

Advances in Group Theory and Applications
© 2024 AGTA - www.advgrouptheory.com/journal
19 (2024), pp. 1–55 ISSN: 2499-1287
DOI: 10.32037/agta-2024-007

Prime Factorizations of Finite Groups, I *

S. Takamura

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

Abstract

In this and two consecutive papers, we develop a theory of prime factorizations of groups. We first introduce the notion of prime factorizations of a group, which naturally generalizes the factorization of a finite abelian group given by the fundamental theorem of finite abelian groups. We then define an equivalence relation on them in terms of an operation "mutation". We show that any finite group admits a prime factorization, which is generally not unique — a group with a unique prime factorization (up to equivalence) is called a *unique factorization group* (UFG). We completely classify finite UFGs: A finite group is a UFG if and only if it is cyclic, and a finite group admits *no* nontrivial prime factorization if and only if it is cyclic of prime power order. We also develop methods to construct from prime factorizations of a group, inequivalent prime factorizations of the group. Moreover we provide examples of prime factorizations of groups.

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

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

Contents

1 Introduction 2
2 Preparation: Sects and sect monoids 9
2.1 Irredundancy of sects 12

* 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.

2.2 Irredundantization of sects 14
2.3 Finiteness on irredundant sects of finite groups . . . 18
3 Prime factorizations of groups 20
3.1 Mutation and equivalence of sects 26
3.2 Mutation and irredundancy 30
4 Pushforward and pullback of sects 34
4.1 Pushforward and pullback of mutations 41
4.2 Refinement and irreducibility of sects 44
4.3 Pullback of prime factorizations 48
References 54

1 Introduction

The present paper is the foremost of a three-paper work that will appear on this journal (see [17] and [18]).

Historically, factorizations $G = H_1H_2$ of a group G into *two* subgroups H_1 and H_2, where $H_1H_2 := \{h_1h_2 : h_1 \in H_1, h_2 \in H_2\}$, were considered as a generalization of semidirect products, and have been long studied. See [2] and [3] for development. Factorizations of the form $G = H_1H_2H_1$ were also classically studied, e.g., [8], [9], and a recent work [1]. In this paper, we study factorizations

$$G = H_1H_2 \dots H_n$$

of arbitrary length $n \geqslant 2$; we even study subgroup products

$$H_1H_2 \dots H_n$$

that do not give factorizations of groups — this helps characterizing factorizations of groups. Among factorizations of groups, we are concerned with prime ones (to be formulated below); they naturally generalize the factorizations of finite abelian groups given by the fundamental theorem of finite abelian groups. We describe their properties and classify finite groups with only one prime factorization "up to equivalence" — to introduce an appropriate equivalence relation on prime factorizations is one of essential ingredients in our work.

Remark 1.1 Recently in light of application to cryptography, another kind of factorizations of finite groups (factorizations into special subsets of groups) are also studied, e.g. [5], [7].

We begin with our motivation in a wider context. Given a generating set

$$\gamma_1, \gamma_2, \ldots, \gamma_n$$

of a finite group G, any element g of G is expressed in $\gamma_1, \gamma_2, \ldots, \gamma_n$. Yet in general, generators $\gamma_1, \gamma_2, \ldots, \gamma_n$ may not appear in this order (such as $g = \gamma_3^4\gamma_1^2\gamma_5^3\gamma_2$). In other words, $\gamma_1, \gamma_2, \ldots, \gamma_n$ are generally *unordered* generators of G. In contrast, if any element g of G is written in the form $g = \gamma_1^{m_1}\gamma_2^{m_2}\ldots\gamma_n^{m_n}$ with m_i $(i = 1, 2, \ldots, n)$ integers, then $\gamma_1, \gamma_2, \ldots, \gamma_n$ are *ordered* generators, which we call *creators* of G (in the case of abelian G, there is no difference between generators and creators). More invariantly, creators $\gamma_1, \gamma_2, \ldots, \gamma_n$ are characterized as follows:

Let H_i $(i = 1, 2, \ldots, n)$ *be the cyclic subgroup of* G *generated by* γ_i*, then the following holds*:

$$G = H_1 H_2 \ldots H_n, \tag{1.1}$$

where the right hand side is

$$\{h_1 h_2 \ldots h_n : h_i \in H_i \ (i = 1, 2, \ldots, n)\}.$$

Note that (1.1) means that any element g of G is expressed in the form $g = h_1 h_2 \ldots h_n$, that is,

$$g = \gamma_1^{m_1}\gamma_2^{m_2}\cdots\gamma_n^{m_n}$$

for some integers m_i $(i = 1, 2, \ldots, n)$. We point out that for a group action of G on a set X, this expression can be used for describing the intermediate process of the action: $x \in X \mapsto gx \in X$ is "interpolated" by a composition

$$x \longmapsto h_n x \longmapsto \ldots \longmapsto h_2 h_3 \ldots h_n x \longmapsto h_1 h_2 \ldots h_n x \,(= gx). \tag{1.2}$$

Besides, the orbit Gx of x is given by

$$\left\{\gamma_1^{m_1}\gamma_2^{m_2}\ldots\gamma_n^{m_n}x \,:\, m_i \in \mathbb{N}_i \ (i = 1, 2, \ldots, n)\right\},$$

where $\mathbb{N}_i = \{1, 2, \ldots, \mathrm{ord}(\gamma_i)\}$ with $\mathrm{ord}(\gamma_i)$ the order of γ_i. Thus Gx is parametrized by $(m_1, m_2, \ldots, m_n) \in \mathbb{N}_1 \times \mathbb{N}_2 \times \ldots \times \mathbb{N}_n$.

We now proceed to a general setup for factorizations of groups. Let H_i be a (not necessarily cyclic) subgroup of a group G, and consider a subset of G given by

$$H_1H_2\dots H_n := \{h_1h_2\dots h_n \,:\, h_i \in H_i\,(i=1,2,\dots,n)\}, \tag{1.3}$$

which is called a *sect* of G. This is generally not a subgroup of G. If this is equal to G, then $G = H_1H_2\dots H_n$ is called a *factorization* of G of *length* n. A basic example is a factorization of a finite abelian group given by the fundamental theorem of finite abelian groups (*caution*: In general a finite abelian group has other factorizations, see, for instance, [17, Lemma 6.6]). In the spirit of factorizations, a generalization of abelian groups is a *factorized group* — a group G with a factorization $G = H_1H_2\dots H_n$ such that

$$H_iH_j = H_jH_i \quad \text{for any } i,j \in \{1,2,\dots,n\}.$$

See [4] for properties of factorized groups. In this case, the factorization $G = H_1H_2\dots H_n$ is said to be *permutative*.

We point out that besides the trivial factorization ($G = G$), there are uninteresting factorizations, such as

$$G = GG,\ G = GGG,\ G = GGGG,$$

and so on. These factorizations are simply obtained from $G = G$ by multiplying G from the right successively; in other words, the Gs on the right hand sides are, except for one G, unnecessary — in this sense these factorizations are redundant. A less nontrivial redundant factorization is $G = H_1H_2H_3$ such that $H_1 \subset H_2$; this condition implies $H_1H_2 = H_2$, so $G = H_1H_2H_3$ reduces to $G = H_2H_3$ (i.e. H_1 is redundant in $H_1H_2H_3$). More generally, a sect $H_1H_2\dots H_n$ is *redundant* if the removal of some factor H_i causes no effect, i.e.

$$H_1H_2\dots\breve{H}_i\dots H_n = H_1H_2\dots H_n \quad \text{(as subsets of } G), \tag{1.4}$$

where $\breve{H}_i$ signifies the removal of H_i. On the other hand $H_1H_2\dots H_n$ is *irredundant* if

$$H_1H_2\dots\breve{H}_i\dots H_n \subsetneq H_1H_2\dots H_n \quad \text{for any } i = 1,2,\dots,n. \tag{1.5}$$

Finally, a factorization $G = H_1H_2\dots H_n$ is said to be *(ir)redundant*

if $H_1H_2\dots H_n$ is (ir)redundant. We mainly focus on irredundant factorizations.

If a (nonidentity) group admits only the trivial factorization, then the group is called *atomic*. An irredundant factorization of a group into atomic subgroups is called a *prime factorization* of the group. We show that a finite group is atomic if and only if it is a cyclic group of prime power order (Theorem 3.13) and that any finite group admits a prime factorization (Theorem 3.16).

Remark 1.2 For infinite groups, the situation is different. For instance, the additive group $\mathbb{Z}$ of integers has *no* atomic subgroup — any subgroup of $\mathbb{Z}$ admits a nontrivial irredundant factorization (Proposition 3.17). Thus $\mathbb{Z}$ cannot have a prime factorization.

Equivalence relation on factorizations of groups

Naively, a *unique factorization group* (UFG) is a group with only one prime factorization. This however does not make much sense as it is — for instance if a factorization $G = H_1H_2\dots H_n$ is permutative, i.e., $H_iH_j = H_jH_i$ for any $i,j \in \{1,2,\dots,n\}$, then we may freely change the order of the factors $H_1, H_2, \dots, H_n$ in $G = H_1H_2\dots H_n$, but we do not want to distinguish the resulting factorizations, just as for the prime factorization of an integer. Although a factorization $G = H_1H_2\dots H_n$ is not permutative, if some adjacent factors are permutable, say $H_iH_{i+1} = H_{i+1}H_i$, then we may replace H_iH_{i+1} in $G = H_1H_2\dots H_n$ with $H_{i+1}H_i$, obtaining a factorization

$$G = H_1H_2\dots H_{i+1}H_i\dots H_n.$$

We however do not want to distinguish this and $G = H_1H_2\dots H_n$.

The above construction of a "new" factorization obtained starting from $G = H_1H_2\dots H_n$ involves an artificial condition

$$H_iH_{i+1} = H_{i+1}H_i.$$

Actually, there is another construction which is free from any condition and works for *any* factorization $G = H_1H_2\dots H_n$: First take the inverse, that is, $G^{-1} = H_n^{-1}\dots H_2^{-1}H_1^{-1}$. Here,

$$G^{-1} = G \quad \text{and} \quad H_i^{-1} = H_i \quad (i = 1,2,\dots,n)$$

by the invertibility of groups, thus $G = H_n \dots H_2 H_1$, which is generally different from $G = H_1 H_2 \dots H_n$ (except for the "symmetric" case, e.g., $G = H_1 H_2 H_3 H_2 H_1$). We however do not want to distinguish $G = H_n \dots H_2 H_1$ and $G = H_1 H_2 \dots H_n$; otherwise the notion of a unique factorization group does not make much sense. We thus intend to define an equivalent relation $\sim$ on factorizations of a group G such that:

(a) If $H_i H_{i+1} = H_{i+1} H_i$, then

$$G = H_1 H_2 \dots H_i H_{i+1} \dots H_n \sim G = H_1 H_2 \dots H_{i+1} H_i \dots H_n.$$

(b) $G = H_1 H_2 \dots H_n \sim G = H_n \dots H_2 H_1$.

How can we define an equivalence relation on factorizations of G *that unifies* (a) *and* (b)*?*

A hint is that in (a) and (b), the parts to be reversed, $H_i H_{i+1}$ and $H_1 H_2 \dots H_n$, are both subgroups of G — this is obvious for the latter as $G = H_1 H_2 \dots H_n$ and for the former, this follows from the fact that $H_i H_{i+1} = H_{i+1} H_i$ is equivalent to $H_i H_{i+1}$ being a subgroup of G (see Corollary 2.6). We generalize (a) and (b) *uniformly* in light of the following observation: If a subsect

$$H_i H_{i+1} \dots H_j \quad (1 \leqslant i < j \leqslant n)$$

of a sect $H_1 H_2 \dots H_n$ is equal to a subgroup of G, then

$$H_i H_{i+1} \dots H_j = H_j \dots H_{i+1} H_i$$

(see Lemma 2.2), thus $H_i H_{i+1} \dots H_j$ in $G = H_1 H_2 \dots H_n$ may be replaced with its reverse $H_j \dots H_{i+1} H_i$, so

$$G = H_1 H_2 \dots H_j \dots H_{i+1} H_i \dots H_n. \tag{1.6}$$

This is a common generalization of the reversed factorizations in (a) and (b). Based on this, we define an equivalence relation on factorizations of G as follows: *If* $H_1 H_2 \dots H_n$ *contains a subsect* $H_i H_{i+1} \dots H_j$ *that is equal to a subgroup of* G*, then*

$$\begin{aligned} G &= H_1 H_2 \dots H_i H_{i+1} \dots H_j \dots H_n \\ &\sim H_1 H_2 \dots H_j \dots H_{i+1} H_i \dots H_n = G. \end{aligned}$$

The morphism associated with this equivalence, i.e.

$$H_1H_2\dots H_iH_{i+1}\dots H_j\dots H_n \longrightarrow H_1H_2\dots H_j\dots H_{i+1}H_i\dots H_n$$

is called a *mutation along* $H_iH_{i+1}\dots H_j$. The *identity mutation* is just

$$H_1H_2\dots H_n \to H_1H_2\dots H_n$$

which is the morphism associated with the reflexive law

$$G = H_1H_2\dots H_n \sim G = H_1H_2\dots H_n.$$

We now adopt the following definition: A group with a unique prime factorization "up to equivalence" is a *unique factorization group* (UFG). We completely classify finite UFGs: A finite group is a UFG if and only if it is cyclic (see [17, Theorem 10.43]). For a cyclic group G of order n with prime factorization $n = p_1^{m_1}p_2^{m_2}\dots p_l^{m_l}$, its unique prime factorization is $G = \mathbb{Z}_{p_1^{m_1}}\mathbb{Z}_{p_2^{m_2}}\dots\mathbb{Z}_{p_l^{m_l}}$.

Noncyclic finite abelian groups are not UFGs and also finite *non* abelian groups are not UFGs.

Example 1.3 A direct product $G = \mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n}$ of cyclic groups of prime power orders p^m and p^n has (at least) $m + n + 1$ prime factorizations (see [17, Lemma 6.6]), where some of them are *not* direct products (see [17, Lemma 6.7]). For a nonabelian example, the quaternion group Q_8 has three prime factorizations

$$Q_8 = M_1M_2 = M_1M_3 = M_2M_3$$

(see [18, Example 12.3]), where M_1, M_2 an M_3 are maximal subgroups of Q_8 (they are isomorphic to $\mathbb{Z}_4$). Section 12 of [18] provides more examples of prime factorizations of finite groups.

For a finite abelian group G, there is a subtle difference between a prime factorization of G in our sense and the prime factorization of G given by the fundamental theorem of finite abelian groups. In the latter, G is *isomorphic* to a *direct product* of cyclic groups of prime power orders, whereas in the former, the factorization of G is *equal* to a sect — *not necessarily a direct product* — composed of cyclic subgroups of prime power orders. As such, our prime factorization is more affected by the internal structure of G — *how cyclic subgroups of prime power orders are located in* G.

Comparison

It may be heuristic to compare prime factorizations of finite groups and those of algebraic numbers (below, $\mathbb{Q}$ is the rational number field and $\mathfrak{p}^\sigma$ is the image of $\mathfrak{p}$ under σ):

Algebraic number theory	Prime factorization of groups
E: algebraic extension of $\mathbb{Q}$ with integer ring $\mathcal{O}_E$	G: finite group
$p\mathcal{O}_E = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ (p: a prime): prime factorization of $p\mathcal{O}_E$ into prime ideals of $\mathcal{O}_E$	$G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$: prime factorization of G into cyclic subgroups of prime power order
$\mathrm{Gal}(E/\mathbb{Q})$: Galois group of $E/\mathbb{Q}$	$\mathrm{Aut}(G)$: automorphism group of G
$p\mathcal{O}_E = \mathfrak{p}_1^\sigma\mathfrak{p}_2^\sigma\dots\mathfrak{p}_l^\sigma$ ($\sigma \in \mathrm{Gal}(E/\mathbb{Q})$)	$G = \mathfrak{p}_1^\sigma\mathfrak{p}_2^\sigma\dots\mathfrak{p}_l^\sigma$ ($\sigma \in \mathrm{Aut}(G)$)
class number of E	number of (inequivalent) prime factorizations of G
unique factorization domain	unique factorization group

Besides, as in algebraic number theory, let us say that a prime factorization $G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ of a group G is *ramified* if $\mathfrak{p}_i = \mathfrak{p}_j$ for some distinct $i, j \in \{1, 2, \dots, l\}$; otherwise, i.e. $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_l$ are distinct, it is *unramified*. We show that if G is a quasi-Dedekind group (in particular an abelian group), then any prime factorization of G is unramified (see [18, Theorem 12.16]). A non-quasi-Dedekind group may have a ramified prime factorization (see [18, Example 12.17]).

Main results

We summarize the main results obtained in this and the consecutive papers [17] and [18]:

(1) Any finite group admits a prime factorization (Theorem 3.16) and the number of prime factorizations of a finite group is finite (Theorem 3.19).

(2) A finite group is atomic if and only if it is a cyclic group of prime power order (Theorem 3.13).

(3) A finite group is a unique factorization group if and only if it is cyclic (see [17, Theorem 10.43]). For a cyclic group G of order n

with prime factorization $n = p_1^{m_1} p_2^{m_2} \dots p_l^{m_l}$, its unique prime factorization is $G = \mathbb{Z}_{p_1^{m_1}} \mathbb{Z}_{p_2^{m_2}} \dots \mathbb{Z}_{p_l^{m_l}}$.

(4) For a quasi-Dedekind group (in particular an abelian group), any prime factorization of it is unramified (for more details we refer the reader to [18, Theorem 12.16]).

2 Preparation: Sects and sect monoids

Let G be a group. A *sect* is a subset of G given by a product of a finite number of subgroups of G, that is, for subgroups $H_1, H_2, \dots, H_n$ of G,

$$H_1 H_2 \dots H_n := \{h_1 h_2 \dots h_n : h_i \in H_i \ \ (i = 1, 2, \dots, n)\}, \qquad (2.1)$$

where n is called the *length* of $H_1 H_2 \dots H_n$. Another order of product generally yields another sect: for a permutation σ of $1, 2, \dots, n$, in general $H_1 H_2 \dots H_n \neq H_{\sigma(1)} H_{\sigma(2)} \dots H_{\sigma(n)}$ (as subsets of G). Note next the following auxiliary result.

Lemma 2.1 $H_i \subset H_1 H_2 \dots H_n$ $(i = 1, 2, \dots, n)$.

Proof — As $1 \in H_j$ $(j = 1, 2, \dots, n)$, $H_1 H_2 \dots H_n$ contains

$$1 \cdot 1 \cdot \dots \cdot H_i \cdot \dots \cdot 1,$$

that is, H_i. □

A sect $H_1 H_2 \dots H_n$ is generally not a direct product

$$H_1 \times H_2 \times \dots \times H_n.$$

In fact a sect $H_1 H_2 \dots H_n$ is generally even not a subgroup of G.

Lemma 2.2 *A sect $H_1 H_2 \dots H_n$ is a subgroup of G if and only if the following hold:*

(i) $H_n \dots H_2 H_1 = H_1 H_2 \dots H_n$

(ii) $H_1 H_2 \dots H_n H_1 H_2 \dots H_n = H_1 H_2 \dots H_n$.

Proof — Note first that

$$\begin{aligned}(H_1H_2\dots H_n)^{-1} &= \left\{(h_1h_2\dots h_n)^{-1} \,:\, h_i \in H_i \ (i=1,2,\dots,n)\right\}\\ &= \left\{h_n^{-1}\dots h_2^{-1}h_1^{-1} \,:\, h_i \in H_i \ (i=1,2,\dots,n)\right\}\\ &= H_n\dots H_2H_1\end{aligned}$$

as $h_i^{-1} \in H_i$ $(i = 1,2,\dots,n)$. Hence (i) is equivalent to the invertibility of $H_1H_2\dots H_n$. On the other hand, (ii) is equivalent to the multiplication-closedness of $H_1H_2\dots H_n$. Therefore (i) and (ii) are equivalent to $H_1H_2\dots H_n$ being a subgroup of G. □

Corollary 2.3 *For a sect $H_1H_2\dots H_n$ of a group G, if H_i and H_j for any $i,j \in \{1,2,\dots,n\}$ permute, i.e. $H_iH_j = H_jH_i$, then $H_1H_2\dots H_n$ is a subgroup of G.*

Proof — It suffices to check that under the condition

$$H_iH_j = H_jH_i \quad \text{for any } i \text{ and } j, \tag{2.2}$$

conditions (i) an (ii) in Lemma 2.2 are satisfied. Note that (i) is obviously satisfied. Next, using (2.2), we rewrite the left hand side of (ii) as $H_1^2H_2^2\dots H_n^2$, which is equal to $H_1H_2\dots H_n$ as $H_i^2 = H_i$ (the multiplication-closedness of a subgroup). Hence (ii) is satisfied. □

The following result is basic.

Lemma 2.4 *For a sect $H_1H_2\dots H_n$ of a group G, if (2.2) holds, then for any permutation σ of $1,2,\dots,n$, we have*

$$H_{\sigma(1)}H_{\sigma(2)}\dots H_{\sigma(n)} = H_1H_2\dots H_n.$$

Proof — Any permutation σ is expressed as a composition of transpositions, so the assertion follows from the condition (2.2). □

The following result is often used in later discussion.

Corollary 2.5 *For a sect $H_1H_2\dots H_n$ of a group G, if $H_1,H_2,\dots,H_n$ are permutable subgroups (e.g. normal subgroups) of G, then for any permutation σ of $1,2,\dots,n$, we have*

$$H_{\sigma(1)}H_{\sigma(2)}\dots H_{\sigma(n)} = H_1H_2\dots H_n.$$

Proof — If $H_1, H_2, \ldots, H_n$ are permutable subgroups of G, then the condition (2.2) is satisfied. □

Note that in Lemma 2.2, if $n = 2$, then (ii) is unnecessary as it follows from (i):

$$H_1H_2H_1H_2 = H_1(H_2H_1)H_2 = H_1(H_1H_2)H_2 = H_1^2H_2^2 = H_1H_2.$$

Hence, the following result is satisfied.

Corollary 2.6 *A sect* H_1H_2 *of length* 2 *of a group* G *is a subgroup of* G *if and only if* $H_1H_2 = H_2H_1$.

A group is called *Dedekind* if every subgroup is normal, e.g., abelian groups. Nonabelian Dedekind groups are called *Hamiltonian*, e.g., the quaternion group Q_8.

The notion of Dedekindness is generalized as follows.

Definition 2.7 A group is *quasi-Dedekind* if every subgroup is permutable, i.e. $HK = KH$ for any subgroups H and K of G. If it is nonabelian, it is called *quasi-Hamiltonian*.

Corollary 2.8 *If a group* G *is quasi-Dedekind, then any sect of* G *is a subgroup of* G.

Proof — This follows from Corollary 2.3. □

In what follows, to clarify discussion we regard a sect of G as a "word" of subgroups of G — more formally an element of the "sect monoid" $S(G)$ of G. In this paper, we introduce the following definition.

Definition 2.9 The *sect monoid* $S(G)$ of a group G is the set of sects of G equipped with multiplication of two sects given by

$$H_1H_2\ldots H_n \cdot K_1K_2\ldots K_m := H_1H_2\ldots H_nK_1K_2\ldots K_m,$$

and the identity element given by the identity subgroup of G. Relations of $S(G)$ are given by equations between sects with the same underlying sets, such as

$$H_1H_2\ldots H_n = K_1K_2\ldots K_m,$$

as subsets of G.

In the present paper we do not go into details about the monoid structure on $S(G)$; it will be described in our another paper.

2.1 Irredundancy of sects

If a sect $H_1H_2\dots H_n$ of a group G is equal to a subgroup K of G, then the equation $K = H_1H_2\dots H_n$ is called a *factorization* of K. If $n = 1$, then $K = H_1$ is a *trivial* factorization.

Remark 2.10 Given a finite group K, to show/find a factorization

$$K = H_1H_2\dots H_n$$

generally requires lots of computations — the initial computation of elements of $H_1H_2\dots H_n$, in principle, contains many overlaps, and further computation is necessary to check among them, which are equal by using relations between elements of K.

Observe that for any subgroups $H_1, H_2, \dots, H_n$ of a subgroup K of G, we have $H_1H_2\dots H_n \subset K$. Here if (at least) one o $H_1, H_2, \dots, H_n$ is K, then $K = H_1H_2\dots H_n$. This factorization is however uninteresting: say $H_j = K$, then the rest $H_1, H_2, \dots, H_{j-1}, H_{j+1}, \dots, H_n$ are removable and the factorization $K = H_1H_2\dots H_n$ is essentially $K = H_j$ (trivial). When we discuss prime factorizations of groups, we focus on irredundant ones.

Definition 2.11 (i) A sect $H_1H_2\dots H_n$ is *irredundant* if the removal of any factor H_i strictly shrinks it, i.e.,

$$H_1H_2\dots\breve{H}_i\dots H_n \subsetneq H_1H_2\dots H_n \quad (i = 1, 2, \dots, n),$$

where $\breve{H}_i$ signifies the removal of H_i.

(ii) Suppose that a sect $H_1H_2\dots H_n$ is redundant. Then for some factor H_i, $H_1H_2\dots\breve{H}_i\dots H_n = H_1H_2\dots H_n$. Such H_i is called a *redundant factor* and said to be *removable* from $H_1H_2\dots H_n$; or alternatively $H_1H_2\dots H_n$ is *redundant at* H_i.

For irredundant sects, the following properties are often used in our later discussions.

Lemma 2.12 *Let* $H_1H_2\dots H_n$ *be an irredundant sect of a group* G. *If* (2.2) *holds, then* $H_1, H_2, \dots, H_n$ *are distinct.*

Proof — Otherwise, say $H_i = H_j$ for some i, j $(i \neq j)$. Without loss of generality, we may assume that $i < j$. Using (2.2), in $H_1H_2\dots H_n$

we may shift H_i to the next to H_j, and then we obtain the following:

$$\begin{aligned} H_1H_2\dots H_i\dots H_j\dots H_n &= H_1H_2\dots H_iH_j\dots H_n \\ &= H_1H_2\dots H_j\dots H_n \\ &= H_1H_2\dots \breve{H}_i\dots H_n. \end{aligned}$$

where in the second equality we used that $H_iH_j = H_jH_j = H_j$. Hence,

$$H_1H_2\dots H_n = H_1H_2\dots \breve{H}_i\dots H_n.$$

This contradicts the irredundancy of $H_1H_2\dots H_n$. □

Remark 2.13 The condition (2.2) also implies that $H_1H_2\dots H_n$ is a subgroup of G (see Corollary 2.3).

Corollary 2.14 *Let $H_1H_2\dots H_n$ be an irredundant sect of a group G. If $H_1, H_2, \dots, H_n$ are permutable subgroups* (e.g. *normal subgroups*) *of G, then $H_1, H_2, \dots, H_n$ are distinct.*

Proof — If $H_1, H_2, \dots, H_n$ are permutable subgroups of G, then the condition (2.2) is satisfied, thus the assertion holds. □

Note that even if a sect $H_1H_2\dots H_n$ is irredundant, a removed sect $H_1H_2\dots \breve{H}_i\dots H_n$ may not be irredundant: the irredundancy of the former merely means

$$H_1H_2\dots \breve{H}_i\dots H_n \subsetneq H_1H_2\dots H_n,$$

but does not mean the irredundancy of the latter — possibly

$$H_1H_2\dots \breve{H}_i\dots \breve{H}_j\dots H_n = H_1H_2\dots \breve{H}_i\dots H_n \tag{2.3}$$

for some j. However (2.3) does *not* occur when $H_1, H_2, \dots, H_n$ are permutable with each other, i.e., (2.2) holds. Namely in this case,

$$H_1H_2\dots \breve{H}_i\dots \breve{H}_j\dots H_n \subsetneq H_1H_2\dots \breve{H}_i\dots H_n$$

for any j, that is, $H_1H_2\dots \breve{H}_i\dots H_n$ is irredundant. We show this by contradiction. Suppose that (2.3) holds. From (2.2), we may rearrange the order of $H_1, H_2, \dots, H_n$ and after renumbering if necessary, we

may assume that $i = 1$ and $j = 2$; then (2.3) is given by

$$\breve{H}_1\breve{H}_2H_3\dots H_n = \breve{H}_1H_2H_3\dots H_n. \tag{2.4}$$

Multiplying this by H_1 from the left yields

$$H_1\breve{H}_2H_3\dots H_n = H_1H_2H_3\dots H_n,$$

which however contradicts the irredundancy of $H_1H_2\dots H_n$. Therefore $\breve{H}_1H_2H_3\dots H_n$ is irredundant. More generally, repeating this argument shows that for any factors

$$H_{i_1}, H_{i_2}, \dots, H_{i_k} \quad (1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n),$$

their removed sect $H_1\dots\breve{H}_{i_1}\dots\breve{H}_{i_2}\dots\breve{H}_{i_k}\dots H_n$ is irredundant. We thus obtain the following proposition.

Proposition 2.15 *Let $H_1H_2\dots H_n$ be an irredundant sect such that*

$$H_1, H_2, \dots, H_n$$

are permutable with each other. Then any sect obtained by successive removals of factors from $H_1H_2\dots H_n$ is irredundant.

We return to factorizations of groups.

Definition 2.16 A factorization $K = H_1H_2\dots H_n$ for a subgroup K of a group G is said to be *irredundant* if $H_1H_2\dots H_n$ is irredundant.

For any (not necessarily irredundant) factorization $K = H_1H_2\dots H_n$, we have $H_i \subset K$ $(i = 1, 2, \dots, n)$ by Lemma 2.1. Note the following lemma.

Lemma 2.17 *If $K = H_1H_2\dots H_n$ is a nontrivial irredundant factorization of a subgroup K of G, then $H_i \subsetneq K$ for any i.*

Proof — Otherwise, say $H_j = K$ for some j, then any other factor is removable, so $K = H_1H_2\dots H_n$ is not irredundant. □

2.2 Irredundantization of sects

To obtain irredundant sects from redundant ones, we may proceed as follows: For a redundant sect $H_1H_2\dots H_n$, removing redundant

factors successively, we finally reach to an irredundant sect

$$H_{i_1}H_{i_2}\dots H_{i_k} \quad (1 \leqslant i_i < i_2 < \dots < i_k \leqslant n).$$

This operation (and also the resulting sect) is called an *irredundantization* of $H_1H_2\dots H_n$. Note that an irredundantization of a sect is not necessarily unique.

Example 2.18 The symmetric group $\mathfrak{S}_3$ has four nontrivial proper subgroups: Three nonnormal subgroups

$$H_k \simeq \mathbb{Z}_2 \quad (k = 1, 2, 3),$$

where H_k is generated by a transposition $(i\,j)$ with $i, j \in \{1, 2, 3\}$ distinct from k, and one normal subgroup $N \simeq \mathbb{Z}_3$ generated by a cyclic permutation $(1\,2\,3)$. Note that H_iH_j, for distinct i, j, is *not* a subgroup of $\mathfrak{S}_3$ (as $|H_iH_j| = 4$ does not divide $|\mathfrak{S}_3| = 6$). Consequently $H_iH_j \neq H_jH_i$ (Corollary 2.6); on the other hand $H_iN = NH_i$ by the normality of N. By computation, the nontrivial irredundant factorizations of $\mathfrak{S}_3$ are as follows (these are the prime factorizations of $\mathfrak{S}_3$):

$$\mathfrak{S}_3 = \begin{cases} H_iH_jH_k & (\text{distinct } i, j, k \in \{1, 2, 3\}), \\ H_iH_jH_i & (\text{distinct } i, j \in \{1, 2, 3\}), \\ H_iN\,(= NH_i) & (i = 1, 2, 3). \end{cases} \tag{2.5}$$

- A factorization $\mathfrak{S}_3 = H_1H_2H_3N$ has four irredundantizations:
  1. $\mathfrak{S}_3 = H_1\breve{H}_2\breve{H}_3N = H_1N$.
  2. $\mathfrak{S}_3 = \breve{H}_1H_2\breve{H}_3N = H_2N$.
  3. $\mathfrak{S}_3 = \breve{H}_1\breve{H}_2H_3N = H_3N$.
  4. $\mathfrak{S}_3 = H_1H_2H_3\breve{N} = H_1H_2H_3$.

- A factorization $\mathfrak{S}_3 = H_1H_2H_1H_3H_1$ has seven irredundantizations:
  1. $\mathfrak{S}_3 = H_1H_2\breve{H}_1\breve{H}_3H_1 = H_1H_2H_1$.
  2. $\mathfrak{S}_3 = H_1H_2H_1\breve{H}_3\breve{H}_1 = H_1H_2H_1$.

3. $\mathfrak{S}_3 = \breve{H}_1\breve{H}_2H_1H_3H_1 = H_1H_3H_1$.
4. $\mathfrak{S}_3 = H_1\breve{H}_2\breve{H}_1H_3H_1 = H_1H_3H_1$.
5. $\mathfrak{S}_3 = \breve{H}_1H_2H_1H_3\breve{H}_1 = H_2H_1H_3$.
6. $\mathfrak{S}_3 = \breve{H}_1H_2\breve{H}_1H_3H_1 = H_2H_3H_1$.
7. $\mathfrak{S}_3 = H_1H_2\breve{H}_1H_3\breve{H}_1 = H_1H_2H_3$.

As we saw above, an irredundantization of a sect is generally not unique. Next for each irredundantization of a sect, we show that the order of removing factors is freely changeable while the resulting irredundant sects are the same — *an irredundantization is uniquely determined by the set of removed factors but not the order of removals of them.* Let $H_1H_2\dots H_n$ be a (not necessarily redundant) sect. The operation to remove a factor H_i from it (or more generally from a sect with a factor H_i) is called the *removal operator* of H_i and denoted by O_i.

Claim 2.19 *Removal operators commute. Namely for a sect* $H_1H_2\dots H_n$, *we have* $O_j \circ O_i = O_i \circ O_j$ *for distinct* $i, j \in \{1, 2, \dots, n\}$.

Proof — In fact

$$\begin{cases} O_i \circ O_j : H_1H_2\dots H_n \xrightarrow{O_j} H_1H_2\dots\breve{H}_j\dots H_n \\ \qquad\qquad\qquad\qquad \xrightarrow{O_i} H_1H_2\dots\breve{H}_i\dots\breve{H}_j\dots H_n, \\ O_j \circ O_i : H_1H_2\dots H_n \xrightarrow{O_i} H_1H_2\dots\breve{H}_i\dots H_n \\ \qquad\qquad\qquad\qquad \xrightarrow{O_j} H_1H_2\dots\breve{H}_i\dots\breve{H}_j\dots H_n. \end{cases}$$

Hence, both $O_j \circ O_i$ and $O_i \circ O_j$ transform $H_1H_2\dots H_n$ to

$$H_1H_2\dots\breve{H}_i\dots\breve{H}_j\dots H_n,$$

so $O_j \circ O_i = O_i \circ O_j$. □

We can say more. Suppose that $H_1H_2\dots H_n$ is redundant at H_i and its removal $H_1H_2\dots\breve{H}_i\dots H_n$ is redundant at H_j. Namely,

$$\begin{aligned} H_1H_2\dots H_n &= H_1H_2\dots\breve{H}_i\dots H_n \\ &= H_1H_2\dots\breve{H}_i\dots\breve{H}_j\dots H_n. \end{aligned} \tag{2.6}$$

We then claim that $H_1H_2\dots H_n$ is redundant at H_j, that is,

$$H_1H_2\dots H_n = H_1H_2\dots \breve{H}_j\dots H_n. \tag{2.7}$$

To see this, note first that

$$H_1H_2\dots H_n \supset H_1H_2\dots \breve{H}_j\dots H_n \supset H_1H_2\dots \breve{H}_i\dots \breve{H}_j\dots H_n. \tag{2.8}$$

Here $H_1H_2\dots H_n = H_1H_2\dots \breve{H}_i\dots \breve{H}_j\dots H_n$ (see (2.6)). Consequently,

$$H_1H_2\dots H_n = H_1H_2\dots \breve{H}_j\dots H_n, \tag{2.9}$$

so the following counterpart of (2.6) holds:

$$\begin{aligned} H_1H_2\dots H_n &= H_1H_2\dots \breve{H}_j\dots H_n \\ &= H_1H_2\dots \breve{H}_i\dots \breve{H}_j\dots H_n. \end{aligned} \tag{2.10}$$

Therefore $H_1H_2\dots H_n$ is redundant at H_j and its removal

$$H_1H_2\dots \breve{H}_j\dots H_n$$

is redundant at H_i. We summarize this result as follows:

Lemma 2.20 *If a sect $H_1H_2\dots H_n$ is redundant at H_i and its removal $H_1H_2\dots \breve{H}_i\dots H_n$ is redundant at H_j ($j \neq i$), then $H_1H_2\dots H_n$ is redundant at H_j and its removal $H_1H_2\dots \breve{H}_j\dots H_n$ is redundant at H_i — the resulting sect $H_1H_2\dots \breve{H}_i\dots \breve{H}_j\dots H_n$ does not depend on the order of removals of H_i and H_j.*

Let $H_1H_2\dots H_n$ be a redundant sect. Suppose that an irredundantization of $H_1H_2\dots H_n$ is given by removing factors $H_{i_1}, H_{i_2}, \dots, H_{i_k}$ in this order. Repeated application of Lemma 2.20 then ensures that the resulting irredundant sect does *not* depend on the order of removing the factors $H_{i_1}, H_{i_2}, \dots, H_{i_k}$. We formalize this result as follows:

Proposition 2.21 *An irredundantization of a sect does not depend on the order of removals of factors. In fact the order of removals is freely changeable while the resulting irredundant sect is the same.*

2.3 Finiteness on irredundant sects of finite groups

We shall show that the number of irredundant sects of a finite group is finite. To this end, we first show the boundedness of the lengths of irredundant sects of a finite group. *In what follows, unless otherwise mentioned, a group is assumed to be nontrivial and any factor of a sect is assumed to be nontrivial.*

Lemma 2.22 *Let $H_1H_2\dots H_n$ be an irredundant sect of a (not necessarily finite) group. Then the successive removals of rightmost factors yield a strictly decreasing sequence of sects:*

$$\begin{aligned} H_1H_2\dots H_n &\supsetneq H_1H_2\dots H_{n-1} \\ &\supsetneq H_1H_2\dots H_{n-2} \\ &\supsetneq \dots \supsetneq H_1H_2 \supsetneq H_1. \end{aligned} \tag{2.11}$$

Proof — Since $H_1H_2\dots H_n$ is irredundant, in particular

$$H_1H_2\dots H_n \supsetneq H_1H_2\dots H_{n-1}.$$

Here we claim that $H_1H_2\dots H_{n-1}$ is irredundant at H_{n-1}. Otherwise $H_1H_2\dots H_{n-1} = H_1H_2\dots H_{n-2}$. Then multiplying this by H_n from the right yields $H_1H_2\dots H_n = H_1H_2\dots H_{n-2}H_n$. This means that H_{n-1} is redundant in $H_1H_2\dots H_n$, which contradicts the irredundancy of $H_1H_2\dots H_n$. Hence,

$$H_1H_2\dots H_{n-1} \supsetneq H_1H_2\dots H_{n-2}.$$

Here we claim that $H_1H_2\dots H_{n-2}$ is irredundant at H_{n-2}. Otherwise $H_1H_2\dots H_{n-2} = H_1H_2\dots H_{n-3}$. Then, multiplying by $H_{n-1}H_n$ from the right yields $H_1H_2\dots H_n = H_1H_2\dots H_{n-3}H_{n-1}H_n$. This means that H_{n-2} is redundant in $H_1H_2\dots H_n$, which contradicts the irredundancy of $H_1H_2\dots H_n$. Hence,

$$H_1H_2\dots H_{n-2} \supsetneq H_1H_2\dots H_{n-3}.$$

Repeating, this argument gives (2.11). □

Remark 2.23 The same argument used in the proof of Lemma 2.22, shows that for an irredundant sect $H_1H_2\dots H_n$ of a group, the successive removals of leftmost factors yield a strictly decreasing se-

quence of sects:

$$H_1H_2\dots H_n \supsetneq H_2H_3\dots H_n \supsetneq H_3H_4\dots H_n \supsetneq \dots \supsetneq H_{n-1}H_n \supsetneq H_n.$$

By a *finite sect*, we mean a sect consisting of a finite number of elements. Any sect of a finite group is finite. Note the following lemma.

Lemma 2.24 *If a finite sect* $H_1H_2\dots H_n$ *of a group is irredundant, then*

$$|H_1H_2\dots H_n| \geqslant n+1.$$

Proof — From Lemma 2.22, we have

$$\begin{aligned}|H_1H_2\dots H_n| &> |H_1H_2\dots H_{n-1}| > |H_1H_2\dots H_{n-2}|\\ &> \dots > |H_1H_2| > |H_1|.\end{aligned}$$

Here, $|H_1| \geqslant 2$, so

$$|H_1H_2\dots H_n| > |H_1H_2\dots H_{n-1}| > \dots > |H_1H_2| > 2. \tag{2.12}$$

This implies that $|H_1H_2\dots H_n| \geqslant n+1$. □

In Lemma 2.24, the irredundancy of $H_1H_2\dots H_n$ is essential. Moreover, if $H_1H_2\dots H_n$ is redundant, $|H_1H_2\dots H_n| \geqslant n+1$ fails.

Example 2.25 If $H_1 = H_2 = \dots = H_n$, then $H_1H_2\dots H_n = H_1$ (redundant), so $|H_1H_2\dots H_n| = |H_1|$. Take a sufficiently large n such that $n+1 > |H_1|$, then $n+1 > |H_1H_2\dots H_n|$.

Proposition 2.26 *If a sect* $H_1H_2\dots H_n$ *of a finite group* G *is irredundant, then* $n \leqslant |G|-1$. *If, moreover,* $H_1H_2\dots H_n$ *is proper in* G, i.e.,

$$H_1H_2\dots H_n \subsetneq G,$$

then $n \leqslant |G|-2$.

Proof — First, as $G \supset H_1H_2\dots H_n$, we have $|G| \geqslant |H_1H_2\dots H_n|$. Since $|H_1H_2\dots H_n| \geqslant n+1$ (see Lemma 2.24), so $n \leqslant |G|-1$. If, moreover, $G \supsetneq H_1H_2\dots H_n$, then $|G| > |H_1H_2\dots H_n|$, so $n < |G|-1$, that is, $n \leqslant |G|-2$. □

Remark 2.27 In the above, by convention G is nontrivial. Otherwise the inequality $n \leqslant |G|-1$ fails; indeed if $G = \{1\}$, then $n \leqslant |G|-1$ becomes $n \leqslant 0$, which is absurd.

We now show the following result.

Theorem 2.28 *The number of irredundant sects of a finite group is finite.*

Proof — The lengths of irredundant sects of a finite group G are bounded by $|G|-1$ (see Proposition 2.26). Observe that, for each positive integer n ($1 \leqslant n \leqslant |G|-1$), the number of irredundant sects of length n is at most finite (possibly zero), because for an irredundant sect $H_1H_2\dots H_n$ of length n, we have that the number of possible factors $H_1, H_2, \dots, H_n$ is finite (as the number of subgroups of G is finite). Hence, the total number of irredundant sects of G is finite. □

3 Prime factorizations of groups

Unless otherwise mentioned, groups are assumed to be nontrivial. We shall show that if a finite group is *not* cyclic of prime power order, then it factorizes into its maximal subgroups. To that end, first note the following:

Lemma 3.1 *If a finite group G has exactly one maximal subgroup, then G is a cyclic group of prime power order.*

Proof — Let M be the unique maximal subgroup of G and take any element $x \in G \setminus M$. Then, the cyclic subgroup $\langle x\rangle$ generated by x is *not* contained in M. Thus, the uniqueness of the maximal subgroup M of G implies that $\langle x\rangle$ is G itself. Namely, G is a cyclic group generated by x. Let n be the order of G. We claim that n is a prime power. Otherwise, let $n = p_1^{m_1}p_2^{m_2}\dots p_l^{m_l}$ ($l \geqslant 2$) be the prime factorization and take the nontrivial direct product decomposition

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

into cyclic groups of prime power orders (by the fundamental theorem of finite abelian groups). However, G has more than one maximal subgroup — for $i = 1, 2, \dots, l$, the subgroups

$$\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \dots \times \mathbb{Z}_{p_i^{m_i-1}} \times \dots \times \mathbb{Z}_{p_l^{m_l}}$$

are maximal. This contradicts the assumption. □

Remark 3.2 Cyclic groups of prime power orders have only one minimal subgroup. Yet in contrast to the case of a maximal subgroup (see Lemma 3.1), there are other finite groups with only one minimal subgroup — generalized quaternion groups (see [11, p. 229] and [19, p. 2]). Both are p-groups (the latter are2-groups). In fact, if a finite group is not a p-group, say its order is divisible by primes the $p_1, p_2, \ldots, p_l$ ($l \geqslant 2$), then, by Cauchy's theorem, the group has minimal subgroups

$$\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_l},$$

so the classification of finite groups with only one minimal subgroup reduces to that of p-groups with only one minimal subgroup, which is given by [20, Theorem 15, p. 118] and [12, Theorem 5.3.7, p. 114].

The maximal subgroup of a cyclic group $\mathbb{Z}_{p^m}$ of prime power order is $\mathbb{Z}_{p^{m-1}}$, and in turn the maximal subgroup of $\mathbb{Z}_{p^{m-1}}$ is $\mathbb{Z}_{p^{m-2}}$, and so on. Thus the subgroup poset of $\mathbb{Z}_{p^m}$ is "straight":

$$\mathbb{Z}_{p^m} \supsetneq \mathbb{Z}_{p^{m-1}} \supsetneq \ldots \supsetneq \mathbb{Z}_{p^2} \supsetneq \mathbb{Z}_p \supsetneq \{1\}.$$

For any other finite group, its subgroup poset is *not* straight, as it has more than one maximal subgroup (see Lemma 3.1). This confirms the following corollary (see [15, p. 887]).

Corollary 3.3 *A finite group has a "straight" subgroup poset if and only if it is a cyclic group of prime power order*: *In fact,*

$$\mathbb{Z}_{p^m} \supsetneq \mathbb{Z}_{p^{m-1}} \supsetneq \ldots \supsetneq \mathbb{Z}_{p^2} \supsetneq \mathbb{Z}_p \supsetneq \{1\}.$$

Now we give factorizations of finite groups into their maximal subgroups.

Lemma 3.4 *Let* G *be a finite group that is not cyclic of prime power order; so* G *has more than one maximal subgroup* (*by* Lemma 3.1)*, say they are* $M_1, M_2, \ldots, M_l$. *Then* $G = M_1 M_2 \ldots M_l$ (*caution: This factorization may not be irredundant*).

Proof — Assuming that $G \supsetneq M_1 M_2 \ldots M_l$, we deduce a contradiction. Take any element $x \in G \setminus M_1 M_2 \ldots M_l$. Noting that

$$M_1 M_2 \ldots M_l \supset M_i \quad (i = 1, 2, \ldots, l),$$

we have $x \notin M_i$ ($i = 1, 2, \ldots, l$). Hence, the cyclic subgroup $\langle x \rangle$ generated by x is contained in none of $M_1, M_2, \ldots, M_l$. This contradicts

the fact that $M_1, M_2, \ldots, M_l$ exhaust all maximal subgroups of G. □

To obtain irredundant factorizations from redundant ones, we only have to apply irredundantization of the sects in the factorizations (see Section 2.2). This is used for showing the following.

Lemma 3.5 *Any finite group* G *other than cyclic groups of prime power orders admits a nontrivial irredundant factorization into maximal subgroups of* G.

Proof — Take the factorization $G = M_1 M_2 \ldots M_l$ in Lemma 3.4, which may be redundant. Removing all redundant factors, if any, from

$$M_1 M_2 \ldots M_l$$

successively yields an irredundant factorization

$$G = M_{i_1} M_{i_2} \ldots M_{i_k} \quad (1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant l).$$

Here, $k \geqslant 2$; otherwise $G = M_{i_1}$, but this contradicts the assumption that M_k is a maximal subgroup of G (which must be proper in G). □

Proposition 3.6 *Suppose that* G *is a finite quasi-Dedekind group that is not cyclic of prime power order; so* G *has more than one maximal subgroup by* Lemma 3.1*, say* $M_1, M_2, \ldots, M_l$ $(l \geqslant 2)$ *are the maximal subgroups of* G*. Then* $G = M_i M_j$ *for any distinct* $i, j \in \{1, 2, \ldots, l\}$*. Moreover,*

$$G = M_i M_j$$

is an irredundant factorization.

Proof — Since G is quasi-Dedekind, $M_i M_j$ is a subgroup of G by Corollary 2.8. Besides $M_i M_j$ properly contains the maximal subgroups M_i and M_j, so it coincides with G, that is, $G = M_i M_j$. This factorization is irredundant, as $M_i M_j \supsetneq M_i$ and $M_i M_j \supsetneq M_j$. □

We next give irredundant factorizations into cyclic subgroups.

Lemma 3.7 *Any finite group* G *other than cyclic groups admits a nontrivial irredundant factorization into cyclic subgroups of* G.

Proof — Let $\{g_1, g_2, \ldots, g_m\}$ be the set of nontrivial elements of G, and let Z_i $(i = 1, 2, \ldots, m)$ be the cyclic subgroup of G generated by g_i. Then, by (2.2), $G = Z_1 Z_2 \ldots Z_m$. In fact,

$$Z_1 Z_2 \ldots Z_m \supset Z_i \quad (i = 1, 2, \ldots, m)$$

by Lemma 2.1, so the right hand side contains any g_i and the identity of G. This factorization may be redundant. Removing redundant factors, if any, from $Z_1 Z_2 \dots Z_l$ successively yields an irredundant factorization $G = Z_{i_1} Z_{i_2} \dots Z_{i_k}$ ($1 \leqslant i_1 < i_2 < \dots < i_k \leqslant l$) by cyclic groups. Here, $l \geqslant 2$; otherwise $G = Z_{i_1}$, which however contradicts the assumption that G is not cyclic. □

Remark 3.8 It is more practical to take the maximal ones among

$$Z_1, Z_2, \dots, Z_l,$$

say $Z_{j_1}, Z_{j_2}, \dots, Z_{j_k}$ ($1 \leqslant j_1 < j_2 < \dots < j_k \leqslant l$), then any element of G is contained in (at least) one of them, and $G = Z_{j_1} Z_{j_2} \dots Z_{j_k}$. Removing redundant factors, if any, from the right hand side successively yields an irredundant factorization of G by cyclic subgroups.

Theorem 3.9 *If a finite group* G *is not a cyclic group of prime power order, then it admits a nontrivial irredundant factorization into cyclic subgroups of prime power order.*

Proof — By Lemma 3.7, G has a nontrivial irredundant factorization by cyclic subgroups. Now as H_i is a finite abelian group, the fundamental theorem of abelian groups ensures that it may be factorized as

$$H_i = \mathfrak{p}_{i,1} \times \mathfrak{p}_{i,2} \times \dots \times \mathfrak{p}_{i,l_i} \, (= \mathfrak{p}_{i,1} \mathfrak{p}_{i,2} \dots \mathfrak{p}_{i,l_i})$$

into cyclic groups of prime power orders. Putting this into (2.2) yields a factorization of G as a (not necessarily irredundant) sect of cyclic subgroups of prime power orders. Finally take an irredundantization, then we reach to an irredundant factorization of G consisting of cyclic subgroups of prime power orders. This factorization is nontrivial, as G itself is not a cyclic group of prime power order (by assumption). □

Remark 3.10 We may alternatively show Theorem 3.9 in terms of maximal subgroups. To that end, it is convenient to show a modified assertion: *Any nontrivial subgroup* H *of a finite group* G *admits an irredundant factorization into cyclic subgroups of prime power order*. We show this by induction on the order of H — here we need to be careful about the first step of the induction: It generally does *not* begin with the smallest nontrivial group, i.e. a group of order 2, but

begins with the minimal subgroups of G; note that the poset of nontrivial subgroups of G is generally not "straight" but spreads out with more than one minimal subgroup (see Remark 3.2). Since minimal subgroups of G are cyclic of prime order, the assertion for them is trivial — they themselves give the desired irredundant factorizations. Next we show the assertion for a nontrivial subgroup H of G under the assumption that the assertion for nontrivial subgroups of orders strictly less than $|H|$ is valid. If H is cyclic of prime power order, then H itself gives the desired irredundant factorization. Otherwise the number of maximal subgroups of H is at least two, say

$$M_1, M_2, \dots, M_l \quad (l \geqslant 2).$$

Then, $H = M_1 M_2 \dots M_l$ (see Lemma 3.4). Here, $|M_i| < |H|$, thus by the induction hypothesis, M_i admits an irredundant factorization by cyclic subgroups of prime power orders. Substituting them into

$$H = M_1 M_2 \dots M_l$$

yields a factorization of H by cyclic subgroups of prime power orders. Its irredundantization is the desired factorization.

We next show the following result.

Lemma 3.11 *Any cyclic group $\mathbb{Z}_{p^m}$ of prime power order admits no nontrivial irredundant factorization.*

Proof — Otherwise, say $\mathbb{Z}_{p^m} = H_1 H_2 \dots H_n$ $(n \geqslant 2)$ is a nontrivial irredundant factorization. As this factorization is nontrivial,

$$H_i \subsetneq \mathbb{Z}_{p^n} \quad (i = 1, 2, \dots, n)$$

by Lemma 2.17. Observe next that the subgroup poset of $\mathbb{Z}_{p^m}$ is "straight":

$$\mathbb{Z}_{p^m} \supsetneq \mathbb{Z}_{p^{m-1}} \supsetneq \dots \supsetneq \mathbb{Z}_{p^2} \supsetneq \mathbb{Z}_p \supsetneq \{1\}$$

(see Corollary 3.3). Hence, there is a maximal one H_k among

$$H_1, H_2, \dots, H_n,$$

that is, by (2.2), $H_k \supset H_i$ for any $i = 1, 2, \dots, n$. Now as $\mathbb{Z}_{p^m}$ is abelian, $H_1, H_2, \dots, H_n$ mutually commute. This fact, together with condition (2.2), implies that $H_1 H_2 \dots H_n = H_k$. That is, $\mathbb{Z}_{p^m} = H_k$. This contradicts the fact that $H_k \subsetneq \mathbb{Z}_{p^m}$. □

Definition 3.12 A nonidentity group is said to be *atomic* if it admits no nontrivial irredundant factorization.

Theorem 3.9 is restated as: *Finite groups that are not cyclic of prime power orders are not atomic*. Consequently, the converse of Lemma 3.11 holds, and the following result is established.

Theorem 3.13 *A finite group is atomic if and only if it is a cyclic group of prime power order.*

We now introduce a key concept in this paper.

Definition 3.14 An irredundant factorization of a group into atomic subgroups is called a *prime factorization* of the group.

For finite groups, using Theorem 3.13, we may "explicitize" this definition as follows.

Definition 3.15 An irredundant factorization of a finite group into cyclic subgroups of prime power orders is called a *prime factorization* of the group.

Combining Theorem 3.9 and Theorem 3.13 yields the following result.

Theorem 3.16 *Any finite group admits a prime factorization — it admits a nontrivial prime factorization if and only if it is not a cyclic group of prime power order.*

For infinite groups, the situation is different. For instance, the following result holds.

Proposition 3.17 *The additive group $\mathbb{Z}$ of integers has no atomic subgroup (in particular $\mathbb{Z}$ itself is not atomic). In fact, any subgroup of $\mathbb{Z}$ admits a nontrivial irredundant factorization. Consequently $\mathbb{Z}$ cannot have a prime factorization.*

Proof — Let H be a subgroup of $\mathbb{Z}$. Taking the smallest positive integer n in H, then $H = n\mathbb{Z}$. We show that $n\mathbb{Z}$ admits a nontrivial irredundant factorization. Take relatively prime integers a and b greater than 1. Then

$$\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$$

because the right hand side contains a generator $1 \in \mathbb{Z}$, as there exist integers u and v satisfying $ua + vb = 1$. Note that $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ is irredundant, as $a\mathbb{Z} \subsetneq \mathbb{Z}$ and $b\mathbb{Z} \subsetneq \mathbb{Z}$. Multiplying $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ by n yields $n\mathbb{Z} = na\mathbb{Z} + nb\mathbb{Z}$. This is irredundant, as $na\mathbb{Z} \subsetneq n\mathbb{Z}$ and $nb\mathbb{Z} \subsetneq n\mathbb{Z}$. This confirms that $n\mathbb{Z}$ admits a nontrivial irredundant factorization. □

Finiteness on irredundant factorizations and prime factorizations

The number of irredundant sects of a finite group is finite (for more details see Theorem 2.28). In particular the following result holds.

Theorem 3.18 *The number of irredundant factorizations of a finite group is finite.*

A prime factorization is a special case of an irredundant factorization. Hence the following result holds.

Theorem 3.19 *The number of prime factorizations of a finite group is finite.*

3.1 Mutation and equivalence of sects

Let $H_1H_2\cdots H_n$ be a sect of a group G. Then, in general,

$$H_1H_2\dots H_n \neq H_n\dots H_2H_1.$$

If $H_1H_2\dots H_n = H_n\dots H_2H_1$, then $H_1H_2\dots H_n$ is called *self-reversal*. This is for example the case if $H_1H_2\dots H_n$ is equal to a subgroup of G (see Lemma 2.2).

A *subsect* of a sect $H_1H_2\dots H_n$ is a sect consisting of successive factors of $H_1H_2\dots H_n$, i.e. of the form $H_iH_{i+1}\dots H_j$ $(1 \leqslant i < j \leqslant n)$; the sect itself is a subsect. A subsect $H_iH_{i+1}\dots H_j$ is *regular* if it is equal to a subgroup of G; in other words it gives a factorization of the subgroup. In particular, for a factorization $G = H_1H_2\dots H_n$, the sect $H_1H_2\dots H_n$ is regular.

Note the following statements:

(a) For a subsect H_iH_{i+1} of length 2, the following holds (see Corollary 2.6):

$$H_iH_{i+1} \text{ is regular } \iff H_iH_{i+1} = H_{i+1}H_i.$$

(b) For a subsect $H_iH_{i+1}\dots H_j$ of length greater than two, *only* the following holds (see Lemma 2.2):

$$H_iH_{i+1}\dots H_j \text{ is regular } \implies H_iH_{i+1}\dots H_j = H_j\dots H_{i+1}H_i.$$

Here "$\Longleftarrow$" generally fails. For instance, $H_1H_2H_1$ is trivially self-reversal, but generally not regular.

Suppose that a sect $H_1H_2\dots H_n$ contains a regular subsect

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

As $H_iH_{i+1}\dots H_j = H_j\dots H_{i+1}H_i$ (see (b)), we have

$$H_1H_2\dots \underbrace{H_iH_{i+1}\dots H_j}\dots H_n = H_1H_2\dots \underbrace{H_j\dots H_{i+1}H_i}\dots H_n \quad (3.1)$$

where, by convention, "subsects in question" are underbraced for emphasis.

While (3.1) is a relation of the sect monoid $S(G)$ (see Definition 2.9), we introduce an equivalence relation on $S(G)$ under which the two sects in (3.1) are equivalent. To that end, we regard $S(G)$ as a small category with objects being sects of G and morphisms given by compositions of elementary mutations — an *elementary mutation* is a morphism from a sect $H_1H_2\dots H_n$ with a regular subsect $H_iH_{i+1}\dots H_j$ to the sect replacing the regular subsect with its reverse, that is,

$$\begin{aligned}\mu : H_1H_2\dots \underbrace{H_iH_{i+1}\dots H_j}\dots H_n \\ \longrightarrow H_1H_2\dots \underbrace{H_j\dots H_{i+1}H_i}\dots H_n.\end{aligned} \quad (3.2)$$

Remark 3.20 The small category $S(G)$ is actually a groupoid, as any morphism μ has an inverse:

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

For simplicity, we shall denote a sect by one letter $\mathcal{H}$ and such.

Definition 3.21 Two sects $\mathcal{H}$ and $\mathcal{H}'$ of a group are *equivalent* (notation: $\mathcal{H} \sim \mathcal{H}'$) if there exists a sequence of elementary mutations that transforms one to the other, such as

$$\mu_1 : \mathcal{H}_1 = \mathcal{H} \to \mathcal{H}_2,\ \mu_2 : \mathcal{H}_2 \to \mathcal{H}_3,\ \dots,\ \mu_l : \mathcal{H}_l \to \mathcal{H}_{l+1} = \mathcal{H}'. \quad (3.3)$$

Then $\mathcal{H}'$ (resp. $\mathcal{H}$) is called a *mutant* of $\mathcal{H}$ (resp. $\mathcal{H}'$), and the composition $\mu_l \circ \dots \circ \mu_2 \circ \mu_1$ is called a *mutation*.

Example 3.22 For a sect $H_1H_2H_3H_4$ such that

$$H_2H_3 = H_3H_2 \quad (3.4)$$

and

$$H_1H_3 = H_3H_1, \tag{3.5}$$

we have the following mutation composed of two elementary mutations:

$$H_1H_2H_3H_4 \xrightarrow{(3.4)} H_1H_3H_2H_4 \xrightarrow{(3.5)} H_3H_1H_2H_4. \tag{3.6}$$

The small category $S(G)$ is divided into equivalent sects, and the quotient of $S(G)$ under the equivalence relation is denoted by $S(G)/\sim$. Note that for a sect $\mathcal{H}$ of G, the sects of G equivalent to it are nothing but the mutants of $\mathcal{H}$.

As mutations permute factors of sects, the following result holds.

Lemma 3.23 *Let* $H_1H_2\dots H_n$ *be a sect of a group* G. *Then any sect of* G *equivalent to* $H_1H_2\dots H_n$ *is of the form* $H_{\sigma(1)}H_{\sigma(2)}\dots H_{\sigma(n)}$ *for some permutation* $\sigma \in \mathfrak{S}_n$, *and*

$$H_1H_2\dots H_n = H_{\sigma(1)}H_{\sigma(2)}\dots H_{\sigma(n)} \quad \textit{in the sect monoid } S(G)$$

The converse of Lemma 3.23 does *not* hold — "equal" and "equivalence" should not be confused: Even if

$$H_1H_2\dots H_n = H_{\sigma(1)}H_{\sigma(2)}\dots H_{\sigma(n)}$$

in $S(G)$, they are generally *not* equivalent in $S(G)$.

Remark 3.24 (Weak version) One may wonder that in defining mutation, instead of $H_iH_{i+1}\dots H_j$ being regular, it suffices to assume a weaker condition

$$H_iH_{i+1}\dots H_j = H_j\dots H_{i+1}H_i.$$

Yes, replacing regular subsects with self-reversal ones, we may define *weak elementary mutation*, *weak mutation*, and *weak equivalence*. However they are *not* good for our purpose, as weak equivalence is not functorial with respect to pullback via homomorphisms. In contrast, the equivalence in terms of regular subsects is functorial with respect to *both* pushforward and pullback via homomorphisms (Proposition 4.16).

Remark 3.25 (Advantage of regularity) Besides the functoriality stated in Remark 3.24, the concept of regularity of sects has another advantage. Noting that a regular sect is nothing but a sect that gives a

factorization of a subgroup, it fits inductive determination of factorizations of subgroups with respect to the orders of subgroups or the lengths of sects factorizing subgroups.

Quotient sect monoids

Consider sects of a group G. If

$$H_1H_2\dots\underline{H_iH_{i+1}\dots H_j}\dots H_n \sim H_1H_2\dots\underline{H_j\dots H_{i+1}H_i}\dots H_n \quad (3.7)$$

and

$$K_1K_2\dots\underline{K_kK_{k+1}\dots K_l}\dots K_m \sim K_1K_2\dots\underline{K_l\dots K_{k+1}K_k}\dots K_m, \quad (3.8)$$

then

$$H_1H_2\dots\underline{H_iH_{i+1}\dots H_j}\dots H_nK_1K_2\dots\underline{K_kK_{k+1}\dots K_l}\dots K_m$$

$$\sim H_1H_2\dots\underline{H_j\dots H_{i+1}H_i}\dots H_nK_1K_2\dots\underline{K_l\dots K_{k+1}K_k}\dots K_m.$$

In general, for sects $\mathcal{H},\mathcal{I},\mathcal{K},\mathcal{L}$ of the group G, if $\mathcal{H}\sim\mathcal{I}$ (via a mutation α) and $\mathcal{K}\sim\mathcal{L}$ (via a mutation β), then $\mathcal{HK}\sim\mathcal{IL}$ (via a mutation $\alpha\circ\beta\,(=\beta\circ\alpha)$). Thus the monoid structure on $S(G)$ (Definition 2.9) descends to the quotient set $S(G)/\sim$.

Definition 3.26 The quotient set $S(G)/\sim$ with induced monoid structure from $S(G)$ is called the *quotient sect monoid* of G.

Convention 3.27 For a mutation $\mu : H_1H_2\dots H_n \to K_1K_2\dots K_n$, the permutation of indices induced by it is also denoted by μ; therefore $H_1H_2\dots H_n$ is mapped to $H_{\mu(1)}H_{\mu(2)}\dots H_{\mu(n)}$, which coincides with $K_1K_2\dots K_n$, that is, $H_{\mu(i)} = K_i$ $(i = 1, 2, \dots, n)$ — this is stronger than "$H_{\mu(1)}H_{\mu(2)}\dots H_{\mu(n)}$ is equal to $K_1K_2\dots K_n$ as subsets o G".

Definition 3.28 Two prime factorizations

$$G = p_1p_2\dots p_l \quad \text{and} \quad G = q_1q_2\dots q_m$$

are *equivalent* if $l = m$ and there exists a mutation that maps one to the other — say, via a mutation $\mu : p_1p_2\dots p_l \to q_1q_2\dots q_l$, then

$$p_{\mu(i)} = q_i \qquad (i = 1, 2, \dots, l).$$

3.2 Mutation and irredundancy

In this section, we fix a group G and consider sects of G. Note first the following result.

Lemma 3.29 *A sect* $H_1H_2\dots H_n$ *is redundant* (*resp. irredundant*) *if and only if its reverse* $H_n\dots H_2H_1$ *is redundant* (*resp. irredundant*).

Proof — Note that, by symmetry, it suffices to show "$\Longrightarrow$". Suppose that $H_1H_2\dots H_n$ is redundant, say at H_k:

$$H_1H_2\dots\breve{H}_k\dots H_n = H_1H_2\dots H_n. \tag{3.9}$$

Taking the inverse yields $(H_1H_2\dots\breve{H}_k\dots H_n)^{-1} = (H_1H_2\dots H_n)^{-1}$, that is,

$$H_n\dots\breve{H}_k\dots H_2H_1 = H_n\dots H_2H_1. \tag{3.10}$$

This means that $H_n\dots H_2H_1$ is redundant at H_k. □

Remark 3.30 As seen from the proof of Lemma 3.29, the following holds: *A sect* $H_1H_2\dots H_n$ *is redundant at* H_k *if and only if its reverse* $H_n\dots H_2H_1$ *is redundant at* H_k.

The partial converse version of Lemma 3.29 does *not* hold — in general, there is *no* implication between

$$\text{"a sect } H_1H_2\dots\underbrace{H_iH_{i+1}\dots H_j}\dots H_n \text{ is redundant"}$$

and

$$\text{"its partial reverse } H_1H_2\dots\underbrace{H_j\dots H_{i+1}H_i}\dots H_n \text{ is redundant"}.$$

Similarly, there is *no* implication for irredundant sects.

Example 3.31 (1) For a sect $H_1\,\underbrace{H_2H_1}$, its partial reverse $H_1\,\underbrace{H_1H_2}$ is redundant (as $H_1H_1 = H_1$), no matter whether $H_1H_2H_1$ is redundant or not.

(2) For a sect $H_1\,\underbrace{H_2H_3}$ with $H_1 \supset H_3$, its partial reverse $H_1\,\underbrace{H_3H_2}$ is redundant (as $H_1H_3 = H_1$), no matter whether $H_1H_2H_3$ is redundant or not.

Let $H_iH_{i+1}\dots H_j$ be a subsect of a sect $H_1H_2\dots H_n$. By Lemma 3.29, the following holds: $H_iH_{i+1}\dots H_j$ *is redundant* (resp. *irredundant*) *if and only if its reverse* $H_j\dots H_{i+1}H_i$ *is redundant* (resp. *irredundant*). However, as shown by Example 3.31, the following equivalence does *not* hold:

(i) $H_1H_2\dots\underline{H_iH_{i+1}\dots H_j}\dots H_n$ *is redundant* (resp. *irredundant*)

(ii) *its partial inverse* $H_1H_2\dots\underline{H_j\dots H_{i+1}H_i}\dots H_n$ *is redundant* (resp. *irredundant*).

The following result however holds.

Lemma 3.32 *Let* $H_iH_{i+1}\dots H_j$ *be a self-reversal subsect of a sect*

$$H_1H_2\dots H_n$$

and H_k *be a factor of* $H_1H_2\dots H_n$ *outside* $H_iH_{i+1}\dots H_j$. *Then the following are equivalent:*

(i) H_k *is redundant* (*resp. irredundant*) *in*

$$H_1H_2\dots\underline{H_iH_{i+1}\dots H_j}\dots H_n$$

(ii) H_k *is redundant* (*resp. irredundant*) *in*

$$H_1H_2\dots\underline{H_j\dots H_{i+1}H_i}\dots H_n.$$

Proof — We only show "$\Longrightarrow$" (by symmetry, "$\Longleftarrow$" is shown in the same way). If H_k is redundant in $H_1H_2\dots\underline{H_iH_{i+1}\dots H_j}\dots H_n$, then

$$\begin{aligned} &H_1H_2\dots\breve{H}_k\dots\underline{H_iH_{i+1}\dots H_j}\dots H_n\\ &\quad= H_1H_2\dots\underline{H_iH_{i+1}\dots H_j}\dots H_n, \end{aligned} \tag{3.11}$$

where note that H_k lies outside $H_iH_{i+1}\dots H_j$ by assumption. Since

$$H_iH_{i+1}\dots H_j = H_j\dots H_{i+1}H_i \quad \text{by assumption,}$$

we may replace $H_iH_{i+1}\dots H_j$ in (3.11) with

$$H_j\dots H_{i+1}H_i,$$

hence

$$H_1H_2\dots\breve{H}_k\dots\underbrace{H_j\dots H_{i+1}H_i}\dots H_n$$
$$=H_1H_2\dots\underbrace{H_j\dots H_{i+1}H_i}\dots H_n.$$

This means that H_k is redundant in $H_1H_2\dots\underbrace{H_j\dots H_{i+1}H_i}\dots H_n$. □

Proposition 3.33 *Assume that* $H_iH_{i+1}\dots H_j$ *is a regular subsect of a sect* $H_1H_2\dots H_n$*; in particular* $H_iH_{i+1}\dots H_j$ *is self-reversal. Then the following hold:*

(1) *The mutation*

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

preserves (ir)redundancy at any factor H_k *outside* $H_iH_{i+1}\dots H_j$.

(2) *The mutation* μ *in* (1) *induces a mutation between the removals of* H_k:

$$\overline{\mu}:\ H_1H_2\dots\breve{H}_k\dots\underbrace{H_iH_{i+1}\dots H_j}\dots H_n$$
$$\longrightarrow H_1H_2\dots\breve{H}_k\dots\underbrace{H_j\dots H_{i+1}H_i}\dots H_n,$$

so

$$H_1H_2\dots\breve{H}_k\dots\underbrace{H_iH_{i+1}\dots H_j}\dots H_n$$
$$\sim H_1H_2\dots\breve{H}_k\dots\underbrace{H_j\dots H_{i+1}H_i}\dots H_n.$$

Moreover, it holds that $\overline{\mu}$ *preserves (ir)redundancy at any factor* H_l $(l\neq k)$ *outside* $H_iH_{i+1}\dots H_j$.

Proof — Note that (1) is a restatement of Lemma 3.32. We show (2). As $H_iH_{i+1}\dots H_j$ is regular and H_k lies outside $H_iH_{i+1}\dots H_j$, the mutation $\overline{\mu}$ is defined. By Lemma 3.32, $\overline{\mu}$ preserves (ir)redundancy at H_l. □

Remark 3.34 In Proposition 3.33, if H_k lies in $H_iH_{i+1}\dots H_j$, then $H_iH_{i+1}\dots\breve{H}_k\dots H_j$ is

(i) neither necessarily regular

(ii) nor necessarily self-reversal.

In general, it holds that

$$H_i H_{i+1} \dots \breve{H}_k \dots H_j \neq H_j \dots \breve{H}_k \dots H_{i+1} H_i, \tag{3.12}$$

so, in general,

$$\begin{aligned} & H_1 H_2 \dots \underbrace{H_i H_{i+1} \dots \breve{H}_k \dots H_j} \dots H_n \\ & \neq H_1 H_2 \dots \underbrace{H_j \dots \breve{H}_k \dots H_{i+1} H_i} \dots H_n. \end{aligned}$$

Moreover from (i), in general we *cannot* even define a mutation

$$\begin{aligned} & H_1 H_2 \dots \underbrace{H_i H_{i+1} \dots \breve{H}_k \dots H_j} \dots H_n \\ & \longrightarrow H_1 H_2 \dots \underbrace{H_j \dots \breve{H}_k \dots H_{i+1} H_i} \dots H_n. \end{aligned}$$

Remark 3.35 For an irredundant sect $\mathcal{H}$, if a mutant $\mathcal{H}'$ of $\mathcal{H}$ is redundant, let $\mathcal{H}'_{\text{irred}}$ be an irredundantization of $\mathcal{H}'$. Then the length of $\mathcal{H}'_{\text{irred}}$ is strictly shorter than that of $\mathcal{H}$, and $\mathcal{H}'_{\text{irred}}$ is said to be *semi-equivalent* to $\mathcal{H}$. Here "irredundantization removing redundant factors from a sect" is in spirit similar to "blowdown in algebraic geometry contracting an exceptional subvariety of a variety", and in this viewpoint, "semi-equivalence between sects" corresponds to "birationality between varieties".

4 Pushforward and pullback of sects

Let $\pi : G \to G'$ be a group homomorphism. For a sect $H_1H_2 \dots H_n$ of G, its image $\pi(H_1H_2 \dots H_n)$ is a sect of G'. Indeed

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

which is a sect of G', as $\pi(H_i)$ $(i = 1, 2, \dots, n)$ are subgroups of G'. For $n = 2$, we have $\pi(H_1H_2) = \pi(H_1)\pi(H_2)$. This means that π induces a monoid homomorphism $S(G) \to S(G')$ between the sect monoids of G and G'; note that the identity E of $S(G)$ is mapped to the identity E' of $S(G')$, where E (resp. E') is the identity subgroup of G (resp. G'). We formalize this below.

Lemma 4.1 *A homomorphism $\pi : G \to G'$ between groups induces a monoid homomorphism $\pi_* : S(G) \to S(G')$ between sect monoids.*

Consequently the following result holds.

Corollary 4.2 *Let $\pi : G \to G'$ be a homomorphism between groups. Then π maps relations of the sect monoid $S(G)$ to relations of $S(G')$: a relation $H_1H_2 \dots H_n = K_1K_2 \dots K_m$ is mapped to a relation*

$$\pi(H_1)\pi(H_2) \dots \pi(H_n) = \pi(K_1)\pi(K_2) \dots \pi(K_m).$$

Remark 4.3 In particular, π maps a self-reversal

$$H_1H_2 \dots H_n = H_n \dots H_2H_1$$

to a self-reversal $\pi(H_1)\pi(H_2) \dots \pi(H_n) = \pi(H_n) \dots \pi(H_2)\pi(H_1)$.

On the other hand for a sect $H'_1H'_2 \dots H'_n$ of G', in general

$$\pi^{-1}(H'_1H'_2 \dots H'_n) \neq \pi^{-1}(H'_1)\pi^{-1}(H'_2) \dots \pi^{-1}(H'_n) \qquad (4.1)$$

and, in addition, π^{-1} does not even define a monoid homomorphism $S(G') \to S(G)$. Note that in (4.1), the right hand side is a sect,

as $\pi^{-1}(H'_i)$ $(i = 1, 2, \ldots, n)$ are subgroups of G, whereas the left hand side is not necessarily a sect. In general, we merely have

$$\pi^{-1}(H'_1 H'_2 \ldots H'_n) \supset \pi^{-1}(H'_1)\pi^{-1}(H'_2)\ldots\pi^{-1}(H'_n). \tag{4.2}$$

Indeed

$$\begin{aligned}\pi^{-1}(H'_1 H'_2 \ldots H'_n) &= \bigcup_{\substack{h'_i \in H'_i \\ (i=1,2,\ldots,n)}} \pi^{-1}(h'_1 h'_2 \ldots h'_n) \\ &\supset \bigcup_{\substack{h'_i \in H'_i \\ (i=1,2,\ldots,n)}} \pi^{-1}(h'_1)\pi^{-1}(h'_2)\ldots\pi^{-1}(h'_n) \qquad (4.3) \\ &= \pi^{-1}(H'_1)\pi^{-1}(H'_2)\ldots\pi^{-1}(H'_n).\end{aligned}$$

where the inclusion is due to Remark 4.4 below.

Remark 4.4 The inclusion

$$\pi^{-1}(h'_1 h'_2 \ldots h'_n) \supset \pi^{-1}(h'_1)\pi^{-1}(h'_2)\ldots\pi^{-1}(h'_n)$$

is confirmed as follows: If $x \in \pi^{-1}(h'_1)\pi^{-1}(h'_2)\ldots\pi^{-1}(h'_n)$, then

$$x = y_1 y_2 \ldots y_n \quad \text{for some } y_i \in \pi^{-1}(h'_i).$$

Then

$$\pi(x) = \pi(y_1)\pi(y_2)\ldots\pi(y_n) = h'_1 h'_2 \ldots h'_n.$$

Thus $x \in \pi^{-1}(h'_1 h'_2 \ldots h'_n)$.

Definition 4.5 Let $\pi : G \to G'$ be a homomorphism between groups. Then the following hold:

(1) The *image* (or the *pushforward*) of a sect $H_1 H_2 \ldots H_n$ of G is a sect $\pi(H_1)\pi(H_2)\ldots\pi(H_n)$ of G'.

(2) The *pullback* of a sect $H'_1 H'_2 \ldots H'_n$ of G' is a sect

$$\pi^{-1}(H'_1)\pi^{-1}(H'_2)\ldots\pi^{-1}(H'_n)$$

of G. It is denoted by $\pi^*(H'_1H'_2\dots H'_n)$, which is generally not equal to $\pi^{-1}(H'_1H'_2\dots H'_n)$.

Caution 4.6 In (2), from the very definition of π^*, we have

$$\pi^*(H'_1H'_2) = \pi^*(H'_1)\pi^*(H'_2).$$

This however does *not* imply that $\pi^* : S(G') \to S(G)$ is a homomorphism. In fact this is not even well-defined — even if

$$H'_1H'_2\dots H'_n = K'_1K'_2\dots K'_m$$

in $S(G')$, their images may be distinct in $S(G)$: In general

$$\pi^*(H'_1H'_2\dots H'_n) \neq \pi^*(K'_1K'_2\dots K'_m),$$

that is, $\pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n) \neq \pi^{-1}(K'_1)\pi^{-1}(K'_2)\dots\pi^{-1}(K'_m)$ (distinct as subsets of G).

The following is a special case of Corollary 4.2.

Lemma 4.7 *Let $\pi : G \to G'$ be a homomorphism between groups. Then it maps a factorization $K = H_1H_2\dots H_n$ of a subgroup K of G to a factorization $\pi(K) = \pi(H_1)\pi(H_2)\dots\pi(H_n)$ of the subgroup $\pi(K)$ of G'.*

Remark 4.8 Even if $H_1H_2\dots H_n$ is irredundant,

$$\pi(H_1)\pi(H_2)\dots\pi(H_n)$$

is not necessarily irredundant, for instance, when $\pi(H_i) = \{1\}$, for some i, or when $\pi(H_1) = \pi(H_2)$ (then $\pi(H_1)$ or $\pi(H_2)$ is removable from $\pi(H_1)\pi(H_2)\dots\pi(H_n)$).

The following is immediate from Lemma 4.7.

Lemma 4.9 *Let $\pi : G \to G'$ be a group homomorphism. If $H_iH_{i+1}\dots H_j$ is a regular subsect of a sect $H_1H_2\dots H_n$, then its image*

$$\pi(H_i)\pi(H_{i+1})\dots\pi(H_j)$$

is a regular subsect of a sect $\pi(H_1)\pi(H_2)\dots\pi(H_n)$. In particular, it holds that $\pi(H_i)\pi(H_{i+1})\dots\pi(H_j)$ is self-reversal, i.e.

$$\pi(H_i)\pi(H_{i+1})\dots\pi(H_j) = \pi(H_j)\dots\pi(H_{i+1})\pi(H_i). \tag{4.4}$$

More generally if a sect $H_1H_2\dots H_n$ is self-reversal, then its image

$$\pi(H_1)\pi(H_2)\dots\pi(H_n)$$

is always self-reversal — a special case of Corollary 4.2: *pushforward preserves relations of* $S(G)$. In contrast, pullback generally does *not* preserve relations of $S(G')$ (see Caution 4.6). Nevertheless regular subsects are preserved — they are functorial under pullback (not only under pushforward). To show this, we begin with preparation.

Lemma 4.10 *Let* H *and* K *be subgroups of a group. If* $H \supset K$, *then*

$$HK = H.$$

Proof — By the multiplication-closedness of H, if $H \supset K$, then HK is equal to H. □

Now let $\pi : G \to G'$ be a *surjective* homomorphism between groups. Let $G' = H'_1H'_2\dots H'_n$ be a factorization of G'. Consider its preimage

$$\pi^{-1}(G') = \pi^{-1}(H'_1H'_2\dots H'_n).$$

Here $\pi^{-1}(G') = G$ and

$$\pi^{-1}(H'_1H'_2\dots H'_n) \supset \pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n),$$

as shown in (4.3). Thus

$$G \supset \pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n). \tag{4.5}$$

For brevity, we set $H_i := \pi^{-1}(H'_i)$; then $G \supset H_1H_2\dots H_n$. Actually $G = H_1H_2\dots H_n$ holds. To see this, we first show the following — the surjectivity of π is used for (2).

Claim 4.11 *The following statements are satisfied:*

(1) $\pi(H_1H_2\dots H_n) = G'$.

(2) *Let* N *be the kernel of* $\pi : G \to G'$. *Then* $G = H_1H_2\dots H_nN$.

Proof — (1) It is enough to observe that

$$\pi(H_1H_2\dots H_n) = \pi(H_1)\pi(H_2)\dots\pi(H_n) = H'_1H'_2\dots H'_n = G'.$$

(2) As π is surjective, we may assume that $G' = G/N$. Write G as a disjoint union of N-cosets, i.e.,

$$G = \coprod_{i \in I} a_i N.$$

Set $a_i' := a_i N$, then the quotient group G' consists of a_i' ($i \in I$), where in terms of π, a_i' is $\pi(a_i)$. Conversely for a subset J of I, the disjoint union $\coprod_{j \in J} a_j N$ coincides with G precisely when the quotient group G' consists of a_j' ($j \in J$), and in this case $J = I$.

Now write

$$H_1 H_2 \dots H_n N = \bigcup_{a \in H_1 H_2 \dots H_n} aN.$$

As the right hand side is a union of N-cosets, we may express it as a disjoint union:

$$H_1 H_2 \dots H_n N = \coprod_{j \in J} a_j N, \tag{4.6}$$

where $J \subset I$. Under π, this is mapped to

$$\pi(H_1 H_2 \dots H_n N) = \bigcup_{j \in J} \pi(a_j N),$$

which, as $\pi(N) = \{1\}$, is rewritten as $\pi(H_1 H_2 \dots H_n) = \{\pi(a_j)\}_{j \in J}$. Then by (1), $G' = \{\pi(a_j)\}_{j \in J}$, that is, G' consists of $a_j' := a_j N$ ($j \in J$). As explained above, this implies that $G = \coprod_{j \in J} a_j N$. This with (4.6) implies that $G = H_1 H_2 \dots H_n N$ (and $J = I$). □

The following result in fact holds.

Claim 4.12 *It holds that* $G = H_1 H_2 \dots H_n$.

Proof — From Claim 4.11 (2), it suffices to show that

$$H_1 H_2 \dots H_n N = H_1 H_2 \dots H_n.$$

As $1 \in H_i$ ($i = 1, 2, \dots, n$), we have

$$\pi^{-1}(\{1\}) \subset \pi^{-1}(H_i'),$$

that is, $N \subset H_i$. Then $H_i N = H_i$ by Lemma 4.10. In particular, we obtain that $H_n N = H_n$, so $H_1 H_2 \dots H_n N = H_1 H_2 \dots H_n$. □

Lemma 4.13 *Let $\pi : G \to G'$ be a* surjective *homomorphism between groups. For a factorization $G' = H'_1 H'_2 \dots H'_n$ of G', setting*

$$H_i := \pi^{-1}(H'_i),$$

then the following hold:

(1) $G = H_1 H_2 \dots H_n$.

(2) *If $G' = H'_1 H'_2 \dots H'_n$ is irredundant, then $G = H_1 H_2 \dots H_n$ in* (1) *is also irredundant.*

Proof — (1) is nothing but Claim 4.12. We show (2) by contradiction. Suppose that $H_1 H_2 \dots H_n$ is redundant, say at H_j. Then

$$H_1 H_2 \dots \check{H}_j \dots H_n = H_1 H_2 \dots H_n,$$

so

$$\pi(H_1)\pi(H_2)\dots\widetilde{\pi(H_j)}\dots\pi(H_n) = \pi(H_1)\pi(H_2)\dots\pi(H_n), \tag{4.7}$$

that is, $H'_1 H'_2 \dots \check{H}'_j \dots H'_n = H'_1 H'_2 \dots H'_n$. This means that H'_j is redundant, which contradicts the irredundancy of $H'_1 H'_2 \dots H'_n$. □

Remark 4.14 In Lemma 4.13, the surjectivity of π is inevitable. For instance, consider an injective homomorphism $\pi : G \hookrightarrow G'$. Then for a factorization $G' = H'_1 H'_2 \dots H'_n$, in general

$$\pi^{-1}(G') \neq \pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n), \tag{4.8}$$

that is, $G \neq \pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n)$. Or regarding G as a subgroup of G' via π, in general

$$G \neq (H'_1 \cap G)(H'_2 \cap G)\dots(H'_n \cap G),$$

where the right hand side is generally strictly smaller than G. Note that any homomorphism $\pi : G \to G'$ is expressed as a composition

$$\pi : G \xrightarrow{\alpha} \pi(G) \xhookrightarrow{\beta} G',$$

where α and β are surjective and injective homomorphisms respec-

tively. If π is not surjective, then β is nontrivial, and in general

$$\pi^{-1}(G') \neq \pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n).$$

Corollary 4.15 *Let $\pi : G \to G'$ be a* surjective *homomorphism between groups. For a factorization $K' = H'_1H'_2\dots H'_n$ of a subgroup K' of G', the following hold:*

(1) $K = \pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n)$, *where $K := \pi^{-1}(K')$ is a subgroup of G.*

(2) *If $K' = H'_1H'_2\dots H'_n$ is irredundant, then*

$$K = \pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n)$$

in (1) *is also irredundant.*

Proof — Apply Lemma 4.13 to the restriction $\pi|_K : K \to K'$ (which is a surjective homomorphism). □

We summarize the above results as follows.

Proposition 4.16 (Functoriality) *Let $\pi : G \to G'$ be a homomorphism between groups. Then the following hold:*

(1) *For a factorization $K = H_1H_2\dots H_n$, setting*

$$K' := \pi(K) \quad \textit{and} \quad H'_i := \pi(H_i) \qquad (i = 1, 2, \dots, n),$$

then $K' = H'_1H'_2\dots H'_n$ (see Lemma 4.7*). Here, even if the factorization $K = H_1H_2\dots H_n$ is irredundant, $K' = H'_1H'_2\dots H'_n$ is not necessarily irredundant (see* Remark 4.8*).*

(2) *Suppose that the homomorphism π is surjective. Then, for a factorization $K' = H'_1H'_2\dots H'_n$, setting*

$$K := \pi^{-1}(K') \quad \textit{and} \quad H_i := \pi^{-1}(H'_i) \qquad (i = 1, 2, \dots, n),$$

then $K = H_1H_2\dots H_n$, where if $K' = H'_1H'_2\dots H'_n$ is irredundant, then $K = H_1H_2\dots H_n$ is also irredundant (see Corollary 4.15*).*

Definition 4.17 In Proposition 4.16:

(i) The factorization $K' = H'_1H'_2\dots H'_n$ in (1) is called the *image* (or *pushforward*) of $K = H_1H_2\dots H_n$.

(ii) The factorization $K = H_1 H_2 \dots H_n$ in (2) is called the *pullback* of $K' = H'_1 H'_2 \dots H'_n$.

Remark 4.18 Let $\pi : G \to G'$ be a surjective homomorphism between groups. Prime factorizations of G' are generally *not* preserved under pullback. Similarly, prime factorizations of G are generally *not* preserved under pushforward — but in an "opposite" way:

(1) Pullback: For a prime factorization $G' = \mathfrak{p}'_1 \mathfrak{p}'_2 \dots \mathfrak{p}'_l$, its pullback $G = \mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_l$, where $\mathfrak{P}_i = \pi^{-1}(\mathfrak{p}'_i)$, is irredundant (see Lemma 4.13 (2)), but $\mathfrak{P}_i$ may not be cyclic.

(2) Pushforward: For a prime factorization $G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m$, its image $G' = \mathfrak{Q}_1 \mathfrak{Q}_2 \dots \mathfrak{Q}_m$, where $\mathfrak{Q}_i := \pi(\mathfrak{p}_i)$, may not be irredundant (see Remark 4.8), but every $\mathfrak{Q}_i$ is cyclic (of prime power order, as it divides the prime power order of $\mathfrak{p}_i$).

4.1 Pushforward and pullback of mutations

We state immediate consequences of Proposition 4.16 (1).

Lemma 4.19 (Pushforward of mutation) *Let $\pi : G \to G'$ be a homomorphism between groups. Let $H_1 H_2 \dots H_n$ be a sect of G with a regular subsect $H_i H_{i+1} \dots H_j$. Then by Proposition 4.16 (1), its pushforward (or its image)*

$$\pi(H_i)\pi(H_{i+1}) \dots \pi(H_j)$$

is a regular subsect of $\pi(H_1)\pi(H_2) \dots \pi(H_n)$, and the following holds:

(i) *A mutation*

$$\begin{aligned} \mu : H_1 H_2 \dots \underbrace{H_i H_{i+1} \dots H_j} \dots H_n \\ \longrightarrow H_1 H_2 \dots \underbrace{H_j \dots H_{i+1} H_i} \dots H_n \end{aligned} \tag{4.9}$$

is pushed forward to a mutation

$$\begin{aligned} \overline{\mu} : \pi(H_1)\pi(H_2) \dots \underbrace{\pi(H_i)\pi(H_{i+1}) \dots \pi(H_j)} \dots \pi(H_n) \\ \longrightarrow \pi(H_1)\pi(H_2) \dots \underbrace{\pi(H_j) \dots \pi(H_{i+1})\pi(H_i)} \dots \pi(H'_n). \end{aligned} \tag{4.10}$$

(ii) *Accordingly an equivalence*

$$H_1H_2\dots\underbrace{H_iH_{i+1}\dots H_j}\dots H_n \sim H_1H_2\dots\underbrace{H_j\dots H_{i+1}H_i}\dots H_n \tag{4.11}$$

is pushed forward to an equivalence

$$\begin{aligned}&\pi(H_1)\pi(H_2)\dots\underbrace{\pi(H_i)\pi(H_{i+1})\dots\pi(H_j)}\dots\pi(H_n)\\ &\quad\sim \pi(H_1)\pi(H_2)\dots\underbrace{\pi(H_j)\dots\pi(H_{i+1})\pi(H_i)}\dots\pi(H_n).\end{aligned} \tag{4.12}$$

Recall that for sects $\mathcal{H},\mathcal{I},\mathcal{K},\mathcal{L}$ of G, if the following hold:

(i) $\mathcal{H}\sim\mathcal{I}$ (via a mutation α)

(ii) $\mathcal{K}\sim\mathcal{L}$ (via a mutation β),

then

$$\mathcal{H}\mathcal{K}\sim\mathcal{I}\mathcal{L} \tag{4.13}$$

via a mutation $\alpha\circ\beta=\beta\circ\alpha$ (see the paragraph above Definition 3.26). By Lemma 4.19 (ii), from (i) and (ii) we have $\pi(\mathcal{H})\sim\pi(\mathcal{I})$ (via a mutation $\overline{\alpha}$) and $\pi(\mathcal{K})\sim\pi(\mathcal{L})$ (via a mutation $\overline{\beta}$). Then, as in (4.13),

$$\pi(\mathcal{H})\pi(\mathcal{K})\sim\pi(\mathcal{I})\pi(\mathcal{L})$$

via a mutation $\overline{\alpha}\circ\overline{\beta}=\overline{\beta}\circ\overline{\alpha}$. Therefore the following result holds.

Proposition 4.20 *Let $\pi:G\to G'$ be a homomorphism between groups. Then the monoid homomorphism $\pi_*:S(G)\to S(G')$ induced from π descends to a monoid homomorphism $\overline{\pi_*}:S(G)/\sim\to S(G')/\sim$ between quotient sect monoids.*

We next state immediate consequences of Proposition 4.16 (2).

Lemma 4.21 (Pullback of mutation) *Let $\pi:G\to G'$ be a* surjective *homomorphism. Let $H'_1H'_2\dots H'_n$ be a sect of G' with a regular subsect $H'_iH'_{i+1}\dots H'_j$. Then by* Proposition 4.16 (2)*, its pullback*

$$\pi^{-1}(H'_i)\pi^{-1}(H'_{i+1})\dots\pi^{-1}(H'_j)$$

is a regular subsect of $\pi^{-1}(H'_1)\pi^{-1}(H'_2)\dots\pi^{-1}(H'_n)$, and the following holds:

(i) *A mutation*

$$\begin{aligned}\mu : H_1'H_2'\dots\underbrace{H_i'H_{i+1}'\dots H_j'}\dots H_n' \\ \longrightarrow H_1'H_2'\dots\underbrace{H_j'\dots H_{i+1}'H_i'}\dots H_n'\end{aligned} \tag{4.14}$$

is pulled back to a mutation

$$\begin{aligned}\widetilde{\mu} : \pi^{-1}(H_1')\pi^{-1}(H_2')\dots\underbrace{\pi^{-1}(H_i')\pi^{-1}(H_{i+1}')\dots\pi^{-1}(H_j')}\dots\pi^{-1}(H_n') \\ \longrightarrow\pi^{-1}(H_1')\pi^{-1}(H_2')\dots\underbrace{\pi^{-1}(H_j')\dots\pi^{-1}(H_{i+1}')\pi^{-1}(H_i')}\dots\pi^{-1}(H_n').\end{aligned}$$

(ii) *Accordingly an equivalence*

$$\begin{aligned}H_1'H_2'\dots\underbrace{H_i'H_{i+1}'\dots H_j'}\dots H_n' \\ \sim H_1'H_2'\dots\underbrace{H_j'\dots H_{i+1}'H_i'}\dots H_n'\end{aligned} \tag{4.15}$$

is pulled back to an equivalence

$$\begin{aligned}\pi^{-1}(H_1')\pi^{-1}(H_2')\dots\underbrace{\pi^{-1}(H_i')\pi^{-1}(H_{i+1}')\dots\pi^{-1}(H_j')}\dots\pi^{-1}(H_n') \\ \sim \pi^{-1}(H_1')\pi^{-1}(H_2')\dots\underbrace{\pi^{-1}(H_j')\dots\pi^{-1}(H_{i+1}')\pi^{-1}(H_i')}\dots\pi^{-1}(H_n').\end{aligned}$$

Remark 4.22 Lemma 4.21 (ii) does *not* ensure that there is a homomorphism $\overline{\pi^*} : S(G')/\sim \to S(G)/\sim$, because in the first place,

$$\pi^* : S(G') \to S(G)$$

is generally not even well-defined (see Caution 4.6), so there is *no* counterpart of Proposition 4.20.

In the following, (1) and (2) are consequences of Lemma 4.19 (ii) and Lemma 4.21 (ii), respectively.

Corollary 4.23 *Let $\pi : G \to G'$ be a homomorphism between groups.*

(1) *If two factorizations $G = H_1H_2\dots H_n$ and $G = K_1K_2\dots K_m$ are*

equivalent, then their images

$$\pi(G) = H'_1 H'_2 \dots H'_n \quad \textit{and} \quad \pi(G) = K'_1 K'_2 \dots K'_m$$

are equivalent, where $H'_i := \pi(H_i)$ *and* $K'_j := \pi(K_j)$. *Alternatively: If* $\pi(G) = H'_1 H'_2 \dots H'_n$ *and* $\pi(G) = K'_1 K'_2 \dots K'_m$ *are inequivalent, then* $G = H_1 H_2 \dots H_n$ *and* $G = K_1 K_2 \dots K_m$ *are inequivalent.*

(2) *Suppose that* π *is surjective. If two factorizations* $G' = H'_1 H'_2 \dots H'_n$ *and* $G' = K'_1 K'_2 \dots K'_m$ *are equivalent, then their pullbacks*

$$G = H_1 H_2 \dots H_n \quad \textit{and} \quad G = K_1 K_2 \dots K_m$$

are equivalent, where $H_i := \pi^{-1}(H'_i)$ *and* $K_j := \pi^{-1}(K'_j)$. *Alternatively: If* $G' = H'_1 H'_2 \dots H'_n$ *and* $G' = K'_1 K'_2 \dots K'_m$ *are inequivalent, then* $G = H_1 H_2 \dots H_n$ *and* $G = K_1 K_2 \dots K_m$ *are inequivalent.*

4.2 Refinement and irreducibility of sects

There are two fundamental operations on sects, from which key concepts are defined:

$$\begin{cases} \text{1. removal of factors} \rightsquigarrow \text{(ir)redundancy,} \\ \text{2. splitting of factors} \rightsquigarrow \text{(ir)reducibility.} \end{cases}$$

We already defined (ir)redundancy of sects. We shall define (ir)reducibility of sects.

Definition 4.24 (1) A sect $H_1 H_2 \dots H_n$ of a group G is *reducible* if some factor H_i splits nontrivially, i.e. admits a nontrivial irredundant factorization

$$H_i = K_1 K_2 \dots K_m \qquad (m \geqslant 2).$$

Otherwise, i.e. if *no* factor H_i $(i = 1, 2, \dots, n)$ splits nontrivially, then $H_1 H_2 \dots H_n$ is *irreducible*.

(2) A factorization $G = H_1 H_2 \dots H_n$ is *(ir)reducible* if $H_1 H_2 \dots H_n$ is so.

(Ir)redundancy and (ir)reducibility are far from equivalent.

Example 4.25 For a redundant sect H_1H_1, if the group H_1 is cyclic of prime power orders, then H_1 has no nontrivial splitting (see Theorem 3.13), so H_1H_1 is irreducible.

From the definition of irreducibility, (1) of the following holds, while (2) follows from (1).

Lemma 4.26 (1) *A subgroup H of a group is irreducible* (*as a sect of length* 1) *if and only if H is atomic.*

(2) *A sect $H_1H_2 \dots H_n$ of a group is irreducible if and only if every factor H_i is atomic.*

Remark 4.27 A prime factorization $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$ is nothing but an irredundant irreducible factorization, i.e. $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$ is irredundant and irreducible.

For finite groups, atomic subgroups are cyclic groups of prime power orders (see Theorem 3.13). The following is a consequence of Lemma 4.26 (2).

Corollary 4.28 *A sect $H_1H_2 \dots H_n$ of a finite group is irreducible if and only if every factor H_i is cyclic of prime power order.*

Let $\pi : G \to G'$ be a homomorphism between groups. For an *irredundant* sect $H'_1H'_2 \dots H'_n$ of G', its pullback

$$H_1H_2 \dots H_n \quad (\text{where } H_i := \pi^{-1}(H'_i))$$

is also irredundant (see Lemma 4.13), but even if $H'_1H'_2 \dots H'_n$ is *irreducible*, its pullback $H_1H_2 \dots H_n$ is not necessarily irreducible — even if H'_i is cyclic of prime power order, H_i may not be so.

Refinements of sects

Let $H_1H_2 \dots H_n$ be a sect of a group. If H_i ($i = 1, 2, \dots, n$) admits an *irredundant* factorization, say $H_i = K_{i,1}K_{i,2} \dots K_{i,l_i}$ (this factorization may be trivial, i.e. $H_i = H_i$), then substituting them into $H_1H_2 \dots H_n$ yields

$$\begin{aligned} &H_1H_2 \dots H_n \\ &= K_{1,1}K_{1,2} \dots K_{1,l_1}K_{2,1}K_{2,2} \dots K_{2,l_2} \dots K_{n,1}K_{n,2} \dots K_{n,l_n}. \end{aligned} \tag{4.16}$$

Definition 4.29 The sect on the right hand side of (4.16) is a *refinement* of $H_1H_2\dots H_n$. The *trivial refinement* is $H_1H_2\dots H_n$ itself.

Even if $H_1H_2\dots H_n$ is irredundant, its refinement may not be irredundant.

Example 4.30 If H_1H_2 is an irredundant sect of an *abelian* group with factorizations $H_1 = AB$ and $H_2 = AC$, then

$$H_1H_2 = ABAC = AABC.$$

Here $AABC$ is redundant, as $AA = A$.

We show some result needed for our subsequent construction. Recall that for a sect $H_1H_2\dots H_n$, we have

$$H_i \subset H_1H_2\dots H_n \quad \text{for } i = 1, 2, \dots, n$$

(see Lemma 2.1). Moreover the following result holds.

Lemma 4.31 *If a sect* $H_1H_2\dots H_n$ $(n \geqslant 2)$ *is irredundant, then*

$$H_i \subsetneq H_1H_2\dots H_n \quad \textit{for} \quad i = 1, 2, \dots, n. \tag{4.17}$$

Proof — As $H_1H_2\dots H_n$ is irredundant,

$$H_1H_2\dots \breve{H}_k\dots H_n \subsetneq H_1H_2\dots H_n \quad \text{for any } k = 1, 2, \dots, n.$$

On the other hand, $H_i \subset H_1H_2\dots \breve{H}_k\dots H_n$ for any $i = 1, 2, \dots, \breve{k}, \dots n$ (see Lemma 2.1). Hence, $H_i \subsetneq H_1H_2\dots H_n$. As $k \in \{1, 2, \dots, n\}$ is arbitrary, this holds for arbitrary $i \in \{1, 2, \dots, n\}$.
Another proof by contradiction: If $H_i = H_1H_2\cdots H_n$, then

$$H_1, H_2, \dots, \breve{H}_i, \dots, H_n$$

are removable from the right hand side. This contradicts the assumption that $H_1H_2\dots H_n$ is irredundant. □

Remark 4.32 If a sect $H_1H_2\dots H_n$ $(n \geqslant 2)$ is redundant, possibly $H_i = H_1H_2\dots H_n$. For example, $H_1 = H_1H_1$.

For sects of *finite* groups, the following result holds from (4.17).

Corollary 4.33 *Let* $H_1H_2\dots H_n$ $(n \geqslant 2)$ *be an irredundant sect of a finite group. Then* $|H_i| < |H_1H_2\dots H_n|$ *for* $i = 1, 2, \dots, n$.

Applying this to irredundant factorizations yields the following result.

Corollary 4.34 *Let* $K = H_1 H_2 \dots H_n$ $(n \geqslant 2)$ *be an irredundant factorization of a subgroup* K *of a finite group. Then* $|H_i| < |K|$ *for* $i = 1, 2, \dots, n$.

Let $H_1 H_2 \dots H_n$ be a sect of a *finite* group G. We show that the procedure of refinements of $H_1 H_2 \dots H_n$ terminates at at most finite steps, yielding an irreducible sect. If every H_i is atomic, then we have that $H_1 H_2 \dots H_n$ itself is irreducible, and there is nothing to show. Otherwise let

$$H_i = H_{i,1} H_{i,2} \dots H_{i,n_i} \quad (n_i \geqslant 2)$$

be a *nontrivial* irredundant factorization of H_i. Thus, if every factor $H_{i,j}$ $(j = 1, 2, \dots, n_i)$ is atomic, then the procedure stops. Otherwise, let

$$H_{i,j} = H_{i,j,1} H_{i,j,2} \dots H_{i,j,n_{i,j}} \quad (n_{i,j} \geqslant 2)$$

be a *nontrivial* irredundant factorization of $H_{i,j}$. If every

$$H_{i,j,k} \quad (k = 1, 2, \dots, n_{i,j})$$

is atomic, then the procedure stops. Otherwise, we repeat the procedure and obtain, by Corollary 4.34, a strictly decreasing sequence

$$|H_i| > |H_{i,j}| > |H_{i,j,k}| > \dots,$$

which terminates at *at most* $|G|$ steps (for any H_i), and so we reach an irreducible sect.

Caution: Even if we begin with irredundant $H_1 H_2 \dots H_n$, the resulting irreducible sect is not necessarily irredundant (as seen from Example 4.30).

Factorization version: If $G = H_1 H_2 \dots H_n$ is a factorization of a finite group G, then as above, $|H_i| > |H_{i,j}| > |H_{i,j,k}| > \dots$, and this procedure terminates at at most $|G|$ steps, and obtain an irreducible factorization of G (which is not necessarily irredundant). Note: If we begin with an *irredundant* factorization $G = H_1 H_2 \dots H_n$, then

$$|G| > |H_i| > |H_{i,j}| > |H_{i,j,k}| > \dots$$

We formalize the above results as follows.

Theorem 4.35 *The procedure of refinements of a sect of a finite group terminates at finite steps. Similarly the procedure of refinements of a factorization of a finite group terminates at finite steps.*

In contrast, for infinite groups, the procedure of refinements of a sect does not necessarily terminate at finite steps:

Example 4.36 Any subgroup of the additive group $\mathbb{Z}$ of integers admits a *nontrivial* irredundant factorization (see Proposition 3.17), so any factorization $\mathbb{Z} = H_1 H_2 \dots H_n$ ($n \geqslant 2$) admits a further (nontrivial) refinement, and the procedure of refinements of $\mathbb{Z}$ lasts infinitely.

4.3 Pullback of prime factorizations

Let N be a *nontrivial proper* normal subgroup of a group G and

$$\pi : G \to G' := G/N$$

be the quotient homomorphism. Let

$$G' = H_1' H_2' \dots H_n'$$

be an *irredundant* factorization of G' and

$$G = \pi^{-1}(H_1')\pi^{-1}(H_2') \dots \pi^{-1}(H_n')$$

be its pullback. For later application, we consider the case that each factor $\pi^{-1}(H_i')$ is either of the following:

(i) a cyclic group $\mathfrak{p}_i$ of prime power order such that $N \subset \mathfrak{p}_i$, or

(ii) a semidirect product $\mathfrak{p}_i \ltimes N$ (i.e. $\mathfrak{p}_i N$ with $\mathfrak{p}_i \cap N = \{1\}$) for some cyclic group $\mathfrak{p}_i$ of prime power order.

Definition 4.37 Depending on (i) or (ii), $\pi^{-1}(H_i')$ is of *single type* or *double type*.

Lemma 4.38 *If $\pi^{-1}(H_i')$ is of single type or double type, then the following hold:*

(1) $\pi(\mathfrak{p}_i) = H_i'$. *Here in the case of single type,* $\pi(\mathfrak{p}_i) = \mathfrak{p}_i/N$, *while in the case of double type,* $\pi(\mathfrak{p}_i) \simeq \mathfrak{p}_i$ *canonically* (*convention: We identify* $\pi(\mathfrak{p}_i)$ *with* $\mathfrak{p}_i$). *Consequently,*

$$H_i' = \begin{cases} \mathfrak{p}_i/N & (\textit{single type}), \\ \mathfrak{p}_i & (\textit{double type}). \end{cases}$$

(2) H_i' *is cyclic of prime power order.*

Proof — (1) For single type, from $\pi^{-1}(H_i') = \mathfrak{p}_i$ we have $H_i' = \pi(\mathfrak{p}_i)$. As $\mathfrak{p}_i \supset N$, we have $\pi(\mathfrak{p}_i) = \mathfrak{p}_i/N$. For double type, from

$$\pi^{-1}(H_i') = \mathfrak{p}_i N$$

we have $H_i' = \pi(\mathfrak{p}_i N) = \pi(\mathfrak{p}_i)$ as $\pi(N) = \{1\}$. Here $\pi(\mathfrak{p}_i) \simeq \mathfrak{p}_i$ canonically. In fact,

$$\pi : G \to G' := G/N$$

maps $\mathfrak{p}_i$ injectively into G', as $\mathfrak{p}_i \cap N = \{1\}$.

(2) For single type, $H_i' = \mathfrak{p}_i/N$ by (1), which is cyclic of prime power order, as it is a quotient of a cyclic group of prime power order. For double type, $H_i' = \mathfrak{p}_i$ by (1), which is cyclic of prime power order by assumption. □

Definition 4.39 An irredundant factorization

$$G' = H_1' H_2' \dots H_n'$$

is π-*primary* if $\pi^{-1}(H_i')$ $(i = 1, 2, \dots, n)$ is of either single or double type.

From Lemma 4.38 (2), the following result holds.

Corollary 4.40 *If* $G' = H_1' H_2' \dots H_n'$ *is a* π*-primary irredundant factorization, then every* H_i' *is cyclic of prime power order, and* $G' = H_1' H_2' \dots H_n'$ *is a prime factorization of* G'.

In what follows, suppose that $G' = H_1' H_2' \dots H_n'$ is π-primary and let $G = H_1 H_2 \dots H_n$ be its pullback, where $H_i := \pi^{-1}(H_i')$ is $\mathfrak{p}_i N$ for double type and $\mathfrak{p}_i$ for single type.

Claim 4.41 *Depending on whether*

(a) *every* H_i $(i = 1, 2, \dots, n)$ *is of double type*

or

(b) *at least one* H_i *is of single type,* G *has the following factorization:*

$$G = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_n N & \textit{in the case of (a)}, \\ \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_n & \textit{in the case of (b)}. \end{cases} \tag{4.18}$$

Proof — Note first that regardless of single type or double type,

$$\mathfrak{p}_i N = N\mathfrak{p}_i \quad (\text{as N is normal in G}) \tag{4.19}$$

and $N\mathfrak{p}_i N = \mathfrak{p}_i NN = \mathfrak{p}_i N$ (as $NN = N$). Besides, for single type,

$$\mathfrak{p}_i N = N\mathfrak{p}_i = \mathfrak{p}_i \quad (\text{as } N \subset \mathfrak{p}_i). \tag{4.20}$$

The assertion is then confirmed as follows:
(a) Since every H_i $(i = 1, 2, \dots, n)$ is of double type, using (4.19) we may rewrite $G = H_1H_2\dots H_n$ as follows:

$$\begin{aligned} G &= \mathfrak{p}_1 N\mathfrak{p}_2 N\dots\mathfrak{p}_n N \\ &= \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_n NN\dots N \\ &= \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_n N \end{aligned} \tag{4.21}$$

where, in the last equality, we use $NN\dots N = N$.
(b) Say H_k is of single type, then for a double type $\mathfrak{p}_j N$ if any, in $H_1H_2\dots H_n$ we shift N and then make N disappear as follows:

$$\begin{aligned} H_1H_2\dots H_n &= \dots\mathfrak{p}_j N\dots\mathfrak{p}_k\dots \\ &= \dots\mathfrak{p}_j\dots N\mathfrak{p}_k\dots \qquad \text{by (4.19)} \\ &= \dots\mathfrak{p}_j\dots\mathfrak{p}_k\dots \qquad \text{by (4.20)} \end{aligned} \tag{4.22}$$

Thus $G = H_1H_2\dots H_n$ is rewritten as $G = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_n$. □

In Claim 4.41, the following further result holds.

Claim 4.42 *For a π-primary irredundant factorization*

$$G' = H_1'H_2'\dots H_n',$$

depending on whether

(a) *every* $H_i := \pi^{-1}(H_i)$ $(i = 1, 2, \dots, n)$ *is of double type*

or

(b) *at least one* H_i *is of single type, the following hold:*

(a) *Either*

(a1) $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n N$ *is irredundant*

or

(a2) $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n N$ *is redundant at* N *and* $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$ *is irredundant.*

(b) $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$ *is irredundant.*

Proof — (a) If $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n N$ is *not* irredundant, there are two possibilities:
Case 1 Some $\mathfrak{p}_j$ is redundant.
Case 2 N is redundant.

We first show that Case 1 does *not* occur. Otherwise

$$G = \mathfrak{p}_1\mathfrak{p}_2 \dots \breve{\mathfrak{p}}_j \dots \mathfrak{p}_n N.$$

This is under π mapped to

$$G' = \pi(\mathfrak{p}_1)\pi(\mathfrak{p}_2) \dots \widetilde{\pi(\mathfrak{p}_j)} \dots \pi(\mathfrak{p}_n)\pi(N) = H_1'H_2' \dots \breve{H}_j' \dots H_n'$$

as $\pi(\mathfrak{p}_i) = H_i'$ (see Lemma 4.38 (1)) and $\pi(N) = \{1\}$. That is,

$$G' = H_1'H_2' \dots \breve{H}_j' \dots H_n'. \tag{4.23}$$

This contradicts the irredundancy of $G' = H_1'H_2' \dots H_n'$. Hence, Case 2 occurs, and $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$. We claim that this is irredundant. Otherwise, say it is redundant at $\mathfrak{p}_j$. Then

$$G = \mathfrak{p}_1\mathfrak{p}_2 \dots \breve{\mathfrak{p}}_j \dots \mathfrak{p}_n,$$

which is under π mapped to

$$G' = \pi(\mathfrak{p}_1)\pi(\mathfrak{p}_2) \dots \widetilde{\pi(\mathfrak{p}_j)} \dots \pi(\mathfrak{p}_n) = H_1'H_2' \dots \breve{H}_j' \dots H_n'.$$

That is, $G' = H'_1 H'_2 \dots \overset{\vee}{H}{}'_j \dots H'_n$. This contradicts the irredundancy of $G' = H'_1 H'_2 \dots H'_n$. Therefore $G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n$ is irredundant.

(b) As in Case 2 of (a), we can show that if $G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n$ is not irredundant, then $G' = H'_1 H'_2 \dots H'_n$ is not irredundant (a contradiction). □

Moreover the following result holds.

Claim 4.43 *Depending on whether*

(a) *every* H_i $(i = 1, 2, \dots, n)$ *is of double type*

or

(b) *at least one* H_i *is of single type, the following hold:*

(a) *The irredundant factorization* $G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n$ *in* (a2) *of* Claim 4.42 *is a prime factorization. Moreover if* N *is cyclic of prime power order, the irredundant factorization* $G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n N$ *in* (a1) *is also a prime factorization.*

(b) *The irredundant factorization* $G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n$ *in* (b) *of* Claim 4.42 *is a prime factorization.*

Proof — Any of these irredundant factorizations is *primary* (i.e. every factor is cyclic of prime power order), therefore it is a prime factorization. □

Claim 4.43 yields the following result.

Claim 4.44 *Suppose that* N *is cyclic of prime power order. Then from any* π*-primary irredundant factorization of* G'*, we obtain a prime factorization of* G.

Definition 4.45 The prime factorization of G obtained in Claim 4.44 is called the *induced prime factorization* of G from a π-primary irredundant factorization of G'. Explicitly it is given by

$$\begin{cases} \text{(i)} \quad G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n & \text{in the case of (a2) or (b),} \\ \text{(ii)} \quad G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n N & \text{in the case of (a1).} \end{cases} \tag{4.24}$$

Notation: For the convenience of description, we express the induced prime factorization as $G = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_l$, where we set

$$\begin{cases} \text{(i)} \quad l := n & \text{in the case of (a2) or (b),} \\ \text{(ii)} \quad l := n + 1 \text{ and } \mathfrak{p}_l := N & \text{in the case of (a1).} \end{cases} \tag{4.25}$$

Claim 4.46 *The homomorphism* $\pi : G \to G'$ *maps the induced prime factorization* $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_l$ *to* $G' = H'_1H'_2 \dots H'_n$.

Proof — We separate into two cases as in (4.25).
(i) In this case, $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$, so

$$\pi(G) = \pi(\mathfrak{p}_1)\pi(\mathfrak{p}_2) \dots \pi(\mathfrak{p}_n) = H'_1H'_2 \dots H'_n$$

as $\pi(\mathfrak{p}_i) = H'_i$ (see Lemma 4.38 (1)). On the other hand, it holds that $\pi(G) = G'$ (by the surjectivity of π). Hence the image is

$$G' = H'_1H'_2 \dots H'_n.$$

(ii) In this case, $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_nN$. Since $\pi(N) = \{1\}$, we have

$$\pi(G) = \pi(\mathfrak{p}_1)\pi(\mathfrak{p}_2) \dots \pi(\mathfrak{p}_n) = H'_1H'_2 \dots H'_n.$$

Since $\pi(G) = G'$, the image is

$$G' = H'_1H'_2 \dots H'_n$$

which completes the proof. □

The following result plays a key role in our later discussion.

Lemma 4.47 *Let* G *be a finite group and* N *be a nontrivial proper normal cyclic subgroup of prime power order of* G. *Let* $\pi : G \to G' := G/N$ *be the quotient homomorphism. If*

$$G' = H'_1H'_2 \dots H'_n \quad \textit{and} \quad G' = K'_1K'_2 \dots K'_m$$

are π*-primary* inequivalent *prime factorizations of* G', *then the induced prime factorizations*

$$G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_l \quad \textit{and} \quad G = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_k$$

from them are inequivalent.

Proof — Recall that π maps $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_l$ and $G = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_k$ to the factorizations $G' = H'_1H'_2 \dots H'_n$ and $G' = K'_1K'_2 \dots K'_m$, respectively (see Claim 4.46). We show the assertion by contradiction. Suppose that $G = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_l$ and $G = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_k$ are equivalent. Then,

by Corollary 4.23, $G' = H'_1 H'_2 \dots H'_n$ and $G' = K'_1 K'_2 \dots K'_m$ are equivalent, which contradicts the assumption. □

We state a consequence of Lemma 4.47.

Corollary 4.48 *Let* G *be a finite group and* N *be a nontrivial proper normal cyclic subgroup of prime power order of* G. *Let* $\pi : G \to G' := G/N$ *be the quotient homomorphism. If* G' *has two* π*-primary inequivalent prime factorizations of* G', *then* G *has two inequivalent prime factorizations.*

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, II", *Adv. Group Theory Appl.*, to appear.

[18] S. Takamura: "Prime Factorizations of Finite Groups, III", *Adv. Group Theory Appl.*, to appear.

[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