ISRAEL JOURNAL OF MATHEMATICS 76 (1991), 265–288

A BRAIDLIKE PRESENTATION OF Sp(n, p)

BY

BRONISLAW WAJNRYB*

Department of Mathematics
Technion—Israel Institute of Technology, Haifa 32000, Israel

ABSTRACT

For n even and p an odd prime a symplectic group Sp(n,p) is a quotient of the Artin braid group B_{n+1}. If $s_1, \ldots, s_n$ are standard generators of B_{n+1} then the kernel of the corresponding epimorphism is the normal closure of just four elements: $s_1^p, (s_1 s_2)^6, s_1^{(p+1)/2} s_2^4 s_1^{(p-1)/2} s_2^{-2} s_1^{-1} s_2^2$ and $(s_1 s_2 s_3)^4 A^{-1} s_1^{-2} A$, where $A = s_2 s_3^{-1} s_2^{(p-1)/2} s_4 s_3^2 s_4$, all of them lying in the subgroup B_5. Sp(n,p) acts on a vector space and the image of the subgroup B_n of B_{n+1} in Sp(n,p), denoted Sp$(n-1,p)$, is a stabilizer of one vector. A sequence of inclusions $\cdots B_{k+1} \cdot B_k \cdots$ induces a sequence of inclusions $\cdots$Sp(k,p) $\cdot$Sp$(k-1,p)\cdots$, which can be used to study some finite-valued invariants of knots and links in the 3-sphere via the Markov theorem.

Introduction

In [A] Joachim Assion gave a very simple presentation of the symplectic group Sp$(n,3)$ as a quotient of the Artin braid group B_{n+1}. In this paper we shall describe a similar presentation of Sp(n,p) for any prime number $p > 3$.

The braid group B_n was first considered by A. Hurwitz in 1891 and more thoroughly investigated by E. Artin in 1925 . Since then it has become an important topic in many fields of mathematics like topology, algebraic geometry, combinatorics and group theory .

* Partially supported by the Technion VPR-Fund.
Received December 2, 1990

B_n can be described abstractly as a group with generators $T_1, \cdots, T_{n-1}$ and with relations

$$\text{(R1)} \qquad T_iT_{i+1}T_i = T_{i+1}T_iT_{i+1} \quad \text{for } i = 1, \ldots, n-2,$$

$$\text{(R2)} \qquad T_iT_j = T_jT_i \quad \text{for } |i-j| > 1.$$

The group B_n is known to be residually finite but not many finite quotients of B_n are known explicitly. If we add the relation

$$\text{(R3)} \qquad (T_1)^p = 1$$

we get a group $B_{n,p}$ investigated by Coxeter in [C] . This group is finite if and only if $1/p + 1/n > 1/2$. For $p = 2$ we get the symmetric group S_n.

If $p = 3$ then one more relation

$$\text{(R6)} \qquad (T_1T_2T_3)^4 = A^{-1}T_1^2A,$$

where $A = T_2T_3^{-1}T_2^{(p-1/2)}T_4T_3^2T_4$, transforms $B_{n,p}$ into a finite group $\mathbf{G}_n$. For n odd $\mathbf{G}_n$ is isomorphic to $\mathrm{Sp}(n,3)$ and for n even $\mathbf{G}_n$ is isomorphic to the stabilizer of one vector in $\mathrm{Sp}(n+1,3)$ where $\mathrm{Sp}(n+1,3)$ is considered as a group of linear transformations of an $(n+1)$-dimensional vector space over $\mathbf{Z}/3\mathbf{Z}$. This is the result of Assion in [A] .

Our goal is to prove the following result (for $p > 3$ a prime number):

Theorem 1: *Let $\mathbf{G}_n$ be a group with generators $T_1, \cdots, T_{n-1}$ and relations*

R1 $\quad T_iT_{i+1}T_i = T_{i+1}T_iT_{i+1}$ *for* $i = 1, \cdots, n-2$,

R2 $\quad T_iT_j = T_jT_i$ *for* $|i-j| > 1$,

R3 $\quad (T_1)^p = 1$,

R4 $\quad (T_1T_2)^6 = 1$,

R5 $\quad T_1^{(p+1/2)}T_2^4T_1^{(p-1/2)} = T_2^{-2}T_1T_2^2$,

R6 $\quad (T_1T_2T_3)^4 = A^{-1}T_1^2A$, *where* $A = T_2T_3^{-1}T_2^{(p-1/2)}T_4T_3^2T_4$.

Then a correspondence $T_i \to T_i$ extends to a monomorphism of $\mathbf{G}_n$ into $\mathbf{G}_{n+1}$. For n even $\mathbf{G}_{n+1}$ is isomorphic to the symplectic group $Sp(n,p)$ and the image of $\mathbf{G}_n$ in $\mathbf{G}_{n+1}$ is the stabilizer of one vector .

1. Notation and Preliminaries

Let p be a fixed prime number greater than 3 and let F be a field with p elements. Let V_k be a k-dimensional vector space over F with a fixed basis $\delta_1,\dots,\delta_k$ and with an alternating, bilinear, intersection form given by $(\delta_i,\delta_{i+1}) = 1$ for $i = 1,\dots,k-1$ and $(\delta_i,\delta_j) = 0$ for $|i-j| > 1$. There is a natural sequence of embeddings $V_1 \subset V_2 \subset \cdots$ corresponding to $\{\delta_1\} \subset \{\delta_1,\delta_2\} \subset \cdots$. For k even the form is non-degenerate and the symplectic group $\mathrm{Sp}(k,p)$ can be identified with the group $\mathrm{Sp}(k,F)$ of the linear transformations of V_k which preserve the intersection form.

Linear transformations act on vectors of V_k on the right side. For every $v \in V_k$ we denote by θ_v the linear transformation of V_k defined by $(u)\theta_v = u-(u,v)v$ (the symplectic transvection with respect to vector v).

Transvection with respect to a basis vector δ_i will be denoted by θ_i. Clearly $(\theta_v)^p = 1$, so we can treat exponents of transvections as elements of the field F. For $\alpha \in F$ we shall write $\theta_{i,\alpha}$ for $(\theta_i)^\alpha$ and $\theta_{v,\alpha}$ for $(\theta_v)^\alpha$. Conjugation in a group will be denoted by "*" so $A^*B = B^{-1}AB$ for any pair of elements A, B in a group.

Let $e_{2m+1} = \delta_1+\delta_3+\ldots+\delta_{2m+1}$. Clearly $(e_{2m+1},\delta_{2m+2}) = 1$ and $(e_{2m+1},\delta_i) = 0$ for $i \neq 2m+2$.

For k even define

$$\mathrm{Sp}^\sim(k,F) = \mathrm{Sp}(k,F) = \{h \in \mathrm{Aut}(V_k) | ((u)h,(v)h) = (u,v) \text{ for all } u,v \in V_k\}$$

and $\mathrm{Sp}^\sim(k-1,F) = \mathrm{Stab}_{\mathrm{Sp}(k,F)}(e_{k-1})$. Then $\mathrm{Sp}^\sim(k-2,F)$ can be identified with $\mathrm{Stab}_{\mathrm{Sp}(k,F)}\{e_{k-1},\delta_k\}$. If $h \in \mathrm{Sp}(k-2,F)$ we can extend it to $h' \in \mathrm{Sp}^\sim(k,F)$ letting $(e_{k-1})h' = e_{k-1}$ and $(\delta_k)h' = \delta_k$.

We want to find a presentation of the group $\mathrm{Sp}^\sim(k,F)$ for any k.

We denote by $\mathbf{G}_n$ a group with generators $T_1,\dots,T_{n-1}$ and relations

R1 $(T_{i+1})^*T_i = (T_i)^*(T_{i+1})^{-1}$ for $i = 1,\dots,n-2$,

R2 $T_iT_j = T_jT_i$ for $|i-j| > 1$,

R3 $(T_1)^p = 1$,

R4 $(T_1T_2)^6 = 1$,

R5 $((T_2)^4)^*T_1^{(p-1/2)} = (T_1)^*T_2^2$,

R6 $(T_1T_2T_3)^4 = ((T_1)^2)^*T_2T_3^{-1}T_2^{(p-1/2)}T_4T_3^2T_4$ (only for $n > 4$).

The first two relations R1 and R2 define the classical braid group B_n so $\mathbf{G}_n$ is a quotient of B_n.

By relations R1 and R3 $(T_i)^p = 1$ for all i so, as in the case of the transvections, we can consider exponents of T_i's as elements of F. We shall write $T_{i,a}$ for $(T_i)^a$, e.g. $T_{1,1/2} = T_{1,(p+1/2)} = (T_1)^{(p+1/2)}$.

Let $\phi_n(T_i) = \theta_i, i = 1, \ldots, n-1$. Direct verification shows that ϕ_n maps relations R1–R6 onto true relations in $\mathrm{Sp}^\sim(n-1,F)$ so ϕ_n extends to a homomorphism $\phi_n : \mathbf{G}_n \to \mathrm{Sp}^\sim(n-1,F)$. Theorem 1 of the introduction is equivalent to

THEOREM 1: *ϕ_n is an isomorphism.*

We shall now prove Theorem 1 for $n = 3$. We shall use a known presentation of $\mathrm{Sp}(2,p) = \mathrm{Sp}\,(2,F)$.

1.1 PROPOSITION (J.G. Sunday): *The group $\mathrm{Sp}(2,p)$ has a presentation with generators S,T and relations $S^p = T^2 = (ST)^3 = (S^{(p+1/2)}TS^4T)^2$ where*

$$S = \begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

1.2 PROPOSITION: *ϕ_3 is an isomorphism.*

Proof: In our standard basis δ_1, δ_2 the transvections θ_1, θ_2 are represented by matrices

$$\theta_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad \text{and} \qquad \theta_2 = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

where the action is on the right on row vectors. Let $D = \theta_1\theta_2\theta_1$. Then $T = D$ and $S = D^2\theta_1$. So $\phi_3 : \mathbf{G}_3 \to \mathrm{Sp}(2,p)$ is onto. We shall define the inverse map ψ. Let $\psi(S) = (T_1T_2T_1)^2T_1 = A, \psi(T) = T_1T_2T_1 = B$. We have to check that the relations defined in 1.1 are mapped onto relations in $\mathbf{G}_3$. We have $T_1B = BT_2$ by R1 and $T_iB^2 = B^2T_i$ by R1. $B^4 = (T_1T_2)^6 = 1$ by R1 and R4. So $A^p = B^{2p}T_1^p = B^2$ and

$$(AB)^3 = B^2T_1B^3T_1B^3T_1B = T_1T_2T_1B^9 = B^{10} = B^2.$$

Finally

$$\begin{aligned}
(A^{(p+1/2)}BA^4B)^2 &= (B^{p+1}T_1^{(p+1/2)}B^9T_1^4B)^2 \\
&= B^{p+1}T_1^{(p+1/2)}B^9T_1^4B^{p+2}T_1^{(p+1/2)}B^9T_1^4B \\
&= T_1^{(p+1/2)}T_2^4T_1^{(p+1/2)}T_2^4 \\
&= (\text{by R5 and R3}) \quad T_2^{-2}T_1T_2^2T_1T_2^4 \\
&= (\text{by R1 }) \quad B^2
\end{aligned}$$

as required. ∎

1.3 LEMMA: *If $u \in V_n, h \in$ $\mathrm{Sp}^{\sim}(n,F)$ and $v = (u)h$ then $\theta_v = (\theta_u)^*h$.*

Proof: For any $w \in V_n$ we have

$$(w)h^{-1}\theta_u h = ((w)h^{-1} - ((w)h^{-1},u)u)h = w - ((w)h^{-1},u)(u)h$$

$$= w - (w,(u)h)(u)h = w - (w,v)v = (w)\theta_v. \quad ∎$$

1.4 COROLLARY: *The following relations are satisfied in $\mathbf{G}_n$:*
R7 $(T_{i,b})^*T_{i+1,a} = (T_{i+1,ba^2})^*T_{i,-1/a}$.

Proof: It suffices to prove the corollary for $b = 1$. Since the pair T_i, T_{i+1} is conjugate to the pair T_1, T_2 in $\mathbf{G}_n$, it suffices to prove the corollary for $i = 1$. We denote by L the left side of R7 and by R the right side. We apply ϕ_n to both sides of R7. $\phi_n(T_1) = \theta_1$. Let $u = (\delta_1)T_{2,a} = \delta_1 - a\delta_2$. By 1.3, $\phi_n(L) = \theta_u$. $\phi_n(T_2) = \theta_2$. Let $w = a\delta_2$. Then $\theta_w = \theta_{2,a^2}$,

$$(w)\theta_{1,-1/a} = w + (1/a)(w,\delta_1)\delta_1 = -u.$$

Clearly $\theta_u = \theta_{-u}$ and, by 1.3, $\phi_n(R) = \theta_u$. Thus $\phi_n(R) = \phi_n(L)$. But by 1.2, ϕ_n restricted to the subgroup of $\mathbf{G}_n$ generated by T_1 and T_2 is a monomorphism, so $R = L$. ∎

2. Relations Between $\mathbf{G}_n$ and $\mathbf{G}_{n-1}$ for n Even

We fix an even number $n \geq 4$ and assume that Theorem 1 is true for $n-1$. In this section we shall prove that ϕ_n is an isomorphism and in section 4 we shall prove that ϕ_{n+1} is an isomorphism. Theorem 1 will follow by induction.

Let $\mathbf{H}_{i,k}$ be the subgroup of $\mathbf{G}_n$ generated by $T_i, T_{i+1}, \ldots, T_k$, $k < n$. It follows from our assumptions that ϕ_n restricted to $\mathbf{H}_{1,n-2}$ is a monomorphism .

2.1 LEMMA: *Suppose that ϕ_m restricted to $\mathbf{H}_{1,k}$ is a monomorphism for some $k < m$ (this is true in particular for $m = n$ and $k < n-1$). Let $A, B \in \mathbf{H}_{i,i+k-1}, i+k-1 < m$, be such that $\phi_m(A) = \phi_m(B)$. Then $A = B$.*

Proof: Let $D = T_{m-1}T_{m-2}\cdots T_1$. For $j < m-1, T_j^*D = T_{j+1}$ so

$$D^{-1}\mathbf{H}_{1,k}D = \mathbf{H}_{2,k+1} \quad \text{and } D^{1-i}\mathbf{H}_{1,k}D^{i-1} = \mathbf{H}_{i,i+k-1}.$$

Let $\phi_m(D) = d \in \mathrm{Sp}^\sim(m-1, F)$. Then for $A \in \mathbf{H}_{1,k}, \phi_m(A)^*d = \phi_m(A^*D)$. It follows that ϕ_m restricted to $\mathbf{H}_{i,i+k-1}$ is a monomorphism. ∎

For k odd, $k < n$, let E_k denote the transvection with respect to vector e_k. Let $\Gamma_1 = T_1$ and for k odd, $k > 1$ let

$$\Gamma_k = (\Gamma_{k-2})^* T_{k-1} T_{k,-1} T_{k-1,-1/2} T_{k+1} T_{k,2} T_{k+1}.$$

2.2 Lemma: (i) $\phi_n(\Gamma_k) = E_k$ *for* $k = 1, 3, \ldots, n-1$.
(ii) $\phi_n(\Gamma_k^2) = (E_{k-2}\theta_{k-1}\theta_k)^4$ *for* $k = 3, \ldots, n-1$.

Proof: (i) follows by induction from Lemma 1.3 and definitions. The action of both sides of (ii) on V_n can be compared directly. ∎

2.3 Lemma: (i) Γ_{n-3} *commutes with* T_k *for* k *not equal to* $n-2$.
(ii) *Let* $\sigma(T_1) = \Gamma_{n-3}, \sigma(T_2) = T_{n-2}, \sigma(T_3) = T_{n-1}$. *Then* σ *extends to a homomorphism* $\sigma : \mathbf{G}_4 \to \mathbf{G}_n$.
(iii) $(\Gamma_{n-3}T_{n-2}T_{n-1})^{4p} = 1$.

Proof: $\Gamma_{n-3} \in \mathbf{H}_{1,n-2}$. By 2.2, $\phi_n(\Gamma_{n-3}) = E_{n-3}$. Clearly E_{n-3} commutes with θ_k for $k < n-2$, hence Γ_{n-3} commutes with T_k for $k < n-2$ by 2.1 . Also by 2.2 and 2.1,

$$\Gamma_{n-3}^2 = (\Gamma_{n-5}T_{n-4}T_{n-3})^4 \in \mathbf{H}_{1,n-3}, \quad (\Gamma_{n-3})^p = 1,$$

hence $\Gamma_{n-3} \in \mathbf{H}_{1,n-3}$, and Γ_{n-3} commutes with T_{n-1} by R2. There exists $h \in \mathrm{Sp}^\sim(n-1, p)$ such that $(\delta_1)h = e_{n-3}$ and $(\delta_2)h = \delta_{n-2}$. Thus, by 1.3, any relation between θ_1 and θ_2 corresponds to a relation between E_{n-3} and θ_{n-2}. Since $\Gamma_{n-3} \in \mathbf{H}_{1,n-3}$ it follows by 2.1, 2.2 and the definitions that σ takes relations R1–R5 onto relations in $\mathbf{G}_n$. It remains to prove (iii) for $n = 4$.

$$\begin{aligned}(T_1T_2T_3)^4 &= (T_1T_2)^3 T_3T_2T_{1,2}T_2T_3 \quad \text{(by R1 and R2)}\\ &= T_{1,-2}(T_{2,-1}T_{1,-2}T_{2,-1}T_3T_2T_{1,2}T_2)T_3 \quad \text{(by R4 and R1).}\end{aligned}$$

Each factor of the last expression has order p in $\mathbf{G}_n$, by R3 . If we prove that the factors commute with each other we are done . By R1 and R2 the first factor commutes with the others and we have

$$T_{2,-1}T_{1,-2}T_{2,-1}T_3T_2T_{1,2}T_2T_3 = T_3T_2T_{1,2}T_2T_3T_{2,-1}T_{1,-2}T_{2,-1}.$$

By R4 and R1 we have $T_2T_{1,2}T_2 = T_{1,-4}T_{2,-1}T_{1,-2}T_{2,-1}$. Since also T_1 commutes with T_3 and with $T_2T_{1,2}T_2$ we are done. ∎

It follows from Lemma 2.3 that there exists a split epimorphism $\rho_n : \mathbf{G}_n \to \mathbf{G}_{n-1} \cong \mathbf{H}_{1,n-2}$ such that $\rho_n(T_j) = T_j$ for $j = 1, \ldots, n-2$ and $\rho_n(T_{n-1}) = \Gamma_{n-3}$. Let $C_1 = \Gamma_{n-3}T_{n-1,-1}, C_i = C^*_{i-1}T_{n-i}$ for $i = 2, \ldots, n-2$. Clearly C_i belongs to the kernel of ρ_n.

2.4 Lemma: (i) *$\ker \rho_n$ is generated by $C_1, \ldots, C_{n-2}$, and $C_i^p = 1$ for $i = 1, \ldots, n-2$.*
(ii) *Let C be the commutator $C = [C_1, C_2]$. Then $C^p = 1$ and the commutant subgroup $(\ker \rho_n)'$ is cyclic, central, generated by C.*

Proof: (i) Clearly $\Gamma^p_{n-3} = 1$ and Γ_{n-3} commutes with T_{n-1}, hence $C_i^p = 1$ for $i = 1, \ldots, n-2$. Since ρ_n splits $\ker\rho_n$ is generated by the conjugates of C_1 by the elements of $\mathbf{H}_{1,n-2}$. It suffices to prove that $C_i^*T_j$ belongs to the subgroup $\mathbf{K}$ generated by $C_1, \ldots, C_{n-2}$ for $j = 1, \ldots, n-2$. It follows from R1, R2, and 2.3 that $C_i^*T_j = C_i$ for $j < n-i-1$ or $j > n-i$. Also $C_i^*T_{n-i-1} = C_{i+1}$ for $i < n-2$.

We shall prove that $C_2^*T_{n-2} = C_2C_1^{-1}C_2$. We have

$$C_2C_1^{-1}C_2 =$$
$$T_{n-2,-1}T_{n-1,-1}\Gamma_{n-3}T_{n-2}\Gamma^{-1}_{n-3}T_{n-1}T_{n-2,-1}\Gamma_{n-3}T_{n-1,-1}T_{n-2} =$$

(by R1 and 2.3ii)

$$T_{n-2,-1}T_{n-1,-1}T_{n-2,-1}\Gamma_{n-3}T_{n-2}T_{n-1}T_{n-2,-1}\Gamma_{n-3}T_{n-1,-1}T_{n-2} =$$

(by R1 and 2.3i)

$$T_{n-2,-1}T_{n-1,-1}T_{n-2,-1}T_{n-1,-1}\Gamma_{n-3}T_{n-2}T_{n-1}\Gamma_{n-3}T_{n-1,-1}T_{n-2} =$$

(by R1 and 2.3i)

$$T_{n-2,-2}T_{n-1,-1}T_{n-2,-1}\Gamma_{n-3}T_{n-2}\Gamma_{n-3}T_{n-2} =$$

(by R1 and 2.3ii)

$$T_{n-2,-2}T_{n-1,-1}T_{n-2,-1}T_{n-2}\Gamma_{n-3}T_{n-2,2} =$$

$$T_{n-2,-1}C_2T_{n-2,1} = C_2^*T_{n-2}$$

as required .

We shall prove now by induction that $C_j^*T_{n-j} = C_jC_{j-1}^{-1}C_j \in \mathbf{K}$ for $j = 2,\ldots,n-2$. Conjugating each term of the last equality by $T_{n-j-1}T_{n-j}$ we get $(C_{j+1}^*T_{n-j-1}) = C_{j+1}C_j^{-1}C_{j+1}$. Starting from the equality $C_2^*T_{n-2} = C_2C_1^{-1}C_2$ we get the required result by induction .

It remains to conjugate C_{n-2} by T_1, but since $\mathbf{H}_{1,n-2}$ is also generated by $T_2, T_3, \ldots, T_{n-2}, \Gamma_{n-3}$ we shall conjugate by Γ_{n-3} instead.

$$C_{n-2}^*\Gamma_{n-3} =$$

(by 2.3)

$$(C_2^*\Gamma_{n-3})^*T_{n-3}T_{n-4}\cdots T_2.$$

$$C_2^*\Gamma_{n-3} = \Gamma_{n-3}^{-1}T_{n-2,-1}T_{n-1,-1}\Gamma_{n-3}T_{n-2}\Gamma_{n-3} =$$

(by 2.1 and 2.3ii)

$$\Gamma_{n-3}^{-1}T_{n-2,-1}T_{n-1,-1}T_{n-2}\Gamma_{n-3}T_{n-2} =$$

(by 2.1)

$$\Gamma_{n-3}^{-1}T_{n-1}T_{n-2,-1}T_{n-1,-1}\Gamma_{n-3}T_{n-2} = C_1^{-1}C^2 \in \mathbf{K}.$$

(ii)

$$C = C_1C_2C_1^{-1}C_2^{-1} =$$

$$\Gamma_{n-3}T_{n-1,-1}T_{n-2,-1}T_{n-1,-1}\Gamma_{n-3}T_{n-2}\Gamma_{n-3}^{-1}T_{n-1}T_{n-2,-1}T_{n-1}\Gamma_{n-3}^{-1}T_{n-2} =$$

(by 2.3ii)

$$\Gamma_{n-3}T_{n-1,-1}T_{n-2,-1}T_{n-1,-1}T_{n-2,-1}\Gamma_{n-3}T_{n-2}T_{n-1}T_{n-2,-1}T_{n-1}\Gamma_{n-3}^{-1}T_{n-2} =$$

(by R1)

$$\Gamma_{n-3}T_{n-1,-1}T_{n-2,-1}T_{n-1,-1}T_{n-2,-1}\Gamma_{n-3}T_{n-1,-1}T_{n-2}T_{n-1}T_{n-1}\Gamma_{n-3}^{-1}T_{n-2} =$$

(by 2.3i)

$$\Gamma_{n-3}T_{n-1,-1}T_{n-2,-1}T_{n-1,-1}T_{n-2,-1}T_{n-1,-1}\Gamma_{n-3}T_{n-2}\Gamma_{n-3}^{-1}T_{n-1}T_{n-1}T_{n-2} =$$

(by R1 and 2.3ii)

$$\Gamma_{n-3}(T_{n-1,-1}T_{n-2,-1})^3\Gamma_{n-3}T_{n-2}T_{n-1}T_{n-1}T_{n-2}.$$

By R4 and R1 the expression in the bracket is equal to $(T_{n-2}T_{n-1})^3$, so by R1 and 2.3 we have $C = (\Gamma_{n-3}T_{n-2}T_{n-1})^4$. By 2.3iii, $C^p = 1$.

We shall prove that C lies in the center of $\mathbf{G}_n$. By R1, R2, and 2.3, C commutes with T_i for $i \neq n-3$. We have seen before that

$$\begin{aligned} C &= \Gamma_{n-3}(T_{n-1}T_{n-2})^{-3}\Gamma_{n-3}T_{n-2}T_{n-1}T_{n-1}T_{n-2} \\ &= \Gamma_{n-3}T_{n-1,-2}(\Gamma^*_{n-3}T_{n-2}T_{n-1}T_{n-1}T_{n-2}). \end{aligned}$$

Since T_{n-3} commutes with Γ_{n-3} and with T_{n-1} it remains to prove that it commutes with $\Gamma^*_{n-3}T_{n-2}T_{n-1,2}T_{n-2}$ or that

$$A = \Gamma^*_{n-3}T_{n-2}T_{n-1,2}T_{n-2}T_{n-3}T_{n-2,-1}T_{n-1,-2}T_{n-2,-1}$$

is equal to Γ_{n-3}. By R1 and R2

$$A = \Gamma^*_{n-3}T_{n-2}T_{n-3,-1}T_{n-1,2}T_{n-2}T_{n-1,-2}T_{n-3}T_{n-2,-1} =$$

(by R7)

$$\Gamma^*_{n-3}T_{n-2}T_{n-3,-1}T_{n-2,-1/2}T_{n-1,4}T_{n-2,1/2}T_{n-3}T_{n-2,-1}.$$

Let $u = (e_{n-3})T_{n-2}T_{n-3,-1}T_{n-2,-1/2} = e_{n-5} + 2\delta_{n-3} = (e_{n-5})T_{n-4}T_{n-3,2}T_{n-4}$. Then by 1.3,

$$\phi_n(\Gamma^*_{n-3}T_{n-2}T_{n-3,-1}T_{n-2,-1/2}) = \theta_u = \phi_n(\Gamma^*_{n-5}T_{n-4}T_{n-3,2}T_{n-4}).$$

By 2.1 we have $\Gamma^*_{n-3}T_{n-2}T_{n-3,-1}T_{n-2,-1/2} = \Gamma^*_{n-5}T_{n-4}T_{n-3,2}T_{n-4}$ commutes with T_{n-1}. Therefore

$$\Gamma^*_{n-3}T_{n-2}T_{n-3,-1}T_{n-2,-1/2}T_{n-1,4} = \Gamma^*_{n-3}T_{n-2}T_{n-3,-1}T_{n-2,-1/2}$$

and $A = \Gamma_{n-3}$. So C belongs to the center of $\mathbf{G}_n$. Now for $i < j$ we have

$$[C_i, C_j] = [C_1, C_2]^{*}T_{n-3}T_{n-4}\cdots T_{n-j}T_{n-2}T_{n-3}\cdots T_{n-i} = C.$$

Therefore the commutant subgroup of $\ker\rho_n$ is the cyclic subgroup of order p generated by C. This concludes the proof of Lemma 2.4. ∎

We shall define a map $\rho' : \mathrm{Sp}^{\sim}(n-1,F) \to \mathrm{Sp}^{\sim}(n-2,F)$. First let $p_{n-1} : V_{n-1} \to V_{n-2}$ be a linear map such that $(\delta_i)p_{n-1} = \delta_i$ for $i < n-1$ and $(\delta_{n-1})p_{n-1} = -e_{n-3}$ so ker p_{n-1} is spanned by e_{n-1}. Now for $u \in V_{n-2}$ and $h \in \mathrm{Sp}^{\sim}(n-1,F)$ let $(u)\rho'(h) = ((u)h)p_{n-1}$. It is easy to check that ρ' is a homomorphism and we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \to \ker_{\rho_n} & \to & \mathbf{G}_n & \overset{\rho_n}{\to} & \mathbf{G}_{n-1} & \to & 1 \\ & \phi_n|\ker_{\rho_n}\downarrow & & \phi_n\downarrow & & \phi_{n-1}\downarrow & & \\ 1 & \to \ker_{\rho'} & \to & \mathrm{Sp}^{\sim}(n-1,F) & \to & \mathrm{Sp}^{\sim}(n-2,F) & \to & 1 \end{array}$$

We want to prove that ϕ_n is an isomorphism. By the induction hypothesis ϕ_{n-1} is an isomorphism, so it suffices to prove that $\phi_n|\ker\rho_n$ is an isomorphism. We shall determine $\ker\rho'$. If $h \in \ker\rho'$ then $(\delta_j)h = \delta_j + a_j e_{n-1}$ for $j = 1, \ldots, n-1$. Also $(e_{n-1})h = e_{n-1}$. It follows that the correspondence $h \to (a_1, \ldots, a_{n-2})$ defines a homomorphism, say μ, of $\ker\rho'$ into an abelian group F^{n-2}. Let $h_i = \phi_n(C_i)$ for $i = 1, \ldots, n-2$. Then $h_i \in \ker\rho'$. $(\delta_j)h_1 = \delta_j$ for $j < n-2$ and $(\delta_{n-2})h_1 = \delta_{n-2} + e_{n-1}$. It follows that $(\delta_j)h_i = \delta_j$ for $j < n-i-1$ and $(\delta_{n-i-1})h_i = \delta_{n-i-1} + e_{n-1}$. Thus $\mu(h_i), i = 1, \ldots, n-2$ form a basis of F^{n-2} and μ is onto. If h belongs to $\ker\mu$ then $(\delta_j)h = \delta_j$ for $j = 1, \ldots, n-1, (\delta_n)h = \delta_n + ae_{n-1}$ so $\ker\mu$ is a cyclic group of order p, or a trivial group. But $(\delta_n)\phi_n(C) = \delta_n + 2e_{n-1}$ and $\phi_n(C) \in \ker\mu$. So $\ker\mu$ is not trivial, $\ker\rho'$ has p^{n-1} elements and $\phi_n|\ker\rho_n$ is onto. By Lemma 2.4 $\ker\rho_n$ has at most p^{n-1} elements, so $\phi_n|\ker\rho_n$ is an isomorphism . We have proven the following:

2.6 PROPOSITION: *ϕ_n is an isomorphism.*

3. Some Properties of $\mathbf{G}_{n+1}$

We assume that $n > 2$ is a fixed even number and that ϕ_n is an isomorphism. Thus ϕ_{n+1} restricted to $\mathbf{H}_{1,n-1}$ is a monomorphism.

We let $S = (T_n)^* T_{n-1,-1} T_{n-2,-2} T_{n-1,-1} \in \mathbf{G}_{n+1}$ and we let $\mathbf{H}$ be the subgroup of $\mathbf{G}_{n+1}$ generated by $T_1, \ldots, T_{n-2}, S, T_n$. This section will be devoted to a proof of the following

3.1 PROPOSITION: *Let $W \in \mathbf{G}_{n+1}$ be such that $(\delta_n)W = \delta_n$. Then $W \in \mathbf{H}$.*

An element W of $\mathbf{G}_{n+1}$ can be written in a form $W \equiv \prod_{i=1}^{s} T_{j(i),a(i)}$ where by "$\equiv$" we mean equality in a free group while $W = W_1$ means equality in the group

$\mathbf{G}_{n+1}$. We shall say that a word $W = \prod_{i=1}^{s} T_{j(i),\alpha(i)}$ is reduced if $j(i) \neq j(i+1)$ and $\alpha(i) \neq 0$ for $i = 1, \ldots, s$. If W is reduced then the length of W is $\ell(W) = s$. We shall say that W represents a vector $u \in V_n$ if $(\delta_n)W = u$. We want to prove by induction on $\ell(W)$ that if W represents δ_n then $W \in \mathbf{H}$. Applying consecutive terms of W to δ_n we get a sequence of vectors . We shall prove Proposition 3.1 by induction on the "complexity" of these vectors . If $v = \Sigma_{i=1}^{n} a_i \delta_i \in V_n$ we let $a_0 = 0 = a_{n+1}$ to unify notation .

3.2 DEFINITION. Let $0 \neq v = \Sigma_{i=1}^{n} a_i \delta_i \in V_n$. Let a_r be the first non-zero coordinate of v. Then $r(v) = r$. Let $e(v) = 1$ if $a_n = 0$ or $a_n = 1$ and $e(v) = 2$ otherwise. A coordinate a_i is **passive** if $a_i = 0$ and $a_{i-1} = a_{i+1} \neq 0$. Let P be the number of the passive coordinates of v and let N be the number of the non-zero coordinates of v. Vector v is **special** if

$$v \neq \delta_n \quad \text{and} \quad v = b(\delta_{n-2k} + \delta_{n-2k+2} + \ldots + \delta_n).$$

The **complexity** of v equals $c(v) = 2(n-r) + e(v) + 1$ if v is special and $c(v) = 2(n-r) + e(v) + P - N$ if v is not special. ∎

3.3 DEFINITION. Let $0 \neq v = \Sigma_{i=1}^{n} a_i \delta_i V_n$. A coordinate a_j is **reducing** if $a_{j+1} \neq a_{j-1}$ and if, after we replace a_j by a suitable b_j, the complexity of v decreases. $T_{j,\alpha}$ **reduces** v if $c((v)T_{j,\alpha}) < c(v)$.

If a_j is a reducing coordinate of v then $T_{j,\alpha}$ reduces v for a suitable choice of α because $(v)T_{j,\alpha} = v + \alpha(a_{j+1} - a_{j-1})\delta_j$, so we can change a_j into an arbitrary b_j.

3.4 LEMMA: *Let $0 \neq v = \Sigma_{i=1}^{n} a_i \delta_i \in V_n$. Let a_r be the first non-zero coordinate of v. Let a_j be a coordinate of v such that $a_{j+1} \neq a_{j-1}$. Let $w = (v)T_{j,\alpha}, \alpha \neq 0$, and let $b_j = a_j + \alpha(a_{j+1} - a_{j-1})$ be the j-coordinate of w. Then*

(i) $|c(w) - c(v)| \leq 1$.

(ii) *a_j is a reducing coordinate of v if and only if one of the following is satisfied:*

(a) *$j = n, a_{n-1} \neq 0, a_n \neq 1$. $T_{j,\alpha}$ reduces v if $b_n = 1$, i.e. if $\alpha = (1 - a_j)/(a_{j+1} - a_{j-1})$.*

(b) *$r < j < n, a_j = 0, a_{j+1} \neq a_{j-1}$. $T_{j,\alpha}$ reduces v if it does not introduce a new passive coordinate, i.e. $T_{j,\alpha}$ does not reduce v for at most one value of α.*

(c) *$r < j < n, a_j \neq 0, a_j$ has a passive neighbour and a nonzero neighbour. $T_{j,\alpha}$ reduces v whenever $b_j \neq 0$, i.e. $T_{j,\alpha}$ does not reduce v for exactly one value of $\alpha, \alpha = -a_j/(a_{j+1} - a_{j-1})$.*

(d) $j = r, a_{r+1} \neq 0$ *and* $v - a_r\delta_r$ *is not special.* $T_{j,\alpha}$ *reduces* v *when* $b_j = 0$, *i.e.* $\alpha = -a_j/(a_{j+1} - a_{j-1})$.

(e) $j = r - 1$ *and* v *is special.* $T_{j,\alpha}$ *reduces* v *for all* α.

Proof: Follows from the definitions. ∎

3.5 LEMMA: *Let* $0 \neq v = \Sigma_{i=1}^{n} a_i\delta_i \in V_n$. *Then*
(i) $c(v) \geq 0$. $c(v) = 0$ *if and only if* $v = \delta_n$. v *has a reducing coordinate .*
(ii) *If* $a_t, a_{t+1} \neq 0$ *then there exists a reducing coordinate* $a_m, m \leq t$, *unless* $t = r(v)$ *and* $v - a_r\delta_r$ *is special.*
(iii) *Suppose* a_j *is a reducing coordinate of* v *satisfying* 3.4ii(b) *or* 3.4ii(c). *Let* $|k - j| = 1$, *let* $w = (v)T_{k,\beta}$, *and let* b_k *be the* k*-coordinate of* w. *Then* a_j *is a reducing coordinate of* w *and satisfies again* 3.4ii(b) *or* 3.4ii(c) *with the exception of the following cases:*
(a) $a_j = 0, a_k \neq 0$ *and the neighbours of* a_j *in* w *are equal to zero. Then* N *decreases so* $c(w) > c(v)$.
(b) $a_j = 0, a_k \neq 0$ *and the neighbours of* a_j *in* w *are equal but not zero. Then* a_j *becomes passive so* P *increases and* $c(w) > c(v)$.
(c) $a_j = 0, a_k = 0$ *and the neighbours of* a_j *in* w *are equal. Then* a_j *becomes passive so* P *increases by 1 and* N *increases by 1,* $c(w) = c(v)$. *Also* a_k *satisfies* 3.4ii(b) *and is reducing.*
(d) $a_j \neq 0, a_k \neq 0, n > k > r$ *and* $b_k = 0$. *Then, if* a_k *has a passive neighbour,* $c(w) = c(v)$ *and* a_k *is reducing. If* a_k *has no passive neighbour then* $c(w) > c(v)$.
(e) $a_j \neq 0, a_k \neq 0, a_k \neq 1, k = n, b_k = 0$. *Then* a_k *is reducing and* $c(w) = c(v)$.
(f) $a_j \neq 0, a_k = 1, k = n, b_k = 0$. *Then* $c(w) > c(v)$.
(g) $a_j \neq 0, a_k \neq 0, k = r = j - 1, b_k = 0$ *and* w *is special . Then* $c(w) > c(v)$.
(h) $a_j \neq 0, a_k \neq 0, k = r = j - 1, b_k = 0$ *and* w *is not special .*

Proof: Part (i) follows from the definitions . Suppose $a_{t-i-1} = 0, a_{t-i} \neq 0, a_{t-i+1} \neq 0, \ldots, a_t \neq 0, a_{t+1} \neq 0$. If a_{t-i-1} is passive then a_{t-i} is reducing. If a_{t-i-1} is not passive and $t - i \neq r$ then a_{t-i-1} is reducing. If $t - i = r$ then a_{t-i} is reducing by 3.3iii(b) unless $t = r$ and $v - a_r\delta_r$ is special . This proves part (ii). Part (iii) follows from definitions. ∎

3.6 LEMMA–DEFINITION: *Let* $0 \neq v = \Sigma_{i=1}^{n} a_i\delta_i \in V_n$ *and let* $r(v) = r$. *There exists a reduced word* $W = \Pi_{i=1}^{s} T_{j(i),\alpha(i)}$ *of length* $c(v)$ *representing* v. *There is no shorter word representing* v, *so* W *is called a* **minimal representative** *of* v.

If $T_{j,\alpha}$ reduces v then there is a minimal representative of v with the last term $T_{j,-\alpha}$. A minimal representative W satisfies the following:

For all i, $j(i) > r-1$ if v is not special and $j(i) > r-2$ if v is special. $j(i) = n$ for at most one value of i and $j(i) \neq n$ if $a_n = 1$.

If $m < n$ then $j(i) = m$ for at most two values of i.

If $a_m \neq 0$ is not reducing and has a non-zero neighbour then $j(i) = m$ for at most one value of i.

Proof: If $T_{j,\alpha}$ reduces v then $(v)T_{j,\alpha}$ has lower complexity, so the existence of W with the last term $T_{j,-\alpha}$ follows from 3.5i by induction on $c(v)$. There is no shorter representative of v by 3.4i . If v is not special then it will never become special in the reduction process, so the j-coordinate will never become reducing for $j < r$ and $j(i) > r-1$ for all i. If v is special then $(v)T_{r-1,a}$ is not special and $j(i) > r-2$. If $a_n = 1$ then a_n is not reducing and the n-coordinate will never become reducing in the reduction process, by 3.4ii(a), so $j(i) \neq n$. Let $W_k = \Pi_{i=1}^{k} T_{j(i),\alpha(i)}$ and let $v_k = (\delta_n)W_k$. Then $c(v_{k+1}) = c(v_k) + 1$ for all k. If $j(t) = n$ then the n-coordinate of v_t is not 1 and a later change of the n-coordinate would not increase the complexity so $j(i) \neq n$ for $i > t$. Let $m < n$ and let t_1 be the smallest value such that $j(t_1) = m$. Then the m-coordinate of v_{t_1} is not zero. If t_2 is the next such value then the m-coordinate of v_{t_2} is reducing. Either v_{t_2} is special and we cannot increase its complexity by one move or $m > r(v_{t_2})$. The m-coordinate is zero or it has a passive neighbour. If we increase complexity getting vector v_s, the neighbour remains passive and $m > r(vs)$. A later change of the m-coordinate would not increase the complexity, so $j(i) \neq m$ for $i > t_2$. If the m-coordinate of v_{t_2} is not zero it has a passive neighbour , and the neighbour will remain passive in v . If a_m is not reducing in v then its other neighbour must be zero, so a_m has no non-zero neighbour. This completes the proof of the lemma. ∎

We shall fix now a reduced word $W = \Pi_{i=1}^{s} T_{j(i),\alpha(i)}$ representing δ_n. Let $W_k = \Pi_{i=1}^{k} T_{j(i),\alpha(i)}$ and let $v_k = (\delta_n)W_k$. Let q be the smallest index such that $c(v_q) \geq c(v_{q+1})$, i.e. $c(v_k) < k$ for $k > q$. We shall prove that $W \in \mathbf{H}$ by induction on $s = \ell(W)$ and for a given s by induction on q. If $s = 0$ then $W = 1 \in \mathbf{H}$.

If $q = 0$ then $c(\delta_n) \geq c(v_1)$, hence $v_1 = \delta_n, j(1) \neq n-1, T_{j(1),\alpha(1)} \in \mathbf{H}$, and $\Pi_{i=2}^{s} T_{j(i),\alpha(i)}$ also represents δ_n. Therefore $W \in \mathbf{H}$ by induction on s.

Let $v_q = \Sigma_{i=1}^{n} a_i\delta_i$. Let a_r be the first nonzero coordinate of v_q.

Let $j(q) = j, \alpha(q) = \alpha, j(q+1) = k, \alpha(q+1) = \beta$. Then a_j is a reducing coordinate of v_q, since $c(v_q) > c(v_{q-1})$ and $v_{q-1} = (v_{q-1})T_{j,-\alpha}$.

3.7 LEMMA: (i) *If $T_{j,\gamma}$ reduces v_q and $T_{m,\delta}$ reduces v_{q+1} and V is any minimal representative of $(v_q)T_{j,\gamma}$ and U is any minimal representative of $(v_{q+1})T_{m,\delta}$, then we may assume $W \equiv VT_{j,\gamma}T_{k,\beta}T_{m,\delta}U^{-1}$ and $\ell(W) < 2q+2$. If $W' \equiv \Pi_{i=1}^{s} T_{j'(i),\alpha'(i)}$ and W' represents δ_n and*

$$\ell(W') < 2q+2 \quad \text{and} \quad v'_k = (\delta_n)\Pi_{i=1}^{k} T_{j'(i),\alpha'(i)}$$

then $c(v'_{q+1}) < q+1$.

(ii) *If a_k is reducing then we may assume that $T_{k,\beta}$ reduces v_q. Also we may switch j and k and assume that $W = W' \equiv \Pi_{i=1}^{s} T_{j'(i),\alpha'(i)}$ with $v'_q = v_q, j'(q) = k, j'(q+1) = j$.*

(iii) *If a_k is not reducing and V is any minimal representative of v_q, then we can replace W_q by V in W.*

(iv) *If $|j-k| = 1$ and there exists γ such that $T_{j,\gamma}$ reduces v_q and v_{q+1}, then $W = W'_{q-1}T_{k,1/\gamma}T_{j,\beta\gamma^2}T_{k,-1/\gamma}U \equiv W', \ell(W') = \ell(W), v'_{q-1} = (v_q)T_{j,\gamma}, v'_q = (v'_{q-1})T_{k,1/\gamma}$. If $c(v'_q) \leq c(v_{q-1})$ then $W \in \mathbf{H}$. In particular if $v_q = v_{q+1}$ then $T_{j,-\alpha}$ reduces v_{q+1}, so*

$$W = W_{q-1}T_{k,1-1/\alpha}T_{j,\beta\alpha^2}T_{k,1/\alpha}(W_{q-1})^{-1} \quad \text{and} \quad v'_q = (v_{q-1})T_{k,-1/\alpha}.$$

If $c(v'_q) \leq c(v_{q-1})$ then $W \in \mathbf{H}$.

Proof: (i) Let $W \equiv W_{q-1}T_{j,\alpha}T_{k,\beta}U_1$. Let V be any minimal representative of $(v_q)T_{j,\gamma}$ and let U be any minimal representative of $(v_{q+1})T_{m,\delta}$. Then

$$W \equiv (W_{q-1}T_{j,\alpha-\gamma}V^{-1})VT_{j,\gamma}T_{k,\beta}T_{m,\delta}U^{-1}(UT_{m,-\delta}U_1).$$

Brackets represent δ_n and have length smaller than $\ell(W)$. By induction it suffices to prove that $W \in \mathbf{H}$ for $W \equiv VT_{j,\gamma}T_{k,\beta}T_{m,\delta}U^{-1}$ and then $\ell(W) < 2q+2$. The second statement of (i) is obvious from definitions .

(ii) If $T_{k,\varepsilon}$ reduces v_q and V is a minimal representative of $(v_q)T_{k,\varepsilon}$, then $W = W_qT_{k,\beta}U = (W_qT_{k,\varepsilon}V^{-1})(VT_{k,\beta-\varepsilon}U)$, both brackets represent δ_n and the second bracket has length smaller than $\ell(W)$ since $\ell(V) = q-1 \leq \ell(U)$. So we may assume $T_{k,\beta} = T_{k,\varepsilon}$ reduces v_q. Now, by (i), $W = W_{q-1}T_{j,\alpha}T_{k,\beta}U$

where $U^{-1}T_{k,-\beta}$ is a minimal representative of v_q. It suffices to prove that $W' = W^{-1} = U^{-1}T_{k,-\beta}T_{j,\alpha}W_{q-1} \in \mathbf{H}$ which proves (ii) .

(iii) If a_k is not reducing and V is any minimal representative of v_q, then $W = W_qT_{k,\beta}U = (W_qV^{-1})(VT_{k,\beta}U)$. Both brackets represent δ_n and $\ell(W_qV^{-1}) = 2q < 2q+1 = \ell(W)$ so we may assume $W = VT_{k,\beta}U$.

(iv) By (i) we may assume $W = W'_{q-1}T_{j,-\gamma}T_{k,\beta}T_{j,\gamma}U$ with $v'_{q-1} = (v_q)T_{j,\gamma}$. Now by R7, $W = W'_{q-1}T_{k,1/\gamma}T_{j,\beta\gamma^2}T_{k,-1/\gamma}U$ as required .

If $c(v'_q) \leq c(v_{q-1})$ then $W \in \mathbf{H}$ by induction on q. ∎

3.8 LEMMA: *If either $v_q = v_{q+1}$ or $|k-j| > 1$, then $W = W' \equiv \Pi_{i=1}^{s} T_{j'(i),\alpha'(i)}$ and $j'(i) = j$ for at most one value of $i \leq q$. If also $j = n$ then $j'(i) \neq n$ for all $i \leq q$.*

If $|k-j| = 1$ and $r < j < n$, and $r < k < n$ or $k = n$ and $a_n \neq 1$, then $T_{j,\gamma}$ does not reduce v_q or v_{q+1} for at most two values of γ. In particular $W = W' \equiv \Pi_{i=1}^{s} T_{j'(i),\alpha'(i)}$ and $j'(i) = j$ for at most one value of $i \leq q$.

Proof: *If $|k-j| > 1$ then, by R2, we can replace $T_{j,\alpha}T_{k,\beta}$ by $T_{k,\beta}T_{j,\alpha}$ in W getting W'. Now $j'(i) = j$ a smaller number of times than $j(i) = j$ for $i \leq q$. If $|j-k| = 1$ and $v_q = v_{q+1}$ then, by 3.7iv, $W'_q = W_{q-1}T_{k,-1/\alpha}$ and again $j'(i) = j$ a smaller number of times than $j(i) = j$ for $i \leq q$. Suppose now $|k-j| = 1$ and $v_q \neq v_{q+1}$. a_j is reducing and $n > j > r$. So a_j satisfies 3.4iib or 3.4iic . We have $c(v_q) \geq c(v_{q+1})$ and, by 3.7ii, if a_k is reducing then $c(v_q) > c(v_{q+1})$, therefore by 3.5 a_j is a reducing coordinate of v_{q+1}. By 3.4iib and 3.4iic $T_{j,\gamma}$ does not reduce v_q or v_{q+1} for at most two values of γ. Since $p > 3$ there exists γ such that $T_{j,\gamma}$ reduces v_q and v_{q+1} and then, by 3.7iv,*

$$W = W' \equiv \prod_{i=1}^{s} T_{j'(i),\alpha'(i)}, \quad j'(q) = k \quad \text{and} \quad v'_{q-1} = (v_q)T_{j,\gamma}.$$

Since $n > j > r$ the j-coordinate of v'_{q-1} is not reducing, not zero, and has a non-zero neighbour . Thus $j'(i) = j$ for at most one value of $i < q+1$, by 3.6.
∎

3.9 LEMMA: (i) *If $W \in \mathbf{H}_{n-2,n}$ then $W \in \mathbf{H}$.*
(ii) *If $W \in \mathbf{H}_{1,n-1}$ then $W \in \mathbf{H}$.*
(iii) *If $v_q = \beta(\delta_r + \delta_{r+2} + \ldots + \delta_{n-2}) + \delta_n$, r even, $\beta \neq 1$, then $W \in \mathbf{H}$.*

Proof: (i) $(\delta_i)W = \delta_i$ for $i < n-3$ and $i = n$. $(\delta_{n-3})W = \delta_{n-3} + a\delta_{n-2} + b\delta_{n-1} + c\delta_n$. Since $((\delta_{n-3})W, \delta_n) = 0$ we have $b = 0$. If also $c = 0$ then $(\delta_{n-3})WT_{n-2,a} =$

δ_{n-3}. Now $(\delta_{n-1})WT_{n-2,a} = \alpha\delta_{n-2} + \beta\delta_{n-1} + \gamma\delta_n$. The intersection form is preserved so $\alpha = 0, \beta = 1$. $(\delta_{n-1})WT_{n-2,\alpha}T_{n,\gamma} = \delta_{n-1}$. We must also have $(\delta_{n-2})WT_{n-2,\alpha}T_{n,\gamma} = \delta_{n-2}$. It follows that $\phi_{n+1}(WT_{n-2,a}T_{n,\gamma}) = 1$ hence $W = T_{n,-\gamma}T_{n-2,-\alpha} \in \mathbf{H}$, by 2.1.

If $c \neq 0$ then $(\delta_{n-3})WT_{n-2,a-2c} = \delta_{n-3} + 2c\delta_{n-2} + c\delta_n$. Let $u = 2\delta_{n-2} + \delta_n = (\delta_n)T_{n-1,-1}T_{n-2,-2}T_{n-1,-1}$. Then, by 1.3, $\phi_{n+1}(S) = T_u$ hence

$$(\delta_{n-3})WT_{n-2,a-2c}S^{c/2} = \delta_{n-3}.$$

We continue as in the case $c = 0$ and get $\phi_{n+1}(WT_{n-2,a-2c}S^{c/2}T_{n,\gamma}) = 1$, so by 2.1, $W = T_{n,-\gamma}S^{-c/2}T_{n-2,2c-a} \in \mathbf{H}$.

(ii) Let $A = \phi_{n+1}(W)$. The subspace V_{n-1} is A-invariant and $(\delta_n)A = \delta_n$. For $i < n-1, (\delta_i)A \in V_{n-1}$ and $((\delta_i)A, \delta_n) = 0$, hence V_{n-2} is A-invariant. There exists $B \in \mathrm{Sp}(n-2, F)$ such that A restricted to V_{n-2} equals B. Then $(\delta_i)AB^{-1} = \delta_i$ for $i \neq n-1$. Also $(\delta_{n-1})AB^{-1} \in V_{n-1}$. Since the intersection form is preserved it follows that $(\delta_{n-1})AB^{-1} = \delta_{n-1}$ and $A = B$. Since ϕ_{n-1} is an isomorphism there exists $W_1 \in \mathbf{H}_{1,n-2}$ such that $\phi_{n-1}(W_1) = B = A$. Now, by 2.1, $W = W_1 \in \mathbf{H}_{1,n-2} \subset \mathbf{H}$.

(iii) Let U be a minimal representative of v_q. Since $a_n = 1, U \in \mathbf{H}_{r,n-1}$, by 3.6. If $k \neq n$ then v_{q+1} also has the last coordinate equal to 1 and, by 3.6 and 3.7i, $W \in \mathbf{H}_{1,n-1}$ so $W \in \mathbf{H}$, by part (ii). We may assume $k = n$. Then $v_q = v_{q+1}$ and, by 3.7i, $W = UT_{n,\beta}U^{-1}$. Since a_n is not reducing we can choose for U any minimal representative of v_q, by 3.7ii , e.g.

$$\begin{aligned}U^{-1} =& T_{n-1,\beta/1-\beta}T_{n-2}T_{n-3}\cdots\\ & T_{r+1}T_{r,-1}T_{r+1,-1/2}T_{r+2,-2}T_{r+3,-1/2}\cdots\\ & T_{n-2,-2}T_{n-1,-\beta}.\end{aligned}$$

Then $(\delta_n)U^{-1} = \alpha(\delta_r + \delta_{r+2} + \ldots + \delta_{n-2}) + \delta_n = w$, where $\alpha = \beta/\beta - 1$. By 1.3, $\phi_{n+1}(W) = \theta_{w,\beta}$. Also $W \in \mathbf{H}_{2,n}$.

Let $u_1 = \alpha\delta_{n-2} + \delta_n, u_2 = \alpha(\delta_{r+1} + \delta_{r+3} + \ldots + \delta_{n-3}), u_3 = w + u_2, u_4 = w - u_2$. Let U_1 be a minimal representative of u_1. By 3.6, $U_1 \in \mathbf{H}_{n-2,n}$. Let $A_1 = (T_n)^*U_1$. Then $\phi_{n+1}(A_1) = \theta_{u_1}$, by 1.3 , hence $(\delta_n)A_1 = \delta_n$ and $A_1 \in \mathbf{H}$ by (i). $u_3 = (u_1)T_{n-3}T_{n-4}\cdots T_r, u_4 = (u_1)T_{n-3,-1}T_{n-4,-1}\cdots T_{r,-1}$. Applying Lemma 3.6 with n replaced by $n-2$ we find $U_2 \in \mathbf{H}_{r,n-2}$ such that $(\delta_{n-2})U_2 = u_2$. Let $A_2 = (T_{n-2})^*U_2, A_3 = (A_1)T_{n-3}T_{n-4}\cdots T_r, A_4 = (A_1)T_{n-3,-1}T_{n-4,-1}\cdots T_{r,-1}$.

Then $A_i \in \mathbf{H}, A_i \in \mathbf{H}_{2,n}, \phi_{n+1}(A_i) = \theta_{u_i}$ for $i = 1,2,3,4$. Also $\theta_{u_3}\theta_{u_4} = (\theta_w)^2(\theta_{u_2})^2$. Indeed since $(w, u_2) = 0$, we have

$$\begin{aligned}(v)\theta_{u_3}\theta_{u_4} &= v - (v, w+u_2)(w+u_2) - (v, w-u_2)(w-u_2)\\ &= v - 2(v,w)w - 2(v,u_2)u_2 = (v)(\theta_w)^2(\theta_{u_2})^2\end{aligned}$$

for any vector $v \in V_{n+1}$. Therefore $(\theta_{w,\beta})^2 = \phi_{n+1}(W^2) = \phi_{n+1}((A_3A_4A_2^{-2})^p)$. By 2.1, $W^2 \in \mathbf{H}$ and, since $W^p = 1, W \in \mathbf{H}$. ∎

3.10 Corollary: (i) *If* $a_n = 1$ *then* $W \in \mathbf{H}$.
(ii) *If* $a_i = 0$ *for* $i < n-2$ *and* $v_q \neq b(\delta_{n-2} + \delta_n)$, *then* $W \in \mathbf{H}$.

Proof: (i) By 3.6, $W_q \in H_{1,n-1}$. If also $k \neq n$ then the last coordinate of v_{q+1} is also equal to 1 and, by 3.6 and 3.7i, $W \in \mathbf{H}_{1,n-1}$, so $W \in \mathbf{H}$ by 3.9 . Suppose $k = n$. If $T_{k,\beta}$ changes the n-coordinate of v_q then, by 3.2, $c(v_{q+1}) > c(v_q)$ contrary to the choice of q. So suppose $v_{q+1} = v_q$. If there exists a reducing coordinate a_m of v_q different from a_{n-1} then, by 3.7i and 3.7iii, $W = W_{q-1}T_{m,\gamma}T_{n,\beta}T_{m,-\gamma}W_{q-1}^{-1}$. Now $T_{m,\gamma}$ cancels reducing the length of W. So we may assume that $a_{n-1} = 0$ is the only reducing coordinate of v_q. But then it follows easily from 3.4 that

$$v_q = b(\delta_r + \delta_{r+2} + \ldots + \delta_{n-2}) + \delta_n,$$

r even, and we are done by 3.9.
(ii) If $v_q \neq b(\delta_{n-2} + \delta_n)$ then $W_q \in \mathbf{H}_{n-2,n}$ by 3.6 . If $k > n-3$ then, by 3.6 and 3.7i, $W_q \in \mathbf{H}_{n-2,n}$ and we are done by 3.9. If $k < n-3$ then T_k commutes with W_q and $\ell(W)$ decreases. If $a_{n-2} = 0$ and $k = n-3$ then T_k commutes with W_q and $\ell(W)$ decreases. If $a_{n-2} \neq 0$ then T_{n-3} increases $c(v_q)$, so $k \neq n-3$. ∎

3.11 Lemma: *If* $j(i) = n-1$ *for only one value of* $i < q+1$, *then* $W \in \mathbf{H}$.

Proof: We may assume $j(1) = n-1$. Otherwise $T_{j(1),\alpha(1)} \in \mathbf{H}$ and we can reduce $\ell(W)$. By 3.10 we may assume that $j(i) = n$ for exactly one value of $i < q+1$. Since T_n commutes with $T_{j(i),\alpha(i)}$ for $i = 2,\ldots,q$ we may assume $j(2) = n$ or $j(q) = n$ as convenient. We have $a_{n-1} \neq 0$. If $k \neq n-1$ we let $j(q) = n$ and we are done by 3.8 and 3.10 . So we may assume $k = n-1$.

Case 1: $a_n = a_{n-2}$. Then $v_q = v_{q+1}$ and $j(q) = n$ so, by 3.8, $W = W'$ with $j'(q) = n-1$ and $j'(i) < n$ for all $i \leq q$. We are done by 3.10.

CASE 2: $a_n \neq a_{n-2} \neq 0$. We assume $j(2) = n$, so $j(q) < n$. If $j(q) < n-2$ then the j-coordinate is reducing for both v_q and v_{q+1}. By 3.7i we may assume

$$W = W_{q-1}T_{j,\alpha}T_{k,\beta}T_{j,\gamma}U = W_{q-1}T_{j,\alpha-\gamma}T_{k,\beta}U$$

and $\ell(W)$ reduces. If $j(q) = n-2$ then a_{n-2} is reducing, so either $r = n-2$, and we are done by 3.9 , or a_{n-3} is passive. In the latter case

$$v_q = \ldots + a_{n-4}\delta_{n-4} + a_{n-2}\delta_{n-2} + a_{n-1}\delta_{n-1} + a_n\delta_n$$

where $a_{n-4} = a_{n-2}$;

$$v_{q+1} = \ldots + a_{n-4}\delta_{n-4} + a_{n-2}\delta_{n-2} + b_{n-1}\delta_{n-1} + a_n\delta_n.$$

Since $p > 3$ there exists γ such that $T_{n-2,\gamma}$ reduces v_q and v_{q+1}. Also

$$v'_{q-1} = (v_q)T_{n-2,\gamma} = \ldots + a_{n-4}\delta_{n-4} + b_{n-2}\delta_{n-2} + a_{n-1}\delta_{n-1} + a_n\delta_n$$

and we can choose γ such that $T_{n-1,1/\gamma}$ does not increase $c(v'_{q-1})$. We are done by 3.7iv .

CASE 3: $a_n \neq a_{n-2} = 0$ and $a_{n-1} = a_{n-3}$. Then a_{n-2} is not reducing and we may assume $j(q) < n$, so $j(q) < n-2$. If $j(q) < n-3$ then $T_{j(q),-\alpha}$ reduces v_{q+1} and we are done by 3.7i . If $j(q) = n-3$ then a_{n-3} is reducing, so $a_{n-4} \neq 0$ and there exists a reducing coordinate a_t with $t < n-3$, by 3.5ii . Clearly a_t is reducing in v_{q+1} and, by 3.7i, we may assume

$$W = W_{q-1}T_{j,\alpha}T_{k,\beta}T_{t,\gamma}U = W_{q-1}T_{j,\alpha}T_{t,\gamma}T_{k,\beta}U.$$

Now $j(q+1) = t \neq n-1$, so we are done by 3.8 and 3.10 as before.

CASE 4: $a_n \neq a_{n-2} = 0$ and $a_{n-1} \neq a_{n-3}$. Now a_{n-1} is not reducing and a_{n-2} is reducing, so we may assume $j(q) = n-2$ by 3.7ii. We have

$$v_q = \ldots + a_{n-3}\delta_{n-3} + a_{n-1}\delta_{n-1} + a_n\delta_n,$$

$$v_{q+1} = \ldots + a_{n-3}\delta_{n-3} + b_{n-1}\delta_{n-1} + a_n\delta_n, \quad b_{n-1} \neq a_{n-3}.$$

Since $p > 3$ there exists γ such that $T_{n-2,\gamma}$ reduces v_q and v_{q+1} and $T_{n-1,1/\gamma}$ does not increase $c(v'_{q-1})$, where

$$v'_{q-1} = (v_q)T_{n-2,\gamma} = \ldots + a_{n-3}\delta_{n-3} + b_{n-2}\delta_{n-2} + a_{n-1}\delta_{n-1} + a_n\delta_n,$$

$$(v'_{q-1})T_{n-1,1/\gamma} = \ldots + a_{n-3}\delta_{n-3} + b_{n-2}\delta_{n-2} + b_{n-1}\delta_{n-1} + a_n\delta_n,$$

$$b_{n-2} = \gamma(a_{n-1} - a_{n-3}),$$

and

$$b_{n-1} = a_{n-1} + 1/\gamma(a_n - b_{n-2}) = 1/\gamma a_n + a_{n-3}.$$

We are done by 3.7iv. ∎

3.12 Lemma: *If for some $m < n$ we have $j(i) = m$ for at most one value of $i \leq q$, then $W \in \mathbf{H}$.*

Proof (by induction on m, downwards): If $m = n-1$ we are done by 3.11. Suppose that the lemma is true for m and suppose that $j(i) = m-1$ for at most one value of $i < q+1$.

Case 1: There exists i_0 such that $j(i) < m$ for $i > i_0$ and $j(i) \neq m-1$ for $i \leq i_0$ (e.g. $j(i) \neq m-1$ for all $i \leq q$ and $i_0 = q$, in particular $m = 1$). By R2 we may assume that $j(i) \geq m$ for $i \leq s$ and $j(i) \leq m-1$ for $i > s$. By 3.10 and the induction hypothesis we may assume that $j(i) = n$ for one value of $i \leq q$ and, for $t = m, m+1, \ldots, n-1, j(i) = t$ for two values of $i \leq q$. Thus $c(v_s) = 2(n-m)+1 = s$ and $r(v_s) \geq m$. In Definition 3.2, if v is not special then $P < N-1$. Thus $c(v_s) < 2(n-r) + e(v_s) - 1$. It follows that v_s is special, $r(v_s) = m+1$, and for $i > s, (v_s)T_{j(i)} = v_s$. Therefore $s = q$ and, by 3.4ii, $j = m$. Then $k \neq m, v_q = v_{q+1}$ and, by 3.8, $W = W' \equiv \Pi_{i=1}^{s} T_{j'(i),\alpha'(i)}$ and $j'(i) = j$ for at most one value of $i \leq q$. We are done by the induction hypothesis.

Case 2: $j(i_0) = m-1$ and, for some $s > i_0, j(s) > m-1$. By R2 we may assume that $j = j(q) > m-1 \geq r$. If $v_q = v_{q+1}$ or $|j-k| > 1$ or $|j-k| = 1$ and $r < j < n$ and $r < k < n$ or $k = n$ and $a_n \neq 1$, or $k = r$ and the r-coordinate of v_{q+1} is not zero, then by 3.8, $W = W' \equiv \Pi_{i=1}^{s} T_{j'(i),\alpha'(i)}$ and $j'(i) = j$ for at most one value of $i < q+1$. Then we are done by the induction hypothesis. We have $a_n \neq 1$ by 3.10. Let us consider the remaining cases .

$j = r+1, k = r$, and the r-coordinate of v_{q+1} equals 0 . Then $j = m, m-1 = r, c(v_q) = q = 2(n-r)$. Also v_{q+1} is not special, $r(v_{q+1}) = r+1, c(v_{q+1}) = q-1 = 2(n-r-1)+1$, which is impossible for a non-special vector by 3.2.

$j = n, k = n-1$. Consider the highest index $t < q$ such that $j(t) > m-1$. If $t < i_0$ we may assume that $j(i) < m-1$ for all $i > i_0$, by R2 , and we are done by Case 1. If $t > i_0$ and $j(t) < n-1$ we may assume, by R2, that $m-1 < j(q) < n$

and we are done by 3.8. Let us suppose that $j(t) = n-1$. We may assume by R2 that $t = q-1$. Then $a_{n-1} \neq 0$, because a_n is reducing, and a_{n-1} is reducing in v_{q-1}. Therefore a_{n-2} is passive. Since $v_q \neq v_{q+1}$ we have $a_n \neq 0$, hence a_{n-1} is reducing in v_q. So

$$v_q = \ldots + a_{n-3}\delta_{n-3} + a_{n-1}\delta_{n-1} + a_n\delta_n$$

with $a_{n-3} = a_{n-1} \neq 0$ and $a_n \neq 0$, $a_n \neq 1$. By 3.7ii we may switch j and k and assume $j = n-1, k = n$. Then, by 3.8, $W = W' \equiv \Pi_{i=1}^{s} T_{j'(i),\alpha'(i)}$ with $v'_{q-1} = (v_q)T_{n-1,\gamma}$ and $v'_q = (v'_{q-1})T_{n,\delta}$. Now $c(v'_{q-1}) \geq c(v'_q)$, by 3.2, and we are done by induction on q.

This concludes the proof of Proposition 3.1. ∎

4. Proof of Theorem 1

We fix an even number $n \geq 4$ and assume that ϕ_{n+1} restricted to $\mathbf{H}_{1,n-1}$ is a monomorphism.

4.1 LEMMA: *Let $\sigma_n(T_1) = \Gamma_{n-1}, \sigma_n(T_2) = T_n$. Let $\tau_n(T_1) = \Gamma_{n-3}, \tau_n(T_2) = T_{n-2}, \tau_n(T_3) = T_{n-1}, \tau_n(T_4) = T_n$. Then σ_n extends to a homomorphism $\sigma_n : \mathbf{G}_3 \to \mathbf{G}_{n+1}$, and τ_n extends to a homomorphism $\tau_n : \mathbf{G}_5 \to \mathbf{G}_{n+1}$. Also Γ_{n-1} commutes with T_k for $k = 1, 2, \ldots, n-1$, and*

$$(\Gamma_{n-1})^2 = (\Gamma_{n-3}T_{n-2}T_{n-1})^4 \in \mathbf{H}_{1,n-1}.$$

Proof: By 1.3 and 2.1 we have the following fact, which will be used repeatedly:

(P) Let $T_j, T_k, W, W_1 \in \mathbf{H}_{1,n-1}$ (respectively $T_j, T_k, W, W_1 \in \mathbf{H}_{2,n}$). Suppose that $v = (a\delta_j)W = (b\delta_k)W_1$. Then $(T_{j,a^2})^*W = (T_{k,b^2})^*W_1$ (since

$$\theta_v = \phi_{n+1}((T_{j,a^2})^*W) = \phi_{n+1}((T_{k,b^2})^*W_1)).$$

We first prove the lemma for $n = 4$. Let

$$U = T_4T_{3,-1}T_{4,-1/2}T_{3,2}T_{2,-1}T_{3,-2}T_{2,-1}T_{4,-1/2}T_{3,-1}T_4.$$

Then $(\delta_1)U = e_3, (\delta_2)U = \delta_4, (\delta_3)U = -\delta_3, (\delta_4)U = \delta_2$. By (P) we have $(T_2)^*U = T_4, (T_3)^*U = T_3, (T_4)^*U = T_2$. Also

$$(T_1)^*U = (T_1)^*T_{2,-1}T_{3,-2}T_{2,-1}T_{4,-1/2}T_{3,-1}T_4.$$

We shall prove that $(T_1)^*U = \Gamma_3$.

By (P), $(T_1)^*T_2T_{3,-1}T_{2,-1/2} = (T_1)^*T_{2,2}T_{3,-1/2}T_{2,-1}$ hence

$$\Gamma_3 = (T_1)^*T_{2,2}T_{3,-1/2}T_{2,-1}T_4T_{3,2}T_4.$$

Now, by conjugation, the equality $\Gamma_3 = (T_1)^*U$ is equivalent to

$$(T_1)^*T_{2,2}T_{3,-1/2}T_4 = (T_1)^*T_{2,-1}T_{3,-2}T_{2,-1}T_{4,-1/2}T_{3,-3}T_2.$$

We have

$$(T_1)^*T_{2,-1}T_{3,-2}T_{2,-1}T_{4,-1/2}T_{3,-3}T_2 =$$

(by R2)

$$(T_1)^*T_{2,-1}T_{3,-2}T_{4,-1/2}T_{2,-1}T_{3,-3}T_2 =$$

(by R1)

$$(T_1)^*T_{2,-1}T_{3,-2}T_{4,-1/2}T_3T_{2,-3}T_{3,-1} =$$

(by R1 and R2)

$$(T_2)^*T_{3,-2}T_{4,-1/2}T_3T_1T_{2,-3}T_{3,-1} =$$

(by (P))

$$(T_2)^*T_{3,-2}T_{4,-1/2}T_1T_{2,-3}T_{3,-1} =$$

(by R2)

$$(T_2)^*T_{3,-2}T_1T_{2,-3}T_{4,-1/2}T_{3,-1} =$$

(by(P)

$$(T_1)^*T_{2,2}T_3T_{4,-1/2}T_{3,-1} =$$

(by R1 and R2)

$$(T_1)^*T_{2,2}T_{3,-1/2}T_4$$

as required.

So σ_4 is a homomorphism and τ_4 is an identity.

Since T_1 commutes with T_3 and T_4, Γ_3 commutes with T_2 and T_3. Also $(\Gamma_3)^*T_1 = \Gamma_3$ by R1 and (P) so Γ_3 commutes with T_1.

$$(\Gamma_3)^2 = (T_1T_2T_3)^4 \qquad \text{by R6.}$$

Let now $n \geq 6$ and assume σ_{n-2} and τ_{n-2} are homomorphisms. Let

$U_0 =$

$$T_{n-2}T_{n-3,-1}T_{n-2,-1/2}T_{n-3,2}T_{n-4,-1}T_{n-3,-2}T_{n-4,-1}T_{n-2,-1/2}T_{n-3,-1}T_{n-2},$$

$$U_1 = (T_{n-1})^*T_{n-2}T_{n-3,-1}T_{n-2,-1/2}T_{n-4}T_{n-3,2}T_{n-4}.$$

Let $W_2 = T_{n-1}T_{n-2}T_{n-3,-1}T_{n-2,-1/2}T_{n-4}T_{n-3,2}$ and $U_2 = (T_n)^*W_2$. Let

$$W_3 = T_{n-1}T_{n-2}T_{n-3}T_{n-4,-1}T_{n-3,-1/2}T_{n-2,-1}T_{n-1,-1} \quad \text{and } U_3 = (T_n)^*W_3.$$

Let $U = U_0U_1U_2U_3$.

We claim that

$$(\Gamma_{n-5})^*U = \Gamma_{n-3}, (T_{n-4})^*U = T_{n-2}, (T_{n-3})^*U = T_{n-1}, (T_{n-2})^*U = T_n.$$

By direct computation one can check that

$$(\delta_{n-4})U = \delta_{n-2}, (\delta_{n-3})U = \delta_{n-1}, (\delta_{n-2})U = \delta_n,$$

so the last three claims follow from (P).

Also $(e_{n-5})U_0U_1 = e_{n-3}$ and, since $U_0U_1 \in \mathbf{H}_{1,n-1}$, we have, by (P), $(\Gamma_{n-5})U_0U_1 = \Gamma_{n-3}$. Furthermore $W_2, W_3 \in \mathbf{H}_{1,n-1}$ and

$$(e_{n-3})W_2^{-1} = e_{n-5} + (1/2)\delta_{n-3} = (e_{n-5})T_{n-4}T_{n-3,1/2}T_{n-4,-2}$$

so by (P), $(\Gamma_{n-3})^*W_2^{-1} = (\Gamma_{n-5})^*T_{n-4}T_{n-3,1/2}T_{n-4,-2}$ and $(\Gamma_{n-3})^*U_2 = \Gamma_{n-3}$ by R2.

$$(e_{n-3})W_3^{-1} = e_{n-5} - (1/2)\delta_{n-4} + \delta_{n-3} = (e_{n-5})T_{n-4,1/2}T_{n-3,2}$$

so by (P) $(\Gamma_{n-3})^*W_3^{-1} = (\Gamma_{n-5})^*T_{n-4,1/2}T_{n-3,2}$ and $(\Gamma_{n-3})^*U_3 = \Gamma_{n-3}$ by R2. Thus $(\Gamma_{n-5})^*U = \Gamma_{n-3}$ as required.

Now composition of τ_{n-2} with conjugation by U extends τ_n.

$$\Gamma_{n-3} = (\Gamma_{n-5})^*T_{n-4}T_{n-3,1/2}T_{n-4,-2}T_{n-2}T_{n-3,2}T_{n-2}.$$

Therefore

$$(\Gamma_{n-3})^*U = (\Gamma_{n-3})^*T_{n-2}T_{n-1,1/2}T_{n-2,-2}T_nT_{n-1,2}T_n = \Gamma_{n-1},$$

and composition of σ_{n-2} with conjugation by U extends σ_n.

Since $(\Gamma_{n-3})^2 = (\Gamma_{n-5}T_{n-4}T_{n-3})^4$, by induction hypothesis, we have

$$(\Gamma_{n-1})^2 = (\Gamma_{n-3}T_{n-2}T_{n-1})^4$$

by conjugation by U. Since Γ_{n-3} commutes with T_{n-4} and T_{n-3}, Γ_{n-1} commutes with T_{n-2} and T_{n-1}.

For $k < n-2$

$$(\Gamma_{n-1})^* T_k = (\text{by R2}) \quad (\Gamma_{n-3})^* T_{n-2} T_{n-1,1/2} T_{n-2,-2} T_k T_n T_{n-1,2} T_n$$

$$= (\text{by (P)}) \quad (\Gamma_{n-3})^* T_{n-2} T_{n-1,1/2} T_{n-2,-2} T_n T_{n-1,2} T_n = \Gamma_{n-1}.$$

This concludes the proof of Lemma 4.1. ∎

4.2 COROLLARY: *There exists a split epimorphism* $\rho_{n+2} : \mathbf{G}_{n+2} \to \mathbf{G}_{n+1}$ *such that* $\rho_{n+2}(T_{n+1}) = \Gamma_{n-1}$ *and* $\rho_{n+2}(T_k) = T_k$ *for* $k < n+1$.

Proof: By Lemma 4.1, ρ_{n+2} preserves relations R1–R6 .

We have to prove that ϕ_{n+1} is an isomorphism. It follows from 3.6 that for every vector $0 \neq v \in V_n$ there exists $W \in \mathbf{G}_{n+1}$ such that $(\delta_n)W = v$. Then $\theta_v = \phi_{n+1}((T_n)^* W)$. It is known that transvections θ_v generate Sp(n,p), so ϕ_{n+1} is onto. We shall prove that ϕ_{n+1} is a monomorphism.

Suppose $A \in \ker \phi_{n+1}$. $\mathbf{G}_{n+1}$ is generated by $T_1, T_2, \ldots, T_n$. Γ_{n-1} is a conjugate of T_1 by an element of $\mathbf{H}_{2,n}$ so $\mathbf{G}_{n+1}$ is also generated by $T_2, \ldots, T_n, \Gamma_{n-1}$. We can write A as a word in letters $T_2, \ldots, T_n, \Gamma_{n-1} : A = W(T_2, \ldots, T_n, \Gamma_{n-1})$. Let $A_1 = W(T_2, \ldots, T_n, T_{n+1}) \in \mathbf{G}_{n+2}$. Let $\rho_{n+2} : \mathbf{G}_{n+2} \to \mathbf{G}_{n+1}$ be the epimorphism defined in 4.2. Then $\rho_{n+2}(T_{n+1}) = \Gamma_{n-1}, \rho_{n+2}(A_1) = A$. ∎

4.3 LEMMA: $A = 1$.

Proof: Consider the commutative diagram of section 2 with n replaced by $n+2$.

$$\begin{array}{ccccccccc}
1 & \to & \ker \rho_{n+2} & \to & \mathbf{G}_{n+2} & \stackrel{\rho_{n-2}}{\to} & \mathbf{G}_{n+1} & \to & 1 \\
\phi_n | \ker \rho_{n+2} & & \downarrow & & \phi_{n+2} \downarrow & & \phi_{n+1} \downarrow & & \\
1 & \to & \ker \rho' & \to & \mathrm{Sp}^{\sim}(n+1,F) & \stackrel{\rho'}{\to} & \mathrm{Sp}^{\sim}(n,F) & \to & 1
\end{array}$$

We have $\phi_{n+1}\rho_{n+2} = \rho'\phi_{n+2}$. Thus $\phi_{n+2}(A_1) \in \ker \rho'$. Therefore $(\delta_{n+1})A_1 = \delta_{n+1} + a e_{n+1}$ and, since $A_1 \in \mathbf{H}_{2,n+1}$, the coefficient of δ_1 in $(\delta_{n+1})A_1$ equals zero. So $(\delta_{n+1})A_1 = \delta_{n+1}$. Let $D = T_1 T_2 \cdots T_{n+1} \in \mathbf{G}_{n+2}$. $(\delta_{n+1})D =$

$\delta_n, D^{-1}\mathbf{H}_{2,n+1}D = \mathbf{H}_{1,n}$. In particular $A_2 = (A_1)^*D \in \mathbf{H}_{1,n}$, and $(\delta_n)A_2 = \delta_n$. By Proposition 3.1, $A_2 \in \mathbf{H}$, hence $A_1 \in D\mathbf{H}D^{-1}$, which is generated by $T_2, T_3, \ldots, T_{n-1}, \quad DSD^{-1}, T_{n+1}$, where

$$S = (T_n)^*T_{n-1,-1}T_{n-2,-2}T_{n-1,-1}, \quad DSD^{-1} = (T_{n+1})^*T_{n,-1}T_{n-1,-2}T_{n,-1}.$$

Now $\rho_{n+2}(T_{n+1}) = \Gamma_{n-1} \in \mathbf{H}_{1,n-1}$, and

$$\begin{aligned}\rho_{n+2}(DSD^{-1}) &= (\Gamma_{n-1})^*T_{n,-1}T_{n-1,-2}T_{n,-1} \\ &= (\Gamma_{n-3})^*T_{n-2}T_{n-1,-1}T_{n-2,-1/2} \in \mathbf{H}_{1,n-1}.\end{aligned}$$

Therefore $\rho_{n+2}(A_1) = A \in \mathbf{H}_{1,n-1}$. But ϕ_{n+1} restricted to $\mathbf{H}_{1,n-1}$ is a monomorphism, hence $A = 1$.

This concludes the proof of Theorem 1. ∎

ACKNOWLEDGEMENT: In the present version of the paper the main idea of the proof of Theorem 1 as well as most of the ideas in sections 2 and 4 are taken from the unpublished paper of B. Moishezon [M] , in which a new proof of the result of Assion was given (the case $p = 3$). The author is greatly indebted to Professor Moishezon for his contribution to this paper .

References

[A] J. Assion, *Einige endliche Faktorgruppen der Zopfgruppen*, Math. Z. **163** (1978), 291–302.

[B] J. Birman, *Braids, Links and Mapping Class Groups*, Ann. Math. Studies **82** (1974).

[C] H. S. M. Coxeter, *Factor groups of the braid group*, Proc. 4th Can. Math. Congress, Toronto Univ. Press, 1959, pp. 95–122.

[M] B. Moishezon, *Finite quotients of braid groups related to symplectic groups over* **Z**/*3*, preprint.

[S] J. G. Sunday, *Presentations of the groups* SL(*2,m*) *and* PSL(*2,m*), Can. J. Math. **24** (1972), 1129–1131.

[W] B. Wajnryb, *Symplectic groups over a field with three elements*, preprint.