氏名(本籍・生年月日)　中正 和久(大阪府　昭和５３年１１月７日)
学位の種類　博　士（工　学）
学位記番号　甲 第 ６５４ 号
学位授与の日付　平成２８年３月２０日
学位授与の要件　信州大学学位規程　第５条第１項該当
学位論文題目　Mizarによる群の直和分解の形式化
論文審査委員　主査　教　授　師玉康成　助教 山崎浩
教　授　和崎克己　助教 岡崎裕之
准教授 カワモトポーリン・ナオミ
准教授 宮島啓一（茨城大学）
准教授 アダムグラボフスキ(ビャウィストク大学)

論 文 内 容 の 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．