1.2 A RELATION BETWEEN $U(\frac{p-1}{2})$ AND Sp(p-1,Z)

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **47 (2001)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.04.2024**

It is the group of isometries of the skew-symmetric bilinear form

$$\begin{aligned} \langle\ ,\ \rangle\colon R^{2n} \times R^{2n} &\longrightarrow R \\ (x,y) &\longmapsto \langle x,y\rangle := x^{\mathrm{T}} J y\,. \end{aligned}$$

It follows from a result of Bürgisser [5] that elements of odd prime order p exist in $\mathrm{Sp}\,(2n,\mathbf{Z})$ if and only if $2n \geqslant p-1$.

PROPOSITION 1.1. *The eigenvalues of a matrix $Y \in \mathrm{Sp}\,(p-1,\mathbf{Z})$ of odd prime order p are the primitive p-th roots of unity, hence the zeros of the polynomial*

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

Proof. If λ is an eigenvalue of Y, we have $\lambda = 1$ or $\lambda = \xi$, a primitive p-th root of unity, and the characteristic polynomial of Y divides $x^p - 1$ and has integer coefficients. Since $m(x)$ is irreducible over $\mathbf{Q}$, the claim follows. $\square$

1.2 A RELATION BETWEEN $\mathrm{U}\big(\frac{p-1}{2}\big)$ AND $\mathrm{Sp}\,(p-1,\mathbf{Z})$

Let $X \in \mathrm{U}(n)$, i.e., $X \in \mathrm{GL}(n,\mathbf{C})$ and $X^*X = I_n$ where $X^* = \overline{X}^{\mathrm{T}}$ and I_n is the $n \times n$-identity matrix. We can write $X = A + iB$ with $A, B \in \mathrm{M}(n,\mathbf{R})$, the ring of real matrices. We now define the following map

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

The map ϕ is an injective homomorphism. Moreover, it is well-known that ϕ maps $\mathrm{U}(n)$ onto a maximal compact subgroup of $\mathrm{Sp}\,(2n,\mathbf{R})$. In this section we will prove the following theorem.

THEOREM 1.2. *Let $X \in \mathrm{U}((p-1)/2)$ be of odd prime order p. We define $\phi\colon \mathrm{U}((p-1)/2) \to \mathrm{Sp}\,(p-1,\mathbf{R})$ as above. Then $\phi(X) \in \mathrm{Sp}\,(p-1,\mathbf{R})$ is conjugate to $Y \in \mathrm{Sp}\,(p-1,\mathbf{Z})$ if and only if the eigenvalues $\lambda_1,\ldots,\lambda_{(p-1)/2}$ of X are such that*

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

is a complete set of primitive p-th roots of unity.

The condition on the eigenvalues of X is necessary: It is an easy computation to show that if $\lambda_1, \dots, \lambda_{(p-1)/2}$ are the eigenvalues of $X \in \mathrm{U}((p-1)/2)$, then

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

are the eigenvalues of $\phi(X) \in \mathrm{Sp}(p-1, \mathbf{R})$. So if $\phi(X) \in \mathrm{Sp}(p-1, \mathbf{R})$ is conjugate to $Y \in \mathrm{Sp}(p-1, \mathbf{Z})$, the condition on the eigenvalues of $X \in \mathrm{U}((p-1)/2)$ holds by Proposition 1.1. That the condition on the eigenvalues is also sufficient will be proved in 1.2.2.

Note that $X_1, X_2 \in \mathrm{U}(n)$ are conjugate in $\mathrm{U}(n)$ if and only if $\phi(X_1), \phi(X_2)$ are conjugate in $\mathrm{Sp}(2n, \mathbf{R})$, because $\phi(\mathrm{U}(n))$ is a maximal compact subgroup of $\mathrm{Sp}(2n, \mathbf{R})$. The eigenvalues of a unitary matrix X determine the conjugacy class of X in $\mathrm{U}((p-1)/2)$. We will take any $Y \in \mathrm{Sp}(p-1, \mathbf{Z})$ of prime order p and show, assuming Y is conjugate in $\mathrm{Sp}(p-1, \mathbf{R})$ to $\phi(X)$, how to compute the eigenvalues of $X \in \mathrm{U}((p-1)/2)$. Then we will prove that if we run through the conjugacy classes of matrices $Y \in \mathrm{Sp}(p-1, \mathbf{Z})$ of prime order p, we will run through the conjugacy classes of matrices $X \in \mathrm{U}((p-1)/2)$ that satisfy the necessary condition. An interesting corollary is the following (see also 1.2.2).

COROLLARY 1.3. *The number of conjugacy classes of elements of order p in $\mathrm{Sp}(p-1, \mathbf{Z})$ that are conjugate in $\mathrm{Sp}(p-1, \mathbf{R})$ to elements of the form $\phi(X)$, where $X \in \mathrm{U}((p-1)/2)$, is greater or equal to $2^{(p-1)/2}$.*

1.2.1 INVARIANT SUBSPACES

Each matrix $Y \in \mathrm{Sp}(p-1, \mathbf{Z})$ of odd prime order p defines an isomorphism $\sigma\colon \mathbf{Z}^{p-1} \to \mathbf{Z}^{p-1}$, which is an isometry of the skew-symmetric bilinear form $q\colon \mathbf{Z}^{p-1} \times \mathbf{Z}^{p-1} \to \mathbf{Z}$ defined by $q(x,y) := \langle x, y\rangle = x^{\mathrm{T}} J y$ where $x, y \in \mathbf{Z}^{p-1}$ and J is like in the definition of the symplectic group. From now on we will sometimes take the $\mathbf{R}$-linear or the $\mathbf{C}$-linear extensions of σ and of q without making any remark. But this will always be clear from the context.

Let $v_j \in \mathbf{C}^{p-1}$ be an eigenvector corresponding to the eigenvalue $\xi^j := e^{j2\pi i/p}$ of the $\mathbf{C}$-linear extension of σ. Then the complex conjugate $\overline{v}_j$ is an eigenvector to the eigenvalue ξ^{-j} because σ is given by a real matrix. The real vectors $v_j + \overline{v}_j$ and $-i(v_j - \overline{v}_j)$ span a σ-invariant subspace of $\mathbf{R}^{p-1}$, which we will denote by V_j. The dimension of V_j is 2 and $\mathbf{R}^{p-1} = V_1 \oplus \cdots \oplus V_{(p-1)/2}$. The space $V_j \otimes_{\mathbf{R}} \mathbf{C}$ is the sum of the eigenspaces corresponding to ξ^j and ξ^{-j}.

DEFINITION. We define the *sign* of V_j to be

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

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

LEMMA 1.4. *The sign* $\operatorname{sign}(V_j)$ *is well-defined, i.e., independent of the choice of* x.

Proof. Let $0 \neq x := \alpha(v_j + \overline{v}_j) + \beta(-i(v_j - \overline{v}_j)) \in V_j$ where $\alpha, \beta \in \mathbf{R}$ and $v_j, \overline{v}_j$ as above. Then a simple computation shows that

$$q(x, \sigma(x)) = -2i(\alpha^2 + \beta^2) q(v_j, \overline{v}_j) \sin\theta_j \neq 0,$$

with $\theta_j := j2\pi/p$. Therefore, $\operatorname{sign} q(x, \sigma(x))$ does not depend on the choice of $0 \neq x \in V_j$. □

For $x \in V_j$, $y \in V_k$ with $j \neq k$, $j, k = 1, \dots, (p-1)/2$, we have $q(x, y) = 0$. Therefore q is nondegenerate on V_j and $q(v_j, \overline{v}_j) = -q(\overline{v}_j, v_j) \neq 0$. Because $\sin\theta_j > 0$, we have

$$\operatorname{sign}(V_j) = \operatorname{sign}(-iq(v_j, \overline{v}_j)).$$

This equation implies that $-i \operatorname{sign}(V_j) q(v_j, \overline{v}_j)$ is positive. We define a new basis of V_j by:

$$\begin{aligned} u_j &:= (-2i \operatorname{sign}(V_j)\, q(v_j, \overline{v}_j))^{-1/2}(v_j + \overline{v}_j), \\ \widetilde{u}_j &:= -\operatorname{sign}(V_j)\,(-2i \operatorname{sign}(V_j)\, q(v_j, \overline{v}_j))^{-1/2}(-i(v_j - \overline{v}_j)). \end{aligned}$$

LEMMA 1.5. *The vectors* $u_1, \dots, u_{(p-1)/2}$, $\widetilde{u}_1, \dots, \widetilde{u}_{(p-1)/2}$ *form a symplectic basis of* $\mathbf{R}^{p-1}$.

Proof. It is clear that this is a basis of $\mathbf{R}^{p-1}$. For $i \neq j$ with $i,j = 1, \dots, (p-1)/2$

$$\begin{aligned} &q(u_i, u_j) = q(\widetilde{u}_i, \widetilde{u}_j) = q(u_i, \widetilde{u}_j) = 0, \\ &q(u_j, \widetilde{u}_j) = 1. \end{aligned}$$

This shows that the basis $u_1, \dots, u_{(p-1)/2}$, $\widetilde{u}_1, \dots, \widetilde{u}_{(p-1)/2}$ is symplectic. □

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

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

We want to write this matrix in the form

$$\begin{pmatrix} \cos\vartheta_j & \sin\vartheta_j \\ -\sin\vartheta_j & \cos\vartheta_j \end{pmatrix},$$

because in this case $\sigma\colon \mathbf{R}^{p-1} \to \mathbf{R}^{p-1}$ is given in the basis $u_1, \dots, u_{(p-1)/2}$, $\widetilde{u}_1, \dots, \widetilde{u}_{(p-1)/2}$ by the image of a diagonal matrix in $X \in \mathrm{U}((p-1)/2)$ with the $e^{i\vartheta_j}$, $j = 1, \dots, (p-1)/2$, being the eigenvalues of X. Comparing both 2×2-matrices we see that we should put

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

This proves the following

PROPOSITION 1.6. *Let $Y \in \mathrm{Sp}\,(p-1, \mathbf{Z})$ of odd prime order p define an isometry $\sigma\colon \mathbf{Z}^{p-1} \to \mathbf{Z}^{p-1}$. Let $\xi := e^{i2\pi/p}$, $\mathbf{R}^{p-1} = V_1 \oplus \cdots \oplus V_{(p-1)/2}$ where V_j, $j = 1, \dots, (p-1)/2$, is the invariant subspace corresponding to the eigenvalues ξ^j, ξ^{p-j} of the extension of σ to an isomorphism of $\mathbf{R}^{p-1}$. Then there exists $X \in \mathrm{U}((p-1)/2)$ such that Y is conjugate to $\phi(X) \in \mathrm{Sp}\,(p-1, \mathbf{R})$. Moreover,*

if $\operatorname{sign}(V_j) = -1$ then ξ^j is an eigenvalue of X, and
if $\operatorname{sign}(V_j) = 1$ then ξ^{-j} is an eigenvalue of X.

1.2.2 THE PROOF OF THEOREM 1.2

It remains to show that the condition on the eigenvalues of $X \in \mathrm{U}((p-1)/2)$ is sufficient. We put $\mathbf{Z}/2\mathbf{Z} = \{\pm 1\}$. Let $\mathcal{M}$ be the set of $Y \in \mathrm{Sp}\,(p-1, \mathbf{Z})$ of odd prime order p. We define a mapping

$$\begin{aligned} \psi\colon \mathcal{M} &\longrightarrow (\mathbf{Z}/2\mathbf{Z})^{(p-1)/2} \\ Y &\longmapsto \left(\operatorname{sign}(V_1), \dots, \operatorname{sign}(V_{(p-1)/2})\right), \end{aligned}$$

where V_j and $\operatorname{sign}(V_j)$, $j = 1, \dots, (p-1)/2$, are defined as above. It follows from Proposition 1.6 that the necessary condition in Theorem 1.2 is sufficient if and only if ψ is surjective. Therefore we now have to prove the surjectivity of ψ. First we will prove that in each conjugacy class of matrices of order p in $\mathrm{Sp}\,(p-1, \mathbf{Z}[1/p])$ one can find a matrix in $\mathrm{Sp}\,(p-1, \mathbf{Z})$. Let $\mathcal{M}_p$ be the set of matrices of order p in $\mathrm{Sp}\,(p-1, \mathbf{Z}[1/p])$. With the same procedure as for $Y \in \mathcal{M}$, we can define V_j, $\operatorname{sign}(V_j)$, $j = 1, \dots, (p-1)/2$, for $Y_p \in \mathcal{M}_p$, and we get statements for $\mathrm{Sp}\,(p-1, \mathbf{Z}[1/p])$ that are similar to those for

$\mathrm{Sp}(p-1,\mathbf{Z})$. We will show the surjectivity of the mapping

$$\begin{aligned}\psi_p\colon \mathcal{M}_p &\longrightarrow (\mathbf{Z}/2\mathbf{Z})^{(p-1)/2}\\ Y_p &\longmapsto \left(\mathrm{sign}(V_1),\ldots,\mathrm{sign}(V_{(p-1)/2})\right).\end{aligned}$$

Then we have shown that ψ is surjective since matrices of $\mathcal{M}_p$ that are in the same conjugacy class have the same image under ψ_p.

Let P be the set of pairs $(\mathfrak{a},a)$, where $0\neq\mathfrak{a}\subseteq\mathbf{Z}[\xi]$ is an ideal and $a\in\mathbf{Z}[\xi]$ such that $\mathfrak{a}\bar{\mathfrak{a}}=(a)\subseteq\mathbf{Z}[\xi]$ is a principal ideal. The bar denotes complex conjugation and $\bar{\mathfrak{a}}=\{\overline{\alpha}\mid\alpha\in\mathfrak{a}\}$. Let P_p be the set of pairs $(\mathfrak{a}_p,a)$, where $0\neq\mathfrak{a}_p\subseteq\mathbf{Z}[1/p][\xi]$ is an ideal and $a\in\mathbf{Z}[1/p][\xi]$ such that $\mathfrak{a}_p\bar{\mathfrak{a}}_p=(a)\subseteq\mathbf{Z}[1/p][\xi]$ is a principal ideal. We define an equivalence relation on P and on P_p:

$$\begin{aligned}(\mathfrak{a},a)\sim(\mathfrak{b},b)\Leftrightarrow{}&\exists\,\lambda,\mu\in\mathbf{Z}[\xi]\setminus\{0\}\text{ such that}\\ &\lambda\mathfrak{a}=\mu\mathfrak{b}\text{ and }\lambda\overline{\lambda}a=\mu\overline{\mu}b\end{aligned}$$

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

We denote by $[\mathfrak{a},a]$ and $[\mathfrak{a}_p,a]$ the equivalence class of $(\mathfrak{a},a)$ and $(\mathfrak{a}_p,a)$ respectively. Moreover, $\mathcal{P}$ and $\mathcal{P}_p$ denote the sets of equivalence classes in P and P_p respectively. The sets of equivalence classes $\mathcal{P}$ and $\mathcal{P}_p$ are abelian groups. The multiplication is given by $[\mathfrak{a},a][\mathfrak{b},b]=[\mathfrak{a}\mathfrak{b},ab]$, the units in $\mathcal{P}$ and $\mathcal{P}_p$ are $[\mathbf{Z}[\xi],1]$ and $[\mathbf{Z}[1/p][\xi],1]$ respectively, and the inverse of $[\mathfrak{a},a]$ is $[\bar{\mathfrak{a}},a]$ because

$$[\mathfrak{a},a][\bar{\mathfrak{a}},a]=[\mathfrak{a}\bar{\mathfrak{a}},a^2]=[(a),a^2]=[\mathcal{O},1]$$

where $\mathcal{O}=\mathbf{Z}[\xi]$ if $[\mathfrak{a},a]\in\mathcal{P}$, and $\mathcal{O}=\mathbf{Z}[1/p][\xi]$ if $[\mathfrak{a},a]\in\mathcal{P}_p$.

According to the articles of Brown [4] and of Sjerve and Yang [11], a bijection exists between the elements of $\mathcal{P}$ (resp. $\mathcal{P}_p$) and the conjugacy classes of elements of order p in $\mathrm{Sp}(p-1,\mathbf{Z})$ (resp. $\mathrm{Sp}(p-1,\mathbf{Z}[1/p])$). For the convenience of the reader, we will recall how this bijection is constructed. Let $Y\in\mathrm{Sp}(p-1,\mathbf{Z})$ be of odd prime order p. Let $\mathfrak{a}$ be a $\mathbf{Z}[\xi]$-module whose underlying $\mathbf{Z}$-module is $\mathbf{Z}^{p-1}$, with the action of ξ given by Y. Such a module is a fractional ideal in $\mathbf{Q}(\xi)$. Let

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

be an eigenvector of Y to the eigenvalue ξ, that is $Yv_1=\xi v_1$. Then the module $\mathfrak{a}$ we described above is the ideal

$$\mathfrak{a}=\mathbf{Z}\alpha_1+\cdots+\mathbf{Z}\alpha_{p-1}.$$

Since the eigenvector v_1 is unique up to multiples, the ideal $\mathfrak{a}$ is unique up to fractional equivalence. Let $Y' = GYG^{-1}$ with $G \in \mathrm{Sp}\,(p-1, \mathbf{Z})$. Then $w_1 = Gv_1$ is an eigenvector for Y' to the eigenvalue ξ and the corresponding ideal is also $\mathfrak{a}$. Let $a = D^{-1}v_1^{\mathrm{T}}Jv_1$, where $D = p\,\xi^{(p+1)/2}/(\xi - 1)$, then $[\mathfrak{a}, a]$ is the equivalence class we are searching for. So we have defined a mapping, which sends the conjugacy class of Y to the equivalence class $[\mathfrak{a}, a] \in \mathcal{P}$. In [11] is shown that this mapping is a bijection. The construction for $\mathrm{Sp}\,(p-1, \mathbf{Z}[1/p])$ is analogous.

Let $\mathcal{C}_0 := \mathcal{C}_0(\mathbf{Z}[\xi])$ be the subgroup of the ideal class group $\mathcal{C} = \mathcal{C}(\mathbf{Z}[\xi])$ given by

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

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

$$\mathcal{C}_{p0} = \{\mathfrak{a}_p \in \mathcal{C}_p \mid \mathfrak{a}_p\bar{\mathfrak{a}}_p = (a),\ \ a = \bar{a} \text{ for some } a \in \mathbf{Z}[1/p][\xi]\}\,.$$

It follows directly from the definition, that for $\mathfrak{a} \in \mathcal{C}_0$ (resp. $\mathfrak{a} \in \mathcal{C}_{p0}$) holds $[\mathfrak{a}, a] \in \mathcal{P}$ (resp. $[\mathfrak{a}, a] \in \mathcal{P}_p$). But here we have $a = \bar{a}$, which was not requested in the definition of $\mathcal{P}$ and $\mathcal{P}_p$. But for an equivalence class $[\mathfrak{a}, a]$ we can always choose a such that $a = \bar{a}$. For a proof of this fact see [11].

Let U be the group of units in $\mathbf{Z}[\xi]$ and $U^+ := \{u \in U \mid u = \bar{u}\}$ the group of units in $\mathbf{Z}[\xi + \xi^{-1}]$. Let $N\colon \mathbf{Q}(\xi) \to \mathbf{Q}(\xi + \xi^{-1})$, $a \mapsto N(a) = a\bar{a}$, be the norm mapping and $N(U) := \{u\bar{u} = N(u) \mid u \in U\}$. Let U_p be the group of units in $\mathbf{Z}[1/p][\xi]$ and $U_p^+ := \{u \in U_p \mid u = \bar{u}\}$, $N(U_p) := \{u\bar{u} \mid u \in U_p\}$. Clearly $N(U) \subset U^+$, $N(U_p) \subset U_p^+$, and we can define the abelian groups $U^+/N(U)$ and $U_p^+/N(U_p)$. It is well-known (see Washington [12]) that $U_p = U \cdot \langle 1 - \xi\rangle$ where $\langle 1 - \xi\rangle$ is the group generated by $1 - \xi$, and $U_p^+ = U^+ \cdot \langle (1-\xi)(1-\xi^{-1})\rangle$ where $\langle (1-\xi)(1-\xi^{-1})\rangle$ is the subgroup of $\langle 1 - \xi\rangle$ generated by $(1-\xi)(1-\xi^{-1})$. Hence

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

where the last equation is a consequence of the Dirichlet unit theorem.

According to the articles of Brown [4] and of Sjerve and Yang [11], there are short exact sequences of abelian groups

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

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

where $\delta(uN(U)) = [\mathbf{Z}[\xi], u]$, $\delta_p(uN(U)) = [\mathbf{Z}[1/p][\xi], u]$, $\eta([\mathfrak{a}, a]) = [\mathfrak{a}]$ and $\eta_p([\mathfrak{a}_p, a]) = [\mathfrak{a}_p]$. Theorem 3 in the article of Sjerve and Yang [11] states that the number of elements in $\mathcal{P}$ is $2^{(p-1)/2}h^-$. Here $h^- := h/h^+$ where h and h^+ are the class numbers of $\mathbf{Q}(\xi)$ and $\mathbf{Q}(\xi+\xi^{-1})$ respectively. It follows from Proposition 7 in the article of Brown [4] that the cardinality of $\mathcal{P}_p$ is $2^{(p-1)/2}h^-$ too.

Now we will define homomorphisms ρ_1, ρ and ρ_2 such that the following diagram commutes.

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

We define a homomorphism of abelian groups:

$$\begin{aligned} \rho_1\colon U^+/N(U) &\longrightarrow U_p^+/N(U_p) \\ uN(U) &\longmapsto uN(U_p)\,. \end{aligned}$$

We have already seen that $U_p = U\cdot\langle 1-\xi\rangle$ where $\langle 1-\xi\rangle$ is the subgroup generated by $1-\xi$. This implies that

$$N(U_p) = N(U)\cdot\big\langle(1-\xi)(1-\xi^{-1})\big\rangle\,.$$

Let $uN(U) \neq vN(U) \in U^+/N(U)$, then $uN(U_p) \neq vN(U_p)$. Indeed, if $uN(U_p) = vN(U_p)$, then $w \in N(U_p)$ exists with $u = wv$. But $w \notin N(U)$ since $uN(U) \neq vN(U)$. On the other hand $u = wv$ and $u, v \in U^+$ imply that $w \in U^+$. But $N(U_p) \nsubseteq U^+$ and this yields a contradiction. Therefore ρ_1 is injective and ρ_1 is an isomorphism since the equation (*) holds.

Now we will define $\rho_2\colon \mathcal{C}_0 \to \mathcal{C}_{p0}$. Let $\mathfrak{a} \subseteq \mathbf{Z}[\xi]$ be an ideal. Then we consider the ideal $\mathfrak{a}_p \in \mathbf{Z}[1/p][\xi]$ generated by the elements αz with $\alpha \in \mathfrak{a}$, $z \in \mathbf{Z}[1/p][\xi]$. Since each $z \in \mathbf{Z}[1/p][\xi]$ can be written as $z = z'/p^r$, where $r \in \mathbf{N}$ and $z' \in \mathbf{Z}[\xi]$, we get $\mathfrak{a}_p = \mathfrak{a}\mathbf{Z}[1/p][\xi]$. So we can define a homomorphism

$$\begin{aligned} \rho_2\colon \mathcal{C}_0 &\longrightarrow \mathcal{C}_{p0} \\ [\mathfrak{a}] &\longmapsto [\mathfrak{a}_p]\,. \end{aligned}$$

Let $[\mathfrak{a}], [\mathfrak{b}] \in \mathcal{C}_0$, $[\mathfrak{a}] \neq [\mathfrak{b}]$. Then $[\mathfrak{a}_p] \neq [\mathfrak{b}_p]$. Indeed, let $\mathfrak{a}$ and $\mathfrak{b}$ be representatives of $[\mathfrak{a}]$ and $[\mathfrak{b}]$ respectively. Then $[\mathfrak{a}_p] = [\mathfrak{b}_p]$ would mean that there exist $\lambda, \mu \in \mathbf{Z}[1/p][\xi]$ with $\lambda\mathfrak{a}_p = \mu\mathfrak{b}_p$. But then we would have $[\mathfrak{a}] = [\mathfrak{b}]$. Herewith ρ_2 is injective and ρ_2 is an isomorphism since $|\mathcal{C}_0| = |\mathcal{C}_{0p}| = h^- < \infty$.

Now it remains to define

$$\begin{aligned}\rho\colon \mathcal{P} &\longrightarrow \mathcal{P}_p\\ [\mathfrak{a}, a] &\longmapsto [\mathfrak{a}_p, a]\,.\end{aligned}$$

Let $\mathfrak{a}\overline{\mathfrak{a}} = (a)$. Then $\mathfrak{a}_p\overline{\mathfrak{a}}_p = (a)$, a principal ideal in $\mathbf{Z}[1/p][\xi]$, and herewith ρ is well-defined. It follows directly from the definitions that $\rho \circ \delta = \delta_p \circ \rho_1$ and $\rho_2 \circ \eta = \eta_p \circ \rho$. So the squares commute and, as a consequence of the five-lemma, ρ is an isomorphism.

Since $\mathcal{P}$ and $\mathcal{P}_p$ are isomorphic, each conjugacy class of elements of order p in $\mathrm{Sp}\,(p-1, \mathbf{Z}[1/p])$ contains an element of $\mathrm{Sp}\,(p-1, \mathbf{Z})$. This means that the isomorphism $\rho\colon \mathcal{P} \to \mathcal{P}_p$ corresponds to mapping conjugacy classes of elements of order p in $\mathrm{Sp}\,(p-1, \mathbf{Z})$ to conjugacy classes of elements of order p in $\mathrm{Sp}\,(p-1, \mathbf{Z}[1/p])$.

Now we will recall parts of the discussion in [11] that are important for our purposes. Let $Y \in \mathrm{Sp}\,(p-1, \mathbf{Z})$ be of prime order p and let

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

be an eigenvector corresponding to the eigenvalue ξ, that is $Yv_1 = \xi v_1$. Let $\mathfrak{a}$ be the $\mathbf{Z}$-module generated by $\alpha_1, \ldots, \alpha_{p-1}$. Then $\mathfrak{a}$ is an integral ideal in $\mathbf{Z}[\xi]$ where the action of ξ on the $\mathbf{Z}$-module $\mathfrak{a}$ is given by Y. Let $\gamma_j \in \mathrm{Gal}(\mathbf{Q}(\xi)/\mathbf{Q})$ with $\gamma_j(\xi) = \xi^j$, $j = 1, \ldots, p-1$, be an element of the Galois group. Then $v_j = (\gamma_j(\alpha_1), \ldots, \gamma_j(\alpha_{p-1}))^{\mathrm{T}}$ is an eigenvector to the eigenvalue ξ^j. Now let $a = D^{-1} v_1^{\mathrm{T}} J \overline{v}_1$ where $D = p\,\xi^{(p+1)/2}/(\xi - 1)$, $D = -\overline{D}$. Then Sjerve and Yang showed that $(\mathfrak{a}, a)$ is a pair with $\mathfrak{a}\overline{\mathfrak{a}} = (a)$. Following the same procedure, we can find for a given matrix $Y_p \in \mathrm{Sp}\,(p-1, \mathbf{Z}[1/p])$ an ideal $\mathfrak{a}_p \subseteq \mathbf{Z}[1/p][\xi]$ such that $\mathfrak{a}_p\overline{\mathfrak{a}}_p = (a)$.

The sign of the invariant subspace corresponding to the eigenvalues ξ^j, ξ^{-j} of Y is

$$\mathrm{sign}(V_j) = \mathrm{sign}\,\mathrm{Im}\big(q(v_j, \overline{v}_j)\big) = \mathrm{sign}(-i\gamma_j(Da))$$

where the sign of $z \in \mathbf{Z}[\xi + \xi^{-1}]$ is the sign of $\iota(z)$ for the real embedding ι of $\mathbf{Z}[\xi + \xi^{-1}]$ with $\iota(\xi + \xi^{-1}) = e^{i2\pi/p} + e^{-i2\pi/p}$. Now we see that ψ is surjective if and only if

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

with

$$a \longmapsto \big(\mathrm{sign}(\gamma_1(a)), \ldots, \mathrm{sign}(\gamma_{(p-1)/2}(a))\big)$$

is surjective. We call $a \in \mathbf{Q}(\xi)$ a Hermitian square if $x \in \mathbf{Q}(\xi)$ exists such that $x\overline{x} = a$. Now we use Lemma 2.3 in the article of Alexander, Conner, Hamrick and Vick [2]. We repeat the statement of this lemma.

LEMMA 1.7. *Let* $\mathfrak{a} \neq 0$ *be a* $\mathbf{Z}[1/p][\xi]$*-ideal with* $\mathfrak{a}\bar{\mathfrak{a}} = a\mathbf{Z}[1/p][\xi]$. *Then* a *is a Hermitian square if and only if it is positive in every ordering of* $\mathbf{Q}(\xi + \xi^{-1})$.

This implies that

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

with

$$a \longmapsto \big(\operatorname{sign}(\gamma_1(a)), \ldots, \operatorname{sign}(\gamma_{(p-1)/2}(a))\big)$$

is surjective. But then ψ_p is surjective and therefore ψ is surjective too. Herewith we have completed the proof of Theorem 1.2.

1.2.3 CONCERNING LEMMA 1.7

We give here some more information on Lemma 1.7 since it is crucial in the proof of Theorem 1.2 and only a sketch of a proof is given in [2].

One direction is obvious. To see that the lemma is true, it is necessary to study Hilbert symbols in $\mathbf{Q}(\xi + \xi^{-1})$. We define $\sigma := \xi + \xi^{-1} - 2$. Then $\mathbf{Q}(\xi) = \mathbf{Q}(\xi + \xi^{-1})(\sqrt{\sigma})$. Let $\mathfrak{p}$ be a prime in $\mathbf{Q}(\xi + \xi^{-1})$. A fundamental property of the Hilbert symbol is

$$\left(\frac{a, \sigma}{\mathfrak{p}}\right) = 1 \quad \Leftrightarrow \quad a \text{ is a norm of the extension } \mathbf{Q}(\xi)/\mathbf{Q}(\xi + \xi^{-1})\,.$$

A proof of this property can be found in the books [9] and [10] of Neukirch. So a is a Hermitian square if and only if

$$\left(\frac{a, \sigma}{\mathfrak{p}}\right) = 1 \text{ for all primes, finite or infinite, in } \mathbf{Q}(\xi + \xi^{-1})\,.$$

We first consider the infinite primes. Therefore we use the connection of the Hilbert symbol with the norm residue symbol (see [9] and [10]). For infinite primes we have the norm residue symbol for $\mathbf{C}/\mathbf{R}$

$$(\ ,\mathbf{C}/\mathbf{R}) \colon \mathbf{R}^* \longrightarrow \operatorname{Gal}(\mathbf{C}/\mathbf{R})$$

defined by

$$(a, \mathbf{C}/\mathbf{R})\sqrt{-1} = \sqrt{-1}^{\ \operatorname{sign}(a)}\,.$$

The kernel of this homomorphism is

$$\mathbf{R}_{>0} = N_{\mathbf{C}/\mathbf{R}}(\mathbf{C}^*) = \{z\bar{z} \mid z \in \mathbf{C}^*\}$$

where $\mathbf{C}^*$ and $\mathbf{R}^*$ denote the multiplicative subgroup of $\mathbf{C}$ and $\mathbf{R}$ respectively. So the positivity required in Lemma 1.7 implies that the Hilbert symbol is 1 at infinite primes. It remains to consider the finite primes. The Hilbert symbol is also 1 at the inert primes because of the following lemma.

LEMMA 1.8. *If $a \in \mathbf{Q}(\xi+\xi^{-1})$, then there is a fractional ideal $\mathfrak{a} \subset \mathbf{Q}(\xi)$ with $\mathfrak{a}\bar{\mathfrak{a}} = a\mathbf{Z}[\xi]$ if and only if at every inert prime $\mathfrak{p} \subset \mathbf{Z}[\xi+\xi^{-1}]$ we have*

$$\left(\frac{a, \sigma}{\mathfrak{p}}\right) = 1.$$

Proof. See [1]. □

If $\mathfrak{p}$ is a prime in $\mathbf{Q}(\xi+\xi^{-1})$ that splits, then the Hilbert symbol

$$\left(\frac{a, \sigma}{\mathfrak{p}}\right) = 1$$

(see [1]). So it remains to consider the ramified primes in $\mathbf{Q}(\xi+\xi^{-1})$. But the only prime that ramifies is $\sigma\mathbf{Z}[\xi+\xi^{-1}]$. Then, by the reciprocity law of Hilbert symbols (see [9]), the Hilbert symbol at this prime is 1.

This proves Lemma 1.7.

1.2.4 AN INTERESTING REMARK

Let U be the group of units in $\mathbf{Z}[\xi]$ and $U^+ = \{u \in U \mid u = \bar{u}\}$. Let $u \in U^+ \setminus N(U)$ where N is the norm map. Then $[\mathfrak{a}, a] \in \mathcal{P}$ implies that $[\mathfrak{a}, ua] \in \mathcal{P}$ and $[\mathfrak{a}, a] \neq [\mathfrak{a}, ua]$. Let Y be a representative of the conjugacy class of matrices corresponding to $[\mathfrak{a}, a]$. We have seen that the $\mathrm{sign}(V_j)$ of Y is given by a. Let us fix the ideal $\mathfrak{a}$. The question that arises now is if the restriction of ψ to the conjugacy classes of matrices corresponding to $[\mathfrak{a}, ua]$, where u is as above, is surjective. But this restriction is not surjective for each prime. Let h and h^+ be the class numbers of $\mathbf{Q}(\xi)$ and $\mathbf{Q}(\xi+\xi^{-1})$ respectively. Then $h^- = h/h^+$. Let C denote the group of cyclotomic units in $\mathbf{Q}(\xi)$ and let $C^+ = C \cap \mathbf{Z}[\xi+\xi^{-1}]$. It is known that $[\mathbf{Z}[\xi+\xi^{-1}]^* : C^+] = h^+$. We can find in the article of Garbanati [8] that h^- is odd if and only if C^+ contains units of all signatures, which means that every totally positive unit in C^+ is the square of a unit of C. So in case h^- is odd,

$$\begin{aligned} \omega\colon U^+ \setminus N(U) &\longrightarrow (\mathbf{Z}/2\mathbf{Z})^{(p-1)/2} \\ u &\longmapsto \left(\mathrm{sign}(\gamma_1(u)), \ldots, \mathrm{sign}(\gamma_{(p-1)/2}(u))\right) \end{aligned}$$

is surjective, and this implies the surjectivity of ψ'. However it may be possible that $\mathbf{Z}[\xi+\xi^{-1}]^*$ contains units of all signatures even if C^+ does not. This can only happen if h^+ is even and then we do not know if ω is surjective. If h^- is even and h^+ is odd, we have no surjectivity of ω, and the restriction of ψ' to $\{a \in \mathbf{Z}[\xi] \mid (\mathfrak{a}, a) \in P\}$ for a fixed ideal $\mathfrak{a}$ is not surjective either. This happens for example for the primes 29 and 113.