信州大学審査学位論文

Mizarによる群の直和分解の形式化

2016年3月

中正 和久

要旨

本論文は, 定理証明支援系 Mizar による形式化数学ライブラリの開発の一環として行なった, 群の直和分解の形式化に関する成果についてまとめたものである.

形式化数学とは, 公理系を出発点とし推論規則を有限回適用して得られる定理を対象とする数学の総称である. このようにして得られる定理の証明は, 計算機による厳密かつ機械的な検証が可能である. 数学を厳密な形で形式化する試みは, 20世紀初頭のヒルベルト・プログラムから長年にわたり続けられてきた. 1960 年代に入ってからは計算機による検証プログラムの開発が活発化し, 四色問題や Jordan の閉曲線定理, Feit-Thompson の定理, ケプラー予想など, 証明が複雑なため人間による査読が困難な定理が自動検証されてきた.

Mizar プロジェクトは, Andrzej Trybulec により1973年頃に開始された, 形式化数学の記述言語・検証システムおよびライブラリを構築する活動である. Mizar 言語の最大の特徴は可読性で, 言語仕様を知らずとも数学の素養があれば内容を理解できるほどである. 1989年からは Mizar 数学ライブラリの構築が開始され, 2015 年には 54360の定理, 10955の定義, 271万行のテキストにより構成される大規模ライブラリへと成長した.

本論文で扱っている群の直和分解を形式化した当初の目的は, 離散対数問題を形式化することであった. 現代の情報セキュリティを支える基盤技術の一つである公開鍵暗号の幾つかは, 離散対数問題の計算複雑度を仮定して設計されている. このため, 離散対数問題を形式化して計算複雑度を議論することは, 情報セキュリティの堅牢性を保証することにつながり意義が大きい. ある群における離散対数問題は, その直和分解に現われる部分群上での離散対数問題へと帰着されるため, 離散対数問題の形式化において群の直和分解を形式化することが必要不可欠である.

今回の群の直和分解に関する形式化が, 他の定理証明支援系が有する数学ライブラリに比べて優位な点は, 内部直和分解について群の可換性および群の族の有限性を仮定していない点である. このような一般的な形での形式化が必要である根拠は, 非可換群, あるいは無限個の群への直和分解が, 自然科学の様々な分野で自然に現われることに基づく. 例えば, 素粒子物理におけるゲージ理論では非可換リー群とその直和が重要な役割を果たす. また, バナッハ空間は無限個の群の直和であるノルム線形空間を完備化することにより得られる.

非可換な無限個の群の族への内部直和分解を形式化するには, 幾つかの本質的な困難が生じる. 無限個の群の直積の元が直和に含まれる条件は, 単位元と異なる成分が有限個であることと同値だが, これを効率的に扱うためには, 関連する定義と多数の補題を準備する必要があった. また, 内部直和分解を形式化するには, 直和の各成分同士が可換で群演算の順序を考慮しなくてよい事実が本質的な役割を果たすが, あらかじめ群の可換性を仮定しない場合は, 群演算の順序の扱いに工夫が必要で, 証明の難易度が格段に増す. このような理由から, これまで非可換・無限個の場合は内部直和分解の形式化が避けられてきたが, 本論文で解説する成果はこれらの課題をクリアしている.

数学の形式化においては, 上記のような問題固有の難しさのほかに, 形式化全般に共通する困難が存在する. 近年, 形式化ライブラリが大規模化するにしたがい, ライブラリの検索性・閲覧性の改善が喫緊の課題となっている. 筆者等は, この課題を解決するためにMizar言語専用のドキュメンテーション生成器を開発した. 本論文では, 開発したツールの紹介とともに, 開発経緯・既存のツールとの比較, 今後の展望について解説している.

目次

第1章

序論

1.1 はじめに

本論文は, 信州大学大学院 総合工学系研究科 師玉・山崎・岡崎研究室の形式化プロジェクトにおいて, 筆者が行なった群の直和分解の形式化の成果に基づいている. 2015年現在, 当研究室では暗号理論, 画像処理, 関数解析をはじめとする, 工学的志向の強い分野を中心に形式化を進めている.

本研究は, この中の暗号理論に属するもので, 具体的には離散対数問題 [1] の計算複雑度の形式化を目指すプロジェクトの一環として進められた. 現代の情報セキュリティを支える基盤技術の一つである公開鍵暗号の多くは, 有限巡回群上での離散対数問題の計算複雑度を仮定して設計されている. このため, 離散対数問題を形式化して計算複雑度を議論することは, 情報セキュリティの堅牢性を保証することにつながり意義が大きい. ある群での離散対数問題は, その群の直和分解に現われる部分群における離散対数問題に帰着されるため, 離散対数問題を形式化するうえで群の直和分解を形式化することは必要不可欠である. 一般に離散対数問題の計算困難さを利用した暗号に利用される群は有限可換群であるため, 以下の有限可換群の基本定理が重要な役割を果たす.

定理 1.1.1. (有限可換群の基本定理 その1)
有限可換群 G は, 有限個の準素巡回群の直和に同型である.

$$G \simeq \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_r}$$

ここで, r は正整数, $q_1, \cdots, q_r$ は素数の冪で, q_i の順序を除くと G により一意的に定まる.

この有限可換群の基本定理を形式化することが当初の目標であったため, 群の直和分解については有限個の可換群への分解に限定した場合のみを形式化する予定であった. しかし, 群論は現代数学における最も汎用的な道具の一つであり, また直和分解は群論における最も基本的な道具の一つであるため, より一般化した形で形式化されることが望ましい. 例えば, 素粒子物理における標準理論のゲージ対称性は, $U(1) \oplus SU(2) \oplus SU(3)$ という非可換群の直和として表される. また, バナッハ空間はノルム線形空

間を完備化することにより得られるが, 完備化対象となるノルム線形空間は無限個の群の直和として表現される [2]. このように, 非可換群, あるいは無限個の群に対する直和分解は, 数学や理論物理の様々な場面で自然に現われるため, これらのケースに対応できる形で群の直和分解を形式化することには大いに意義がある. 非可換かつ非可算無限個の群に対する内部直和分解を扱った形式化は Coq, Isabelle などの他の定理証明支援系のライブラリにも収録されておらず今回が新規の成果である.

1.2 離散対数問題と暗号

G を任意の有限乗法群, $g \in G$ の元としたとき $\langle g \rangle$ を g により生成される部分巡回群とする. このとき, G における離散対数問題は以下のように定式化される.

定義 1.2.1. (離散対数問題)
$g \in G$ および $a \in \langle g \rangle$ が与えられたとき, $g^x = a$ を満たす整数 x を決定せよ.

一般に暗号では, 累乗を求めるのが容易(=効率の良いアルゴリズムが知られている)で, 離散対数を求めるのが難しい(=効率の良いアルゴリズムが見つかっていない)群が用いられる. 例えば, 自然数 n を法とする既約剰余類群 $(\mathbb{Z}/n\mathbb{Z})^\times$ において, 累乗を求める操作としてはバイナリ法など n のビット数に対して計算量が多項式時間となるアルゴリズムが知られている. 逆に, 離散対数を求めるアルゴリズムには指数計算法など準指数時間のアルゴリズムが知られているが, これらのアルゴリズムを用いても十分大きく適切な n をとれば, 限られた計算機資源によって離散対数問題を現実的な時間で解くことは不可能である.

既約剰余類群 $(\mathbb{Z}/n\mathbb{Z})^\times$ は可換であるから, 有限可換群の基本定理(定理 1.1.1)により準素巡回群の直和に同型である. 離散対数問題は直和を構成する部分群ごとに考えればよいため, $(\mathbb{Z}/n\mathbb{Z})^\times$ の離散対数問題は, その直和を構成する部分群の離散対数問題に帰着される. このため, n を選択する際には, $(\mathbb{Z}/n\mathbb{Z})^\times$ が小さな位数の群の族によって直和分解されないように注意を払う必要がある. Pohlig-Hellman のアルゴリズム [3] によると, 位数 m の有限巡回群の離散対数問題の計算量は, m の素因数分解を $m = p_1^{e_1} \cdots p_k^{e_k}$ とすると $O(\sum_{i=1}^{k}(e_i(\log m + \sqrt{p_i})))$ 回の群演算と評価されることが知られている. このため, 自然数 n を法とする剰余類環の既約剰余類群を用いた暗号では, 位数が素数であるような既約剰余類群の部分群上で離散対数問題を考える. 実際の運用では, n が素数 p のとき既約剰余類群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数は $p-1$ であるから, 十分に大きな素数 p, q に対して $q \mid p-1$ が成り立つように p を選択し, 位数 q の部分群を用いることが多い.

離散対数問題の計算複雑性を安全性の根拠とする暗号方式には, Diffie-Hellman 鍵共有, ElGamal暗号などがある.

1.3 形式化数学とその意義

形式化数学とは, 形式体系に基づいて構築される数学の総称である. 形式体系は, 記号・文法・公理系・推論規則・定理などを基本要素とし, 定理の証明は命題に推論規則を有限回適用して公理系に帰着させる機械的な操作によってなされる. このようにして得られる定理の証明は機械的に検証できるため, 計算機によって厳密性を保証することができる. 形式体系の論理学からの基礎付けは [4] などを参照されたい.

形式化数学の意義は, 1994年に発表された QED manifesto [5] で詳しく解説されている. QED manifesto とは, 「人類が有する全ての重要な数学知識や数学技術を効率的に表現しつつ, 内部的には厳密に形式化された表現で全ての証明を自動検証するシステムを構築し, これにより最高水準の数学的厳密性を保証する」ことを目指したプロジェクトの提起書で, 1994年に Robert Boyer等を中心としたグループにより宣言された. 宣言書では, その取り組みの意義を以下のように9点取り上げている.

1. 絶えず増大する数学知識の厳密さを保証し管理する.
2. ハイテク産業で使える信頼度の高いモデリングツールを提供する.
3. 論理的思考能力を養うための教育ツールを提供する.
4. 数学文化の継承と普及を促す.
5. 数学が堕落しないように保全する.
6. 数学出版物から不具合や重複を除去し, 査読を一部自動化する.
7. 一貫性のある数学体系を確立する助けとなる.
8. 研究者が有する暗黙知の公開を促す.
9. 数学者の深層意識を開拓する.

QED manifesto により構築されるシステムの将来的な応用可能性は純粋数学に留まらない. 特に, 取り組みの意義として2番目に取り上げられている「ハイテク産業へのモデリングツール提供」は工学的に大きな意味を持つ. 情報産業の発達に伴い, 運輸, 医療, 金融, エネルギーなどの基幹業務を支えるミッションクリティカルシステムは増加の一途を辿っている. これらのシステムが予期せぬ誤動作や障害による停止を起こした場合, 人命・経済などの社会的損失が極めて大きなものとなる可能性がある. 定理証明支援系などを用いた形式手法は, 情報システムおよびそれを支える数学理論やアルゴリズムの信頼性および安全性を飛躍的に高める手法である. 近年, 形式手法に対する産業界からの期待が高まっており, プロジェクトへの部分的な適用事例も増加している. ISO/IEC 15708 やIEC 61508 などの規格では、高信頼性が問われる情報機器の開発において形式手法を利用することが推奨されている [6]. QED manifesto により形式化システムが構築されれば, 産業界へもたらす恩恵は極めて大きなものとなるこ

とが予想される.

一例として暗号理論の研究を考えると, ひとたび暗号アルゴリズムや暗号プロトコルが形式言語で記述されれば, 以下のようなことが自動的に実行可能となるであろう.

1. 暗号アルゴリズムや暗号プロトコルが誤りなく動作することを検証する.
2. 暗号アルゴリズムや暗号プロトコルの計算量や強度(解読計算量)を評価する.
3. 安全性証明が論理的に正しいことや, セキュリティを脅かす攻撃が存在するかを検証する.
4. プログラム言語で書かれたプロトタイプを自動生成しパフォーマンスを実測する.

これらは部分的にはすでに実現されている技術で, 人手による従来の研究手法に比べて, 暗号技術の堅牢性をより強力に保証するとともに, 研究のリードタイムを削減することに寄与している. 将来の暗号技術者は, Web 上に構築された暗号理論に関する形式化ライブラリに基づいて, ライブラリに登録された暗号方式や暗号プロトコルを安全かつ少ない労力で情報システムへ組み込むことができるようになるであろう.

情報技術が発展した今日, QED manifesto の実現可能性は大いに増しているが, その実現にはまだ程遠い状況にあるといえる. Freek Wiedijk は2007年の論文 [7] で, QED manifesto が実現していない原因は, キラーアプリケーションの不在とそれによって生じる人材不足にある結論づけている. 筆者等が行なった形式化においても, 形式化支援ツールが未成熟であることから多くの困難に直面した. 今回, 筆者等はこれらの困難の一つである検索にまつわる問題を解決する事を目的とし, Mizar ライブラリのドキュメンテーション生成器を開発した. これに関しては, 2章で詳しく論ずる.

1.4 Mizar プロジェクト

Mizar プロジェクトは, ポーランドの数学・計算機科学者 Andrzej Trybulec により1973年頃に開始された, 形式化数学の記述言語, 検証システムおよびライブラリを構築する活動である. この研究から生み出された数々の独創的な概念や設計思想は, 後続の定理証明支援系に多大な影響を与えてきた.

Mizar 言語の最大の特徴は可読性の高さで, 数学の素養さえあれば言語仕様を知らずとも内容が理解できるほどである. このことは, 他人が書いたアーティクルを理解する助けとなっており, ひいては形式化数学ライブラリの構築を進めるにあたっての利点となっている. 言語の可読性を高める工夫としては, 自然言語に近い構文, 自然演繹に則った推論規則により実現された宣言的な言語仕様, 一階述語論理を中心とした論理体系などが挙げられる.

Mizar ライブラリの構築が始まったのは1989年のことである. 2015年には, 54360の定理, 10955の定義, 271万行のテキストからなるライブラリへと成長を遂げ, 形式化数学ライブラリとしては規模・網羅性ともに最大となっている. Mizar ライブラリに収録されている代表的な定理には, Jordan 閉曲線定

理, Brouwer の不動点定理, Gödel の完全性定理, 代数学の基本定理などがある.

Mizar プロジェクトの詳細については, [8] や [9] が詳しいので参照されたい.

1.5 群論の形式化の状況

群論は定理証明支援系によって最も盛んに形式化されてきた分野の一つで, 多くのライブラリが提供されている. これは,

1. 群論は他の数学分野に比べて直観に依存した概念が少なく形式化しやすい分野で, 定理証明支援系の有用性を評価するには格好の材料であった.
2. 群論は, 代数学にとどまらず, 解析学, 幾何学や物理学全般の基礎付けに必須の道具であるため, 他の理論に先んじて形式化する必要があった.
3. 有限単純群の分類理論に代表されるように, 有限群論における重要な結果の多くは初等的ではあるが複雑に入り組んだ証明を含んでおり, 人間系による査読が極めて困難であった.

などの事情による. しかし, 1とは矛盾することであるが, 今回形式化の対象とした直和分解は群論の中では比較的直観的に理解しやすい概念で, 教科書に書かれた人間による証明と形式化された証明との間には大きなギャップが生じていた. 今回の形式化で参考としたのは, Rotman [10], Robinson [11] および Bourbaki [12] による群論の標準的な教科書である. この中で, 群の内部直和分解に関する一連の証明を最も詳しく記述していたのは Bourbaki (代数学 第1章第6節)であった. この教科書では, 群の演算により定義される部分群の族の直和から群への標準的な写像が同型写像であることを内部直和分解の定義とすることが妥当であることを示す議論において「証明は帰納法により直ぐ示される」と書かれているが, Mizarにおける形式化証明では同様の議論に1000行近くを費やしている. また, Bourbaki の教科書では, 有限個の群からなる族に対してのみが対象で, 無限個の群からなる族のケースは取り扱われていない. これらの事情により, 今回の Mizar による群の直和分解の形式化は, 最終的に9500行にまで膨らむ結果となった.

近年の群論の形式化における最も特筆すべき成果は, 2012年に完了した INRIA と Microsoft Research による Feit-Thompson の定理の形式化 [13] である. Feit-Thompsonの定理とは, 「奇数位数の有限群はすべて可解である」ことを述べた定理で, 奇数位数定理とも呼ばれる. 本定理は, 有限単純群の分類を進めるに当たって最初に証明しなければならないマイルストーンであった. 定理の形式化では, 定理証明支援系 Coq と, その拡張ライブラリ SSReflect [14] が用いられた. SSReflectは, Coqで四色問題の形式化をする際に開発されたライブラリで, 特に有限の対象に対する取り扱いに秀でている. 本形式化プロジェクトは2006年から6年間, 15人のメンバーによって進められ, 生み出された形式化ライブラリは, 4000の定義, 13000の定理, 15万行ものテキストとなっている. これらのライブラリには, 群の基

礎理論のみならず, 群の指標および表現の理論, 複素数および代数学の基本定理と代数的閉体, ガロア理論など, 今後多くの応用が見込まれる理論や定理が含まれている.

上記のプロジェクトの成果により, 現時点で Coq(SSReflect) が有する群論ライブラリは大学学部生レベルをはるかに超え, 既存の形式化された群論ライブラリの中では最も充実している. それでもなお, Mizar ライブラリにおいて群論の形式化が必要であったのは, Mizar と Coq(SSReflect) は基盤となる論理体系が異なっており容易に相互変換できないことが主因である. Mizar におけるは実数の取り扱いは Coq よりも容易で, このため解析学や幾何学については Coq よりも進んだライブラリを有する. 今後, Mizar において解析学や幾何学から群論を利用することが見込まれており, それに先んじて群論ライブラリを整備することには意義がある. Coq(SSReflect) の群論ライブラリは対象を有限の場合に特化したものが多いが, 解析学や幾何学で登場する群構造は必ずしもそうとは限らないため今後の展開次第では不足が見込まれる.

表1.1は, 現在までに Mizar ライブラリに収録されている群論関連の論文一覧である(ただし`GROUP_21`は査読中). このうち, `GROUP_18` から `GROUP_21` は今回の一連の形式化で執筆を行なった論文である. また, `GROUP_7` および `GROUP_12` は群の直積と直和に関するもので今回の形式化にも深く関係する. なぜなら, 直和分解とは群の直和との同型性を定義とする概念であるためである.

1.6 本論文の構成

非可換な無限個の群の族への内部直和分解の形式化では, 形式化全般にみられる難しさの他にも, 幾つかの本質的な困難が生じる. 一つには, 無限個の群の直積の元が直和に含まれる条件は, 単位元と異なる成分が有限個であることと同値だが, これを効率的に扱うために関連する定義と多数の補題を準備する必要があった. また, 内部直和分解を形式化するには, 直和の各成分同士が可換で群演算の順序を考慮しなくてよい事実が本質的な役割を果たすが, あらかじめ群の可換性を仮定しない場合は, 群演算の順序の扱いに工夫が必要で, 証明の難易度が格段に増す. 本論文では, これらの困難と工夫に焦点を絞り解説してゆく.

2章では, 形式化全般にみられる困難についての考察と, その一つである検索にまつわる問題を解決するために開発した Mizar ライブラリのドキュメンテーション生成器について解説する.

3章では, 群の直和分解を議論するのに必要な群論の基礎として, 群, 部分群, 群準同形, 群の族, 群の直積と直和の定義などとその Mizar 上での形式化について解説する. これらの形式化は, 本研究の前からすでに Mizar ライブラリに登録されていたものである. また, 圏論的視点から群の外部直和分解および内部直和分解について概説する.

4章では, 群の直和分解の Mizar 上での形式化について解説する. 直和の概念は, 本研究が始まる前にすでに Mizar 上で形式化されていたものの, 条件記述が複雑で長かったため, 直積の元が直和に含まれ

論文識別名	論文	内容
GROUP_1	[15]	群と可換群, 累乗, 位数の定義と基本的な定理
GROUP_2	[16]	部分群と剰余群の定義, 2つの部分群を含む最小の群や共通集合, Lagrangeの定理
GROUP_3	[17]	共役, 正規部分群, 部分群のなす集合
GROUP_4	[18]	部分群の集合のなす束構造, Frattini部分群
GROUP_5	[19]	群の交換子, 群の中心
GROUP_6	[20]	群の準同形写像と同型写像, 商群
GROUP_7	[21]	群の直積と直和
GROUP_8	[22]	群の指数に関する諸定理
GROUP_9	[23]	Jordan-Höldの定理
GROUP_10	[24]	Sylowの定理
GROUP_11	[25]	部分群に関する諸定理
GROUP_12	[26]	群の直積とその正規部分群
GROUP_14	[27]	有限巡回群による有限巡回群の直積分解
GROUP_17	[28]	有限可換p-群による有限可換群の直和分解
GROUP_18	[29]	有限巡回群による有限可換p-群の直和分解
GROUP_19	[30]	群の直和分解の定義
GROUP_20	[31]	群の直和分解と同値な表現
GROUP_21	-	群の直和分解の諸定理
GROUPP_1	[32]	p-群, 可換p-群の諸性質
GRSOLV_1	[33]	可解群
GR_CY_1	[34]	巡回群とその性質
GR_CY_2	[35]	巡回群と準同形写像

表1.1 Mizar ライブラリに収録されている群論関連の論文一覧

ることを議論するにはいささか扱いにくいものであった. このため, 本研究では新たに群を値域に持つ写像の台を用意して, その諸性質を形式化することにより, 直積の元が直和に含まれることを簡素な条件で判定できるように工夫している. 上記に加えて, 非可換群に対する内部直和分解の形式化の困難さについて述べたい.

5章では, 内部直和分解・外部直和分解と同値な性質と, その形式化について解説する. GROUP_17, GROUP_18 では, 有限可換p-群による有限可換群の直和分解と有限巡回群による有限可換p-群の直和分解が形式化されているが, これらの形式化では, 直和分解をこの直和分解と同値な性質として証明している. このため, 本章の結果は, GROUP_17, GROUP_18 の議論に正確な根拠を与えるものである. また, 本章では内部直和分解と外部直和分解の同値性についての定理と形式化を解説する.

6章では, 直和分解の不変性とその形式化について述べる. 本章で解説する一連の不変性は, 直和分解

に有限性を仮定すれば, 直和の可換性と結合性により導かれる. しかし, 本研究のように直和分解に有限性を仮定しない一般のケースでは, その形式化は複雑化する.

7章では, 本研究の応用例として, 有限可換群の基本定理について解説する. ここでは, 有限可換群の基本定理がどのように形式化されるか, その中で本研究で形式化された一連の定義・定理がどのように適用されるかについて詳しく論じる.

8章では, 結論として本研究の成果と今後の展望について述べる.

本論文の3章から7章は, 定義・定理とその形式化についての解説が主である. また, 定義・定理の証明および形式化の方針が自明ではないと思われる場合にかぎり, その解説を行なっている.

本論文における筆者の貢献は, 2, 4, 5, 6章全体ならびに, 7章の有限可換p-群の巡回群への分解の形式化の一部である.

第2章

Mizarライブラリのドキュメンテーション生成器

本章では, Mizar ライブラリを用いた形式証明における検索の問題を解決するために開発したドキュメンテーション生成器について解説する. これらの結果は [36] の成果に基づいている.

2.1 動機

序章でも取り上げたとおり, 情報システムおよびそれを支える数学理論やアルゴリズムの信頼性や安全性を形式検証によって担保することは必要不可欠であるとの認識が一般に広がりつつある. しかし, 形式手法によって数学定理やアルゴリズムが厳密に正しいことを計算機によって検証するためには, 人間にとっては冗長と考えられるレベルまで咀嚼して形式証明を記述する必要があるため, 厳密な適用には大きなコストがかかる. このことは, 技術者が形式手法を利用することを躊躇する最大の要因となっており, 形式検証システムが普及することの妨げとなっている.

今回の一連の形式化を Mizar 上で進める中で筆者が直面した困難の中で, 特に形式化全般に当てはまると考えられる問題を以下に列挙する.

1. 検索の難しさ
   新たな定理を証明するためには, ライブラリに収録されている定義・定理を引用して論理展開を進める. しかし近年, ライブラリが巨大化したため, それらを検索することが難しくなってきている.
2. 厳密な記述の難しさ
   自然言語で書かれた定義・定理を, 計算機が解釈可能な言語に書き直すことには熟練を要する. これは, 人間が自明と認識している箇所を厳密に記述することの難しさなどに起因している.
3. 計算機による推論の貧弱さ

手証明では明らかと思われるような論理展開であっても, 計算機が解釈するには困難な場合が多く, より詳細な論理展開の記述が要求される.

4. **型変換の煩雑さ**
   証明記述言語の型付けが強いため, 煩雑な型変換が必要である. これは証明の本質とは無関係な作業であるが, ほとんどの証明記述言語が抱える問題点である.
5. **学習コストの高さ**
   言語仕様の複雑さ, マニュアル類の不備, エラーメッセージの曖昧さなどが要因である.

特に, 1の検索の困難性の解決は, 3の計算機による推論の貧弱さの解決にも必要なため, 他に比べても重要度が高い. Mizar ライブラリは, 2015年時点で271万行の定義・定理およびその証明記述からなり, 毎年新たに約10万行のアーティクルが登録されている. 形式化ライブラリの開発プロジェクトにおける新規加入者にとっては, 何がどこで形式化されているかを把握することが年を追う毎に困難となっている. 熟練した Mizar ライブラリ執筆者にとっても, 執筆の中で最も時間が掛かる作業はライブラリから引用に使う定義・定理を検索することである. Mizar ライブラリの開発作業においては, 以下のような様々な状況で検索作業が生じる.

1. 新たにライブラリを開発するにあたって, すでに同様の理論が形式化されていないかを調査する.
2. ライブラリ開発において利用できそうな定理や定義を検索する.
3. 構文や証明方針が分からない場合に参考となりそうな類似物を検索する.
4. 自動検証器による推論を通すために引用する定義や定理を検索する.
5. 定義や定理を引用するにあたって, どのアーティクルを環境部へ追加しなければならないかを調べる.

一説によると, Mizar による形式証明において検索が占める時間は証明作業全体の半分近くにのぼるともいわれている. このため, 検索性および閲覧性の向上は, 形式化ライブラリ執筆における最大の課題といっても過言ではない. Mizar ライブラリの開発における検索に関連した問題については, [37] が詳しい. また, 形式化数学ライブラリの検索技術に関する最新の研究状況としては [38] が詳しい.

2.2 既存の検索・閲覧ツールの課題

Mizar ライブラリの検索・閲覧ツールとして広く利用されてきた既存ツールは, HTML-ized MML [39, 40] と MML Query [37, 41] である.

HTML-ized MML は, ライブラリを HTML 化してシンボルの参照関係にハイパーリンクを張り巡らせるツールである. 閲覧者はシンボルに埋め込まれたハイパーリンクをクリックすることにより, その定

義や定理を素早く直観的に閲覧することができる. HTML-ized MML は, 90年代の終わり頃に *Journal of Formalized Mathematics* の Web 閲覧機能の一部として導入された. その後, Mizar 構文解析器の XML (XML-ized MML) 化に伴い Josef Urban により再実装され現在に至っている. HTML-ized MML は, その効率的かつ直観的なデザインから, Mizar ライブラリ執筆者に幅広く利用されている. しかし, 本システムには検索機能がなく, ドキュメントが組織化されいないという問題点があった.

MML Query は, Mizar ライブラリの検索エンジンである. 利用者は, MML Query 独自の検索文法により, 正規表現によるテキスト検索よりも多様な検索設定が可能である. また, MML Query は定義や定理を引用する際に, 環境部へどのアーティクルを追加するべきかを調べる目的にも使われる. しかし, その代償として, 利用者は複雑な検索文法を学ぶ必要があり, 初心者にとっては敷居の高いシステムとなっていた.

このような事情から, Mizarライブラリの執筆者は, これらのツールを状況に応じて使い分けつつ, 必要に応じてテキストエディタにより Mizar ライブラリを直接閲覧したり正規表現によって検索することを余儀なくされていた.

2.3 ドキュメンテーション生成器の着想と設計

今回作成したドキュメンテーション生成器のアイデアは, ソフトウェア開発における API リファレンス自動生成システムから来ている. ソフトウェア開発の世界では, Doxygen や RDoc など数多くのAPI リファレンス自動生成システムが存在する. これらは, インクリメンタル検索, ハイパーリンクによる参照・被参照, ドキュメントの組織化など共通した機能を有する. API リファレンス自動生成システムは, ライブラリが更新される毎に自動的に API ドキュメントを作り直すことができ, ソフトウェア開発のリードタイム削減に大きく寄与している.

このような考察から, 筆者は Mizar 言語専用のドキュメンテーション生成器がライブラリ執筆の手間を大幅に軽減するであろうと考えるに至り開発に着手した. 開発工数を最小化するため, 本ツールは HTML-ized MML を文書整形してインクリメンタル検索機能を加えるアプリケーションとした.

2.4 ドキュメンテーション生成器の機能

今回のドキュメンテーション生成器は Python で書かれており, 以下の3ステップから構成される.

1. HTML-ized MML を解析し, シンボルとシンボル同士の相互関連情報を読み込む.
2. 読み込んだシンボル情報をクリーニングし, 閲覧しやすいように構成する.
3. シンボル情報を1シンボルにつき1ページの HTML ファイルとして書き出す.

これらのステップの処理は, 通常のデスクトップ PC を用いて数分程度で終わる.

ドキュメンテーション生成器により生成される HTML ドキュメントの主な機能を以下に列挙する.

1. **シンボルリスト**
   左ペインのリストには, Mizar ライブラリに登録されている 9000 近いシンボルが列挙されている. シンボルの種類は, シンボルの左側に表示されているアイコンによって識別できる. リスト内のシンボルをクリックすると, そのシンボルに関する情報がメインフレームに読み込まれる.
2. **インクリメンタル検索**
   左ペインのリスト上部にインクリメンタル検索ボックスが配置されている. 検索では大文字・小文字は区別されない. 複数の検索語句をスペース区切りで入力すると, リスト中でそれらの語句を全て含むシンボルが絞り込まれる. 内部的には独自の検索テーブルが用意されており, 検索に要する時間は数十から数百ミリ秒である. インクリメンタル検索により, 利用者がシンボルの正確な綴りを覚えていなくとも, 部分的なスペルから検索を行なうことが可能である.
3. **ソースコード**
   シンボルの定義に関するソースコードは, HTML-ized MML から引き継がれている. このため, ソースコード内の太字シンボルをクリックすると, その定義へジャンプするのは, HTML-ized MML の機能と同様である.
4. **被参照リスト**
   HTML-ized MML では, シンボルからその定義を参照することは可能であったが, あるシンボルを定義に用いているシンボルを逆参照する機能はなかった. 本システムでは, このようなシンボルを被参照シンボルリストとしてページ内で列挙している.

図2.1はドキュメンテーション生成器により作成された HTML ドキュメントのスクリーンショットである.

2.5 成果と今後の課題

Mizar ライブラリ上で動作するドキュメンテーション生成器が開発されたことにより, 従来の MML Query や正規表現によるテキスト検索よりも素早く直観的にシンボルを検索することが可能となり, 検索効率が大幅に向上した. また, 被参照リストを閲覧することにより, 特定のシンボルを用いた定義を容易に検索することが可能となったため, 同じ意味を持つシンボルを重複して定義することの予防に役立っている, これらの利点から, 本システムは Mizar ライブラリ執筆者から大いに人気を博している.

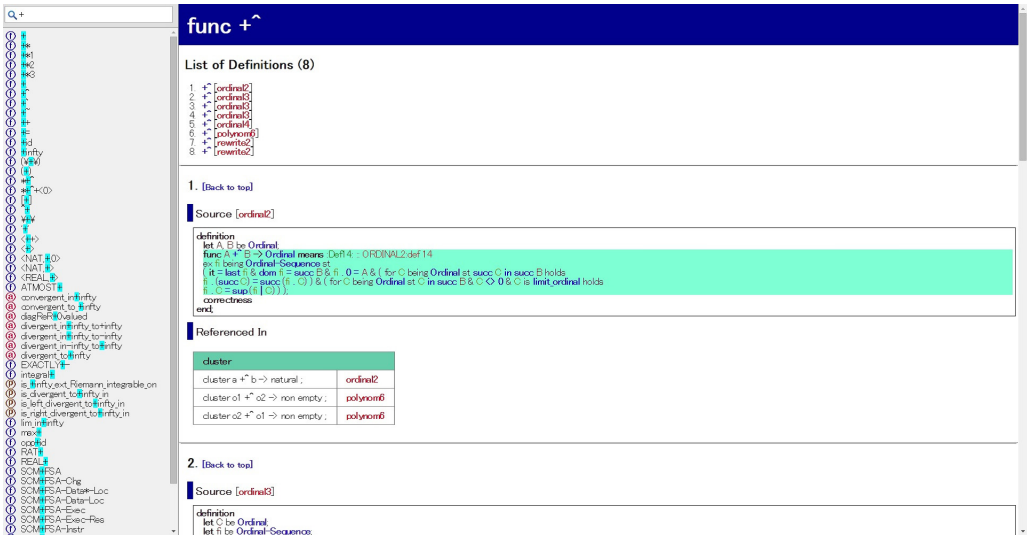


図2.1 ドキュメンテーション生成器のスクリーンショット

本システムにより生成された最新のドキュメントは信州大学の Web サイト [*1] で公開されており常時アクセス可能である.

本システムの今後の課題および将来の拡張可能性について以下に列挙する.

1. **XML-ized MMLを用いた再実装**

   今回の実装は HTML-ized MML を読み込んでドキュメントを生成する仕組みとなっている. HTML-ized MML は XML-ized MML から生成されるが, この処理には通常のデスクトップ PC で数十時間を要する. XML-ized MML は自動検証システムの中間生成物としても使われている汎用フォーマットで, ドキュメンテーション生成器でも直接 XML-ized MML を読み込んで解析するように修正することが望ましい. ただし, HTML-ized MML に埋め込まれているシンボルの参照関係が XML-ized MML には埋め込まれておらず, ドキュメンテーション生成器が XML-ized MML を直接読み込むためにはシンボルの参照関係の解決が必要となる.

2. **定理検索機能**

   定理の表現は一通りではないため, その検索にはセマンティックな解析が必要となる. これには, 自動推論で研究されている機械学習法 [42, 43] が有効と考えられる.

3. **多言語への拡張**

   現在, ドキュメンテーション生成器が稼働している形式記述言語は Mizar 言語のみである. シン

[*1] http://webmizar.cs.shinshu-u.ac.jp/mmlfe/current/

ボルの検索・閲覧には極めて有効な仕組みのため, 今後 Coq, Isabelle など他の形式記述言語への組み込みを行いたい.

4. **タグコメント機能**

   ソフトウェア開発で使われる API リファレンス自動生成システムでは, API の作者・目的・使用方法などをソースコード中にタグ付けされたコメントとして埋め込むことにより API リファレンスに反映される. Mizar 言語は比較的可読性の高い形式記述言語であるが, それでも直接ソースコードから著者の意図を読み取るのが難しいことがある. このため, タグコメント機能を実装することには大いに意義がある. 今後, 異なる形式記述言語間においてタグコメントを標準化し, ドキュメンテーション生成器が様々な形式言語を処理できるようにすることは有益と考えられる.

また, 本システムに組み込まれたインクリメンタル検索は, 今後 Mizar の統合開発環境を開発する際に重要な機能となると考えられる.

第3章

群論からの準備

本章では, 群論からの準備として, 群, 部分群, 群準同形, 群の族, 群の直積と直和などの定義と, それらのMizar上での形式化について解説する. また, 圏論的視点から群の外部直和分解および内部直和分解について概説する. 集合論の教科書としては [44] を, 群論の教科書としては [10, 11, 12] を参考とした. また, 数学全般の用語は [45] を参考とした. Mizar上での形式化としては, [15, 16, 17, 20, 21, 30, 46, 47, 48, 49]を参考とした.

3.1 群と部分群

定義 3.1.1. (マグマ)
マグマとは二項演算の定義された集合のことで, 集合 S と S 上の2項演算 $\cdot : S \times S \to S$の組 $(S, \cdot)$ で表される.

以後, マグマ $(S, \cdot)$ に対し S を台集合, $\cdot$ を演算とよぶ. Mizar上で, マグマはstructを用いて以下のように形式化されている.

形式化 3.1.2. (マグマ)

```
:: ALGSTR_0.ABS line 285
definition
  struct (1-sorted) multMagma (#
    carrier -> set,
    multF -> BinOp of the carrier
  #);
end;
```

定義 3.1.3. (群)
空でない集合 S に対して, マグマ $(S, \cdot)$ が群であるとは,

1. (結合法則) S の任意の元 x, y, z に対して, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ が成り立つ.
2. (単位元の存在) S の要素 e が存在し, 任意の $x \in S$ に対して $x \cdot e = x$ が成り立つ.
3. (逆元の存在) S の任意の要素 x に対し, ある $y \in S$ が存在して $x \cdot y = y \cdot x = e$ が成り立つ.

を満たすものである.

Mizar上ではマグマの結合法則, 単位元の存在, 逆元の存在は以下のように形式化されている.

形式化 3.1.4. (群法則)

```
definition
  let IT be multMagma;

  attr IT is unital means
:: GROUP_1:def 1
  ex e being Element of IT st for h being Element of IT
  holds h * e = h & e * h = h;

  attr IT is Group-like means
:: GROUP_1:def 2
  ex e being Element of IT st for h being Element of IT
  holds h * e = h & e * h = h &
  ex g being Element of IT st h * g = e & g * h = e;

  attr IT is associative means
:: GROUP_1:def 3
  for x,y,z being Element of IT holds (x*y)*z = x*(y*z);
end;
```

それぞれ, `GROUP_1:def 1` は単位元の存在, `GROUP_1:def 2` は単位元の存在と逆元の存在, `GROUP_1:def 3` は結合法則に対応している. これらを用いてMizar上で群は以下のように形式化されている.

形式化 3.1.5. (群)

```
:: GROUP_1.ABS line 66
definition
  mode Group is Group-like associative non empty multMagma;
end;
```

演算が可換である群を可換群(アーベル群)とよび, 以下のように定義される.

定義 3.1.6. (可換群)

群 G に対して, 任意の $x, y \in G$ が $x \cdot y = y \cdot x$ を満たすとき, G は**可換群(アーベル群)**であるという.

可換群はMizar上で以下のように形式化されている.

形式化 3.1.7. (可換群)

```
definition
  let IT be multMagma;
  attr IT is commutative means
:: GROUP_1:def 12
  for x, y being Element of IT holds x*y = y*x;
end;
```

群の台集合の部分集合が演算に対して群を形成するとき, 部分群であるという. 定義は以下のようになる.

定義 3.1.8. (部分群)
群 $G = (S, \cdot)$ に対して, S の空でない部分集合 T と$\cdot$ の T 上への自然な制限 $\cdot_T = \cdot \restriction_{T\times T}$ の組 $H = (T, \cdot_T)$ が群となるとき, H は G の**部分群**であるという.

部分群のMizar上での形式化は以下のようになる.

形式化 3.1.9. (部分群)

```
definition
  let G be Group-like non empty multMagma;
  mode Subgroup of G -> Group-like non empty multMagma means
:: GROUP_2:def 5
  the carrier of it c= the carrier of G &
  the multF of it = (the multF of G) || the carrier of it;
end;
```

ここで, `the multF of G` および `the carrier of G` はそれぞれ群 G の演算および台集合である. また, `(the multF of G) || the carrier of it` は演算 $\cdot$ の T 上への自然な制限 $\cdot \restriction_{T\times T}$ である.
左剰余類と右剰余類は以下のように定義される.

定義 3.1.10. (剰余類)
群 G とその部分群 H に対して, G の元 x が与えられたとき, $x \cdot h$ $(h \in H)$ という形の元全体の集合を xH と書き, H の**左剰余類**とよぶ. 同様に, $h \cdot x$ $(h \in H)$ という形の元全体の集合を Hx と書き, H の**右剰余類**とよぶ.

左剰余類と右剰余類は, Mizar上で以下のように定義されている.

形式化 3.1.11. (剰余類)

```
definition
```

```
  let G,H;
  func Left_Cosets H -> Subset-Family of G means
:: GROUP_2:def 15
  A in it iff ex a st A = a * H;
  func Right_Cosets H -> Subset-Family of G means
:: GROUP_2:def 16
  A in it iff ex a st A = H * a;
end;
```

群 G において, 左剰余類と右剰余類が一致するような部分群 H を正規部分群とよぶ. これは, 任意の $x \in G$ に対して, $xH = Hx$ が成り立つことで, 以下の定義と同値である.

定義 3.1.12. (正規部分群)
群 G の部分群 H が, すべての $x \in G$ に対して, $x^{-1}Hx = H$ を満たすとき, H は G の**正規部分群**であるという.

特に, 可換群の部分群はすべて正規部分群である. 正規部分群は Mizar 上で以下のように形式化されている.

形式化 3.1.13. (正規部分群)

```
definition
  let G;
  let IT be Subgroup of G;
  attr IT is normal means
:: GROUP_3:def 13
  for a holds IT |^ a = the multMagma of IT;
end;
```

ここで, `H |^ a` は, $a^{-1}Ha$ に相当するファンクタである.

3.2 群準同形

群から群への写像で, 演算を保つものを群準同形とよび, 以下のように定義される.

定義 3.2.1. (群準同形)
G, H を群とする. 写像 $f : G \to H$ が**群準同形**であるとは, 任意の $x, y \in G$ に対して,

$$f(x \cdot y) = f(x) \cdot f(y)$$

が成り立つことをいう. また, このような写像の集合を $Hom(G, H)$ と表記する.

群準同形は Mizar 上ではマグマ準同形と群準同形の集合として定義されている.

形式化 3.2.2. (マグマ準同形)

```
definition
  let G, H be non empty multMagma;
  let f be Function of G, H;
  attr f is multiplicative means
:: GROUP_6:def 6
  for a, b being Element of G holds f.(a * b) = f.a * f.b;
end;
```

形式化 3.2.3. (群準同形の集合)

```
:: GROUP_6.ABS line 276
definition
  let G,H;
  mode Homomorphism of G,H is multiplicative Function of G, H;
end;
```

特に, 群準同形の中で写像として全単射なものは**群同型**とよばれる. Mizar上では, 全単射な写像はアトリビュート `bijective` として形式化されている.

形式化 3.2.4. (同型な写像)

```
definition
  let X, Y;
  let f be X-defined Y-valued Function;
  attr f is bijective means
:: FUNCT_2:def 4
  f is one-to-one onto;
end;
```

3.3 群の族

群の族とは添字付けされた群の集合で, 集合を定義域とし群の集合を値域とする写像として定義される. Mizar上では, 集合の族にアトリビュートを付与することによって群の族を形式化している.

定義 3.3.1. (集合の族)
集合 I を定義域とする写像を I を添字集合とする**集合の族**という. 添字記法を用いて, $\{X_i\}_{i\in I}$, あるいは $\{X_i \mid i \in I\}$ とも表記する.

Mizar上では集合の族は以下のように形式化されている.

形式化 3.3.2. (集合の族)

```
:: PBOOLE.ABS line 47
```

```
definition
  let I be set;
  mode ManySortedSet of I is total I-defined Function;
end;
```

ここで, total I-defined Function とは, 定義域が集合 I であるような写像である. この定義を用いて, Mizar上ではマグマを値にもつ集合の族をマグマの族として形式化している.

形式化 3.3.3. (マグマの族)

```
definition
  let R be Relation;
  attr R is multMagma-yielding means
:: GROUP_7:def 1
  for y being set st y in rng R holds y is non empty multMagma;
end;

:: GROUP_7.ABS line 60
definition
  let I be set;
  mode multMagma-Family of I is multMagma-yielding ManySortedSet of I;
end;
```

上の形式化では, GROUP_7:def 1 で Relation がマグマに値を持つことを示すアトリビュートを multMagma-yielding として形式化し, その次に multMagma-yielding をアトリビュートとして持つ集合の族をマグマの族として形式化している. さらに, 群の族はマグマの族にアトリビュートを付与することにより形式化される.

形式化 3.3.4. (マグマの族に付随するアトリビュート)

```
definition
  let I be set, F be multMagma-Family of I;
  attr F is Group-like means
:: GROUP_7:def 3
  for i being set st i in I ex Fi being
  Group-like non empty multMagma st Fi = F.i;

  attr F is associative means
:: GROUP_7:def 4
  for i being set st i in I ex Fi being
  associative non empty multMagma st Fi = F.i;
end;
```

それぞれ, GROUP_7:def 3 は単位元と逆元の存在, GROUP_7:def 4 は結合法則に対応する.

定義 3.3.5. (群の族)

集合 I を定義域とする写像で, その値が全て群であるものを I を添字集合とする**群の族**という.

Mizar上で群の族は以下のように形式化されている.

形式化 3.3.6. (群の族)

```
:: GROUP_19.ABS line 44
definition
  let I be set;
  mode Group-Family of I is associative Group-like multMagma-Family of I;
end;
```

3.4 群の直積と直和

定義 3.4.1. (直積集合)

集合 I により添字付けられた集合の族 $\{X_i\}_{i\in I}$ に対して,

$$\prod_{i\in I} X_i = \{f : I \to \bigcup_{i\in I} X_i \mid \forall i \in I, f(i) \in X_i\}$$

を集合の族 $\{X_i\}_{i\in I}$ の**直積集合**とよぶ.

上の定義において, 写像 f は, 各 $i \in I$ に対して X_i の元 x_i を対応させれば定まるので, f を $\bigcup_{i\in I} X_i$ の元の族 $(x_i)_{i\in I}$ と同一視すると,

$$\prod_{i\in I} X_i = \{(x_i)_{i\in I} \mid \forall i \in I, x_i \in X_i\}$$

と書くことができる. Mizar 上で直積集合は以下のように形式化されている.

形式化 3.4.2. (直積集合)

```
definition
  let f be Function;
  func product f -> set means
:: CARD_3:def 5
  for x being object holds x in it iff ex g st x = g & dom g = dom f &
  for y being object st y in dom f holds g.y in f.y;
end;
```

直積集合の定義を用いて, 群の直積は以下のように定義される.

定義 3.4.3. (群の直積)

集合 I の任意の元 $i \in I$ に対して群 $G_i = (S_i, \cdot_i)$ が定義されているとする. 集合 I により添字付けら

れた群の族 $\{G_i\}_{i\in I}$ に対して, 群の台集合の族 $\{S_i\}_{i\in I}$ の直積集合 $\prod_{i\in I} S_i$ の元 $(x_i)_{i\in I}$, $(y_i)_{i\in I}$ に

$$(x_i)_{i\in I} \cdot (y_i)_{i\in I} := (x_i \cdot_i y_i)_{i\in I}$$

によって演算を定義した集合の組 $(\prod_{i\in I} S_i, \cdot)$ を**群の直積**とよび, $\prod_{i\in I} G_i$ と表す.

群の直積もまた群である. Mizar上ではまずマグマの直積を以下のように形式化している.

形式化 3.4.4. (マグマの直積)

```
definition
  let I be set, F be multMagma-Family of I;
  func product F -> strict multMagma means
:: GROUP_7:def 2
  the carrier of it = product Carrier F &
  for f, g being Element of product Carrier F, i being set st i in I
  ex Fi being non empty multMagma, h being Function
  st Fi = F.i & h = (the multF of it).(f,g) & h.i = (the multF of Fi).(f.i,g.i);
end;
```

上記の形式化において, `F` が集合 `I` を定義域としマグマを値とする写像であるのに対し, `Carrier F` は, 集合 `I` を定義域としマグマの台集合を値とする. ファンクタ `Carrier` は Mizar 上で以下のように形式化されている.

形式化 3.4.5. (`Carrier` の定義)

```
definition
  let J be set, A be 1-sorted-yielding ManySortedSet of J;
  func Carrier A -> ManySortedSet of J means
:: PRALG_1:def 13
  for j be set st j in J ex R being 1-sorted
  st R = A.j & it.j = the carrier of R;
end;
```

Mizar上では群の直積が群となることをクラスタを用いて形式化している.

形式化 3.4.6. (群の直積)

```
:: GROUP_7.ABS line 135
registration
  let I be set, F be Group-like multMagma-Family of I;
  cluster product F -> Group-like;
end;

registration
  let I be set, F be associative multMagma-Family of I;
  cluster product F -> associative;
```

```
end;
```

群の直和は, 群の直積の部分群として以下のように定義される.

定義 3.4.7. (群の直和)
集合 I の任意の元 $i \in I$ に対して群 $G_i = (S_i, \cdot_i)$ が定義されているとする. 群の直積 $\prod_{i\in I} G_i$ に対し, その台集合の部分集合 $\coprod_{i\in I} S_i$ を

$$\coprod_{i\in I} S_i := \{(x_i)_{i\in I} \mid x_i \in S_i,\ x_i\text{が}G_i\text{の単位元と異なるのは有限個に限る}\}$$

と定義すると, $\coprod_{i\in I} S_i$ は群の直積において部分群をなす. この部分群を**群の直和**とよび $\bigoplus_{i\in I} G_i$ と表す.

群の直和は**制限直積**とよばれることもある. Mizar上では群の直和は以下のように形式化されている.

形式化 3.4.8. (群の直和)

```
definition
  let I be set, F be associative Group-like multMagma-Family of I;
  func sum F -> strict Subgroup of product F means
:: GROUP_7:def 9
  for x being object holds x in the carrier of it
  iff
  ex g being Element of product Carrier F, J being finite Subset of I,
     f being ManySortedSet of J
  st g = 1_product F & x = g +* f
   & for j being set st j in J ex G being Group-like non empty multMagma st
     G = F.j & f.j in the carrier of G & f.j <> 1_G;
end;
```

定義 3.4.7 において, 特に集合 I が有限集合であれば直和と直積は等しい. この事実は, Mizar 上で以下のように形式化されている.

形式化 3.4.9. (群の直積と直和の一致)

```
theorem :: GROUP_7:9
  for I being finite set, F being associative Group-like
  multMagma-Family of I holds product F = sum F;
```

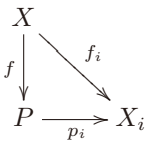
3.5 群の直和分解の圏論的考察

本節では, 圏論的視点から群の直和分解を概説する. 一般に, 圏論において直積および双対直積は以下のように定義される.

定義 3.5.1. (圏論的直積)

圏 C の対象の族 $\{X_i\}_{i\in I}$ の**圏論的直積**とは, C の対象 P で以下を満たす:

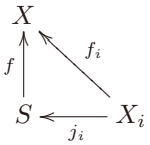
射 $p_i : P \to X_i$ の族 $\{p_i\}_{i\in I}$ が存在し, 任意の対象 X と射の族 $\{f_i : X \to X_i\}_{i\in I}$ に対し, $p_i \circ f = f_i$ $(i \in I)$ であるような射 $f : X \to P$ が一意的に存在する.



定義 3.5.2. (圏論的双対直積)

圏 C の対象の族 $\{X_i\}_{i\in I}$ の**圏論的相対直積**とは, C の対象 S で以下を満たす:

射 $j_i : X_i \to S$ の族 $\{j_i\}_{i\in I}$ が存在し, 任意の対象 X と射の族 $\{f_i : X_i \to X\}_{i\in I}$ に対し, $f \circ j_i = f_i$ $(i \in I)$ であるような射 $f : S \to X$ が一意的に存在する.



群を対象とし群準同型を射とする圏においては, 圏論的直積は群の直積, 圏論的双対直積は群の自由積が対応する. 群の自由積は以下のように構成される.

定義 3.5.3. (群の自由積)

$\{G_\lambda\}_{\lambda\in\Lambda}$ を互いに共通集合を持たない群の族とする. このとき, $\{G_\lambda\}_{\lambda\in\Lambda}$ の自由積 G は以下のように定義される.

- G の元は $\bigcup_{\lambda\in\Lambda} G_\lambda$ の元の有限列 $g = [g_1, g_2, \cdots, g_r]$ で, 隣り合う元同士 (g_i, g_{i+1}) が同一の G_λ に属さないものからなる.
- G の群演算は, $x = [x_1, \cdots, x_r]$, $y = [y_1, \cdots, y_s]$ に対して$z = x \cdot y = [x_1, \cdots, x_r, y_1, \cdots, y_s]$ と定義される. ただし, 演算結果で有限列の隣り合う元 z_i, z_{i+1} が同一の群 G_λ に所属するならば, $z = [z_1, \cdots, z_{i-1}, z_i \cdot z_{i+1}, z_{i+2}, \cdots, z_r]$ と逐次的に縮退される.

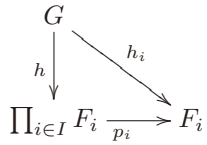
群の自由積は, Mizar上ではまだ形式化されていない. 特に, 可換群の圏においては, 圏論的双対直積は群の直和が対応する.

これらの事実を踏まえて, 群の直積分解は以下のように定義される.

定義 3.5.4. (群の直積分解)

群 G に対して, 群の族 $\{F_i\}_{i\in I}$ と群準同形の族 $\{h_i : G \to F_i\}$ が与えられると, 群の圏の直積の一意

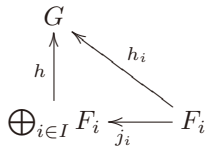
性から可換図式において h が一意に定まる.



このとき, h が群同型であれば, 群の族 $\{F_i\}_{i\in I}$ (と群準同形の族 $\{h_i : G \to F_i\}$) は G の**直積分解**であるという.

同様に, 可換群の外部直和分解は以下のように定義される.

定義 3.5.5. (可換群の外部直和分解)
可換群 G に対して, 可換群の族 $\{F_i\}_{i\in I}$ と群準同形の族 $\{h_i : F_i \to G\}$ が与えられると, 可換群の圏の直和の一意性から可換図式において h が一意に定まる.



このとき, h が群同型であれば, 可換群の族 $\{F_i\}_{i\in I}$ (と群準同形の族 $\{h_i : F_i \to G\}$) は G の**外部直和分解**であるとよばれる.

逆に, 群準同形 $h : \bigoplus_{i\in I} F_i \to G$ が与えられると, 可換図式を満たすような群準同形の族 $\{h_i : F_i \to G\}$ が一意に定まるため, 群準同形 h の存在を外部直和分解の定義としてよい.

可換群の内部直和分解は, 外部直和分解の特別なケースで, 以下のように定義される.

定義 3.5.6. (可換群の内部直和分解)
可換群の外部直和分解の可換図式において, さらに可換群の族 $\{F_i\}_{i\in I}$ が G の部分群であり, 群準同形の族 $\{h_i : F_i \to G\}$ が部分群としての自然な埋め込みであるとき, $\{F_i\}_{i\in I}$ は G の**内部直和分解**であるとよばれる.

内部直和分解において, $(x_i)_{i\in I} \in \bigoplus_{i\in I} F_i$ の各i-成分 x_i のうち, 単位元でない成分は高々有限個であることから, 群 G における $(x_i)_{i\in I}$ の成分の総乗 $\prod_{i\in I} x_i$ を考えることができる. このとき, 可換図式における射の準同型性から $h : (x_i)_{i\in I} \mapsto \prod_{i\in I} x_i$ であることがわかる.

直和分解の定義は, 可換図式における写像 h に注目することにより, さらに G が一般の群の場合へと拡張することができる.

定義 3.5.7. (群の外部直和分解)

群 G が, 群の族 $\{F_i\}_{i\in I}$ により作られる直和 $\bigoplus_{i\in I} F_i$ に対して同型である, すなわち, ある群同形 $h : \bigoplus_{i\in I} F_i \to G$ が存在するならば, 群の族 $\{F_i\}_{i\in I}$ は G の**外部直和分解**であるという.

$(x_i)_{i\in I} \in \bigoplus_{i\in I} F_i$ の任意の2成分は可換, すなわち任意の $i, j \in I$ に対して$x_i \cdot x_j = x_j \cdot x_i$ が G 上で成り立つことから, 群 G における総乗 $\prod_{i\in I} x_i$ は一意に定まる. この事実により, 群の内部直和分解は以下のように定義される.

定義 3.5.8. (群の内部直和分解)
群 G および群の族 $\{F_i\}_{i\in I}$ が

(A1) 任意の $i \in I$ に対して F_i は G の部分群である.
(A2) $h : (x_i)_{i\in I} \mapsto \prod_{i\in I} x_i$ が $\bigoplus_{i\in I} F_i$ から G への群同型である.

を満たすとき, $\{F_i\}_{i\in I}$ は G の**内部直和分解**であるという.

これらの定義から, 内部直和分解であれば外部直和分解であることは自明である. 群の外部直和分解ならびに内部直和分解の形式化については, 次章にて解説をおこなう.

第4章

群の直和分解の形式化

本章では, 群の直和分解のMizar上での形式化について解説する. 前章で解説した通り, 群の直和分解には外部直和分解と内部直和分解があり, 今回の形式化ではこれらを明確に区別している. 群の内部直和分解の形式化においては, 無限個の群の直積と非可換群の扱いが本質的な課題となる. 無限個の群の直積の元が直和に含まれる条件は, 単位元と異なる成分が有限個であることと同値だが, これを効率的に扱うためには, 関連する定義と幾つかの補題を準備する必要があった. また, 内部直和分解を形式化するには, 直和の各成分同士が可換で群演算の順序を考慮しなくてよい事実が本質的な役割を果たすが, あらかじめ群の可換性を仮定しない場合は, 群演算の順序の扱いに工夫が必要で, 証明の難易度が格段に増す. 本章では, このような課題に対する形式化上の工夫に焦点を当てて論ずる. 本章の形式化は, 主に [30] の結果に基づいている.

4.1 群の族への写像の台

Mizar 上では形式化 3.4.8 により群の直和が形式化されているが, このままでは扱いにくい. そこで, より扱いやすい条件として, 群の直積の元が直和に含まれる条件「直積の元を写像とみたとき, 台が有限であること」に着目し, これを形式化した. まずは, 群の族への写像の台を定義する.

定義 4.1.1. (群の族への写像の台)
I を集合, $F = \{F_i\}_{i \in I}$ を群の族, $a = (a_i)_{i \in I}$ を I を定義域とし各 $i \in I$ を F_i の元 a_i へ移す写像とする. このとき, a の台を

$$\mathrm{support}(a, F) := \{i \in I \mid a_i \neq 1_{F_i}\}$$

と定義する. ここで, 1_{F_i} は群 F_i の単位元である.

群の族への写像の台は, Mizar 上では以下のように形式化した.

形式化 4.1.2. (群の族への写像の台)

```
definition
  let I be set;
  let F be Group-Family of I;
  let a be Function;
  func support(a,F) -> Subset of I means
:: GROUP_19:def 1
  for i be object holds i in it iff (a.i <> 1_F.i & i in I);
end;
```

定義 4.1.1 を用いると, 群の直積の元 $a = (a_i)_{i \in I}$ が直和に入る条件は, $\mathrm{support}(a, F)$ が有限集合であることと同値である. Mizar 上では以下のように形式化される.

形式化 4.1.3. (群の直積の元が直和に入る条件)

```
theorem :: GROUP_19:8
  for I be set,
      F be Group-Family of I,
      a be Element of product F
  holds
    a in sum F
  iff
    support(a,F) is finite;
```

また, Mizar 上では, 記述を簡約化するため, 群の直和の元の台が有限集合であることをクラスタ登録している.

形式化 4.1.4. (群の直和における元の台の有限性)

```
:: GROUP_19 line 127
registration
  let I be set;
  let F be Group-Family of I;
  let a be Element of sum F;
  cluster support(a,F) -> finite;
end;
```

4.2　群への写像の台

内部直和分解で群の族 $\{F_i\}_{i \in I}$ を扱う場合, これらはある群 G の部分群である. このため, 写像の台は, 群の族に対してだけではなく, 群に対しても定義しておくと都合が良い.

定義 4.2.1. (群への写像の台)

I を集合, G を群, $a : I \to G$ を写像とする. このとき, $a = (a_i)_{i \in I}$ の台を

$$\mathrm{support}(a) := \{i \in I \mid a_i \neq 1_G\}$$

と定義する. ここで, 1_G は G の単位元である.

Mizar上では以下のように形式化した.

形式化 4.2.2. (群への写像の台)

```
definition
  let I be set;
  let G be Group;
  let a be Function of I,G;
  func support a -> Subset of I means
:: GROUP_19:def 2
  for i be object holds i in it iff (a.i <> 1_G & i in I);
end;
```

さらに, Mizar上では有限な台をもつ群への写像をアトリビュートとして形式化している.

形式化 4.2.3. (有限な台をもつ群への写像)

```
definition
  let I be set;
  let G be Group;
  let a be Function of I,G;
  attr a is finite-support means
:: GROUP_19:def 3
  support a is finite;
end;
```

4.3 群の直積・直和と写像の台の諸性質

群の直積の元を写像とみたとき, 元が直和に含まれることと, 写像の台が有限集合であることは同値であった. このため, 群の直積・直和と写像の台に関する諸性質をまとめておくと, このあとの形式化が簡約化される. Mizar 上での一連の形式化では, 1000行ほどを費やしてこれら諸性質を定理群としてまとめている. この節では, その中から幾つかの定理を抜粋して紹介する.

定理 4.3.1. (群への写像の台と部分群の族への写像の台)
I を集合, G を群, $H = \{H_i\}_{i \in I}$ を G の部分群の族とする. このとき, $x : I \to G$ と $y \in \prod_{i \in I} H_i$ が写像として一致するなら, $\mathrm{support}(x) = \mathrm{support}(y, H)$.

証明は support の定義より自明. 上の定理を Mizar 上で形式化すると, 以下のようになる.

形式化 4.3.2. (群への写像の台と部分群の族への写像の台)

```
theorem :: GROUP_19:9
  for I be set,
      G be Group,
      H be Group-Family of I,
      x be Function of I,G,
      y be Element of product H
  st x = y
   & for i be object st i in I holds H.i is Subgroup of G
  holds support(x) = support(y,H);
```

定理 4.3.3. (写像の台が空の場合)

I を非空集合, G を群, $F = \{F_i\}_{i \in I}$ を G の部分群の族, $x : I \to G$, $y \in \prod_{i \in I} F_i$とする. このとき,

$$\forall i \in I, x(i) = 1_G \iff \mathrm{support}(x) = \emptyset$$
$$y\text{が}\prod_{i \in I} F_i\text{の単位元} \iff \mathrm{support}(y, F) = \emptyset$$

証明は support の定義より自明. 以下は, 上の定理を Mizar 上で形式化したものである.

形式化 4.3.4. (写像の台が空の場合)

```
theorem :: GROUP_19:11
  for I be non empty set,
      F be Group-Family of I holds
  support(1_product F,F) is empty;

theorem :: GROUP_19:12
  for I be non empty set, G be Group,
      a be Function of I,G
  st a = I --> 1_G
  holds support(a) is empty;

theorem :: GROUP_19:13
  for I be non empty set, G be Group,
      F be Group-Family of I
  st for i be Element of I holds F.i is Subgroup of G
  holds 1_product F = I --> 1_G;

theorem :: GROUP_19:14
  for I be non empty set,
      F be Group-Family of I,
      G be Group,
      x be finite-support Function of I,G
  st support(x) = {}
```

```
 & for i be object st i in I holds F.i is Subgroup of G
holds x = 1_product F;
```

定理 4.3.5. (プリミティブな写像の台)

I を空でない集合, G を群, $F = \{F_i\}_{i\in I}$ を G の部分群の族, $x : I \to G$, $y \in \prod_{i\in I} F_i$ を写像とする. このとき,

$$x : i \mapsto \begin{cases} g \in G & (i = j) \\ 1_G & (\text{上記以外}) \end{cases} \Rightarrow \mathrm{support}(x) \subset \{j\}.$$

$$y : i \mapsto \begin{cases} g \in F_j & (i = j) \\ 1_{F_i} & (\text{上記以外}) \end{cases} \Rightarrow \mathrm{support}(y, F) \subset \{j\}.$$

この定理をMizar上で形式化したものは以下である.

形式化 4.3.6. (プリミティブな写像の台)

```
theorem :: GROUP_19:17
  for I be non empty set,
      F be Group-Family of I,
      x be Element of product F,
      i be Element of I,
      g be Element of F.i
  st x = 1_product F +* (i,g)
  holds support(x,F) c= {i};

theorem :: GROUP_19:19
  for I be non empty set, G be Group,
      i be Element of I, g be Element of G,
      a be Function of I,G
  st a = (I --> 1_G) +* (i,g)
  holds support(a) c= {i};
```

上の形式化で使われている記号 `+*(x,y)` は, 写像の置き換え操作

$$f\texttt{+*}(x, y) : i \mapsto \begin{cases} y & (i = x) \\ f(i) & (\text{上記以外}) \end{cases}$$

を意味する.

定理 4.3.7. (台が共通集合を持たない2元の可換性)

I を空でない集合, $F = \{F_i\}_{i\in I}$ を群の族とする. $x, y \in \prod_{i\in I} F_i$ の台が共通集合を持たないとき, x と y は可換である. すなわち,

$$\mathrm{support}(x, F) \cap \mathrm{support}(y, F) = \emptyset \Rightarrow x \cdot y = y \cdot x.$$

証明. $x = (x_i)_{i\in I}$, $y = (y_i)_{i\in I}$ とする. 群の直積の定義から, $x \cdot y = (x_i \cdot y_i)_{i\in I}$. ここで,

$\mathrm{support}(x,F) \cap \mathrm{support}(y,F) = \emptyset$ から, 任意の $i \in I$ に対して x_i または y_i のどちらかは単位元に等しいので, $x_i \cdot y_i = y_i \cdot x_i$. ゆえに, $x \cdot y = (x_i \cdot y_i)_{i \in I} = (y_i \cdot x_i)_{i \in I} = y \cdot x$. □

上の定理は, Mizar 上で以下のように形式化した.

形式化 4.3.8. (台が共通集合を持たない二元の可換性)

```
theorem :: GROUP_19:32
  for I be non empty set,
      F be Group-Family of I,
      a,b be Element of product F
  st support(a,F) misses support(b,F)
  holds a * b = b * a;
```

4.4　群演算による総乗

群の内部直和分解を形式化するには, 群 G の元の有限集合 $x = \{x_i \in G \mid i \in I\}$ に対して群演算を適用する必要がある. 一般に, 非可換群においては, 元の有限集合に対して演算をどの順序で適用するかによって結果が異なってくるため形式化では注意が必要となる. まず, 群演算による総乗について述べる.

定義 4.4.1. (群演算による総乗)
I を空でない集合, G を群, $f : I \to G$ は $\mathrm{support}(f)$ が有限集合である写像とする. このとき, G の元の集合 $f(I)$ が G 上で可換であるとき,

$$\prod f := \prod_{i \in \mathrm{support}(f)} f(i)$$

は, 群演算をどの順序で適用するかに依らず一意に定まる. これを **群演算による総乗** とよぶ.

上の定義においては f の像が G で可換であることを仮定している. Mizar 上の形式化では, まず定義域が有限集合である場合に群演算による総乗を形式化している.

形式化 4.4.2. (有限集合上での群演算による総乗)

```
definition
  let G be non empty multMagma,
  I be finite set,
  b be (the carrier of G)-valued total I -defined Function;
  func Product b -> Element of G means
:: GROUP_17:def 1
  ex f being FinSequence of G st it = Product f & f = b*canFS(I);
end;
```

上記の形式化において, `canFS(I)`は有限集合 `I` の順列を一つ選び, 1から始まる正整数で添字付けし

た有限列である．特に canFS(I) は Mizar システムにより任意に定められる有限列のため, 順序不定となり注意が必要である．(例えば, $I = \{1, 2\}$ のとき, canFS(I) $= [1, 2]$ となるか $[2, 1]$ となるかは分からないため, Mizar 利用者はこの順序に依存しないように形式化しなければならない.) b は定義域を I とする G への写像であるから, f = b*canFS(I) は b の像を1から始まる整数で添字付けした有限列となる．有限列 $f = (f_1, f_2, \ldots, f_n)$ に対する群演算による総乗は, $f_1 \cdot f_2 \cdots f_n$ である．このため, GROUP_17:def 1 の定義では, b の像が非可換であれば群演算による総乗 Product b は不定となる．この形式化には危うい面があるが, 何らかの不定な順列を経由することなしに群演算による総乗を形式化することはできない．有限集合 I が順序集合であることを条件として群演算の総乗を定義することで順序に依存する問題は避けられるものの, すでに多くの形式化がこの定義を用いておこなわれているため, 今回の形式化でもこの方針を踏襲することとした．

上記の形式化を用いて, 定義域が無限集合の場合にも適用できるように, 有限な台をもつ群 G への写像に対して群演算による総乗を形式化した．

形式化 4.4.3. (無限集合上での群演算による総乗)

```
definition
  let I be set;
  let G be Group;
  let a be finite-support Function of I,G;
  func Product a -> Element of G equals
:: GROUP_19:def 4
  Product(a|support(a));
end;
```

上記の形式化において support(a) は, G の単位元以外を値に持つ a の定義域の部分集合であるから, 単位元を除く a の像は全て a|support(a) の像に含まれる．この形式化も定義 4.4.2 に依存しているため, a の像が非可換であれば Product(a) は不定となる．形式化においては, a の像が G 上で可換であることを前提条件として Product(a) を利用している．

4.5 群の外部直和分解

群の外部直和分解(定義 3.5.7)は, Mizar 上で群同型を用いて以下のように形式化した．

形式化 4.5.1. (群の外部直和分解)

```
definition
  let I be non empty set;
  let G be Group;
  mode DirectSumComponents of G,I -> Group-Family of I means
:: GROUP_19:def 8
```

```
  ex h be Homomorphism of sum it, G st h is bijective;
end;
```

4.6 群の内部直和分解

Mizar 上では, 群の内部直和分解(定義 3.5.8)を外部直和分解のアトリビュートとして形式化した.

形式化 4.6.1. (群の内部直和分解)

```
definition
  let I be non empty set;
  let G be Group;
  let F be DirectSumComponents of G,I;
  attr F is internal means
:: GROUP_19:def 9
   (for i be Element of I holds F.i is Subgroup of G)
  & ex h be Homomorphism of sum F, G
    st h is bijective
     & for x be finite-support Function of I,G st x in sum F holds
       h.x = Product x;
end;
```

上記の形式化において, `h` が well-defined であること, つまり `Product x` が一意に定まることを示す必要があるが, これは $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} F_i$ であることと h が群同型であることにより, $i, j \in I$ に対して $x_i \cdot x_j = x_j \cdot x_i$ が G 上で成り立つことから導かれる.

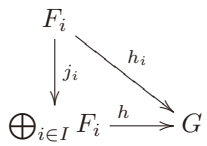
群の内部直和分解の定義 3.5.8 において, $h : (x_i)_{i\in I} \mapsto \prod_{i\in I} x_i$ が一意に定まることの議論は, $\{F_i\}_{i\in I}$ が互いに可換であることによる. このため, $\{F_i\}_{i\in I}$ が互いに可換であることを明示的に内部直和分解の定義に加えておくと, 今後の形式化の見通しが良くなる.

定理 4.6.2. (群の内部直和分解の書き換え)
I を空でない集合, G を群とする. このとき, 群の族 $\{F_i\}_{i\in I}$ が G の内部直和分解であることと以下の条件が成り立つことは同値.

(B1) 各 $i \in I$ に対して F_i は G の部分群.
(B2) 任意の $i, j \in I$, $i \neq j$ に対して, F_i の元と F_j の元は可換. すなわち, $x_i \in F_i$, $x_j \in F_j$ ならば, (G 上の演算において) $x_i \cdot x_j = x_j \cdot x_i$.
(B3) $y \in G$ ならば, ある $(x_i)_{i\in I} \in \bigoplus_{i\in I} F_i$ が存在し, (x_i を G の元とみたとき) $y = \prod_{i\in I} x_i$ の形に一意に表される.

証明. ($\Rightarrow$) (B1) および (B3) は定義 3.5.8 より自明.

(B2) は



において, h が群同形であることと, 直積における2元の可換性(定理 4.3.7)から示される.

($\Leftarrow$) 定義 3.5.8 の (A1) は自明. (A2) は, h が集合として全単射であることは (B3) より自明で, 群準同形となることは後述する定理 4.6.4 により証明される. □

上記の定理をMizar上で形式化した定理は以下である.

形式化 4.6.3. (群の内部直和分解の書き換え)

```
theorem :: GROUP_19:54
  for I be non empty set,
      G be Group,
      F be Group-Family of I
  holds
    F is internal DirectSumComponents of G,I
  iff
   (for i be Element of I holds F.i is Subgroup of G)
  &(for i,j be Element of I, gi,gj be Element of G
    st i <> j & gi in F.i & gj in F.j holds gi * gj = gj * gi)
  &(for y be Element of G
    ex x be finite-support Function of I,G
    st x in sum F & y = Product x)
  &(for x1,x2 be finite-support Function of I,G
    st x1 in sum F & x2 in sum F & Product x1 = Product x2 holds x1 = x2);
```

標準的な教科書 [*1] では $\{F_i\}_{i\in I}$ の元が互いに可換であることを条件に含めた上記の定理 4.6.2 における内部直和分解と同値な性質を定義としているが, 今回の形式化では, 圏論的相対直積の延長であり, 内部直和分解が外部直和分解の特殊形であることが明示的に分かる定義 3.5.8 を群の内部直和分解の定義として採用した.

定理 4.6.2 の $\Leftarrow$ 方向の証明で残っていた$h : (x_i)_{i\in I} \mapsto \prod_{i\in I} x_i$ が群準同形となることの証明は, 以下の定理による.

定理 4.6.4. (部分群の可換性と成分総乗の準同形性)
I を空でない集合, G を群, $\{F_i\}_{i\in I}$ を G の部分群の族とする. このとき, $\{F_i\}_{i\in I}$ が G で可換, すなわち任意の $i, j \in I$, $x_i \in F_i$, $x_j \in F_j$ に対して(G の元として) $x_i \cdot x_j = x_j \cdot x_i$ が成り立つならば, $h : (x_i)_{i\in I} \mapsto \prod_{i\in I} x$ は $\bigoplus_{i\in I} F_i$ から G への群準同形写像である.

[*1] [12] の1章6節の定義7

証明. ここでは形式化証明の方針について述べる. 形式化証明では, Product において群演算がどの順序で適用されるかについて注意を払わなければならない.

I が有限集合の場合: 集合 I の元の個数の帰納法で証明する. $\sharp I = 1$ の場合は自明. $\sharp I = n$ の場合に成り立つと仮定し, $\sharp I = n+1$ の場合を証明する. このとき, Product の定義より, ある $i \in I$ が存在し, $I' = I \setminus \{i\}$ とすると, $x \in \prod_{i\in I} H_i$ に対して, $\mathrm{Product}(x) = \mathrm{Product}(x \restriction_{I'}) \cdot x_i$ が成り立つ. ゆえに,

$$\begin{aligned}
\mathrm{Product}(x \cdot y) &= \mathrm{Product}(x \restriction_{I'} \cdot y \restriction_{I'},\ x_i \cdot y_i) && (4.1)\\
&= \mathrm{Product}(x \restriction_{I'} \cdot y \restriction_{I'}) \cdot (x_i \cdot y_i) && (4.2)\\
&= \mathrm{Product}(x \restriction_{I'}) \cdot \mathrm{Product}(y \restriction_{I'}) \cdot x_i \cdot y_i && (4.3)\\
&= \mathrm{Product}(x \restriction_{I'}) \cdot x_i \cdot \mathrm{Product}(y \restriction_{I'}) \cdot y_i && (4.4)\\
&= \mathrm{Product}(x) \cdot \mathrm{Product}(y) && (4.5)
\end{aligned}$$

上の等式変形で, (4.2) から (4.3) では帰納法の仮定を, (4.3) から (4.4) では可換性の仮定を用いている.

I が無限集合の場合: $x = (x_i)_{i\in I},\ y = (y_i)_{i\in I} \in \prod_{i\in I} H_i$ とする. $\{x_i\}_{i\in I},\ \{y_i\}_{i\in I}$ の中で, 単位元と異なる元は有限個であるから, x_i と y_i のいずれかが単位元と異なる $i \in I$ も有限個しかない. このような I の有限部分集合を I' とおくと, I が有限集合の場合に帰着することができ,

$$\begin{aligned}
\mathrm{Product}(x \cdot y) &= \mathrm{Product}((x \cdot y) \restriction_{I'})\\
&= \mathrm{Product}(x \restriction_{I'}) \cdot \mathrm{Product}(y \restriction_{I'})\\
&= \mathrm{Product}(x) \cdot \mathrm{Product}(y).
\end{aligned}$$

□

上記の定理を Mizar で形式化したものが以下である.

形式化 4.6.5. (部分群の可換性と成分総乗の準同形性)

```
theorem :: GROUP_19:53
  for I be non empty set, G be Group,
      F be Group-Family of I,
      sx,sy being Element of sum F,
      x,y,xy be finite-support Function of I,G
  st (for i be Element of I holds F.i is Subgroup of G)
   & (for i,j be Element of I, gi,gj be Element of G
      st i <> j & gi in F.i & gj in F.j
      holds gi * gj = gj * gi)
   & sx = x & sy = y & sx * sy = xy
  holds Product xy = Product(x) * Product(y);
```

第5章

群の直和分解と同値な表現

本章では, 群の内部直和分解と同値な表現と外部直和分解と内部直和分解の同値性に関する定理と, これらの Mizar 上での形式化について解説する. 本章の形式化は, 主に[30, 31]の結果に基づいている.

5.1 集合間の写像の直積

外部直和分解と内部直和分解の同値性の形式化証明では, 群準同形写像の直積が登場する. 本節では, 群準同形写像の直積を形式化する準備として, 集合間の写像の直積について形式化を解説する.

定義 5.1.1. (集合間の写像の直積)
I を非空集合, $\{F_i\}_{i\in I}$, $\{G_i\}_{i\in I}$ を非空集合の族, $\{h_i : F_i \to G_i\}_{i\in I}$ を集合間の写像の族とする. このとき, **集合間の写像の直積** $h = \prod_{i\in I} h_i$ を, $\prod_{i\in I} F_i$ から $\prod_{i\in I} G_i$ への写像で, $h : (x_i)_{i\in I} \mapsto (h_i(x_i))_{i\in I}$ と定義する.

Mizar 上では, 以下のように形式化している.

形式化 5.1.2. (集合間の写像の直積)

```
definition
  let F, G be non-empty non empty Function,
      h be non empty Function;
  assume
   dom F = dom G = dom h
    & for i be object st i in dom h holds h.i is Function of F.i,G.i;
  func ProductMap(F,G,h) -> Function of product F,product G means
:: GROUP_19:def 5
  for x being Element of product F, i being object st i in dom h holds
  ex hi be Function of F.i,G.i st hi = h.i & (it.x).i = hi.(x.i);
end;
```

集合間の写像の直積は, 単射性・全射性を保つ.

定理 5.1.3. (集合間の写像の直積による単射性・全射性の保存)
I を非空集合, $\{F_i\}_{i\in I}$, $\{G_i\}_{i\in I}$ を非空集合の族, $\{h_i : F_i \to G_i\}_{i\in I}$ を集合間の写像の族とする.
このとき,

1. 任意の $i \in I$ に対して h_i が単射なら, $\prod_{i\in I} h_i$ も単射.
2. 任意の $i \in I$ に対して h_i が全射なら, $\prod_{i\in I} h_i$ も全射.
3. 任意の $i \in I$ に対して h_i が全単射なら, $\prod_{i\in I} h_i$ も全単射.

が成り立つ.

上記の定理は, Mizar上で以下の3つの定理で形式化した.

形式化 5.1.4. (集合間の写像の直積による単射性・全射性の保存)

```
theorem :: GROUP_19:35
  for F,G be non-empty non empty Function,
        h be non empty Function
  st dom F = dom G = dom h
   & for i be object st i in dom h holds
     ex hi be Function of F.i,G.i
     st hi = h.i & hi is onto
  holds ProductMap(F,G,h) is onto;

theorem :: GROUP_19:36
  for F,G be non-empty non empty Function,
        h be non empty Function
  st dom F = dom G = dom h
   & for i be object st i in dom h holds
     ex hi be Function of F.i,G.i st hi = h.i & hi is one-to-one
  holds ProductMap(F,G,h) is one-to-one;

theorem :: GROUP_19:37
  for F,G be non-empty non empty Function,
        h be non empty Function
  st dom F = dom G = dom h
   & for i be object st i in dom h holds
     ex hi be Function of F.i,G.i st hi = h.i & hi is bijective
  holds ProductMap(F,G,h) is bijective;
```

5.2 群準同形の直積と直和

定義 5.2.1. (群準同形の直積)
I を非空集合, $\{F_i\}_{i\in I}$, $\{G_i\}_{i\in I}$ を群の族, $\{h_i : F_i \to G_i\}_{i\in I}$ を群準同形の族とする. このとき, **群準同形の直積** $h = \prod_{i\in I} h_i$ は, $\prod_{i\in I} F_i$ から $\prod_{i\in I} G_i$ への群準同形で, $h : (x_i)_{i\in I} \mapsto (h_i(x_i))_{i\in I}$ と定義される.

証明. $x = (x_i)_{i\in I}$, $y = (y_i)_{i\in I}$ を $\prod_{i\in I} F_i$ の元とすると, 群の直積の定義と各 h_i が群準同形であることから,

$$h(x \cdot y) = (h_i(x_i \cdot y_i))_{i\in I} = (h_i(x_i) \cdot h_i(y_i))_{i\in I} = h(x) \cdot h(y).$$

ゆえに, h は群準同形である. □

Mizar上では, 集合間の写像の直積を用いて, 群準同形の直積を以下のように形式化した.

形式化 5.2.2. (群準同形の直積)

```
definition
  let I be non empty set,
      F,G be Group-Family of I,
      h be non empty Function;
  assume
   I = dom h
    & for i be object st i in I holds h.i is Homomorphism of F.i,G.i;
  func ProductMap(F,G,h) -> Homomorphism of product F,product G equals
:: GROUP_19:def 6
  ProductMap(Carrier F,Carrier G,h);
end;
```

集合間の写像の場合と同様に, 群準同形の直積に対しても, 同型性が引き継がれる. Mizar上では, 以下のように形式化した.

形式化 5.2.3. (群準同形の直積による同型性の保存)

```
theorem :: GROUP_19:40
  for I be non empty set,
      F,G be Group-Family of I,
      h be non empty Function
  st I = dom h
   & for i be object st i in I holds
     ex hi be Homomorphism of F.i,G.i
     st hi = h.i & hi is bijective
  holds ProductMap(F,G,h) is bijective;
```

定理 5.2.4. (群準同形の直積による直和の像)
I を非空集合, $\{F_i\}_{i\in I}$, $\{G_i\}_{i\in I}$ を群の族, $\{h_i : F_i \to G_i\}_{i\in I}$ を群準同形の族とする. このとき, 群準同形の直積 $h = \prod_{i\in I} h_i$ に対して, $h(\bigoplus_{i\in I} F_i) \subset \bigoplus_{i\in I} G_i$ が成り立つ.

証明. $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} F_i$ とすると, 直和の定義より x_i が F_i の単位元と異なる $i \in I$ は高々有限個である. $h_i : F_i \to G_i$ は群準同形だから, 単位元は単位元へ移る. ゆえに, $h_i(x_i)$ が G_i の単位元と異なる $i \in I$ も高々有限個である. したがって, $h(x) = (h_i(x_i))_{i\in I}$ は直和 $\bigoplus_{i\in I} G_i$ の元である. □

このことから, 群準同形の直積の定義域を直和へ制限すると, その値域も直和へ収まることが分かった.

定義 5.2.5. (群準同形の直和)
I を非空集合, $\{F_i\}_{i\in I}$, $\{G_i\}_{i\in I}$ を群の族, $\{h_i : F_i \to G_i\}_{i\in I}$ を群準同形の族とする. このとき, $\prod_{i\in I} h_i$ の $\bigoplus_{i\in I} F_i$ への制限を $\bigoplus_{i\in I} h_i$ と定義する. この写像は, $\bigoplus_{i\in I} F_i$ から $\bigoplus_{i\in I} G_i$ への群準同形となる. これを**群準同形の直和**とよぶ.

Mizar 上では, この群準同形の直和を以下のように形式化した.

形式化 5.2.6. (群準同形の直和)

```
definition
  let I be non empty set,
      F,G be Group-Family of I,
      h be non empty Function;
  assume
   I = dom h
    & for i be object st i in I holds
      h.i is Homomorphism of F.i,G.i;
  func SumMap(F,G,h) -> Homomorphism of sum F,sum G equals
:: GROUP_19:def 7
  ProductMap(F,G,h) | sum F;
end;
```

群準同形の直和も同型性を保存する.

定理 5.2.7. (群準同形の直和による同型性の保存)
I を非空集合, $\{F_i\}_{i\in I}$, $\{G_i\}_{i\in I}$ を群の族, $\{h_i : F_i \to G_i\}_{i\in I}$ を群準同形の族とする. このとき, 任意の $i \in I$ に対して h_i が群同型であれば, $h = \bigoplus_{i\in I} h_i$ も $\bigoplus_{i\in I} F_i$ から$\bigoplus_{i\in I} G_i$ への群同型である.

Mizar 上では, 上の定理を以下のように形式化した.

形式化 5.2.8. (群準同形の直和による同型性の保存)

```
theorem :: GROUP_19:41
  for I be non empty set,
      F,G be Group-Family of I,
      h be non empty Function
  st I = dom h
   & for i be object st i in I holds
     ex hi be Homomorphism of F.i,G.i
     st hi = h.i
      & hi is bijective
  holds SumMap(F,G,h) is bijective;
```

5.3 群の内部直和分解と同値な条件

本節では, 以下の群の内部直和分解と同値な条件に関する定理とその形式化について解説する.

定理 5.3.1. (群の内部直和分解と同値な条件) [*1]

I を非空集合, G を群, $\{F_i\}_{i\in I}$ を群の族とする. このとき, $\{F_i\}_{i\in I}$ が G の内部直和分解であることと以下の3条件を満たすことは同値.

(C1) 任意の $i \in I$ に対して F_i は G の正規部分群.
(C2) $G = \langle \bigcup_{i\in I} F_i \rangle$
(C3) $F_j \cap \langle \bigcup_{i\in I, i\neq j} F_i \rangle = \{1_G\}$

ただし, $\langle S \rangle$ は G の元の集合 S により生成される G の部分群である.

証明. ($\Rightarrow$) 定理 4.6.2 の (B1), (B2), (B3) を仮定し, (C1), (C2), (C3) を示す. (B3) より, G の任意の元 g は $\{F_i\}_{i\in I}$ の有限個の元の積の形で書ける. これを, $g = h_{i_1} \cdots h_{i_n}$ $(h_{i_k} \in F_{i_k})$ とする.

(C1): 任意の $f \in F_j$ に対して,

$$g \cdot f \cdot g^{-1} = \prod_{k=1}^{n} h_{i_k} \cdot f \cdot g^{-1} \tag{5.1}$$

$$= h_j \cdot f \cdot \prod_{k=1, i_k \neq j}^{n} h_{i_k} \cdot g^{-1} \tag{5.2}$$

$$= h_j \cdot f \cdot h_j^{-1} \cdot \prod_{k=1}^{n} h_{i_k} \cdot g^{-1} \tag{5.3}$$

$$= h_j \cdot f \cdot h_j^{-1} \in F_j \tag{5.4}$$

上の式変形では, 可換性に関する条件 (B2) を用いている. これにより, F_i は G の正規部分群であるこ

[*1] [12] の1章6節の命題7

とが分かった.

(C2): G の任意の元 g は, $g = h_{i_1} \cdots h_{i_n}$ $(h_{i_k} \in F_{i_k})$ の形に書けるのであったから, $G = \langle \bigcup_{i \in I} F_i \rangle$ である.

(C3): $x \in F_j \cap \langle \bigcup_{i \in I, i \neq j} F_i \rangle$ と仮定すると, $x = h_j \cdot 1_{F_{i_1}} \cdots 1_{F_{i_n}} = 1_{F_j} \cdot h_{i_1} \cdots h_{i_n}$, $i_k \neq j$ と2通りの形に書ける. (B3) により, この表現は一意であるから, h_j, $h_{i_1}, \ldots, h_{i_n}$ はすべて単位元となり, ゆえに x も単位元となる.

($\Leftarrow$) (C1), (C2), (C3)を仮定し, 定理 4.6.2 の (B1), (B2), (B3) を示す.

(B1): (C1) より F_i は G の部分群である.

(B2): $f_i \in F_i$, $f_j \in F_j$ とする. このとき F_j が G の正規部分群であることから,

$$f_i \cdot f_j \cdot f_i^{-1} \cdot f_j^{-1} = (f_i \cdot f_j \cdot f_i^{-1}) \cdot f_j^{-1} \in (f_i \cdot F_j \cdot f_i^{-1}) \cdot f_j^{-1} \subset F_j \cdot F_j = F_j.$$

同様に, $f_i \cdot f_j \cdot f_i^{-1} \cdot f_j^{-1} \in F_i$ もいえる. ゆえに, $f_i \cdot f_j \cdot f_i^{-1} \cdot f_j^{-1} \in F_i \cap F_j$ だが, (C3) より $F_i \cap F_j = \{1_G\}$ なので, $f_i \cdot f_j \cdot f_i^{-1} \cdot f_j^{-1} = 1_G$. ゆえに, $f_i \cdot f_j = f_j \cdot f_i$ となって可換性が示された.

(B3): G の元が $g = f_{i_1} \cdots f_{i_n} = h_{i_1} \cdots h_{i_n}$ $(f_{i_k}, h_{i_k} \in F_i)$ と2通りに表されたと仮定する. このとき,

$$f_{i_1} \cdot h_{i_1}^{-1} = (h_{i_2} \cdots h_{i_n}) \cdot (f_{i_2} \cdots f_{i_n})^{-1} \tag{5.5}$$
$$= (h_{i_2} \cdot f_{i_2}^{-1}) \cdots (h_{i_n} \cdot f_{i_n}^{-1}) \tag{5.6}$$

ここで, 5.5 から 5.6 の変形では, (B2) の F_i の元と F_j の元の可換性を用いている. ここで, $f_{i_1} \cdot h_{i_1}^{-1} \in F_{i_1}$ および$(h_{i_2} \cdot f_{i_2}^{-1}) \cdots (h_{i_n} \cdot f_{i_n}^{-1}) \in \langle \bigcup_{i \in I, i \neq i_1} F_i \rangle$ であるから, (C3) より, $f_{i_1} \cdot h_{i_1}^{-1} = 1_G$. ゆえに, $f_{i_1} = h_{i_1}$. 同様のことが $i_2, \ldots, i_n$ にもいえるので一意性が示された. □

上記の定理をMizar上で形式化したものが以下である.

形式化 5.3.2. (群の内部直和分解と同値な条件)

```
theorem :: GROUP_20:16
  for I be non empty set,
      G be strict Group,
      F be Group-Family of I
  holds
    F is internal DirectSumComponents of G,I
  iff
      (for i be Element of I holds F.i is normal Subgroup of G)
    & (ex UF be Subset of G st UF = Union Carrier F & gr(UF) = G)
    & for i be Element of I holds
      ex UFi be Subset of G
      st UFi = Union((Carrier F) | (I \ {i}))
       & [#](gr(UFi)) /\ [#](F.i) = {1_G};
```

形式化での証明方針は自然言語による証明とほぼ同じであるが, 証明中には長さ不定の有限列が度々現れることや, 可換性の議論の煩雑さから, 形式化証明は補題も含めるとおよそ1000行ほどの長い記述となった.

5.4 群の内部直和分解と外部直和分解の同値性

記述の便宜をはかるため, ここで各成分から直和への埋め込みに関する記号を定義する.

定義 5.4.1. I を非空集合, $\{F_i\}_{i\in I}$ を群の族, $F = \bigoplus_{i\in I} F_i$ とする. $x_i \in F_i$ に対して, $1_F \diamond x_i \in F$ を

$$(1_F \diamond x_i)_j := \begin{cases} x_i & (j = i) \\ 1_{F_j} & (j \neq i) \end{cases}$$

と定義する. ($1_F \diamond x_i$ がどの群に属するか明らかな場合は, $1 \diamond x_i$ のように F を省略することとする.)

この演算子はMizar上で `1ProdHom(F,i)` として以下のように形式化している.

形式化 5.4.2. `definition`

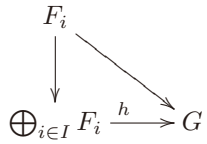
```
  let I be non empty set,
  F be associative Group-like multMagma-Family of I,
  i be Element of I;
  func ProjSet(F,i) -> Subset of product F means
:: GROUP_12:def 1
  for x be set holds x in it iff
  ex g be Element of F.i st x = 1_product F +* (i,g);
end;

definition
  let I be non empty set,
  F be associative Group-like multMagma-Family of I,
  i be Element of I;
  func ProjGroup(F,i) -> strict Subgroup of product F means
:: GROUP_12:def 2
  the carrier of it = ProjSet(F,i);
end;

definition
  let I, F, i;
  func 1ProdHom (F,i) -> Homomorphism of F.i, ProjGroup(F,i) means
:: GROUP_12:def 3
  for x be Element of F.i holds it.x = 1_product F +* (i,x);
end;
```

定理 5.4.3. (群準同形と総乗)

I を非空集合, G を群, $\{F_i\}_{i\in I}$ を G の部分群の族, $F = \bigoplus_{i\in I} F_i$ とする. このとき, 群準同形 $h : \bigoplus_{i\in I} F_i \to G$ が, 任意の F_i の元 x_i に対して $h(1_F \diamond x_i) = x_i$ を満たすならば, 任意の $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} F_i$ に対して $h(x) = \prod_{i\in I} x_i$ である.



証明. $x = \prod_{i\in I} 1_F \diamond x_i$ であるから, h の準同型性より, $h(x) = \prod_{i\in I} h(1_F \diamond x_i) = \prod_{i\in I} x_i$. □

Mizar上では以下のように形式化した.

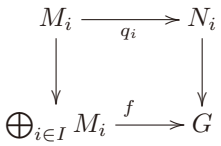
形式化 5.4.4. (群準同形と総乗)

```
theorem :: GROUP_20:18
  for I be non empty set,
      G be Group,
      F be Subgroup-Family of I,G,
      h be Homomorphism of sum F,G,
      a be finite-support Function of I,G
  st a in sum F
   & for i be Element of I, x be Element of F.i
     holds h.(1ProdHom(F,i).x) = x
  holds h.a = Product a;
```

上記の定理を用いて, 群の内部直和分解と外部直和分解の同値性を以下のように示している.

定理 5.4.5. (群の内部直和分解と外部直和分解の同値性)
I を非空集合, G を群, $\{M_i\}_{i\in I}$ を G の外部直和分解とする. このとき, 外部直和分解に関する群同型 $f : \bigoplus_{i\in I} M_i \to G$ と, G の内部直和分解 $\{N_i\}_{i\in I}$ が存在し $f(M_i) = N_i$ を満たす.

証明. 外部直和分解の定義より, ある群同型 $f : \bigoplus_{i\in I} M_i \to G$ が存在する.



$N_i = f(M_i)$ とすると, f の準同形性から N_i は G の部分群となる. $q_i = f \restriction_{M_i}$ と置くと, f は群同型だから, q_i も群同型. ゆえに, $q = \bigoplus_{i\in I} q_i$ とおくと, $q : \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} N_i$ は群同型. したがって, $h = f \circ q^{-1} : \bigoplus_{i\in I} N_i \to G$ は群同型である. $N = \bigoplus_{i\in I} N_i$ とおく. $y = (y_i)_{i\in I} \in \bigoplus_{i\in I} N_i$ に対

して, $x_i = q_i^{-1}(y_i) \in M_i$ とおくと,

$$\begin{aligned} h(1_N \diamond y_i) &= f \circ q^{-1}(1_N \diamond y_i) \\ &= f \circ q_i^{-1}(y_i) \\ &= f(x_i) \\ &= f \restriction_{M_i} (x_i) \\ &= q_i(x_i) \\ &= y_i. \end{aligned}$$

したがって, h の準同型性から定理 5.4.3 が使えて, $h(y) = \prod_{i \in I} y_i$ である. よって, 定義 3.5.8 より, $\{N_j\}_{i \in I}$ は G の内部直和分解である. □

上記の定理を Mizar 上で形式化したものが以下である.

形式化 5.4.6. (群の内部直和分解と外部直和分解の同値性)

```
theorem :: GROUP_20:19
  for I be non empty set,
      G be Group,
      M be DirectSumComponents of G,I
  holds
  ex f be Homomorphism of sum M,G,
     N be internal DirectSumComponents of G,I
  st f is bijective
   & for i be Element of I holds
     ex qi be Homomorphism of M.i,N.i
     st qi = f * 1ProdHom(M,i)
      & qi is bijective;
```

この定理により, 多くの場合, 外部直和分解と内部直和分解は同等に取り扱ってよいことがわかる.

第6章

群の直和分解の不変性

本章では, 群の直和分解に関する幾つかの不変性と, その Mizar 上での形式化について解説する. 本章の形式化は, 主に GROUP_21 の結果に基づいている. (GROUP_21 は *Journal of Formalized Mathematicis* へ投稿・査読中である.)

6.1 添字置換に対する群の直和分解の不変性

本節では, 群の族の添字置換に対して群の直和分解の性質は不変であることを示す. この操作は, 単に群の族の添字を置き換えるだけであるから, 直観的には明らかである. しかし, 形式化となると添字の置き換えによる影響をクリアにしなければならず自明ではない. まず, 群の族の添字変換, 添字置換を以下のように定義する.

定義 6.1.1. (群の族の添字変換, 添字置換)
I, J を非空集合, $\{F_j\}_{j\in J}$ を群の族とする. このとき, 任意の写像 $a : I \to J$ に対して, $\{F_{a(i)}\}_{i\in I}$ を写像 a による群の族 $\{F_j\}_{j\in J}$ の**添字変換**とよぶ. また, 特に写像 a が全単射のときには, **添字置換**とよぶ.

群の族 $F = \{F_j\}_{j\in J}$ は集合 J から群を値に持つ写像と見なせる. したがって, $a : I \to J$ に対して写像の合成 $F \circ a$ もまた群の族とみなせる. Mizar 上ではこの事実を用いて添字変換を以下のように形式化している.

形式化 6.1.2. (群の族の添字変換)

```
definition
  let I,J be non empty set,
      a be Function of I,J,
      F be Group-Family of J;
  redefine func F * a -> Group-Family of I;
```

```
end;
```

定義 6.1.3. (添字変換による直積間写像)

I, J を非空集合, $\{F_j\}_{j\in J}$ を群の族, $a : I \to J$ を写像とする. このとき, 写像 $\Gamma_a : \prod_{j\in J} F_j \to \prod_{i\in I} F_{a(i)}$ を$\Gamma_a : x \mapsto x \circ a$ で定義し, **添字変換による直積間写像**とよぶ. 特に, a が全単射のときには Γ_a を**添字置換による直積間写像**とよぶ.

上記の定義を, Mizar上では以下のように形式化している.

形式化 6.1.4. (添字変換による直積間写像)

```
definition
  let I,J be non empty set;
  let a be Function of I,J;
  let F be multMagma-Family of J;
  func trans_prod(F,a) -> Function of product F, product(F*a) means
:: GROUP_21:def 2
  for x be Element of product F holds it.x = x*a;
end;
```

定理 6.1.5. (添字変換による直積間写像の準同型性)

I, J を非空集合, $\{F_j\}_{j\in J}$ を群の族, $a : I \to J$ を写像とする. このとき, 添字変換による直積間写像 $\Gamma_a : \prod_{j\in J} F_j \to \prod_{i\in I} F_{a(i)}$ は群準同型である

証明. $x = (x_j)_{j\in J}, y = (y_j)_{j\in J} \in \prod_{j\in J} F_j$ に対して,

$$\begin{aligned}\Gamma_a(x \cdot y) &= \Gamma_a((x_j \cdot y_j)_{j\in J}) \\ &= (x_{a(i)} \cdot y_{a(i)})_{i\in I} \\ &= (x_{a(i)})_{i\in I} \cdot (y_{a(i)})_{i\in I} \\ &= \Gamma_a(x) \cdot \Gamma_a(y).\end{aligned}$$

□

Mizar 上では, 直積間写像の準同型性を示した後, redefine する形で形式化した.

形式化 6.1.6. (添字変換による直積間写像の準同型性)

```
theorem :: GROUP_21:5
  for I,J be non empty set,
      a be Function of I,J,
      F be multMagma-Family of J
  holds trans_prod(F,a) is multiplicative;

definition
  let I,J be non empty set;
```

```
  let a be Function of I,J;
  let F be Group-Family of J;
  redefine func trans_prod(F,a) -> Homomorphism of product F, product(F*a);
end;
```

さらに, 添字置換による直積間写像は同型性を保つ.

定理 6.1.7. (添字置換による直積間写像の同型性)
I, J を非空集合, $\{F_j\}_{j\in J}$ を群の族, $a : I \to J$ を写像とする. a が全単射であれば, 添字置換による直積間写像 $\Gamma_a : \prod_{j\in J} F_j \to \prod_{i\in I} F_{a(i)}$ は群同型である.

証明. a の逆写像を用いると, ${\Gamma_a}^{-1} : x \mapsto x \circ a^{-1}$. ゆえに Γ_a は群同型である. □

本定理はMizar上で以下のように形式化している.

形式化 6.1.8. (添字置換による直積間写像の同型性)

```
theorem :: GROUP_21:9
  for I,J be non empty set,
      a be Function of I,J,
      F be multMagma-Family of J
  st a is bijective
  holds trans_prod(F,a) is bijective;
```

同様に, 添字置換による直和間写像が定義できる.

定義 6.1.9. (添字置換による直和間写像)
I, J を非空集合, $\{F_j\}_{j\in J}$ を群の族, $a : I \to J$ を写像とする. このとき, 写像 $\gamma_a : \bigoplus_{j\in J} F_j \to \bigoplus_{i\in I} F_{a(i)}$ を$\gamma_a : x \mapsto x \circ a$ で定義し, **添字置換による直積間写像**とよぶ.

証明. γ_a が well-defined であること, すなわち, γ_a の像が $\bigoplus_{i\in I} F_{a(i)}$ に入っていることを示せばよいが, これは直和の定義より自明. □

Mizar上では, 直積間写像を直和へ制限することにより形式化した.

形式化 6.1.10. (添字置換による直和間写像)

```
definition
  let I,J be non empty set;
  let a be Function of I,J;
  let F be Group-Family of J;
  assume
   a is bijective;
  func trans_sum(F,a) -> Function of sum F, sum(F*a) equals
:: GROUP_21:def 3
```

```
  trans_prod(F,a) | (sum F);
end;

definition
  let I,J be non empty set;
  let a be Function of I,J;
  let F be Group-Family of J;
  assume
   a is bijective;
  redefine func trans_sum(F,a) -> Homomorphism of sum F, sum(F*a);
end;
```

添字置換による直和間写像もまた同型性を保つ.

定理 6.1.11. (添字置換による直和間写像の同型性)
I, J を非空集合, $\{F_j\}_{j\in J}$ を群の族, $a : I \to J$ を写像とする. a が全単射であれば, 添字置換による直和間写像 $\gamma_a : \bigoplus_{j\in J} F_j \to \bigoplus_{i\in I} F_{a(i)}$ は同型である.

証明. a の逆写像を用いると, $\gamma_a^{-1} : x \mapsto x \circ a^{-1}$. □

本定理は, Mizar 上で以下のように形式化した.

形式化 6.1.12. (添字置換による直和間写像の同型性)

```
theorem :: GROUP_21:15
  for I,J be non empty set,
      a be Function of I,J,
      F be Group-Family of J
  st a is bijective
  holds trans_sum(F,a) is bijective;
```

添字置換に対する群の外部直和分解の不変性は以下のように表される.

定理 6.1.13. (添字置換に対する外部直和分解の不変性)
G を群, I, J を非空集合, $\{F_j\}_{j\in J}$ を群の族, $a : I \to J$ を全単射写像とする. このとき, $\{F_j\}_{j\in J}$ が G の外部直和分解であれば, $\{F_{a(i)}\}_{i\in I}$ も G の外部直和分解である.

証明. 外部直和分解の定義から, 群同型 $f : \bigoplus_{j\in J} F_j \to G$ が存在する. また, 定理 6.1.11より, 添字置換による直和間写像 $\gamma_a : \bigoplus_{j\in J} F_j \to \bigoplus_{i\in I} F_{a(i)}$ は群同型である. したがって, $f \circ {\gamma_a}^{-1}$ は $\bigoplus_{i\in I} F_{a(i)}$ から G への群同型であるから, $\{F_{a(i)}\}_{i\in I}$ も G の外部直和分解である. □

添字置換に対する群の外部直和分解の不変性は, Mizar上で以下のように形式化した.

形式化 6.1.14. (添字置換による群の外部直和分解の不変性)

```
theorem :: GROUP_21:16
  for G be Group,
      I,J be non empty set,
      F be DirectSumComponents of G,J,
      a be Function of I,J st a is bijective
  holds F * a is DirectSumComponents of G,I;
```

添字置換に対する群の内部直和分解の不変性は以下のようになる.

定理 6.1.15. (添字置換に対する内部直和分解の不変性)
G を群, I, J を非空集合, $\{F_j\}_{j\in J}$ を群の族, $a : I \to J$ を全単射写像とする. このとき, $\{F_j\}_{j\in J}$ が G の内部直和分解であれば, $\{F_{a(i)}\}_{i\in I}$ も G の内部直和分解である.

証明. $i \in I$, $j = a(i) \in J$, $E_i = F_j$, $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} E_i$, $y = (y_j)_{j\in J} \in \bigoplus_{j\in J} F_j$ で, G の元として $x_i = y_j$ を満たすとする. $\{F_j\}_{j\in J}$ が G の内部直和分解であることから, ある群同形 $f : \bigoplus_{j\in J} F_j \to G$ が存在し $f(1_F \diamond y_j) = y_j$ を満たす. $h = f \circ {\gamma_a}^{-1}$ とすると, f が群同型であることと定理 6.1.11 より h は群同形である. $E = \bigoplus_{i\in I} E_i$, $F = \bigoplus_{j\in J} F_j$ とおくと, $h(1_E \diamond x_i) = f({\gamma_a}^{-1}(1_E \diamond x_i)) = f(1_F \diamond y_j) = y_j = x_i$. ゆえに, 定理 5.4.3 より $h(x) = \prod_{i\in I} x_i$, したがって, $\{E_i\}_{i\in I} = \{F_{a(i)}\}_{i\in I}$ も G の内部直和分解である. □

Mizar上での形式化は以下のようになる.

形式化 6.1.16. (添字置換による群の内部直和分解の不変性)

```
theorem :: GROUP_21:21
  for G be Group,
      I,J be non empty set,
      F be internal DirectSumComponents of G,J,
      a be Function of I,J st a is bijective
  holds F * a is internal DirectSumComponents of G,I;
```

6.2 平坦化と階層化に対する群の直和分解の不変性

本節以降では以下の略記を用いる.

定義 6.2.1. (直和分解の略記)
I を非空集合, G を群, $\{F_i\}_{i\in I}$ を群の族とする. このとき, $G \simeq \bigoplus_{i\in I} F_i$ で $\{F_i\}_{i\in I}$ が G の外部直和分解であることを表す. また, $G \equiv \bigoplus_{i\in I} F_i$ で $\{F_i\}_{i\in I}$ が G の内部直和分解であることを表す.

準備として, 群の二重族を以下のように定義する.

定義 6.2.2. (群の二重族)

I を非空集合, $\{J_i\}_{i\in I}$ を非空集合の族とする. 任意の $i \in I$ に対して, $G_i = \{F_{i,j}\}_{j\in J_i}$ は群の族であるとする. このとき, $\{G_i\}_{i\in I}$ は**群の二重族**である. 以後, $\{G_i\}_{i\in I} = \{F_{i,j}\}_{i\in I, j\in J_i}$ と表記する.

Mizar上では以下のように形式化している.

形式化 6.2.3. (群の二重族)

```
definition
  let I be non empty set;
  let J be ManySortedSet of I;
  mode multMagma-Family of I,J -> ManySortedSet of I means
:: GROUP_21:def 4
  for i be Element of I holds it.i is multMagma-Family of J.i;
end;

definition
  let I be non empty set;
  let J be ManySortedSet of I;
  mode Group-Family of I,J -> multMagma-Family of I,J means
:: GROUP_21:def 5
  for i be Element of I holds it.i is Group-Family of J.i;
end;
```

群の二重族は, 二重添字を持った群の族とも考えられる. 以下は, 群の二重族の添字を単一化し, 群の族へ変換する操作である.

定義 6.2.4. (群の二重族の平坦化)

I を非空集合, $\{J_i\}_{i\in I}$ を空でなく互いに共通部分を持たない集合の族とする. このとき, 集合 $\{(i,j) \mid i \in I,\ j \in J_i\}$ と $\bigcup_{i\in I} J_i$ は, $f : (i,j) \mapsto j$ により一対一に対応する. この対応により, $\tilde{F}_j = F_{i,j}$ と書くと, $\{\tilde{F}_j\}_{j\in\bigcup_{i\in I} J_i}$ は群の族とみなせる. $\{\tilde{F}_j\}_{j\in\bigcup_{i\in I} J_i}$ を $\{F_{i,j}\}_{i\in I, j\in J_i}$ の**平坦化**とよぶ. 以降では, $F_{i,j}$ の元 $x_{i,j}$ の $\tilde{F}_j$ の元への対応を $\tilde{x}_j$ と表記することにする.

Mizar上では以下のように形式化した.

形式化 6.2.5. (群の二重族の平坦化)

```
definition
  let I be non empty set;
  let J be disjoint_valued ManySortedSet of I;
  let F be Group-Family of I,J;
  redefine func Union F -> Group-Family of Union J;
end;
```

上の形式化においては, Union F が $\tilde{F}$ に相当する.

群の族 $\{F_i\}_{i\in I}$ の直積化は $\prod_{i\in I} F_i$ で与えられた. これを群の二重族に対して適用すると, 以下のようになる.

定義 6.2.6. (直積束)

I を非空集合, $\{J_i\}_{i\in I}$ を非空集合の族, $\{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. このとき, $\{F_{i,j}\}_{i\in I, j\in J_i}$ の**直積束** を $\{\prod_{j\in J_i} F_{i,j}\}_{i\in I}$ と定義する.

上記の定義は, Mizar 上では以下のように形式化した.

形式化 6.2.7. (直積束)

```
definition
  let I be non empty set;
  let J be ManySortedSet of I;
  let F be multMagma-Family of I,J;
  func prod_bundle F -> multMagma-Family of I means
:: GROUP_21:def 6
  for i be Element of I holds it.i = product(F.i);
end;

definition
  let I be non empty set;
  let J be ManySortedSet of I;
  let F be Group-Family of I,J;
  redefine func prod_bundle F -> Group-Family of I;
end;
```

これと同様に, 直和についても直和束が定義できる.

定義 6.2.8. (直和束)

I を非空集合, $\{J_i\}_{i\in I}$ を非空集合の族, $\{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. このとき, $\{F_{i,j}\}_{i\in I, j\in J_i}$ の**直和束** を $\{\bigoplus_{j\in J_i} F_{i,j}\}_{i\in I}$ と定義する.

Mizar 上では以下のように形式化した.

形式化 6.2.9. (直和束)

```
definition
  let I be non empty set;
  let J be ManySortedSet of I;
  let F be Group-Family of I,J;
  func sum_bundle F -> Group-Family of I means
:: GROUP_21:def 7
```

```
  for i be Element of I holds it.i = sum(F.i);
end;
```

直積束をさらに直積化することにより, 群が生成される. この操作を以下のように定義する.

定義 6.2.10. (二重直積)

I を非空集合, $\{J_i\}_{i\in I}$ を非空集合の族, $\{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. このとき, $\{F_{i,j}\}_{i\in I, j\in J_i}$ の**二重直積**を $\prod_{i\in I}\prod_{j\in J_i} F_{i,j}$ と定義する.

Mizar上では, 以下のように二重直積を形式化した.

形式化 6.2.11. (二重直積)

```
definition
  let I be non empty set;
  let J be ManySortedSet of I;
  let F be multMagma-Family of I,J;
  func dprod F -> multMagma equals
:: GROUP_21:def 8
  product(prod_bundle F);
end;

definition
  let I be non empty set;
  let J be non-empty ManySortedSet of I;
  let F be Group-Family of I,J;
  redefine func dprod F -> Group;
end;
```

直和に対しても同様に, 二重直和を定義できる.

定義 6.2.12. (二重直和)

I を非空集合, $\{J_i\}_{i\in I}$ を非空集合の族, $\{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. このとき, **二重直和** を $\bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ と定義する.

Mizar上では, 以下のように二重直和を形式化した.

形式化 6.2.13. (二重直和)

```
definition
  let I be non empty set;
  let J be non-empty ManySortedSet of I;
  let F be Group-Family of I,J;
  func dsum F -> Group equals
:: GROUP_21:def 9
```

```
  sum(sum_bundle F);
end;
```

定理 6.2.14. (二重直積と二重直和の関係)
I を非空集合, $\{J_i\}_{i\in I}$ を非空集合の族, $\{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. このとき, $\bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ は $\prod_{i\in I}\prod_{j\in J_i} F_{i,j}$ の部分群である.

証明. 任意の $i \in I$ に対して, $\bigoplus_{j\in J_i} F_{i,j}$ は $\prod_{j\in J_i} F_{i,j}$ の部分群である. ゆえに, $\prod_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ は $\prod_{i\in I}\prod_{j\in J_i} F_{i,j}$ の部分群である. また, $\bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ は $\prod_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ の部分群であるから定理が成り立つ. □

以下は, 上記の定理を Mizar 上で形式化したものである.

形式化 6.2.15. (二重直積と二重直和の関係)

```
theorem :: GROUP_21:25
  for I be non empty set,
      J be non-empty ManySortedSet of I,
      F be Group-Family of I,J
  holds dsum F is Subgroup of dprod F;
```

二重直積から平坦化直積への自然な写像を考えると, これは群同型になる.

定義 6.2.16. (二重直積から平坦化直積への自然な群同形)
I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, $F = \{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. このとき, $\prod_{i\in I}\prod_{j\in J_i} F_{i,j}$ から $\prod_{j\in\bigcup_{i\in I} J_i} \tilde{F}_j$ への自然な群同形を

$$\Phi_F : ((x_{i,j})_{j\in J_i})_{i\in I} \mapsto (\tilde{x}_j)_{j\in\bigcup_{i\in I} J_i}$$

と定義する.

Mizar 上では群同型の定理と合せて以下のように形式化した.

形式化 6.2.17. (二重直積から平坦化直積への自然な群同形)

```
theorem :: GROUP_21:26
  for I be non empty set,
      J be non-empty disjoint_valued ManySortedSet of I,
      F be Group-Family of I,J,
      y be Element of product(Union F),
      i be Element of I
  holds y | (J.i) in product(F.i);

theorem :: GROUP_21:27
  for I be non empty set,
```

```
      J be non-empty disjoint_valued ManySortedSet of I,
      F be Group-Family of I,J
  holds dprod2prod F is bijective;
```

また, 逆写像として, 平坦化直積から二重直積への自然な群同形も定義できる.

定義 6.2.18. (平坦化直積から二重直積への自然な群同形)
I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, $F = \{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. このとき, $\prod_{j\in\bigcup_{i\in I} J_i} \tilde{F}_j$ から $\prod_{i\in I}\prod_{j\in J_i} F_{i,j}$ への自然な群同形を Φ_F の逆写像

$$\Psi_F : (\tilde{x}_j)_{j\in\bigcup_{i\in I} J_i} \mapsto ((x_{i,j})_{j\in J_i})_{i\in I}$$

として定義する.

Mizar 上では以下のように形式化した.

形式化 6.2.19. (平坦化直積から二重直積への自然な群同形)

```
definition
  let I be non empty set;
  let J be non-empty disjoint_valued ManySortedSet of I;
  let F be Group-Family of I,J;
  func prod2dprod F -> Homomorphism of product(Union F), dprod F equals
:: GROUP_21:def 11
  (dprod2prod F)";
end;

theorem :: GROUP_21:28
  for I be non empty set,
      J be non-empty disjoint_valued ManySortedSet of I,
      F be Group-Family of I,J
  holds
    for x be Element of product(Union F), i be Element of I holds
    x | (J.i) = ((prod2dprod F).x).i;
```

直和を扱いやすくするために写像の台を導入したのと同様に, 直和束を扱いやすくするために写像の台の族を定義しておく.

定義 6.2.20. (写像の台の族)
I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, $F = \{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族, x を写像とする. このとき, x の F に関する**写像の台の族**は, I を添字とする集合の族で, $\text{supp-family}_{x,F} : i \mapsto \text{support}(x \restriction_{J_i}, F)$ と定義される.

Mizar 上では以下のように形式化した.

形式化 6.2.21. (写像の台の族)

```
definition
  let I be non empty set,
      J be non-empty disjoint_valued ManySortedSet of I,
      F be Group-Family of I,J,
      x be Function;
  func supp_restr(x,F) -> disjoint_valued ManySortedSet of I means
:: GROUP_21:def 12
  for i be Element of I holds it.i = support(x | (J.i), F.i);
end;
```

これらを用いて, 二重直積から平坦化直積への群同型を直和へ制限すると, 二重直和から平坦化直和への群同型となることが証明できる.

定理 6.2.22. (二重直和から平坦化直和への群同形)
I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, $F = \{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. このとき, Φ_F の 二重直和への制限 $\phi_F = \Phi_F \restriction_{\bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}}$ は, $\bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ から $\bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{F}_j$ への群同型となる.

証明. $((x_{i,j})_{j\in J_i})_{i\in I} \in \bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ とする. このとき, 任意の $i \in I$ に対して, $(x_{i,j})_{j\in J_i} \in \bigoplus_{j\in J_i} F_{i,j}$ より, $\{x_{i,j} \mid j \in J_i\}$ で単位元でないものは高々有限個. また, $((x_{i,j})_{j\in J_i})_{i\in I} \in \bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ より$\{x_{i,j} \mid j \in J_i\}$ が単位元でないものを含む $i \in I$ もまた高々有限個. ゆえに, $\{x_{i,j} \mid i \in I, j \in J_i\}$ で単位元でないものは高々有限個である. したがって, $(\tilde{x}_j)_{j\in\bigcup_{i\in I} J_i} \in \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{F}_j$

逆に, $(\tilde{x}_j)_{j\in\bigcup_{i\in I} J_i} \in \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{F}_j$ とすると, $\{x_{i,j} \mid i \in I, j \in J_i\}$ で単位元でないものは高々有限個である. ゆえに, $\{x_{i,j} \mid j \in J_i\}$ が単位元でないものを含む $i \in I$ は高々有限個, かつ 任意の $i \in I$ に対して $\{x_{i,j} \mid j \in J_i\}$ が単位元でないものも高々有限個である. したがって, $((x_{i,j})_{j\in J_i})_{i\in I} \in \bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$.

準同型性は明らかなので, 定理が成り立つ. □

Mizar 上では, 以下のように形式化している. 形式化証明においては, 写像の台の有限性に関する議論を行なっているが, 本質的には上の証明と同様である.

形式化 6.2.23. (二重直和から平坦化直和への群同形)

```
definition
  let I be non empty set;
  let J be non-empty disjoint_valued ManySortedSet of I;
  let F be Group-Family of I,J;
```

```
  func dsum2sum F -> Homomorphism of dsum(F), sum(Union F) equals
:: GROUP_21:def 13
  (dprod2prod F) | (dsum F);
end;

theorem :: GROUP_21:37
  for I be non empty set,
      J be non-empty disjoint_valued ManySortedSet of I,
      F be Group-Family of I,J
  holds dsum2sum(F) is bijective;
```

また, 逆写像についても同様に定義される.

定義 6.2.24. (平坦化直和から二重直和への群同形)
I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, $F = \{F_{i,j}\}_{i\in I, j\in J_i}$ を群の二重族とする. $\psi_F = {\phi_F}^{-1}$ と定義すると, これは, $\bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{F}_j$ から $\bigoplus_{i\in I}\bigoplus_{j\in J_i} F_{i,j}$ への群同型である.

以上の準備を用いて, 以下の定理を形式化できる.

定理 6.2.25. (平坦化に対する群の外部直和分解の不変性)
I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, G を群とする. また, $\{M_i\}_{i\in I}$, $\{N_{i,j}\}_{i\in I, j\in J_i}$ を群の族とする. このとき, $G \simeq \bigoplus_{i\in I} M_i$ かつ任意の $i \in I$ に対して $M_i \simeq \bigoplus_{j\in J_i} N_{i,j}$ ならば, $G \simeq \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ である.

証明. $G \simeq \bigoplus_{i\in I} M_i$ から, 群同型 $f : \bigoplus_{i\in I} M_i \to G$ が存在する. また, 任意の $i \in I$ に対して $M_i \simeq \bigoplus_{j\in J_i} N_{i,j}$ だから, 群同型 $g_i : \bigoplus_{j\in J_i} N_{i,j} \to M_i$ が存在する. よって, $g = \bigoplus_{i\in I} g_i$ とすると, $g : \bigoplus_{i\in I}\bigoplus_{j\in J_i} N_{i,j} \to \bigoplus_{i\in I} M_i$ は群同型. また, $\psi_N : \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j \to \bigoplus_{i\in I}\bigoplus_{j\in J_i} N_{i,j}$ は群同型. ゆえに, これらを合成した写像 $f \circ g \circ \psi_N : \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j \to G$ は群同型であるから, $G \simeq \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ である. □

Mizar 上では以下のようにこの定理を形式化した.

形式化 6.2.26. (平坦化に対する群の外部直和分解の不変性)

```
theorem :: GROUP_21:42
  for I be non empty set,
      J be non-empty disjoint_valued ManySortedSet of I,
      G be Group,
      M be DirectSumComponents of G,I,
      N be Group-Family of I,J
  st for i be Element of I holds
     N.i is DirectSumComponents of M.i,J.i
```

```
holds
  Union N is DirectSumComponents of G,Union J;
```

内部直和分解に対しては, 以下のようになる.

定理 6.2.27. (平坦化に対する群の内部直和分解の不変性)
I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, G を群とする. また, $\{M_i\}_{i\in I}$, $\{N_{i,j}\}_{i\in I, j\in J_i}$ を群の族とする. このとき, $G \equiv \bigoplus_{i\in I} M_i$ かつ任意の $i \in I$ に対して $M_i \equiv \bigoplus_{j\in J_i} N_{i,j}$ ならば, $G \equiv \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ である.

証明. 外部直和分解の証明中で登場した $f \circ g \circ \psi_N$ が, 定理 5.4.3 の条件を満たすことを示せば十分. $A = \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$, $B = \bigoplus_{i\in I} \bigoplus_{j\in J_i} N_{i,j}$, $C_i = \bigoplus_{j\in J_i} N_{i,j}$, $D = \bigoplus_{i\in I} M_i$ とおく.

$\hat{x}_j \in \tilde{N}_j$ に対して, $\psi_N(1_A \diamond \hat{x}_j) = 1_B \diamond (1_{C_i} \diamond x_{i,j})$. 内部直和分解の仮定 $M_i \equiv \bigoplus_{j\in J_i} N_{i,j}$ より, $g_i(1_{C_i} \diamond x_{i,j}) = x_{i,j}$. よって $g(1_B \diamond (1_{C_i} \diamond x_{i,j})) = 1_D \diamond x_{i,j}$. 内部直和分解の仮定 $G \equiv \bigoplus_{i\in I} M_i$ より, $f(1_D \diamond x_{i,j}) = x_{i,j}$. ゆえに, $(f \circ g \circ \psi_N)(1_A \diamond \hat{x}_j) = x_{i,j} = \hat{x}_j$. これは, 定理 5.4.3 の条件を満たすため, $G \equiv \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ である. □

上記の定理は, Mizar 上で以下のように形式化した.

形式化 6.2.28. (平坦化に対する群の内部直和分解の不変性)

```
theorem :: GROUP_21:43
  for I be non empty set,
      J be non-empty disjoint_valued ManySortedSet of I,
      G be Group,
      M be internal DirectSumComponents of G,I,
      N be Group-Family of I,J
  st for i be Element of I holds
     N.i is internal DirectSumComponents of M.i,J.i
  holds
    Union N is internal DirectSumComponents of G,Union J;
```

平坦化の逆の操作に相当する階層化についても形式化している.

定理 6.2.29. (階層化に対する群の外部直和分解の不変性)
I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, G を群とする. また, $\{M_i\}_{i\in I}$, $\{N_{i,j}\}_{i\in I, j\in J_i}$ を群の族とする. このとき, $G \simeq \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ かつ任意の $i \in I$ に対して $M_i \simeq \bigoplus_{j\in J_i} N_{i,j}$ ならば, $G \simeq \bigoplus_{i\in I} M_i$ である.

証明. $G \simeq \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ から, 群同型 $f : \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j \to G$ が存在する. また, 任意の $i \in I$ に対して $M_i \simeq \bigoplus_{j\in J_i} N_{i,j}$ だから, 群同型 $g_i : \bigoplus_{j\in J_i} N_{i,j} \to M_i$ が存在する. よって, $g = \bigoplus_{i\in I} g_i$ とすると,

$g^{-1} : \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I}\bigoplus_{j\in J_i} N_{i,j}$ は群同型. また, $\phi_N : \bigoplus_{i\in I}\bigoplus_{j\in J_i} N_{i,j} \to \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ は群同型. ゆえに, これらを合成した写像 $f\circ\phi_N\circ g^{-1} : \bigoplus_{i\in I} M_i \to G$ は群同型であるから, $G \simeq \bigoplus_{i\in I} M_i$ である. □

上の定理の形式化は以下のようになる.

形式化 6.2.30. (階層化に対する群の外部直和分解の不変性)

```
theorem :: GROUP_21:44
  for I be non empty set,
      J be non-empty disjoint_valued ManySortedSet of I,
      G be Group,
      M be Group-Family of I
  for N be Group-Family of I,J
  st Union N is DirectSumComponents of G,Union J
   & for i be Element of I holds
     N.i is DirectSumComponents of M.i,J.i
  holds
    M is DirectSumComponents of G,I;
```

また, 内部直和分解に対しては以下のようになる.

定理 6.2.31. (階層化に対する群の内部直和分解の不変性)

I を非空集合, $\{J_i\}_{i\in I}$ を互いに共通部分を持たない非空集合の族, G を群とする. また, $\{M_i\}_{i\in I}$, $\{N_{i,j}\}_{i\in I, j\in J_i}$ を群の族とする. このとき, $G \equiv \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ かつ任意の $i\in I$ に対して $M_i \equiv \bigoplus_{j\in J_i} N_{i,j}$ ならば, $G \equiv \bigoplus_{i\in I} M_i$ である.

証明. 外部直和分解の証明中で登場した $f\circ\phi_N\circ g^{-1}$ が, 定理 5.4.3 の条件を満たすことを示せば十分.

$A = \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$, $B = \bigoplus_{i\in I}\bigoplus_{j\in J_i} N_{i,j}$, $C_i = \bigoplus_{j\in J_i} N_{i,j}$, $D = \bigoplus_{i\in I} M_i$ とおく.

内部直和分解の仮定 $M_i \equiv \bigoplus_{j\in J_i} N_{i,j}$ より, $x_i = (x_{i,j})_{j\in J_i} \in \bigoplus_{j\in J_i} N_{i,j}$ に対して, $g_i(x_i) = \prod_{j\in J_i} x_{i,j}$. $y_i = \prod_{j\in J_i} x_{i,j} \in M_i$ とすると, $g(1_B \diamond x_i) = 1_D \diamond y_i$. よって $g^{-1}(1_D \diamond y_i) = 1_B \diamond x_i$.

$\phi_N(1_B \diamond x_i) = \phi_N(1_B \diamond (x_{i,j})_{j\in J_i}) = \phi_N(1_B \diamond (\prod_{j\in J_i} 1_{C_i} \diamond x_{i,j})) = \prod_{j\in J_i} 1_A \diamond x_{i,j}$.

内部直和分解の仮定 $G \equiv \bigoplus_{j\in\bigcup_{i\in I} J_i} \tilde{N}_j$ より, $f(\prod_{j\in J_i} 1_A \diamond x_{i,j}) = \prod_{j\in J_i} f(1_A \diamond x_{i,j}) = \prod_{j\in J_i} x_{i,j} = y_i$.

ゆえに, $(f\circ\phi_N\circ g^{-1})(1_D \diamond y_i) = y_i$. これは, 定理 5.4.3 の条件を満たすため, $G \equiv \bigoplus_{i\in I} M_i$ である. □

Mizar 上では以下のように形式化した.

形式化 6.2.32. (階層化に対する群の内部直和分解の不変性)

```
theorem :: GROUP_21:45
  for I be non empty set,
      J be non-empty disjoint_valued ManySortedSet of I,
      G be Group,
      M be Subgroup-Family of I,G
  for N be Group-Family of I,J
  st Union N is internal DirectSumComponents of G,Union J
   & for i be Element of I holds
     N.i is internal DirectSumComponents of M.i,J.i
  holds
    M is internal DirectSumComponents of G,I;
```

これらの定理の系として, 単位群追加に対する直和分解の不変性に関する以下の定理が成り立つ.

定理 6.2.33. (単位群追加に対する外部直和分解の不変性)
I, J を $I \subset J$ を満たす非空集合, G を群, $\{X_i\}_{i\in I}$, $\{Y_j\}_{j\in J}$ を群の族で, $\{Y_j\}_{j\in J}$ は $\{X_i\}_{i\in I}$ に単位群を加えた族とする. このとき, $G \simeq \bigoplus_{i\in I} X_i$ ならば, $G \simeq \bigoplus_{j\in J} Y_j$

証明. 以下, 単位群を E とおく. $\{Z_k\}_{k\in J\setminus I} = \{Y_j\}_{j\in J}\setminus\{X_i\}_{i\in I}$ とすると, 定理の仮定より $\{Z_k\}_{k\in J\setminus I}$ は全て単位群だから, $E \simeq \bigoplus_{k\in J\setminus I} Z_k$ は自明. $X = \bigoplus_{i\in I} X_i$ とおくと,定理の仮定から, $G \simeq X$. また, $G \simeq (X \times E)$ も自明. ゆえに, 平坦化に対する群の外部直和分解の不変性から, $G \simeq \bigoplus_{j\in J} Y_j$. □

以下は, Mizar 上の形式化である.

形式化 6.2.34. (単位群追加に対する外部直和分解の不変性)

```
theorem :: GROUP_21:49
  for G be Group,
      I1,I2 be non empty set,
      F1 be DirectSumComponents of G,I1,
      F2 be Group-Family of I2
  st I1 misses I2
   & for i be Element of I2 holds card(F2.i) = 1
  holds F1 +* F2 is DirectSumComponents of G,I1 \/ I2;
```

内部直和分解に対しても同様の議論ができる.

定理 6.2.35. (単位群追加に対する内部直和分解の不変性)
I, J を $I \subset J$ を満たす非空集合, G を群, $\{X_i\}_{i\in I}$, $\{Y_j\}_{j\in J}$ を群の族で, $\{Y_j\}_{j\in J}$ は $\{X_i\}_{i\in I}$ に単位群を加えた族とする. このとき, $G \equiv \bigoplus_{i\in I} X_i$ ならば, $G \equiv \bigoplus_{j\in J} Y_j$

以下は, Mizar 上の形式化である.

形式化 6.2.36. (単位群追加に対する内部直和分解の不変性)

```
theorem :: GROUP_21:50
  for G be Group,
      I1, I2 be non empty set,
      F1 be internal DirectSumComponents of G,I1,
      F2 be Subgroup-Family of I2,G
  st I1 misses I2 & F2 = I2 --> (1).G
  holds
  F1 +* F2 is internal DirectSumComponents of G,I1 \/ I2;
```

第7章

有限可換群の基本定理への応用

本章では, 前章までで解説した群の直和分解の応用事例として, 有限可換群の基本定理について解説する. 有限可換群の基本定理は, 全て有限可換群が巡回群に直和分解できることを示した定理である. 有限可換群の基本定理の証明は, [50, 51] を参考とした. 本章の形式化は, 主に[28, 29]の結果に基づいている. また, 本章の一部はまだ Mizar 上で形式化されていない.

7.1 有限可換群の有限可換p-群への分解

定理 7.1.1. (互いに素な位数を持つ二つの群への直和分解)
G を有限可換群とする. このとき, G の位数 $|G|$ が互いに素な正整数h, k の積 $|G| = hk$ の形に書けるとき, ある G の部分群 H, K で $|H| = h$, $|K| = k$ を満たし, $G \equiv H \times K$ (内部直和分解) となるものが存在する.

証明は, [51] の定理18から定理19までの議論(pp.131–136)を参照されたい. この定理は, Mizar 上で以下のように形式化されている.

形式化 7.1.2. (互いに素な位数を持つ二つの群への直和分解)

```
theorem :: GROUP_17:18
  for G being finite commutative Group,
  h,k be non zero Nat
  st card G = h*k & h,k are_coprime
  ex H,K being strict finite Subgroup of G st
  card H = h & card K = k &
  (the carrier of H) /\ (the carrier of K) = {1_G} &
  ex F being Homomorphism of product <*H,K*>,G
  st F is bijective
  & for a,b be Element of G st a in H & b in K
  holds F.(<*a,b*>) = a*b;
```

上記の定理を逐次的に適用すると, 有限可換p-群への分解となる.

定理 7.1.3. (有限可換群の有限可換p-群への直和分解)
G を有限可換群とする. G の位数の素因数分解が $|G| = {p_1}^{l_1} \cdots {p_n}^{l_n}$ の形に書けるならば, ある G の部分群の族 $\{H_i\}_{1 \leq i \leq n}$ で $|H_i| = {p_i}^{l_i}$ を満たすものが存在して, $G \equiv \bigoplus_{i=1}^{n} H_i$ と書ける.

この定理は, Mizar 上で以下のように形式化されている.

形式化 7.1.4. (有限可換群の有限可換p-群への直和分解)

```
theorem :: GROUP_17:35
  for G being strict finite commutative Group st card G > 1 holds
  ex I be non empty finite set,
  F be associative Group-like commutative multMagma-Family of I st
  I = support (prime_factorization card G)
  & (for p be Element of I holds F.p is strict Subgroup of G &
  card (F.p) = (prime_factorization card G).p) &
  (for p,q be Element of I st p <> q holds
  (the carrier of (F.p)) /\ (the carrier of (F.q)) = {1_G})
  &
  (for y be Element of G
    ex x be (the carrier of G)-valued total I -defined Function
  st (for p be Element of I holds x.p in F.p) & y = Product x)
  &
  for x1,x2 be (the carrier of G)-valued total I -defined Function st
  (for p be Element of I holds x1.p in F.p) &
  (for p be Element of I holds x2.p in F.p) &
  Product x1 = Product x2 holds x1=x2;
```

7.2　有限可換p-群の巡回群への分解

定理 7.2.1. (有限可換p-群の位数最大の巡回群による直和分解)
G を位数が素数累乗の可換群とする. a を G の位数最大の元とすると, ある G の部分群 H が存在し, $G \equiv \langle a \rangle \times H$ (内部直和分解) と書ける.

証明. p を素数, $|G| = p^n$ とし, n に関する帰納法で示す.

$n = 0$ ならば $|G| = 1$ ゆえ明らか.

a を G の位数最大の元とすると, $|G| = \langle a \rangle$ ならば, H を単位群とすると成り立つ. $G \neq \langle a \rangle$ する. $b \in G$ を, $b \notin \langle a \rangle$ ととる. 剰余群 $G/\langle a \rangle$ もまた 有限可換p-群なので, $b\langle a \rangle = p^s$ と書ける. ここで, $c = b^{p^{s-1}}$ とおくと, $c\langle a \rangle$ の位数は p. よって, $c \notin \langle a \rangle$, $c^p \in \langle a \rangle$. このとき, $c^p = a^m$ と書ける. もし $p \nmid m$ であれば, a^m の位数は a の位数に等しいため, c の位数は a の位数より大きくなり, これは a の

位数が最大であることに矛盾する. ゆえに, $p \mid m$. $m = m'p$, $d = ca^{-m'}$ とおくと, $d \notin \langle a \rangle$ で $d^p = 1_G$ が成り立つ. $\langle d \rangle$の位数が素数であることから, $\langle d \rangle \cap \langle a \rangle = 1_G$.

自然な全射 $\pi : G \to G/\langle d \rangle$ を考える. π を $\langle a \rangle$ に制限すると, これは単射なので, $|\pi(\langle a \rangle)| = |\langle \pi(a) \rangle| = |\langle a \rangle|$. ゆえに $\pi(a)$ は $G/\langle d \rangle$ の位数最大の元である. ここで帰納法の仮定から, $G/\langle d \rangle$ のある部分群 U が存在して, $G/\langle d \rangle \equiv \langle \pi(a) \rangle \times U$ となる.

$U' = \pi^{-1}(U)$ に対して, $G \equiv \langle a \rangle \times U'$ を示す. G は可換群なので, $\langle a \rangle$, U はそれぞれ正規部分群. $x \in \langle a \rangle \cap U'$ とすると, $\pi(x) \in \langle \pi(a) \rangle \cap U = \{1_G\}$. よって, $x \in \langle a \rangle \cap \mathrm{Ker}(\pi) = \{1_G\}$ となり, $\langle a \rangle \cap U' = \{1_G\}$ がいえる. π は全射なので, $u' \in U'$ で, $\pi(u') = u$ となるものが存在する. このとき, $\pi(a^i u') = \pi(a)^i u = \pi(g)$ より $g \in a^i u' \langle d \rangle$ なので$g \in a^i u' d^j$ となる整数 j がある. $\pi(d^j) = 1 \in U$ なので, $u'd^j \in U'$ となり, $G = \langle a \rangle U'$ である. 以上より, $G = \langle a \rangle \times U'$. □

この定理は, Mizar 上で以下のように形式化した.

形式化 7.2.2. (有限可換p-群の位数最大の巡回群による直和分解)

```
theorem :: GROUP_18:19
  for G being strict finite commutative Group, p being Prime, m be Nat
  st card(G) = p|^m
  ex K be normal strict Subgroup of G, n, k be Nat, g be Element of G st
  ord g = upper_bound Ordset G & K is finite commutative
  & (the carrier of K) /\ (the carrier of gr{g}) = {1_G}
  & (for x be Element of G
  holds ex b1, a1 be Element of G st b1 in K & a1 in gr{g} & x = b1*a1)
  & ord g = p|^n
  & k = m - n & n <= m
  & card K = p|^k
  & ex F being Homomorphism of product <*K,gr{g}*>, G st F is bijective
  & for a,b be Element of G st a in K & b in gr{g}
  holds F.(<*a,b*>) = a*b;
```

この定理を逐次的に用いると, 有限可換p-群は巡回群に直和分解できる.

定理 7.2.3. (有限可換p-群の巡回群への分解)
G を有限可換p-群とすると, G の部分巡回群の族 $\{H_i\}_{1 \leq i \leq n}$ が存在し, $G \equiv \bigoplus_{i=1}^{n} H_i$.

上の定理は, Mizar 上で以下のように形式化されている.

形式化 7.2.4. (有限可換p-群の巡回群への分解)

```
theorem :: GROUP_18:21
  for G being strict finite commutative Group, p being Prime, m be Nat
  st card(G) = p|^m holds
  ex k be non zero Nat, a be k-element FinSequence of G,
```

```
Inda be k-element FinSequence of NAT,
F be associative Group-like commutative multMagma-Family of Seg k
st (for i be Nat st i in Seg k holds ex ai be Element of G
st ai = a.i & F.i = gr{ai} & ord(ai) = p|^(Inda.i))
& (for i be Nat st 1 <= i & i <= k -1 holds Inda.i <= Inda.(i+1))
& (for p,q be Element of Seg k st p <> q
holds (the carrier of (F.p)) /\ (the carrier of (F.q)) ={1_G})
& (for y be Element of G holds
ex x be (the carrier of G)-valued total (Seg k) -defined Function
st (for p be Element of Seg k holds x.p in F.p) & y = Product x)
& for x1, x2 be (the carrier of G)-valued total (Seg k) -defined Function
st (for p be Element of Seg k holds x1.p in F.p)
 & (for p be Element of Seg k holds x2.p in F.p)
 & Product x1 = Product x2 holds x1 = x2;
```

7.3　有限可換群の基本定理

前節までの準備から, 有限可換群の基本定理が証明できる. 本節で紹介する定理はまだ形式化されていない.

定理 7.3.1. (有限可換群の基本定理 その1)
G を有限可換群とする. このとき, G の部分巡回群の族 $\{H_i\}_{1\leq i\leq n}$ が存在して, $G \equiv \bigoplus_{i=1}^{n} H_i$ と書ける.

証明. 定理 7.1.3 から, G は素数累乗を位数とする部分群の族 $\{M_i\}_{1\leq i\leq m}$ により, $G \equiv \bigoplus_{i=1}^{m} M_i$ と書ける. 同様に, 定理 7.2.3 から, 任意の $1 \leq i \leq m$ に対し, あるM_i の部分群の族 $\{N_{i,j}\}_{1\leq j\leq n_j}$ によって, $M_i \equiv \bigoplus_{j=1}^{n_j} N_{i,j}$ と書ける.

ここで, 添字置換に対する内部直和分解の不変性(定理 6.1.15)から, $M_i \equiv \bigoplus_{j\in J_i} N_{i,j}$ で $\{J_i\}_{1\leq i\leq m}$ は互いに共通部分を持たない有限集合の族とみてよい. ゆえに, 平坦化に対する群の内部直和分解の不変性(定理 6.2.27)より, $G \equiv \bigoplus_{j\in\bigcup_{i=1}^{m} J_i} \hat{N}_j$. ここで, $\hat{N}_j$ は巡回群で, $\bigcup_{i=1}^{m} J_i$ は有限集合である. したがって, ふたたび添字置換に対する内部直和分解の不変性(定理 6.1.15)から, G の部分巡回群の族 $\{H_i\}_{1\leq i\leq n}$ によって $G \equiv \bigoplus_{i=1}^{n} H_i$ と書き直せるから, 定理は証明された. □

さらに, 以下のような表現が可能である.

定理 7.3.2. (有限可換群の基本定理 その2 (存在))
G を有限可換群とする. このとき, G の部分巡回群の族 $\{G_i\}_{1\leq i\leq n}$ で, $G \equiv \bigoplus_{i=1}^{n} G_i$ (内部直和分解) で, $|G_{i+1}|$ が $|G_i|$ を割り切る $(1 \leq i \leq n-1)$ ものが存在する.

証明. $|G|$ を割り切る素因数を $\{p_1, p_2, \ldots, p_r\}$ とし, 有限可換群の有限可換p-群への直和分解(定理7.1.3)から$G \equiv P_1 \times \cdots \times P_r$, 各 $|P_i|$ は p_i の累乗であるものする. このとき, 有限可換p-群の巡回群への分解(定理 7.2.3)から, 各 P_i は 位数を $\{f_{i,j}\}_{1\leq j\leq l(i)}$ とする巡回群の族 $\{C_{f_{i,j}}\}_{1\leq j\leq l(i)}$ によって$P_i \equiv \bigoplus_{j=1}^{l(i)} C_{f_{i,j}}$ と書ける. ここで, 各 $f_{i,j}$ は p_i の冪で, $f_{i,1} \geq f_{i,1} \geq \cdots \geq f_{i,l(i)}$ としておくと, $f_{i,j+1} \mid f_{i,j}$ である. $l(i)(i = 1, 2, ..., r)$ のうち, 最大のものを l とし, $l(i) < l$ なる i は, $f_{i,l(i)+1} = \cdots = f_{i,l} = 1$ として長さを一定にしておく. これは, 単位群追加に対する内部直和分解の不変性(定理 6.2.35) により保証される.

$G_j = C_{f_{i,1}} \cdots C_{f_{i,r}}$ とおくと, 直積因子の巡回群の位数が互いに素であることから, G_jは位数$\prod_{i=1}^{r} f_{i,j}$ の巡回群と同型で, $G_j \equiv \bigoplus_{j=1}^{r} C_{f_{i,j}}$ である. また, 各 i に対して $f_{i,j+1} \mid f_{i,j}$ なので, $|G_{j+1}|$ は $|G_j|$ の約数である. よって, 階層化に対する群の内部直和分解の不変性(定理 6.2.31)から, $G \equiv \bigoplus_{i=1}^{l} G_i$ が求める条件の巡回部分群の族による内部直和分解である. □

定理 7.3.3. (有限可換群の基本定理 その2 (一意性))
有限可換群 G を 定理 7.3.2 のように表す. 位数を $e_i = |G_i|$ としたとき, その列 $e_1, \ldots, e_r$ は一意に定まる.

証明. C_e で位数 e の巡回群を表すものとする. $G \equiv \bigoplus_{i=1}^{r} C_{e_i} \equiv \bigoplus_{j=1}^{s} C_{f_j}, e_{i+1} \mid e_i\ (i = 1, \ldots, r-1)$, $f_{j+1} \mid f_j\ (j = 1, \ldots, s-1)$ と二通りに書けたとする. 自然数 m に対して, $(G, m) = \{g \in G \mid g^m = 1_G\}$ とおく. $a = (a_i) \in \bigoplus_{i=1}^{r} C_{e_i}$ に対して, $a \in (G, m)$ であることと, 各 i に対して $a_i \in (C_{e_i}, m)$ となることは同値. また, 巡回群に対しては, $|(C_n, m)| = \gcd(m, n)$ である.

自然数 m に対して, $S(m)$ で, $m \mid e_i$ なる i の数を, $T(m)$ で, $m \mid f_j$ なる j の数を表すものとする. $e_{i+1} \mid e_i$ という仮定から, $i < j$ で $m \mid e_j$ ならば $m \mid e_i$ であることに注意しておく. f_i についても同様.

p を素数とする. (G, p) を考えると, 上記のことから $|(G, p)| = p^{S(p)} = p^{T(p)}$ である. ゆえに, $S(p) = T(p)$ が成り立つ. また,

$$|(G, p^2)| = p^{2S(p^2)} + p^{S(p)} = p^{2T(p^2)} + p^{T(p)}$$

となるので, $S(p^2) = T(p^2)$ も成り立つ. 同様に繰り返して, 任意の l に対して $S(p^l) = T(p^l)$ である. $e_{i+1} \mid e_i$, $f_{j+1} \mid f_j$ に注意すれば, $p^l \mid e_i$ と $p^l \mid f_i$ が同値になる事が分かる.

以上が全ての素数について成り立つので, $e_i = f_i$. これから一意性が示された. □

第8章

結論

8.1 本論文での結果

本論文では, 群, 部分群, 群準同形, 群の族, 群の直積と直和の定義とその形式化について触れたのち, 群の直和分解に関する形式化として, 以下の定義および定理の形式化の成果を解説した.

- 群の直和に含まれる元の性質
- 無限個の非可換群に対する群の直和分解の定義, 特に外部直和分解と内部直和分解の違い
- 群の内部直和分解と同値な表現に関する定理
- 群の外部直和分解と内部直和分解の同値性に関する定理
- 群の族の添字置換に対する群の直和分解の不変性
- 平坦化および階層化に対する群の直和分解の不変性

また, これらの形式化の応用として, 有限可換群の基本定理の形式化についての現在までの成果(有限可換群の有限可換p-群への内部直和分解, 有限可換p-群の巡回群への内部直和分解) および, 今後の形式化方針について解説した. これらの形式化の成果は, 現代の数理科学の様々な分野から利用される群論の根幹をなすものであるため, 今後幅広い応用が期待される.

また, 第2章では, 今回筆者が開発した Mizar ライブラリのドキュメンテーション生成器について解説した. 本ツールは, インクリメンタル検索により従来のツールよりも素早く直観的にシンボルを検索することができるようになったこと, また, 被参照リストにより特定のシンボルを用いた定義を容易に検索することが可能になったことなどから, 利用者から高い評価を得ている.

8.2 Mizar上での今後の群論の形式化の方向性

第1章で触れた通り, 本形式化の当初の目的は, 暗号理論への応用が主であった. 離散対数問題を形式化するうえで, 有限可換群の基本定理が基本的な役割を担う. 今後の形式化では, まずは有限可換群の基本定理の形式化を完成し, 離散対数問題およびその周辺事実の形式化を進める.

また, 有限可換群の基本定理の拡張として, 以下の有限生成可換群の基本定理の形式化を進める.

定理 8.2.1. (有限生成可換群の基本定理)
有限生成可換群 G は, 有限個の無限巡回群と準素巡回群の直和に同型である.

$$G \simeq \mathbb{Z}^n \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_r}$$

ここで, n, r は正整数, $q_1, \cdots, q_r$ は素数の冪で, q_i の順序を除くと G により一意的に定まる. 特に, G が有限群であれば, $n = 0$ である.

有限可換群の基本定理は, 有限生成可換群の基本定理における捻れ成分に相当し, 証明のかなりの部分を占める.

8.3 形式化支援ツールの今後の開発の方向性

第2章で触れたとおり, 今回作成したツールを強化する目的として, XML-ized MMLを用いた再実装, 定理検索機能の追加, 多言語への拡張, タグコメント機能の追加などを進めたい.

また, 形式化支援ツールの可能性はこれらに留まらない. 他に有望と思われる形式化支援ツールとしては, ソフトウェア開発におけるIDE(統合開発環境)に相当するアプリケーションの構築がある. Coq や Isabelle については, jEdit などの統合開発環境へのプラグインの構築が進められている. 現時点で Mizar には Emacs プラグインが存在するが, ユーザーからはモダンな統合開発環境でのプラグイン開発が待望されている.

謝辞

本論文を執筆するにあたり, 主指導教官としてご指導ならびにご鞭撻を賜りました, 信州大学学術研究院工学系 師玉康成教授に, 心よりの感謝とともに御礼申し上げます. 信州大学学術研究院工学系 山崎浩助教ならびに信州大学学術研究院工学系 岡崎裕之助教には, 研究を進めるにあたってゼミ等で多くのご助言をいただきましたこと, 心より感謝御礼申し上げます. 信州大学学術研究院工学系 和崎克己教授, 信州大学学術研究院工学系 カワモト・ポーリン・ナオミ 准教授 には, セミナーをはじめ, 日本 Mizar 学会などでご助言を頂く機会をいただくきましたこと, 深く感謝申し上げます. 師玉研究室OBの渡瀬泰成博士には, 博士論文作成にあたり, 草稿段階から数多くの有益なご助言を頂きました. 心より感謝御礼申し上げます. 茨城大学工学部 宮島啓一准教授には, 大変お忙しい中, 本博士論文審査に加わって頂きましたこと, 心より深謝申し上げます.

Bialystok 大学の Roman Matuszewski 先生, Adam Grabowski 先生, Artur Kornilowicz 先生, Adam Naumowicz 先生には, Mizar 論文の執筆にあたり, Bialystok で開かれた学会をはじめ, 多くの場面でご指導を頂きましたこと, 心より感謝御礼申し上げます. Radboud 大学の Josef Urban 先生には, Mizar ライブラリのドキュメント生成ツールの開発にあたり, HTML-ized MML の開発者として有益なご助言を頂きました. 心より感謝御礼申し上げます.

参考文献

[1] Jan L Camenisch, Jean-Marc Piveteau, and Markus A Stadler. Blind signatures based on the discrete logarithm problem. Advances in Cryptology—EUROCRYPT'94, pp. 428–432. Springer, 1995.

[2] Kosaku Yosida. *Functional Analysis (Springer Classics in Mathematics)*. Springer, 6th ed. 1995 edition, 4 1996.

[3] Johannes Buchmann. *Introduction to Cryptography (Undergraduate Texts in Mathematics)*. Springer, 2nd edition, 7 2004.

[4] Joseph R Shoenfield. *Mathematical logic*, Vol. 21. Addison-Wesley Reading, 1967.

[5] Robert Boyer, et al. The qed manifesto. *Automated Deduction–CADE*, Vol. 12, pp. 238–251, 1994.

[6] 中島震. ソフトウェア工学の道具としての形式手法. ソフトウェアエンジニアリング最前線, 近代科学社, pp. 27–48, 2007.

[7] Freek Wiedijk. The qed manifesto revisited. *Studies in Logic, Grammar and Rhetoric*, Vol. 10, No. 23, pp. 121–133, 2007.

[8] Roman Matuszewski and Piotr Rudnicki. Mizar: the first 30 years. *Mechanized mathematics and its applications*, Vol. 4, No. 1, pp. 3–24, 2005.

[9] Adam Grabowski, Artur Kornilowicz, and Adam Naumowicz. Mizar in a nutshell. *J. Formalized Reasoning*, Vol. 3, No. 2, pp. 153–245, 2010.

[10] Joseph Rotman. *An introduction to the theory of groups*, Vol. 148. Springer Science & Business Media, 2012.

[11] Derek Robinson. *A Course in the Theory of Groups*, Vol. 80. Springer Science & Business Media, 2012.

[12] ブルバキ数学原論〈〔第5〕〉代数1 (1968年). 東京図書, 1968.

[13] Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, RussellO'Connor, Sidi Ould Bihaほか. A machine-

checked proof of the odd order theorem. In *Interactive Theorem Proving*, pp. 163–179. Springer, 2013.

[14] Iain Whiteside, David Aspinall, and Gudmund Grov. An essence of ssreflect. In *Intelligent Computer Mathematics*, pp. 186–201. Springer, 2012.

[15] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, Vol. 1, No. 5, pp. 821–827, 1990.

[16] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, Vol. 1, No. 5, pp. 855–864, 1990.

[17] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, Vol. 1, No. 5, pp. 955–962, 1990.

[18] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, Vol. 2, No. 1, pp. 41–47, 1991.

[19] Wojciech A. Trybulec. Commutator and center of a group. *Formalized Mathematics*, Vol. 2, No. 4, pp. 461–466, 1991.

[20] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, Vol. 2, No. 4, pp. 573–578, 1991.

[21] Artur Korniłowicz. The product of the families of the groups. *Formalized Mathematics*, Vol. 7, No. 1, pp. 127–134, 1998.

[22] Gijs Geleijnse and Grzegorz Bancerek. Properties of groups. *Formalized Mathematics*, Vol. 12, No. 3, pp. 347–350, 2004.

[23] Marco Riccardi. The Jordan-Hölder theorem. *Formalized Mathematics*, Vol. 15, No. 2, pp. 35–51, 2007.

[24] Marco Riccardi. The Sylow theorems. *Formalized Mathematics*, Vol. 15, No. 3, pp. 159–165, 2007.

[25] Xiquan Liang and Dailu Li. On rough subgroup of a group. *Formalized Mathematics*, Vol. 17, No. 3, pp. 213–217, 2009.

[26] Hiroyuki Okazaki, Kenichi Arai, and Yasunari Shidama. Normal subgroup of product of groups. *Formalized Mathematics*, Vol. 19, No. 1, pp. 23–26, 2011.

[27] Kenichi Arai, Hiroyuki Okazaki, and Yasunari Shidama. Isomorphisms of direct products of finite cyclic groups. *Formalized Mathematics*, Vol. 20, No. 4, pp. 343–347, 2012.

[28] Hiroyuki Okazaki, Hiroshi Yamazaki, and Yasunari Shidama. Isomorphisms of direct products of finite commutative groups. *Formalized Mathematics*, Vol. 21, No. 1, pp. 65–74, 2013.

[29] Hiroshi Yamazaki, Hiroyuki Okazaki, Kazuhisa Nakasho, and Yasunari Shidama. Isomor-

phisms of direct products of cyclic groups of prime power order. *Formalized Mathematics*, Vol. 21, No. 3, pp. 207–211, 2013.

[30] Kazuhisa Nakasho, Hiroshi Yamazaki, Hiroyuki Okazaki, and Yasunari Shidama. Definition and properties of direct sum decomposition of groups. *Formalized Mathematics*, Vol. 23, No. 1, pp. 15–27, 2015.

[31] Kazuhisa Nakasho, Hiroyuki Okazaki, Hiroshi Yamazaki, and Yasunari Shidama. Equivalent expressions of direct sum decomposition of groups. *Formalized Mathematics*, Vol. 23, No. 1, pp. 67–73, 2015.

[32] Xiquan Liang and Dailu Li. Some properties of p-groups and commutative p-groups. *Formalized Mathematics*, Vol. 19, No. 1, pp. 11–15, 2011.

[33] Katarzyna Zawadzka. Solvable groups. *Formalized Mathematics*, Vol. 5, No. 1, pp. 145–147, 1996.

[34] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, Vol. 2, No. 5, pp. 623–627, 1991.

[35] Dariusz Surowik. Isomorphisms of cyclic groups. Some properties of cyclic groups. *Formalized Mathematics*, Vol. 3, No. 1, pp. 29–32, 1992.

[36] Kazuhisa Nakasho and Yasunari Shidama. Documentation generator focusing on symbols for the html-ized mizar library. In *Intelligent Computer Mathematics - International Conference, CICM 2015, Washington, DC, USA, July 13-17, 2015, Proceedings*, pp. 343–347, 2015.

[37] Grzegorz Bancerek and Piotr Rudnicki. Information retrieval in mml. In *MKM*, Vol. 3, pp. 119–132. Springer, 2003.

[38] Ferruccio Guidi and Claudio Sacerdoti Coen. A survey on retrieval of mathematical knowledge. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, Vol. 9150 of *Lecture Notes in Computer Science*, pp. 296–315. Springer International Publishing, 2015.

[39] Jesse Alama, Kasper Brink, Lionel Mamane, and Josef Urban. Large formal wikis: Issues and solutions. In *Intelligent Computer Mathematics*, pp. 133–148. Springer, 2011.

[40] Josef Urban, Jesse Alama, Piotr Rudnicki, and Herman Geuvers. A wiki for mizar: Motivation, considerations, and initial prototype. In *Intelligent Computer Mathematics*, pp. 455–469. Springer, 2010.

[41] Grzegorz Bancerek and Josef Urban. Integrated semantic browsing of the mizar mathematical library for authoring mizar articles. In *Mathematical Knowledge Management*, pp. 44–57.

Springer, 2004.

[42] Jesse Alama, Tom Heskes, Daniel Kühlwein, Evgeni Tsivtsivadze, and Josef Urban. Premise selection for mathematics by corpus analysis and kernel methods. *Journal of automated reasoning*, Vol. 52, No. 2, pp. 191–213, 2014.

[43] Josef Urban. Momm—fast interreduction and retrieval in large libraries of formalized mathematics. *International Journal on Artificial Intelligence Tools*, Vol. 15, No. 01, pp. 109–130, 2006.

[44] N. Bourbaki. *Theory of Sets (Ettore Majorana International Science)*. Springer, 1st ed. 1968. 2nd printing 2004 edition, 11 2004.

[45] 日本数学会（編）. 岩波数学辞典. 岩波書店, 第4, 3 2007.

[46] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, Vol. 4, No. 1, pp. 15–22, 1993.

[47] Beata Madras. Product of family of universal algebras. *Formalized Mathematics*, Vol. 4, No. 1, pp. 103–108, 1993.

[48] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, Vol. 1, No. 3, pp. 589–593, 1990.

[49] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, Vol. 1, No. **1**, pp. 153–164, 1990.

[50] 花木章秀. 群論, 2011. `http://math.shinshu-u.ac.jp/~hanaki/edu/group/group2011pre.pdf`.

[51] 遠山啓. 代数的構造. 筑摩書房, 2011.