

《 ガロア理論の頂を踏む いただき ◎ 目次 》

はじめに 3

第1章 「整数」

- 1** 最大公約数を求める 24
 ▶ ユークリッドの互除法
 定理 1.1 互除法の原理 26
 定理 1.2 1 次不定方程式 30
 定理 1.3 1 次不定方程式 31
- 2** 余りの計算 33
 ▶ 剰余類
 定義 1.1 合同式 34
 定義 1.2 合同式 34
 定理 1.4 合同式の性質 35
- 3** 正六角形を回転させよう 38
 ▶ 巡回群
 定義 1.3 群の定義 41
- 4** 群が同じということ 44
 ▶ 群の同型
 定義 1.4 群の同型 45
- 5** 一部の元でも群になる 50
 ▶ 部分群
 定理 1.5 巡回群の部分群 51
- 6** 2つの群から群を作る 53
 ▶ 群の直積
 定義 1.5 群の直積 54
 定理 1.6 中国剰余定理 58
 定理 1.7 中国剰余定理：3 数 61
 定理 1.8 $\mathbb{Z}/n\mathbb{Z}$ の分解 62

- 7** 掛け算だって群になる！ 64
 ▶ 既約剰余類群
 定義 1.6 既約剰余類群 66
- 8** $(\mathbb{Z}/p\mathbb{Z})^*$ は直積で書けるか？ 68
 ▶ 既約剰余類群の構造分析
 定理 1.9 既約剰余類の分解 70
 定義 1.7 オイラー関数 71
 定理 1.10 既約剰余類の元の個数 72
- 9** $(\mathbb{Z}/p\mathbb{Z})^*$ は、巡回群である 73
 ▶ 原始根で生成
 定理 1.11 F_p 上の 1 次方程式 76
 定理 1.12 F_p 上での剰余の定理 78
 定理 1.13 F_p 上での因数定理 78
 定理 1.14 F_p 上の方程式の解の個数 78
- 10** 素数 p の原始根は確かにある 80
 ▶ 原始根の存在証明
 定理 1.15 a が生成する巡回群 80
 定理 1.16 原始根の存在 81
 定理 1.17 $(\mathbb{Z}/p\mathbb{Z})^*$ は巡回群 85
- 11** 既約剰余類群を解剖する 87
 ▶ $(\mathbb{Z}/p^n\mathbb{Z})^*$ の構造
 定理 1.18 $(\mathbb{Z}/2^n\mathbb{Z})^*$ の構造 88
 定理 1.19 $(\mathbb{Z}/p^n\mathbb{Z})^*$ の構造 92
 定理 1.20 既約剰余類群の構造 96

第2章 「群」

- 1** 正三角形の対称性を調べる 98
 ▶ 二面体群
 定理 2.1 g による入れ替え 101
 定理 2.2 g が部分集合に作用 102
 定義 2.1 二面体群 103

2	部分群から剰余群を作る	104
	▶一般の剰余群	
	(定理 2.3) 剰余類	110
	(定理 2.4) ラグランジュの定理	112
	(定理 2.5) 位数乗は単位元	114
	(定理 2.6) フェルマーの小定理, オイラーの定理	115
	(定理 2.7) 剰余類の単位元	115
3	立方体の対称性を調べよう	116
	▶ $S(P_6)$	
	(定理 2.8) 剰余群	126
	(定理 2.9) 巡回群の剰余群は巡回群	132
	(定理 2.10) 半分の部分群は正規部分群	134
4	同型写像じゃなくたって	135
	▶準同型写像	
	(定義 2.2) 群の準同型写像	135
	(定理 2.11) $\text{Im} f$ は群	138
	(定理 2.12) $\text{Ker} f$ は群	139
	(定理 2.13) 準同型定理	140
5	同型を作ろう	144
	▶第2同型定理, 第3同型定理	
	(定理 2.14) 部分群であるための条件	145
	(定理 2.15) 部分群の演算	146
	(定理 2.16) 第2同型定理	147
	(定理 2.17) 第3同型定理	150
6	あみだくじのなす群	153
	▶対称群 S_n	
	(定理 2.18) 置換は互換の積	164
	(定理 2.19) 対称群の生成元	166
	(定理 2.20) 置換の奇偶性	167
	(定理 2.21) 交代群	171
	(定理 2.22) 交代群と対称群	171
	(定理 2.23) 交代群は三換の積	172
	(定理 2.24) 交代群の生成元	173

7	巡回群の入れ子構造	175
	▶可解群	
	(定義 2.3) 可解群	178
	(定理 2.25) 巡回群の直積は可解群	179
	(定理 2.26) 交代群の非可解性	180
	(定理 2.27) 可解群の部分群も可解群	181
	(定理 2.28) 対称群の非可解性	183
	(定理 2.29) 準同型写像の像でも可解群	183
	(定理 2.30) 剰余群も可解群	184

第3章 「多項式」

1	基本対称式で表そう	192
	▶対称式	
	(定理 3.1) 対称式の基本定理	195
2	多項式における素数	199
	▶既約多項式	
	(定理 3.2) F_p 上の多項式は整域	201
	(定理 3.3) 有理数係数多項式の既約性, この対偶	202
	(定理 3.4) Eisenstein の判定条件	204
3	整数と多項式のアナロジー	207
	▶多項式の合同式	
	(定理 3.5) 多項式の1次不定方程式	211
	(定理 3.6) 既約多項式の性質	213
4	既約多項式で割っても体	216
	▶ $Q[x]/(f(x))$	
	(定理 3.7) 既約多項式による体	221

	定義 5.6	次元	318
	定理 5.16	線形空間の一致	319
5	方程式の解を含む体	320	
	▶ 最小分解体 $Q(\alpha_1, \alpha_2, \dots, \alpha_n)$		
	定義 5.7	最小分解体	320
	定理 5.17	同型写像が自己同型写像になる条件	326
	定理 5.18	自己同型写像の積も自己同型写像	329
	定理 5.19	自己同型群	330
6	4 次方程式の例	333	
	▶ 中間体		
7	2 段拡大	339	
	▶ $Q(\alpha, \beta)$		
	定理 5.20	次元の積公式	348
	定理 5.21	同型写像の延長	355
	定理 5.22	$Q(\alpha, \beta)$ に作用する同型写像	358
8	固定群と固定体が対応してる！	360	
	▶ ガロア対応		
	定理 5.23	固定体	364
	定理 5.24	固定群	365
9	拡大体はすべて単拡大体	366	
	▶ $Q(\alpha_1, \dots, \alpha_n) = Q(\theta)$		
	定理 5.25	原始元の存在	374
	定理 5.26	代数的拡大体は単拡大体	375
	定理 5.27	最小分解体は単体拡大	376
10	同型写像ではみ出ない	377	
	▶ ガロア拡大体		
	定理 5.28	(最小分解体の次数) = (ガロア群の位数)	377
	定義 5.8	ガロア拡大	380
	定理 5.29	$Q(\alpha)$ がガロア拡大体になる条件	381
11	2 段拡大理論で証明しよう	383	
	▶ ガロア対応の証明		
	定理 5.30	最小分解体の正規性	384
	定理 5.31	M のガロア群	387

定理 5.32	次数公式	391
定理 5.33	ガロア対応 M から始めて	394
定理 5.34	ガロア対応 H から	396

12	M/Q はガロア拡大か？.....	398
	▶ 中間体がガロア拡大体になる条件	
	定理 5.35 $\sigma(M)$ と $\sigma H \sigma^{-1}$ の対応.....	405
	定理 5.36 中間体がガロア拡大体になる条件	406

第 6 章 「根号で表す」

1	1 の n 乗根をベキ根で表す	412
	▶ 円分方程式の可解性	
	定理 6.1 1 の n 乗根のベキ根表現	416
2	3 次方程式をベキ根で解く	422
	▶ 3 次方程式の解の公式	
3	3 次方程式のガロア対応を調べよう	427
	▶ ベキ根拡大	
4	4 次方程式をベキ根で解こう	437
	▶ 4 次方程式の解の公式	
5	4 次方程式のガロア対応を調べよう	441
	▶ 累巡回拡大体	
	定理 6.2 可解群と累巡回拡大の対応	447
6	1 のベキ根の作る体	453
	▶ 円分体とガロア群	
	定理 6.3 円分体のガロア群	457
7	$x^n - a = 0$ の作る拡大体	463
	▶ クンマー拡大	
	定理 6.4 ベキ根拡大から巡回拡大を作る	467
8	巡回拡大は $x^n - a = 0$ で作れる	472
	▶ 巡回拡大からベキ根拡大へ	
	定理 6.5 巡回拡大からベキ根拡大を作る	473
	定理 6.6 デデキントの補題	476

定理 6.7 ベキ根拡大を作るベキ根の存在 478

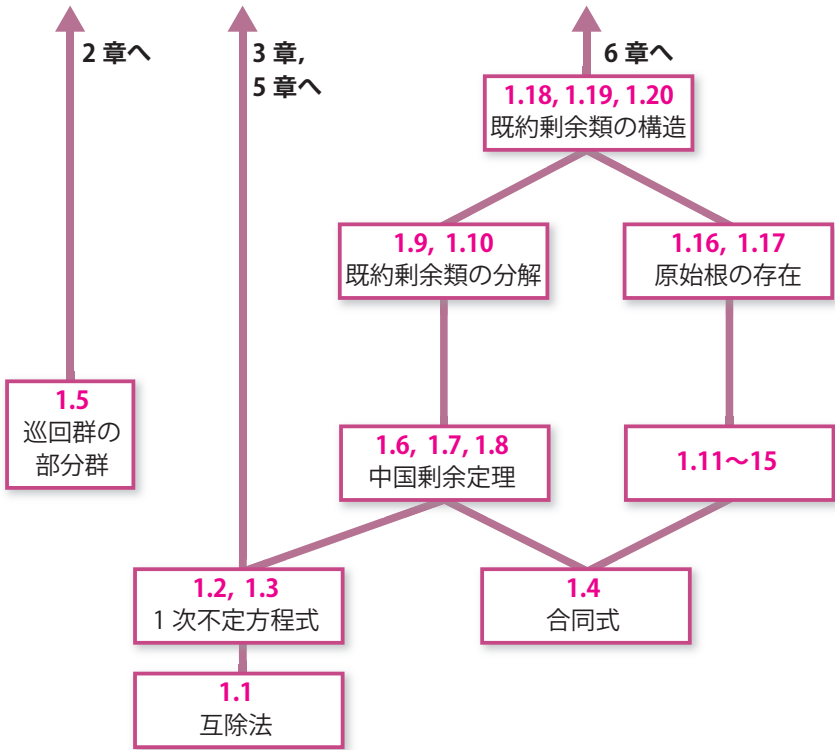
9 ピークの定理に立とう！ 480
 ▶ベキ根で解ける方程式の条件
 ピークの定理 480
 定理 6.8 可解群のとき解はベキ根で表される 480
 定理 6.9 累ベキ根拡大体のガロア閉包 481
 定理 6.10 解がベキ根で表されるときは可解群 486

10 5次方程式の解の公式はない 488
 ▶ガロア群が可解群でない方程式
 定理 6.11 位数 p の元の存在—コーシーの定理 488

おわりに 496

索 引 502

第 1 章 「整数」



この章の目標は、既約剰余類の構造（定理 1.20）を理解することです。そこに至るまで、互除法、不定方程式、中国剰余定理などを積み上げていきます。定理 1.1 から定理 1.20 に至るまでの道順を意識してください。定理 1.11 から定理 1.15 までは原始根の存在（定理 1.16）を示すために用意した定理です。

また、定理 1.18、定理 1.19 では、パラレルな議論が展開されます。初めは片方だけでも十分かもしれません。

互除法、不定方程式は、第 3 章、第 5 章でも当たり前のように使います。十分に理解しておきましょう。

この章では、すでに群の定義が出てきます。整数の剰余類を通して群に慣れてください。