathrm{H}^{2j}(B\mathrm{U}(n),\mathbb{Z})$, $j = 1,\dots,n$. The map ϕ identifies $\mathrm{U}(n)$ with a maximal compact subgroup of $\mathrm{Sp}(2n,\mathbb{R})$. Bürgisser proved in his paper [5] that elements of odd prime order p exist in $\mathrm{Sp}(2n,\mathbb{Z})$, the group of symplectic $2n\times 2n$-matrices over $\mathbb{Z}$, if and only if $2n \geqslant p-1$. Therefore a faithful representation $\rho : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1,\mathbb{Z})$ exists. We can consider any representation $\widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{U}((p-1)/2)$ as a representation $\phi \circ \widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1,\mathbb{R})$. We will determine the properties $\widetilde{\rho}$ has to fulfil to factor up to conjugation through a representation $\rho : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1,\mathbb{Z})$. This problem is equivalent to the question for which matrices $X \in \mathrm{U}((p-1)/2)$ of odd prime order p the image $\phi(X) \in \mathrm{Sp}(p-1,\mathbb{R})$ is conjugate to some $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$. At this point arithmetical problems appear, which are related to the theory of cyclotomic fields. The answer to the question is given by the following theorem.

Theorem 2.9. *Let $X \in \mathrm{U}((p-1)/2)$ be of odd prime order p. Then the image $\phi(X) \in \mathrm{Sp}(p-1,\mathbb{R})$ of X is conjugate to $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ if and only if the eigenvalues $\lambda_1,\dots,\lambda_{(p-1)/2}$ of X are such that*

$$\{\lambda_1,\dots,\lambda_{(p-1)/2},\overline{\lambda}_1,\dots,\overline{\lambda}_{(p-1)/2}\}$$

is a complete set of primitive pth roots of unity.

The number of conjugacy classes of $X \in \mathrm{U}((p-1)/2)$ that satisfy this condition equals $2^{(p-1)/2}$. We will show the following result.

Theorem 3.2. *Let p be an odd prime. Then for any $n = 1, \ldots, (p-1)/2$ a representation $\widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{U}((p-1)/2)$ can be chosen such that the nth Chern class $c_n(\widetilde{\rho})$ is not zero and the representation $\phi \circ \widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1, \mathbb{R})$ factors, up to conjugation, through a representation $\rho : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1, \mathbb{Z})$.*

We will obtain a relation between the symplectic classes $d_j(\rho)$ and the Chern classes $c_j(\widetilde{\rho})$. This will allow us to use our previous result (Theorem 3.2) in order to show the following theorem.

Theorem 3.3. *The universal symplectic classes $d_j(\mathbb{Z}) \in \mathrm{H}^{2j}(\mathrm{Sp}(\mathbb{Z}), \mathbb{Z})$, $j \geqslant 1$, have infinite order.*

For the p-primary component of the Farrell cohomology of $\mathrm{Sp}(p-1, \mathbb{Z})$, the following holds:

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(p-1, \mathbb{Z}), \mathbb{Z})_{(p)} \cong \prod_{P \in \mathfrak{P}} \widehat{\mathrm{H}}^*(N(P), \mathbb{Z})_{(p)}$$

where $\mathfrak{P}$ is a set of representatives for the conjugacy classes of subgroups of $\mathrm{Sp}(p-1, \mathbb{Z})$ of order p and $N(P)$ denotes the normalizer of $P \in \mathfrak{P}$. Moreover, we have

$$\widehat{\mathrm{H}}^*(N(P), \mathbb{Z})_{(p)} \cong \left(\widehat{\mathrm{H}}^*(C(P), \mathbb{Z})_{(p)}\right)^{N(P)/C(P)}$$

where $C(P)$ is the centralizer of P. In order to make use of these facts, we will have to study the conjugacy classes of elements and subgroups of order p in $\mathrm{Sp}(p-1, \mathbb{Z})$. For those subgroups we will determine the structure of $C(P)$ and of $N(P)/C(P)$. After that we will compute the number of conjugacy classes of those subgroups for which $N(P)/C(P)$ has a given structure. Here again arithmetical questions are involved. In the articles of Sjerve and Yang [10] and Brown [3] is shown that the number of conjugacy classes of elements of order p in $\mathrm{Sp}(p-1, \mathbb{Z})$ is $2^{(p-1)/2}h^-$ where h^- denotes the relative class number of the cyclotomic field $\mathbb{Q}(\xi)$, ξ a primitive pth root of unity. If h^- is odd, each conjugacy class of matrices of order p in $\mathrm{Sp}(p-1, \mathbb{R})$ that lifts to $\mathrm{Sp}(p-1, \mathbb{Z})$ splits into h^- conjugacy classes in $\mathrm{Sp}(p-1, \mathbb{Z})$. We will prove the following concerning the periodicity of the p-primary part of the Farrell cohomology of $\mathrm{Sp}(p-1, \mathbb{Z})$.

Theorem 4.6. *Let p be an odd prime for which h^- is odd and let y be such that $p - 1 = 2^r y$ and y is odd. Then the period of $\widehat{\mathrm{H}}^*(\mathrm{Sp}(p-1, \mathbb{Z}), \mathbb{Z})_{(p)}$ is $2y$.*

Moreover, we will explicitly compute this cohomology for primes p with $h^- = 1$.

Chapter 1

Cyclotomic fields

1.1 Number fields

Let $\mathbb{Q}$ be the field of rational numbers. For an odd prime p let ξ be a root of the polynomial

$$m(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Then ξ is a primitive pth root of unity. The roots of unity form a multiplicative group of order p. We consider the field extension $\mathbb{Q}(\xi)/\mathbb{Q}$. The minimal polynomial of this extension is $m(x)$, and the field $\mathbb{Q}(\xi)$ is a $(p-1)$-dimensional $\mathbb{Q}$-vector space with $\mathbb{Q}$-basis $\xi, \ldots, \xi^{p-1}$. This means that any $x \in \mathbb{Q}(\xi)$ can uniquely be written as

$$x = a_1\xi + \cdots + a_{p-1}\xi^{p-1}$$

with $a_1, \ldots, a_{p-1} \in \mathbb{Q}$. Moreover, $\xi, \ldots, \xi^{p-1}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\xi]$, the ring of integers in $\mathbb{Q}(\xi)$. Furthermore,

$$\xi + \xi^{p-1}, \ldots, \xi^{(p-1)/2} + \xi^{(p+1)/2}$$

is a $\mathbb{Q}$-basis of $\mathbb{Q}(\xi + \overline{\xi})$, the maximal real subfield of $\mathbb{Q}(\xi)$, and a $\mathbb{Z}$-basis of $\mathbb{Z}[\xi + \overline{\xi}]$, the ring of integers of $\mathbb{Q}(\xi + \overline{\xi})$.
The Galois group $\mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$ is the group of the automorphisms of $\mathbb{Q}(\xi)$ that leave $\mathbb{Q}$ fixed. It is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^*$. An automorphism $\gamma_j \in \mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$ is determined by the image of ξ. In order to set the notation, we define for $j = 1, \ldots, p-1$

$$\begin{array}{rccc} \gamma_j : & \mathbb{Q}(\xi) & \longrightarrow & \mathbb{Q}(\xi) \\ & \xi & \longmapsto & \xi^j. \end{array}$$

Definition. Let ξ be a primitive pth root of unity. We define the conjugates of $x \in \mathbb{Q}(\xi)$ to be the images of x under the different elements of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$.

Definition. Let F be an extension of degree n of the field K. The trace and the norm of an element $x \in F$ are defined to be the trace and the determinant of the transformation

$$\begin{array}{rccc} T_x : & F & \longrightarrow & F \\ & \alpha & \longmapsto & x\alpha \end{array}$$

of the K-vector space F:

$$Tr_{F/K}(x) := \mathrm{tr}(T_x), \quad N_{F/K}(x) := \det(T_x).$$

There is another way to define the trace and the norm of an element $x \in F$. In the characteristic polynomial

$$f_x(\lambda) = \det(\lambda I - T_x) = \lambda^n - a_{n-1}\lambda^{n-1} + \cdots + (-1)^n a_0$$

of T_x we find the trace and the norm:

$$a_{n-1} = Tr_{F/K}(x), \quad a_0 = N_{F/K}(x).$$

Since $T_{x+y} = T_x + T_y$ and $T_{xy} = T_x \circ T_y$, we get the homomorphisms

$$Tr_{F/K} : F \longrightarrow K \quad \text{and} \quad N_{F/K} : F^* \longrightarrow K^*.$$

If the extension F/K is separable, we get the following interpretation of the trace and the norm.

Proposition 1.1. *Let F/K be a separable extension of degree n of the field K and let $\sigma_j : F \longrightarrow \overline{K}$, $j = 1, \ldots, n$, be the n different embeddings of F in the algebraic closure $\overline{K}$ of K that let K fixed. Then for $x \in F$*

i) $f_x(\lambda) = \prod_{j=1}^{n} (\lambda - \sigma_j(x))$,

ii) $Tr_{F/K}(x) = \sum_{j=1}^{n} \sigma_j(x)$,

iii) $N_{F/K}(x) = \prod_{j=1}^{n} \sigma_j(x)$.

Proof. The characteristic polynomial $f_x(\lambda)$ of the transformation T_x is a power of the minimal polynomial $m_x(\lambda)$ of x

$$\begin{aligned} f_x(\lambda) &= m_x(\lambda)^d, \\ m_x(\lambda) &= \lambda^l + c_{l-1}\lambda^{l-1} + \cdots + c_0 \end{aligned}$$

where $d = [F : K[x]]$ and $l = [K[x] : K]$. Indeed, $1, x, \ldots, x^{l-1}$ is a K-basis of $K[x]$. If $\alpha_1, \ldots, \alpha_d$ is a basis of F over $K[x]$, then

$$\alpha_1, \alpha_1 x, \ldots, \alpha_1 x^{l-1}; \ldots; \alpha_d, \alpha_d x, \ldots, \alpha_d x^{l-1}$$

is a K-basis of F. The matrix of the linear transformation $T_x : y \longmapsto xy$ in this basis has matrices on the diagonal and zeros in the other entries. The matrices on the diagonal are all equal to

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{l-1} \end{pmatrix}.$$

We can easily check that the characteristic polynomial of this matrix is

$$m_x(\lambda) = \lambda^l + c_{l-1}\lambda^{l-1} + \cdots + c_0,$$

and so the matrix of T_x has the characteristic polynomial $f_x(\lambda) = m_x(\lambda)^d$. The relation

$$\sigma \sim \tau \ \Leftrightarrow \ \sigma(x) = \tau(x)$$

defines an equivalence relation, which splits $\mathrm{Mor}_K(F, \overline{K})$ into l equivalence classes of cardinality d. Let $\sigma_1, \ldots, \sigma_l$ be a set of representatives. Then

$$m_x(\lambda) = \prod_{j=1}^{l} (\lambda - \sigma_j(x))$$

and

$$f_x(\lambda) = \prod_{j=1}^{l} (\lambda - \sigma_j(x))^d = \prod_{j=1}^{l} \prod_{\sigma \sim \sigma_j} (\lambda - \sigma(x)) = \prod_{\sigma} (\lambda - \sigma(x)).$$

This proves the first assertion and the second and third assertion follow immediately. □

We will mainly apply Proposition 1.1 to compute the norm of an $x \in \mathbb{Q}(\xi)$ over $\mathbb{Q}$. The trace and the norm of $x \in \mathbb{Q}(\xi)$ are the sum and the product of its conjugates.

1.2 The ring of integers

Definition. Let F be a finite extension of the field $\mathbb{Q}$ of rational numbers. An element of F is called an algebraic integer if it is the root of a monic polynomial

$$x^k + a_{k-1}x^{k-1} + \cdots + a_0$$

with coefficients $a_i \in \mathbb{Z}$, $i = 0, \ldots, k-1$.

Proposition 1.2. *Let p be an odd prime. Then, for a primitive pth root of unity ξ, the ring of algebraic integers in $\mathbb{Q}(\xi)$ is $\mathbb{Z}[\xi]$.*

Proof. See Washington [11]. □

We take any embedding of $\mathbb{Q}(\xi)$ into the complex numbers. Complex conjugation acts as an automorphism sending ξ to $\overline{\xi}$. The maximal real subfield of $\mathbb{Q}(\xi)$ is the fixed field under complex conjugation. It is $\mathbb{Q}(\xi + \overline{\xi}) = \mathbb{Q}(\xi) \cap \mathbb{R}$. The field $\mathbb{Q}(\xi + \overline{\xi})$ has $(p-1)/2$ real embeddings and no complex embeddings into $\mathbb{C}$. On the other hand $\mathbb{Q}(\xi)$ has no real embeddings and $(p-1)/2$ pairs of complex embeddings.

Proposition 1.3. *Let p be an odd prime. Then for a primitive pth root of unity ξ the ring of algebraic integers in $\mathbb{Q}(\xi + \overline{\xi})$ is $\mathbb{Z}[\xi + \overline{\xi}]$.*

Proof. See Washington [11]. □

Proposition 1.4. *Let p be an odd prime and ξ a primitive pth root of unity. Let ε be a unit of $\mathbb{Z}[\xi]$. Then $\varepsilon_1 \in \mathbb{Q}(\xi + \overline{\xi})$ and $r \in \mathbb{Z}$ exist such that $\varepsilon = \xi^r \varepsilon_1$. It is even possible to choose $\varepsilon_1 \in \mathbb{Z}[\xi + \overline{\xi}]$.*

Lemma 1.5. *Let F be a number field. If $\alpha \in F$ is an algebraic integer all of whose conjugates have norm 1, then α is a root of unity.*

Proof of Lemma 1.5. Let $p_\alpha(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ with α as a zero. The other zeros of $p_\alpha(x)$ are conjugates of α. We set

$$p_\alpha(x) = a_k x^k + \cdots + a_1 x + a_0.$$

Then a_j, $j = 0, \ldots, k$, is a sum of $\binom{k}{j}$ products of conjugates of α and so we know that

$$|a_j| \leqslant \binom{k}{j} \cdot 1.$$

This shows that the coefficients are bounded and the bounds depend only on the degree of α over $\mathbb{Q}$. It follows that there are only finitely many irreducible polynomials that have a power of α as a root. Therefore there exist only finitely many powers of α. This implies that α is a root of unity. Indeed, if α is not a root of unity, we can find no n that satisfies $\alpha^n = 1$ and all powers of α are different. □

Proof of Proposition 1.4. Let $\alpha = \varepsilon/\overline{\varepsilon}$. Since ε is a unit, $\overline{\varepsilon}$ is a unit and α is an algebraic integer. Each conjugate of α has absolute value 1 because complex conjugation commutes with the elements of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$. It follows from Lemma 1.5 that α is a root of unity. So $\alpha = \varepsilon/\overline{\varepsilon} = \pm\xi^a$ for some $a \in \mathbb{Z}$. The roots of unity in $\mathbb{Q}(\xi)$ are all of this form. First we suppose that $\varepsilon/\overline{\varepsilon} = -\xi^a$. Since $\varepsilon \in \mathbb{Z}[\xi]$, we can write

$$\varepsilon = b_0 + b_1\xi + \cdots + b_{p-2}\xi^{p-2}, \quad \overline{\varepsilon} = b_0 + b_1\xi^{-1} + \cdots + b_{p-2}\xi^2.$$

Then $\varepsilon \equiv \overline{\varepsilon} \equiv b_0 + b_1 + \cdots + b_{p-2} \pmod{1-\xi}$. So we obtain that

$$\overline{\varepsilon} \equiv \varepsilon = -\xi^a\overline{\varepsilon} \equiv -\overline{\varepsilon} \pmod{1-\xi}.$$

Therefore $2\varepsilon \equiv 0 \pmod{1-\xi}$. We know that $2 \notin (1-\xi)$. Because $(1-\xi) \subset \mathbb{Z}[\xi]$ is a prime ideal, $\overline{\varepsilon} \in (1-\xi)$. This is impossible since $\overline{\varepsilon}$ is a unit. Therefore $\varepsilon/\overline{\varepsilon} = +\xi^a$. Let $2r \equiv a \pmod{p}$, and let $\varepsilon_1 = \xi^{-r}\varepsilon$. Then $\varepsilon = \xi^r\varepsilon_1$, and the equation $\xi^{2r} = \varepsilon/\overline{\varepsilon}$ is equivalent to $\xi^{-r}\varepsilon = \xi^r\overline{\varepsilon}$. Herewith we obtain $\varepsilon_1 = \xi^{-r}\varepsilon = \xi^r\overline{\varepsilon} = \overline{\varepsilon}_1$. It now follows that $\overline{\varepsilon}_1 = \varepsilon_1 \in \mathbb{Q}(\xi + \overline{\xi})$. Since $\varepsilon \in \mathbb{Z}[\xi]$, $\xi^{-r} \in \mathbb{Z}[\xi]$ as well as $\xi^{-r}\varepsilon \in \mathbb{Q}(\xi + \overline{\xi})$, it follows that $\xi^{-r}\varepsilon \in \mathbb{Z}[\xi + \overline{\xi}]$. So we have shown the existence of $\varepsilon_1 \in \mathbb{Z}[\xi + \overline{\xi}]$. □

Proposition 1.4 is equivalent to the following proposition.

Proposition 1.6. *Let W be the group of roots of unity in $\mathbb{Q}(\xi)$ where ξ is a primitive pth root of unity for an odd prime p. Then*

$$\big[\mathbb{Z}[\xi], W\,\mathbb{Z}[\xi + \overline{\xi}]\big] = 1.$$

Proof. See Washington [11]. □

Definition. A Dedekind domain is a commutative ring with 1 without zero divisors, such that for any pair of ideals $\mathfrak{a} \subseteq \mathfrak{b}$ there exists an ideal $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Proposition 1.7. *The set $\mathcal{O} = \mathcal{O}(F)$, consisting of all algebraic integers in the number field F, is a Dedekind domain with quotient field F.*

Proof. See Milnor [7]. □

Let $\mathcal{O}$ be the ring of algebraic integers of a number field F. We consider $\mathcal{O}^*$, the group of units in $\mathcal{O}$. In general $\mathcal{O}^*$ is not finite, but it contains the finite group W of roots of unity in F. Let r be the number of real embeddings $\rho : F \to \mathbb{R}$ and s the number of conjugate pairs of complex embeddings $\sigma, \overline{\sigma} : F \to \mathbb{C}$.

Theorem 1.8 (Dirichlet unit theorem). *Let $\mathcal{O}$ be the ring of algebraic integers of a number field F. The group of units $\mathcal{O}^*$ in $\mathcal{O}$ is the direct product of the finite cyclic group W of roots of unity in F and a free abelian group of rank $r+s-1$ where r is the number of real embeddings $\rho : F \to \mathbb{R}$ and s the number of conjugate pairs of complex embeddings $\sigma, \overline{\sigma} : F \to \mathbb{C}$.*

Proof. See Neukirch [9]. □

We already know that for $F = \mathbb{Q}(\xi)$ the number of real embeddings $r = 0$ and the number of conjugate pairs of complex embeddings $s = (p-1)/2$. For $F = \mathbb{Q}(\xi + \overline{\xi})$ we have $r = (p-1)/2$ and $s = 0$. So we can state the following corollary.

Corollary 1.9. *Let C_p be the cyclic group of odd prime order p, and let ξ be a primitive pth root of unity. Then the groups of units in $\mathbb{Z}[\xi]$ and $\mathbb{Z}[\xi+\overline{\xi}]$ are*

$$\mathbb{Z}[\xi]^* \cong \mathbb{Z}^{\frac{p-3}{2}} \times \{\pm 1\} \times C_p,$$
$$\mathbb{Z}[\xi+\overline{\xi}]^* \cong \mathbb{Z}^{\frac{p-3}{2}} \times \{\pm 1\}.$$

1.3 The group of ideal classes and class numbers

Definition. Two nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in the Dedekind domain $\mathcal{O}$ belong to the same ideal class if there exist nonzero elements x and y in $\mathcal{O}$ so that $x\mathfrak{a} = y\mathfrak{b}$.

Proposition 1.10. *The ideal classes of $\mathcal{O}$ form an abelian group under multiplication with the class of principal ideals as identity element.*

Proof. See Neukirch [9]. □

Definition. The group of ideal classes of the Dedekind domain $\mathcal{O}$ is called the ideal class group $\mathcal{C}(\mathcal{O})$ of $\mathcal{O}$.

Let $\mathcal{O}$ be a Dedekind domain and F its quotient field.

Definition. An ideal of F is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of F. It is also called fractional ideal. An integral ideal is an ideal $\mathfrak{a} \subseteq \mathcal{O}$.

Proposition 1.11. *The fractional ideals form an abelian group $\mathcal{J}$. The unity is $\mathcal{O}$ and the inverse of an ideal $\mathfrak{a}$ is $\mathfrak{a}^{-1} = \{x \in F \mid x\mathfrak{a} \subseteq \mathcal{O}\}$.*

Proof. See Neukirch [9]. □

The fractional principal ideals $(a) = a \cdot \mathcal{O}$, $a \in F^*$, form a subgroup of the group of fractional ideals $\mathcal{J}$. We denote this group by $\mathcal{H}$. The factor group $\mathcal{J}/\mathcal{H}$ is naturally isomorphic to the ideal class group $\mathcal{C}(\mathcal{O})$.

Proposition 1.12. *The ideal class group $\mathcal{C}(\mathcal{O}) = \mathcal{J}/\mathcal{H}$ is finite.*

Proof. See Neukirch [9]. □

Definition. The order

$$h := [\mathcal{J} : \mathcal{H}]$$

is called the class number of F.

Let $\mathcal{O}^*$ be the units in $\mathcal{O}$. Then we have an exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow F^* \longrightarrow \mathcal{J} \longrightarrow \mathcal{C}(\mathcal{O}) \longrightarrow 1$$

where the third arrow is given by $a \mapsto (a)$. This is proved in Neukirch [9].

1.4 Cyclotomic units

A number field is called totally real if all its embeddings into $\mathbb{C}$ lie in $\mathbb{R}$ and totally imaginary if none of its embeddings lie in $\mathbb{R}$. A CM-field is a totally imaginary quadratic extension of a totally real number field. All of the fields $\mathbb{Q}(\xi_n)$, where ξ_n is a primitive nth root of unity, are CM-fields.

Theorem 1.13. *Let F be a CM-field, F^+ its maximal real subfield, and let h and h^+ be the respective class numbers. Then h^+ divides h.*

Proof. See Washington [11]. □

Definition. The quotient

$$h^- := \frac{h}{h^+}$$

is called the relative class number.

As before, we denote by ξ a primitive pth root of unity where p is an odd prime. Let V be the multiplicative group of units in $\mathbb{Q}(\xi)$ generated by

$$\{\pm\xi, 1 - \xi^a \mid a = 1, \ldots, p-1\}.$$

Let U be the group of units of $\mathbb{Z}[\xi]$.

Definition. The intersection

$$C = V \cap U \subset \mathbb{Z}[\xi]$$

is called the group of cyclotomic units of $\mathbb{Q}(\xi)$. For $\mathbb{Q}(\xi)^+$ we define the group of cyclotomic units

$$C^+ = U^+ \cap C$$

where U^+ is the group of units of $\mathbb{Z}[\xi + \overline{\xi}]$.

Lemma 1.14. *For $p \neq 2$ the following assertions hold.*

i) The cyclotomic units of $\mathbb{Q}(\xi)^+$ are generated by -1 and the units

$$\zeta_a = \xi^{(1-a)/2} \cdot \frac{1-\xi^a}{1-\xi},$$

$a = 2, \ldots, \frac{p-1}{2}$.

ii) The cyclotomic units of $\mathbb{Q}(\xi)$ are generated by ξ and the cyclotomic units of $\mathbb{Q}(\xi)^+$.

Proof. It is obvious that ζ_a is real. Since $1-\xi^a$ and $1-\xi^{-a}$ differ only by the factor $-\xi^a$, we just need to consider $a = 2, \ldots, (p-1)/2$. We now suppose that

$$\zeta = \pm\xi^d \prod_{a=1}^{(p-1)/2} (1-\xi^a)^{c_a}$$

is a cyclotomic unit of $\mathbb{Q}(\xi)$. The ideals $(1-\xi^a)$, $a = 1, \ldots, (p-1)/2$, are all the same. Indeed, this is true if and only if $(1-\xi^a)/(1-\xi^b) \in \mathbb{Z}[\xi]^*$, $a, b = 1, \ldots, (p-1)/2$. Since $(1-\xi^b)/(1-\xi^a)$ is an inverse of $(1-\xi^a)/(1-\xi^b)$, it remains to show that $(1-\xi^a)/(1-\xi^b) \in \mathbb{Z}[\xi]$, $a, b = 1, \ldots, (p-1)/2$. If $z \in \mathbb{Z}[\xi]$, all its conjugates are in $\mathbb{Z}[\xi]$ and therefore it suffices to verify that $(1-\xi^a)/(1-\xi) \in \mathbb{Z}[\xi]$, $a = 2, \ldots, (p-1)/2$. But

$$(1-\xi^a)/(1-\xi) = (1 + \xi + \cdots + \xi^{a-1}) \in \mathbb{Z}[\xi].$$

Moreover, the ideals $(1-\xi^a)$ contain no units, and therefore $\sum c_a = 0$ because if $\sum c_a > 0$, then $\prod(1-\xi^a)^{c_a}$ is an element of the ideal $(1-\xi)$ and not a unit. If $\sum c_a < 0$, then $\prod(1-\xi^a)^{-c_a}$ is an element of the ideal $(1-\xi)$ and its inverse $\prod(1-\xi^a)^{c_a}$ is not a unit. Now we can write

$$\zeta = \pm\xi^d \prod \left(\frac{1-\xi^a}{1-\xi}\right)^{c_a} = \pm\xi^e \prod_{a \neq 1} \zeta_a^{c_a}$$

where $e = d + \frac{1}{2}\sum c_a(a-1)$. This shows the second assertion. If $\zeta \in \mathbb{Q}(\xi)^+$, then $\pm\xi^d$ must be real since each factor in the above product is real. Hence $\pm\xi^d$ equals ± 1. $\square$

Proposition 1.15. *Let p be an odd prime and ξ a primitive pth root of unity. The cyclotomic units C^+ of $\mathbb{Q}(\xi)^+$ are of finite index in the full unit group $U^+ \subset \mathbb{Z}[\xi + \overline{\xi}]$ and*

$$h^+ = [U^+ : C^+]$$

where h^+ is the class number of $\mathbb{Q}(\xi)^+$.

Proof. See Washington [11]. $\square$

Chapter 2

The symplectic group

2.1 Definition

Definition. Let R be a commutative ring with 1. The general linear group $\mathrm{GL}(n, R)$ is defined to be the multiplicative group of invertible $n \times n$-matrices over R.

Definition. We define the symplectic group $\mathrm{Sp}(2n, R)$ over the ring R to be

$$\mathrm{Sp}(2n, R) := \left\{ Y \in \mathrm{GL}(2n, R) \;\middle|\; Y^{\mathrm{T}} J Y = J \right\}$$

where

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

and I_n is the $n \times n$-identity matrix.

Proposition 2.1. $\mathrm{Sp}(2n, R)$ *is a group.*

Proof. It is clear that $I_{2n} \in \mathrm{Sp}(2n, R)$. If $X, Y \in \mathrm{Sp}(2n, R)$, $XY^{-1} \in \mathrm{Sp}(2n, R)$ because

$$\begin{aligned} (XY^{-1})^{\mathrm{T}} J (XY^{-1}) &= (Y^{-1})^{\mathrm{T}} X^{\mathrm{T}} J X Y^{-1} = (Y^{-1})^{\mathrm{T}} J Y^{-1} \\ &= (Y^{-1})^{\mathrm{T}} Y^{\mathrm{T}} J Y Y^{-1} = (Y Y^{-1})^{\mathrm{T}} J Y Y^{-1} \\ &= J. \end{aligned}$$

Therefore $\mathrm{Sp}(2n, R)$ is a subgroup of $\mathrm{GL}(2n, R)$. $\square$

2.2 Elements of finite order in $\mathrm{Sp}(2n, \mathbb{Z})$

Theorem 2.2. *Let φ be the Euler φ-function. Let $m = \prod_{i=1}^{h} p_i^{a_i} \in \mathbb{N}$, $m \neq 2$, where p_i, $i = 1, \ldots, h$, are primes that satisfy the condition $p_i < p_{i+1}$, and $a_i \geqslant 1$ for $i = 1, \ldots, h$. There exists a matrix $A \in \mathrm{Sp}(2n, \mathbb{Z})$ of order m if and only if*

i) $\sum\limits_{i=2}^{h} \varphi(p_i^{a_i}) \leqslant 2n$, *if* $m \equiv 2 \pmod 4$

ii) $\sum\limits_{i=1}^{h} \varphi(p_i^{a_i}) \leqslant 2n$, *if* $m \not\equiv 2 \pmod 4$.

If $m = 2$, then $A \in \mathrm{Sp}(2n, \mathbb{Z})$ of order 2 exists for each $n > 0$.

Proof. See Bürgisser [5]. □

We consider elements of odd prime order p. Since for the Euler φ-function $\varphi(p) = p - 1$, a matrix $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$ of order p exists.

Proposition 2.3. *The eigenvalues of a matrix $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$ of odd prime order p are the primitive pth roots of unity, hence the zeros of the polynomial*

$$m(x) = x^{p-1} + \cdots + x + 1,$$

and the trace of Y is -1.

Proof. If λ is an eigenvalue of Y, λ^p is an eigenvalue of Y^p and we have $\lambda^p = 1$. Therefore $\lambda = 1$ or $\lambda = \xi$, a primitive pth root of unity. The trace of a matrix in $\mathrm{Sp}(p-1, \mathbb{Z})$ is an integer. Since the trace is the sum of the eigenvalues, these are $\xi^{p-1}, \ldots, \xi$, the $p-1$ different primitive pth roots of unity. We know that

$$\xi^{p-1} + \cdots + \xi = -1.$$

This shows that the trace of Y is -1. □

Now we consider elements of order p^l, with $1 < l \in \mathbb{Z}$. Let $Y \in \mathrm{Sp}(2n, \mathbb{Z})$ be of order p^l. Such a matrix Y exists for n with $\varphi(p^l) \leqslant 2n$. Since in the set $\{1, \ldots, p, \ldots, p^l\}$ $\gcd(k, p^l) \neq 1$ for each pth number k, we obtain $\varphi(p^l) = p^l - p^{l-1}$. Let $Y \in \mathrm{Sp}(p^l - p^{l-1}, \mathbb{Z})$ be of order p^l. The eigenvalues of Y are p^lth roots of unity. It is trivial that a p^{l-1}th root of unity is also a p^lth root of unity. Now we define $\zeta := e^{i2\pi/p^l}$, $\eta := e^{i2\pi/p^{l-1}}$ and consider the set

$$M := \{\zeta^{p^l-1}, \ldots, \zeta\} \setminus \{\eta^{p^{l-1}-1}, \ldots, \eta\}.$$

If $\lambda \in M$, then $\overline{\lambda} \in M$ and $|M| = (p^l - 1) - (p^{l-1} - 1) = \varphi(p^l)$. Moreover, M is the set of eigenvalues of Y. Indeed, since

$$\begin{aligned} x^{p^l} - 1 &= (x-1)(x^{p^l-1} + \cdots + x + 1), \\ x^{p^{l-1}} - 1 &= (x-1)(x^{p^{l-1}-1} + \cdots + x + 1), \end{aligned}$$

we get

$$\begin{aligned} 0 &= \zeta^{p^l-1} + \cdots + \zeta + 1, \\ 0 &= \eta^{p^{l-1}-1} + \cdots + \eta + 1, \end{aligned}$$

which yields

$$\zeta^{p^l-1} + \cdots + \zeta + 1 - \eta^{p^{l-1}-1} - \cdots - \eta - 1 = \sum_{\lambda \in M} \lambda = 0 = \operatorname{tr} Y.$$

Now we consider elements of order m. Let $n \in \mathbb{N}$ be the smallest number such that $Y \in \mathrm{Sp}(2n,\mathbb{Z})$ of order m exists. We consider the case $m \not\equiv 2 \pmod 4$. Then

$$2n = \sum_{i=1}^{h} \varphi(p_i^{a_i})$$

where $m = \prod_{i=1}^h p_i^{a_i}$ with $p_i < p_{i+1}$ and $a_i \geqslant 1$. The eigenvalues of Y are mth roots of unity. From our discussion of the case $m = p^l$, we can conclude that the set of eigenvalues of Y is the set of primitive $p_i^{a_i}$th and $p_i^{a_i-1}$th roots of unity for $i = 1, \ldots, h$. Let $Y_i \in \mathrm{Sp}(p^{a_i} - p^{a_i-1}, \mathbb{Z})$ be an element of order $p_i^{a_i}$. Since the set of eigenvalues of Y is the union of the eigenvalues of the Y_i, we get

$$\operatorname{tr} Y = \sum_{i=1}^{h} \operatorname{tr} Y_i.$$

For $a_i = 1$ we know that $\operatorname{tr} Y_i = -1$ and for $a_i > 1$ we have $\operatorname{tr} Y_i = 0$. So we get

$$\begin{aligned} \operatorname{tr} Y &= -(\text{the number of primes } p \text{ for which } p|m, \text{ but } p^2 \nmid m) \\ &= -\big|\{i \mid a_i = 1\}\big|. \end{aligned}$$

2.3 An embedding of $\mathrm{U}(n)$ in $\mathrm{Sp}(2n,\mathbb{R})$

Let $X \in \mathrm{U}(n)$, i.e. $X \in \mathrm{GL}(n,\mathbb{C})$ and $X^*X = I_n$ where I_n is the $n \times n$-identity matrix. If we separate each entry of X in its real and imaginary part, we can write

$$X = A + iB$$

with $A, B \in M(n, \mathbb{R})$, the ring of real matrices. The condition $X^*X = I_n$ yields

$$\begin{aligned} X^*X &= (A^{\mathrm{T}} - iB^{\mathrm{T}})(A + iB) \\ &= (A^{\mathrm{T}}A + B^{\mathrm{T}}B) + i(A^{\mathrm{T}}B - B^{\mathrm{T}}A) \\ &= I_n. \end{aligned}$$

So we get

$$X = A + iB \in \mathrm{U}(n) \;\Leftrightarrow\; \left\{ \begin{array}{ll} A^{\mathrm{T}}A + B^{\mathrm{T}}B & = I_n \\ A^{\mathrm{T}}B - B^{\mathrm{T}}A & = 0. \end{array} \right.$$

We now define the following map

$$\begin{array}{rccc} \phi : & \mathrm{U}(n) & \longrightarrow & \mathrm{Sp}(2n, \mathbb{R}) \\ & X = A + iB & \longmapsto & \begin{pmatrix} A & B \\ -B & A \end{pmatrix} =: \phi(X). \end{array}$$

We know that $\phi(X) \in \mathrm{Sp}(2n, \mathbb{R})$ if and only if $\phi(X)^{\mathrm{T}}J\phi(X) = J$. This condition becomes

$$\begin{aligned} \phi(X)^{\mathrm{T}}J\phi(X) &= \begin{pmatrix} A^{\mathrm{T}} & -B^{\mathrm{T}} \\ B^{\mathrm{T}} & A^{\mathrm{T}} \end{pmatrix} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \\ &= \begin{pmatrix} -A^{\mathrm{T}}B + B^{\mathrm{T}}A & A^{\mathrm{T}}A + B^{\mathrm{T}}B \\ -B^{\mathrm{T}}B - A^{\mathrm{T}}A & B^{\mathrm{T}}A - A^{\mathrm{T}}B \end{pmatrix} \\ &= J. \end{aligned}$$

This proves that $\phi(A + iB) \in \mathrm{Sp}(2n, \mathbb{R})$ if and only if $X = A + iB \in \mathrm{U}(n)$, hence ϕ is well-defined. Moreover, ϕ maps the identity to the identity and ϕ is a homomorphism. For $X = A + iB$ and $X' = A' + iB'$ a computation shows

$$\begin{array}{l} \phi(X') \cdot \phi(X) = \phi(X'X) \\ (\phi(X))^{-1} = (\phi(X))^{\mathrm{T}} = \phi(X^*) = \phi(X^{-1}). \end{array}$$

We have the following lemma.

Lemma 2.4. *The homomorphism*

$$\phi : \mathrm{U}(n) \longrightarrow \mathrm{Sp}(2n, \mathbb{R}) \cap \mathrm{SO}(2n)$$

is an isomorphism.

Proof. We already know that $(\phi(X))^{-1} = (\phi(X))^{\mathrm{T}}$, and this means that $\phi(\mathrm{U}(n)) \subset \mathrm{SO}(2n)$. The homomorphism ϕ is injective. We have to show that

$$\phi : \mathrm{U}(n) \longrightarrow \mathrm{Sp}(2n, \mathbb{R}) \cap \mathrm{SO}(2n)$$

is surjective. A matrix $Y \in \mathrm{Sp}(2n,\mathbb{R}) \cap \mathrm{SO}(2n)$ has to satisfy the equations $Y^{\mathrm{T}}JY = J$ and $Y^{\mathrm{T}}Y = I_{2n}$, which are equivalent to the condition $JY = YJ$. For

$$Y = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

the equation $JY = YJ$ implies $C = -B$ and $D = A$, so

$$Y = \begin{pmatrix} A & B \\ -B & A \end{pmatrix},$$

which shows that $Y = \phi(A+iB)$ with $A+iB \in \mathrm{U}(n)$. So we have proved that ϕ is surjective and hence an isomorphism. $\square$

Lemma 2.5. *Let* $p_Y(x) = \sum_{i=0}^{2n} c_i x^i$ *be the characteristic polynomial of the matrix* $Y \in \mathrm{Sp}(2n,\mathbb{R})$*. Then* $c_i = c_{2n-i}$ *for* $i = 0,\ldots,2n$*.*

Proof. The equation $Y^{\mathrm{T}}JY = J$ implies that $p_{Y^{\mathrm{T}}}(x) = p_{Y^{-1}}(x)$. Indeed, the condition on Y to be symplectic can be written as $Y^{\mathrm{T}}J = JY^{-1}$. Using $Y^{-1} = Y^{\mathrm{T}}$ we get $Y^{\mathrm{T}} = JY^{-1}J^{-1}$. Since we know that the characteristic polynomial of $JY^{-1}J^{-1}$ is equal to the characteristic polynomial of Y^{-1}, we get $p_{Y^{\mathrm{T}}}(x) = p_{Y^{-1}}(x)$. But $p_{Y^{\mathrm{T}}} = p_Y$ and for $x \neq 0$ we have

$$\begin{aligned} p_{Y^{-1}}(x) &= \det\bigl(Y^{-1} - x\,I_{2n}\bigr) = \det\bigl(x\,Y^{-1}(x^{-1}\,I_{2n} - Y)\bigr) \\ &= x^{2n}(-1)^{2n}p_Y(x^{-1}) = x^{2n}p_Y(x^{-1}). \end{aligned}$$

Now

$$p_Y(x) = x^{2n}p_Y(x^{-1})$$

and the claim is proved for all $x \in \mathbb{R}\setminus\{0\}$. $\square$

The proof of Lemma 2.5 shows that if λ is an eigenvalue of $Y \in \mathrm{Sp}(2n,\mathbb{R})$, λ^{-1} is also an eigenvalue of Y. The characteristic polynomial $p_Y(x)$ of Y has real coefficients, hence the complex conjugate of a zero of $p_Y(x)$ is also a zero of $p_Y(x)$. This proves that if λ is an eigenvalue of Y, then $\overline{\lambda}$ is also an eigenvalue of Y.

We now define a skew-symmetric bilinear form on $\mathbb{R}^{2n}$

$$\begin{array}{rccc} \langle\ ,\ \rangle : & \mathbb{R}^{2n}\times\mathbb{R}^{2n} & \longrightarrow & \mathbb{R} \\ & (v,w) & \longmapsto & \langle v,w\rangle := v^{\mathrm{T}}Jw. \end{array}$$

The group of isometries of this bilinear form is $\mathrm{Sp}(2n,\mathbb{R})$.

Lemma 2.6. *Let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of $X \in \mathrm{U}(n)$. Then*

$$\{\lambda_1, \dots, \lambda_n, \overline{\lambda}_1, \dots, \overline{\lambda}_n\}$$

is the set of eigenvalues of $\phi(X)$ where $\phi : \mathrm{U}(n) \to \mathrm{Sp}(2n, \mathbb{R})$ is defined as above.

Proof. For any $Y \in \mathrm{Sp}(2n, \mathbb{R}) \cap \mathrm{SO}(2n)$ we can find $X \in \mathrm{U}(n)$ with $\phi(X) = Y$. For each $X \in \mathrm{U}(n)$ there exists a $Z \in \mathrm{U}(n)$ such that $Z^{-1}XZ$ is a diagonal matrix. For $k = 1, \dots, n$ let $\lambda_k = a_k + ib_k$ with $a_k, b_k \in \mathbb{R}$ be the eigenvalues of X. Then

$$\phi(Z^{-1}XZ) = \begin{pmatrix} a_1 & & 0 & b_1 & & 0 \\ & \ddots & & & \ddots & \\ 0 & & a_n & 0 & & b_n \\ -b_1 & & 0 & a_1 & & 0 \\ & \ddots & & & \ddots & \\ 0 & & -b_n & 0 & & a_n \end{pmatrix} = \phi(Z^{-1})\phi(X)\phi(Z).$$

The characteristic polynomial of this matrix is

$$p_Y(\lambda) = \det \begin{pmatrix} a_1 - \lambda & & 0 & b_1 & & 0 \\ & \ddots & & & \ddots & \\ 0 & & a_n - \lambda & 0 & & b_n \\ -b_1 & & 0 & a_1 - \lambda & & 0 \\ & \ddots & & & \ddots & \\ 0 & & -b_n & 0 & & a_n - \lambda \end{pmatrix}.$$

To compute the determinant, we first add i times the $(n+j)$th column to the jth column $\forall j = 1, \dots, n$, and then we subtract i times the jth row from the $(n+j)$th row $\forall j = 1, \dots, n$. We obtain

$$\begin{aligned} p_Y(\lambda) &= (a_1 + ib_1 - \lambda) \cdots (a_n + ib_n - \lambda)(a_1 - ib_1 - \lambda) \cdots (a_n - ib_n - \lambda) \\ &= (\lambda_1 - \lambda) \cdots (\lambda_n - \lambda)(\overline{\lambda}_1 - \lambda) \cdots (\overline{\lambda}_n - \lambda). \end{aligned}$$

$\square$

Corollary 2.7. *Let $\mu_1, \dots, \mu_n$ be the eigenvalues of $X \in \mathrm{U}(n)$ and let*

$$\lambda_1, \dots, \lambda_n, \overline{\lambda}_1, \dots, \overline{\lambda}_n$$

be the eigenvalues of $\phi(X) \in \mathrm{Sp}(2n, \mathbb{R})$. Then for all $j = 1, \dots, n$ exists $1 \leqslant k \leqslant n$ such that

$$\textit{either} \quad \mu_j = \lambda_k \quad \textit{or} \quad \mu_j = \overline{\lambda}_k.$$

Proof. This is just Lemma 2.6. $\square$

Proposition 2.8. *Let $X \in \mathrm{U}((p-1)/2)$ be of odd prime order p, and let ϕ be defined as above. If $\phi(X) \in \mathrm{Sp}(p-1,\mathbb{R})$ is conjugate to some matrix $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$, the eigenvalues $\lambda_1,\ldots,\lambda_{(p-1)/2}$ of $X \in \mathrm{U}((p-1)/2)$ are such that*

$$\{\lambda_1,\ldots,\lambda_{(p-1)/2},\overline{\lambda}_1,\ldots,\overline{\lambda}_{(p-1)/2}\}$$

is the set of primitive pth roots of unity.

Proof. Let $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ be of odd prime order p. We have seen in Proposition 2.3 that the eigenvalues of Y are the primitive pth roots of unity. Now the proposition follows directly from Lemma 2.6 with $n = (p-1)/2$. $\square$

This yields a necessary condition on $X \in \mathrm{U}((p-1)/2)$ such that $\phi(X)$ is conjugate to $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$. Now the question is whether the image $\phi(X)$ of each matrix $X \in \mathrm{U}((p-1)/2)$ that satisfies this condition is conjugate to a matrix $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$. To find the answer, we have to solve the following problem.
Given an element $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ of odd prime order p, how can we find $X \in \mathrm{U}((p-1)/2)$ such that $\phi(X)$ is conjugate to Y?

2.4 A necessary and sufficient condition

For $X \in \mathrm{U}(n)$ we can find real matrices $A, B \in M(n,\mathbb{R})$ such that $X = A+iB$. We have already defined the homomorphism

$$\begin{array}{rrcl} \phi: & \mathrm{U}(n) & \longrightarrow & \mathrm{Sp}(2n,\mathbb{R}) \\ & X = A+iB & \longmapsto & \begin{pmatrix} A & B \\ -B & A \end{pmatrix}. \end{array}$$

We will prove the following theorem.

Theorem 2.9. *Let $X \in \mathrm{U}((p-1)/2)$ be of odd prime order p. Then the image $\phi(X) \in \mathrm{Sp}(p-1,\mathbb{R})$ of X is conjugate to $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ if and only if the eigenvalues $\lambda_1,\ldots,\lambda_{(p-1)/2}$ of X are such that*

$$\{\lambda_1,\ldots,\lambda_{(p-1)/2},\overline{\lambda}_1,\ldots,\overline{\lambda}_{(p-1)/2}\}$$

is a complete set of primitive pth roots of unity.

In Proposition 2.8 we have shown that if $\phi(X) \in \mathrm{Sp}(p-1,\mathbb{R})$ is conjugate to $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$, the condition on the eigenvalues of $X \in \mathrm{U}((p-1)/2)$

holds. Now we have to show that for any X that satisfies the condition on the eigenvalues a matrix Y exists such that $\phi(X)$ is conjugate to Y.
The eigenvalues of a unitary matrix X determine the conjugacy class of X. We will take any $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ of prime order p and show, assuming Y is conjugate to $\phi(X)$, how to compute the eigenvalues of $X \in \mathrm{U}((p-1)/2)$. Then we will prove that if we run through the conjugacy classes of matrices $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ of prime order p, we will run through the conjugacy classes of matrices $X \in \mathrm{U}((p-1)/2)$ that satisfy the necessary condition.
The matrix Y defines an isomorphism $\sigma : \mathbb{Z}^{p-1} \to \mathbb{Z}^{p-1}$. We will consider σ as an isomorphism $\sigma : \mathbb{R}^{p-1} \to \mathbb{R}^{p-1}$ by linear extension. Then we will define subspaces V_j, $j = 1, \ldots, (p-1)/2$, of $\mathbb{R}^{p-1}$ that are invariant under σ. A sign $\mathrm{sign}(V_j)$ defined on these spaces will tell us which are the eigenvalues of $X \in \mathrm{U}((p-1)/2)$ with $\phi(X)$ conjugate to Y.
In the last part, we will show that if we run through all conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$, we will run through all the combinations of $\mathrm{sign}(V_1), \ldots, \mathrm{sign}(V_{(p-1)/2})$ and therefore through all conjugacy classes of matrices $X \in \mathrm{U}((p-1)/2)$ that satisfy the condition on the eigenvalues. An interesting corollary is the following.

Corollary 2.10. *The number of conjugacy classes of elements of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$ that are conjugate to elements of the form $\phi(X)$, where X is in $\mathrm{U}((p-1)/2)$, is greater or equal to $2^{(p-1)/2}$.*

2.4.1 The decomposition of $\mathbb{R}^{p-1}$

Let p be an odd prime, and let $m(x)$ be the minimal polynomial of the field extension $\mathbb{Q}(\xi)/\mathbb{Q}$ where ξ is a primitive pth root of unity. We know that $m(x)$ is irreducible over $\mathbb{Q}$ and, by Proposition 2.3, that it is equal to the characteristic polynomial of any $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ of order p.
Let σ be an isomorphism $\sigma : \mathbb{Z}^{p-1} \to \mathbb{Z}^{p-1}$ where $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ is the matrix that defines σ in the standard basis of $\mathbb{Z}^{p-1}$. Then σ is an isometry of the skew-symmetric bilinear form $q : \mathbb{Z}^{p-1} \times \mathbb{Z}^{p-1} \to \mathbb{Z}$. In the standard basis

$$\begin{array}{rccc} q := \langle\ ,\ \rangle : & \mathbb{Z}^{p-1} \times \mathbb{Z}^{p-1} & \longrightarrow & \mathbb{Z} \\ & (x,y) & \longmapsto & \langle x,y\rangle := x^{\mathrm{T}} J y \end{array}$$

where J is like in the definition of the symplectic group. Without making any special remark, we will extend the $\mathbb{Z}$-automorphism $\sigma : \mathbb{Z}^{p-1} \to \mathbb{Z}^{p-1}$ to a $\mathbb{R}$-automorphism $\sigma : \mathbb{R}^{p-1} \to \mathbb{R}^{p-1}$ or to a $\mathbb{C}$-automorphism $\sigma : \mathbb{C}^{p-1} \to \mathbb{C}^{p-1}$. We can also extend the alternating $\mathbb{Z}$-bilinear form $q : \mathbb{Z}^{p-1} \times \mathbb{Z}^{p-1} \to \mathbb{Z}$ to an alternating $\mathbb{R}$-bilinear form $q : \mathbb{R}^{p-1} \times \mathbb{R}^{p-1} \to \mathbb{R}$ or to an alternating $\mathbb{C}$-bilinear form $q : \mathbb{C}^{p-1} \times \mathbb{C}^{p-1} \to \mathbb{C}$.

Over $\mathbb{R}$ the polymonial $m(x)$ splits in factors of degree 2:

$$m(x) = 1 + \cdots + x^{p-1} = \prod_{j=1}^{(p-1)/2} f_j(x)$$

where

$$\begin{aligned} f_j(x) &= \left(x - \xi^j\right)\left(x - \overline{\xi^j}\right) = \left(x - \xi^j\right)\left(x - \xi^{-j}\right) \\ &= x^2 - 2\cos(j2\pi/p)\, x + 1 \in \mathbb{R}[x]. \end{aligned}$$

Definition. Let $\sigma : \mathbb{R}^{p-1} \to \mathbb{R}^{p-1}$ be an isomorphism of odd prime order p whose eigenvalues are the primitive pth roots of unity. Let f_j be the polynomial

$$f_j(x) := \left(x - \xi^j\right)\left(x - \xi^{-j}\right)$$

where $\xi := e^{i2\pi/p}$. Then we define for $j = 1, \ldots, \frac{p-1}{2}$ the subspace

$$V_j := \ker f_j(\sigma)$$

of $\mathbb{R}^{p-1}$.

Then

$$\mathbb{R}^{p-1} = V_1 \oplus \cdots \oplus V_{(p-1)/2}$$

with $\dim V_j = 2$, $j = 1, \ldots, (p-1)/2$. The characteristic polynomial of $\sigma|_{V_j}$ is $f_j(x)$, and V_j is the σ-invariant subspace of $\mathbb{R}^{p-1}$ corresponding to the eigenvalues ξ^j and ξ^{-j}. So we have $\sigma(V_j) = V_j$. Let

$$q_j := q|_{V_j} : V_j \times V_j \longrightarrow \mathbb{R}$$

be the restriction of q on V_j. The bilinear form q_j is skew-symmetric.
Now we will consider the complexification. Let $v_j \in \mathbb{C}^{p-1}$ be an eigenvector of σ to the eigenvalue ξ^j. Then $\overline{v}_j$ is an eigenvector to the eigenvalue ξ^{-j} because

$$\sigma(v_j) = \xi^j v_j \quad \Leftrightarrow \quad \sigma(\overline{v}_j) = \overline{\sigma(v_j)} = \overline{\xi^j v_j} = \xi^{-j}\overline{v}_j.$$

The vectors v_j and $\overline{v}_j$ are linearly independent. Indeed, if they were linearly dependent, we would have $\lambda v_j = \overline{v}_j$ and $\sigma(\lambda v_j) = \lambda\sigma(v_j) = \lambda\xi^j v_j = \xi^j\overline{v}_j$, but $\sigma(\lambda v_j) = \sigma(\overline{v}_j) = \xi^{-j}\overline{v}_j$. This yields a contradiction since $\xi^j \neq 1$. Thus the real vectors

$$w_j := v_j + \overline{v}_j, \qquad \widetilde{w}_j := -i(v_j - \overline{v}_j)$$

are also linearly independent. Since v_j and $\overline{v}_j$ are mapped to multiples of themselves, w_j and $\widetilde{w}_j$ are mapped to linear combinations of themselves. Moreover,

$w_j, \widetilde{w}_j \in \mathbb{R}^{p-1}$ span a 2-dimensional subspace of $\mathbb{R}^{p-1}$, which is V_j since the restriction of σ to this space has the eigenvalues ξ^j and ξ^{-j}. Constructing for all V_j, $j = 1, \dots, (p-1)/2$, such a basis w_j, $\widetilde{w}_j$, we get a basis

$$w_1, \dots, w_{(p-1)/2}, \widetilde{w}_1, \dots, \widetilde{w}_{(p-1)/2}$$

of $\mathbb{R}^{p-1}$.

Lemma 2.11. *For any $x \in V_j$, $y \in V_k$ with $j \neq k$ and $j, k = 1, \dots, (p-1)/2$ we have*

$$q(x, y) = 0.$$

Proof. This follows from the fact that

$$q(v_j, v_k) = q(\sigma(v_j), \sigma(v_k)) = q(\xi^j v_j, \xi^k v_k) = \xi^j \xi^k q(v_j, v_k)$$

implies either $\xi^j \xi^k = 1$ or $q(v_j, v_k) = 0$. Since $\xi^j \xi^k = 1$ means that $\xi^k = \xi^{-j}$, the equation $\xi^j \xi^k = 1$ is a contradiction to $j, k = 1, \dots, (p-1)/2$. So we must have $q(v_j, v_k) = 0$. □

Since q is regular, q is not degenerate on V_j. This implies that q_j is not degenerate. For linearly independent $x, y \in V_j$ we have $q_j(x, y) \neq 0$. Choose any nonzero $x \in V_j$. Since p is odd, x and $\sigma(x)$ form a basis of V_j. The eigenvalues of $\sigma|_{V_j}$ are ξ^j and ξ^{-j}, and we have $(\sigma|_{V_j})^p = 1$. So $\sigma|_{V_j} : V_j \to V_j$ is a rotation of $\pm j\, 2\pi/p$. We set $\theta_j := j 2\pi/p$. Then

$$\begin{aligned}
\sigma(w_j) &= \sigma(v_j + \overline{v}_j) = \xi^j v_j + \xi^{-j} \overline{v}_j \\
&= (\cos\theta_j + i \sin\theta_j)\, v_j + (\cos\theta_j - i\sin\theta_j)\, \overline{v}_j \\
&= \cos\theta_j\, (v_j + \overline{v}_j) + i \sin\theta_j\, (v_j - \overline{v}_j) \\
&= \cos\theta_j\ w_j - \sin\theta_j\ \widetilde{w}_j
\end{aligned}$$

and

$$\begin{aligned}
\sigma(\widetilde{w}_j) &= \sigma(-i(v_j - \overline{v}_j)) = -i(\xi^j v_j - \xi^{-j} \overline{v}_j) \\
&= -i((\cos\theta_j + i\sin\theta_j)\, v_j - (\cos\theta_j - i \sin\theta_j)\, \overline{v}_j) \\
&= \sin\theta_j\, (v_j + \overline{v}_j) - i \cos\theta_j\, (v_j - \overline{v}_j) \\
&= \sin\theta_j\ w_j + \cos\theta_j\ \widetilde{w}_j.
\end{aligned}$$

2.4.2 Definition of the sign of V_j

Definition. We define the sign $\operatorname{sign}(V_j)$ of V_j to be

$$\operatorname{sign}(V_j) := \operatorname{sign} q(x, \sigma(x))$$

where $x \in V_j$ is any nonzero element.

Lemma 2.12. *The sign* $\operatorname{sign}(V_j)$ *is well-defined, i.e. independent of the choice of* x.

Proof. Let w_j, $\widetilde{w}_j$ be the basis of V_j that we defined above. Set $0 \neq x \in V_j$, i.e. $x := \alpha w_j + \beta \widetilde{w}_j$ with $\alpha \neq 0$ or $\beta \neq 0$. Then

$$\begin{aligned}
q(x, \sigma(x)) &= q(\alpha\, w_j + \beta\, \widetilde{w}_j, \sigma(\alpha\, w_j + \beta\, \widetilde{w}_j)) \\
&= q(\alpha w_j + \beta \widetilde{w}_j, (\alpha \cos\theta_j + \beta \sin\theta_j)\, w_j + (\beta\cos\theta_j - \alpha \sin\theta_j)\, \widetilde{w}_j) \\
&= \alpha(\beta\cos\theta_j - \alpha\sin\theta_j)\, q(w_j, \widetilde{w}_j) + \beta(\alpha\cos\theta_j + \beta\sin\theta_j)\, q(\widetilde{w}_j, w_j) \\
&= -(\alpha^2 + \beta^2)\sin\theta_j\, q(w_j, \widetilde{w}_j).
\end{aligned}$$

We have $\alpha^2 + \beta^2 > 0$. Let $\theta_j = j2\pi/p$ for $j = 1, \ldots, (p-1)/2$. Herewith we have $\sin\theta_j > 0$, and therefore

$$\operatorname{sign} q(x, \sigma(x)) = \operatorname{sign}(-q(w_j, \widetilde{w}_j))$$

does not depend on the choice of α and β. So we can choose any nonzero $x \in V_j$. ◻

Lemma 2.13. *We have*

$$\operatorname{sign}(V_j) = \operatorname{sign} \operatorname{Im}\big(q(v_j, \overline{v}_j)\big).$$

Proof. Since $q(x, \sigma(x))$ is real and

$$q(x, \sigma(x)) = -2i\,(\alpha^2 + \beta^2)\, \sin\theta_j\; q(v_j, \overline{v}_j),$$

$q(v_j, \overline{v}_j)$ is purely imaginary. So we have

$$\begin{aligned}
\operatorname{sign} q(x, \sigma(x)) &= \operatorname{sign}\big(-q(w_j, \widetilde{w}_j)\big) = \operatorname{sign}\big(-q\big(v_j + \overline{v}_j, -i\,(v_j - \overline{v}_j)\big)\big) \\
&= \operatorname{sign}\big(-2i\, q(v_j, \overline{v}_j)\big) = \operatorname{sign}\big(-i\, q(v_j, \overline{v}_j)\big) \\
&= \operatorname{sign}\operatorname{Im}\big(q(v_j, \overline{v}_j)\big).
\end{aligned}$$

◻

We consider the vectors w_j, $\widetilde{w}_j$, $j = 1, \ldots, (p-1)/2$. It follows from Lemma 2.11 that for $i, j = 1, \ldots, (p-1)/2$ with $i \neq j$ the following is true:

$$q(w_i, w_j) = q(\widetilde{w}_i, \widetilde{w}_j) = q(w_i, \widetilde{w}_j) = 0,$$

but

$$q(w_j, \widetilde{w}_j) \neq 0.$$

We define for $j = 1, \ldots, \frac{p-1}{2}$ real constants

$$\begin{aligned} c_j &:= \bigl(\operatorname{sign}\bigl(q(w_j, \widetilde{w}_j)\bigr)\, q(w_j, \widetilde{w}_j)\bigr)^{-\frac{1}{2}} \\ &= \bigl(-\operatorname{sign}(V_j)\, q(w_j, \widetilde{w}_j)\bigr)^{-\frac{1}{2}} \end{aligned}$$

and vectors in V_j:

$$u_j := c_j\ w_j, \qquad \widetilde{u}_j := -\operatorname{sign}(V_j)\ c_j\ \widetilde{w}_j.$$

These u_j, $\widetilde{u}_j$ form a basis of V_j, and therefore we have constructed a basis $u_1, \ldots, u_{(p-1)/2}, \widetilde{u}_1, \ldots, \widetilde{u}_{(p-1)/2}$ of $\mathbb{R}^{p-1}$.

Lemma 2.14. *The vectors $u_1, \ldots, u_{(p-1)/2}, \widetilde{u}_1, \ldots, \widetilde{u}_{(p-1)/2}$ form a symplectic basis of $\mathbb{R}^{p-1}$.*

Proof. For $i \neq j$ with $i, j = 1, \ldots, \frac{p-1}{2}$

$$\begin{aligned} q(u_i, u_j) &= q(\widetilde{u}_i, \widetilde{u}_j) = q(u_i, \widetilde{u}_j) = 0, \\ q(u_j, \widetilde{u}_j) &= -\operatorname{sign}(V_j)\ c_j^2\ q(w_j, \widetilde{w}_j) = 1. \end{aligned}$$

In the basis $u_1, \ldots, u_{(p-1)/2}, \widetilde{u}_1, \ldots, \widetilde{u}_{(p-1)/2}$, the form q is given by the matrix J, and since σ is an isometry of q, σ is given by a matrix $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$. $\square$

With these definitions we can compute

$$\begin{aligned} \sigma(u_j) = Y\, u_j &= c_j\, Y\, w_j \\ &= c_j\ \cos\theta_j\ w_j - c_j\ \sin\theta_j\ \widetilde{w}_j \\ &= \cos\theta_j\ u_j - (-\operatorname{sign}(V_j)) \sin\theta_j\ \widetilde{u}_j, \end{aligned}$$

and

$$\begin{aligned} \sigma(\widetilde{u}_j) = Y\, \widetilde{u}_j &= -\operatorname{sign}(V_j)\, c_j\, Y\, \widetilde{w}_j \\ &= -\operatorname{sign}(V_j)\, c_j\ \sin\theta_j\ w_j - \operatorname{sign}(V_j)\, c_j\ \cos\theta_j\ \widetilde{w}_j \\ &= -\operatorname{sign}(V_j)\ \sin\theta_j\ u_j + \cos\theta_j\ \widetilde{u}_j. \end{aligned}$$

The matrix corresponding to $\sigma|_{V_j} : V_j \to V_j$ in the basis $u_j, \widetilde{u}_j$ is the following:

$$\begin{pmatrix} \cos\theta_j & -\operatorname{sign}(V_j) \sin\theta_j \\ \operatorname{sign}(V_j) \sin\theta_j & \cos\theta_j \end{pmatrix}.$$

Now we see that the matrix corresponding to $\sigma : \mathbb{R}^{p-1} \to \mathbb{R}^{p-1}$ in the basis $u_1, \ldots, u_{(p-1)/2}, \widetilde{u}_1, \ldots, \widetilde{u}_{(p-1)/2}$ is

$$\begin{pmatrix} \cos\theta_j & 0 & -\mathcal{S}_1 \sin\theta_1 & 0 \\ & \ddots & & \ddots \\ 0 & \cos\theta_{\frac{p-1}{2}} & 0 & -\mathcal{S}_{\frac{p-1}{2}} \sin\theta_{\frac{p-1}{2}} \\ \mathcal{S}_1 \sin\theta_1 & 0 & \cos\theta_j & 0 \\ & \ddots & & \ddots \\ 0 & \mathcal{S}_{\frac{p-1}{2}} \sin\theta_{\frac{p-1}{2}} & 0 & \cos\theta_{\frac{p-1}{2}} \end{pmatrix}$$

where $\mathcal{S}_j := \operatorname{sign}(V_j)$, $j = 1, \ldots, \frac{p-1}{2}$. We want this matrix to look like

$$\begin{pmatrix} \cos\vartheta_1 & 0 & \sin\vartheta_1 & 0 \\ & \ddots & & \ddots \\ 0 & \cos\vartheta_{\frac{p-1}{2}} & 0 & \sin\vartheta_{\frac{p-1}{2}} \\ -\sin\vartheta_1 & 0 & \cos\vartheta_1 & 0 \\ & \ddots & & \ddots \\ 0 & -\sin\vartheta_{\frac{p-1}{2}} & 0 & \cos\vartheta_{\frac{p-1}{2}} \end{pmatrix},$$

because in this case the $e^{i\vartheta_j}$, $j = 1, \ldots, (p-1)/2$, are the eigenvalues of the $X \in \mathrm{U}((p-1)/2)$ we are searching for. Comparing both matrices we get

$$\vartheta_j := \begin{cases} \theta_j & \text{if } \operatorname{sign}(V_j) = -1 \\ 2\pi - \theta_j & \text{if } \operatorname{sign}(V_j) = +1. \end{cases}$$

This proves the following proposition.

Proposition 2.15. *Let $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$ of odd prime order p define an isomorphism $\sigma : \mathbb{Z}^{p-1} \to \mathbb{Z}^{p-1}$. Let $\xi := e^{i2\pi/p}$, $\mathbb{R}^{p-1} = V_1 \oplus \cdots \oplus V_{(p-1)/2}$ where V_j, $j = 1, \ldots, (p-1)/2$, is the invariant subspace corresponding to the eigenvalues ξ^j, ξ^{p-j} of the extension of σ to an isomorphism of $\mathbb{R}^{p-1}$. Then there exists $X \in \mathrm{U}((p-1)/2)$ such that Y is conjugate to $\phi(X) \in \mathrm{Sp}(p-1, \mathbb{R})$. Moreover,*

if $\operatorname{sign}(V_j) = -1$, ξ^j is eigenvalue of $X \in \mathrm{U}((p-1)/2)$, and
if $\operatorname{sign}(V_j) = 1$, ξ^{-j} is eigenvalue of $X \in \mathrm{U}((p-1)/2)$.

2.4.3 The proof of the necessary and sufficient condition

The sign of a nonzero real number can be considered as an element of $\mathbb{Z}/2\mathbb{Z}$ if we define

$$\begin{array}{rccl} \psi' : & \mathbb{R} \setminus \{0\} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & x & \longmapsto & \psi'(x) = \begin{cases} 0 & \text{if } x > 0 \\ 1 & \text{if } x < 0. \end{cases} \end{array}$$

Let $\gamma_j \in \mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$ with $\gamma_j(\xi) = \xi^j$ where ξ is a primitive pth root of unity and $j = 1, \ldots, p-1$. For $v_1 = (\alpha_1, \ldots, \alpha_{p-1}) \in \mathbb{Z}[\xi]^{p-1}$ we define the vector

$$v_j := (\gamma_j(\alpha_1), \ldots, \gamma_j(\alpha_{p-1}))^{\mathrm{T}}.$$

Let $\mathcal{M}$ be the set of $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$ with $Y^p = 1, Y \neq 1$. If v_1 is an eigenvector to the eigenvalue ξ of $Y \in \mathcal{M}$, v_j is an eigenvector to the eigenvalue ξ^j. We define a mapping

$$\begin{array}{rccl} \psi : & \mathcal{M} & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^{(p-1)/2} \\ & Y & \longmapsto & \big(\psi'(-i\langle v_1, v_{p-1}\rangle), \ldots, \psi'(-i\langle v_{(p-1)/2}, v_{(p+1)/2}\rangle)\big) \end{array}$$

where $\mathrm{sign}(-i\langle v_j, v_{p-j}\rangle) = \mathrm{sign}(V_j)$, $j = 1, \ldots, (p-1)/2$. It follows from Proposition 2.15 that the necessary condition is sufficient if ψ is surjective. Therefore we now have to prove the surjectivity of ψ. First we will prove that in each conjugacy class of matrices of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/p])$ one can find a matrix in $\mathrm{Sp}(p-1, \mathbb{Z})$. Let $\mathcal{M}_p$ be the set of matrices of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/p])$. We will show the surjectivity of the mapping

$$\begin{array}{rccl} \psi_p : & \mathcal{M}_p & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^{(p-1)/2} \\ & Y & \longmapsto & \big(\psi'(-i\langle v_1, v_{p-1}\rangle), \ldots, \psi'(-i\langle v_{(p-1)/2}, v_{(p+1)/2}\rangle)\big) \end{array}$$

where v_1 is an eigenvector of Y to the eigenvalue ξ. Then we have shown that ψ is surjective since matrices of $\mathcal{M}_p$ that are in the same conjugacy class have the same image under ψ_p.

In the article of Sjerve and Yang [10] is shown that a bijection exists between the conjugacy classes of elements of order p in $\mathrm{Sp}(p-1, \mathbb{Z})$ and some equivalence classes of pairs $(\mathfrak{a}, a)$ where $\mathfrak{a} \subseteq \mathbb{Z}[\xi]$ is an ideal and $a \in \mathbb{Z}[\xi]$. In the article of Brown [3] is shown that a bijection exists between the conjugacy classes of elements of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/p])$ and some equivalence classes of pairs $(\mathfrak{a}, a)$ where $\mathfrak{a}$ is an ideal in $\mathbb{Z}[1/p][\xi]$ and $a \in \mathbb{Z}[1/p][\xi]$.

Let P be the set of pairs $(\mathfrak{a}, a)$ consisting of an integral ideal $0 \neq \mathfrak{a} \subseteq \mathbb{Z}[\xi]$ and an element $a \in \mathbb{Z}[\xi]$ such that $\mathfrak{a}\overline{\mathfrak{a}} = (a) \subseteq \mathbb{Z}[\xi]$ is a principal ideal and $a = \overline{a}$. The bar denotes complex conjugation and $\overline{\mathfrak{a}} = \{\overline{\alpha} \mid \alpha \in \mathfrak{a}\}$. We define an equivalence relation $\sim$ on P:

$$(\mathfrak{a}, a) \sim (\mathfrak{b}, b) \quad \Leftrightarrow \quad \begin{array}{l} \exists \lambda, \mu \in \mathbb{Z}[\xi] \setminus \{0\} \text{ such that} \\ \lambda\mathfrak{a} = \mu\mathfrak{b} \text{ and } \lambda\overline{\lambda}a = \mu\overline{\mu}b. \end{array}$$

We denote by $[\mathfrak{a}, a]$ the equivalence class of $(\mathfrak{a}, a)$, and $\mathcal{P}$ denotes the set of equivalence classes of P.
Let P_p be the set of pairs $(\mathfrak{a}_p, a)$ consisting of an ideal $0 \neq \mathfrak{a}_p \subseteq \mathbb{Z}[1/p][\xi]$ and $a \in \mathbb{Z}[1/p][\xi]$ such that $\mathfrak{a}_p\overline{\mathfrak{a}}_p = (a) \subseteq \mathbb{Z}[1/p][\xi]$ is a principal ideal and $a = \overline{a}$. We define an equivalence relation on P_p:

$$(\mathfrak{a}_p, a) \sim (\mathfrak{b}_p, b) \quad \Leftrightarrow \quad \begin{array}{l} \exists \lambda, \mu \in \mathbb{Z}[1/p][\xi] \setminus \{0\} \text{ such that} \\ \lambda\mathfrak{a}_p = \mu\mathfrak{b}_p \text{ and } \lambda\overline{\lambda}a = \mu\overline{\mu}b. \end{array}$$

We denote by $[\mathfrak{a}_p, a]$ the equivalence class of $(\mathfrak{a}_p, a)$, and $\mathcal{P}_p$ denotes the set of equivalence classes of P_p.
The sets of equivalence classes $\mathcal{P}$ and $\mathcal{P}_p$ are abelian groups. The multiplication is given by $[\mathfrak{a}, a][\mathfrak{b}, b] = [\mathfrak{a}\mathfrak{b}, ab]$, the inverse of $[\mathfrak{a}, a]$ is $[\overline{\mathfrak{a}}, a]$, and the unit in $\mathcal{P}$ and $\mathcal{P}_p$ are $[\mathbb{Z}[\xi], 1]$ and $[\mathbb{Z}[1/p][\xi], 1]$ respectively.
Let $\mathcal{C}_0 := \mathcal{C}_0(\mathbb{Z}[\xi])$ be the subgroup of the ideal class group $\mathcal{C} = \mathcal{C}(\mathbb{Z}[\xi])$ given by

$$\mathcal{C}_0 = \{\mathfrak{a} \in \mathcal{C} \mid \mathfrak{a}\overline{\mathfrak{a}} = (a), a = \overline{a} \text{ for some } a \in \mathbb{Z}[\xi]\}.$$

Let $\mathcal{C}_p := \mathcal{C}(\mathbb{Z}[1/p][\xi])$ denote the ideal class group of the Dedekind domain $\mathbb{Z}[1/p][\xi]$. We define a subgroup $\mathcal{C}_{p0} := \mathcal{C}_0(\mathbb{Z}[1/p][\xi])$ of $\mathcal{C}_p$:

$$\begin{aligned} \mathcal{C}_{p0} &= \mathcal{C}_0(\mathbb{Z}[1/p][\xi]) \\ &= \{\mathfrak{a}_p \in \mathcal{C}_p \mid \mathfrak{a}_p\overline{\mathfrak{a}}_p = (a), a = \overline{a} \text{ for some } a \in \mathbb{Z}[1/p][\xi]\}. \end{aligned}$$

Let U be the group of units in $\mathbb{Z}[\xi]$ and $U^+ = \{u \in U \mid u = \overline{u}\}$ the group of units in $\mathbb{Z}[\xi + \overline{\xi}]$. Let $N : \mathbb{Q}(\xi) \to \mathbb{Q}(\xi + \overline{\xi})$, $a \mapsto N(a) = a\overline{a}$, be the norm mapping and $N(U) := \{u\overline{u} = N(u) \mid u \in U\}$. Let U_p be the group of units in $\mathbb{Z}[1/p][\xi]$ and $U_p^+ = \{u \in U_p \mid u = \overline{u}\}$, $N(U_p) = \{u\overline{u} \mid u \in U_p\}$. Clearly $N(U) \subset U^+$, $N(U_p) \subset U_p^+$, and we can define the abelian groups $U^+/N(U)$ and $U_p^+/N(U_p)$.
According to Theorem 2 in the article of Sjerve and Yang [10], there is a short exact sequence of abelian groups

$$1 \longrightarrow U^+/N(U) \xrightarrow{\ \delta\ } \mathcal{P} \xrightarrow{\ \eta\ } \mathcal{C}_0 \longrightarrow 1$$

where $\delta(uN(U)) = [\mathbb{Z}[\xi], u]$, $\eta([\mathfrak{a}, a]) = [\mathfrak{a}]$. Theorem 3 in the article of Sjerve and Yang [10] states that the number of elements in $\mathcal{P}$ is $2^{(p-1)/2}h^-$. Here $h^- := h/h^+$ where h and h^+ are the class numbers of $\mathbb{Q}(\xi)$ and $\mathbb{Q}(\xi + \overline{\xi})$ respectively. A short introduction to this subject can be found in the chapter about cyclotomic fields. In the article of Brown [3] we find that there is a short exact sequence

$$1 \longrightarrow U_p^+/N(U_p) \xrightarrow{\delta_p} \mathcal{P}_p \xrightarrow{\eta_p} \mathcal{C}_{p0} \longrightarrow 1$$

where $\delta_p(uN(U)) = [\mathbb{Z}[1/p][\xi], u]$, $\eta_p([\mathfrak{a}_p, a]) = [\mathfrak{a}_p]$. Moreover, a bijection exists between the conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/p])$ and $\mathcal{P}_p$. Proposition 7 in the article of Brown [3] states that the cardinality of $\mathcal{P}_p$ is $[U_p^+ : N(U_p)]h^-$. Now we have to determine the first factor. It is well-known (see Washington [11]) that the prime above p in $\mathbb{Q}(\xi)$ is principal and generated by $1-\xi$. The prime above p in $\mathbb{Q}(\xi+\overline{\xi})$ is principal and generated by $(1-\xi)(1-\overline{\xi}) = N(1-\xi)$. It is clear that for any $x \in U_p^+$ either $x \in U^+$ or there exists $y \in \mathbb{Z}[\xi]$ such that $xy = p^r$ for some $r \in \mathbb{Z}$. This implies that $U_p = U \cdot \langle 1-\xi \rangle$ where $\langle 1-\xi \rangle$ is the group generated by $1-\xi$, and $U_p^+ = U^+ \cdot \langle (1-\xi)(1-\overline{\xi}) \rangle$ where $\langle (1-\xi)(1-\overline{\xi}) \rangle$ is the subgroup of $\langle 1-\xi \rangle$ generated by $(1-\xi)(1-\overline{\xi})$. Hence

$$[U_p^+ : N(U_p)] = [U^+ : N(U)] = 2^{(p-1)/2}.$$

The last equation is a consequence of the Dirichlet unit theorem:

$$U^+ \cong \mathbb{Z}^{(p-3)/2} \times \mathbb{Z}/2\mathbb{Z}.$$

Therefore the number of classes in $\mathcal{P}$ is equal to the number of classes in $\mathcal{P}_p$, which is $2^{(p-1)/2}h^-$.
Now we will define homomorphisms ρ_1, ρ and ρ_2 such that the following diagram commutes.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & U^+/N(U) & \xrightarrow{\delta} & \mathcal{P} & \xrightarrow{\eta} & \mathcal{C}_0 & \longrightarrow & 1 \\
 & & \rho_1 \big\downarrow & & \rho \big\downarrow & & \rho_2 \big\downarrow & & \\
1 & \longrightarrow & U_p^+/N(U_p) & \xrightarrow{\delta_p} & \mathcal{P}_p & \xrightarrow{\eta_p} & \mathcal{C}_{p0} & \longrightarrow & 1
\end{array}$$

We define a homomorphism of abelian groups:

$$\begin{array}{rccc}
\rho_1 : & U^+/N(U) & \longrightarrow & U_p^+/N(U_p) \\
 & uN(U) & \longmapsto & uN(U_p).
\end{array}$$

Let $uN(U) \neq vN(U) \in U^+/N(U)$, then $uN(U_p) \neq vN(U_p)$ since $\langle 1-\xi \rangle$ is not a subgroup of U. Therefore ρ_1 is injective and ρ_1 is an isomorphism since

$$|U^+/N(U)| = |U_p^+/N(U_p)| = 2^{(p-1)/2}.$$

Now we will define $\rho_2 : \mathcal{C}_0 \to \mathcal{C}_{p0}$. Let $(a) = a\mathbb{Z}[\xi] \subseteq \mathbb{Z}[\xi]$ be a principal ideal. Then $a\mathbb{Z}[1/p][\xi]$ is a principal ideal in $\mathbb{Z}[1/p][\xi]$. Let $\mathfrak{a} \subseteq \mathbb{Z}[\xi]$ be an ideal. Then we consider the ideal $\mathfrak{a}_p \in \mathbb{Z}[1/p][\xi]$ generated by the elements αz with $\alpha \in \mathfrak{a}$, $z \in \mathbb{Z}[1/p][\xi]$. An element of $\mathfrak{a}_p$ is a finite sum $\sum_{i=1}^n \alpha_i z_i$ with $\alpha_i \in \mathfrak{a}$, $z_i \in \mathbb{Z}[1/p][\xi]$. For each $z_i \in \mathbb{Z}[1/p][\xi]$ exists $r_i \in \mathbb{N}$ with $p^{r_i} z_i \in \mathbb{Z}[\xi]$. Let $r := \max\{r_i \mid i = 1, \ldots, n\}$. Then $p^r z_i \in \mathbb{Z}[\xi]$ for $i = 1, \ldots, n$, $1/p^r \in \mathbb{Z}[1/p][\xi]$ and $\alpha_i p^r z_i \in \mathfrak{a}$. Herewith we get

$$\sum_{i=1}^{n} \alpha_i z_i = \frac{1}{p^r} \sum_{i=1}^{n} \alpha_i p^r z_i \in \mathbb{Z}[1/p][\xi].$$

Thus $\mathfrak{a}_p = \mathfrak{a}\mathbb{Z}[1/p][\xi]$ and we can define a homomorphism

$$\begin{array}{rccc} \rho_2 : & \mathcal{C}_0 & \longrightarrow & \mathcal{C}_{p0} \\ & [\mathfrak{a}] & \longmapsto & [\mathfrak{a}_p]. \end{array}$$

Let $[\mathfrak{a}], [\mathfrak{b}] \in \mathcal{C}_0$, $[\mathfrak{a}] \neq [\mathfrak{b}]$. Then $[\mathfrak{a}_p] \neq [\mathfrak{b}_p]$. Indeed, let $\mathfrak{a}$ and $\mathfrak{b}$ be representatives of $[\mathfrak{a}]$ and $[\mathfrak{b}]$ respectively. Then it is clear that $\mathfrak{a} \neq \mathfrak{b}$. It is even true that $\mathfrak{a}_p \neq \mathfrak{b}_p$ since if $\mathfrak{a} \neq \mathfrak{b}$, there exists an $\alpha \in \mathfrak{a}$ with $\alpha \notin \mathfrak{b}$ and then $\alpha\mathbb{Z}[\xi] \nsubseteq \mathfrak{b}$. This implies $[\mathfrak{a}_p] \neq [\mathfrak{b}_p]$ because $[\mathfrak{a}_p] = [\mathfrak{b}_p]$ would mean that there exist $\lambda, \mu \in \mathbb{Z}[1/p][\xi]$ with $\lambda\mathfrak{a}_p = \mu\mathfrak{b}_p$. For each $\beta \in \mathfrak{b}_p$ would exist $\alpha \in \mathfrak{a}_p$ with $\lambda\alpha = \mu\beta$. Let $r, s \in \mathbb{N}$ be the smallest numbers such that $p^r\lambda, p^s\mu \in \mathbb{Z}[\xi]$; then for each $\beta \in \mathfrak{b}$ exists $\alpha \in \mathfrak{a}$ with $p^r\lambda\alpha = p^s\mu\beta$. Herewith ρ_2 is injective and ρ_2 is an isomorphism since $|\mathcal{C}_0| = |\mathcal{C}_{0p}| = h^- < \infty$. Now it remains to define

$$\begin{array}{rccc} \rho : & \mathcal{P} & \longrightarrow & \mathcal{P}_p \\ & [\mathfrak{a}, a] & \longmapsto & [\mathfrak{a}_p, a]. \end{array}$$

Let $\mathfrak{a}\overline{\mathfrak{a}} = (a)$. Then $\mathfrak{a}_p\overline{\mathfrak{a}}_p = (a)$, a principal ideal in $\mathbb{Z}[1/p][\xi]$, since if $x \in \mathfrak{a}_p\overline{\mathfrak{a}}_p$,

$$x = \sum_{i=1}^{n} \alpha_i z_i' \overline{\beta}_i z_i'' = \sum_{i=1}^{n} \alpha_i \overline{\beta}_i z_i \in a\mathbb{Z}[1/p][\xi]$$

where $\alpha_i, \beta_i \in \mathfrak{a}$ and $z_i', z_i'' \in \mathbb{Z}[1/p][\xi]$ with $z_i = z_i' z_i''$, $i = 1, \ldots, n$. Therefore ρ is well defined.

It follows directly from the definitions that

$$\rho \circ \delta = \delta_p \circ \rho_1 \quad \text{and} \quad \rho_2 \circ \eta = \eta_p \circ \rho.$$

Therefore the squares commute and, as a consequence of the five-lemma, ρ is an isomorphism.

In the articles of Brown [3] and of Sjerve and Yang [10] is shown that a bijection exists between the elements in $\mathcal{P}$, resp. $\mathcal{P}_p$, and the conjugacy classes of

elements of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$, resp. $\mathrm{Sp}(p-1,\mathbb{Z}[1/p])$. Since $\mathcal{P}$ and $\mathcal{P}_p$ are isomorphic, each conjugacy class in $\mathrm{Sp}(p-1,\mathbb{Z}[1/p])$ contains an element of $\mathrm{Sp}(p-1,\mathbb{Z})$. This means that the isomorphism $\rho:\mathcal{P}\to\mathcal{P}_p$ corresponds to mapping conjugacy classes of elements of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$ to conjugacy classes of elements of order p in $\mathrm{Sp}(p-1,\mathbb{Z}[1/p])$.
Now we will recall parts of the discussion in [10] that are important for our purposes. Let $Y\in\mathrm{Sp}(p-1,\mathbb{Z})$ be of prime order p and

$$v_1=(\alpha_1,\dots,\alpha_{p-1})^{\mathrm{T}}\in\mathbb{Z}[\xi]^{p-1}$$

be an eigenvector corresponding to ξ, that is $Yv_1=\xi v_1$. Let $\mathfrak{a}$ be the $\mathbb{Z}$-module generated by $\alpha_1,\dots,\alpha_{p-1}$, $\mathfrak{a}=\mathbb{Z}\alpha_1+\dots+\mathbb{Z}\alpha_{p-1}$. Then $\mathfrak{a}$ is an integral ideal in $\mathbb{Z}[\xi]$ where the action of ξ on the $\mathbb{Z}$-module $\mathfrak{a}$ is given by Y. This means that $\xi\alpha_i=\sum_{j=1}^{p-1}y_{ij}\alpha_j$ where $(y_{ij})_{i,j=1,\dots,p-1}=Y$. Moreover, $\alpha_1,\dots,\alpha_{p-1}$ are independent over $\mathbb{Z}$. Let $\gamma_j\in\mathrm{Gal}(\mathbb{Q}(\xi),\mathbb{Q})$ with $\gamma_j(\xi)=\xi^j$, $j=1,\dots,p-1$, be an element of the Galois group. Then $v_j=(\gamma_j(\alpha_1),\dots,\gamma_j(\alpha_{p-1}))^{\mathrm{T}}$ is an eigenvector to the eigenvalue ξ^j. The eigenvectors $v_1,\dots,v_{p-1}$ are linearly independent over $\mathbb{Z}$ and by this the $\alpha_1,\dots,\alpha_{p-1}$ are independent over $\mathbb{Z}$. Now let $a=D^{-1}v_1^{\mathrm{T}}J\overline{v}_1$ where $D=p\xi^{(p+1)/2}/(\xi-1)$, $D=-\overline{D}$. Then Sjerve and Yang showed that $(\mathfrak{a},a)$ is a pair with $\mathfrak{a}\overline{\mathfrak{a}}=(a)$. Following the same procedure, we can find for a given matrix $Y_p\in\mathrm{Sp}(p-1,\mathbb{Z}[1/p])$ an ideal $\mathfrak{a}_p\subseteq\mathbb{Z}[1/p][\xi]$ such that $\mathfrak{a}_p\overline{\mathfrak{a}}_p=(a)$.
In Lemma 2.13 we showed that for $j=1,\dots,(p-1)/2$ the sign of the invariant subspaces V_j corresponding to the eigenvalues ξ^j, ξ^{-j} is

$$\mathrm{sign}(V_j)=\mathrm{sign}(\mathrm{Im}\langle v_j,v_{p-j}\rangle)=\mathrm{sign}(-i\langle v_j,v_{p-j}\rangle)$$

where v_j is the eigenvector corresponding to the eigenvalue ξ^j. We get by the definition

$$\mathrm{sign}(-i\langle v_j,v_{p-j}\rangle)=\mathrm{sign}(-i\gamma_j(Da))$$

where the sign of $z\in\mathbb{Z}[\xi+\overline{\xi}]$ is the sign of $\iota(z)$ for the real embedding ι of $\mathbb{Z}[\xi+\overline{\xi}]$ with $\iota(\xi+\overline{\xi})=e^{i2\pi/p}+e^{-i2\pi/p}$. Now we see that ψ is surjective if and only if

$$\psi'':\{a\in\mathbb{Z}[\xi]\mid\exists\mathfrak{a}\text{ with }(\mathfrak{a},a)\in P\}\longrightarrow(\mathbb{Z}/2\mathbb{Z})^{(p-1)/2}$$

with

$$a\longmapsto(\psi'(\gamma_1(a)),\dots,\psi'(\gamma_{(p-1)/2}(a)))$$

is surjective. Because of a remark in the article of Alexander, Conner, Hamrick and Vick [1],

$$\psi''_p:\{a\in\mathbb{Z}[1/p][\xi]\mid\exists\mathfrak{a}\text{ with }(\mathfrak{a},a)\in P_p\}\longrightarrow(\mathbb{Z}/2\mathbb{Z})^{(p-1)/2}$$

with

$$a \longmapsto (\psi'(\gamma_1(a)), \ldots, \psi'(\gamma_{(p-1)/2}(a)))$$

is surjective. With the same procedure as for $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$, we can define V_j, $\mathrm{sign}(V_j)$, $j = 1, \ldots, (p-1)/2$, for $Y_p \in \mathrm{Sp}(p-1, \mathbb{Z}[1/p])$, and we get the statement of Proposition 2.15 and Lemma 2.13 for matrices of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/p])$. Then we see that

$$\psi_p : \mathcal{M}_p \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{(p-1)/2}$$

is surjective and therefore

$$\psi : \mathcal{M} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{(p-1)/2}$$

is surjective too. Herewith we have finished the proof of Theorem 2.9.

2.4.4 An interesting remark

We have seen in the proof of Theorem 2.9 that a bijection exists between the conjugacy classes of matrices of odd prime order p in $\mathrm{Sp}(p-1, \mathbb{Z})$ and the equivalence classes $[\mathfrak{a}, a] \in \mathcal{P}$ where $\mathfrak{a} \subseteq \mathbb{Z}[\xi]$ is an ideal such that $\mathfrak{a}\overline{\mathfrak{a}} = (a)$ for an $a \in \mathbb{Z}[\xi + \overline{\xi}]$. Let $(\mathfrak{a}, a)$ be a representative of such a class and let $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$ be a representative of the conjugacy class corresponding to $[\mathfrak{a}, a]$. Let $v_1 = (\alpha_1, \ldots, \alpha_{p-1})^{\mathrm{T}}$ be an eigenvector of Y corresponding to the eigenvalue ξ. Then we already know that $\alpha_1, \ldots, \alpha_{p-1}$ form a $\mathbb{Z}$-basis of $\mathfrak{a}$ and $a = D^{-1} v_1^{\mathrm{T}} J \overline{v}_1$ where $D = p\xi^{(p+1)/2}/(\xi - 1)$, $D = -\overline{D}$. Let V_j be the invariant subspace corresponding to the eigenvalues ξ^j and ξ^{-j}. We have already seen that $\mathrm{sign}(V_j) = \mathrm{sign}(-i\gamma_j(Da))$ where the sign of $z \in \mathbb{Z}[\xi + \overline{\xi}]$ is the sign of $\iota(z)$ for a real embedding ι of $\mathbb{Z}[\xi + \overline{\xi}]$. Let U be the group of units in $\mathbb{Z}[\xi]$ and $U^+ = \{u \in U \mid u = \overline{u}\}$. Let $u \in U^+ \setminus N(U)$ where N is the norm map. Then $[\mathfrak{a}, ua] \in \mathcal{P}$ and $[\mathfrak{a}, a] \neq [\mathfrak{a}, ua]$. Let Y_u be a representative of the conjugacy class of matrices corresponding to $[\mathfrak{a}, ua]$. We denote by $\mathrm{sign}_u(V_j)$ the sign of the invariant subspace V_j of Y_u corresponding to the eigenvalues ξ^j and ξ^{-j}. Then

$$\begin{aligned}\mathrm{sign}_u(V_j) &= \mathrm{sign}(-i\gamma_j(Dua)) \\ &= \mathrm{sign}(\gamma_j(u))\,\mathrm{sign}(-i\gamma_j(Da)).\end{aligned}$$

We define ψ'' as in the proof of Theorem 2.9. If

$$\begin{array}{rccl}\psi''' : & U^+ & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^{(p-1)/2} \\ & u & \longmapsto & (\mathrm{sign}(\gamma_1(u)), \ldots, \mathrm{sign}(\gamma_{(p-1)/2}(u)))\end{array}$$

is surjective, then ψ'' is surjective. But ψ''' is not surjective for each prime. Let h and h^+ be the class numbers of $\mathbb{Q}(\xi)$ and $\mathbb{Q}(\xi+\overline{\xi})$ respectively. Then $h^- = h/h^+$. Let C denote the group of cyclotomic units in $\mathbb{Q}(\xi)$ and let $C^+ = C \cap \mathbb{Z}[\xi+\overline{\xi}]$. It is known that $[\mathbb{Z}[\xi+\overline{\xi}]^* : C^+] = h^+$. We can find in the article of Garbanati [6] that h^- is odd if and only if C^+ contains units of all signatures, which means that every totally positive unit in C^+ is the square of a unit of C. So in case h^- is odd, we have surjectivity. However it may be possible that $\mathbb{Z}[\xi+\overline{\xi}]^*$ contains units of all signatures even if C^+ does not. This can only happen if h^+ is even and then we do not know if ψ''' is surjective. If h^- is even and h^+ is odd, we have no surjectivity. This happens for example for the primes 29 and 113. The case where h^- is odd is very interesting because of the following proposition.

Proposition 2.16. *If the homomorphism*

$$\begin{array}{rccl} \psi''' : & U^+ & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^{(p-1)/2} \\ & u & \longmapsto & (\operatorname{sign}(\gamma_1(u)), \ldots, \operatorname{sign}(\gamma_{(p-1)/2}(u))) \end{array}$$

is surjective, each $X \in \mathrm{U}((p-1)/2)$ for which $\phi(X) \in \mathrm{Sp}(p-1,\mathbb{R})$ is conjugate to a matrix $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ yields h^- conjugacy classes in $\mathrm{Sp}(p-1,\mathbb{Z})$.

Proof. In the preceding discussion we have already seen that a bijection exists between conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$ and the elements $[\mathfrak{a}, a] \in \mathcal{P}$. Let $u_1, u_2 \in U^+$ with $u_1 N(U) \neq u_2 N(U)$. Then, if $[\mathfrak{a}, a] \in \mathcal{P}$, we have $[\mathfrak{a}, u_1 a] \neq [\mathfrak{a}, u_2 a] \in \mathcal{P}$. If ψ''' is surjective, we get for each class $uN(U)$ a matrix Y_u with a different combination of signs. Herewith there exists for each $\mathfrak{a}$ for which $a \in \mathbb{Z}[\xi+\overline{\xi}]$ exists with $[\mathfrak{a}, a] \in \mathcal{P}$ a bijection between the matrices $X \in \mathrm{U}((p-1)/2)$ that satisfy the conditions stated in Theorem 2.9 and the equivalence classes $[\mathfrak{a}, ua]$ where $u \in U^+$ is a representative of the class $uN(U) \in U^+/N(U)$. Since h^- ideals $\mathfrak{a}$ exist with $[\mathfrak{a}, a] \in \mathcal{P}$, we can choose for each $X \in \mathrm{U}((p-1)/2)$ the matrix $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ with $\phi(X) \in \mathrm{Sp}(p-1,\mathbb{R})$ conjugate to Y in h^- different conjugacy classes. □

2.5 Conjugacy classes of subgroups of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$

We have shown that a surjection exists that maps the conjugacy classes of matrices $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ of odd prime order p onto the conjugacy classes of matrices X in $\mathrm{U}((p-1)/2)$ that satisfy

$$\left\{\lambda_1, \ldots, \lambda_{(p-1)/2}, \overline{\lambda}_1, \ldots, \overline{\lambda}_{(p-1)/2}\right\} = \left\{e^{i2\pi/p}, \ldots, e^{i(p-1)2\pi/p}\right\}$$

where $\lambda_1,\dots,\lambda_{(p-1)/2}$ are the eigenvalues of X, and $\overline{\lambda}$ denotes the complex conjugate of λ. It is clear that $\det X = e^{l2\pi i/p}$ for some $1 \leqslant l \leqslant p$. If $X \in \mathrm{U}((p-1)/2)$ satisfies this condition on the eigenvalues, then so does X^k, $k = 1,\dots,p-1$. If $\det X \neq 1$, $\det X^k \neq \det X^l$ for any $k \neq l$ with $k,l = 1,\dots,p$, and the X^k are in different conjugacy classes. If $\det X = e^{l2\pi i/p}$ for some $1 \leqslant l < p$, then

$$\left\{\det X,\dots,\det X^{p-1}\right\} = \left\{e^{i2\pi/p},\dots,e^{i(p-1)2\pi/p}\right\}.$$

If $\det X = 1$, it is possible that some k exists such that X and X^k are in the same conjugacy class. In this section we will analyse when and how many times this happens. The number of conjugacy classes of matrices $X \in \mathrm{U}((p-1)/2)$ that satisfy the necessary and sufficient condition is $2^{(p-1)/2}$. Herewith we will be able to compute the number of conjugacy classes of subgroups of matrices of order p in $\mathrm{U}((p-1)/2)$. We remember that the number of conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$ is $2^{(p-1)/2}h^-$. If $h^- = 1$, a bijection exists between the conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$ and the conjugacy classes of matrices of order p in $\mathrm{U}((p-1)/2)$ that satisfy the condition required in Theorem 2.9.

Let $X \in \mathrm{U}((p-1)/2)$ with $X^p = 1$, $X \neq 1$. Then X generates a subgroup S of order p in $\mathrm{U}((p-1)/2)$. If $\det X = 1$, it is possible that X is conjugate to $X' \in S$ with $X \neq X'$. Two matrices in $\mathrm{U}((p-1)/2)$ are conjugate to each other if and only if they have the same eigenvalues. The set of eigenvalues of X is

$$\left\{e^{ig_1 2\pi/p},\dots,e^{ig_{(p-1)/2}2\pi/p}\right\}$$

where $1 \leqslant g_l \leqslant p-1$ for $l = 1,\dots,\frac{p-1}{2}$ and

$$g_l \neq p - g_j, \qquad g_l \neq g_j$$

for all $l \neq j$ with $l,j = 1,\dots,(p-1)/2$. If we consider the g_j as elements of $(\mathbb{Z}/p\mathbb{Z})^*$, the condition on the g_j is equivalent to

$$g_l \neq -g_j, \qquad g_l \neq g_j$$

for all $l \neq j$ with $l,j = 1,\dots,(p-1)/2$. The matrix X is conjugate to X^κ for some κ if the eigenvalues of X and X^κ are the same. This is equivalent to

$$\{g_1,\dots,g_{(p-1)/2}\} = \{\kappa g_1,\dots,\kappa g_{(p-1)/2}\} \subset (\mathbb{Z}/p\mathbb{Z})^*$$

where g_j and κg_j, $j = 1,\dots,(p-1)/2$, denote the corresponding congruence classes. Now we introduce some notation that will be used in the whole section. Let

$$G := \{g_1,\dots,g_{(p-1)/2}\} \subset (\mathbb{Z}/p\mathbb{Z})^*,$$

then

$$\kappa G := \{\kappa g_1, \ldots, \kappa g_{(p-1)/2}\} \subset (\mathbb{Z}/p\mathbb{Z})^*$$

for some $\kappa \in (\mathbb{Z}/p\mathbb{Z})^*$. Let x be a generator of the multiplicative cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ and let K be a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ with $|K| = k$. Then K is cyclic and k divides $p-1$. Let $m := (p-1)/k$, then x^m generates K.
First we will prove the following proposition.

Proposition 2.17. *Let $G \subset (\mathbb{Z}/p\mathbb{Z})^*$ be a subset with $|G| = (p-1)/2$. Then the following are equivalent.*

i) For all $g_j, g_l \in G$ holds $g_j \neq -g_l$ and $\kappa \in (\mathbb{Z}/p\mathbb{Z})^*$ exists with $\kappa G = G$, $\kappa \neq 1$.

ii) An integer $h \in \mathbb{N}$, $1 \leqslant h \leqslant (p-1)/2$, and $n_j \in (\mathbb{Z}/p\mathbb{Z})^*$, $j = 1, \ldots, h$, exist with

$$G = \bigcup_{j=1}^{h} n_j K$$

where $n_j \notin K$ $\forall j = 2, \ldots, h$, and for all $\kappa' \in K$, $n_j \neq -n_l\kappa'$ $\forall n_j, n_l$ where $j, l = 1, \ldots, h$, and the order of the subgroup K generated by κ is odd.

Then we will analyse the uniqueness of this decomposition of G. This will enable us to determine the number of $G \subset (\mathbb{Z}/p\mathbb{Z})^*$ with $|G| = (p-1)/2$ and $G = \kappa G$ for some $1 \neq \kappa \in (\mathbb{Z}/p\mathbb{Z})^*$. Herewith we will determine the number of conjugacy classes of subgroups of order p in $\mathrm{U}((p-1)/2)$ whose group elements satisfy the necessary and sufficient condition.

Lemma 2.18. *Let $G \subset (\mathbb{Z}/p\mathbb{Z})^*$ with $|G| = (p-1)/2$. Then $1 \neq \kappa \in (\mathbb{Z}/p\mathbb{Z})^*$ exists with $\kappa G = G$ if and only if $1 \leqslant h \leqslant (p-1)/2$ and $n_j \in (\mathbb{Z}/p\mathbb{Z})^*$, $j = 1, \ldots, h$, exist with*

$$G = \bigcup_{j=1}^{h} n_j K$$

where $n_j \notin K$ for $j = 2, \ldots, h$, and K is the subgroup generated by κ.

Proof. $\underline{\Leftarrow}$: Let $\kappa^l \in K$. Then

$$\begin{aligned}\kappa^l G = \kappa^l \bigcup_{j=1}^{h} n_j K = \bigcup_{j=1}^{h} n_j \kappa^l K = \bigcup_{j=1}^{h} n_j K \\ = G.\end{aligned}$$

$\underline{\Rightarrow}$: Without loss of generality we assume that $1 \in G$. If $1 \notin G$, $\lambda \in (\mathbb{Z}/p\mathbb{Z})^*$ exists with $1 \in \lambda G$ because $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative group. Then we have

$$\kappa\lambda G = \lambda\kappa G = \lambda G.$$

Moreover, if we can decompose λG as required, this is also true for G. Indeed,

$$\lambda G = \bigcup_{j=1}^{h} n'_j K \quad \Rightarrow \quad G = \bigcup_{j=1}^{h} n_j K$$

where $n_j = \lambda^{-1} n'_j$, $j = 1, \ldots, h$. In fact $\lambda \notin K$ since if $\lambda \in K$, then $\lambda G = G$ and $1 \notin G$ would imply that $1 \notin \lambda G$.
We can show that $k = |K| \leqslant |G|$. Indeed, if $\kappa G = G$ and $1 \in G$, then $\kappa \in G$. Moreover, we have $\kappa^l \in K$ and $\kappa^l G = G$ for $l = 1, \ldots, k$. This shows that $K \subseteq G$ and $k = |K| \leqslant |G|$.
If $K = G$, we have finished the proof. If $K \subsetneq G$, we consider $G'_1 = G \setminus K$. We have $1 \notin G'_1$ because $1 \in K$. For all $\kappa^l \in K$ we have

$$\begin{aligned}\kappa^l G'_1 &= \kappa^l (G \setminus K) = \kappa^l G \setminus \kappa^l K = G \setminus K \\ &= G'_1.\end{aligned}$$

Now $\lambda_1 \in (\mathbb{Z}/p\mathbb{Z})^*$ exists with $1 \in \lambda_1 G'_1 =: G_1$. In the same way as we did it for G, we can show that $k = |K| \leqslant |G_1|$. Then we have $G = K \cup \lambda_1^{-1} G_1$. Now we make the same construction with G_1 instead of with G. We will have finished after $h := (p-1)/2k$ steps. Let $n_1 := 1$, $n_j := n_{j-1}\lambda_{j-1}^{-1}$ for $j = 2, \ldots, h$. Then

$$G = \bigcup_{j=1}^{h} n_j K.$$

□

Let $G = \{g_1, \ldots, g_{(p-1)/2}\} \subset (\mathbb{Z}/p\mathbb{Z})^*$ with $|G| = (p-1)/2$ and $\kappa G = G$ for some $\kappa \in (\mathbb{Z}/p\mathbb{Z})^*$ with $\kappa \neq 1$, $\kappa^k = 1$. The following lemma will give an answer to the question when G satisfies the conditions

$$g_l \neq g_j, \qquad g_l \neq -g_j$$

for all $j \neq l$ with $j, l = 1, \ldots, \frac{p-1}{2}$.

Lemma 2.19. *Let $G = \bigcup_{j=1}^{h} n_j K \subset (\mathbb{Z}/p\mathbb{Z})^*$ be defined as in Lemma 2.18. Then $g_j \neq -g_l$ for all $g_j, g_l \in G$ if and only if $\kappa^j \neq -\kappa^l$ for all $\kappa^j, \kappa^l \in K$ and $n_j \neq -n_l\kappa$ for all $j, l = 1, \ldots, h$ and for all $\kappa \in K$.*

Proof. $\underline{\Rightarrow}$: Suppose there exist $\kappa^j, \kappa^l \in K$ with $\kappa^j = -\kappa^l$. Then $n_1\kappa^j = -n_1\kappa^l$, and since $n_1\kappa^j, n_1\kappa^l \in G$ ($n_1K \subseteq G$), we have found $g_j := n_1\kappa^j \in G$ and $g_l := n_1\kappa^l \in G$ with $g_j = n_1\kappa^j = -n_1\kappa^l = -g_l$.
$\underline{\Leftarrow}$: Suppose $g_j, g_l \in G$ exist with $g_j = -g_l$. Let $g_j = n_j\kappa^j$, $g_l = n_l\kappa^l$. Then $n_j\kappa^j = -n_l\kappa^l$, and we have found $\kappa^{j-l} \in K$ with $n_l = -n_j\kappa^{j-l}$. □

The question, which now arises, is whether subgroups $K \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ exist that satisfy the condition $\kappa^j \neq -\kappa^l$ for all $\kappa^j, \kappa^l \in K$. To answer to this question, we first state a lemma.

Lemma 2.20. *Let x be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Then*

$$x^m + x^{m+(p-1)/2} = 0.$$

Proof. Since p is a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field and $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ contains the additive inverse of each of its elements. Therefore $x + x^2 + \cdots + x^{p-1} = 0$. A computation shows

$$x + x^2 + \cdots + x^{p-1} = \left(1 + x^{(p-1)/2}\right)\left(x + \cdots + x^{(p-1)/2}\right).$$

The order of $x^{(p-1)/2}$ is 2 since $x^{p-1} = 1$ and therefore $x^{(p-1)/2} = -1$. Now we get

$$x^m + x^{m+(p-1)/2} = x^m\left(1 + x^{(p-1)/2}\right) = 0.$$

□

Lemma 2.21. *Let $K \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ be a subgroup of order $(p-1)/m$. Let x be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ and x^m a generator of K. Then $\kappa^j \neq -\kappa^l$ for all $\kappa^j, \kappa^l \in K$ if and only if m does not divide $(p-1)/2$.*

Proof. Because of the statement of Lemma 2.20, a subgroup K exists that contains two elements κ^j, κ^l with $\kappa^j = -\kappa^l$ if and only if $m \in \mathbb{Z}$ exists with $x^m, x^{m+(p-1)/2} \in K$. Moreover, x^m generates K if $m = (p-1)/2k$. Then $x^{m+(p-1)/2} \in K$ if and only if $x^{(p-1)/2} \in K$. This happens if and only if m divides $(p-1)/2$. □

Proof of Proposition 2.17. We consider the divisors of $p-1$. Let $r \in \mathbb{Z}$ be maximal such that $2^r | p-1$. Then $r \geqslant 1$ since $2|p-1$. We define y such that $p-1 = 2^r y$. Then $2^{r-1}y = (p-1)/2$. Now it is clear that $m|p-1$ and $m \nmid (p-1)/2$ if and only if $m = 2^r y'$ where $y'|y$. This happens if and only if $k = (p-1)/m$ is odd. Herewith we see that a subgroup K decomposes a set G as required in Lemma 2.19 if and only if the order of K is odd. We can show that $|K| = (p-1)/m$ divides $(p-1)/2$. Indeed,

$$\frac{p-1}{2}\left(\frac{p-1}{m}\right)^{-1} = \frac{m}{2} = \frac{2^r y'}{2} = 2^{r-1}y' \in \mathbb{Z}$$

since $r \geqslant 1$. With the preceding lemmas we have shown Proposition 2.17. □

We did not analyse the uniqueness of the decomposition

$$G = \bigcup_{j=1}^{h} n_j K$$

of the set G. It is evident that the n_j can be permuted and multiplied with any $\kappa^l \in K$, but we will see that K and h are not uniquely determined. The next lemma states that instead of K we could take any nontrivial subgroup of K.

Lemma 2.22. *Let $G = \bigcup_{j=1}^{h} n_j K \subset (\mathbb{Z}/p\mathbb{Z})^*$ be as in Proposition 2.17. Let $|K| = k$ be odd and not a prime. Let $K' \neq K$ be a nontrivial subgroup of K. Then $1 \leqslant h' \leqslant (p-1)/2$ and $n'_i \in (\mathbb{Z}/p\mathbb{Z})^*$, $i = 1, \dots, h'$, exist so that*

$$G = \bigcup_{i=1}^{h'} n'_i K'$$

where $n'_i \notin K'$ for $i = 2, \dots, h'$, and $n'_i \neq -n'_l \kappa'$ $\forall i, l = 1, \dots, h'$, $\forall \kappa' \in K'$.

Proof. We set $k' := |K'|$. Then k' divides k. Let x be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, $m := (p-1)/k$, $m' := (p-1)/k'$. Since $K' \subset K$, we get $k' < k$ and $m' > m$. Moreover, m divides m' because

$$\frac{m'}{m} = \frac{p-1}{k'} \frac{k}{p-1} = \frac{k}{k'} \in \mathbb{Z}.$$

Now we define l such that $m' = ml$. Then $k = k'l$. Because of the definitions, $h = (p-1)/2k = m/2$. Let $h' := m'/2$. Then $h' = hl$. It is easy to check that

$$K = \bigcup_{r=1}^{l} x^{rm} K',$$

but herewith we get

$$\begin{aligned} G &= \bigcup_{j=1}^{h} n_j K = \bigcup_{j=1}^{h} n_j \left(\bigcup_{r=1}^{l} x^{rm} K' \right) = \bigcup_{j=1}^{h} \bigcup_{r=1}^{l} n_j x^{rm} K' \\ &= \bigcup_{i=1}^{h'=hl} n'_i K'. \end{aligned}$$

The n'_i are all different since all the n_j and all the x^{rm} are different. Moreover, at most one $n'_i \in K'$, namely $n_1 x^{lm}$ if $n_1 \in K'$. For all $\kappa' \in K'$ holds $n'_l \neq -n'_i \kappa'$ $\forall n'_l, n'_i$ with $i, l = 1, \dots, h'$. ∎

Now we will consider for a given G the group K for which $|K|$ is maximal and allows the decomposition $G = \bigcup_{j=1}^{h} n_j K$.
Our next aim is to determine the number of sets G.

Lemma 2.23. *Let $K \subset (\mathbb{Z}/p\mathbb{Z})^*$ be a nontrivial subgroup of odd order k. Then there exist $2^{(p-1)/2k}$ different sets G with $|G| = (p-1)/2$ and*

$$G = \bigcup_{j=1}^{h} n_j K$$

where $h = \frac{p-1}{2k}$ and all the conditions of Proposition 2.17 are fulfilled.

Proof. Let $M \subset (\mathbb{Z}/p\mathbb{Z})^*$ be a subgroup of order $m := (p-1)/k$. Let x be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Then x^m and x^k generate K and M respectively. If k and m have no common divisors, then $K \cap M = \{1\}$ and

$$(\mathbb{Z}/p\mathbb{Z})^* = \{ab \mid a \in K,\ b \in M\}.$$

Since k divides $(p-1)/2$, it follows from $b \in M$ that $-b \in M$. If k and m have common divisors, then

$$(\mathbb{Z}/p\mathbb{Z})^* = \left\{ x^l a \,\middle|\, a \in K,\ l = 1, \ldots, m \right\}.$$

We get $x^{m(k-1)/2}K = K$ since $(x^m)^{(k-1)/2} \in K$ and herewith

$$x^l K = x^{l + m\frac{k-1}{2}} K.$$

Now we can write

$$\begin{aligned} (\mathbb{Z}/p\mathbb{Z})^* &= \left\{ x^l a,\ x^{l+\frac{m}{2}} a \,\middle|\, a \in K,\ l = 1, \ldots, m/2 \right\} \\ &= \left\{ x^l a,\ x^{l+\frac{m}{2}+\frac{m(k-1)}{2}} \,\middle|\, a \in K,\ l = 1, \ldots, m/2 \right\}, \end{aligned}$$

but

$$m\frac{k-1}{2} + \frac{m}{2} + l = \frac{mk}{2} + l = \frac{p-1}{2} + l,$$

and therefore

$$x^l = -x^{\frac{p-1}{2}+l} = -x^{m\frac{k-1}{2}+\frac{m}{2}+l}.$$

Herewith we can write

$$(\mathbb{Z}/p\mathbb{Z})^* = \left\{ x^l a,\ -x^l a \,\middle|\, a \in K,\ l = 1, \ldots, m/2 \right\},$$

which means that

$$(\mathbb{Z}/p\mathbb{Z})^* = \bigcup_{j=1}^{m} n_j K$$

where $\forall j = 1, \ldots, m$ exist $\kappa \in K$ and $1 \leqslant i \leqslant m$ such that $n_i = -\kappa n_j$. So for a given group K we can find $2^{(p-1)/2k} = 2^{m/2}$ sets G that fulfil the required conditions. $\square$

The evident question that arises is how many sets G with

$$G = \bigcup_{j=1}^{h} n_j K$$

cannot be written as

$$G = \bigcup_{i=1}^{h'} n_i' K'$$

where K' is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ with $K \subsetneq K'$. Let $\mathcal{N}_k$ be the number of such G.
To determine $\mathcal{N}_k$ we have to subtract the number $\mathcal{N}_{k'}$ from $2^{(p-1)/2k}$ for each odd $k' \neq k$ with $k|k'$, $k'|p-1$. The integer k' is the order of the group K' with $K \subset K'$. Therefore we get a recursive formula

$$\mathcal{N}_k = 2^{(p-1)/2k} - \sum_{\substack{k' \text{ odd},\ k'>k \\ k|k',\ k'|p-1}} \mathcal{N}_{k'}.$$

Let $y \in \mathbb{Z}$ be such that $p-1 = 2^r y$ and y is odd. Then

$$\mathcal{N}_y = 2^{(p-1)/2y} = 2^{2^{r-1}}$$

closes the formula.
Let $p-1 = 2^r p_1^{r_1} \dots p_l^{r_l}$ be a factorisation of $p-1$ into primes where $p_1, \dots, p_l$ are odd and $p_i \neq p_j$ $\forall i \neq j$ with $i, j = 1, \dots, l$. Since $p-1$ is even, $r \geqslant 1$. Let K be of order $k = p_1^{s_1} \dots p_l^{s_l}$ where $0 \leqslant s_j \leqslant r_j$ for $j = 1, \dots, l$. Let x be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Then K is generated by x^m, $m = 2^r p_1^{r_1-s_1} \dots p_l^{r_l-s_l}$. If $k' = p_1^{t_1} \dots p_l^{t_l}$ where $s_j \leqslant t_j \leqslant r_j$ for $j = 1, \dots, l$, then K is a proper subgroup of K' of order k' if $s_j < t_j$ for some $1 \leqslant j \leqslant l$. Herewith $-1 + \prod_{j=1}^{l}(r_j - s_j + 1)$ groups K' exist such that K is a proper subgroup of K'.
We will say that G is decomposed by K if

$$G = \bigcup_{j=1}^{h} n_j K$$

as in Proposition 2.17. Now the number of sets G that are decomposed by K and for which no $K' \supsetneq K$ exists such that G is decomposed by K' is

$$\mathcal{N}_k = 2^{(p-1)/2k} - \sum_{y \in T_k} \mathcal{N}_y$$

where

$$T_k := \{y \mid y \text{ odd},\ k|y,\ y \neq k \text{ and } y|p-1\}.$$

Now we have to determine the number of sets G that satisfy the conditions of Proposition 2.17. Let this be the number $\mathcal{N}_G$. One easily sees that

$$\mathcal{N}_G = \sum_{\substack{K\subset(\mathbb{Z}/p\mathbb{Z})^* \\ K\neq\{1\}, \\ |K| \text{ odd}}} \mathcal{N}_{|K|} = \sum_{\substack{k|p-1 \\ k\neq 1 \\ k \text{ odd}}} \mathcal{N}_k.$$

Now let $G \subset (\mathbb{Z}/p\mathbb{Z})^*$ with $|G| = (p-1)/2$, such that $\forall g_i, g_j \in G$, $g_i \neq -g_j$. Let $\mathcal{N}_1$ be the number of sets G for which no $\kappa \in (\mathbb{Z}/p\mathbb{Z})^*$, $\kappa \neq 1$, exists such that $\kappa G = G$. Then

$$\mathcal{N}_1 = 2^{(p-1)/2} - \mathcal{N}_G = 2^{(p-1)/2} - \sum_{\substack{1\neq k|\, p-1 \\ k \text{ odd}}} \mathcal{N}_k.$$

This formula shows that $\mathcal{N}_1$ is not a special case but simply $\mathcal{N}_k$ for $k = 1$.

Definition. Let $G \subset (\mathbb{Z}/p\mathbb{Z})^*$ with $|G| = (p-1)/2$ and $g_i \neq -g_j$ for all $g_i, g_j \in G$. We define the multiplicity $\mathcal{V}_G$ of G to be the number of $\kappa \in (\mathbb{Z}/p\mathbb{Z})^*$ with $\kappa G = G$. This is the order of the group K with $|K|$ maximal and $\kappa G = G$ for all $\kappa \in K$.

It follows from the definitions that $\mathcal{V}_G = k$ and that the number of G with $\mathcal{V}_G = k$ is $\mathcal{N}_k$. It is possible that $\mathcal{V}_G = 1$.

Lemma 2.24. *Let G be as in Proposition 2.17 with multiplicity $\mathcal{V}_G = k$. Then each lG, $l \in (\mathbb{Z}/p\mathbb{Z})^*$, has also multiplicity $\mathcal{V}_{lG} = k$.*

Proof. Let k' be the multiplicity of lG. Let K be the subgroup of order k with $\kappa G = G$ for all $\kappa \in K$. We have

$$\kappa l G = l\kappa G = lG \quad \forall l \in (\mathbb{Z}/p\mathbb{Z})^*.$$

Therefore $K' \supseteq K$ where $K' \subset (\mathbb{Z}/p\mathbb{Z})^*$ is a subgroup of order k'. This means that $k' \geqslant k$. Let $\kappa' \in K' \setminus K$. Then $\kappa' lG = lG$ and $\kappa' lG = l\kappa' G$ imply that $\kappa' G = G$. This is a contradiction, and therefore $\kappa' \in K$. $\square$

We will consider each set G as the set of eigenvalues of a matrix in $\mathrm{U}((p-1)/2)$ that satisfies the necessary and sufficient condition.

Definition. We define a matrix $X_G \in \mathrm{U}\big(\frac{p-1}{2}\big)$ with the eigenvalues

$$\big\{e^{ig_1 2\pi/p}, \ldots, e^{ig_{(p-1)/2} 2\pi/p}\big\}$$

where $G = \{g_1, \ldots, g_{(p-1)/2}\} \subset (\mathbb{Z}/p\mathbb{Z})^*$. We used the same notation for the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ and their representatives in $\mathbb{Z}$.

Let G have the multiplicity k. Then G yields k elements of the group generated by X_G. Now we are convinced of the fact that the following proposition is true.

Proposition 2.25. *The number of conjugacy classes of subgroups of order p in $\mathrm{U}((p-1)/2)$ whose group elements satisfy the necessary and sufficient condition is*

$$\mathcal{K}(p) = \frac{1}{p-1} \sum_{\substack{k \text{ odd} \\ k|p-1}} k\mathcal{N}_k.$$

We cannot simplify the formulas for $\mathcal{K}(p)$ and $\mathcal{N}_k$, but a special case appears.

Lemma 2.26. *Let $p-1 = 2^r y$ where y is odd. Let p_1 be an odd prime with $p_1|y$. Let s be maximal such that $p_1^s|y$. Let $k := y/p_1^t$ with $0 < t < s$. Then we get*

$$\mathcal{N}_k = 2^{2^{r-1}p_1^t} - 2^{2^{r-1}p_1^{t-1}}.$$

Proof. We know that $\frac{p-1}{2k} = 2^{r-1}p_1^t$. Therefore

$$\begin{aligned}
\mathcal{N}_k &= 2^{\frac{p-1}{2k}} - \mathcal{N}_{kp_1} - \cdots - \mathcal{N}_{kp_1^t} \\
&= 2^{\frac{p-1}{2k}} - \left(2^{\frac{p-1}{2kp_1}} - \sum_{i=2}^{t} \mathcal{N}_{kp_1^i} \right) - \sum_{i=2}^{t} \mathcal{N}_{kp_1^i} \\
&= 2^{\frac{p-1}{2k}} - 2^{\frac{p-1}{2kp_1}} \\
&= 2^{2^{r-1}p_1^t} - 2^{2^{r-1}p_1^{t-1}}.
\end{aligned}$$

□

Now we consider the case $p-1 = 2^r p_1^s$. Then p_1^t, $t = 1, \dots, s$, are odd divisors of $p-1$. Then Lemma 2.26 yields

$$\begin{aligned}
\mathcal{N}_{p_1^s} &= 2^{2^{r-1}} \\
\mathcal{N}_{p_1^{s-t}} &= 2^{2^{r-1}p_1^t} - 2^{2^{r-1}p_1^{t-1}}
\end{aligned}$$

and

$$\begin{aligned}
\mathcal{K}(p) &= \frac{1}{p-1} \sum_{t=0}^{s} p_1^{s-t} \mathcal{N}_{p_1^{s-t}} \\
&= \frac{1}{p-1} \left(p_1^s 2^{2^{r-1}} + \sum_{t=1}^{s} p_1^{s-t} \left(2^{2^{r-1}p_1^t} - 2^{2^{r-1}p_1^{t-1}} \right) \right) \\
&= \dots \\
&= \frac{1}{p-1} \left(2^{2^{r-1}p_1^s} + \sum_{t=1}^{s} \left(p_1^t - p_1^{t-1} \right) 2^{2^{r-1}p_1^{s-t}} \right).
\end{aligned}$$

Chapter 3

Symplectic characteristic classes

3.1 Introduction

It is well-known that

$$\mathrm{H}^*(B\mathrm{U}(n), \mathbb{Z}) = \mathbb{Z}[c_1, \ldots, c_n]$$

where the $c_j \in \mathrm{H}^{2j}(B\mathrm{U}(n), \mathbb{Z})$, $j = 1, \ldots, n$, are the universal Chern classes. Moreover,

$$\mathrm{H}^*(B\mathrm{Sp}(2n, \mathbb{R}), \mathbb{Z}) = \mathbb{Z}[d_1, \ldots, d_n]$$

where the $d_j \in \mathrm{H}^{2j}(B\mathrm{Sp}(2n, \mathbb{R}), \mathbb{Z})$, $j = 1, \ldots, n$, are the symplectic classes. The previously defined homomorphism $\phi : \mathrm{U}(n) \to \mathrm{Sp}(2n, \mathbb{R})$ is injective and induces

$$\mathrm{H}^*(B\mathrm{Sp}(2n, \mathbb{R}), \mathbb{Z}) \xrightarrow{\cong} \mathrm{H}^*(B\mathrm{U}(n), \mathbb{Z})$$

such that the d_j's map to the c_j's. Now let

$$\begin{array}{rccc} \rho : & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathrm{Sp}(2n, \mathbb{Z}), \\ \widetilde{\rho} : & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathrm{U}(n) \end{array}$$

be representations of $\mathbb{Z}/p\mathbb{Z}$. They induce homomorphisms

$$\begin{array}{rccc} \rho^* : & \mathrm{H}^*(\mathrm{Sp}(2n, \mathbb{Z}), \mathbb{Z}) & \longrightarrow & \mathrm{H}^*(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}), \\ \widetilde{\rho}^* : & \mathrm{H}^*(B\mathrm{U}(n), \mathbb{Z}) & \longrightarrow & \mathrm{H}^*(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}) \end{array}$$

since $\mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Sp}(2n, \mathbb{Z})$ are discrete groups. Moreover, using the restriction

$$\begin{array}{rccc} \mathrm{res} : & \mathrm{H}^{2j}(B\mathrm{Sp}(2n, \mathbb{R}), \mathbb{Z}) & \longrightarrow & \mathrm{H}^{2j}(\mathrm{Sp}(2n, \mathbb{Z}), \mathbb{Z}) \\ & d_j = d_j(\mathbb{R}) & \longmapsto & d_j(\mathbb{Z}), \end{array}$$

we define $d_j(\rho) := \rho^* d_j(\mathbb{Z})$, the symplectic class of the representation ρ. Note that, strictly speaking, the class $d_j(\mathbb{Z}) \in \mathrm{H}^{2j}(\mathrm{Sp}(2n, \mathbb{Z}), \mathbb{Z})$ depends also on n;

but it is well-known that $\mathrm{H}^{2j}(\mathrm{Sp}(2n,\mathbb{Z}),\mathbb{Z})$ is independent of n for $n \gg j$. Any representation $\widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{U}(n)$ induces a representation

$$\phi \circ \widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Sp}(2n,\mathbb{R}).$$

Since ϕ is injective, we can consider any representation in $\mathrm{U}(n)$ as a representation in $\mathrm{Sp}(2n,\mathbb{R})$. We say that the representation $\widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{U}(n)$ factors through $\mathrm{Sp}(2n,\mathbb{Z})$ if

$$\mathbb{Z}/p\mathbb{Z} \xrightarrow{\ \widetilde{\rho}\ } \mathrm{U}(n) \xrightarrow{\ \phi\ } \mathrm{Sp}(2n,\mathbb{R})$$

has the property that the image $\phi(\widetilde{\rho}(x))$ of any $x \in \mathbb{Z}/p\mathbb{Z}$ is conjugate to an element in $\mathrm{Sp}(2n,\mathbb{Z})$. Then $d_j(\rho) = \widetilde{\rho}^* c_j$.
Each representation $\widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{U}(n)$ can be written as a direct sum of 1-dimensional representations:

$$\widetilde{\rho} = \bigoplus_{j=0}^{p-1} m_j \widetilde{\rho}_j : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{U}(n)$$

where

$$\begin{array}{rccc} \widetilde{\rho}_j : & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathrm{U}(1) \\ & x & \longmapsto & e^{j\,2\pi i/p}, \end{array}$$

m_j is the multiplicity and x is a generator of $\mathbb{Z}/p\mathbb{Z}$. Let $\widetilde{\rho} : G \to \mathrm{U}(n)$ be a representation of a discrete group G. Then $\widetilde{\rho}$ induces

$$\begin{array}{rcccl} \widetilde{\rho}^* : & \mathrm{H}^*(B\mathrm{U}(n),\mathbb{Z}) & \longrightarrow & \mathrm{H}^*(G,\mathbb{Z}) & \\ & c_j & \longmapsto & \widetilde{\rho}^*(c_j) & =: c_j(\widetilde{\rho}). \end{array}$$

We define the total Chern class of the representation $\widetilde{\rho}$ to be

$$c(\widetilde{\rho}) := 1 + c_1(\widetilde{\rho}) + c_2(\widetilde{\rho}) + \cdots + c_n(\widetilde{\rho}).$$

It has the well-known properties $c(\rho \oplus \sigma) = c(\rho)c(\sigma)$, $c(m\rho) = c(\rho)^m$ where ρ and σ are two representations of G. Herewith we get

$$\begin{aligned} c(\widetilde{\rho}) &= c\left(\bigoplus_{j=0}^{p-1} m_j \widetilde{\rho}_j\right) = \prod_{j=0}^{p-1} c(\widetilde{\rho}_j)^{m_j} \\ &= \prod_{j \in \mathbb{Z}/p\mathbb{Z}} (1 + jx)^{m_j} \in \mathrm{H}^*(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}) \end{aligned}$$

where $x = c_1(\widetilde{\rho}_1) \in \mathrm{H}^2(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ is a generator.

3.2 On the characteristic classes of symplectic representations of $\mathbb{Z}/p\mathbb{Z}$

We are going to show that for each $n = 1, \dots, p-1$ we can find a representation $\widetilde{\rho} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{U}((p-1)/2)$ that factors through $\mathrm{Sp}(p-1, \mathbb{Z})$ and for which the universal Chern class $c_n(\widetilde{\rho}) \neq 0$. Thus $\widetilde{\rho}^*(c_n) = d_n(\rho) \neq 0$ where $\rho : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1, \mathbb{Z})$ is the representation corresponding to $\widetilde{\rho}$. The representation $\widetilde{\rho}$ factors through $\mathrm{Sp}(p-1, \mathbb{Z})$ if the image $\widetilde{\rho}(x)$ of a generator $x \in \mathbb{Z}/p\mathbb{Z}$ satisfies the necessary and sufficient condition stated in Theorem 2.9. Let $\mathcal{U}$ be the set of subsets $\mathcal{I} \subset (\mathbb{Z}/p\mathbb{Z})^*$ with $|\mathcal{I}| = (p-1)/2$, and $j \in \mathcal{I}$ implies $p - j \notin \mathcal{I}$. The number of elements in $\mathcal{U}$ is $2^{(p-1)/2}$. We always assume the elements $j \in \mathcal{I}$ to be represented by integers j with $1 \leqslant j < p$. Note that we will use the same notation for the elements of $\mathcal{I}$ and their representatives. We define

$$\widetilde{\rho}_{\mathcal{I}} = \bigoplus_{j \in \mathcal{I}} \widetilde{\rho}_j$$

where $\widetilde{\rho}_j$ is defined as above. The total Chern class of this representation is

$$c(\widetilde{\rho}_{\mathcal{I}}) = \prod_{j \in \mathcal{I}} \bigl(1 + jx\bigr).$$

For a given $\mathcal{I}$ we define

$$-\mathcal{I} := \{p - j \mid j \in \mathcal{I}\} \in \mathcal{U}.$$

Then $\mathcal{I} \cup -\mathcal{I} = (\mathbb{Z}/p\mathbb{Z})^*$ and

$$\begin{aligned}
c(\widetilde{\rho}_{\mathcal{I}})c(\widetilde{\rho}_{-\mathcal{I}}) &= \prod_{j \in \mathcal{I}} (1 + jx)\bigl(1 + (p-j)x\bigr) \\
&= \prod_{k \in (\mathbb{Z}/p\mathbb{Z})^*} (1 + kx) = \prod_{k \in (\mathbb{Z}/p\mathbb{Z})^*} k \left(\frac{1}{k} + x\right) \\
&= \prod_{k \in (\mathbb{Z}/p\mathbb{Z})^*} k \prod_{k \in (\mathbb{Z}/p\mathbb{Z})^*} (k + x) = - \prod_{k \in (\mathbb{Z}/p\mathbb{Z})^*} (k + x) \\
&= 1 - x^{p-1}.
\end{aligned}$$

Lemma 3.1. *Let $\mathcal{I} \in \mathcal{U}$. Then*

$$c(\widetilde{\rho}_{\mathcal{I}}) = \sum_{n=0}^{(p-1)/2} a_n x^n \quad \Rightarrow \quad c(\widetilde{\rho}_{-\mathcal{I}}) = \sum_{n=0}^{(p-1)/2} (-1)^n a_n x^n$$

where $a_0 := 1$ and $a_n = \displaystyle\sum_{J \subseteq \mathcal{I},\ |J| = n} \prod_{j \in J} j$.

Proof. This is obvious because

$$c(\widetilde{\rho}_{\mathcal{I}}) = \prod_{j\in\mathcal{I}} \bigl(1+jx\bigr) = 1 + \sum_{n=1}^{(p-1)/2} \left(x^n \sum_{J\subseteq\mathcal{I},\ |J|=n} \ \prod_{j\in J} j \right)$$

and

$$c(\widetilde{\rho}_{-\mathcal{I}}) = \prod_{j\in\mathcal{I}} \bigl(1-jx\bigr) = 1 + \sum_{n=1}^{(p-1)/2} \left((-1)^n x^n \sum_{J\subseteq\mathcal{I},\ |J|=n} \ \prod_{j\in J} j \right).$$

$\square$

Theorem 3.2. *For an odd prime p let $\mathcal{I}\subset(\mathbb{Z}/p\mathbb{Z})^*$ with $|\mathcal{I}|=(p-1)/2$, and $j\in\mathcal{I}$ implies $p-j\notin\mathcal{I}$. Let a representative of $j\in\mathcal{I}$ be an integer j with $1\leqslant j<p$. We define the representation*

$$\widetilde{\rho}_{\mathcal{I}} := \bigoplus_{j\in\mathcal{I}} \widetilde{\rho}_j : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{U}\left(\frac{p-1}{2}\right)$$

with

$$\begin{array}{rccc} \widetilde{\rho}_j : & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathrm{U}(1) \\ & z & \longmapsto & e^{j\,2\pi i/p} \end{array}$$

for a generator z of $\mathbb{Z}/p\mathbb{Z}$. Then for any integer $n=1,\dots,(p-1)/2$ the subset $\mathcal{I}$ can be chosen such that the nth Chern class $c_n(\widetilde{\rho}_{\mathcal{I}})$ is not zero.

Proof. Let $x := c_1(\widetilde{\rho}_1)$; then the nth Chern class $c_n(\widetilde{\rho}_{\mathcal{I}})$ is not zero if and only if the coefficient of x^n in the total Chern class

$$c(\widetilde{\rho}_{\mathcal{I}}) = \prod_{j\in\mathcal{I}} c(\widetilde{\rho}_j) = \prod_{j\in\mathcal{I}} \bigl(1+jx\bigr)$$

is not zero. Let $\mathcal{I} := \{j_1,\dots,j_{(p-1)/2}\}\in\mathcal{U}$; then we denote by $\mathcal{I}_l\in\mathcal{U}$ the set

$$\mathcal{I}_l := \{j_1,\dots,j_{l-1},-j_l,j_{l+1},\dots,j_{(p-1)/2}\}.$$

We assume that $1\leqslant n\leqslant(p-1)/2$ exists such that for each set $\mathcal{I}\in\mathcal{U}$ the coefficient a_n of x^n in $c(\widetilde{\rho}_{\mathcal{I}})$ is zero. It is impossible that $n=(p-1)/2$ because

$$a_{(p-1)/2} = \prod_{j\in\mathcal{I}} j \neq 0.$$

Now let $n\neq 0$, $n\neq(p-1)/2$; then we define for any $l=1,\dots,(p-1)/2$

$$b_n^l := \sum_{\substack{J\subseteq\mathcal{I}\setminus\{j_l\}\\ |J|=n}} \ \prod_{j\in J} j, \qquad b_0^l := 1.$$

Now let

$$c(\widetilde{\rho}_{\mathcal{I}}) := \sum_{n=0}^{(p-1)/2} a_n x^n;$$

then $a_n = b_n^l + j_l b_{n-1}^l$. Because of our assumption, the coefficients of x^n in $c(\widetilde{\rho}_{\mathcal{I}})$ and in $c(\widetilde{\rho}_{\mathcal{I}_l})$ are $b_n^l + j_l b_{n-1}^l = 0$ and $b_n^l - j_l b_{n-1}^l = 0$ respectively. This implies that $b_n^l = 0$, $b_{n-1}^l = 0$ and

$$\begin{aligned} a_{n+1} &= \sum_{\substack{J \subseteq \mathcal{I} \\ |J|=n+1}} \prod_{j \in J} j \\ &= \frac{1}{n+1} \sum_{j_l \in \mathcal{I}} \Big(j_l \sum_{\substack{J \subseteq \mathcal{I} \setminus \{j_l\} \\ |J|=n}} \prod_{j \in J} j \Big) = \frac{1}{n+1} \sum_{j_l \in \mathcal{I}} j_l \, b_n^l = 0. \end{aligned}$$

The factor $1/(n+1)$ appears because in the second line we have $n+1$ times each term appearing in the sum of the first line. Therefore $a_{n+1} = 0$ for each set $\mathcal{I} \in \mathcal{U}$, and by induction we get $a_{(p-1)/2} = 0$ for each set $\mathcal{I} \in \mathcal{U}$, which is impossible. □

Let $\mathrm{Sp}(\mathbb{Z}) = \bigcup_{n \geqslant 1} \mathrm{Sp}(2n, \mathbb{Z})$.

Theorem 3.3. *For every $j \geqslant 1$, $d_j(\mathbb{Z}) \in \mathrm{H}^{2j}(\mathrm{Sp}(\mathbb{Z}), \mathbb{Z})$ has infinite order.*

Proof. This theorem is a corollary of Theorem 3.2. It is well-known that for $p \gg j$

$$\mathrm{H}^{2j}(\mathrm{Sp}(\mathbb{Z}), \mathbb{Z}) \xrightarrow{\cong} \mathrm{H}^{2j}(\mathrm{Sp}(p-1, \mathbb{Z}), \mathbb{Z}).$$

In Theorem 3.2 we have shown that for any odd prime p and any integer $n = 1, \ldots, (p-1)/2$ a representation $\widetilde{\rho}_{\mathcal{I}} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{U}((p-1)/2)$ exists that factors through $\mathrm{Sp}(p-1, \mathbb{Z})$ and for which the nth Chern class $c_n(\widetilde{\rho}_{\mathcal{I}})$ is not zero. Then the nth symplectic class $d_n(\rho_{\mathcal{I}})$ is not zero, too. Here the representation $\rho_{\mathcal{I}} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Sp}(p-1, \mathbb{Z})$ is the one corresponding to $\widetilde{\rho}_{\mathcal{I}}$. We have an induced homomorphism

$$\begin{array}{rccc} \rho_{\mathcal{I}}^* : & \mathrm{H}^{2j}(\mathrm{Sp}(p-1, \mathbb{Z}), \mathbb{Z}) & \longrightarrow & \mathrm{H}^{2j}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}) \\ & d_j(\mathbb{Z}) & \longmapsto & d_j(\rho_{\mathcal{I}}). \end{array}$$

Herewith for any p the class $d_j(\mathbb{Z}) \in \mathrm{H}^{2j}(\mathrm{Sp}(p-1, \mathbb{Z}), \mathbb{Z})$ is not zero and has either infinite order or finite order divisible by p, since it restricts non-trivially to $\mathrm{H}^{2j}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z})$. This shows that $d_j(\mathbb{Z}) \in \mathrm{H}^{2j}(\mathrm{Sp}(\mathbb{Z}), \mathbb{Z})$ has infinite order. □

Chapter 4

The Farrell cohomology of $\mathrm{Sp}(p-1,\mathbb{Z})$

4.1 An introduction to Farrell cohomology

We will give a short introduction to the Farrell cohomology theory. More details and the proofs can be found in the book of Brown [4].
We say that a group G is virtually torsion-free if G has a torsion-free subgroup of finite index. All such subgroups have the same cohomological dimension, which is called the virtual cohomological dimension of G and denoted by $\operatorname{vcd} G$. If G is finite, $\operatorname{vcd} G = 0$. A complete resolution for G is an acyclic chain complex F of projective $\mathbb{Z}G$-modules together with an ordinary projective resolution $\varepsilon : P \to \mathbb{Z}$ over $\mathbb{Z}G$ such that F and P coincide in sufficiently high dimensions. Such a complete resolution (F, P, ε) exists for groups G with $\operatorname{vcd} G < \infty$. We can even choose (F, P, ε) such that F and P coincide in dimensions $\geqslant \operatorname{vcd} G$. In what follows, we always assume that $\operatorname{vcd} G < \infty$. It is well-known that the groups $\mathrm{Sp}(2n,\mathbb{Z})$ have finite vcd.
Let (F, P, ε) be a complete resolution for G and let M be a $\mathbb{Z}G$-module. We define

$$\widehat{\mathrm{H}}^*(G, M) = \mathrm{H}^*(\mathrm{Hom}_G(F, M))$$

to be the Farrell cohomology of G with coefficients in M. If G is finite, the Farrell cohomology and the Tate cohomology of G coincide.

Definition. An elementary abelian p-group of rank $r \geqslant 0$ is a group that is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$.

It is well-known that $\widehat{\mathrm{H}}^i(G,\mathbb{Z})$ is a torsion group for every $i \in \mathbb{Z}$. We write $\widehat{\mathrm{H}}^i(G,\mathbb{Z})_{(p)}$ for the p-primary part of this torsion group, i.e. the subgroup of elements of order some power of p.

We will use the following theorem.

Theorem 4.1. *Let G be a group such that $\operatorname{vcd} G < \infty$ and let p be a prime. Suppose that every elementary abelian p-subgroup of G has rank $\leqslant 1$. Then*

$$\widehat{\mathrm{H}}^*(G,\mathbb{Z})_{(p)} \cong \prod_{P\in\mathfrak{P}} \widehat{\mathrm{H}}^*(N(P),\mathbb{Z})_{(p)}$$

where $\mathfrak{P}$ is a set of representatives for the conjugacy classes of subgroups of G of order p and $N(P)$ denotes the normalizer of P.

Proof. See Brown's book [4]. □

We also have

$$\widehat{\mathrm{H}}^*(G,\mathbb{Z}) \cong \prod_{p} \widehat{\mathrm{H}}^*(G,\mathbb{Z})_{(p)}$$

where p ranges over the primes such that G has p-torsion.
A group G of finite virtual cohomological dimension is said to have periodic cohomology if for some $d \neq 0$ there is an element $u \in \widehat{\mathrm{H}}^d(G,\mathbb{Z})$ that is invertible in the ring $\widehat{\mathrm{H}}^*(G,\mathbb{Z})$. Cup product with u then gives a periodicity isomorphism $\widehat{\mathrm{H}}^i(G,M) \cong \widehat{\mathrm{H}}^{i+d}(G,M)$ for any G-module M and any $i \in \mathbb{Z}$.
Similarly we say that G has p-periodic cohomology if the p-primary component $\widehat{\mathrm{H}}^*(G,\mathbb{Z})_{(p)}$, which is itself a ring, contains an invertible element of non-zero degree d. Then we have

$$\widehat{\mathrm{H}}^i(G,M)_{(p)} \cong \widehat{\mathrm{H}}^{i+d}(G,M)_{(p)},$$

and the smallest positive d that satisfies this condition is called the p-period of G.

Proposition 4.2. *The following are equivalent:*

i) G has p-periodic cohomology.

ii) Every elementary abelian p-subgroup of G has rank $\leqslant 1$.

Proof. See Brown's book [4]. □

Remark. Ash [2] used Theorem 4.1 to compute the Farrell cohomology of $\mathrm{GL}(n,\mathbb{Z})$, $n = p-1,\dots,2p-3$, with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Another application of Theorem 4.1 is given by Naffah [8], who calculated the integral Farrell cohomology ring of $\mathrm{PSL}_2(\mathbb{Z}[1/n])$.

4.2 About normalizers

In order to use Theorem 4.1, we have to analyse the structure of the normalizers of subgroups of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$. We already analysed the conjugacy classes of subgroups of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$. Let N be the normalizer and let C be the centralizer of such a subgroup. Then we have a short exact sequence

$$1 \longrightarrow C \longrightarrow N \longrightarrow N/C \longrightarrow 1.$$

Moreover, it follows from the discussion in the paper of Brown [3] that for p an odd prime

$$C \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z},$$

and therefore N is a finite group. We will use the following well-known proposition.

Proposition 4.3. *Let*

$$1 \longrightarrow U \longrightarrow G \longrightarrow Q \longrightarrow 1$$

be a short exact sequence with Q a finite group of order prime to p. Then

$$\widehat{\mathrm{H}}^*(G,\mathbb{Z})_{(p)} \cong \left(\widehat{\mathrm{H}}^*(U,\mathbb{Z})_{(p)}\right)^Q.$$

Applying this to our case, we get

$$\widehat{\mathrm{H}}^*(N,\mathbb{Z})_{(p)} \cong \left(\widehat{\mathrm{H}}^*(C,\mathbb{Z})_{(p)}\right)^{N/C}.$$

Therefore we have to determine N/C and its action on $C \cong \mathbb{Z}/2p\mathbb{Z}$. From now on, if we consider subgroups or elements of order p in $\mathrm{U}((p-1)/2)$, we mean those which satisfy the condition of Theorem 2.9. In what follows we assume that p is an odd prime for which $h^- = 1$, because in this case we have a bijection between the conjugacy classes of subgroups of order p in $\mathrm{U}((p-1)/2)$ and those in $\mathrm{Sp}(p-1,\mathbb{Z})$. Therefore, in order to determine the structure of the conjugacy classes of subgroups of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$, we can consider the corresponding conjugacy classes in $\mathrm{U}((p-1)/2)$. We have already seen that in a subgroup of $\mathrm{U}((p-1)/2)$ of order p different elements can be in the same conjugacy class. Let $\mathcal{N}_k$ be the number of conjugacy classes of elements of order p in $\mathrm{U}((p-1)/2)$ where k powers of one element are in the same conjugacy class. Let $\mathcal{K}_k$ be the number of conjugacy classes of subgroups of $\mathrm{U}((p-1)/2)$ in which k elements are conjugate to each other. Then the number $\mathcal{K}(p)$ of conjugacy classes of subgroups of order p in $\mathrm{U}((p-1)/2)$ is

$$\mathcal{K}(p) = \sum_{\substack{k \mid p-1,\\ k \text{ odd}}} \mathcal{K}_k.$$

If in a subgroup k elements are conjugate to each other, then $|N/C| = k$ and

$$N/C \cong \mathbb{Z}/k\mathbb{Z} \subseteq \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathrm{Aut}(\mathbb{Z}/2p\mathbb{Z})$$

where $k|p-1$ and k is odd. This means that N/C is isomorphic to a subgroup of $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$. So we get the short exact sequence

$$1 \longrightarrow \mathbb{Z}/2p\mathbb{Z} \longrightarrow N \longrightarrow \mathbb{Z}/k\mathbb{Z} \longrightarrow 1.$$

Moreover, we have an injection $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/2p\mathbb{Z} \hookrightarrow N$. Applying the proposition to this case yields

$$\widehat{\mathrm{H}}^*(N,\mathbb{Z})_{(p)} \cong \left(\widehat{\mathrm{H}}^*(\mathbb{Z}/2p\mathbb{Z},\mathbb{Z})_{(p)}\right)^{\mathbb{Z}/k\mathbb{Z}}.$$

The action of $\mathbb{Z}/k\mathbb{Z}$ on $\mathbb{Z}/2p\mathbb{Z}$ is given by the action of $\mathbb{Z}/k\mathbb{Z}$ as a subgroup of the group of automorphisms of $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/2p\mathbb{Z}$.
The following is a well-known result.

Lemma 4.4. *The Farrell cohomology of* $\mathbb{Z}/l\mathbb{Z}$ *is*

$$\widehat{\mathrm{H}}^*(\mathbb{Z}/l\mathbb{Z},\mathbb{Z}) = \mathbb{Z}/l\mathbb{Z}\,[x,x^{-1}]$$

where $\deg x = 2$, $x \in \widehat{\mathrm{H}}^2(\mathbb{Z}/l\mathbb{Z},\mathbb{Z})$, *and* $\langle x\rangle \cong \mathbb{Z}/l\mathbb{Z}$.

This yields for an odd prime p

$$\widehat{\mathrm{H}}^*(\mathbb{Z}/2p\mathbb{Z},\mathbb{Z})_{(p)} = \left(\mathbb{Z}/2p\mathbb{Z}[x,x^{-1}]\right)_{(p)} = \mathbb{Z}/p\mathbb{Z}[x,x^{-1}].$$

In order to compute

$$\left(\widehat{\mathrm{H}}^*(\mathbb{Z}/2p\mathbb{Z},\mathbb{Z})_{(p)}\right)^{\mathbb{Z}/k\mathbb{Z}},$$

we have to consider the action of $\mathbb{Z}/k\mathbb{Z}$ on $\mathbb{Z}/p\mathbb{Z}[x,x^{-1}]$. We have $px = 0$ and $x \in \widehat{\mathrm{H}}^2(\mathbb{Z}/2p\mathbb{Z},\mathbb{Z})$. The action is given by $x \mapsto qx$ with q such that $(q,p) = 1$, $q^k \equiv 1 \pmod{p}$ and k is the smallest number such that this is fulfilled. The action of $\mathbb{Z}/k\mathbb{Z}$ on

$$\widehat{\mathrm{H}}^{2m}(\mathbb{Z}/2p\mathbb{Z},\mathbb{Z})_{(p)} = (\langle x^m\rangle) \cong \mathbb{Z}/p\mathbb{Z}$$

is given by

$$x^m \mapsto q^m x^m.$$

The $\mathbb{Z}/k\mathbb{Z}$-invariants of $\widehat{\mathrm{H}}^*(\mathbb{Z}/2p\mathbb{Z},\mathbb{Z})_{(p)}$ are the $x^m \in \widehat{\mathrm{H}}^{2m}(\mathbb{Z}/2p\mathbb{Z},\mathbb{Z})_{(p)}$ with $x^m \mapsto x^m$, or equivalently $q^m \equiv 1 \pmod{p}$. Herewith we get

$$\begin{aligned}\widehat{\mathrm{H}}^*(N,\mathbb{Z})_{(p)} &= \left(\widehat{\mathrm{H}}^*(\mathbb{Z}/2p\mathbb{Z},\mathbb{Z})_{(p)}\right)^{\mathbb{Z}/k\mathbb{Z}} = \left(\mathbb{Z}/p\mathbb{Z}[x,x^{-1}]\right)^{\mathbb{Z}/k\mathbb{Z}}\\ &= \mathbb{Z}/p\mathbb{Z}[x^k,x^{-k}].\end{aligned}$$

Let p be a prime with $h^- = 1$. Then $\mathcal{K}_k$ conjugacy classes of subgroups exist for which $|N/C| = k$. Theorem 4.1 yields

Proposition 4.5. *Let p be an odd prime for which $h^- = 1$. Then*

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(p-1,\mathbb{Z}),\mathbb{Z})_{(p)} \cong \prod_{\substack{k \mid p-1 \\ k \text{ odd}}} \left(\prod_1^{\mathcal{K}_k} \mathbb{Z}/p\mathbb{Z}[x^k, x^{-k}] \right).$$

If $Y \in \mathrm{Sp}(p-1,\mathbb{Z})$ is a matrix of order p whose conjugacy class corresponds to the equivalence class $[\mathfrak{a}, a] \in \mathcal{P}$, the conjugacy class of Y^k corresponds to $[\gamma_{-k}(\mathfrak{a}), \gamma_{-k}(a)]$ where $\gamma_{-k} \in \mathrm{Gal}(\mathbb{Q}(\xi),\mathbb{Q})$ is defined by $\gamma_{-k}(\xi) = \xi^{-k}$. For a definition of $\mathcal{P}$ see the proof of Theorem 2.9. If h^- is odd, a bijection exists between the conjugacy classes of matrices of order p in $\mathrm{U}((p-1)/2)$ that satisfy the conditions of Theorem 2.9 and the conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1,\mathbb{Z})$ that correspond to the equivalence classes $[\mathbb{Z}[\xi], u] \in \mathcal{P}$. In this case we get

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(p-1,\mathbb{Z}),\mathbb{Z})_{(p)} \cong \prod_{\substack{k \mid p-1 \\ k \text{ odd}}} \left(\prod_1^{\widetilde{\mathcal{K}}_k} \mathbb{Z}/p\mathbb{Z}[x^k, x^{-k}] \right)$$

where $\widetilde{\mathcal{K}}_k$ denotes the number of conjugacy classes of subgroups of order p of $\mathrm{Sp}(p-1,\mathbb{Z})$ in which k elements are conjugate to each other. If h^- is odd, $\widetilde{\mathcal{K}}_k \geqslant \mathcal{K}_k$. If h^- is even, it may be possible that no subgroup of $\mathrm{Sp}(p-1,\mathbb{Z})$ of order p exists for which $|N/C| = k$.
Now it remains to determine $\mathcal{K}_k$, the number of conjugacy classes of subgroups of $\mathrm{U}((p-1)/2)$ of order p with $N/C \cong \mathbb{Z}/k\mathbb{Z}$. Therefore we need $\mathcal{N}_k$, the number of conjugacy classes of elements $X \in \mathrm{U}((p-1)/2)$ of order p for which $1 = j_1 < \cdots < j_k < p$ exist such that the X^{j_l}, $l = 1, \ldots, k$, are in the same conjugacy class than X and k is maximal. One such class yields k elements in a group for which $|N/C| = k$ and therefore

$$\mathcal{K}_k = k\mathcal{N}_k \frac{1}{p-1}.$$

We recall the formula for $\mathcal{N}_k$:

$$\mathcal{N}_k = 2^{\frac{p-1}{2k}} - \sum_{\substack{k' \text{ odd},\ k' > k \\ k \mid k',\ k' \mid p-1}} \mathcal{N}_{k'}.$$

Now we have everything we need to compute the p-primary part of the Farrell cohomology of $\mathrm{Sp}(p-1,\mathbb{Z})$ for some examples of primes with $h^- = 1$.

4.3 The p-primary part of the Farrell cohomology of $\mathrm{Sp}(p-1,\mathbb{Z})$ for $3 \leqslant p \leqslant 19$

$p=3$: It is $\mathrm{Sp}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})$. We just have $k=1$ and get

$$\mathcal{N}_1 = 2^1 = 2 \qquad\qquad \mathcal{K}_1 = \mathcal{N}_1 \tfrac{1}{p-1} = 1.$$

This means that one conjugacy class exists with $N = C$. Therefore

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(2,\mathbb{Z}),\mathbb{Z})_{(3)} \cong \mathbb{Z}/3\mathbb{Z}[x,x^{-1}],$$

and $\mathrm{Sp}(2,\mathbb{Z})$ has 3-period 2.

$p=5$: We just have $k=1$ and get

$$\mathcal{N}_1 = 2^2 = 4 \qquad\qquad \mathcal{K}_1 = \mathcal{N}_1 \tfrac{1}{p-1} = 1.$$

This means that one conjugacy class exists with $N = C$. Therefore

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(4,\mathbb{Z}),\mathbb{Z})_{(5)} \cong \mathbb{Z}/5\mathbb{Z}[x,x^{-1}],$$

and $\mathrm{Sp}(4,\mathbb{Z})$ has 5-period 2.

$p=7$: Here $k \in \{1,3\}$ and we get

$$\mathcal{N}_3 = 2^{\frac{3}{3}} = 2 \qquad\qquad \mathcal{K}_3 = 3\mathcal{N}_3 \tfrac{1}{p-1} = 1$$
$$\mathcal{N}_1 = 2^3 - 2 = 6 \qquad\qquad \mathcal{K}_1 = \mathcal{N}_1 \tfrac{1}{p-1} = 1.$$

This means that one conjugacy class exists with $N/C \cong \mathbb{Z}/3\mathbb{Z}$, and one class exists with $N = C$. Therefore

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(6,\mathbb{Z}),\mathbb{Z})_{(7)} \cong \mathbb{Z}/7\mathbb{Z}[x^3,x^{-3}] \times \mathbb{Z}/7\mathbb{Z}[x,x^{-1}],$$

and $\mathrm{Sp}(6,\mathbb{Z})$ has 7-period 6.

$p=11$: Here $k \in \{1,5\}$ and we get

$$\mathcal{N}_5 = 2 \qquad\qquad \mathcal{K}_5 = 5\mathcal{N}_5 \tfrac{1}{p-1} = 1$$
$$\mathcal{N}_1 = 2^5 - 2 = 30 \qquad\qquad \mathcal{K}_1 = \mathcal{N}_1 \tfrac{1}{p-1} = 3.$$

This means that one conjugacy class exists with $N/C \cong \mathbb{Z}/5\mathbb{Z}$ and 3 classes exist with $N = C$. Therefore

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(10,\mathbb{Z}),\mathbb{Z})_{(11)} \cong \mathbb{Z}/11\mathbb{Z}[x^5,x^{-5}] \times \prod_1^3 \mathbb{Z}/11\mathbb{Z}[x,x^{-1}],$$

and $\mathrm{Sp}(10,\mathbb{Z})$ has 11-period 10.

$p = 13$**:** Here $k \in \{1, 3\}$ and we get

$$\mathcal{N}_3 = 2^{\frac{6}{3}} = 4 \qquad\qquad \mathcal{K}_3 = 3\mathcal{N}_3 \tfrac{1}{p-1} = 1$$
$$\mathcal{N}_1 = 2^6 - 4 = 60 \qquad\qquad \mathcal{K}_1 = \mathcal{N}_1 \tfrac{1}{p-1} = 5.$$

This means that one conjugacy class exists with $N/C \cong \mathbb{Z}/3\mathbb{Z}$ and 5 classes exist with $N = C$. Therefore

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(12, \mathbb{Z}), \mathbb{Z})_{(13)} \cong \mathbb{Z}/13\mathbb{Z}[x^3, x^{-3}] \times \prod_1^5 \mathbb{Z}/13\mathbb{Z}[x, x^{-1}],$$

and $\mathrm{Sp}(12, \mathbb{Z})$ has 13-period 6.

$p = 17$**:** We just have $k = 1$ and get

$$\mathcal{N}_1 = 2^8 = 256 \qquad\qquad \mathcal{K}_1 = \mathcal{N}_1 \tfrac{1}{p-1} = 16.$$

This means that 16 conjugacy classes exist with $N = C$. Therefore

$$\widehat{\mathrm{H}}^*(\mathrm{Sp}(16, \mathbb{Z}), \mathbb{Z})_{(17)} \cong \prod_1^{16} \mathbb{Z}/17\mathbb{Z}[x, x^{-1}],$$

and $\mathrm{Sp}(16, \mathbb{Z})$ has 17-period 2.

$p = 19$**:** Here $k \in \{1, 3, 9\}$ and we get

$$\mathcal{N}_9 = 2^{\frac{9}{9}} = 2 \qquad\qquad \mathcal{K}_9 = 9\mathcal{N}_9 \tfrac{1}{p-1} = 1$$
$$\mathcal{N}_3 = 2^{\frac{9}{3}} - 2 = 6 \qquad\qquad \mathcal{K}_3 = 3\mathcal{N}_3 \tfrac{1}{p-1} = 1$$
$$\mathcal{N}_1 = 2^9 - 2 - 6 = 504 \qquad\qquad \mathcal{K}_1 = \mathcal{N}_1 \tfrac{1}{p-1} = 28.$$

This means that one conjugacy class exists with $N/C \cong \mathbb{Z}/9\mathbb{Z}$, one class exists with $N/C \cong \mathbb{Z}/3\mathbb{Z}$, and 28 classes exist with $N = C$.

$$\begin{aligned}\widehat{\mathrm{H}}^*(\mathrm{Sp}(18, \mathbb{Z}), \mathbb{Z})_{(19)} \cong\ & \mathbb{Z}/19\mathbb{Z}[x^9, x^{-9}] \times \mathbb{Z}/19\mathbb{Z}[x^3, x^{-3}] \\ & \times \prod_1^{28} \mathbb{Z}/19\mathbb{Z}[x, x^{-1}],\end{aligned}$$

and $\mathrm{Sp}(18, \mathbb{Z})$ has 19-period 18.

4.4 The p-period of the Farrell cohomology of Sp$(p-1,\mathbb{Z})$

For $3 \leqslant p \leqslant 19$ we have computed the period of $\widehat{\mathrm{H}}^*(\mathrm{Sp}(p-1,\mathbb{Z}),\mathbb{Z})_{(p)}$. We can determine the p-period of Sp$(p-1,\mathbb{Z})$ for any odd prime p for which h^- is odd where h^- denotes the relative class number of the cyclotomic field $\mathbb{Q}(\xi)$, ξ a primitive pth root of unity.

Theorem 4.6. *Let p be an odd prime for which h^- is odd and let y be such that $p-1 = 2^r y$ and y is odd. Then the period of $\widehat{\mathrm{H}}^*(\mathrm{Sp}(p-1,\mathbb{Z}),\mathbb{Z})_{(p)}$ is $2y$.*

Proof. Each conjugacy class of subgroups of order p in U$((p-1)/2)$ whose group elements satisfy the condition required in Theorem 2.9 yields at least one conjugacy class in Sp$(p-1,\mathbb{Z})$. This implies that the p-primary part of the Farrell cohomology of Sp$(p-1,\mathbb{Z})$ is a product

$$\prod_{\substack{k|p-1,\\ k \text{ odd}}} \left(\prod_{1}^{\widetilde{\mathcal{K}}_k} \mathbb{Z}/p\mathbb{Z}[x^k, x^{-k}] \right)$$

where $\widetilde{\mathcal{K}}_k$ denotes the number of conjugacy classes of subgroups of order p of Sp$(p-1,\mathbb{Z})$ in which k elements are conjugate to each other. There are $\mathcal{K}_k$ such subgroups in U$((p-1)/2)$, and, because h^- is odd, each such subgroup gives at least one such subgroup of Sp$(p-1,\mathbb{Z})$. Therefore $\widetilde{\mathcal{K}}_k \geqslant \mathcal{K}_k$. Moreover, the period of $\mathbb{Z}/p\mathbb{Z}[x^k, x^{-k}]$ is $2k$. Herewith the period of the p-primary part of the Farrell cohomology is $2y$. ☐

If p is a prime for which h^- is even, the p-period of $\widehat{\mathrm{H}}^*(\mathrm{Sp}(p-1,\mathbb{Z}),\mathbb{Z})$ is $2z$ where z is odd and divides $p-1$. The period is not necessarily y because there may be no subgroup of order p in which y elements are conjugate in Sp$(p-1,\mathbb{Z})$ even if we know that they are conjugate in Sp$(p-1,\mathbb{R})$.

Chapter 5

Examples

5.1 The companion matrix

In this section we will show an application of the construction we did in order to prove Theorem 2.9.
Let us first examine the construction in the paper of Bürgisser [5]. For an odd prime p let ξ be a primitive pth root of unity. The minimal polynomial of the extension $\mathbb{Q}(\xi)/\mathbb{Q}$ is

$$m(x) := 1 + x + \cdots + x^{p-1}.$$

We define the companion matrix B of $m(x)$ as

$$B := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ -1 & -1 & \cdots & -1 & -1 \end{pmatrix} \in \mathrm{GL}(p-1, \mathbb{Z}).$$

Then $\det B = 1$ and $B^p = I$. Now we set

$$\overline{D} := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 1 & \cdots & 1 & 1 \end{pmatrix} \quad \text{and} \quad D := \begin{pmatrix} 0 & \overline{D} \\ -\overline{D}^{\mathrm{T}} & 0 \end{pmatrix}.$$

It is obvious that $D \in \mathrm{SL}(p-1, \mathbb{Z})$ is skew-symmetric and defines an alternating bilinear form

$$\begin{array}{rccl} q: & \mathbb{Z}^{p-1} \times \mathbb{Z}^{p-1} & \longrightarrow & \mathbb{Z} \\ & (x, y) & \longmapsto & q(x, y) := x^{\mathrm{T}} D y \end{array}$$

on $\mathbb{Z}^{p-1}$ endowed with the standard basis. The matrix B defines a $\mathbb{Z}$-automorphism σ, which is an isometry of q, i.e.

$$q(x, y) = q(\sigma(x), \sigma(y)) = q(Bx, By).$$

This is equivalent to $B^{\mathrm{T}}DB = D$. A matrix $G \in \mathrm{GL}(p-1, \mathbb{Z})$ exists such that $G^{\mathrm{T}}DG = J$. Then $G^{-1}BG = Y \in \mathrm{Sp}(p-1, \mathbb{Z})$ and Y has order p. The companion matrix B is conjugate to $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$. We will explicitly determine the eigenvalues of $X \in \mathrm{U}((p-1)/2)$ with $\phi(X) \in \mathrm{Sp}(p-1, \mathbb{R})$ conjugate to $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$. Therefore we have to compute the eigenvectors of σ and then $\mathrm{sign}(V_j)$ of the invariant subspaces V_j.
Now we will determine a basis of the spaces V_j, $j = 1, \ldots, (p-1)/2$, in order to compute $\mathrm{sign}(V_j)$ explicitly. We consider the complexifications of σ and of q. Let

$$v := (x_1, \ldots, x_{p-1})^{\mathrm{T}}$$

be an eigenvector of B corresponding to the eigenvalue λ. Then v satisfies the equation

$$\begin{pmatrix} -\lambda & 1 & 0 & \cdots & 0 \\ 0 & -\lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & -\lambda & 1 \\ -1 & \cdots & -1 & -1 & -1-\lambda \end{pmatrix} \begin{pmatrix} x_1 \\ \\ \vdots \\ \\ x_{p-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \\ \vdots \\ \\ 0 \end{pmatrix}.$$

Let $x_{p-1} := \lambda^{p-1}$. Then we get $x_{p-2} = \lambda^{p-2}, \ldots, x_1 = \lambda$. So

$$\begin{aligned} v &= \left(\lambda\,,\, \lambda^2\,,\, \ldots\,,\, \lambda^{\frac{p-1}{2}}\,,\, \lambda^{-\frac{p-1}{2}}\,,\, \ldots\,,\, \lambda^{-2}\,,\, \lambda^{-1}\right)^{\mathrm{T}}, \\ \overline{v} &= \left(\lambda^{-1}\,,\, \lambda^{-2}\,,\, \ldots\,,\, \lambda^{-\frac{p-1}{2}}\,,\, \lambda^{\frac{p-1}{2}}\,,\, \ldots\,,\, \lambda^2\,,\, \lambda\right)^{\mathrm{T}} \end{aligned}$$

where v is the eigenvector corresponding to the eigenvalue λ and $\overline{v}$ is the eigenvector corresponding to the eigenvalue $\overline{\lambda}$. Moreover, we have

$$D = \left(\begin{array}{ccc|ccc} & & & 1 & & 0 \\ & 0 & & \vdots & \ddots & \\ & & & 1 & \cdots & 1 \\ \hline -1 & \cdots & -1 & & & \\ & \ddots & \vdots & & 0 & \\ 0 & & -1 & & & \end{array}\right)$$

and

$$D\overline{v} = \begin{pmatrix} \lambda^{\frac{p-1}{2}} \\ \lambda^{\frac{p-1}{2}} + \lambda^{\frac{p-3}{2}} \\ \vdots \\ \lambda^{\frac{p-1}{2}} + \cdots + \lambda \\ -\lambda^{-1} - \cdots - \lambda^{-\frac{p-1}{2}} \\ \vdots \\ -\lambda^{-\frac{p-3}{2}} - \lambda^{-\frac{p-1}{2}} \\ -\lambda^{-\frac{p-1}{2}} \end{pmatrix}.$$

This yields

$$\begin{aligned} q(v,\overline{v}) &= v^{\mathrm{T}} D\overline{v} \\ &= \lambda^{\frac{p-1}{2}+1} + \left(\lambda^{\frac{p-1}{2}+2} + \lambda^{\frac{p-1}{2}+1}\right) + \cdots + \left(\lambda^{p-1} + \cdots + \lambda^{\frac{p-1}{2}+1}\right) \\ &\quad - \left(\lambda^{\frac{p-1}{2}} + \cdots + \lambda\right) - \cdots - \left(\lambda^{\frac{p-1}{2}} + \lambda^{\frac{p-1}{2}-1}\right) - \lambda^{\frac{p-1}{2}} \\ &= -\lambda - 2\lambda^2 - \cdots - \frac{p-1}{2}\lambda^{\frac{p-1}{2}} + \frac{p-1}{2}\lambda^{-\frac{p-1}{2}} + \cdots + 2\lambda^{-2} + \lambda^{-1} \\ &= \sum_{j=1}^{(p-1)/2} j(\lambda^{-j} - \lambda^{j}) \\ &= -2i \sum_{j=1}^{(p-1)/2} j \sin\theta_j, \end{aligned}$$

and therefore

$$iq(v_j,\overline{v}_j) = 2\sum_{k=1}^{(p-1)/2} k\sin\theta_{kj}.$$

We have already computed

$$\begin{aligned} \operatorname{sign}(V_j) := \operatorname{sign} q(x,Bx) &= \operatorname{sign}(-iq(v_j,\overline{v}_j)) \\ &= \operatorname{sign}\left(-2\sum_{k=1}^{\frac{p-1}{2}} k\sin(k\theta_j)\right). \end{aligned}$$

Proposition 5.1. *For the invariant subspaces V_j, $j = 1, \ldots, (p-1)/2$, of the isometry given by the companion matrix B the following is true.*

If j is odd, $\operatorname{sign}(V_j) = -1$, *and*
if j is even, $\operatorname{sign}(V_j) = 1$.

We will first prove a lemma.

Lemma 5.2. *For any $n \in \mathbb{N} \setminus \{0\}$ and any $x \in \mathbb{R}$, $x \neq 0$,*

$$\frac{d}{dx} \sum_{k=1}^{n} \cos kx = \frac{1}{2} \; \frac{n \sin((n+1)x) - (n+1)\sin(nx)}{1 - \cos x} \, .$$

Proof of Lemma 5.2. We first have to check that for any $n \in \mathbb{N} \setminus \{0\}$ and any $x \in \mathbb{R}$, $x \neq 0$,

$$\sum_{k=1}^{n} \cos(kx) = \frac{\cos \frac{(n+1)x}{2} \; \sin \frac{nx}{2}}{\sin \frac{x}{2}} \, .$$

Indeed, we have

$$\begin{aligned}
&(e^{ix} - e^{-ix}) \sum_{k=1}^{n} e^{ikx} + e^{-ikx} \\
&\quad = \sum_{k=1}^{n} \left(e^{i(k+1)x} - e^{-i(k+1)x} - e^{i(k-1)x} + e^{-i(k-1)x} \right) \\
&\quad = \sum_{k=2}^{n+1} e^{ikx} - e^{-ikx} - \sum_{k=0}^{n-1} e^{ikx} - e^{-ikx} \\
&\quad = e^{i(n+1)x} - e^{-i(n+1)x} + e^{inx} - e^{-inx} - \left(e^{ix} - e^{-ix} + 1 - 1 \right) \\
&\quad = 2i \sin((n+1)x) + 2i \sin(nx) - 2i \sin x,
\end{aligned}$$

and herewith

$$\begin{aligned}
\sum_{k=1}^{n} \cos kx &= \frac{1}{2} \sum_{k=1}^{n} e^{ikx} + e^{-ikx} \\
&= \frac{1}{2} \; \frac{2i \; \sin((n+1)x) + 2i \; \sin(nx) - 2i \; \sin x}{2i \; \sin x} \\
&= \frac{1}{2} \; \frac{2 \sin \frac{(2n+1)x}{2} \cos \frac{x}{2} - \sin x}{\sin x} \\
&= \frac{1}{2} \; \frac{\sin \frac{(2n+1)x}{2} - \sin \frac{x}{2}}{\sin \frac{x}{2}} \\
&= \frac{\cos \frac{(n+1)x}{2} \; \sin \frac{nx}{2}}{\sin \frac{x}{2}} \, .
\end{aligned}$$

Using some well-known trigonometric formulas, we get

$$\begin{aligned}\frac{d}{dx}\sum_{k=1}^{n}\cos kx &= \frac{d}{dx}\frac{\cos\frac{(n+1)x}{2}\ \sin\frac{nx}{2}}{\sin\frac{x}{2}}\\ &= \dots\\ &= \frac{1}{2}\ \frac{n\sin((n+1)x)-(n+1)\sin(nx)}{1-\cos x}.\end{aligned}$$

□

Proof of Proposition 5.1. We consider the function

$$f(x) := -2\sum_{k=1}^{n} k\sin(kx) = \frac{d}{dx}\left(2\sum_{k=1}^{n}\cos(kx)\right).$$

Lemma 5.2 yields

$$-2\sum_{k=1}^{n} k\sin kx = \frac{n\sin((n+1)x)-(n+1)\sin(nx)}{1-\cos x}.$$

We now consider the case $n = (p-1)/2$ and $x = \theta_j$ where $\theta_j = j2\pi/p$, $j = 1,\dots,(p-1)/2$. Then we have

$$\begin{aligned}-2\sum_{k=1}^{(p-1)/2} k\sin(k\theta_j) &= \frac{\frac{p-1}{2}\sin\left(\frac{p+1}{2}\,\theta_j\right)-\frac{p+1}{2}\sin\left(\frac{p-1}{2}\,\theta_j\right)}{1-\cos\theta_j}\\ &= \frac{-\frac{p-1}{2}\sin\left(\frac{-1-p}{2}\,\theta_j\right)-\frac{p+1}{2}\sin\left(\frac{p-1}{2}\,\theta_j\right)}{1-\cos\theta_j}\\ &= \frac{-p\sin\left(\frac{p-1}{2}\,\theta_j\right)}{1-\cos\theta_j}\end{aligned}$$

since

$$\sin\left(\frac{-1-p}{2}\ \theta_j\right) = \sin\left(\frac{-1-p+2p}{2}\ \theta_j\right).$$

In the case we are considering $\theta_j := j2\pi/p$ for $j = 1,\dots,(p-1)/2$. Therefore $\cos\theta_j \neq 1\ \forall j$ since $j \neq np\ \forall n \in \mathbb{N}$ and $1-\cos\theta_j > 0$. Herewith we get

$$\begin{aligned}\operatorname{sign}(V_j) &= \operatorname{sign}\left(-2\sum_{k=1}^{(p-1)/2} k\sin(k\theta_j)\right)\\ &= \operatorname{sign}\left(-p\,\frac{\sin(\frac{p-1}{2}\,\theta_j)}{1-\cos\theta_j}\right)\\ &= \operatorname{sign}\left(-p\,\sin\left(\frac{p-1}{2}\,\theta_j\right)\right).\end{aligned}$$

We now have to consider two cases.

j is even: then $\exists k$, $1 \leqslant k \leqslant \frac{p-1}{4}$ such that $j = 2k$. Then

$$\begin{aligned}\sin\left(\frac{p-1}{2}\,\theta_j\right) &= \sin\left(\frac{p-1}{2}\,j\,\frac{2\pi}{p}\right) = \sin\left(k(p-1)\frac{2\pi}{p}\right)\\ &= -\sin\left(k\,\frac{2\pi}{p}\right)\end{aligned}$$

and with the preceding computations

$$\begin{aligned}\operatorname{sign}(V_j) &= \operatorname{sign}\left(-p\,\sin\left(\frac{p-1}{2}\,\theta_j\right)\right)\\ &= \operatorname{sign}\left(p\,\sin\left(k\,\frac{2\pi}{p}\right)\right)\\ &= 1.\end{aligned}$$

j is odd: then $\exists k$, $0 \leqslant k < \frac{p-1}{4}$ such that $j = 2k+1$. Then

$$\begin{aligned}\sin\left(\frac{p-1}{2}\,\theta_j\right) &= \sin\left(\frac{p-1}{2}\,j\,\frac{2\pi}{p}\right) = \sin\left(\frac{p-1}{2}\,(2k+1)\,\frac{2\pi}{p}\right)\\ &= \sin\left((2k+1)\frac{(p-1)\pi}{p}\right)\\ &= \sin\left((2k+1)\frac{\pi}{p}\right)\end{aligned}$$

and

$$\begin{aligned}\operatorname{sign}(V_j) &= \operatorname{sign}\left(-p\,\sin\left(\frac{p-1}{2}\,\theta_j\right)\right)\\ &= \operatorname{sign}\left(-p\,\sin\left((2k+1)\frac{\pi}{p}\right)\right)\\ &= -1,\end{aligned}$$

since $\sin\left((2k+1)\frac{\pi}{p}\right) > 0$ for $(2k+1) = 1, \ldots, \frac{p-1}{2}$.

$\square$

If we compare Proposition 2.15 and Proposition 5.1, we get the following result.

Proposition 5.3. *For an odd prime p let $\xi := e^{i2\pi/p}$. Let $Y \in \mathrm{Sp}(p-1, \mathbb{Z})$ be conjugate in $\mathrm{GL}(p-1,\mathbb{Z})$ to the companion matrix $B \in \mathrm{GL}(p-1,\mathbb{Z})$. Let V_j, $j = 1, \ldots, (p-1)/2$, be the invariant subspace corresponding to the eigenvalues ξ^j and ξ^{-j} of Y. We choose $X \in \mathrm{U}((p-1)/2)$ such that $\phi(X) \in \mathrm{Sp}(p-1,\mathbb{Z})$ is conjugate to $Y \in \mathrm{Sp}(p-1,\mathbb{R})$. Then the following holds for $j = 1, \ldots, (p-1)/2$.*

If j is odd, ξ^j is eigenvalue of X, and
if j is even, ξ^{-j} is eigenvalue of X.

Herewith the set of eigenvalues of X is

$$\left\{\xi^j \mid j \text{ odd}, 1 \leqslant j \leqslant p-1, \right\}.$$

Proof. We just have to justify the last statement, but this is clear because if j is even, $1 \leqslant j \leqslant (p-1)/2$, then $\xi^{-j} = \xi^{p-j}$ where $p-j$ is odd and $(p-3)/2 \leqslant p-j \leqslant p-1$. □

5.2 The examples $p = 5$ and $p = 7$

The companion matrix

$$B := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \end{pmatrix} \in \mathrm{GL}(4,\mathbb{Z})$$

is conjugate to the matrix

$$Y = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & -1 & -1 \end{pmatrix} \in \mathrm{Sp}(4,\mathbb{Z}), \text{ with } Y^5 = I.$$

The eigenvalues of Y are $\{\xi, \xi^2, \xi^3, \xi^4\}$, $\xi = e^{i2\pi/5}$. We will show by a direct calculation that the eigenvalues of $X \in \mathrm{U}(2)$ with $\phi(X) \in \mathrm{Sp}(4,\mathbb{R})$ conjugate to Y are $\{\xi, \xi^3\}$. Like in the general case, Y defines a $\mathbb{Z}$-automorphism σ of $\mathbb{Z}^4$ that acts as an isometry of the $\mathbb{Z}$-bilinear form q defined by $\langle x, y\rangle = x^T J y$. Without making a remark, we will extend σ linearly to an $\mathbb{R}$-automorphism of $\mathbb{R}^4$ or take its complexification. In the same way we will extend q linearly to an $\mathbb{R}$-bilinear form on $\mathbb{R}^4$ or take its complexification.
For $j = 1, \ldots, 4$ let v_j be the eigenvector of Y with eigenvalue ξ^j. Since $\overline{\xi} = \xi^4$ and $\overline{\xi^2} = \xi^3$, we can choose $v_1, \ldots, v_4$ such that $\overline{v}_1 = v_4$ and $\overline{v}_2 = v_3$. Let $f_j(x) := (x - \xi^j)(x - \xi^{-j})$, $j = 1, 2$, then we define $V_j := \ker f_j(\sigma)$ and

$$w_j := v_j + \overline{v}_j, \quad \widetilde{w}_j := -i(v_j - \overline{v}_j)$$

is a basis of V_j. Moreover, it is easy to check that for $\theta_j := j\frac{2\pi}{5}$, $j = 1, 2$,

$$\begin{aligned} Y w_j &= \cos\theta_j\, w_j - \sin\theta_j\, \widetilde{w}_j, \\ Y \widetilde{w}_j &= \sin\theta_j\, w_j + \cos\theta_j\, \widetilde{w}_j. \end{aligned}$$

It is easy to compute the eigenvectors of Y. We get

$$\begin{aligned} v_1 &:= \left(\xi^3 + \xi^4\,,\, \xi^4\,,\, 1\,,\, \xi\right)^{\mathrm{T}}, \quad v_4 := \left(\xi + \xi^2\,,\, \xi\,,\, 1\,,\, \xi^4\right)^{\mathrm{T}} = \overline{v}_1, \\ v_2 &:= \left(\xi + \xi^3\,,\, \xi^3\,,\, 1\,,\, \xi^2\right)^{\mathrm{T}}, \quad v_3 := \left(\xi^2 + \xi^4\,,\, \xi^2\,,\, 1\,,\, \xi^3\right)^{\mathrm{T}} = \overline{v}_2. \end{aligned}$$

Then

$$\begin{aligned} \operatorname{sign}(V_1) &= \operatorname{sign}(-2i\langle v_1, \overline{v}_1\rangle) = \operatorname{sign}\bigl(2\left(\xi^3 - \xi^2\right) + \left(\xi^4 - \xi\right)\bigr) \\ &= \operatorname{sign}\left(-2i\left(2\sin\frac{4\pi}{5} + \sin\frac{2\pi}{5}\right)\right) \\ &= -1, \\ \operatorname{sign}(V_2) &= \operatorname{sign}(-2i\langle v_2, \overline{v}_2\rangle) = \operatorname{sign}\bigl(2\left(\xi - \xi^4\right) + \left(\xi^3 - \xi^2\right)\bigr) \\ &= \operatorname{sign}\left(2i\left(2\sin\frac{2\pi}{5} - \sin\frac{4\pi}{5}\right)\right) \\ &= +1. \end{aligned}$$

We define the real numbers

$$\begin{aligned} c_1 &:= \bigl(-\operatorname{sign}(V_1)\,(-2i\langle v_1, \overline{v}_1\rangle)\bigr)^{-\frac{1}{2}} = (2i\langle v_1, \overline{v}_1\rangle)^{-\frac{1}{2}}, \\ c_2 &:= \bigl(-\operatorname{sign}(V_2)\,(-2i\langle v_2, \overline{v}_2\rangle)\bigr)^{-\frac{1}{2}} = (-2i\langle v_2, \overline{v}_2\rangle)^{-\frac{1}{2}} \end{aligned}$$

and herewith vectors $\in \mathbb{R}^4$

$$\begin{aligned} u_1 &:= c_1\, w_1 = (2i\langle v_1, \overline{v}_1\rangle)^{-\frac{1}{2}}\,(v_1 + \overline{v}_1), \\ \widetilde{u}_1 &:= -\operatorname{sign}(V_1)\, c_1\, \widetilde{w}_1 = -(2i\langle v_1, \overline{v}_1\rangle)^{-\frac{1}{2}}\, i(v_1 - \overline{v}_1), \\ u_2 &:= c_2\, w_2 = (-2i\langle v_2, \overline{v}_2\rangle)^{-\frac{1}{2}}\,(v_2 + \overline{v}_2), \\ \widetilde{u}_2 &:= -\operatorname{sign}(V_2)\, c_2\, \widetilde{w}_2 = (-2i\langle v_2, \overline{v}_2\rangle)^{-\frac{1}{2}}\, i(v_2 - \overline{v}_2). \end{aligned}$$

A computation shows that

$$\begin{aligned} \langle u_1, \widetilde{u}_1\rangle &= \langle u_2, \widetilde{u}_2\rangle = 1, \\ \langle u_1, u_2\rangle &= \langle u_1, \widetilde{u}_2\rangle = \langle \widetilde{u}_1, u_2\rangle = \langle \widetilde{u}_1, \widetilde{u}_2\rangle = 0. \end{aligned}$$

The vectors u_1, u_2, $\widetilde{u}_1$, $\widetilde{u}_2$ form a basis of $\mathbb{R}^4$. Let S be the transformation matrix

$$S := \begin{pmatrix} u_1 & u_2 & \widetilde{u}_1 & \widetilde{u}_2 \end{pmatrix}.$$

Then $S^{\mathrm{T}}JS = J$ and the basis u_1, u_2, $\widetilde{u}_1$, $\widetilde{u}_2$ is a symplectic basis. Because of the construction of u_1, u_2, $\widetilde{u}_1$, $\widetilde{u}_2$, the matrix $S^{-1}YS$ is

$$\begin{aligned} S^{-1}YS &= \begin{pmatrix} \cos\frac{2\pi}{5} & 0 & \sin\frac{2\pi}{5} & 0 \\ 0 & \cos\frac{4\pi}{5} & 0 & -\sin\frac{4\pi}{5} \\ -\sin\frac{2\pi}{5} & 0 & \cos\frac{2\pi}{5} & 0 \\ 0 & \sin\frac{4\pi}{5} & 0 & \cos\frac{4\pi}{5} \end{pmatrix} \\ &= \begin{pmatrix} \cos\frac{2\pi}{5} & 0 & \sin\frac{2\pi}{5} & 0 \\ 0 & \cos\frac{6\pi}{5} & 0 & \sin\frac{6\pi}{5} \\ -\sin\frac{2\pi}{5} & 0 & \cos\frac{2\pi}{5} & 0 \\ 0 & -\sin\frac{6\pi}{5} & 0 & \cos\frac{6\pi}{5} \end{pmatrix}. \end{aligned}$$

This shows that the eigenvalues of $X \in \mathrm{U}(2)$, with $\phi(X)$ conjugate to Y, are

$$\xi := e^{i2\pi/5} \text{ and } \xi^3.$$

For $p = 7$ we can make a similar computation. We have

$$Y := \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & -1 & -1 & -1 \end{pmatrix} \in \mathrm{Sp}(6,\mathbb{Z}), \text{ with } Y^7 = I.$$

The eigenvalues of $X \in \mathrm{U}(3)$, with $\phi(X)$ conjugate to Y, are

$$\xi := e^{i2\pi/7}, \xi^3 \text{ and } \xi^5.$$

5.3 On the signature of units

For an odd prime p let ξ be a primitive pth root of unity. The equation $\gamma_j(\xi) = \xi^j$ defines $\gamma_j \in \mathrm{Gal}(\mathbb{Q}(\xi),\mathbb{Q})$, $j = 1,\ldots,p-1$. Let $U = \mathbb{Z}[\xi]^*$, $U^+ = \mathbb{Z}[\xi+\overline{\xi}]^*$. We already defined

$$\begin{aligned} \psi''' : \ U^+ &\longrightarrow (\mathbb{Z}/2\mathbb{Z})^{(p-1)/2} \\ u &\longmapsto (\mathrm{sign}(\gamma_1(u)),\ldots,\mathrm{sign}(\gamma_{(p-1)/2}(u))) \end{aligned}$$

where the sign of $z \in \mathbb{Z}[\xi+\overline{\xi}]$ is the sign of $\iota(z)$ for the real embedding ι of $\mathbb{Z}[\xi+\overline{\xi}]$ with $\iota(\xi+\overline{\xi}) = e^{i2\pi/p} + e^{-i2\pi/p}$. We will consider $\mathbb{Z}/2\mathbb{Z}$ to be an additive group. Then the sign of a positive number is 0 and the sign of a negative number is 1.

Now we will determine some primes for which ψ''' is surjective without using class numbers. In fact we will check if ψ''' is already surjective when we restrict ψ''' to the cyclotomic units of $\mathbb{Q}(\xi+\overline{\xi})$. If ψ''' restricted to the cyclotomic units is not surjective, then we do not know if ψ''' is surjective. We already know that the cyclotomic units of $\mathbb{Q}(\xi+\overline{\xi})$ are generated by -1 and

$$\zeta_a = \frac{\xi^{a/2} - \xi^{-a/2}}{\xi^{1/2} - \xi^{-1/2}}$$

for $a = 2, \ldots, (p-1)/2$. If the images under ψ''' of these $(p-1)/2$ generators form a basis of $(\mathbb{Z}/2\mathbb{Z})^{(p-1)/2}$, the homomorphism ψ''' is surjective. This happens if and only if the matrix

$$Z := \begin{pmatrix} \operatorname{sign}(-1) & \operatorname{sign}(-1) & \cdots & \operatorname{sign}(-1) \\ \operatorname{sign}\big(\zeta_2\big) & \operatorname{sign}\big(\gamma_2(\zeta_2)\big) & \cdots & \operatorname{sign}\big(\gamma_{(p-1)/2}(\zeta_2)\big) \\ \vdots & \vdots & & \vdots \\ \operatorname{sign}\big(\zeta_{(p-1)/2}\big) & \operatorname{sign}\big(\gamma_2(\zeta_{(p-1)/2})\big) & \cdots & \operatorname{sign}\big(\gamma_{(p-1)/2}(\zeta_{(p-1)/2})\big) \end{pmatrix}$$

is invertible. For the embedding $\iota : \mathbb{Z}[\xi+\overline{\xi}] \to \mathbb{R}$ with $\iota(\xi+\overline{\xi}) = e^{i2\pi/p} + e^{-i2\pi/p}$ we get $\operatorname{sign}(\zeta_j) = 0$ for $j = 2, \ldots, (p-1)/2$. So Z is invertible if and only if

$$T := \begin{pmatrix} \operatorname{sign}\big(\gamma_2(\zeta_2)\big) & \cdots & \operatorname{sign}\big(\gamma_{(p-1)/2}(\zeta_2)\big) \\ \vdots & & \vdots \\ \operatorname{sign}\big(\gamma_2(\zeta_{(p-1)/2})\big) & \cdots & \operatorname{sign}\big(\gamma_{(p-1)/2}(\zeta_{(p-1)/2})\big) \end{pmatrix}$$

is invertible. Since $\iota(\gamma_j(\zeta_a)) = \sin(ja\pi/p)/\sin(j\pi/p)$ and $\sin(j\pi/p) > 0$ for $j = 1, \ldots, (p-1)/2$, the matrix T is equal to

$$T = \begin{pmatrix} \operatorname{sign}\left(\sin\left(2\frac{2\pi}{p}\right)\right) & \ldots & \operatorname{sign}\left(\sin\left(\frac{p-1}{2}\frac{2\pi}{p}\right)\right) \\ \vdots & & \vdots \\ \operatorname{sign}\left(\sin\left(2\frac{(p-1)\pi}{2p}\right)\right) & \ldots & \operatorname{sign}\left(\sin\left(\frac{p-1}{2}\frac{(p-1)\pi}{2p}\right)\right) \end{pmatrix}.$$

We recall that $\lfloor x \rfloor \in \mathbb{Z}$ with $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$. If $(j,p) = 1$, then $\sin(j\pi/p)$ is positive if $\lfloor j/p \rfloor \equiv 0 \pmod 2$ and negative if $\lfloor j/p \rfloor \equiv 1 \pmod 2$. This we can use to compute with Mathematica the matrix T and check if its determinant is 0 or 1.

- ```
  T[p_]:=Table[Mod[Floor[(j k*2)/p],2],
                {j,2,(p-1)/2},{k,2,(p-1)/2}]
  ```
- ```
  Do[If[EvenQ[Det[T[Prime[i]]]],Print[Prime[i]],n=0],
     {i,3,100}]
  ```

The first primes that yield $\det T = 0$ are 29, 113, 163, 197, 239, 277, 311, 337, 349, 373, 397, 421, 463, 491, 547.

Bibliography

[1] J. P. Alexander, P. E. Conner, G. C. Hamrick, and J. W. Vick, *Witt classes of integral representations of an Abelian p-group*, Bull. of the AMS **6** (1974), 1179–1182.

[2] A. Ash, *Farrell cohomology of $GL(n, \mathbb{Z})$*, Israel J. of Math. **67** (1989), 327–336.

[3] K. S. Brown, *Euler Characteristics of Discrete Groups and G-Spaces*, Invent. Math. **27** (1974), 229–264.

[4] ———, *Cohomology of Groups*, GTM, vol. 87, Springer, 1982.

[5] B. Bürgisser, *Elements of finite order in symplectic groups*, Arch. Math. **39** (1982), 501–509.

[6] D. A. Garbanati, *Unit signatures, and even class numbers, and relative class numbers*, J. reine angew. Math. **274-275** (1975), 376–384.

[7] J. Milnor, *Introduction to algebraic K-theory*, Annals of Mathematical Studies, vol. 72, Princeton Univ. Press, 1974.

[8] N. Naffah, *On the Integral Farrell Cohomology Ring of $PSL_2(\mathbb{Z}[1/n])$*, Diss. ETH No. 11675, ETH Zürich, 1996.

[9] J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1992.

[10] D. Sjerve and Q. Yang, *Conjugacy Classes of p-Torsion in* $\mathrm{Sp}_{p-1}(\mathbb{Z})$, J. of Algebra **195** (1997), 580–603.

[11] L. C. Washington, *Introduction to cyclotomic fields*, 2 ed., GTM, vol. 83, Springer, 1997.

Curriculum Vitae

I was born in Bremen, Germany, on November 13, 1968.

In 1979, at the end of the primary school in Germany, I moved to Neuchâtel, Switzerland, changing primary language from German to French.

In 1988 I graduated with the Maturité fédérale de type C and the Baccalauréat scientifique (mathematics and science diploma) at the Gymnase Cantonal de Neuchâtel.

In autumn 1994 I obtained the degree of Holder of the Diploma in Mathematics of the Swiss Federal Institute of Technology in Zurich.

Since 1995 I am working as an assistant in the group for algebra and topology at the ETHZ. In this group I began my doctoral studies under the supervision of Prof. Dr. G. Mislin.

This work was completed in autumn 1999.