学位論文の審査結果の要旨

数学定理の証明を形式化言語で記述し，その論証の正しさを人手によらず計算機で機械的に厳密かつ迅速に検証できるシステムの重要性はロバート·ボイヤーらが提唱したQEDマニュフェストでも掲げられており，現在では複数のプロジェクトで形式化言語とシステムが開発され，その具現化に向けた研究が進行している．申請者はそれらの国際共同研究プロジェクトの一つである，定理証明支援系Mizarを用いた形式証明のライブラリの構築・編纂と処理システムの開発・改良の研究に従事している．本論文は，その一環として行なわれた，群の直和分解の形式化と，システムの改良研究に関する成果について報告している．

Mizarシステムは，主に一階述語論理に基づく定理証明支援系で，タルスキ・グロタンディーク集合論を公理系とするライブラリを構築している．形式記述の読み易さが非常に高いことが特徴であり，同様の定理証明支援系を用いたプロジェクトの中ではライブラリ編纂が最も進んでいるが，過去幾多の数学研究者の長年の努力によって得られてきた膨大な数の数学定理とその証明の全てを，計算機によって検証可能なように形式化記述言語で再記述し，その論証の正しさを単純な推論規則に還元して機械検証することは一朝一夕には実現できない．図式などを用いた視覚的イメージや直観に訴える従来の人間系による証明手法は使えず，多くの場合，計算機検証に向いた別証明を記述する必要が生ずる．申請者が参加するMizarプロジェクトも開始から40年を経過しているがまだその途上にある．処理システムも完全とは言えず，申請者が行っているように具体的な数学定理証明のライブラリ開発と処理システムの改良研究を並行して行う必要がある．今回，申請者が報告する成果は群の直和分解の形式化とその作成過程で行ったシステムの改良研究に関するものである．

申請者はデータ通信における計算機プログラムの検証のためのライブラリ構築を目指している．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ため，離散対数問題の形式化は重要な意味を持つ．また，ある群での離散対数問題はその直和分解に現われる部分群での離散対数問題に帰着されるため，群の直和分解の形式化が不可欠である．今回の群の直和分解の形式化が他の形式化数学ライブラリに比べて優位な点は，群の可換性および群の族の有限性を仮定していない点にある．申請者が形式化を行った非可換群，あるいは無限個の群に対する直和分解は，数学や理論物理に限っても様々な場面で自然に現われるため有用性が高い．しかしながら，非可換な無限個の群の族への直和分解を形式

化するには，非可換無限個の群要素の演算を可換有限個の場合に落とし込む必要があり，形式化証明は極めて複雑化する．本論文の成果はこれらの課題を解決した新規の成果である．

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の一つとして，ライブラリの検索・閲覧の問題がある．形式化ライブラリの大規模化に伴い，ライブラリの検索・閲覧は年を追う毎に困難になっている．形式化ライブラリの開発で最も時間が掛かる作業はライブラリから引用する定義・定理を検索することであり，検索性および閲覧性の向上は形式化における最大の課題の一つである．申請者は上記のライブラリ構築を進める中でこの課題に直面し，Mizar言語専用のドキュメンテーション生成器を開発した。論文では，ドキュメンテーション生成器の紹介とともに，開発経緯，既存のツールとの比較，今後の展望などを解説している．

以上，本論文は審査付き原著論文３編および審査付き国際会議発表論文１編に基づいてまとめられており，当講座の学位審査の目安を満足している．形式化数学記述言語システムとそれによる定理証明支援系の研究分野において，十分な新規性，有用性があり，本論文の成果は学位に値するものと認める．

公表主要論文名

論文発表（１）（レフェリー制のある学術雑誌）

(1) Kazuhisa Nakasho, Hiroyuki Okazaki, Hiroshi Yamazaki, Yasunari Shidama: Equivalent Expressions of Direct Sum Decomposition of Groups. Formalized Mathematics 23(1): 67-73 (2015)

(2) Kazuhisa Nakasho, Hiroshi Yamazaki, Hiroyuki Okazaki, Yasunari Shidama: Definition and Properties of Direct Sum Decomposition of Groups. Formalized Mathematics 23(1): 15-27 (2015)

(3) Hiroshi Yamazaki, Hiroyuki Okazaki, Kazuhisa Nakasho, Yasunari Shidama: Isomorphisms of Direct Products of Cyclic Groups of Prime Power Order. Formalized Mathematics 21(3): 207-211 (2013)

論文発表（２）（レフェリー制のある国際会議議事録）

(1) Kazuhisa Nakasho, Yasunari Shidama: Documentation Generator Focusing on Symbols for the HTML-ized Mizar Library. 8th Conferences on Intelligent Computer Mathematics (CICM 2015), LNAI 9150, 343-347, Proceedings (2015)