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

Cornelia Minette Busch*

September 2005

Abstract

For any odd prime $p$ we consider representations of a group of order $p$ in the symplectic group $\text{Sp}(p-1, \mathbb{Z}[1/n])$ 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 $\mathbb{Z}[1/n]$. This is used for the study of these classes. In particular we determine the centralizer $C(P)$ and $N(P)/C(P)$ where $N(P)$ denotes the normalizer.

2000 Mathematics Subject Classification: 20G05, 20G10
Keywords: Representation theory, Cohomology theory

1 Introduction

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

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

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

*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.
Theorem 3.14. The number of conjugacy classes of matrices of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n]), 0 \neq n \in \mathbb{Z}$, is

$$|C_0|2^{\frac{p-1}{2}} + \tau$$

where $C_0$ is the ideal class group of $\mathbb{Z}[1/n][\xi]$ and $\tau$ is the number of inert primes in $\mathbb{Z}[\xi \pm \xi^{-1}]$ 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 $\mathbb{Z}[1/n][\xi]$, $\xi$ a primitive $p$th root of unity, and the conjugacy classes of matrices of order $p$. We define equivalence classes $[a,a]$ of pairs $(a,a)$ where $a \subseteq \mathbb{Z}[1/n][\xi]$ is an ideal with $a\overline{a} = (a)$ and the equivalence relation is

$$(a,a) \sim (b,b) \iff \exists \lambda, \mu \in \mathbb{Z}[1/n][\xi] \setminus \{0\} \lambda a = \mu b, \lambda \overline{a} = \mu \overline{b}.$$

We show that a bijection exists between the conjugacy classes of elements of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n])$ and the set of equivalence classes $[a,a]$. Sjerve and Yang (see [11]) construct an analogous bijection for $\text{Sp}(p-1, \mathbb{Z})$. We use the bijection described above in order to study the subgroups of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n])$. We consider the case where $n \in \mathbb{Z}$ is such that $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi \pm \xi^{-1}]$ 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 $\mathbb{Z}[1/n][\xi \pm \xi^{-1}]$ are principal ideal domains. Then the centralizer $C(P)$ of a subgroup $P$ of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n])$ is

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

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

Theorem 4.2. Let $n \in \mathbb{Z}$ be such that $\mathbb{Z}[1/n][\xi]$ and $\mathbb{Z}[1/n][\xi \pm \xi^{-1}]$ 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 $\text{Sp}(p-1, \mathbb{Z}[1/n])$. 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, exists a subgroup of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n])$ with $N(P)/C(P) \cong \mathbb{Z}/j\mathbb{Z}$.

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

Let $U((p-1)/2) \subseteq \text{GL}((p-1)/2, \mathbb{C})$ be the group of unitary matrices.

We consider the homomorphism

$$U\left(\frac{p-1}{2}\right) \longrightarrow \text{Sp}(p-1, \mathbb{R})$$

$$X = A + iB \longmapsto \begin{pmatrix} A & B \\ -B & A \end{pmatrix}$$
where $A, B \in M(n, \mathbb{R})$. 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 $\text{Sp}(p-1, \mathbb{Z})$. This is used in [4] to analyze the subgroups of order $p$ in $\text{Sp}(p-1, \mathbb{Z})$ by considering the corresponding subgroups in $U((p-1)/2)$. 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 $\xi$ be a primitive $p$th 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 $\gamma_j \in \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ be given by $\gamma_j(\xi) = \xi^j$. To simplify the notations, we define $x^{(i)} := \gamma_j(x)$ for any $x \in \mathbb{Q}(\xi)$ and $\gamma_j \in \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ as above. The Galois automorphism $\gamma_j$ 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 $a$ be an additive subgroup of $L$. The complementary set $a'$ of $a$ is the set of $x \in L$ such that $\text{tr}_{L/K}(xa) \subseteq A$. The different of the extension $B/A$ is defined to be

$$DB/A := B'_{L/K}.$$  

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 $G = \text{Gal}(K/\mathbb{Q})$ be the Galois group of the extension and let $q$ be a prime ideal of $\mathcal{O}$. The subgroup

$$G_q = \{ \sigma \in G \mid \sigma q = q \}$$

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

$$Z_q = \{ x \in K \mid \sigma x = x \text{ for all } \sigma \in G_q \}$$

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

$$q^{f_q} \equiv 1 \mod p.$$
Then \((q) = (q_1 \cdots q_r)\) where \(q_1, \ldots, q_r\) are pairwise different prime ideals in \(\mathbb{Q}(\xi)\) and all have residue class degree \(f_q\) (see Neukirch [8]).

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

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

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

The ramified case: \(p^+ \mathbb{Z}[\xi] = p^2\) where \(p := (1 - \xi)\) is the only prime ideal in \(\mathbb{Z}[\xi]\) that lies over \(p\). Moreover \(p^+ \mathbb{Z}[\xi] := ((1 - \xi)(1 - \xi^{-1})) = p\bar{p}\) 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 \(q \subseteq \mathcal{O}_K\). We define

\[
\mathcal{O}_K^S := \left\{ \frac{f}{g} \mid f, g \in \mathcal{O}_K, g \not\equiv 0 \mod q \text{ for } q \not\subseteq S \right\}.
\]

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 \(\mathcal{C}(\mathcal{O}_K), \mathcal{C}(\mathcal{O}_K^S)\), 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

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

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].
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 $\text{Sp}(p-1,\mathbb{Z})$. Since for our purpose it is important to understand the bijection and some proofs need a slightly different approach for the group $\text{Sp}(p-1,\mathbb{Z}[1/n])$, we present in this subsection some of the proofs for the convenience of the reader.

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

$$(a, a) \sim (b, b) \iff \exists \lambda, \mu \in \mathbb{Z}[1/n][\xi], \lambda, \mu \neq 0 \lambda a = \mu b, \lambda \lambda a = \mu \mu b.$$ 

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

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

$$\alpha^T J\overline{\alpha}(i) = \delta_{i,1} aD$$

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

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

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

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

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

then we have $M = N$.

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

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

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

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

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 $M = 0$. \hfill \Box

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

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 $Y \in \text{Sp}(p-1, \mathbb{Z}[1/n])$ be of order $p$. The eigenvalues of $Y$ are the primitive $p$th roots of unity. An eigenvector $\alpha = (\alpha_1, \ldots, \alpha_{p-1})^T \in (\mathbb{Z}[1/n])^{p-1}$ exists for the eigenvalue $\xi = e^{2\pi i/p}$, i.e. $Y \alpha = \xi \alpha$. The $\alpha_1, \ldots, \alpha_{p-1}$ are $\mathbb{Z}[1/n]$-linear independent. Let $a$ be the $\mathbb{Z}[1/n]$-module generated by $\alpha_1, \ldots, \alpha_{p-1}$. Let $a = D^{-1} \alpha^T J \overline{\alpha}$. Then $a \subseteq \mathbb{Z}[1/n][\xi]$ is a $\mathbb{Z}[1/n][\xi]$-ideal and $a = \overline{a}$.

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

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

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

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

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

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

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

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


Proof. Let \( Y \) and \( \tilde{Y} \) be conjugate. Then \( Q \in \text{Sp}(p-1, \mathbb{Z}[1/n]) \) exists such that \( \tilde{Y} = Q^{-1}YQ \). Then \( Q\tilde{Y} = YQ \) and for the eigenvector \( \beta \) to the eigenvalue \( \xi \) of \( \tilde{Y} \) we get
\[
YQ\beta = Q\tilde{Y}\beta = \xi Q\beta
\]
and therefore \( Q\beta \) is an eigenvector of \( Y \). But \( \alpha \) is also an eigenvector to the eigenvalue \( \xi \) of \( Y \). So \( \lambda,\mu \in \mathbb{Z}[1/n][\xi], \lambda, \mu \neq 0 \), exist such that
\[
\lambda\alpha = \mu Q\beta = Q\mu\beta.
\]
This shows that \( [a,a] = [b,b] \).

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 \( \lambda a = \mu b \) and \( \lambda \lambda a = \mu \mu b \). Then a matrix \( Q \in \text{GL}(p-1, \mathbb{Z}[1/n]) \) exists such that \( \lambda a = \mu Q\beta \). We have
\[
\mu Q\tilde{Y}\beta = \mu Q\xi\beta = \xi \mu Q\beta = \xi \lambda \alpha = \lambda Y \alpha = \mu YQ\beta
\]
and therefore
\[
Q\tilde{Y}\beta = YQ\beta.
\]
Since \( \beta_1,\ldots,\beta_{p-1} \) are \( \mathbb{Z}[1/n] \)-linear independent, we have \( Q\tilde{Y} = YQ \) and herewith
\[
\tilde{Y} = Q^{-1}YQ.
\]
It remains to show that \( Q \in \text{Sp}(p-1, \mathbb{Z}[1/n]) \). For \( i = 2,\ldots,p-1 \) we have
\[
\beta^T Q^T JQ \beta(i) = \frac{\lambda \lambda}{\mu \mu} \alpha^T J \alpha(i) = 0 = \beta^T J \beta(i)
\]
and for \( i = 1 \) we have
\[
\beta^T Q^T JQ \beta = \frac{\lambda \lambda}{\mu \mu} \alpha^T J \alpha = \frac{b}{a} \alpha^T J \alpha = \beta^T J \beta
\]
because \( \lambda \lambda a = \mu \mu b \) implies that \( \frac{\lambda \lambda}{\mu \mu} = \frac{b}{a} \). Now it follows from Lemma 3.2 that \( Q^T JQ = J \) and this means that \( Q \in \text{Sp}(p-1, \mathbb{Z}[1/n]) \).

**Lemma 3.6.** The mapping \( \psi \) is surjective.

Proof. Let \( (a,a) \) and \( \alpha = (\alpha_1,\ldots,\alpha_{p-1})^T \) be be like in Lemma 3.1. Then \( \xi \alpha_1,\ldots,\xi \alpha_{p-1} \) is a new basis of \( a \). Therefore \( X \in \text{GL}(p-1, \mathbb{Z}[1/n]) \) exists with \( X\alpha = \xi \alpha \). It is evident that the order of \( X \) is \( p \). We show that \( X \in \text{Sp}(p-1, \mathbb{Z}[1/n]) \). We have
\[
\alpha^T X^T JX \alpha(i) = \frac{\xi}{\xi \xi} \alpha^T J \alpha(i) = \delta_{1i} \alpha^T J \alpha
\]
hence
\[\alpha^T X^T J X \overline{\alpha(i)} = \alpha^T J \overline{\alpha(i)} .\]

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

Let \(\mathcal{I}\) be the set of equivalence classes of pairs \((a, a) \in I\) defined above. We define a multiplication on \(\mathcal{I}\) by
\[ [a, a] \cdot [b, b] = [ab, ab]. \]

The unit is \([\mathbb{Z}[1/n][\xi], 1]\) and the inverse of \([a, a]\) is \([\overline{a}, a]\) since
\[ [a, a] \cdot [\overline{a}, a] = [(a), a^2] = [\mathbb{Z}[1/n][\xi], 1]. \]

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

i) \((\lambda a, \lambda \overline{a}) \in I,\)

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

**Proof.** Trivial.

Let
\[ N : \mathbb{Q}(\xi) \rightarrow \mathbb{Q}(\xi + \xi^{-1}) \]
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 \((a, a), (a, b) \in I.\) Then \([a, a] = [a, b] \text{ if and only if }\)
\[ \frac{a}{b} \in N(\mathbb{Z}[1/n][\xi]^*). \]

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

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

**Proof.** If \(\lambda a = \mu b,\) then \(\lambda \overline{a} = \mu \overline{b}\) and herewith
\[ (\lambda \overline{a}) = \lambda a \overline{a} = \mu b \overline{b} = (\mu \overline{a} b).\]

But then a unit \(u \in \mathbb{Z}[1/n][\xi + \xi^{-1}]^* \text{ exists with } \lambda \overline{a} = \mu \overline{a} ub.\) Herewith
\[ [a, a] = [\lambda a, \lambda \overline{a} a] = [\mu b, \mu \overline{a} ub] = [b, ub].\]
Proposition 3.10. Let $C_0$ be the ideal class group of $\mathbb{Z}[1/n][\xi]$. Then the sequence

$$1 \rightarrow \mathbb{Z}[1/n][\xi + \xi^{-1}]^*/N(\mathbb{Z}[1/n][\xi]^*) \xrightarrow{\delta} \mathcal{I} \twoheadrightarrow C_0 \rightarrow 1$$

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

Proof. Lemma 3.8 implies that $\delta$ is injective and $\eta$ 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 $\eta$ is equal to the image of $\delta$. □

Corollary 3.11. The number of conjugacy classes of matrices of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n])$ is equal to

$$|C_0| \cdot (\mathbb{Z}[1/n][\xi + \xi^{-1}]^*/N(\mathbb{Z}[1/n][\xi]^*))$$

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

If $\mathbb{Z}[1/n][\xi]$ is a principal ideal domain the cardinality of $C_0$ is 1 and the number of conjugacy classes of matrices of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n])$ 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 $a_1, \ldots, a_h$ be representatives of the ideal classes of $\mathbb{Q}(\xi)$. For $j = 1, \ldots, h$ choose $n_j \in a_j$ 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 $n = \prod_{j=1}^h n_j \in a_k$ for any $k$ with $1 \leq k \leq h$. For more details see Lang [6] and Neukirch [8].

3.2 The number of conjugacy classes

Let $N : \mathbb{Q}(\xi) \rightarrow \mathbb{Q}(\xi + \xi^{-1})$ be the norm mapping defined above. Let $n \in \mathbb{Z}$ and $\xi$ a primitive $p$th root of unity. This is the aim of this section is to compute the number of conjugacy classes of elements of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n])$. 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

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

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

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

**Proposition 3.12.** Let \( p \) be an odd prime and let \( \xi \) be a primitive \( p \)th 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
\[
[(\mathbb{Z}[\xi + \xi^{-1}]|S^+|^*: N((\mathbb{Z}[\xi]|S|^*))] = 2^{\frac{p-1}{2} + \tau}
\]
where \( \tau \) is the number of inert primes in \( S^+ \).

**Proof.** Let \( S := \{q_1, \ldots, q_k\} \) 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 \( q_j \in S, j = 1, \ldots, k, g_j \in q_j \) 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 \( S^+ := T^+ \cup \{q^+\} \) where \( q^+ \in \mathbb{Z}[\xi + \xi^{-1}], q^+ \not\in T^+ \), 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 \( q^+ \) is inert. Then \( S = T \cup \{q\} \) where \( q \) is the prime that lies over \( q^+ \).

ii) The prime \( q^+ \) splits in \( \mathbb{Z}[\xi] \). Then \( S = T \cup \{q, \overline{q}\} \) where \( q, \overline{q} \) are the primes that lie over \( q^+ \).

iii) The prime \( q^+ \) lies over \( p \). Then \( S = T \cup \{p\} \) where \( p = (1 - \xi) \), 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 \( q^+ \) is inert or if it lies over \( p \), cases i) and iii) above, then
\[
(\mathbb{Z}[\xi]|S|^*) \cong Z[\xi]^* \times Z[|S|] \cong Z[\xi]^* \times Z[|T|] \times \mathbb{Z}
\]
\[
\cong (\mathbb{Z}[\xi]|T|^*) \times \mathbb{Z}
\]
and if the prime \( q^+ \) 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
\[
\left[ (\mathbb{Z}[\xi + \xi^{-1}]^{S+})^* : N((\mathbb{Z}[\xi]^{S})^*) \right]
\]
in relation to the index
\[
\left[ (\mathbb{Z}[\xi + \xi^{-1}]^{T+})^* : N((\mathbb{Z}[\xi]^{T})^*) \right].
\]
If the prime \( q^+ \) is inert, then
\[
\left[ (\mathbb{Z}[\xi + \xi^{-1}]^{S+})^* : N((\mathbb{Z}[\xi]^{S})^*) \right] = 2 \left[ (\mathbb{Z}[\xi + \xi^{-1}]^{T+})^* : N((\mathbb{Z}[\xi]^{T})^*) \right].
\]
If the prime \( q^+ \) splits in \( \mathbb{Z}[\xi] \) or if it lies over \( p \), then
\[
\left[ (\mathbb{Z}[\xi + \xi^{-1}]^{S+})^* : N((\mathbb{Z}[\xi]^{S})^*) \right] = \left[ (\mathbb{Z}[\xi + \xi^{-1}]^{T+})^* : N((\mathbb{Z}[\xi]^{T})^*) \right].
\]
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.

**Theorem 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 \( \tau \) 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.

**Theorem 3.14.** The number of conjugacy classes of matrices of order \( p \) in \( \text{Sp}(p-1, \mathbb{Z}[1/n]) \), \( 0 \neq n \in \mathbb{Z} \), is
\[
|C_0|2^{\frac{p-1}{2}+\tau}
\]
where \( C_0 \) is the ideal class group of \( \mathbb{Z}[1/n][\xi] \) and \( \tau \) 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 Theorem 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 \( \text{Sp}(p-1, \mathbb{Z}[1/n]) \). We use the bijection between...
the set \( \mathcal{I} \) of equivalence classes \([a,a]\) and the conjugacy classes of matrices of order \( p \). Each conjugacy class of matrices generates a conjugacy class of subgroups of order \( p \) in \( \text{Sp}(p-1,\mathbb{Z}[1/n]) \). We determine the equivalence classes \([a,a]\) that correspond to the conjugacy classes of the elements of a subgroup.

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

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

be an eigenvector of \( Y \) to the eigenvalue \( \xi = e^{i2\pi/p} \). It is obvious that \( Y^\ell \alpha = \xi^\ell \alpha \). Let \( \gamma_k \in \text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q}) \) be such that \( \gamma_k(\xi) = \xi^k \). Then \( \gamma_k(\xi^\ell) = \xi^{k\ell} \).

If \( kl \equiv 1 \mod p \), then \( \gamma_k(\xi^\ell) = \xi \) and moreover

\[
Y^\ell \gamma_k(\alpha) = \gamma_k(Y^\ell \alpha) = \gamma_k(\xi^\ell \alpha) = \gamma_k(\xi^\ell) \gamma_k(\alpha) = \xi^{k\ell} \gamma_k(\alpha) = \xi \gamma_k(\alpha).
\]

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

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

So the conjugacy class of \( Y^\ell \) corresponds to the equivalence class \([b,b]\) with

\[
b = \gamma_k(\alpha)
\]

\[
b = D^{-1} \gamma_k(Da) = D^{-1} \gamma_k(D) \gamma_k(a).
\]

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 \( p \nmid n \), 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 \( u = \overline{\alpha}, v = -\overline{\alpha} \), then \( Du = -D\overline{u} \) and \( Dv = D\overline{v} \). 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 \( p \nmid n \). Let \( N(P) \) denote the normalizer and \( C(P) \) the centralizer of a subgroup \( P \) of order \( p \) in \( \text{Sp}(p-1,\mathbb{Z}[1/n]) \).

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, exists a subgroup of order \( p \) in \( \text{Sp}(p-1,\mathbb{Z}[1/n]) \) 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 \( a \) in the pair \([a,a]\) is a principal ideal. If \( a = (x) \), then \((x) \overline{(x)} = (x\overline{x}) = (a)\), i.e. a unit \( u \) exists such that \( a = ux\overline{x} \). Then

\[
[a,a] = [(x), a] = [\mathbb{Z}[1/n][\xi], u].
\]
The conjugacy class of $Y \in \text{Sp}(p - 1, \mathbb{Z}[1/n])$ corresponds to $[\mathbb{Z}[1/n][\xi], u]$. For $1 < l < p - 1$ we have seen that the conjugacy class of $Y^l$ corresponds to $[\mathbb{Z}[1/n][\xi], D^{-1} \gamma_k(Du)]$ where $\gamma_k \in \text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ is defined such 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

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

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 $\gamma_k$ and $u$ such that $\gamma_k(Du) = Du$. The automorphism $\gamma_{p-1} (= \gamma_{-1})$ has order 2, i.e. $\gamma_{p-1}$ 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 $\gamma_k \in \text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ generates a subgroup $\langle \gamma_k \rangle \subseteq \text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ and the order of this subgroup divides $p - 1$, the order of $\text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$. Let $j = |\langle \gamma_k \rangle|$ denote the order of $\gamma_k$. If $j$ is even the order of $\gamma_k^{j/2}$ is 2 and on the other hand $\gamma_k^j(Du) = Du$ for any $1 < r < j$. This yields a contradiction and therefore $\gamma_k(Du) = Du$ cannot be satisfied if the order of $\gamma_k$ is even. This implies that if $\gamma_k$ and $u$ exist with $\gamma_k(Du) = Du$, then the order of $\gamma_k$ is odd.

The main theorem of Galois theory says that a subfield $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}[\xi]$ corresponds to the subgroup $\langle \gamma_k \rangle \subseteq \text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ 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 $\gamma_k \in \text{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ be of odd order $j$. Since complex conjugation commutes with the Galois automorphisms, we get for any $r$, $1 \leq r \leq j$, $\gamma_k^r(D) = -\gamma_k^r(\overline{D})$. 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 $\gamma_k$ since

$$\gamma_k \left( \prod_{r=1}^{j} \gamma_k^r(D) \right) = \prod_{r=1}^{j} \gamma_k(\gamma_k^r(D)) = \prod_{r=1}^{j} \gamma_k^r(D).$$

Now consider the composition $\gamma_k \circ \gamma_{p-1} = \gamma_{-k}$ where the order of $\gamma_k$ is odd. The order of $\gamma_{-k}$ 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 cyclotomic units in any subfield $L$ of $\mathbb{Q}(\xi_m)$ where $\xi_m$ is a $m$th 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 $w := \prod_{r=1}^{j-1} \gamma_k(\gamma^r(D)) \in \mathbb{Z}[1/n][\xi]$. Then

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

since $j$ is odd. Moreover $Dw = \prod_{r=1}^{j} \gamma_{k^r}(\gamma^r(D))$ and therefore $\gamma_k(Dw) = Dw$. We have $Dw = -Dw$ 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 $\gamma_k \in \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ of odd order, we found $u \in \mathbb{Z}[1/n][\xi + \xi^{-1}]$ with $\gamma_k(Du) = D_u$ and such that

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

If $Y \in \text{Sp}(p-1, \mathbb{Z}[1/n])$ 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 $Y^{l'}$ where $1 \leq r \leq j$ and $j$ is the order of $\gamma_k$. Indeed $\gamma_k(\xi^{l'}) = \xi$ for $1 \leq r \leq j$ and therefore $l' \equiv 1 \mod p$ (since $\gamma_{k,l} = \text{id}$) and $Y^{l'} = Y$ because the order of $Y$ is $p$. The $l'$ 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 $\gamma_l \in \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ with $\gamma_l(\xi) = \xi^l$. Then $\gamma_l = \gamma_k^{-1}$ and if $j$ is the order of $\gamma_k$, then $j$ is also the order of $\gamma_l$. Therefore $l' \equiv 1 \mod p$. This means that $Y^{l'} = Y$ and the $Y^{l'}$, $1 \leq r \leq j$ 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 the matrix $Y \in \text{Sp}(p-1, \mathbb{Z}[1/n])$, and if $j$ is maximal with this property, then we have for this subgroup $N(P)/C(P) \cong \mathbb{Z}/2\mathbb{Z}$ 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 $Y \in \text{Sp}(p-1, \mathbb{Z}[1/n])$ 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 $\text{Sp}(p-1, \mathbb{Z}[1/n])$, for which $N(P)/C(P) \cong \mathbb{Z}/j\mathbb{Z}$. 

\[ 4.2 \text{ The centralizer of subgroups of order } p \]

**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 the centralizer $C(P)$ of a subgroup $P$ of order $p$ in $\text{Sp}(p-1, \mathbb{Z}[1/n])$ is

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

where $\sigma^+ = \sigma$ if $p \nmid n$, $\sigma^+ = \sigma + 1$ if $p \mid n$ and $\sigma$ 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 $Y \in \text{Sp}(p-1, \mathbb{Z}[1/n])$ be of order $p$ and let $[a, a]$ be the equivalence class corresponding to the conjugacy class of $Y$. Let $P$ be the subgroup generated by $Y$. Let $Z \in \text{Sp}(p-1, \mathbb{Z}[1/n])$ 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 $\alpha$ is an eigenvector of $Y$ to the eigenvalue $\xi$, 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
\[
(Z\alpha)^T J \overline{Z\alpha}^{(i)} = \alpha^T Z^T JZ\alpha^{(i)} = w\alpha^T Jw^{(i)}\overline{\alpha}^{(i)}
= w\overline{w}^{(i)}\alpha^T J\overline{\alpha}^{(i)} = \delta_{i1}aw\overline{w}^{(i)}D
\]
and, since $\delta_{i1} = 0$ for $i \neq 1$, we get
\[ (Z\alpha)^T J \overline{Z\alpha} = aw\overline{w}D. \]
But $Z \in \text{Sp}(p-1, \mathbb{Z}[1/n])$ and therefore
\[ (Z\alpha)^T J \overline{Z\alpha} = \alpha^T Z^T JZ\alpha = \alpha^T J\alpha = aD. \]
This implies that $w\overline{w} = 1$. In order to determine the centralizer $C(P)$ of a subgroup $P \subseteq \text{Sp}(p-1, \mathbb{Z}[1/n])$ 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
\[ N: \mathbb{Z}[1/n][\xi]^* \rightarrow \mathbb{Z}[1/n][\xi + \xi^{-1}]^* \]
\[ x \mapsto x\overline{x}. \]
Brown [1] and Sjerve and Yang [11] showed that the kernel of the norm mapping
\[ N': \mathbb{Z}[\xi]^* \rightarrow \mathbb{Z}[\xi + \xi^{-1}]^* \]
\[ x \mapsto x\overline{x} \]
is the set of roots of unity
\[ \ker(N') = \{ \pm \xi^r \mid \xi^p = 1, 1 \leq r \leq p \}. \]
It is obvious that $\ker(N') \subseteq \ker(N)$. The prime ideals that lie over the primes in $Z$ and divide $n$ yield units in $\mathbb{Z}[1/n][\xi]^* \setminus \mathbb{Z}[\xi]^*$. Let $q^+ \subseteq \mathbb{Z}[\xi + \xi^{-1}]$ be a prime over a prime $q \mid n$ and let $q \subseteq \mathbb{Z}[\xi]$ be a prime over $q^+$. If $q^+$ is inert, then $q = \overline{q}$ and if $q^+$ splits, then $q^+\mathbb{Z}[\xi] = q\overline{q}$. A generalization for $S$-units of the Dirichlet unit theorem says that for each prime $q_j$, $j = 1, \ldots, k$, over $n$ a $g_j \in q_j$ 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 \( w^{-1}w = w^2 \neq 1 \) 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 \( \sigma \) if \( p \nmid n \) and to \( \sigma + 1 \) if \( p \mid n \) where

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

This difference is equal to the number of primes in \( \mathbb{Z}[\xi + \xi^{-1}] \) that split or ramify in \( \mathbb{Q}[\xi] \) 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. \( \square \)

### 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 \( \text{Sp}(p-1, \mathbb{Z}[1/n]) \). Let \( p \) be an odd prime, \( \xi \) a primitive \( p \)-th 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 \( p \nmid n \). Then the action of \( N(P)/C(P) \) on \( C(P) \) is given by the action of the Galois group \( \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \) 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 \( \text{Sp}(p-1, \mathbb{Z}[1/n]) \) is given by the kernel of the norm mapping \( \mathbb{Z}[1/n][\xi]^* \rightarrow \mathbb{Z}[1/n][\xi + \xi^{-1}]^*, x \mapsto x^p \). 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 \( \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \). Herewith the action of the quotient \( N(P)/C(P) \) on the centralizer \( C(P) \) is given by the action of the subgroup of \( \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \) corresponding to \( N(P)/C(P) \) on the kernel of the norm mapping \( \mathbb{Z}[1/n][\xi]^* \rightarrow \mathbb{Z}[1/n][\xi + \xi^{-1}]^* \). Since it is nontrivial, the action of \( N(P)/C(P) \) on \( C(P) \) is faithful. \( \square \)

### References

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

[2] K. S. Brown, *Cohomology of Groups*, GTM 87, Springer 1982.

[3] C. Busch, *Symplectic characteristic classes*, L’Enseignement Mathématique 47 (2001), 115-130.
On $p$-torsion in symplectic groups

[4] C. Busch, *The Farrell cohomology of $\text{Sp}(p-1, \mathbb{Z})$*, Documenta Mathematica 7 (2002), 239-254.

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

[6] S. Lang, *Algebraic number theory*, Addison Wesley 1970.

[7] N. Naffah, *On the Integral Farrell Cohomology Ring of $\text{PSL}_2(\mathbb{Z}[1/n])$*, Diss. ETH No. 11675, ETH Zürich, 1996.

[8] J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften 322, Springer 1999.

[9] J.-P. Serre, *Local Fields*, GTM 67, Springer 1979.

[10] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181-234.

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

[12] L. C. Washington *Introduction to cyclotomic fields*, GTM 83, Springer 1997.

Cornelia M. Busch
Katholische Universität Eichstätt-Ingolstadt
MGF
D-85071 Eichstätt
Germany