計算機代数の基礎理論
長坂 耕作·岩根 秀直編著·北本 卓也·讃岐 勝·照井 章·鍋島 克輔著
https://www.kyoritsu-pub.co.jp/bookdetail/9784320113732

目 次

第 1 章　序章 **1**
1.1　計算機代数とは 1
1.1.1　計算機代数，計算代数，数式処理の謎 2
1.1.2　計算機代数は計算機だけの学問ではない 3
1.1.3　計算機代数の学術コミュニティ 3
1.2　数式処理システムと計算機代数 4
1.3　読み進め方と記法について 5
1.3.1　本書での基本的な記法 6
1.3.2　多項式の表記について 7
1.3.3　方程式の解について 7
1.3.4　アルゴリズムの記法について 7
第 2 章　アルゴリズムとその評価 **9**
2.1　発見的方法からアルゴリズムへ 9
2.2　計算量とアルゴリズムの評価 13
2.3　確率的アルゴリズムとミラー・ラビン素数判定法 26
2.4　多項式の加減乗除算と行列式の計算量 31
第 3 章　最大公約因子 **34**
3.1　最大公約元・最大公約因子 34
3.2　ユークリッドの互除法と剰余列 35
3.2.1　最大公約数と最大公約因子 36
3.2.2　ユークリッド整域における最大公約元 37
3.2.3　一意分解整域上の多項式環における最大公約因子 39
3.2.4　多項式剰余列と係数膨張 42
3.2.5　整数係数多項式の最大公約因子計算の実際 45
3.3　拡張ユークリッドの互除法 46
3.4　モジュラー法による効率化 49

計算機代数の基礎理論
長坂 耕作·岩根 秀直編著·北本 卓也·讃岐 勝·照井 章·鍋島 克輔著
https://www.kyoritsu-pub.co.jp/bookdetail/9784320113732

3.4.1 十分に大きな素数の見積もり 50
3.4.2 ヘンゼルの補題を用いる方法（ヘンゼル構成） 52
3.4.3 中国剰余定理 60
3.5 無平方分解 62
3.5.1 標数 0 の一意分解整域上の無平方分解 63
3.5.2 有限体上の無平方分解 66

第 4 章 終結式とその応用 69

4.1 はじめに 69
4.2 終結式と共通零点 70
4.2.1 多項式の行列による表現 70
4.2.2 シルベスター写像と最大公約因子 73
4.2.3 終結式とその性質 74
4.2.4 終結式の応用：単純拡大表現の導出 79
4.3 部分終結式と最大公約因子 82
4.3.1 部分終結式 82
4.3.2 部分終結式と共通因子 88
4.3.3 環準同型 92
4.3.4 部分終結式列の定理 97

第 5 章 有限体上の因数分解 103

5.1 有限体上の多項式 103
5.2 バールカンプアルゴリズム 104
5.2.1 バールカンプアルゴリズムの流れとその理論的背景 105
5.2.2 f-簡約多項式の存在性 107
5.2.3 f-簡約多項式の計算 108
5.2.4 f-簡約多項式を用いた既約因子の計算方法 112
5.2.5 バールカンプアルゴリズムの効率化 113
5.2.6 バールカンプアルゴリズムの実際 115
5.3 因子次数分離分解・同次因子分離分解と効率化 118
5.3.1 因子次数分離分解 (DDF) 119
5.3.2 同次因子分離分解 (EDF) の枠組み 121
5.3.3 奇標数の場合の分離多項式 122
5.3.4 偶標数の場合の分離多項式 123

5.3.5 同次因子分離分解のアルゴリズム 124

第 6 章 一意分解整域上の因数分解 128

6.1 ヘンゼル構成 128
6.1.1 3 つ以上の既約因子に対するヘンゼル構成 129
6.2 試し割りに基づくアルゴリズム 131
6.2.1 整数係数多項式の因数分解の流れ 131
6.2.2 多項式ノルムと因子係数上界 133
6.2.3 ザッセンバウスアルゴリズム 134
6.2.4 偽因子の検出と効率化 137
6.2.5 整数係数多項式の因数分解の実際 140
6.3 多項式時間アルゴリズムと効率化 143
6.3.1 因数分解と多項式時間アルゴリズム 143
6.3.2 整数格子と最短ベクトル 144
6.3.3 L^3 アルゴリズム 150
6.3.4 ナップザックアルゴリズム 154
6.3.5 多項式時間アルゴリズムの実際 162

第 7 章 代数方程式の根とその計算法 167

7.1 実根と符号変化の数 167
7.2 スツルム列による実根の数え上げ 170
7.3 スツルム・ハビッチ列による実根の数え上げ 173
7.4 ブダン・フーリエの定理とデカルトの符号律 180

第 8 章 計算機代数の世界 184

8.1 基本演算 184
8.1.1 多項式の評価 184
8.1.2 多項式の乗算 185
8.1.3 行列の乗算 186
8.1.4 連立線形方程式 187
8.2 多変数多項式や拡大体への拡張 188
8.2.1 多変数多項式の最大公約因子 188
8.2.2 多変数多項式の因数分解 189
8.2.3 代数拡大体上の因数分解 191
8.3 グレブナー基底とその周辺 192

8.3.1 グレブナー基底 . . . 192
8.3.2 包括的グレブナー基底系 . . . 194
8.4 実閉体上の限量子消去 . . . 195
8.4.1 限量子消去の概要 . . . 195
8.4.2 Cylindrical Algebraic Decomposition . . . 196
8.4.3 限量子消去の応用 . . . 198
8.5 数値・数式融合計算 . . . 199
8.5.1 近似 GCD . . . 200
8.5.2 近似因数分解 . . . 202
8.5.3 安定化理論 . . . 203
8.6 無限級数・冪級数演算とその応用例 . . . 204
8.6.1 超幾何級数の和 . . . 204
8.6.2 超幾何級数とその漸化式 . . . 205
8.6.3 打ち切り冪級数 . . . 207

付 録 代数の基礎 210

A.1 群・環・体について . . . 210
A.1.1 基本的な予備知識の確認 . . . 210
A.1.2 群・環・体の定義といくつかの性質 . . . 211
A.2 剰余環と有限体について . . . 213
A.2.1 イデアルとその性質 . . . 214
A.2.2 イデアルによる剰余類と剰余環 . . . 214
A.2.3 準同型写像と準同型定理 . . . 215
A.2.4 直積と直和 . . . 216
A.2.5 有限体と商体 . . . 218
A.3 多項式環とその性質 . . . 219
A.3.1 多項式環の性質 . . . 220
A.3.2 ガウスの補題と多項式の既約性 . . . 222
A.3.3 代数的拡大と超越的拡大 . . . 222

参考文献 225

索 引 234