

はじめに

## 第1章 「整数」

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

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

## 第2章 「群」

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

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

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

### 第3章 「多項式」

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

## 第4章 「複素数」

- 1 2次方程式から複素数が出てくる ..... 224
- ▶ 複素数
- 定理** 代数学の基本定理 ..... 224
- 定理4.1** 共役複素数の計算法則 ..... 228
- 定理4.2** 共役と組み合わせると実数 ..... 228
- 定理4.3** 共役複素数はまた解 ..... 230
- 2 複素数が活躍する舞台 ..... 231
- ▶ 複素平面
- 定理4.4** 複素数の積における絶対値と偏角 ..... 234
- 定理4.5** 複素数の商における絶対値と偏角 ..... 235
- 定理4.6** 複素数の $n$ 乗 ..... 237
- 3 円を $n$ 等分する点 ..... 238
- ▶ 1の $n$ 乗根
- 定理4.7** 1の $n$ 乗根 ..... 239
- 定理4.8** 複素数の $n$ 乗根 ..... 241
- 定理4.9** 1の原始 $n$ 乗根 ..... 244
- 4 1の原始 $n$ 乗根を解に持つ方程式 ..... 245
- ▶ 円分多項式
- 定義4.1** 円分多項式 ..... 245
- 定理4.10** 素数次の円分多項式 ..... 246
- 定理4.11** 1の $n$ 乗根の和の公式 ..... 247
- 5  $n$ 次方程式には必ず解がある ..... 252
- ▶ 代数学の基本定理
- 定理4.12** 代数学の基本定理 ..... 253
- 定理4.13** 複素数係数2次方程式の解の存在 ..... 253
- 定理4.14** 実数係数多項式の解の存在 ..... 254
- 定理4.15** 複素数係数方程式の解の存在 ..... 257
- 定理4.16** 代数学の基本定理：因数分解バージョン ..... 259
- 6  $n$ が合成数でも円分多項式は既約 ..... 266
- ▶  $\phi(x)$ の既約性の証明
- 定理4.17**  $\text{mod } p$ での $p$ 乗 ..... 266

- 定理4.18** 解から解を作る ..... 266
- 定理4.19** 円分多項式の既約性 ..... 269

## 第5章 「体と自己同型写像」

- 1 無理数の計算を簡単にしよう ..... 272
- ▶  $Q(\sqrt{3})$ の対称性
- 定義5.1** 体の定義 ..... 273
- 定義5.2** 体の同型写像 ..... 280
- 定理5.1** 有理数は同型写像で不変 ..... 282
- 2 この計算どこかで見たぞ ..... 284
- ▶  $Q[x]/(f(x)) \cong Q(\alpha)$
- 定理5.2** 最小多項式と既約多項式 ..... 287
- 定理5.3** 単拡大体 $Q(\alpha)$ の元の表現の一意性 ..... 288
- 定理5.4** 多項式の剰余類群と単拡大体 ..... 291
- 3 同型は $n$ 個 ..... 292
- ▶  $Q(\alpha_1) \cong Q(\alpha_2) \cong \dots \cong Q(\alpha_n)$
- 定理5.5**  $f(x)$ が引き起こす同型 ..... 292
- 定理5.6** 同型写像と有理関数は順序交換可能 ..... 296
- 定理5.7** 同型写像は解を共役な解に移す ..... 296
- 定理5.8** 同型写像は解の置換を引き起こす  
        : 解のシャッフル ..... 297
- 定理5.9**  $Q(\alpha_i)$ の同型 ..... 299
- 定理5.10**  $Q(\alpha)$ に作用する同型写像は $n$ 個 ..... 301
- 4 体の次元を捉えよう ..... 305
- ▶ 線形代数の補足
- 定義5.3** 線形空間 ..... 306
- 定義5.4** 1次独立・1次従属の定義 ..... 308
- 定理5.11** 1次独立・1次従属 ..... 309
- 定義5.5** 基底の定義 ..... 310
- 定理5.12** 表現の一意性 ..... 311
- 定理5.13** 基底の完全性 ..... 311
- 定理5.14**  $Q(\alpha)$ の基底 ..... 313
- 定理5.15** 線形空間の次元 ..... 316

	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