

Advances in Group Theory and Applications
© 2025 AGTA - www.advgrouptheory.com/journal
22 (2025), pp. 1–26 ISSN: 2499-1287
DOI: 10.32037/agta-2025-011

Prime Factorizations of Finite Groups, III *

S. Takamura

(*Received Apr. 16, 2023; Accepted Aug. 12, 2023 — Comm. by Adolfo Ballester-Bolinches*)

Abstract

This is the third part of our three consecutive papers which develop a theory of prime factorizations of groups. In this part, we introduce the notions of pure sects and pure factorizations. Besides, we describe examples of prime factorizations of groups.

Mathematics Subject Classification (2020): 20E34, 20D40

Keywords: subgroup product; group factorization;
unique factorization group; atomic subgroup

Contents

1 Purity and decompositions of sects 2
1.1 Pure sects and pure factorizations 2
1.2 Decompositions of sects 5
2 Examples of prime factorizations of finite groups 12
2.1 Ramification of prime factorizations of finite groups . . 21
References 25

This paper is the third in a three-part series, the foremost appeared in [17], and the second in [18], both published in this journal.

* We would like to thank Ryota Hirakawa and Kenjiro Sasaki for many inspiring discussions. This work was partly supported by Grant-in-Aid for Scientific Research(C) Grant Number JP20K03533.

1 Purity and decompositions of sects

1.1 Pure sects and pure factorizations

A factorization $G = H_1H_2 \dots H_n$ of a group G is always equivalent to its reverse factorization $G = H_n \dots H_2H_1$, in fact the reverse mutation gives this equivalence (note that since $H_1H_2 \dots H_n$ itself is regular, the reverse mutation exists). We however point out that there are factorizations that are not equivalent to any other factorizations except for their reverse factorizations. Such factorizations are said to be "pure". We first formulate the purity of sects. In what follows, a *nontrivial* subsect of a sect $H_1H_2 \dots H_n$ means a subsect of length greater than 1, in other words it is not any of H_i $(i = 1, 2, \dots, n)$.

Definition 1.1 A sect $H_1H_2 \dots H_n$ $(n \geqslant 2)$ of a group G is *pure* if it contains no proper nontrivial regular subsect, in other words no proper subsect $H_iH_{i+1} \dots H_j$ $(1 \leqslant i < j \leqslant n)$ of length greater than 1 is a subgroup of G. If moreover $H_1H_2 \dots H_n$ itself is not a subgroup of G, then $H_1H_2 \dots H_n$ is *strongly pure*.

If a sect is strongly pure, then its lack of nontrivial regular subsect implies that it admits no nontrivial mutation at all — in the case of pure (but not strongly pure), it only admits the reverse mutation. Thus strongly pure sects are considered as isolated among sects.

Example 1.2 For the symmetric group $\mathfrak{S}_3$ of degree 3, let H_1, H_2 and H_3 be its cyclic subgroups of order 2 generated by transpositions $(1\,2)$, $(2\,3)$ and $(3\,1)$ respectively. Then $H_iH_j \neq H_jH_i$ for distinct i and j, so H_iH_j is not regular by [17, Corollary 2.6], thus strongly pure. On the other hand, $H_1H_2H_3$ is pure but not strongly pure (indeed $H_1H_2H_3$ is equal to the group $\mathfrak{S}_3$).

Note next the following result.

Lemma 1.3 *If a sect* $H_1H_2 \dots H_n$ $(n \geqslant 3)$ *is pure* (*or* $n = 2$ *and strongly pure*), *then* $H_iH_{i+1} \neq H_{i+1}H_i$ *for* $i = 1, 2, \dots, n-1$.

Proof — This is immediate because $H_iH_{i+1} = H_{i+1}H_i$ is equivalent to H_iH_{i+1} being a subgroup of G (see [17, Corollary 2.6]). □

Remark 1.4 A sect as in Lemma 1.3 is *rigid* (see [18, Definition 5.1]), which is in particular tight, and the end conjugation method to construct inequivalent sects is applicable.

We shall shift from sects to factorizations.

Definition 1.5 A factorization $G = H_1H_2 \dots H_n$ ($n \geqslant 2$) of a group G is *pure* if $H_1H_2 \dots H_n$ is pure. (For factorizations, "strongly pure" makes no sense, indeed for a factorization $G = H_1H_2 \dots H_n$, the sect $H_1H_2 \dots H_n$ is a group.)

A pure factorization $G = H_1H_2 \dots H_n$ admits no nontrivial mutation except for the reverse mutation

$$G = H_1H_2 \dots H_n \to G = H_n \dots H_2H_1.$$

Thus it is not equivalent to any other factorization of G except for the reverse one, and a pure factorization is isolated among factorizations of G.

Remark 1.6 A factorization $G = H_1H_2$ of length 2 is trivially pure, because H_1H_2 contains no sects of length greater than 1. A factorization $G = H_1H_2H_3$ of length 3 is pure if and only if $H_1H_2 \neq H_2H_1$ and $H_2H_3 \neq H_3H_2$. For example, let H_1, H_2 and H_3 be the cyclic subgroups of order 2 of $\mathfrak{S}_3$ in Example 1.2, then $\mathfrak{S}_3 = H_1H_2H_3$ and this is pure.

As noted just above, factorizations of length 2 are always pure. How about sects of length 2 that are not factorizations?

Let us recall first that if $H_1H_2 = H_2H_1$, then H_1H_2 is a subgroup (see [17, Corollary 2.6]), hence H_1H_2 gives a factorization of the subgroup. We thus consider the case that $H_1H_2 \neq H_2H_1$. This condition ensures that we may apply the end conjugation method to construct a sect inequivalent to H_1H_2: For $g \in G$ with $gH_2g^{-1} \neq H_2$ (i.e. $g \notin N_G(H_2)$), a sect $H_1(gH_2g^{-1})$ is inequivalent to H_1H_2. In fact H_1H_2, being strongly pure, has no nontrivial mutation at all, and so if $H_1(gH_2g^{-1})$ is equivalent to H_1H_2, then necessarily

$$H_1(gH_2g^{-1}) \equiv H_1H_2 \quad \text{(identical)},$$

but then we obtain that $gH_2g^{-1} = H_2$, which contradicts the assumption $gH_2g^{-1} \neq H_2$. We point out that even if H_1H_2 is irredundant, then $H_1(gH_2g^{-1})$ may not be irredundant (see Example 1.7 below). Similarly for $k \in G$ with $kH_1k^{-1} \neq H_1$, a sect $(kH_1k^{-1})H_2$ is inequivalent to H_1H_2, though it may not be irredundant even if H_1H_2 is irredundant.

Example 1.7 For $G = \mathfrak{S}_4$, take subgroups $H_1 = \langle (34) \rangle (\simeq \mathbb{Z}_2)$ and $H_2 = \langle (12), (123) \rangle (\simeq \mathfrak{S}_3)$. Then $H_1H_2 (= \mathfrak{S}_3 \amalg (34)\mathfrak{S}_3)$ is irredundant. Next for $g = (14)$, we have

$$gH_2g^{-1} = \langle (42), (423) \rangle = \langle (34), (234) \rangle,$$

which contains H_1, thus

$$H_1(gH_2g^{-1}) = gH_2g^{-1},$$

so $H_1(gH_2g^{-1})$ is redundant.

We point out that even in the case that $H_1H_2 = H_2H_1$, if H_1H_2 is irredundant, then the above construction by the end conjugation method for the case $H_1H_2 \neq H_2H_1$ works. To see this, note first that as $H_1H_2 = H_2H_1$, the sect H_1H_2 admits only one nontrivial mutation $H_1H_2 \to H_2H_1$. Thus if $H_1(gH_2g^{-1})$ with $gH_2g^{-1} \neq H_2$ is equivalent to H_1H_2, then necessarily

$$H_1(gH_2g^{-1}) \equiv H_2H_1 \quad \text{(identical)},$$

that is, $H_1 = H_2$ and $gH_2g^{-1} = H_1$. However $H_1 = H_2$ implies that H_1H_2 is not irredundant, which is a contradiction. Hence we obtain that $H_1(gH_2g^{-1})$ is not equivalent to H_1H_2. We here point out that while $H_1H_2 = H_2H_1$, in general $H_1(gH_2g^{-1}) \neq (gH_2g^{-1})H_1$.

Example 1.8 For $G = \mathfrak{S}_4$, take subgroups

$$H_1 = \langle (12) \rangle (\simeq \mathbb{Z}_2) \quad \text{and} \quad H_2 = \langle (12)(34) \rangle (\simeq \mathbb{Z}_2).$$

Then

$$H_1H_2 = H_2H_1 = \langle (12), (34) \rangle (\simeq K_4).$$

On the other hand, for $g = (24)$ we have that $gH_2g^{-1} = \langle (14)(23) \rangle$, and $H_1(gH_2g^{-1}) \neq (gH_2g^{-1})H_1$; indeed

$$\begin{cases} H_1(gH_2g^{-1}) = \{1, (12), (14)(23), (1423)\}, \\ (gH_2g^{-1})H_1 = \{1, (12), (14)(23), (1324)\}. \end{cases} \tag{1.1}$$

Remark 1.9 Another example can be immediately constructed by interchanging H_2 and gH_2g^{-1} in Example 1.7 while keeping the oth-

ers the same. Namely for $G = \mathfrak{S}_4$, take subgroups

$$H_1 = \langle (3\,4) \rangle \, (\simeq \mathbb{Z}_2) \quad \text{and} \quad H_2 = \langle (3\,4), (2\,3\,4) \rangle \, (\simeq \mathfrak{S}_3).$$

Then $H_1H_2 = H_2H_1$ $(= H_2)$. However for $g = (1\,4)$, we have

$$gH_2g^{-1} = \langle (3\,1), (2\,3\,1) \rangle = \langle (1\,2), (1\,2\,3) \rangle,$$

and so $H_1(gH_2g^{-1}) \neq (gH_2g^{-1})H_1$. Yet this example is unsatisfactory in that H_1H_2 is not irredundant (indeed $H_1H_2 = H_2$).

1.2 Decompositions of sects

In general a sect is not permutative and far from being a subgroup, which makes it hard to treat. To clarify which parts of a sect are complicated, we introduce its *canonical decomposition*. First, for a sect

$$\mathcal{H} := H_1H_2 \dots H_n,$$

let $\mathcal{L}$ and $\mathcal{R}$ be its left and right permutative parts if any — here if $H_1H_2 \neq H_2H_1$, then $\mathcal{L}$ is empty and if $H_1H_2 = H_2H_1$, then $\mathcal{L}$ is the subsect $H_1H_2 \dots H_l$ $(2 \leqslant l \leqslant n)$ of $\mathcal{H}$ with l the maximum such that $H_iH_j = H_jH_i$ for any $i, j \in \{1, 2, \dots, l\}$. Similarly if

$$H_{n-1}H_n \neq H_nH_{n-1},$$

then $\mathcal{R}$ is empty and if $H_{n-1}H_n = H_nH_{n-1}$, then $\mathcal{R}$ is the subsect $H_r \dots H_{n-1}H_n$ $(1 \leqslant r \leqslant n-1)$ of $\mathcal{H}$ with r the minimum such that $H_iH_j = H_jH_i$ for any $i, j \in \{r, \dots, n-1, n\}$. Both $\mathcal{L}$ and $\mathcal{R}$, being permutative, are regular (see [18, Lemma 4.1 (1)]). In the extreme case that $\mathcal{H}$ itself is permutative, $\mathcal{L} = \mathcal{R} = \mathcal{H}$. In this case $\mathcal{H}$ is a subgroup, thus easy to treat. In what follows, we consider the case that $\mathcal{H}$ is nonpermutative.

Notation 1.10 $\mathcal{L} \cap \mathcal{R}$ (resp. $\mathcal{L} \cup \mathcal{R}$) denotes the set of common factors in $\mathcal{L}$ and $\mathcal{R}$ (resp. the set of factors contained in $\mathcal{L}$ or $\mathcal{R}$). (*caution*: Here $\mathcal{L}$ and $\mathcal{R}$ are not regarded as subsets of G, and $\mathcal{L} \cap \mathcal{R}$ and $\mathcal{L} \cup \mathcal{R}$ are not set-theoretic intersection and union as subsets of G).

If

$$\mathcal{L} := H_1H_2 \dots H_l \qquad \text{and} \qquad \mathcal{R} := H_rH_{r+1} \dots H_n$$

have no common factor, or equivalently $l < r$, then $\mathcal{L}$ and $\mathcal{R}$ are said *not to intersect*, $\mathcal{L}$ and $\mathcal{R}$ are said *not to intersect*, and $\mathcal{L} \cap \mathcal{R} = \emptyset$. In

this case, $\mathcal{M} := \mathcal{H} \setminus (\mathcal{L} \cup \mathcal{R})$ of $\mathcal{H}$, the *outside of* $\mathcal{L}$ *and* $\mathcal{R}$, is nonempty. This subsect of $\mathcal{H}$ is called the *middle part* of $\mathcal{H}$. Unlike $\mathcal{L}$ and $\mathcal{R}$, it is generally neither permutative nor regular, so it is the complicated part of $\mathcal{H}$. Now $\mathcal{H}$ is decomposed as follows:

$$\mathcal{H} = \underbrace{H_1 H_2 \dots H_l}_{\mathcal{L}} \underbrace{H_{l+1} \dots H_{r-1}}_{\mathcal{M}} \underbrace{H_r H_{r+1} \dots H_n}_{\mathcal{R}}. \tag{1.2}$$

In the case $l + 1 \leqslant r$, $\mathcal{M}$ is empty. In fact:

- If $l + 1 = r$, then $\mathcal{H} = \underbrace{H_1 H_2 \dots H_l}_{\mathcal{L}} \underbrace{H_r H_{r+1} \dots H_n}_{\mathcal{R}}$.
- If $r < l$, then $\mathcal{L} \cap \mathcal{R} \neq \emptyset$ and

$$\underbrace{H_1 H_2 \dots \overbrace{H_r H_{r+1} \dots H_l}^{\mathcal{R}} \dots H_n}_{\mathcal{L}}, \tag{1.3}$$

  where $\mathcal{L} \cap \mathcal{R}$ is the subsect $H_r H_{r+1} \dots H_l$.

Definition 1.11 For a sect $H_1 H_2 \dots H_n$, the set of factors H_i such that $H_i H_j = H_j H_i$ for any $j \in \{1, 2, \dots, n\}$ is called its *central set* and denoted by $\mathcal{CS}$.

Lemma 1.12 *For a sect* $\mathcal{H}$ *with* $\mathcal{L} \cap \mathcal{R} \neq \emptyset$*, any factor of* $\mathcal{L} \cap \mathcal{R}$ *belongs to the central set of* $\mathcal{H}$*.*

Proof — Any factor of $\mathcal{L} \cap \mathcal{R}$ is permutable with any factor of $\mathcal{L}$ and $\mathcal{R}$ (by definition). Now from the assumption $\mathcal{L} \cap \mathcal{R} \neq \emptyset$, we have

$$\mathcal{L} \cup \mathcal{R} = \mathcal{H}$$

(see (1.3)), so any factor of $\mathcal{L} \cap \mathcal{R}$ is permutable with any factor of $\mathcal{H}$, so it is contained in the central set of $\mathcal{H}$. □

As a consequence of Lemma 1.12, the following result holds.

Corollary 1.13 *If the central set of a sect* $\mathcal{H}$ *is empty, then* $\mathcal{L} \cap \mathcal{R} = \emptyset$*.*

For the central set $\mathcal{CS}$ of a sect $\mathcal{H}$, we have $(\mathcal{L} \cap \mathcal{R}) \subset \mathcal{CS}$ (see Lemma 1.12), but in general $\mathcal{L} \cap \mathcal{R} \neq \mathcal{CS}$. In fact even if $\mathcal{L} \cap \mathcal{R} = \emptyset$, possibly $\mathcal{CS} \neq \emptyset$:

Example 1.14 For a sect

$$\mathcal{H} = \underbrace{H_1H_2H_3}_{\mathcal{L}}\, H_4H_5H_6\, \underbrace{H_7H_8}_{\mathcal{R}}$$

such that $H_iH_4 \neq H_4H_i$ $(i = 1,2,3)$ and $H_6H_j \neq H_jH_6$ $(j = 7,8)$, possibly $\mathcal{CS} = \{H_5\}$, while $\mathcal{L} \cap \mathcal{R} = \emptyset$.

Lemma 1.15 *Let $\mathcal{H}$ and $\mathcal{H}'$ be sects of a group with nonempty central sets $\mathcal{CS}$ and $\mathcal{CS}'$ respectively. If a mutation maps $\mathcal{H}$ to $\mathcal{H}'$, then it maps $\mathcal{CS}$ to $\mathcal{CS}'$ bijectively.*

Proof — Noting that a mutation merely permutes factors of a sect, the statement follows from the definition of a central set. □

Remark 1.16 Unlike the central set, a mutation does not necessarily map the left and right permutative parts of a sect to those of another sect.

As a consequence of Lemma 1.15, the following result holds.

Corollary 1.17 *The central set of a sect is preserved under equivalence of sects.*

For a sect $\mathcal{H}$, if $\mathcal{L} \cap \mathcal{R} \neq \emptyset$, that is, $\mathcal{H}$ is of the form in (1.3), then the factors of $\mathcal{L} \cap \mathcal{R} (= H_rH_{r+1} \dots H_l)$ are contained in the central set $\mathcal{CS}$ of $\mathcal{H}$ (see Lemma 1.12). Let $\mathcal{H}'$ be a sect obtained from $\mathcal{H}$ by shifting the factors of $\mathcal{CS}$ to the left of $\mathcal{H}$ — in particular the factors of $H_rH_{r+1} \dots H_l$ are shifted to the left of $\mathcal{H}$, accordingly in the resulting sect $\mathcal{H}'$, its left and right permutative parts $\mathcal{L}'$ and $\mathcal{R}'$ do not intersect: $\mathcal{L}' \cap \mathcal{R}' = \emptyset$. We also point out that since any factor in $\mathcal{CS}$ is permutable with any factor of $\mathcal{H}$, the above operation to shift the factors of $\mathcal{CS}$ is a mutation, so $\mathcal{H}'$ is equivalent to $\mathcal{H}$. Moreover by construction, the central set $\mathcal{CS}'$ of $\mathcal{H}'$ coincides with $\mathcal{CS}$ (and $\mathcal{CS}' \subset \mathcal{L}'$). Based on these observations, we adopt the following convention.

Convention 1.18 (1) For a sect $\mathcal{H}$, let $\{H_{i_1}, H_{i_2}, \dots, H_{i_c}\}$ be its central set if any. Shifting these factors to the left of $\mathcal{H}$, we assume that the central set is $\{H_1, H_2, \dots, H_c\}$ after renumbering if necessarily. This operation does not change the equivalence class of $\mathcal{H}$.

(2) Under (1), without loss of generality, we assume that $\mathcal{L} \cap \mathcal{R} = \emptyset$.

In the notation of Convention 1.18 (1), the subsect $H_1H_2\dots H_c$ of $\mathcal{H}$ is called the *center* of $\mathcal{H}$, and denoted by $\mathcal{C}$:

$$\mathcal{H} = \mathcal{C}H_{c+1}H_{c+2}\dots H_n\ (= H_{c+1}H_{c+2}\dots H_n\mathcal{C}). \tag{1.4}$$

Note that the center $\mathcal{C}$ is permutative, so it is regular (see [18, Lemma 4.1 (1)]).

For a while, we consider a sect $\mathcal{H}$ with nonempty center $\mathcal{C}$ (so the left permutative part $\mathcal{L}$ is nonempty as $\mathcal{C} \subset \mathcal{L}$) and with nonempty right permutative part $\mathcal{R}$.

Lemma 1.19 *If the center $\mathcal{C} = H_1H_2\dots H_c$ of a sect $\mathcal{H} = H_1H_2\dots H_n$ is a proper subsect of $\mathcal{H}$, i.e. $c < n$, then*

(1) $H_{c+1} \in \mathcal{L}$,

(2) $H_{c+1} \notin \mathcal{R}$.

Proof — (1) Since $\mathcal{C}$ is the center of $\mathcal{H}$, we have $H_iH_j = H_jH_i$ for any $H_i \in \mathcal{C}$ and $H_j \in \mathcal{H}$. In particular $H_iH_{c+1} = H_{c+1}H_i$ for any $H_i \in \mathcal{C}$. This means that $H_{c+1} \in \mathcal{L}$.

(2) We show this by contradiction. Suppose that $H_{c+1} \in \mathcal{R}$. This with (1) implies that $\mathcal{L} \cap \mathcal{R}$. Thus $H_{c+1} \in \mathcal{C}$ (see Lemma 1.12), which is contradictory to $\mathcal{C} = H_1H_2\dots H_c$. □

Note next the following result.

Lemma 1.20 *If the center $\mathcal{C} = H_1H_2\dots H_c$ of a sect $\mathcal{H} = H_1H_2\dots H_n$ is a proper subsect of $\mathcal{H}$, i.e. $c < n$, then its complement*

$$\mathcal{D} := H_{c+1}H_{c+2}\dots H_n$$

is not permutative.

Proof — If $\mathcal{D}$ is permutative, then for any H_i ($i = c+1, c+2, \dots, n$), we have

$$H_iH_j = H_jH_i \tag{1.5}$$

for any $H_j \in \mathcal{H}$ (in fact for $H_j \in \mathcal{C}$ this is by the definition of $\mathcal{C}$ and for $H_j \in \mathcal{D}$ by the permutativity assumption of $\mathcal{D}$). However (1.5) implies that $H_i \in \mathcal{C}$, which is contradictory to $H_i \in \mathcal{D}$. □

For a sect $\mathcal{H}$, consider its decomposition $\mathcal{H} = \mathcal{L}\mathcal{M}\mathcal{R}$ into the left permutative part $\mathcal{L}$, the middle part $\mathcal{M}$ and the right permutative part $\mathcal{R}$, where possibly $\mathcal{M} = \emptyset$, but $\mathcal{L} \cap \mathcal{R} = \emptyset$ by Convention 1.18 (2),

and in the case that $\mathcal{H}$ is permutative we adopt the convention that the decomposition is $\mathcal{H} = \mathcal{L}$ with $\mathcal{M} = \mathcal{R} = \emptyset$. There are thus three cases:

Case 1 $\mathcal{M} = \mathcal{R} = \emptyset$:

$$\mathcal{H} = \underbrace{H_1 H_2 \dots H_n}_{\mathcal{L}}. \tag{1.6}$$

Case 2 $\mathcal{M} = \emptyset$:

$$\mathcal{H} = \underbrace{H_1 H_2 \dots H_l}_{\mathcal{L}} \underbrace{H_r H_{r+1} \dots H_n}_{\mathcal{R}}. \tag{1.7}$$

Case 3 $\mathcal{M} \neq \emptyset$:

$$\mathcal{H} = \underbrace{H_1 H_2 \dots H_l}_{\mathcal{L}} \underbrace{H_{l+1} \dots H_{r-1}}_{\mathcal{M}} \underbrace{H_r H_{r+1} \dots H_n}_{\mathcal{R}}. \tag{1.8}$$

Definition 1.21 We refer to $\mathcal{H} = \mathcal{L}\mathcal{M}\mathcal{R}$ as the *canonical decomposition* of $\mathcal{H}$.

Remark 1.22 For a sect $\mathcal{H}$ with nonempty center $\mathcal{C}$, we adopted the convention "the shifting of $\mathcal{C}$ to the left of $\mathcal{L}$" (so $\mathcal{C} \subset \mathcal{L}$). Instead if we adopt the other convention "the shifting of $\mathcal{C}$ to the right of $\mathcal{R}$" (so $\mathcal{C} \subset \mathcal{R}$), then the canonical decomposition of $\mathcal{H}$ differs from the previous one.

We give an example of a canonical decomposition.

Example 1.23 Let $\mathcal{H} := H_1 H_2 H_3$ be a sect of a group G such that H_2 is normal in G, H_1 and H_3 are nonnormal in G, and $H_1 H_3 \neq H_3 H_1$. From the normality of H_2, we have

$$H_1 H_2 = H_2 H_1 \qquad \text{and} \qquad H_2 H_3 = H_3 H_2;$$

these with $H_1 H_3 \neq H_3 H_1$ imply that the central set of $\mathcal{H}$ consists only of H_2. Shift H_2 to the left of $\mathcal{H}$. Then the resulting sect has the following canonical decomposition:

$$\underbrace{H_2 H_1}_{\mathcal{L}} \underbrace{H_3}_{\mathcal{M}}. \tag{1.9}$$

Recall that a sect $\mathcal{H} := H_1 H_2 \dots H_n$ is *tight* if

$$H_1 H_2 \neq H_2 H_1 \qquad \text{and} \qquad H_{n-1} H_n \neq H_n H_{n-1},$$

or equivalently

$$\mathcal{L} = \emptyset \qquad \text{and} \qquad \mathcal{R} = \emptyset$$

(then $\mathcal{C} = \emptyset$ from the convention that $\mathcal{C} \subset \mathcal{L}$). In this case, the canonical decomposition of $\mathcal{H}$ consists only of the middle part, i.e. $\mathcal{H} = \mathcal{M}$. Conversely if $\mathcal{H} = \mathcal{M}$, then $\mathcal{L} = \emptyset$ and $\mathcal{R} = \emptyset$. The following result thus holds.

Lemma 1.24 *A sect $\mathcal{H}$ is tight if and only if its canonical decomposition consists only of the middle part*: $\mathcal{H} = \mathcal{M}$.

We point out that the canonical decomposition $\mathcal{H} = \mathcal{L}\mathcal{M}\mathcal{R}$ of a sect $\mathcal{H}$ may be further divided by subdividing the middle part $\mathcal{M}$ repeatedly. To describe this, it is convenient to write $\mathcal{H} = \mathcal{L}\mathcal{M}\mathcal{R}$ as

$$\mathcal{H} = \mathcal{L}_1\mathcal{M}_1\mathcal{R}_1.$$

If $\mathcal{M}_1 \neq \emptyset$, take its canonical decomposition $\mathcal{M}_1 = \mathcal{L}_2\mathcal{M}_2\mathcal{R}_2$, and substitute it into $\mathcal{H} = \mathcal{L}_1\mathcal{M}_1\mathcal{R}_1$, then

$$\mathcal{H} = \mathcal{L}_1\mathcal{L}_2\mathcal{M}_2\mathcal{R}_2\mathcal{R}_1$$

(if $\mathcal{M}_1 = \emptyset$, we do nothing). Next if $\mathcal{M}_2 \neq \emptyset$, take its canonical decomposition $\mathcal{M}_2 = \mathcal{L}_3\mathcal{M}_3\mathcal{R}_3$, and substitute it into $\mathcal{H} = \mathcal{L}_1\mathcal{L}_2\mathcal{M}_2\mathcal{R}_2\mathcal{R}_1$. Then

$$\mathcal{H} = \mathcal{L}_1\mathcal{L}_2\mathcal{L}_3\mathcal{M}_3\mathcal{R}_3\mathcal{R}_2\mathcal{R}_1.$$

Repeating this procedure until the middle part becomes tight or empty, we obtain the *fine decomposition* of $\mathcal{H}$ with *tight part* $\mathcal{M}_k$ (possibly $\mathcal{M}_k = \emptyset$):

$$\mathcal{H} = \mathcal{L}_1\mathcal{L}_2 \dots \mathcal{L}_k\mathcal{M}_k\mathcal{R}_k \dots \mathcal{R}_2\mathcal{R}_1, \tag{1.10}$$

where $\mathcal{L}_i$ and $\mathcal{R}_i$ ($i = 1, 2, \dots, k$) are called the i*th* left and right permutative parts of $\mathcal{H}$. Note that they are regular [18, Lemma 4.1 (1)]. In the extreme case that $\mathcal{M}_k$ consists of a single factor, i.e. of the form $\mathcal{M}_k = H_i$, the tightness of $\mathcal{M}_k$ is trivial.

Permutators

Let $\mathcal{H} := H_1H_2 \dots H_n$ be a sect. A *permutator* $\mathcal{P}$ of a factor $H_i \in \mathcal{H}$ is a maximal permutative subsect of $\mathcal{H}$ with $H_i \in \mathcal{P}$. This is not necessarily unique — there may exist another permutator $\mathcal{P}'$ with $H_i \in \mathcal{P}'$.

Example 1.25 Let $\mathcal{H} := H_1H_2H_3H_4$ be a sect with

$$H_1H_2 \neq H_2H_1,\ H_2H_3 = H_3H_2,\ H_3H_4 = H_4H_3 \text{ and } H_2H_4 \neq H_4H_2.$$

Then the permutators of factors of $\mathcal{H}$ are

$$\mathcal{P} := H_1,\ \mathcal{Q} := H_2H_3 \quad \text{and} \quad \mathcal{R} := H_3H_4.$$

Here both $\mathcal{Q}$ and $\mathcal{R}$ are permutators of H_3. On the other hand, $\mathcal{P}$ is the permutator of H_1, $\mathcal{Q}$ is the permutator of H_2, and $\mathcal{R}$ is the permutator of H_4.

Let $\mathcal{H} := H_1H_2 \dots H_n$ be a sect. For an "inside" factor H_i $(1 < i < n)$ of $\mathcal{H}$, the non-uniqueness of its permutator (such as that of H_3 in Example 1.25) is due to the existence of both sides of H_i, that is, H_{i-1} and H_{i+1}. In contrast, the end factors H_1 and H_n of $\mathcal{H}$ are one-sided, and their permutators are unique:

- If $H_1H_2 = H_2H_1$, then the permutator of H_1 coincides with the left permutative part $\mathcal{L}$, and otherwise it is H_1 (in this case $\mathcal{L}$ is empty).
- If $H_{n-1}H_n = H_nH_{n-1}$, then the permutator of H_n coincides with the right permutative part $\mathcal{R}$, and otherwise it is H_n (in this case $\mathcal{R}$ is empty).

Cocenters

For a sect $\mathcal{H} := H_1H_2 \dots H_n$ with center $\mathcal{C} := H_1H_2 \dots H_c$ $(c \leqslant n)$, the complement $\mathcal{D} := H_{c+1}H_{c+2} \dots H_n$ of $\mathcal{C}$ in $\mathcal{H}$ is called the *cocenter*, where if $\mathcal{C}$ is the whole of $\mathcal{H}$, then $\mathcal{D} = \emptyset$ and if $\mathcal{C} = \emptyset$, then $\mathcal{D}$ is the whole of $\mathcal{H}$. The decomposition $\mathcal{H} = \mathcal{C}\mathcal{D}$ is called the *center-cocenter decomposition* of $\mathcal{H}$.

Lemma 1.26 *If a sect $\mathcal{H}$ is nonpermutative, then the following hold*:

(1) *Its cocenter $\mathcal{D}$ is not empty.*

(2) *$\mathcal{D}$ is nonpermutative.*

(3) *The center of $\mathcal{D}$ is empty.*

Proof — (1) If $\mathcal{D}$ is empty, then $\mathcal{H} = \mathcal{C}$. In particular $\mathcal{H}$ is permutative, which contradicts the assumption.

(2) From the definition of a center, we have that $\mathcal{C}$ is permutative and any factor $H_i \in \mathcal{C}$ is permutable with any factor $H_j \in \mathcal{D}$, i.e., $H_iH_j = H_jH_i$. Here if $\mathcal{D}$ is permutative, then moreover any two factors of $\mathcal{CD}$ $(= \mathcal{H})$ are permutable, i.e. $\mathcal{H}$ is permutative, which contradicts the assumption.

(3) Suppose that the center of $\mathcal{D}$ is not empty, say, contains a factor H_i; then $H_iH_j = H_jH_i$ for any $H_j \in \mathcal{D}$. Besides, from the definition of the center $\mathcal{C}$ of $\mathcal{H}$, we have $H_iH_k = H_kH_i$ for any $H_k \in \mathcal{C}$. Hence H_i is permutable with any factor of $\mathcal{CD}(= \mathcal{H})$, so $H_i \in \mathcal{C}$, which is contradictory to $H_i \in \mathcal{D}$. □

For the center-cocenter decomposition $\mathcal{H} = \mathcal{CD}$, we cannot further decompose $\mathcal{D}$ into its center and cocenter (note that the former is empty by Lemma 1.26 (3)). In contrast, for the canonical decomposition $\mathcal{H} = \mathcal{LMR}$, we can generally further decompose the middle part $\mathcal{M}$, and obtain the fine decomposition

$$\mathcal{H} = \mathcal{L}_1\mathcal{L}_2 \dots \mathcal{L}_k\mathcal{M}_k\mathcal{R}_k \dots \mathcal{R}_2\mathcal{R}_1$$

(see (1.10)).

Remark 1.27 For two decompositions $\mathcal{H} = \mathcal{CD}$ and $\mathcal{H} = \mathcal{LMR}$, note that $\mathcal{C} \subset \mathcal{L}$ (by Convention 1.18 (1)), so $\mathcal{MR} \subset \mathcal{D}$. Here $\mathcal{D}$ has no center, but $\mathcal{MR} \subset \mathcal{D}$ does *not* necessarily imply that $\mathcal{M}$ and $\mathcal{R}$ have no center.

2 Examples of prime factorizations of finite groups

Let G be a finite *quasi-Dedekind group*, i.e. every subgroup is permutable: $HK = KH$ for any subgroups H and K of G. Notice that if G is not cyclic of prime power order, it has more than one maximal subgroup (see [17, Lemma 3.1]), say $M_1, M_2, \dots, M_n$ $(n \geqslant 2)$ are its maximal subgroups. Then

$$G = M_iM_j$$

for any distinct $i, j \in \{1, 2, \dots, n\}$ and $G = M_iM_j$ is an irredundant factorization (see [17, Proposition 3.6]). Here if M_i and M_j are cyclic

of prime power order, then $G = M_i M_j$ is a prime factorization of G. Hence if G has at least three maximal subgroups that are cyclic of prime power order, then G has at least three (inequivalent) prime factorizations: say that G has such subgroups M_1, M_2, M_3, then

$$G = M_1M_2 = M_1M_3 = M_2M_3$$

are prime factorizations of G, which are mutually inequivalent because a mutation $M_iM_j \to M_jM_i$ does not map M_iM_j to another prime factorization M_kM_l ($\{k,l\} \neq \{i,j\}$). Consequently G is not a unique factorization group (in particular G is not cyclic by [18, Theorem 6.43]). This confirms the following:

Lemma 2.1 *Suppose that* G *is a finite quasi-Dedekind group that is not cyclic of prime power order. If* G *has at least three maximal subgroups that are cyclic of prime power order, then* G *admits at least three* (*inequivalent*) *prime factorizations.*

Remark 2.2 Consider a finite cyclic group G such that its order $|G|$ is not a prime power; let

$$|G| = p_1^{m_1} p_2^{m_2} \dots p_l^{m_l}$$

($l \geqslant 2$) be the prime factorization, then G is a direct product

$$\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \dots \times \mathbb{Z}_{p_l^{m_l}}$$

by the fundamental theorem of finite abelian groups. The number of its maximal subgroups that are cyclic of prime power orders is at most two. Here "two" occurs when $|G| = pq$ for some distinct primes p and q; indeed the maximal subgroups of $G = \mathbb{Z}_p \times \mathbb{Z}_q$ are $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Examples of "one" or "none" are as follows:

(i) One: For $G = \mathbb{Z}_{p^m q} \simeq \mathbb{Z}_{p^m} \times \mathbb{Z}_q$ (where $m \geqslant 2$), its maximal subgroups are $\mathbb{Z}_{p^m} \times \{1\}$ (only this is cyclic of prime power order) and $\mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_q$ (noncyclic).

(ii) None: For $G = \mathbb{Z}_{p^m q^n} \simeq \mathbb{Z}_{p^m} \times \mathbb{Z}_{q^n}$ (where $m, n \geqslant 2$), its maximal subgroups are $\mathbb{Z}_{p^m} \times \mathbb{Z}_{q^{n-1}}$ (noncyclic) and $\mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{q^n}$ (noncyclic).

(iii) None: For $G = \mathbb{Z}_{pqr} \simeq \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$ (where p, q, r are distinct primes), the maximal subgroups are $\mathbb{Z}_p \times \mathbb{Z}_q \times \{1\}$, $\mathbb{Z}_p \times \{1\} \times \mathbb{Z}_r$, and $\{1\} \times \mathbb{Z}_q \times \mathbb{Z}_r$ (all are noncyclic).

Example 2.3 The quaternion group Q_8 is Hamiltonian (i.e. nonabelian Dedekind) and contains three maximal subgroups M_1, M_2, M_3 (which are isomorphic to $\mathbb{Z}_{2^2}$), and $Q_8 = M_1M_2 = M_1M_3 = M_2M_3$. Thus Q_8 is not a UFG.

Example 2.4 The number of prime factorizations of $G = \mathbb{Z}_p \times \mathbb{Z}_p$ is $p(p+1)/2$. In fact G has $p+1$ nontrivial proper subgroups, which are isomorphic to $\mathbb{Z}_p$ and maximal, and the product of each two among them yields a prime factorization of G. To give the $p+1$ subgroups explicitly, instead of $G = \mathbb{Z}_p \times \mathbb{Z}_p$ write $G = \langle x \rangle \times \langle y \rangle$, where x and y are generators of the two $\mathbb{Z}_p$'s. The $p+1$ subgroups are then $\langle x \rangle$, $\langle y \rangle$ and $\langle xy^i \rangle$, where $i = 1, 2, \ldots, p-1$. We remark that $\langle xy^i \rangle = \langle x^{i'} y \rangle$, where i' $(1 \leqslant i' \leqslant p-1)$ is the only integer satisfying $ii' \equiv 1 \bmod p$.

Comparison: Let p and q be distinct primes. Then $\mathbb{Z}_p \times \mathbb{Z}_q$ is isomorphic to a cyclic group $\mathbb{Z}_{pq}$, so it is a UFG [18, Theorem 6.43]. To the contrary, a nontrivial semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is not a UFG (e.g. a dihedral group $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$ with n odd prime; see Example 2.5). Compare the Hasse diagrams in Figure 2.1 of subgroup posets of $\mathbb{Z}_p \times \mathbb{Z}_q$, $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_p \rtimes \mathbb{Z}_q$.

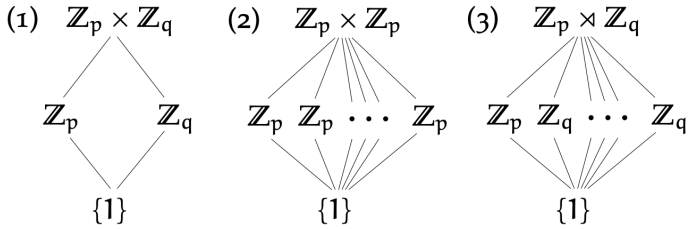


Figure 2.1: (1): $\mathbb{Z}_p \times \mathbb{Z}_q$ $(p \neq q)$ has two maximal subgroups $\mathbb{Z}_p$ and $\mathbb{Z}_q$.
(2): $\mathbb{Z}_p \times \mathbb{Z}_p$ has $p+1$ maximal subgroups $\mathbb{Z}_p$'s.
(3): The semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ has $p+1$ maximal subgroups: one $\mathbb{Z}_p$ and p $\mathbb{Z}_q$'s (see Example 2.5).

Let $G = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_l$ be a prime factorization of a group G. Its *conjugate* by $g \in G$ is

$$gGg^{-1} = g\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_l g^{-1},$$

that is,

$$G = (g\mathfrak{p}_1 g^{-1})(g\mathfrak{p}_2 g^{-1}) \ldots (g\mathfrak{p}_l g^{-1}).$$

Two prime factorizations $G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ and $G = \mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_l$ of a group G are *conjugate* if there exists $g \in G$ that transforms one to the other, that is,

$$G = (g\mathfrak{p}_1g^{-1})(g\mathfrak{p}_2g^{-1})\dots(g\mathfrak{p}_lg^{-1})$$

coincides with $G = \mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_l$; this is equivalent to simultaneous conjugation $g\mathfrak{p}_ig^{-1} = \mathfrak{q}_i$ $(i = 1, 2, \dots, l)$.

Example 2.5 Let n be an integer greater than 2. The dihedral group of degree n is given by

$$D_n = \langle a, b : a^n = b^2 = 1,\ bab^{-1} = a^{-1}\rangle. \tag{2.1}$$

It contains cyclic subgroups $\mathbb{Z}_n := \langle a\rangle$ and $\mathbb{Z}_2 := \langle b\rangle$. Here we have that $\mathbb{Z}_n \cap \mathbb{Z}_2 = \{1\}$, $\mathbb{Z}_n$ is normal in D_n, and D_n is expressed as a semidirect product $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2\ (= \mathbb{Z}_n\mathbb{Z}_2)$, which is a prime factorization of D_n. Still D_n has other prime factorizations. To see this, note that D_n has n cyclic subgroups of order 2:

$$\mathbb{Z}_2^{(i)} := \langle a^ib\rangle$$

$(i = 0, 1, \dots, n-1)$ with $\mathbb{Z}_2^{(0)} = \mathbb{Z}_2 = \langle b\rangle$. Here $\mathbb{Z}_n \cap \mathbb{Z}_2^{(i)} = \{1\}$ for any i, and D_n has semidirect product expressions

$$D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2^{(i)}\ (= \mathbb{Z}_n\mathbb{Z}_2^{(i)})$$

$(i = 0, 1, \dots, n-1)$, thus D_n has n prime factorizations:

$$D_n = \mathbb{Z}_n\mathbb{Z}_2^{(0)} = \mathbb{Z}_n\mathbb{Z}_2^{(1)} = \mathbb{Z}_n\mathbb{Z}_2^{(2)} = \dots = \mathbb{Z}_n\mathbb{Z}_2^{(n-1)}. \tag{2.2}$$

They are mutually inequivalent — there exists no mutation between $\mathbb{Z}_n\mathbb{Z}_2^{(i)}$ and $\mathbb{Z}_n\mathbb{Z}_2^{(j)}$ for distinct i, j, because $\mathbb{Z}_2^{(i)} \neq \mathbb{Z}_2^{(j)}$. We however point out that they may be conjugate — possibly

$$g\mathbb{Z}_n\mathbb{Z}_2^{(i)}g^{-1} = \mathbb{Z}_n\mathbb{Z}_2^{(j)}$$

for some $g \in D_n$ (see Lemma 2.6 (2) below).

Lemma 2.6 *In* Example 2.5, *the following hold*:

(1) (1.a) $a^k\mathbb{Z}_2^{(i)}a^{-k} = \mathbb{Z}_2^{(i+2k)}$ *for any integer* k *and* $i = 0, 1, \dots, n-1$.

(1.b) $b\mathbb{Z}_2^{(i)}b^{-1} = \mathbb{Z}_2^{(n-i)}$ *for* $i = 0, 1, \ldots, n-1$.

(1.c) $(a^k b)\mathbb{Z}_2^{(i)}(a^k b)^{-1} = \mathbb{Z}_2^{(n-i+2k)}$ *for any integer* k *and for any* $i = 0, 1, \ldots, n-1$.

(2) (2.a) *If* n *is odd, all prime factorizations*

$$D_n = \mathbb{Z}_n\mathbb{Z}_2^{(i)}$$

$(i = 0, 1, \ldots, n-1)$ *are conjugate.*

(2.b) *If* n *is even, there are two conjugacy classes of prime factorizations:*

$$\begin{cases} D_n = \mathbb{Z}_n\mathbb{Z}_2^{(i)} & \text{for } i = 0, 2, 4, \ldots, n-2, \\ D_n = \mathbb{Z}_n\mathbb{Z}_2^{(i)} & \text{for } i = 1, 3, 5, \ldots, n-1. \end{cases}$$

Proof — (1) First from $bab^{-1} = a^{-1}$ we have $ba^k b^{-1} = a^{-k}$, so

$$ba^k = a^{-k}b. \tag{2.3}$$

Replacing k with $-k$, we have

$$ba^{-k} = a^k b. \tag{2.4}$$

Then, by (2.4), (1.a) is confirmed as follows:

$$a^k(a^i b)a^{-k} = a^{i+k}ba^{-k} = a^{i+k}a^k ba^{i+2k}b.$$

Next, by (2.3), (1.b) is confirmed as follows:

$$b(a^i b)b^{-1} = ba^i = a^{-i}b = a^{n-i}b \quad \text{as } a^n = 1.$$

Besides (1.c) follows from combining (1.a) and (1.b).

(2) Note first that for any $g \in D_n$, we have

$$g\mathbb{Z}_n\mathbb{Z}_2^{(i)}g^{-1} = (g\mathbb{Z}_n g^{-1})(g\mathbb{Z}_2^{(i)}g^{-1}) = \mathbb{Z}_n(g\mathbb{Z}_2^{(i)}g^{-1})$$

as $\mathbb{Z}_n$ is normal. We thus only have to focus on the conjugates $g\mathbb{Z}_2^{(i)}g^{-1}$ for $g \in D_n$ and investigate when $\mathbb{Z}_2^{(i)}$ and $\mathbb{Z}_2^{(j)}$ are conjugate.

(2.a): It suffices to show that if n is odd, then $\mathbb{Z}_2^{(i)}$ and $\mathbb{Z}_2^{(j)}$ for any i, j are conjugate, for which it suffices to show that

$$j \equiv i + 2k \bmod n$$

for some integer k (indeed then from (1.a), $\mathbb{Z}_2^{(j)} = a^k \mathbb{Z}_2^{(i)} a^{-k}$). If $j - i$ itself is even, this is trivial. If $j - i$ is odd, then $j - i + n$ is even (as n is odd), say $j - i + n = 2k$, then

$$j - i \equiv 2k \bmod n.$$

(2.b): If n is even, then from (1.a), under the conjugations by a^k ($k = 0, 1, \ldots, n-1$), we have that $\mathbb{Z}_2^{(0)}, \mathbb{Z}_2^{(2)}, \ldots, \mathbb{Z}_2^{(n-2)}$ are conjugate and $\mathbb{Z}_2^{(1)}, \mathbb{Z}_2^{(3)}, \ldots, \mathbb{Z}_2^{(n-1)}$ are conjugate. It thus remains to show that $\mathbb{Z}_2^{(i)}$ with even i and $\mathbb{Z}_2^{(j)}$ with odd j are not conjugate under any element of D_n; it suffices to check this only for an element of the form $a^k b$ (as any element of D_n is either of the form a^k or $a^k b$ for some integer k). First

$$(a^k b)\mathbb{Z}_2^{(i)}(a^k b)^{-1} = \mathbb{Z}_2^{(n-i+2k)}$$

(see (1.c)). Here $n - i + 2k$ is a shift of i by an even integer; indeed their difference

$$(n - i + 2k) - i = n - 2i + 2k$$

is even (as n is even). Hence $\mathbb{Z}_2^{(i)}$ with even i cannot be conjugate to $\mathbb{Z}_2^{(j)}$ with odd j. □

Quotient UFGs

Let $K_1 K_2 \ldots K_m$ be a regular sect of a group G, i.e. setting

$$H := K_1 K_2 \ldots K_m,$$

then H is a subgroup of G. The conjugation by $g \in G$ yields

$$gHg^{-1} = (gK_1g^{-1})(gK_2g^{-1}) \ldots (gK_mg^{-1}). \tag{2.5}$$

Here since gK_ig^{-1} ($i = 1, 2, \ldots, m$) are subgroups of G, the right hand side is a sect of G; this is regular (because the left hand side gHg^{-1}

is a subgroup of G). The following result thus holds.

Lemma 2.7 *The conjugation action of a group* G *on the set* $S(G)$ *of sects of* G *maps regular sects to regular sects.*

Recall that the equivalence relation $\sim$ on the set of sects of G is defined via mutation. A mutation of a sect $H_1H_2\dots H_n$ along a regular subsect

$$H_iH_{i+1}\dots H_j$$

($1 \leqslant i < j \leqslant n$) is given by

$$\mu : H_1H_2\dots\underbrace{H_iH_{i+1}\dots H_j}\dots H_n \longrightarrow H_1H_2\dots\underbrace{H_j\dots H_{i+1}H_i}\dots H_n.$$

Its *conjugate mutation* μ^g for $g \in G$ is given as follows (below, we set $H^g := gHg^{-1}$):

$$\mu^g : H_1^gH_2^g\dots\underbrace{H_i^gH_{i+1}^g\dots H_j^g}\dots H_n^g \longrightarrow H_1^gH_2^g\dots\underbrace{H_j^g\dots H_{i+1}^gH_i^g}\dots H_n^g.$$

Thus, for two sects $\mathcal{H}$ and $\mathcal{K}$, if $\mathcal{H} \sim \mathcal{K}$ (say, via a mutation μ), then $\mathcal{H}^g \sim \mathcal{K}^g$ (via μ^g). Hence the conjugation action of G on the set $S(G)$ of sects of G induces an action on the set $S(G)/\sim$ of equivalence classes of sects of G. The following result is thus confirmed.

Proposition 2.8 *The conjugation action of a group* G *on the set* $S(G)$ *of sects of* G *descends to an action on the set* $S(G)/\sim$ *of equivalence classes of sects of* G*, and its quotient* $(S(G)/\sim)/G$ *is defined.*

Recall that a factorization $G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ of a (not necessarily finite) group G is a prime factorization if $\mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ is irredundant and atomic (i.e. every $\mathfrak{p}_i$ ($i = 1, 2, \dots, l$) is atomic). Its conjugate is a factorization

$$G = \mathfrak{p}_1^g\mathfrak{p}_2^g\dots\mathfrak{p}_l^g,$$

which is also a prime factorization; indeed note that it is irredundant (see [18, Lemma 5.16]) and atomic (see [18, Lemma 5.17]). Hence the following result holds.

Lemma 2.9 *The conjugation action of a group* G *maps prime factorizations of* G *to prime factorizations of* G: $g \in G$ *maps a prime factorization*

$$G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$$

to a prime factorization

$$G = \mathfrak{p}_1^g \mathfrak{p}_2^g \dots \mathfrak{p}_l^g.$$

Example 2.10 The symmetric group $\mathfrak{S}_3$ has four nontrivial proper subgroups: three nonnormal subgroups $H_k \simeq \mathbb{Z}_2$ ($k = 1,2,3$) generated by a transposition $(i\,j)$, where $i,j \in \{1,2,3\}$ is distinct from k, and one normal subgroup $N \simeq \mathbb{Z}_3$ generated by a cyclic permutation $(1\,2\,3)$. Following [17, Example 2.18], the prime factorizations of $\mathfrak{S}_3$ are as follows:

$$\mathfrak{S}_3 = \begin{cases} H_i H_j H_k & (\text{distinct } i,j,k \in \{1,2,3\}), \\ H_i H_j H_i & (\text{distinct } i,j \in \{1,2,3\}), \\ H_i N\,(= N H_i) & (i = 1,2,3). \end{cases} \tag{2.6}$$

Observe that the number of sects $H_i H_j H_k$ (distinct $i,j,k \in \{1,2,3\}$) is $3! = 6$. Yet since $H_i H_j H_k$ is a group, $H_i H_j H_k \sim H_k H_j H_i$ by the definition of equivalence, so the number of equivalence classes of $H_i H_j H_k$ (distinct $i,j,k \in \{1,2,3\}$) is $6/2 = 3$. The total number of equivalence classes in (2.6) is thus $3+3+3 = 9$. We next claim that the number of conjugacy classes of prime factorizations of $\mathfrak{S}_3$ is only 3 with representatives given by

$$\mathfrak{S}_3 = \begin{cases} H_1 H_2 H_3, \\ H_1 H_2 H_1, \\ H_1 N\,(= N H_1). \end{cases} \tag{2.7}$$

This follows from the following: for $\sigma \in \mathfrak{S}_3$, we have

$$\sigma H_1 H_2 H_3 \sigma^{-1} = H_{\sigma(1)} H_{\sigma(2)} H_{\sigma(3)}$$

(see Remark 2.11 below). Hence any $H_i H_j H_k$ (distinct $i,j,k \in \{1,2,3\}$) is conjugate to $H_1 H_2 H_3$. Similarly

$$\sigma H_1 H_2 H_1 \sigma^{-1} = H_{\sigma(1)} H_{\sigma(2)} H_{\sigma(1)},$$

and any $H_i H_j H_i$ (distinct $i,j \in \{1,2,3\}$) is conjugate to $H_1 H_2 H_1$.

Remark 2.11 Let $\mathfrak{S}_3$ act on $1,2,3$ by permutation. Then the above subgroup H_k of $\mathfrak{S}_3$ is the stabilizer of $k \in \{1,2,3\}$. Thus for any $\sigma \in \mathfrak{S}_3$,

we have $\sigma H_k \sigma^{-1} = H_{\sigma(k)}$ (the stabilizer of $\sigma(k)$ is conjugate to the stabilizer of k). Consequently the conjugation by σ induces a permutation

$$H_1, H_2, H_3 \mapsto H_{\sigma(1)}, H_{\sigma(2)}, H_{\sigma(3)}.$$

Hence

$$\begin{aligned} \sigma H_1 H_2 H_3 \sigma^{-1} &= (\sigma H_1 \sigma^{-1})(\sigma H_2 \sigma^{-1})(\sigma H_3 \sigma^{-1}) \\ &= H_{\sigma(1)} H_{\sigma(2)} H_{\sigma(3)}. \end{aligned} \tag{2.8}$$

Let $\mathrm{PF}(G)$ be the set of prime factorizations of a group G, and consider the conjugation action of G on it: $g \in G$ maps a prime factorization

$$G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_l$$

to a prime factorization

$$G = \mathfrak{p}_1^g \mathfrak{p}_2^g \dots \mathfrak{p}_l^g$$

(see Lemma 2.9). Now let

$$\mathrm{PF}(G)/\sim$$

be the set of equivalence classes of prime factorizations of G. Note that $\mathrm{PF}(G)/\sim$ is a singleton if and only if G is a unique factorization group.

Proposition 2.12 *The conjugation action of* G *on the set* $\mathrm{PF}(G)$ *of prime factorizations of* G *descends to an action on* $\mathrm{PF}(G)/\sim$*, and the quotient*

$$(\mathrm{PF}(G)/\sim)/G$$

is defined.

Proof — This is shown in the same way as Proposition 2.8. □

Definition 2.13 A group G is a *conjugation-quotient UFG* if

$$(\mathrm{PF}(G)/\sim)/G$$

is a singleton.

Example 2.14 In Lemma 2.1, if M_1, M_2, M_3 are normal (e.g. when G is Dedekind), the factorizations

$$G = M_1 M_2 = M_2 M_3 = M_1 M_3$$

are not conjugate (indeed for any $g \in G$,

$$gM_ig^{-1} = (gM_ig^{-1})(gM_jg^{-1}) = M_iM_j$$

by the normality of M_i and M_j). Hence such G is not a conjugation-quotient UFG. For example, Q_8 is not a conjugation-quotient UFG.

For *abelian* groups, conjugations are trivial operations, so "conjugationquotient UFG" coincides with "UFG"; in the case of finite groups, UFG's are cyclic groups (see [18, Theorem 6.43]). Thus a finite abelian group is a conjugation-quotient UFG if and only if it is cyclic. *Does there exist a nonabelian finite group that is a conjugation-quotient UFG?*

2.1 Ramification of prime factorizations of finite groups

An irredundant sect $H_1H_2 \dots H_n$ of a group G is *unramified* if the groups $H_1, H_2, \dots, H_n$ are distinct; notice that this is for example the case when $H_iH_j = H_jH_i$ for any $i, j \in \{1, 2, \dots, n\}$ (see [17, Corollary 2.14]), in particular when $H_1, H_2, \dots, H_n$ are permutable subgroups (e.g. normal subgroups) of G — this is always the case for subgroups of quasi-Dedekind groups (e.g. abelian groups), and the following result holds.

Lemma 2.15 *If G is a quasi-Dedekind group (in particular an abelian group), then any irredundant sect of G is unramified.*

The factorization version of unramifiedness is as follows: An irredundant factorization $G = H_1H_2 \dots H_n$ of a group G is *unramified* if

$$H_1H_2 \dots H_n$$

is unramified. From Lemma 2.16, the following result holds.

Theorem 2.16 *If G is a quasi-Dedekind group, then any irredundant factorization (in particular any prime factorization) of G is unramified.*

Since abelian groups are quasi-Dedekind, their prime factorizations are always unramified. In contrast, a prime factorization of a nonabelian group may be ramified:

Example 2.17 For the symmetric group $\mathfrak{S}_3$ of degree 3, let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be its cyclic subgroups of order two generated by transpositions $(1\,2)$ and $(2\,3)$ respectively. Then $\mathfrak{S}_3 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_1$ (by computation), which is a ramified prime factorization.

The automorphism group $\mathrm{Aut}(G)$ of a group G acts on sects of G as in the result below.

Lemma 2.18 *For $\sigma \in \mathrm{Aut}(G)$ and a sect $H_1H_2\dots H_n$ of G,*

$$\sigma(H_1H_2\dots H_n) = \sigma(H_1)\sigma(H_2)\dots\sigma(H_n). \tag{2.9}$$

Proof — Since $\sigma \in \mathrm{Aut}(G)$, for $h_1h_2\dots h_n \in H_1H_2\dots H_n$ where $h_i \in H_i$ $(i = 1, 2, \dots, n)$ we have

$$\sigma(h_1h_2\dots h_n) = \sigma(h_1)\sigma(h_2)\dots\sigma(h_n).$$

Thus

$$\begin{aligned}\sigma(H_1H_2\dots H_n) &= \left\{\sigma(h_1h_2\dots h_n) \,:\, h_i \in H_i\,(i = 1, 2, \dots, n)\right\}\\ &= \left\{\sigma(h_1)\sigma(h_2)\dots\sigma(h_n) \,:\, h_i \in H_i\,(i = 1, 2, \dots, n)\right\}\\ &= \sigma(H_1)\sigma(H_2)\dots\sigma(H_n).\end{aligned}$$

Therefore the proof is complete. □

Remark 2.19 We point out that Lemma 2.18 ensures that $\sigma \in \mathrm{Aut}(G)$ is a monoid-homomorphism (indeed a monoid-automorphism) of the sect monoid $S(G)$ of G.

Lemma 2.20 *Let $K_1K_2\dots K_m$ be a regular sect of a group G. Then for any $\sigma \in \mathrm{Aut}(G)$, its image $\sigma(K_1K_2\dots K_m)$, or $\sigma(K_1)\sigma(K_2)\dots\sigma(K_m)$ (by* Lemma 2.18*), is a regular sect of G.*

Proof — Set $H := K_1K_2\dots K_m$ (which is a subgroup of G by hypothesis). Then $\sigma(H) = \sigma(K_1K_2\dots K_m)$, so $\sigma(H) = \sigma(K_1)\sigma(K_2)\dots\sigma(K_m)$ by Lemma 2.18. Here since σ is an automorphism, $\sigma(H)$ is a subgroup of G, so $\sigma(K_1)\sigma(K_2)\dots\sigma(K_m)$ is a regular sect of G. □

For simplicity, we set $H^\sigma := \sigma(H)$. For a sect $H_1H_2\dots H_n$ with a regular subsect $H_iH_{i+1}\dots H_j$ $(1 \leqslant i < j \leqslant n)$, the mutation with respect to $H_iH_{i+1}\dots H_j$ is given by

$$\begin{aligned}\mu : H_1H_2\dots &\underbrace{H_iH_{i+1}\dots H_j}\dots H_n\\ &\longrightarrow H_1H_2\dots \underbrace{H_j\dots H_{i+1}H_i}\dots H_n.\end{aligned} \tag{2.10}$$

Then $\sigma \in \mathrm{Aut}(G)$ induces a mutation μ^σ given by

$$\begin{aligned} \mu^\sigma : H_1^\sigma H_2^\sigma \dots \underbrace{H_i^\sigma H_{i+1}^\sigma \dots H_j^\sigma} \dots H_n^\sigma \\ \longrightarrow H_1^\sigma H_2^\sigma \dots \underbrace{H_j^\sigma \dots H_{i+1}^\sigma H_i^\sigma} \dots H_n^\sigma. \end{aligned} \tag{2.11}$$

Consequently: *For two sects $\mathcal{H}$ and $\mathcal{K}$ of a group G, if $\mathcal{H} \sim \mathcal{K}$, then*

$$\mathcal{H}^\sigma \sim \mathcal{K}^\sigma$$

for any $\sigma \in \mathrm{Aut}(G)$. Hence the action of $\mathrm{Aut}(G)$ on $S(G)$ descends to $S(G)/\!\sim$, and its quotient $(S(G)/\!\sim)/\mathrm{Aut}(G)$ is defined.

We shall show that $\mathrm{Aut}(G)$ maps prime factorizations to prime factorizations. To that end, note the following result.

Lemma 2.21 *Let G be a group. Then the following hold*:

(1) *Irredundancy of a sect of G is preserved under the action of $\mathrm{Aut}(G)$.*

(2) *Atomicity of a subgroup of G is preserved under the action of $\mathrm{Aut}(G)$. In fact for any $\sigma \in \mathrm{Aut}(G)$, a subgroup H of G is atomic if and only if H^σ $(:= \sigma(H))$ is atomic.*

Proof — (1) Let $H_1 H_2 \dots H_n$ be an irredundant sect of G. We show that for any $\sigma \in \mathrm{Aut}(G)$, its image $H_1^\sigma H_2^\sigma \dots H_n^\sigma$ is irredundant. Otherwise

$$H_1^\sigma H_2^\sigma \dots H_n^\sigma = H_1^\sigma H_2^\sigma \dots \widetilde{H_i^\sigma} \dots H_n^\sigma \tag{2.12}$$

for some i. Applying σ^{-1} to this yields

$$H_1 H_2 \dots H_n = H_1 H_2 \dots \widetilde{H}_i \dots H_n,$$

which contradicts the irredundancy of $H_1 H_2 \dots H_n$.

(2) We show "$\Longrightarrow$" by contradiction. If H^σ is not atomic, then it admits a nontrivial irredundant factorization, say

$$H^\sigma = K_1 K_2 \dots K_m$$

$(m \geqslant 2)$. Applying σ^{-1} to this yields

$$H = K_1^{\sigma^{-1}} K_2^{\sigma^{-1}} \dots K_m^{\sigma^{-1}},$$

which is irredundant by (1), so gives a nontrivial irredundant factorization of H. This contradicts the atomicity of H. Thus we obtain that "$\Longrightarrow$" is confirmed. Similarly "$\Longleftarrow$" is confirmed by interchanging the roles of H and H^σ and the roles of σ and σ^{-1}. □

Let $G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ be a prime factorization, i.e. $\mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ is irredundant and every factor $\mathfrak{p}_i$ is atomic. From Lemma 2.21, we have that, for any $\sigma \in \mathrm{Aut}(G)$, its image $G = \mathfrak{p}_1^\sigma\mathfrak{p}_2^\sigma\dots\mathfrak{p}_l^\sigma$ is also a prime factorization of G, and the following result is obtained.

Corollary 2.22 *The automorphism group of* $\mathrm{Aut}(G)$ *of a group* G *maps prime factorizations of* G *to prime factorizations of* G*:* $\sigma \in \mathrm{Aut}(G)$ *maps a prime factorization* $G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ *to a prime factorization*

$$G = \mathfrak{p}_1^\sigma\mathfrak{p}_2^\sigma\dots\mathfrak{p}_l^\sigma.$$

Furthermore the following result holds.

Lemma 2.23 *If two prime factorizations are equivalent, then their images under* $\sigma \in \mathrm{Aut}(G)$ *are also equivalent.*

Proof — As described in (2.10) and (2.11), $\sigma \in \mathrm{Aut}(G)$ transforms a mutation between two prime factorizations to a mutation between their images under σ. The assertion thus follows. □

The automorphism group $\mathrm{Aut}(G)$ of a group G naturally acts on the set $\mathrm{PF}(G)$ of prime factorizations of G: $\sigma \in \mathrm{Aut}(G)$ maps a prime factorization $G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ to $G = \mathfrak{p}_1^\sigma\mathfrak{p}_2^\sigma\dots\mathfrak{p}_l^\sigma$ (see Corollary 2.22). This action preserves the equivalence relation $\sim$ on prime factorizations of G see (Lemma 2.23). Thus the action of $\mathrm{Aut}(G)$ on $\mathrm{PF}(G)$ descends to $\mathrm{PF}(G)/\sim$, and the quotient $(\mathrm{PF}(G)/\sim)/\mathrm{Aut}(G)$ is defined. If $(\mathrm{PF}(G)/\sim)/\mathrm{Aut}(G)$ is a singleton, then G is called an *Aut-quotient UFG*. *Does there exist a noncyclic finite abelian group that is an Aut-quotient UFG?*

Remark 2.24 For abelian groups, their conjugation actions are trivial, so the concept "conjugation-quotient UFG" coincides with "UFG". In contrast the automorphism groups of abelian groups are generally nontrivial, and the concept "Aut-quotient UFG" is different from "conjugation-quotient UFG".

REFERENCES

[1] S.H. Alavi – C.E. Praeger: "On triple factorisations of finite groups", *J. Group Theory* 14 (2011), 341–360.

[2] B. Amberg – S. Franciosi – F. de Giovanni: "Products of Groups", *Clarendon*, Oxford (1993).

[3] B. Amberg – L. Kazarin: "Factorizations of groups and related topics", *Sci. China Ser. A* 52 (2009), 217–230.

[4] A. Ballester-Bolinches – R. Esteban-Romero – M. Asaad: "Products of Finite Groups", *de Gruyter*, Berlin (2010).

[5] V. Božović – N. Pace: "On group factorizations using free mappings", *J. Algebra Appl.* 7 (2008), 647–662.

[6] K. Conrad: "Subgroups of cyclic groups";
url:`https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicgp.pdf`

[7] K. Corrádi – S. Szabó: "Factoring a finite abelian group by prime complexes", *Math. Pannon.* 16 (2005), 79–94.

[8] D. Gorenstein: "On finite groups of the form ABA", *Canadian J. Math.* 14 (1962), 195–236.

[9] M.M. Guterman: "On ABA-groups of finite order", *Trans. Amer. Math. Soc.* 139 (1969), 109–143.

[10] R. Hirakawa – K. Sasaki – S. Takamura: "Poset-blowdowns of generalized quaternion groups", *Int. J. Group Theory* 13 (2024), 133–160.

[11] R.R. Khazal: "A note on minimal and maximal subgroups in a finite group", *J. Univ. Kuwait* (*Sci.*) 16 (1989), 229–236.

[12] H. Kurzweil – B. Stellmacher: "The Theory of Finite Groups", *Springer*, New York (2004).

[13] O.U. Lenz: "The Classifying Space of a Monoid", Master thesis, *University of Leiden* (2011);
url: `www.universiteitleiden.nl/binaries/content/assets/science/mi/scripties/lenzmaster.pdf`

[14] H.E. Rose: "A Course on Finite Groups", *Springer*, London (2010).

[15] S. Takamura: "Classification of finite groups with birdcage-shaped Hasse diagrams", *Osaka J. Math.* 58 (2021), 885–897.

[16] S. Takamura: "Blowdown maps between subgroup posets", *Tokyo J. of Math.* 45 (2022), 467–499.

[17] S. Takamura: "Prime Factorizations of Finite Groups, I", *Adv. Group Theory Appl.* 19 (2024), 1–55.

[18] S. Takamura: "Prime Factorizations of Finite Groups, II", *Adv. Group Theory Appl.* 21 (2025), 11–109.

[19] M. Tărnăuceanu: "Finite groups with many isolated subgroups", (2021); *arXiv*:2111.14015.

[20] H. Zassenhaus: "The Theory of Groups", *Chelsea*, New York (1949).

Shigeru Takamura
Department of Mathematics
Kyoto University
Kitashirakawa Oiwake-cho
606-8502 Sakyo-ku, Kyoto (Japan)
e-mail: takamura@math.kyoto-u.ac.jp