

研究タイトル：

# 代数曲線の退化の分裂



氏名：	荒川達也 / ARAKAWA Tatsuya	E-mail：	arakawa@ice.gunma-ct.ac.jp
職名：	准教授	学位：	博士(理学)
所属学会・協会：	日本数学会, 電子情報通信学会		

キーワード：代数曲線束, 退化族, 分裂族, 原子ファイバー, 2重被覆, モノドロミー, 一般型曲面

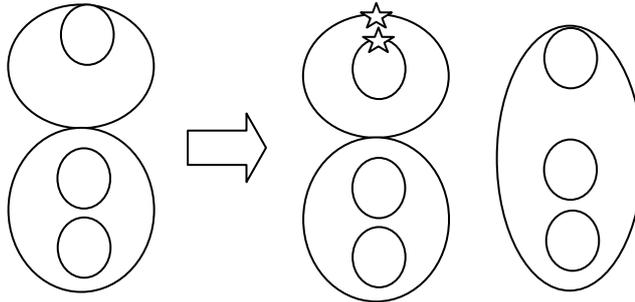
- 技術相談  
 提供可能技術：
- ・代数曲線の退化の分裂
  - ・原子ファイバーの分類
  - ・分裂族のモノドロミー

## 研究内容：代数曲線の退化族の分裂族の構成と解析

複雑な特異ファイバーを1本だけ含む代数曲線の退化に対し、複数の単純な特異ファイバーをもつ族への局所変形を一般に「退化の分裂」と呼ぶ。特に、それ以上分裂しない最も単純な特異ファイバーを「原子ファイバー」と呼び、その分類は「低次元代数幾何学」の中心テーマとひとつとされている。

筆者は足利正氏との共同研究により種数2および種数3超楕円曲線の退化族の分裂族の構成方法(=「解析的フィッシュン」)を導入し、原子ファイバーの候補のリストアップを行った。さらにその後、いくつかの不変量の分裂保存性を示すことにより、リスト中の退化たちが実際に分裂をもたないことを示した。

下に種数3超楕円曲線の退化の分裂の例を示す：



さらにその後「分裂族のモノドロミー」に着目し、特に超楕円的対合の分岐因子への作用(点の置換)に注目することにより分裂のモノドロミーを表現する方法を提案し、単純なケースにおいては置換モノドロミーのデータによって分裂後の特異ファイバーから分裂前の特異ファイバーを回復できることを示した。現在は本手法の有効性の検討と精密化および一般化の方法を模索している。

例えば上図の場合、星印で表示した点の置換によって「分裂のモノドロミー」を表示することができるが、しかしそれだけのデータでは分裂前(矢印の前)の特異ファイバーを再現することはできない。そこで点の置換よりも詳細な情報を表示する方法の導入が今後の課題と考えられる。

なお本研究の主要な対象である「超楕円曲線」は、現在暗号技術において実用化が進んでいる楕円曲線の一般化であり、楕円曲線暗号の一般化である「超楕円曲線暗号」の研究も盛んに行われている。本研究が扱う「超楕円曲線の退化」は将来的に、例えば暗号の脆弱性の検討などに応用される可能性が考えられる。

### 提供可能な設備・機器：

名称・型番(メーカー)	