Pierce, R.S.
Osaka J. Math.
16 (1979), 317-348

SYMMETRIC GROUPOIDS. II

R.S. PIERCE*

(Received July 19, 1977)

Introduction

This paper is a sequel to the author's work [8]. It is concerned with the structure of symmetric groupoids (alias "symmetric sets," or "symmetric spaces"), and with the interplay between symmetric groupoids and groups that are generated by involutions (GI groups). As in [8], it is this close relationship between symmetric groupoids and GI groups that provides our *leitsatz*. Recent work on symmetric groupoids by other authors (for instance [2], [4], and [6]) has followed a similar path.

The notation and terminology of [8] will be used without explanation or apology in this paper. Our numbering here begins with Section 5; references to material in Sections 1 through 4 are to the relevant parts of [8]. Nevertheless, the dependence of this work on the earlier one is more apparent than real: the following four sections of this paper can be read with only occasional reference to Sections 1, 2, and 4 in [8].

5. Structure

A few fairly obvious statements can be made concerning the algebraic structure of symmetric groupoids. They will be made in this section.

Definition 5.1. Let A be a symmetric groupoid. A subset B of A is a subgroupoid of A if B is closed under the binary operation of A. If B satisfies

$$a\circ b\in B \quad \text{for all} \quad a\in A \quad \text{and} \quad b\in B,$$

then B is called a *normal subgroupoid* of A

Notation. We write $B<A$ if B is a subgroupoid of A, and $B\lhd A$ if B is a normal subgroupoid of A.

Lemma 5.2. *Let A be a symmetric groupoid, and suppose that $B\subseteq A$. Then B is a normal subgroupoid of A if and only if $\xi(b)\in B$ for all $b\in B$ and*

* Supported in part by NSF Grant MCS76-06632

$\xi \in \Lambda(A)$.

This lemma is a corollary of 1.13.1.

Corollary 5.3. *If A is a symmetric groupoid, and $a \in A$, then $\Lambda(A)a = \{\xi(a) : \xi \in \Lambda(A)\}$ is a normal subgroupoid of A.*

The normal subgroupoids of A that have the form $\Lambda(A)a$ will be called *principal*. Since $\Lambda(A)$ is a group, it is clear that if $b \in \Lambda(A)a$, then $\Lambda(A)b = \Lambda(A)a$. Thus, every symmetric groupoid is partitioned into a disjoint union of principal symmetric groupoids.

Lemma 5.4. *The set of all normal subgroupoids of a symmetric groupoid A is a complete atomic Boolean algebra under set operations. The atoms of this Boolean algebra are the principal normal subgroupoids of A.*

Corollary 5.5. *Every symmetric groupoid decomposes uniquely as a disjoint union of its principal normal subgroupoids.*

NOTATION and TERMINOLOGY. Let $\{A_i : i \in J\}$ be the set of distinct principal normal subgroupoids of A, so that $A = \bigcup_{i \in J} A_i$, where the sets that occur in this union are disjoint. This expression will be called the *principal decomposition* of A, and the subgroupoids A_i will be called the *principal components* of A. If $|J| = 1$, that is, $A = \Lambda(A)a$ for every $a \in A$, then A will be called a *principal* symmetric groupoid.

The following observation is a direct consequence of these observations.

Lemma 5.6. *Let G be a GI group, and suppose that $A < I(G)$ is such that $\langle A \rangle = G$. A subset B of A is a normal subgroupoid of A if and only if B is closed under conjugation by elements of G. In this case, the principal decomposition of B coincides with the expression of B as a union of conjugate classes in G. Moreover, $\langle B \rangle$ is a normal subgroup of G, and $G/\langle B \rangle = \langle \{a\langle B \rangle : a \in A - B\} \rangle$.*

Lemma 5.7. *Let $f : A \to B$ be a homomorphism of symmetric groupoids such that $f(\mathcal{Z}^n(A)) \subseteq \mathcal{Z}^n(B)$ for all $n < \omega$, that is, $f \in \mathcal{S}_\omega$. If A_i is a principal component of A, then there is a principal component B_j of B such that $f(A_i) \subseteq B_j$.*

Proof. If $A_i = \Lambda(A)a$, then by 1.15, $f(A_i) = \Lambda(f)(\Lambda(A))(f(a)) \subseteq \Lambda(B)(f(a))$.

Corollary 5.8. *If $f : A \to B$ is a surjective homomorphism of symmetric groupoids, then f maps the principal components of A onto the principal components of B.*

Proof. By 2.7 and 1.16, $f \in \mathcal{S}_\omega$ and $\Lambda(f)$ is surjective. Thus, $f(\Lambda(A)a) = \Lambda(B)f(a)$.

DEFINITION 5.9. Let A be a symmetric groupoid. A normal subgroupoid

B of A is called a *factor* of A if $b \circ a = a$ for all $a \in A - B$ and $b \in B$. If $A \neq \emptyset$, and the only factors of A are $\emptyset$ and A, then A is called *indecomposable.*

Lemma 5.10. *Let A be a symmetric groupoid.*

5.10.1 *If B is a factor of A, C is a factor of B, and $C \lhd A$, then C is a factor of A.*

5.10.2. *If $\{B_i : i \in J\}$ is a set of factors of A, then $\bigcup_{i \in J} B_i$ and $\bigcap_{i \in J} B_i$ are factors of A.*

Proof. Let $a \in A - C$, $b \in C \subseteq B$. Either $a \in A - B$, or $a \in B - C$. In both cases, $b \circ a = a$. Hence, C is a factor of A. The proof of 5.10.2 is similar.

In general, the complement of a factor needn't be a factor. An instance of this phenomenon is provided by the symmetric groupoid A of Example 4.13 and its factor $B = \{a, c\}$. However, for a fairly general class of symmetric groupoids, the set of factors is closed under complementation. We will call symmetric groupoid *balanced* if it satisfies the law

$$u \circ v = v \rightarrow v \circ u = u .$$

Every special symmetric groupoid is balanced, but by 4.21 there are balanced groupoids that are not special.

Lemma 5.11. *Let A be a balanced symmetric groupoid. A subset B of A is a factor of A if and only if $a \circ b = b$ for all $b \in B$ and $a \in A - B$.*

Proof. Since A is balanced, this condition is necessary in order that B be a factor. For the converse, it is enough to show that $c \circ b \in B$ for all $c \in B$, $b \in B$. If $c \circ b \in A - B$, then $c \circ (b \circ c) = (c \circ b) \circ c = c$. Hence, $b \circ c = c \circ (c \circ (b \circ c)) = c$. Since A is balanced and $c \circ b \neq b$, this is impossible.

Corollary 5.12. *If A is a balanced symmetric groupoid, then the set of all factors of A is a complete, atomic Boolean algebra under set operations. Thus, A is uniquely a disjoint union of indecomposable factors.*

Lemma 5.13. *Let B be a factor of the symmetric groupoid A. Then the inclusion mapping $h: B \rightarrow A$ induces an injective group homomorphism $\Lambda(h): \Lambda(B) \rightarrow \Lambda(A)$. The restriction map $f: \xi \rightarrow \xi \mid (A - B)$ is a surjective homomorphism of $\Lambda(A)$ to $\Lambda(A - B)$ such that Ker $f \supseteq \mathrm{Im}\, \Lambda(h)$.*

Proof. Let $(b_1, \cdots, b_n) \in \mathcal{Z}(B)$. Then $\lambda_{b_1} \cdots \lambda_{b_n}(c) = c$ for all $c \in B$, and, since B is a factor, for all $c \in A$ as well. Thus, $(b_1, \cdots, b_n) \in \mathcal{Z}(A)$. By 1.15, h induces a homomorphism $\Lambda(h)$: $\Lambda(B) \rightarrow \Lambda(A)$. Since h is injective, so is $\Lambda(h)$ by 1.15. To prove the second statement, let $\xi = \lambda_{a_1} \cdots \lambda_{a_n}$, where $a_{i_1}, \cdots, a_{i_m} \in A - B$, and the remaining a_i are elements of B. Since B is a factor, it follows that if $a \in A-B$, then $\xi(a)=\lambda_{a_{i_1}} \cdots \lambda_{a_{i_m}}(a)$. Hence, $\xi|(A-B) \in \Lambda(A-B)$, so that f is a surjective homomorphism of $\Lambda(A)$ to $\Lambda(A-B)$. If $\xi \in \mathrm{Im}\,\Lambda(h)$, then $\xi=\lambda_{a_1} \cdots \lambda_{a_m}$ with $a_i \in B$. Consequently, $\xi(a)=a$ for all $a \in A-B$. That is, $\xi \in \mathrm{Ker}\, f$.

Proposition 5.14. *Assume that the symmetric groupoid A is a disjoint union of factors: $A=\bigcup_{i\in J} B_i$. Then $\Lambda(A) \cong \sum_{i\in J} \Lambda(B_i)$.*

Proof. By 5.13, the inclusion maps $B_i \to A$ induce group homomorphisms $f_i: \Lambda(B_i) \to \Lambda(A)$. Also, the restriction maps $\xi \to \xi|B_i$ are homomorphisms g_i: $\Lambda(A) \to \Lambda(B_i) = \Lambda(A - \bigcup_{j\neq i} B_j)$, and $\mathrm{Im} f_i \subseteq \mathrm{Ker}\, g_j$ if $i \neq j$. If a and b are in B_i, then $(g_i f_i(\lambda_a))(b)=\lambda_a(b)$, so that $g_i f_i$ is the identity homomorphism of $\Lambda(B_i)$. Finally, $M(A) \subseteq \bigcup_{i\in J} \mathrm{Im} f_i$ implies $\Lambda(A)=\langle \bigcup_{i\in J} \mathrm{Im} f_i\rangle$. The proposition therefore follows from a standard characterization of direct sums of groups. (See [9], 4.2.1 for example.)

Corollary 5.15. *If A is a balanced symmetric groupoid, then $\Lambda(A) \cong \sum_{i\in J} \Lambda(B_i)$, where each B_i is an indecomposable symmetric groupoid.*

Corollary 5.16. *Let G be a GI group with trivial center. Suppose that A is a subgroupoid of $I(G)$ such that $\langle A\rangle = G$. If $B \lhd A$, then the following conditions are equivalent:*

5.16.1. *B is a factor of A;*

5.16.2. *B centralizes $A-B$ (as subsets of G);*

5.16.3. *$G=\langle B\rangle \times \langle A-B\rangle$.*

This corollary follows from 1.11 and 5.14. Unfortunately, it is not true in general that if A is an indecomposable symmetric groupoid, then $\Lambda(A)$ is an indecomposable group.

The concept of a normal subgroupoid of a symmetric groupoid can be generalized.

DEFINITION 5.17. Let B be a subgroupoid of symmetric groupoid A. A subset C of A will be called a *B-submodule* of A if it satisfies: $b \in B$ and $c \in C$ implies $b \circ c \in C$.

Lemma 5.18. *Let B be a subgroupoid of the symmetric groupoid A. Denote $\Lambda_A(B)=\langle\{\lambda_b : b \in B\}\rangle$. A subset C of A is a B-submodule of A if and only if $\xi(c) \in C$ for all $\xi \in \Lambda_A(B)$ and $c \in C$. For each $a \in A$, the set $\Lambda_A(B)a = \{\xi(a) : \xi \in \Lambda_A(B)\}$ is B-submodule of A, and $\{\Lambda_A(B)a : a \in A\}$ is a partition of A that refines the principal decomposition of A.*

This lemma follows routinely from 5.17. The special case $B=\{b\}$ is worth examining in more detail. Plainly, $\Lambda_A(\{b\})=\{1_A, \lambda_b\}$ and $\Lambda_A(\{b\})a=\{a, b\circ a\}$.

We will use the following notation and terminology. Denote $O_b(a)=\{a, b\circ a\}$, and call this set the *b-orit* of *a*. If $|O_b(a)|=2$, then this orbit is said to be *non-trivial*; if $|O_b(a)|=1$, then $O_b(a)$ is called *trivial*. We will denote the set of all non-trivial *b*-orbits in A by $\mathcal{O}_b(A)$.

Lemma 5.19. *Let A be a symmetric groupoid conatining the elements a, b, and c.*

5.19.1. *$O_b(b)$ is trivial.*

5.19.2. *$O_b(a)=O_b(b\circ a)$.*

5.19.3. *If $\xi\in\Lambda(A)$, then $O_{\xi(b)}(\xi(a))=\xi(O_b(a))$. In particular, $O_{c\circ b}(c\circ a)=\lambda_c(O_b(a))=c\circ O_b(a)$.*

5.19.4. *If $\mathcal{O}_b(A)=\mathcal{O}_c(A)$, then $\lambda_b=\lambda_c$.*

5.19.5. *If A is balanced, then $O_b(a)$ is non-trivial if and only if $O_a(b)$ is non-trivial.*

Proof. The properties 5.19.1, 5.19.2, and 5.19.3 are consequences of the three axioms that define symmetric groupoids, and the fact that $\Lambda(A)\subseteq \operatorname{Aut} A$. If $\mathcal{O}_b(A)=\mathcal{O}_c(A)$, then $O_b(a)=O_c(a)$ for all $a\in A$. Hence, $b\circ a=c\circ a$ for all $a\in A$, that is, $\lambda_b=\lambda_c$. By definition, A is balanced if and only if $|O_b(a)|=|O_a(b)|$ for all a and b.

Corollary 5.20. *If b and c belong to the same principal component of the symmetric groupoid A, then the cardinal number of non-trivial b-orbits in A is the same as the cardinal number of non-trivial c-orbits in A, that is $|\mathcal{O}_b(A)|=|\mathcal{O}_c(A)|$.*

Proof. If $c=\xi(b)$, $\xi\in\Lambda(A)$, then by 5.19.3, ξ maps $\mathcal{O}_b(A)$ bijectively to $\mathcal{O}_c(A)$.

DEFINITION 5.21. Let A be a symmetric groupoid. For $b\in A$, define the *degree of A at b* to be the cardinal number

$$d_A(b) = |\bigcup \mathcal{O}_b(A)| = 2|\mathcal{O}_b(A)|.$$

If b and c belong to the same principal component of A, then $d_A(b)=d_A(c)$ by 5.20. In particular, if A is principal, then the degree function is a constant, which we will call the *degree of A*, and denote d_A.

EXAMPLE 5.22. Let S_n be the symmetric group on $n\geq 3$ letters. Denote the conjugate class of transpositions in S_n by J_n. Then J_n is a principal symmetric groupoid, $\langle J_n\rangle=S_n$, and $Z(J_n)$ is the identity congruence. If $b=(1,2)$, then the non-trivial b-orbits are $\{(1,3),(2,3)\}$, $\{(1,4),(2,4)\}$, $\cdots$, and $\{(1,n),(2,n)\}$. Thus, the degree of J_n is $2(n-2)$.

EXAMPLE 5.23. Let H be an abelian group. Denote by D_H the generalized dihedral group over H, that is, the relative holomorph $\operatorname{Hol}(H, -1_H)$. Thus, H

is a subgroup of index 2 in D_H: $D_H = H \cup aH$, where $a^2=1$, and $axa=x^{-1}$ for all $x \in H$. Then $K_H = I(D_H) - I(H) = aH$ plainly generates D_H. The principal decomposition of K_H is easily seen to be $K_H = \bigcup axH^2$, where x ranges over a set of representatives of the cosets of H^2 in H. Since $(ax)(ay)(ax) = a(x^2y^{-1})$, the orbit $O_{ax}(ay)$ is trivial if and only if $x^2=y^2$, that is, $yx^{-1} \in I(H)$. Thus, the degree of K_H at ax is $|H - I(H)|$. In particular, if H is a finite group of odd order n, then K_H is principal of degree $n-1$. Also, in this case $Z(K_H)$ is the identity congruence on K_H, since D_H is easily seen to have trivial center.

In case the group H in 5.23 is cyclic of order n, the group D_H is the ordinary dihedral group of order $2n$. As usual, this group will be denoted by D_n. The corresponding symmetric groupoid K_H will be designated by K_n.

6. Graphic methods

To each symmetric groupoid we can assign a directed graph. This device makes it possible to cast many questions about the structure of symmetric groupoids in geometrical form. In many cases, this graphical approach provides new insight into the structural problems.

DEFINITION 6.1. Let A be a symmetric groupoid. The graph of A is

$$\mathcal{S}(A) = (A, \mathcal{E}(A)),$$

where $\mathcal{E}(A) = \{(a, b) : a \circ b \neq b\}$ is the set of edges of $\mathcal{S}(A)$.

Since $a \circ a = a$, it is clear that $\mathcal{S}(A)$ is a directed graph without loops. If A is balanced, then $(a, b) \in \mathcal{E}(A)$ implies $(b, a) \in \mathcal{E}(A)$. In this case, $\mathcal{S}(A)$ will be interpreted as an undirected graph $\cdots$ the edges (a,b) and (b, a) will be identified.

Proposition 6.2. *If A is a symmetric groupoid, then $\Lambda(A)$ acts as a group of automorphisms of $\mathcal{S}(A)$. This group action is transitive on vertices if and only A is principal.*

Proof. Since $\Lambda(A)$ is a subgroup of Aut A, it is obvious from Definition 6.1 that the elements of $\Lambda(A)$ permute the edges of $\mathcal{S}(A)$. By definition, A is principal if and only if $\Lambda(A)$ is transitive on A.

If A is a balanced symmetric groupoid, then it is obvious that the degree of A at an element b coincides with the local degree (or valence) of the graph $\mathcal{S}(A)$ at b (see [7], p. 7).

The following observation is essentially a geometric formulation of 5.11.

Lemma 6.3. *Let A be a balanced symmetric groupoid. Then the decomposition of A into a disjoint union of indecomposable factors coincides with the decomposition of the vertex set of $\mathcal{S}(A)$ into connected components.*

Corollary 6.4. *Let A be a balanced symmetric groupoid. Assume that A is principal, and that the degree d_A of A is finite. Let B be a non-empty subset of A such that for all $b\in B$, the number of $c\in B$ such that $(b, c)\in\mathcal{E}(A)$ is d_A. Then $B=A$.*

EXAMPLE 6.5. Let H be an abelian group of odd order. By 5.23, $\mathcal{S}(K_H)$ is the complete graph on $|H|$ vertices. Moreover, by 1.11 and 5.23, $D_H\cong\Lambda(K_H)$. Thus, if H_1 and H_2 are non-isomorphic abelian groups of the same odd order, then $\mathcal{S}(K_{H_1})\cong\mathcal{S}(K_{H_2})$ and $K_{H_1}\ncong K_{H_2}$.

In general, the graph of a symmetric groupoid A will be the complete graph on its vertex set if and only if $a\circ b\neq b$ for all $a\neq b$, that is, A is an F-space in the terminology of Doro [2]. As Doro shows in [2], F-spaces are cryptomorphic with finite B-loops (in the sense of Glauberman [3]).

By enriching the structure of $\mathcal{S}(A)$, it is possible to recover A. This possibility results from a well known, elementary observation concerning universal algebras.

Lemma 6.6. *Let V be a variety of universal algebras such that for some natural number n, all operations of the algebras in V have arity at most n. Let F denote the free V-algebra on n generators. Suppose that A and B are algebras of V, and f is a mapping from A to B. Then f is a homomorphism if and only if for every homomorphism $g\colon F\to A$, the map $fg\colon F\to B$ is a homomorphism.*

Proof. It suffices to show that if 0 is an *m-ary* operation of the algebras in V, and if $(a_1, \cdots, a_m)\in A^m$, then $f(0(a_1, \cdots, a_m))=0(f(a_1), \cdots, f(a_m))$. Let F be freely generated by $u_1, \cdots, u_n$, where $n\geq m$ by assumption. Then there is a homomorphism g: $F\to A$ such that $g(u_i)=a_i$ for $1\leq i\leq m$. By hypothesis, fg is a homomorphism. Therefore, $f(0(a_1, \cdots, a_m))=f(0(g(u_1), \cdots, g(u_m)))= fg(0(u_1, \cdots, u_m))=0(fg(u_1), \cdots, fg(u_m))=0(f(a_1)), \cdots, f(a_m))$.

The usefulness of this observation for symmetric groupoids rests on the simple form of the free symmetric groupoid on two generators. The following result can be derived from 4.12, but we will give a straightforward direct proof.

Proposition 6.7. *For $m, n\in \boldsymbol{Z}$, define $m\circ n=2m-n$. Then $(\boldsymbol{Z}, \circ)$ is a symmetric groupoid that is freely generated by each pair of elements $\{k, k+1\}$, $k\in\boldsymbol{Z}$. The automorphism group of $(\boldsymbol{Z}, \circ)$ is generated by the mappings $\lambda_0\colon n\to -n$, and $\alpha\colon n\to n-1$.*

Proof. Plainly, $(\boldsymbol{Z}, \circ)$ is a symmetric groupoid, and if $k\in\boldsymbol{Z}$, then $(k+1)\circ k=k+2$, $k\circ(k+1)=k-1$, $(k+1)\circ k\circ(k+1)=k+3$, $k\circ(k+1)\circ k=k-2$, and so on. Therefore, $\boldsymbol{Z}$ is generated as a groupoid by $\{k, k+1\}$. To prove that $\{k, k+1\}$ is a free generating set, let A be a symmetric groupoid, and $a, b\in A$. Define $g(k)=b$, $g(k+1)=a$, and inductively $g(k+n+1)=g(k+n)\circ g(k+n-1)$,

$g(k-n)=g(k-n+1)\circ g(k-n+2)$ for $n\geq 1$. Then g: $\boldsymbol{Z}\rightarrow A$ is a well defined mapping that satisfies $g(n+2)=g(n+1)\circ g(n)$ and $g(n)=g(n+1)\circ g(n+2)$ for all $n\in\boldsymbol{Z}$. Using this observation, it follows by induction on $m-n$ that $g(m)\circ g(n)=g(2m-n)=g(m\circ n)$ for all $m\geq n$. If $m<n$, then $m>2m-n$, so that $g(m)\circ g(2m-n)=g(n)$. Thus, $g(m)\circ g(n)=g(m\circ n)$ in this case also. Plainly, λ_0 and α are automorphisms of $(\boldsymbol{Z}, \circ)$. Let $h\in\mathrm{Aut}(\boldsymbol{Z}, \circ)$. If $h(0)=0$, then for $n\geq 1$, $h(n)=h(1\circ 0\circ 1\circ\cdots)=h(1)\circ h(0)\circ h(1)\circ\cdots=h(1)\circ 0\circ h(1)\circ\cdots=nh(1)$, and $h(-n)=h(0\circ n)=0\circ h(n)=-nh(1)$. Since h maps $\boldsymbol{Z}$ bijectively to itself, it follows that either $h=1_{\boldsymbol{Z}}$, or $h=\lambda_0$. In general, if $h(0)=r\in\boldsymbol{Z}$, then $(\alpha^r h)(0)=0$, so that either $h=\alpha^{-r}$, or $h=\alpha^{-r}\lambda_0=\lambda_0\alpha^r$.

Henceforth, when $\boldsymbol{Z}$ is considered as a symmetric groupoid, we will assume tacitly that $m\circ n=2m-n$.

By 6.7, $\mathrm{Aut}(\boldsymbol{Z})\cong D_{\boldsymbol{Z}}$, the infinite dihedral group. It is easy to see that $\Lambda(\boldsymbol{Z})$ is a subgroup of index 2 in $\mathrm{Aut}(\boldsymbol{Z})$, and that $\Lambda(\boldsymbol{Z})\cong D_{\boldsymbol{Z}}$ also.

DEFINITION 6.8. Let A be a symmetric groupoid. A *cycle in* A is a groupoid homomorphism of $\boldsymbol{Z}$ to A. If A is balanced, a *cycle in* $\mathcal{S}(A)$ is a homomorphism γ from $\boldsymbol{Z}$ to A such that $\mathcal{E}(\gamma)=\{(\gamma(n), \gamma(n+1)): n\in\boldsymbol{Z}\}\subseteq\mathcal{E}(A)$. In this case, $\mathcal{E}(\gamma)$ is called the edge set of γ. Cycles γ and δ in A are called *equivalent* if $\delta=\gamma h$ for some $h\in\mathrm{Aut}(\boldsymbol{Z})$.

Cycles in symmetric groupoids were introduced by Nobusawa in [5]. Our definition is equivalent to his. The notion of a cycle in the graph of a balanced symmetric groupoid is more geometrical, and of course more restrictive.

Proposition 6.9. *Let A be a balanced symmetric groupoid, $(a, b)\in\mathcal{E}(A)$, and $k\in\boldsymbol{Z}$. Then there is a unique cycle γ in $\mathcal{S}(A)$ such that $\gamma(k)=b$ and $\gamma(k+1)=a$.*

Proof. By 6.7, there is a unique cycle γ in A such that $\gamma(k)=b$ and $\gamma(k+1)=a$. Assume that there is some smallest $n\geq k$ such that $\gamma(n+1)=\gamma(n-1)$. Then $n\geq k+2$, since A is balanced and $(a, b)\in\mathcal{E}(A)$. Since $\gamma(n-1)=\gamma(n+1)=\gamma(n)\circ\gamma(n-1)$, the assumption that A is balanced yields $\gamma(n)=\gamma(n-1)\circ\gamma(n)=\gamma(n-1)\circ(\gamma(n-1)\circ\gamma(n-2))=\gamma(n-2)$, contrary to the minimality of n. Thus, $\gamma(n+1)\neq\gamma(n-1)$ for all $n\geq k$. Similarly, $\gamma(n+1)\neq\gamma(n-1)$ for $n<k$, so that γ is a cycle in $\mathcal{S}(A)$.

Theorem 6.10. *Let $f: A\rightarrow B$ be a bijective mapping between balanced symmetric groupoids. Then f is an isomorphism of groupoids if and only if f is a graph isomorphism of $\mathcal{S}(A)$ to $\mathcal{S}(B)$, and $\gamma\rightarrow f\gamma$ maps cycles in $\mathcal{S}(A)$ to cycles in $\mathcal{S}(B)$.*

Proof. If γ is a cycle in A, then either (1) $\gamma(k)=\gamma(k+1)$ for some $k\in\boldsymbol{Z}$, (2) $\gamma(k)\neq\gamma(k+1)$ and $(\gamma(k), \gamma(k+1))\notin\mathcal{E}(A)$ for some $k\in\boldsymbol{Z}$, or (3) γ is a cycle in $\mathcal{S}(A)$. In case 1, $\gamma(n)=\gamma(k)$ for all $n\in\boldsymbol{Z}$, and $f\gamma$ is plainly a cycle in B. In case 2, $\gamma(n)=\gamma(k)$ if $n\equiv k\ (\mathrm{mod}\ 2)$, and $\gamma(n)=\gamma(k+1)$ if $n\equiv k+1\ (\mathrm{mod}\ 2)$.

Then $f\gamma$ is a cycle in B for all such cycles γ in A if and only if f maps $\mathcal{E}(A)$ bijectively to $\mathcal{E}(B)$. Thus, 6.10 follows from 6.6.

Corollary 6.11. *If A is a balanced symmetric groupoid, γ is a cycle in $\mathcal{S}(A)$, and $\xi\in\Lambda(A)$, then $\xi\gamma$ is a cycle in $\mathcal{S}(A)$. Moreover, if $\xi(\gamma(k))=\gamma(k)$ and $\xi(\gamma(k+1))=\gamma(k+1)$ for some $k\in\boldsymbol{Z}$, then $\xi\gamma=\gamma$.*

Lemma 6.12. *Let A be a balanced symmetric groupoid, and suppose that γ and δ are cycles in $\mathcal{S}(A)$. If $\mathcal{E}(\gamma)\cap\mathcal{E}(\delta)\neq\emptyset$, then δ is equivalent to γ. Conversely, if δ is equivalent to γ, then $\mathcal{E}(\delta)=\mathcal{E}(\gamma)$. Thus, edge sets of cycles partition $\mathcal{E}(A)$.*

Proof. If $(\gamma(n), \gamma(n+1))=(\delta(m), \delta(m+1))$, then either $\gamma(n)=\delta(m)$, $\gamma(n+1)=\delta(m+1)$, and $\delta=\gamma\alpha^{m-n}$, or $\gamma(n)=\delta(m+1)$, $\gamma(n+1)=\delta(m)$, and $\delta=\gamma\lambda_0\alpha^{m+1+n}$, by 6.11. The converse is clear.

According to Definition 6.8, the structure of a cycle in a symmetric groupoid is determined by a congruence relation on the symmetric groupoid $(\boldsymbol{Z}, \circ)$. We will now characterize these congruences.

Lemma 6.13. *Let Γ be an equivalence relation on $\boldsymbol{Z}$. Then Γ is a congruence relation of the symmetric groupoid $(\boldsymbol{Z}, \circ)$ if and only if*

6.13.1. *$(m, n)\in\Gamma$ and $k\in\boldsymbol{Z}$ implies $(2k-m, 2k-n)\in\Gamma$ and $(m-2k, n-2k)\in\Gamma$.*

When 6.13.1 is satisfied, the factor groupoid $\boldsymbol{Z}/\Gamma$ is balanced if and only if

6.13.2. *$(m, n)\in\Gamma$, $m\equiv n$ (mod 2) implies $((1/2)(n+m), (1/2)(3n-m))\in\Gamma$.*

Proof. An equivalence relation Γ on a groupoid is a congruence relation if and only if it is stable under right and left multiplication, that is, $(m, n)\in\Gamma$ implies $(k\circ m, k\circ n)\in\Gamma$ and $(m\circ k, n\circ k)\in\Gamma$ for all $k\in\boldsymbol{Z}$. Therefore, 6.13.1 is necessary and sufficient for Γ to be a congruence relation. Note that $(k\circ n, n)\in\Gamma$ means $(2k-n, n)\in\Gamma$. Denote $m=2k-n$, so that $m\equiv n\ (\mathrm{mod}\ 2)$ and $k=(1/2)(n+m)$. Then $(m, n)\in\Gamma$ if and only if $(k\circ n, n)\in\Gamma$, and $((1/2)(3n-m), (1/2)(n+m))\in\Gamma$ if and only if $(n\circ k, k)\in\Gamma$. The equivalence 6.13.2 is an immediate consequence of these observations.

It is possible to give an explicit description of the congruence relations on $(\boldsymbol{Z}, \circ)$. For this purpose, we will use the notation

$$\begin{aligned}\Gamma_r &= \{(m, n)\colon m\equiv n\ (\mathrm{mod}\ r)\}\,,\\ \Gamma_r^e &= \{(m, n)\colon m\equiv n\ (\mathrm{mod}\ r)\,,\quad m\equiv n\equiv 0\ (\mathrm{mod}\ 2)\}\,,\\ \Gamma_r^0 &= \{(m, n)\colon m\equiv n\ (\mathrm{mod}\ r)\,,\quad m\equiv n\equiv 1\ (\mathrm{mod}\ 2)\}\,,\end{aligned}$$

where r is a non-negative integer. Also note that $\Gamma_0=\{(m, m)\colon m\in\boldsymbol{Z}\}$ is the identity congruence on $\boldsymbol{Z}$.

Proposition 6.14. *The congruence relations on* $(\boldsymbol{Z}, \circ)$ *are the sets*

$$\Gamma_r, \quad \textit{where} \quad 0 \leq r \in \boldsymbol{Z},$$

$$\Gamma_{2r} \cup \Gamma_r^e \quad \textit{and} \quad \Gamma_{2r} \cup \Gamma_r^0, \quad \textit{where} \quad 2 \leq r \in 2\boldsymbol{Z}.$$

Proof. Evidently, Γ_r, $\Gamma_{2r} \cup \Gamma_r^e$, and $\Gamma_{2r} \cup \Gamma_r^0$ satisfy 6.13.1 Suppose that Γ is a congruence relation on $(\boldsymbol{Z}, \circ)$.

(1) If $(k, k+r) \in \Gamma$, then $\Gamma_{2r} \subseteq \Gamma$. In fact, $(k, k+r) \in \Gamma$ implies $(n, 2r+n) \in \Gamma$ for all $n \in \boldsymbol{Z}$ by 6.13.1. It follows by induction on $|(m-n)/2r|$ that if $m \equiv n$ (mod 2r), then $(m, n) \in \Gamma$.

(2) If $(k, k+r) \in \Gamma$, where $r \geq 1$ is odd, then $\Gamma_r \subseteq \Gamma$. Indeed, by 6.13.1, either $(0, r) \in \Gamma$ or $(1, r+1) \in \Gamma$. Since $r = 2t+1$ for some $t \in \boldsymbol{Z}$, it follows that $(0, r) = (0, 2t+1) \in \Gamma$ if and only if $(-2t-2, -1) \in \Gamma$, which is equivalent to $(r+1, 1) = (2t+2, 1) \in \Gamma$. Consequently, if $(k, k+r) \in \Gamma$ with r odd, then $(n, n+r) \in \Gamma$ for all $n \in \boldsymbol{Z}$, that is, $\Gamma_r \subseteq \Gamma$. Assume that $\Gamma \neq \Gamma_0$. Then there is a smallest integer $r \geq 1$ such that $(k, k+r) \in \Gamma$ for some $k \in \boldsymbol{Z}$. By 6.13.1, either $(0, r) \in \Gamma$ or $(1, r+1) \in \Gamma$. Suppose that $(0, r) \in \Gamma$.

(3) $\Gamma_{2r} \cup \Gamma_r^e \subseteq \Gamma$. In fact, $\Gamma_{2r} \subseteq \Gamma$ by (1), and $\Gamma_r \subseteq \Gamma$ if r is odd. If r is even, then it follows from 6.13.1 and the assumption $(0, r) \in \Gamma$ that $(m, m+nr) \in \Gamma$ for all even integers m and arbitrary $n \in \boldsymbol{Z}$. That is, $\Gamma_r^e \subseteq \Gamma$.

(4) If $m \in \boldsymbol{Z}$ and $0 < s \in \boldsymbol{Z}$ satisfy $(m, m+s) \in \Gamma$, then r divides s. To prove this assertion, write $2s = qr + t$ with $q \in \boldsymbol{Z}$, $0 \leq t < r$. Since $\Gamma_{2r} \subseteq \Gamma$ and $\Gamma_{2s} \subseteq \Gamma$ by (1), it follows easily that $(2m, 2m+t) \in \Gamma$, so that $t = 0$ by the minimality of r. Thus, $2s = qr$. If q is even, then r divides s, as claimed. Suppose that $q = 2u+1$, $u \in \boldsymbol{Z}$, and r is even. Then $2s+1 = 2ur + r + 1$, so that $(1, r+1) \in \Gamma$, since $\Gamma_{2r} \subseteq \Gamma$ and $\Gamma_{2s} \subseteq \Gamma$. Since also $(0, r) \in \Gamma$, it follows that $\Gamma_r \subseteq \Gamma$. The equality $s = ur + (r/2)$ then yields $(m+s, m+(r/2)) \in \Gamma$, which implies that $(m, m+(r/2)) \in \Gamma$, because $(m, m+s) \in \Gamma$. Since this inclusion contradicts the minimality of r, (4) is proved.

(5) If $(m, m+s) \in \Gamma - (\Gamma_{2r} \cup \Gamma_r^e)$, then $\Gamma_r \subseteq \Gamma$. In fact, by (2) there is nothing to prove if r is odd. Assume therefore that r and s are even. Then m is odd, since $(m, m+s) \notin \Gamma_r^e$; and $s = (2v+1)r$ for some $v \in \boldsymbol{Z}$, because $(m, m+s) \notin \Gamma_{2r}$. By 6.13.1, $(1, 2vr+r+1) = (1, s+1) \in \Gamma$, so that $(1, r+1) \in \Gamma$, because $\Gamma_{2r} \subseteq \Gamma$. As before, it follows that $\Gamma_r \subseteq \Gamma$. Combining (3), (4), and (5) gives the conclusion that either $\Gamma = \Gamma_{2r} \cup \Gamma_r^e$ or $\Gamma = \Gamma_r$. Finally, suppose that $(0, r) \notin \Gamma$. Then $(1, r+1) \in \Gamma$, so that the congruence $\Delta = \{(m-1, n-1)\colon m, n \in \Gamma\}$ satisfies $(0, r) \in \Delta$. Thus, Δ is either $\Gamma_{2r} \cup \Gamma_r^e$ or Γ_r. Consequently, Γ is either $\Gamma_{2r} \cup \Gamma_r^0$ or Γ_r.

Lemma 6.15. *If* Γ *is a congruence relation on the symmetric groupoid* $(\boldsymbol{Z}, \circ)$, *then* $\boldsymbol{Z}/\Gamma$ *is balanced if and only if* Γ *has one of the forms* $\Gamma_r (0 \leq r \in \boldsymbol{Z})$, *or* $\Gamma_{2r} \cup \Gamma_r^e$ *or* $\Gamma_{2r} \cup \Gamma_r^0$ $(4 \leq r \in 4\boldsymbol{Z})$.

Proof. If $\Gamma=\Gamma_{2r}\cup\Gamma_r^e$, with r even and $\boldsymbol{Z}/\Gamma$ balanced, then $r\equiv 0 \pmod 4$. In fact, by 6.13.2, $(0, r)\in\Gamma$ implies $((1/2)r, (3/2)r)\in\Gamma$, so that $r/2$ must be even. Similarly, if $\Gamma=\Gamma_{2r}\cup\Gamma_r^0$ satisfies 6.13.2, then also $r\equiv 0 \pmod 4$. Conversely, it is a routine matter to check that if $r\equiv 0 \pmod 4$, then $\Gamma_{2r}\cup\Gamma_r^e$ and $\Gamma_{2r}\cup\Gamma_r^0$ satisfy 6.13.2. Obviously, Γ_r satisfies 6.13.2 for all non-negative integers r.

Corollary 6.16. *Let γ be a cycle in the graph of the balanced symmetric groupoid A. Considered as a homomorphism of $(\boldsymbol{Z}, \circ)$ to A, the kernel of γ is one of the following congruence relations*: Γ_r $(0\leq r\in\boldsymbol{Z}, r\neq 1, 2)$ *or* $\Gamma_{2r}\cup\Gamma_r^e$ *or* $\Gamma_{2r}\cup\Gamma_r^0$ $(4\leq r\in 4\boldsymbol{Z})$.

Lemma 6.17 *If Γ is a congruence relation on the symmetric groupoid $(\boldsymbol{Z}, \circ)$, then $\boldsymbol{Z}/\Gamma$ is special if and only if $\Gamma=\Gamma_r$ with $0\leq r\in\boldsymbol{Z}$.*

Proof. If $\boldsymbol{Z}/\Gamma$ is special, then there is a cycle γ in some $I(G)$ such that $\operatorname{Ker}\gamma=\Gamma$. If $\gamma(1)=a$ and $\gamma(0)=b$, then $\gamma(r)=\gamma(0)$ if and only if $(ab)^r=1$, and $\gamma(r+1)=\gamma(1)$ if and only if $(ab)^r a=a$. Thus, $\gamma(r)=\gamma(0)$ is equivalent to $\gamma(r+1)=\gamma(1)$. Consequently, Γ cannot be $\Gamma_{2r}\cup\Gamma_r^e$ or $\Gamma_{2r}\cup\Gamma_r^0$. On the other hand, $\boldsymbol{Z}/\Gamma_r$ is isomorphic to a subgroupoid of $I(D_r)$, where D_r is the dihedral group of order $2r$.

Corollary 6.18. *Let A be a special symmetric groupoid. If γ is a cycle in $\mathcal{S}(A)$, then either*

6.18.1 $\gamma(m)\neq\gamma(n)$ *if* $m\neq n$ *in* $\boldsymbol{Z}$, *or*

6.18.2. *there exists* $r\geq 3$ *such that* $\gamma(m)=\gamma(n)$ *if and only if* $m\equiv n (\mathrm{mod}\ r)$.

If γ is a cycle in the graph of a balanced symmetric groupoid, define the *order* or γ to be $|\mathcal{E}(\gamma)|$, and denote this cardinal number by $|\gamma|$. If the symmetric groupoid whose graph contains γ is special, then by 6.18, $|\gamma|=|\{\gamma(n)\colon n\in\boldsymbol{Z}\}|$. In this case, if $|\gamma|=r$ is finite, then $\gamma(m)=\gamma(n)$ if and only if $m\equiv n \pmod r$.

Lemma 6.19. *Let A be a special symmetric groupoid. Let γ be a cycle in $\mathcal{S}(A)$, such that $d_A(\gamma(0))=d$ is finite. Then $|\gamma|\leq d+2$.*

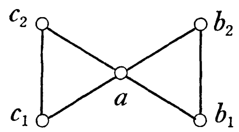
Proof. Let $|\gamma|=r$. By 6.18.2, $\gamma(m)=\gamma(n)$ if and only if $m\equiv n \pmod r$. In particular, if $b=\gamma(0)$, then $b\circ\gamma(n)=\gamma(-n)\neq\gamma(n)$ for $1\leq n<r/2$. Therefore, $\{\gamma(n), \gamma(-n)\}$, $1\leq n<r/2$, are distinct, non-trivial b-orbits in A. Thus, $d\geq r-2$.

Proposition 6.20. *Let A be a principal symmetric groupoid such that $Z(A)=I_A$. Assume that A has finite degree d. Then every cycle in $\mathcal{S}(A)$ has order $\leq d+1$. If there is a cycle of order $d+1$ in A, then $A=K_{d+1}$ (see 5.23). If $d\equiv 0 \pmod 4$, then there is no cycle of order d in $\mathcal{S}(A)$.*

Proof. The hypothesis $Z(A)=I_A$ implies that A is special by 1.9. If γ is a cycle in $\mathcal{S}(A)$, then $|\gamma|\leq d+2$ by 6.19. Assume that $|\gamma|=d+2$. Denote $b=\gamma(0)$, $c=\gamma((d/2)+1)$. Then $\mathcal{O}_b(A)=\{\{\gamma(n), \gamma(-n)\}: 1\leq n\leq d/2\}=\mathcal{O}_c(A)$, as in the proof of 6.19. By 5.19.4, $\lambda_b=\lambda_c$. Therefore, $(b, c)\in Z(A)$. This contradicts the hypothesis that $Z(A)=I_A$, because $b\neq c$ by 6.18. Therefore, every cycle in $\mathcal{S}(A)$ has order at most $d+1$. If there is a cycle γ of order $d+1$, then by 6.4, 6.8, and 6.17, $A=\{\gamma(n): n\in \boldsymbol{Z}\}\cong \boldsymbol{Z}/\Gamma_{d+1}\cong K_{d+1}$. Finally, assume that $d\equiv 0 \pmod 4$, and there is a cycle δ of order d in $\mathcal{S}(A)$. Denote $b=\delta(0)$, $c=\delta(d/2)$, $e=\delta(d/4)$, $f=\delta(-d/4)$. For $1\leq k<d/2$, $O_k=\{\delta(d/4-k), \delta(d/4+k)\}$ is a non-trivial e- and f-orbit. Therefore, $\mathcal{O}_e(A)=\{O_1, O_2, \cdots, O_{d/2-1}, \{a_1, a_2\}\}$, and $\mathcal{O}_f(A)=\{O_1, O_2, \cdots, O_{d/2-1}, \{b_1, b_2\}\}$ for suitable a_1, a_2, b_1, b_2 in $A-\{\delta(n): n\in \boldsymbol{Z}\}$. Since $Z(A)=I_A$ and $e\neq f$, it follows from 5.19.4 that $\{a_1, a_2\}\neq\{b_1, b_2\}$. As above, $b\circ\delta(n)=\delta(-n)=c\circ\delta(n)$, so that $\{\delta(n), \delta(-n)\}$ is a non-trivial b- and c-orbit. In particular, $\lambda_b(e)=f=\lambda_c(e)$ and $\lambda_b(0_k)=0_{d/2-k}=\lambda_c(0_k)$. Thus, $\lambda_b(\{a_1, a_2\})=\{b_1, b_2\}=\lambda_c\{(a_1, a_2\})$ by 5.19.3. If a_1, a_2, b_1, and b_2 were distinct, then there would be $d+1$ non-trivial b-orbits. Thus, it can be assumed that $\lambda_b(a_1)=a_1=b_1$ and $\lambda_b(a_2)=b_2\neq a_2$. It follows that $\lambda_c(a_2)=b_2$, which contradicts the hypothesis $Z(A)=I_A$, since it implies that $\lambda_b=\lambda_c$ by 5.19.4.

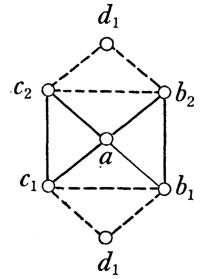
Corollary 6.21. *Let A be a principal symmetric groupoid such that $Z(A)=I_A$.*
6.21.1. *If $d_A=2$, then $A\cong K_3$.*
6.21.2. *If $d_A=4$, then $A\cong K_5$ or $A\cong J_4$.*

Proof. Assume that $d_A=2$. By 6.9, there is a cycle γ in $\mathcal{S}(A)$. By 6.20, $|\gamma|=3$, and $A\cong K_3$. Assume that $d_A=4$. By 6.20, the possible orders of cycles in $\mathcal{S}(A)$ are 3 and 5; moreover, if $\mathcal{S}(A)$ contains a cycle of order 5, then $A\cong K_5$. Therefore, assume that every cycle in $\mathcal{S}(A)$ has order 3. It follows that every element of A is in the image of exactly two inequivalent cycles. Let $a\in A$. The two cycles that pass through a form a subgraph of $\mathcal{S}(A)$ whose diagram is



Let γ be the cycle that passes through b_1 and is disjoint from ab_1b_2, say $b_1=\gamma(2)$. Since all cycles in $\mathcal{S}(A)$ have order 3, it follows that $\gamma(n)\neq b_2$ for all $n\in \boldsymbol{Z}$. Thus, $\lambda_a\gamma\neq\gamma$, since $\lambda_a(b_1)=b_2$. This observation implies that either $\lambda_a(\gamma(0))\neq\gamma(0)$ or $\lambda_a(\gamma(1))\neq\gamma(1)$ by 6.11. Hence, one of $\gamma(0)$ or $\gamma(1)$ is c_1 or c_2. Without loss of generality, assume that $(b_1, c_1)\in\mathcal{E}(\gamma)$. Let d_1 be the remaining element in the image of γ. Then d_1 is distinct from a, b_1, c_1, and c_2. Consequently, $\lambda_a(d_1)=d_1$, and $\mathcal{E}(\lambda_a\gamma)=\{(b_2, c_2), (c_2, d_1), (d_1, b_2)\}$. By 6.4, $A=$

$\{a, b_1, b_2, c_1, c_2, d_1\}$, and the diagram of $\mathcal{S}(A)$ with its four cycles is



The cycles in this graph are (a, b_1, b_2), (a, c_1, c_2), (b_1, c_1, d_1), and (b_2, c_2, d_1). Comparing $\mathcal{S}(A)$ and its cycle structure with the graph and cycle structure of $\mathcal{S}(J_4)$, we conclude by 6.10 that the mapping $a \to (1, 2)$, $b_1 \to (1, 3)$, $b_3 \to (2, 3)$, $c_1 \to (1, 4)$, $c_2 \to (2, 4)$, $d \to (3, 4)$ is a groupoid isomorphism of A to J_4.

The cycles in the graph of a balanced symmetric groupoid can be used to present the groupoid. A *presentation* of a symmetric groupoid is defined in the same way as the presentations of groups, rings, and so on. In detail, a presentation of a symmetric groupoid A is a surjective homomorphism p of the free symmetric groupoid A_α on the set $\{u_\xi: \xi < \alpha\}$ of involutions (indexed by a cardinal number α) to A, together with a set $R \subseteq A_\alpha^2$ such that $\operatorname{Ker} p$ is the smallest congruence relation on A_α that contains R. It is customary to designate such a presentation of A by writing

$$A = \langle a_\xi,\ \xi < \alpha:\ v_k(a) = w_k(a),\ k \in K \rangle\,,$$

where $a_\xi = p(u_\xi)$, and if $R = \{(v_k, w_k): k \in K\}$, then $v_k(a)$ and $w_k(a)$ are the polynomial expressions that are obtained from the reduced representations of v_k and w_k respectively by substituting a_ξ for u_ξ, $\xi < \alpha$, in v_k and w_k.

Proposition 6.22. *Let A be be a balanced symmetric groupoid. Let $D = \{a \in A: a \circ b = b$ for all $b \in A\}$. Suppose that $\{\gamma_k: k \in K\}$ is a set of representatives of the distinct equivalence classes of cycles in $\mathcal{S}(A)$. Let $\{a_\xi: \xi < \alpha\}$ be a well ordering (without repetition) of the set $D \cup \{\gamma_k(0), \gamma_k(1): k \in K\}$, where α is a cardinal number. Denote by A_α the symmetric groupoid that is freely generated by the set $\{u_\xi: \xi < \alpha\}$ of involutions. Let $p: A_\alpha \to A$ be the homomorphism such that $p(u_\xi) = a_\xi$ for all $\xi < \alpha$. For $k \in K$, define δ_k to be the cycle in $\mathcal{S}(A_\alpha)$ that satisfies $\delta_k(0) = u_\xi$ if $\gamma_k(0) = a_\xi$ and $\delta_k(1) = u_\eta$ if $\gamma_k(1) = a_\eta$. Define R to be the subset of A_α^2 that consists of all pairs of the following kinds:*

6.22.1. *$(u_\xi \circ u_\eta, u_\eta)$, where $a_\eta \in D$;*

6.22.2. *$(u_\xi \circ \delta_k(m), \delta_k(m))$, where $a_\xi \circ \gamma_k(m) = \gamma_k(m)$;*

6.22.3. *$(\delta_k(m), \delta_l(n))$, where $\gamma_k(m) = \gamma_l(n)$.*

Then (p, R) is a presentation of A.

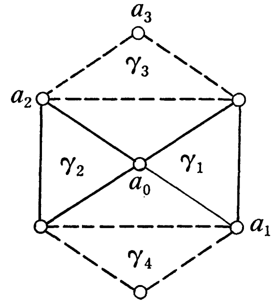
Proof. By 6.7 and the definition of δ_k, it follows that $p(\delta_k(m)) = \gamma_k(m)$ for all $k \in K$ and $m \in \boldsymbol{Z}$. Also, by 6.7, every element of A is either in D or of the form $\gamma_k(m)$. Thus, p is surjective. It is obvious that $R \subseteq \operatorname{Ker} p$. To complete the proof, we must show that $\operatorname{Ker} p$ is contained in the smallest congruence relation Γ on A that contains R. The heart of the proof is the implication:

(*) $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, \delta_k(m)) \in \operatorname{Ker} p$ implies
$(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, \delta_k(m)) \in \Gamma$.

This will be established by induction on r. If $r=1$, then $a_{\xi_1} = \gamma_k(m) \notin D$. Thus, $a_{\xi_1} = \gamma_l(n)$ for some $l \in K$ and $n=0$ or 1. Then $(u_{\xi_1}, \delta_k(m)) \in R \subseteq \Gamma$ by 6.22.3. Assume that (*) is valid for $r-1$, where $r>1$. Then the hypothesis $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, \delta_k(m)) \in \operatorname{Ker} p$ means that $a_{\xi_1}\circ\cdots\circ a_{\xi_r} = \gamma_k(m)$. Let $b = a_{\xi_2}\circ\cdots\circ a_{\xi_r}$. Then $a_{\xi_1}\circ b = \gamma_k(m)$. If $b = \gamma_k(m)$, then $a_{\xi_1}\circ\gamma_k(m) = \gamma_k(m)$. It follows from 6.22.2 and the induction hypothesis that $(u_{\xi_1}\circ\delta_k(m), \delta_k(m)) \in R \subseteq \Gamma$ and $(u_{\xi_2}\circ\cdots\circ u_{\xi_r}, \delta_k(m)) \in \Gamma$. Consequently, $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, \delta_k(m)) \in \Gamma$, because Γ is a congruence relation. Assume that $b \neq \gamma_k(m)$. Then there exists $l \in K$ and $n \in \boldsymbol{Z}$ such that $a_{\xi_1} = \gamma_l(n)$, $b = \gamma_l(n-1)$, and $\gamma_k(m) = \gamma_l(n+1)$. By the case $r=1$, the induction hypothesis, and 6.22.3, it follows that $(u_{\xi_1}, \delta_l(n)) \in \Gamma$, $(u_{\xi_2}\circ\cdots\circ u_{\xi_r}, \delta_l(n-1)) \in \Gamma$, and $(\delta_k(m), \delta_l(n+1)) \in \Gamma$. Consequently $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, \delta_l(n+1)) = (u_{\xi_1}\circ\cdots\circ u_{\xi_r}, \delta_l(n)\circ\delta_l(n-1)) \in \Gamma$, and therefore $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, \delta_k(m)) \in \Gamma$. This completes the inductive proof of (*). To complete the proof of 6.22, it suffices to show that if $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, u_\eta) \in \operatorname{Ker} p$, then $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, u_\eta) \in \Gamma$. If $a_\eta \notin D$, this implication is a special case of (*). Assume that $a_\eta \in D$. Again we induce on r. If $r=1$, then $a_{\xi_1} = a_\eta$, so that $\xi_1 = \eta$, and $u_{\xi_1} = u_\eta$. Assume that $r>1$. Then $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, u_\eta) \in \operatorname{Ker} p$ implies $a_{\xi_1}\circ\cdots\circ a_{\xi_r} = a_\eta$. Hence, $a_{\xi_2}\circ\cdots\circ a_{\xi_r} = a_{\xi_1}\circ a_\eta = a_\eta$, since $a_\eta \in D$ and A is balanced. By the induction hypothesis and 6.22.1, $(u_{\xi_2}\circ\cdots\circ u_{\xi_r}, u_\eta) \in \Gamma$ and $(u_{\xi_1}\circ u_\eta, u_\eta) \in R \subseteq \Gamma$. Thus, $(u_{\xi_1}\circ\cdots\circ u_{\xi_r}, u_\eta) \in \Gamma$.

In general, the presentation described in 6.22 is highly redundant. However, it provides a foundation on which to build a more efficient presentation. We illustrate this possibility by a simple example.

EXAMPLE 6.23. The symmetric groupoid J_4 has four equivalence classes of cycles. Select representatives of these cycles as shown in the next diagram: $\gamma_1(0)=a_0$, $\gamma_1(1)=a_1$; $\gamma_2(0)=a_0$, $\gamma_2(1)=a_2$; $\gamma_3(0)=a_3$, $\gamma_3(1)=a_2$; $\gamma_4(0)=a_3$, $\gamma_4(1)=a_1$.



The construction 6.22 yields the presentation (omitting trivial relations, such as $a_1=a_1$):

$$\begin{aligned} J_4 = \langle a_0, a_1, a_2, a_3\colon\ & a_0\circ a_3 = a_3,\ a_1\circ a_2 = a_2,\ a_1\circ a_0\circ a_1 = a_0\,, \\ & a_2\circ a_0\circ a_2 = a_0,\ a_2\circ a_3\circ a_2 = a_3,\ a_1\circ a_3\circ a_1 = a_3\,, \\ & a_1\circ a_0 = a_2\circ a_3,\ a_1\circ a_3 = a_2\circ a_0\rangle\,. \end{aligned}$$

Using the fact that $a_1\circ a_2=a_2$, the last two of these relations are equivalent to $a_0=a_1\circ a_2\circ a_3$. Thus, a_0 can be omitted from the list of generators of J_4. Moreover, if a_0 is defined to be $a_1\circ a_2\circ a_3$, then it is easily seen that the relations $a_0\circ a_3=a_3$, $a_1\circ a_0\circ a_1=a_0$, and $a_2\circ a_0\circ a_2=a_0$ are consequences of the remaining relations listed above. Consequently, J_4 has the simple presentation

$$J_4 = \langle a_1, a_2, a_3\colon\ a_1\circ a_2 = a_2,\ a_1\circ a_3 = a_3\circ a_1,\ a_2\circ a_3 = a_3\circ a_2\rangle\,.$$

7. Generation by involutions

Throughout this section, G is a group, and A is a subgroupoid of $I(G)$ such that $\langle A\rangle=G$. We will study in some detail how the elements of G can be represented as products of the involutions in A. One of our objectives is to relate $|A|$ and $|G|$. If A is infinite, then $|A|=|G|$, so that this problem is interesting only when A is finite.

NOTATION 7.1.

7.1.1. If A is any set, let $S(A)$ denote the set of all finite sequences of elements of A, including the empty sequence $\emptyset$.

7.1.2. Let $\sigma=(a_0, \cdots, a_{r-1})$ and $\tau=(b_0, \cdots, b_{s-1})$ be elements of $S(A)$. Denote $\sigma\tau=(a_0, \cdots, a_{r-1}, b_0, \cdots, b_{s-1})$ and $\sigma^{-1}=(a_{r-1}, \cdots, a_0)$.

7.1.3. Let $\sigma=(a_0, \cdots, a_{r-1})\in S(A)$. Denote $\{\sigma\}=\{a_0, \cdots, a_{r-1}\}$, $|\sigma|=|\{\sigma\}|$, $||\sigma||=r$.

7.1.4. Assume that $A\subseteq M$, where M is a monoid (that is, an associative groupoid with an identity element 1). For $\sigma=(a_0, a_1, \cdots, a_{r-1})\in S(A)$, define $\Pi\sigma=a_0a_1\cdots a_{r-1}\in M$, and $\Pi\emptyset=1$.

Lemma 7.2. *Under the binary operation $(\sigma, \tau)\to\sigma\tau$, and with $\emptyset$ as the identity element, the set $S(A)$ is a monoid with A as a set of free generators. If $A\subseteq M$, where M is a monoid, then $\Pi\colon S(A)\to M$ is a homomorphism of monoids.*

These facts are well known and easily proved.

Assume that G is a group, and A is a subgroupoid of $I(G)$ such that $\langle A\rangle=G$. It then follows that the product mapping Π of 7.1.4 is surjective. Let Γ be the kernel of this homomorphism, that is, Γ is the congruence relation on the monoid $S(A)$ that is defined by

$$\Gamma = \{(\sigma, \tau): \Pi\sigma = \Pi\tau\} .$$

One of the main objectives of this section is to determine canonical representatives of the equivalence classes modulo Γ.

Lemma 7.3. *The congruence relation* Γ *includes all pairs of the forms*:
7.3.1. $(\rho\sigma\tau, \rho\sigma'\tau)$, $\sigma=(a, b, a)$, $\sigma'=(a\circ b)$;
7.3.2. $(\rho\pi\tau, \rho\tau)$, $\pi=(a, a)$;

where ρ *and* τ *are arbitrary elements of* $S(A)$.

This lemma is clear from our hypotheses and notation.

The pairs 7.3.1 and 7.3.2 are described without referring to the product operation in the ambient group G; only the groupoid operation of A enters the definition. For any symmetric groupoid A, let Γ_0 be the equivalence relation on $S(A)$ that is generated by all pairs of the forms 7.3.1 and 7.3.2. Write $\sigma\sim\tau$ if $(\sigma, \tau)\in\Gamma_0$. In particular, if (σ, τ) or (τ, σ) is of the form 7.3.1 or 7.3.2, or if $\sigma=\tau$, then $\sigma\sim\tau$ will be called a *primitive equivalence*. By definition, $\sigma\sim\tau$ if and only if there is a sequence of primitive equivalences $\sigma_0\sim\sigma_1$, $\sigma_1\sim\sigma_2$, $\cdots$, $\sigma_{r-1}\sim\sigma_r$ such that $\sigma=\sigma_0$ and $\tau=\sigma_r$.

Lemma 7.4. *The equivalence relation* Γ_0 *is a congruence relation on* $S(A)$. *Moreover,* $S(A)/\Gamma_0$ *is a group. If* p: $S(A)\to S(A)/\Gamma_0$ *is the natural projection, then* $p|A$ *is a groupoid homomorphism of* A *to* $I(S(A)/\Gamma_0)$ *such that* $\langle p(A)\rangle=S(A)/\Gamma_0$.

Proof. If $\sigma_1\sim\sigma_2$ is a primitive equivalence, and $\rho, \tau\in S(A)$, then $\rho\sigma_1\tau\sim\rho\sigma_2\tau$ is a primitive equivalence. It follows that Γ_0 is a congruence relation. The last assertion of the lemma is clear, and it implies that $S(A)/\Gamma_0$ is a group.

It follows from the definition of Γ_0 that the group $S(A)/\Gamma_0$ is identical with the group E_A that was introduced in 4.14, and that with this identification, $p|A$ corresponds to the homomorphism f_A.

Lemma 7.5. *Let* $a_0, a_1, \cdots, a_{r-1}$ *be elements of the symmetric groupoid* A, *where* $r\geq 2$. *Then*

$$\begin{aligned}&(a_0, \cdots, a_{i-1}, a_i, a_{i+1}, \cdots, a_{i+j-1}, a_{i+j}, a_{i+j+1}, \cdots, a_{r-1})\sim\\&(a_0, \cdots, a_{i-1}, a_i\circ a_{i+1}, \cdots, a_i\circ a_{i+j}, a_i, a_{i+j+1}, \cdots, a_{r-1})\sim\\&(a_0, \cdots, a_{i-1}, a_{i+j}, a_{i+j}\circ a_i, \cdots, a_{i+j}\circ a_{i+j-1}, a_{i+j+1}, \cdots, a_{r-1}) .\end{aligned}$$

Proof. If $r=2$, then there is a sequence of primitive equivalences $(a_0\circ a_1, a_0)\sim(a_0, a_1, a_0, a_0)\sim(a_0, a_1)\sim(a_1, a_1, a_0, a_1)\sim(a_1, a_1\circ a_0)$. The general case follows from the case $r=2$, using induction and the fact that Γ_0 is a congruence relation.

Henceforth in this section, assume that G is a group, and that A is a subgroupoid of $I(G)-\{1\}$ such that $\langle A\rangle=G$. Both of the congruence relations

Γ and Γ_0 are defined on $S(A)$. By 7.3, $\Gamma_0 \subseteq \Gamma$. In other words,

$$\sigma \sim \tau \quad \text{implies} \quad \Pi\sigma = \Pi\tau .$$

This fact will be used often in the rest of this section.

DEFINITION 7.6. Let $x \in G$. The *A-length* of x (or just the length of x when this abbreviation will not cause confusion) is defined to be

$$l(x) = \min \{||\sigma||: \sigma \in S(A),\ \Pi\sigma = x\} .$$

A sequence $\sigma \in S(A)$ is *reduced* if $l(\Pi\sigma) = ||\sigma||$.

Lemma 7.7. *Let $x, y \in G$.*
7.7.1. *$l(x)=0$ if and only if $x=1$.*
7.7.2. *$l(x)=1$ if and only if $x \in A$.*
7.7.3. *$l(xy) \leq l(x)+l(y)$.*
7.7.4. *$l(x^{-1})=l(x)$.*
7.7.5. *$l(yxy^{-1})=l(x)$.*

Corollary 7.8. *If $\sigma, \tau \in S(A)$ are such that $\sigma\tau$ is reduced, then σ and τ are reduced.*

Proof. By 7.7.3, $||\sigma\tau|| = l(\Pi\sigma\tau) \leq l(\Pi\sigma) + l(\Pi\tau) \leq ||\sigma||| + |\tau|| = ||\sigma\tau||$.

Corollary 7.9. *Every subsequence of a reduced sequence in $S(A)$ is reduced.*

Proof. Let $\sigma = (a_0, \cdots, a_{r-1}) \in S(A)$ be reduced, and suppose that $0 \leq i_0 < i_1 < \cdots < i_{t-1} \leq r-1$. By repeated use of 7.5 we obtain $\sigma \sim \tau = (a_{i_0}, \cdots, a_{i_{t-1}}, b_1, \cdots, b_{r-t})$ with $b_j \in A$. By 7.3, $\Pi\tau = \Pi\sigma$, so that τ is reduced. Thus $(a_{i_0}, \cdots, a_{i_{t-1}})$ is reduced by 7.8.

DEFINITION 7.10. If $x \in G$, and $a \in A$, then a *divides* x if there exist $y, z \in G$ such that $x = yaz$ and $l(x) = l(y) + l(z) + 1$.

NOTATION. Write $a|x$ if a divides x, and $a \not| x$ if a does not divide x.

Lemma 7.11. *If $x \in G$ and $a \in A$, then $a|x$ if and only if $x = aw$ for some $w \in G$ such that $l(w) = l(x) - 1$.*

Proof. Assume that $x = yaz$, where $l(x) = l(y) + l(z) + 1$. Let $y = \Pi\sigma$, $z = \Pi\tau$ with $l(y) = ||\sigma||$, $l(z) = ||\tau||$. By 7.5, $\sigma a \tau \sim a\rho\tau$, where $||\rho|| = ||\sigma||$. Thus, $x = aw$, where $w = \Pi\rho\tau$ has length $l(x) - 1$.

Lemma 7.12. *Let $x \in G$, and $a \in A$.*
7.12.1. *$l(x) - 1 \leq l(ax) \leq l(x) + 1$.*
7.12.2. *$l(ax) = l(x) - 1$ if and only if $a|x$.*

These assertions follow respectively from 7.7.3 and 7.11.
In general, it is not true that if $a \not| x$, then $l(ax)=l(x)+1$.

Lemma 7.13. *The following conditions on the pair* (G, A) *are equivalent.*
7.13.1. *If* $a \in A$ *and* $x \in G$ *satisfy* $a \not| x$, *then* $l(ax)=l(x)+1$.
7.13.2. *If* $\sigma \in S(A)$, *then* $l(\Pi\sigma) \equiv ||\sigma||$ (*mod* 2).

Proof. Assume that 7.13.2 fails. Let σ be a counterexample to 7.13.2 for which $||\sigma||$ is minimal, say $\sigma=(a_0, a_1, \cdots, a_{r-1})$. Since $1 \notin A$, $r \geq 2$. Denote $x=\Pi\sigma$. By assumption, $l(x) \equiv r-1 \pmod 2$. The minimality of r implies $a_1 \cdots a_{r-1}=a_0 x$ has length that is congruent to $r-1 \pmod 2$. By 7.12, $l(a_0 x)=l(x)$ and $a_0 \not| x$, so that 7.13.1 fails. Conversely, if 7.13.1 is not satisfied, then by 7.12 there exists $a \in A$ and $x \in G$ such that $l(ax)=l(x)$. Let $x=\Pi\tau$, where $||\tau||=l(x)$. Then $\sigma=(a, \tau)$ furnishes a contradiction to 7.13.2.

In the next section, it will be shown that the pairs (G, A) satisfying the equivalent conditions 7.13.1 and 7.13.2 occur rather frequently.

NOTATION 7.14. Assume that a well ordering $\leq$ of A is given. As usual, write $a \geq b$ interchangeably with $b \leq a$; and write $a>b$ or $b<a$ if $b \leq a$ and $b \neq a$. For $x \in G-\{1\}$, denote

$$\mu(x) = \min \{a \in A\colon a \text{ divides } x\}.$$

Lemma 7.15. *For* $x \in G-\{1\}$ *and* $a \in A$, *the following statements are equivalent*:
7.15.1. $\mu(x)=a$;
7.15.2. $a \mid x$ *and* $b \not| x$ *for all* $b<a$;
7.15.3. $l(ax)=l(x)-1$ *and* $l(bx) \geq l(x)$ *for all* $b<a$.
In particular, $\mu(x)=x$ *if and only if* $x \in A$.

Proof. The equivalence of 7.15.1, 7.15.2, and 7.15.3 follows easily from the definition of $\mu(x)$ and 7.12. The last statement is a consequence of 7.7.2 and 7.7.1.

DEFINITION 7.16. Let $x \in G$. The *standard sequence* corresponding to x is the element $\sigma_x \in S(A)$ that is defined by $\sigma_1=\emptyset$ and $\sigma_x=(a_0, a_1, \cdots, a_{r-1})$, where $x \neq 1$, $r=l(x)$, $a_0=\mu(x)$, $a_1=\mu(a_0 x)$, $a_2=\mu(a_1 a_0 x)$, $\cdots$, $a_{r-1}=\mu(a_{r-2} \cdots a_0 x)$.

Proposition 7.17. *Let* $x \in G$, *and suppose that* $\sigma_x=(a_0, a_1, \cdots, a_{r-1})$. *Then*
7.17.1. $\Pi\sigma_x=x$,
7.17.2. $a_0<a_1<\cdots<a_{r-1}$,
7.17.3. σ_x *is reduced,*
7.17.4. $\mu(a_k a_{k+1} \cdots a_{r-1})=a_k$ *for all* $k<r$.

Proof. If $r=0$, then $x=1$, $\sigma_x=\phi$, and all statements of the proposition are vacuously true. Proceeding inductively with $r \geq 1$, note that the standard sequence of a_0x is $(a_1, \cdots, a_{r-1})$ by 7.15.3. Thus, $a_0x = a_1 \cdots a_{r-1}$, and $x = a_0a_1 \cdots a_{r-1} = \Pi\sigma_x$. Consequently, $a_1 | x$, so that by 7.15.2, $a_0 \leq a_1$. Plainly, $a_0 \neq a_1$. Moreover, $l(\Pi\sigma_x) = l(x) = r = ||\sigma_x||$, that is, σ_x is reduced. Finally, $\mu(a_ka_{k+1} \cdots a_{r-1}) = a_k$ for $k \geq 1$ by the induction hypothesis and the fact that $\sigma_{a_0x} = (a_1, \cdots, a_{r-1})$; and $\mu(a_0a_1 \cdots a_{r-1}) = \mu(x) = a_0$ by the definition of σ_x.

Lemma 7.18. *Let $\sigma = (a_0, a_1, \cdots, a_{r-1}) \in S(A)$ satisfy $\mu(a_ka_{k+1} \cdots a_{r-1}) = a_k$ for all $k < r$. Then $\sigma = \sigma_x$, where $x = \Pi\sigma$.*

Proof. This is clear from the definition of σ_x, when it is noted that the hypothesis implies $l(x) = r$.

DEFINITION 7.19. A *standard sequence* in A is an element $\sigma = (a_0, a_1, \cdots, a_{r-1})$ in $S(A)$ such that

$$\mu(a_ka_{k+1} \cdots a_{r-1}) = a_k$$

for all $k < r$.

By 7.17.4 and 7.18, the standard sequences in A are exactly the sequences σ_x for a unique $x \in G$. Thus, our objective of providing canonical representatives of the Γ-classes is attained.

Theorem 7.20. *The mapping $\sigma \to \Pi\sigma$ is a bijective map from the set of standard sequences in A to the the group G. Thus, the standard sequences in A form a set of representatives of the Γ-classes in $S(A)$.*

The rest of this section is concerned with applications of 7.20. Our first observation is an obvious, but interesting consequence of 7.20.

Corollary 7.21. $|G| = |\{\sigma \in S(A): \sigma$ *is standard*$\}|$. *In particular, if A is finite, then $|G| \leq 2^{|A|}$.*

The equality $|G| = 2^{|A|}$ is attained if G is an elementary abelian 2-group, and A is a basis of G. If G is not commutative, then this estimate can be improved. However, before pursuing this development, we present a different generalization of 7.21.

Lemma 7.22. *Let H be a subgroup of G such that $|A - H| = m$ is finite. Then $[G: H] \leq 2^m$.*

Proof. Let $A - H = \{b_1, b_2, \cdots, b_m\}$. We can assume that the well ordering $\leq$ of A that was introduced in 7.14 satisfies $b_1 < b_2 < \cdots < b_m < c$ for all $c \in A \cap H$. Then by 7.17.2, every standard sequence $\sigma \in S(A)$ has the form $\sigma = \tau_1\tau_2$, where $\tau_1 \in S(A - H)$ and $\tau_2 \in S(A \cap H)$. Consequently, $\Pi\sigma = \Pi\tau_1\Pi\tau_2$, and $\Pi\tau_2 \in H$. By 7.20, the elements $\Pi\tau_1$ form a set of representatives of the cosets of H in G. Thus, $[G: H] \leq 2^m$.

Proposition 7.23. *Let G be a group, and suppose that $A < I(G) - \{1\}$ is such that $\langle A \rangle = G$. Assume that $A = A_1 \cup A_2 \cup \cdots \cup A_s$ is the principal decomposition of A, that is, A is the union of exactly s conjugate classes in G. Choose $a_i \in A_i$, and assume that the degree $d_i = d_A(a_i)$ of A at a_i is finite. Then A and G are finite, and $|A| \leq s \cdot 2^n$, where $n = \sum_{i=1}^s d_i$.*

Proof. Let $B_i = A - C_G(a_i) = \{b \in A: a_i \circ b \neq b\}$. Thus, $|B_i| = d_i$. Denote $B = \bigcup_{i=1}^s B_i = A - H$, where $H = \bigcap_{i=1}^s C_G(a_i)$ is a subgroup of G. Then $|B| \leq n$, so that by 7.22, $[G: H] \leq 2^n$. Therefore, $|A_i| = [G: C_G(a_i)] \leq [G: H] \leq 2^n$, and $|A| = \sum_{i=1}^s |A_i| \leq s \cdot 2^n$. By 7.21, G is also finite.

Corollary 7.24. *Let A be a principal, special symmetric groupoid whose degree $d_A = d$ is finite. Then $|A| \leq 2^d$. In particular, there are only a finite number of isomorphism classes of principal, special symmetric groupoids of a given degree d.*

Lemma 7.25. *Assume that the pair (G, A) satisfies the conditions in* 7.13 *Then every subsequence of a standard sequence in A is standard.*

Proof. It is sufficient to prove that if $\sigma = (a_0, \cdots, a_{r-1}, b, c_0, \cdots, c_{s-1})$ is standard, then $\tau = (a_0, \cdots, a_{r-1}, c_0, \cdots, c_{s-1})$ is standard. If $r = 0$, this conclusion is obvious. Assume that $r \geq 1$, and proceed by induction on r. By 7.17.3 and 7.9, $l(\Pi\tau) = r + s$. If $d < a_0$, then $d \not| \Pi\sigma$ by 7.15.2. Therefore, by 7.13.1, $l(d\Pi\sigma) = r + s + 2$, so that $l(d\Pi\tau) = r + s + 1$ according to 7.9. This argument shows that $\mu(\Pi\tau) = a_0$ by 7.15. The induction is therefore complete.

In the remainder of this section, it will be assumed that (G, A) satisfies the conditions in 7.13. Consequenctly, every subsequence of a standard sequence in A is standard. It is also convenient to adopt the hypothesis that A is finite, say $|A| = m$. Our results are valid in the infinite case, but they are uninteresting if A is infinite.

Lemma 7.26. *Let $W = \{\tau_1, \tau_2, \cdots, \tau_n\}$ be a set of non-standard sequences in $S(A)$. Then*

7.26.1. $|G| \leq \sum_{V \subseteq W} (-1)^{|V|} 2^{m - |\cup V|}$,

where $\bigcup V = \{\tau_{i_1}\} \cup \cdots \cup \{\tau_{i_r}\} \subseteq A$ (in the notation of 7.1.3) *if $V = \{\tau_{i_1}, \cdots, \tau_{i_r}\} \subseteq W$.*

Proof. By 7.21, 7.25, and 7.17.2, $|G| \leq |U|$, where $U = \{\sigma \in S(A): \sigma$ is strictly increasing, $\{\tau_i\} \nsubseteq \{\sigma\}$, $1 \leq i \leq n\}$. Let P denote the set of all subsets of A, and for $1 \leq i_1 < i_2 < \cdots \ldots < i_r \leq n$, denote $P(i_1, i_2, \cdots, i_r) = \{S \in P: \{\tau_{i_1}\} \subseteq S, \{\tau_{i_2}\} \subseteq S, \cdots, \{\tau_{i_r}\} \subseteq S\}$. The inclusion-exclusion pinciple yields

(*) $|U| = |P| - \sum_{i_1} |P(i_1)| + \sum_{i_1 < i_2} |P(i_1, i_2)| - \cdots + (-1)^n |P(1, 2, \cdots, n)|$.

If $V=\{\tau_{i_1}, \tau_{i_2}, \cdots, \tau_{i_r}\}$, then there is plainly a bijective correspondence between $P(i_1, i_2, \cdots, i_r)$ and the set of all subsests of $A-\bigcup V$. Thus, $|P(i_1, i_2, \cdots, i_r)|=2^{m-|\cup V|}$, and 7.26.1 follows from (*).

Corollary 7.27. *Let $W=\{\tau_1, \tau_2, \cdots, \tau_n\}$ be a set of non-standard sequences in $S(A)$, and suppose that $W=W_1\cup W_2\cup\cdots\cup W_k$, where $(\bigcup W_i)\cap(\bigcup W_j)=\emptyset$ if $i\neq j$. Then*

7.27.1. $|G|\leq 2^m \prod_{i=1}^k (\sum_{V_i\subseteq W_i}(-1)^{|V_i|}2^{-|\cup V_i|})$.

Proof. For $V\subseteq W$, denote $V_i=V\cap W_i$, $1\leq i\leq k$. Then V is the disjoint union $V_1\cup V_2\cup\cdots\cup V_k$, $|V|=|V_1|+|V_2|+\cdots+|V_k|$, and $|\bigcup V|=|\bigcup V_1|+|\bigcup V_2|+\cdots+|\bigcup V_k|$. By 7.26.1,

$$\begin{aligned}|G|&\leq 2^m \textstyle\sum_{V_1\subseteq W_1,\cdots,V_k\subseteq W_k}(-1)^{|V_1|+\cdots+|V_k|}2^{-(|\cup V_1|+\cdots+|\cup V_k|)}\\ &= 2^m \textstyle\prod_{i=1}^k (\sum_{V_i\subseteq W_i}(-1)^{|V_i|}2^{-|\cup V_i|}).\end{aligned}$$

To use 7.26 and 7.27, we need some non-standard sequences. The following lemma provides a few of them.

Lemma 7.28. *Let $a<b<c$ in A be such that either $a=b\circ c$, $b=c\circ a$, or $c=a\circ b$. Then (b, c) is not standard.*

Proof. In these respective cases, 7.3 and 7.5 yield: $(b, c)\sim(a, b)$; $(b, c)\sim(a, a\circ c)$; $(b, c)\sim(a, a\circ b\circ a)$. By 7.4, (b, c) is not standard.

Lemma 7.29. *Let $A=A_1\cup\cdots\cup A_s\cup\cdots\cup A_t$ be the principal decomposition of A, where $|A_i|\geq 2$ for $1\leq i\leq s$, and $|A_i|=1$ for $s<i\leq t$. Then*

7.29.1. $|G|\leq(3/4)^s 2^m$.

Proof. If $m=0$ or 1, or if $s=0$, 7.29.1 follows from 7.21. We proceed by induction on m, assuming that $s\geq 1$. Denote $B=A_2\cup\cdots\cup A_s\cup\cdots\cup A_t$, $N=\langle B\rangle\lhd G$, $C=\{aN: a\in A_1\}$, and $H=G/N=\langle C\rangle$ (see 5.6). By the induction hypothesis, $|N|\leq(3/4)^{s-1}2^{m-|A_1|}$. If $|C|=1<|A_1|$, then $|H|\leq 2\leq(1/2)2^{|A_1|}$, so that $|G|=|H|\cdot|N|<(3/4)^s 2^m$. If $|C|>1$, then by 5.8 and 7.28, there is a non-standard $\tau\in S(C)$ with $|\tau|=2$. Applying 7.26 with $W=\{\tau\}$ gives $|H|\leq(-1)^{|\emptyset|}2^{|C|}+(-1)^{|\{\tau\}|}2^{|C|-|\tau|}=(3/4)2^{|C|}\leq(3/4)2^{|A_1|}$. Hence, $|G|\leq(3/4)^s 2^m$ in this case also.

Lemma 7.30. *Assume that $a\in A$, and $d_A(a)=d\geq 2$. Then*

7.30.1. $|G|\leq(3/4)^{d/2}2^m$.

Proof. By Definition 5.21, there exist distinct elements $b_1, c_1, b_2, c_2, \cdots, b_{d/2}, c_{d/2}$ in A such that $a\circ b_i=c_i$ for $1\leq i\leq d/2$. Choose the well ordering of A so that $a<b_1<c_1<b_2<c_2<\cdots<b_{d/2}<c_{d/2}$. By 7.28, $\tau_i=\{b_i, c_i\}$ is non-standard.

The estimate 7.30.1 follows from 7.27 by taking $W=\{\tau_1, \tau_2, \cdots, \tau_{d/2}\}$ and W_i to be the singleton τ_i for $1\leq i\leq d/2$.

We conclude this section with an example. It will be shown that the estimate 7.27.1 is sharp when it is applied to the pair (S_n, J_n) of 5.22.

EXAMPLE 7.31. Let $G=S_n$ be the symmetric group on $n\geq 3$ letters, and let $A=J_n$ be the symmetric groupoid consisting of all transpositions in S_n. Then (S_n, J_n) satisfies 7.13.2, so that 7.27 is applicable in this case. For $1\leq i<j\leq n$, denote $a_{ij}=a_{ji}=(i,j)$. Then $A=\{a_{ij}\colon 1\leq i<j\leq n\}$ has cardinality $(1/2)n(n-1)$. Order A lexicographically: $a_{ij}<a_{kl}$ if $\min\{i,j\}<\min\{k,l\}$ or $\min\{i,j\}=\min\{k,l\}$ and $\max\{i,j\}<\max\{k,l\}$. If $i<j<k$, then $a_{ij}<a_{ik}<a_{jk}$ and $a_{ij}\circ a_{ik}=a_{jk}$, so that (a_{ik}, a_{jk}) is non-standard by 7.28. For $k\geq 3$, let $W_k=\{(a_{ik}, a_{jk})\}\colon i<j<k\}$, and $W=W_3\cup\cdots\cup W_n$. By 7.27.1, we have

7.31.1. $|G|\leq 2^{(1/2)n(n-1)}\prod_{k=3}^{n}N_k$,

where $N_k=\sum_{V_k\subseteq W_k}(-1)^{|V_k|}2^{-|\cup V_k|}$. For a fixed $k\geq 3$, we can identify W_k with the set $P_2(I_{k-1})$ of all two element subsets of I_{k-1}, where $I_l=\{1, 2, \cdots, l\}$ for any natural number l. Making this identification, $N_k=\sum_{V\subseteq P_2(I_{k-1})}(-1)^{|V|}2^{-|\cup V|}=\sum_{U\subseteq I_{k-1}}2^{-|U|}(\sum_{V\subseteq P_2(U),\, \cup V=U}(-1)^{|V|})$. The parenthetical sum in this last expression depends only on $|U|$, so that if we denote

7.31.2. $a_r=\sum_{V\subseteq P_2(I_r),\, \cup V=I_r}(-1)^{|V|}$,

then

7.31.3. $N_k=\sum_{r=0}^{k-1}a_r\binom{k-1}{r}2^{-r}$.

If $V\subseteq P_2(I_{r+1})$ and $\bigcup V=I_{r+1}$, then V is uniquely the disjoint union $V'\cup(I_r-\bigcup V')\times\{r+1\}\cup T\times\{r+1\}$, where $V'\subseteq P_2(I_r)$, $T\subseteq\bigcup V'$, and $T\neq\emptyset$ if $\bigcup V'=I_r$. Conversely, each pair (V', T) satisfying these conditions gives rise to $V\subseteq P_2(I_{r+1})$ such that $\bigcup V=I_{r+1}$. Using these observations, a straightforward calculation based on 7.31.2 gives the recursion relation $a_{r+1}=(-1)^r-a_r$. Since $a_0=(-1)^0=1$, it follows by induction that

7.31.4. $a_r=(-1)^{r-1}(r-1)$.

Hence, 7.31.4 and 7.31.3 yield $N_k=1+(1/2)\sum_{s=1}^{k-2}s\binom{k-1}{s+1}(-1/2)^s$. This sum can be evaluated by differentiating the binomial expansion of $x^{-1}(1+x)^{k-1}$, obtaining $\sum_{s=1}^{k-2}s\binom{k-1}{s+1}x^s=x^{-1}(1+((k-2)x-1)(1+x)^{k-2})$. Consequently, $N_k=k(1/2)^{k-1}$. Substituting this value of N_k into 7.31.1 and simplifying gives $|G|\leq n!$ Thus, the apparently crude estimate given by 7.27.1 is sharp for the case under consideration. Some interesting byproducts come from this conclusion. First, we see that for the given ordering of J_n, the non-standard sequences of length 2 are exactly those of the form (a_{ik}, a_{jk}) with $i<j<k$. Second, a strictly increasing sequence of length greater than 2 in J_n is standard if and only if it contains no non-standard subsequence of length 2. Combining these observations with Theorem 7.20 gives a canonical form for the representation of permutations as products of transpositions.

Corollary 7.32. *The elements of S_n, $n\geq 3$, are canonically represented as products of transpositions in the form $(i_1, k_1)(i_2, k_2)\cdots(i_m, k_m)$, where*

7.32.1. $1\leq i_j<k_j\leq n$ *for* $1\leq i\leq m$,
7.32.2. $i_1\leq i_2\leq\cdots\leq i_m$,
7.32.3. *if* $i_j=i_{j+1}$, *then* $k_j<k_{j+1}$,
7.32.4. $k_1, k_2, \cdots, k_m$ *are distinct.*

8. Symmetrically presented groups

In this section, as in the last one, the objects of our interest are pairs (G, A), where G is a group, $A<I(G)$, and $\langle A\rangle=G$. Now, however, the group G will be more closely related to its generating symmetric groupoid A. To a considerable extent, this section is a continuation of the work that was started in Section 4.

Proposition 8.1. *Let G be a group, and suppose that A is a subgroupoid of $I(G)$ such that $\langle A\rangle=G$. The following conditions are equivalent.*

8.1.1. Π: $S(A)\to G$ *has kernel* Γ_0.

8.1.2. *If H is a group, and f: $A\to I(H)$ is a groupoid homomorphism, then f extends to a group homomorphism of G to H.*

8.1.3. *The groupoid homomorphism f_A: $A\to I(E_A)$ that was defined in* 4.14 *extends to an isomorphism of G to E_A.*

Proof. (1) 8.1.1 implies 8.1.2. Let f: $A\to I(H)$ be a groupoid homomorphism. It can be assumed that $H=\langle f(A)\rangle$. Let f': $S(A)\to S(f(A))$ be the monoid homomorphism induced by f, and let Π': $S(f(A))\to H$ be defined as in 7.1.4. Plainly, the kernel Γ of $\Pi'f'$ includes all pairs of the form 7.3.1 and 7.3.2, so that $\Gamma_0\subseteq\Gamma$. Thus, there is a group homomorphism g: $G\to H$ such that $\Pi'f'=g\Pi$. In particular, $g(a)=f(a)$ for all $a\in A$.

(2) 8.1.2 implies 8.1.3. By virtue of 8.1.2, there is a group homomorphism g: $G\to E_A$ extending f_A. It follows easily from 4.14.3 that g is surjective. By 4.14.4, there is a group homomorphism h: $E_A\to G$ such that hf_A is the inclusion map of A to G. Since $G=\langle A\rangle$, it follows that $hg=1_G$. Thus, g is an isomorphism.

(3) 8.1.3 implies 8.1.1. Let g: $G\to E_A$ be the isomorphism that extends

f_A. By the remark following 7.4, there is a monoid homomorphism k: $S(A)\to E_A$ such that Ker $k=\Gamma_0$. It is also easy to see that the restriction of k to the one element sequences of $S(A)$ coincides with the corresponding restriction of $g\Pi$. Hence, $g\Pi=k$, and Ker $\Pi=$Ker $k=\Gamma_0$.

DEFINITION 8.2. Let G be a group, and suppose that A is a subgroupoid $I(G)$ such that $G=\langle A\rangle$. Then G is *symmetrically presented* by A if the equivalent conditions of 8.1 are satisfied.

Corollary 8.3. *If A is a special symmetric groupoid, then there is a group G such that G is symmetrically presented by A. Moreover, G is uniquely determined to within an isomorphism that fixes the elements of A.*

This corollary is a special case of 4.14 and 4.15. The result was found independently by S. Doro; it appears in his paper [2].

It is useful to note that if G is symmetrically presented by A, then $1\notin A$. In fact, the mapping sends every element of A to -1 in the multiplicative group $H=\{1, -1\}$ is a groupoid homomorphism of A to $I(H)$ that surely cannot be extended to a group homomorphism if $1\in A$. This same argument gives the stronger conclusion that no element of A can be in the commutator subgroup G' of G. In particular, $G\neq G'$. A more precise version of this observation will be established later in this section.

Corollary 8.4. *Assume that the group G is symmetrically presented by the symmetric groupoid A. Let H be a group such that there is an injective groupoid homomorphism f: $A\to I(H)$, and $H=\langle f(A)\rangle$. Then there is a surjective group homomorphism g: $G\to H$ extending f, and Ker $g\subseteq C(G)$.*

Proof. The homomorphism g exists by 8.1.2, and $g(G)=g(\langle A\rangle)=\langle g(A)\rangle=\langle f(A)\rangle=H$. The inclusion Ker $g\subseteq C(G)$ is a special case of our next lemma.

Lemma 8.5. *Let G be a group, $A<I(G)$ such that $\langle A\rangle=G$, and suppose that g: $G\to H$ is a surjective group homomorphism.*

8.5.1. *If $g|A$ is injective, then $g^{-1}(C(H))=C(G)$.*
8.5.2. *If $Z(A)=I_A$ and Ker $g\subseteq C(G)$, then $g|A$ is injective.*

Proof. Since g is surjective, $C(G)\subseteq g^{-1}(C(H))$. Suppose that $g(x)\in C(H)$, where $x=a_1a_2\cdots a_n$, $a_i\in A$. Then for all $b\in A$, $g(b)=g(x)g(b)g(x)^{-1}=g(a_1\circ a_2\circ\cdots\circ a_n\circ b)$. If $g|A$ is injective, then $b=a_1\circ a_2\circ\cdots\circ a_n\circ b=xbx^{-1}$ for all $b\in A$. Hence, $x\in C(G)$ because $\langle A\rangle=G$. The implication 8.5.2 is a consequence of the observation that $Z(A)=\{(a, b)\in A^2\colon ab\in C(G)\}$, and $g(a)=g(b)$ implies $ab\in$ Ker $g\subseteq C(G)$ for $a, b\in A$.

The result 8.4 shows that the groups H that are generated by a given subgroupoid A of $I(H)$ can be found among the central homomorphs of the unique group G that is symmetrically presented by A. Not all GI groups are symmetrically presented by a symmetric groupoid A. For example, if G is a finite, non-abelian simple group, then G is generated by involutions (by the Feit-Thompson theorem), but G cannot be symmetrically presented because $G'=G$. However, by 8.4 and 8.5, $G=H/C(H)$, where H is symmetrically presented by any class of involutions.

EXAMPLE 8.6. Let G_α be the free GI group on a set of α involutions. Then G_α is symmetrically presented by $I(G_\alpha)-\{1\}$. In fact, by 4.12 and 4.4, any groupoid homomorphism from $I(G_\alpha)-\{1\}$ to $I(H)$, where H is a group, extends to a group homomorphism of G_α to H. Thus, $(G_\alpha, I(G_\alpha)-\{1\})$ satisfies 8.1.2.

EXAMPLE 8.7. For $n\geq 2$, the symmetric group S_n is symmetrically presented by the symmetric groupoid J_n of all transpositions. If $n=2$, this assertion is obvious. If $n\geq 3$, then it follows from Example 7.31 that Γ_0 is the kernel of the homomorphism $\Pi\colon S(J_n)\to S_n$, that is, 8.1.1 is satisfied.

Proposition 8.8. *Let G be a group that admits a presentation*

$$G=\langle a_\xi,\ \xi<\alpha\colon a_\xi^2=1,\ \xi<\alpha;\ w_k(a)=1,\ k\in K\rangle,$$

where a is α cardinal number, and for every $k\in K$, $w_k(a)$ is a word of the form

8.8.1. $a_\eta a_{\xi_1}\cdots a_{\xi_{r-1}}a_{\xi_r}a_{\xi_{r-1}}\cdots a_{\xi_1}$.

Let A be the union of the conjugate classes of the elements a_ξ, $\xi<\alpha$. Then G is symmetrically presented by A.

Proof. Plainly, $A<I(G)$ and $\langle A\rangle=G$. Let F be the free group on $\{x_\xi\colon \xi<\alpha\}$, and define the homomorphism $p\colon F\to G$ by the condition $p(x_\xi)=a_\xi$ for all $\xi<\alpha$. By the definition of a presentation, p is surjective, and $\operatorname{Ker} p$ is the smallest normal subgroup of G that contains all words of the form x_ξ^2, $\xi<\alpha$, and $w_k=x_\eta x_{\xi_1}\cdots x_{\xi_{r-1}}x_{\xi_r}x_{\xi_{r-1}}\cdots x_{\xi_1}$. Suppose that H is a group, and $f\colon A\to I(H)$ is a groupoid homomorphism. Define a group homomorphism $h\colon F\to H$ by the condition $h(x_\xi)=f(a_\xi)$ for all $\xi<\alpha$. Then $h(x_\xi^2)=f(a_\xi)^2=1$, since $f(a_\xi)\in I(H)$. Hence, $x_\xi^2\in\operatorname{Ker} h$. Also, $h(x_{\xi_1}\cdots x_{\xi_{r-1}}x_{\xi_r}x_{\xi_{r-1}}\cdots x_{\xi_1})=h(x_{\xi_1})\cdots h(x_{\xi_r})\cdots h(x_{\xi_1})=f(a_{\xi_1})\cdots f(a_{\xi_r})\cdots f(a_{\xi_1})=f(a_{\xi_1})\circ\cdots\circ f(a_{\xi_r})=f(a_{\xi_1}\circ\cdots\circ a_{\xi_r})=f(a_\eta)=h(x_\eta)$, where $w_k(a)=a_\eta a_{\xi_1}\cdots a_{\xi_{r-1}}a_{\xi_r}a_{\xi_{r-1}}\cdots a_{\xi_1}$ (so that $a_\eta=a_{\xi_1}\circ\cdots\circ a_{\xi_r}$ in A). Consequently, $w_k=(x_\eta^2)(x_\eta^{-1}x_{\xi_1}\cdots x_{\xi_{r-1}}x_{\xi_r}x_{\xi_{r-1}}\cdots x_{\xi_1})\in\operatorname{Ker} h$. Thus, $\ker p\subseteq\operatorname{Ker} h$, so that h factors through p. That is, there is a group homomorphism $g\colon G\to H$ such that $h=gp$. In particular, $g(a_\xi)=g(p(x_\xi))=h(x_\xi)=f(a_\xi)$. Since G is generated as a group by $\{a_\xi\colon\xi<\alpha\}$, it follows that A is generated as a groupoid by $\{a_\xi\colon\xi<\alpha\}$. Consequently, $g\,|\,A=f$, so that G is symmetrically presented by A, according to 8.1.2.

Corollary 8.9. *Every Coxeter group G is symmetrically presented by a subgroupoid of $I(G)$.*

Proof. Every Coxeter group G has a presentation $G=\langle a_1, \cdots, a_n: a_i^2=1, 1\leq i\leq n; (a_ia_j)^{p_{ij}}=1, 1\leq i<j\leq n$, where $p_{ij}\geq 2\rangle$ (see [1]). Plainly, $(a_ia_j)^{p_{ij}}$ is of the form 8.8.1.

Since the symmetric group S_n is a Coxeter group, this corollary generalizes Example 8.7.

There is a converse of 8.8.

Proposition 8.10. *Let A be a special symmetric groupoid with a presentation*

8.10.1. $A=\langle a_\xi, \xi<\alpha: v_{0k}(a)=v_{1k}(a), k\in K\rangle$,

where $v_{0k}(a)$ and $v_{ik}(a)$ are words in the language of groupoids involving the generators a_ξ. For $k\in K$, define $w_k(a)=a_{\eta_s}a_{\eta_{s-1}}\cdots a_{\eta_1}a_{\xi_1}\cdots a_{\xi_{r-1}}a_{\xi_r}a_{\xi_{r-1}}\cdots a_{\xi_1}a_{\eta_1}\cdots a_{\eta_{s-1}}$ whenever $v_{0k}(a)=a_{\xi_1}\circ\cdots\circ a_{\xi_{r-1}}\circ a_{\xi_r}$, and $v_{1k}(a)=a_{\eta_1}\circ\cdots\circ a_{\eta_{s-1}}\circ a_{\eta_s}$. Let G be the group that is symmetrically presented by A. Then G has the presentation

8.10.2. $G=\langle a_\xi, \xi<\alpha: a_\xi^2=1, \xi<\alpha; w_k(a)=1, k\in K\rangle$.

Proof. Let G_α be the group that is freely generated by the set $\{u_\xi: \xi<\alpha\}$ of involutions (as in 4.3), and denote $A_\alpha=I(G_\alpha)-\{1\}$. By 4.12, A_α is the free symmetric groupoid on $\{u_\xi: \xi<\alpha\}$. Let N be the smallest normal subgroup of G_α that includes all of the words w_k, and denote by Γ the smallest congruence relation on A_α that contains all of the pairs (v_{0k}, v_{1k}), $k\in K$. Here, w_k represents the group word that is obtained from $w_k(a)$ by replacing each occurrence of a_ξ by u_ξ, and v_{0k}, v_{1k} are the groupoid words obtained from $v_{0k}(a)$, $v_{1k}(a)$ by the same replacements. If $\Delta=\{(v_0, v_1)\in A_\alpha^2: v_1^{-1}v_0\in N\}$, then because Δ is a congruence relation on A_α that obviously includes all pairs $(v_{0k}\, v_{1k})$, $k\in K$, it follows that $\Gamma\subseteq\Delta$. Since 8.10.1 is a presentation of A, the kernel of the homomorphism $p: A_\alpha\rightarrow A$ such that $p(u_\xi)=a_\xi$ for all $\xi<\alpha$ is Γ. By the hypothesis that A is special and the fact noted in 8.6 that G_α is symmetrically presented by A_α, it follows that p can be extended to a group homomorphism $g: G_\alpha\rightarrow H$, where H is a group such that $A<I(H)$. Plainly, $N\subseteq \operatorname{Ker} g$, and $\Gamma=\operatorname{Ker} p=\operatorname{Ker} g\,|\,A_\alpha\supseteq\Delta$. Therefore, $\Gamma=\Delta$. By the proof of 4.3, the group G_α has a presentation $G_\alpha=\langle u_\xi, \xi<\alpha: u_\xi^2=1, \xi<\alpha\rangle$. Therefore, by 8.8, the group G defined by 8.10.2 is symmetrically presented by A_α/Γ, that is, by A.

Taken together, 8.8 and 8.10 imply the following closure property of the class of symmetrically presented groups.

Corollary 8.11. *Assume that G_i is symmetrically presented by A_i for each i in the index set J. Then the free product $G=*_{i\in J}G_i$ is symmetrically presented* *by the union of the conjugate classes in G of the elements in* $\bigcup_{i\in J} A_i$.

There is an analogous result for direct sums.

Lemma 8.12. *Assume that* G_i *is symmetrically presented by* A_i *for each* i *in the index set* J. *Then the direct sum* $G=\sum_{i\in J} G_i$ *is symmetrically presented* $A=\bigcup_{i\in J} A_i$.

Proof. Plainly, $A<I(G)$ and $\langle A\rangle=\langle\bigcup_{i\in J} A_i\rangle=\sum_{i\in J} G_i=G$. Let f: $A\rightarrow I(H)$ be a groupoid homomorphism, where H is some group. By 8.1.2, there exist group homomorphisms g_i: $G_i\rightarrow H$ such that $g_i\,|\,A_i=f\,|\,A_i$ for all $i\in J$. If $i\neq j$, $a\in A_i$ and $b\in A_j$, then $g_i(a)g_j(b)g_i(a)=f(a)f(b)f(a)=f(a\circ b)=f(b)=g_j(b)$. Since $G_i=\langle A_i\rangle$ and $G_j=\langle A_j\rangle$, it follows that $g_i(G_i)$ centralizes $g_j(G_j)$. Consequently, there is a homomorphism g: $G\rightarrow H$ such that $g\,|\,G_i=g_i$ for all $i\in J$. In particular, g extends f. By 8.1.2, G is symmetrically presented by A.

There is a straightforward converse of 8.12. It will be omitted.

The results of Section 7 can be improved considerably when they are applied to pairs (G, A) such that G is symmetrically presented by A. In fact, even slightly weaker hypotheses give these improvements.

HYPOTHESES and NOTATION 8.13. Assume that G is a group, $A<I(G)-\{1\}$, and $\langle A\rangle=G$. Let $A=\bigcup_{i\in J} A_i$ be the principal decomposition of A. For $i\in J$, and $\sigma=(a_0, a_1, \cdots, a_{r-1})\in S(A)$, denote

$$\|\sigma\|_i = |\{k<r:\ a_k\in A_i\}|.$$

Lemma 8.14. *With the notation and hypotheses of* 8.13, *and the relation* Γ_0 *defined in Section* 7,

8.14.1 *if* $(\sigma, \tau)\in\Gamma_0$, *then* $\|\sigma\|_i\equiv\|\tau\|_i$ (*mod* 2) *for all* $i\in J$.

In particular, if G *is symmetrically presented by* A, *then*

8.14.2 *if* $\sigma, \tau\in S(A)$ *satisfy* $\Pi\sigma=\Pi\tau$, *then* $\|\sigma\|_i\equiv\|\tau\|_i$ (*mod* 2) *for all* $i\in J$.

Proof. If $b\in A_i$ and $a\in A$, then $a\circ b\in A_i$. It follows that 8.14.1 is satisfied whenever (σ, τ) has one of the forms 7.3.1 or 7.3.2. The general case of 8.14.1 follows by induction on the length of a sequence of primitive equivalences connecting σ and τ. The implication 8.14.2 is a direct consequence of 8.8.1 and 8.14.1.

The property 8.14.2 of symmetrically presented groups makes it possible to define a signature map that generalizes the notion of the sign of a permutation. It turns out that the pairs (G, A) satisfying 8.14.2 are considerably more common than the prototype: G is symmetrically presented by A. It therefore seems worthwhile to introduce yet another definition.

TERMINOLOGY 8.15. A pair (G, A) that satisfies the hypotheses of 8.13 will be called an S-pair if the implication 8.14.2 is satisfied.

If (G, A) is an S-pair, then the equivalent conditions of 7.13 are plainly satisfied. Therefore, the various estimates of $|G|$ that were developed in the last part of Section 7 are applicable in this case.

Lemma 8.16. *Assume that the conventions of* 8.13 *are in effect.*

8.16.1. *If $a\in A_i$ and $b\in A_i$, then $ab\in G'$.*

8.16.2. *Every element of G' can be expressed in the form $\Pi\sigma$, where $\sigma\in S(A)$ satisfies $||\sigma||_i\equiv 0$ (mod 2) for all $i\in J$.*

8.16.3. *If $\{a_i: i\in J\}$ is a set of representatives of the principal components of A, then G/G' is an elementary abelian 2-group that is spanned by $\{a_iG': i\in J\}$.*

8.16.4. *If $\{a_i: i\in J\}$ is a set of representatives of the principal components of A, then $\{a_iG': i\in J\}$ are distinct, non-zero, linearly independent elements of G/G' if and only if (G, A) is an S-pair.*

Proof. (1) By 5.6, if $a, b\in A_i$, then $b=xax^{-1}=xa^{-1}x^{-1}$ for some $x\in G$. Hence, $ab=axa^{-1}x^{-1}\in G'$.

(2) It sufficies to observe that if $x, y\in G$, say $x=\Pi\rho$, $y=\Pi\tau$, then $xyx^{-1}y^{-1}=\Pi\sigma$, where $\sigma=\rho\tau\rho^{-1}\tau^{-1}$ satisfies $||\sigma||_i\equiv 0$ (mod 2) for all $i\in J$.

(3) Since $G=\langle A\rangle$, it follows that G/G' is an abelian GI group, hence an elementary 2-group. If $f: G\rightarrow G/G'$ is the natural projection, then $G/G'=f(G)=f(\langle A\rangle)=\langle f(A)\rangle=\langle\{f(a_i): i\in J\}\rangle$ by 8.16.1.

(4) Assume that (G, A) is an S-pair. By 8.16.2, $\sigma\in S(A)$ and $\Pi\sigma\in G'$ implies $||\sigma||_i\equiv 0$ (mod 2) for all $i\in J$. It follows that if $i_1, \cdots, i_r$ are distinct elements of J, then $a_{i_1}\cdots a_{i_r}\notin G'$. Hence, passing to additive notation, $a_{i_1}G'+\cdots+a_{i_r}G'\neq 0$ in G/G'. Conversely, if (G, A) is not an S-pair, then there exist σ, $\tau\in S(A)$ such that $\Pi\sigma=\Pi\tau$, and $||\sigma||_j\not\equiv||\tau||_j$ (mod 2) for some $j\in J$. Let $\rho=\sigma\tau^{-1}$. Then $\Pi\rho=1$ and $K=\{i\in J: ||\rho||_i\equiv 1 \text{ (mod 2)}\}$ is not empty. By 8.16.1, $\sum_{i\in K}a_iG'=0$ in G/G'.

Corollary 8.17. *If (G, A) satisfies the hypotheses of* 8.13, *and A is principal, then (G, A) is an S-pair if and only if $|G/G'|=2$.*

Corollary 8.18. *Let G be a finite 2-group. The following conditions are equivalent.*

8.18.1. *There exists $A<I(G)$ such that (G, A) is an S-pair.*

8.18.2. *G is generated by involutions.*

8.18.3. *G/G' has a generating set that consists of cosets of the form aG', where $a\in I(G)$.*

Proof. By the definition of S-pairs, 8.18.1 implies 8.18.2, and 8.18.2

implies 8.18.3 by 8.16.3. If 8.18.3 is satisfied, say $\{a_1G', \cdots, a_rG'\}$ is a basis of G/G' such that $a_i \in I(G)$ for $1 \leq i \leq r$, let A be the union of the conjugate classes of these a_i. Then $A < I(G) - \{1\}$, and $\langle A \rangle = G$ by the Burnside basis theorem. By 8.16.4, (G, A) is an S-pair.

Corollary 8.19. *If (G, A) is an S-pair, and $A \subset C < I(G)$, then (G, C) is not an S-pair.*

Proposition 8.20. *Assume that the hypotheses of* 8.13 *are satisfied, and that (G, A) is an S-pair. Define the signature map* **sgn**: $G \to \{-1, 1\}^J$ *by* $(\mathbf{sgn}\, x)(i) = (-1)^{\|\sigma\|_i}$, *where $x = \Pi\sigma$, $\sigma \in S(A)$. Then* **sgn** *is a well defined, group homomorphism of G onto the subgroup F_J of $\{-1, 1\}^J$ that consists of all ψ such that $\psi(i) = 1$ for almost all $i \in J$. The kernel of* **sgn** *is the commutator subgroup G' of G.*

Proof. Since (G, A) is an S-pair, the definition of **sgn** is well posed. Also, **sgn** is a homomorphism because $\|\sigma\tau\|_i = \|\sigma\|_i + \|\tau\|_i$ for all $\sigma, \tau \in S(A)$, and $i \in J$. If $\psi \in F_J$, let $K = \{i \in J : \psi(i) = -1\}$, and select an arbitrary $a_i \in A_i$ for each $i \in K$. Plainly, if $x = \prod_{i \in K} a_i$, then $\mathbf{sgn}\, x = \psi$. Conversely, it is clear that $\mathbf{sgn}\, x \in F_J$ for all $x \in G$. Hence, F_J is the image of **sgn**. It follows from 8.16.1 and 8.16.2 that the kernel of **sgn** is G'.

Corollary 8.21. *If (G, A) is an S-pair, and $f: G \to H$ is a surjective homomorphism of groups such that $\mathrm{Ker}\, f \subseteq G'$, then $(H, f(A))$ is an S-pair.*

Proof. Since $\mathrm{Ker}\, f \subseteq G' = \mathrm{Ker}\,(\mathbf{sgn})$, the signature map factors through f, that is, $\mathbf{sgn} = hf$ for some homomorphism $h: H \to F_J$. It follows that $f(A) \subseteq I(H) - \{1\}$ and that $f(A_i) \cap f(A_j) = \emptyset$ if $i \neq j$ in J. We conclude from 5.8 that $f(A) = \bigcup_{i \in J} f(A_i)$ is the principal decomposition of $f(A)$. Moreover, if $\sigma \in S(A)$, then $\|f\sigma\|_i = \|\sigma\|_i$. Consequently, $\Pi f\sigma = \Pi f\tau$ implies $\Pi\sigma\tau^{-1} \in \mathrm{Ker}\, f \subseteq G'$, so that $\|f\sigma\|_i = \|\sigma\|_i \equiv \|\tau\|_i = \|f\tau\|_i \pmod 2$ for all $i \in J$. Thus, $(H, f(A))$ is an S-pair.

If a pair (G, A) is given satisfying the hypotheses 8.13, then the criterion 8.16.4 can generally be used to determine whether or not (G, A) is an S-pair. Unfortunately, there is no effective criterion for determining whether G is symmetrically presented by A. The rest of this section is devoted to constructing the group that is symmetrically presented by a symmetric groupoid of the form K_H, where H is a 2-divisible abelian group (see 5.23).

EXAMPLE 8.22. Let H be an arbitrary abelian group, written multiplicatively. Let $L = \Lambda^2 H$ be the homogeneous component of degree 2 in the exterior algebra of H. Then L is an abelian group that will also be written multiplicatively. The map $H \times H \to L$ defined by $(x, y) \to x \wedge y$ is easily seen to be a factor set with respect to the trivial action of H on L. Let M be the corresponding extension of L by H. Thus, there is a surjective homomorphism p: $M \rightarrow H$ with Ker $p=L$, and a cross section π: $H \rightarrow M$ (satisfying $p\pi=1_H$) such that:

(1) each element of M is uniquely represented in the form $\pi(x)l$ with $x \in H$ and $l \in L$;

(2) $(\pi(x)l)(\pi(y)m)=\pi(xy)(x \wedge y)lm$, $(\pi(x)l)^{-1}=\pi(x^{-1})l^{-1}$, and $\pi(1)=1$.

Since $\pi(xy)^{-1}\pi(x)\pi(y)=x \wedge y$, it follows that

(3) $M=\langle \pi(x)\colon x \in H \rangle$.

Define θ: $M \rightarrow M$ by $\theta(\pi(x)l)=\pi(x^{-1})l$. By a routine calculation.

(4) $\theta \in \operatorname{Aut} M$, $\theta^2=1_M$, and $\{w \in M\colon \theta(w)=w^{-1}\}=\{\pi(x)\colon x \in H\}$.

The facts given in (3) and (4) imply that θ can be used to construct a generalized dihedral group over M. Specifically, define G to be the semidirect product

(5) $G=M \times_\theta \langle a \rangle = M \cup aM$,

where $a^2=1$ and $awa=\theta(w)$ for all $w \in M$. Denote $A=\{a\pi(x)\colon x \in H\}$. It follows from (3) and (4) that $A < I(G)-\{1\}$ and $\langle A \rangle = G$. In fact,

(6) $(a\pi(x)) \circ (a\pi(y)) = a\pi(x^2y^{-1})$.

Let $D_H=H \times_{-1_H} \langle a \rangle$ be the generalized dihedral group over H that was defined in 5.23. The projection homomorphism p: $M \rightarrow H$ induces a surjective homomorphism f: $G \rightarrow D_H$ by $f(a^i w)=a^i p(w)$ $(i=0, 1; w \in M)$ such that Ker $f=L$. Since $f(a\pi(x))=ax$, it follows that $f \mid A$ is a groupoid isomorphism to A to K_H. A routine calculation shows that if H is not an elementary abelian 2-group, then $C(D_H)=H_2$. It follows from 8.5.1 that if H is not an elementary abelian 2-group, then

(7) $C(G)=\{\pi(x)l\colon x \in H_2, l \in L\}$.

In particular, if $I(H)=\{1\}$, then $C(G)=L$. The commutator subgroup of G is easily calculated to be

(8) $G'=\{\pi(x)l\colon x \in H^2, l \in L^2\}$.

Let G_H denote the group that is symmetrically presented by K_H. In more detail, there is an injective mapping $x \rightarrow a(x)$ from H to $I(G_H)$ such that $a(x) \circ a(y) = a(x^2y^{-1})$ for all x and y in H, and G_H is symmetrically presented by $\{a(x)\colon x \in H\}$. By 8.1.2, there is a surjective group homomorphism g: $G_H \rightarrow G$ such that $g(a(x))=a\pi(x)$ for all $x \in H$. Consequently, the homomorphism $h=fg$: $G_H \rightarrow D_H$ satisfies $h(a(x))=ax$.

(9) Ker $h=\{a(x_1)a(x_2)\cdots a(x_{2n})\colon x_1x_3\cdots x_{2n-1}=x_2x_4\cdots x_{2n}\}$. In fact, $h(a(x_1)a(x_2)\cdots a(x_r))=ax_1x_2^{-1}x_3\cdots x_r$ if r is odd, and $h(a(x_1)a(x_2)\cdots a(x_r))=x_1^{-1}x_2x_3^{-1}\cdots x_r$ if r is even; (9) follows, since $G_H=\langle \{a(x)\colon x \in H\} \rangle$.

For $x, y \in H$, denote $b(x, y)=a(x)a(1)a(y)a(xy)$. By (9), $b(x, y) \in \operatorname{Ker} h$. In particular, $b(x, y) \in C(G_H)$ by 8.5.

(10) $g(b(x, y))=x \wedge y$.

In fact, $g(b(x, y))=a\pi(x)\pi(y)a\pi(xy)=(\pi(x)\pi(y))^{-1}\pi(xy)=x \wedge y$.

(11) $\operatorname{Ker} h = \langle\{b(x, y) \colon x, y \in H\}\rangle$.

Indeed, suppose that $a(x_1)a(x_2)\cdots a(x_{2n}) \in \operatorname{Ker} h$, with $x_1x_3\cdots x_{2n-1} = x_2x_4\cdots x_{2n}$ $(n \geq 2)$ in accordance with (8). Then $a(x_1)a(x_2)\cdots a(x_{2n}) = b(x_1, x_2^{-1})b(x_1x_2^{-1}, x_3)$ $a(x_1x_2^{-1}x_3)a(x_4)\cdots a(x_{2n})$, and $(x_1x_2^{-1}x_3)x_5\cdots x_{2n-1} = x_4x_6\cdots x_{2n}$. Thus, (11) follows by induction on n.

We now develop some properties of the mapping $b \colon H \times H \to C(G_H)$. Let x, y, and z be any elements of H.

(12) $b(x, y) = b(y, x)^{-1}$.

In fact, $b(x, y)b(y, x) = a(x)a(1)a(y)b(y, x)a(xy) = a(x)a(1)a(y)a(y)a(1)a(x)a(xy)a(xy)$ $=1$.

(13) $b(1, x) = b(x, 1) = 1$.

(14) $b(x, y) = b(x, x^{-1}y) = b(xy^{-1}, y)$.

Since $a(x) \circ a(y) = a(x^2y^{-1})$, we have $a(y)a(xy)a(x) = a(x^{-1}y)$, so that $b(x, y) =$ $a(x)a(1)a(y)a(xy) = a(x)a(1)a(x^{-1}y)a(y) = b(x, x^{-1}y)$. Also, $b(x, y) = b(xy^{-1}, y)$ by (12).

(15) $b(zx, y)b(zy, x) = b(z, x)b(z, y)$.

Indeed, $b(zx, y)b(zy, x) = a(zx)a(y)a(1)b(zy, x)a(zxy) = a(zx)a(1)a(y)a(zy)a(1)a(x)$ $= a(zx)a(z)a(z)a(1)a(y)a(zy)a(1)a(x) = a(zx)a(z)b(z, y)a(1)a(x) = b(x, z)^{-1}b(z, y) =$ $b(z, x)b(z, y)$ by (12).

(16) $b(x^2, y) = b(x, y)^2 = b(x, y^2)$.

By (13), (14), and (15), $b(x, y) = b(x, y)b(x, x^{-1}x) = b(x, y)b(x, x) = b(x^2, y)b(xy, x)$ $= b(x^2, y)b(y, x)$, so that (16) follows from (12).

(17) $b(xy, z)^2 = b(x, z)^2b(y, z)^2$.

By (15), $b(xy, z)b(xz, y) = b(x, y)b(x, z)$ and $b(xy, z)b(yz, x) = b(y, x)b(y, z)$. Multiplying these equalities, and using (12) and (15) gives $b(x, z)b(y, z) =$ $b(xy, z)^2b(xz, y)b(yz, x) = b(xy, z)^2b(z, x)b(z, y)$. Thus, (17) follows, using (12).

It follows from (16) and (17) that if the group H is 2-divisible (that is, $H^2 = H$), then $b(xy, z) = b(x, z)b(y, z)$ for all x, y, and z in H. Thus, by (12), b is an alternating bilinear mapping from $H \times H$ to $C(G_H)$. The universal property of Λ^2H then implies that there is a group homomorphism $k \colon \Lambda^2H \to C(G_H)$ such that $k(x \wedge y) = b(x, y)$ for all $x, y \in H$. It follows from (10) that k is the inverse of $g \mid C(G_H)$. Summarizing: if H is a 2-divisible abelian group, then the center $C(G_H)$ of the group G_H that is symmetrically presented by K_H is isomorphic to Λ^2H; moreover, G_H is isomorphic to the group G whose construction was described above (since $\operatorname{Ker} g = \{1\}$ by 8.5).

UNIVERSITY OF ARIZONA

References

[1] H.S.M. Coxeter: *Discrete groups generated by reflections,* Ann. of Math. **35** (1934), 588–621.

[2] S. Doro: *The algebraic structure of symmetric spaces,* to appear.

[3] G. Glauberman: *On loops of odd order,* J. Algebra **1** (1964), 374–396.

[4] M. Kano, H. Nagao, and N. Nobusawa: *On finite homogeneous symmetric sets,* Osaka J. Math. **13** (1976), 399–406.

[5] N. Nobusawa: *On symmetric structure of a finite set,* Osaka J. Math. **11** (1974), 569–575.

[6] N. Nobusawa: *Simple symmetric sets and simple groups,* Osaka J. Math. **16** (1979)

[7] O. Ore: Theory of graphs, Providence, 1962.

[8] R.S. Pierce: *Symmetric groupoids,* Osaka J. Math. **15** (1978), 51–76.

[9] W.R. Scott: Group theory, Englewood Cliffs, 1964.