New York Journal of Mathematics

New York J. Math. **12** (2006) 169–182.

Conjugacy classes of p-torsion in symplectic groups over S-integers

Cornelia Minette Busch

Abstract. For any odd prime p we consider representations of a group of order p in the symplectic group $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ of $(p-1)\times(p-1)$-matrices over the ring $\mathbb{Z}[1/n]$, $0 \neq n \in \mathbb{N}$. We construct a relation between the conjugacy classes of subgroups P of order p in the symplectic group and the ideal class group in the ring $\mathbb{Z}[1/n]$ and we use this relation for the study of these conjugacy classes. In particular we determine the centralizer $C(P)$ and $N(P)/C(P)$ where $N(P)$ denotes the normalizer.

Contents

1. Introduction

We define the group of symplectic matrices $\mathrm{Sp}(2n, R)$ over a ring R to be the subgroup of matrices $M \in \mathrm{GL}(2n, R)$ that satisfy

$$M^{\mathrm{T}} J M = J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Received September 28, 2005.

Mathematics Subject Classification. 20G05, 20G10.

Key words and phrases. Representation theory, cohomology theory.

Research supported by a grant "Estancias de jóvenes doctores y tecnólogos extranjeros en España" (SB 2001-0138) from the Ministerio de Educación, Cultura y Deporte.

ISSN 1076-9803/06

where $1 \in \mathrm{M}(n, R)$ denotes the identity. Our motivation for studying subgroups of odd prime order p in the symplectic group $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$, $0 \neq n \in \mathbb{N}$, is given by the fact that the p-primary part of the Farrell cohomology of $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ is determined by the Farrell cohomology of the normalizer of subgroups of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ (see Brown [2]). First we consider the conjugacy classes of elements of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ and get the following result.

Theorem 3.14. *There are*

$$|\mathcal{C}_0| 2^{\frac{p-1}{2}+\tau}$$

conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$, $0 \neq n \in \mathbb{Z}$. Here $\mathcal{C}_0$ is the ideal class group of $\mathbb{Z}[1/n][\xi]$, ξ a primitive pth root of unity, and τ is the number of inert primes in $\mathbb{Z}[\xi+\xi^{-1}]$ that lie over primes in $\mathbb{Z}$ that divide n.

In order to prove this theorem we establish a relation between some ideal classes in $\mathbb{Z}[1/n][\xi]$ and the conjugacy classes of matrices of order p. We define equivalence classes $[\mathfrak{a}, a]$ of pairs $(\mathfrak{a}, a)$ where $\mathfrak{a} \subseteq \mathbb{Z}[1/n][\xi]$ is an ideal with $\mathfrak{a}\overline{\mathfrak{a}} = (a)$ and the equivalence relation is

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

We show that a bijection exists between the conjugacy classes of elements of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ and the set of equivalence classes $[\mathfrak{a}, a]$. Sjerve and Yang (see [11]) construct an analogous bijection for $\mathrm{Sp}(p-1, \mathbb{Z})$. We use the bijection described above in order to study the subgroups of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. We consider the case where $n \in \mathbb{Z}$ is such that $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi+\xi^{-1}]$ are principal ideal domains because in this case the ideal class group of those rings is trivial. We get the following results.

Theorem 4.1. *Let $n \in \mathbb{Z}$ be such that $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi+\xi^{-1}]$ are principal ideal domains and moreover $p \mid n$. Let $N(P)$ denote the normalizer and $C(P)$ the centralizer of a subgroup P of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. Then*

$$N(P)/C(P) \cong \mathbb{Z}/j\mathbb{Z}$$

where $j \mid p-1$, j odd. For each j with $j \mid p-1$, j odd, there exists a subgroup of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ with $N(P)/C(P) \cong \mathbb{Z}/j\mathbb{Z}$.

Theorem 4.2. *Let $n \in \mathbb{Z}$ be such that $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi+\xi^{-1}]$ are principal ideal domains. Then for a subgroup P of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$, the centralizer $C(P)$ is*

$$C(P) \cong \mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}^{\sigma^+}.$$

Here $\sigma^+ = \sigma$ if $p \nmid n$, $\sigma^+ = \sigma+1$ if $p \mid n$ and σ is the number of primes in $\mathbb{Z}[\xi+\xi^{-1}]$ that split in $\mathbb{Z}[\xi]$ and lie over primes in $\mathbb{Z}$ that divide n.

An application of these theorems is given in [5]; moreover they are a generalization of the results of Naffah [7] on the normalizer of $\mathrm{SL}(2, \mathbb{Z}[1/n])$.

Let $\mathrm{U}\big(\frac{p-1}{2}\big) \subset \mathrm{GL}\big(\frac{p-1}{2}, \mathbb{C}\big)$ be the group of unitary matrices. We consider the homomorphism

$$\begin{array}{rcl} \mathrm{U}\big(\frac{p-1}{2}\big) & \longrightarrow & \mathrm{Sp}(p-1, \mathbb{R}) \\ X = A + iB & \longmapsto & \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \end{array}$$

where $A, B \in \mathrm{M}(n, \mathbb{R})$. In [3] a condition is given for the matrix X such that the image of X is conjugate to a matrix of order p in $\mathrm{Sp}(p-1, \mathbb{Z})$. This is used in [4] to analyze the subgroups of order p in $\mathrm{Sp}(p-1, \mathbb{Z})$ by considering the corresponding subgroups in $\mathrm{U}\left(\frac{p-1}{2}\right)$. Here we avoid the unitary group by taking an arithmetical approach.

2. A recall of algebraic number theory

For the convenience of the reader, we give a short introduction to algebraic number theory. More details and the proofs can be found in the books of Lang [6], Neukirch [8] and Washington [12].

Let p be an odd prime and let ξ be a primitive pth root of unity. Then $\mathbb{Z}[\xi]$ is the ring of integers of the cyclotomic field $\mathbb{Q}(\xi)$ and $\mathbb{Z}[\xi+\xi^{-1}]$ is the ring of integers of the maximal real subfield $\mathbb{Q}(\xi+\xi^{-1})$ of $\mathbb{Q}(\xi)$. For an integer $0 \neq n \in \mathbb{Z}$ we consider the ring $\mathbb{Z}[1/n]$ and the extensions $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi+\xi^{-1}]$. It is well-known that $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi+\xi^{-1}]$ are Dedekind rings. For $j = 1, \ldots, p-1$ let the Galois automorphism $\gamma_j \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ be given by $\gamma_j(\xi) = \xi^j$. To simplify the notations, we define $x^{(j)} := \gamma_j(x)$ for any $x \in \mathbb{Q}(\xi)$ and $\gamma_j \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ as above. The Galois automorphism γ_j acts componentwise on a vector in $\mathbb{Q}(\xi)^k$.

Let A be a Dedekind ring and K the quotient field of A. Let L be a finite separable extension of K and B the integral closure of A in L. Let $\mathfrak{a}$ be an additive subgroup of L. The complementary set $\mathfrak{a}'$ of $\mathfrak{a}$ is the set of $x \in L$ such that $\mathrm{tr}_{L/K}(x\mathfrak{a}) \subseteq A$. The different of the extension B/A is defined to be

$$D_{B/A} := {B'}^{-1}_{L/K}.$$

In $\mathbb{Z}[\xi]$ the different is generated by $D = p\xi^{(p+1)/2}/(\xi - 1)$. It is a principal ideal. This is also true for $\mathbb{Z}[1/n][\xi]$ (see Lang [6] or Serre [9]).

Let $\mathcal{O}$ be the ring of integers of a number field K. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ be the Galois group of the extension and let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$. The subgroup

$$G_{\mathfrak{q}} = \{\sigma \in G \mid \sigma\mathfrak{q} = \mathfrak{q}\}$$

is called the decomposition group of $\mathfrak{q}$ over $\mathbb{Q}$. The fixed field

$$Z_{\mathfrak{q}} = \{x \in K \mid \sigma x = x \text{ for all } \sigma \in G_{\mathfrak{q}}\}$$

is called the decomposition field of $\mathfrak{q}$ over $\mathbb{Q}$. The decomposition group of a prime ideal $\sigma\mathfrak{q}$ that is conjugate to $\mathfrak{q}$ is the conjugate subgroup $G_{\sigma\mathfrak{q}} = \sigma G_{\mathfrak{q}} \sigma^{-1}$. Let $\mathfrak{q} \subset \mathcal{O}$ be a prime ideal in $\mathcal{O}$ over the prime (q) in $\mathbb{Z}$. Let $\kappa(\mathfrak{q}) := \mathcal{O}/\mathfrak{q}$ and $\kappa(q) := \mathbb{Z}/q\mathbb{Z}$. The degree $f_{\mathfrak{q}}$ of the extension of fields $\kappa(\mathfrak{q})/\kappa(q)$ is called the residue class degree of $\mathfrak{q}$. We recall the following property. For any prime $q \neq p$ let $f_q \in \mathbb{N}$ be the smallest positive integer such that

$$q^{f_q} \equiv 1 \bmod p.$$

Then $(q) = (\mathfrak{q}_1 \cdots \mathfrak{q}_r)$ where $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are pairwise different prime ideals in $\mathbb{Q}(\xi)$ and all have residue class degree f_q (see Neukirch [8]).

Let p, q and ξ be as above. Let $\mathfrak{q}^+ \subseteq \mathbb{Z}[\xi+\xi^{-1}]$ be a prime ideal that lies over q. We consider the ideal $\mathfrak{q}^+\mathbb{Z}[\xi] \subset \mathbb{Z}[\xi]$ generated by $\mathfrak{q}^+$. Any prime $q \neq p$ is unramified and the prime p ramifies. Let $\sigma \in G := \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ with $\sigma(x) = \overline{x}$. The Galois group G acts transitively on the set of prime ideals over q. It is known that $f_q = |G_{\mathfrak{q}}|$. We have the following three cases:

(i) The prime $\mathfrak{q}^+$ is inert: $\mathfrak{q}^+\mathbb{Z}[\xi] = \mathfrak{q}$, a prime ideal in $\mathbb{Z}[\xi]$ that lies over q.

$$\begin{aligned} \mathfrak{q}^+\mathbb{Z}[\xi] = \mathfrak{q} \quad &\Leftrightarrow \quad \mathfrak{q} = \overline{\mathfrak{q}} \\ &\Leftrightarrow \quad \sigma \in G_\mathfrak{q}, \text{ i.e., } G_\mathfrak{q} \text{ contains an element of order 2,} \\ &\Leftrightarrow \quad f_q \text{ is even.} \end{aligned}$$

(ii) Primes that split in $\mathbb{Z}[\xi]$: $\mathfrak{q}^+\mathbb{Z}[\xi] = \mathfrak{q}\overline{\mathfrak{q}}$ where $\mathfrak{q}$ is a prime ideal in $\mathbb{Z}[\xi]$ that lies over q.

$$\begin{aligned} \mathfrak{q}^+\mathbb{Z}[\xi] = \mathfrak{q}\overline{\mathfrak{q}} \quad &\Leftrightarrow \quad \mathfrak{q} \neq \overline{\mathfrak{q}} \\ &\Leftrightarrow \quad \sigma \notin G_\mathfrak{q}, \text{ i.e., } G_\mathfrak{q} \text{ does not contain an element of order 2,} \\ &\Leftrightarrow \quad f_q \text{ is odd.} \end{aligned}$$

(iii) The ramified case: $\mathfrak{p}^+\mathbb{Z}[\xi] = \mathfrak{p}^2$ where $\mathfrak{p} := (1-\xi)$ is the only prime ideal in $\mathbb{Z}[\xi]$ that lies over p. Moreover $\mathfrak{p}^+\mathbb{Z}[\xi] := ((1-\xi)(1-\xi^{-1})) = \mathfrak{p}\overline{\mathfrak{p}}$ is the only prime ideal in $\mathbb{Z}[\xi+\xi^{-1}]$ that lies over p.

Let $\mathcal{O}_K$ be a Dedekind ring and let S be a finite set of prime ideals $\mathfrak{q} \subseteq \mathcal{O}_K$. We define

$$\mathcal{O}_K^S := \left\{ \frac{f}{g} \;\middle|\; f, g \in \mathcal{O},\ g \not\equiv 0 \bmod \mathfrak{q} \text{ for } \mathfrak{q} \notin S \right\}.$$

Let K be the quotient field of $\mathcal{O}_K$. We call the group $(\mathcal{O}_K^S)^*$ the group of S-units of K. Let $\mathcal{C}(\mathcal{O}_K)$, resp. $\mathcal{C}(\mathcal{O}_K^S)$, denote the ideal class group of $\mathcal{O}_K$, resp. $\mathcal{O}_K^S$.

Proposition 2.1. *For the group $(\mathcal{O}_K^S)^*$ defined above we have an isomorphism*

$$(\mathcal{O}_K^S)^* \cong \mu(K) \times \mathbb{Z}^{|S|+r+s-1}$$

where $\mu(K)$ denotes the group of roots of unity of K, r denotes the number of real embeddings of K and s denotes the number of conjugate pairs of complex embeddings of K.

Proof. See Neukirch [8]. □

Therefore

$$\begin{aligned} (\mathcal{O}_K^S)^* &\cong \mu(K) \times \mathbb{Z}^{r+s-1} \times \mathbb{Z}^{|S|} \\ &\cong \mathcal{O}_K^* \times \mathbb{Z}^{|S|}. \end{aligned}$$

3. Matrices of order p

3.1. A relation between matrices and ideal classes. The results obtained in this section are based on the bijection given by Proposition 3.3. Sjerve and Yang prove in [11] the analogous statement of this proposition for the group $\mathrm{Sp}(p-1,\mathbb{Z})$. Since for our purpose it is important to understand the bijection and some proofs need a slightly different approach for the group $\mathrm{Sp}(p-1,\mathbb{Z}[1/n])$, we present in this subsection some of the proofs for the convenience of the reader.

Definition. Let I be the set of pairs $(\mathfrak{a}, a)$ where $\mathfrak{a} \subseteq \mathbb{Z}[1/n][\xi]$ is a $\mathbb{Z}[1/n][\xi]$-ideal and $0 \neq a \in \mathbb{Z}[1/n][\xi]$ is such that $\mathfrak{a}\overline{\mathfrak{a}} = (a) \subseteq \mathbb{Z}[1/n][\xi]$. Here $\overline{\mathfrak{a}}$ denotes the ideal generated by the complex conjugates of the elements of $\mathfrak{a}$. We define an equivalence relation on I.

$$\begin{aligned} (\mathfrak{a}, a) \sim (\mathfrak{b}, b) \quad \Leftrightarrow \quad &\exists \lambda, \mu \in \mathbb{Z}[1/n][\xi],\ \lambda, \mu \neq 0 \\ &\lambda\mathfrak{a} = \mu\mathfrak{b},\ \lambda\overline{\lambda}a = \mu\overline{\mu}b. \end{aligned}$$

Let $[\mathfrak{a}, a]$ denote the equivalence class of the pair $(\mathfrak{a}, a)$ and let $\mathcal{I}$ be the set of equivalence classes $[\mathfrak{a}, a]$.

Lemma 3.1. *Let $(\mathfrak{a}, a)$ be a pair consisting of a $\mathbb{Z}[1/n][\xi]$-ideal $\mathfrak{a} \subseteq \mathbb{Z}[1/n][\xi]$ and $0 \neq a \in \mathbb{Z}[1/n][\xi]$. Then $(\mathfrak{a}, a) \in I$ if and only if a $\mathbb{Z}[1/n]$-basis $\alpha_1, \ldots, \alpha_{p-1}$ of $\mathfrak{a}$ exists such that*

$$\alpha^{\mathrm{T}} J \overline{\alpha}^{(i)} = \delta_{1i} a D$$

where $D = p\xi^{(p+1)/2}/(\xi - 1)$ and $\alpha = (\alpha_1, \ldots, \alpha_{p-1})^{\mathrm{T}}$.

Proof. The proof is analogous to the proof of Lemma 2.3 in [11]. □

Lemma 3.2. *Let M, N be two $(p-1)\times(p-1)$-matrices over $\mathbb{Z}[1/n]$ and let*

$$\alpha = (\alpha_1, \ldots, \alpha_{p-1})^{\mathrm{T}} \in \mathbb{Z}[1/n][\xi]^{p-1}$$

where $\alpha_1, \ldots, \alpha_{p-1}$ are $\mathbb{Z}[1/n]$-linear independent. If for $i = 1, \ldots, p-1$

$$\alpha^{\mathrm{T}} M \overline{\alpha}^{(i)} = \alpha^{\mathrm{T}} N \overline{\alpha}^{(i)}$$

then we have $M = N$.

Proof. It suffices to prove the case $N = 0$ because

$$\alpha^{\mathrm{T}} M \overline{\alpha}^{(i)} = \alpha^{\mathrm{T}} N \overline{\alpha}^{(i)} \quad \Leftrightarrow \quad \alpha^{\mathrm{T}} (M - N) \overline{\alpha}^{(i)} = 0 = \alpha^{\mathrm{T}} 0 \overline{\alpha}^{(i)}.$$

Let $a_i = \alpha^{\mathrm{T}} M \overline{\alpha}^{(i)}$, then $a_i^{(k)} = \alpha^{(k)\mathrm{T}} M (\overline{\alpha}^{(i)})^{(k)}$. For all k, l with $1 \leqslant k, l \leqslant p-1$ let i be such that $1 \leqslant i \leqslant p-1$ and $ki \equiv l \bmod p$. Then $(\overline{\alpha}^{(i)})^{(k)} = \overline{\alpha}^{(l)}$ and therefore $\alpha^{(k)\mathrm{T}} M \overline{\alpha}^{(l)} = 0$ for $k, l = 1, \ldots, p-1$. This implies $A^{\mathrm{T}} M B = 0$ where

$$A := \left(\alpha_i^{(j)}\right) \text{ and } B := \left(\overline{\alpha}_i^{(j)}\right)$$

are $(p-1)\times(p-1)$-matrices. Since $\alpha_1, \ldots, \alpha_{p-1}$ are $\mathbb{Z}[1/n]$-linear independent we have $\det A \neq 0$ and $\det B \neq 0$. But this yields $M = 0$. □

Proposition 3.3. *A bijection ψ exists between the set of conjugacy classes of elements of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ and the set of equivalence classes of pairs $[\mathfrak{a}, a] \in \mathcal{I}$.*

In order to prove this proposition, we first construct the bijection and then we show that the mapping we constructed is a bijection (Lemma 3.5, Lemma 3.6).

Let $Y \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ be of order p. The eigenvalues of Y are the primitive pth roots of unity. An eigenvector

$$\alpha = (\alpha_1, \ldots, \alpha_{p-1})^{\mathrm{T}} \in (\mathbb{Z}[1/n][\xi])^{p-1}$$

exists for the eigenvalue $\xi = e^{i2\pi/p}$ (i.e., $Y\alpha = \xi\alpha$). The $\alpha_1, \ldots, \alpha_{p-1}$ are $\mathbb{Z}[1/n]$-linear independent. Let $\mathfrak{a}$ be the $\mathbb{Z}[1/n]$-module generated by $\alpha_1, \ldots, \alpha_{p-1}$. Let $a = D^{-1} \alpha^{\mathrm{T}} J \overline{\alpha}$. Then $\mathfrak{a} \subseteq \mathbb{Z}[1/n][\xi]$ is a $\mathbb{Z}[1/n][\xi]$-ideal and $a = \overline{a}$.

Lemma 3.4. *The pair $(\mathfrak{a}, a)$ we construct above is an element of I.*

Proof. By Lemma 3.1 it suffices to show that $\alpha^{\mathrm{T}} J \overline{\alpha}^{(i)} = 0$ for $i = 2, \ldots, p-1$. Since $Y\alpha = \xi\alpha$ we have

$$Y\alpha^{(i)} = \xi^i \alpha^{(i)} \text{ and } Y\overline{\alpha}^{(i)} = \frac{1}{\xi^i}\, \overline{\alpha}^{(i)},$$

$2 \leqslant i \leqslant p-1$. Therefore

$$\alpha^{\mathrm{T}} J\overline{\alpha}^{(i)} = \frac{\xi^i}{\xi}\,\alpha^{\mathrm{T}} Y^{\mathrm{T}} JY\overline{\alpha}^{(i)} = \frac{\xi^i}{\xi}\,\alpha^{\mathrm{T}} J\overline{\alpha}^{(i)}$$

where the last equation follows from the fact that $Y \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. Since $\xi \neq \xi^j$ we get $\alpha^{\mathrm{T}} J\overline{\alpha}^{(i)} = 0$. □

Let $Y, \widetilde{Y} \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ be matrices of odd prime order p. Let $\alpha \in (\mathbb{Z}[1/n][\xi])^{p-1}$, resp. $\beta \in (\mathbb{Z}[1/n][\xi])^{p-1}$ be an eigenvector of Y, resp. $\widetilde{Y}$, to the eigenvalue ξ, i.e., $Y\alpha = \xi\alpha$ and $\widetilde{Y}\beta = \xi\beta$. Let $\alpha = (\alpha_1, \ldots, \alpha_{p-1})^{\mathrm{T}}$, $\beta = (\beta_1, \ldots, \beta_{p-1})^{\mathrm{T}}$. Let $\mathfrak{a} \subseteq \mathbb{Z}[1/n][\xi]$, resp. $\mathfrak{b} \subseteq \mathbb{Z}[1/n][\xi]$, be the ideal with $\mathbb{Z}[1/n]$-basis $\alpha_1, \ldots, \alpha_{p-1}$, resp. $\beta_1, \ldots, \beta_{p-1}$. We define $a = D^{-1}\alpha^{\mathrm{T}} J\overline{\alpha}$ and $b = D^{-1}\beta^{\mathrm{T}} J\overline{\beta}$. We show the injectivity of ψ.

Lemma 3.5. *Let $Y, \widetilde{Y} \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ be matrices of odd prime order p. Then Y and $\widetilde{Y}$ are conjugate if and only if $[\mathfrak{a}, a] = [\mathfrak{b}, b]$.*

Proof. Let Y and $\widetilde{Y}$ be conjugate. Then $Q \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ exists such that $\widetilde{Y} = Q^{-1}YQ$. Then $Q\widetilde{Y} = YQ$ and for the eigenvector β to the eigenvalue ξ of $\widetilde{Y}$ we get

$$YQ\beta = Q\widetilde{Y}\beta = \xi Q\beta$$

and therefore $Q\beta$ is an eigenvector of Y. But α is also an eigenvector to the eigenvalue ξ of Y. So $\lambda, \mu \in \mathbb{Z}[1/n][\xi]$, $\lambda, \mu \neq 0$, exist such that

$$\lambda\alpha = \mu Q\beta = Q\mu\beta.$$

Then $\lambda\mathfrak{a} = \mu\mathfrak{b}$ and for $a = D^{-1}\alpha^{\mathrm{T}} J\overline{\alpha}$, $b = D^{-1}\beta^{\mathrm{T}} J\overline{\beta}$ we get $\lambda\overline{\lambda}a = \mu\overline{\mu}\,b$. This shows that $[\mathfrak{a}, a] = [\mathfrak{b}, b]$.

In order to show the other direction we assume that $\lambda, \mu \in \mathbb{Z}[1/n][\xi]$, $\lambda, \mu \neq 0$, exist such that $\lambda\mathfrak{a} = \mu\mathfrak{b}$ and $\lambda\overline{\lambda}a = \mu\overline{\mu}b$. Then a matrix $Q \in \mathrm{GL}(p-1, \mathbb{Z}[1/n])$ exists such that $\lambda\alpha = \mu Q\beta$. We have

$$\mu Q\widetilde{Y}\beta = \mu Q\xi\beta = \xi\mu Q\beta = \xi\lambda\alpha = \lambda Y\alpha = \mu YQ\beta$$

and therefore

$$Q\widetilde{Y}\beta = YQ\beta.$$

Since $\beta_1, \ldots, \beta_{p-1}$ are $\mathbb{Z}[1/n]$-linear independent, we have $Q\widetilde{Y} = YQ$ and herewith

$$\widetilde{Y} = Q^{-1}YQ.$$

It remains to show that $Q \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. For $i = 2, \ldots, p-1$ we have

$$\beta^{\mathrm{T}} Q^{\mathrm{T}} JQ\,\overline{\beta}^{(i)} = \frac{\lambda\overline{\lambda}^{(i)}}{\mu\overline{\mu}^{(i)}}\,\alpha^{\mathrm{T}} J\,\overline{\alpha}^{(i)} = 0 = \beta^{\mathrm{T}} J\,\overline{\beta}^{(i)}$$

and for $i = 1$ we have

$$\beta^{\mathrm{T}} Q^{\mathrm{T}} JQ\,\overline{\beta} = \frac{\lambda\overline{\lambda}}{\mu\overline{\mu}}\,\alpha^{\mathrm{T}} J\,\overline{\alpha} = \frac{b}{a}\,\alpha^{\mathrm{T}} J\,\overline{\alpha} = \beta^{\mathrm{T}} J\,\overline{\beta}$$

because $\lambda\overline{\lambda}\,a = \mu\overline{\mu}\,b$ implies that $\frac{\lambda\overline{\lambda}}{\mu\overline{\mu}} = \frac{b}{a}$. Now it follows from Lemma 3.2 that $Q^{\mathrm{T}} JQ = J$ and this means that $Q \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. □

Lemma 3.6. *The mapping ψ is surjective.*

Proof. If $(\mathfrak{a}, a)$ and $\alpha = (\alpha_1, \ldots, \alpha_{p-1})^{\mathrm{T}}$ are as in Lemma 3.1, then $\xi\alpha_1, \ldots, \xi\alpha_{p-1}$ is a new basis of $\mathfrak{a}$. Therefore $X \in \mathrm{GL}(p-1, \mathbb{Z}[1/n])$ exists with $X\alpha = \xi\alpha$. It is evident that the order of X is p. We show that $X \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. We have

$$\alpha^{\mathrm{T}} X^{\mathrm{T}} J X \overline{\alpha}^{(i)} = \frac{\xi}{\xi^i}\, \alpha^{\mathrm{T}} J \overline{\alpha}^{(i)} = \delta_{1i} \alpha^{\mathrm{T}} J\, \overline{\alpha}$$

hence

$$\alpha^{\mathrm{T}} X^{\mathrm{T}} J X\, \overline{\alpha}^{(i)} = \alpha^{\mathrm{T}} J\, \overline{\alpha}^{(i)}.$$

The last equation and Lemma 3.2 imply that $X^{\mathrm{T}} J X = J$ and therefore $X \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. □

Let $\mathcal{I}$ be the set of equivalence classes of pairs $(\mathfrak{a}, a) \in I$ defined above. We define a multiplication on $\mathcal{I}$ by

$$[\mathfrak{a}, a] \cdot [\mathfrak{b}, b] = [\mathfrak{a}\mathfrak{b}, ab].$$

The unit is $[\mathbb{Z}[1/n][\xi], 1]$ and the inverse of $[\mathfrak{a}, a]$ is $[\overline{\mathfrak{a}}, a]$ since

$$[\mathfrak{a}, a] \cdot [\overline{\mathfrak{a}}, a] = [(a), a^2] = [\mathbb{Z}[1/n][\xi], 1].$$

Lemma 3.7. *Let $(\mathfrak{a}, a) \in I$, $\lambda \in \mathbb{Z}[1/n][\xi]$, $\lambda \neq 0$. Then:*

(i) $(\lambda\mathfrak{a}, \lambda\overline{\lambda} a) \in I$.
(ii) $(\mathfrak{a}, \lambda a) \in I$ *if and only if* $\lambda \in \mathbb{Z}[1/n][\xi + \xi^{-1}]^*$.

Proof. Trivial. □

Let

$$N : \mathbb{Q}(\xi) \longrightarrow \mathbb{Q}(\xi + \xi^{-1})$$

be the norm mapping, i.e., $N(x) = x\overline{x}$ for $x \in \mathbb{Q}(\xi)$. Then

$$N(\mathbb{Z}[1/n][\xi]^*) \subseteq \mathbb{Z}[1/n][\xi + \xi^{-1}]^*.$$

Lemma 3.8. *Let $(\mathfrak{a}, a), (\mathfrak{a}, b) \in I$. Then $[\mathfrak{a}, a] = [\mathfrak{a}, b]$ if and only if*

$$\frac{a}{b} \in N(\mathbb{Z}[1/n][\xi]^*).$$

Proof. Suppose that $[\mathfrak{a}, a] = [\mathfrak{a}, b]$. Then $\lambda, \mu \in \mathbb{Z}[1/n][\xi]$, $\lambda, \mu \neq 0$, exist such that $\lambda\mathfrak{a} = \mu\mathfrak{a}$ and $\lambda\overline{\lambda}\, a = \mu\overline{\mu}\, b$. Let $u = \mu/\lambda$, then $u \in \mathbb{Z}[1/n][\xi]^*$ (since $\mathfrak{a} = (\mu/\lambda)\,\mathfrak{a}$) and $a/b = \mu\overline{\mu}/\lambda\overline{\lambda} = u\overline{u}$. This shows that $a/b \in N(\mathbb{Z}[1/n][\xi]^*)$. Now let $a/b = u\overline{u}$ for some $u \in \mathbb{Z}[1/n][\xi]^*$. Then $[\mathfrak{a}, a] = [\mathfrak{a}, u\overline{u}\, b] = [u\mathfrak{a}, u\overline{u}\, b] = [\mathfrak{a}, b]$. □

Lemma 3.9. *Let $(\mathfrak{a}, a), (\mathfrak{b}, b) \in I$ and $\lambda\mathfrak{a} = \mu\mathfrak{b}$ for some $\lambda, \mu \in \mathbb{Z}[1/n][\xi]$, $\lambda, \mu \neq 0$. Then $u \in \mathbb{Z}[1/n][\xi + \xi^{-1}]^*$ exists such that $[\mathfrak{a}, a] = [\mathfrak{b}, ub]$.*

Proof. If $\lambda\mathfrak{a} = \mu\mathfrak{b}$, then $\overline{\lambda}\overline{\mathfrak{a}} = \overline{\mu}\overline{\mathfrak{b}}$ and herewith

$$(\lambda\overline{\lambda}\, a) = \lambda\mathfrak{a}\overline{\lambda}\overline{\mathfrak{a}} = \mu\mathfrak{b}\overline{\mu}\overline{\mathfrak{b}} = (\mu\overline{\mu}\, b).$$

But then a unit $u \in \mathbb{Z}[1/n][\xi + \xi^{-1}]^*$ exists with $\lambda\overline{\lambda}\, a = \mu\overline{\mu}\, ub$. Herewith

$$[\mathfrak{a}, a] = [\lambda\mathfrak{a}, \lambda\overline{\lambda}\, a] = [\mu\mathfrak{b}, \mu\overline{\mu}\, ub] = [\mathfrak{b}, ub].$$ □

Proposition 3.10. *Let $\mathcal{C}_0$ be the ideal class group of $\mathbb{Z}[1/n][\xi]$. Then the sequence*

$$1 \longrightarrow \mathbb{Z}[1/n][\xi + \xi^{-1}]^*/N(\mathbb{Z}[1/n][\xi]^*) \xrightarrow{\delta} \mathcal{I} \xrightarrow{\eta} \mathcal{C}_0 \longrightarrow 1$$

where $\delta([u]) = [\mathbb{Z}[1/n][\xi], u]$, $\eta([\mathfrak{a}, a]) = [\mathfrak{a}]$, is a short exact sequence.

Proof. Lemma 3.8 implies that δ is injective and η is well-defined and surjective. Moreover

$$\eta(\delta([u])) = \eta([\mathbb{Z}[1/n][\xi], u]) = [\mathbb{Z}[1/n][\xi]]$$

and Lemma 3.9 implies that the kernel of η is equal to the image of δ. □

Corollary 3.11. *There are*

$$|\mathcal{C}_0| \cdot \left[\mathbb{Z}[1/n][\xi+\xi^{-1}]^* : N(\mathbb{Z}[1/n][\xi]^*)\right]$$

conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$.

Proof. This corollary is a direct consequence of Proposition 3.10 because the number of conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ is equal to the cardinality of $\mathcal{I}$. □

If $\mathbb{Z}[1/n][\xi]$ is a principal ideal domain the cardinality of $\mathcal{C}_0$ is 1 and the number of conjugacy classes of matrices of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ is given only by the index defined above. In fact we can choose $n \in \mathbb{Z}$ such that $\mathbb{Z}[1/n][\xi]$ is a principal ideal domain. Indeed let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be representatives of the ideal classes of $\mathbb{Q}(\xi)$. For $j = 1, \ldots, h$ choose $n_j \in \mathfrak{a}_j$ with $n_j \in \mathbb{Z}[1/n][\xi]$. It is possible to choose the n_j such that $n_j \in \mathbb{Z}$. Then $n = \prod_{j=1}^{h} n_j \in \mathfrak{a}_k$ for any k with $1 \leqslant k \leqslant h$. For more details see Lang [6] and Neukirch [8].

3.2. The number of conjugacy classes. Let $N : \mathbb{Q}(\xi) \longrightarrow \mathbb{Q}(\xi+\xi^{-1})$ be the norm mapping defined above. Let $n \in \mathbb{Z}$ and ξ a primitive pth root of unity. The aim of this section is to compute the number of conjugacy classes of elements of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. Therefore we use Corollary 3.11.

Kummer proved that $\mathbb{Z}[1/n][\xi]^* = \mathbb{Z}[1/n][\xi+\xi^{-1}]^* \times \langle -\xi \rangle$ where $\langle -\xi \rangle$ is the group of roots of unity in $\mathbb{Q}(\xi)$. This implies that

$$\left[\mathbb{Z}[\xi+\xi^{-1}]^* : N(\mathbb{Z}[\xi]^*)\right] = \left[\mathbb{Z}[\xi+\xi^{-1}]^* : (\mathbb{Z}[\xi+\xi^{-1}]^*)^2\right].$$

Moreover $\mathbb{Z}[\xi+\xi^{-1}]^* \cong \mathbb{Z}^{(p-3)/2} \times \mathbb{Z}/2\mathbb{Z}$ because of the Dirichlet unit theorem. Therefore

$$\left[\mathbb{Z}[\xi+\xi^{-1}]^* : N(\mathbb{Z}[\xi]^*)\right] = 2^{\frac{p-1}{2}}.$$

Since the prime above p in $\mathbb{Z}[\xi]$ is principal, generated by $1-\xi$, and the prime above p in $\mathbb{Z}[\xi+\xi^{-1}]$ is principal, generated by $N(1-\xi) = (1-\xi)(1-\xi^{-1})$, we get

$$\left[\mathbb{Z}[1/p][\xi+\xi^{-1}]^* : N(\mathbb{Z}[1/p][\xi]^*)\right] = 2^{\frac{p-1}{2}}.$$

Proposition 3.12. *Let p be an odd prime and let ξ be a primitive pth root of unity. Let S^+ be a finite set of prime ideals in $\mathbb{Z}[\xi+\xi^{-1}]$, and let S be the set of the prime ideals in $\mathbb{Z}[\xi]$ that lie over those in S^+. Then*

$$\left[\left(\mathbb{Z}[\xi+\xi^{-1}]^{S^+}\right)^* : N\left(\left(\mathbb{Z}[\xi]^S\right)^*\right)\right] = 2^{\frac{p-1}{2}+\tau}$$

where τ is the number of inert primes in S^+.

Proof. Let $S := \{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$ be a set of prime ideals in $\mathbb{Z}[\xi]$. Then the isomorphism given by the generalization of the Dirichlet unit theorem implies that for each prime ideal $\mathfrak{q}_j \in S$, $j = 1, \ldots, k$, $g_j \in \mathfrak{q}_j$ exists such that each unit $u \in (\mathbb{Z}[\xi]^S)^*$ can be written

$$u = u' g_1^{n_1} \cdots g_k^{n_k}$$

where $u' \in \mathbb{Z}[\xi]^*$, $n_j \in \mathbb{Z}$, $j = 1, \ldots, k$. We compute the index we want to know by induction on the number of primes in S^+. Let T^+ be a finite set of prime ideals in $\mathbb{Z}[\xi + \xi^{-1}]$. Let T be the set of those prime ideals in $\mathbb{Z}[\xi]$ that lie over the prime ideals in T^+. Define $S^+ := T^+ \cup \{\mathfrak{q}^+\}$ where $\mathfrak{q}^+ \subset \mathbb{Z}[\xi + \xi^{-1}]$, $\mathfrak{q}^+ \notin T^+$, is a prime ideal. Let S be the set of the prime ideals in $\mathbb{Z}[\xi]$ that lie over the prime ideals in S^+. We have the following possibilities:

(i) The prime $\mathfrak{q}^+$ is inert. Then $S = T \cup \{\mathfrak{q}\}$ where $\mathfrak{q}$ is the prime that lies over $\mathfrak{q}^+$.
(ii) The prime $\mathfrak{q}^+$ splits in $\mathbb{Z}[\xi]$. Then $S = T \cup \{\mathfrak{q}, \overline{\mathfrak{q}}\}$ where $\mathfrak{q}$, $\overline{\mathfrak{q}}$ are the primes that lie over $\mathfrak{q}^+$.
(iii) The prime $\mathfrak{q}^+$ lies over p. Then $S = T \cup \{\mathfrak{p}\}$ where $\mathfrak{p} = (1 - \xi)$, the prime over p.

We have

$$(\mathbb{Z}[\xi + \xi^{-1}]^{S^+})^* \cong (\mathbb{Z}[\xi + \xi^{-1}]^{T^+})^* \times \mathbb{Z}\,.$$

If the prime $\mathfrak{q}^+$ is inert or if it lies over p, cases (i) and (iii) above, then

$$\begin{aligned}(\mathbb{Z}[\xi]^S)^* &\cong \mathbb{Z}[\xi]^* \times \mathbb{Z}^{|S|} \cong \mathbb{Z}[\xi]^* \times \mathbb{Z}^{|T|} \times \mathbb{Z} \\ &\cong (\mathbb{Z}[\xi]^T)^* \times \mathbb{Z}\end{aligned}$$

and if the prime $\mathfrak{q}^+$ splits in $\mathbb{Z}[\xi]$, case (ii) above, then

$$(\mathbb{Z}[\xi]^S)^* \cong (\mathbb{Z}[\xi]^T)^* \times \mathbb{Z}^2.$$

We give a formula for the index

$$\left[\left(\mathbb{Z}[\xi + \xi^{-1}]^{S^+}\right)^* : N\left(\left(\mathbb{Z}[\xi]^S\right)^*\right)\right]$$

in relation to the index

$$\left[\left(\mathbb{Z}[\xi + \xi^{-1}]^{T^+}\right)^* : N\left(\left(\mathbb{Z}[\xi]^T\right)^*\right)\right].$$

If the prime $\mathfrak{q}^+$ is inert, then

$$\left[\left(\mathbb{Z}[\xi + \xi^{-1}]^{S^+}\right)^* : N\left(\left(\mathbb{Z}[\xi]^S\right)^*\right)\right] = 2\left[\left(\mathbb{Z}[\xi + \xi^{-1}]^{T^+}\right)^* : N\left(\left(\mathbb{Z}[\xi]^T\right)^*\right)\right].$$

If the prime $\mathfrak{q}^+$ splits in $\mathbb{Z}[\xi]$ or if it lies over p, then

$$\left[\left(\mathbb{Z}[\xi + \xi^{-1}]^{S^+}\right)^* : N\left(\left(\mathbb{Z}[\xi]^S\right)^*\right)\right] = \left[\left(\mathbb{Z}[\xi + \xi^{-1}]^{T^+}\right)^* : N\left(\left(\mathbb{Z}[\xi]^T\right)^*\right)\right].$$

This shows that if we add an inert prime to the set S the index is multiplied by 2, and if we add primes that split or the prime over p, then the index does not change. □

Corollary 3.13. *Let $n \in \mathbb{Z}$. Then*

$$\left[\mathbb{Z}[1/n][\xi + \xi^{-1}]^* : N(\mathbb{Z}[1/n][\xi]^*)\right] = 2^{\frac{p-1}{2} + \tau}$$

where τ is the number of inert primes in $\mathbb{Z}[\xi + \xi^{-1}]$ that lie over primes in $\mathbb{Z}$ that divide n.

Proof. Let $n \in \mathbb{Z}$ and let S^+, resp. S, be the prime ideals in $\mathbb{Z}[\xi + \xi^{-1}]$, resp. $\mathbb{Z}[\xi]$, over the primes in $\mathbb{Z}$ that divide n. Then the assumption follows directly from Proposition 3.12. □

Now we have the main result of this section.

Theorem 3.14. *There are*

$$|\mathcal{C}_0| 2^{\frac{p-1}{2}+\tau}$$

conjugacy classes of matrices of order p *in* $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$, $0 \neq n \in \mathbb{Z}$. *Here* $\mathcal{C}_0$ *is the ideal class group of* $\mathbb{Z}[1/n][\xi]$ *and* τ *is the number of inert primes in* $\mathbb{Z}[\xi+\xi^{-1}]$ *that lie over primes in* $\mathbb{Z}$ *that divide* n.

Proof. This follows directly from Corollary 3.11 and Corollary 3.13. □

4. Subgroups of order p

4.1. The quotient of the normalizer by the centralizer of subgroups of order p. The aim is to study the centralizers and normalizers of conjugacy classes of subgroups of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. We use the bijection between the set $\mathcal{I}$ of equivalence classes $[\mathfrak{a}, a]$ and the conjugacy classes of matrices of order p. Each conjugacy class of matrices generates a conjugacy class of subgroups of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. We determine the equivalence classes $[\mathfrak{a}, a]$ that correspond to the conjugacy classes of the elements of a subgroup.

Let $Y \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ be of odd prime order p. We have seen that the conjugacy class of Y corresponds to an equivalence class $[\mathfrak{a}, a]$. Let

$$\alpha = (\alpha_1, \ldots, \alpha_{p-1})^{\mathrm{T}} \in \big(\mathbb{Z}[1/n][\xi]\big)^{p-1}$$

be an eigenvector of Y to the eigenvalue $\xi = e^{i2\pi/p}$. It is obvious that $Y^l = \xi^l \alpha$. Let $\gamma_k \in \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ be such that $\gamma_k(\xi) = \xi^k$. Then $\gamma_k(\xi^l) = \xi^{kl}$. If $kl \equiv 1 \bmod p$, then $\gamma_k(\xi^l) = \xi$ and moreover

$$Y^l \gamma_k(\alpha) = \gamma_k(Y^l \alpha) = \gamma_k(\xi^l \alpha) = \gamma_k(\xi^l)\gamma_k(\alpha) = \xi^{kl}\gamma_k(\alpha) = \xi\gamma_k(\alpha).$$

So $\gamma_k(\alpha)$ is the eigenvector of Y^l to the eigenvalue ξ. Let $\mathfrak{b}$ be the ideal given by the $\mathbb{Z}[1/n]$-basis $\gamma_k(\alpha_1), \ldots, \gamma_k(\alpha_{p-1})$. Moreover let

$$b = D^{-1}(\gamma_k(\alpha))^{\mathrm{T}} J \gamma_k(\overline{\alpha}) = D^{-1}\gamma_k(\alpha^{\mathrm{T}} J \overline{\alpha}).$$

So the conjugacy class of Y^l corresponds to the equivalence class $[\mathfrak{b}, b]$ with

$$\mathfrak{b} = \gamma_k(\mathfrak{a})$$
$$b = D^{-1}\gamma_k(Da) = D^{-1}\gamma_k(D)\gamma_k(a).$$

Let S be a multiplicative set such that $S^{-1}\mathbb{Z} = \mathbb{Z}[1/n]$. Then $S^{-1}\mathbb{Z}[\xi] = \mathbb{Z}[1/n][\xi]$ and the different in $\mathbb{Z}[\xi]$ and in $\mathbb{Z}[1/n][\xi]$ are both principal ideals generated by $D = p\,\xi^{(p+1)/2}/(\xi-1)$. If $p \mid n$, then D is a unit in $\mathbb{Z}[1/n][\xi]$ since $(\xi-1)$ is a prime that divides p. If $u, v \in \mathbb{Z}[1/n][\xi]^*$ are units with $u = \overline{u}$, $v = -\overline{v}$, then $Du = -\overline{Du}$ and $Dv = \overline{Dv}$. This shows that the multiplication with D defines an isomorphism on $\mathbb{Z}[1/n][\xi]^*$ that yields a bijection between the real and the purely imaginary units.

Theorem 4.1. *Let* $n \in \mathbb{Z}$ *be such that* $\mathbb{Z}[1/n][\xi]$ *and* $\mathbb{Z}[1/n][\xi+\xi^{-1}]$ *are principal ideal domains and moreover* $p \mid n$. *Let* $N(P)$ *denote the normalizer and* $C(P)$ *the centralizer of a subgroup* P *of order* p *in* $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. *Then*

$$N(P)/C(P) \cong \mathbb{Z}/j\mathbb{Z}$$

where $j \mid p-1$, j *odd. For each* j *with* $j \mid p-1$, j *odd, there exists a subgroup of order* p *in* $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ *with* $N(P)/C(P) \cong \mathbb{Z}/j\mathbb{Z}$.

Proof. Let n be such that $\mathbb{Z}[1/n][\xi]$ is a principal ideal domain. Then the ideal $\mathfrak{a}$ in the pair $[\mathfrak{a}, a]$ is a principal ideal. If $\mathfrak{a} = (x)$, then $(x)\overline{(x)} = (x\overline{x}) = (a)$, i.e., a unit u exists such that $a = ux\overline{x}$. Then

$$[\mathfrak{a}, a] = [(x), a] = [\mathbb{Z}[1/n][\xi], u].$$

The conjugacy class of $Y \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ corresponds to $[\mathbb{Z}[1/n][\xi], u]$. We have seen that the conjugacy class of Y^l, $1 < l < p-1$, corresponds to the equivalence class $[\mathbb{Z}[1/n][\xi], D^{-1}\gamma_k(Du)]$ where $\gamma_k \in \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ is defined so that $\gamma_k(\xi^l) = \xi$. The matrices Y and Y^l are conjugate if and only if

$$[\mathbb{Z}[1/n][\xi], u] = [\mathbb{Z}[1/n][\xi], D^{-1}\gamma_k(Du)].$$

Lemma 3.8 shows that this equation is satisfied if and only if $\omega \in \mathbb{Z}[1/n][\xi]^*$ exists such that

$$D^{-1}\gamma_k(Du) = u\omega\overline{\omega}. \tag{1}$$

We know that $u \in \mathbb{Z}[1/n][\xi + \xi^{-1}]^*$ and this implies that Du is purely imaginary. First we check if $u \in \mathbb{Z}[1/n][\xi + \xi^{-1}]^*$ exists such that a special case of (1) holds, namely the case with $\omega = 1$, i.e., we try to find γ_k and u such that $\gamma_k(Du) = Du$. The automorphism $\gamma_{p-1}(= \gamma_{-1})$ has order 2, i.e., γ_{p-1} yields the complex conjugation. Since u is real and therefore Du purely imaginary, we get $\gamma_{p-1}(Du) = -Du$. This proves that neither $\gamma_k(Du) = Du$ nor (1) can be satisfied if $k = p-1$ (the image of $\omega\overline{\omega}$ under any embedding of $\mathbb{Z}[1/n][\xi]$ in $\mathbb{C}$ is a positive real number). Any automorphism $\gamma_k \in \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ generates a subgroup $\langle\gamma_k\rangle \subseteq \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ and the order of this subgroup divides $p-1$, the order of $\mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$. Let $j = |\langle\gamma_k\rangle|$ denote the order of γ_k. If j is even the order of $\gamma_k^{j/2}$ is 2 and on the other hand $\gamma_k^r(Du) = Du$ for any $1 < r < j$. This yields a contradiction and therefore $\gamma_k(Du) = Du$ cannot be satisfied if the order of γ_k is even. This implies that if γ_k and u exist with $\gamma_k(Du) = Du$, then the order of γ_k is odd.

The main theorem of Galois theory says that a subfield $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\xi)$ corresponds to the subgroup $\langle\gamma_k\rangle \subseteq \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ and that

$$K = \{x \in \mathbb{Q}(\xi) \mid \forall \gamma_{k^r} \in \langle\gamma_k\rangle,\ \gamma_{k^r}(x) = x\}.$$

Let $n \in \mathbb{Z}$ with $p \mid n$, We have seen that in this case $D = p\xi^{(p+1)/2}/(\xi - 1)$ is a unit in $\mathbb{Z}[1/n][\xi]$. We also know that $D = -\overline{D}$. Let $\gamma_k \in \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ be of odd order j. Since complex conjugation commutes with the Galois automorphisms, we get for any r, $1 \leqslant r \leqslant j$, $\gamma_{k^r}(D) = -\overline{\gamma_{k^r}(D)}$. Since j is odd,

$$\prod_{r=1}^{j} \gamma_{k^r}(D) = (-1)^j \prod_{r=1}^{j} \gamma_{k^r}(\overline{D}) = -\prod_{r=1}^{j} \gamma_{k^r}(\overline{D}).$$

Moreover this product is invariant under γ_k since

$$\gamma_k\Big(\prod_{r=1}^{j} \gamma_{k^r}(D)\Big) = \prod_{r=1}^{j} \gamma_k\big(\gamma_{k^r}(D)\big) = \prod_{r=1}^{j} \gamma_{k^r}(D).$$

Now consider the composition $\gamma_k \circ \gamma_{p-1} = \gamma_{-k}$ where the order of γ_k is odd. The order of γ_{-k} is even and $\langle\gamma_k\rangle$ is a subgroup of $\langle\gamma_{-k}\rangle$. Let L denote the subfield $\mathbb{Q} \subseteq L \subseteq K \subseteq \mathbb{Q}(\xi)$ corresponding to $\langle\gamma_{-k}\rangle$. Sinnott constructs in [10] cyclotomic units in any subfield L of $\mathbb{Q}(\xi_m)$ where ξ_m is a mth root of unity. This means that units exist in L, that are contained in no subfield of L. Let $v \in L$ be such a unit

$(v \in \mathbb{Z}[\xi])$. Then $\gamma_{p-1}(v) = v$, $\gamma_k(v) = v$ since $\langle \gamma_{-k} \rangle$ fixes the elements of L. Let $w := \prod_{r=1}^{j-1} \gamma_{k^r}(D) \in \mathbb{Z}[1/n][\xi]$. Then

$$w = \prod_{r=1}^{j-1} \gamma_{k^r}(D) = (-1)^{j-1} \prod_{r=1}^{j-1} \overline{\gamma_{k^r}(D)} = \overline{w}$$

since j is odd. Moreover $Dw = \prod_{r=1}^{j} \gamma_{k^r}(D)$ and therefore $\gamma_k(Dw) = Dw$. We have $Dw = -\overline{Dw}$ since $w = \overline{w}$. Now $wv = \overline{wv}$ is a unit. Let $u = wv$, then the construction implies that

$$\gamma_k(Du) = \gamma_k(Dwv) = Dwv = Du.$$

So for any $\gamma_k \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ of odd order, we found $u \in \mathbb{Z}[1/n][\xi + \xi^{-1}]^*$ with $\gamma_k(Du) = Du$ and such that

$$[\mathbb{Z}[1/n][\xi], u] = [\mathbb{Z}[1/n][\xi], D^{-1}\gamma_k(Du)].$$

If $Y \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ is in the corresponding equivalence class then this is also true for Y^l with l such that $\gamma_k(\xi^l) = \xi$. If Y is conjugate to Y^l with $\gamma_k(\xi^l) = \xi$, then Y is also conjugate to Y^{l^r} where $1 \leqslant r \leqslant j$ and j is the order of γ_k. Indeed $\gamma_{k^r}(\xi^{l^r}) = \xi$ for $1 \leqslant r \leqslant j$ and therefore $l^j \equiv 1 \bmod p$ (since $\gamma_{k^j} = id$) and $Y^{l^j} = Y$ because the order of Y is p. The l^r form a cyclic subgroup of $\mathbb{Z}/p\mathbb{Z}$.

Let $k, l \in \mathbb{Z}$ be as above, i.e., $\gamma_k(\xi^l) = \xi$. Let $\gamma_l \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ with $\gamma_l(\xi) = \xi^l$. Then $\gamma_l = \gamma_k^{-1}$ and if j is the order of γ_k, then j is also the order of γ_l. Therefore $l^j \equiv 1 \bmod p$. This means that $Y^{l^j} = Y$ and the Y^{l^r}, $1 \leqslant r \leqslant j$ are conjugate to Y. We know that j is odd and $j \mid p-1$.

If j elements are conjugate in the subgroup generated by $Y \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$, and if j is maximal with this property, then for this subgroup $N(P)/C(P) \cong \mathbb{Z}/j\mathbb{Z}$ since $\langle \gamma_k \rangle \cong \mathbb{Z}/j\mathbb{Z}$. Since we showed that for any odd divisor $j \mid p-1$ a matrix $Y \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ exists for which j powers are conjugate, we showed that for any $j \mid p-1$, j odd, a subgroup of order p exists in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$, for which $N(P)/C(P) \cong \mathbb{Z}/j\mathbb{Z}$. □

4.2. The centralizer of subgroups of order p.

Theorem 4.2. *Let $n \in \mathbb{Z}$ be such that $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi + \xi^{-1}]$ are principal ideal domains. Then for a subgroup P of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$, the centralizer $C(P)$ is*

$$C(P) \cong \mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}^{\sigma^+}.$$

Here $\sigma^+ = \sigma$ if $p \nmid n$, $\sigma^+ = \sigma + 1$ if $p \mid n$ and σ is the number of primes in $\mathbb{Z}[\xi + \xi^{-1}]$ that split in $\mathbb{Z}[\xi]$ and lie over primes in $\mathbb{Z}$ that divide n.

Proof. Let $Y \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ be of order p and let $[\mathfrak{a}, a]$ be the equivalence class corresponding to the conjugacy class of Y. Let P be the subgroup generated by Y. Let $Z \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ be an element of the centralizer of Y, i.e., $Z^{-1}YZ = Y$ or $YZ = ZY$. Then Z is an element of the centralizer of P. If α is an eigenvector of Y to the eigenvalue ξ, then so is $Z\alpha$:

$$\xi Z\alpha = Z\xi\alpha = ZY\alpha = YZ\alpha.$$

But this means that $Z\alpha = w\alpha$ for some $w \in \mathbb{Z}[1/n][\xi]$ and w is a unit since Z is invertible. Therefore

$$\begin{aligned}(Z\alpha)^{\mathrm{T}} J\overline{Z\alpha}^{(i)} &= \alpha^{\mathrm{T}} Z^{\mathrm{T}} JZ\overline{\alpha}^{(i)} = w\alpha^{\mathrm{T}} J\overline{w}^{(i)}\overline{\alpha}^{(i)} \\ &= w\overline{w}^{(i)}\alpha^{\mathrm{T}} J\overline{\alpha}^{(i)} = \delta_{1i} a w\overline{w}^{(i)} D\end{aligned}$$

and, since $\delta_{1i} = 0$ for $i \neq 1$, we get

$$(Z\alpha)^{\mathrm{T}} J\overline{Z\alpha} = aw\overline{w}D.$$

But $Z \in \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ and therefore

$$(Z\alpha)^{\mathrm{T}} J\overline{Z\alpha} = \alpha^{\mathrm{T}} Z^{\mathrm{T}} JZ\overline{\alpha} = \alpha^{\mathrm{T}} J\overline{\alpha} = aD.$$

This implies that $w\overline{w} = 1$. In order to determine the centralizer $C(P)$ of a subgroup $P \subseteq \mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ of order p, we have to find the units $w \in \mathbb{Z}[1/n][\xi]^*$ that satisfy $w\overline{w} = 1$. This corresponds to the kernel of the norm mapping

$$\begin{array}{rccc} N: & \mathbb{Z}[1/n][\xi]^* & \longrightarrow & \mathbb{Z}[1/n][\xi+\xi^{-1}]^* \\ & x & \longmapsto & x\overline{x}. \end{array}$$

Brown [1] and Sjerve and Yang [11] showed that the kernel of the norm mapping

$$\begin{array}{rccc} N': & \mathbb{Z}[\xi]^* & \longrightarrow & \mathbb{Z}[\xi+\xi^{-1}]^* \\ & x & \longmapsto & x\overline{x} \end{array}$$

is the set of roots of unity

$$\ker(N') = \{\pm\xi^r \mid \xi^p = 1, 1 \leqslant r \leqslant p\}.$$

It is obvious that $\ker(N') \subseteq \ker(N)$. The prime ideals that lie over the primes in $\mathbb{Z}$ and divide n yield units in $\mathbb{Z}[1/n][\xi]^* \setminus \mathbb{Z}[\xi]^*$. Let $\mathfrak{q}^+ \subseteq \mathbb{Z}[\xi+\xi^{-1}]$ be a prime over a prime $q \mid n$ and let $\mathfrak{q} \subseteq \mathbb{Z}[\xi]$ be a prime over $\mathfrak{q}^+$. If $\mathfrak{q}^+$ is inert, then $\mathfrak{q} = \overline{\mathfrak{q}}$ and if $\mathfrak{q}^+$ splits, then $\mathfrak{q}^+\mathbb{Z}[\xi] = \mathfrak{q}\overline{\mathfrak{q}}$. A generalization for S-units of the Dirichlet unit theorem says that for each prime $\mathfrak{q}_j$, $j = 1, \ldots, k$, over n a $g_j \in \mathfrak{q}_j$ exists such that any unit $u \in (\mathbb{Z}[1/n][\xi])^*$ can be written as

$$u = u' g_1^{n_1} \cdots g_k^{n_k}$$

where $u' \in \mathbb{Z}[\xi]^*$, $n_j \in \mathbb{Z}$, $j = 1, \ldots, k$. So the group of units $\mathbb{Z}[1/n][\xi+\xi^{-1}]^*$ is generated by $\mathbb{Z}[\xi+\xi^{-1}]^*$, the inert primes over n, the primes over n that split and, if $p \mid n$, the prime over p. The inert primes yield nontrivial elements in $\mathbb{Z}[1/n][\xi+\xi^{-1}]^*/N(\mathbb{Z}[1/n][\xi]^*)$ since for those holds $w\overline{w} = w^2 \neq 1$ for $w \neq \pm 1$. The centralizer $C(P)$ is a finitely generated group whose torsion subgroup is isomorphic to the group of roots of unity in $\mathbb{Q}(\xi)$ and whose rank is equal to σ if $p \nmid n$ and to $\sigma + 1$ if $p \mid n$ where

$$\sigma^+ = \mathrm{rank}\big(\mathbb{Z}[1/n][\xi]^*\big) - \mathrm{rank}\big(\mathbb{Z}[1/n][\xi+\xi^{-1}]^*\big).$$

This difference is equal to the number of primes in $\mathbb{Z}[\xi+\xi^{-1}]$ that split or ramify in $\mathbb{Z}[\xi]$ and lie over primes in $\mathbb{Z}$ that divide n. This follows directly from a generalization of the Dirichlet unit theorem and proves our theorem. □

4.3. The action of the normalizer on the centralizer of subgroups of order *p*.

Theorem 4.3. *Let $N(P)$ be the normalizer and $C(P)$ the centralizer of a subgroup P of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. Let p be an odd prime, ξ a primitive pth root of unity, $n \in \mathbb{Z}$ such that $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi + \xi^{-1}]$ are principal ideal domains and moreover $p \mid n$. Then the action of $N(P)/C(P)$ on $C(P)$ is given by the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ on the group of units $\mathbb{Z}[1/n][\xi]^*$. Moreover $N(P)/C(P)$ acts faithfully on $C(P)$.*

Proof. We have seen in the proof of Theorem 4.2 that the centralizer of a subgroup of order p in $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$ is given by the kernel of the norm mapping $\mathbb{Z}[1/n][\xi]^* \longrightarrow \mathbb{Z}[1/n][\xi + \xi^{-1}]^*$, $x \longmapsto x\overline{x}$. Herewith the centralizer is isomorphic to a subgroup of the group of units $\mathbb{Z}[1/n][\xi]^*$. In the proof of Theorem 4.1 we identify the quotient $N(P)/C(P)$ with a subgroup of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$. Herewith the action of the quotient $N(P)/C(P)$ on the centralizer $C(P)$ is given by the action of the subgroup of $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ corresponding to $N(P)/C(P)$ on the kernel of the norm mapping $\mathbb{Z}[1/n][\xi]^* \longrightarrow \mathbb{Z}[1/n][\xi + \xi^{-1}]^*$. Since it is nontrivial, the action of $N(P)/C(P)$ on $C(P)$ is faithful. □

References

[1] Brown, Kenneth S. Euler characteristics of discrete groups and G-spaces. *Invent. Math.* **27** (1974), 229–264. MR0385007 (52 #5877), Zbl 0294.20047.

[2] Brown, Kenneth S. Cohomology of groups. Graduate Texts in Mathematics, 87. *Springer-Verlag, New York-Berlin*, 1982. MR0672956 (83k:20002), Zbl 0584.20036.

[3] Busch, Cornelia. Symplectic characteristic classes. *Enseign. Math.* (2) **47** (2001), no. 1-2, 115–130. MR1844897 (2002f:20068), Zbl 1065.20060.

[4] Busch, Cornelia. The Farrell cohomology of $\mathrm{Sp}(p-1, \mathbb{Z})$. *Documenta Mathematica* **7** (2002), 239–254. MR1938122 (2003i:20082), Zbl 1025.20033.

[5] Busch, Cornelia. On p-periodicity in the Farrell cohomology of $\mathrm{Sp}(p-1, \mathbb{Z}[1/n])$. Preprint (2005).

[6] Lang, Serge. Algebraic number theory. *Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont.*, 1970. MR0282947 (44 #181), Zbl 0211.38404.

[7] Naffah, Nadim. On the integral Farrell cohomology ring of $\mathrm{PSL}_2(\mathbb{Z}[1/n])$. Diss. ETH No. 11675, *ETH, Zürich*, 1996.

[8] Neukirch, Jürgen. Algebraic number theory. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der mathematischen Wissenschaften, 322. *Springer-Verlag, Berlin*, 1999. MR1697859 (2000m:11104), Zbl 0956.11021.

[9] Serre, Jean-Pierre. Local fields. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. *Springer-Verlag, New York-Berlin*, 1979. MR0554237 (82e:12016), Zbl 0423.12016.

[10] Sinnott, Warren. On the Stickelberger ideal and the circular units of an abelian field. *Invent. Math.* **62** (1980), 181–234. MR0595586 (82i:12004), Zbl 0465.12001.

[11] Sjerve, Denis; Yang, Qingjie. Conjugacy classes of p-torsion in $\mathrm{Sp}_{p-1}(\mathbb{Z})$. *J. Algebra* **195** (1997), 580–603. MR1469641 (98k:20082), Zbl 0888.20024.

[12] Washington, Lawrence C. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. *Springer-Verlag, New York*, 1997. MR1421575 (97h:11130), Zbl 0966.11047.

KATHOLISCHE UNIVERSITÄT EICHSTÄTT-INGOLSTADT, MGF, D-85071 EICHSTÄTT, GERMANY
cornelia.busch@ku-eichstaett.de

This paper is available via http://nyjm.albany.edu/j/2006/12-10.html.