

まえがき

人類はまず数を I, II, III のように数字で表す記数法を生み出した。そして、未知数に文字を割り当て、満たすべき条件を方程式として書き表し、記号操作等で解を求めることを考えるようになった。方程式は古代から用いられてきた問題解決の手法であり、代数学の源流の一つである。特に有名な問題として、一般に代数方程式の係数から解を求める「解の公式」が存在するか、というものがある。この問題は、長い歴史を経て 19 世紀に解決されたが、その過程で「体」や「群」といった代数系の概念が抽出され、抽象代数学の発展が促された。そこで本書でも、方程式を話題の中心に据えて、解の公式はもちろんとし、広く代数に関わる内容を扱うことにした。

方程式の話題は代数の範囲で完結するものではない。まず、ガロア (Galois) 理論により、解の公式が存在するかどうかは解の対称性によって判定されるように、方程式は幾何とも深い関わりがある。円や放物線のように、代数方程式の解の全体は単なる集合ではなく代数多様体と呼ばれる図形になり、幾何の対象になる。図形の幾何的性質はその上の関数のなす環の代数的性質と対応させて調べることができる。次に、代数学は本来、問題を有限回の具体的な手続きで解く方法を与えるという、計算的側面をもつ。近代の抽象代数学で現れた、いつ終わるかはわからないが存在する、という論法は、数学ではない、神学だ、と言われたという伝説があるほどである。古典的なアルゴリズムとして、最大公約数を求めるユークリッド (Euclid) の互除法や、連立 1 次方程式を簡約化する掃き出し法 (消去法) が基本的である。現代では高次の連立方程式の簡約化としてグレブナー (Gröbner) 基底の理論もある。この計算的側面は、近年の計算機の発展に伴いますます重要になっている。さらに、線形方程式・不等式と応用数学との関わりも重要であり、純粋数学だけを学んでは気付かない興味深い話題がある。これら代数を越えたところに広がる様々な風景をも、楽しみながら訪ねて行けたらと思うのである。

各章では、まず高校数学程度で意味が理解できる例題を提示し、その解法を通じて、代数学の様々な要点を取り上げていく。具体的な問題を解くときには、さまざまな代数構造が混ざって出てくるので、講義のように系統だてて「線形代数」「群論」「環論」「体論」と順を追って述べることはしない。それぞれの問題に即して接することで、生きた題材の全体に触れ、同時に、問題を解く力もつけられればと思う。予備知識は高校数学 + a (行列の基礎程度) しか基本的には仮定していないが、興味をもたれた部分や省略してある部分 (ほとんどは標準的な代数学のテキストに載っている) は必要に応じて補っていただければと思う。

もし本書を通じて読者に代数を用いる面白さを少しでも感じていただくことができたなら、そしてさらに先の世界へと勉強を続けていただけたら、本当にありがたい、というのが筆者の思いである。

本書は、雑誌『数理科学』に 2 年余りにわたり連載した内容を一冊にまとめたものである。毎回毎回なかなか原稿が完成しない筆者を辛抱強く見守ってくださった大溝良平氏、一冊にまとめるにあたり編集を担当してくださった平勢耕介氏のサイエンス社のお二人を始め、支えてくださった皆様に心から感謝いたします。

2017 年 6 月

小林 正典

目次

第 1 章	方程式の複素数解	1
1.1	方程式を「解く」とは	1
1.2	除法の原理	2
1.3	複素数	3
1.3.1	実数の組としての複素数	3
1.3.2	平面の点としての複素数	4
1.4	解の公式	5
1.5	例題 1.1 の解答	6
1.6	補足	8
1.6.1	連立 1 次方程式を解くということ	8
1.6.2	倍角公式	9
1.6.3	代数的数	9
1.6.4	文献	9
第 2 章	分母の有理化	10
2.1	第 2 章の問題	10
2.2	因数分解の公式の利用	10
2.3	最大公約元とユークリッドの互除法	12
2.4	最小多項式	14
2.5	代数的数の有理式	16
2.6	代数的数と拡大次数	17
第 3 章	2 つの剰余定理	20
3.1	第 3 章の問題	20
3.2	連立 1 次方程式による解法	20
3.3	剰余定理による言い換え	21
3.4	整数の除法	22
3.5	整数の合同	23
3.6	環とイデアル	23
3.7	互いに素	24
3.8	中国剰余定理	25
3.9	ラグランジュの補間公式	26

3.10	多変数への拡張	28
第4章	因数分解	30
4.1	第4章の問題	30
4.2	実数・複素数係数の因数分解	30
4.3	整数係数の因数分解	31
4.3.1	未定係数法	31
4.3.2	p を法とする還元	32
4.4	分解の存在と一意性	33
4.4.1	既約分解の存在	33
4.4.2	一意分解整域	34
4.4.3	UFD の例	35
4.5	アイゼンシュタインの既約性判定法	36
4.6	有理数係数の因数分解	37
第5章	共役元とノルム	39
5.1	第5章の問題	39
5.2	共役元	40
5.3	2次体の場合	42
5.4	基底と表現行列	42
5.5	行列式	43
5.6	掛け算写像	45
第6章	解と係数の関係	48
6.1	第6章の問題	48
6.2	解と係数の関係	48
6.3	基本対称式	49
6.4	べき和	50
6.5	単項対称式	51
6.6	辞書式順序・先頭項	52
6.7	基本定理の証明	53
6.8	対称群	53
6.9	例題の解答	55
6.10	多項式の根の存在	56
第7章	判別式	57
7.1	第7章の問題	57
7.2	判別式と差積	58

7.3	終結式	59
7.4	交代式	60
7.5	交代群	62
7.6	対合	63
7.7	結論と例題の解答	65
第 8 章	二重根号	66
8.1	二重根号	66
8.2	複二次式	67
8.3	2次拡大	68
8.4	体の自己同型	69
8.5	アルティンの定理	71
8.6	例題の解答と結論	73
第 9 章	1 のべき根	75
9.1	第 9 章の問題	75
9.2	巡回群	76
9.3	有限生成アーベル群の基本定理	78
9.4	乗法群	79
9.5	例題の解答	81
9.6	1 のべき根	82
第 10 章	軌道分解	84
10.1	第 10 章の問題	84
10.2	群作用	84
10.3	ラグランジュの定理, 共役元	86
10.4	軌道・固定群定理	86
10.5	巡回置換分解	88
10.6	類等式	89
10.7	シルベスターの公式	91
10.8	例題の解答	92
第 11 章	自己同型群	93
11.1	第 11 章の問題	93
11.2	運動群	93
11.3	有限体上の線形変換群	94
11.4	内部自己同型群	96
11.5	交換子群	97

11.6	位数の小さい群	98
11.7	例題の解答	100
第 12 章	ガロアの基本定理	102
12.1	第 12 章の問題	102
12.2	分離拡大	103
12.3	ガロアの基本定理	105
12.4	例題の解答	106
12.5	円分拡大のガロア群	109
第 13 章	解の公式	111
13.1	解の公式	111
13.2	第 13 章の問題	112
13.3	べき根拡大と巡回拡大	113
13.4	可解群	114
13.5	方程式のガロア群	116
13.6	アルティン・シュライヤー拡大	118
第 14 章	軌跡	120
14.1	第 14 章の問題	120
14.2	軌跡	121
14.3	包絡線	122
14.4	定義イデアルと共通零点集合	124
14.5	ヒルベルトの基底定理・グレブナー基底と消去法	125
14.6	例題の解答	127
第 15 章	連立 1 次方程式	129
15.1	第 15 章の問題	129
15.2	掃き出し法	129
15.3	R 加群	130
15.4	R 加群の準同型	133
15.5	単因子論	134
15.6	例題の解答	136
15.7	「不自由」な場合	137
第 16 章	連立 1 次不等式	138
16.1	第 16 章の問題	138
16.2	不等式の標準形	138

16.3	不等式の消去法	140
16.4	構造定理 1	141
16.5	構造定理 2	143
16.6	ファルカシュの補題	144
16.7	線形計画法の双対定理	145
16.8	例題の解答	146
第 17 章	図形と式	148
17.1	鶏が先か卵が先か	148
17.2	双対	148
17.3	双対基底	150
17.4	零化空間	151
17.5	ヒルベルトの零点定理	153
17.6	座標環	155
第 18 章	$1 + 1 = 1$	157
18.1	工程計画問題	157
18.2	トロピカル代数	157
18.3	トロピカル化	158
18.4	p 進数	160
18.5	付値	161
18.6	付値の同値類	163
第 19 章	グラフ	166
19.1	第 19 章の問題	166
19.2	グラフと行列	166
19.3	マルコフ過程	168
19.4	ペロン・フロベニウスの定理	169
19.5	例題の解答	171
19.6	ADE	172
	参考文献	175
	索引	176