Polynomials afg

From Wikipedia, the free encyclopedia

Contents

1 Abel polynomials **1**

1.1 Examples . . . 1

1.2 References . . . 1

1.3 External links . . . 2

2 Abel–Ruffini theorem **3**

2.1 Interpretation . . . 3

2.2 Lower-degree polynomials . . . 3

2.3 Quintics and higher . . . 4

2.4 Proof . . . 4

2.5 History . . . 5

2.6 See also . . . 6

2.7 Notes . . . 6

2.8 References . . . 6

2.9 Further reading . . . 6

2.10 External links . . . 6

3 Actuarial polynomials **7**

3.1 See also . . . 7

3.2 References . . . 7

4 Additive polynomial **8**

4.1 Definition . . . 8

4.2 Examples . . . 8

4.3 The ring of additive polynomials . . . 9

4.4 The fundamental theorem of additive polynomials . . . 9

4.5 See also . . . 9

4.6 References . . . 9

4.7 External links . . . 9

5 Alexander polynomial **10**

5.1 Definition . . . 10

5.2 Computing the polynomial . . . 10

5.3 Basic properties of the polynomial . . . 11

5.4 Geometric significance of the polynomial . . . 11
5.5 Relations to satellite operations . . . 12
5.6 Alexander–Conway polynomial . . . 12
5.7 Relation to Khovanov homology . . . 13
5.8 Notes . . . 13
5.9 References . . . 13
5.10 External links . . . 13

6 Algebraic equation **14**
6.1 History . . . 14
6.2 Areas of study . . . 15
6.3 See also . . . 15
6.4 References . . . 16

7 Algebraic variety **17**
7.1 Introduction and definitions . . . 18
7.1.1 Affine varieties . . . 18
7.1.2 Projective varieties and quasi-projective varieties . . . 19
7.1.3 Abstract varieties . . . 19
7.2 Examples . . . 19
7.2.1 Subvariety . . . 20
7.2.2 Affine variety . . . 20
7.2.3 Projective variety . . . 21
7.3 Basic results . . . 22
7.4 Isomorphism of algebraic varieties . . . 22
7.5 Discussion and generalizations . . . 22
7.6 Algebraic manifolds . . . 23
7.7 See also . . . 23
7.8 Footnotes . . . 24
7.9 References . . . 24

8 All one polynomial **25**
8.1 Definition . . . 25
8.2 Properties . . . 25
8.3 References . . . 26
8.4 External links . . . 26

9 Almost linear hash function **27**
9.1 References . . . 28

10 Alternating polynomial **29**
10.1 Relation to symmetric polynomials . . . 29
10.2 Vandermonde polynomial . . . 29

10.2.1 Ring structure . . . 30
10.3 Representation theory . . . 30
10.4 Unstable . . . 31
10.5 See also . . . 31
10.6 Notes . . . 31
10.7 References . . . 31

11 Angelescu polynomials **32**
11.1 See also . . . 32
11.2 References . . . 32

12 Appell sequence **33**
12.1 Equivalent characterizations of Appell sequences . . . 33
12.2 Recursion formula . . . 34
12.3 Subgroup of the Sheffer polynomials . . . 34
12.4 Different convention . . . 35
12.5 See also . . . 35
12.6 References . . . 35
12.7 External links . . . 36

13 Bell polynomials **37**
13.1 Complete Bell polynomials . . . 37
13.2 Combinatorial meaning . . . 38
13.2.1 Examples . . . 38
13.3 Properties . . . 38
13.3.1 Stirling numbers and Bell numbers . . . 39
13.3.2 Touchard polynomials . . . 39
13.3.3 Convolution identity . . . 39
13.4 Applications of Bell polynomials . . . 40
13.4.1 Faà di Bruno's formula . . . 40
13.4.2 Moments and cumulants . . . 40
13.4.3 Representation of polynomial sequences of binomial type . . . 40
13.5 Software . . . 41
13.6 See also . . . 41
13.7 References . . . 41

14 Bernoulli polynomials **43**
14.1 Representations . . . 44
14.1.1 Explicit formula . . . 44
14.1.2 Generating functions . . . 44
14.1.3 Representation by a differential operator . . . 44
14.1.4 Representation by an integral operator . . . 44
14.2 Another explicit formula . . . 45

14.3 Sums of *p*th powers . . . 46
14.4 The Bernoulli and Euler numbers . . . 46
14.5 Explicit expressions for low degrees . . . 46
14.6 Maximum and minimum . . . 47
14.7 Differences and derivatives . . . 47
14.7.1 Translations . . . 48
14.7.2 Symmetries . . . 48
14.8 Fourier series . . . 48
14.9 Inversion . . . 49
14.10 Relation to falling factorial . . . 50
14.11 Multiplication theorems . . . 50
14.12 Integrals . . . 50
14.13 Periodic Bernoulli polynomials . . . 51
14.14 See also . . . 51
14.15 References . . . 51

15 Bernstein polynomial **53**
15.1 Definition . . . 54
15.2 Example . . . 54
15.3 Properties . . . 54
15.4 Approximating continuous functions . . . 55
15.4.1 Proof . . . 56
15.5 See also . . . 56
15.6 Notes . . . 57
15.7 References . . . 57
15.8 External links . . . 57

16 Bernstein–Sato polynomial **58**
16.1 Definition and properties . . . 58
16.2 Examples . . . 58
16.3 Applications . . . 59
16.4 References . . . 60

17 Binomial **61**
17.1 Definition . . . 61
17.2 Operations on simple binomials . . . 61
17.3 See also . . . 62
17.4 Notes . . . 62
17.5 References . . . 62

18 Boas–Buck polynomials **63**
18.1 References . . . 63

19 Bollobás–Riordan polynomial **64**
19.1 History . . . 64
19.2 Formal definition . . . 64
19.3 See also . . . 64
19.4 References . . . 64

20 Bombieri norm **66**
20.1 Bombieri scalar product for homogeneous polynomials . . . 66
20.2 Bombieri inequality . . . 67
20.3 Invariance by isometry . . . 67
20.4 Other inequalities . . . 67
20.5 See also . . . 67
20.6 References . . . 68

21 Boole polynomials **69**
21.1 See also . . . 69
21.2 References . . . 69

22 Bracket polynomial **70**
22.1 Definition . . . 70
22.2 Further reading . . . 70
22.3 External links . . . 70

23 Bring radical **71**
23.1 Normal forms . . . 71
23.1.1 Principal quintic form . . . 71
23.1.2 Bring–Jerrard normal form . . . 72
23.1.3 Brioschi normal form . . . 72
23.2 Series representation . . . 73
23.3 Solution of the general quintic . . . 73
23.4 Other characterizations . . . 74
23.4.1 The Hermite–Kronecker–Brioschi characterization . . . 74
23.4.2 Glasser's derivation . . . 76
23.4.3 The method of differential resolvents . . . 78
23.4.4 Doyle–McMullen iteration . . . 79
23.5 See also . . . 80
23.6 Notes . . . 80
23.7 References . . . 81
23.8 External links . . . 81

24 Bézout matrix **82**
24.1 Definition . . . 82
24.2 Examples . . . 82

24.3 Properties . . . 83
24.4 Applications . . . 83
24.5 References . . . 83

25 Caloric polynomial **85**
25.1 References . . . 85
25.2 External links . . . 85

26 Casus irreducibilis **86**
26.1 Formal statement and proof . . . 86
26.2 Solution in non-real radicals . . . 87
26.3 Non-algebraic solution in terms of real quantities . . . 87
26.4 Relation to angle trisection . . . 87
26.5 Generalization . . . 88
26.6 Notes . . . 88
26.7 References . . . 88
26.8 External links . . . 88

27 Cavalieri's quadrature formula **89**
27.1 Forms . . . 90
27.1.1 Negative n . . . 90
27.1.2 $n = -1$ . . . 90
27.1.3 Alternative forms . . . 91
27.2 Proof . . . 91
27.3 History . . . 92
27.4 References . . . 92
27.4.1 History . . . 93
27.4.2 Proofs . . . 93
27.5 External links . . . 93

28 Characteristic polynomial **96**
28.1 Motivation . . . 96
28.2 Formal definition . . . 96
28.3 Examples . . . 97
28.4 Properties . . . 97
28.5 Characteristic polynomial of a product of two matrices . . . 98
28.6 Secular function and secular equation . . . 98
28.6.1 Secular function . . . 99
28.6.2 Secular equation . . . 99
28.7 See also . . . 99
28.8 References . . . 99
28.9 External links . . . 99

29 Coefficient **100**
29.1 Linear algebra . . . 100
29.2 Examples of physical coefficients . . . 101
29.3 See also . . . 101
29.4 References . . . 101

30 Coefficient diagram method **102**
30.1 See also . . . 103
30.2 References . . . 103
30.3 External links . . . 103

31 Complex conjugate root theorem **104**
31.1 Examples and consequences . . . 104
31.1.1 Corollary on odd-degree polynomials . . . 104
31.2 Simple proof . . . 105
31.3 Notes . . . 106

32 Complex quadratic polynomial **107**
32.1 Forms . . . 107
32.2 Conjugation . . . 107
32.2.1 Between forms . . . 107
32.2.2 With doubling map . . . 108
32.3 Family . . . 108
32.4 Map . . . 108
32.5 Notation . . . 108
32.6 Critical items . . . 109
32.6.1 Critical point . . . 109
32.6.2 Critical value . . . 109
32.6.3 Critical orbit . . . 109
32.6.4 Critical sector . . . 110
32.6.5 Critical polynomial . . . 110
32.6.6 Critical curves . . . 111
32.7 Planes . . . 111
32.7.1 Parameter plane . . . 112
32.7.2 Dynamical plane . . . 113
32.8 Derivatives . . . 114
32.8.1 Derivative with respect to c . . . 114
32.8.2 Derivative with respect to z . . . 115
32.8.3 Schwarzian derivative . . . 115
32.9 See also . . . 116
32.10 References . . . 116
32.11 External links . . . 117

33 Constant function **118**
33.1 Basic properties . . . 118
33.2 Other properties . . . 118
33.3 References . . . 120
33.4 External links . . . 120

34 Constant term **121**
34.1 See also . . . 122

35 Content (algebra) **123**
35.1 See also . . . 123
35.2 References . . . 123

36 Continuant (mathematics) **124**
36.1 Definition . . . 124
36.2 Applications . . . 124
36.3 References . . . 125

37 Cubic function **126**
37.1 History . . . 127
37.2 Critical points of a cubic function . . . 130
37.3 Roots of a cubic function . . . 130
37.3.1 The nature of the roots . . . 130
37.3.2 General formula for roots . . . 132
37.3.3 Reduction to a depressed cubic . . . 133
37.3.4 Cardano's method . . . 133
37.3.5 Vieta's substitution . . . 135
37.3.6 Lagrange's method . . . 136
37.3.7 Trigonometric (and hyperbolic) method . . . 137
37.3.8 Factorization . . . 138
37.3.9 Geometric interpretation of the roots . . . 139
37.4 Collinearities . . . 140
37.5 Applications . . . 140
37.6 See also . . . 140
37.7 Notes . . . 140
37.8 References . . . 142
37.9 External links . . . 143

38 Cyclotomic polynomial **147**
38.1 Examples . . . 147
38.2 Properties . . . 149
38.2.1 Fundamental tools . . . 149
38.2.2 Easy cases for the computation . . . 149

38.2.3 Integers appearing as coefficients . . . 150
38.2.4 Gauss's formula . . . 150
38.2.5 Lucas's formula . . . 151
38.3 Cyclotomic polynomials over Zp . . . 151
38.4 Prime Cyclotomic numbers . . . 152
38.5 Applications . . . 152
38.6 See also . . . 152
38.7 Notes . . . 152
38.8 References . . . 153
38.9 External links . . . 153

39 Degree of a polynomial **154**
39.1 Names of polynomials by degree . . . 154
39.2 Other examples . . . 155
39.3 Behavior under polynomial operations . . . 155
39.3.1 Behaviour under addition . . . 155
39.3.2 Behaviour under scalar multiplication . . . 155
39.3.3 Behaviour under multiplication . . . 156
39.3.4 Behaviour under composition . . . 156
39.4 Degree of the zero polynomial . . . 156
39.5 Computed from the function values . . . 157
39.6 Extension to polynomials with two or more variables . . . 157
39.7 Degree function in abstract algebra . . . 157
39.8 See also . . . 158
39.9 Notes . . . 158
39.10 References . . . 158
39.11 External links . . . 158

40 Delta operator **159**
40.1 Examples . . . 159
40.2 Basic polynomials . . . 160
40.3 See also . . . 160
40.4 References . . . 160

41 Denisyuk polynomials **161**
41.1 See also . . . 161
41.2 References . . . 161

42 Derivation of the Routh array **162**
42.1 The Cauchy index . . . 162
42.2 The Routh criterion . . . 164
42.3 Sturm's theorem . . . 165
42.4 References . . . 167

43 Descartes' rule of signs **168**
43.1 Descartes' rule of signs . . . 168
43.1.1 Positive roots . . . 168
43.1.2 Negative roots . . . 168
43.1.3 Example: real roots . . . 168
43.1.4 Complex roots . . . 169
43.1.5 Example: zero coefficients, complex roots . . . 169
43.2 Special case . . . 169
43.3 Generalizations . . . 170
43.4 See also . . . 170
43.5 Notes . . . 170
43.6 External links . . . 170

44 Dickson polynomial **171**
44.1 Definition . . . 171
44.2 Properties . . . 172
44.3 Links to other polynomials . . . 172
44.4 Permutation polynomials and Dickson polynomials . . . 173
44.5 References . . . 173

45 Difference polynomials **174**
45.1 Definition . . . 174
45.2 Moving differences . . . 174
45.3 Generating function . . . 175
45.4 See also . . . 175
45.5 References . . . 175

46 Discriminant **176**
46.1 Definition . . . 176
46.2 Formulas for low degrees . . . 177
46.3 Homogeneity . . . 178
46.4 Quadratic formula . . . 180
46.5 Discriminant of a polynomial . . . 180
46.6 Nature of the roots . . . 181
46.6.1 Quadratic . . . 182
46.6.2 Cubic . . . 182
46.6.3 Higher degrees . . . 182
46.7 Discriminant of a polynomial over a commutative ring . . . 182
46.8 Generalizations . . . 183
46.8.1 Discriminant of a conic section . . . 183
46.8.2 Discriminant of a quadratic form . . . 183
46.8.3 Discriminant of an algebraic number field . . . 184

46.9 Alternating polynomials . . . 184
46.10 References . . . 184
46.11 External links . . . 185

47 Divided power structure **186**
47.1 Definition . . . 186
47.2 Examples . . . 186
47.3 Constructions . . . 187
47.4 Applications . . . 187
47.5 References . . . 187

48 Division polynomials **188**
48.1 Definition . . . 188
48.2 Properties . . . 189
48.3 See also . . . 189
48.4 References . . . 189

49 Ehrhart polynomial **191**
49.1 Definition . . . 191
49.2 Examples of Ehrhart Polynomials . . . 191
49.3 Ehrhart Quasi-Polynomials . . . 192
49.4 Examples of Ehrhart Quasi-Polynomials . . . 193
49.5 Interpretation of coefficients . . . 193
49.6 Ehrhart Series . . . 193
49.6.1 Ehrhart series for rational polytopes . . . 193
49.7 Toric Variety . . . 194
49.8 Generalizations . . . 194
49.9 See also . . . 194
49.10 Notes . . . 194
49.11 References . . . 195

50 Eisenstein's criterion **196**
50.1 Examples . . . 196
50.1.1 Cyclotomic polynomials . . . 197
50.2 History . . . 197
50.3 Basic proof . . . 198
50.4 Advanced explanation . . . 198
50.5 Generalization . . . 199
50.5.1 Example . . . 200
50.6 See also . . . 200
50.7 References . . . 200

51 Equally spaced polynomial **201**

51.1 Properties . . . 201
51.2 References . . . 201

52 Equioscillation theorem 202
52.1 Statement . . . 202
52.2 Algorithms . . . 202
52.3 References . . . 202

53 Exponential polynomial 203
53.1 Definition . . . 203
53.1.1 In fields . . . 203
53.1.2 In abelian groups . . . 203
53.2 Properties . . . 204
53.3 Applications . . . 204
53.4 Notes . . . 204

54 External ray 205
54.1 History . . . 205
54.2 Notation . . . 205
54.3 Polynomials . . . 205
54.3.1 Dynamical plane = z-plane . . . 205
54.3.2 Parameter plane = c-plane . . . 207
54.3.3 External angle . . . 209
54.3.4 Computation of external argument . . . 209
54.4 Transcendental maps . . . 209
54.5 Images . . . 209
54.5.1 Dynamic rays . . . 209
54.5.2 Parameter rays . . . 209
54.6 Programs that can draw external rays . . . 211
54.7 See also . . . 211
54.8 References . . . 211
54.9 External links . . . 212

55 Faber polynomials 213
55.1 References . . . 213

56 Factor theorem 214
56.1 Factorization of polynomials . . . 214
56.1.1 Example . . . 214
56.2 References . . . 215

57 Factorization of polynomials 216
57.1 Formulation of the question . . . 216
57.2 Primitive part–content factorization . . . 217

57.3 Square-free factorization . . . 218
57.4 Classical methods . . . 218
57.4.1 Obtaining linear factors . . . 218
57.4.2 Kronecker's method . . . 218
57.5 Modern methods . . . 219
57.5.1 Factoring over finite fields . . . 219
57.5.2 Factoring univariate polynomials over the integers . . . 219
57.5.3 Factoring over algebraic extensions (Trager's method) . . . 220
57.6 See also . . . 221
57.7 Bibliography . . . 221
57.8 Further reading . . . 221

58 Factorization of polynomials over finite fields 222
58.1 Background . . . 222
58.1.1 Finite field . . . 222
58.1.2 Irreducible polynomials . . . 222
58.1.3 Complexity . . . 223
58.2 Factoring algorithms . . . 223
58.2.1 Square-free factorization . . . 223
58.2.2 Distinct-degree factorization . . . 224
58.2.3 Equal-degree factorization . . . 225
58.2.4 Victor Shoup's algorithm . . . 226
58.3 Rabin's test of irreducibility . . . 227
58.4 See also . . . 228
58.5 References . . . 228
58.6 External links . . . 228
58.7 Notes . . . 228

59 Fekete polynomial 229
59.1 References . . . 230
59.2 External links . . . 230

60 Fibonacci polynomials 231
60.1 Definition . . . 231
60.2 Identities . . . 232
60.3 Combinatorial interpretation . . . 233
60.4 References . . . 233
60.5 Further reading . . . 234
60.6 External links . . . 234

61 Gauss's lemma (polynomial) 235
61.1 Formal statements . . . 235
61.2 Proofs of the primitivity statement . . . 236

61.2.1 A variation, valid over arbitrary commutative rings . . . 236
61.2.2 A proof valid over any GCD domain . . . 237
61.3 Proof of the irreducibility statement . . . 237
61.4 Implications . . . 237
61.5 Notes . . . 238

62 Gauss–Lucas theorem 239
62.1 Formal statement . . . 239
62.2 Special cases . . . 239
62.3 Proof . . . 239
62.4 See also . . . 240
62.5 Notes . . . 240
62.6 References . . . 241
62.7 External links . . . 241

63 Generalized Appell polynomials 242
63.1 Special cases . . . 242
63.2 Explicit representation . . . 242
63.3 Recursion relation . . . 243
63.4 See also . . . 243
63.5 References . . . 244

64 Gould polynomials 245
64.1 References . . . 245

65 Grace–Walsh–Szegő theorem 246
65.1 Statement . . . 246
65.2 Notes and references . . . 246

66 List of polynomial topics 247
66.1 Terminology . . . 247
66.2 Basics . . . 247
66.2.1 Elementary abstract algebra . . . 248
66.3 Theory of equations . . . 248
66.4 Calculus with polynomials . . . 249
66.5 Polynomial interpolation . . . 249
66.6 Weierstrass approximation theorem . . . 249
66.7 Linear algebra . . . 249
66.8 Named polynomials and polynomial sequences . . . 250
66.9 Knot polynomials . . . 251
66.10 Algorithms . . . 251
66.11 Text and image sources, contributors, and licenses . . . 252
66.11.1 Text . . . 252

66.11.2 Images 256
66.11.3 Content license 259

Chapter 1

Abel polynomials

The **Abel polynomials** in mathematics form a polynomial sequence, the *n*th term of which is of the form

$p_n(x) = x(x - an)^{n-1}$.

The sequence is named after Niels Henrik Abel (1802-1829), the Norwegian mathematician.

This polynomial sequence is of binomial type: conversely, every polynomial sequence of binomial type may be obtained from the Abel sequence in the umbral calculus.

1.1 Examples

For a=1, the polynomials are (sequence A137452 in OEIS)

$p_0(x) = 1;$

$p_1(x) = x;$

$p_2(x) = -2x + x^2;$

$p_3(x) = 9x - 6x^2 + x^3;$

$p_4(x) = -64x + 48x^2 - 12x^3 + x^4;$

For a=2, the polynomials are

$p_0(x) = 1;$

$p_1(x) = x;$

$p_2(x) = -4x + x^2;$

$p_3(x) = 36x - 12x^2 + x^3;$

$p_4(x) = -512x + 192x^2 - 24x^3 + x^4;$

$p_5(x) = 10000x - 4000x^2 + 600x^3 - 40x^4 + x^5;$

$p_6(x) = -248832x + 103680x^2 - 17280x^3 + 1440x^4 - 60x^5 + x^6;$

1.2 References

- Rota, Gian-Carlo; Shen, Jianhong; Taylor, Brian D. (1997). "All Polynomials of Binomial Type Are Represented by Abel Polynomials". *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze Sér. 4* **25** (3–4): 731–738. MR 1655539. Zbl 1003.05011.

1.3 External links

- Weisstein, Eric W., "Abel Polynomial", *MathWorld*.

Chapter 2

Abel–Ruffini theorem

Not to be confused with Abel's theorem.

$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

A general solution to any quadratic equation can be given using the quadratic formula above. Similar formulas exist for polynomial equations of degree 3 and 4. But no such formula is possible for 5th degree polynomials; the real solution $-1.1673...$ to the 5th degree equation below cannot be written using basic arithmetic operations and nth roots:

$x^5 - x + 1 = 0$

In algebra, the **Abel–Ruffini theorem** (also known as **Abel's impossibility theorem**) states that there is no *general* algebraic solution—that is, solution in radicals— to polynomial equations of degree five or higher with arbitrary coefficients.[1] The theorem is named after Paolo Ruffini, who made an incomplete proof in 1799, and Niels Henrik Abel, who provided a proof in 1823. Évariste Galois independently proved the theorem in a work that was posthumously published in 1846.[2]

2.1 Interpretation

The theorem does *not* assert that some higher-degree polynomial equations have *no* solution. In fact, the opposite is true: *every* non-constant polynomial equation in one unknown, with real or complex coefficients, has at least one complex number as a solution (and thus, by polynomial division, as many complex roots as its degree, counting repeated roots); this is the fundamental theorem of algebra. These solutions can be computed to any desired degree of accuracy using numerical methods such as the Newton–Raphson method or Laguerre method, and in this way they are no different from solutions to polynomial equations of the second, third, or fourth degrees. The theorem only shows that the solutions of some of these equations cannot be expressed via a general expression in radicals.

Also, the theorem does *not* assert that some higher-degree polynomial equations have roots which cannot be expressed in terms of radicals. While this is now known to be true, it is a stronger claim, which was only proven a few years later by Galois. The theorem only shows that there is no *general* solution in terms of radicals which gives the roots to a generic polynomial with arbitrary coefficients. It did not by itself rule out the possibility that each polynomial may be solved in terms of radicals on a case-by-case basis.

2.2 Lower-degree polynomials

The solutions of any second-degree polynomial equation can be expressed in terms of addition, subtraction, multiplication, division, and square roots, using the familiar quadratic formula: The roots of the following equation are shown below:

$ax^2 + bx + c = 0, a \neq 0$

$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Analogous formulas for third- and fourth-degree equations, using cube roots and fourth roots, have been known since the 16th century.

2.3 Quintics and higher

The Abel–Ruffini theorem says that there are *some* fifth-degree equations whose solution cannot be so expressed. The equation $x^5 - x + 1 = 0$ is an example. (See Bring radical.) Some other fifth degree equations *can* be solved by radicals, for example $x^5 - x^4 - x + 1 = 0$, which factors into $(x - 1)(x - 1)(x + 1)(x + i)(x - i) = 0$. The precise criterion that distinguishes between those equations that can be solved by radicals and those that cannot was given by Évariste Galois and is now part of Galois theory: a polynomial equation can be solved by radicals if and only if its Galois group (over the rational numbers, or more generally over the base field of admitted constants) is a solvable group.

Today, in the modern algebraic context, we say that second, third and fourth degree polynomial equations can always be solved by radicals because the symmetric groups S_2, S_3 and S_4 are solvable groups, whereas S_n is not solvable for $n \geq 5$. This is so because for a polynomial of degree n with indeterminate coefficients (i.e., given by symbolic parameters), the Galois group is the full symmetric group S_n (this is what is called the "general equation of the n-th degree"). This remains true if the coefficients are concrete but algebraically independent values over the base field.

2.4 Proof

The following proof is based on Galois theory (for a short explanation of Arnold's proof that does not rely on prior knowledge in group theory see [3]). Historically, Ruffini and Abel's proofs precede Galois theory and Arnold's. For a modern presentation of Abel's proof see the books of Tignol or Pesic.

One of the fundamental theorems of Galois theory states that a polynomial $f(x) \in F[x]$ is solvable by radicals over F if and only if its splitting field K over F has a solvable Galois group,[4] so the proof of the Abel–Ruffini theorem comes down to computing the Galois group of the general polynomial of the fifth degree.

Let y_1 be a real number transcendental over the field of rational numbers Q , and let y_2 be a real number transcendental over $Q(y_1)$, and so on to y_5 which is transcendental over $Q(y_1, y_2, y_3, y_4)$. These numbers are called independent transcendental elements over Q. Let $E = Q(y_1, y_2, y_3, y_4, y_5)$ and let

$$f(x) = (x - y_1)(x - y_2)(x - y_3)(x - y_4)(x - y_5) \in E[x].$$

Expanding $f(x)$ out yields the elementary symmetric functions of the y_n :

$$s_1 = y_1 + y_2 + y_3 + y_4 + y_5$$

$$s_2 = y_1y_2 + y_1y_3 + y_1y_4 + y_1y_5 + y_2y_3 + y_2y_4 + y_2y_5 + y_3y_4 + y_3y_5 + y_4y_5$$

$$s_3 = y_1y_2y_3 + y_1y_2y_4 + y_1y_2y_5 + y_1y_3y_4 + y_1y_3y_5 + y_1y_4y_5 + y_2y_3y_4 + y_2y_3y_5 + y_2y_4y_5 + y_3y_4y_5$$

$$s_4 = y_1y_2y_3y_4 + y_1y_2y_3y_5 + y_1y_2y_4y_5 + y_1y_3y_4y_5 + y_2y_3y_4y_5$$

$$s_5 = y_1y_2y_3y_4y_5.$$

The coefficient of x^n in $f(x)$ is thus $(-1)^{5-n}s_{5-n}$. Let $F = Q(s_i)$ be the field obtained by adjoining the symmetric functions to the rationals (the s_i are all transcendental, because the y_i are independent). Because our independent transcendentals y_n act as indeterminates over Q , every permutation σ in the symmetric group on 5 letters S_5 induces a distinct automorphism σ' on E that leaves Q fixed and permutes the elements y_n . Since an arbitrary rearrangement of the roots of the product form still produces the same polynomial, e.g.:

$$(y - y_3)(y - y_1)(y - y_2)(y - y_5)(y - y_4)$$

is still the same polynomial as

$$(y - y_1)(y - y_2)(y - y_3)(y - y_4)(y - y_5)$$

the automorphisms σ' also leave f fixed, so they are elements of the Galois group $G(E/F)$. So we have shown that $S_5 \subseteq G(E/F)$; however there could possibly be automorphisms there that are not in S_5 . However, since the relative automorphism group for the splitting field of a quintic polynomial has at most 5! elements, it follows that $G(E/F)$ is isomorphic to S_5 . Generalizing this argument shows that the Galois group of every general polynomial of degree n is isomorphic to S_n .

And what of S_5 ? The only composition series of S_5 is $S_5 \geq A_5 \geq \{e\}$ (where A_5 is the alternating group on five letters, also known as the icosahedral group). However, the quotient group $A_5/\{e\}$ (isomorphic to A_5 itself) is not an abelian group, and so S_5 is not solvable, so it must be that the general polynomial of the fifth degree has no solution in radicals. Since the first nontrivial normal subgroup of the symmetric group on n letters is always the alternating group on n letters, and since the alternating groups on n letters for $n \geq 5$ are always simple and non-abelian, and hence not solvable, it also says that the general polynomials of all degrees higher than the fifth also have no solution in radicals.

Note that the above construction of the Galois group for a fifth degree polynomial only applies to the *general polynomial*, specific polynomials of the fifth degree may have different Galois groups with quite different properties, e.g. $x^5 - 1$ has a splitting field generated by a primitive 5th root of unity, and hence its Galois group is abelian and the equation itself solvable by radicals; moreover the argument does not provide any rational-valued quintic that has S_5 or A_5 as its Galois group. However, since the result is on the general polynomial, it does say that a general "quintic formula" for the roots of a quintic using only a finite combination of the arithmetic operations and radicals in terms of the coefficients is impossible. Q.E.D.

2.5 History

Around 1770, Joseph Louis Lagrange began the groundwork that unified the many different tricks that had been used up to that point to solve equations, relating them to the theory of groups of permutations, in the form of Lagrange resolvents. This innovative work by Lagrange was a precursor to Galois theory, and its failure to develop solutions for equations of fifth and higher degrees hinted that such solutions might be impossible, but it did not provide conclusive proof. The theorem, however, was first nearly proved by Paolo Ruffini in 1799, but his proof was mostly ignored. He had several times tried to send it to different mathematicians to get it acknowledged, amongst them, French mathematician Augustin-Louis Cauchy, but it was never acknowledged, possibly because the proof was spanning 500 pages. The proof also, as was discovered later, contained an error. In modern terms, Ruffini failed to prove that the splitting field is one of the fields in the tower of radicals which corresponds to the hypothesized solution by radicals; this assumption fails, for example, for Cardano's solution of the cubic; it splits not only the original cubic but also the two others with the same discriminant. While Cauchy felt that the assumption was minor, most historians believe that the proof was not complete until Abel proved this assumption. The theorem is thus generally credited to Niels Henrik Abel, who published a proof that required just six pages in 1824.[5]

Proving that some quintic (and higher) equations were unsolvable by radicals did not completely settle the matter, because the Abel–Ruffini theorem does not provide necessary and sufficient conditions for saying precisely which quintic (and higher) equations are unsolvable by radicals; for example $x^5 - 1 = 0$ is solvable. Abel was working on a complete characterization when he died in 1829.[6] Furthermore, Ian Stewart notes that "for all that Abel's methods could prove, every particular quintic equation might be soluble, with a special formula for each equation."[7]

In 1830 Galois (at the age of 18) submitted to the Paris Academy of Sciences a memoir on his theory of solvability by radicals; Galois' paper was ultimately rejected in 1831 as being too sketchy and for giving a condition in terms of the roots of the equation instead of its coefficients. Galois then died in 1832 and his paper—"Memoire sur les conditions de resolubilite des equations par radicaux"—remained unpublished until 1846 when it was published by Joseph Liouville accompanied by some of his own explanations.[6] Prior to this publication, Liouville announced Galois' result to the Academy in a speech he gave on 4 July 1843.[8] According to Allan Clark, Galois's characterization "dramatically supersedes the work of Abel and Ruffini."[9]

In 1963, Vladimir Arnold discovered a topological proof of the Abel–Ruffini theorem,[10] which served as a starting point for topological Galois theory.[11]

2.6 See also

- Theory of equations
- Constructible number

2.7 Notes

[1] Jacobson (2009), p. 211.

[2] Galois, Évariste (1846). "OEuvres mathématiques d'Évariste Galois.". *Journal des mathématiques pures et appliquées* **XI**: 381–444. Retrieved 2009-02-04.

[3] "Short proof of Abel's theorem that 5th degree polynomial equations cannot be solved".

[4] Fraleigh (1994, p. 401)

[5] du Sautoy, Marcus. "January: Impossibilities". *Symmetry: A Journey into the Patterns of Nature*. ISBN 978-0-06-078941-1.

[6] Jean-Pierre Tignol (2001). *Galois' Theory of Algebraic Equations*. World Scientific. pp. 232–233 and 302. ISBN 978-981-02-4541-2.

[7] Stewart, 3rd ed., p. xxiii

[8] Stewart, 3rd ed., p. xxiii

[9] Allan Clark (1984) [1971]. *Elements of Abstract Algebra*. Courier Corporation. p. 131. ISBN 978-0-486-14035-3.

[10] "Tribute to Vladimir Arnold" (PDF). *Notices of the American Mathematical Society* **59** (3): 393. March 2012. doi:10.1090/noti810.

[11] "Vladimir Igorevich Arnold". 2010.

2.8 References

- Edgar Dehn. *Algebraic Equations: An Introduction to the Theories of Lagrange and Galois*. Columbia University Press, 1930. ISBN 0-486-43900-3.
- Jacobson, Nathan (2009), *Basic algebra* **1** (2nd ed.), Dover, ISBN 978-0-486-47189-1
- John B. Fraleigh. *A First Course in Abstract Algebra.* Fifth Edition. Addison-Wesley, 1994. ISBN 0-201-59291-6.
- Ian Stewart. *Galois Theory*. Chapman and Hall, 1973. ISBN 0-412-10800-3.
- Abel's Impossibility Theorem at Everything2

2.9 Further reading

- Peter Pesic (2003). *Abel's Proof: An Essay on the Sources and Meaning of Mathematical Unsolvability*. MIT Press. ISBN 978-0-262-66182-9.

2.10 External links

- Mémoire sur les équations algébriques, ou l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré PDF - the first proof in French (1824)
- Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré PDF - the second proof in French (1826)
- "A video presentation on Arnold's proof".

Chapter 3

Actuarial polynomials

In mathematics, the **actuarial polynomials** $a(\beta)$
$n(x)$ are polynomials studied by Toscano (1950) given by the generating function

$$\sum_n \frac{a_n^{(\beta)}(x)}{n!} t^n = \exp(\beta t + x(1 - e^t))$$

(Roman 1984, 4.3.4), Boas & Buck (1958).

3.1 See also

- Umbral calculus

3.2 References

- Boas, Ralph P.; Buck, R. Creighton (1958), *Polynomial expansions of analytic functions*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge. **19**, Berlin, New York: Springer-Verlag, MR 0094466
- Roman, Steven (1984), *The umbral calculus*, Pure and Applied Mathematics **111**, London: Academic Press Inc. [Harcourt Brace Jovanovich Publishers], ISBN 978-0-12-594380-2, MR 741185 Reprinted by Dover, 2005
- Toscano, Letterio (1950), "Una classe di polinomi della matematica attuariale", *Rivista di Matematica della Università di Parma* (in Italian) **1**: 459–470, MR 0040480, Zbl 0040.03204

Chapter 4

Additive polynomial

In mathematics, the **additive polynomials** are an important topic in classical algebraic number theory.

4.1 Definition

Let k be a field of characteristic p, with p a prime number. A polynomial $P(x)$ with coefficients in k is called an **additive polynomial**, or a **Frobenius polynomial**, if

$$P(a+b) = P(a) + P(b)$$

as polynomials in a and b. It is equivalent to assume that this equality holds for all a and b in some infinite field containing k, such as its algebraic closure.

Occasionally **absolutely additive** is used for the condition above, and **additive** is used for the weaker condition that $P(a + b) = P(a) + P(b)$ for all a and b in the field. For infinite fields the conditions are equivalent, but for finite fields they are not, and the weaker condition is the "wrong" one and does not behave well. For example, over a field of order q any multiple P of $x^q - x$ will satisfy $P(a + b) = P(a) + P(b)$ for all a and b in the field, but will usually not be (absolutely) additive.

4.2 Examples

The polynomial x^p is additive. Indeed, for any a and b in the algebraic closure of k one has by the binomial theorem

$$(a+b)^p = \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n}.$$

Since p is prime, for all $n = 1, ..., p-1$ the binomial coefficient $\binom{p}{n}$ is divisible by p, which implies that

$$(a+b)^p \equiv a^p + b^p \mod p$$

as polynomials in a and b.

Similarly all the polynomials of the form

$$\tau_p^n(x) = x^{p^n}$$

are additive, where n is a non-negative integer.

4.3 The ring of additive polynomials

It is quite easy to prove that any linear combination of polynomials $\tau_p^n(x)$ with coefficients in k is also an additive polynomial. An interesting question is whether there are other additive polynomials except these linear combinations. The answer is that these are the only ones.

One can check that if $P(x)$ and $M(x)$ are additive polynomials, then so are $P(x) + M(x)$ and $P(M(x))$. These imply that the additive polynomials form a ring under polynomial addition and composition. This ring is denoted

$$k\{\tau_p\}.$$

This ring is not commutative unless k equals the field $\mathbb{F}_p = \mathbf{Z}/p\mathbf{Z}$ (see modular arithmetic). Indeed, consider the additive polynomials ax and x^p for a coefficient a in k. For them to commute under composition, we must have

$$(ax)^p = ax^p,$$

or $a^p - a = 0$. This is false for a not a root of this equation, that is, for a outside $\mathbb{F}_p$.

4.4 The fundamental theorem of additive polynomials

Let $P(x)$ be a polynomial with coefficients in k, and $\{w_1,\ldots,w_m\} \subset k$ be the set of its roots. Assuming that the roots of $P(x)$ are distinct (that is, $P(x)$ is separable), then $P(x)$ is additive if and only if the set $\{w_1,\ldots,w_m\}$ forms a group with the field addition.

4.5 See also

- Drinfeld module
- Additive map

4.6 References

- David Goss, *Basic Structures of Function Field Arithmetic*, 1996, Springer, Berlin. ISBN 3-540-61087-1.

4.7 External links

- Weisstein, Eric W., "Additive Polynomial", *MathWorld*.

Chapter 5

Alexander polynomial

In mathematics, the **Alexander polynomial** is a knot invariant which assigns a polynomial with integer coefficients to each knot type. James Waddell Alexander II discovered this, the first knot polynomial, in 1923. In 1969, John Conway showed a version of this polynomial, now called the **Alexander–Conway polynomial**, could be computed using a skein relation, although its significance was not realized until the discovery of the Jones polynomial in 1984. Soon after Conway's reworking of the Alexander polynomial, it was realized that a similar skein relation was exhibited in Alexander's paper on his polynomial.[1]

5.1 Definition

Let K be a knot in the 3-sphere. Let X be the infinite cyclic cover of the knot complement of K. This covering can be obtained by cutting the knot complement along a Seifert surface of K and gluing together infinitely many copies of the resulting manifold with boundary in a cyclic manner. There is a covering transformation t acting on X. Consider the first homology (with integer coefficients) of X, denoted $H_1(X)$. The transformation t acts on the homology and so we can consider $H_1(X)$ a module over $\mathbb{Z}[t, t^{-1}]$. This is called the **Alexander invariant** or **Alexander module**.

The module is finitely presentable; a presentation matrix for this module is called the **Alexander matrix**. If the number of generators, r, is less than or equal to the number of relations, s, then we consider the ideal generated by all r by r minors of the matrix; this is the zero'th Fitting ideal or **Alexander ideal** and does not depend on choice of presentation matrix. If $r > s$, set the ideal equal to 0. If the Alexander ideal is principal, take a generator; this is called an Alexander polynomial of the knot. Since this is only unique up to multiplication by the Laurent monomial $\pm t^n$, one often fixes a particular unique form. Alexander's choice of normalization is to make the polynomial have a positive constant term.

Alexander proved that the Alexander ideal is nonzero and always principal. Thus an Alexander polynomial always exists, and is clearly a knot invariant, denoted $\Delta_K(t)$. The Alexander polynomial for the knot configured by only one string is a polynomial of t^2 and then it is the same polynomial for the mirror image knot. Namely, it can not distinguish between the knot and one for its mirror image.

5.2 Computing the polynomial

The following procedure for computing the Alexander polynomial was given by J. W. Alexander in his paper.

Take an oriented diagram of the knot with n crossings; there are $n + 2$ regions of the knot diagram. To work out the Alexander polynomial, first one must create an incidence matrix of size $(n, n + 2)$. The n rows correspond to the n crossings, and the $n + 2$ columns to the regions. The values for the matrix entries are either 0, 1, −1, t, $-t$.

Consider the entry corresponding to a particular region and crossing. If the region is not adjacent to the crossing, the entry is 0. If the region is adjacent to the crossing, the entry depends on its location. The following table gives the entry, determined by the location of the region at the crossing from the perspective of the incoming undercrossing line.

on the left before undercrossing: $-t$

on the right before undercrossing: 1

on the left after undercrossing: t

on the right after undercrossing: -1

Remove two columns corresponding to adjacent regions from the matrix, and work out the determinant of the new n by n matrix. Depending on the columns removed, the answer will differ by multiplication by $\pm t^n$. To resolve this ambiguity, divide out the largest possible power of t and multiply by -1 if necessary, so that the constant term is positive. This gives the Alexander polynomial.

The Alexander polynomial can also be computed from the Seifert matrix.

After the work of Alexander R. Fox considered a copresentation of the knot group $\pi_1(S^3 \backslash K)$, and introduced non-commutative differential calculus Fox (1961), which also permits one to compute $\Delta_K(t)$. Detailed exposition of this approach about higher Alexander polynomials can be found in the book Crowell & Fox (1963).

5.3 Basic properties of the polynomial

The Alexander polynomial is symmetric: $\Delta_K(t^{-1}) = \Delta_K(t)$ for all knots K.

> From the point of view of the definition, this is an expression of the Poincaré Duality isomorphism $\overline{H_1 X} \simeq \mathrm{Hom}_{\mathbb{Z}[t,t^{-1}]}(H_1 X, G)$ where G is the quotient of the field of fractions of $\mathbb{Z}[t,t^{-1}]$ by $\mathbb{Z}[t,t^{-1}]$, considered as a $\mathbb{Z}[t,t^{-1}]$ -module, and where $\overline{H_1 X}$ is the conjugate $\mathbb{Z}[t,t^{-1}]$ -module to $H_1 X$ ie: as an abelian group it is identical to $H_1 X$ but the covering transformation t acts by t^{-1} .

and it evaluates to a unit on 1: $\Delta_K(1) = \pm 1$.

> From the point of view of the definition, this is an expression of the fact that the knot complement is a homology circle, generated by the covering transformation t . More generally if M is a 3-manifold such that $rank(H_1 M) = 1$ it has an Alexander polynomial $\Delta_M(t)$ defined as the order ideal of its infinite-cyclic covering space. In this case $\Delta_M(1)$ is, up to sign, equal to the order of the torsion subgroup of $H_1 M$.

It is known that every integral Laurent polynomial which is both symmetric and evaluates to a unit at 1 is the Alexander polynomial of a knot (Kawauchi 1996).

5.4 Geometric significance of the polynomial

Since the Alexander ideal is principal, $\Delta_K(t) = 1$ if and only if the commutator subgroup of the knot group is perfect (i.e. equal to its own commutator subgroup).

For a topologically slice knot, the Alexander polynomial satisfies the Fox–Milnor condition $\Delta_K(t) = f(t)f(t^{-1})$ where $f(t)$ is some other integral Laurent polynomial.

Twice the knot genus is bounded below by the degree of the Alexander polynomial.

Michael Freedman proved that a knot in the 3-sphere is topologically slice; i.e., bounds a "locally-flat" topological disc in the 4-ball, if the Alexander polynomial of the knot is trivial (Freedman and Quinn, 1990).

Kauffman (1983) describes the first construction of the Alexander polynomial via state sums derived from physical models. A survey of these topic and other connections with physics are given in Kauffman (2001).

There are other relations with surfaces and smooth 4-dimensional topology. For example, under certain assumptions, there is a way of modifying a smooth 4-manifold by performing a surgery that consists of removing a neighborhood of a two-dimensional torus and replacing it with a knot complement crossed with S^1. The result is a smooth 4-manifold homeomorphic to the original, though now the Seiberg–Witten invariant has been modified by multiplication with the Alexander polynomial of the knot.[2]

Knots with symmetries are known to have restricted Alexander polynomials. See the symmetry section in (Kawauchi 1996). Nonetheless, the Alexander polynomial can fail to detect some symmetries, such as strong invertibility.

If the knot complement fibers over the circle, then the Alexander polynomial of the knot is known to be *monic* (the coefficients of the highest and lowest order terms are equal to ± 1). In fact, if $S \to C_K \to S^1$ is a fiber bundle where C_K is the knot complement, let $g : S \to S$ represent the monodromy, then $\Delta_K(t) = Det(tI - g_*)$ where $g_* : H_1 S \to H_1 S$ is the induced map on homology.

5.5 Relations to satellite operations

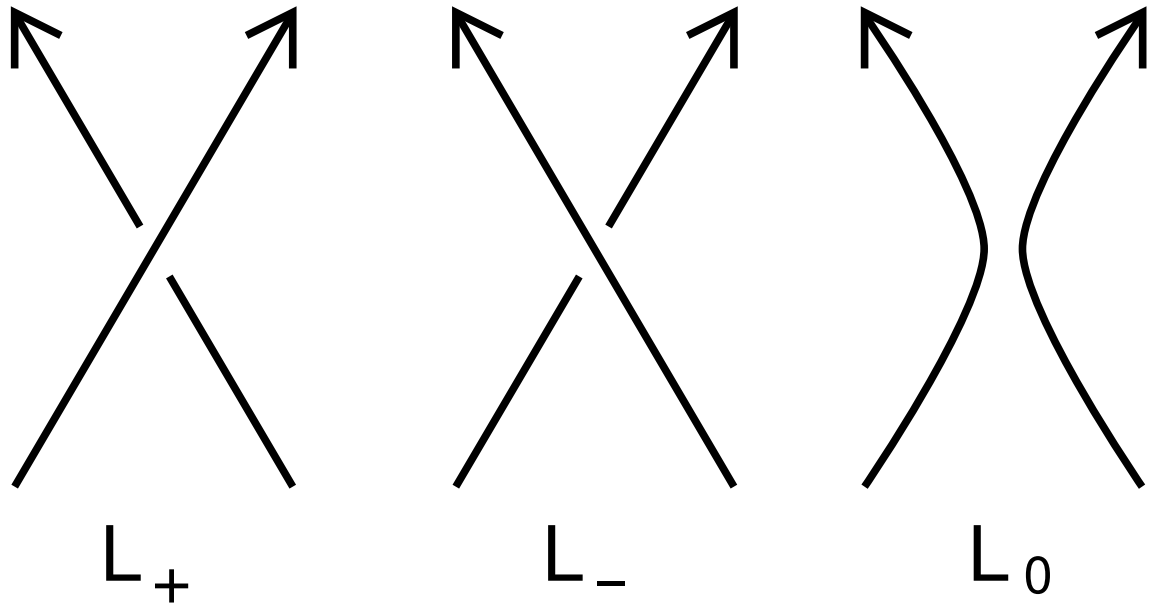
If a knot K is a satellite knot with companion K' i.e.: there exists an embedding $f : S^1 \times D^2 \to S^3$ such that $K = f(K')$ where $S^1 \times D^2 \subset S^3$ is an unknotted solid torus, then $\Delta_K(t) = \Delta_{f(S^1 \times \{0\})}(t^a)\Delta_{K'}(t)$. Where $a \in \mathbb{Z}$ is the integer that represents $K' \subset S^1 \times D^2$ in $H_1(S^1 \times D^2) = \mathbb{Z}$.

Examples: For a connect-sum $\Delta_{K_1 \# K_2}(t) = \Delta_{K_1}(t)\Delta_{K_2}(t)$. If K is an untwisted Whitehead double, then $\Delta_K(t) = \pm 1$.

5.6 Alexander–Conway polynomial

Alexander proved the Alexander polynomial satisfies a skein relation. John Conway later rediscovered this in a different form and showed that the skein relation together with a choice of value on the unknot was enough to determine the polynomial. Conway's version is a polynomial in z with integer coefficients, denoted $\nabla(z)$ and called the **Alexander–Conway polynomial** (also known as **Conway polynomial** or **Conway–Alexander polynomial**).

Suppose we are given an oriented link diagram, where L_+, L_-, L_0 are link diagrams resulting from crossing and smoothing changes on a local region of a specified crossing of the diagram, as indicated in the figure.



Here are Conway's skein relations:

- $\nabla(O) = 1$ (where O is any diagram of the unknot)
- $\nabla(L_+) - \nabla(L_-) = z\nabla(L_0)$

The relationship to the standard Alexander polynomial is given by $\Delta_L(t^2) = \nabla_L(t - t^{-1})$. Here Δ_L must be properly normalized (by multiplication of $\pm t^{n/2}$) to satisfy the skein relation $\Delta(L_+) - \Delta(L_-) = (t^{1/2} - t^{-1/2})\Delta(L_0)$. Note that this relation gives a Laurent polynomial in $t^{1/2}$.

See knot theory for an example computing the Conway polynomial of the trefoil.

5.7 Relation to Khovanov homology

In Ozsvath & Szabo (2004) and Rasmussen (2003) the Alexander polynomial is presented as Euler characteristic of a complex, whose homology are isotopy invariants of the considered knot K , therefore Floer homology theory is a categorification of the Alexander polynomial. For detail, see Khovanov homology Khovanov (2003).

5.8 Notes

[1] Alexander describes his skein relation toward the end of his paper under the heading "miscellaneous theorems", which is possibly why it got lost. Joan Birman mentions in her paper *New points of view in knot theory* (Bull. Amer. Math. Soc. (N.S.) 28 (1993), no. 2, 253–287) that Mark Kidwell brought her attention to Alexander's relation in 1970.

[2] Fintushel and Stern (1997) – Knots, links, and 4-manifolds

5.9 References

- Alexander, J. W. (1928). "Topological invariants of knots and links". *Trans. Amer. Math. Soc.* **30** (2): 275–306. doi:10.2307/1989123.
- Crowell, R.; Fox, R. (1963). *Introduction to Knot Theory*. Ginn and Co. after 1977 Springer Verlag.
- Adams, Colin C. (2004). *The Knot Book: An elementary introduction to the mathematical theory of knots* (Revised reprint of the 1994 original ed.). Providence, RI: American Mathematical Society. ISBN 0-8218-3678-1. (accessible introduction utilizing a skein relation approach)
- Fox, R. (1961). "A quick trip through knot theory, In Topology of ThreeManifold" (Proceedings of 1961 Topology Institute at Univ. of Georgia, edited by M.K.Fort ed.). Englewood Cliffs. N. J.: Prentice-Hall. pp. 120–167.
- Freedman, Michael H.; Quinn, Frank (1990). *Topology of 4-manifolds*. Princeton Mathematical Series **39**. Princeton, NJ: Princeton University Press. ISBN 0-691-08577-3.
- Kauffman, Louis (1983). "Formal Knot Theory". Princeton University press.
- Kauffman, Louis (2001). *Knots and Physics*. World Scientific Publishing Companey.
- Kawauchi, Akio (1996). *A Survey of Knot Theory*. Birkhauser. (covers several different approaches, explains relations between different versions of the Alexander polynomial)
- Khovanov, M. (2006). "Link homology and categorification". Proceedings of the ICM-2006. arXiv:math/0605339.
- Ozsvath, Peter; Szabo, Zoltan (2004). "Holomorphic disks and knot invariants". *Adv. Math., no., 58-−6*. Adv. Math. **186** (1): 58–116. arXiv:math/0209056. Bibcode:2002math.....9056O. doi:10.1016/j.aim.2003.05.001. class=math.GT
- Rasmussen, J. (2003). "Floer homology and knot complements". PhD thesis Harvard University. p. 6378. arXiv:math/0306378. Bibcode:2003math.....6378R.
- Rolfsen, Dale (1990). *Knots and Links* (2nd ed.). Berkeley, CA: Publish or Perish. ISBN 0-914098-16-0. (explains classical approach using the Alexander invariant; knot and link table with Alexander polynomials)

5.10 External links

- Hazewinkel, Michiel, ed. (2001), "Alexander invariants", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- "Main Page" and "The Alexander-Conway Polynomial", *The Knot Atlas*. – knot and link tables with computed Alexander and Conway polynomials

Chapter 6

Algebraic equation

In mathematics, an **algebraic equation** or **polynomial equation** is an equation of the form

$$P = Q$$

where *P* and *Q* are polynomials with coefficients in some field, often the field of the rational numbers. For most authors, an algebraic equation is *univariate*, which means that it involves only one variable. On the other hand, a polynomial equation may involve several variables, in which case it is called *multivariate* and the term *polynomial equation* is usually preferred to *algebraic equation*.

For example,

$$x^5 - 3x + 1 = 0$$

is an algebraic equation with integer coefficients and

$$y^4 + \frac{xy}{2} = \frac{x^3}{3} - xy^2 + y^2 - \frac{1}{7}$$

is a multivariate polynomial equation over the rationals.

Some but not all polynomial equations with rational coefficients have a solution that is an algebraic expression with a finite number of operations involving just those coefficients (that is, can be solved algebraically). This can be done for all such equations of degree one, two, three, or four; but for degree five or more it can only be done for some equations but not for all. A large amount of research has been devoted to compute efficiently accurate approximations of the real or complex solutions of an univariate algebraic equation (see Root-finding algorithm) and of the common solutions of several multivariate polynomial equations (see System of polynomial equations).

6.1 History

The study of algebraic equations is probably as old as mathematics: the Babylonian mathematicians, as early as 2000 BC could solve some kind of quadratic equations (displayed on Old Babylonian clay tablets).

The algebraic equations over the rationals with only one variable are also called univariate equations. They have a very long history. Ancient mathematicians wanted the solutions in the form of radical expressions, like $x = \frac{1+\sqrt{5}}{2}$ for the positive solution of $x^2 - x - 1 = 0$. The ancient Egyptians knew how to solve equations of degree 2 in this manner. In the 9th century Muhammad ibn Musa al-Khwarizmi and other Islamic mathematicians derived the quadratic formula, the general solution of equations of degree 2, and recognized the importance of the discriminant. During the Renaissance in 1545, Gerolamo Cardano found the solution to equations of degree 3 and Lodovico Ferrari solved equations of degree 4. Finally Niels Henrik Abel proved, in 1824, that equations of degree 5 and equations of higher degree are not always solvable using radicals. Galois theory, named after Évariste Galois, was introduced to give criteria deciding if an equation is solvable using radicals.

6.2 Areas of study

The algebraic equations are the basis of a number of areas of modern mathematics: Algebraic number theory is the study of (univariate) algebraic equations over the rationals. Galois theory has been introduced by Évariste Galois for getting criteria deciding if an algebraic equation may be solved in terms of radicals. In field theory, an algebraic extension is an extension such that every element is a root of an algebraic equation over the base field. Transcendence theory is the study of the real numbers which are not solutions to an algebraic equation over the rationals. A Diophantine equation is a (usually multivariate) polynomial equation with integer coefficients for which one is interested in the integer solutions. Algebraic geometry is the study of the solutions in an algebraically closed field of multivariate polynomial equations.

Two equations are equivalent if they have the same set of solutions. In particular the equation $P = Q$ is equivalent with $P - Q = 0$. It follows that the study of algebraic equations is equivalent to the study of polynomials.

A polynomial equation over the rationals can always be converted to an equivalent one in which the coefficients are integers. For example, multiplying through by 42 = 2·3·7 and grouping its terms in the first member, the previously mentioned polynomial equation $y^4 + \frac{xy}{2} = \frac{x^3}{3} - xy^2 + y^2 - \frac{1}{7}$ becomes

$$42y^4 + 21xy - 14x^3 + 42xy^2 - 42y^2 + 6 = 0.$$

Because sine, exponentiation, and $1/T$ are not polynomial functions,

$$e^T x^2 + \frac{1}{T}xy + \sin(T)z - 2 = 0$$

is *not* a polynomial equation in the four variables *x*, *y*, *z*, and *T* over the rational numbers. However, it is a polynomial equation in the three variables *x*, *y*, and *z* over the field of the elementary functions in the variable *T*.

As for any equation, the solutions of an equation are the values of the variables for which the equation is true. For univariate algebraic equations these are also called **roots**, even if, properly speaking, one should say *the **solutions** of the algebraic equation P=0 are the **roots** of the polynomial P*. When solving an equation, it is important to specify in which set the solutions are allowed. For example, for an equation over the rationals one may look for solutions in which all the variables are integers. In this case the equation is a diophantine equation. One may also be interested only in the real solutions. However, for univariate algebraic equations, the number of solutions is finite, and all solutions are contained in any algebraically closed field containing the coefficients—for example, the field of complex numbers in the case of equations over the rationals. It follows that without precision "root" and "solution" usually mean "solution in an algebraically closed field".

6.3 See also

- Algebraic function
- Algebraic number
- Root finding
- Linear equation (degree = 1)
- Quadratic equation (degree = 2)
- Cubic equation (degree = 3)
- Quartic equation (degree = 4)
- Quintic equation (degree = 5)
- Sextic equation (degree = 6)
- Septic equation (degree = 7)
- System of linear equations

- System of polynomial equations
- Linear Diophantine equation
- Linear equation over a ring
- Cramer's theorem (algebraic curves), on the number of points usually sufficient to determine a bivariate n-th degree curve

6.4 References

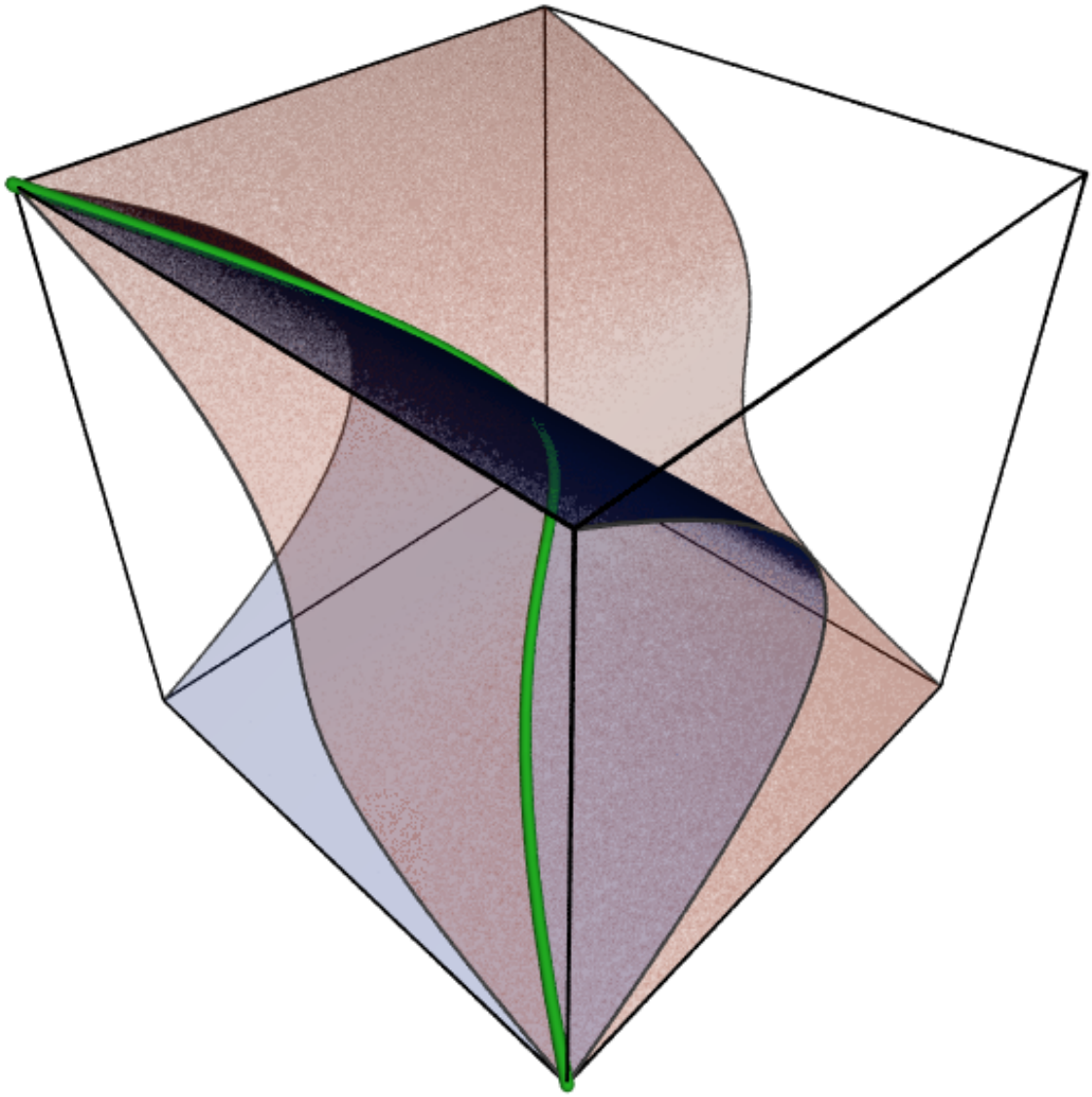
- Hazewinkel, Michiel, ed. (2001), "Algebraic equation", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Weisstein, Eric W., "Algebraic Equation", *MathWorld*.

Chapter 7

Algebraic variety

This article is about algebraic varieties. For the term "variety of algebras", and an explanation of the difference between a variety of algebras and an algebraic variety, see variety (universal algebra).

In mathematics, **algebraic varieties** (also called **varieties**) are one of the central objects of study in algebraic



The twisted cubic is a projective algebraic variety.

geometry. Classically, an algebraic variety was defined to be the set of solutions of a system of polynomial equations, over the real or complex numbers. Modern definitions of an algebraic variety generalize this notion in several different ways, while attempting to preserve the geometric intuition behind the original definition.[1]:58

Conventions regarding the definition of an algebraic variety differ slightly. For example, some authors require that an "*algebraic variety*" is, by definition, *irreducible* (which means that it is not the union of two smaller sets that are closed in the Zariski topology), while others do not. When the former convention is used, non-irreducible algebraic varieties are called **algebraic sets**.

The notion of variety is similar to that of manifold, the difference being that a variety may have singular points, while a manifold will not. In many languages, both varieties and manifolds are named by the same word.

Proven around the year 1800, the fundamental theorem of algebra establishes a link between algebra and geometry by showing that a monic polynomial (an algebraic object) in one variable with complex coefficients is determined by the set of its roots (a geometric object) in the complex plane. Generalizing this result, Hilbert's Nullstellensatz provides a fundamental correspondence between ideals of polynomial rings and algebraic sets. Using the Nullstellensatz and related results, mathematicians have established a strong correspondence between questions on algebraic sets and questions of ring theory. This correspondence is the specificity of algebraic geometry among the other subareas of geometry.

7.1 Introduction and definitions

An *affine variety* over an algebraically closed field is conceptually the easiest type of variety to define, which will be done in this section. Next, one can define projective and quasi-projective varieties in a similar way. The most general definition of a variety is obtained by patching together smaller quasi-projective varieties. It is not obvious that one can construct genuinely new examples of varieties in this way, but Nagata gave an example of such a new variety in the 1950s.

7.1.1 Affine varieties

Main article: Affine variety

Let k be an algebraically closed field and let $\mathbf{A}^n$ be an affine *n*-space over k. The polynomials *f* in the ring *k*[x_1, ..., *xn*] can be viewed as k-valued functions on $\mathbf{A}^n$ by evaluating *f* at the points in $\mathbf{A}^n$, i.e. by choosing values in *A* for each *xi*. For each set *S* of polynomials in *k*[x_1, ..., *xn*], define the zero-locus *Z*(*S*) to be the set of points in $\mathbf{A}^n$ on which the functions in *S* simultaneously vanish, that is to say

$$Z(S) = \{x \in \mathbf{A}^n \mid f(x) = 0 \text{ all for } f \in S\}.$$

A subset *V* of $\mathbf{A}^n$ is called an **affine algebraic set** if *V* = *Z*(*S*) for some *S*.[1]:2 A nonempty affine algebraic set *V* is called **irreducible** if it cannot be written as the union of two proper algebraic subsets.[1]:3 An irreducible affine algebraic set is also called an **affine variety**.[1]:3 (Many authors use the phrase *affine variety* to refer to any affine algebraic set, irreducible or not[note 1])

Affine varieties can be given a natural topology by declaring the closed sets to be precisely the affine algebraic sets. This topology is called the Zariski topology.[1]:2

Given a subset *V* of $\mathbf{A}^n$, we define *I*(*V*) to be the ideal of all polynomial functions vanishing on *V*:

$$I(V) = \{f \in k[x_1, \cdots, x_n] \mid f(x) = 0 \text{ all for } x \in V\}.$$

For any affine algebraic set *V*, the **coordinate ring** or **structure ring** of *V* is the quotient of the polynomial ring by this ideal.[1]:4

7.1.2 Projective varieties and quasi-projective varieties

Main articles: Projective variety and Quasi-projective variety

Let k be an algebraically closed field and let $\mathbf{P}^n$ be the projective n-space over k. Let f in $k[x_0, ..., xn]$ be a homogeneous polynomial of degree d. It is not well-defined to evaluate f on points in $\mathbf{P}^n$ in homogeneous coordinates. However, because f is homogeneous, $f(\lambda x_0, ..., \lambda xn) = \lambda^d f(x_0, ..., xn)$, it *does* make sense to ask whether f vanishes at a point $[x_0 : ... : xn]$. For each set S of homogeneous polynomials, define the zero-locus of S to be the set of points in $\mathbf{P}^n$ on which the functions in S vanish:

$$Z(S) = \{x \in \mathbf{P}^n \mid f(x) = 0 \text{ all for } f \in S\}.$$

A subset V of $\mathbf{P}^n$ is called a **projective algebraic set** if $V = Z(S)$ for some S.[1]:9 An irreducible projective algebraic set is called a **projective variety**.[1]:10

Projective varieties are also equipped with the Zariski topology by declaring all algebraic sets to be closed.

Given a subset V of $\mathbf{P}^n$, let $I(V)$ be the ideal generated by all homogeneous polynomials vanishing on V. For any projective algebraic set V, the **coordinate ring** of V is the quotient of the polynomial ring by this ideal.[1]:10

A **quasi-projective variety** is a Zariski open subset of a projective variety. Notice that every affine variety is quasi-projective.[2] Notice also that the complement of an algebraic set in an affine variety is a quasi-projective variety; in the context of affine varieties, such a quasi-projective variety is usually not called a variety but a constructible set.

7.1.3 Abstract varieties

In classical algebraic geometry, all varieties were by definition quasiprojective varieties, meaning that they were open subvarieties of closed subvarieties of projective space. For example, in Chapter 1 of Hartshorne a *variety* over an algebraically closed field is defined to be a quasi-projective variety,[1]:15 but from Chapter 2 onwards, the term **variety** (also called an **abstract variety**) refers to a more general object, which locally is a quasi-projective variety, but when viewed as a whole is not necessarily quasi-projective; i.e. it might not have an embedding into projective space.[1]:105 So classically the definition of an algebraic variety required an embedding into projective space, and this embedding was used to define the topology on the variety and the regular functions on the variety. The disadvantage of such a definition is that not all varieties come with natural embeddings into projective space. For example, under this definition, the product $\mathbf{P}^1 \times \mathbf{P}^1$ is not a variety until it is embedded into the projective space; this is usually done by the Segre embedding. However, any variety that admits one embedding into projective space admits many others by composing the embedding with the Veronese embedding. Consequently many notions that should be intrinsic, such as the concept of a regular function, are not obviously so.

The earliest successful attempt to define an algebraic variety abstractly, without an embedding, was made by André Weil. In his *Foundations of Algebraic Geometry*, Weil defined an abstract algebraic variety using valuations. Claude Chevalley made a definition of a scheme, which served a similar purpose, but was more general. However, it was Alexander Grothendieck's definition of a scheme that was both most general and found the most widespread acceptance. In Grothendieck's language, an abstract algebraic variety is usually defined to be an integral, separated scheme of finite type over an algebraically closed field,[note 2] although some authors drop the irreducibility or the reducedness or the separateness condition or allow the underlying field to be not algebraically closed.[note 3] Classical algebraic varieties are the quasiprojective integral separated finite type schemes over an algebraically closed field.

Existence of non-quasiprojective abstract algebraic varieties

One of the earliest examples of a non-quasiprojective algebraic variety were given by Nagata.[3] Nagata's example was not complete (the analog of compactness), but soon afterwards he found an algebraic surface that was complete and non-projective.[4] Since then other examples have been found.

7.2 Examples

7.2.1 Subvariety

A **subvariety** is a subset of a variety that is itself a variety (with respect to the structure induced from the ambient variety). For example, every open subset of a variety is a variety. See also closed immersion.

Hilbert's Nullstellensatz says that closed subvarieties of an affine or projective variety are in one-to-one correspondence with the prime ideals or homogeneous prime ideals of the coordinate ring of the variety.

7.2.2 Affine variety

Example 1

Let $k = \mathbf{C}$, and $\mathbf{A}^2$ be the two-dimensional affine space over $\mathbf{C}$. Polynomials in the ring $\mathbf{C}[x, y]$ can be viewed as complex valued functions on $\mathbf{A}^2$ by evaluating at the points in $\mathbf{A}^2$. Let subset S of $\mathbf{C}[x, y]$ contain a single element $f(x, y)$:

$$f(x, y) = x + y - 1.$$

The zero-locus of $f(x, y)$ is the set of points in $\mathbf{A}^2$ on which this function vanishes: it is the set of all pairs of complex numbers (x, y) such that $y = 1 - x$, commonly known as a line. This is the set $Z(f)$:

$$Z(f) = \{(x, 1 - x) \in \mathbf{C}^2\}.$$

Thus the subset $V = Z(f)$ of $\mathbf{A}^2$ is an algebraic set. The set V is not empty. It is irreducible, as it cannot be written as the union of two proper algebraic subsets. Thus it is an affine algebraic variety.

Example 2

Let $k = \mathbf{C}$, and $\mathbf{A}^2$ be the two-dimensional affine space over $\mathbf{C}$. Polynomials in the ring $\mathbf{C}[x, y]$ can be viewed as complex valued functions on $\mathbf{A}^2$ by evaluating at the points in $\mathbf{A}^2$. Let subset S of $\mathbf{C}[x, y]$ contain a single element $g(x, y)$:

$$g(x, y) = x^2 + y^2 - 1.$$

The zero-locus of $g(x, y)$ is the set of points in $\mathbf{A}^2$ on which this function vanishes, that is the set of points (x,y) such that $x^2 + y^2 = 1$. As $g(x, y)$ is an absolutely irreducible polynomial, this is an algebraic variety. The set of its real points (that is the points for which x and y are real numbers), is known as the unit circle; this name is also often given to the whole variety.

Example 3

The following example is neither a hypersurface, nor a linear space, nor a single point. Let $\mathbf{A}^3$ be the three-dimensional affine space over $\mathbf{C}$. The set of points (x, x^2, x^3) for x in $\mathbf{C}$ is an algebraic variety, and more precisely an algebraic curve that is not contained in any plane.[note 4] It is the twisted cubic shown in the above figure. It may be defined by the equations

$$y - x^2 = 0$$
$$z - x^3 = 0$$

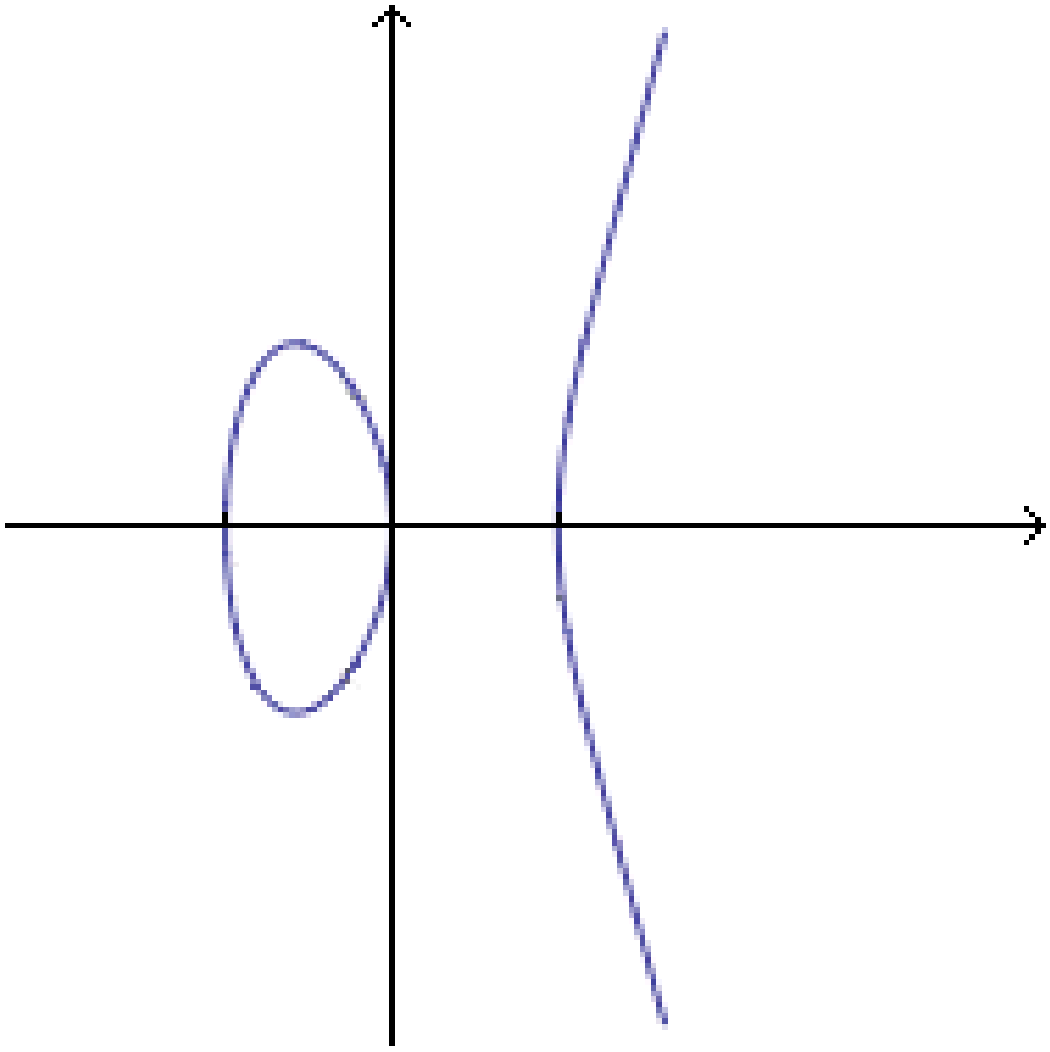
The fact that the set of the solutions of this system of equations is irreducible needs a proof. The simplest results from the fact that the projection $(x, y, z) \to (x, y)$ is injective on the set of the solutions and that its image is an irreducible plane curve.

For more difficult examples, a similar proof may always be given, but may imply a difficult computation: first a Gröbner basis computation to compute the dimension, followed by a random linear change of variables (not always needed); then a Gröbner basis computation for another monomial ordering to compute the projection and to prove that it is injective, and finally a polynomial factorization to prove the irreducibility of the image.

7.2.3 Projective variety

A projective variety is a closed subvariety of a projective space. That is, it is the zero locus of a set of homogeneous polynomials that generate a prime ideal.

Example 1



The affine plane curve $y^2 = x^3 - x$. *The corresponding projective curve is called an elliptic curve.*

A plane projective curve is the zero locus of an irreducible homogeneous polynomial in three indeterminates. The projective line $\mathbf{P}^1$ is an example of a projective curve, since it appears as the zero locus of one homogeneous coordinate in the projective plane. For another example, first consider the affine cubic curve:

$$y^2 = x^3 - x$$

in the 2-dimensional affine space (over a field of characteristic not two). It has the associated cubic homogeneous polynomial equation:

$$y^2z = x^3 - xz^2$$

which defines a curve in $\mathbf{P}^2$ called an elliptic curve. The curve has genus one (genus formula); in particular, it is not isomorphic to the projective line $\mathbf{P}^1$, which has genus zero. Using genus to distinguish curves is very basic: in fact, the genus is the first invariant one uses to classify curves (see also the construction of moduli of algebraic curves).

Example 2

Let V be a finite-dimensional vector space. The Grassmannian variety $Gn(V)$ is the set of all n-dimensional subspaces of V. It is a projective variety: it is embedded into a projective space via the Plücker embedding:

$$G_n(V) \hookrightarrow \mathbf{P}(\wedge^n V),\ \langle b_1, \dots, b_n \rangle \mapsto [b_1 \wedge \cdots \wedge b_n]$$

where *bi* are any set of linearly independent vectors in V, $\wedge^n V$ is the n-th exterior power of V and the bracket $[w]$ means the line spanned by the nonzero vector w.

The Grassmannian variety comes with a natural vector bundle (or locally free sheaf to be precise) called the tautological bundle, which is important in the study of characteristic classes such as Chern classes.

7.3 Basic results

- An affine algebraic set V is a variety if and only if $I(V)$ is a prime ideal; equivalently, V is a variety if and only if its coordinate ring is an integral domain.[5]:52[1]:4
- Every nonempty affine algebraic set may be written uniquely as a finite union of algebraic varieties (where none of the varieties in the decomposition is a subvariety of any other).[1]:5
- The **dimension** of a variety may be defined in various equivalent ways. See Dimension of an algebraic variety for details.

7.4 Isomorphism of algebraic varieties

See also: morphism of varieties

Let V_1, V_2 be algebraic varieties. We say V_1 and V_2 are isomorphic, and write $V_1 \cong V_2$, if there are regular maps $\varphi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that the compositions $\psi \circ \varphi$ and $\varphi \circ \psi$ are the identity maps on V_1 and V_2 respectively.

7.5 Discussion and generalizations

The basic definitions and facts above enable one to do classical algebraic geometry. To be able to do more — for example, to deal with varieties over fields that are not algebraically closed — some foundational changes are required. The modern notion of a variety is considerably more abstract than the one above, though equivalent in the case of varieties over algebraically closed fields. An *abstract algebraic variety* is a particular kind of scheme; the generalization to schemes on the geometric side enables an extension of the correspondence described above to a wider class of rings. A scheme is a locally ringed space such that every point has a neighbourhood that, as a locally ringed space, is isomorphic to a spectrum of a ring. Basically, a variety over k is a scheme whose structure sheaf is a sheaf of k-algebras with the property that the rings R that occur above are all integral domains and are all finitely generated k-algebras, that is to say, they are quotients of polynomial algebras by prime ideals.

This definition works over any field k. It allows you to glue affine varieties (along common open sets) without worrying whether the resulting object can be put into some projective space. This also leads to difficulties since one can introduce somewhat pathological objects, e.g. an affine line with zero doubled. Such objects are usually not considered varieties, and are eliminated by requiring the schemes underlying a variety to be *separated*. (Strictly speaking, there is also a third condition, namely, that one needs only finitely many affine patches in the definition above.)

Some modern researchers also remove the restriction on a variety having integral domain affine charts, and when speaking of a variety only require that the affine charts have trivial nilradical.

A complete variety is a variety such that any map from an open subset of a nonsingular curve into it can be extended uniquely to the whole curve. Every projective variety is complete, but not *vice versa*.

These varieties have been called 'varieties in the sense of Serre', since Serre's foundational paper FAC on sheaf cohomology was written for them. They remain typical objects to start studying in algebraic geometry, even if more general objects are also used in an auxiliary way.

One way that leads to generalisations is to allow reducible algebraic sets (and fields k that aren't algebraically closed), so the rings R may not be integral domains. A more significant modification is to allow nilpotents in the sheaf of rings. A nilpotent in a field must be 0: these if allowed in coordinate rings aren't seen as *coordinate functions*.

From the categorical point of view, nilpotents must be allowed, in order to have finite limits of varieties (to get fiber products). Geometrically this says that fibres of good mappings may have 'infinitesimal' structure. In the theory of schemes of Grothendieck these points are all reconciled: but the general *scheme* is far from having the immediate geometric content of a *variety*.

There are further generalizations called algebraic spaces and stacks.

7.6 Algebraic manifolds

Main article: Algebraic manifold

An algebraic manifold is an algebraic variety that is also an m-dimensional manifold, and hence every sufficiently small local patch is isomorphic to k^m. Equivalently, the variety is smooth (free from singular points). When k is the real numbers, **R**, algebraic manifolds are called Nash manifolds. Algebraic manifolds can be defined as the zero set of a finite collection of analytic algebraic functions. Projective algebraic manifolds are an equivalent definition for projective varieties. The Riemann sphere is one example.

7.7 See also

- Variety (disambiguation) — listing also several mathematical meanings
- Function field of an algebraic variety
- Dimension of an algebraic variety
- Singular point of an algebraic variety
- Birational geometry
- Abelian variety
- Motive
- Scheme
- Analytic variety
- Zariski–Riemann space
- Semi-algebraic set

7.8 Footnotes

[1] Hartshorne, p.xv, notes that his choice is not conventional; see for example, Harris, p.3

[2] Hartshorne 1976, pp. 104–105

[3] Liu, Qing. *Algebraic Geometry and Arithmetic Curves*, p. 55 Definition 2.3.47, and p. 88 Example 3.2.3

[4] Harris, p.9; that it is irreducible is stated as an exercise in Hartshorne p.7

7.9 References

[1] Hartshorne, Robin (1977). *Algebraic Geometry*. Springer-Verlag. ISBN 0-387-90244-9.

[2] Hartshorne, Exercise I.2.9, p.12

[3] Nagata, Masayoshi (1956), "On the imbedding problem of abstract varieties in projective varieties", *Memoirs of the College of Science, University of Kyoto. Series A: Mathematics* **30**: 71–82, MR 0088035

[4] Nagata, Masayoshi (1957), "On the imbeddings of abstract surfaces in projective varieties", *Memoirs of the College of Science, University of Kyoto. Series A: Mathematics* **30**: 231–235, MR 0094358

[5] Harris, Joe (1992). *Algebraic Geometry - A first course*. Springer-Verlag. ISBN 0-387-97716-3.

- Cox, David; John Little; Don O'Shea (1997). *Ideals, Varieties, and Algorithms* (second ed.). Springer-Verlag. ISBN 0-387-94680-2.
- Eisenbud, David (1999). *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag. ISBN 0-387-94269-6.
- Milne, James S. (2008). "Algebraic Geometry". Retrieved 2009-09-01.

This article incorporates material from Isomorphism of varieties on PlanetMath, which is licensed under the Creative Commons Attribution/Share-Alike License.

Chapter 8

All one polynomial

An **all one polynomial** (AOP) is a polynomial in which all coefficients are one. Over the finite field of order two, conditions for the AOP to be irreducible are known, which allow this polynomial to be used to define efficient algorithms and circuits for multiplication in finite fields of characteristic two.[1] The AOP is a 1-equally spaced polynomial.[2]

8.1 Definition

An AOP of degree m has all terms from x^m to x^0 with coefficients of 1, and can be written as

$$AOP_m(x) = \sum_{i=0}^{m} x^i$$

or

$$AOP_m(x) = x^m + x^{m-1} + \cdots + x + 1$$

or

$$AOP_m(x) = \frac{x^{m+1} - 1}{x - 1}$$

thus the roots of the **all one polynomial** of degree m are all (m+1)th roots of unity other than unity itself.

8.2 Properties

Over GF(2) the AOP has many interesting properties, including:

- The Hamming weight of the AOP is m + 1, the maximum possible for its degree[3]
- The AOP is irreducible if and only if m + 1 is prime and 2 is a primitive root modulo m + 1[1]
- The only AOP that is a primitive polynomial is x^2 + x + 1.

Despite the fact that the Hamming weight is large, because of the ease of representation and other improvements there are efficient implementations in areas such as coding theory and cryptography.[1]

Over $\mathbb{Q}$, the AOP is irreducible whenever m + *1* is prime p, and therefore in these cases, the *p*th cyclotomic polynomial.[4]

8.3 References

[1] Cohen, Henri; Frey, Gerhard; Avanzi, Roberto; Doche, Christophe; Lange, Tanja; Nguyen, Kim; Vercauteren, Frederik (2005), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Mathematics and Its Applications, CRC Press, p. 215, ISBN 9781420034981.

[2] Itoh, Toshiya; Tsujii, Shigeo (1989), "Structure of parallel multipliers for a class of fields GF(2^m)", *Information and Computation* **83** (1): 21–40, doi:10.1016/0890-5401(89)90045-X.

[3] Reyhani-Masoleh, Arash; Hasan, M. Anwar (2003), "On low complexity bit parallel polynomial basis multipliers", *Cryptographic Hardware and Embedded Systems - CHES 2003*, Lecture Notes in Computer Science **2779**, Springer, pp. 189–202, doi:10.1007/978-3-540-45238-6_16.

[4] Sugimura, Tatsuo; Suetugu, Yasunori (1991), "Considerations on irreducible cyclotomic polynomials", *Electronics and Communications in Japan* **74** (4): 106–113, doi:10.1002/ecjc.4430740412, MR 1136200.

8.4 External links

- all one polynomial at PlanetMath.org.

Chapter 9

Almost linear hash function

An **almost linear function** is a function h such that, for every inputs x and y, one of the following two equations hold:

1. $h(x+y) = h(x) + h(y)$
2. $h(x+y) = h(x) + h(y) + 1$.

If equation 1 always holds, then h is a linear function. But if in some cases equation 2 holds, then h is almost linear.

The almost-linearity concept is mainly used with hash functions. A hash function can be used to map a large domain (e.g. the numbers between 0 and $M-1$) to a much smaller domain (e.g. the numbers between 0 and $m-1$, where $m < M$). It is easy to create a linear hash function, e.g. for every constant a, the following function is linear:

$$h(x) = ax \bmod m$$

However, this family of functions is missing some other features that are required from a hash function, e.g. it is not universal. In contrast, the following function is both universal and almost linear, for every odd constant a and for every M, m which are powers of 2:[1][2]

$$h(x) = (ax \mod M) \div (M/m)$$

where $\div$ means integer division (taking only the integral part of the result and discarding the remainder).

For example, if $M = 64$, $m = 16$ and $a = 1$:

$$h(x) = (x \bmod 64) \div 4$$

For every x, y:

$$x = 4(x \div 4) + x \bmod 4$$

$$y = 4(y \div 4) + y \bmod 4$$

$$x + y = 4(x \div 4 + y \div 4) + (x \bmod 4) + (y \bmod 4)$$

Hence, if $(x \bmod 4) + (y \bmod 4) < 4$, then it is discarded in the integer division by 4, and we get:

$$h(x+y) = x \div 4 + y \div 4 = h(x) + h(y)$$

The only other option is that $4 \leq (x \bmod 4) + (y \bmod 4) < 8$. In this case, dividing it by 4 gives an integer part of 1, and we get:

$$h(x + y) = x \div 4 + y \div 4 + 1 = h(x) + h(y) + 1$$

This proves that *h* is an almost-linear function.

9.1 References

[1] Dietzfelbinger, M.; Hagerup, T.; Katajainen, J.; Penttonen, M. (1997). "A Reliable Randomized Algorithm for the Closest-Pair Problem". *Journal of Algorithms* **25**: 19. doi:10.1006/jagm.1997.0873.

[2] Kopelowitz, Tsvi; Pettie, Seth; Porat, Ely (2014). "3SUM Hardness in (Dynamic) Data Structures". arXiv:1407.6756 [cs.DS].

Chapter 10

Alternating polynomial

In algebra, an **alternating polynomial** is a polynomial $f(x_1, \ldots, x_n)$ such that if one switches any two of the variables, the polynomial changes sign:

$$f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = -f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n).$$

Equivalently, if one permutes the variables, the polynomial changes in value by the sign of the permutation:

$$f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right) = \operatorname{sgn}(\sigma) f(x_1, \ldots, x_n).$$

More generally, a polynomial $f(x_1, \ldots, x_n, y_1, \ldots, y_t)$ is said to be *alternating in* $x_1, \ldots, x_n$ if it changes sign if one switches any two of the x_i , leaving the y_j fixed.[1]

10.1 Relation to symmetric polynomials

Products of symmetric and alternating polynomials (in the same variables $x_1, \ldots, x_n$) behave thus:

- the product of two symmetric polynomials is symmetric,
- the product of a symmetric polynomial and an alternating polynomial is alternating, and
- the product of two alternating polynomials is symmetric.

This is exactly the addition table for parity, with "symmetric" corresponding to "even" and "alternating" corresponding to "odd". Thus, the direct sum of the spaces of symmetric and alternating polynomials forms a superalgebra (a $\mathbf{Z}_2$ -graded algebra), where the symmetric polynomials are the even part, and the alternating polynomials are the odd part. This grading is unrelated to the grading of polynomials by degree.

In particular, alternating polynomials form a module over the algebra of symmetric polynomials (the odd part of a superalgebra is a module over the even part); in fact it is a free module of rank 1, with as generator the Vandermonde polynomial in *n* variables.

If the characteristic of the coefficient ring is 2, there is no difference between the two concepts: the alternating polynomials are precisely the symmetric polynomials.

10.2 Vandermonde polynomial

Main article: Vandermonde polynomial

The basic alternating polynomial is the Vandermonde polynomial:

$$v_n = \prod_{1 \le i < j \le n} (x_j - x_i).$$

This is clearly alternating, as switching two variables changes the sign of one term and does not change the others.[2]

The alternating polynomials are exactly the Vandermonde polynomial times a symmetric polynomial: $a = v_n \cdot s$ where s is symmetric. This is because:

- v_n is a factor of every alternating polynomial: $(x_j - x_i)$ is a factor of every alternating polynomial, as if $x_i = x_j$, the polynomial is zero (since switching them does not change the polynomial, we get

  $f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = -f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n),$
  so $(x_j - x_i)$ is a factor), and thus v_n is a factor.

- an alternating polynomial times a symmetric polynomial is an alternating polynomial; thus all multiples of v_n are alternating polynomials

Conversely, the ratio of two alternating polynomials is a symmetric function, possibly rational (not necessarily a polynomial), though the ratio of an alternating polynomial over the Vandermonde polynomial is a polynomial. Schur polynomials are defined in this way, as an alternating polynomial divided by the Vandermonde polynomial.

10.2.1 Ring structure

Thus, denoting the ring of symmetric polynomials by Λn, the ring of symmetric and alternating polynomials is $\Lambda_n[v_n]$, or more precisely $\Lambda_n[v_n]/\langle v_n^2 - \Delta \rangle$, where $\Delta = v_n^2$ is a symmetric polynomial, the discriminant.

That is, the ring of symmetric and alternating polynomials is a quadratic extension of the ring of symmetric polynomials, where one has adjoined a square root of the discriminant.

Alternatively, it is:

$$R[e_1, \ldots, e_n, v_n]/\langle v_n^2 - \Delta \rangle.$$

If 2 is not invertible, the situation is somewhat different, and one must use a different polynomial W_n , and obtains a different relation; see Romagny.

10.3 Representation theory

For more details on this topic, see Representation theory of the symmetric group.

From the perspective of representation theory, the symmetric and alternating polynomials are subrepresentations of the action of the symmetric group on *n* letters on the polynomial ring in *n* variables. (Formally, the symmetric group acts on *n* letters, and thus acts on derived objects, particularly free objects on *n* letters, such as the ring of polynomials.)

The symmetric group has two 1-dimensional representations: the trivial representation and the sign representation. The symmetric polynomials are the trivial representation, and the alternating polynomials are the sign representation. Formally, the scalar span of any symmetric (resp., alternating) polynomial is a trivial (resp., sign) representation of the symmetric group, and multiplying the polynomials tensors the representations.

In characteristic 2, these are not distinct representations, and the analysis is more complicated.

If $n > 2$, there are also other subrepresentations of the action of the symmetric group on the ring of polynomials, as discussed in representation theory of the symmetric group.

10.4 Unstable

Alternating polynomials are an unstable phenomenon (in the language of stable homotopy theory): the ring of symmetric polynomials in *n* variables can be obtained from the ring of symmetric polynomials in arbitrarily many variables by evaluating all variables above x_n to zero: symmetric polynomials are thus *stable* or *compatibly defined.* However, this is not the case for alternating polynomials, in particular the Vandermonde polynomial.

10.5 See also

- Symmetric polynomial
- Euler class

10.6 Notes

[1] *Polynomial Identities and Asymptotic Methods,* p. 12

[2] Rather, it only rearranges the other terms: for $n = 3$, switching x_1 and x_2 changes $(x_2 - x_1)$ to $(x_1 - x_2) = -(x_2 - x_1)$, and exchanges $(x_3 - x_1)$ with $(x_3 - x_2)$, but does not change their sign.

10.7 References

- A. Giambruno, Mikhail Zaicev, *Polynomial Identities and Asymptotic Methods,* AMS Bookstore, 2005 ISBN 978-0-8218-3829-7, pp. 352
- The fundamental theorem of alternating functions, by Matthieu Romagny, September 15, 2005

Chapter 11

Angelescu polynomials

In mathematics, **Angelescu polynomials** $\pi n(x)$ are generalizations of the Laguerre polynomials introduced by Angelescu (1938) given by the generating function

$$\phi\left(\frac{t}{1-t}\right)\exp\left(-\frac{xt}{1-t}\right)=\sum_{n=0}^{\infty}\pi_n(x)t^n$$

Boas & Buck (1958, p.41)

11.1 See also

11.2 References

- Angelescu, A. (1938), "Sur certains polynomes généralisant les polynomes de Laguerre.", *C. R. Acad. Sci. Roumanie* (in French) **2**: 199–201, JFM 64.0328.01
- Boas, Ralph P.; Buck, R. Creighton (1958), *Polynomial expansions of analytic functions*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge. **19**, Berlin, New York: Springer-Verlag, MR 0094466

Chapter 12

Appell sequence

In mathematics, an **Appell sequence**, named after Paul Émile Appell, is any polynomial sequence $\{pn(x)\}n = 0, 1, 2, \ldots$ satisfying the identity

$$\frac{d}{dx}p_n(x) = np_{n-1}(x),$$

and in which $p_0(x)$ is a non-zero constant.

Among the most notable Appell sequences besides the trivial example $\{ x^n \}$ are the Hermite polynomials, the Bernoulli polynomials, and the Euler polynomials. Every Appell sequence is a Sheffer sequence, but most Sheffer sequences are not Appell sequences.

12.1 Equivalent characterizations of Appell sequences

The following conditions on polynomial sequences can easily be seen to be equivalent:

- For $n = 1, 2, 3, \ldots$,

  $$\frac{d}{dx}p_n(x) = np_{n-1}(x)$$

  and $p_0(x)$ is a non-zero constant;

- For some sequence $\{cn\}n = 0, 1, 2, \ldots$ of scalars with $c_0 \neq 0$,

  $$p_n(x) = \sum_{k=0}^{n} \binom{n}{k} c_k x^{n-k};$$

- For the same sequence of scalars,

  $$p_n(x) = \left(\sum_{k=0}^{\infty} \frac{c_k}{k!} D^k \right) x^n,$$

  where

$$D = \frac{d}{dx};$$

- For $n = 0, 1, 2, ...,$

$$p_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} p_k(x) y^{n-k}.$$

12.2 Recursion formula

Suppose

$$p_n(x) = \left(\sum_{k=0}^{\infty} \frac{c_k}{k!} D^k \right) x^n = Sx^n,$$

where the last equality is taken to define the linear operator S on the space of polynomials in x. Let

$$T = S^{-1} = \left(\sum_{k=0}^{\infty} \frac{c_k}{k!} D^k \right)^{-1} = \sum_{k=1}^{\infty} \frac{a_k}{k!} D^k$$

be the inverse operator, the coefficients ak being those of the usual reciprocal of a formal power series, so that

$$Tp_n(x) = x^n.$$

In the conventions of the umbral calculus, one often treats this formal power series T as representing the Appell sequence $\{pn\}$. One can define

$$\log T = \log \left(\sum_{k=0}^{\infty} \frac{a_k}{k!} D^k \right)$$

by using the usual power series expansion of the log(1 + x) and the usual definition of composition of formal power series. Then we have

$$p_{n+1}(x) = (x - (\log T)')p_n(x).$$

(This formal differentiation of a power series in the differential operator D is an instance of Pincherle differentiation.)

In the case of Hermite polynomials, this reduces to the conventional recursion formula for that sequence.

12.3 Subgroup of the Sheffer polynomials

The set of all Appell sequences is closed under the operation of umbral composition of polynomial sequences, defined as follows. Suppose { pn(x) : n = 0, 1, 2, 3, ... } and { qn(x) : n = 0, 1, 2, 3, ... } are polynomial sequences, given by

$$p_n(x) = \sum_{k=0}^{n} a_{n,k} x^k \text{ and } q_n(x) = \sum_{k=0}^{n} b_{n,k} x^k.$$

Then the umbral composition $p \circ q$ is the polynomial sequence whose nth term is

$$(p_n \circ q)(x) = \sum_{k=0}^{n} a_{n,k} q_k(x) = \sum_{0 \le k \le \ell \le n} a_{n,k} b_{k,\ell} x^\ell$$

(the subscript n appears in p_n, since this is the n term of that sequence, but not in q, since this refers to the sequence as a whole rather than one of its terms).

Under this operation, the set of all Sheffer sequences is a non-abelian group, but the set of all Appell sequences is an abelian subgroup. That it is abelian can be seen by considering the fact that every Appell sequence is of the form

$$p_n(x) = \left(\sum_{k=0}^{\infty} \frac{c_k}{k!} D^k \right) x^n,$$

and that umbral composition of Appell sequences corresponds to multiplication of these formal power series in the operator D.

12.4 Different convention

Another convention followed by some authors (see *Chihara*) defines this concept in a different way, conflicting with Appell's original definition, by using the identity

$$\frac{d}{dx} p_n(x) = p_{n-1}(x)$$

instead.

12.5 See also

- Sheffer sequence
- Umbral calculus
- Generalized Appell polynomials
- Wick product

12.6 References

- Appell, Paul (1880). "Sur une classe de polynômes". *Annales scientifiques de l'École Normale Supérieure 2me série* **9**: 119–144.
- Roman, Steven; Rota, Gian-Carlo (1978). "The Umbral Calculus". *Advances in Mathematics* **27** (2): 95–188. doi:10.1016/0001-8708(78)90087-7..
- Rota, Gian-Carlo; Kahaner, D.; Odlyzko, Andrew (1973). "Finite Operator Calculus". *Journal of Mathematical Analysis and its Applications* **42** (3): 685–760. doi:10.1016/0022-247X(73)90172-8. Reprinted in the book with the same title, Academic Press, New York, 1975.
- Steven Roman. *The Umbral Calculus.* Dover Publications.
- Theodore Seio Chihara (1978). *An Introduction to Orthogonal Polynomials.* Gordon and Breach, New York. ISBN 0-677-04150-0.

12.7 External links

- Hazewinkel, Michiel, ed. (2001), "Appell polynomials", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Appell Sequence at MathWorld

Chapter 13

Bell polynomials

For a different family of polynomials $B_n(x)$ occasionally called Bell polynomials, see Touchard polynomials.

In combinatorial mathematics, the **Bell polynomials**, named in honor of Eric Temple Bell, are a triangular array of polynomials given by

$$B_{n,k}(x_1, x_2, \ldots, x_{n-k+1})$$

$$= \sum \frac{n!}{j_1! j_2! \cdots j_{n-k+1}!} \left(\frac{x_1}{1!}\right)^{j_1} \left(\frac{x_2}{2!}\right)^{j_2} \cdots \left(\frac{x_{n-k+1}}{(n-k+1)!}\right)^{j_{n-k+1}},$$

where the sum is taken over all sequences $j_1, j_2, j_3, \ldots, j_{n-k+1}$ of non-negative integers such that

$$j_1 + j_2 + \cdots + j_{n-k+1} = k \quad \text{and} \quad j_1 + 2j_2 + 3j_3 + \cdots + (n-k+1)j_{n-k+1} = n.$$

13.1 Complete Bell polynomials

The sum

$$B_n(x_1, \ldots, x_n) = \sum_{k=1}^{n} B_{n,k}(x_1, x_2, \ldots, x_{n-k+1})$$

is sometimes called the *n*th **complete Bell polynomial**. In order to contrast them with complete Bell polynomials, the polynomials *Bn,k* are sometimes called *partial* or *incomplete* Bell polynomials.

The complete Bell polynomials satisfy the following identity

$$B_n(x_1,\ldots,x_n) = \det\begin{bmatrix} x_1 & \binom{n-1}{1}x_2 & \binom{n-1}{2}x_3 & \binom{n-1}{3}x_4 & \binom{n-1}{4}x_5 & \cdots & \cdots & x_n \\ -1 & x_1 & \binom{n-2}{1}x_2 & \binom{n-2}{2}x_3 & \binom{n-2}{3}x_4 & \cdots & \cdots & x_{n-1} \\ 0 & -1 & x_1 & \binom{n-3}{1}x_2 & \binom{n-3}{2}x_3 & \cdots & \cdots & x_{n-2} \\ 0 & 0 & -1 & x_1 & \binom{n-4}{1}x_2 & \cdots & \cdots & x_{n-3} \\ 0 & 0 & 0 & -1 & x_1 & \cdots & \cdots & x_{n-4} \\ 0 & 0 & 0 & 0 & -1 & \cdots & \cdots & x_{n-5} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & -1 & x_1 \end{bmatrix}.$$

13.2 Combinatorial meaning

If the integer *n* is partitioned into a sum in which "1" appears j_1 times, "2" appears j_2 times, and so on, then the number of partitions of a set of size *n* that collapse to that partition of the integer *n* when the members of the set become indistinguishable is the corresponding coefficient in the polynomial.

13.2.1 Examples

For example, we have

$$B_{6,2}(x_1,x_2,x_3,x_4,x_5) = 6x_5x_1 + 15x_4x_2 + 10x_3^2$$

because there are

6 ways to partition a set of 6 as 5 + 1,
15 ways to partition a set of 6 as 4 + 2, and
10 ways to partition a set of 6 as 3 + 3.

Similarly,

$$B_{6,3}(x_1,x_2,x_3,x_4) = 15x_4x_1^2 + 60x_3x_2x_1 + 15x_2^3$$

because there are

15 ways to partition a set of 6 as 4 + 1 + 1,
60 ways to partition a set of 6 as 3 + 2 + 1, and
15 ways to partition a set of 6 as 2 + 2 + 2.

13.3 Properties

- $B_{n,k}(1!,2!,\ldots,(n-k+1)!) = \binom{n}{k}\binom{n-1}{k-1}(n-k)!$

13.3.1 Stirling numbers and Bell numbers

The value of the Bell polynomial *Bn,k*(x_1,x_2,...) on the sequence of factorials equals an unsigned Stirling number of the first kind:

$$B_{n,k}(0!, 1!, \ldots, (n-k)!) = c(n,k) = \begin{bmatrix} n \\ k \end{bmatrix}.$$

The value of the Bell polynomial *Bn,k*(x_1,x_2,...) on the sequence of ones equals a Stirling number of the second kind:

$$B_{n,k}(1, 1, \ldots, 1) = S(n,k) = \begin{Bmatrix} n \\ k \end{Bmatrix}.$$

The sum of these values gives the value of the complete Bell polynomial on the sequence of ones:

$$B_n(1, 1, \ldots, 1) = \sum_{k=1}^{n} B_{n,k}(1, 1, \ldots, 1) = \sum_{k=1}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix},$$

which is the *n*th Bell number.

13.3.2 Touchard polynomials

Main article: Touchard polynomials

Touchard polynomial $T_n(x) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \cdot x^k$ can be expressed as the value of the complete Bell polynomial on all arguments being x:

$$T_n(x) = B_n(x, x, \ldots, x).$$

13.3.3 Convolution identity

For sequences *xn*, *yn*, *n* = 1, 2, ..., define a sort of convolution by:

$$(x \diamondsuit y)_n = \sum_{j=1}^{n-1} \binom{n}{j} x_j y_{n-j}$$

Note that the bounds of summation are 1 and *n* − 1, not 0 and *n* .

Let $x_n^{k\diamondsuit}$ be the *n*th term of the sequence

$$\underbrace{x \diamondsuit \cdots \diamondsuit x}_{k \text{ factors}}.$$

Then

$$B_{n,k}(x_1, \ldots, x_{n-k+1}) = \frac{x_n^{k\diamondsuit}}{k!}.$$

For example, let us compute $B_{4,3}(x_1, x_2)$. We have

$$x = (x_1\ ,\ x_2\ ,\ x_3\ ,\ x_4\ , \ldots)$$

$x \diamondsuit x = (0,\ 2x_1^2\ ,\ 6x_1x_2\ ,\ 8x_1x_3 + 6x_2^2\ , \dots)$

$x \diamondsuit x \diamondsuit x = (0\ ,\ 0\ ,\ 6x_1^3\ ,\ 36x_1^2x_2\ , \dots)$

and thus,

$$B_{4,3}(x_1, x_2) = \frac{(x \diamondsuit x \diamondsuit x)_4}{3!} = 6x_1^2x_2.$$

13.4 Applications of Bell polynomials

13.4.1 Faà di Bruno's formula

Main article: Faà di Bruno's formula

Faà di Bruno's formula may be stated in terms of Bell polynomials as follows:

$$\frac{d^n}{dx^n} f(g(x)) = \sum_{k=1}^{n} f^{(k)}(g(x)) B_{n,k}\left(g'(x), g''(x), \dots, g^{(n-k+1)}(x)\right).$$

Similarly, a power-series version of Faà di Bruno's formula may be stated using Bell polynomials as follows. Suppose

$$f(x) = \sum_{n=1}^{\infty} \frac{a_n}{n!} x^n \qquad \text{and} \qquad g(x) = \sum_{n=1}^{\infty} \frac{b_n}{n!} x^n.$$

Then

$$g(f(x)) = \sum_{n=1}^{\infty} \frac{\sum_{k=1}^{n} b_k B_{n,k}(a_1, \dots, a_{n-k+1})}{n!} x^n.$$

In particular, the complete Bell polynomials appear in the exponential of a formal power series:

$$\exp\left(\sum_{n=1}^{\infty} \frac{a_n}{n!} x^n\right) = \sum_{n=0}^{\infty} \frac{B_n(a_1, \dots, a_n)}{n!} x^n.$$

13.4.2 Moments and cumulants

The sum

$$B_n(\kappa_1, \dots, \kappa_n) = \sum_{k=1}^{n} B_{n,k}(\kappa_1, \dots, \kappa_{n-k+1})$$

is the *n*th moment of a probability distribution whose first *n* cumulants are κ_1, ..., κn. In other words, the *n*th moment is the *n*th complete Bell polynomial evaluated at the first *n* cumulants.

13.4.3 Representation of polynomial sequences of binomial type

For any sequence a_1, a_2, …, *an* of scalars, let

$$p_n(x) = \sum_{k=1}^{n} B_{n,k}(a_1, \ldots, a_{n-k+1}) x^k.$$

Then this polynomial sequence is of binomial type, i.e. it satisfies the binomial identity

$$p_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} p_k(x) p_{n-k}(y).$$

Example: For $a_1 = \ldots = an = 1$, the polynomials $p_n(x)$ are called Touchard polynomials.

More generally, we have this result:

Theorem: All polynomial sequences of binomial type are of this form.

If we define a formal power series

$$h(x) = \sum_{k=1}^{\infty} \frac{a_k}{k!} x^k,$$

then for all *n*,

$$h^{-1}\left(\frac{d}{dx}\right) p_n(x) = n p_{n-1}(x).$$

13.5 Software

Bell polynomials are implemented in:

- Mathematica as BellY,
- Maple as IncompleteBellB,
- Sage as bell_polynomial.

13.6 See also

- Bell matrix
- Exponential formula

13.7 References

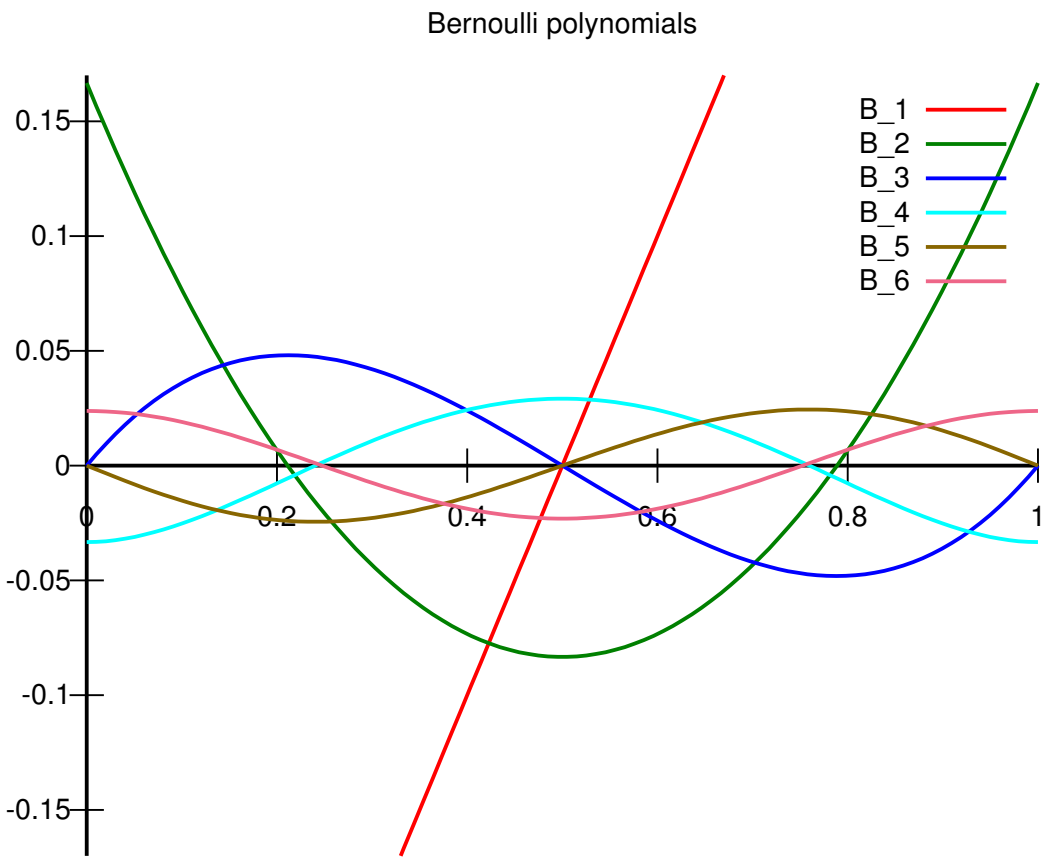
- Eric Temple Bell (1927–1928). "Partition Polynomials". *Annals of Mathematics* **29** (1/4): 38–46. doi:10.2307/1967979. JSTOR 1967979. MR 1502817.
- Louis Comtet (1974). *Advanced Combinatorics: The Art of Finite and Infinite Expansions*. Dordrecht, Holland / Boston, U.S.: Reidel Publishing Company.
- Steven Roman. The Umbral Calculus. Dover Publications.

- Vassily G. Voinov, Mikhail S. Nikulin (1994). "On power series, Bell polynomials, Hardy-Ramanujan-Rademacher problem and its statistical applications". *Kybernetika* **30** (3): 343–358. ISSN 0023-5954.
- Andrews, George E. (1998). *The Theory of Partitions*. Cambridge Mathematical Library (1st pbk ed.). Cambridge University Press. pp. 204–211. ISBN 0-521-63766-X.
- Silvia Noschese, Paolo E. Ricci (2003). "Differentiation of Multivariable Composite Functions and Bell Polynomials". *Journal of Computational Analysis and Applications* **5** (3): 333–340. doi:10.1023/A:1023227705558.
- Abbas, Moncef; Bouroubi, Sadek (2005). "On new identities for Bell's polynomial". *Disc. Math* (293): 5–10. doi:10.1016/j.disc.2004.08.023. MR 2136048.
- Khristo N. Boyadzhiev (2009). "Exponential Polynomials, Stirling Numbers, and Evaluation of Some Gamma Integrals". *Abstract and Applied Analysis* **2009**: Article ID 168672. doi:10.1155/2009/168672. (contains also elementary review of the concept Bell-polynomials)
- V. V. Kruchinin (2011). "Derivation of Bell Polynomials of the Second Kind". arXiv:1104.5065.
- Griffiths, Martin (2012). "Families of sequences from a class of multinomial sums". *Journal of Integer Sequences* **15**. MR 2872465.

Chapter 14

Bernoulli polynomials

In mathematics, the **Bernoulli polynomials** occur in the study of many special functions and in particular the Riemann zeta function and the Hurwitz zeta function. This is in large part because they are an Appell sequence, i.e. a Sheffer sequence for the ordinary derivative operator. Unlike orthogonal polynomials, the Bernoulli polynomials are remarkable in that the number of crossings of the x-axis in the unit interval does not go up as the degree of the polynomials goes up. In the limit of large degree, the Bernoulli polynomials, appropriately scaled, approach the sine and cosine functions.



Bernoulli polynomials

14.1 Representations

The Bernoulli polynomials *Bn* admit a variety of different representations. Which among them should be taken to be the definition may depend on one's purposes.

14.1.1 Explicit formula

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} b_{n-k} x^k,$$

for $n \geq 0$, where *bk* are the Bernoulli numbers.

14.1.2 Generating functions

The generating function for the Bernoulli polynomials is

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}.$$

The generating function for the Euler polynomials is

$$\frac{2e^{xt}}{e^t + 1} = \sum_{n=0}^{\infty} E_n(x) \frac{t^n}{n!}.$$

14.1.3 Representation by a differential operator

The Bernoulli polynomials are also given by

$$B_n(x) = \frac{D}{e^D - 1} x^n$$

where $D = d/dx$ is differentiation with respect to x and the fraction is expanded as a formal power series. It follows that

$$\int_a^x B_n(u)\, du = \frac{B_{n+1}(x) - B_{n+1}(a)}{n+1}\ .$$

cf. integrals below.

14.1.4 Representation by an integral operator

The Bernoulli polynomials are the unique polynomials determined by

$$\int_x^{x+1} B_n(u)\, du = x^n.$$

The integral transform

$$(Tf)(x) = \int_x^{x+1} f(u)\, du$$

on polynomials f, simply amounts to

$$(Tf)(x) = \frac{e^D - 1}{D} f(x) = \sum_{n=0}^{\infty} \frac{D^n}{(n+1)!} f(x)$$
$$= f(x) + \frac{f'(x)}{2} + \frac{f''(x)}{6} + \frac{f'''(x)}{24} + \cdots .$$

This can be used to produce the inversion formulae below.

14.2 Another explicit formula

An explicit formula for the Bernoulli polynomials is given by

$$B_m(x) = \sum_{n=0}^{m} \frac{1}{n+1} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (x+k)^m.$$

Note the remarkable similarity to the globally convergent series expression for the Hurwitz zeta function. Indeed, one has

$$B_n(x) = -n\zeta(1-n, x)$$

where $\zeta(s, q)$ is the Hurwitz zeta; thus, in a certain sense, the Hurwitz zeta generalizes the Bernoulli polynomials to non-integer values of n.

The inner sum may be understood to be the nth forward difference of x^m; that is,

$$\Delta^n x^m = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} (x+k)^m$$

where Δ is the forward difference operator. Thus, one may write

$$B_m(x) = \sum_{n=0}^{m} \frac{(-1)^n}{n+1} \Delta^n x^m.$$

This formula may be derived from an identity appearing above as follows. Since the forward difference operator Δ equals

$$\Delta = e^D - 1$$

where D is differentiation with respect to x, we have, from the Mercator series

$$\frac{D}{e^D - 1} = \frac{\log(\Delta + 1)}{\Delta} = \sum_{n=0}^{\infty} \frac{(-\Delta)^n}{n+1}.$$

As long as this operates on an mth-degree polynomial such as x^m, one may let n go from 0 only up to m.

An integral representation for the Bernoulli polynomials is given by the Nörlund–Rice integral, which follows from the expression as a finite difference.

An explicit formula for the Euler polynomials is given by

$$E_m(x) = \sum_{n=0}^{m} \frac{1}{2^n} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (x+k)^m \,.$$

This may also be written in terms of the Euler numbers *Ek* as

$$E_m(x) = \sum_{k=0}^{m} \binom{m}{k} \frac{E_k}{2^k} \left(x - \frac{1}{2}\right)^{m-k} \,.$$

14.3 Sums of *p*th powers

We have

$$\sum_{k=0}^{x} k^p = \frac{B_{p+1}(x+1) - B_{p+1}(0)}{p+1}$$

(assuming 0^0=1). See Faulhaber's formula for more on this.

14.4 The Bernoulli and Euler numbers

The Bernoulli numbers are given by $B_n = B_n(0)$.

This definition gives $\zeta(-n) = -\frac{1}{n+1} B_{n+1}$ for $n = 0, 1, 2 \cdots$.

An alternate convention defines the Bernoulli numbers as $B_n = B_n(1)$.

The two conventions differ only for $n = 0$ since $B_1(1) = 1/2 = -B_1(0)$.

The Euler numbers are given by $E_n = 2^n E_n(1/2)$.

14.5 Explicit expressions for low degrees

The first few Bernoulli polynomials are:

$$B_0(x) = 1$$

$$B_1(x) = x - 1/2$$

$$B_2(x) = x^2 - x + 1/6$$

$$B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$$

$$B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30}$$

$$B_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x$$

$$B_6(x) = x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 + \frac{1}{42}.$$

The first few Euler polynomials are

$$E_0(x) = 1$$

$$E_1(x) = x - 1/2$$
$$E_2(x) = x^2 - x$$
$$E_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{4}$$
$$E_4(x) = x^4 - 2x^3 + x$$
$$E_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{2}x^2 - \frac{1}{2}$$
$$E_6(x) = x^6 - 3x^5 + 5x^3 - 3x.$$

14.6 Maximum and minimum

At higher *n*, the amount of variation in *Bn*(*x*) between *x* = 0 and *x* = 1 gets large. For instance,

$$B_{16}(x) = x^{16} - 8x^{15} + 20x^{14} - \frac{182}{3}x^{12} + \frac{572}{3}x^{10} - 429x^8 + \frac{1820}{3}x^6 - \frac{1382}{3}x^4 + 140x^2 - \frac{3617}{510}$$

which shows that the value at *x* = 0 (and at *x* = 1) is −3617/510 ≈ −7.09, while at *x* = 1/2, the value is 118518239/3342336 ≈ +7.09. D.H. Lehmer[1] showed that the maximum value of *Bn*(*x*) between 0 and 1 obeys

$$M_n < \frac{2n!}{(2\pi)^n}$$

unless *n* is 2 modulo 4, in which case

$$M_n = \frac{2\zeta(n)n!}{(2\pi)^n}$$

(where $\zeta(x)$ is the Riemann zeta function), while the minimum obeys

$$m_n > \frac{-2n!}{(2\pi)^n}$$

unless *n* is 0 modulo 4, in which case

$$m_n = \frac{-2\zeta(n)n!}{(2\pi)^n}.$$

These limits are quite close to the actual maximum and minimum, and Lehmer gives more accurate limits as well.

14.7 Differences and derivatives

The Bernoulli and Euler polynomials obey many relations from umbral calculus:

$$\Delta B_n(x) = B_n(x+1) - B_n(x) = nx^{n-1},$$
$$\Delta E_n(x) = E_n(x+1) - E_n(x) = 2(x^n - E_n(x)).$$

(Δ is the forward difference operator).

These polynomial sequences are Appell sequences:

$$B_n'(x) = nB_{n-1}(x),$$
$$E_n'(x) = nE_{n-1}(x).$$

14.7.1 Translations

$$B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x) y^{n-k}$$

$$E_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} E_k(x) y^{n-k}$$

These identities are also equivalent to saying that these polynomial sequences are Appell sequences. (Hermite polynomials are another example.)

14.7.2 Symmetries

$$B_n(1-x) = (-1)^n B_n(x), \quad n \geq 0,$$

$$E_n(1-x) = (-1)^n E_n(x)$$

$$(-1)^n B_n(-x) = B_n(x) + n x^{n-1}$$

$$(-1)^n E_n(-x) = -E_n(x) + 2x^n$$

$$B_n\left(\frac{1}{2}\right) = \left(\frac{1}{2^{n-1}} - 1\right) B_n, \quad n \geq 0\text{below. theorems multiplication the from}$$

Zhi-Wei Sun and Hao Pan [2] established the following surprising symmetry relation: If $r + s + t = n$ and $x + y + z = 1$, then

$$r[s,t;x,y]_n + s[t,r;y,z]_n + t[r,s;z,x]_n = 0,$$

where

$$[s,t;x,y]_n = \sum_{k=0}^{n} (-1)^k \binom{s}{k} \binom{t}{n-k} B_{n-k}(x) B_k(y).$$

14.8 Fourier series

The Fourier series of the Bernoulli polynomials is also a Dirichlet series, given by the expansion

$$B_n(x) = -\frac{n!}{(2\pi i)^n} \sum_{k \neq 0} \frac{e^{2\pi i k x}}{k^n} = -2n! \sum_{k=1}^{\infty} \frac{\cos\left(2k\pi x - \frac{n\pi}{2}\right)}{(2k\pi)^n}.$$

Note the simple large n limit to suitably scaled trigonometric functions.

This is a special case of the analogous form for the Hurwitz zeta function

$$B_n(x) = -\Gamma(n+1) \sum_{k=1}^{\infty} \frac{\exp(2\pi i k x) + e^{i\pi n} \exp(2\pi i k (1-x))}{(2\pi i k)^n}.$$

This expansion is valid only for $0 \leq x \leq 1$ when $n \geq 2$ and is valid for $0 < x < 1$ when $n = 1$.

The Fourier series of the Euler polynomials may also be calculated. Defining the functions

$$C_\nu(x) = \sum_{k=0}^{\infty} \frac{\cos((2k+1)\pi x)}{(2k+1)^\nu}$$

and

$$S_\nu(x) = \sum_{k=0}^{\infty} \frac{\sin((2k+1)\pi x)}{(2k+1)^\nu}$$

for $\nu > 1$, the Euler polynomial has the Fourier series

$$C_{2n}(x) = \frac{(-1)^n}{4(2n-1)!}\pi^{2n} E_{2n-1}(x)$$

and

$$S_{2n+1}(x) = \frac{(-1)^n}{4(2n)!}\pi^{2n+1} E_{2n}(x).$$

Note that the C_ν and S_ν are odd and even, respectively:

$$C_\nu(x) = -C_\nu(1-x)$$

and

$$S_\nu(x) = S_\nu(1-x).$$

They are related to the Legendre chi function χ_ν as

$$C_\nu(x) = \mathrm{Re}\chi_\nu(e^{ix})$$

and

$$S_\nu(x) = \mathrm{Im}\chi_\nu(e^{ix}).$$

14.9 Inversion

The Bernoulli and Euler polynomials may be inverted to express the monomial in terms of the polynomials. Specifically, evidently from the above section on #Representation by an integral operator, it follows that

$$x^n = \frac{1}{n+1}\sum_{k=0}^{n} \binom{n+1}{k} B_k(x)$$

and

$$x^n = E_n(x) + \frac{1}{2}\sum_{k=0}^{n-1} \binom{n}{k} E_k(x).$$

14.10 Relation to falling factorial

The Bernoulli polynomials may be expanded in terms of the falling factorial $(x)_k$ as

$$B_{n+1}(x) = B_{n+1} + \sum_{k=0}^{n} \frac{n+1}{k+1} \left\{ n \atop k \right\} (x)_{k+1}$$

where $B_n = B_n(0)$ and

$$\left\{ n \atop k \right\} = S(n,k)$$

denotes the Stirling number of the second kind. The above may be inverted to express the falling factorial in terms of the Bernoulli polynomials:

$$(x)_{n+1} = \sum_{k=0}^{n} \frac{n+1}{k+1} \left[n \atop k \right] (B_{k+1}(x) - B_{k+1})$$

where

$$\left[n \atop k \right] = s(n,k)$$

denotes the Stirling number of the first kind.

14.11 Multiplication theorems

The multiplication theorems were given by Joseph Ludwig Raabe in 1851:

For a natural number $m \geq 1$,

$$B_n(mx) = m^{n-1} \sum_{k=0}^{m-1} B_n\left(x + \frac{k}{m}\right)$$

$$E_n(mx) = m^n \sum_{k=0}^{m-1} (-1)^k E_n\left(x + \frac{k}{m}\right) \quad \text{for } m = 1, 3, \ldots$$

$$E_n(mx) = \frac{-2}{n+1} m^n \sum_{k=0}^{m-1} (-1)^k B_{n+1}\left(x + \frac{k}{m}\right) \quad \text{for } m = 2, 4, \ldots$$

14.12 Integrals

Indefinite integrals

$$\int_a^x B_n(t)\, dt = \frac{B_{n+1}(x) - B_{n+1}(a)}{n+1}$$

$$\int_a^x E_n(t)\, dt = \frac{E_{n+1}(x) - E_{n+1}(a)}{n+1}$$

Definite integrals

$$\int_0^1 B_n(t)B_m(t)\,dt = (-1)^{n-1}\frac{m!n!}{(m+n)!}B_{n+m} \quad \text{for } m,n \geq 1$$

$$\int_0^1 E_n(t)E_m(t)\,dt = (-1)^n 4(2^{m+n+2}-1)\frac{m!n!}{(m+n+2)!}B_{n+m+2}$$

14.13 Periodic Bernoulli polynomials

A **periodic Bernoulli polynomial** *Pn*(*x*) is a Bernoulli polynomial evaluated at the fractional part of the argument *x*. These functions are used to provide the remainder term in the Euler–Maclaurin formula relating sums to integrals. The first polynomial is a sawtooth function.

Strictly these functions are not polynomials at all and more properly should be termed the periodic Bernoulli functions.

The following properties are of interest, valid for all x :

$P_k(x)$ all for continuous is $k \neq 1$
$P'_k(x)$ for continuous is and exists $k = 0, k \geq 3$
$P'_k(x) = kP_{k-1}(x), k \geq 3$

14.14 See also

- Bernoulli numbers
- Stirling polynomial

14.15 References

[1] D.H. Lehmer, "On the Maxima and Minima of Bernoulli Polynomials", *American Mathematical Monthly*, volume 47, pages 533–538 (1940)

[2] Zhi-Wei Sun; Hao Pan (2006). "Identities concerning Bernoulli and Euler polynomials". *Acta Arithmetica* **125**: 21–39. arXiv:math/0409035. doi:10.4064/aa125-1-3.

- Milton Abramowitz and Irene A. Stegun, eds. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, (1972) Dover, New York. *(See Chapter 23)*
- Apostol, Tom M. (1976), *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag, ISBN 978-0-387-90163-3, MR 0434929, Zbl 0335.10001 *(See chapter 12.11)*
- Dilcher, K. (2010), "Bernoulli and Euler Polynomials", in Olver, Frank W. J.; Lozier, Daniel M.; Boisvert, Ronald F.; Clark, Charles W., *NIST Handbook of Mathematical Functions*, Cambridge University Press, ISBN 978-0521192255, MR 2723248
- Cvijović, Djurdje; Klinowski, Jacek (1995). "New formulae for the Bernoulli and Euler polynomials at rational arguments". *Proceedings of the American Mathematical Society* **123**: 1527–1535. doi:10.2307/2161144.
- Guillera, Jesus; Sondow, Jonathan (2008). "Double integrals and infinite products for some classical constants via analytic continuations of Lerch's transcendent". *The Ramanujan Journal* **16** (3): 247–270. arXiv:math.NT/0506319. doi:10.1007/s11139-007-9102-0. *(Reviews relationship to the Hurwitz zeta function and Lerch transcendent.)*

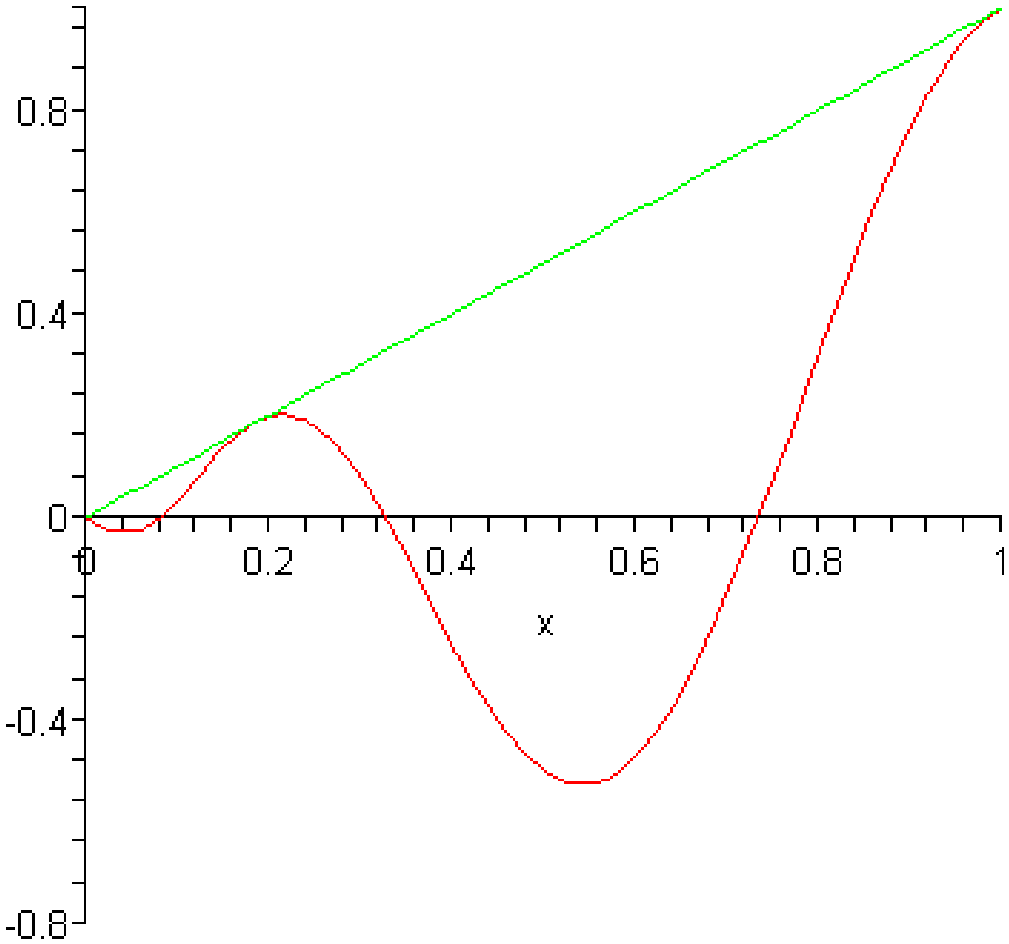
- Hugh L. Montgomery; Robert C. Vaughan (2007). *Multiplicative number theory I. Classical theory*. Cambridge tracts in advanced mathematics **97**. Cambridge: Cambridge Univ. Press. pp. 495–519. ISBN 0-521-84903-9.

Chapter 15

Bernstein polynomial

For the Bernstein polynomial in D-module theory, see Bernstein–Sato polynomial.

In the mathematical field of numerical analysis, a **Bernstein polynomial**, named after Sergei Natanovich Bernstein,



Bernstein polynomials approximating a curve

is a polynomial in the **Bernstein form**, that is a linear combination of **Bernstein basis polynomials**.

A numerically stable way to evaluate polynomials in Bernstein form is de Casteljau's algorithm.

Polynomials in Bernstein form were first used by Bernstein in a constructive proof for the Stone–Weierstrass approximation theorem. With the advent of computer graphics, Bernstein polynomials, restricted to the interval $x \in [0, 1]$, became important in the form of Bézier curves.

15.1 Definition

The $n + 1$ **Bernstein basis polynomials** of degree n are defined as

$$b_{\nu,n}(x) = \binom{n}{\nu} x^{\nu} (1-x)^{n-\nu}, \quad \nu = 0, \ldots, n.$$

where $\binom{n}{\nu}$ is a binomial coefficient.

The Bernstein basis polynomials of degree n form a basis for the vector space Πn of polynomials of degree at most n.

A linear combination of Bernstein basis polynomials

$$B_n(x) = \sum_{\nu=0}^{n} \beta_\nu b_{\nu,n}(x)$$

is called a **Bernstein polynomial** or **polynomial in Bernstein form** of degree n. The coefficients β_ν are called **Bernstein coefficients** or **Bézier coefficients**.

15.2 Example

The first few Bernstein basis polynomials are:

$$\begin{aligned}
&b_{0,0}(x) = 1,\\
&b_{0,1}(x) = 1 - x, && b_{1,1}(x) = x\\
&b_{0,2}(x) = (1-x)^2, && b_{1,2}(x) = 2x(1-x), && b_{2,2}(x) = x^2\\
&b_{0,3}(x) = (1-x)^3, && b_{1,3}(x) = 3x(1-x)^2, && b_{2,3}(x) = 3x^2(1-x), && b_{3,3}(x) = x^3\\
&b_{0,4}(x) = (1-x)^4, && b_{1,4}(x) = 4x(1-x)^3, && b_{2,4}(x) = 6x^2(1-x)^2, && b_{3,4}(x) = 4x^3(1-x), && b_{4,4}(x) = x^4
\end{aligned}$$

15.3 Properties

The Bernstein basis polynomials have the following properties:

- $b_{\nu,n}(x) = 0$, if $\nu < 0$ or $\nu > n$.
- $b_{\nu,n}(0) = \delta_{\nu,0}$ and $b_{\nu,n}(1) = \delta_{\nu,n}$ where δ is the Kronecker delta function.
- $b_{\nu,n}(x)$ has a root with multiplicity ν at point $x = 0$ (note: if $\nu = 0$, there is no root at 0).
- $b_{\nu,n}(x)$ has a root with multiplicity $(n - \nu)$ at point $x = 1$ (note: if $\nu = n$, there is no root at 1).
- $b_{\nu,n}(x) \geq 0$ for $x \in [0,\ 1]$.
- $b_{\nu,n}\,(1 - x) = b_{n-\nu,n}(x)$.
- The derivative can be written as a combination of two polynomials of lower degree:

  $b'_{\nu,n}(x) = n\,(b_{\nu-1,n-1}(x) - b_{\nu,n-1}(x))$.

- The integral is constant for a given n

$$\int_0^1 b_{\nu,n}(x)dx = \frac{1}{n+1}; \forall \nu = 0, 1 \dots n$$

- If $n \neq 0$, then $b_{\nu,n}(x)$ has a unique local maximum on the interval $[0,\ 1]$ at $x = \frac{\nu}{n}$. This maximum takes the value:

$$\nu^{\nu} n^{-n} (n-\nu)^{n-\nu} \binom{n}{\nu}.$$

- The Bernstein basis polynomials of degree n form a partition of unity:

$$\sum_{\nu=0}^{n} b_{\nu,n}(x) = \sum_{\nu=0}^{n} \binom{n}{\nu} x^{\nu} (1-x)^{n-\nu} = (x + (1-x))^n = 1.$$

- By taking the first derivative of $(x+y)^n$ where $y = 1 - x$, it can be shown that

$$\sum_{\nu=0}^{n} \nu b_{\nu,n}(x) = nx$$

- The second derivative of $(x+y)^n$ where $y = 1 - x$ can be used to show

$$\sum_{\nu=1}^{n} \nu(\nu-1) b_{\nu,n}(x) = n(n-1)x^2$$

- A Bernstein polynomial can always be written as a linear combination of polynomials of higher degree:

$$b_{\nu,n-1}(x) = \frac{n-\nu}{n} b_{\nu,n}(x) + \frac{\nu+1}{n} b_{\nu+1,n}(x).$$

15.4 Approximating continuous functions

Let f be a continuous function on the interval [0, 1]. Consider the Bernstein polynomial

$$B_n(f)(x) = \sum_{\nu=0}^{n} f\left(\frac{\nu}{n}\right) b_{\nu,n}(x).$$

It can be shown that

$$\lim_{n\to\infty} B_n(f)(x) = f(x)$$

uniformly on the interval [0, 1].[1] This is a stronger statement than the proposition that the limit holds for each value of *x* separately; that would be pointwise convergence rather than uniform convergence. Specifically, the word *uniformly* signifies that

$$\lim_{n\to\infty} \sup \{\, |f(x) - B_n(f)(x)| \,:\, 0 \leq x \leq 1 \,\} = 0.$$

Bernstein polynomials thus afford one way to prove the Weierstrass approximation theorem that every real-valued continuous function on a real interval [*a*, *b*] can be uniformly approximated by polynomial functions over $\mathbf{R}$.[2]

A more general statement for a function with continuous k^{th} derivative is

$$\left\|B_n(f)^{(k)}\right\|_\infty \leq \frac{(n)_k}{n^k}\left\|f^{(k)}\right\|_\infty \text{ and } \left\|f^{(k)} - B_n(f)^{(k)}\right\|_\infty \to 0$$

where additionally

$$\frac{(n)_k}{n^k} = \left(1 - \frac{0}{n}\right)\left(1 - \frac{1}{n}\right)\cdots\left(1 - \frac{k-1}{n}\right)$$

is an eigenvalue of *Bn*; the corresponding eigenfunction is a polynomial of degree *k*.

15.4.1 Proof

Suppose *K* is a random variable distributed as the number of successes in *n* independent Bernoulli trials with probability *x* of success on each trial; in other words, *K* has a binomial distribution with parameters *n* and *x*. Then we have the expected value E(*K*/*n*) = *x*.

By the weak law of large numbers of probability theory,

$$\lim_{n\to\infty} P\left(\left|\frac{K}{n} - x\right| > \delta\right) = 0$$

for every $\delta > 0$. Moreover, this relation holds uniformly in *x*, which can be seen from its proof via Chebyshev's inequality, taking into account that the variance of *K*/*n*, equal to *x*(1-*x*)/*n*, is bounded from above by 1/(4*n*) irrespective of *x*.

Because *f*, being continuous on a closed bounded interval, must be uniformly continuous on that interval, one infers a statement of the form

$$\lim_{n\to\infty} P\left(\left|f\left(\frac{K}{n}\right) - f\left(x\right)\right| > \varepsilon\right) = 0$$

uniformly in *x*. Taking into account that *f* is bounded (on the given interval) one gets for the expectation

$$\lim_{n\to\infty} E\left(\left|f\left(\frac{K}{n}\right) - f\left(x\right)\right|\right) = 0$$

uniformly in *x*. To this end one splits the sum for the expectation in two parts. On one part the difference does not exceed ε; this part cannot contribute more than ε. On the other part the difference exceeds ε, but does not exceed 2*M*, where *M* is an upper bound for |*f*(x)|; this part cannot contribute more than 2*M* times the small probability that the difference exceeds ε.

Finally, one observes that the absolute value of the difference between expectations never exceeds the expectation of the absolute value of the difference, and that E(*f*(*K*/*n*)) is just the Bernstein polynomial *Bn*(*f*, *x*).

See for instance.[3]

15.5 See also

- Bézier curve
- Polynomial interpolation
- Newton form
- Lagrange form
- Binomial QMF

15.6 Notes

[1] Natanson (1964) p.6

[2] Natanson (1964) p.3

[3] L. Koralov and Y. Sinai, "Theory of probability and random processes" (second edition), Springer 2007; see page 29, Section "Probabilistic proof of the Weierstrass theorem".

15.7 References

- Caglar, Hakan; Akansu, Ali N. (July 1993). "A generalized parametric PR-QMF design technique based on Bernstein polynomial approximation". *IEEE Transactions on Signal Processing* **41** (7): 2314–2321. Zbl 0825.93863.
- Korovkin, P.P. (2001), "Bernstein polynomials", in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Natanson, I.P. (1964). *Constructive function theory. Volume I: Uniform approximation*. Translated by Alexis N. Obolensky. New York: Frederick Ungar. MR 0196340. Zbl 0133.31101.

15.8 External links

- BERNSTEIN POLYNOMIALS by Kenneth I. Joy
- From Bézier to Bernstein
- Weisstein, Eric W., "Bernstein Polynomial", *MathWorld*.
- *This article incorporates material from properties of Bernstein polynomial on PlanetMath, which is licensed under the Creative Commons Attribution/Share-Alike License.*

Chapter 16

Bernstein–Sato polynomial

In mathematics, the **Bernstein–Sato polynomial** is a polynomial related to differential operators, introduced independently by Bernstein (1971) and Sato and Shintani (1972, 1974), Sato (1990). It is also known as the **b-function**, the **b-polynomial**, and the **Bernstein polynomial**, though it is not related to the Bernstein polynomials used in approximation theory. It has applications to singularity theory, monodromy theory and quantum field theory.

Coutinho (1995) gives an elementary introduction, and Borel (1987) and Kashiwara (2003) give more advanced accounts.

16.1 Definition and properties

If $f(x)$ is a polynomial in several variables then there is a non-zero polynomial $b(s)$ and a differential operator $P(s)$ with polynomial coefficients such that

$$P(s)f(x)^{s+1} = b(s)f(x)^s.$$

The Bernstein–Sato polynomial is the monic polynomial of smallest degree amongst such $b(s)$. Its existence can be shown using the notion of holonomic D-modules.

Kashiwara (1976) proved that all roots of the Bernstein–Sato polynomial are negative rational numbers.

The Bernstein–Sato polynomial can also be defined for products of powers of several polynomials (Sabbah 1987). In this case it is a product of linear factors with rational coefficients.

Nero Budur, Mircea Mustaţă, and Morihiko Saito (2006) generalized the Bernstein–Sato polynomial to arbitrary varieties.

Note, that the Bernstein–Sato polynomial can be computed algorithmically. However, such computations are hard in general. There are implementations of related algorithms in computer algebra systems RISA/Asir, Macaulay2 and SINGULAR.

Daniel Andres, Viktor Levandovskyy, and Jorge Martín-Morales (2009) presented algorithms to compute the Bernstein–Sato polynomial of an affine variety together with an implementation in the computer algebra system SINGULAR.

Berkesch & Leykin (2010) described some of the algorithms for computing Bernstein–Sato polynomials by computer.

16.2 Examples

- If $f(x) = x_1^2 + \cdots + x_n^2$ then

$$\sum_{i=1}^{n} \partial_i^2 f(x)^{s+1} = 4(s+1)\left(s+\frac{n}{2}\right) f(x)^s$$

so the Bernstein–Sato polynomial is

$$b(s) = (s+1)\left(s + \frac{n}{2}\right).$$

- If $f(x) = x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}$ then

$$\prod_{j=1}^{r} \partial_{x_j}^{n_j} \quad f(x)^{s+1} = \prod_{j=1}^{r} \prod_{i=1}^{n_j} (n_j s + i) \quad f(x)^s$$

so

$$b(s) = \prod_{j=1}^{r} \prod_{i=1}^{n_j} \left(s + \frac{i}{n_j}\right).$$

- The Bernstein–Sato polynomial of $x^2 + y^3$ is

$$(s+1)\left(s + \frac{5}{6}\right)\left(s + \frac{7}{6}\right).$$

- If *tij* are n^2 variables, then the Bernstein–Sato polynomial of det(*tij*) is given by

$$s(s+1)\cdots(s+n-1)$$

which follows from

$$\Omega(\det(t_{ij})^s) = s(s+1)\cdots(s+n-1)\det(t_{ij})^{s-1}$$

where Ω is Cayley's omega process, which in turn follows from the Capelli identity.

16.3 Applications

- If $f(x)$ is a non-negative polynomial then $f(x)^s$, initially defined for s with non-negative real part, can be analytically continued to a meromorphic distribution-valued function of s by repeatedly using the functional equation

$$f(x)^s = \frac{1}{b(s)} P(s) f(x)^{s+1}.$$

It may have poles whenever $b(s + n)$ is zero for a non-negative integer n.

- If $f(x)$ is a polynomial, not identically zero, then it has an inverse g that is a distribution; in other words, $fg = 1$ as distributions. (Warning: the inverse is not unique in general, because if f has zeros then there are distributions whose product with f is zero, and adding one of these to an inverse of f is another inverse of f. The usual proof of uniqueness of inverses fails because the product of distributions is not always defined, and need not be associative even when it is defined.) If $f(x)$ is non-negative the inverse can be constructed using the Bernstein–Sato polynomial by taking the constant term of the Laurent expansion of $f(x)^s$ at $s = -1$. For arbitrary $f(x)$ just take $\bar{f}(x)$ times the inverse of $\bar{f}(x)f(x)$.

- The Malgrange–Ehrenpreis theorem states that every differential operator with constant coefficients has a Green's function. By taking Fourier transforms this follows from the fact that every polynomial has a distributional inverse, which is proved in the paragraph above.

- Etingof (1999) showed how to use the Bernstein polynomial to define dimensional regularization rigorously, in the massive Euclidean case.

- The Bernstein-Sato functional equation is used in computations of some of the more complex kinds of singular integrals occurring in quantum field theory (Tkachov 1997). Such computations are needed for precision measurements in elementary particle physics as practiced e.g. at CERN (see the papers citing (Tkachov 1997)). However, the most interesting cases require a simple generalization of the Bernstein-Sato functional equation to the product of two polynomials $(f_1(x))^{s_1}(f_2(x))^{s_2}$, with x having 2-6 scalar components, and the pair of polynomials having orders 2 and 3. Unfortunately, a brute force determination of the corresponding differential operators $P(s_1, s_2)$ and $b(s_1, s_2)$ for such cases has so far proved prohibitively cumbersome. Devising ways to bypass the combinatorial explosion of the brute force algorithm would be of great value in such applications.

16.4 References

- Andres, Daniel; Levandovskyy, Viktor; Martín-Morales, Jorge (2009), "Principal Intersection and Bernstein-Sato Polynomial of an Affine Variety", *Proc. ISSAC 2009* (Association for Computing Machinery): 231, arXiv:1002.3644, doi:10.1145/1576702.1576735

- Berkesch, Christine; Leykin, Anton (2010), "Algorithms for Bernstein-Sato polynomials and multiplier ideals", *Proc. ISSAC 2010*, arXiv:1002.1475

- Bernstein, J. (1971), "Modules over a ring of differential operators. Study of the fundamental solutions of equations with constant coefficients", *Functional Analysis and Its Applications* **5** (2): 89–101, doi:10.1007/BF01076413, MR 0290097

- Budur, Nero; Mustaţă, Mircea; Saito, Morihiko (2006), "Bernstein-Sato polynomials of arbitrary varieties", *Compositio Mathematica* **142** (3): 779–797, doi:10.1112/S0010437X06002193, MR 2231202

- Borel, Armand (1987), *Algebraic D-Modules*, Perspectives in Mathematics **2**, Boston, MA: Academic Press, ISBN 0-12-117740-8

- Coutinho, S. C. (1995), *A primer of algebraic D-modules*, London Mathematical Society Student Texts **33**, Cambridge: Cambridge University Press, ISBN 0-521-55908-1

- Etingof, Pavel (1999), "Note on dimensional regularization", *Quantum fields and strings: a course for mathematicians, Vol. 1,(Princeton, NJ, 1996/1997)*, Providence, R.I.: Amer. Math. Soc., pp. 597–607, ISBN 978-0-8218-2012-4, MR 1701608

- Kashiwara, Masaki (1976), "B-functions and holonomic systems. Rationality of roots of B-functions", *Inventiones Mathematicae* **38** (1): 33–53, doi:10.1007/BF01390168, MR 0430304

- Kashiwara, Masaki (2003), *D-modules and microlocal calculus*, Translations of Mathematical Monographs **217**, Providence, R.I.: American Mathematical Society, ISBN 978-0-8218-2766-6, MR 1943036

- Sabbah, Claude (1987), "Proximité évanescente. I. La structure polaire d'un D-module", *Compositio Mathematica* **62** (3): 283–328, MR 901394

- Sato, Mikio; Shintani, Takuro (1972), "On zeta functions associated with prehomogeneous vector spaces", *Proceedings of the National Academy of Sciences of the United States of America* **69** (5): 1081–1082, doi:10.1073/pnas.69.5.1081, JSTOR 61638, MR 0296079

- Sato, Mikio; Shintani, Takuro (1974), "On zeta functions associated with prehomogeneous vector spaces", *Annals of Mathematics*, Second Series **100** (1): 131–170, doi:10.2307/1970844, JSTOR 1970844, MR 0344230

- Sato, Mikio (1990) [1970], "Theory of prehomogeneous vector spaces (algebraic part)---the English translation of Sato's lecture from Shintani's note", *Nagoya Mathematical Journal* **120**: 1–34, MR 1086566

- Tkachov, Fyodor V. (1997), "Algebraic algorithms for multiloop calculations. The first 15 years. What's next?", *Nucl. Instrum. Meth. A* **389**: 309–313, arXiv:hep-ph/9609429, doi:10.1016/S0168-9002(97)00110-1

Chapter 17

Binomial

For other uses, see Binomial (disambiguation).

In algebra, a **binomial** is a polynomial which is the sum of two terms, which are monomials.[1] It is the simplest kind of polynomial after the monomials.

17.1 Definition

A binomial is a polynomial, which is the sum of two monomials. A binomial in a single indeterminate (also known as a univariate binomial) can be written in the form

$ax^n - bx^m$,

where a and b are numbers, and n and m are distinct nonnegative integers and x is a symbol which is called an indeterminate or, for historical reasons, a variable. In some contexts, the exponents m and n may be negative, in which case the monomial is a Laurent binomial.

More generally, a binomial may be written[2] as:

$ax_1^{n_1} \cdots x_i^{n_i} - bx_1^{m_1} \cdots x_i^{m_i}$

Some examples of binomials are:

$3x - 2x^2$

$xy + yx^2$

$x^2 + y^2$

17.2 Operations on simple binomials

- The binomial $x^2 - y^2$ can be factored as the product of two other binomials.

  $x^2 - y^2 = (x + y)(x - y)$.

  This is a special case of the more general formula: $x^{n+1} - y^{n+1} = (x - y) \sum_{k=0}^{n} x^k \, y^{n-k}$.

  This can also be extended to $x^2 + y^2 = x^2 - (iy)^2 = (x - iy)(x + iy)$ when working over the complex numbers

- The product of a pair of linear binomials $(ax + b)$ and $(cx + d)$ is a trinomial:

$$(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd.$$

- A binomial raised to the n^{th} power, represented as

$$(x + y)^n$$

can be expanded by means of the binomial theorem or, equivalently, using Pascal's triangle. For example, the square $(x + y)^2$ of the binomial $x + y$ is equal to the sum of the squares of the two terms and twice the product of the terms, that is $x^2 + 2xy + y^2$. The numbers (1,2,1) appearing as multipliers for the terms in this expansion are binomial coefficients two rows down from the top of Pascal's triangle. The expansion of the *n*th power uses the numbers *n* rows down from the top of the triangle.

- An application of above formula for the square of a binomial is the "(m,n)-formula" for generating Pythagorean triples: for $m < n$, let $a = n^2 - m^2$, $b = 2mn$, $c = n^2 + m^2$, then $a^2 + b^2 = c^2$.

- Binomials that are sums or differences of cubes can be factored into lower-order polynomials as follows:

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2)$$
$$x^3 - y^3 = (x - y)(x^2 + xy + y^2)$$

17.3 See also

- Completing the square
- Binomial distribution
- Binomial-QMF (Daubechies Wavelet Filters)
- The list of factorial and binomial topics contains a large number of related links.

17.4 Notes

[1] Weisstein, Eric. "Binomial". Wolfram MathWorld. Retrieved 29 March 2011.

[2] Sturmfels, Bernd (2002). "Solving Systems of Polynomial Equations". *CBMS Regional Conference Series in Mathematics* (Conference Board of the Mathematical Sciences) (97): 62. Retrieved 21 March 2014.

17.5 References

- L. Bostock and S. Chandler (1978). Pure Mathematics 1. ISBN 0-85950-092-6. pp. 36
- Hazewinkel, Michiel, ed. (2001), "Binomial", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4

Chapter 18

Boas–Buck polynomials

In mathematics, **Boas–Buck polynomials** are sequences of polynomials $\Phi(r)$ $n(x)$ given by generating functions of the form

$$C(zt^r B(t)) = \sum_{n\geq 0} \Phi_n^{(r)}(z)t^n$$

The case r=1, sometimes called generalized Appell polynomials, was studied by Boas and Buck (1958).

18.1 References

- Boas, Ralph P.; Buck, R. Creighton (1958), *Polynomial expansions of analytic functions*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge. **19**, Berlin, New York: Springer-Verlag, MR 0094466

Chapter 19

Bollobás–Riordan polynomial

The **Bollobás–Riordan polynomial** can mean a 3-variable invariant polynomial of graphs on orientable surfaces, or a more general 4-variable invariant of ribbon graphs, generalizing the Tutte polynomial.

19.1 History

These polynomials were discovered by Bollobás and Riordan (2001, 2002).

19.2 Formal definition

The 3-variable Bollobás–Riordan polynomial is given by

$$RG(x,y,z) = \sum_F x^{r(G)-r(F)} y^{n(F)} z^{k(F)-bc(F)+n(F)}$$

where

- $v(G)$ is the number of vertices of G;
- $e(G)$ is the number of its edges of G;
- $k(G)$ is the number of components of G;
- $r(G)$ is the rank of G such that $r(G) = v(G) - k(G)$;
- $n(G)$ is the nullity of such that $n(G) = e(G) - r(G)$;
- $bc(G)$ is the number of connected components of the boundary of G.

19.3 See also

- Graph invariant

19.4 References

- Bollobás, Béla; Riordan, Oliver (2001), "A polynomial invariant of graphs on orientable surfaces", *Proceedings of the London Mathematical Society. Third Series* **83** (3): 513–531, doi:10.1112/plms/83.3.513, ISSN 0024-6115, MR 1851080

- Bollobás, Béla; Riordan, Oliver (2002), "A polynomial of graphs on surfaces", *Mathematische Annalen* **323** (1): 81–96, doi:10.1007/s002080100297, ISSN 0025-5831, MR 1906909

Chapter 20

Bombieri norm

In mathematics, the **Bombieri norm**, named after Enrico Bombieri, is a norm on homogeneous polynomials with coefficient in $\mathbb{R}$ or $\mathbb{C}$ (there is also a version for non homogeneous univariate polynomials). This norm has many remarkable properties, the most important being listed in this article.

20.1 Bombieri scalar product for homogeneous polynomials

To start with the geometry, the *Bombieri scalar product* for homogeneous polynomials with *N* variables can be defined as follows using multi-index notation:

$\forall \alpha, \beta \in \mathbb{N}^N$

by definition different monomials are orthogonal, so that

$$\langle X^\alpha | X^\beta \rangle = 0 \text{ if } \alpha \neq \beta,$$

while

$\forall \alpha \in \mathbb{N}^N$

by definition

$$\|X^\alpha\|^2 = \frac{\alpha!}{|\alpha|!}.$$

In the above definition and in the rest of this article the following notation applies:

if

$\alpha = (\alpha_1, \ldots, \alpha_N) \in \mathbb{N}^N,$

write

$|\alpha| = \Sigma_{i=1}^N \alpha_i$

and

$\alpha! = \Pi_{i=1}^N (\alpha_i!)$

and

$X^\alpha = \Pi_{i=1}^N X_i^{\alpha_i}$.

20.2 Bombieri inequality

The fundamental property of this norm is the Bombieri inequality:

let P, Q be two homogeneous polynomials respectively of degree $d^\circ(P)$ and $d^\circ(Q)$ with N variables, then, the following inequality holds:

$$\frac{d^\circ(P)!d^\circ(Q)!}{(d^\circ(P)+d^\circ(Q))!}\|P\|^2\|Q\|^2 \leq \|P\cdot Q\|^2 \leq \|P\|^2\|Q\|^2.$$

Here the Bombieri inequality is the left hand side of the above statement, while the right side means that the Bombieri norm is an algebra norm. Giving the left hand side is meaningless without that constraint, because in this case, we can achieve the same result with any norm by multiplying the norm by a well chosen factor.

This multiplicative inequality implies that the product of two polynomials is bounded from below by a quantity that depends on the multiplicand polynomials. Thus, this product can not be arbitrarily small. This multiplicative inequality is useful in metric algebraic geometry and number theory.

20.3 Invariance by isometry

Another important property is that the Bombieri norm is invariant by composition with an isometry:

let P, Q be two homogeneous polynomials of degree d with N variables and let h be an isometry of $\mathbb{R}^N$ (or $\mathbb{C}^N$). Then, the we have $\langle P\circ h|Q\circ h\rangle = \langle P|Q\rangle$. When $P = Q$ this implies $\|P\circ h\| = \|P\|$.

This result follows from a nice integral formulation of the scalar product:

$$\langle P|Q\rangle = \binom{d+N-1}{N-1}\int_{S^N} P(Z)\overline{Q(Z)}\,d\sigma(Z)$$

where S^N is the unit sphere of $\mathbb{C}^N$ with its canonical measure $d\sigma(Z)$.

20.4 Other inequalities

Let P be a homogeneous polynomial of degree d with N variables and let $Z \in \mathbb{C}^N$. We have:

- $|P(Z)| \leq \|P\|\,\|Z\|_E^d$
- $\|\nabla P(Z)\|_E \leq d\|P\|\,\|Z\|_E^d$

where $\|\cdot\|_E$ denotes the Euclidean norm.

The Bombieri norm is useful in polynomial factorization, where it has some advantages over the Mahler measure, according to Knuth (Exercises 20-21, pages 457-458 and 682-684).

20.5 See also

- Grassmann manifold

- Hardy space
- Homogeneous polynomial
- Plücker embedding

20.6 References

- Beauzamy, Bernard; Bombieri, Enrico; Enflo, Per; Montgomery, Hugh L. (1990). "Products of polynomials in many variables". *Journal of Number Theory* **36** (2): 219–245. doi:10.1016/0022-314X(90)90075-3. MR 1072467. hdl:2027.42/28840.
- Beauzamy, Bernard; Enflo, Per; Wang, Paul (October 1994). "Quantitative estimates for polynomials in one or several variables: From analysis and number theory to symbolic and massively parallel computation". *Mathematics Magazine* **67** (4): 243–257. doi:10.2307/2690843. JSTOR 2690843. MR 1300564.
- Bombieri, Enrico; Gubler, Walter (2006). *Heights in Diophantine geometry*. Cambridge U. P. ISBN 0-521-84615-3. MR 2216774.
- Knuth, Donald E. (1997). "4.6.2 Factorization of polynomials". *Seminumerical algorithms*. *The Art of Computer Programming* **2** (Third ed.). Reading, Massachusetts: Addison-Wesley. pp. 439–461, 678–691. ISBN 0-201-89684-2. MR 633878.

Chapter 21

Boole polynomials

In mathematics, the **Boole polynomials** $sn(x)$ are polynomials given by the generating function

$$\sum s_n(x)t^n/n! = \frac{(1+t)^x}{1+(1+t)^\lambda}$$

(Roman 1984, 4.5), (Jordan 1939, sections 113–117).

21.1 See also

- Umbral calculus
- Peters polynomials, a generalization of Boole polynomials.

21.2 References

- Boas, Ralph P.; Buck, R. Creighton (1958), *Polynomial expansions of analytic functions*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge. **19**, Berlin, New York: Springer-Verlag, MR 0094466
- Boole, G. (1860/1970), *Calculus of finite differences*.
- Jordan, Charles (1939), *Calculus of Finite Differences*, Hungarian Agent Eggenberger Book-Shop, Budapest, ISBN 978-0-8284-0033-6, MR 0000441, Reprinted by Chelsea 1965
- Roman, Steven (1984), *The umbral calculus*, Pure and Applied Mathematics **111**, London: Academic Press Inc. [Harcourt Brace Jovanovich Publishers], ISBN 978-0-12-594380-2, MR 741185 Reprinted by Dover, 2005

Chapter 22

Bracket polynomial

In the mathematical field of knot theory, the **bracket polynomial** (also known as the **Kauffman bracket**) is a polynomial invariant of framed links. Although it is not an invariant of knots or links (as it is not invariant under type I Reidemeister moves), a suitably "normalized" version yields the famous knot invariant called the Jones polynomial. The bracket polynomial plays an important role in unifying the Jones polynomial with other quantum invariants. In particular, Kauffman's interpretation of the Jones polynomial allows generalization to invariants of 3-manifolds.

The bracket polynomial was discovered by Louis Kauffman in 1987.

22.1 Definition

The bracket polynomial of any (unoriented) link diagram L , denoted $\langle L \rangle$, is a polynomial in the variable A , characterized by the three rules:

- $\langle O \rangle = 1$, where O is the standard diagram of the unknot
- 

- $\langle O \cup L \rangle = (-A^2 - A^{-2})\langle L \rangle$

The pictures in the second rule represent brackets of the link diagrams which differ inside a disc as shown but are identical outside. The third rule means that adding a circle disjoint from the rest of the diagram multiplies the bracket of the remaining diagram by $-A^2 - A^{-2}$.

22.2 Further reading

- Louis H. Kauffman, *State models and the Jones polynomial.* Topology 26 (1987), no. 3, 395-−407. (introduces the bracket polynomial)

22.3 External links

- Weisstein, Eric W., "Bracket Polynomial", *MathWorld*.

Chapter 23

Bring radical

In algebra, a **Bring radical** or **ultraradical** of a complex number a is a root of the polynomial

$$x^5 + x + a.$$

The root is chosen so the radical of a real number is real, and the radical is a differentiable function of a in the complex plane, with a branch cut along the negative real line below -1.

George Jerrard showed that some quintic equations can be solved in closed form using radicals and Bring radicals, which had been introduced by Erland Bring.

23.1 Normal forms

The quintic equation is rather difficult to obtain solutions for directly, with five independent coefficients in its most general form:

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

The various methods for solving the quintic that have been developed generally attempt to simplify the quintic using Tschirnhaus transformations to reduce the number of independent coefficients.

23.1.1 Principal quintic form

The general quintic may be reduced into what is known as the **principal quintic form**, with the quartic and cubic terms removed:

$$x^5 + c_2x^2 + c_1x + c_0 = 0$$

If the roots of a general quintic and a principal quintic are related by a quadratic Tschirnhaus transformation:

$$y_k = x_k^2 + \alpha x_k + \beta$$

the coefficients α and β may be determined by using the resultant, or by means of the power sums of the roots and Newton's identities. This leads to a system of equations in α and β consisting of a quadratic and a linear equation, and either of the two sets of solutions may be used to obtain the corresponding three coefficients of the principal quintic form.[1]

This form is used by Felix Klein's solution to the quintic.[2]

23.1.2 Bring–Jerrard normal form

It is possible to simplify the quintic still further and eliminate the quadratic term, producing the **Bring–Jerrard normal form**:

$$x^5 + d_1 x + d_0 = 0$$

Using the power-sum formulae again with a cubic transformation as Tschirnhaus tried does not work, since the resulting system of equations results in a sixth-degree equation.

In 1796 Bring found a way around this by using a quartic Tschirnhaus transformation to relate the roots of a principal quintic to those of a Bring–Jerrard quintic:

$$z_k = x_k^4 + \alpha x_k^3 + \beta x_k^2 + \gamma x_k + \delta$$

The extra parameter this fourth-order transformation provides allowed Bring to decrease the degrees of the other parameters. This leads to a system of five equations in six unknowns, which then requires the solution of a cubic and a quadratic equation. This method was also discovered by Jerrard in 1852,[3] but it is likely that he was unaware of Bring's previous work in this area.[4] The full transformation may readily be accomplished using a computer algebra package such as Mathematica[5] or Maple.[6] As might be expected from the complexity of these transformations, the resulting expressions can be enormous, particularly when compared to the solutions in radicals for lower degree equations, taking many megabytes of storage for a general quintic with symbolic coefficients.[5]

Regarded as an algebraic function, the solutions to

$$x^5 + d_1 x + d_0 = 0$$

involve two variables, d_1 and d_0, however the reduction is actually to an algebraic function of one variable, very much analogous to a solution in radicals, since we may further reduce the Bring–Jerrard form. If we for instance set

$$z = \frac{x}{\sqrt[4]{-\frac{d_1}{5}}}$$

then we reduce the equation to the form

$$z^5 - 5z - 4t = 0$$

which involves z as an algebraic function of a single variable t, where $t = -(d_0/4)(-d_1/5)^{-5/4}$. A similar transformation suffices to reduce the equation to

$$y^5 - y + a = 0$$

which is the form required by the Hermite-Kronecker-Brioschi method, Glasser's method, and the Cockle-Harley method of differential resolvents described below.

23.1.3 Brioschi normal form

There is another one-parameter normal form for the quintic equation, known as **Brioschi normal form**:

$$x^5 - 10Cx^3 + 45C^2x - C^2 = 0$$

which can be derived by using the following rational Tschirnhaus transformation

$$z_k = \frac{\lambda + \mu y_k}{\frac{y_k^2}{C} - 3}$$

to relate the roots of a principal quintic to a Brioschi quintic. The values of the parameters λ and μ may be derived by using polyhedral functions on the Riemann sphere, and is related to the partition of an object of icosahedral symmetry into five objects of tetrahedral symmetry.[7]

It is to be noted that this Tschirnhaus transformation is rather simpler than the difficult one used to transform a principal quintic into Bring–Jerrard form. This normal form is used by the Doyle–McMullen iteration method and the Kiepert method.

23.2 Series representation

A Taylor series for Bring radicals, as well as a representation in terms of hypergeometric functions can be derived as follows. The equation $x^5 + x + a = 0$ can be rewritten as $x^5 + x = -a$; by setting $f(x) = x^5 + x$, the desired solution is $x = f^{-1}(-a)$.

The series for f^{-1} can then be obtained by reversion of the Taylor series for $f(x)$ (which is simply $x + x^5$), giving:

$$f^{-1}(a) = \sum_{k=0}^{\infty} \binom{5k}{k} \frac{(-1)^k a^{4k+1}}{4k+1} = a - a^5 + 5a^9 - 35a^{13} + ...$$

where the absolute values of the coefficients are sequence A002294 in the OEIS. The series confirms that $f^{-1}(a)$ is odd. This gives

$$BR(a) = f^{-1}(-a) = -f^{-1}(a) = -a + a^5 - 5a^9 + 35a^{13} + ...$$

The series converges for $|a| < 4/(5 \cdot \sqrt[4]{5}) \approx 0.53499$ and can be analytically continued in the complex plane. The above result can be written in hypergeometric form as:[5]

$$BR(a) = -a \; {}_4F_3\left(\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}; \frac{1}{2}, \frac{3}{4}, \frac{5}{4}; -5\left(\frac{5a}{4}\right)^4\right)$$

Compare with the hypergeometric functions that arise in Glasser's derivation and the method of differential resolvents below.

23.3 Solution of the general quintic

We now may express the roots of any polynomial

$$x^5 + px + q$$

in terms of the Bring radical as

$$\sqrt[4]{-\frac{p}{5}}\,\mathrm{BR}\left(-\frac{1}{4}\left(-\frac{5}{p}\right)^{\frac{5}{4}} q\right)$$

and its four conjugates. We have a reduction to the Bring–Jerrard form in terms of solvable polynomial equations, and we used transformations involving polynomial expressions in the roots only up to the fourth degree, which means inverting the transformation may be done by finding the roots of a polynomial solvable in radicals. This procedure produces extraneous solutions, but when we have found the correct ones by numerical means we can also write down the roots of the quintic in terms of square roots, cube roots, and the Bring radical, which is therefore an algebraic solution in terms of algebraic functions of a single variable — an algebraic solution of the general quintic.

23.4 Other characterizations

Many other characterizations of the Bring radical have been developed, the first of which is in terms of elliptic modular functions by Charles Hermite in 1858, and further methods later developed by other mathematicians.

23.4.1 The Hermite–Kronecker–Brioschi characterization

In 1858, Charles Hermite[8] published the first known solution to the general quintic equation in terms of elliptic transcendents, and at around the same time Francesco Brioschi[9] and Leopold Kronecker[10] came upon equivalent solutions. Hermite arrived at this solution by generalizing the well-known solution to the cubic equation in terms of trigonometric functions and finds the solution to a quintic in Bring–Jerrard form:

$$x^5 - x + a = 0$$

into which any quintic equation may be reduced by means of Tschirnhaus transformations as has been shown. He observed that elliptic functions had an analogous role to play in the solution of the Bring–Jerrard quintic as the trigonometric functions had for the cubic. If K and K' are the periods of an elliptic integral of the first kind:

$$K = \int_0^{\frac{\pi}{2}} \frac{d\varphi}{\sqrt{1 - k^2 \sin^2 \varphi}}$$

$$K' = \int_0^{\frac{\pi}{2}} \frac{d\varphi}{\sqrt{1 - k'^2 \sin^2 \varphi}}$$

the elliptic nome is given by:

$$q = e^{-\frac{\pi K'}{K}}$$

and

$$k^2 + k'^2 = 1$$

With

$$q = e^{-\frac{\pi K'}{K}} = e^{\mathrm{i}\pi\tau}$$

define the two elliptic modular functions:

$$\sqrt[4]{k} = \varphi(\tau) = \sqrt{\frac{\vartheta_{10}(0;\tau)}{\vartheta_{00}(0;\tau)}}$$

$$\sqrt[4]{k'} = \psi(\tau) = \sqrt{\frac{\vartheta_{01}(0;\tau)}{\vartheta_{00}(0;\tau)}}$$

where $\vartheta_{00}(0;\tau)$ and similar are Jacobi theta functions.

If *n* is a prime number, we can define two values *u* and *v* as follows:

$$v = \varphi(n\tau)$$

and

$$u = \varphi(\tau)$$

The parameters u and v are linked by an equation of degree $n + 1$ known as the modular equation, whose $n + 1$ roots are given by:

$$\epsilon\varphi(n\tau)$$

and

$$\varphi\left(\frac{\tau + 16m}{n}\right)$$

where ε is 1 or −1 depending on whether 2 is a quadratic residue with respect to n or not, and m is an integer modulo n. For $n = 5$, we have the modular equation of the sixth degree:

$$u^6 - v^6 + 5u^2v^2(u^2 - v^2) + 4uv(1 - u^4v^4) = 0$$

with six roots as shown above.

The modular equation of the sixth degree may be related to the Bring–Jerrard quintic by the following function of the six roots of the modular equation:

$$\Phi(\tau) = \left[\varphi(5\tau) + \varphi\left(\frac{\tau}{5}\right)\right]\left[\varphi\left(\frac{\tau + 16}{5}\right) - \varphi\left(\frac{\tau + 64}{5}\right)\right]\left[\varphi\left(\frac{\tau + 32}{5}\right) - \varphi\left(\frac{\tau + 48}{5}\right)\right]$$

The five quantities $\Phi(\tau)$, $\Phi(\tau + 16)$, $\Phi(\tau + 32)$, $\Phi(\tau + 48)$, $\Phi(\tau + 64)$ are the roots of a quintic equation with coefficients rational in $\varphi(\tau)$:

$$\Phi^5 - 2000\varphi^4(\tau)\psi^{16}(\tau)\Phi - 1600\sqrt{5}\varphi^3(\tau)\psi^{16}(\tau)\left[1 + \varphi^8(\tau)\right] = 0$$

which may be readily converted into the Bring–Jerrard form by the substitution:

$$\Phi = 2\sqrt[4]{125}\varphi(\tau)\psi^4(\tau)x$$

leading to the Bring–Jerrard quintic:

$$x^5 - x + a = 0$$

where

$$a = \frac{2[1 + \varphi^8(\tau)]}{\sqrt[4]{5^5}\varphi^2(\tau)\psi^4(\tau)}$$

The Hermite–Kronecker–Brioschi method then amounts to finding a value for τ that corresponds to the value of a, and then using that value of τ to obtain the roots of the corresponding modular equation. To do this, let

$$A = \frac{a\sqrt[4]{5^5}}{2}$$

and calculate the required elliptic modulus k by solving the quartic equation:

$$k^4 + A^2k^3 + 2k^2 - A^2k + 1 = 0$$

The roots of this equation are:

$$k = \tan\frac{\alpha}{4}, \tan\frac{\alpha + 2\pi}{4}, \tan\frac{\pi - \alpha}{4}, \tan\frac{3\pi - \alpha}{4}$$

where $\sin\alpha = \frac{4}{A^2}$ [11] (note that some important references erroneously give it as $\sin\alpha = \frac{1}{4A^2}$ [7][8]). Any of these roots may be used as the elliptic modulus for the purposes of the method. The value of τ may be easily obtained from the elliptic modulus k by the relations given above. The roots of the Bring–Jerrard quintic are then given by:

$$x_i = \frac{\Phi(\tau + 16i)}{2\sqrt[4]{125}\varphi(\tau)\psi^4(\tau)}$$

for $i = 0, \ldots, 4$.

It may be seen that this process uses a generalization of the nth root, which may be expressed as:

$$\sqrt[n]{x} = \exp\left(\frac{1}{n}\ln x\right)$$

or more to the point, as

$$\sqrt[n]{x} = \exp\left(\frac{1}{n}\int_1^x \frac{dt}{t}\right).$$

The Hermite–Kronecker–Brioschi method essentially replaces the exponential by an elliptic modular function, and the integral $\int_1^x \frac{dt}{t}$ by an elliptic integral. Kronecker thought that this generalization was a special case of a still more general theorem, which would be applicable to equations of arbitrarily high degree. This theorem, known as Thomae's formula, was fully expressed by Hiroshi Umemura in 1984, who used Siegel modular forms in place of the exponential/elliptic modular function, and the integral by a hyperelliptic integral.[12]

23.4.2 Glasser's derivation

This derivation due to M. L. Glasser[13] generalizes the series method presented earlier in this article to find a solution to any trinomial equation of the form:

$$x^N - x + t = 0$$

In particular, the quintic equation can be reduced to this form by the use of Tschirnhaus transformations as shown above. Let $x = \zeta^{-\frac{1}{N-1}}$, the general form becomes:

$$\zeta = e^{2\pi i} + t\phi(\zeta)$$

where

$$\phi(\zeta) = \zeta^{\frac{N}{N-1}}$$

A formula due to Lagrange states that for any analytic function f , in the neighborhood of a root of the transformed general equation in terms of ζ , above may be expressed as an infinite series:

$$f(\zeta) = f(e^{2\pi \mathrm{i}}) + \sum_{n=1}^{\infty} \frac{t^n}{n!} \frac{d^{n-1}}{da^{n-1}} [f'(a)|\phi(a)|^n]_{a=e^{2\pi \mathrm{i}}}$$

If we let $f(\zeta) = \zeta^{-\frac{1}{N-1}}$ in this formula, we can come up with the root:

$$x_k = e^{-\frac{2k\pi \mathrm{i}}{N-1}} - \frac{t}{N-1} \sum_{n=0}^{\infty} \frac{(te^{\frac{2k\pi \mathrm{i}}{N-1}})^n}{\Gamma(n+2)} \cdot \frac{\Gamma\left(\frac{Nn}{N-1}+1\right)}{\Gamma\left(\frac{n}{N-1}+1\right)}$$

$k = 1, 2, 3, \ldots, N-1$

By the use of the Gauss multiplication theorem the infinite series above may be broken up into a finite series of hypergeometric functions:

$$\psi_n(q) = \left(\frac{e^{\frac{2n\pi \mathrm{i}}{N-1}} t}{N-1}\right)^q N^{\frac{qN}{N-1}} \frac{\prod_{k=0}^{N-1} \Gamma\left(\frac{q}{N-1} + \frac{1+k}{N}\right)}{\Gamma\left(\frac{q}{N-1}+1\right) \prod_{k=0}^{N-2} \Gamma\left(\frac{q+k+2}{N-1}\right)} == \left(\frac{te^{\frac{2n\pi \mathrm{i}}{N-1}}}{N-1}\right)^q N^{\frac{qN}{N-1}} \prod_{k==2}^{N} \frac{\Gamma\left(\frac{q}{N-1} + \frac{k-1}{N}\right)}{\Gamma\left(\frac{q+k}{N-1}\right)}$$

$$x_n = e^{-\frac{2n\pi \mathrm{i}}{N-1}} - \frac{t}{(N-1)^2} \sqrt{\frac{N}{2\pi(N-1)}} \sum_{q=0}^{N-2} \psi_n(q)_{(N+1)}F_N \left[\begin{matrix} \frac{qN+N-1}{N(N-1)}, \ldots, \frac{q+N-1}{N-1}, 1; \\ \frac{q+2}{N-1}, \ldots, \frac{q+N}{N-1}, \frac{q+N-1}{N-1}; \\ \left(\frac{te^{\frac{2n\pi \mathrm{i}}{N-1}}}{N-1}\right)^{N-1} N^N \end{matrix}\right], \quad n = 1, 2, 3, \ldots, N-1$$

$$x_N = \sum_{m=1}^{N-1} \frac{t}{(N-1)^2} \sqrt{\frac{N}{2\pi(N-1)}} \sum_{q=0}^{N-2} \psi_m(q)_{(N+1)}F_N \left[\begin{matrix} \frac{qN+N-1}{N(N-1)}, \ldots, \frac{q+N-1}{N-1}, 1; \\ \frac{q+2}{N-1}, \ldots, \frac{q+N}{N-1}, \frac{q+N-1}{N-1}; \\ \left(\frac{te^{\frac{2m\pi \mathrm{i}}{N-1}}}{N-1}\right)^{N-1} N^N \end{matrix}\right]$$

and the trinomial of the form,has roots

$ax^N+bx^2+c=0, N \equiv 1 \pmod 2$

$$x_N = -\frac{a}{2b}\sqrt{\left(\frac{c}{b}\right)^{N-1}}{}_{N-1}F_{N-2}\left[\begin{matrix} \frac{N+1}{2N}, \frac{N+3}{2N}, \cdots, \frac{N-2}{N}, \frac{N-1}{N}, \frac{N+1}{N}, \frac{N+2}{N}, \cdots, \frac{3N-3}{2N}, \frac{3N-1}{2N}; \\ \frac{N+1}{2N-4}, \frac{N+3}{2N-4}, \cdots, \frac{N-4}{N-2}, \frac{N-3}{N-2}, \frac{N-1}{N-2}, \frac{N}{N-2}, \cdots, \frac{3N-5}{2N-4}, \frac{3}{2}; \\ -\frac{a^2 c^{N-2}}{4b^N (N-2)^{N-2}} \end{matrix}\right] + \sqrt{\frac{c}{b}}\mathrm{i}_{N-1}F_{N-2}\left[\begin{matrix} \frac{1}{2N}, \frac{3}{2N}, \cdots, \frac{N-4}{2N}, \frac{N-2}{2N}, \frac{N}{2} \\ \frac{3}{2N-4}, \frac{5}{2N-} \\ -\frac{a^2}{4b^N(} \end{matrix}\right]$$

$$x_{N-1} = -\frac{a}{2b}\sqrt{\left(\frac{c}{b}\right)^{N-1}}{}_{N-1}F_{N-2}\left[\begin{matrix} \frac{N+1}{2N}, \frac{N+3}{2N}, \cdots, \frac{N-2}{N}, \frac{N-1}{N}, \frac{N+1}{N}, \frac{N+2}{N}, \cdots, \frac{3N-3}{2N}, \frac{3N-1}{2N}; \\ \frac{N+1}{2N-4}, \frac{N+3}{2N-4}, \cdots, \frac{N-4}{N-2}, \frac{N-3}{N-2}, \frac{N-1}{N-2}, \frac{N}{N-2}, \cdots, \frac{3N-5}{2N-4}, \frac{3}{2}; \\ -\frac{a^2 c^{N-2}}{4b^N (N-2)^{N-2}} \end{matrix}\right] - \sqrt{\frac{c}{b}}\mathrm{i}_{N-1}F_{N-2}\left[\begin{matrix} \frac{1}{2N}, \frac{3}{2N}, \cdots, \frac{N-4}{2N}, \frac{N-2}{2N} \\ \frac{3}{2N-4}, \frac{2N} \\ -\frac{}{4b^} \end{matrix}\right]$$

$$x_n = -e^{\frac{2n\pi \mathrm{i}}{N-2}} \sqrt[N-2]{\frac{b}{a}}{}_{N-1}F_{N-2}\left[\begin{matrix} -\frac{1}{N(N-2)}, -\frac{1}{N(N-2)} + \frac{1}{N}, -\frac{1}{N(N-2)} + \frac{2}{N}, \cdots, -\frac{1}{N(N-2)} + \frac{1}{N}, \frac{N-5}{2N}, -\frac{1}{N(N-2)} + \frac{N-3}{2N}, -\frac{1}{N(N-2)} + \\ \frac{1}{N-2}, \frac{2}{N-2}, \cdots, \frac{2N-5}{2N-4}, ; \\ -\frac{a^2 c^{N-2}}{4b^N (N-2)^{N-2}} \end{matrix}\right]$$

$$+ \sqrt[N-2]{\frac{b}{a}} \sum_{q=1}^{N-3} \frac{\Gamma\left(\frac{2q-1}{N-2}+q\right)}{\Gamma\left(\frac{2q-1}{N-2}+1\right)} \cdot \left(-\frac{c}{b} \sqrt[N-2]{\frac{a^2}{b^2}}\right)^q \cdot \frac{e^{\frac{2n(1-2q)}{N-2}\pi \mathrm{i}}}{q!}{}_{N-1}F_{N-2}\left[\begin{matrix} \frac{Nq-1}{N(N-2)}, \frac{Nq-1}{N(N-2)} + \frac{1}{N}, \frac{Nq-1}{N(N-2)} + \frac{2}{N}, \cdots, \frac{Nq-1}{N(N-2)} + \frac{N-3}{2N}, \frac{Nq-1}{N(N-2)} \\ \frac{q+1}{N-2}, \frac{q+2}{N-2}, \cdots, \frac{N-4}{N-2}, \frac{N-3}{N-2}, \frac{N-1}{N-2}, \frac{N}{N-2}, \cdots, \frac{q+N-} \\ -\frac{a^2 c^{N-2}}{4b^N (N-2)^{N-2}} \end{matrix}\right]$$

A root of the equation can thus be expressed as the sum of at most $N-1$ hypergeometric functions. Applying this method to the reduced Bring–Jerrard quintic, define the following functions:

$$F_1(t) = {}_4F_3\left(\frac{-1}{20}, \frac{3}{20}, \frac{7}{20}, \frac{11}{20}; \frac{1}{4}, \frac{1}{2}, \frac{3}{4}; \frac{3125t^4}{256}\right)$$

$$F_2(t) = {}_4F_3\left(\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}; \frac{1}{2}, \frac{3}{4}, \frac{5}{4}; \frac{3125t^4}{256}\right)$$

$$F_3(t) = {}_4F_3\left(\frac{9}{20}, \frac{13}{20}, \frac{17}{20}, \frac{21}{20}; \frac{3}{4}, \frac{5}{4}, \frac{3}{2}; \frac{3125t^4}{256}\right)$$

$$F_4(t) = {}_4F_3\left(\frac{7}{10}, \frac{9}{10}, \frac{11}{10}, \frac{13}{10}; \frac{5}{4}, \frac{3}{2}, \frac{7}{4}; \frac{3125t^4}{256}\right)$$

which are the hypergeometric functions that appear in the series formula above. The roots of the quintic are thus:

$$\begin{aligned}
x_1 &= -tF_2(t) \\
x_2 &= -F_1(t) + \tfrac{1}{4}tF_2(t) + \tfrac{5}{32}t^2F_3(t) + \tfrac{5}{32}t^3F_4(t) \\
x_3 &= F_1(t) + \tfrac{1}{4}tF_2(t) + \tfrac{5}{32}t^2F_3(t) + \tfrac{5}{32}t^3F_4(t) \\
x_4 &= -\mathrm{i}F_1(t) + \tfrac{1}{4}tF_2(t) - \tfrac{5}{32}\mathrm{i}t^2F_3(t) - \tfrac{5}{32}t^3F_4(t) \\
x_5 &= \mathrm{i}F_1(t) + \tfrac{1}{4}tF_2(t) - \tfrac{5}{32}\mathrm{i}t^2F_3(t) - \tfrac{5}{32}t^3F_4(t)
\end{aligned}$$

This is essentially the same result as that obtained by the method of differential resolvents developed by James Cockle and Robert Harley in 1860.

23.4.3 The method of differential resolvents

James Cockle[14] and Robert Harley[15] developed a method for solving the quintic by means of differential equations. They consider the roots as being functions of the coefficients, and calculate a differential resolvent based on these equations. The Bring–Jerrard quintic is expressed as a function:

$$f(x) = x^5 - x + a$$

and a function $\phi(a)$ is to be determined such that:

$$f[\phi(a)] = 0$$

The function ϕ must also satisfy the following four differential equations:

$$\frac{df[\phi(a)]}{da} = 0$$

$$\frac{d^2f[\phi(a)]}{da^2} = 0$$

$$\frac{d^3f[\phi(a)]}{da^3} = 0$$

$$\frac{d^4f[\phi(a)]}{da^4} = 0$$

Expanding these and combining them together yields the differential resolvent:

$$\frac{(256-3125a^4)}{1155}\frac{d^4\phi}{da^4} - \frac{6250a^3}{231}\frac{d^3\phi}{da^3} - \frac{4875a^2}{77}\frac{d^2\phi}{da^2} - \frac{2125a}{77}\frac{d\phi}{da} + \phi = 0$$

The solution of the differential resolvent, being a fourth order ordinary differential equation, depends on four constants of integration, which should be chosen so as to satisfy the original quintic. This is a Fuchsian ordinary differential equation of hypergeometric type,[16] whose solution turns out to be identical to the series of hypergeometric functions that arose in Glasser's derivation above.[6]

This method may also be generalized to equations of arbitrarily high degree, with differential resolvents which are partial differential equations, whose solutions involve hypergeometric functions of several variables.[17][18] A general formula for differential resolvents of arbitrary univariate polynomials is given by Nahay's powersum formula. [19][20]

23.4.4 Doyle–McMullen iteration

In 1989, Peter Doyle and Curt McMullen derived an iteration method[21] that solves a quintic in Brioschi normal form:

$$x^5 - 10Cx^3 + 45C^2x - C^2 = 0.$$

The iteration algorithm proceeds as follows:

1. Set $Z = 1 - 1728C$
2. Compute the rational function

$$T_Z(w) = w - 12\frac{g(Z,w)}{g'(Z,w)}$$

where $g(Z,w)$ is a polynomial function given below, and g' is the derivative of $g(Z,w)$ with respect to w

3. Iterate $T_Z[T_Z(w)]$ on a random starting guess until it converges. Call the limit point w_1 and let $w_2 = T_Z(w_1)$.
4. Compute

$$\mu_i = \frac{100Z(Z-1)h(Z,w_i)}{g(Z,w_i)}$$

where $h(Z,w)$ is a polynomial function given below. Do this for both w_1 and $w_2 = T_Z(w_1)$.

5. Finally, compute

$$x_i = \frac{(9+\sqrt{15}\mathrm{i})\mu_i + (9-\sqrt{15}\mathrm{i})\mu_{3-i}}{90}$$

for *i* = 1, 2. These are two of the roots of the Brioschi quintic.

The two polynomial functions $g(Z,w)$ and $h(Z,w)$ are as follows:

$$
\begin{aligned}
g(Z,w) = {} & 91125Z^6 \\
& + (-133650w^2 + 61560w - 193536)Z^5 \\
& + (-66825w^4 + 142560w^3 + 133056w^2 - 61140w + 102400)Z^4 \\
& + (5940w^6 + 4752w^5 + 63360w^4 - 140800w^3)Z^3 \\
& + (-1485w^8 + 3168w^7 - 10560w^6)Z^2 \\
& + (-66w^{10} + 440w^9)Z \\
& + w^{12}
\end{aligned}
$$

$$
\begin{aligned}
h(Z,w) = {} & (1215w - 648)Z^4 \\
& + (-540w^3 - 216w^2 - 1152w + 640)Z^3 \\
& + (378w^5 - 504w^4 + 960w^3)Z^2 \\
& + (36w^7 - 168w^6)Z \\
& + w^9
\end{aligned}
$$

This iteration method produces two roots of the quintic. The remaining three roots can be obtained by using synthetic division to divide the two roots out, producing a cubic equation. It is to be noted that due to the way the iteration is formulated, this method seems to always find two complex conjugate roots of the quintic even when all the quintic coefficients are real and the starting guess is real. This iteration method is derived by from the symmetries of the icosahedron and is closely related to the method Felix Klein describes in his book.[2]

23.5 See also

- Theory of equations

23.6 Notes

[1] Adamchik, Victor (2003). "Polynomial Transformations of Tschirnhaus, Bring, and Jerrard" (PDF). *ACM SIGSAM Bulletin* **37** (3): 91. doi:10.1145/990353.990371.

[2] Klein, Felix (1888). *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*. Trübner & Co. ISBN 0-486-49528-0.

[3] Jerrard, George Birch (1859). *An essay on the resolution of equations*. London: Taylor and Francis.

[4] Adamchik, pp. 92–93

[5] "Solving the Quintic with Mathematica". Wolfram Research.

[6] Drociuk, Richard J. (2000). "On the Complete Solution to the Most General Fifth Degree Polynomial". arXiv:math.GM/0005026 [math.GM].

[7] King, R. Bruce (1996). *Beyond the Quartic Equation*. Birkhäuser. p. 131. ISBN 3-7643-3776-1.

[8] Hermite, Charles (1858). "Sur la résolution de l'équation du cinquème degré". *Comptes Rendus de l'Académie des Sciences* **XLVI** (I): 508–515.

[9] Brioschi, Francesco (1858). "Sul Metodo di Kronecker per la Risoluzione delle Equazioni di Quinto Grado". *Atti dell'i. R. Istituto Lombardo di scienze, lettere ed arti* **I**: 275–282.

[10] Kronecker, Leopold (1858). "Sur la résolution de l'equation du cinquième degré, extrait d'une lettre adressée à M. Hermite". *Comptes Rendus de l'Académie des Sciences* **XLVI** (I): 1150–1152.

[11] Davis, Harold T. (1962). *Introduction to Nonlinear Differential and Integral Equations*. Dover. p. 173. ISBN 0-486-60971-5.

[12] Umemura, Hiroshi (1984). "Resolution of algebraic equations by theta constants". In David Mumford. *Tata Lectures on Theta II*. Birkhäuser. pp. 3.261–3.272. ISBN 3-7643-3109-7.

[13] Glasser, M. Lawrence (1994). "The quadratic formula made hard: A less radical approach to solving equations". arXiv:math.CA/9411224.

[14] Cockle, James (1860). "Sketch of a Theory of Transcendental Roots". *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* **20**: 145–148.

[15] Harley, Robert (1862). "On the Transcendental Solution of Algebraic Equations". *Quart. J. Pure Appl. Math* **5**: 337–361.

[16] Slater, Lucy Joan (1966). *Generalized Hypergeometric Functions*. Cambridge University Press. pp. 42–44. ISBN 978-0-521-06483-5.

[17] Birkeland, Richard (1927). "Über die Auflösung algebraischer Gleichungen durch hypergeometrische Funktionen". *Mathematische Zeitschrift* **26**: 565–578. doi:10.1007/BF01475474.

[18] Mayr, Karl (1937). "Über die Auflösung algebraischer Gleichungssysteme durch hypergeometrische Funktionen". *Monatshefte für Mathematik und Physik* **45**: 280–313. doi:10.1007/BF01707992.

[19] Nahay, John (2004). "Powersum formula for differential resolvents". *International Journal of Mathematics & Mathematical Sciences.* **2004** (7): 365–371. doi:10.1155/S0161171204210602.

[20] Nahay, John (2000). "Linear Differential Resolvents (Doctoral dissertation), Rutgers University, Piscataway, NJ. Richard M. Cohn, advisor.".

[21] Doyle, Peter; Curt McMullen (1989). "Solving the quintic by iteration" (PDF). *Acta Math* **163**: 151–180. doi:10.1007/BF02392735.

- Mirzaei, Raoof(2012). "Spinors and Special functions for Solving Equation of nth degree". International Mathematica Symposium.

23.7 References

- Felix Klein, *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*, trans. George Gavin Morrice, Trübner & Co., 1888. ISBN 0-486-49528-0.
- R. Bruce King, *Beyond the Quartic Equation*, Birkhäuser, 1996. ISBN 3-7643-3776-1
- Harold T. Davis, *Introduction to Nonlinear Differential and Integral Equations*, Dover, 1962, ISBN 0-486-60971-5, Chapter 6, especially Sections 20 and 21

23.8 External links

- M. Hazewinkel (2001), "Tschirnhausen transformation", in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Weisstein, Eric W., "Bring–Jerrard Quintic Form", *MathWorld*.
- Weisstein, Eric W., "Bring Quintic Form", *MathWorld*.

Chapter 24

Bézout matrix

In mathematics, a **Bézout matrix** (or **Bézoutian** or **Bezoutiant**) is a special square matrix associated with two polynomials, introduced by Sylvester (1853) and Cayley (1857) and named after Étienne Bézout. Such matrices are sometimes used to test the stability of a given polynomial.

24.1 Definition

Let $f(z)$ and $g(z)$ be two complex polynomials of degree at most n with coefficients (note that any coefficient could be zero):

$$f(z) = \sum_{i=0}^{n} u_i z^i, \qquad g(z) = \sum_{i=0}^{n} v_i z^i.$$

The **Bézout matrix** of order n associated with the polynomials f and g is

$$B_n(f,g) = (b_{ij})_{i,j=1,\ldots,n}$$

where the coefficients result from the identity

$$\frac{f(x)g(y) - f(y)g(x)}{x-y} = \sum_{i,j=1}^{n} b_{ij}\, x^{i-1}\, y^{j-1}.$$

It is in $\mathbb{C}^{n\times n}$ and the entries of that matrix are such that if we note for each i,j=1,...,n, $m_{ij} = \min\{i, n+1-j\}$, then:

$$b_{ij} = \sum_{k=1}^{m_{ij}} u_{j+k-1}v_{i-k} - u_{i-k}v_{j+k-1}.$$

To each Bézout matrix, one can associate the following bilinear form, called the Bézoutian:

$$\text{Bez} : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C} : (x,y) \mapsto \text{Bez}(x,y) = x^* B_n(f,g) y.$$

24.2 Examples

- For n=3, we have for any polynomials f and g of degree (at most) 3:

$$B_3(f,g) = \begin{bmatrix} u_1v_0 - u_0v_1 & u_2v_0 - u_0v_2 & u_3v_0 - u_0v_3 \\ u_2v_0 - u_0v_2 & u_2v_1 - u_1v_2 + u_3v_0 - u_0v_3 & u_3v_1 - u_1v_3 \\ u_3v_0 - u_0v_3 & u_3v_1 - u_1v_3 & u_3v_2 - u_2v_3 \end{bmatrix}.$$

- Let $f(x) = 3x^3 - x$ and $g(x) = 5x^2 + 1$ be two polynomials. Then:

$$B_4(f,g) = \begin{bmatrix} -1 & 0 & 3 & 0 \\ 0 & 8 & 0 & 0 \\ 3 & 0 & 15 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The last row and column are all zero as *f* and *g* have degree strictly less than *n* (equal 4). The other zero entries are because for each *i*=0,...,n, either u_i or v_i is zero.

24.3 Properties

- $B_n(f,g)$ is symmetric (as a matrix);
- $B_n(f,g) = -B_n(g,f)$;
- $B_n(f,f) = 0$;
- $B_n(f,g)$ is bilinear in (*f*,*g*);
- $B_n(f,g)$ is in $\mathbb{R}^{n\times n}$ if *f* and *g* have real coefficients;
- $B_n(f,g)$ is nonsingular with $n = max(deg(f), deg(g))$ if and only if *f* and *g* have no common roots.
- $B_n(f,g)$ with $n = max(deg(f), deg(g))$ has determinant which is the resultant of *f* and *g*.

24.4 Applications

An important application of Bézout matrices can be found in control theory. To see this, let $f(z)$ be a complex polynomial of degree *n* and denote by *q* and *p* the real polynomials such that $f(iy)=q(y)+ip(y)$ (where *y* is real). We also note *r* for the rank and σ for the signature of $B_n(p,q)$. Then, we have the following statements:

- $f(z)$ has *n*-*r* roots in common with its conjugate;
- the left *r* roots of $f(z)$ are located in such a way that:
  - $(r+\sigma)/2$ of them lie in the open left half-plane, and
  - $(r-\sigma)/2$ lie in the open right half-plane;
- *f* is Hurwitz stable if and only if $B_n(p,q)$ is positive definite.

The third statement gives a necessary and sufficient condition concerning stability. Besides, the first statement exhibits some similarities with a result concerning Sylvester matrices while the second one can be related to Routh-Hurwitz theorem.

24.5 References

- Cayley, Arthur (1857), "Note sur la methode d'elimination de Bezout", *J. Reine Angew. Math.* **53**: 366–367
- Kreĭn, M. G.; Naĭmark, M. A. (1981) [1936], "The method of symmetric and Hermitian forms in the theory of the separation of the roots of algebraic equations", *Linear and Multilinear Algebra* **10** (4): 265–308, doi:10.1080/03081088108817420, ISSN 0308-1087, MR 638124

- Pan, Victor; Bini, Dario (1994). *Polynomial and matrix computations*. Basel, Switzerland: Birkhäuser. ISBN 0-8176-3786-9.
- Pritchard, Anthony J.; Hinrichsen, Diederich (2005). *Mathematical systems theory I: modelling, state space analysis, stability and robustness*. Berlin: Springer. ISBN 3-540-44125-5.
- Sylvester, James Joseph (1853), "On a Theory of the Syzygetic Relations of Two Rational Integral Functions, Comprising an Application to the Theory of Sturm's Functions, and That of the Greatest Algebraical Common Measure", *Philosophical Transactions of the Royal Society of London* (The Royal Society) **143**: 407–548, doi:10.1098/rstl.1853.0018, ISSN 0080-4614, JSTOR 108572

Chapter 25

Caloric polynomial

In differential equations, the *m*th-degree **caloric polynomial** (or **heat polynomial**) is a "parabolically *m*-homogeneous" polynomial *Pm*(*x*, *t*) that satisfies the heat equation

$$\frac{\partial P}{\partial t} = \frac{\partial^2 P}{\partial x^2}.$$

"Parabolically *m*-homogeneous" means

$P(\lambda x, \lambda^2 t) = \lambda^m P(x,t)$ for $\lambda > 0$.

The polynomial is given by

$$P_m(x,t) = \sum_{\ell=0}^{\lfloor m/2 \rfloor} \frac{m!}{\ell!(m-2\ell)!} x^{m-2\ell} t^\ell.$$

It is unique up to a factor.

With $t = -1$, this polynomial reduces to the *m*th-degree Hermite polynomial in *x*.

25.1 References

- Cannon, John Rozier (1984), *The One-Dimensional Heat Equation*, Encyclopedia of Mathematics and Its Applications **23** (1st ed.), Reading/Cambridge: Addison-Wesley Publishing Company/Cambridge University Press, pp. XXV+483, ISBN 978-0-521-30243-2, MR 0747979, Zbl 0567.35001. Contains an extensive bibliography on various topics related to the heat equation.

25.2 External links

- Zeroes of complex caloric functions and singularities of complex viscous Burgers equation

Chapter 26

Casus irreducibilis

In algebra, ***casus irreducibilis*** (Latin for "the irreducible case") is one of the cases that may arise in attempting to solve a cubic equation with integer coefficients with roots that are expressed with radicals. Specifically, if a cubic polynomial is irreducible over the rational numbers and has three real roots, then in order to express the roots with radicals, one must introduce complex-valued expressions, even though the resulting expressions are ultimately real-valued.

One can decide whether a given irreducible cubic polynomial is in *casus irreducibilis* using the discriminant D, via Cardano's formula.[1] Let the cubic equation be given by

$$ax^3 + bx^2 + cx + d = 0.$$

Then the discriminant D appearing in the algebraic solution is given by

$$D = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2.$$

- If $D < 0$, then the polynomial has two complex roots, so *casus irreducibilis* does not apply.
- If $D = 0$, then there are three real roots, and two of them are equal and can be found by the Euclidean algorithm and the quadratic formula. All roots are real and expressible by real radicals. The polynomial is not irreducible.
- If $D > 0$, then there are three distinct real roots. Either a rational root exists and can be found using the rational root test, in which case the cubic polynomial can be factored into the product of a linear polynomial and a quadratic polynomial, the latter of which can be solved via the quadratic formula; or no such factorization can occur, so the polynomial is *casus irreducibilis*: all roots are real, but require complex numbers to express them in radicals.

26.1 Formal statement and proof

More generally, suppose that F is a formally real field, and that $p(x) \in F[x]$ is a cubic polynomial, irreducible over F, but having three real roots (roots in the real closure of F). Then *casus irreducibilis* states that it is impossible to find any solution of $p(x) = 0$ by real radicals.

To prove this, note that the discriminant D is positive. Form the field extension $F(\sqrt{D})$. Since this is F or a quadratic extension of F (depending in whether or not D is a square in F), $p(x)$ remains irreducible in it. Consequently, the Galois group of $p(x)$ over $F(\sqrt{D})$ is the cyclic group C_3. Suppose that $p(x) = 0$ can be solved by real radicals. Then $p(x)$ can be split by a tower of cyclic extensions

$$F \subset F(\sqrt{\Delta}) \subset F(\sqrt{\Delta}, \sqrt[p_1]{\alpha_1}) \subset \cdots \subset K \subset K(\sqrt[3]{\alpha})$$

At the final step of the tower, $p(x)$ is irreducible in the penultimate field K, but splits in $K(\sqrt[3]{\alpha})$ for some α. But this is a cyclic field extension, and so must contain a primitive root of unity.

However, there are no primitive 3rd roots of unity in a real closed field. Indeed, suppose that ω is a primitive 3rd root of unity. Then, by the axioms defining an ordered field, ω, ω^2, and 1 are all positive. But if ω^2>ω, then cubing both sides gives 1>1, a contradiction; similarly if ω>ω^2.

26.2 Solution in non-real radicals

The equation $ax^3 + bx^2 + cx + d = 0$ can be depressed to a monic trinomial by dividing by a and substituting $x = t - \frac{b}{3a}$ (the Tschirnhaus transformation), giving the equation

$$t^3 + pt + q = 0$$

where

$$p = \frac{3ac - b^2}{3a^2}$$

$$q = \frac{2b^3 - 9abc + 27a^2d}{27a^3}.$$

Then regardless of the number of real roots, by Cardano's solution the three roots are given by

$$t_k = \omega_k \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \omega_k^2 \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

where ω_k (k=1, 2, 3) is a cube root of 1: $\omega_1 = 1$, $\omega_2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, and $\omega_3 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, where i is the imaginary unit.

Casus irreducibilis occurs when none of the roots is rational and when all three roots are distinct and real; the case of three distinct real roots occurs if and only if $\frac{q^2}{4} + \frac{p^3}{27} < 0$, in which case Cardano's formula involves first taking the square root of a negative number, which is imaginary, and then taking the cube root of a complex number (which cannot itself be placed in the form $\alpha + \beta i$ with specifically given expressions in real radicals for α and β , since doing so would require independently solving the original cubic). Note that even in the reducible case in which one of three real roots is rational and hence can be factored out by polynomial long division, Cardano's formula (unnecessarily in this case) expresses that root (and the others) in terms of non-real radicals.

26.3 Non-algebraic solution in terms of real quantities

Main article: Cubic function § Trigonometric (and hyperbolic) method

While *casus irreducibilis* cannot be solved in radicals in terms of real quantities, it *can* be solved trigonometrically in terms of real quantities.[2] Specifically, the depressed monic cubic equation $t^3 + pt + q = 0$ is solved by

$$t_k = 2\sqrt{-\frac{p}{3}} \cos\left(\frac{1}{3}\arccos\left(\frac{3q}{2p}\sqrt{\frac{-3}{p}}\right) - k\frac{2\pi}{3}\right) \quad \text{for} \quad k = 0, 1, 2\,.$$

These solutions are in terms of real quantities if and only if $\frac{q^2}{4} + \frac{p^3}{27} < 0$ — i.e., if and only if there are three real roots.

26.4 Relation to angle trisection

The distinction between the reducible and irreducible cubic cases with three real roots is related to the issue of whether or not an angle with rational cosine or rational sine is trisectible by the classical means of compass and unmarked

straightedge. If the cosine of an angle θ is known to have a particular rational value, then one third of this angle has a cosine that is one of the three real roots of the equation

$$4x^3 - 3x - \cos(\theta) = 0.$$

Likewise, if the sine of θ is known to have a particular rational value, then one third of this angle has a sine that is one of the three real roots of the equation

$$-4y^3 + 3y - \sin(\theta) = 0.$$

In either case, if the rational root test reveals a real root of the equation, x or y minus that root can be factored out of the polynomial on the left side, leaving a quadratic that can be solved for the remaining two roots in terms of a square root; then all of these roots are classically constructible since they are expressible in no higher than square roots, so in particular $\cos(\theta/3)$ or $\sin(\theta/3)$ is constructible and so is the associated angle $\theta/3$. On the other hand, if the rational root test shows that there is no real root, then *casus irreducibilis* applies, $\cos(\theta/3)$ or $\sin(\theta/3)$ is not constructible, the angle $\theta/3$ is not constructible, and the angle θ is not classically trisectible.

26.5 Generalization

Casus irreducibilis can be generalized to higher degree polynomials as follows. Let $p \in F[x]$ be an irreducible polynomial which splits in a formally real extension R of F (i.e., p has only real roots). Assume that p has a root in $K \subseteq R$ which is an extension of F by radicals. Then the degree of p is a power of 2, and its splitting field is an iterated quadratic extension of F.[3]

Casus irreducibilis for quintic polynomials is discussed by Dummit.[4]:p.17

26.6 Notes

[1] Cox (2012), Theorem 1.3.1, p. 15.

[2] Cox (2012), Section 1.3B Trigonometric Solution of the Cubic, pp. 18–19.

[3] Cox (2012), Theorem 8.6.5, p. 222.

[4] David S. Dummit Solving Solvable Quintics

26.7 References

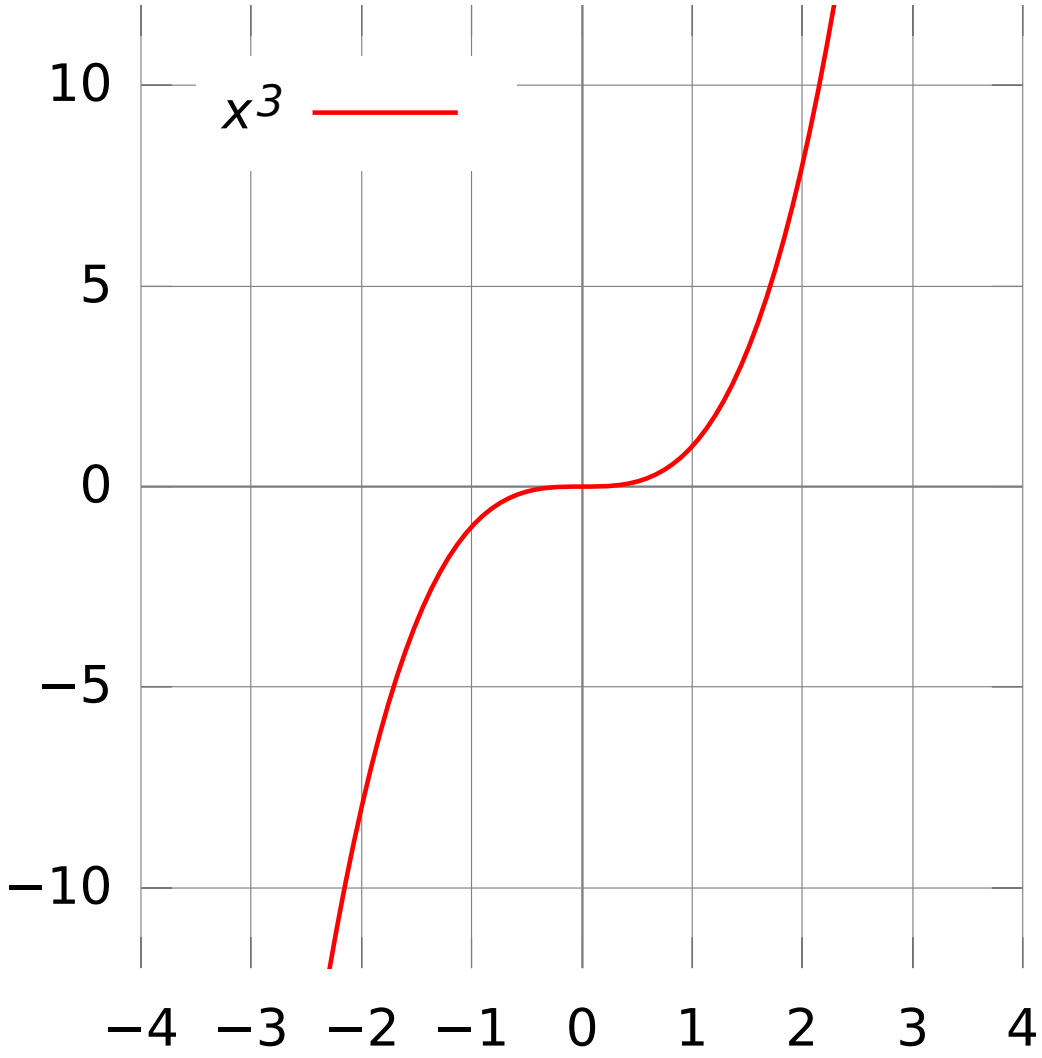
- Cox, David A. (2012), *Galois Theory*, Pure and Applied Mathematics (2nd ed.), John Wiley & Sons, doi:10.1002/9781118218457 ISBN 978-1-118-07205-9. See in particular Section 1.3 Cubic Equations over the Real Numbers (pp. 15–22) and Section 8.6 The Casus Irreducibilis (pp. 220–227).
- van der Waerden, Bartel Leendert (2003), *Modern Algebra I*, F. Blum, J.R. Schulenberg, Springer, ISBN 978-0-387-40624-4

26.8 External links

- casus irreducibilis at PlanetMath.org.

Chapter 27

Cavalieri's quadrature formula



Cavalieri's quadrature formula computes the area under the cubic curve, together with other higher powers.

In calculus, **Cavalieri's quadrature formula**, named for 17th-century Italian mathematician Bonaventura Cavalieri, is the integral

$$\int_0^a x^n \, dx = \tfrac{1}{n+1} \, a^{n+1} \qquad n \geq 0,$$

and generalizations thereof. This is the definite integral form; the indefinite integral form is:

$$\int x^n \, dx = \tfrac{1}{n+1} \, x^{n+1} + C \qquad n \neq -1.$$

There are additional forms, listed below. Together with the linearity of the integral, this formula allows one to compute the integrals of all polynomials.

The term "quadrature" is a traditional term for area; the integral is geometrically interpreted as the area under the curve $y = x^n$. Traditionally important cases are $y = x^2$, the quadrature of the parabola, known in antiquity, and $y = 1/x$, the quadrature of the hyperbola, whose value is a logarithm.

27.1 Forms

27.1.1 Negative *n*

For negative values of n (negative powers of x), there is a singularity at $x = 0$, and thus the definite integral is based at 1, rather than 0, yielding:

$$\int_1^a x^n \, dx = \tfrac{1}{n+1}(a^{n+1} - 1) \qquad n \neq -1.$$

Further, for negative fractional (non-integer) values of n, the power x^n is not well-defined, hence the indefinite integral is only defined for positive x. However for n a negative integer the power x^n is defined for all non-zero x, and the indefinite integrals and definite integrals are defined, and can be computed via a symmetry argument, replacing x by $-x$, and basing the negative definite integral at -1.

Over the complex numbers the definite integral (for negative values of n and x) can be defined via contour integration, but then depends on choice of path, specifically winding number – the geometric issue is that the function defines a covering space with a singularity at 0.

27.1.2 *n* = −1

There is also the exceptional case $n = -1$, yielding a logarithm instead of a power of x:

$$\int_1^a \frac{1}{x} \, dx = \ln a,$$

$$\int \frac{1}{x} \, dx = \ln x + C, \qquad x > 0$$

(where "ln" means the natural logarithm, i.e. the logarithm to the base $e = 2.71828...$).

The improper integral is often extended to negative values of x via the conventional choice:

$$\int \frac{1}{x} \, dx = \ln |x| + C, \qquad x \neq 0.$$

Note the use of the absolute value in the indefinite integral; this is to provide a unified form for the integral, and means that the integral of this odd function is an even function, though the logarithm is only defined for positive inputs, and in fact, different constant values of C can be chosen on either side of 0, since these do not change the derivative. The more general form is thus:[1]

$$\int \frac{1}{x}\,dx = \begin{cases} \ln|x| + C^- & x < 0 \\ \ln|x| + C^+ & x > -0 \end{cases}$$

Over the complex numbers there is not a global antiderivative for $1/x$, due this function defining a non-trivial covering space; this form is special to the real numbers.

Note that the definite integral starting from 1 is not defined for negative values of a, since it passes through a singularity, though since $1/x$ is an odd function, one can base the definite integral for negative powers at -1. If one is willing to use improper integrals and compute the Cauchy principal value, one obtains $\int_{-c}^{c} \frac{1}{x}\,dx = 0$, which can also be argued by symmetry (since the logarithm is odd), so $\int_{-1}^{1} \frac{1}{x}\,dx = 0$, so it makes no difference if the definite integral is based at 1 or -1. As with the indefinite integral, this is special to the real numbers, and does not extend over the complex numbers.

27.1.3 Alternative forms

The integral can also be written with indexes shifted, which simplify the result and make the relation to n-dimensional differentiation and the n-cube clearer:

$$\int_0^a x^{n-1}\,dx = \tfrac{1}{n}a^n \qquad n \geq 1.$$

$$\int x^{n-1}\,dx = \tfrac{1}{n}x^n + C \qquad n \neq 0.$$

More generally, these formulae may be given as:

$\int (ax+b)^n dx = \frac{(ax+b)^{n+1}}{a(n+1)} + C$ (for $n \neq -1$)

$\int \frac{1}{ax+b} dx = \frac{1}{a}\ln|ax+b| + C$

More generally:

$$\int \frac{1}{ax+b}\,dx = \begin{cases} \frac{1}{a}\ln|ax+b| + C^- & x < -b/a \\ \frac{1}{a}\ln|ax+b| + C^+ & x > -b/a \end{cases}$$

27.2 Proof

The modern proof is to use an anti-derivative: the derivative of x^n is shown to be nx^{n-1} – for non-negative integers. This is shown from the binomial formula and the definition of the derivative – and thus by the fundamental theorem of calculus the antiderivative is the integral. This method fails for $\int \frac{1}{x}\,dx$, as the candidate antiderivative is $\frac{1}{0}\cdot x^0$, which is undefined due to division by zero. The logarithm function, which is the actual antiderivative of $1/x$, must be introduced and examined separately.

For positive integers, this proof can be geometrized:[2] if one considers the quantity x^n as the volume of the n-cube (the hypercube in n dimensions), then the derivative is the change in the volume as the side length is changed – this is x^{n-1}, which can be interpreted as the area of n faces, each of dimension $n-1$ (fixing one vertex at the origin, these are the n faces not touching the vertex), corresponding to the cube increasing in size by growing in the direction of these faces – in the 3-dimensional case, adding 3 infinitesimally thin squares, one to each of these faces. Conversely, geometrizing the fundamental theorem of calculus, stacking up these infinitesimal $(n-1)$ cubes yields a (hyper)-pyramid, and n of these pyramids form the n-cube, which yields the formula. Further, there is an n-fold cyclic symmetry of the n-cube around the diagonal cycling these pyramids (for which a pyramid is a fundamental domain). In the case of the cube (3-cube), this is how the volume of a pyramid was originally rigorously established: the cube has 3-fold symmetry, with fundamental domain a pyramids, dividing the cube into 3 pyramids, corresponding to the fact that the volume of a pyramid is one third of the base times the height. This illustrates geometrically the equivalence between the quadrature of the parabola and the volume of a pyramid, which were computed classically by different means.

Alternative proofs exist – for example, Fermat computed the area via an algebraic trick of dividing the domain into certain intervals of unequal length;[3] alternatively, one can prove this by recognizing a symmetry of the graph $y = x^n$ under inhomogeneous dilation (by d in the x direction and d^n in the y direction, algebraicizing the n dimensions of the y direction),[4] or deriving the formula for all integer values by expanding the result for $n = -1$ and comparing coefficients.[5]

27.3 History

A detailed discussion of the history, with original sources, is given in (Laubenbacher & Pengelley 1998, Chapter 3, Analysis: Calculating Areas and Volumes); see also history of calculus and history of integration.

The case of the parabola was proven in antiquity by the ancient Greek mathematician Archimedes in his *The Quadrature of the Parabola* (3rd century BCE), via the method of exhaustion. Of note is that Archimedes computed the area *inside* a parabola – a so-called "parabolic segment" – rather than the area under the graph $y = x^2$, which is instead the perspective of Cartesian geometry. These are equivalent computations, but reflect a difference in perspective. The Ancient Greeks, among others, also computed the volume of a pyramid or cone, which is mathematically equivalent.

In the 11th century, the Islamic mathematician Ibn al-Haytham (known as *Alhazen* in Europe) computed the integrals of cubics and quartics (degree three and four) via mathematical induction, in his *Book of Optics*.[6]

The case of higher integers was computed by Cavalieri for n up to 9, using his method of indivisibles (Cavalieri's principle).[7] He interpreted these as higher integrals as computing higher-dimensional volumes, though only informally, as higher-dimensional objects were as yet unfamiliar.[8] This method of quadrature was then extended by Italian mathematician Evangelista Torricelli to other curves such as the cycloid, then the formula was generalized to fractional and negative powers by English mathematician John Wallis, in his *Arithmetica Infinitorum* (1656), which also standardized the notion and notation of rational powers – though Wallis incorrectly interpreted the exceptional case $n = -1$ (quadrature of the hyperbola) – before finally being put on rigorous ground with the development of integral calculus.

Prior to Wallis's formalization of fractional and negative powers, which allowed *explicit* functions $y = x^{p/q}$, these curves were handled *implicitly,* via the equations $x^p = ky^q$ and $x^p y^q = k$ (p and q always positive integers) and referred to respectively as **higher parabolae** and **higher hyperbolae** (or "higher parabolas" and "higher hyperbolas"). Pierre de Fermat also computed these areas (except for the exceptional case of -1) by an algebraic trick – he computed the quadrature of the higher hyperbolae via dividing the line into equal intervals, and then computed the quadrature of the higher parabolae by using a division into *unequal* intervals, presumably by inverting the divisions he used for hyperbolae.[9] However, as in the rest of his work, Fermat's techniques were more ad hoc tricks than systematic treatments, and he is not considered to have played a significant part in the subsequent development of calculus.

Of note is that Cavalieri only compared areas to areas and volumes to volumes – these always having *dimensions,* while the notion of considering an area as consisting of *units* of area (relative to a standard unit), hence being unitless, appears to have originated with Wallis;[10][11] Wallis studied fractional and negative powers, and the alternative to treating the computed values as unitless numbers was to interpret fractional and negative dimensions.

The exceptional case of -1 (the standard hyperbola) was first successfully treated by Grégoire de Saint-Vincent in his *Opus geometricum quadrature circuli et sectionum coni* (1647), though a formal treatment had to wait for the development of the natural logarithm, which was accomplished by Nicholas Mercator in his *Logarithmotechnia* (1668).

27.4 References

[1] "Reader Survey: log|x| + C", Tom Leinster, *The* n-*category Café*, March 19, 2012

[2] (Barth 2004), (Carter & Champanerkar 2006)

[3] See Rickey.

[4] (Wildberger 2002)

[5] (Bradley 2003)

[6] Victor J. Katz (1995), "Ideas of Calculus in Islam and India", *Mathematics Magazine* **68** (3): 163–174 [165–9 & 173–4]

[7] (Struik 1986, pp. 215–216)

[8] (Laubenbacher & Pengelley 1998) – see Informal pedagogical synopsis of the Analysis chapter for brief form

[9] See Rickey reference for discussion and further references.

[10] Ball, 281

[11] Britannica, 171

27.4.1 History

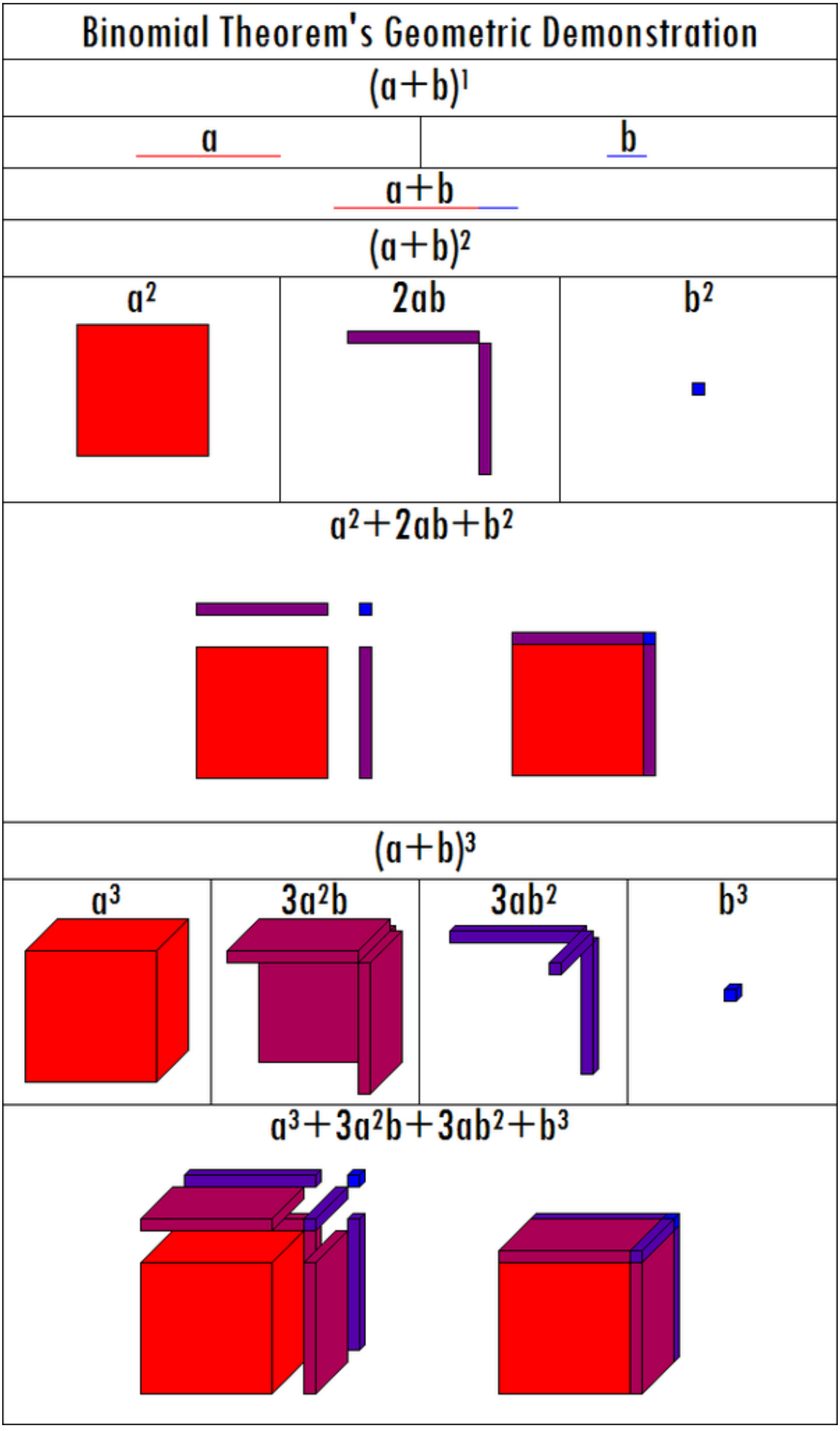
- Cavalieri, *Geometria indivisibilibus (continuorum nova quadam ratione promota)* (Geometry, exposed in a new manner with the aid of indivisibles of the continuous), 1635.
- Cavalieri, *Exercitationes Geometricae Sex* ("Six Geometrical Exercises"), 1647
  - in Dirk Jan Struik, editor, *A source book in mathematics, 1200–1800* (Princeton University Press, Princeton, New Jersey, 1986). ISBN 0-691-08404-1, ISBN 0-691-02397-2 (pbk).
- *Mathematical expeditions: chronicles by the explorers,* Reinhard Laubenbacher, David Pengelley, 1998, Section 3.4: "Cavalieri Calculates Areas of Higher Parabolas", pp. 123–127/128
- *A short account of the history of mathematics,* Walter William Rouse Ball, "Cavalieri", p. 278–281
- "Infinitesimal calculus", *Encyclopaedia of Mathematics*
- *The Britannica Guide to Analysis and Calculus,* by Educational Britannica Educational, p. 171 – discusses Wallace primarily

27.4.2 Proofs

- "Fermat's Integration of Powers", in *Historical Notes for Calculus Teachers* by V. Frederick Rickey – gives Fermat's algebraic proof of the formula in modern language
- Wildberger, N. J. (2002). "A new proof of Cavalieri's quadrature formula". *The American Mathematical Monthly* **109** (9): 843–845. doi:10.2307/3072373.
- Bradley, David M. (May 2003). "Remark on Cavalieri's quadrature formula". *The American Mathematical Monthly* **110** (5): 437. arXiv:math/0505059. Bibcode:2005math.....5059B, appeared in print at end of Zeros of the Alternating Zeta Function on the Line R(S) = 1
- Barth, N. R. (2004). "Computing Cavalieri's quadrature formula by a symmetry of the n-cube". *The American Mathematical Monthly* **111** (9): 811–813. doi:10.2307/4145193.
- Carter, J. Scott; Champanerkar, Abhijit (2006). "A geometric method to compute some elementary integrals". arXiv:math/0608722 [math.HO].
- *A geometric proof of Cavalieri's quadrature formula,* Ilan Vardi

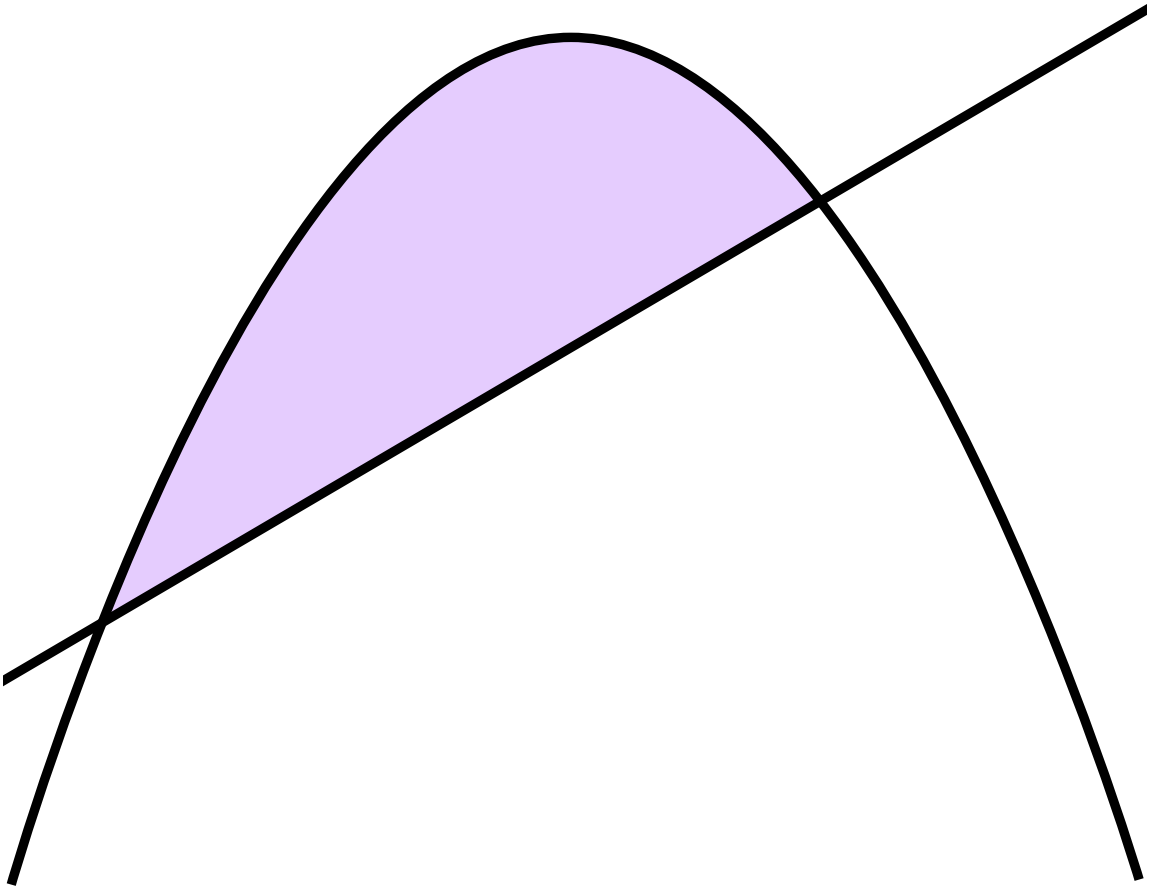
27.5 External links

- Weisstein, Eric W., "Cavalieri's Quadrature Formula", *MathWorld*.
- Cavalieri Integration
- D. J. Struik, *A Source Book in Mathematics, 1200-1800*, p. 214



The derivative $(x^n)' = nx^{n-1}$ *can be geometrized as the infinitesimal change in volume of the* n*-cube, which is the area of* n *faces, each of dimension* n − *1.*

Integrating this picture – stacking the faces – geometrizes the fundamental theorem of calculus, yielding a decomposition of the n-cube



Archimedes computed the area of parabolic segments in his The Quadrature of the Parabola.

Chapter 28

Characteristic polynomial

This article is about the characteristic polynomial of a matrix or of an endomorphism of vector spaces. For the characteristic polynomial of a matroid, see Matroid. For that of a graded poset, see Graded poset.

In linear algebra, the **characteristic polynomial** of a square matrix is a polynomial, which is invariant under matrix similarity and has the eigenvalues as roots. It has the determinant and the trace of the matrix as coefficients. The **characteristic polynomial** of an endomorphism of vector spaces of finite dimension is the characteristic polynomial of the matrix of the endomorphism over any base; it does not depend on the choice of a basis. The **characteristic equation** is the equation obtained by equating to zero the characteristic polynomial.

The **characteristic polynomial of a graph** is the characteristic polynomial of its adjacency matrix. It is a graph invariant, though it is not complete: the smallest pair of non-isomorphic graphs with the same characteristic polynomial have five nodes.[1]

28.1 Motivation

Given a square matrix A, we want to find a polynomial whose zeros are the eigenvalues of A. For a diagonal matrix A, the characteristic polynomial is easy to define: if the diagonal entries are a_1, a_2, a_3, etc. then the characteristic polynomial will be:

$$(t - a_1)(t - a_2)(t - a_3)\cdots .$$

This works because the diagonal entries are also the eigenvalues of this matrix.

For a general matrix A, one can proceed as follows. A scalar λ is an eigenvalue of A if and only if there is an eigenvector $\mathbf{v} \neq 0$ such that

$$A\mathbf{v} = \lambda\mathbf{v},$$

or

$$(\lambda I - A)\mathbf{v} = 0$$

(where $\boldsymbol{I}$ is the identity matrix). Since $\mathbf{v}$ is non-zero, this means that the matrix $\lambda\,\boldsymbol{I} - A$ is singular (non-invertible), which in turn means that its determinant is 0. Thus the roots of the function $\det(\lambda\,\boldsymbol{I} - A)$ are the eigenvalues of A, and it is clear that this determinant is a polynomial in λ.

28.2 Formal definition

We consider an $n \times n$ matrix A. The characteristic polynomial of A, denoted by $p_A(t)$, is the polynomial defined by

$$p_A(t) = \det(t\boldsymbol{I} - A)$$

where $\boldsymbol{I}$ denotes the n-by-n identity matrix.

Some authors define the characteristic polynomial to be det(A - $t\,\boldsymbol{I}$). That polynomial differs from the one defined here by a sign $(-1)^n$, so it makes no difference for properties like having as roots the eigenvalues of A; however the current definition always gives a monic polynomial, whereas the alternative definition always has constant term det(A).

28.3 Examples

Suppose we want to compute the characteristic polynomial of the matrix

$$A = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}.$$

We now compute the determinant of

$$tI - A = \begin{pmatrix} t-2 & -1 \\ 1 & t-0 \end{pmatrix}$$

which is $(t-2)t - 1(-1) = t^2 - 2t + 1$, the characteristic polynomial of A.

Another example uses hyperbolic functions of a hyperbolic angle φ. For the matrix take

$$A = \begin{pmatrix} \cosh(\phi) & \sinh(\phi) \\ \sinh(\phi) & \cosh(\phi) \end{pmatrix}.$$

Its characteristic polynomial is

$$\det(tI - A) = (t - \cosh(\phi))^2 - \sinh^2(\phi) = t^2 - 2t\ \cosh(\phi) + 1 = (t - e^{\phi})(t - e^{-\phi}).$$

28.4 Properties

The polynomial $pA(t)$ is monic (its leading coefficient is 1) and its degree is n. The most important fact about the characteristic polynomial was already mentioned in the motivational paragraph: the eigenvalues of A are precisely the roots of $pA(t)$ (this also holds for the minimal polynomial of A, but its degree may be less than n). The coefficients of the characteristic polynomial are all polynomial expressions in the entries of the matrix. In particular its constant coefficient pA (0) is det(−A) = $(-1)^n$ det(A), the coefficient of t^n is one, and the coefficient of t^{n-1} is tr(−A) = −tr(A), where tr(A) is the matrix trace of A. (The signs given here correspond to the formal definition given in the previous section;[2] for the alternative definition these would instead be det(A) and $(-1)^{n-1}$ tr(A) respectively.[3])

For a 2×2 matrix A, the characteristic polynomial is thus given by

$$t^2 - \operatorname{tr}(A)t + \det(A).$$

Using the language of exterior algebra, one may compactly express the characteristic polynomial of an n×n matrix A as

$$p_A(t) = \sum_{k=0}^{n} t^{n-k}(-1)^k \operatorname{tr}(\Lambda^k A)$$

where $\operatorname{tr}(\Lambda^k \mathrm{A})$ is the trace of the k^{th} exterior power of A, which has dimension $\binom{n}{k}$. This trace may be computed as the sum of all principal minors of A of size k; when the characteristic is 0 it may alternatively be computed as a single determinant, that of the $k \times k$ matrix,

$$\frac{1}{k!}\begin{vmatrix} \operatorname{tr} A & k-1 & 0 & \cdots & \\ \operatorname{tr} A^2 & \operatorname{tr} A & k-2 & \cdots & \\ \vdots & \vdots & & \ddots & \vdots \\ \operatorname{tr} A^{k-1} & \operatorname{tr} A^{k-2} & & \cdots & 1 \\ \operatorname{tr} A^k & \operatorname{tr} A^{k-1} & & \cdots & \operatorname{tr} A \end{vmatrix}.$$

The Cayley–Hamilton theorem states that replacing t by A in the characteristic polynomial (interpreting the resulting powers as matrix powers, and the constant term c as c times the identity matrix) yields the zero matrix. Informally speaking, every matrix satisfies its own characteristic equation. This statement is equivalent to saying that the minimal polynomial of A divides the characteristic polynomial of A.

Two similar matrices have the same characteristic polynomial. The converse however is not true in general: two matrices with the same characteristic polynomial need not be similar.

The matrix A and its transpose have the same characteristic polynomial. A is similar to a triangular matrix if and only if its characteristic polynomial can be completely factored into linear factors over K (the same is true with the minimal polynomial instead of the characteristic polynomial). In this case A is similar to a matrix in Jordan normal form.

28.5 Characteristic polynomial of a product of two matrices

If A and B are two square $n \times n$ matrices then characteristic polynomials of AB and BA coincide:

$$p_{AB}(t) = p_{BA}(t).$$

When A is non-singular this result follows from the fact that AB and BA are similar:

$$BA = A^{-1}(AB)A.$$

For the case where both A and B are singular, one may remark that the desired identity is an equality between polynomials in t and the coefficients of the matrices. Thus, to prove this equality, it suffices to prove that it is verified on a non-empty open subset (for the usual topology, or, more generally, for the Zariski topology) of the space of all the coefficients. As the non-singular matrices form such an open subset of the space of all matrices, this proves the result.

More generally, if A is a matrix of order $m \times n$ and B is a matrix of order $n \times m$, then AB is $m \times m$ and BA is $n \times n$ matrix, and one has

$$p_{BA}(t) = t^{n-m} p_{AB}(t).$$

To prove this, one may suppose $n > m$, by exchanging, if needed, A and B. Then, by bordering A on the bottom by $n - m$ rows of zeros, and B on the right, by, $n - m$ columns of zeros, one gets two $n \times n$ matrices A' and B' such that $B'A' = BA$, and $A'B'$ is equal to AB bordered by $n - m$ rows and columns of zeros. The result follows from the case of square matrices, by comparing the characteristic polynomials of $A'B'$ and AB.

28.6 Secular function and secular equation

28.6.1 Secular function

The term **secular function** has been used for what is now called *characteristic polynomial* (in some literature the term secular function is still used). The term comes from the fact that the characteristic polynomial was used to calculate secular perturbations (on a time scale of a century, i.e. slow compared to annual motion) of planetary orbits, according to Lagrange's theory of oscillations.

28.6.2 Secular equation

Secular equation may have several meanings.

- In linear algebra it is sometimes used in place of characteristic equation.
- In astronomy it is the algebraic or numerical expression of the magnitude of the inequalities in a planet's motion that remain after the inequalities of a short period have been allowed for.[4]
- In molecular orbital calculations relating to the energy of the electron and its wave function it is also used instead of the characteristic equation.

28.7 See also

- Characteristic equation
- Minimal polynomial
- Invariants of tensors
- Companion matrix

28.8 References

[1] "Characteristic Polynomial of a Graph - Wolfram MathWorld". Retrieved August 26, 2011.

[2] Proposition 28 in these lecture notes

[3] Theorem 4 in these lecture notes

[4] "secular equation". Retrieved January 21, 2010.

- T.S. Blyth & E.F. Robertson (1998) *Basic Linear Algebra*, p 149, Springer ISBN 3-540-76122-5 .
- John B. Fraleigh & Raymond A. Beauregard (1990) *Linear Algebra* 2nd edition, p 246, Addison-Wesley ISBN 0-201-11949-8 .
- Werner Greub (1974) *Linear Algebra* 4th edition, pp 120–5, Springer, ISBN 0-387-90110-8 .
- Paul C. Shields (1980) *Elementary Linear Algebra* 3rd edition, p 274, Worth Publishers ISBN 0-87901-121-1 .
- Gilbert Strang (1988) *Linear Algebra and Its Applications* 3rd edition, p 246, Brooks/Cole ISBN 0-15-551005-3 .

28.9 External links

- R. Skip Garibaldi. The characteristic polynomial and determinant are not ad hoc constructions. http://arxiv.org/abs/math/0203276

Chapter 29

Coefficient

For other uses, see Coefficient (disambiguation).

In mathematics, a **coefficient** is a multiplicative factor in some term of a polynomial, a series or any expression; it is usually a number, but in any case does not involve any variables of the expression. For instance in

$$7x^2 - 3xy + 1.5 + y$$

the first two terms respectively have the coefficients 7 and −3. The third term 1.5 is a constant. The final term does not have any explicitly written coefficient, but is considered to have coefficient 1, since multiplying by that factor would not change the term. Often coefficients are numbers as in this example, although they could be parameters of the problem, as *a*, *b*, and *c*, where "c" is a constant, in

$$ax^2 + bx + c$$

when it is understood that these are not considered variables. Thus a polynomial in one variable *x* can be written as

$$a_k x^k + \cdots + a_1 x^1 + a_0$$

for some integer k , where $a_k, \ldots, a_1, a_0$ are coefficients; to allow this kind of expression in all cases one must allow introducing terms with 0 as coefficient. For the largest i with $a_i \neq 0$ (if any), a_i is called the **leading coefficient** of the polynomial. So for example the leading coefficient of the polynomial

$$4x^5 + x^3 + 2x^2$$

is 4.

Specific coefficients arise in mathematical identities, such as the binomial theorem which involves binomial coefficients; these particular coefficients are tabulated in Pascal's triangle.

29.1 Linear algebra

In linear algebra, the **leading coefficient** of a row in a matrix is the first nonzero entry in that row. So, for example, given

$$M = \begin{pmatrix} 1 & 2 & 0 & 6 \\ 0 & 2 & 9 & 4 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

The leading coefficient of the first row is 1; 2 is the leading coefficient of the second row; 4 is the leading coefficient of the third row, and the last row does not have a leading coefficient.

Though coefficients are frequently viewed as constants in elementary algebra, they can be variables more generally. For example, the coordinates $(x_1, x_2, \ldots, x_n)$ of a vector v in a vector space with basis $\{e_1, e_2, \ldots, e_n\}$, are the coefficients of the basis vectors in the expression

$$v = x_1e_1 + x_2e_2 + \cdots + x_ne_n.$$

29.2 Examples of physical coefficients

1. *Coefficient of Thermal Expansion* (thermodynamics) (dimensionless) - Relates the change in temperature to the change in a material's dimensions.
2. *Partition Coefficient* (*KD*) (chemistry) - The ratio of concentrations of a compound in two phases of a mixture of two immiscible solvents at equilibrium. H2O is a coefficient
3. *Hall coefficient* (electrical physics) - Relates a magnetic field applied to an element to the voltage created, the amount of current and the element thickness. It is a characteristic of the material from which the conductor is made.
4. *Lift coefficient* (*CL* or *CZ*) (Aerodynamics) (dimensionless) - Relates the lift generated by an airfoil with the dynamic pressure of the fluid flow around the airfoil, and the plan-form area of the airfoil.
5. *Ballistic coefficient* (BC) (Aerodynamics) (units of kg/m^2) - A measure of a body's ability to overcome air resistance in flight. BC is a function of mass, diameter, and drag coefficient.
6. *Transmission Coefficient* (quantum mechanics) (dimensionless) - Represents the probability flux of a transmitted wave relative to that of an incident wave. It is often used to describe the probability of a particle tunnelling through a barrier.
7. *Damping Factor* a.k.a. *viscous damping coefficient* (Physical Engineering) (units of newton-seconds per meter) - relates a damping force with the velocity of the object whose motion is being damped.

A coefficient is a number placed in front of a term in a chemical equation to indicate how many molecules (or atoms) take part in the reaction. For example, in the formula

$$2H_2 + O_2 \rightarrow 2H_2O$$

the number 2's in front of H_2 and H_2O are stoichiometric coefficients.

29.3 See also

- Degree of a polynomial
- Monic polynomial

29.4 References

- Sabah Al-hadad and C.H. Scott (1979) *College Algebra with Applications*, page 42, Winthrop Publishers, Cambridge Massachusetts ISBN 0-87626-140-3 .
- Gordon Fuller, Walter L Wilson, Henry C Miller, (1982) *College Algebra*, 5th edition, page 24, Brooks/Cole Publishing, Monterey California ISBN 0-534-01138-1 .
- Steven Schwartzman (1994) *The Words of Mathematics: an etymological dictionary of mathematical terms used in English*, page 48, Mathematics Association of America, ISBN 0-88385-511-9.

Chapter 30

Coefficient diagram method

In control theory, the **coefficient diagram method** (CDM) is an algebraic approach applied to a polynomial loop in the parameter space, where a special diagram called a "*coefficient diagram*" is used as the vehicle to carry the necessary information, and as the criterion of good design.[1] The performance of the closed loop system is monitored by the coefficient diagram.

The most considerable advantages of CDM can be listed as follows:[2]

1. The design procedure is easily understandable, systematic and useful. Therefore, the coefficients of the CDM controller polynomials can be determined more easily than those of the PID or other types of controller. This creates the possibility of an easy realisation for a new designer to control any kind of system.

2. There are explicit relations between the performance parameters specified before the design and the coefficients of the controller polynomials as described in.[3] For this reason, the designer can easily realize many control systems having different performance properties for a given control problem in a wide range of freedom.

3. The development of different tuning methods is required for time delay processes of different properties in PID control. But it is sufficient to use the single design procedure in the CDM technique. This is an outstanding advantage.[4]

4. It is particularly hard to design robust controllers realizing the desired performance propefties for unstable, integrating and oscillatory processes having poles near the imaginary axis. It has been reported that successful designs can be achieved even in these cases by using CDM.[5]

5. It is theoretically proven that CDM design is equivalent to LQ design with proper state augmentation. Thus, CDM can be considered an “improved LQG”, because the order of the controller is smaller and weight selection rules are also given.[6]

It is usually required that the controller for a given plant should be designed under some practical limitations. The controller is desired to be of minimum degree, minimum phase (if possible) and stable. It must have enough bandwidth and power rating limitations. If the controller is designed without considering these limitations, the robustness property will be very poor, even though the stability and time response requirements are met. CDM controllers designed while considering all these problems is of the lowest degree, has a convenient bandwidth and results with a unit step time response without an overshoot. These properties guarantee the robustness, the sufficient damping of the disturbance effects and the low economic property.[7]

Although the main principles of CDM have been known since the 1950s,[8][9][10] the first systematic method was proposed by Shunji Manabe.[11] He developed a new method that easily builds a target characteristic polynomial to meet the desired time response. CDM is an algebraic approach combining classical and modern control theories and uses polynomial representation in the mathematical expression. The advantages of the classical and modern control techniques are integrated with the basic principles of this method, which is derived by making use of the previous experience and knowledge of the controller design. Thus, an efficient and fertile control method has appeared as a tool with which control systems can be designed without needing much experience and without confronting many problems.

Many control systems have been designed successfully using CDM.[12][13] It is very easy to design a controller under the conditions of stability, time domain performance and robustness. The close relations between these conditions and coefficients of the characteristic polynomial can be simply determined. This means that CDM is effective not

only for control system design but also for controller parameters tuning.

30.1 See also

- Polynomials

30.2 References

[1] S. Manabe (1998), "*Coefficient Diagram Method*", 14th IFAC Symp. on Automatic Control in Aerospace, Seoul.

[2] S.E. Hamamci, "*A robust polynomial-based control for stable processes with time delay*", Electrical Engineering, vol: 87, pp.163–172, 2005.

[3] S. Manabe (1998), "*Coefficient Diagram Method*", 14th IFAC Symp. on Automatic Control in Aerospace, Seoul.

[4] S.E. Hamamci, I. Kaya and D.P. Atherton, "*Smith predictor design by CDM*", Proceedings of the ECC'01 European Control Conference, Semina´rio de Vilar, Porto, Portugal, 2001.

[5] S. Manabe, "*A low cost inverted pendulum system for control system education*", The 3rd IFAC Symposium on advances in Control Education, Tokyo, 1994.

[6] S. Manabe, "*Analytical weight selection for LQ design*", Proceedings of the 8th Workshop on Astrodynamics and Flight Mechanics, Sagamihara, ISAS, 1998.

[7] S. Manabe and Y.C. Kim, "*Recent development of coefficient diagram method*", Proceedings of the ASSC'2000 3rd Asian Control Conference, Shanghai, 2000.

[8] D. Graham and R.C. Lathrop, "*The synthesis of optimum transient response: criteria and standard forms*", AIEE Trans., vol:72, pp.273–288, 1953.

[9] P. Naslin, *Essentials of optimal control*, Boston Technical Publishers, Cambridge, MA, 1969.

[10] A.V. Lipatov and N. Sokolov, "*Some sufficient conditions for stability and instability of continuous linear stationary systems*", Automat. Remote Control, vol:39, pp.1285–1291, 1979.

[11] Y.C. Kim and S. Manabe, "*Introduction to coefficient diagram method*" Proceedings of the SSSC'01, Prague, 2001.

[12] S. Manabe, "*A low cost inverted pendulum system for control system education*", The 3rd IFAC Symposium on advances in Control Education, Tokyo, 1994.

[13] S.E. Hamamci, M. Koksal and S. Manabe, "*On the control of some nonlinear systems with the coefficient diagram method*", Proceedings of the 4th Asian Control Conference, Singapore, 2002.

30.3 External links

- Coefficient Diagram Method

.

Chapter 31

Complex conjugate root theorem

In mathematics, the **complex conjugate root theorem** states that if P is a polynomial in one variable with real coefficients, and $a + bi$ is a root of P with a and b real numbers, then its complex conjugate $a - bi$ is also a root of P.[1]

It follows from this (and the fundamental theorem of algebra), that if the degree of a real polynomial is odd, it must have at least one real root.[2] That fact can also be proven by using the intermediate value theorem.

31.1 Examples and consequences

- The polynomial $x^2 + 1 = 0$ has roots $\pm i$.
- Any real square matrix of odd degree has at least one real eigenvalue. For example, if the matrix is orthogonal, then 1 or −1 is an eigenvalue.
- The polynomial

  $$x^3 - 7x^2 + 41x - 87$$

  has roots

  $$3,\ 2 + 5i,\ 2 - 5i,$$

  and thus can be factored as

  $$(x - 3)(x - 2 - 5i)(x - 2 + 5i).$$

  In computing the product of the last two factors, the imaginary parts cancel, and we get

  $$(x - 3)(x^2 - 4x + 29).$$

  The non-real factors come in pairs which when multiplied give quadratic polynomials with real coefficients. Since every polynomial with complex coefficients can be factored into 1st-degree factors (that is one way of stating the fundamental theorem of algebra), it follows that every polynomial with real coefficients can be factored into factors of degree no higher than 2: just 1st-degree and quadratic factors.

31.1.1 Corollary on odd-degree polynomials

It follows from the present theorem and the fundamental theorem of algebra that if the degree of a real polynomial is odd, it must have at least one real root.[2]

This can be proved as follows.

- Since non-real complex roots come in conjugate pairs, there are an even number of them;
- But a polynomial of odd degree has an odd number of roots;
- Therefore some of them must be real.

This requires some care in the presence of multiple roots; but a complex root and its conjugate do have the same multiplicity (and this lemma is not hard to prove). It can also be worked around by considering only irreducible polynomials; any real polynomial of odd degree must have an irreducible factor of odd degree, which (having no multiple roots) must have a real root by the reasoning above.

This corollary can also be proved directly by using the intermediate value theorem.

31.2 Simple proof

One proof of the theorem is as follows:[2]

Consider the polynomial

$$P(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n$$

where all *ar* are real. Suppose some complex number ζ is a root of *P*, that is $P(\zeta) = 0$. It needs to be shown that

$$P(\overline{\zeta}) = 0$$

as well.

If $P(\zeta) = 0$, then

$$a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_n\zeta^n = 0$$

which can be put as

$$\sum_{r=0}^{n} a_r \zeta^r = 0.$$

Now

$$P(\overline{\zeta}) = \sum_{r=0}^{n} a_r \left(\overline{\zeta}\right)^r$$

and given the properties of complex conjugation,

$$\sum_{r=0}^{n} a_r \left(\overline{\zeta}\right)^r = \sum_{r=0}^{n} a_r \overline{\zeta^r} = \sum_{r=0}^{n} \overline{a_r \zeta^r} = \overline{\sum_{r=0}^{n} a_r \zeta^r}.$$

Since,

$$\overline{\sum_{r=0}^{n} a_r \zeta^r} = \overline{0}$$

it follows that

$$\sum_{r=0}^{n} a_r \left(\overline{\zeta}\right)^r = \overline{0} = 0.$$

That is,

$$P(\overline{\zeta}) = a_0 + a_1\overline{\zeta} + a_2 \left(\overline{\zeta}\right)^2 + \cdots + a_n \left(\overline{\zeta}\right)^n = 0.$$

31.3 Notes

[1] Anthony G. O'Farell and Gary McGuire (2002). "Complex numbers, 8.4.2 Complex roots of real polynomials". *Maynooth Mathematical Olympiad Manual*. Logic Press. p. 104. ISBN 0954426908. Preview available at Google books

[2] Alan Jeffrey (2005). "Analytic Functions". *Complex Analysis and Applications*. CRC Press. pp. 22–23. ISBN 158488553X.

Chapter 32

Complex quadratic polynomial

A **complex quadratic polynomial** is a quadratic polynomial whose coefficients are complex numbers.

32.1 Forms

When the quadratic polynomial has only one variable (univariate), one can distinguish its 4 main forms:

- The general form: $f(x) = a_2x^2 + a_1x + a_0 \qquad$ where $\qquad a_2 \neq 0$
- The factored form used for logistic map $f_r(x) = rx(1 - x)$
- $f_\theta(x) = x^2 + e^{2\pi\theta i}x$ which has an indifferent fixed point with multiplier $\lambda = e^{2\pi\theta i}$ at the origin[1]
- The monic and centered form, $f_c(x) = x^2 + c$

The **monic and centered form** has the following properties:

- It is the simplest form of a nonlinear function with one coefficient (parameter),
- It is an unicritical polynomial, i.e. it has one critical point,
- It is a centered polynomial (the sum of its critical points is zero),[2]
- It can be **postcritically finite**, i.e. If the orbit of the critical point is finite. It is when critical point is periodic or preperiodic.[3]
- It is a unimodal function,
- It is a rational function,
- It is an entire function.

32.2 Conjugation

32.2.1 Between forms

Since $f_c(x)$ is affine conjugate to the general form of the quadratic polynomial it is often used to study complex dynamics and to create images of Mandelbrot, Julia and Fatou sets.

When one wants change from θ to c :[4]

$$c = c(\theta) = \frac{e^{2\pi\theta i}}{2}\left(1 - \frac{e^{2\pi\theta i}}{2}\right)$$

When one wants change from r to c :[5]

$$c = c(r) = \frac{1-(r-1)^2}{4}$$

32.2.2 With doubling map

There is semi-conjugacy between the dyadic transformation (here named doubling map) and the quadratic polynomial.

32.3 Family

The family of quadratic polynomials $f_c : z \to z^2 + c$ parametrised by $c \in \mathbb{C}$ is called:

- **the Douady-Hubbard family of quadratic polynomials**[6]
- **quadratic family**

32.4 Map

The monic and centered form is typically used with variable z and parameter c :

$$f_c(z) = z^2 + c.$$

When it is used as an evolution function of the discrete nonlinear dynamical system:

$$z_{n+1} = f_c(z_n)$$

it is named **quadratic map**:[7]

$$f_c : z \to z^2 + c.$$

This iteration leads to the Mandelbrot set.

32.5 Notation

Here f^n denotes the *n*-th iteration of the function f not exponentiation

$$f_c^n(z) = f_c^1(f_c^{n-1}(z))$$

so

$$z_n = f_c^n(z_0).$$

Because of the possible confusion it is customary to write $f^{\circ n}$ for the *n*th iterate of the function f.

32.6 Critical items

32.6.1 Critical point

A **critical point** of f_c is a point z_{cr} in the dynamical plane such that the derivative vanishes:

$f'_c(z_{cr}) = 0.$

Since

$f'_c(z) = \frac{d}{dz} f_c(z) = 2z$

implies

$z_{cr} = 0$

we see that the only (finite) critical point of f_c is the point $z_{cr} = 0$.
z_0 is an initial point for Mandelbrot set iteration.[8]

32.6.2 Critical value

A **critical value** z_{cv} of f_c is the image of a critical point:

$z_{cv} = f_c(z_{cr})$

Since

$z_{cr} = 0$

we have

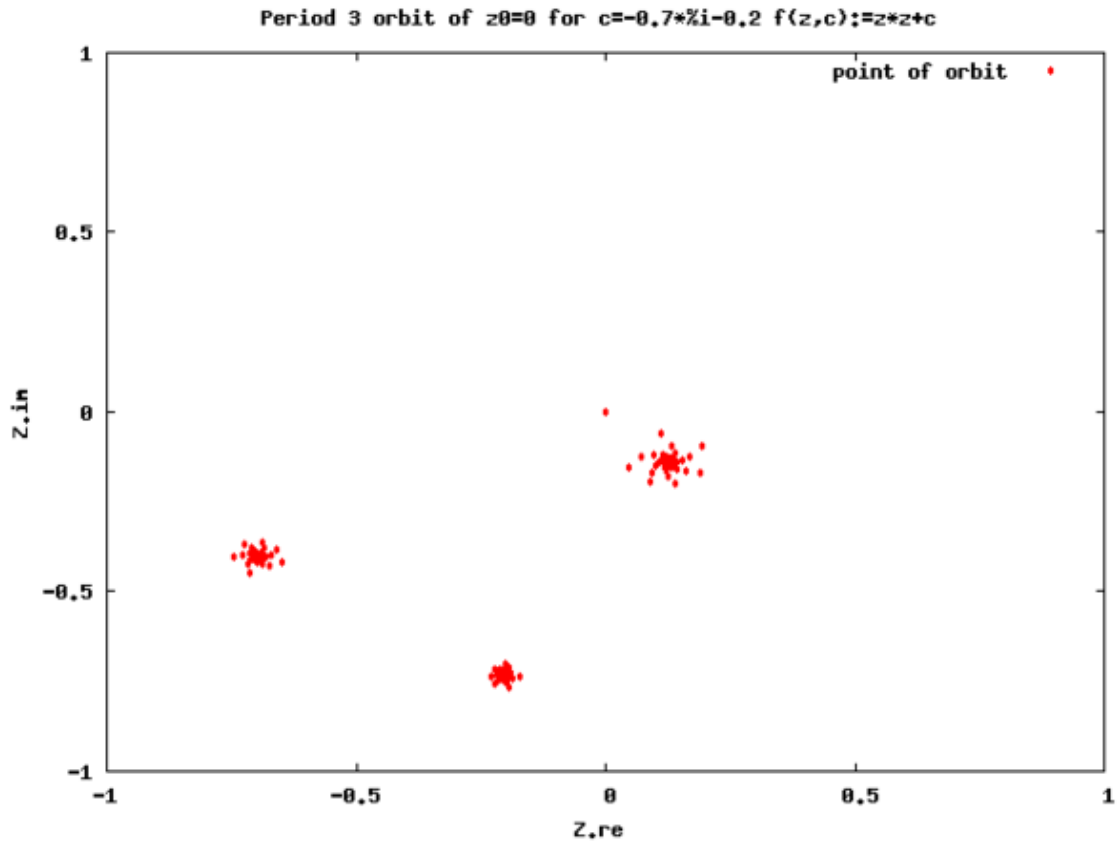
$z_{cv} = c.$

So the parameter c is the critical value of $f_c(z)$.

32.6.3 Critical orbit

Forward orbit of a critical point is called a **critical orbit**. Critical orbits are very important because every attracting periodic orbit attracts a critical point, so studying the critical orbits helps us understand the dynamics in the Fatou set.[9][10][11]

$z_0 = z_{cr} = 0$
$z_1 = f_c(z_0) = c$
$z_2 = f_c(z_1) = c^2 + c$
$z_3 = f_c(z_2) = (c^2 + c)^2 + c$
...
This orbit falls into an attracting periodic cycle.



Dynamical plane with critical orbit falling into 3-period cycle

32.6.4 Critical sector

The critical sector is a sector of the dynamical plane containing the critical point.

32.6.5 Critical polynomial

$P_n(c) = f_c^n(z_{cr}) = f_c^n(0)$

so

$P_0(c) = 0$

$P_1(c) = c$

$P_2(c) = c^2 + c$

$P_3(c) = (c^2 + c)^2 + c$

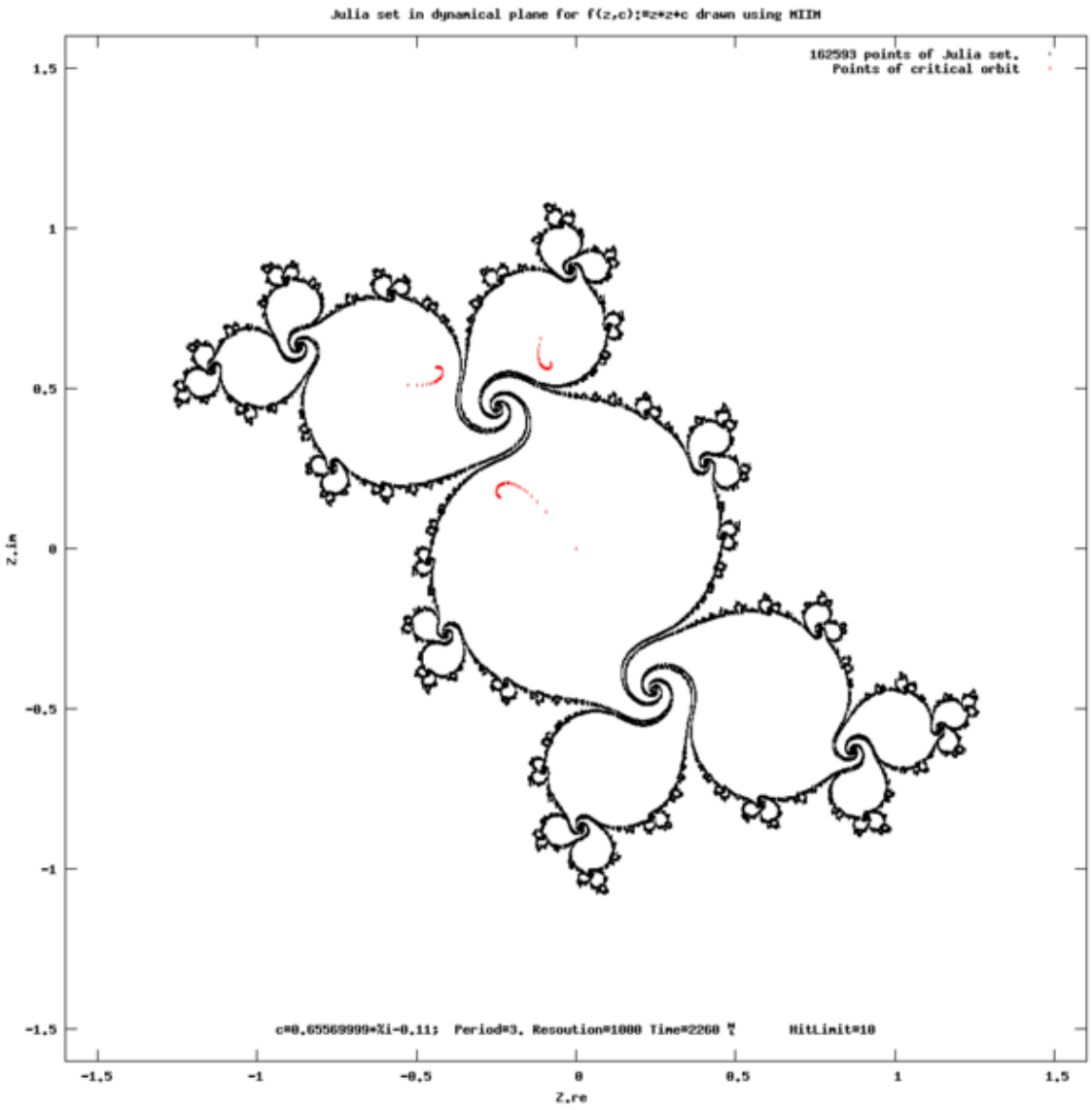
These polynomials are used for:

- finding centers of these Mandelbrot set components of period n. Centers are roots of n-th critical polynomials

$centers = \{c : P_n(c) = 0\}$

- finding roots of Mandelbrot set components of period n (local minimum of $P_n(c)$)
- Misiurewicz points

$M_{n,k} = \{c : P_k(c) = P_{k+n}(c)\}$



Dynamical plane with Julia set and critical orbit.

32.6.6 Critical curves

Diagrams of critical polynomials are called **critical curves**.[12]

These curves create skeleton of bifurcation diagram.[13] (the dark lines[14])

32.7 Planes

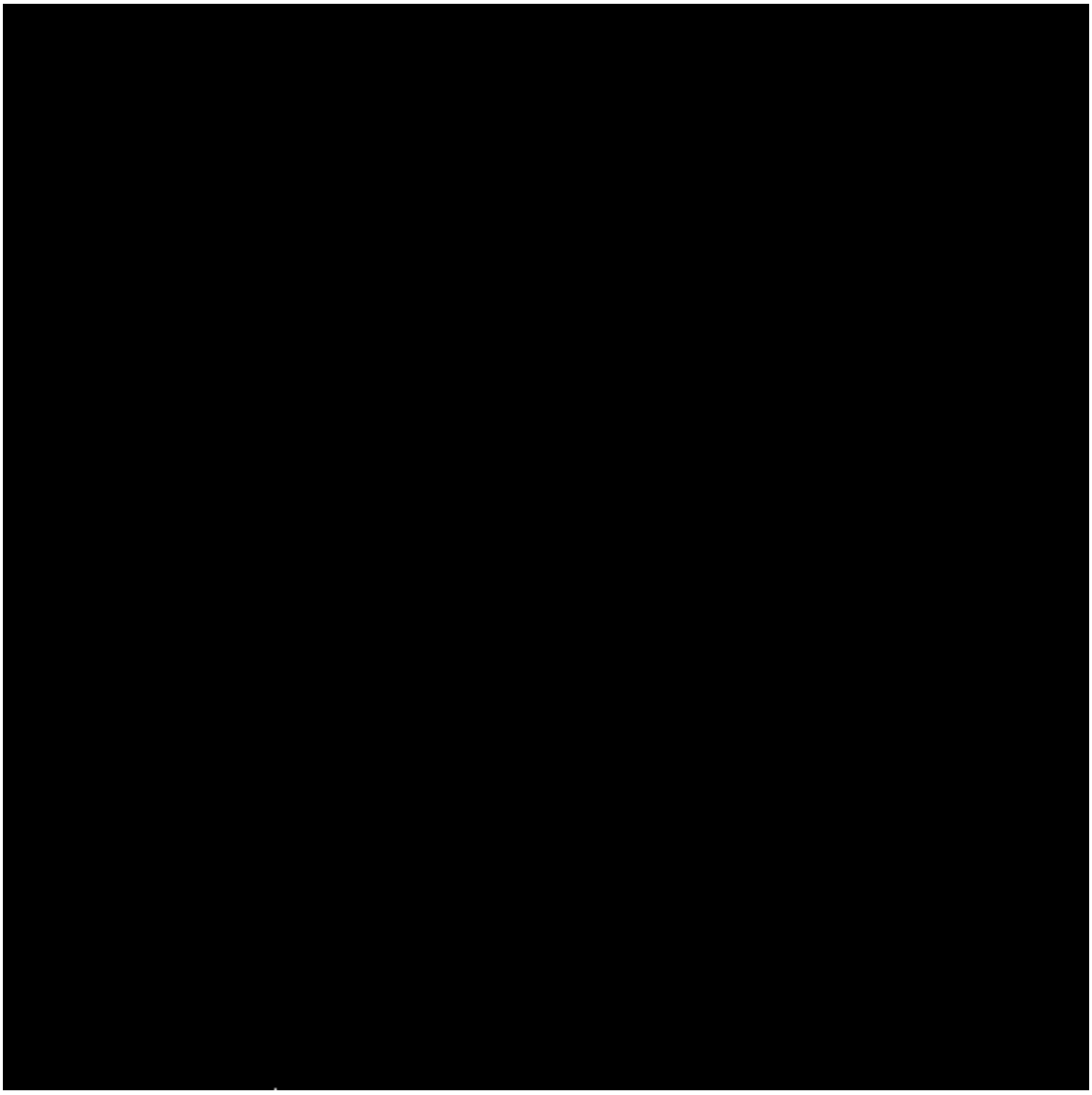
One can use the Julia-Mandelbrot 4-dimensional space for a global analysis of this dynamical system.[15]

In this space there are 2 basic types of 2-D planes:

- the dynamical (dynamic) plane, f_c -plane or **c-plane**
- the parameter plane or **z-plane**

There is also another plane used to analyze such dynamical systems **w-plane**:

- the conjugation plane[16]



Dynamical plane : changes of critical orbit along internal ray of main cardioid for angle 1/6

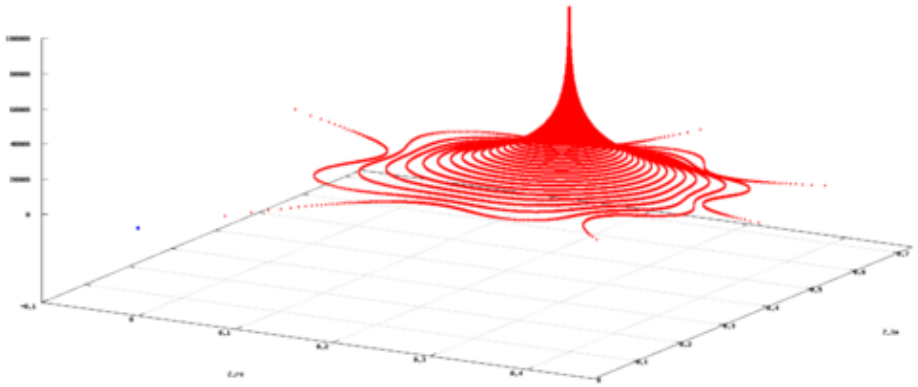
- model plane[17]

32.7.1 Parameter plane

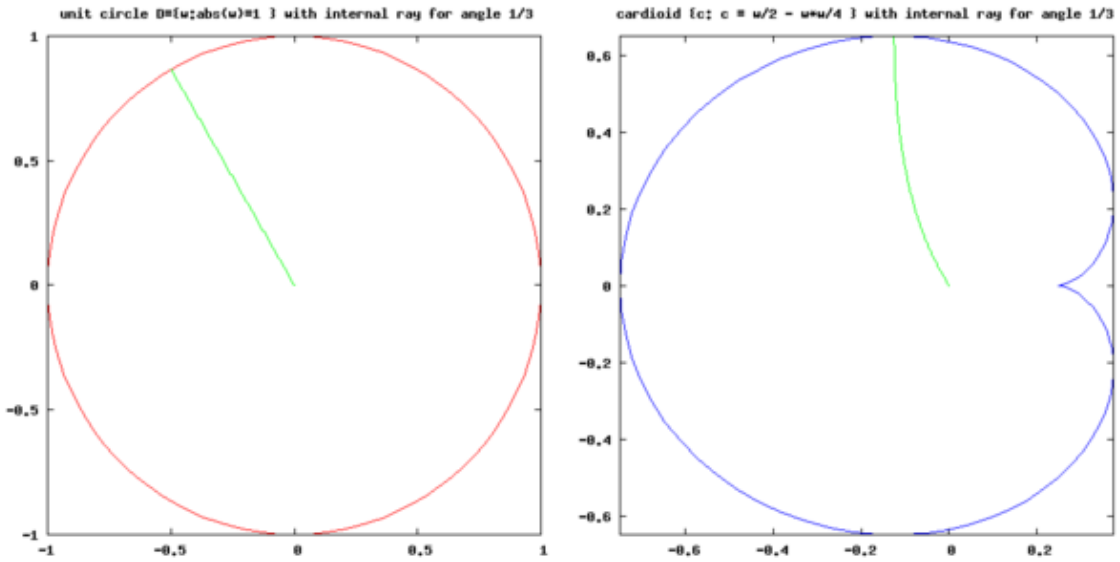
The phase space of a quadratic map is called its **parameter plane**. Here:
$z0 = z_{cr}$ is constant and c is variable.
There is no dynamics here. It is only a set of parameter values. There are no orbits on the parameter plane.
The parameter plane consists of:

- The Mandelbrot set
  - The bifurcation locus = boundary of Mandelbrot set
  - Bounded hyperbolic components of the Mandelbrot set = interior of Mandelbrot set[18]

There are many different subtypes of the parameter plane.[19][20]



Critical orbit tending to weakly attracting fixed point with abs(multiplier)=0.99993612384259



w-plane and c-plane

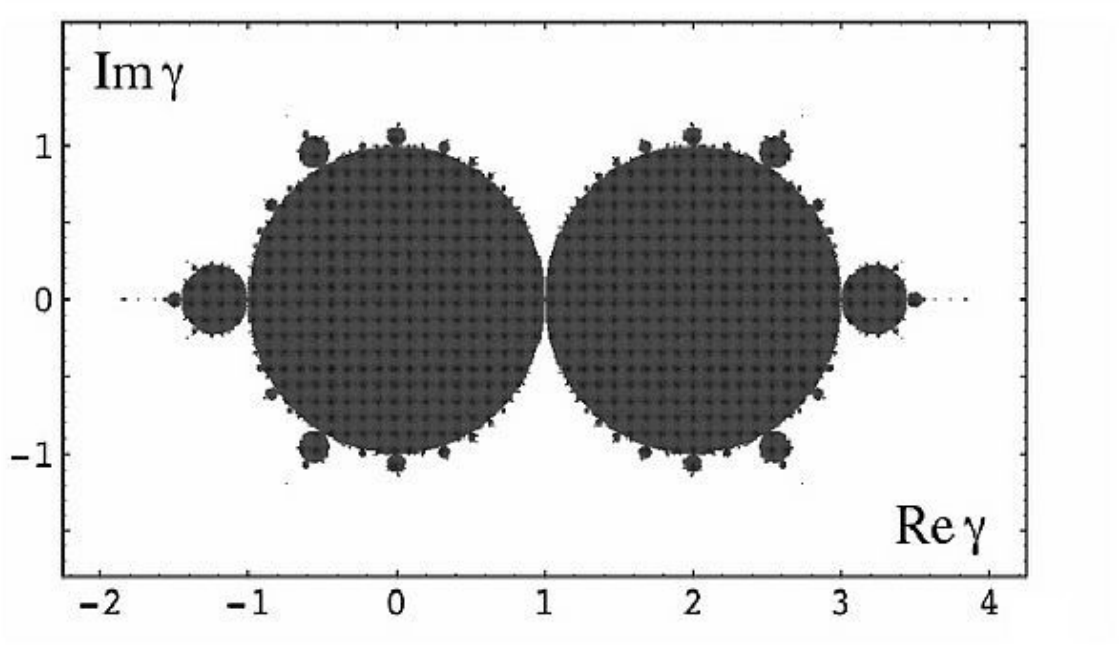
32.7.2 Dynamical plane

On the dynamical plane one can find:

- The Julia set
- The Filled Julia set
- The Fatou set
- Orbits

The dynamical plane consists of:

- Fatou set
- Julia set



Gamma parameter plane for complex logistic map $z_{n+1} = \gamma z_n \left(1 - z_n\right)$,

Here, c is a constant and z is a variable.

The two-dimensional dynamical plane can be treated as a Poincaré cross-section of three-dimensional space of continuous dynamical system.[21][22]

Dynamical z-planes can be divided in two groups :

- f_0 plane for $c = 0$
- f_c planes (all other planes for $c \neq 0$)

32.8 Derivatives

32.8.1 Derivative with respect to *c*

On parameter plane:

- c is a variable
- $z_0 = 0$ is constant

The first derivative of $f_c^n(z_0)$ with respect to c is

$$z'_n = \frac{d}{dc} f_c^n(z_0).$$

This derivative can be found by iteration starting with

$$z'_0 = \frac{d}{dc} f_c^0(z_0) = 1$$

and then replacing at every consecutive step

$$z'_{n+1} = \frac{d}{dc} f_c^{n+1}(z_0) = 2 \cdot f_c^n(z) \cdot \frac{d}{dc} f_c^n(z_0) + 1 = 2 \cdot z_n \cdot z'_n + 1.$$

This can easily be verified by using the chain rule for the derivative.

This derivative is used in the distance estimation method for drawing a Mandelbrot set.

32.8.2 Derivative with respect to z

On dynamical plane:

- z is a variable
- c is a constant

at a **fixed point** z_0

$$f'_c(z_0) = \frac{d}{dz} f_c(z_0) = 2z_0$$

at a **periodic point** z_0 of period p

$$(f_c^p)'(z_0) = \frac{d}{dz} f_c^p(z_0) = \prod_{i=0}^{p-1} f'_c(z_i) = 2^p \prod_{i=0}^{p-1} z_i.$$

It is used to check the stability of periodic (also fixed) points.

at **nonperiodic point**:

z'_n

This derivative can be found by iteration starting with

$z'_0 = 1$

and then :

$z'_n = 2 * z_{n-1} * z'_{n-1}$

This dervative is used for computing external distance to Julia set.

32.8.3 Schwarzian derivative

The Schwarzian derivative (SD for short) of f is:[23]

$$(Sf)(z) = \frac{f'''(z)}{f'(z)} - \frac{3}{2}\left(\frac{f''(z)}{f'(z)}\right)^2$$

32.9 See also

- Misiurewicz point
- Periodic points of complex quadratic mappings
- Mandelbrot set
- Julia set
- Milnor–Thurston kneading theory

32.10 References

[1] Michael Yampolsky, Saeed Zakeri : Mating Siegel quadratic polynomials.

[2] Bodil Branner: Holomorphic dynamical systems in the complex plane. Mat-Report No 1996-42. Technical University of Denmark

[3] Alfredo Poirier : On Post Critically Finite Polynomials Part One: Critical Portraits

[4] Michael Yampolsky, Saeed Zakeri : Mating Siegel quadratic polynomials.

[5] stackexchange questions : Show that the familiar logistic map ...

[6] Yunping Jing : Local connectivity of the Mandelbrot set at certain infinitely renormalizable points Complex Dynamics and Related Topics, New Studies in Advanced Mathematics, 2004, The International Press, 236-264

[7] Weisstein, Eric W. "Quadratic Map." From MathWorld--A Wolfram Web Resourc

[8] Java program by Dieter Röß showing result of changing initial point of Mandelbrot iterations

[9] M. Romera, G. Pastor, and F. Montoya : Multifurcations in nonhyperbolic fixed points of the Mandelbrot map. Fractalia 6, No. 21, 10-12 (1997)

[10] Burns A M : Plotting the Escape: An Animation of Parabolic Bifurcations in the Mandelbrot Set. Mathematics Magazine, Vol. 75, No. 2 (Apr., 2002), pp. 104-116

[11] Khan Academy : Mandelbrot Spirals 2

[12] The Road to Chaos is Filled with Polynomial Curves by Richard D. Neidinger and R. John Annen III. American Mathematical Monthly, Vol. 103, No. 8, October 1996, pp. 640-653

[13] Hao, Bailin (1989). *Elementary Symbolic Dynamics and Chaos in Dissipative Systems*. World Scientific. ISBN 9971-5-0682-3.

[14] M. Romera, G. Pastor and F. Montoya, "Misiurewicz points in one-dimensional quadratic maps", Physica A, 232 (1996), 517-535. Preprint

[15] Julia-Mandelbrot Space at Mu-ency by Robert Munafo

[16] Carleson, Lennart, Gamelin, Theodore W.: Complex Dynamics Series: Universitext, Subseries: Universitext: Tracts in Mathematics, 1st ed. 1993. Corr. 2nd printing, 1996, IX, 192 p. 28 illus., ISBN 978-0-387-97942-7

[17] Holomorphic motions and puzzels by P Roesch

[18] Lasse Rempe, Dierk Schleicher : Bifurcation Loci of Exponential Maps and Quadratic Polynomials: Local Connectivity, Triviality of Fibers, and Density of Hyperbolicity

[19] Alternate Parameter Planes by David E. Joyce

[20] exponentialmap by Robert Munafo

[21] Mandelbrot set by Saratov group of theoretical nonlinear dynamics

[22] Moehlis, Kresimir Josic, Eric T. Shea-Brown (2006) Periodic orbit. Scholarpedia,

[23] The Schwarzian Derivative & the Critical Orbit by Wes McKinney 18.091 20 April 2005

32.11 External links

- M. Nevins and D. Rogers, “Quadratic maps as dynamical systems on the p-adic numbers”
- Wolf Jung : Homeomorphisms on Edges of the Mandelbrot Set. Ph.D. thesis of 2002

Chapter 33

Constant function

Not to be confused with function constant.

In mathematics, a **constant function** is a function whose (output) value is the same for every input value.[1][2][3] For example, the function $y(x) = 4$ is a constant function because the value of $y(x)$ is 4 regardless of the input value x (see image).

33.1 Basic properties

As a real-valued function of a real-valued argument, a constant function has the general form $y(x) = c$ or just $y = c$.

> **Example:** The function $y(x) = 2$ or just $y = 2$ is the specific constant function where the output value is $c = 2$. The domain of this function is the set of all real numbers $\mathbb{R}$. The codomain of this function is just $\{2\}$. The independent variable x does not appear on the right side of the function expression and so its value is "vacuously substituted". Namely $y(0)=2$, $y(-2.7)=2$, $y(\pi)=2$,.... No matter what value of x is input, the output is "2".
>
> **Real-world example:** A store where every item is sold for the price of 1 euro.

The graph of the constant function $y = c$ is a **horizontal line** in the plane that passes through the point $(0, c)$.[4]

In the context of a polynomial in one variable x, the **non-zero constant function** is a polynomial of degree 0 and its general form is $f(x) = c\,,\ c \neq 0$. This function has no intersection point with the x-axis, that is, it has no root (zero). On the other hand, the polynomial $f(x) = 0$ is the **identically zero function**. It is the (trivial) constant function and every x is a root. Its graph is the x-axis in the plane.[5]

A constant function is an even function, i.e. the graph of a constant function is symmetric with respect to the y-axis.

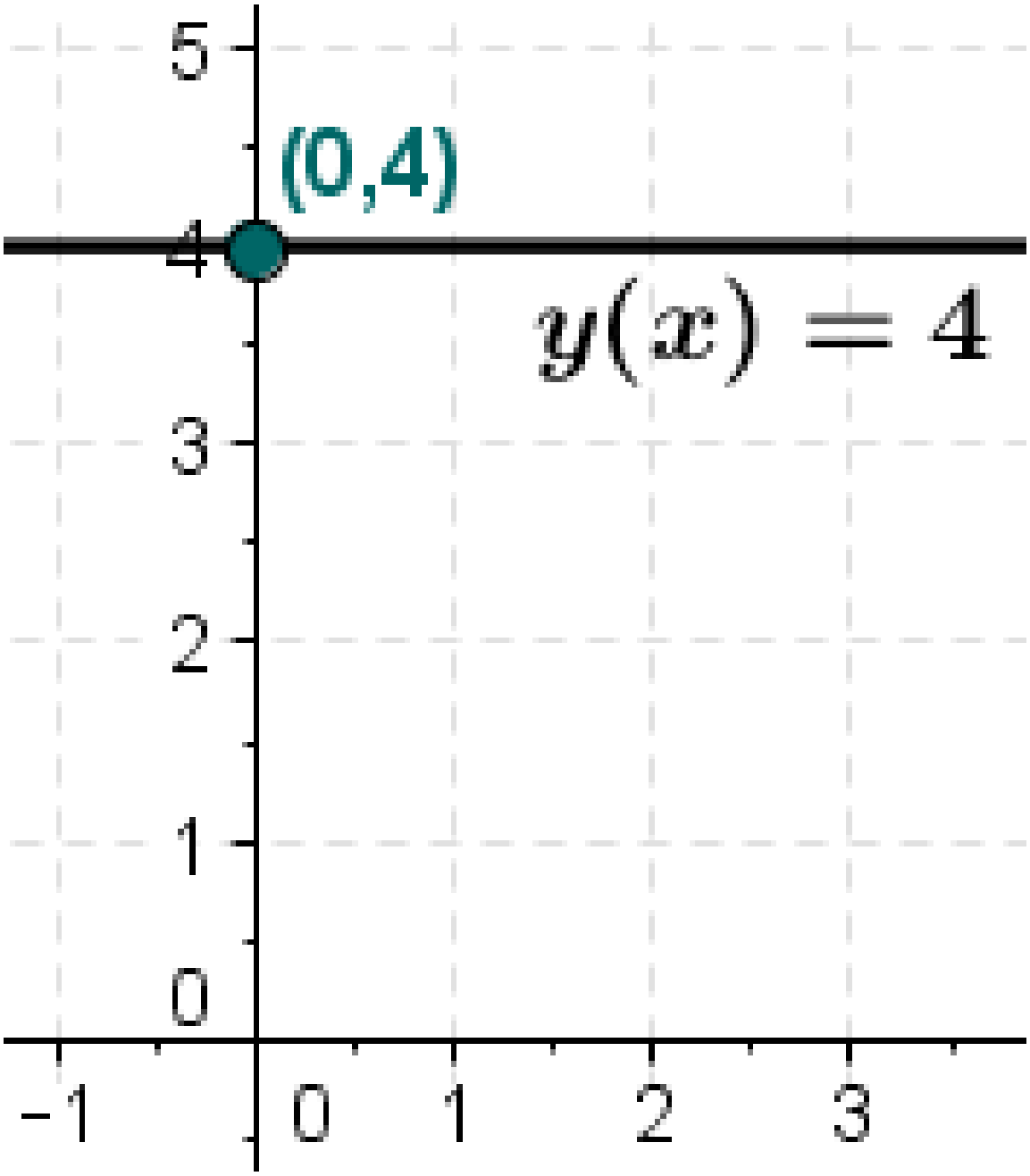
In the context where it is defined, the derivative of a function is a measure of the rate of change of function values with respect to change in input values. Because a constant function does not change, its derivative is 0.[6] This is often written: $(c)' = 0$. The converse is also true. Namely, if $y'(x)=0$ for all real numbers x, then $y(x)$ is a constant function.[7]

> **Example:** Given the constant function $y(x) = -\sqrt{2}$. The derivative of y is the identically zero function $y'(x) = (-\sqrt{2})' = 0$.

33.2 Other properties

For functions between preordered sets, constant functions are both order-preserving and order-reversing; conversely, if f is both order-preserving and order-reversing, and if the domain of f is a lattice, then f must be constant.

- Every constant function whose domain and codomain are the same is idempotent.



Constant function y=*4*

- Every constant function between topological spaces is continuous.
- A constant function factors through the one-point set, the terminal object in the category of sets. This observation is instrumental for F. William Lawvere's axiomatization of set theory, the Elementary Theory of the Category of Sets (ETCS).[8]
- Every set X is isomorphic to the set of constant functions into it. For each element x and any set Y, there is a unique function $\tilde{x} : Y \to X$ such that $\tilde{x}(y) = x$ for all $y \in Y$. Conversely, if a function $f : X \to Y$ satisfies $f(y) = f(y')$ for all $y, y' \in Y$, f is by definition a constant function.
  - As a corollary, the one-point set is a generator in the category of sets.
  - Every set X is canonically isomorphic to the function set X^1 , or hom set $hom(1, X)$ in the category of sets, where 1 is the one-point set. Because of this, and the adjunction between cartesian products and hom in the category of sets (so there is a canonical isomorphism between functions of two variables and functions of one variable valued in functions of another (single) variable, $hom(X \times Y, Z) \cong$

$hom(X(hom(Y,Z))$) the category of sets is a closed monoidal category with the cartesian product of sets as tensor product and the one-point set as tensor unit. In the isomorphisms $\lambda : 1 \times X \cong X \cong X \times 1 : \rho$ natural in X, the left and right unitors are the projections p_1 and p_2 the ordered pairs $(*, x)$ and $(x, *)$ respectively to the element x , where $*$ is the unique point in the one-point set.

A function on a connected set is locally constant if and only if it is constant.

33.3 References

[1] Tanton, James (2005). *Encyclopedia of Mathematics*. Facts on File, New York. p. 94. ISBN 0-8160-5124-0.

[2] C.Clapham, J.Nicholson (2009). "Oxford Concise Dictionary of Mathematics, Constant Function" (PDF). Addison-Wesley. p. 175. Retrieved January 2014.

[3] Weisstein, Eric (1999). *CRC Concise Encyclopedia of Mathematics*. CRC Press, London. p. 313. ISBN 0-8493-9640-9.

[4] Dawkins, Paul (2007). "College Algebra". Lamar University. p. 224. Retrieved January 2014.

[5] Carter, John A.; Cuevas, Gilbert J.; Holliday, Berchie; Marks, Daniel; McClure, Melissa S.publisher=Glencoe/McGraw-Hill School Pub Co (2005). "1". *Advanced Mathematical Concepts - Pre-calculus with Applications, Student Edition* (1 ed.). p. 22. ISBN 978-0078682278.

[6] Dawkins, Paul (2007). "Derivative Proofs". Lamar University. Retrieved January 2014.

[7] "Zero Derivative implies Constant Function". Retrieved January 2014.

[8] Leinster, Tom (27 Jun 2011). "An informal introduction to topos theory". Retrieved 11 November 2014.

- Herrlich, Horst and Strecker, George E., *Category Theory*, Heldermann Verlag (2007).

33.4 External links

- Weisstein, Eric W., "Constant Function", *MathWorld*.
- Constant function at PlanetMath.org.

Chapter 34

Constant term

In mathematics, a **constant term** is a term in an algebraic expression that has a value that is constant or cannot change, because it does not contain any modifiable variables. For example, in the quadratic polynomial

$$x^2 + 2x + 3,$$

the 3 is a constant term.

After like terms are combined, an algebraic expression will have at most one constant term. Thus, it is common to speak of the quadratic polynomial

$$ax^2 + bx + c,$$

where x is the variable, and has a constant term of c. If $c = 0$, then the constant term will not actually appear when the quadratic is written.

It is notable that a term that is constant, with a constant as a multiplicative coefficient added to it (although this expression could be more simply written as their product), still constitutes a constant term as a variable is still not present in the new term. Although the expression is modified, the term (and coefficient) itself classifies as constant. However, should this introduced coefficient contain a variable, while the original number has a constant meaning, this has no bearing if the new term stays constant as the introduced coefficient will always override the constant expression - for example, in $(x + 1)(x - 2)$ when x is multiplied by 2, the result, 2x, is not constant; while 1 * -2 is -2 and still a constant.

Any polynomial written in standard form has a unique constant term, which can be considered a coefficient of x^0. In particular, the constant term will always be the lowest degree term of the polynomial. This also applies to multivariate polynomials. For example, the polynomial

$$x^2 + 2xy + y^2 - 2x + 2y - 4$$

has a constant term of −4, which can be considered to be the coefficient of x^0y^0, where the variables are become eliminated by exponentiated to 0 (any number exponentiated to 0 becomes 1). For any polynomial, the constant term can be obtained by substituting in 0 instead of each variable; thus, eliminating each variable. The concept of exponentiation to 0 can be extended to power series and other types of series, for example in this power series:

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots,$$

a_0 is the constant term. In general a constant term is one that does not involve any variables at all. However in expressions that involve terms with other types of factors than constants and powers of variables, the notion of constant term cannot be used in this sense, since that would lead to calling "4" the constant term of $(x - 3)^2 + 4$, whereas substituting 0 for x in this polynomial makes it evaluate to 13.

34.1 See also

- Constant (mathematics)

Chapter 35

Content (algebra)

In algebra, the **content** of a polynomial with integer coefficients is the greatest common factor of its coefficients. Thus, e.g., the content of $12x^3 + 30x - 20$ equals 2, since this is the greatest common factor of 12, 30, and -20. The definition may be extended to polynomials with coefficients in any fixed unique factorization domain.

A polynomial is *primitive* if it has content unity.

Gauss's lemma for polynomials states that the product of primitive polynomials (with coefficients in the same unique factorization domain) also is primitive. Equivalently, it may be expressed as stating that the content of the product of two polynomials is the product of their contents.

35.1 See also

- Rational root theorem

35.2 References

- B. Hartley; T.O. Hawkes (1970). *Rings, modules and linear algebra*. Chapman and Hall. ISBN 0-412-09810-5.
- Page 181 of Lang, Serge (1993), *Algebra* (Third ed.), Reading, Mass.: Addison-Wesley Pub. Co., ISBN 978-0-201-55540-0, Zbl 0848.13001
- David Sharpe (1987). *Rings and factorization*. Cambridge University Press. pp. 68–69. ISBN 0-521-33718-6.

Chapter 36

Continuant (mathematics)

In algebra, the **continuant** is a multivariate polynomial representing the determinant of a tridiagonal matrix and having applications in generalized continued fractions.

36.1 Definition

The *n*-th *continuant*, *K*(*n*), of a sequence **a** = a_1,...,*an*,... is defined recursively by

$K(0) = 1;$

$K(1) = a_1;$

$K(n) = a_n K(n-1) + K(n-2).$

It may also be obtained by taking the sum of all possible products of a_1,...,*an* in which any pairs of consecutive terms are deleted.

An extended definition takes the continuant with respect to three sequences **a**, **b** and **c**, so that *K*(*n*) is a polynomial of a_1,...,*an*, b_1,...,*bn*–1 and c_1,...,*cn*–1. In this case the recurrence relation becomes

$K(0) = 1;$

$K(1) = a_1;$

$K(n) = a_n K(n-1) - b_{n-1}c_{n-1}K(n-2).$

Since *br* and *cr* enter into *K* only as a product *brcr* there is no loss of generality in assuming that the *br* are all equal to 1.

36.2 Applications

The simple continuant gives the value of a continued fraction of the form $[a_0; a_1, a_2, \ldots]$. The *n*-th convergent is

$$\frac{K(n+1, (a_0, \ldots, a_n))}{K(n, (a_1, \ldots, a_n))}.$$

The extended continuant is precisely the determinant of the tridiagonal matrix

$$\begin{pmatrix} a_1 & b_1 & 0 & \dots & 0 & 0 \\ c_1 & a_2 & b_2 & \dots & 0 & 0 \\ 0 & c_2 & a_3 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \dots & c_{n-1} & a_n \end{pmatrix}.$$

In Muir's book the "extended" continuant is simply called continuant.

36.3 References

- Thomas Muir (1960). *A treatise on the theory of determinants*. Dover Publications. pp. 516–525.
- Cusick, Thomas W.; Flahive, Mary E. (1989). *The Markoff and Lagrange Spectra*. Mathematical Surveys and Monographs **30**. Providence, RI: American Mathematical Society. p. 89. ISBN 0-8218-1531-8. Zbl 0685.10023.
- George Chrystal (1999). *Algebra, an Elementary Text-book for the Higher Classes of Secondary Schools and for Colleges: Pt. 1*. American Mathematical Society. p. 500. ISBN 0-8218-1649-7.

Chapter 37

Cubic function

This article is about cubic equations in one variable. For cubic equations in *two* variables, see cubic plane curve.
In mathematics, a **cubic function** is a function of the form



Graph of a cubic function with 3 real roots (where the curve crosses the horizontal axis—where $y = 0$*). The case shown has two critical points. Here the function is* $f(x) = (x^3 + 3x^2 - 6x - 8) / 4$.

$$f(x) = ax^3 + bx^2 + cx + d,$$

where a is nonzero. In other words, a cubic function is defined by a polynomial of degree three.

Setting $f(x) = 0$ produces a **cubic equation** of the form:

$$ax^3 + bx^2 + cx + d = 0.$$

Usually, the coefficients a, b, c, d are real numbers. However much of the theory of cubic equations for real coefficients applies to other types of coefficients (such as complex ones).[1]

Solving the cubic equation is equivalent to finding the particular value (or values) of x for which $f(x) = 0$. There are various methods to solve cubic equations. The solutions, also called roots, of a cubic equation can always be found algebraically. (This is also true of a quadratic or quartic (fourth degree) equation, but no higher-degree equation, by the Abel–Ruffini theorem). The roots can also be found trigonometrically. Alternatively, one can find a numerical approximation of the roots in the field of the real or complex numbers such as by using root-finding algorithms like Newton's method.

37.1 History

Cubic equations were known to the ancient Babylonians, Greeks, Chinese, Indians, and Egyptians.[2][3][4] Babylonian (20th to 16th centuries BC) cuneiform tablets have been found with tables for calculating cubes and cube roots.[5][6] The Babylonians could have used the tables to solve cubic equations, but no evidence exists to confirm that they did.[7] The problem of doubling the cube involves the simplest and oldest studied cubic equation, and one for which the ancient Egyptians did not believe a solution existed.[8] In the 5th century BC, Hippocrates reduced this problem to that of finding two mean proportionals between one line and another of twice its length, but could not solve this with a compass and straightedge construction,[9] a task which is now known to be impossible. Methods for solving cubic equations appear in *The Nine Chapters on the Mathematical Art*, a Chinese mathematical text compiled around the 2nd century BC and commented on by Liu Hui in the 3rd century.[3] In the 3rd century, the ancient Greek mathematician Diophantus found integer or rational solutions for some bivariate cubic equations (Diophantine equations).[4][10] Hippocrates, Menaechmus and Archimedes are believed to have come close to solving the problem of doubling the cube using intersecting conic sections,[9] though historians such as Reviel Netz dispute whether the Greeks were thinking about cubic equations or just problems that can lead to cubic equations. Some others like T. L. Heath, who translated all Archimedes' works, disagree, putting forward evidence that Archimedes really solved cubic equations using intersections of two cones, but also discussed the conditions where the roots are 0, 1 or 2.[11]

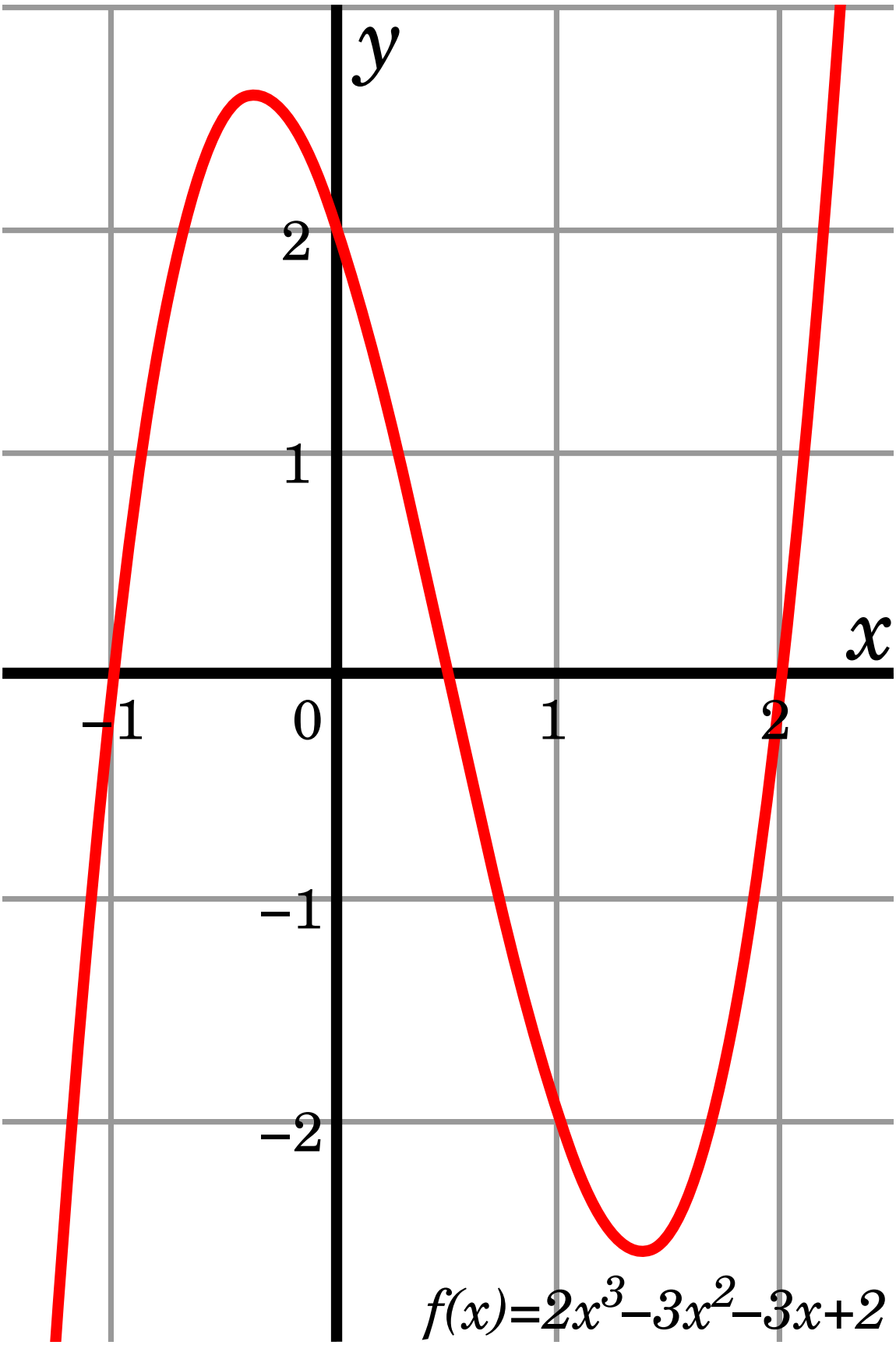
In the 7th century, the Tang dynasty astronomer mathematician Wang Xiaotong in his mathematical treatise titled Jigu Suanjing systematically established and solved 25 cubic equations of the form $x^3 + px^2 + qx = N$, 23 of them with $p, q \neq 0$, and two of them with $q = 0$.[12]

In the 11th century, the Persian poet-mathematician, Omar Khayyám (1048–1131), made significant progress in the theory of cubic equations. In an early paper he wrote regarding cubic equations, he discovered that a cubic equation can have more than one solution and stated that it cannot be solved using compass and straightedge constructions. He also found a geometric solution.[13][14] In his later work, the *Treatise on Demonstration of Problems of Algebra*, he wrote a complete classification of cubic equations with general geometric solutions found by means of intersecting conic sections.[15][16]

In the 12th century, the Indian mathematician Bhaskara II attempted the solution of cubic equations without general success. However, he gave one example of a cubic equation:[17]

$$x^3 + 12x = 6x^2 + 35$$

In the 12th century, another Persian mathematician, Sharaf al-Dīn al-Tūsī (1135–1213), wrote the *Al-Mu'adalat* (*Treatise on Equations*), which dealt with eight types of cubic equations with positive solutions and five types of cubic equations which may not have positive solutions. He used what would later be known as the "Ruffini-Horner method" to numerically approximate the root of a cubic equation. He also developed the concepts of a derivative function and



Two-dimensional graph of a cubic, the polynomial $f(x) = 2x^3 - 3x^2 - 3x + 2$.

the maxima and minima of curves in order to solve cubic equations which may not have positive solutions.[18] He understood the importance of the discriminant of the cubic equation to find algebraic solutions to certain types of cubic equations.[19]

Leonardo de Pisa, also known as Fibonacci (1170–1250), was able to find the positive solution to the cubic equation $x^3 + 2x^2 + 10x = 20$, using the Babylonian numerals. He gave the result as 1,22,7,42,33,4,40 (equivalent to $1 + 22/60 + 7/60^2 + 42/60^3 + 33/60^4 + 4/60^5 + 40/60^6$),[20] which differs from the correct value by only about three trillionths.

In the early 16th century, the Italian mathematician Scipione del Ferro (1465–1526) found a method for solving a class of cubic equations, namely those of the form $x^3 + mx = n$. In fact, all cubic equations can be reduced to this form if we allow m and n to be negative, but negative numbers were not known to him at that time. Del Ferro kept his achievement secret until just before his death, when he told his student Antonio Fiore about it.



Niccolò Fontana Tartaglia

In 1530, Niccolò Tartaglia (1500–1557) received two problems in cubic equations from Zuanne da Coi and announced that he could solve them. He was soon challenged by Fiore, which led to a famous contest between the two. Each

contestant had to put up a certain amount of money and to propose a number of problems for his rival to solve. Whoever solved more problems within 30 days would get all the money. Tartaglia received questions in the form $x^3 + mx = n$, for which he had worked out a general method. Fiore received questions in the form $x^3 + mx^2 = n$, which proved to be too difficult for him to solve, and Tartaglia won the contest.

Later, Tartaglia was persuaded by Gerolamo Cardano (1501–1576) to reveal his secret for solving cubic equations. In 1539, Tartaglia did so only on the condition that Cardano would never reveal it and that if he did write a book about cubics, he would give Tartaglia time to publish. Some years later, Cardano learned about Ferro's prior work and published Ferro's method in his book *Ars Magna* in 1545, meaning Cardano gave Tartaglia 6 years to publish his results (with credit given to Tartaglia for an independent solution). Cardano's promise with Tartaglia stated that he not publish Tartaglia's work, and Cardano felt he was publishing del Ferro's, so as to get around the promise. Nevertheless, this led to a challenge to Cardano by Tartaglia, which Cardano denied. The challenge was eventually accepted by Cardano's student Lodovico Ferrari (1522–1565). Ferrari did better than Tartaglia in the competition, and Tartaglia lost both his prestige and income.[21]

Cardano noticed that Tartaglia's method sometimes required him to extract the square root of a negative number. He even included a calculation with these complex numbers in *Ars Magna*, but he did not really understand it. Rafael Bombelli studied this issue in detail and is therefore often considered as the discoverer of complex numbers.

François Viète (1540–1603) independently derived the trigonometric solution for the cubic with three real roots, and René Descartes (1596–1650) extended the work of Viète.[22]

37.2 Critical points of a cubic function

The critical points of a cubic equation are those values of x where the slope of the cubic function is zero. They are found by setting derivative of the cubic equation equal to zero obtaining: $f\,'(x) = 3ax^2 + 2bx + c = 0$. The solutions of that equation are the critical points of the cubic equation and are given by: (using the quadratic formula)

$$x = \frac{-b \pm \sqrt{b^2 - 3ac}}{3a}.$$

If $b^2 - 3ac > 0$, then the cubic function has a local maximum and a local minimum. If $b^2 - 3ac = 0$, then the cubic's inflection point is the only critical point. If $b^2 - 3ac < 0$, then there are no critical points. In the cases where $b^2 - 3ac \leq 0$, the cubic function is strictly monotonic.

37.3 Roots of a cubic function

The general cubic equation has the form

$$ax^3 + bx^2 + cx + d = 0 \qquad (1)$$

with $a \neq 0$.

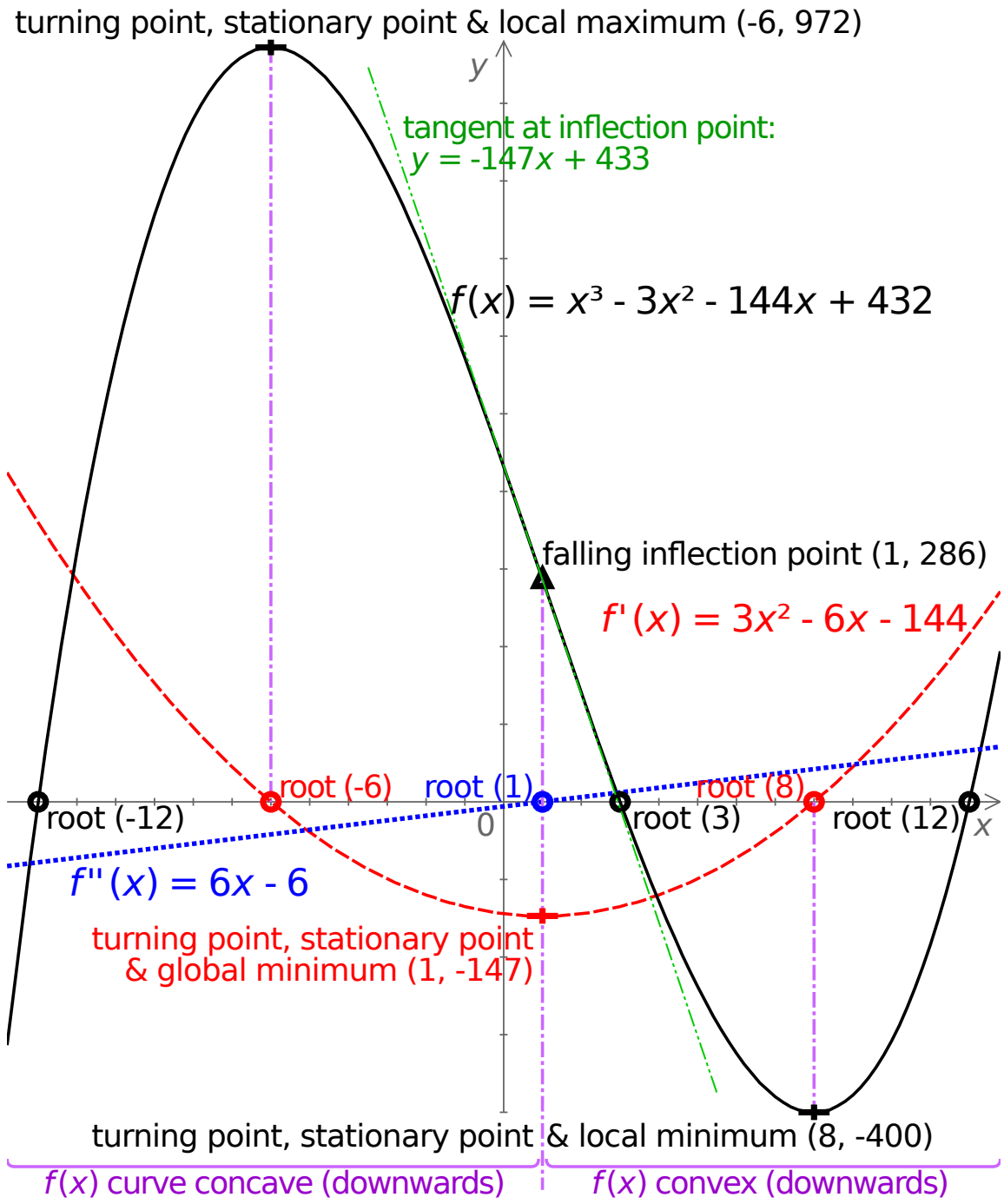
This section describes how the roots of such an equation may be computed. The coefficients a, b, c, d are generally assumed to be real numbers, but most of the results apply when they belong to any field of characteristic not 2 or 3.

37.3.1 The nature of the roots

Every cubic equation (1) with real coefficients has at least one solution x among the real numbers; this is a consequence of the intermediate value theorem. We can distinguish several possible cases using the discriminant,

$$\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2.$$

The following cases need to be considered: [23]



The roots, turning points, stationary points, inflection point and concavity of a cubic polynomial $x^3 - 3x^2 - 144x + 432$ *(black line) and its first and second derivatives (red and blue).*

- If $\Delta > 0$, then the equation has three distinct real roots.
- If $\Delta = 0$, then the equation has a multiple root and all its roots are real.
- If $\Delta < 0$, then the equation has one real root and two nonreal complex conjugate roots.

For information about the location in the complex plane of the roots of a polynomial of any degree, including degree three, see Properties of polynomial roots and Routh–Hurwitz stability criterion

37.3.2 General formula for roots

For the general cubic equation

$$ax^3 + bx^2 + cx + d = 0$$

the general formula for the roots, in terms of the coefficients, is as follows:[24]

$$x_k = -\frac{1}{3a}\left(b + u_k C + \frac{\Delta_0}{u_k C}\right), \qquad k \in \{1, 2, 3\}$$

where

$$u_1 = 1\,, \qquad u_2 = \frac{-1 + i\sqrt{3}}{2}\,, \qquad u_3 = \frac{-1 - i\sqrt{3}}{2}$$

are the three cube roots of unity, and where

$$C = \sqrt[3]{\frac{\Delta_1 + \sqrt{\Delta_1^2 - 4\Delta_0^3}}{2}} \qquad \text{(see below for special cases)}$$

with

$$\Delta_0 = b^2 - 3ac$$
$$\Delta_1 = 2b^3 - 9abc + 27a^2 d$$

and

$$\Delta_1^2 - 4\Delta_0^3 = -27\, a^2\, \Delta\,,$$ where Δ is the discriminant discussed above.

In these formulae, $\sqrt{\ }$ and $\sqrt[3]{\ }$ denote any choice for the square or cube roots. Changing of choice for the square root amounts to exchanging x_2 and x_3 . Changing of choice for the cube root amounts to circularly permuting the roots. Thus the freeness of choosing a determination of the square or cube roots corresponds exactly to the freeness for numbering the roots of the equation.

Four centuries ago, Gerolamo Cardano proposed a similar formula (see below), which still appears in many textbooks:

$$x_k = -\frac{1}{3a}\left(b + u_k C + \bar{u}_k \bar{C}\right)$$

where

$$\bar{C} = \sqrt[3]{\frac{\Delta_1 - \sqrt{\Delta_1^2 - 4\Delta_0^3}}{2}}$$

and $\bar{u}_k$ is the complex conjugate of u_k (note that $C\bar{C} = \Delta_0$).

However, this formula is applicable without further explanation *only* when *a*, *b*, *c*, *d* are real numbers and the operand of the square root, i.e., $\Delta_1^2 - 4\Delta_0^3$, is non-negative. When this operand is real and non-negative, the square root refers to the principal (positive) square root and the cube roots in the formula are to be interpreted as the real ones. Otherwise, there is no real square root and one can arbitrarily choose one of the imaginary square roots (the same one everywhere in the solution). For extracting the complex cube roots of the resulting complex expression, we have also to choose among three cube roots in each part of each solution, giving nine possible combinations of one of three cube roots for the first part of the expression and one of three for the second. The correct combination is such that the two cube roots chosen for the two terms in a given solution expression are complex conjugates of each other (whereby the two imaginary terms in each solution cancel out).

The next sections describe how these formulas may be obtained.

Special cases

If $\Delta \neq 0$ and $\Delta_0 = 0$, the sign of $\sqrt{\Delta_1^2 - 4\Delta_0^3} = \sqrt{\Delta_1^2}$ has to be chosen to have $C \neq 0$, that is one should define $\sqrt{\Delta_1^2} = \Delta_1$, whichever is the sign of Δ_1.

If $\Delta = 0$ and $\Delta_0 = 0$, the three roots are equal:

$$x_1 = x_2 = x_3 = -\frac{b}{3a}.$$

If $\Delta = 0$ and $\Delta_0 \neq 0$, the above expression for the roots is correct but misleading, hiding the fact that no radical is needed to represent the roots. In fact, in this case, there is a double root,

$$x_1 = x_2 = \frac{9ad - bc}{2\Delta_0},$$

and a simple root

$$x_3 = \frac{4abc - 9a^2d - b^3}{a\Delta_0}.$$

37.3.3 Reduction to a depressed cubic

Dividing Equation (1) by a and substituting $t - \frac{b}{3a}$ for x (the Tschirnhaus transformation) we get the equation

$$t^3 + pt + q = 0 \qquad (2)$$

where

$$p = \frac{3ac - b^2}{3a^2}$$
$$q = \frac{2b^3 - 9abc + 27a^2d}{27a^3}.$$

The left hand side of equation (2) is a monic trinomial called a **depressed cubic**.

Any formula for the roots of a depressed cubic may be transformed into a formula for the roots of Equation (1) by substituting the above values for p and q and using the relation $x = t - \frac{b}{3a}$.

Therefore, only Equation (2) is considered in the following.

37.3.4 Cardano's method

The solutions can be found with the following method due to Scipione del Ferro and Tartaglia, published by Gerolamo Cardano in 1545.[25]

This method applies to the depressed cubic

$$t^3 + pt + q = 0\,. \qquad (2)$$

We introduce two variables *u* and *v* linked by the condition

$$u + v = t$$

and substitute this in the depressed cubic (2), giving

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0 \qquad (3)$$

At this point Cardano imposed a second condition for the variables *u* and *v*:

$$3uv + p = 0$$

As the first parenthesis vanishes in (3), we get $u^3 + v^3 = -q$ and $u^3v^3 = -p^3/27$. Thus u^3 and v^3 are the two roots of the equation

$$z^2 + qz - \frac{p^3}{27} = 0\,.$$

At this point, Cardano, who did not know complex numbers, supposed that the roots of this equation were real, that is that $\frac{q^2}{4} + \frac{p^3}{27} > 0$.

Solving this equation and using the fact that u and v may be exchanged, we find

$$u^3 = -\tfrac{q}{2} + \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}} \text{ and } v^3 = -\tfrac{q}{2} - \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}\,.$$

As these expressions are real, their cube roots are well-defined and, like Cardano, we get

$$t_1 = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Given the assumption that $\frac{q^2}{4} + \frac{p^3}{27} > 0$, Equation (2) also has two complex roots. These are obtained by considering the complex cube roots appearing in the above formula; the fact uv is real implies that one is obtained by multiplying the first of the above cube roots by $\frac{-1}{2} + i\frac{\sqrt{3}}{2}$ and the second by $\frac{-1}{2} - i\frac{\sqrt{3}}{2}$, and vice versa for the other one.

If $\frac{q^2}{4} + \frac{p^3}{27}$ is not necessarily positive, we have to choose a cube root of u^3 . As there is no direct way to choose the corresponding cube root of v^3 , one has to use the relation $v = -\frac{p}{3u}$, which gives

$$u = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \qquad (4)$$

and

$$t = u - \frac{p}{3u}\,.$$

Note that the sign of the square root does not affect the resulting t , because changing it amounts to exchanging u and v . We have chosen the minus sign to have $u \neq 0$ when $p = 0$ and $q \neq 0$, in order to avoid a division by zero. With this choice, the above expression for t always works, except when $p = q = 0$, where the second term becomes 0/0. In this case there is a triple root $t = 0$.

Note also that in several cases the solutions are expressed with fewer square or cube roots

If $p = q = 0$ then we have the triple real root

$t = 0.$

If $p = 0$ and $q \neq 0$ then

$u = -\sqrt[3]{q}$ and $v = 0$

and the three roots are the three cube roots of $-q$.

If $p \neq 0$ and $q = 0$ then

$$u = \sqrt{\frac{p}{3}} \qquad \text{and} \qquad v = -\sqrt{\frac{p}{3}},$$

in which case the three roots are

$$t = u + v = 0, \qquad t = \omega_1 u - \frac{p}{3\omega_1 u} = \sqrt{-p}, \qquad t = \frac{u}{\omega_1} - \frac{\omega_1 p}{3u} = -\sqrt{-p},$$

where

$$\omega_1 = e^{i\frac{2\pi}{3}} = -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i.$$

Finally if $4p^3 + 27q^2 = 0$ and $p \neq 0$, there are a double root and an isolated root which may be expressed rationally in terms of p and q , but these expressions may not be immediately deduced from the general expression of the roots:

$$t_1 = t_2 = -\frac{3q}{2p} \quad \text{and} \quad t_3 = \frac{3q}{p}\,.$$

To pass from these roots of t in Equation (2) to the general formulas for roots of x in Equation (1), subtract $\frac{b}{3a}$ and replace p and q by their expressions in terms of a, b, c, d .

37.3.5 Vieta's substitution

Starting from the depressed cubic

$$t^3 + pt + q = 0,$$

we make the following substitution, known as Vieta's substitution:

$$t = w - \frac{p}{3w}$$

This results in the equation

$$w^3 + q - \frac{p^3}{27w^3} = 0.$$

Multiplying by w^3, it becomes a sextic equation in w, which is in fact a quadratic equation in w^3:

$$w^6 + qw^3 - \frac{p^3}{27} = 0$$

The quadratic formula allows this to be solved for w^3. If w_1, w_2 and w_3 are the three cube roots of one of the solutions in w^3, then the roots of the original depressed cubic are

$$t_1 = w_1 - \frac{p}{3w_1}, \quad t_2 = w_2 - \frac{p}{3w_2} \quad \text{and} \quad t_3 = w_3 - \frac{p}{3w_3}.$$

37.3.6 Lagrange's method

In his paper *Réflexions sur la résolution algébrique des équations* ("Thoughts on the algebraic solving of equations"), Joseph Louis Lagrange introduced a new method to solve equations of low degree.

This method works well for cubic and quartic equations, but Lagrange did not succeed in applying it to a quintic equation, because it requires solving a resolvent polynomial of degree at least six.[26][27][28] This is explained by the Abel–Ruffini theorem, which proves that such polynomials cannot be solved by radicals. Nevertheless the modern methods for solving solvable quintic equations are mainly based on Lagrange's method.[28]

In the case of cubic equations, Lagrange's method gives the same solution as Cardano's. By drawing attention to a geometrical problem that involves two cubes of different size Cardano explains in his book *Ars Magna* how he arrived at the idea of considering the unknown of the cubic equation as a sum of two other quantities. Lagrange's method may also be applied directly to the general cubic equation (1) without using the reduction to the depressed cubic equation (2). Nevertheless the computation is much easier with this reduced equation.

Suppose that x_0, x_1 and x_2 are the roots of equation (1) or (2), and define $\zeta = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ (a complex cube root of 1, i.e. a primitive third root of unity) which satisfies the relation $\zeta^2 + \zeta + 1 = 0$. We now set

$$s_0 = x_0 + x_1 + x_2,$$

$$s_1 = x_0 + \zeta x_1 + \zeta^2 x_2,$$

$$s_2 = x_0 + \zeta^2 x_1 + \zeta x_2.$$

This is the discrete Fourier transform of the roots: observe that while the coefficients of the polynomial are symmetric in the roots, in this formula an *order* has been chosen on the roots, so these are not symmetric in the roots. The roots may then be recovered from the three *si* by inverting the above linear transformation via the inverse discrete Fourier transform, giving

$$x_0 = \tfrac{1}{3}(s_0 + s_1 + s_2),$$

$$x_1 = \tfrac{1}{3}(s_0 + \zeta^2 s_1 + \zeta s_2),$$

$$x_2 = \tfrac{1}{3}(s_0 + \zeta s_1 + \zeta^2 s_2).$$

The polynomial s_0 is an elementary symmetric polynomial and is thus equal to $-b/a$ in case of Equation (1) and to zero in case of Equation (2), so we only need to seek values for the other two.

The polynomials s_1 and s_2 are not symmetric functions of the roots: s_0 is invariant, while the two non-trivial cyclic permutations of the roots send s_1 to ζs_1 and s_2 to $\zeta^2 s_2$, or s_1 to $\zeta^2 s_1$ and s_2 to ζs_2 (depending on which permutation), while transposing x_1 and x_2 switches s_1 and s_2 ; other transpositions switch these roots and multiply them by a power of ζ.

Thus, s_1^3 , s_2^3 and $s_1 s_2$ are left invariant by the cyclic permutations of the roots, which multiply them by $\zeta^3 = 1$. Also $s_1 s_2$ and $s_1^3 + s_2^3$ are left invariant by the transposition of x_1 and x_2 which exchanges s_1 and s_2 . As the permutation group S_3 of the roots is generated by these permutations, it follows that $s_1^3 + s_2^3$ and $s_1 s_2$ are symmetric functions of the roots and may thus be written as polynomials in the elementary symmetric polynomials and thus as rational functions of the coefficients of the equation. Let $s_1^3 + s_2^3 = A$ and $s_1 s_2 = B$ in these expressions, which will be explicitly computed below.

We have that s_1^3 and s_2^3 are the two roots of the quadratic equation

$$z^2 - Az + B^3 = 0\,.$$

Thus the resolution of the equation may be finished exactly as described for Cardano's method, with s_1 and s_2 in place of u and v .

Computation of *A* and *B*

Setting $E_1 = x_0+x_1+x_2$, $E_2 = x_0x_1+x_1x_2+x_2x_0$ and $E_3 = x_0x_1x_2$, the elementary symmetric polynomials, we have, using that $\zeta^3 = 1$:

$$s_1^3 = x_0^3 + x_1^3 + x_2^3 + 3\zeta(x_0^2x_1 + x_1^2x_2 + x_2^2x_0) + 3\zeta^2(x_0x_1^2 + x_1x_2^2 + x_2x_0^2) + 6x_0x_1x_2 \,.$$

The expression for s_2^3 is the same with ζ and ζ^2 exchanged. Thus, using $\zeta^2 + \zeta = -1$ we get

$$A = s_1^3 + s_2^3 = 2(x_0^3 + x_1^3 + x_2^3) - 3(x_0^2x_1 + x_1^2x_2 + x_2^2x_0 + x_0x_1^2 + x_1x_2^2 + x_2x_0^2) + 12x_0x_1x_2 \,,$$

and a straightforward computation gives

$$A = s_1^3 + s_2^3 = 2E_1^3 - 9E_1E_2 + 27E_3 \,.$$

Similarly we have

$$B = s_1s_2 = x_0^2 + x_1^2 + x_2^2 + (\zeta + \zeta^2)(x_0x_1 + x_1x_2 + x_2x_0) = E_1^2 - 3E_2 \,.$$

When solving Equation (1) we have

$$E_1 = -b/a \text{ , } E_2 = c/a \text{ and } E_3 = -d/a$$

With Equation (2), we have $E_1 = 0$, $E_2 = p$ and $E_3 = -q$ and thus:

$$A = -27q \text{ and } B = -3p \,.$$

Note that with Equation (2), we have $x_0 = \frac{1}{3}(s_1 + s_2)$ and $s_1s_2 = -3p$, while in Cardano's method we have set $x_0 = u + v$ and $uv = -\frac{1}{3}p$. Thus we have, up to the exchange of u and v :

$$s_1 = 3u \text{ and } s_2 = 3v \,.$$

In other words, in this case, Cardano's and Lagrange's method compute exactly the same things, up to a factor of three in the auxiliary variables, the main difference being that Lagrange's method explains why these auxiliary variables appear in the problem.

37.3.7 Trigonometric (and hyperbolic) method

When a cubic equation has three real roots, the formulas expressing these roots in terms of radicals involve complex numbers. It has been proved that when none of the three real roots is rational—the *casus irreducibilis*— one cannot express the roots in terms of **real radicals**. Nevertheless, purely real expressions of the solutions may be obtained using hypergeometric functions,[29] or more elementarily in terms of trigonometric functions, specifically in terms of the cosine and arccosine functions.

The formulas which follow, due to François Viète,[22] are true in general (except when $p = 0$), are purely real when the equation has three real roots, but involve complex cosines and arccosines when there is only one real root.

Starting from Equation (2), $t^3 + pt + q = 0$, let us set $t = u\cos\theta$. The idea is to choose u to make Equation (2) coincide with the identity

$$4\cos^3\theta - 3\cos\theta - \cos(3\theta) = 0 \,.$$

In fact, choosing $u = 2\sqrt{-\frac{p}{3}}$ and dividing Equation (2) by $\frac{u^3}{4}$ we get

$$4\cos^3\theta - 3\cos\theta - \frac{3q}{2p}\sqrt{\frac{-3}{p}} = 0\,.$$

Combining with the above identity, we get

$$\cos(3\theta) = \frac{3q}{2p}\sqrt{\frac{-3}{p}}$$

and thus the roots are[30]

$$t_k = 2\sqrt{-\frac{p}{3}}\cos\left(\frac{1}{3}\arccos\left(\frac{3q}{2p}\sqrt{\frac{-3}{p}}\right) - \frac{2\pi k}{3}\right) \quad \text{for} \quad k = 0, 1, 2\,.$$

This formula involves only real terms if $p < 0$ and the argument of the arccosine is between −1 and 1. The last condition is equivalent to $4p^3 + 27q^2 \leq 0$, which implies also $p < 0$. Thus the above formula for the roots involves only real terms if and only if the three roots are real.

Denoting by $C(p, q)$ the above value of t_0, and using the inequality $-\pi \leq \arccos(u) \leq \pi$ for a real number *u* such that $-1 \leq u \leq 1$, the three roots may also be expressed as

$$t_0 = C(p, q), \qquad t_2 = -C(p, -q), \qquad t_1 = -t_0 - t_2\,.$$

If the three roots are real, we have

$$t_0 \geq t_1 \geq t_2\,.$$

All these formulas may be straightforwardly transformed into formulas for the roots of the general cubic equation (1), using the back substitution described in Section Reduction to a depressed cubic.

When there is only one real root (and $p \neq 0$), it may be similarly represented using hyperbolic functions, as[31][32]

$$t_0 = -2\frac{|q|}{q}\sqrt{-\frac{p}{3}}\cosh\left(\frac{1}{3}\operatorname{arcosh}\left(\frac{-3|q|}{2p}\sqrt{\frac{-3}{p}}\right)\right) \quad \text{if} \quad 4p^3 + 27q^2 > 0 \text{ and } p < 0\,,$$

$$t_0 = -2\sqrt{\frac{p}{3}}\sinh\left(\frac{1}{3}\operatorname{arsinh}\left(\frac{3q}{2p}\sqrt{\frac{3}{p}}\right)\right) \quad \text{if} \quad p > 0\,.$$

If $p \neq 0$ and the inequalities on the right are not satisfied the formulas remain valid but involve complex quantities.

When $p = \pm 3$, the above values of t_0 are sometimes called the **Chebyshev cube root.**[33] More precisely, the values involving cosines and hyperbolic cosines define, when $p = -3$, the same analytic function denoted $C_{\frac{1}{3}}(q)$, which is the proper Chebyshev cube root. The value involving hyperbolic sines is similarly denoted $S_{\frac{1}{3}}(q)$, when $p = 3$.

37.3.8 Factorization

If the cubic equation $ax^3 + bx^2 + cx + d = 0$ with integer coefficients has a rational real root, it can be found using the rational root test: If the root is *r* = *m* / *n* fully reduced, then *m* is a factor of *d* and *n* is a factor of *a*, so all possible combinations of values for *m* and *n* can be checked for whether they satisfy the cubic equation.

The rational root test may also be used for a cubic equation with rational coefficients: by multiplication by the lowest common denominator) of the coefficients, one gets an equation with integer coefficients which has exactly the same roots.

The rational root test is particularly useful when there are three real roots because the algebraic solution unhelpfully expresses the real roots in terms of complex entities. The rational root test is also helpful in the presence of one real

and two complex roots because it allows all of the roots to be written without the use of cube roots: If *r* is any root of the cubic, then we may factor out (*x*–*r*) using polynomial long division to obtain

$$(x-r)\left(ax^2+(b+ar)x+c+br+ar^2\right)=ax^3+bx^2+cx+d\,.$$

Hence if we know one root, perhaps from the rational root test, we can find the other two by using the quadratic formula to solve the quadratic $ax^2+(b+ar)x+c+br+ar^2$, giving

$$\frac{-b-ra\pm\sqrt{b^2-4ac-2abr-3a^2r^2}}{2a}$$

for the other two roots.

37.3.9 Geometric interpretation of the roots

Three real roots

Viète's trigonometric expression of the roots in the three-real-roots case lends itself to a geometric interpretation in terms of a circle.[22][34] When the cubic is written in depressed form $t^3+pt+q=0$, as shown above, the solution can be expressed as

$$t_k=2\sqrt{-\frac{p}{3}}\cos\left(\frac{1}{3}\arccos\left(\frac{3q}{2p}\sqrt{\frac{-3}{p}}\right)-k\frac{2\pi}{3}\right)\quad\text{for}\quad k=0,1,2\,.$$

Here $\arccos\left(\frac{3q}{2p}\sqrt{\frac{-3}{p}}\right)$ is an angle in the unit circle; taking $\frac{1}{3}$ of that angle corresponds to taking a cube root of a complex number; adding $-k\frac{2\pi}{3}$ for *k* = 1, 2 finds the other cube roots; and multiplying the cosines of these resulting angles by $2\sqrt{-\frac{p}{3}}$ corrects for scale.

For the non-depressed case $x^3+bx^2+cx+d=0$ (shown in the accompanying graph), the depressed case as indicated previously is obtained by defining *t* such that $x=t-\frac{b}{3}$ so $t=x+\frac{b}{3}$. Graphically this corresponds to simply shifting the graph horizontally when changing between the variables *t* and *x*, without changing the angle relationships. This shift moves the point of inflection and the centre of the circle onto the y-axis. Consequently, the roots of the equation in t sum to zero.

One real and two complex roots

In the Cartesian plane If a cubic is plotted in the Cartesian plane, the real root can be seen graphically as the horizontal intercept of the curve. But further,[35][36][37] if the complex conjugate roots are written as $g\pm hi$, then *g* is the abscissa (the positive or negative horizontal distance from the origin) of the tangency point of a line that is tangent to the cubic curve and intersects the horizontal axis at the same place as does the cubic curve; and |*h*| is the square root of the tangent of the angle between this line and the horizontal axis.

In the complex plane With one real and two complex roots, the three roots can be represented as points in the complex plane, as can the two roots of the cubic's derivative. There is an interesting geometrical relationship among all these roots.

The points in the complex plane representing the three roots serve as the vertices of an isosceles triangle. (The triangle is isosceles because one root is on the horizontal (real) axis and the other two roots, being complex conjugates, appear symmetrically above and below the real axis.) Marden's Theorem says that the points representing the roots of the derivative of the cubic are the foci of the Steiner inellipse of the triangle—the unique ellipse that is tangent to the triangle at the midpoints of its sides. If the angle at the vertex on the real axis is less than $\frac{\pi}{3}$ then the major axis of the ellipse lies on the real axis, as do its foci and hence the roots of the derivative. If that angle is greater than $\frac{\pi}{3}$, the major axis is vertical and its foci, the roots of the derivative, are complex. And if that angle is $\frac{\pi}{3}$, the triangle is equilateral, the Steiner inellipse is simply the triangle's incircle, its foci coincide with each other at the incenter, which lies on the real axis, and hence the derivative has duplicate real roots.

Omar Khayyám's solution

As shown in this graph, to solve the third-degree equation $x^3 + a^2x = b$ where $b > 0$, Omar Khayyám constructed the parabola $y = x^2/a$, the circle which has as a diameter the line segment $[0, b/a^2]$ of the positive *x*-axis, and a vertical line through the point above the *x*-axis, where the circle and parabola intersect. The solution is given by the length of the horizontal line segment from the origin to the intersection of the vertical line and the *x*-axis.

A simple modern proof of the method is the following: multiplying by *x* the equation, and regrouping the terms gives

$$\frac{x^4}{a^2} = x\,(\frac{b}{a^2} - x)\,.$$

The left-hand side is the value of y^2 on the parabola. The equation of the circle being $y^2 + x\,(x - \frac{b}{a^2}) = 0$, the right hand side is the value of y^2 on the circle.

37.4 Collinearities

The tangent lines to a cubic at three collinear points intercept the cubic again at collinear points.[38]:p. 425,#290

37.5 Applications

Cubic equations arise in various other contexts.

Marden's theorem states that the foci of the Steiner inellipse of any triangle can be found by using the cubic function whose roots are the coordinates in the complex plane of the triangle's three vertices. The roots of the first derivative of this cubic are the complex coordinates of those foci.

Given the cosine (or other trigonometric function) of an arbitrary angle, the cosine of one-third of that angle is one of the roots of a cubic.

The solution of the general quartic equation relies on the solution of its resolvent cubic.

In analytical chemistry, the Charlot equation, which can be used to find the pH of buffer solutions, can be solved using a cubic equation.

37.6 See also

- Algebraic equation
- Linear equation
- Newton's method
- Polynomial
- Quadratic equation
- Quartic equation
- Quintic equation
- Spline (mathematics)

37.7 Notes

[1] Exceptions include fields of characteristic 2 and 3.

[2] British Museum BM 85200

[3] Crossley, John; W.-C. Lun, Anthony (1999). *The Nine Chapters on the Mathematical Art: Companion and Commentary*. Oxford University Press. p. 176. ISBN 978-0-19-853936-0.

[4] Van der Waerden, Geometry and Algebra of Ancient Civilizations, chapter 4, Zurich 1983 ISBN 0-387-12159-5

[5] Cooke, Roger (8 November 2012). *The History of Mathematics*. John Wiley & Sons. p. 63. ISBN 978-1-118-46029-0.

[6] Nemet-Nejat, Karen Rhea (1998). *Daily Life in Ancient Mesopotamia*. Greenwood Publishing Group. p. 306. ISBN 978-0-313-29497-6.

[7] Cooke, Roger (2008). *Classical Algebra: Its Nature, Origins, and Uses*. John Wiley & Sons. p. 64. ISBN 978-0-470-27797-3.

[8] Guilbeau (1930, p. 8) states that "the Egyptians considered the solution impossible, but the Greeks came nearer to a solution."

[9] Guilbeau (1930, pp. 8–9)

[10] Heath, Thomas L. (April 30, 2009). *Diophantus of Alexandria: A Study in the History of Greek Algebra*. Martino Pub. pp. 87–91. ISBN 978-1578987542.

[11] Archimedes (October 8, 2007). *The works of Archimedes*. Translation by T. L. Heath. Rough Draft Printing. ISBN 978-1603860512.

[12] Mikami, Yoshio (1974) [1913], "Chapter 8 Wang Hsiao-Tung and Cubic Equations", *The Development of Mathematics in China and Japan* (2nd ed.), New York: Chelsea Publishing Co., pp. 53–56, ISBN 978-0-8284-0149-4

[13] A paper of Omar Khayyam, Scripta Math. 26 (1963), pages 323–337

[14] In O'Connor, John J.; Robertson, Edmund F., "Omar Khayyam", *MacTutor History of Mathematics archive*, University of St Andrews. one may read *This problem in turn led Khayyam to solve the cubic equation* $x^3 + 200x = 20x^2 + 2000$ *and he found a positive root of this cubic by considering the intersection of a rectangular hyperbola and a circle. An approximate numerical solution was then found by interpolation in trigonometric tables*. The *then* in the last assertion is erroneous and should, at least, be replaced by *also*. The geometric construction was perfectly suitable for Omar Khayyam, as it occurs for solving a problem of geometric construction. At the end of his article he says only that, for this geometrical problem, if approximations are sufficient, then a simpler solution may be obtained by consulting trigonometric tables. Textually: *If the seeker is satisfied with an estimate, it is up to him to look into the table of chords of Almagest, or the table of sines and versed sines of Mothmed Observatory*. This is followed by a short description of this alternate method (seven lines).

[15] J. J. O'Connor and E. F. Robertson (1999), Omar Khayyam, MacTutor History of Mathematics archive, states, "Khayyam himself seems to have been the first to conceive a general theory of cubic equations."

[16] Guilbeau (1930, p. 9) states, "Omar Al Hay of Chorassan, about 1079 AD did most to elevate to a method the solution of the algebraic equations by intersecting conics."

[17] Datta and Singh, History of Hindu Mathematics, p. 76,Equation of Higher Degree; Bharattya Kala Prakashan, Delhi, India 2004 ISBN 81-86050-86-8

[18] O'Connor, John J.; Robertson, Edmund F., "Sharaf al-Din al-Muzaffar al-Tusi", *MacTutor History of Mathematics archive*, University of St Andrews.

[19] Berggren, J. L. (1990), "Innovation and Tradition in Sharaf al-Din al-Tusi's Muadalat", *Journal of the American Oriental Society* **110** (2): 304–309, doi:10.2307/604533

[20] R. N. Knott and the Plus Team (November 4, 2013), "The life and numbers of Fibonacci", *Plus Magazine*

[21] Katz, Victor (2004). *A History of Mathematics*. Boston: Addison Wesley. p. 220. ISBN 9780321016188.

[22] Nickalls, R. W. D. (July 2006), "Viète, Descartes and the cubic equation" (PDF), *Mathematical Gazette* **90**: 203–208

[23] Irving, Ronald S. (2004), *Integers, polynomials, and rings*, Springer-Verlag New York, Inc., ISBN 0-387-40397-3, Chapter 10 ex 10.14.4 and 10.17.4, pp. 154–156

[24] Press, William H.; Vetterling, William T. (1992). *Numerical Recipes in Fortran 77: The Art of Scientific Computing*. Cambridge University Press. p. 179. ISBN 0-521-43064-X., Extract of page 179

[25] Jacobson 2009, p. 210

[26] Prasolov, Viktor; Solovyev, Yuri (1997), *Elliptic functions and elliptic integrals*, AMS Bookstore, ISBN 978-0-8218-0587-9, §6.2, p. 134

[27] Kline, Morris (1990), *Mathematical Thought from Ancient to Modern Times*, Oxford University Press US, ISBN 978-0-19-506136-9, Algebra in the Eighteenth Century: The Theory of Equations

[28] Daniel Lazard, "Solving quintics in radicals", in Olav Arnfinn Laudal, Ragni Piene, *The Legacy of Niels Henrik Abel*, pp. 207–225, Berlin, 2004,. ISBN 3-540-43826-2

[29] Zucker, I. J., "The cubic equation — a new look at the irreducible case", *Mathematical Gazette* 92, July 2008, 264–268.

[30] Shelbey, Samuel (1975), *CRC Standard Mathematical Tables*, CRC Press, ISBN 0-87819-622-6

[31] These are Formulas (80) and (83) of Weisstein, Eric W. 'Cubic Formula'. From MathWorld—A Wolfram Web Resource. http://mathworld.wolfram.com/CubicFormula.html, rewritten for having a coherent notation.

[32] Holmes, G. C., "The use of hyperbolic cosines in solving cubic polynomials", *Mathematical Gazette* 86. November 2002, 473–477.

[33] Abramowitz, Milton; Stegun, Irene A., eds. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, Dover (1965), chap. 22 p. 773

[34] Nickalls, R. W. D. (November 1993), "A new approach to solving the cubic: Cardan's solution revealed" (PDF), *The Mathematical Gazette* **77** (480): 354–359, doi:10.2307/3619777, ISSN 0025-5572, JSTOR 3619777 See esp. Fig. 2.

[35] Henriquez, Garcia (June–July 1935), "The graphical interpretation of the complex roots of cubic equations", *American Mathematical Monthly* **42** (6): 383–384, doi:10.2307/2301359

[36] Barr, C. F. (1918), *American Mathematical Monthly* **25**: 268, doi:10.2307/2972885 Missing or empty |title= (help)

[37] Barr, C. F. (1917), *Annals of Mathematics* **19**: 157 Missing or empty |title= (help)

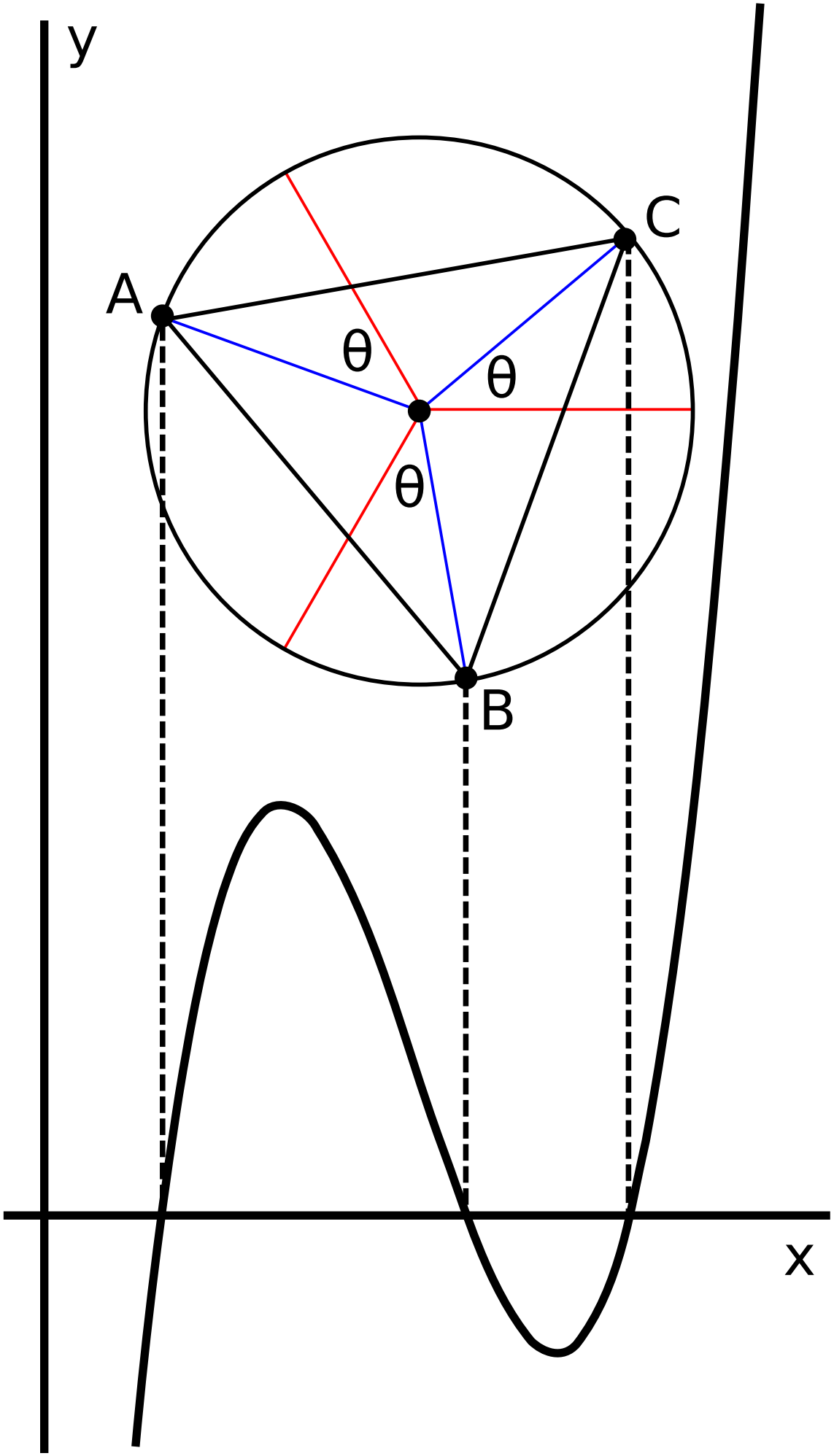
[38] Whitworth, William Allen. *Trilinear Coordinates and Other Methods of Modern Analytical Geometry of Two Dimensions*, Forgotten Books, 2012 (orig. Deighton, Bell, and Co., 1866). http://www.forgottenbooks.com/search?q=Trilinear+coordinates&t=books

37.8 References

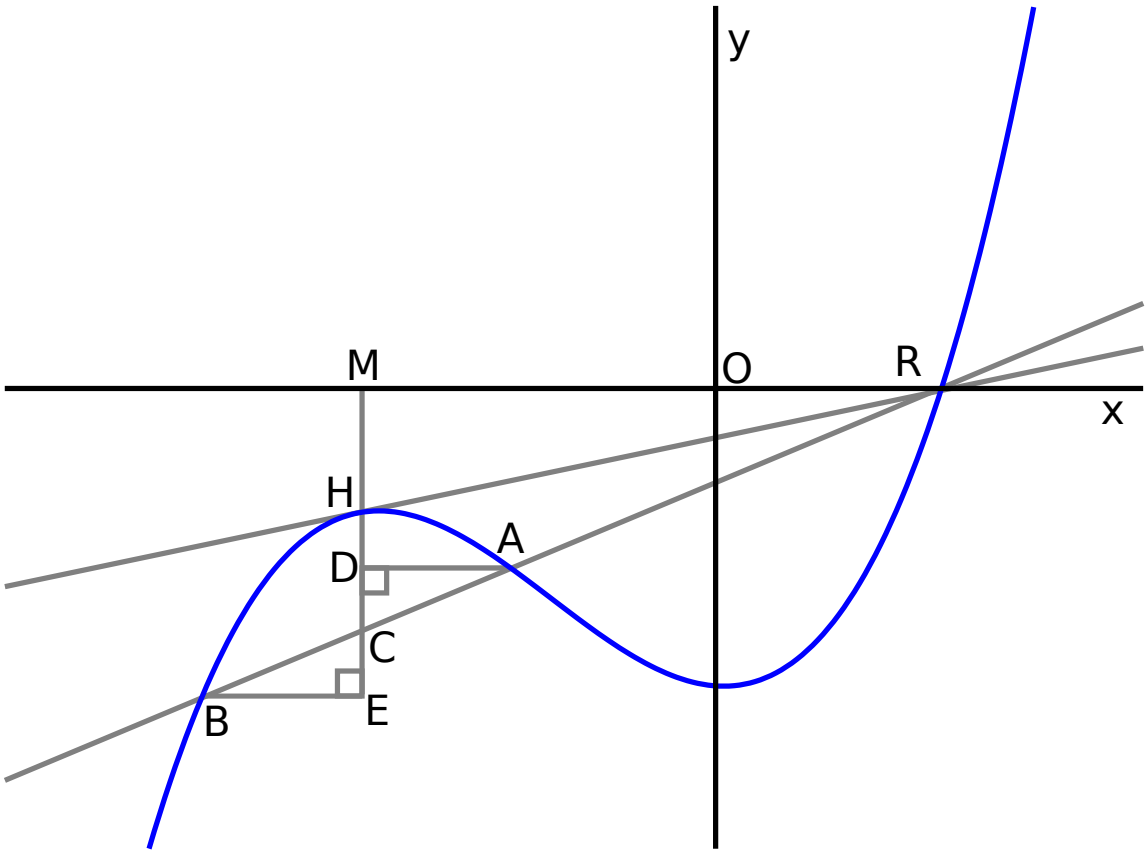
- Anglin, W. S.; Lambek, Joachim (1995), "Mathematics in the Renaissance", *The Heritage of Thales*, Springers, pp. 125–131, ISBN 978-0-387-94544-6 Ch. 24.
- Dence, T. (November 1997), "Cubics, chaos and Newton's method", *Mathematical Gazette* (Mathematical Association) **81**: 403–408, doi:10.2307/3619617, ISSN 0025-5572
- Dunnett, R. (November 1994), "Newton–Raphson and the cubic", *Mathematical Gazette* (Mathematical Association) **78**: 347–348, doi:10.2307/3620218, ISSN 0025-5572
- Guilbeau, Lucye (1930), "The History of the Solution of the Cubic Equation", *Mathematics News Letter* **5** (4): 8–12, doi:10.2307/3027812, JSTOR 3027812
- Jacobson, Nathan (2009), *Basic algebra* **1** (2nd ed.), Dover, ISBN 978-0-486-47189-1
- Mitchell, D. W. (November 2007), "Solving cubics by solving triangles", *Mathematical Gazette* (Mathematical Association) **91**: 514–516, ISSN 0025-5572
- Mitchell, D. W. (November 2009), "Powers of φ as roots of cubics", *Mathematical Gazette* (Mathematical Association) **93**: ???, ISSN 0025-5572
- Press, WH; Teukolsky, SA; Vetterling, WT; Flannery, BP (2007), "Section 5.6 Quadratic and Cubic Equations", *Numerical Recipes: The Art of Scientific Computing* (3rd ed.), New York: Cambridge University Press, ISBN 978-0-521-88068-8
- Rechtschaffen, Edgar (July 2008), "Real roots of cubics: Explicit formula for quasi-solutions", *Mathematical Gazette* (Mathematical Association) **92**: 268–276, ISSN 0025-5572
- Zucker, I. J. (July 2008), "The cubic equation – a new look at the irreducible case", *Mathematical Gazette* (Mathematical Association) **92**: 264–268, ISSN 0025-5572

37.9 External links

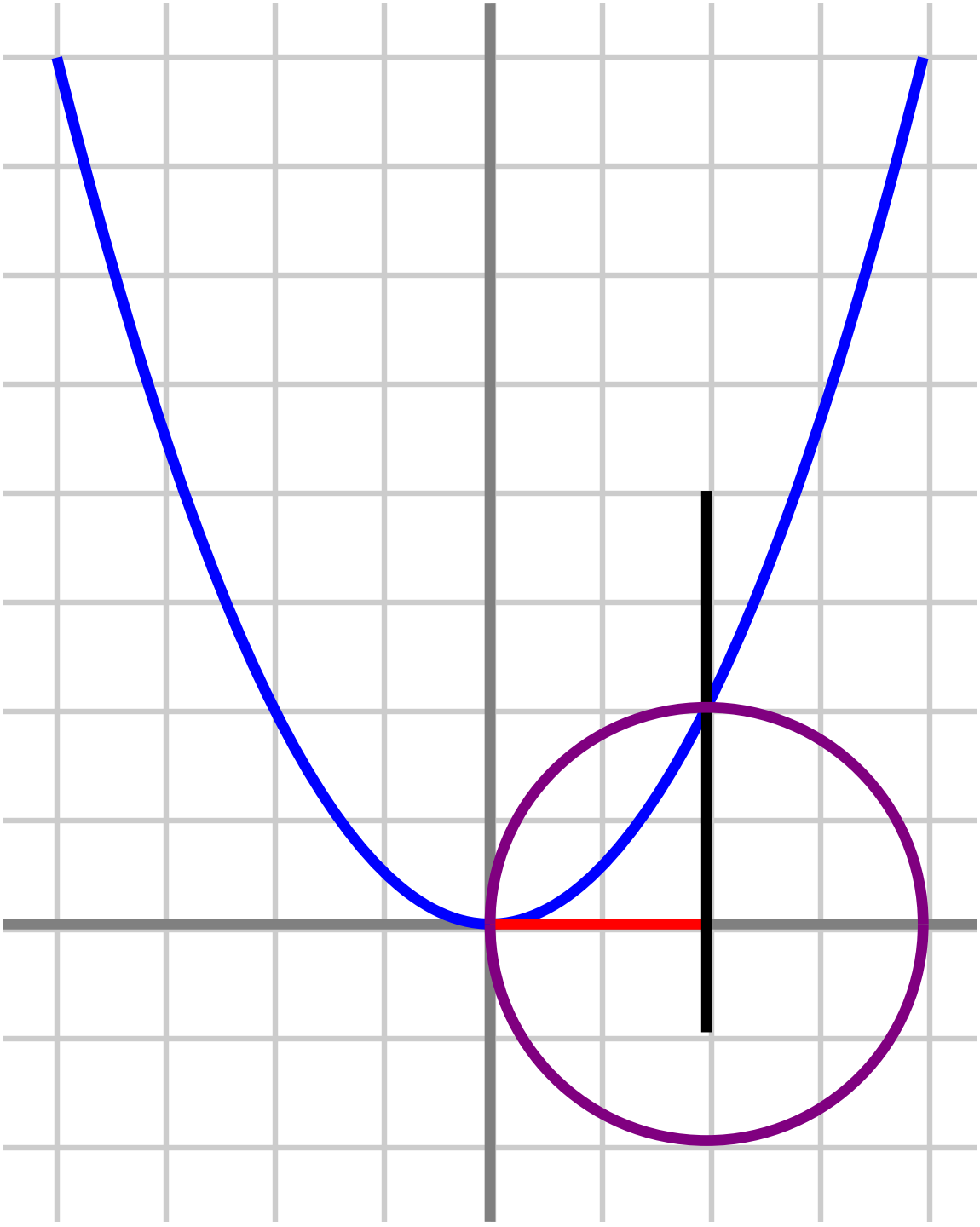
- sums and products of roots
- Hazewinkel, Michiel, ed. (2001), "Cardano formula", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Solving a Cubic by means of Moebius transforms
- Interesting derivation of trigonometric cubic solution with 3 real roots
- Calculator for solving Cubics (also solves Quartics and Quadratics)
- Tartaglia's work (and poetry) on the solution of the Cubic Equation at Convergence
- Cubic Equation Solver.
- Quadratic, cubic and quartic equations on MacTutor archive.
- Cubic Formula at PlanetMath.org.
- Cardano solution calculator as java applet at some local site. Only takes natural coefficients.
- Graphic explorer for cubic functions With interactive animation, slider controls for coefficients
- On Solution of Cubic Equations at Holistic Numerical Methods Institute
- Dave Auckly, Solving the quartic with a pencil American Math Monthly 114:1 (2007) 29—39
- "Cubic Equation" by Eric W. Weisstein, The Wolfram Demonstrations Project, 2007.
- The Cubic Tutorials by John H. Mathews



For the cubic $x^3 + bx^2 + cx + d = 0$ with three real roots, the roots are the projection on the x*-axis of the vertices* A, B, *and* C *of*



The slope of line RA is twice that of RH. Denoting the complex roots of the cubic as g±hi, g = $\overline{OM}$ *(negative here) and* h = $\sqrt{\tan ORH}$ = $\sqrt{RH \text{ line of slope}}$ = $\overline{BE}$ = $\overline{DA}$.



Omar Khayyám's geometric solution of a cubic equation, for the case a=*2,* b=*16, giving the root 2. The fact that the vertical line intersects the* x*-axis at the center of the circle is specific to this particular example*

Chapter 38

Cyclotomic polynomial

In mathematics, more specifically in algebra, the ***n*th cyclotomic polynomial**, for any positive integer *n*, is the unique irreducible polynomial with integer coefficients, which is a divisor of $x^n - 1$ and is not a divisor of $x^k - 1$ for any *k* < *n*. Its roots are the *n*th primitive roots of unity $e^{2i\pi\frac{k}{n}}$, where *k* runs over the integers lower than *n* and coprime to *n*. In other words, the ***n*th cyclotomic polynomial** is equal to

$$\Phi_n(x) = \prod_{\substack{1\le k\le n \\ \gcd(k,n)=1}} \left(x - e^{2i\pi\frac{k}{n}}\right)$$

It may also be defined as the monic polynomial with integer coefficients, which is the minimal polynomial over the field of the rational numbers of any primitive *n*th-root of unity ($e^{2i\pi/n}$ is an example of such a root).

Another important equation, linking the cyclotomic polynomials and primitive roots of unity, is the following one.

$$x^n - 1 = \prod_{1\le k\le n} \left(x - e^{2\pi\cdot \mathrm{i}k/n}\right) = \prod_{d|n} \prod_{\substack{1\le k\le n \\ \gcd(k,n)=d}} \left(x - e^{2\pi\cdot \mathrm{i}k/n}\right) = \prod_{d|n} \Phi_{n/d}(x) = \prod_{d|n} \Phi_d(x)$$

38.1 Examples

If *n* is a prime number then

$$\Phi_n(x) = 1 + x + x^2 + \cdots + x^{n-1} = \sum_{i=0}^{n-1} x^i.$$

If *n*=2*p* where *p* is an odd prime number then

$$\Phi_{2p}(x) = 1 - x + x^2 - \cdots + x^{p-1} = \sum_{i=0}^{p-1} (-x)^i.$$

For *n* up to 30, the cyclotomic polynomials are:[1]

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = x^2 - x + 1$$

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_8(x) = x^4 + 1$$

$$\Phi_9(x) = x^6 + x^3 + 1$$

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$$

$$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{12}(x) = x^4 - x^2 + 1$$

$$\Phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

$$\Phi_{16}(x) = x^8 + 1$$

$$\Phi_{17}(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{18}(x) = x^6 - x^3 + 1$$

$$\Phi_{19}(x) = x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$$

$$\Phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{22}(x) = x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

$$\Phi_{23}(x) = x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{24}(x) = x^8 - x^4 + 1$$

$$\Phi_{25}(x) = x^{20} + x^{15} + x^{10} + x^5 + 1$$

$$\Phi_{26}(x) = x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

$$\Phi_{27}(x) = x^{18} + x^9 + 1$$

$$\Phi_{28}(x) = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$$

$$\Phi_{29}(x) = x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6$$

$$\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$$

The case of the 105th cyclotomic polynomial is interesting because 105 is the lowest integer that is the product of three distinct odd prime numbers and this polynomial is the first one that has a coefficient greater than 1:

$$\begin{aligned}\Phi_{105}(x) = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} \\ & + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} \\ & + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1\end{aligned}$$

38.2 Properties

38.2.1 Fundamental tools

The cyclotomic polynomials are monic polynomials with integer coefficients that are irreducible over the field of the rational numbers. Except for *n* equal to 1 or 2, they are palindromics of even degree.

The degree of Φ_n , or in other words the number of *n*th primitive roots of unity, is $\varphi(n)$, where φ is Euler's totient function.

The fact that Φ_n is an irreducible polynomial of degree $\varphi(n)$ in the ring $\mathbb{Z}[x]$ is a nontrivial result due to Gauss.[2] Depending on the chosen definition, it is either the value of the degree or the irreducibility which is a nontrivial result. The case of prime *n* is easier to prove than the general case, thanks to Eisenstein's criterion.

A fundamental relation involving cyclotomic polynomials is

$$\prod_{d|n} \Phi_d(x) = x^n - 1,$$

which means that each *n*-th root of unity is a primitive *d*-th root of unity for a unique *d* dividing *n*.

The Möbius inversion formula allows the expression of $\Phi_n(x)$ as an explicit rational fraction:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)},$$

where μ is the Möbius function.

The cyclotomic polynomial $\Phi_n(x)$ may be computed by (exactly) dividing $x^n - 1$ by the cyclotomic polynomials of the proper divisors of *n* previously computed recursively by the same method:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}$$

(Recall that $\Phi_1(x) = x - 1$.)

This formula allows to compute $\Phi_n(x)$ on a computer for any *n*, as soon as integer factorization and division of polynomials are available. Many computer algebra systems have a built in function to compute the cyclotomic polynomials. For example this function is called by typing cyclotomic_polynomial(n,'x') in Sage, numtheory[cyclotomic](n,x); in Maple, and Cyclotomic[n,x] in Mathematica.

38.2.2 Easy cases for the computation

As noted above, if *n* is a prime number, then

$$\Phi_n(x) = 1 + x + x^2 + \cdots + x^{n-1} = \sum_{i=0}^{n-1} x^i.$$

If *n* is an odd integer greater than one, then

$$\Phi_{2n}(x) = \Phi_n(-x).$$

In particular, if *n*=2*p* is twice an odd prime, then (as noted above)

$$\Phi_n(x) = 1 - x + x^2 - \cdots + x^{p-1} = \sum_{i=0}^{p-1} (-x)^i.$$

If $n=p^m$ is a prime power (where p is prime), then

$$\Phi_n(x) = \Phi_p(x^{p^{m-1}}) = \sum_{i=0}^{p-1} x^{ip^{m-1}}.$$

More generally, if $n=p^m r$ with r relatively prime to p, then

$$\Phi_n(x) = \Phi_{qr}(x^{q^{m-1}}).$$

These formulas may be applied repeatedly to get a simple expression for any cyclotomic polynomial $\Phi_n(x)$ in term of a cyclotomic polynomial of square free index: If q is the product of the prime divisors of n (its radical), then[3]

$$\Phi_n(x) = \Phi_q(x^{n/q}).$$

This allows to give formulas for the nth cyclotomic polynomial when n has at most one odd prime factor: If p is an odd prime number, and h and k are positive integers, then:

$$\Phi_{2^h}(x) = x^{2^{h-1}} + 1$$

$$\Phi_{p^k}(x) = \sum_{i=0}^{p-1} x^{ip^{k-1}}$$

$$\Phi_{2^h p^k}(x) = \sum_{i=0}^{p-1} (-1)^i x^{i2^{h-1}p^{k-1}}$$

For the other values of n, the computation of the nth cyclotomic polynomial is similarly reduced to that of $\Phi_q(x)$, where q is the product of the distinct odd prime divisors of n. To deal with this case, one has that, for p prime and not dividing n,[4]

$$\Phi_{np}(x) = \Phi_n(x^p)/\Phi_n(x)\,.$$

38.2.3 Integers appearing as coefficients

The problem of bounding the magnitude of the coefficients of the cyclotomic polynomials has been the object of a number of research papers.

If n has at most two distinct odd prime factors, then Migotti showed that the coefficients of Φ_n are all in the set {1, −1, 0}.[5]

The first cyclotomic polynomial for a product of 3 different odd prime factors is $\Phi_{105}(x)$; it has a coefficient −2 (see its expression above). The converse isn't true: $\Phi_{231}(x) = \Phi_{3\times 7\times 11}(x)$ only has coefficients in {1, −1, 0}.

If n is a product of more odd different prime factors, the coefficients may increase to very high values. E.g., $\Phi_{15015}(x) = \Phi_{3\times 5\times 7\times 11\times 13}(x)$ has coefficients running from −22 to 22, $\Phi_{255255}(x) = \Phi_{3\times 5\times 7\times 11\times 13\times 17}(x)$, the smallest n with 6 different odd primes, has coefficients up to ±532.

Let $A(n)$ denote the maximum absolute value of the coefficients of Φn. It is known that for any positive k, the number of n up to x with $A(n) > n^k$ is at least $c(k)\cdot x$ for a positive $c(k)$ depending on k and x sufficiently large. In the opposite direction, for any function $\psi(n)$ tending to infinity with n we have $A(n)$ bounded above by $n^{\psi(n)}$ for almost all n.[6]

38.2.4 Gauss's formula

Let n be odd, square-free, and greater than 3. Then[7][8]

$$4\Phi_n(z) = A_n^2(z) - (-1)^{\frac{n-1}{2}} nz^2 B_n^2(z)$$

where both *An*(*z*) and *Bn*(*z*) have integer coefficients, *An*(*z*) has degree $\varphi(n)/2$, and *Bn*(z) has degree $\varphi(n)/2 - 2$. Furthermore, *An*(*z*) is palindromic when its degree is even; if its degree is odd it is antipalindromic. Similarly, *Bn*(*z*) is palindromic unless *n* is composite and ≡ 3 (mod 4), in which case it is antipalindromic.

The first few cases are

$$\begin{aligned}
4\Phi_5(z) &= 4(z^4 + z^3 + z^2 + z + 1) \\
&= (2z^2 + z + 2)^2 - 5z^2 \\
4\Phi_7(z) &= 4(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) \\
&= (2z^3 + z^2 - z - 2)^2 + 7z^2(z + 1)^2 \\
4\Phi_{11}(z) &= 4(z^{10} + z^9 + z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) \\
&= (2z^5 + z^4 - 2z^3 + 2z^2 - z - 2)^2 + 11z^2(z^3 + 1)^2
\end{aligned}$$

38.2.5 Lucas's formula

Let *n* be odd, square-free and greater than 3. Then[9]

$$\Phi_n(z) = U_n^2(z) - (-1)^{\frac{n-1}{2}} nzV_n^2(z)$$

where both *Un*(*z*) and *Vn*(*z*) have integer coefficients, *Un*(*z*) has degree $\varphi(n)/2$, and *Vn*(z) has degree $\varphi(n)/2 - 1$. This can also be written

$$\Phi_n((-1)^{\frac{n-1}{2}} z) = C_n^2(z) - nzD_n^2(z).$$

If *n* is even, square-free and greater than 2 (this forces *n* to be ≡ 2 (mod 4)),

$$\Phi_{n/2}(-z^2) = C_n^2(z) - nzD_n^2(z)$$

where both *Cn*(*z*) and *Dn*(*z*) have integer coefficients, *Cn*(*z*) has degree $\varphi(n)$, and *Dn*(z) has degree $\varphi(n) - 1$. *Cn*(*z*) and *Dn*(z) are both palindromic.

The first few cases are:

$$\begin{aligned}
\Phi_3(-z) &= z^2 - z + 1 \\
&= (z + 1)^2 - 3z \\
\Phi_5(z) &= z^4 + z^3 + z^2 + z + 1 \\
&= (z^2 + 3z + 1)^2 - 5z(z + 1)^2 \\
\Phi_3(-z^2) &= z^4 - z^2 + 1 \\
&= (z^2 + 3z + 1)^2 - 6z(z + 1)^2
\end{aligned}$$

38.3 Cyclotomic polynomials over *Zp*

For any prime number *p* which does not divide *n*, cyclotomic polynomial Φ_n is irreducible over *Zp* if and only if *p* is a primitive root to mod *n*. That is, the multiplicative order of *p* to mod *n* is $\varphi(n)$, which is also the degree of Φ_n .

38.4 Prime Cyclotomic numbers

The prime numbers of the form $\Phi_n(b)$ (with n, b integers, $n > 2$, $b > 1$) are listed in OEIS A206864, or all primes in OEIS A206942.

The list is about the smallest integer $b > 1$ which $\Phi_n(b)$ is a prime (see OEIS A085398), it is conjectured that such b exists for all positive integer n (See Bunyakovsky conjecture). (For that to allow $b = 1$, see OEIS A117544. In fact, $b = 1$ if and only if n is a prime or a prime power, so you can see this sequence for all positive integer n which is neither a prime nor a prime power. For n is a prime, see OEIS A066180).

The list is about all $n \le 300$ (The b-file of A117544 lists all $n \le 1000$, but it lists 1 if and only if n is a prime or prime power)

For all positive integers $n \le 1000$, the largest three bs are 2706, 2061, and 2042, when n is 545, 601, and 943, and there are 17 values of $n \le 1000$ such that $b > 1000$.

In fact, if p is a prime, then $\Phi_p(b)$ is $\frac{b^p-1}{b-1}$ and a repunit number in base b, (111111...111111)b, so the following is a list of the smallest $b > 1$ which $\Phi_p(b)$ is a prime. (see OEIS A066180)

The list is about the first 100 primes p. (The b-file of A066180 lists the first 200 primes p, up to 1223)

38.5 Applications

Using Φ_n , one can give an elementary proof for the infinitude of primes congruent to 1 modulo n,[10] which is a special case of Dirichlet's theorem on arithmetic progressions.

38.6 See also

- Cyclotomic field
- Aurifeuillean factorization
- Root of unity

38.7 Notes

[1] (sequence A013595 in OEIS)

[2] Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR 1878556

[3] Cox, David A. (2012), "Exercise 12", *Galois Theory* (2nd ed.), John Wiley & Sons, p. 237, doi:10.1002/9781118218457, ISBN 978-1-118-07205-9.

[4] Weisstein, Eric W. "Cyclotomic Polynomial". Retrieved 12 March 2014.

[5] Isaacs, Martin (2009). *Algebra: A Graduate Course*. AMS Bookstore. p. 310. ISBN 978-0-8218-4799-2.

[6] Meier (2008)

[7] Gauss, DA, Articles 356-357

[8] Riesel, pp. 315-316, p. 436

[9] Riesel, pp. 309-315, p. 443

[10] S. Shirali. *Number Theory*. Orient Blackswan, 2004. p. 67. ISBN 81-7371-454-1

38.8 References

Gauss's book *Disquisitiones Arithmeticae* has been translated from Latin into English and German. The German edition includes all of his papers on number theory: all the proofs of quadratic reciprocity, the determination of the sign of the Gauss sum, the investigations into biquadratic reciprocity, and unpublished notes.

- Gauss, Carl Friedrich (1986) [1801]. *Disquisitiones Arithmeticae*. Translated into English by Clarke, Arthur A. (2nd corr. ed.). New York: Springer. ISBN 0387962549.
- Gauss, Carl Friedrich (1965) [1801]. *Untersuchungen uber hohere Arithmetik (Disquisitiones Arithmeticae & other papers on number theory)*. Translated into German by Maser, H. (2nd ed.). New York: Chelsea. ISBN 0-8284-0191-8.
- Lemmermeyer, Franz (2000). *Reciprocity Laws: from Euler to Eisenstein*. Berlin: Springer. doi:10.1007/978-3-662-12893-0. ISBN 978-3-642-08628-1.
- Maier, Helmut (2008), "Anatomy of integers and cyclotomic polynomials", in De Koninck, Jean-Marie; Granville, Andrew; Luca, Florian, *Anatomy of integers. Based on the CRM workshop, Montreal, Canada, March 13-17, 2006*, CRM Proceedings and Lecture Notes **46**, Providence, RI: American Mathematical Society, pp. 89–95, ISBN 978-0-8218-4406-9, Zbl 1186.11010
- Riesel, Hans (1994). *Prime Numbers and Computer Methods for Factorization* (2nd ed.). Boston: Birkhäuser. ISBN 0-8176-3743-5.

38.9 External links

- Weisstein, Eric W., "Cyclotomic polynomial", *MathWorld*.
- Hazewinkel, Michiel, ed. (2001), "Cyclotomic polynomials", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- "Sloane's A013595 : Triangle of coefficients of cyclotomic polynomial Phi_n(x) (exponents in increasing order)", *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation.
- "Sloane's A013594 : Smallest order of cyclotomic polynomial containing n or −n as a coefficient", *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation.

Chapter 39

Degree of a polynomial

The **degree** of a polynomial is the highest degree of its terms when the polynomial is expressed in its canonical form consisting of a linear combination of monomials. The degree of a term is the sum of the exponents of the variables that appear in it. The term **order** has been used as a synonym of *degree* but, nowadays, refers to different, but related, concepts.

For example, the polynomial $7x^2y^3 + 4x - 9$ has three terms. (Notice, this polynomial can also be expressed as $7x^2y^3 + 4x^1y^0 - 9x^0y^0$.) The first term has a degree of 5 (the sum of the powers 2 and 3), the second term has a degree of 1, and the last term has a degree of 0. Therefore, the polynomial has a degree of 5 which is the highest degree of any term.

To determine the degree of a polynomial that is not in standard form (for example $(x+1)^2 - (x-1)^2$), one has to put it first in standard form by expanding the products (by distributivity) and combining the like terms; for example $(x+1)^2 - (x-1)^2 = 4x$ is of degree 1, even though each summand has degree 2. However, this is not needed when the polynomial is expressed as a product of polynomials in standard form, because the degree of a product is the sum of the degrees of the factors.

39.1 Names of polynomials by degree

The following names are assigned to polynomials according to their degree:[1][2][3]

- Special case – zero (see § Degree of the zero polynomial below)
- Degree 0 – constant[4]
- Degree 1 – linear
- Degree 2 – quadratic
- Degree 3 – cubic
- Degree 4 – quartic
- Degree 5 – quintic
- Degree 6 – sextic (or, less commonly, hexic)
- Degree 7 – septic (or, less commonly, heptic)

For higher degrees, names have sometimes been proposed,[5] but they are rarely used:

- Degree 8 – octic
- Degree 9 – nonic
- Degree 10 – decic

Names for degree above three are based on Latin ordinal numbers, and end in *-ic*. This should be distinguished from the names used for the number of variables, the arity, which are based on Latin distributive numbers, and end in *-ary*. For example, a degree two polynomial in two variables, such as $x^2 + xy + y^2$, is called a "binary quadratic": *binary* due to two variables, *quadratic* due to degree two.[lower-alpha 1] There are also names for the number of terms, which are also based on Latin distributive numbers, ending in *-nomial*; the common ones are *monomial*, *binomial*, and (less commonly) *trinomial*; thus $x^2 + y^2$ is a "binary quadratic binomial".

39.2 Other examples

- The polynomial $3 - 5x + 2x^5 - 7x^9$ is a nonic polynomial
- The polynomial $(y - 3)(2y + 6)(-4y - 21)$ is a cubic polynomial
- The polynomial $(3z^8 + z^5 - 4z^2 + 6) + (-3z^8 + 8z^4 + 2z^3 + 14z)$ is a quintic polynomial (as the z^8 are cancelled out)

The canonical forms of the three examples above are:

- for $3 - 5x + 2x^5 - 7x^9$, after reordering, $-7x^9 + 2x^5 - 5x + 3$;
- for $(y-3)(2y+6)(-4y-21)$, after multiplying out and collecting terms of the same degree, $-8y^3 - 42y^2 + 72y + 378$;
- for $(3z^8 + z^5 - 4z^2 + 6) + (-3z^8 + 8z^4 + 2z^3 + 14z)$, in which the two terms of degree 8 cancel, $z^5 + 8z^4 + 2z^3 - 4z^2 + 14z + 6$.

39.3 Behavior under polynomial operations

39.3.1 Behaviour under addition

The degree of the sum (or difference) of two polynomials is equal to or less than the greater of their degrees; the equality holds always when the degrees of the polynomials are different i.e.

$\deg(P + Q) \leq \max(\deg(P), \deg(Q))$

$\deg(P - Q) \leq \max(\deg(P), \deg(Q))$

E.g.

- The degree of $(x^3 + x) + (x^2 + 1) = x^3 + x^2 + x + 1$ is 3. Note that 3 ≤ max(3, 2)
- The degree of $(x^3 + x) - (x^3 + x^2) = -x^2 + x$ is 2. Note that 2 ≤ max(3, 3)

39.3.2 Behaviour under scalar multiplication

The degree of the product of a polynomial by a non-zero scalar is equal to the degree of the polynomial, i.e.

$\deg(cP) = \deg(P)$

E.g.

- The degree of $2(x^2 + 3x - 2) = 2x^2 + 6x - 4$ is 2, just as the degree of $x^2 + 3x - 2$.

Note that for polynomials over a ring containing divisors of zero, this is not necessarily true. For example, in $\mathbf{Z}/4\mathbf{Z}$, $\deg(1 + 2x) = 1$, but $\deg(2(1 + 2x)) = \deg(2 + 4x) = \deg(2) = 0$.

The set of polynomials with coefficients from a given field F and degree smaller than or equal to a given number n thus forms a vector space. (Note, however, that this set is not a ring, as it is not closed under multiplication, as is seen below.)

39.3.3 Behaviour under multiplication

The degree of the product of two polynomials over a field or an integral domain is the sum of their degrees

$\deg(PQ) = \deg(P) + \deg(Q)$

E.g.

- The degree of $(x^3 + x)(x^2 + 1) = x^5 + 2x^3 + x$ is 3 + 2 = 5.

Note that for polynomials over an arbitrary ring, this is not necessarily true. For example, in $\mathbf{Z}/4\mathbf{Z}$, $\deg(2x) + \deg(1 + 2x) = 1 + 1 = 2$, but $\deg(2x(1 + 2x)) = \deg(2x) = 1$.

39.3.4 Behaviour under composition

The degree of the composition of two non-constant polynomials P and Q over a field or integral domain is the product of their degrees:

$\deg(P \circ Q) = \deg(P) \deg(Q)$

E.g.

- If $P = (x^3 + x)$, $Q = (x^2 + 1)$, then $P \circ Q = P \circ (x^2 + 1) = (x^2 + 1)^3 + (x^2 + 1) = x^6 + 3x^4 + 4x^2 + 2$, which has degree 6.

Note that for polynomials over an arbitrary ring, this is not necessarily true. For example, in $\mathbf{Z}/4\mathbf{Z}$, $\deg(2x) \deg(1 + 2x) = 1 \cdot 1 = 1$, but $\deg(2x \circ (1 + 2x)) = \deg(2 + 4x) = \deg(2) = 0$.

39.4 Degree of the zero polynomial

The degree of the zero polynomial is either left undefined, or is defined to be negative (usually −1 or $-\infty$).[6]

Like any constant value, the value 0 can be considered as a (constant) polynomial, called the zero polynomial. It has no nonzero terms, and so, strictly speaking, it has no degree either. As such, its degree is undefined. The propositions for the degree of sums and products of polynomials in the above section do not apply if any of the polynomials involved is the zero polynomial.[7]

It is convenient, however, to define the degree of the zero polynomial to be *negative infinity*, $-\infty$, and introduce the arithmetic rules[8]

$\max(a, -\infty) = a,$

and

$a + -\infty = -\infty.$

These examples illustrate how this extension satisfies the behavior rules above:

- The degree of the sum $(x^3 + x) + (0) = x^3 + x$ is 3. This satisfies the expected behavior, which is that $3 \leq \max(3, -\infty)$.
- The degree of the difference $(x) - (x) = 0$ is $-\infty$. This satisfies the expected behavior, which is that $-\infty \leq \max(1, 1)$.
- The degree of the product $(0)(x^2 + 1) = 0$ is $-\infty$. This satisfies the expected behavior, which is that $-\infty = -\infty + 2$.

39.5 Computed from the function values

The degree of a polynomial f can be computed by the formula

$$\deg f = \lim_{x\to\infty} \frac{\log|f(x)|}{\log x}.$$

This formula generalizes the concept of degree to some functions that are not polynomials. For example:

- The degree of the multiplicative inverse, $1/x$, is −1.
- The degree of the square root, $\sqrt{x}$, is 1/2.
- The degree of the logarithm, $\log x$, is 0.
- The degree of the exponential function, $\exp x$, is ∞.

Another formula to compute the degree of f from its values is

$$\deg f = \lim_{x\to\infty} \frac{xf'(x)}{f(x)}.$$

(This follows from L'Hôpital's rule.)

39.6 Extension to polynomials with two or more variables

For polynomials in two or more variables, the degree of a term is the *sum* of the exponents of the variables in the term; the degree (sometimes called the **total degree**) of the polynomial is again the maximum of the degrees of all terms in the polynomial. For example, the polynomial $x^2y^2 + 3x^3 + 4y$ has degree 4, the same degree as the term x^2y^2.

However, a polynomial in variables x and y, is a polynomial in x with coefficients which are polynomials in y, and also a polynomial in y with coefficients which are polynomials in x.

$$x^2y^2 + 3x^3 + 4y = (3)x^3 + (y^2)x^2 + (4y) = (x^2)y^2 + (4)y + (3x^3)$$

This polynomial has degree 3 in x and degree 2 in y.

39.7 Degree function in abstract algebra

Given a ring R, the polynomial ring R[x] is the set of all polynomials in x that have coefficients chosen from R. In the special case that R is also a field, then the polynomial ring R[x] is a principal ideal domain and, more importantly to our discussion here, a Euclidean domain.

It can be shown that the degree of a polynomial over a field satisfies all of the requirements of the *norm* function in the euclidean domain. That is, given two polynomials $f(x)$ and $g(x)$, the degree of the product $f(x)g(x)$ must be larger than both the degrees of f and g individually. In fact, something stronger holds:

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$

For an example of why the degree function may fail over a ring that is not a field, take the following example. Let R = $\mathbb{Z}/4\mathbb{Z}$, the ring of integers modulo 4. This ring is not a field (and is not even an integral domain) because $2 \times 2 = 4 \equiv 0 \pmod 4$. Therefore, let $f(x) = g(x) = 2x + 1$. Then, $f(x)g(x) = 4x^2 + 4x + 1 = 1$. Thus $\deg(f\cdot g) = 0$ which is not greater than the degrees of f and g (which each had degree 1).

Since the *norm* function is not defined for the zero element of the ring, we consider the degree of the polynomial $f(x) = 0$ to also be undefined so that it follows the rules of a norm in a euclidean domain.

39.8 See also

- Order of a polynomial
- Degree — for other meanings of *degree* in mathematics

39.9 Notes

[1] For simplicity, this is a homogeneous polynomial, with equal degree in both variables separately.

[1] "Names of Polynomials". Retrieved 5 February 2012.

[2] Mac Lane and Birkhoff (1999) define "linear", "quadratic", "cubic", "quartic", and "quintic". (p. 107)

[3] King (2009) defines "quadratic", "cubic", "quartic", "quintic", "sextic", "septic", and "octic".

[4] Shafarevich (2003) says of a polynomial of degree zero, $f(x) = a_0$: "Such a polynomial is called a *constant* because if we substitute different values of x in it, we always obtain the same value a_0 ." (p. 23)

[5] James Cockle proposed the names "sexic", "septic", "octic", "nonic", and "decic" in 1851. (*Mechanics Magazine*, Vol. LV, p. 171)

[6] Shafarevich (2003) says of the zero polynomial: "In this case, we consider that the degree of the polynomial is undefined." (p. 27)
Childs (1995) uses −1. (p. 233)
Childs (2009) uses $-\infty$ (p. 287), however he excludes zero polynomials in his Proposition 1 (p. 288) and then explains that the proposition holds for zero polynomials "with the reasonable assumption that $-\infty + m = -\infty$ for m any integer or $m = -\infty$ ".
Axler (1997) uses $-\infty$. (p. 64)
Grillet (2007) says: "The degree of the zero polynomial 0 is sometimes left undefined or is variously defined as $-1 \in \mathbb{Z}$ or as $-\infty$, as long as deg 0 < deg A for all A ≠ 0." (A is a polynomial.) However, he excludes zero polynomials in his Proposition 5.3. (p. 121)

[7] Barile, Margherita, "Zero Polynomial", *MathWorld*.

[8] Axler (1997) gives these rules and says: "The 0 polynomial is declared to have degree $-\infty$ so that exceptions are not needed for various reasonable results." (p. 64)

39.10 References

- Axler, Sheldon (1997), *Linear Algebra Done Right* (2nd ed.), Springer Science & Business Media
- Childs, Lindsay N. (1995), *A Concrete Introduction to Higher Algebra* (2nd ed.), Springer Science & Business Media
- Childs, Lindsay N. (2009), *A Concrete Introduction to Higher Algebra* (3rd ed.), Springer Science & Business Media
- Grillet, Pierre Antoine (2007), *Abstract Algebra* (2nd ed.), Springer Science & Business Media
- King, R. Bruce (2009), *Beyond the Quartic Equation*, Springer Science & Business Media
- Mac Lane, Saunders; Birkhoff, Garrett (1999), *Algebra* (3rd ed.), American Mathematical Society
- Shafarevich, Igor R. (2003), *Discourses on Algebra*, Springer Science & Business Media

39.11 External links

- Polynomial Order; Wolfram MathWorld

Chapter 40

Delta operator

In mathematics, a **delta operator** is a shift-equivariant linear operator $Q\colon \mathbb{K}[x] \longrightarrow \mathbb{K}[x]$ on the vector space of polynomials in a variable x over a field $\mathbb{K}$ that reduces degrees by one.

To say that Q is **shift-equivariant** means that if $g(x) = f(x + a)$, then

$$(Qg)(x) = (Qf)(x + a).$$

In other words, if f is a "**shift**" of g , then Qf is also a shift of Qg , and has the same "**shifting vector**" a .

To say that *an operator reduces degree by one* means that if f is a polynomial of degree n , then Qf is either a polynomial of degree $n - 1$, or, in case $n = 0$, Qf is 0.

Sometimes a *delta operator* is defined to be a shift-equivariant linear transformation on polynomials in x that maps x to a nonzero constant. Seemingly weaker than the definition given above, this latter characterization can be shown to be equivalent to the stated definition, since shift-equivariance is a fairly strong condition.

40.1 Examples

- The forward difference operator

  $$(\Delta f)(x) = f(x + 1) - f(x)$$

  is a delta operator.

- Differentiation with respect to *x*, written as *D*, is also a delta operator.

- Any operator of the form

  $$\sum_{k=1}^{\infty} c_k D^k$$

  (where $D^n(\mathrm{f}) = \mathrm{f}^{(n)}$ is the n^{th} derivative) with $c_1 \neq 0$ is a delta operator. It can be shown that all delta operators can be written in this form. For example, the difference operator given above can be expanded as

  $$\Delta = e^D - 1 = \sum_{k=1}^{\infty} \frac{D^k}{k!}.$$

- The generalized derivative of time scale calculus which unifies the forward difference operator with the derivative of standard calculus is a delta operator.

- In computer science and cybernetics, the term "discrete-time delta operator" (δ) is generally taken to mean a difference operator

$$(\delta f)(x) = \frac{f(x + \Delta t) - f(x)}{\Delta t},$$

the Euler approximation of the usual derivative with a discrete sample time Δt . The delta-formulation obtains a significant number of numerical advantages compared to the shift-operator at fast sampling.

40.2 Basic polynomials

Every delta operator Q has a unique sequence of "basic polynomials", a polynomial sequence defined by three conditions:

- $p_0(x) = 1$;
- $p_n(0) = 0$;
- $(Qp_n)(x) = np_{n-1}(x),\ \forall n \in \mathbb{N}$.

Such a sequence of basic polynomials is always of binomial type, and it can be shown that no other sequences of binomial type exist. If the first two conditions above are dropped, then the third condition says this polynomial sequence is a Sheffer sequence—a more general concept.

40.3 See also

- Pincherle derivative
- Shift operator
- Umbral calculus

40.4 References

- Nikol'Skii, Nikolai Kapitonovich (1986), *Treatise on the shift operator: spectral function theory*, Berlin, New York: Springer-Verlag, ISBN 978-0-387-15021-5

Chapter 41

Denisyuk polynomials

In mathematics, **Denisyuk polynomials** De$n(x)$ or $Mn(x)$ are generalizations of the Laguerre polynomials introduced by Denisyuk (1954) given by the generating function

$$\sum_{n=0}^{\infty} t^n M_n(x) = \frac{1}{1+t} \exp -\frac{xt}{1-t}$$

(Boas & Buck 1958, p.41).

41.1 See also

41.2 References

- Boas, Ralph P.; Buck, R. Creighton (1958), *Polynomial expansions of analytic functions*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge. **19**, Berlin, New York: Springer-Verlag, MR 0094466
- Denisyuk, I. M. (1954), "Some integrals, matrices and approximations connected with polynomials analogous to the Laguerre polynomials", *Akademiya Nauk Ukrainskoui SSR. Doklady. Seriya A. Fiziko-Matematicheskie i Tekhnicheskie Nauki* (in Ukrainian) **1954**: 239–242, ISSN 0201-8446, MR 0067241

Chapter 42

Derivation of the Routh array

The Routh array is a tabular method permitting one to establish the stability of a system using only the coefficients of the characteristic polynomial. Central to the field of control systems design, the Routh–Hurwitz theorem and Routh array emerge by using the Euclidean algorithm and Sturm's theorem in evaluating Cauchy indices.

42.1 The Cauchy index

Given the system:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \qquad (1)$$
$$= (x - r_1)(x - r_2) \cdots (x - r_n) \qquad (2)$$

Assuming no roots of $f(x) = 0$ lie on the imaginary axis, and letting

N = The number of roots of $f(x) = 0$ with negative real parts, and
P = The number of roots of $f(x) = 0$ with positive real parts

then we have

$$N + P = n \quad (3)$$

Expressing $f(x)$ in polar form, we have

$$f(x) = \rho(x) e^{j\theta(x)} \quad (4)$$

where

$$\rho(x) = \sqrt{\mathfrak{Re}^2[f(x)] + \mathfrak{Im}^2[f(x)]} \quad (5)$$

and

$$\theta(x) = \tan^{-1}\left(\mathfrak{Im}[f(x)]/\mathfrak{Re}[f(x)]\right) \quad (6)$$

from (2) note that

$$\theta(x) = \theta_{r_1}(x) + \theta_{r_2}(x) + \cdots + \theta_{r_n}(x) \quad (7)$$

where

$$\theta_{r_i}(x) = \angle(x - r_i) \quad (8)$$

Now if the i[th] root of $f(x) = 0$ has a positive real part, then (using the notation y=(RE[y],IM[y]))

$$\begin{aligned}\theta_{r_i}(x)\big|_{x=j\infty} &= \angle(x - r_i)\big|_{x=j\infty} \\ &= \angle(0 - \mathfrak{Re}[r_i], \infty - \mathfrak{Im}[r_i]) \\ &= \angle(-\mathfrak{Re}[r_i], \infty) \\ &= \lim_{\phi\to-\infty} \tan^{-1}\phi = -\frac{\pi}{2} \quad (9)\end{aligned}$$

and

$$\theta_{r_i}(x)\big|_{x=-j\infty} = \angle(-\mathfrak{Re}[r_i], -\infty) = \lim_{\phi\to\infty} \tan^{-1}\phi = \frac{\pi}{2} \quad (10)$$

Similarly, if the i[th] root of $f(x) = 0$ has a negative real part,

$$\theta_{r_i}(x)\big|_{x=j\infty} = \angle(-\mathfrak{Re}[r_i], \infty) = \lim_{\phi\to\infty} \tan^{-1}\phi = \frac{\pi}{2} \quad (11)$$

and

$$\theta_{r_i}(x)\big|_{x=-j\infty} = \angle(-\mathfrak{Re}[r_i], -\infty) = \lim_{\phi\to-\infty} \tan^{-1}\phi = -\frac{\pi}{2} \quad (12)$$

Therefore, $\theta_{r_i}(x)\Big|_{x=-j\infty}^{x=j\infty} = -\pi$ when the i[th] root of $f(x)$ has a positive real part, and $\theta_{r_i}(x)\Big|_{x=-j\infty}^{x=j\infty} = \pi$ when the i[th] root of $f(x)$ has a negative real part. Alternatively,

$$\theta(x)\big|_{x=j\infty} = \angle(x - r_1)\big|_{x=j\infty} + \angle(x - r_2)\big|_{x=j\infty} + \cdots + \angle(x - r_n)\big|_{x=j\infty} = \frac{\pi}{2}N - \frac{\pi}{2}P \quad (13)$$

and

$$\theta(x)\big|_{x=-j\infty} = \angle(x - r_1)\big|_{x=-j\infty} + \angle(x - r_2)\big|_{x=-j\infty} + \cdots + \angle(x - r_n)\big|_{x=-j\infty} = -\frac{\pi}{2}N + \frac{\pi}{2}P \quad (14)$$

So, if we define

$$\Delta = \frac{1}{\pi}\theta(x)\Big|_{-j\infty}^{j\infty} \quad (15)$$

then we have the relationship

$$N - P = \Delta \quad (16)$$

and combining (3) and (16) gives us

$$N = \tfrac{n+\Delta}{2} \text{ and } P = \tfrac{n-\Delta}{2} \quad (17)$$

Therefore, given an equation of $f(x)$ of degree n we need only evaluate this function Δ to determine N , the number of roots with negative real parts and P , the number of roots with positive real parts.

Equations (13) and (14) show that at $x = \pm\infty$, $\theta = \theta(x)$ is an integer multiple of $\pi/2$. Note now, in accordance with (6) and Figure 1, the graph of $\tan(\theta)$ vs θ , that varying x over an interval (a,b) where $\theta_a = \theta(x)|_{x=ja}$ and $\theta_b = \theta(x)|_{x=jb}$ are integer multiples of π , this variation causing the function $\theta(x)$ to have increased by π , indicates that in the course of travelling from point a to point b, θ has "jumped" from $+\infty$ to $-\infty$ one more time than it has jumped from $-\infty$ to $+\infty$. Similarly, if we vary x over an interval (a,b) this variation causing $\theta(x)$ to have decreased by π , where again θ is a multiple of π at both $x = ja$ and $x = jb$, implies that $\tan\theta(x) = \mathfrak{Im}[f(x)]/\mathfrak{Re}[f(x)]$ has jumped from $-\infty$ to $+\infty$ one more time than it has jumped from $+\infty$ to $-\infty$ as x was varied over the said interval.

Thus, $\theta(x)\Big|_{-j\infty}^{j\infty}$ is π times the difference between the number of points at which $\mathfrak{Im}[f(x)]/\mathfrak{Re}[f(x)]$ jumps from $-\infty$ to $+\infty$ and the number of points at which $\mathfrak{Im}[f(x)]/\mathfrak{Re}[f(x)]$ jumps from $+\infty$ to $-\infty$ as x ranges over the interval $(-j\infty, +j\infty)$ provided that at $x = \pm j\infty$, $\tan[\theta(x)]$ is defined.

In the case where the starting point is on an incongruity (i.e. $\theta_a = \pi/2 \pm i\pi$, *i* = 0, 1, 2, ...) the ending point will be on an incongruity as well, by equation (16) (since N is an integer and P is an integer, Δ will be an integer). In this case, we can achieve this same index (difference in positive and negative jumps) by shifting the axes of the tangent function by $\pi/2$, through adding $\pi/2$ to θ . Thus, our index is now fully defined for any combination of coefficients in $f(x)$ by evaluating $\tan[\theta] = \mathfrak{Im}[f(x)]/\mathfrak{Re}[f(x)]$ over the interval (a,b) = $(+j\infty, -j\infty)$ when our starting (and thus ending) point is not an incongruity, and by evaluating

$$\tan[\theta'(x)] = \tan[\theta + \pi/2] = -\cot[\theta(x)] = -\mathfrak{Re}[f(x)]/\mathfrak{Im}[f(x)] \quad (18)$$

over said interval when our starting point is at an incongruity.

This difference, Δ , of negative and positive jumping incongruities encountered while traversing x from $-j\infty$ to $+j\infty$ is called the Cauchy Index of the tangent of the phase angle, the phase angle being $\theta(x)$ or $\theta'(x)$, depending as θ_a is an integer multiple of π or not.

42.2 The Routh criterion

To derive Routh's criterion, first we'll use a different notation to differentiate between the even and odd terms of $f(x)$:

$$f(x) = a_0x^n + b_0x^{n-1} + a_1x^{n-2} + b_1x^{n-3} + \cdots \quad (19)$$

Now we have:

$$\begin{aligned} f(j\omega) &= a_0(j\omega)^n + b_0(j\omega)^{n-1} + a_1(j\omega)^{n-2} + b_1(j\omega)^{n-3} + \cdots && (20)\\ &= a_0(j\omega)^n + a_1(j\omega)^{n-2} + a_2(j\omega)^{n-4} + \cdots && (21)\\ &\quad + b_0(j\omega)^{n-1} + b_1(j\omega)^{n-3} + b_2(j\omega)^{n-5} + \cdots \end{aligned}$$

Therefore, if n is even,

$$\begin{aligned} f(j\omega) &= (-1)^{n/2}\left[a_0\omega^n + a_1\omega^{n-2} + a_2\omega^{n-4} + \cdots\right] && (22)\\ &\quad + j(-1)^{(n/2)-1}\left[b_0\omega^{n-1} + b_1\omega^{n-3} + b_2\omega^{n-5} + \cdots\right] \end{aligned}$$

and if n is odd:

$$\begin{aligned} f(j\omega) &= j(-1)^{(n-1)/2}\left[a_0\omega^n + a_1\omega^{n-2} + a_2\omega^{n-4} + \cdots\right] && (23)\\ &\quad + (-1)^{(n-1)/2}\left[b_0\omega^{n-1} + b_1\omega^{n-3} + b_2\omega^{n-5} + \cdots\right] \end{aligned}$$

Now observe that if n is an odd integer, then by (3) $N+P$ is odd. If $N+P$ is an odd integer, then $N-P$ is odd as well. Similarly, this same argument shows that when n is even, $N-P$ will be even. Equation (13) shows that if $N-P$ is even, θ is an integer multiple of π . Therefore, $\tan(\theta)$ is defined for n even, and is thus the proper index to use when n is even, and similarly $\tan(\theta') = \tan(\theta+\pi) = -\cot(\theta)$ is defined for n odd, making it the proper index in this latter case.

Thus, from (6) and (22), for n even:

$$\Delta = I_{-\infty}^{+\infty} \frac{-\mathfrak{Im}[f(x)]}{\mathfrak{Re}[f(x)]} = I_{-\infty}^{+\infty} \frac{b_0\omega^{n-1} - b_1\omega^{n-3} + \cdots}{a_0\omega^n - a_1\omega^{n-2} + \ldots} \quad (24)$$

and from (18) and (23), for n odd:

$$\Delta = I_{-\infty}^{+\infty} \frac{\mathfrak{Re}[f(x)]}{\mathfrak{Im}[f(x)]} = I_{-\infty}^{+\infty} \frac{b_0\omega^{n-1} - b_1\omega^{n-3} + \ldots}{a_0\omega^n - a_1\omega^{n-2} + \ldots} \quad (25)$$

Lo and behold we are evaluating the same Cauchy index for both:

$$\Delta = I_{-\infty}^{+\infty} \frac{b_0\omega^{n-1} - b_1\omega^{n-3} + \ldots}{a_0\omega^n - a_1\omega^{n-2} + \ldots} \quad (26)$$

42.3 Sturm's theorem

Sturm gives us a method for evaluating $\Delta = I_{-\infty}^{+\infty} \frac{f_2(x)}{f_1(x)}$. His theorem states as follows:

Given a sequence of polynomials $f_1(x), f_2(x), \ldots, f_m(x)$ where:

1) If $f_k(x) = 0$ then $f_{k-1}(x) \neq 0$, $f_{k+1}(x) \neq 0$, and $\text{sign}[f_{k-1}(x)] = -\text{sign}[f_{k+1}(x)]$

2) $f_m(x) \neq 0$ for $-\infty < x < \infty$

and we define $V(x)$ as the number of changes of sign in the sequence $f_1(x), f_2(x), \ldots, f_m(x)$ for a fixed value of x , then:

$$\Delta = I_{-\infty}^{+\infty} \frac{f_2(x)}{f_1(x)} = V(-\infty) - V(+\infty) \quad (27)$$

A sequence satisfying these requirements is obtained using the Euclidean algorithm, which is as follows:

Starting with $f_1(x)$ and $f_2(x)$, and denoting the remainder of $f_1(x)/f_2(x)$ by $f_3(x)$ and similarly denoting the remainder of $f_2(x)/f_3(x)$ by $f_4(x)$, and so on, we obtain the relationships:

$$\begin{aligned} f_1(x) &= q_1(x)f_2(x) - f_3(x) \quad (28)\\ f_2(x) &= q_2(x)f_3(x) - f_4(x)\\ &\ldots\\ f_{m-1}(x) &= q_{m-1}(x)f_m(x) \end{aligned}$$

or in general

$$f_{k-1}(x) = q_{k-1}(x)f_k(x) - f_{k+1}(x)$$

where the last non-zero remainder, $f_m(x)$ will therefore be the highest common factor of $f_1(x), f_2(x), \ldots, f_{m-1}(x)$. It can be observed that the sequence so constructed will satisfy the conditions of Sturm's theorem, and thus an algorithm for determining the stated index has been developed.

It is in applying Sturm's theorem (28) to (26), through the use of the Euclidean algorithm above that the Routh matrix is formed.

We get

$$f_3(\omega) = \frac{a_0}{b_0} f_2(\omega) - f_1(\omega) \quad (29)$$

and identifying the coefficients of this remainder by c_0 , $-c_1$, c_2 , $-c_3$, and so forth, makes our formed remainder

$$f_3(\omega) = c_0\omega^{n-2} - c_1\omega^{n-4} + c_2\omega^{n-6} - \cdots \quad (30)$$

where

$$c_0 = a_1 - \frac{a_0}{b_0} b_1 = \frac{b_0 a_1 - a_1 b_0}{b_0}; c_1 = a_2 - \frac{a_0}{b_0} b_2 = \frac{b_0 a_2 - a_0 b_2}{b_0}; \ldots \quad (31)$$

Continuing with the Euclidean algorithm on these new coefficients gives us

$$f_4(\omega) = \frac{b_0}{c_0} f_3(\omega) - f_2(\omega) \quad (32)$$

where we again denote the coefficients of the remainder $f_4(\omega)$ by d_0 , $-d_1$, d_2 , $-d_3$,

making our formed remainder

$$f_4(\omega) = d_0\omega^{n-3} - d_1\omega^{n-5} + d_2\omega^{n-7} - \cdots \quad (33)$$

and giving us

$$d_0 = b_1 - \frac{b_0}{c_0} c_1 = \frac{c_0 b_1 - b_1 c_0}{c_0}; d_1 = b_2 - \frac{b_0}{c_0} c_2 = \frac{c_0 b_2 - b_0 c_2}{c_0}; \ldots \quad (34)$$

The rows of the Routh array are determined exactly by this algorithm when applied to the coefficients of (19). An observation worthy of note is that in the regular case the polynomials $f_1(\omega)$ and $f_2(\omega)$ have as the highest common factor $f_{n+1}(\omega)$ and thus there will be n polynomials in the chain $f_1(x), f_2(x), \ldots, f_m(x)$.

Note now, that in determining the signs of the members of the sequence of polynomials $f_1(x), f_2(x), \ldots, f_m(x)$ that at $\omega = \pm\infty$ the dominating power of ω will be the first term of each of these polynomials, and thus only these coefficients corresponding to the highest powers of ω in $f_1(x), f_2(x), \ldots$, and $f_m(x)$, which are a_0 , b_0 , c_0 , d_0 , ... determine the signs of $f_1(x)$, $f_2(x)$, ..., $f_m(x)$ at $\omega = \pm\infty$.

So we get $V(+\infty) = V(a_0, b_0, c_0, d_0, \ldots)$ that is, $V(+\infty)$ is the number of changes of sign in the sequence $a_0\infty^n$, $b_0\infty^{n-1}$, $c_0\infty^{n-2}$, ... which is the number of sign changes in the sequence a_0 , b_0 , c_0 , d_0 , ... and $V(-\infty) = V(a_0, -b_0, c_0, -d_0, ...)$; that is $V(-\infty)$ is the number of changes of sign in the sequence $a_0(-\infty)^n$, $b_0(-\infty)^{n-1}$, $c_0(-\infty)^{n-2}$, ... which is the number of sign changes in the sequence a_0 , $-b_0$, c_0 , $-d_0$, ...

Since our chain a_0 , b_0 , c_0 , d_0 , ... will have n members it is clear that $V(+\infty) + V(-\infty) = n$ since within $V(a_0, b_0, c_0, d_0, \ldots)$ if going from a_0 to b_0 a sign change has not occurred, within $V(a_0, -b_0, c_0, -d_0, \ldots)$ going from a_0 to $-b_0$ one has, and likewise for all n transitions (there will be no terms equal to zero) giving us n total sign changes.

As $\Delta = V(-\infty) - V(+\infty)$ and $n = V(+\infty) + V(-\infty)$, and from (17) $P = (n - \Delta/2)$, we have that $P = V(+\infty) = V(a_0, b_0, c_0, d_0, \ldots)$ and have derived Routh's theorem -

The number of roots of a real polynomial $f(z)$ ***which lie in the right half plane*** $\mathfrak{Re}(r_i) > 0$ ***is equal to the number of changes of sign in the first column of the Routh scheme.***

And for the stable case where $P = 0$ then $V(a_0, b_0, c_0, d_0, \ldots) = 0$ by which we have Routh's famous criterion:

In order for all the roots of the polynomial $f(z)$ ***to have negative real parts, it is necessary and sufficient that all of the elements in the first column of the Routh scheme be different from zero and of the same sign.***

42.4 References

- Hurwitz, A., “On the Conditions under which an Equation has only Roots with Negative Real Parts”, Rpt. in Selected Papers on Mathematical Trends in Control Theory, Ed. R. T. Ballman et al. New York: Dover 1964
- Routh, E. J., A Treatise on the Stability of a Given State of Motion. London: Macmillan, 1877. Rpt. in Stability of Motion, Ed. A. T. Fuller. London: Taylor & Francis, 1975
- Gantmacher, F.R., Applications of the Theory of Matrices. Trans. J. L. Brenner et al. New York: Interscience, 1959

Chapter 43

Descartes' rule of signs

In mathematics, **Descartes' rule of signs**, first described by René Descartes in his work *La Géométrie*, is a technique for determining an upper bound on the number of positive or negative real roots of a polynomial. It is not a complete criterion, because it does not provide the exact number of positive or negative roots.

The rule is applied by counting the number of sign changes in the sequence formed of the polynomial's coefficients. If a coefficient is zero, that term is simply omitted from the sequence.

43.1 Descartes' rule of signs

43.1.1 Positive roots

The rule states that if the terms of a single-variable polynomial with real coefficients are ordered by descending variable exponent, then the number of positive roots of the polynomial is either equal to the number of sign differences between consecutive nonzero coefficients, or is less than it by an even number. Multiple roots of the same value are counted separately.

43.1.2 Negative roots

As a corollary of the rule, the number of negative roots is the number of sign changes after multiplying the coefficients of odd-power terms by −1, or fewer than it by an even number. This procedure is equivalent to substituting the negation of the variable for the variable itself. For example, to find the number of negative roots of $f(x) = ax^3+bx^2+cx+d$, we equivalently ask how many positive roots there are for $-x$ in $f(-x) = a(-x)^3 + b(-x)^2 + c(-x) + d = -ax^3 + bx^2 - cx + d \equiv g(x)$. Using Descartes' rule of signs on $g(x)$ gives the number of positive roots x_i of g, and since $g(x) = f(-x)$ it gives the number of positive roots $(-x_i)$ of f, which is the same as the number of negative roots x_i of f.

43.1.3 Example: real roots

The polynomial

$$f(x) = +x^3 + x^2 - x - 1$$

has one sign change between the second and third terms (the sequence of pairs of successive signs is ++, +−, −−). Therefore it has exactly one positive root. Note that the leading sign needs to be considered although in this particular example it does not affect the answer. To find the number of negative roots, change the signs of the coefficients of the terms with odd exponents, i.e., apply Descartes' rule of signs to the polynomial $f(-x)$, to obtain a second polynomial

$$f(-x) = -x^3 + x^2 + x - 1$$

This polynomial has two sign changes (the sequence of pairs of successive signs is −+, ++, +−), meaning that this second polynomial has two or zero positive roots; thus the original polynomial has two or zero negative roots.

In fact, the factorization of the first polynomial is

$$f(x) = (x+1)^2(x-1),$$

so the roots are −1 (twice) and 1.

The factorization of the second polynomial is

$$f(-x) = -(x-1)^2(x+1),$$

So here, the roots are 1 (twice) and −1, the negation of the roots of the original polynomial.

43.1.4 Complex roots

Any n^{th} degree polynomial has exactly *n* roots. So if $f(x)$ is a polynomial which does not have a root at 0 (which can be determined by inspection) then the minimum number of complex roots is equal to

$$n - (p+q),$$

where *p* denotes the maximum number of positive roots, *q* denotes the maximum number of negative roots (both of which can be found using Descartes' rule of signs), and *n* denotes the degree of the equation.

43.1.5 Example: zero coefficients, complex roots

The polynomial

$$f(x) = x^3 - 1\,,$$

has one sign change, so the maximum number of positive real roots is 1. From

$$f(-x) = -x^3 - 1\,,$$

we can tell that the polynomial has no negative real roots. So the minimum number of complex roots is

$$3 - (1+0) = 2\,.$$

Since complex roots of a polynomial with real coefficients must occur in conjugate pairs, we can see that x^3 - 1 has exactly 2 complex roots and 1 real (and positive) root.

43.2 Special case

The subtraction of only multiples of 2 from the maximal number of positive roots occurs because the polynomial may have complex roots, which always come in pairs since the rule applies to polynomials whose coefficients are real. Thus if the polynomial is known to have all real roots, this rule allows one to find the exact number of positive and negative roots. Since it is easy to determine the multiplicity of zero as a root, the sign of all roots can be determined in this case.

43.3 Generalizations

If the real polynomial P has k real positive roots counted with multiplicity, then for every $a > 0$ there are at least k changes of sign in the sequence of coefficients of the Taylor series of the function $e^{ax}P(x)$. For a sufficiently large, there are exactly k such changes of sign.[1][2]

In the 1970s Askold Georgevich Khovanskiĭ developed the theory of *fewnomials* that generalises Descartes' rule.[3] The rule of signs can be thought of as stating that the number of real roots of a polynomial is dependent on the polynomial's complexity, and that this complexity is proportional to the number of monomials it has, not its degree. Khovanskiĭ showed that this holds true not just for polynomials but for algebraic combinations of many transcendental functions, the so-called Pfaffian functions.

43.4 See also

- Sturm's theorem
- Rational root theorem
- Polynomial function theorems for zeros
- Properties of polynomial roots
- Gauss–Lucas theorem
- Budan's theorem

43.5 Notes

[1] D.R. Curtiss, *Recent extensions of Descartes' rule of signs*, Annals of Maths., Vol. 19, No. 4, 1918, 251 - 278.

[2] Vladimir P. Kostov, *A mapping defined by the Schur-Szegő composition*, Comptes Rendus Acad. Bulg. Sci. tome 63, No. 7, 2010, 943 - 952.

[3] Khovanskiĭ, A.G. (1991). *Fewnomials*. Translations of Mathematical Monographs. Translated from the Russian by Smilka Zdravkovska. Providence, RI: American Mathematical Society. p. 88. ISBN 0-8218-4547-0. Zbl 0728.12002.

43.6 External links

This article incorporates material from Descartes' rule of signs on PlanetMath, which is licensed under the Creative Commons Attribution/Share-Alike License.

- Descartes' Rule of Signs — Proof of the Rule
- Descartes' Rule of Signs — Basic explanation

Chapter 44

Dickson polynomial

In mathematics, the **Dickson polynomials** (or **Brewer polynomials**), denoted $D_n(x,\alpha)$, form a polynomial sequence introduced by L. E. Dickson (1897) and rediscovered by Brewer (1961) in his study of Brewer sums.

Over the complex numbers, Dickson polynomials are essentially equivalent to Chebyshev polynomials with a change of variable, and in fact Dickson polynomials are sometimes called Chebyshev polynomials. Dickson polynomials are mainly studied over finite fields, when they are not equivalent to Chebyshev polynomials. One of the main reasons for interest in them is that for fixed α, they give many examples of **permutation polynomials**: polynomials acting as permutations of finite fields.

44.1 Definition

$D_0(x,\alpha) = 2$, and for $n > 0$ Dickson polynomials (of the first kind) are given by

$$D_n(x,\alpha) = \sum_{p=0}^{\lfloor n/2 \rfloor} \frac{n}{n-p}\binom{n-p}{p}(-\alpha)^p x^{n-2p}.$$

The first few Dickson polynomials are

$$D_0(x,\alpha) = 2$$

$$D_1(x,\alpha) = x$$

$$D_2(x,\alpha) = x^2 - 2\alpha$$

$$D_3(x,\alpha) = x^3 - 3x\alpha$$

$$D_4(x,\alpha) = x^4 - 4x^2\alpha + 2\alpha^2.$$

The Dickson polynomials of the second kind E_n are defined by

$$E_n(x,\alpha) = \sum_{p=0}^{\lfloor n/2 \rfloor} \binom{n-p}{p}(-\alpha)^p x^{n-2p}.$$

They have not been studied much, and have properties similar to those of Dickson polynomials of the first kind. The first few Dickson polynomials of the second kind are

$$E_0(x,\alpha) = 1$$

$$E_1(x,\alpha) = x$$

$E_2(x,\alpha) = x^2 - \alpha$

$E_3(x,\alpha) = x^3 - 2x\alpha$

$E_4(x,\alpha) = x^4 - 3x^2\alpha + \alpha^2.$

44.2 Properties

The *Dn* satisfy the identities

$D_n(u + \alpha/u, \alpha) = u^n + (\alpha/u)^n\,;$

$D_{mn}(x,\alpha) = D_m(D_n(x,\alpha),\alpha^n)\,.$

For *n*≥2 the Dickson polynomials satisfy the recurrence relation

$D_n(x,\alpha) = xD_{n-1}(x,\alpha) - \alpha D_{n-2}(x,\alpha)$

$E_n(x,\alpha) = xE_{n-1}(x,\alpha) - \alpha E_{n-2}(x,\alpha).$

The Dickson polynomial *Dn* = *y* is a solution of the ordinary differential equation

$(x^2 - 4\alpha)y'' + xy' - n^2y = 0$

and the Dickson polynomial *En* = *y* is a solution of the differential equation

$(x^2 - 4\alpha)y'' + 3xy' - n(n+2)y = 0.$

Their ordinary generating functions are

$$\sum_n D_n(x,\alpha)z^n = \frac{2 - xz}{1 - xz + \alpha z^2}$$

$$\sum_n E_n(x,\alpha)z^n = \frac{1}{1 - xz + \alpha z^2}.$$

44.3 Links to other polynomials

- Dickson polynomials over the complex numbers are related to Chebyshev polynomials *Tn* and *Un* by

$D_n(2xa, a^2) = 2a^nT_n(x)$

$E_n(2xa, a^2) = a^nU_n(x).$

Crucially, the Dickson polynomial *Dn*(*x*,*a*) can be defined over rings in which *a* is not a square, and over rings of characteristic 2; in these cases, *Dn*(*x*,*a*) is often not related to a Chebyshev polynomial.

- The Dickson polynomials with parameter α = 1 or α = −1 are related to the Fibonacci and Lucas polynomials.
- The Dickson polynomials with parameter α = 0 give monomials:

$D_n(x,0) = x^n\,.$

44.4 Permutation polynomials and Dickson polynomials

A **permutation polynomial** (for a given finite field) is one that acts as a permutation of the elements of the finite field.

The Dickson polynomial $Dn(x,\alpha)$ (considered as a function of x with α fixed) is a permutation polynomial for the field with q elements if and only if n is coprime to q^2-1.[1]

M. Fried (1970) proved that any integral polynomial that is a permutation polynomial for infinitely many prime fields is a composition of Dickson polynomials and linear polynomials (with rational coefficients). This assertion has become known as Schur's conjecture, although in fact Schur did not make this conjecture. Since Fried's paper contained numerous errors, a corrected account was given by G. Turnwald (1995), and subsequently P. Müller (1997) gave a simpler proof along the lines of an argument due to Schur.

Further, P. Müller (1997) proved that any permutation polynomial over the finite field $\mathbf{F}q$ whose degree is simultaneously coprime to $q-1$ and less than $q^{1/4}$ must be a composition of Dickson polynomials and linear polynomials.

44.5 References

[1] Lidl & Niederreiter (1997) p.356

- Brewer, B. W. (1961), "On certain character sums", *Transactions of the American Mathematical Society* **99**: 241–245, doi:10.2307/1993392, ISSN 0002-9947, MR 0120202, Zbl 0103.03205
- Dickson, L.E. (1897). "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group I,II". *Ann. Of Math.* (The Annals of Mathematics) **11** (1/6): 65–120; 161–183. doi:10.2307/1967217. ISSN 0003-486X. JFM 28.0135.03. JSTOR 1967217.
- Fried, Michael (1970). "On a conjecture of Schur". *Michigan Math. J.* **17**: 41–55. doi:10.1307/mmj/1029000374. ISSN 0026-2285. MR 0257033. Zbl 0169.37702.
- Lidl, R.; Mullen, G. L.; Turnwald, G. (1993). *Dickson polynomials*. Pitman Monographs and Surveys in Pure and Applied Mathematics **65**. Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York. ISBN 0-582-09119-5. MR 1237403. Zbl 0823.11070.
- Lidl, Rudolf; Niederreiter, Harald (1997). *Finite fields*. Encyclopedia of Mathematics and Its Applications **20** (2nd ed.). Cambridge University Press. ISBN 0-521-39231-4. Zbl 0866.11069.
- Mullen, Gary L. (2001), "D/d120140", in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Müller, Peter (1997). "A Weil-bound free proof of Schur's conjecture". *Finite Fields Appl.* **3**: 25–32. doi:10.1006/ffta.1996.0170. Zbl 0904.11040.
- Rassias, Thermistocles M.; Srivastava, H.M.; Yanushauskas, A. (1991). *Topics in Polynomials of One and Several Variables and Their Applications: A Legacy of P.L.Chebyshev*. World Scientific. pp. 371–395. ISBN 981-02-0614-3.
- Turnwald, Gerhard (1995). "On Schur's conjecture". *J. Austral. Math. Soc. Ser. A* **58** (03): 312–357. doi:10.1017/S1446788700038349. MR 1329867. Zbl 0834.11052.
- Young, Paul Thomas (2002). "On modified Dickson polynomials" (PDF). *Fib. Quarterly* **40** (1): 33–40.

Chapter 45

Difference polynomials

In mathematics, in the area of complex analysis, the **general difference polynomials** are a polynomial sequence, a certain subclass of the Sheffer polynomials, which include the Newton polynomials, **Selberg's polynomials**, and the **Stirling interpolation polynomials** as special cases.

45.1 Definition

The general difference polynomial sequence is given by

$$p_n(z) = \frac{z}{n}\binom{z-\beta n-1}{n-1}$$

where $\binom{z}{n}$ is the binomial coefficient. For $\beta = 0$, the generated polynomials $p_n(z)$ are the Newton polynomials

$$p_n(z) = \binom{z}{n} = \frac{z(z-1)\cdots(z-n+1)}{n!}.$$

The case of $\beta = 1$ generates Selberg's polynomials, and the case of $\beta = -1/2$ generates Stirling's interpolation polynomials.

45.2 Moving differences

Given an analytic function $f(z)$, define the **moving difference** of f as

$$\mathcal{L}_n(f) = \Delta^n f(\beta n)$$

where Δ is the forward difference operator. Then, provided that f obeys certain summability conditions, then it may be represented in terms of these polynomials as

$$f(z) = \sum_{n=0}^{\infty} p_n(z)\mathcal{L}_n(f).$$

The conditions for summability (that is, convergence) for this sequence is a fairly complex topic; in general, one may say that a necessary condition is that the analytic function be of less than exponential type. Summability conditions are discussed in detail in Boas & Buck.

45.3 Generating function

The generating function for the general difference polynomials is given by

$$e^{zt} = \sum_{n=0}^{\infty} p_n(z) \left[\left(e^t - 1 \right) e^{\beta t} \right]^n .$$

This generating function can be brought into the form of the generalized Appell representation

$$K(z, w) = A(w)\Psi(zg(w)) = \sum_{n=0}^{\infty} p_n(z) w^n$$

by setting $A(w) = 1$, $\Psi(x) = e^x$, $g(w) = t$ and $w = (e^t - 1)e^{\beta t}$.

45.4 See also

- Carlson's theorem

45.5 References

- Ralph P. Boas, Jr. and R. Creighton Buck, *Polynomial Expansions of Analytic Functions (Second Printing Corrected)*, (1964) Academic Press Inc., Publishers New York, Springer-Verlag, Berlin. Library of Congress Card Number 63-23263.

Chapter 46

Discriminant

In algebra, the **discriminant** of a polynomial is a function of its coefficients, typically denoted by a capital 'D' or the capital Greek letter Delta (Δ). It gives information about the nature of its roots. Typically, the discriminant is zero if and only if the polynomial has a multiple root. For example, the discriminant of the quadratic polynomial

$$ax^2 + bx + c$$

is

$$\Delta = b^2 - 4ac.$$

Here for real a, b and c, if $\Delta > 0$, the polynomial has two real roots, if $\Delta = 0$, the polynomial has one real double root, and if $\Delta < 0$, the two roots of the polynomial are complex conjugates.

The discriminant of the cubic polynomial

$$ax^3 + bx^2 + cx + d$$

is

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

For higher degrees, the discriminant is always a polynomial function of the coefficients. It becomes significantly longer for the higher degrees. The discriminant of a *general* quartic has 16 terms,[1] that of a quintic has 59 terms,[2] that of a 6th degree polynomial has 246 terms,[3] and the number of terms increases exponentially with the degree.

A polynomial has a multiple root (i.e. a root with multiplicity greater than one) in the complex numbers if and only if its discriminant is zero.

The concept also applies if the polynomial has coefficients in a field which is not contained in the complex numbers. In this case, the discriminant vanishes if and only if the polynomial has a multiple root in any algebraically closed field containing the coefficients.

As the discriminant is a polynomial function of the coefficients, it is defined as long as the coefficients belong to an integral domain R and, in this case, the discriminant is in R. In particular, the discriminant of a polynomial with integer coefficients is always an integer. This property is widely used in number theory.

The term “discriminant” was coined in 1851 by the British mathematician James Joseph Sylvester.[4]

46.1 Definition

In terms of the roots, the discriminant is given by

$$\Delta = a_n^{2n-2}\prod_{i<j}(r_i - r_j)^2 = (-1)^{n(n-1)/2}a_n^{2n-2}\prod_{i\neq j}(r_i - r_j)$$

where a_n is the leading coefficient and $r_1, ..., r_n$ are the roots (counting multiplicity) of the polynomial in some splitting field. It is the square of the Vandermonde polynomial times a_n^{2n-2} .

As the discriminant is a symmetric function in the roots, it can also be expressed in terms of the coefficients of the polynomial, since the coefficients are the elementary symmetric polynomials in the roots; such a formula is given below.

Expressing the discriminant in terms of the roots makes its key property clear, namely that it vanishes if and only if there is a repeated root, but does not allow it to be calculated without factoring a polynomial, after which the information it provides is redundant (if one has the roots, one can tell if there are any duplicates). Hence the formula in terms of the coefficients allows the nature of the roots to be determined without factoring the polynomial.

46.2 Formulas for low degrees

The discriminant of a linear polynomial (degree 1) is rarely considered. If needed, it is commonly defined to be equal to 1 (this is compatible with the usual conventions for the empty product and the determinant of the empty matrix). There is no common convention for the discriminant of a constant polynomial (degree 0).

The quadratic polynomial

$$ax^2 + bx + c$$

has discriminant

$$\Delta = b^2 - 4ac.$$

The cubic polynomial

$$ax^3 + bx^2 + cx + d$$

has discriminant

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

The quartic polynomial

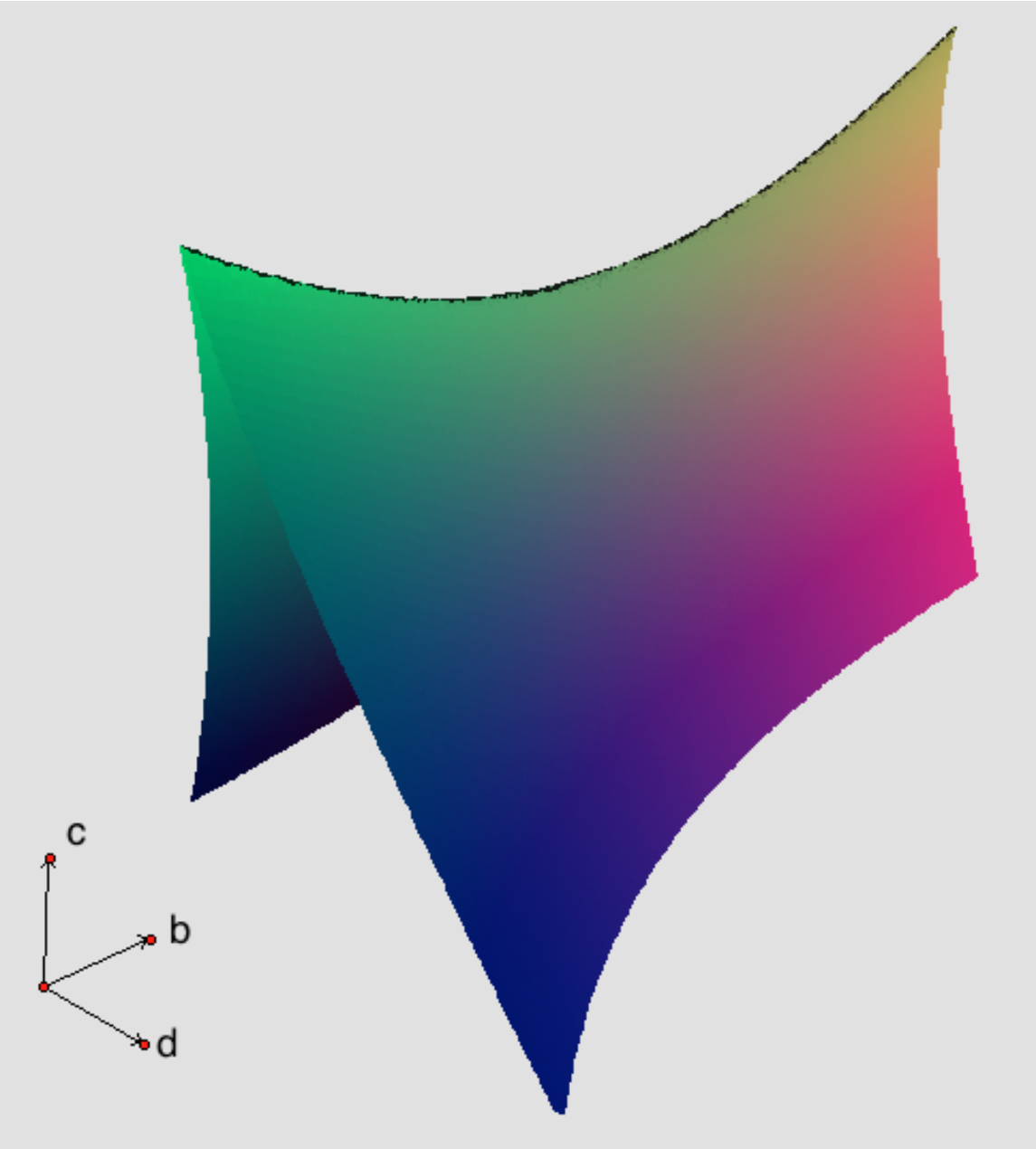
$$ax^4 + bx^3 + cx^2 + dx + e$$

has discriminant

$$\Delta = 256a^3e^3 - 192a^2bde^2 - 128a^2c^2e^2 + 144a^2cd^2e - 27a^2d^4 + 144ab^2ce^2 - 6ab^2d^2e$$
$$-80abc^2de + 18abcd^3 + 16ac^4e - 4ac^3d^2 - 27b^4e^2 + 18b^3cde - 4b^3d^3 - 4b^2c^3e + b^2c^2d^2.$$

These are homogeneous polynomials in the coefficients, respectively of degree 2, 4 and 6. They are also homogeneous in terms of the roots, of respective degrees 2, 6 and 12.

Simpler polynomials have simpler expressions for their discriminants. For example, the monic quadratic polynomial $x^2 + bx + c$ has discriminant $\Delta = b^2 - 4c$. The monic cubic polynomial without quadratic term $x^3 + px + q$ has discriminant $\Delta = -4p^3 - 27q^2$. In terms of the roots, these discriminants are homogeneous polynomials of respective degree 2 and 6.



The zero set of discriminant of the cubic $x^3 + bx^2 + cx + d$ *, i.e. points satisfying* $b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd = 0$.

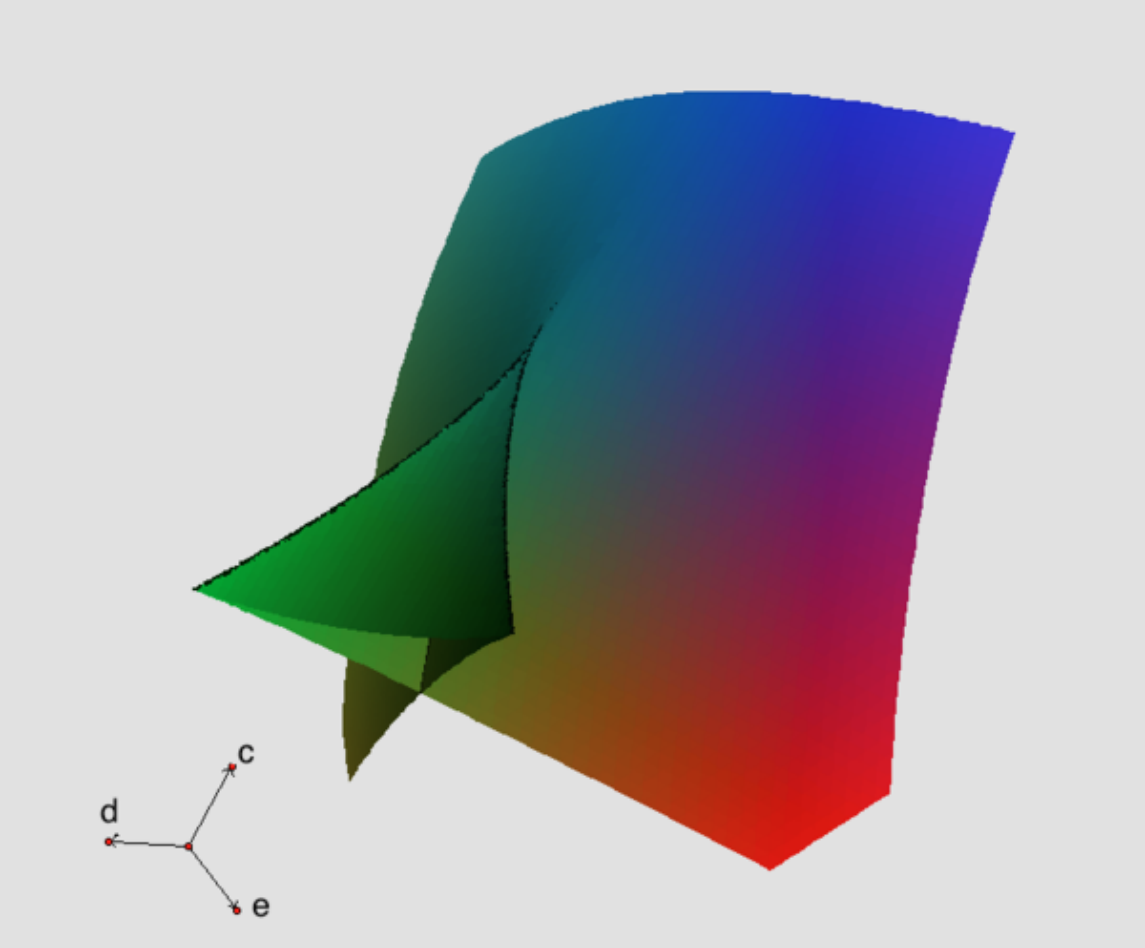
46.3 Homogeneity

The discriminant is a homogeneous polynomial in the coefficients; it is also a homogeneous polynomial in the roots.

In the coefficients, the discriminant is homogeneous of degree $2n-2$; this can be seen two ways. In terms of the roots-and-leading-term formula, multiplying all the coefficients by λ does not change the roots, but multiplies the leading term by λ. In terms of the formula as a determinant of a $(2n-1) \times (2n-1)$ matrix divided by a_n, the determinant of the matrix is homogeneous of degree $2n-1$ in the entries, and dividing by a_n makes the degree $2n-2$; explicitly, multiplying the coefficients by λ multiplies all entries of the matrix by λ, hence multiplies the determinant by λ^{2n-1}.

For a monic polynomial, the discriminant is a polynomial in the roots alone (as the a_n term is one), and is of degree $n(n-1)$ in the roots, as there are $\binom{n}{2} = \frac{n(n-1)}{2}$ terms in the product, each squared.

Let us consider the polynomial



The discriminant of the quartic polynomial $x^4 + cx^2 + dx + e$. The surface represents point (a,b,c) where the polynomial has a repeated roots, the cuspidal edge correspond to polynomials with a triple root and the self intersection to the polynomials with two different repeated roots.

$$P = a_0x^n + a_1x_{n-1} + \cdots + a_n.$$

It follows from what precedes that its discriminant is homogeneous of degree 2*n*−2 in the a_i and quasi-homogeneous of weight *n*(*n*−1) if each a_i is given the weight *i*. In other words, every monomial $a_0^{i_0} \cdots, a_n^{i_n}$ appearing in the discriminant satisfies the two equations

$$i_0 + i_1 + \cdots + i_n = 2n - 2$$

and

$$0\,i_0 + 1\,i_1 + \cdots + n\,i_n = n(n-1)$$

These thus correspond to the partitions of *n*(*n*−1) into at 2*n*−2 (non negative) parts of size at most n

This restricts the possible terms in the discriminant. For the quadratic polynomial $ax^2 + bx + c$ there are only two possibilities for $[i_0, i_1, i_2]$, either [1,0,1] or [0,2,0], given the two monomials *ac* and b^2. For the cubic polynomial $ax^3 + bx^2 + cx + d$, these are the partitions of 6 into 4 parts of size at most 3:

$$a^2d^2 = aadd : 0+0+3+3 \qquad abcd : 0+1+2+3 \qquad ac^3 = accc : 0+2+2+2$$
$$b^3d = bbbd : 1+1+1+3 \qquad b^2c^2 = bbcc : 1+1+2+2.$$

All these five monomials occur effectively in the discriminant.

While this approach gives the possible terms, it does not determine the coefficients. Moreover, in general not all possible terms will occur in the discriminant. The first example is for the quartic polynomial $ax^4+bx^3+cx^2+dx+e$, in which case $(i_0,\ldots,i_4) = (0,1,4,1,0)$ satisfies $0+1+4+1+0 = 6$ and $1\cdot 1+2\cdot 4+3\cdot 1 = 12$, even though the corresponding discriminant does not involve the monomial bc^4d .

46.4 Quadratic formula

The quadratic polynomial $p(x) = ax^2 + bx + c$ has discriminant

$$\Delta = b^2 - 4ac,$$

which is the quantity under the square root sign in the quadratic formula. For real numbers *a*, *b*, *c*, one has:

- When $\Delta > 0$, $P(x)$ has two distinct real roots

$$x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

and its graph crosses the *x*-axis twice.

- When $\Delta = 0$, $P(x)$ has two coincident real roots

$$x_1 = x_2 = -\frac{b}{2a}$$

and its graph is tangent to the *x*-axis.

- When $\Delta < 0$, $P(x)$ has no real roots, and its graph lies strictly above or below the *x*-axis. The polynomial has two distinct complex roots

$$z_{1,2} = \frac{-b \pm i\sqrt{-\Delta}}{2a} = \frac{-b \pm i\sqrt{4ac - b^2}}{2a}.$$

An alternative way to understand the discriminant of a quadratic is to use the characterization as "zero if and only if the polynomial has a repeated root". In that case the polynomial is $(x-r)^2 = x^2 - 2rx + r^2$. The coefficients then satisfy $(-2r)^2 = 4(r^2)$, so $b^2 = 4c$, and a monic quadratic has a repeated root if and only if this is the case, in which case the root is $r = -b/2$. Putting both terms on one side and including a leading coefficient yields $b^2 - 4ac$.

46.5 Discriminant of a polynomial

To find the formula for the discriminant of a polynomial in terms of its coefficients, it is easiest to introduce the resultant. Just as the discriminant of a single polynomial is the product of the square of the differences between distinct roots, the resultant of two polynomials is the product of the differences between their roots, and just as the discriminant vanishes if and only if the polynomial has a repeated root, the resultant vanishes if and only if the two polynomials share a root.

Since a polynomial $p(x)$ has a repeated root if and only if it shares a root with its derivative $p'(x)$, the discriminant $D(p)$ and the resultant $R(p,p')$ both have the property that they vanish if and only if *p* has a repeated root, and they have almost the same degree (the degree of the resultant is one greater than the degree of the discriminant) and thus are equal up to a factor of degree one.

The benefit of the resultant is that it can be computed as a determinant, namely as the determinant of the Sylvester matrix, a $(2n-1)\times(2n-1)$ matrix, whose *n* first rows contain the coefficients of *p* and the $n-1$ last ones the coefficients of its derivative.

The resultant $R(p,p')$ of the general polynomial

$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0$

is equal to the determinant of the (2*n* − 1)×(2*n* − 1) Sylvester matrix:

$$R(p,p') = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \ldots & a_1 & a_0 & 0\ldots & \ldots & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & \ldots & a_1 & a_0 & 0\ldots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \ldots & 0 & a_n & a_{n-1} & a_{n-2} & \ldots & a_1 & a_0 \\ na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \ldots & a_1 & 0 & \ldots & \ldots & 0 \\ 0 & na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \ldots & a_1 & 0 & \ldots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & \ldots & 0 & na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \ldots & a_1 \end{vmatrix}.$$

The discriminant $D(p)$ of $p(x)$ is now given by the formula

$$D(p) = (-1)^{\frac{1}{2}n(n-1)}\frac{1}{a_n}R(p,p').$$

For example, in the case *n* = 4, the above determinant is

$$\begin{vmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ 4a_4 & 3a_3 & 2a_2 & 1a_1 & 0 & 0 & 0 \\ 0 & 4a_4 & 3a_3 & 2a_2 & 1a_1 & 0 & 0 \\ 0 & 0 & 4a_4 & 3a_3 & 2a_2 & 1a_1 & 0 \\ 0 & 0 & 0 & 4a_4 & 3a_3 & 2a_2 & 1a_1 \end{vmatrix}.$$

The discriminant of the degree 4 polynomial is then obtained from this determinant upon dividing by a_4 .

In terms of the roots, the discriminant is equal to

$$a_n^{2n-2}\prod_{i<j}(r_i - r_j)^2$$

where *r*1, ..., *rn* are the complex roots (counting multiplicity) of the polynomial:

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \\ &= a_n(x - r_1)(x - r_2)\ldots(x - r_n). \end{aligned}$$

This second expression makes it clear that *p* has a multiple root if and only if the discriminant is zero. (This multiple root can be complex.)

The discriminant can be defined for polynomials over arbitrary fields, in exactly the same fashion as above. The product formula involving the roots *ri* remains valid; the roots have to be taken in some splitting field of the polynomial. The discriminant can even be defined for polynomials over any commutative ring. However, if the ring is not an integral domain, above division of the resultant by a_n should be replaced by substituting a_n by 1 in the first column of the matrix.

46.6 Nature of the roots

The discriminant gives additional information on the nature of the roots beyond simply whether there are any repeated roots: for polynomials with real coefficients, it also gives information on whether the roots are real or complex. This is most transparent and easily stated for quadratic and cubic polynomials; for polynomials of degree 4 or higher this is more difficult to state.

46.6.1 Quadratic

Because the quadratic formula expressed the roots of a quadratic polynomial as a rational function in terms of the *square root* of the discriminant, the roots of a quadratic polynomial are in the same field as the coefficients if and only if the discriminant is a square in the field of coefficients: in other words, the polynomial factors over the field of coefficients if and only if the discriminant is a square.

As a real number has real square roots if and only if it is nonnegative, and these roots are distinct if and only if it is positive (not zero), the sign of the discriminant allows a complete description of the nature of the roots of a quadratic polynomial with real coefficients: [5]

- $\Delta > 0$: 2 distinct real roots: factors over the reals;
- $\Delta < 0$: 2 distinct complex roots (complex conjugate), does not factor over the reals;
- $\Delta = 0$: 1 real root with multiplicity 2: factors over the reals as a square.

Further, for a quadratic polynomial with rational coefficients, it factors over the rationals if and only if the discriminant – which is necessarily a rational number, being a polynomial in the coefficients – is in fact a square.

46.6.2 Cubic

For more details on this topic, see Cubic polynomial § The nature of the roots.

For a cubic polynomial with real coefficients, the discriminant reflects the nature of the roots as follows: [6]

- $\Delta > 0$: the equation has 3 distinct real roots;
- $\Delta < 0$, the equation has 1 real root and 2 complex conjugate roots;
- $\Delta = 0$: at least 2 roots coincide, and they are all real.

  It may be that the equation has a double real root and another distinct single real root; alternatively, all three roots coincide yielding a triple real root.

If a cubic polynomial has a triple root, it is a root of its derivative and of its second derivative, which is linear. Thus to decide if a cubic polynomial has a triple root or not, one may compute the root of the second derivative and look if it is a root of the cubic and of its derivative.

46.6.3 Higher degrees

More generally, for a polynomial of degree n with real coefficients, we have

- $\Delta > 0$: for some integer k such that $0 \leq k \leq \frac{n}{4}$, there are $2k$ pairs of complex conjugate roots and $n-4k$ real roots, all different;
- $\Delta < 0$: for some integer k such that $0 \leq k \leq \frac{n-2}{4}$, there are $2k+1$ pairs of complex conjugate roots and $n-4k-2$ real roots, all different;
- $\Delta = 0$: at least 2 roots coincide, which may be either real or not real (in this case their complex conjugates also coincide).

46.7 Discriminant of a polynomial over a commutative ring

The definition of the discriminant of a polynomial in terms of the resultant may easily be extended to polynomials whose coefficients belong to any commutative ring. However, as the division is not always defined in such a ring, instead of dividing the determinant by the leading coefficient, one substitutes the leading coefficient by 1 in the

first column of the determinant. This generalized discriminant has the following property which is fundamental in algebraic geometry.

Let f be a polynomial with coefficients in a commutative ring A and D its discriminant. Let φ be a ring homomorphism of A into a field K and $\varphi(f)$ be the polynomial over K obtained by replacing the coefficients of f by their images by φ. Then $\varphi(D) = 0$ if and only if either the difference of the degrees of f and $\varphi(f)$ is at least 2 or $\varphi(f)$ has a multiple root in an algebraic closure of K. The first case may be interpreted by saying that $\varphi(f)$ has a multiple root at infinity.

The typical situation where this property is applied is when A is a (univariate or multivariate) polynomial ring over a field k and φ is the substitution of the indeterminates in A by elements of a field extension K of k.

For example, let f be a bivariate polynomial in X and Y with real coefficients, such that $f = 0$ is the implicit equation of a plane algebraic curve. Viewing f as a univariate polynomial in Y with coefficients depending on X, then the discriminant is a polynomial in X whose roots are the X-coordinates of the singular points, of the points with a tangent parallel to the Y-axis and of some of the asymptotes parallel to the Y-axis. In other words the computation of the roots of the Y-discriminant and the X-discriminant allows to compute all remarkable points of the curve, except the inflection points.

46.8 Generalizations

The concept of discriminant has been generalized to other algebraic structures besides polynomials of one variable, including conic sections, quadratic forms, and algebraic number fields. Discriminants in algebraic number theory are closely related, and contain information about ramification. In fact, the more geometric types of ramification are also related to more abstract types of discriminant, making this a central algebraic idea in many applications.

46.8.1 Discriminant of a conic section

For a conic section defined in plane geometry by the real polynomial

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0,$$

the discriminant is equal to[7]

$$B^2 - 4AC,$$

and determines the shape of the conic section. If the discriminant is less than 0, the equation is of an ellipse or a circle. If the discriminant equals 0, the equation is that of a parabola. If the discriminant is greater than 0, the equation is that of a hyperbola. This formula will not work for degenerate cases (when the polynomial factors).

46.8.2 Discriminant of a quadratic form

There is a substantive generalization to quadratic forms Q over any field K of characteristic $\neq 2$. For characteristic 2, the corresponding invariant is the Arf invariant.

Given a quadratic form Q, the **discriminant** or **determinant** is the determinant of a symmetric matrix S for Q.[8]

Change of variables by a matrix A changes the matrix of the symmetric form by $A^T SA$, which has determinant $(\det A)^2 \det S$, so under change of variables, the discriminant changes by a non-zero square, and thus the class of the discriminant is well-defined in $K/(K^*)^2$, i.e., up to non-zero squares. See also quadratic residue.

Less intrinsically, by a theorem of Jacobi, quadratic forms on K^n can be expressed, after a linear change of variables, in **diagonal form** as

$$a_1 x_1^2 + \cdots + a_n x_n^2.$$

More precisely, a quadratic forms on V may be expressed as a sum

$$\sum_{i=1}^{n} a_i L_i^2$$

where the *Li* are independent linear forms and *n* is the number of the variables (some of the *ai* may be zero). Then the discriminant is the product of the *ai*, which is well-defined as a class in $K/(K^*)^2$.

For *K*=**R**, the real numbers, $(\mathbf{R}^*)^2$ is the positive real numbers (any positive number is a square of a non-zero number), and thus the quotient $\mathbf{R}/(\mathbf{R}^*)^2$ has three elements: positive, zero, and negative. This is a cruder invariant than signature (n_0, n_+, n_-), where n_0 is the number 0s and $n\pm$ is the number of ±1s in diagonal form. The discriminant is then zero if the form is degenerate ($n_0 > 0$), and otherwise it is the parity of the number of negative coefficients, $(-1)^{n-}$.

For *K*=**C**, the complex numbers, $(\mathbf{C}^*)^2$ is the non-zero complex numbers (any complex number is a square), and thus the quotient $\mathbf{C}/(\mathbf{C}^*)^2$ has two elements: non-zero and zero.

This definition generalizes the discriminant of a quadratic polynomial, as the polynomial $ax^2 + bx + c$ homogenizes to the quadratic form $ax^2 + bxy + cy^2$ which has symmetric matrix

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}.$$

whose determinant is $ac - (b/2)^2 = ac - b^2/4$ Up to a factor of –4, this is $b^2 - 4ac$

The invariance of the class of the discriminant of a real form (positive, zero, or negative) corresponds to the corresponding conic section being an ellipse, parabola, or hyperbola.

46.8.3 Discriminant of an algebraic number field

Main article: Discriminant of an algebraic number field

46.9 Alternating polynomials

Main article: Alternating polynomials

The discriminant is a symmetric polynomial in the roots; if one adjoins a square root of it (halves each of the powers: the Vandermonde polynomial) to the ring of symmetric polynomials in *n* variables Λ_n , one obtains the ring of alternating polynomials, which is thus a quadratic extension of Λ_n .

46.10 References

[1] Wang, Dongming (2004). *Elimination practice: software tools and applications*. Imperial College Press. p. 180. ISBN 1-86094-438-8., Chapter 10 page 180

[2] Gelfand, I. M.; Kapranov, M. M.; Zelevinsky, A. V. (1994). *Discriminants, resultants and multidimensional determinants*. Birkhäuser. p. 1. ISBN 3-7643-3660-9., Preview page 1

[3] Dickenstein, Alicia; Emiris, Ioannis Z. (2005). *Solving polynomial equations: foundations, algorithms, and applications*. Springer. p. 26. ISBN 3-540-24326-7., Chapter 1 page 26

[4] J. J. Sylvester (1851) "On a remarkable discovery in the theory of canonical forms and of hyperdeterminants," *Philosophical Magazine*, 4th series, **2** : 391-410; Sylvester coins the word "discriminant" on page 406.

[5] Irving, Ronald S. (2004), *Integers, polynomials, and rings*, Springer-Verlag New York, Inc., ISBN 0-387-40397-3, Chapter 10.3 pp. 153–154

[6] Irving, Ronald S. (2004), *Integers, polynomials, and rings*, Springer-Verlag New York, Inc., ISBN 0-387-40397-3, Chapter 10 ex 10.14.4 and 10.17.4, pp. 154–156

[7] Fanchi, John R. (2006), *Math refresher for scientists and engineers*, John Wiley and Sons, pp. 44–45, ISBN 0-471-75715-2, Section 3.2, page 45

[8] Cassels, J.W.S. (1978). *Rational Quadratic Forms.* London Mathematical Society Monographs **13**. Academic Press. p. 6. ISBN 0-12-163260-1. Zbl 0395.10029.

46.11 External links

- Mathworld article
- Planetmath article

Chapter 47

Divided power structure

In mathematics, specifically commutative algebra, a **divided power structure** is a way of making expressions of the form $x^n/n!$ meaningful even when it is not possible to actually divide by $n!$.

47.1 Definition

Let *A* be a commutative ring with an ideal *I*. A **divided power structure** (or **PD-structure**, after the French *puissances divisées*) on *I* is a collection of maps $\gamma_n : I \to A$ for *n*=0, 1, 2, ... such that:

1. $\gamma_0(x) = 1$ and $\gamma_1(x) = x$ for $x \in I$, while $\gamma_n(x) \in I$ for $n > 0$.
2. $\gamma_n(x + y) = \sum_{i=0}^{n} \gamma_{n-i}(x)\gamma_i(y)$ for $x, y \in I$.
3. $\gamma_n(\lambda x) = \lambda^n \gamma_n(x)$ for $\lambda \in A, x \in I$.
4. $\gamma_m(x)\gamma_n(x) = ((m, n))\gamma_{m+n}(x)$ for $x \in I$, where $((m, n)) = \frac{(m+n)!}{m!n!}$ is an integer.
5. $\gamma_n(\gamma_m(x)) = C_{n,m}\gamma_{mn}(x)$ for $x \in I$, where $C_{n,m} = \frac{(mn)!}{(m!)^n n!}$ is an integer.

For convenience of notation, $\gamma_n(x)$ is often written as $x^{[n]}$ when it is clear what divided power structure is meant.

The term *divided power ideal* refers to an ideal with a given divided power structure, and *divided power ring* refers to a ring with a given ideal with divided power structure.

Homomorphisms of divided power algebras are ring homomorphisms that respects the divided power structure on its source and target.

47.2 Examples

- $\mathbb{Z}\langle x\rangle := \mathbb{Z}[x, \frac{x^2}{2}, \ldots, \frac{x^n}{n!}, \ldots] \subset \mathbb{Q}[x]$ is a divided power algebra, it is the free divided power algebra over $\mathbb{Z}$ on one generator.

- If *A* is an algebra over the rational numbers **Q**, then every ideal *I* has a unique divided power structure where $\gamma_n(x) = \frac{1}{n!} \cdot x^n$. (The uniqueness follows from the easily verified fact that in general, $x^n = n!\gamma_n(x)$.) Indeed, this is the example which motivates the definition in the first place.

- If *A* is a ring of characteristic $p > 0$, where *p* is prime, and *I* is an ideal such that $I^p = 0$, then we can define a divided power structure on *I* where $\gamma_n(x) = \frac{1}{n!}x^n$ if $n < p$, and $\gamma_n(x) = 0$ if $n \geq p$. (Note the distinction between I^p and the ideal generated by x^p for $x \in I$; the latter is always zero if a divided power structure exists, while the former is not necessarily zero.)

- If *M* is an *A*-module, let $S^{\cdot}M$ denote the symmetric algebra of *M* over *A*. Then its dual $(S^{\cdot}M)^{\check{}} = Hom_A(S^{\cdot}M, A)$ has a canonical structure of divided power ring. In fact, it is canonically isomorphic to a natural completion of $\Gamma_A(\check{M})$ (see below) if *M* has finite rank.

47.3 Constructions

If *A* is any ring, there exists a divided power ring

$$A\langle x_1, x_2, \ldots, x_n\rangle$$

consisting of *divided power polynomials* in the variables

$$x_1, x_2, \ldots, x_n,$$

that is sums of *divided power monomials* of the form

$$cx_1^{[i_1]}x_2^{[i_2]}\cdots x_n^{[i_n]}$$

with $c \in A$. Here the divided power ideal is the set of divided power polynomials with constant coefficient 0.

More generally, if *M* is an *A*-module, there is a universal *A*-algebra, called

$$\Gamma_A(M),$$

with PD ideal

$$\Gamma_+(M)$$

and an *A*-linear map

$$M \to \Gamma_+(M).$$

(The case of divided power polynomials is the special case in which *M* is a free module over *A* of finite rank.)

If *I* is any ideal of a ring *A*, there is a universal construction which extends *A* with divided powers of elements of *I* to get a **divided power envelope** of *I* in *A*.

47.4 Applications

The divided power envelope is a fundamental tool in the theory of PD differential operators and crystalline cohomology, where it is used to overcome technical difficulties which arise in positive characteristic.

The divided power functor is used in the construction of co-Schur functors.

47.5 References

- Berthelot, Pierre; Ogus, Arthur (1978). *Notes on Crystalline Cohomology*. Annals of Mathematics Studies. Princeton University Press. Zbl 0383.14010.
- Hazewinkel, Michiel (1978). *Formal Groups and Applications*. Pure and applied mathematics, a series of monographs and textbooks **78**. Elsevier. p. 507. ISBN 0123351502. Zbl 0454.14020.

Chapter 48

Division polynomials

In mathematics the **division polynomials** provide a way to calculate multiples of points on elliptic curves and to study the fields generated by torsion points. They play a central role in the study of counting points on elliptic curves in Schoof's algorithm.

48.1 Definition

The set of division polynomials is a sequence of polynomials in $\mathbb{Z}[x, y, A, B]$ with x, y, A, B free variables that is recursively defined by:

$$\psi_0 = 0$$

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

$$\vdots$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2$$

$$\psi_{2m} = \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 3$$

The polynomial ψ_n is called the n^{th} division polynomial.

48.2 Properties

- In practice, one sets $y^2 = x^3 + Ax + B$, and then $\psi_{2m+1} \in \mathbb{Z}[x, A, B]$ and $\psi_{2m} \in 2y\mathbb{Z}[x, A, B]$.
- The division polynomials form a generic elliptic divisibility sequence over the ring $\mathbb{Q}[x, y, A, B]/(y^2 - x^3 - Ax - B)$.
- If an elliptic curve E is given in the Weierstrass form $y^2 = x^3 + Ax + B$ over some field K , i.e. $A, B \in K$, one can use these values of A, B and consider the division polynomials in the coordinate ring of E . The roots of ψ_{2n+1} are the x -coordinates of the points of $E[2n + 1] \setminus \{O\}$, where $E[2n + 1]$ is the $(2n + 1)^{\text{th}}$ torsion subgroup of E . Similarly, the roots of ψ_{2n}/y are the x -coordinates of the points of $E[2n] \setminus E[2]$.
- Given a point $P = (x_P, y_P)$ on the elliptic curve $E : y^2 = x^3 + Ax + B$ over some field K , we can express the coordinates of the n$^{\text{th}}$ multiple of P in terms of division polynomials:

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right) = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2(x)}, \frac{\psi_{2n}(x,y)}{2\psi_n^4(x)}\right)$$

where ϕ_n and ω_n are defined by:

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1},$$

$$\omega_n = \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y}.$$

Using the relation between ψ_{2m} and ψ_{2m+1} , along with the equation of the curve, the functions ψ_n^2 , $\frac{\psi_{2n}}{y}$, ψ_{2n+1} and ϕ_n are all in $K[x]$.

Let $p > 3$ be prime and let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over the finite field $\mathbb{F}_p$, i.e., $A, B \in \mathbb{F}_p$. The ℓ -torsion group of E over $\bar{\mathbb{F}}_p$ is isomorphic to $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$ if $\ell \neq p$, and to $\mathbb{Z}/\ell$ or $\{0\}$ if $\ell = p$. Hence the degree of ψ_ℓ is equal to either $\frac{1}{2}(l^2 - 1)$, $\frac{1}{2}(l - 1)$, or 0.

René Schoof observed that working modulo the ℓ *th* division polynomial allows one to work with all ℓ -torsion points simultaneously. This is heavily used in Schoof's algorithm for counting points on elliptic curves.

48.3 See also

- Schoof's algorithm

48.4 References

- A. Brown: *Algorithms for Elliptic Curves over Finite Fields*, EPFL — LMA. Available at http://algo.epfl.ch/handouts/en/andrew.pdf
- A. Enge: *Elliptic Curves and their Applications to Cryptography: An Introduction*. Kluwer Academic Publishers, Dordrecht, 1999.
- N. Koblitz: *A Course in Number Theory and Cryptography*, Graduate Texts in Math. No. 114, Springer-Verlag, 1987. Second edition, 1994
- Müller : *Die Berechnung der Punktanzahl von elliptischen kurvenüber endlichen Primkörpern*. Master's Thesis. Universität des Saarlandes, Saarbrücken, 1991.
- G. Musiker: *Schoof's Algorithm for Counting Points on* $E(\mathbb{F}_q)$. Available at http://www-math.mit.edu/~{}musiker/schoof.pdf
- Schoof: *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*. Math. Comp., 44(170):483–494, 1985. Available at http://www.mat.uniroma2.it/~{}schoof/ctpts.pdf

- R. Schoof: *Counting Points on Elliptic Curves over Finite Fields*. J. Theor. Nombres Bordeaux 7:219–254, 1995. Available at http://www.mat.uniroma2.it/~{}schoof/ctg.pdf
- L. C. Washington: *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, New York, 2003.
- J. Silverman: *The Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 106, 1986.

Chapter 49

Ehrhart polynomial

In mathematics, an integral polytope has an associated **Ehrhart polynomial** that encodes the relationship between the volume of a polytope and the number of integer points the polytope contains. The theory of Ehrhart polynomials can be seen as a higher-dimensional generalization of Pick's theorem in the Euclidean plane.

These polynomials are named after Eugène Ehrhart who studied them in the 1960s.

49.1 Definition

Informally, if *P* is a polytope, and *tP* is the polytope formed by expanding *P* by a factor of *t* in each dimension, then *L*(*P*, *t*) is the number of integer lattice points in *tP*.

More formally, consider a lattice *L* in Euclidean space $\mathbf{R}^n$ and a *d*-dimensional polytope *P* in $\mathbf{R}^n$ with the property that all vertices of the polytope are points of the lattice. (A common example is $L = \mathbf{Z}^n$ and a polytope for which all vertices have integer coordinates.) For any positive integer *t*, let *tP* be the *t*-fold dilation of *P* (the polytope formed by multiplying each vertex coordinate, in a basis for the lattice, by a factor of *t*), and let

$$L(P,t) = \#(tP \cap L)$$

be the number of lattice points contained in the polytope *tP*. Ehrhart showed in 1962 that *L* is a rational polynomial of degree *d* in *t*, i.e. there exist rational numbers a_0,...,*ad* such that:

$$L(P,t) = a_d t^d + a_{d-1} t^{d-1} + \ldots + a_0$$

for all positive integers *t*.

The Ehrhart polynomial of the interior of a closed convex polytope *P* can be computed as:

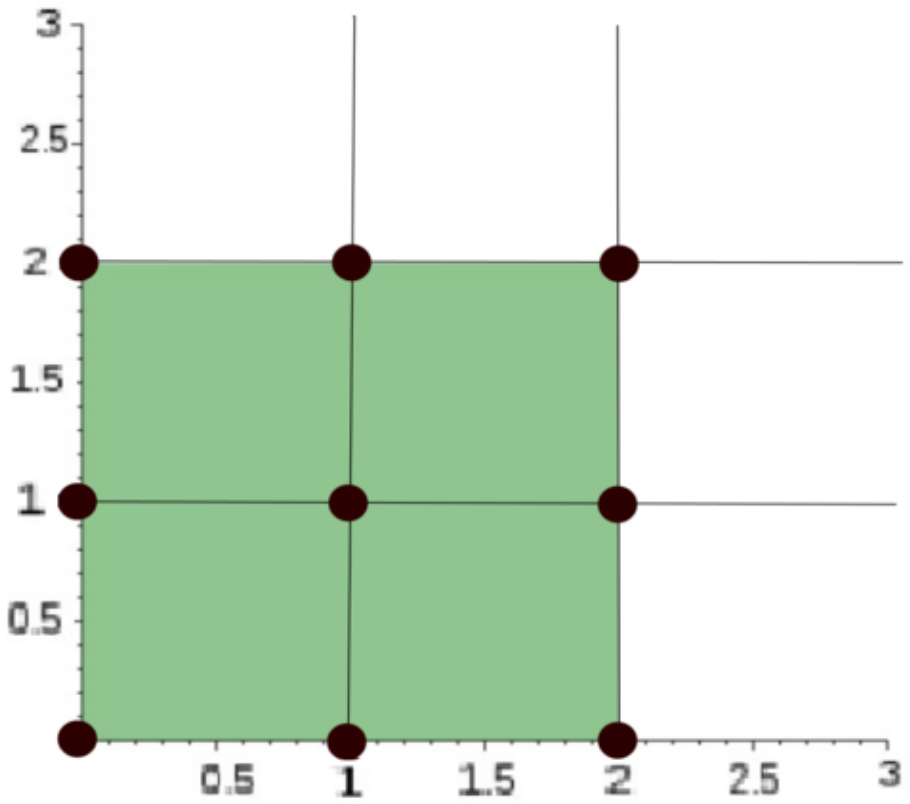
$$L(\text{int}(P),t) = (-1)^d L(P,-t),$$

where *d* is the dimension of *P*. This result is known as Ehrhart-Macdonald reciprocity.[1]

49.2 Examples of Ehrhart Polynomials

Let *P* be a *d*-dimensional unit hypercube whose vertices are the integer lattice points all of whose coordinates are 0 or 1. In terms of inequalities,

$$P = \{x \in \mathbb{Q}^d : 0 \leq x_i \leq 1; 1 \leq i \leq d\}$$



This is the second dilate, t = 2*, of a unit square. It has nine integer points.*

Then the *t*-fold dilation of P is a cube with side length t, containing $(t + 1)^d$ integer points. That is, the Ehrhart polynomial of the hypercube is $L(P,t) = (t + 1)^d$.[2][3] Additionally, if we evaluate *L(P, t)* at negative integers, then

$$L(P, -t) = (-1)^d(t - 1)^d = (-1)^d L(\text{int}(P), t),$$

as we would expect from Ehrhart-Macdonald reciprocity.

Many other figurate numbers can be expressed as Ehrhart polynomials. For instance, the square pyramidal numbers are given by the Ehrhart polynomials of a square pyramid with an integer unit square as its base and with height one; the Ehrhart polynomial in this case is $(t + 1)(t + 2)(2t + 3)/6$.[4]

49.3 Ehrhart Quasi-Polynomials

Let P be a rational polytope. In other words, suppose

$$P = \{x \in \mathbb{Q}^d : Ax \leq b\}$$

where $A \in \mathbb{R}^{k\times d}$ and $b \in \mathbb{Z}^k$. (Equivalently, P is the convex hull of finitely many points in $\mathbb{Q}^d$.) Then define

$$L(P, t) = \#(\{x \in \mathbb{Z}^n : Ax \leq tb\}).$$

In this case, *L(P, t)* is a quasi-polynomial in *t*. Just as with integral polytopes, Ehrhart-Macdonald reciprocity holds, that is,

$$L(\text{int}(P), t) = (-1)^n L(P, -t).$$

49.4 Examples of Ehrhart Quasi-Polynomials

Let *P* be a polygon with vertices *(0,0)*, *(0,2)*, *(1,1)* and *(0,3/2)*. The number of integer points in *tP* will be counted by the quasi-polynomial [5]

$L(P,t) = \frac{7}{4}t^2 + \frac{5}{2}t + \frac{7+(-1)^t}{8}$.

49.5 Interpretation of coefficients

If *P* is closed (i.e. the boundary faces belong to *P*), some of the coefficients of *L*(*P*, *t*) have an easy interpretation:

- the leading coefficient, ad, is equal to the d-dimensional volume of *P*, divided by $d(L)$ (see lattice for an explanation of the content or covolume $d(L)$ of a lattice);
- the second coefficient, ad_{-1}, can be computed as follows: the lattice *L* induces a lattice *LF* on any face *F* of *P*; take the $(d-1)$-dimensional volume of *F*, divide by $2d(LF)$, and add those numbers for all faces of *P*;
- the constant coefficient a_0 is the Euler characteristic of *P*. When *P* is a closed convex polytope, $a_0 = 1$.

49.6 Ehrhart Series

We can define a generating function for the Ehrhart polynomial of an integral n-dimensional polytope *P* as

$Ehr_P(z) = \sum_{t\geq 0} L(P,t)z^t$.

This series can be expressed as a rational function. Specifically, Ehrhart proved (1962) that there exist complex numbers h_i^* , $0 \leq j \leq n$, such that the Ehrhart series of *P* is

$Ehr_P(z) = \frac{\sum_{j=0}^{d} h_j^* z^j}{(1-z)^{n+1}}$,

with $\sum_{j=0}^{d} h_j^* \neq 0$. Additionally, Stanley's non-negativity theorem states that under the given hypotheses, h_i^* will be non-negative integers, for $0 \leq j \leq n$.

Another result by Stanley shows that if *P* is a lattice polytope contained in *Q*, then $h^*_i(P) \leq h^*_i(Q)$ for all *i*.

The h^*-vector is in general not unimodal, but it is whenever it is symmetric, and the polytope has a regular unimodal triangulation.[6]

49.6.1 Ehrhart series for rational polytopes

Similar to the case of polytopes with integer vertices, one defines the Ehrhart series for a rational polytope. For a rational polytope *P*, where *d* is the smallest integer such that *dP* is an integer polytope, (*d* is called the denominator of *P*), then one has

$$Ehr_P(z) = \sum_{t\geq 0} L(P,t)z^t = \frac{\sum_{j=0}^{d(n+1)} h_j^* z^j}{(1-z^d)^{n+1}},$$

where the h^*_i are still non-negative integers. [7] [8]

49.7 Toric Variety

The case $n = d = 2$ and $t = 1$ of these statements yields Pick's theorem. Formulas for the other coefficients are much harder to get; Todd classes of toric varieties, the Riemann–Roch theorem as well as Fourier analysis have been used for this purpose.

If X is the toric variety corresponding to the normal fan of P, then P defines an ample line bundle on X, and the Ehrhart polynomial of P coincides with the Hilbert polynomial of this line bundle.

Ehrhart polynomials can be studied for their own sake. For instance, one could ask questions related to the roots of an Ehrhart polynomial.[9] Furthermore, some authors have pursued the question of how these polynomials could be classified.[10]

49.8 Generalizations

It is possible to study the number of integer points in a polytope P if we dilate some facets of P but not others. In other words, one would like to know the number of integer points in semi-dilated polytopes. It turns out that such a counting function will be what is called a multivariate quasi-polynomial. An Ehrhart-type reciprocity theorem will also hold for such a counting function.[11]

Counting the number of integer points in semi-dilations of polytopes has applications [12] in enumerating the number of different dissections of regular polygons and the number of non-isomorphic unrestricted codes, a particular kind of code in the field of coding theory.

49.9 See also

- Quasi-polynomial

49.10 Notes

[1] Macdonald, Ian G (1971). "Polynomials Associated with Finite Cell-Complexes" (PDF). *Journal of the London Mathematical Society* **2** (1): 181–192. doi:10.1112/jlms/s2-4.1.181.

[2] De Loera, Rambau & Santos (2010)

[3] Mathar (2010)

[4] Beck et al. (2005).

[5] Beck, Matthias; Robins, Sinai (2007). *Computing the Continuous Discretely*. New York: Springer. pp. 46–47.

[6] Athanasiadis, Christos A. (2004). "h*-Vectors, Eulerian Polynomials and Stable Polytopes of Graphs". *Electronic Journal of Combinatorics* **11** (2).

[7] Stanley, Richard P. (1980). "Decompositions of rational convex polytopes". *Ann. Discrete Math.* **6**: 333–342. doi:10.1016/s0167-5060(08)70717-9.

[8] Beck, Matthias; Sottile, Frank (January 2007). "Irrational proofs for three theorems of Stanley". *European Journal of Combinatorics* **28** (1): 403–409. doi:10.1016/j.ejc.2005.06.003.

[9] Braun, Benjamin; Develin, Mike (2008). "Ehrhart Polynomial Roots and Stanley's Non-Negativity Theorem". *American Mathematical Society*. Contemporary Mathematics **452**: 67–78. doi:10.1090/conm/452/08773.

[10] Higashitani, Akihiro (2012). "Classification of Ehrhart Polynomials of Integral Simplices" (PDF). *DMTCS Proceedings*: 587–594.

[11] Beck, Matthias (January 2002). "Multidimensional Ehrhart reciprocity". *Journal of Combinatorial Theory*. Series A **97** (1): 187–194. doi:10.1006/jcta.2001.3220.

[12] Lisonek, Petr (2007). "Combinatorial Families Enumerated by Quasi-polynomials". *Journal of Combinatorial Theory*. Series A **114** (4): 619–630. doi:10.1016/j.jcta.2006.06.013.

49.11 References

- Beck, M.; De Loera, J. A.; Develin, M.; Pfeifle, J.; Stanley, R. P. (2005), "Coefficients and roots of Ehrhart polynomials", *Integer points in polyhedra—geometry, number theory, algebra, optimization*, Contemp. Math. **374**, Providence, RI: Amer. Math. Soc., pp. 15–36, MR 2134759.
- Beck, Matthias; Robins, Sinai (2007), *Computing the Continuous Discretely, Integer-point enumeration in polyhedra*, Undergraduate Texts in Mathematics, New York: Springer-Verlag, ISBN 978-0-387-29139-0, MR 2271992.
- De Loera, Jesús A.; Rambau, Jörg; Santos, Francisco (2010), "9.3.3 Ehrhart polynomials and unimodular triangulations", *Triangulations: Structures for Algorithms and Applications*, Algorithms and Computation in Mathematics **25**, Springer, p. 475, ISBN 978-3-642-12970-4.
- Diaz, Ricardo; Robins, Sinai (1996), "The Ehrhart polynomial of a lattice *n*-simplex", *Electronic Research Announcements of the American Mathematical Society* **2**: 1–6, doi:10.1090/S1079-6762-96-00001-7. Introduces the Fourier analysis approach and gives references to other related articles.
- Ehrhart, Eugène (1962), "Sur les polyèdres rationnels homothétiques à *n* dimensions", *C. R. Acad. Sci. Paris* **254**: 616–618. Definition and first properties.
- Mathar, Richard J. (2010), *Point counts of Dk and some Ak and Ek integer lattices inside hypercubes*, arXiv:1002.3844
- Mustaţă, Mircea (February 2005), "Chapter 13: Ehrhart polynomials", *Lecture notes on toric varieties*.

Chapter 50

Eisenstein's criterion

In mathematics, **Eisenstein's criterion** gives a sufficient condition for a polynomial with integer coefficients to be irreducible over the rational numbers—that is, for it to be unfactorable into the product of non-constant polynomials with rational coefficients. The result is also known as the **Schönemann–Eisenstein theorem**; although this name is rarely used nowadays, it was common in the early 20th century.[1][2]

Suppose we have the following polynomial with integer coefficients.

$$Q = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

If there exists a prime number p such that the following three conditions all apply:

- p divides each *ai* for $i \neq n$,
- p does *not* divide *an*, and
- p^2 does *not* divide a_0,

then Q is irreducible over the rational numbers. It will also be irreducible over the integers, unless all its coefficients have a nontrivial factor in common (in which case Q as integer polynomial will have some prime number, necessarily distinct from p, as an irreducible factor). The latter possibility can be avoided by first making Q primitive, by dividing it by the greatest common divisor of its coefficients (the content of Q). This division does not change whether Q is reducible or not over the rational numbers (see Primitive part–content factorization for details), and will not invalidate the hypotheses of the criterion for p (on the contrary it could make the criterion hold for some prime, even if it did not before the division).

This criterion is certainly not applicable to all polynomials with integer coefficients that are irreducible over the rational numbers, but does allow in certain important particular cases to prove irreducibility with very little effort. In some cases the criterion does not apply directly (for any prime number), but it does apply after transformation of the polynomial, in such a way that irreducibility of the original polynomial can be concluded.

50.1 Examples

Consider the polynomial $Q = 3x^4 + 15x^2 + 10$. In order for Eisenstein's criterion to apply for a prime number p it must divide both non-leading coefficients 15 and 10, which means only $p = 5$ could work, and indeed it does since 5 does not divide the leading coefficient 3, and its square 25 does not divide the constant coefficient 10. One may therefore conclude that Q is irreducible over **Q** (and since it is primitive, over **Z** as well). Note that since Q is of degree 4, this conclusion could not have been established by only checking that Q has no rational roots (which eliminates possible factors of degree 1), since a decomposition into two quadratic factors could also be possible.

Often Eisenstein's criterion does not apply for any prime number. It may however be that it applies (for some prime number) to the polynomial obtained after substitution (for some integer a) of $x + a$ for x; the fact that the polynomial

after substitution is irreducible then allows concluding that the original polynomial is as well. This procedure is known as applying a *shift*.

For example consider $H = x^2 + x + 2$, in which the coefficient 1 of x is not divisible by any prime, Eisenstein's criterion does not apply to H. But if one substitutes $x + 3$ for x in H, one obtains the polynomial $x^2 + 7x + 14$, which satisfies Eisenstein's criterion for the prime number 7. Since the substitution is an automorphism of the ring $\mathbf{Q}[x]$, the fact that we obtain an irreducible polynomial after substitution implies that we had an irreducible polynomial originally. In this particular example it would have been simpler to argue that H (being monic of degree 2) could only be reducible if it had an integer root, which it obviously does not; however the general principle of trying substitutions in order to make Eisenstein's criterion apply is a useful way to broaden its scope.

Another possibility to transform a polynomial so as to satisfy the criterion, which may be combined with applying a shift, is reversing the order of its coefficients, provided its constant term is nonzero (without which it would be divisible by x anyway). This is so because such polynomials are reducible in $R[x]$ if and only if they are reducible in $R[x, x^{-1}]$ (for any integral domain R), and in that ring the substitution of x^{-1} for x reverses the order of the coefficients (in a manner symmetric about the constant coefficient, but a following shift in the exponent amounts to multiplication by a unit). As an example $2x^5 - 4x^2 - 3$ satisfies the criterion for $p = 2$ after reversing its coefficients, and (being primitive) is therefore irreducible in $\mathbf{Z}[x]$.

50.1.1 Cyclotomic polynomials

An important class of polynomials whose irreducibility can be established using Eisenstein's criterion is that of the cyclotomic polynomials for prime numbers p. Such a polynomial is obtained by dividing the polynomial $x^p - 1$ by the linear factor $x - 1$, corresponding to its obvious root 1 (which is its only rational root if $p > 2$):

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Here, as in the earlier example of H, the coefficients 1 prevent Eisenstein's criterion from applying directly. However the polynomial will satisfy the criterion for p after substitution of $x + 1$ for x: this gives

$$\frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1},$$

all of whose non-leading coefficients are divisible by p by properties of binomial coefficients, and whose constant coefficient equal to p, and therefore not divisible by p^2. An alternative way to arrive at this conclusion is to use the identity $(a + b)^p = a^p + b^p$ which is valid in characteristic p (and which is based on the same properties of binomial coefficients, and gives rise to the Frobenius endomorphism), to compute the reduction modulo p of the quotient of polynomials:

$$\frac{(x+1)^p - 1}{x} \equiv \frac{x^p + 1^p - 1}{x} = \frac{x^p}{x} = x^{p-1} \pmod{p},$$

which means that the non-leading coefficients of the quotient are all divisible by p; the remaining verification that the constant term of the quotient is p can be done by substituting 1 (instead of $x + 1$) for x into the expanded form $x^{p-1} + \ldots + x + 1$.

50.2 History

The criterion is named after Gotthold Eisenstein. However, Theodor Schönemann was the first to publish a version of the criterion,[1] in 1846 in Crelle's Journal,[3] which reads in translation

> That $(x - a)^n + pF(x)$ will be irreducible to the modulus p^2 when $F(x)$ to the modulus p does not contain a factor $x-a$.

This formulation already incorporates a shift to a in place of 0; the condition on $F(x)$ means that $F(a)$ is not divisible by p, and so $pF(a)$ is divisible by p but not by p^2. As stated it is not entirely correct in that it makes no assumptions on the degree of the polynomial $F(x)$, so that the polynomial considered need not be of the degree n that its expression suggests; the example $x^2 + p(x^3 + 1) \equiv (x^2 + p)(px + 1) \bmod p^2$, shows the conclusion is not valid without such hypothesis. Assuming that the degree of $F(x)$ does not exceed n, the criterion is correct however, and somewhat stronger than the formulation given above, since if $(x - a)^n + pF(x)$ is irreducible modulo p^2, it certainly cannot decompose in $\mathbf{Z}[x]$ into non-constant factors.

Subsequently Eisenstein published a somewhat different version in 1850, also in Crelle's Journal.[4] This version reads in translation

> When in a polynomial $F(x)$ in x of arbitrary degree the coefficient of the highest term is 1, and all following coefficients are whole (real, complex) numbers, into which a certain (real resp. complex) prime number m divides, and when furthermore the last coefficient is equal to εm, where ε denotes a number not divisible by m: then it is impossible to bring $F(x)$ into the form
>
> $$\left(x^\mu + a_1 x^{\mu-1} + \cdots + a_\mu\right)\left(x^\nu + b_1 x^{\nu-1} + \cdots + b_\nu\right)$$
>
> where $\mu, \nu \geq 1, \mu + \nu = \deg(F(x))$, and all a and b are *whole* (real resp. complex) numbers; the equation $F(x) = 0$ is therefore irreducible.

Here "whole real numbers" are ordinary integers and "whole complex numbers" are Gaussian integers; one should similarly interpret "real and complex prime numbers". The application for which Eisenstein developed his criterion was establishing the irreducibility of certain polynomials with coefficients in the Gaussian integers that arise in the study of the division of the lemniscate into pieces of equal arc-length.

Remarkably Schönemann and Eisenstein, once having formulated their respective criteria for irreducibility, both immediately apply it to give an elementary proof of the irreducibility of the cyclotomic polynomials for prime numbers, a result that Gauss had obtained in his *Disquisitiones Arithmeticae* with a much more complicated proof. In fact, Eisenstein adds in a footnote that the only proof for this irreducibility known to him, other than that of Gauss, is one given by Kronecker in 1845. This shows that he was unaware of *two* different proofs of this statement that Schönemann had given, one in either part of a two-part article, the second of which being the one based on the criterion cited above; this is all the more surprising given the fact that two pages further Eisenstein actually refers (for a different matter) to the first part of Schönemann's article. In a note ("Notiz") that appeared in the following issue of the Journal,[5] Schönemann points this out to Eisenstein, and indicates that the latter's method is not essentially different from the one he used in the second proof.

50.3 Basic proof

To prove the validity of the criterion, suppose Q satisfies the criterion for the prime number p, but that it is nevertheless reducible in $\mathbf{Q}[x]$, from which we wish to obtain a contradiction. From Gauss' lemma it follows that Q is reducible in $\mathbf{Z}[x]$ as well, and in fact can be written as the product $Q = GH$ of two non-constant polynomials G, H (in case Q is not primitive, one applies the lemma to the primitive polynomial Q/c (where the integer c is the content of Q) to obtain a decomposition for it, and multiplies c into one of the factors to obtain a decomposition for Q). Now reduce $Q = GH$ modulo p to obtain a decomposition in $(\mathbf{Z}/p\mathbf{Z})[x]$. But by hypothesis this reduction for Q leaves its leading term, of the form ax^n for a non-zero constant $a \in \mathbf{Z}/p\mathbf{Z}$, as the only nonzero term. But then necessarily the reductions modulo p of G and H also make all non-leading terms vanish (and cannot make their leading terms vanish), since no other decompositions of ax^n are possible in $(\mathbf{Z}/p\mathbf{Z})[x]$, which is a unique factorization domain. In particular the constant terms of G and H vanish in the reduction, so they are divisible by p, but then the constant term of Q, which is their product, is divisible by p^2, contrary to the hypothesis, and one has a contradiction.

50.4 Advanced explanation

Applying the theory of the Newton polygon for the p-adic number field, for an Eisenstein polynomial, we are supposed to take the lower convex envelope of the points

$$(0, 1), (1, v_1), (2, v_2), \ldots, (n - 1, vn_{-1}), (n, 0),$$

where *vi* is the p-adic valuation of *ai* (i.e. the highest power of p dividing it). Now the data we are given on the *vi* for $0 < i < n$, namely that they are at least one, is just what we need to conclude that the lower convex envelope is exactly the single line segment from (0, 1) to (n, 0), the slope being $-1/n$.

This tells us that each root of Q has p-adic valuation $1/n$ and hence that Q is irreducible over the p-adic field (since, for instance, no product of any proper subset of the roots has integer valuation); and *a fortiori* over the rational number field.

This argument is much more complicated than the direct argument by reduction mod p. It does however allow one to see, in terms of algebraic number theory, how frequently Eisenstein's criterion might apply, after some change of variable; and so limit severely the possible choices of p with respect to which the polynomial could have an Eisenstein translate (that is, become Eisenstein after an additive change of variables as in the case of the p-th cyclotomic polynomial).

In fact only primes p ramifying in the extension of **Q** generated by a root of Q have any chance of working. These can be found in terms of the discriminant of Q. For example, in the case $x^2 + x + 2$ given above, the discriminant is -7 so that 7 is the only prime that has a chance of making it satisfy the criterion. Modulo 7, it becomes $(x - 3)^2$—a repeated root is inevitable, since the discriminant is 0 mod 7. Therefore the variable shift is actually something predictable.

Again, for the cyclotomic polynomial, it becomes

$$(x - 1)^{p-1} \bmod p;$$

the discriminant can be shown to be (up to sign) p^{p-2}, by linear algebra methods.

More precisely, only totally ramified primes have a chance of being Eisenstein primes for the polynomial. (In quadratic fields, ramification is always total, so the distinction is not seen in the quadratic case like $x^2 + x + 2$ above.) In fact, Eisenstein polynomials are directly linked to totally ramified primes, as follows: if a field extension of the rationals is generated by the root of a polynomial that is Eisenstein at p then p is totally ramified in the extension, and conversely if p is totally ramified in a number field then the field is generated by the root of an Eisenstein polynomial at p.

50.5 Generalization

Given an integral domain D, let

$$Q = \sum_{i=0}^{n} a_i x^i$$

be an element of $D[x]$, the polynomial ring with coefficients in D.

Suppose there exists a prime ideal **p** of D such that

- $ai \in \mathbf{p}$ for each $i \neq n$,
- $an \notin \mathbf{p}$, and
- $a_0 \notin \mathbf{p}^2$, where $\mathbf{p}^2$ is the ideal product of **p** with itself.

Then Q cannot be written as a product of two non-constant polynomials in $D[x]$. If in addition Q is primitive (i.e., it has no non-trivial *constant* divisors), then it is irreducible in $D[x]$. If D is a unique factorization domain with field of fractions F, then by Gauss's lemma Q is irreducible in $F[x]$, whether or not it is primitive (since constant factors are invertible in $F[x]$); in this case a possible choice of prime ideal is the principal ideal generated by any irreducible element of D. The latter statement gives original theorem for $D = \mathbf{Z}$ or (in Eisenstein's formulation) for $D = \mathbf{Z}[i]$.

The proof of this generalization is similar to the one for the original statement, considering the reduction of the coefficients modulo **p**; the essential point is that a single-term polynomial over the integral domain $D/\mathbf{p}$ cannot decompose as a product in which at least one of the factors has more than one term (because in such a product there can be no cancellation in the coefficient either of the highest or the lowest possible degree).

50.5.1 Example

After **Z**, one of the basic examples of an integral domain is the polynomial ring $D = k[u]$ in the variable u over the field k. In this case, the principal ideal generated by u is a prime ideal. Eisenstein's criterion can then be used to prove the irreducibility of a polynomial such as $Q(x) = x^3 + ux + u$ in $D[x]$. Indeed, u does not divide a_3, u^2 does not divide a_0, and u divides a_0, a_1 and a_2. This shows that this polynomial satisfies the hypotheses of the generalization of Eisenstein's criterion for the prime ideal $\mathbf{p} = (u)$ since, for a principal ideal (u), being an element of (u) is equivalent to being divisible by u.

50.6 See also

- Cohn's irreducibility criterion

50.7 References

[1] David A. Cox, *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, American Mathematical Monthly* ***118*** *Vol 1, January 2011, pp. 3–31.*

[2] H. L. Dorwart, Irreducibility of polynomials, American Mathematical Monthly **42** Vol 6 (1935), 369–381, doi:10.2307/2301357.

[3] Dr. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, Journal für die reine und angewandte Mathematik **32**, pp. 93–118. The criterion is formulated on p. 100

[4] G. Eisenstein *Über die Irredicibilität une einige andere Eigenschaften der Gleichung von welche der Theilung der ganzen Lemniscate abhängt*, Journal für die reine und angewandte Mathematik **39**, pp. 160–179. The criterion is formulated on p. 166

[5] Dr. Schönemann, *Über einige von Herrn Dr. Eisenstein aufgestellte Lehrsätze, irreductible Congruenzen betreffend (S.182 Bd. 39 dieses Journals)*, Journal für die reine und angewandte Mathematik **40**, p. 185–188. The Notiz is on page 188.

- D.J.H. Garling, *A Course in Galois Theory*, Cambridge University Press, (1986), ISBN 0-521-31249-3.
- Hazewinkel, Michiel, ed. (2001), "Algebraic equation", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4

Chapter 51

Equally spaced polynomial

An **equally spaced polynomial** (ESP) is a polynomial used in finite fields, specifically GF(2) (binary). An s-ESP of degree *sm* can be written as:

$$ESP(x) = \sum_{i=0}^{m} x^{si} \text{ for } i = 0, 1, \ldots, m$$

or

$$ESP(x) = x^{sm} + x^{s(m-1)} + \cdots + x^s + 1.$$

51.1 Properties

Over GF(2) the ESP has many interesting properties, including:

- The Hamming weight of the ESP is $m + 1$.

A 1-ESP is known as an all one polynomial and has additional properties including the above.

51.2 References

Chapter 52

Equioscillation theorem

The **equioscillation theorem** concerns the approximation of continuous functions using polynomials when the merit function is the maximum difference (uniform norm). Its discovery is attributed to Chebyshev.

52.1 Statement

Let f be a continuous function from $[a, b]$ to $\mathbf{R}$. Among all the polynomials of degree $\leq n$, the polynomial g minimizes the uniform norm of the difference $||f - g||_\infty$ if and only if there are $n + 2$ points $a \leq x_0 < x_1 < \cdots < x_{n+1} \leq b$ such that $f(x_i) - g(x_i) = \sigma(-1)^i ||f - g||_\infty$ where $\sigma = \pm 1$.

52.2 Algorithms

Several minimax approximation algorithms are available, the most common being the Remez algorithm.

52.3 References

- Notes on how to prove Chebyshev's equioscillation theorem at the Wayback Machine (archived July 2, 2011)
- The Chebyshev Equioscillation Theorem by Robert Mayans

Chapter 53

Exponential polynomial

This article is about polynomials in variables and exponential functions. For the polynomials involving Stirling numbers, see Touchard polynomials.

In mathematics, **exponential polynomials** are functions on fields, rings, or abelian groups that take the form of polynomials in a variable and an exponential function.

53.1 Definition

53.1.1 In fields

An exponential polynomial generally has both a variable x and some kind of exponential function $E(x)$. In the complex numbers there is already a canonical exponential function, the function that maps x to e^x. In this setting the term exponential polynomial is often used to mean polynomials of the form $P(x,e^x)$ where $P \in \mathbf{C}[x,y]$ is a polynomial in two variables.[1][2]

There is nothing particularly special about $\mathbf{C}$ here, exponential polynomials may also refer to such a polynomial on any exponential field or exponential ring with its exponential function taking the place of e^x above.[3] Similarly, there is no reason to have one variable, and an exponential polynomial in n variables would be of the form $P(x_1,...,xn,e^{x_1},...,e^{xn})$, where P is a polynomial in $2n$ variables.

For formal exponential polynomials over a field K we proceed as follows.[4] Let W be a finitely generated $\mathbf{Z}$-submodule of K and consider finite sums of the form

$$\sum_{i=1}^{m} f_i(X)\exp(w_i X)\ ,$$

where the fi are polynomials in $K[X]$ and the $\exp(wiX)$ are formal symbols indexed by wi in W subject to $\exp(u+v) = \exp(u)\exp(v)$.

53.1.2 In abelian groups

A more general framework where the term exponential polynomial may be found is that of exponential functions on abelian groups. Similarly to how exponential functions on exponential fields are defined, given a topological abelian group G a homomorphism from G to the additive group of the complex numbers is called an additive function, and a homomorphism to the multiplicative group of nonzero complex numbers is called an exponential function, or simply an exponential. A product of additive functions and exponentials is called an exponential monomial, and a linear combination of these is then an exponential polynomial on G.[5][6]

53.2 Properties

Ritt's theorem states that the analogues of unique factorization and the factor theorem hold for the ring of exponential polynomials.[4]

53.3 Applications

Exponential polynomials on **R** and **C** often appear in transcendence theory, where they appear as auxiliary functions in proofs involving the exponential function. They also act as a link between model theory and analytic geometry. If one defines an exponential variety to be the set of points in $\mathbf{R}^n$ where some finite collection of exponential polynomials vanish, then results like Khovanskiĭ's theorem in differential geometry and Wilkie's theorem in model theory show that these varieties are well-behaved in the sense that the collection of such varieties is stable under the various set-theoretic operations as long as one allows the inclusion of the image under projections of higher-dimensional exponential varieties. Indeed, the two aforementioned theorems imply that the set of all exponential varieties forms an o-minimal structure over **R**.

53.4 Notes

[1] C. J. Moreno, *The zeros of exponential polynomials*, Compositio Mathematica 26 (1973), pp.69–78.

[2] M. Waldschmidt, *Diophantine approximation on linear algebraic groups*, Springer, 2000.

[3] Martin Bays, Jonathan Kirby, A.J. Wilkie, *A Schanuel property for exponentially transcendental powers*, (2008), arXiv: 0810.4457v1

[4] Everest, Graham; van der Poorten, Alf; Shparlinski, Igor; Ward, Thomas (2003). *Recurrence sequences*. Mathematical Surveys and Monographs **104**. Providence, RI: American Mathematical Society. p. 140. ISBN 0-8218-3387-1. Zbl 1033.11006.

[5] László Székelyhidi, *On the extension ofexponential polynomials*, Mathematica Bohemica **125** (2000), pp.365–370.

[6] P. G. Laird, *On characterizations of exponential polynomials*, Pacific Journal of Mathematics **80** (1979), pp.503–507.

Chapter 54

External ray

An external ray is a curve that runs from infinity toward a Julia or Mandelbrot set.[1] This curve is only sometimes a half-line (ray) but is called ray because it is an image of a ray.

External rays are used in complex analysis, particularly in complex dynamics and geometric function theory.

54.1 History

External rays were introduced in Douady and Hubbard's study of the Mandelbrot set

54.2 Notation

External rays of (connected) Julia sets on dynamical plane are often called **dynamic rays**.

External rays of the Mandelbrot set (and similar one-dimensional connectedness loci) on parameter plane are called **parameter rays**.

54.3 Polynomials

54.3.1 Dynamical plane = z-plane

External rays are associated to a compact, full, connected subset K of the complex plane as :

- the images of radial rays under the Riemann map of the complement of K
- the gradient lines of the Green's function of K
- field lines of Douady-Hubbard potential
- an integral curve of the gradient vector field of the Green's function on neighborhood of infinity[2]

External rays together with equipotential lines of Douady-Hubbard potential (level sets) form a new polar coordinate system for exterior (complement) of K .

In other words the external rays define vertical foliation which is orthogonal to horizontal foliation defined by the level sets of potential.[3]

Uniformization

Let Ψ_c be the mapping from the complement (exterior) of the closed unit disk $\overline{\mathbb{D}}$ to the complement of the filled Julia set Kc .

$\Psi_c : \hat{\mathbb{C}} \setminus \overline{\mathbb{D}} \to \hat{\mathbb{C}} \setminus Kc$

and **Boettcher map**[4](function) Φ_c , which is uniformizing map of basin of attraction of infinity, because it conjugates complement of the filled Julia set Kc and the complement (exterior) of the closed unit disk

$\Phi_c : \hat{\mathbb{C}} \setminus Kc \to \hat{\mathbb{C}} \setminus \overline{\mathbb{D}}$

where :

$\hat{\mathbb{C}}$ denotes the extended complex plane

Boettcher map Φ_c is an isomorphism :

$\Psi_c = \Phi_c^{-1}$

$w = \Phi_c(z) = \lim_{n\to\infty}(f_c^n(z))^{2^{-n}}$

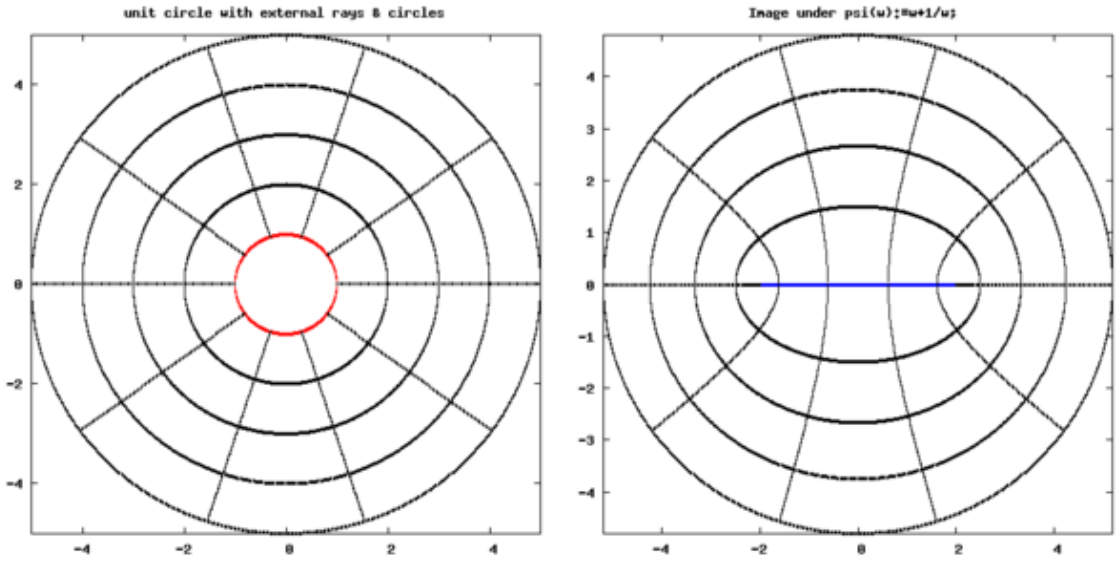
where :

$z \in \hat{\mathbb{C}} \setminus K_c$

$w \in \hat{\mathbb{C}} \setminus \overline{\mathbb{D}}$

w is a **Boettcher coordinate**

Formal definition of dynamic ray



polar coordinate system and Psi_c for c=−2

The **external ray** of angle θ noted as $\mathcal{R}_\theta^K$ is:

- the image under Ψ_c of straight lines $\mathcal{R}_\theta = \{\left(r * e^{2\pi i\theta}\right) : r > 1\}$

$\mathcal{R}_\theta^K = \Psi_c(\mathcal{R}_\theta)$

- set of points of exterior of filled-in Julia set with the same external angle θ

$\mathcal{R}_\theta^K = \{z \in \hat{\mathbb{C}} \setminus Kc : \arg(\Phi_c(z)) = \theta\}$

Properities

External ray for periodic angle θ satisfies :

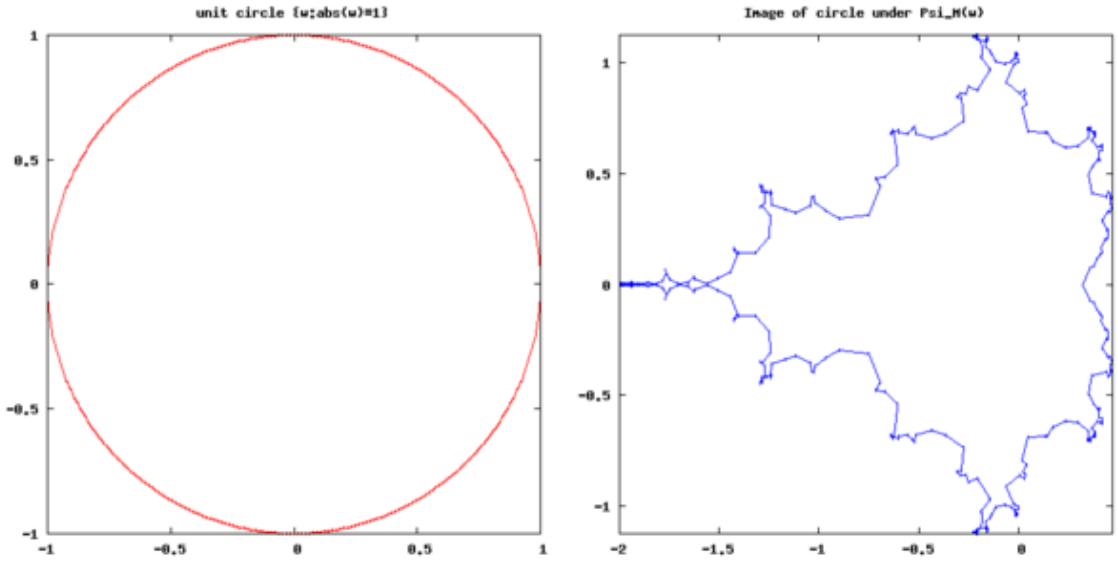
$$f(\mathcal{R}_\theta^K) = \mathcal{R}_{2\theta}^K$$

and its landing point $\gamma_f(\theta))$:[5]

$$f(\gamma_f(\theta)) = \gamma_f(2\theta)$$

54.3.2 Parameter plane = c-plane

Uniformization



Boundary of Mandelbrot set as an image of unit circle under Ψ_M

Let Ψ_M be the mapping from the complement (exterior) of the closed unit disk $\overline{\mathbb{D}}$ to the complement of the Mandelbrot set M .

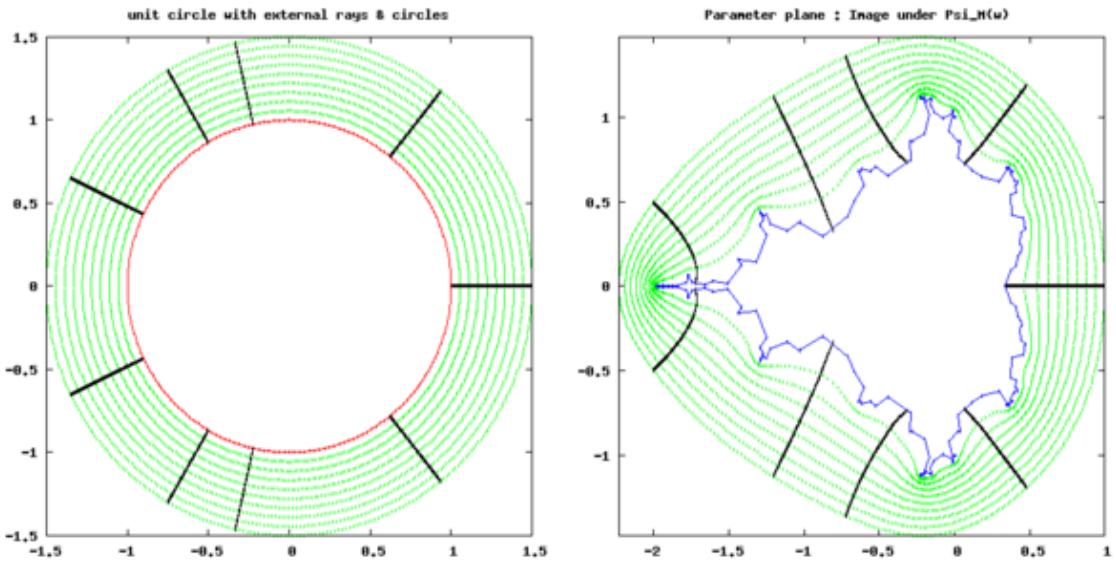
$$\Psi_M : \hat{\mathbb{C}} \setminus \overline{\mathbb{D}} \to \hat{\mathbb{C}} \setminus M$$

and Boettcher map (function) Φ_M , which is uniformizing map[6] of complement of Mandelbrot set, because it conjugates complement of the Mandelbrot set M and the complement (exterior) of the closed unit disk

$$\Phi_M : \hat{\mathbb{C}} \setminus M \to \hat{\mathbb{C}} \setminus \overline{\mathbb{D}}$$

it can be normalized so that :
$\frac{\Phi_M(c)}{c} \to 1 \; as \; c \to \infty$ [7]
where :

$\hat{\mathbb{C}}$ denotes the extended complex plane



Uniformization of complement (exterior) of Mandelbrot set

Jungreis function Ψ_M is the inverse of uniformizing map :

$\Psi_M = \Phi_M^{-1}$

In the case of complex quadratic polynomial one can compute this map using Laurent series about infinity[8][9]

$$c = \Psi_M(w) = w + \sum_{m=0}^{\infty} b_m w^{-m} = w - \frac{1}{2} + \frac{1}{8w} - \frac{1}{4w^2} + \frac{15}{128w^3} + ...$$

where

$c \in \hat{\mathbb{C}} \setminus M$

$w \in \hat{\mathbb{C}} \setminus \overline{\mathbb{D}}$

Formal definition of parameter ray

The **external ray** of angle θ is:

- the image under Ψ_c of straight lines $\mathcal{R}_\theta = \{\left(r * e^{2\pi i\theta}\right) : r > 1\}$

$\mathcal{R}_\theta^M = \Psi_M(\mathcal{R}_\theta)$

- set of points of exterior of Mandelbrot set with the same external angle θ [10]

$\mathcal{R}_\theta^M = \{c \in \hat{\mathbb{C}} \setminus M : \arg(\Phi_M(c)) = \theta\}$

Definition of Φ_M

Douady and Hubbard define:

$\Phi_M(c) \stackrel{\text{def}}{=} \Phi_c(z = c)$

so external angle of point c of parameter plane is equal to external angle of point $z = c$ of dynamical plane

54.3.3 External angle

Angle θ is named **external angle** (argument).[11]

Principal value of external angles are measured in turns modulo 1

1 turn = 360 degrees = 2 * Pi radians

Compare different types of angles :

- external (point of set's exterior)
- internal (point of component's interior)
- plain (argument of complex number)

54.3.4 Computation of external argument

- argument of Böttcher coordinate as an external argument[12]
  - $arg_M(c) = arg(\Phi_M(c))$
  - $arg_c(z) = arg(\Phi_c(z))$
- kneading sequence as a binary expansion of external argument[13][14][15]

54.4 Transcendental maps

For transcendental maps (for example exponential) infinity is not a fixed point but an essential singularity and there is no Boettcher isomorphism.[16][17]

Here dynamic ray is defined as a curve :

- connecting a point in an escaping set and infinity
- lying in an escaping set

54.5 Images

54.5.1 Dynamic rays

- Julia set for with 2 external ray landing on repelling fixed point alpha
- Julia set and 3 external rays landing on fixed point
- Dynamic external rays landing on repelling period 3 cycle and 3 internal rays landing on fixed point
- Julia set with external rays landing on period 3 orbit
- Play media

  Rays landing on parabolic fixed point for periods 2-40

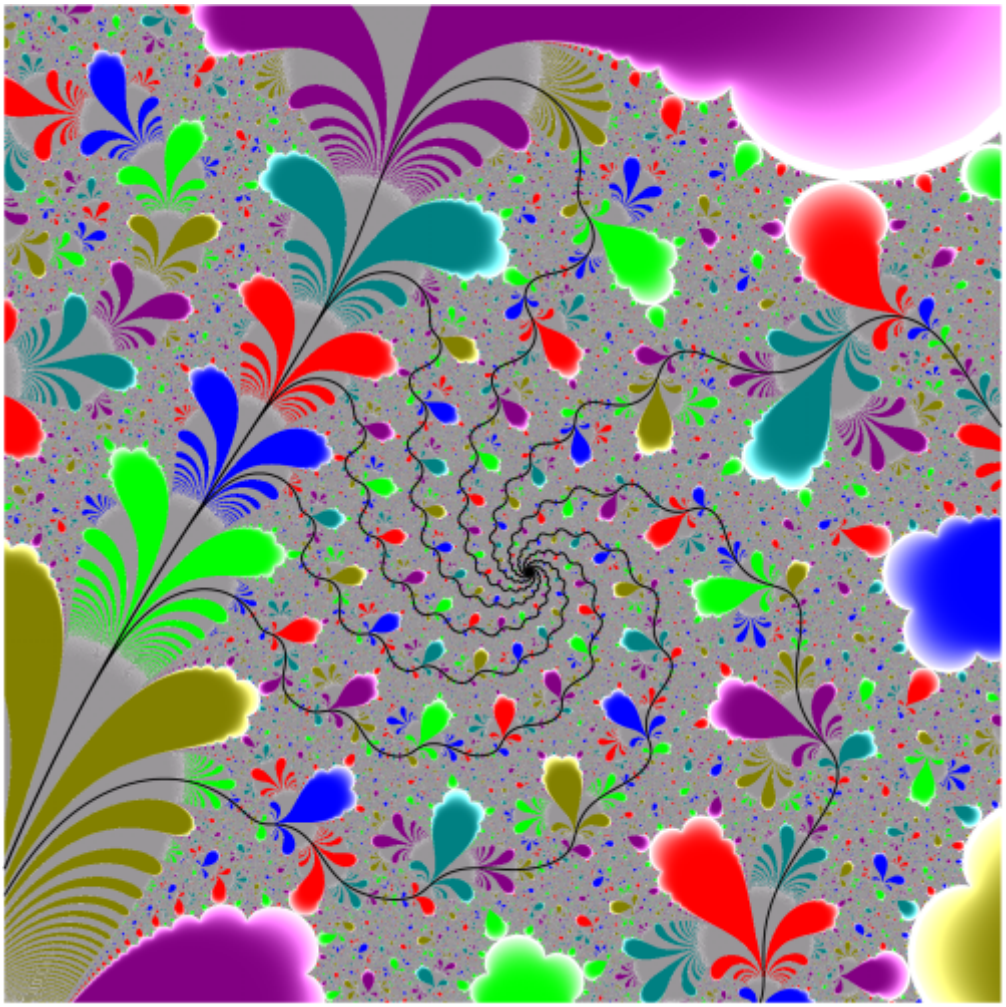
54.5.2 Parameter rays

Mandelbrot set for complex quadratic polynomial with parameter rays of root points

- External rays for angles of the form : n / (2^1 - 1) (0/1; 1/1) landing on the point c= 1/4, which is cusp of main cardioid (period 1 component)

- External rays for angles of the form : n / (2^2 - 1) (1/3, 2/3) landing on the point c= - 3/4, which is root point of period 2 component
- External rays for angles of the form : n / (2^3 - 1) (1/7,2/7) (3/7,4/7) landing on the point c= $-1.75 = -7/4$ (5/7,6/7) landing on the root points of period 3 components.
- External rays for angles of form : n / (2^4 - 1) (1/15,2/15) (3/15, 4/15) (6/15, 9/15) landing on the root point c= $-5/4$ (7/15, 8/15) (11/15,12/15) (13/15, 14/15) landing on the root points of period 4 components.
- External rays for angles of form : n / (2^5 - 1) landing on the root points of period 5 components
- internal ray of main cardioid of angle 1/3: starts from center of main cardioid c=0, ends in the root point of period 3 component, which is the landing point of parameter (external) rays of angles 1/7 and 2/7
- Internal ray for angle 1/3 of main cardioid made by conformal map from unit circle
- Mini Mandelbrot set with period 134 and 2 external rays
-
-
-

Parameter space of the complex exponential family f(z)=exp(z)+c. Eight parameter rays landing at this parameter are drawn in black.



54.6 Programs that can draw external rays

- Mandel - program by Wolf Jung written in C++ using Qt with source code available under the GNU General Public License
- Java applets by Evgeny Demidov (code of mndlbrot::turn function by Wolf Jung has been ported to Java) with free source code
- OTIS by Tomoki KAWAHIRA - Java applet without source code
- Spider XView program by Yuval Fisher
- YABMP by Prof. Eugene Zaustinsky for DOS without source code
- DH_Drawer by Arnaud Chéritat written for Windows 95 without source code
- Linas Vepstas C programs for Linux console with source code
- Program Julia by Curtis T McMullen written in C and Linux commands for C shell console with source code
- mjwinq program by Matjaz Erat written in delphi/windows without source code (For the external rays it uses the methods from quad.c in julia.tar by Curtis T McMullen)
- RatioField by Gert Buschmann, for windows with Pascal source code for Dev-Pascal 1.9.2 (with Free Pascal compiler)
- Mandelbrot program by Milan Va, written in Delphi with source code
- Power MANDELZOOM by Robert Munafo
- ruff by Claude Heiland-Allen

54.7 See also

- external rays of Misiurewicz point
- Orbit portrait
- Periodic points of complex quadratic mappings
- Prouhet-Thue-Morse constant
- Carathéodory's theorem
- Field lines of Julia sets

54.8 References

[1] J. Kiwi : Rational rays and critical portraits of complex polynomials. Ph. D. Thesis SUNY at Stony Brook (1997); IMS Preprint #1997/15.

[2] Yunping Jing : Local connectivity of the Mandelbrot set at certain infinitely renormalizable points Complex Dynamics and Related Topics, New Studies in Advanced Mathematics, 2004, The International Press, 236-264

[3] POLYNOMIAL BASINS OF INFINITY LAURA DEMARCO AND KEVIN M. PILGRIM

[4] How to draw external rays by Wolf Jung

[5] Tessellation and Lyubich-Minsky laminations associated with quadratic maps I: Pinching semiconjugacies Tomoki Kawahira

[6] Irwin Jungreis: The uniformization of the complement of the Mandelbrot set. Duke Math. J. Volume 52, Number 4 (1985), 935-938.

[7] Adrien Douady, John Hubbard, Etudes dynamique des polynomes complexes I & II, Publ. Math. Orsay. (1984-85) (The Orsay notes)

[8] Computing the Laurent series of the map Psi: C-D to C-M. Bielefeld, B.; Fisher, Y.; Haeseler, F. V. Adv. in Appl. Math. 14 (1993), no. 1, 25-−38,

[9] Weisstein, Eric W. "Mandelbrot Set." From MathWorld--A Wolfram Web Resource

[10] An algorithm to draw external rays of the Mandelbrot set by Tomoki Kawahira

[11] http://www.mrob.com/pub/muency/externalangle.html External angle at Mu-ency by Robert Munafo

[12] Computation of the external argument by Wolf Jung

[13] A. DOUADY, Algorithms for computing angles in the Mandelbrot set (Chaotic Dynamics and Fractals, ed. Barnsley and Demko, Acad. Press, 1986, pp. 155-168).

[14] Adrien Douady, John H. Hubbard: Exploring the Mandelbrot set. The Orsay Notes. page 58

[15] Exploding the Dark Heart of Chaos by Chris King from Mathematics Department of University of Auckland

[16] Topological Dynamics of Entire Functions by Helena Mihaljevic-Brandt

[17] Dynamic rays of entire functions and their landing behaviour by Helena Mihaljevic-Brandt

- Lennart Carleson and Theodore W. Gamelin, *Complex Dynamics*, Springer 1993
- Adrien Douady and John H. Hubbard, *Etude dynamique des polynômes complexes*, Prépublications mathémathiques d'Orsay 2/4 (1984 / 1985)
- John W. Milnor, *Periodic Orbits, External Rays and the Mandelbrot Set: An Expository Account*; Géométrie complexe et systèmes dynamiques (Orsay, 1995), Astérisque No. 261 (2000), 277–333. (First appeared as a Stony Brook IMS Preprint in 1999, available as arXiV:math.DS/9905169.)
- John Milnor, *Dynamics in One Complex Variable*, Third Edition, Princeton University Press, 2006, ISBN 0-691-12488-4
- Wolf Jung : Homeomorphisms on Edges of the Mandelbrot Set. Ph.D. thesis of 2002

54.9 External links

- Hubbard Douady Potential, Field Lines by Inigo Quilez
- Drawing Mc by Jungreis Algorithm
- Internal rays of components of Mandelbrot set
- John Hubbard's presentation, The Beauty and Complexity of the Mandelbrot Set, part 3.1
- videos by ImpoliteFruit
- Milan Va. "Mandelbrot set drawing". Retrieved 2009-06-15.

Chapter 55

Faber polynomials

In mathematics, the **Faber polynomials** *Pm* of a Laurent series

$$f(z) = z^{-1} + a_0 + a_1 z + \cdots$$

are the polynomials such that

$$P_m(f) - z^{-m}$$

vanishes at *z*=0. They were introduced by Faber (1903, 1919) and studied by Grunsky (1939) and Schur (1945).

55.1 References

- Curtiss, J. H. (1971), "Faber Polynomials and the Faber Series", *The American Mathematical Monthly* (Mathematical Association of America) **78** (6): 577–596, ISSN 0002-9890, JSTOR 2316567
- Faber, Georg (1903), "Über polynomische Entwickelungen", *Mathematische Annalen* (Springer Berlin / Heidelberg) **57**: 389–408, doi:10.1007/BF01444293, ISSN 0025-5831
- Faber, G. (1919), "Über Tschebyscheffsche Polynome.", *Journal für die reine und angewandte Mathematik* (in German) **150**: 79–106, ISSN 0075-4102, JFM 47.0315.01
- Grunsky, Helmut (1939), "Koeffizientenbedingungen für schlicht abbildende meromorphe Funktionen", *Mathematische Zeitschrift* **45** (1): 29–61, doi:10.1007/BF01580272, ISSN 0025-5874
- Schur, Issai (1945), "On Faber polynomials", *American Journal of Mathematics* **67**: 33–41, ISSN 0002-9327, JSTOR 2371913, MR 0011740
- Suetin, P. K. (1998) [1984], *Series of Faber polynomials*, Analytical Methods and Special Functions **1**, New York: Gordon and Breach Science Publishers, ISBN 978-90-5699-058-9, MR 1676281
- Suetin, P. K. (2001), "f/f038010", in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4

Chapter 56

Factor theorem

In algebra, the **factor theorem** is a theorem linking factors and zeros of a polynomial. It is a special case of the polynomial remainder theorem.[1]

The factor theorem states that a polynomial $f(x)$ has a factor $(x-k)$ if and only if $f(k)=0$ (i.e. k is a root).[2]

56.1 Factorization of polynomials

Main article: Factorization of polynomials

Two problems where the factor theorem is commonly applied are those of factoring a polynomial and finding the roots of a polynomial equation; it is a direct consequence of the theorem that these problems are essentially equivalent.

The factor theorem is also used to remove known zeros from a polynomial while leaving all unknown zeros intact, thus producing a lower degree polynomial whose zeros may be easier to find. Abstractly, the method is as follows:[3]

1. "Guess" a zero a of the polynomial f . (In general, this can be *very hard*, but maths textbook problems that involve solving a polynomial equation are often designed so that some roots are easy to discover.)
2. Use the factor theorem to conclude that $(x-a)$ is a factor of $f(x)$.
3. Compute the polynomial $g(x) = f(x)/(x-a)$, for example using polynomial long division or synthetic division.
4. Conclude that any root $x \neq a$ of $f(x)=0$ is a root of $g(x)=0$. Since the polynomial degree of g is one less than that of f , it is "simpler" to find the remaining zeros by studying g .

56.1.1 Example

Find the factors at

$x^3+7x^2+8x+2.$

To do this you would use trial and error to find the first x value that causes the expression to equal zero. To find out if $(x-1)$ is a factor, substitute $x=1$ into the polynomial above:

$x^3+7x^2+8x+2=(1)^3+7(1)^2+8(1)+2$

$=1+7+8+2$

$=18.$

As this is equal to 18 and not 0 this means $(x-1)$ is not a factor of x^3+7x^2+8x+2 . So, we next try $(x+1)$ (substituting $x=-1$ into the polynomial):

$$(-1)^3+7(-1)^2+8(-1)+2.$$

This is equal to 0 . Therefore $x-(-1)$, which is to say $x+1$, is a factor, and -1 is a root of x^3+7x^2+8x+2.

The next two roots can be found by algebraically dividing x^3+7x^2+8x+2 by $(x+1)$ to get a quadratic, which can be solved directly, by the factor theorem or by the quadratic formula.

$$\frac{x^3+7x^2+8x+2}{x+1}=x^2+6x+2$$

and therefore $(x+1)$ and x^2+6x+2 are the factors of x^3+7x^2+8x+2.

56.2 References

[1] Sullivan, Michael (1996), *Algebra and Trigonometry*, Prentice Hall, p. 381, ISBN 0-13-370149-2.

[2] Sehgal, V K; Gupta, Sonal, *Longman ICSE Mathematics Class 10*, Dorling Kindersley (India), p. 119, ISBN 978-81-317-2816-1.

[3] Bansal, R. K., *Comprehensive Mathematics IX*, Laxmi Publications, p. 142, ISBN 81-7008-629-9.

Chapter 57

Factorization of polynomials

In mathematics and computer algebra, **factorization of polynomials** or **polynomial factorization** is the process of expressing a polynomial with coefficients in a given field or in the integers as the product of irreducible factors with coefficients in same domain. Polynomial factorization is one of the fundamental tools of the computer algebra systems.

The history of polynomial factorization starts with Hermann Schubert who in 1793 described the first polynomial factorization algorithm, and Leopold Kronecker, who rediscovered Schubert's algorithm in 1882 and extended it to multivariate polynomials and coefficients in an algebraic extension. But most of the knowledge on this topic is not older than circa 1965 and the first computer algebra systems. In a survey of the subject, Erich Kaltofen wrote in 1982 (see the bibliography, below):

> When the long-known finite step algorithms were first put on computers, they turned out to be highly inefficient. The fact that almost any uni- or multivariate polynomial of degree up to 100 and with coefficients of a moderate size (up to 100 bits) can be factored by modern algorithms in a few minutes of computer time indicates how successfully this problem has been attacked during the past fifteen years.

Nowadays[1] one can quickly factor any univariate polynomial of degree 1000, and coefficients with thousands of digits.

57.1 Formulation of the question

Polynomial rings over the integers or over a field are unique factorization domains. This means that every element of these rings is a product of a constant and a product of irreducible polynomials (those that are not the product of two non-constant polynomials). Moreover, this decomposition is unique up to multiplication of the factors by invertible constants.

Factorization depends on the base field. For example, the fundamental theorem of algebra, which states that every polynomial with complex coefficients has complex roots, implies that a polynomial with integer coefficients can be factored (with root-finding algorithms) into linear factors over the complex field **C**. Similarly, over the field of reals, the irreducible factors have degree at most two, while there are polynomials of any degree that are irreducible over the field of rationals **Q**.

The question of polynomial factorization makes sense only for coefficients in a *computable field* whose every element may be represented in a computer and for which there are algorithms for the arithmetic operations. Fröhlich and Shepherson have provided examples of such fields for which no factorization algorithm can exist.

The fields of coefficients for which factorization algorithms are known include prime fields (i.e. the field of rationals and prime modular arithmetic) and their finitely generated field extensions. Integer coefficients are also tractable. Kronecker's classical method is interesting only from a historical point of view; modern algorithms proceed by a succession of:

- Square-free factorization

- Factorization over finite fields

and reductions:

- From the multivariate case to the univariate case.
- From coefficients in a purely transcendental extension to the multivariate case over the ground field (see below).
- From coefficients in an algebraic extension to coefficients in the ground field (see below).
- From rational coefficients to integer coefficients (see below).
- From integer coefficients to coefficients in a prime field with p elements, for a well chosen p (see below).

57.2 Primitive part–content factorization

See also: Content (algebra) and Gauss's lemma (polynomial)

In this section, we show that factoring over $\mathbf{Q}$ (the rational numbers) and over $\mathbf{Z}$ (the integers) is essentially the same problem.

The *content* of a polynomial $p \in \mathbf{Z}[X]$, denoted "cont(p)", is, up to its sign, the greatest common divisor of its coefficients. The *primitive part* of p is primpart(p)=p/cont(p), which is a primitive polynomial with integer coefficients. This defines a factorization of p into the product of an integer and a primitive polynomial. This factorization is unique up to the sign of the content. It is a usual convention to choose the sign of the content such that the leading coefficient of the primitive part is positive.

For example,

$$-10x^2 + 5x + 5 = (-5) \cdot (2x^2 - x - 1)$$

is a factorization into content and primitive part.

Every polynomial q with rational coefficients may be written

$$q = \frac{p}{c},$$

where $p \in \mathbf{Z}[X]$ and $c \in \mathbf{Z}$: it suffices to take for c a multiple of all denominators of the coefficients of q (for example their product) and $p = cq$. The *content* of q is defined as:

$$\operatorname{cont}(q) = \frac{\operatorname{cont}(p)}{c},$$

and the *primitive part* of q is that of p. As for the polynomials with integer coefficients, this defines a factorization into a rational number and a primitive polynomial with integer coefficients. This factorization is also unique up to the choice of a sign.

For example,

$$\frac{1}{3}x^5 + \frac{7}{2}x^2 + 2x + 1 = \frac{1}{6}(2x^5 + 21x^2 + 12x + 6)$$

is a factorization into content and primitive part.

Gauss proved that the product of two primitive polynomials is also primitive (Gauss's lemma). This implies that a primitive polynomial is irreducible over the rationals if and only if it is irreducible over the integers. This implies also that the factorization over the rationals of a polynomial with rational coefficients is the same as the factorization over

the integers of its primitive part. On the other hand, the factorization over the integers of a polynomial with integer coefficients is the product of the factorization of its primitive part by the factorization of its content.

In other words, integer GCD computation allows to reduce the factorization of a polynomial over the rationals to the factorization of a primitive polynomial with integer coefficients, and to reduce the factorization over the integers to the factorization of an integer and a primitive polynomial.

Everything that precedes remains true if **Z** is replaced by a polynomial ring over a field *F* and **Q** is replaced by a field of rational functions over *F* in the same variables, with the only difference that "up to a sign" must be replaced by "up to the multiplication by an invertible constant in *F*". This allows to reduce the factorization over a purely transcendental field extension of *F* to the factorization of multivariate polynomials over *F*.

57.3 Square-free factorization

Main article: square-free polynomial

If two or more factors of a polynomial are identical to each other, then the polynomial is a multiple of the square of this factor. In the case of univariate polynomials, this results in multiple roots. In this case, then the multiple factor is also a factor of the polynomial's derivative (with respect to any of the variables, if several). In the case of univariate polynomials over the rationals (or more generally over a field of characteristic zero), Yun's algorithm exploits this to factorize efficiently the polynomial into factors that are not multiple of a square and are therefore called **square-free**. To factorize the initial polynomial, it suffices to factorize each square-free factor. Square-free factorization is therefore the first step in most polynomial factorization algorithms.

Yun's algorithm extends to the multivariate case by considering a multivariate polynomial as an univariate polynomial over a polynomial ring.

In the case of a polynomial over a finite field, Yun's algorithm applies only if the degree is smaller than the characteristic, because, otherwise, the derivative of a non zero polynomial may be zero (over the field with *p* elements, the derivative of a polynomial in x^p is always zero). Nevertheless a succession of GCD computations, starting from the polynomial and its derivative, allows to compute the square-free decomposition; see Polynomial factorization over finite fields#Square-free factorization.

57.4 Classical methods

This section describes textbook methods that can be convenient when computing by hand. These methods are not used for computer computations because they use integer factorization, which at the moment has a much higher complexity than polynomial factorization.

57.4.1 Obtaining linear factors

All linear factors with rational coefficients can be found using the rational root test. If the polynomial to be factored is $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then all possible linear factors are of the form $b_1 x - b_0$, where b_1 is an integer factor of a_n and b_0 is an integer factor of a_0 . All possible combinations of integer factors can be tested for validity, and each valid one can be factored out using polynomial long division. If the original polynomial is the product of factors, at least two of which are of degree 2 or higher, this technique only provides a partial factorization; otherwise the factorization is complete. In particular, if there is exactly one non-linear factor, it will be the polynomial left after all linear factors have been factorized out. Note that in the case of a cubic polynomial, if the cubic is factorisable at all, the rational root test gives a complete factorization, either into a linear factor and an irreducible quadratic factor, or into three linear factors.

57.4.2 Kronecker's method

Since integer polynomials must factor into integer polynomial factors, and evaluating integer polynomials at integer values must produce integers, the integer values of a polynomial can be factored in only a finite number of ways, and produce only a finite number of possible polynomial factors.

For example, consider

$$f(x) = x^5 + x^4 + x^2 + x + 2$$

If this polynomial factors over **Z**, then at least one of its factors must be of degree two or less. We need three values to uniquely fit a second degree polynomial. We'll use $f(0) = 2$, $f(1) = 6$ and $f(-1) = 2$. Note that if one of those values were 0 then you already found a root (and so a factor). If none is 0, then each one has a finite amount of divisors. Now, 2 can only factor as

1×2, 2×1, (−1)×(−2), or (−2)×(−1).

Therefore, if a second degree integer polynomial factor exists, it must take one of the values

1, 2, −1, or −2

at $x = 0$, and likewise at $x = -1$. There are eight different ways to factor 6 (one for each divisor of 6), so there are

4×4×8 = 128

possible combinations, of which half can be discarded as the negatives of the other half, corresponding to 64 possible second degree integer polynomials that must be checked. These are the only possible integer polynomial factors of $f(x)$. Testing them exhaustively reveals that

$$p(x) = x^2 + x + 1$$

constructed from $p(0) = 1$, $p(1) = 3$ and $p(-1) = 1$, factors $f(x)$.

Dividing f by p gives the other factor $q(x) = x^3 - x + 2$, so that $f = pq$. Now one can test recursively to find factors of p and q . It turns out they both are irreducible over the integers, so that the irreducible factorization of f is

$$f(x) = p(x)q(x) = (x^2 + x + 1)(x^3 - x + 2)$$

(*Van der Waerden*, Sections 5.4 and 5.6)

57.5 Modern methods

57.5.1 Factoring over finite fields

Main articles: Factorization of polynomials over finite fields, Berlekamp's algorithm and Cantor–Zassenhaus algorithm

57.5.2 Factoring univariate polynomials over the integers

If $f(x)$ is a univariate polynomial over the integers, assumed to be content-free and square-free, one starts by computing a bound B such that any factor $g(x)$ will have coefficients of absolute value bounded by B . This way, if m is an integer larger than $2B$, and if $g(x)$ is known modulo m , then $g(x)$ can be reconstructed from its image mod m .

The Zassenhaus algorithm proceeds as follows. First, choose a prime number p such that the image of $f(x)$ mod p remains square-free, and of the same degree as $f(x)$. Then factor $f(x)$ mod p . This produces integer polynomials $f_1(x), ..., f_r(x)$ whose product matches $f(x)$ mod p . Next, apply Hensel lifting, this updates the $f_i(x)$ in such a way that now their product matches $f(x)$ mod p^a , where a is chosen in such a way that p^a is larger than $2B$. Modulo p^a , the polynomial $f(x)$ has (up to units) 2^r factors: for each subset of $f_1(x), ..., f_r(x)$, the product is a factor of $f(x)$

mod p^a . However, a factor modulo p^a need not correspond to a so-called "true factor": a factor of $f(x)$ in $Z[x]$. For each factor mod p^a , we can test if it corresponds to a "true" factor, and if so, find that "true" factor, provided that p^a exceeds $2B$. This way, all irreducible "true" factors can be found by checking at most 2^r cases. This is reduced to 2^{r-1} cases by skipping complements. If $f(x)$ is reducible, the number of cases is reduced further by removing those $f_i(x)$ that appear in an already found "true" factor. Zassenhaus algorithm processes each case (each subset) quickly, however, in the worst case, it considers an exponential number of cases.

The first polynomial time algorithm for factoring rational polynomials has been discovered by Lenstra, Lenstra and Lovász and is an application of Lenstra–Lenstra–Lovász lattice basis reduction algorithm, usually called "LLL algorithm". (Lenstra, Lenstra & Lovász 1982) A simplified version of the LLL factorization algorithm is as follows: calculate a complex (or *p*-adic) root α of the polynomial $f(x)$ to high precision, then use the Lenstra–Lenstra–Lovász lattice basis reduction algorithm to find an approximate linear relation between 1, α, α^2, α^3, ... with integer coefficients, which might be an exact linear relation and a polynomial factor of $f(x)$. One can determine a bound for the precision that guarantees that this method produces either a factor, or an irreducibility proof. Although this method is polynomial time, it was not used in practice because the lattice has high dimension and huge entries, which makes the computation slow.

The exponential complexity in the algorithm of Zassenhaus comes from a combinatorial problem: how to select the right subsets of $f_1(x), ..., f_r(x)$. State of the art factoring implementations work in a manner similar to Zassenhaus, except that the combinatorial problem is translated to a lattice problem that is then solved by LLL.[2] In this approach, LLL is not used to compute coefficients of factors, instead, it is used to compute vectors with r entries in {0,1} that encode the subsets of $f_1(x), ..., f_r(x)$ that correspond to the irreducible "true" factors.

57.5.3 Factoring over algebraic extensions (Trager's method)

We can factor a polynomial $p(x) \in K[x]$, where K is a finite field extension of $\mathbb{Q}$. First, using square-free factorization, we may suppose that the polynomial is square-free. Next we write $L = K[x]/p(x)$ explicitly as an algebra over $\mathbb{Q}$. We next pick a random element $\alpha \in L$. By the primitive element theorem, α generates L over $\mathbb{Q}$ with high probability. If this is the case, we can compute the minimal polynomial, $q(y) \in \mathbb{Q}[y]$ of α over $\mathbb{Q}$. Factoring

$$q(y) = \prod_{i=1}^{n} q_i(y)$$

over $\mathbb{Q}[y]$, we determine that

$$L = \mathbb{Q}[\alpha] = \mathbb{Q}[y]/q(y) = \prod_{i=1}^{n} \mathbb{Q}[y]/q_i(y)$$

(notice that L is a reduced ring since $p(x)$ is square-free), where α corresponds to the element $(y, y, \ldots, y)$. Note that this is the unique decomposition of L as a product fields. Hence this decomposition is the same as

$$\prod_{i=1}^{m} K[x]/p_i(x)$$

where

$$p(x) = \prod_{i=1}^{m} p_i(x)$$

is the factorization of $p(x)$ over $K[x]$. By writing $x \in L$ and generators of K as a polynomials in α , we can determine the embeddings of x and K into the components $\mathbb{Q}[y]/q_i(y) = K[x]/p_i(x)$. By finding the minimal polynomial of x in this ring, we have computed $p_i(x)$, and thus factored $p(x)$ over K.

57.6 See also

- Factorization § Polynomials, for elementary heuristic methods and explicit formulas

57.7 Bibliography

[1] An example of degree 2401, taking 7.35 seconds, is found in Section 4 in: Hart, van Hoeij, Novocin: *Practical Polynomial Factoring in Polynomial Time* ISSAC'2011 Proceedings, p. 163-170 (2011).

[2] M. van Hoeij: *Factoring polynomials and the knapsack problem.* J. of Number Theory, 95, 167-189, (2002).

- Fröhlich, A.; Shepherson, J. C. (1955), "On the factorisation of polynomials in a finite number of steps", *Mathematische Zeitschrift* **62** (1), doi:10.1007/BF01180640, ISSN 0025-5874
- Trager, B.M., "Algebraic Factoring and Rational Function Integration", *Proc. SYMSAC 76 http://dl.acm.org/citation.cfm?id=806338"*
- Bernard Beauzamy, Per Enflo, Paul Wang (October 1994). "Quantitative Estimates for Polynomials in One or Several Variables: From Analysis and Number Theory to Symbolic and Massively Parallel Computation". *Mathematics Magazine* **67** (4): 243–257. doi:10.2307/2690843. JSTOR 2690843. (accessible to readers with undergraduate mathematics)
- Cohen, Henri (1993). *A course in computational algebraic number theory*. Graduate Texts in Mathematics **138**. Berlin, New York: Springer-Verlag. ISBN 978-3-540-55640-4. MR 1228206.
- Kaltofen, Erich (1982), "Factorization of polynomials", in B. Buchberger; R. Loos; G. Collins, *Computer Algebra*, Springer Verlag, CiteSeerX: 10.1.1.39.7916
- Knuth, Donald E (1997). "4.6.2 Factorization of Polynomials". *Seminumerical Algorithms*. The Art of Computer Programming **2** (Third ed.). Reading, Massachusetts: Addison-Wesley. pp. 439–461, 678–691. ISBN 0-201-89684-2.
- Lenstra, A. K.; Lenstra, H. W.; Lovász, László (1982). "Factoring polynomials with rational coefficients". *Mathematische Annalen* **261** (4): 515–534. doi:10.1007/BF01457454. ISSN 0025-5831. MR 682664.
- Van der Waerden, *Algebra* (1970), trans. Blum and Schulenberger, Frederick Ungar.

57.8 Further reading

- Kaltofen, Erich (1990), "Polynomial Factorization 1982-1986", in D. V. Chudnovsky; R. D. Jenks, *Computers in Mathematics*, Lecture Notes in Pure and Applied Mathematics **125**, Marcel Dekker, Inc., CiteSeerX: 10.1.1.68.7461
- Kaltofen, Erich (1992), "Polynomial Factorization 1987–1991", *Proceedings of Latin '92* (PDF), Springer Lect. Notes Comput. Sci. **583**, Springer, retrieved October 14, 2012
- Ivanyos, Gabor; Marek, Karpinski; Saxena, Nitin (2009), "Schemes for Deterministic Polynomial Factoring", *Proc. ISSAC 2009*: 191–198, doi:10.1145/1576702.1576730

Chapter 58

Factorization of polynomials over finite fields

In mathematics and computer algebra the factorization of a polynomial consists of decomposing it into a product of irreducible factors. This decomposition is theoretically possible and is unique for polynomials with coefficients in any field, but rather strong restrictions on the field of the coefficients are needed to allow the computation of the factorization by means of an algorithm. In practice, algorithms have been designed only for polynomials with coefficients in a finite field, in the field of rationals or in a finitely generated field extension of one of them.

The case of the **factorization of univariate polynomials over a finite field**, which is the subject of this article, is especially important, because all the algorithms (including the case of multivariate polynomials over the rational numbers), which are sufficiently efficient to be implemented, reduce the problem to this case (see Polynomial factorization). It is also interesting for various applications of finite fields, such as coding theory (cyclic redundancy codes and BCH codes), cryptography (public key cryptography by the means of elliptic curves), and computational number theory.

As the reduction of the factorization of multivariate polynomials to that of univariate polynomials does not have any specificity in the case of coefficients in a finite field, only polynomials with one variable are considered in this article.

58.1 Background

58.1.1 Finite field

Main article: Finite field

The theory of finite fields, whose origins can be traced back to the works of Gauss and Galois, has played a part in various branches of mathematics. Due to the applicability of the concept in other topics of mathematics and sciences like computer science there has been a resurgence of interest in finite fields and this is partly due to important applications in coding theory and cryptography. Applications of finite fields introduce some of these developments in cryptography, computer algebra and coding theory.

A finite field or Galois field is a field with a finite order (number of elements). The order of a finite field is always a prime or a power of prime. For each prime power $q = p^r$, there exists exactly one finite field with q elements, up to isomorphism. This field is denoted $GF(q)$ or $\mathbf{F}q$. If p is prime, $GF(p)$ is the prime field of order p; it is the field of residue classes modulo p, and its p elements are denoted 0, 1, ..., p−1. Thus $a = b$ in $GF(p)$ means the same as $a \equiv b \pmod{p}$.

58.1.2 Irreducible polynomials

Let F be a finite field. As for general fields, a non-constant polynomial f in $F[x]$ is said to be irreducible over F if it is not the product of two polynomials of positive degree. A polynomial of positive degree that is not irreducible over F is called *reducible over F*.

Irreducible polynomials allow us to construct the finite fields of non prime order. In fact, for a prime power q, let $\mathbf{F}q$ be the finite field with q elements, unique up to an isomorphism. A polynomial f of degree n greater than one, which is irreducible over $\mathbf{F}q$, defines a field extension of degree n which is isomorphic to the field with q^n elements: the elements of this extension are the polynomials of degree lower than n; addition, subtraction and multiplication by an element of $\mathbf{F}q$ are those of the polynomials; the product of two elements it the remainder of the division by f of their product as polynomials; the inverse of an element may be computed by the extended GCD algorithm (see Arithmetic of algebraic extensions).

It follows that, to compute in a finite field of non prime order, one needs to generate an irreducible polynomial. For this, the common method is to take a polynomial at random and test it for irreducibility. For sake of efficiency of the multiplication in the field, it is usual to search for polynomials of the shape $x^n + ax + b$.

Irreducible polynomials over finite fields are also useful for Pseudorandom number generators using feedback shift registers and discrete logarithm over $\mathbf{F}_2{}^n$.

Example

The polynomial $P = x^4 + 1$ is irreducible over $\mathbf{Q}$ but not over any finite field.

- On any field extension of $\mathbf{F}_2$, $P = (x+1)^4$.
- On every other finite field, at least one of -1, 2 and -2 is a square, because the product of two non squares is a square and so we have

1. If $-1 = a^2$, then $P = (x^2 + a)(x^2 - a)$.
2. If $2 = b^2$, then $P = (x^2 + bx + 1)(x^2 - bx + 1)$.
3. If $-2 = c^2$, then $P = (x^2 + cx - 1)(x^2 - cx - 1)$.

58.1.3 Complexity

Polynomial factoring algorithms use basic polynomial operations such as products, divisions, gcd, powers of one polynomial modulo another, etc. A multiplication of two polynomials of degree at most n can be done in $O(n^2)$ operations in $\mathbf{F}q$ using "classical" arithmetic, or in $O(n\log(n))$ operations in $\mathbf{F}q$ using "fast" arithmetic. A Euclidean division (division with remainder) can be performed within the same time bounds. The cost of a polynomial greatest common divisor between two polynomials of degree at most n can be taken as $O(n^2)$ operations in $\mathbf{F}q$ using classical methods, or as $O(n\log^2(n))$ operations in $\mathbf{F}q$ using fast methods. For polynomials h, g of degree at most n, the exponentiation $h^q \bmod g$ can be done with $O(\log(q))$ polynomial products, using exponentiation by squaring method, that is $O(n^2\log(q))$ operations in $\mathbf{F}q$ using classical methods, or $O(n\log(q)\log(n))$ operations in $\mathbf{F}q$ using fast methods.

In the algorithms that follow, the complexities are expressed in terms of number of arithmetic operations in $\mathbf{F}q$, using classical algorithms for the arithmetic of polynomials.

58.2 Factoring algorithms

Many algorithms for factoring polynomials over finite fields include the following three stages:

58.2.1 Square-free factorization

The algorithm determines a square-free factorization for polynomials whose coefficients come from the finite field $\mathbf{F}q$ of order $q = p^m$ with p a prime. This algorithm firstly determines the derivative and then computes the gcd of the polynomial and its derivative. If it is not one then the gcd is again divided into the original polynomial, provided that the derivative is not zero (a case that exists for non-constant polynomials defined over finite fields).

This algorithm uses the fact that, if the derivative of a polynomial is zero, then it is a polynomial in x^p, which is, if the coefficients belong to $\mathbf{F}p$, the pth power of the polynomial obtained by substituting x by $x^{1/p}$. If the coefficients do not

belong to $\mathbf{F}p$, the p-th root of a polynomial with zero derivative is obtained by the same substitution on x, completed by applying the inverse of the Frobenius automorphism to the coefficients.

This algorithm works also over a field of characteristic zero, with the only difference that it never enters in the blocks of instructions where pth roots are computed. However, in this case, Yun's algorithm is much more efficient because it computes the greatest common divisors of polynomials of lower degrees. A consequence is that, when factoring a polynomial over the integers, the algorithm which follows is not used: one compute first the square-free factorization over the integers, and to factor the resulting polynomials, one chooses a p such that they remain square-free modulo p.

Algorithm: **SFF** (Square-Free Factorization) **Input**: A monic polynomial f in $\mathbf{F}q[x]$ **Output**: Square-free factorization of f $i \leftarrow 1$; $R \leftarrow 1$; $g \leftarrow f'$; **if** $g \neq 0$ **then** { $c \leftarrow$ **gcd**(f, g); $w \leftarrow f/c$; **while** $w \neq 1$ do { $y \leftarrow$ **gcd**(w, c); $z \leftarrow w/y$; $R \leftarrow R \cdot z^i$; $i \leftarrow i+1$; $w \leftarrow y$; $c \leftarrow c/y$ } **if** $c \neq 1$ **then** { $c \leftarrow c^{1/p}$; **Output**$(R \cdot$**SFF**$(c)^p)$ } else **Output**(R) **else** { $f \leftarrow f^{1/p}$; **Output**(**SFF**$(f)^p$) } **end**.

Example of a square-free factorization

Let

$$f = x^{11} + 2x^9 + 2x^8 + x^6 + x^5 + 2x^3 + 2x^2 + 1 \in \mathbf{F}_3[x],$$

to be factored over the field with three elements.

The algorithm computes first

$$c = \gcd(f, f') = x^9 + 2x^6 + x^3 + 2.$$

Since the derivative is non-zero we have $w = f/c = x^2 + 2$ and we enter the while loop. After one loop we have $y = x + 2$, $z = x + 1$ and $R = x + 1$ with updates $i = 2$, $w = x + 2$ and $c = x^8 + x^7 + x^6 + x^2 + x + 1$. The second time through the loop gives $y = x + 2$, $z = 1$, $R = x + 1$, with updates $i = 3$, $w = x + 2$ and $c = x^7 + 2x^6 + x + 2$. The third time through the loop also does not change R. For the fourth time through the loop we get $y = 1$, $z = x + 2$, $R = (x + 1)(x + 2)^4$, with updates $i = 5$, $w = 1$ and $c = x^6 + 1$. Since $w = 1$, we exit the while loop. Since $c \neq 1$, it must be a perfect cube. The cube root of c, obtained by replacing x^3 by x is $x^2 + 1$, and calling the square-free procedure recursively determines that it is square-free. Therefore, cubing it and combining it with the value of R to that point gives the square-free decomposition

$$f = (x + 1)(x^2 + 1)^3(x + 2)^4.$$

58.2.2 Distinct-degree factorization

This algorithm splits a square-free polynomial into a product of polynomials whose irreducible factors all have the same degree. Let $f \in \mathbf{F}q[x]$ of degree n be the polynomial to be factored.

Algorithm Distinct-degree factorization(DDF) **Input**: A monic square-free polynomial $f \in \mathbf{F}q[x]$ **Output**: The set of all pairs (g, d), such that f has an irreducible factor of degree d and g is the product of all monic irreducible factors of f of degree d. **Begin** $i := 1$; $S := \emptyset$, $f^* := f$; **while** $\deg f^* \geq 2i$ **do** $g = \gcd(f^*, x^{q^i} - x)$ **if** $g \neq 1$, **then** $S := S \cup (g, i)$; $f^* := f^*/g$; **end if** $i := i+1$; **end while**; **if** $f^* \neq 1$, **then** $S := S \cup (f^*, \deg f^*)$; **if** $S = \varnothing$ **then return** $\{(f, 1)\}$ **else return** S **End**

The correctness of the algorithm is based on the following:

Lemma. For $i \geq 1$ the polynomial

$$x^{q^i} - x \in \mathbf{F}_q[x]$$

is the product of all monic irreducible polynomials in $\mathbf{F}q[x]$ whose degree divides i.

At first glance, this is not efficient since it involves computing the GCD of polynomials of a degree which is exponential in the degree of the input polynomial. However

$$g = \gcd\left(f^*, x^{q^i} - x\right)$$

may be replaced by

$$g = \gcd\left(f^*, \left(x^{q^i} - x \mod f^*\right)\right).$$

Therefore we have to compute:

$$x^{q^i} - x \mod f^*,$$

there are two methods:

Method I. Start from the value of

$$x^{q^{i-1}} \mod f^*$$

computed at the preceding step and to compute its q-th power modulo the new f^*, using exponentiation by squaring method. This needs

$$O\left(\log(q)\deg(f)^2\right)$$

arithmetic operations in $\mathbf{F}q$ at each step, and thus

$$O\left(\log(q)\deg(f)^3\right)$$

arithmetic operations for the whole algorithm.

Method II. Using the fact that the q-th power is a linear map over $\mathbf{F}q$ we may compute its matrix with

$$O\left(\deg(f)^2(\log(q) + \deg(f))\right)$$

operations. Then at each iteration of the loop, compute the product of a matrix by a vector (with $O(\deg(f)^2)$ operations). This induces a total number of operations in $\mathbf{F}q$ which is

$$O\left(\deg(f)^2(\log(q) + \deg(f))\right).$$

Thus this second method is more efficient and is usually preferred. Moreover, the matrix that is computed in this method is used, by most algorithms, for equal-degree factorization (see below); thus using it for the distinct-degree factorization saves further computing time.

58.2.3 Equal-degree factorization

Main article: Cantor–Zassenhaus algorithm

In this section, we consider the factorization of a monic squarefree univariate polynomial f, of degree n, over a finite field $\mathbf{F}q$, which has $r \geq 2$ pairwise distinct irreducible factors $f_1, \ldots, f_r$ each of degree d.

We first describe an algorithm by Cantor and Zassenhaus (1981) and then a variant that has a slightly better complexity. Both are probabilistic algorithms whose running time depends on random choices (Las Vegas algorithms), and have a

good average running time. In next section we describe an algorithm by Shoup (1990), which is also an equal-degree factorization algorithm, but is deterministic. All these algorithms require an odd order q for the field of coefficients. For more factorization algorithms see e.g. Knuth's book The Art of Computer Programming volume 2.

Algorithm Cantor–Zassenhaus algorithm. Input: A finite field $\mathbf{F}q$ of odd order q. A monic square free polynomial f in $\mathbf{F}q[x]$ of degree $n = rd$, which has $r \geq 2$ irreducible factors each of degree d Output: The set of monic irreducible factors of f. Factors:=$\{f\}$; while Size(Factors) < r do, Choose h in $\mathbf{F}q[x]$ with deg(h) < n at random; $g := h^{\frac{q^d-1}{2}} - 1 \pmod f$ for each u in Factors with deg(u) > d do if gcd(g, u) ≠ 1 and gcd(g, u) ≠ u, then Factors:= Factors $\setminus \{u\} \cup \{(\gcd(g,u), u/\gcd(g,u))\}$; endif; endwhile return Factors.

The correctness of this algorithm relies on the fact that the ring $\mathbf{F}q[x]/f$ is a direct product of the fields $\mathbf{F}q[x]/fi$ where fi runs on the irreducible factors of f. As all these fields have q^d elements, the component of g in any of these fields is zero with probability

$$\frac{q^d-1}{2q^d} \sim \tfrac{1}{2}.$$

This implies that the polynomial gcd(g, u) is the product of the factors of g for which the component of g is zero.

It has been shown that the average number of iterations of the while loop of the algorithm is less than $2.5 \log_2 r$, giving an average number of arithmetic operations in$\mathbf{F}q$ which is $O(dn^2 \log(r) \log(q))$.[1]

In the typical case where $d\log(q) > n$, this complexity may be reduced to

$$O(n^2(\log(r)\log(q) + n))$$

by choosing h in the kernel of the linear map

$$v \to v^q - v \pmod f$$

and replacing the instruction

$$g := h^{\frac{q^d-1}{2}} - 1 \pmod f$$

by

$$g := h^{\frac{q-1}{2}} - 1 \pmod f.$$

The proof of validity is the same as above, replacing the direct product of the fields $\mathbf{F}q[x]/fi$ by the direct product of their subfields with q elements. The complexity is decomposed in $O(n^2 \log(r) \log(q))$ for the algorithm itself, $O(n^2(\log(q) + n))$ for the computation of the matrix of the linear map (which may be already computed in the square-free factorization) and $O(n^3)$ for computing its kernel. It may be noted that this algorithm works also if the factors have not the same degree (in this case the number r of factors, needed for stopping the while loop, is found as the dimension of the kernel). Nevertheless, the complexity is slightly better if square-free factorization is done before using this algorithm (as n may decrease with square-free factorization, this reduces the complexity of the critical steps).

58.2.4 Victor Shoup's algorithm

Like the algorithms of the preceding section, Victor Shoup's algorithm is an equal-degree factorization algorithm.[2] Unlike them, it is a deterministic algorithm. However, it is less efficient, in practice, that the algorithms of preceding section. For Shoup's algorithm, the input is restricted to polynomials over prime fields $\mathbf{F}q$.

Let $g = g_1 \ldots gk$ be the desired factorization, where the gi are distinct monic irreducible polynomials of degree d. Let $n = \deg(g) = kd$. We consider the ring $R = \mathbf{F}q[x]/g$ and denote also by x the image of x in R. The ring R is the direct

product of the fields *Ri* = **F***q*[*x*]/*gi*, and we denote by *pi* the natural homomorphism from the *R* onto *Ri*. The Galois group of *Ri* over **F***q* is cyclic of order *d*, generated by the field automorphism $u \to u^p$. It follows that the roots of *gi* in *Ri* are

$$p_i(x), p_i(x^q), p_i\left(x^{q^2}\right), p_i\left(x^{q^{d-1}}\right).$$

If $q > n$, the Newton's identities allow to compute the *si* with

Like in the preceding algorithm, this algorithm uses the same subalgebra *B* of *R* as the Berlekamp's algorithm, sometimes called the "Berlekamp subagebra" and defined as

$$\begin{aligned} B &= \{\alpha \in R \ : \ p_1(\alpha), \cdots, p_k(\alpha) \in \mathbf{F}_q\} \\ &= \{u \in R \ : \ u^q = u\} \end{aligned}$$

A subset *S* of *B* is said a separating set if, for every $1 \le i < j \le k$ there exists $s \in S$ such that $p_i(s) \neq p_j(s)$. In the preceding algorithm, a separating set is constructed by choosing at random the elements of *S*. In Shoup's algorithm, the separating set is constructed in the following way. Let *s* in *R*[*Y*] be such that

$$\begin{aligned} s &= (Y - x)\,(Y - x^q) \cdots \left(Y - x^{q^{d-1}}\right) \\ &= s_0 + \cdots + s_{d-1}Y^{d-1} + Y^d \end{aligned}$$

Then $\{s_0, \ldots, s_{d-1}\}$ is a separating set because $p_i(s) = g_i$ for *i* =1, ..., *k* (the two monic polynomials have the same roots). As the *gi* are pairwise distinct, for every pair of distinct indexes (*i*, *j*), at least one of the coefficients *sh* will satisfy $p_i(s_h) \neq p_j(s_h)$.

Having a separating set, Shoup's algorithm proceeds as the last algorithm of the preceding section, simply by replacing the instruction "choose at random *h* in the kernel of the linear map $v \to v^q - v \pmod f$ " by "choose *h* + *i* with *h* in *S* and *i* in {1, ..., *k*−1}".

58.3 Rabin's test of irreducibility

Like distinct-degree factorization algorithm, Rabin's algorithm[3] is based on the Lemma stated above. Distinct-degree factorization algorithm tests every *d* not greater than half the degree of the input polynomial. Rabin's algorithm takes advantage that the factors are not needed for considering fewer *d*. Otherwise, it is similar to distinct-degree factorization algorithm. It is based on the following fact.

Let *p*1, ..., *pk*, be all the prime divisors of *n*, and denote $n/p_i = n_i$, for $1 \le i \le k$ polynomial *f* in **F***q*[*x*] of degree *n* is irreducible in **F***q*[*x*] if and only if $\gcd\left(f, x^{q^{n_i}} - x\right) = 1$, for $1 \le i \le k$, and *f* divides $x^{q^n} - x$. In fact, if *f* has a factor of degree not dividing *n*, then *f* does not divide $x^{q^n} - x$; if *f* has a factor of degree dividing *n*, then this factor divides at least one of the $x^{q^{n_i}} - x$.

Algorithm Rabin Irreducibility Test **Input**: A monic polynomial *f* in **F***q*[*x*] of degree *n*, *p*1, ..., *pk* all distinct prime divisors of *n*. **Output**: Either "*f* is irreducible" or "*f* is reducible". **Begin for** *j* = 1 to *k* **do** $n_j = n/p_j$; **for** *i* = 1 to *k* **do** $h := x^{q^{n_i}} - x \bmod f$; *g* := gcd(*f*, *h*); **if** $g \neq 1$, **then return** 'f is reducible' **and STOP**; **end for**; $g := x^{q^n} - x \bmod f$; **if** *g* = 0, **then return** "f is irreducible", **else return** "*f* is reducible" **end.**

The basic idea of this algorithm is to compute $x^{q^{n_i}} \bmod f$ starting from the smallest $n_1, \ldots, n_k$ by repeated squaring or using the Frobenius automorphism, and then to take the correspondent gcd. Using the elementary polynomial arithmetic, the computation of the matrix of the Frobenius automorphism needs $O(n^2(n + \log q))$ operations in **F***q*, the computation of

$$x^{q^{n_i}} - x \pmod f$$

needs $O(n^3)$ further operations, and the algorithm itself needs $O(kn^2)$ operations, giving a total of $O(n^2(n + \log q))$ operations in **F***q*. Using fast arithmetic (complexity $O(n \log n)$ for multiplication and division, and $O(n(\log n)^2)$ for GCD computation), the computation of the $x^{q^{n_i}} - x \bmod f$ by repeated squaring is $O(n^2 \log n \log q)$, and the algorithm itself is $O(kn(\log n)^2)$, giving a total of $O(n^2 \log n \log q)$ operations in **F***q*.

58.4 See also

- Berlekamp's algorithm
- Cantor–Zassenhaus algorithm
- Polynomial factorization
- Ivanyos-Karpinski-Saxena algorithm[4]

58.5 References

- KEMPFERT,H (1969) On the *Factorization of Polynomials* Department of Mathematics, The Ohio State University,Columbus,Ohio 43210
- Shoup,Victor (1996) *Smoothness and Factoring Polynomials over Finite Fields* Computer Science Department University of Toronto
- Von Zur Gathen, J.; Panario, D. (2001). Factoring Polynomials Over Finite Fields: A Survey. Journal of Symbolic Computation, Volume 31, Issues 1-2, January 2001, 3-−17.
- Gao Shuhong, Panario Daniel,*Test and Construction of Irreducible Polynomials over Finite Fields* Department of mathematical Sciences, Clemson University, South Carolina, 29634-1907, USA. and Department of computer science University of Toronto, Canada M5S-1A4
- Shoup, Victor (1989) New Algorithms for Finding Irreducible Polynomials over Finite Fields Computer Science Department University of Wisconsin–Madison
- Geddes, Keith O.; Czapor, Stephen R.; Labahn, George (1992). Algorithms for computer algebra. Boston, MA: Kluwer Academic Publishers. pp. xxii+585. ISBN 0-7923-9259-0.

58.6 External links

- Some irreducible polynomials http://www.math.umn.edu/~{}garrett/m/algebra/notes/07.pdf
- Field and Galois Theory :http://www.jmilne.org/math/CourseNotes/FT.pdf
- Galois Field:http://designtheory.org/library/encyc/topics/gf.pdf
- Factoring polynomials over finite fields: http://www.science.unitn.it/~{}degraaf/compalg/polfact.pdf

58.7 Notes

[1] Flajolet, Philippe; Steayaert, Jean-Marc (1982), *A branching process arising in dynamic hashing, trie searching and polynomial factorization*, Lecture Notes in Comput. Sci. **140**, Springer, pp. 239–251

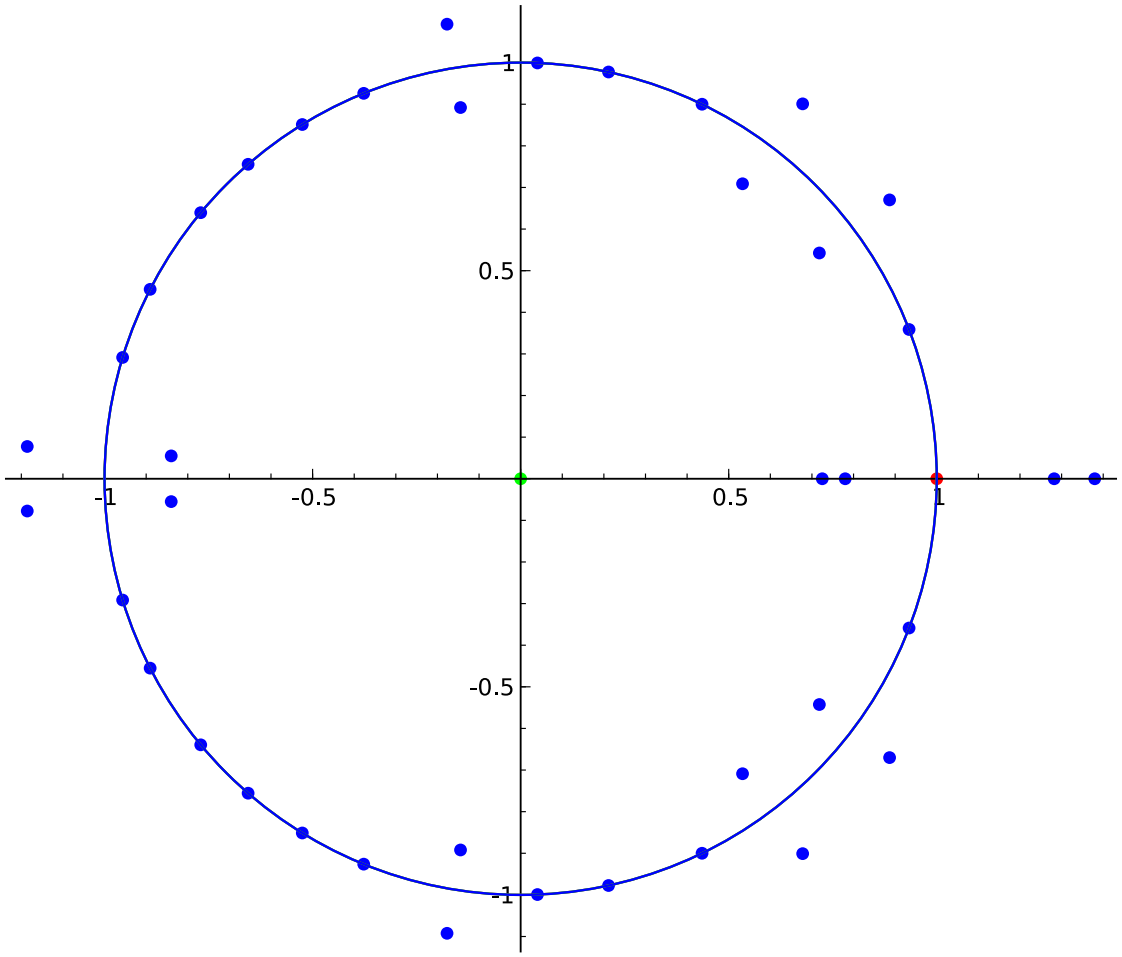
[2] Victor Shoup, On the deterministic complexity of factoring polynomials over finite fields, Information Processing Letters 33:261-267, 1990

[3] Rabin, Michael (1980). "Probabilistic algorithms in finite fields". *SIAM Journal on Computing* **9** (2): 273–280. doi:10.1137/0209024.

[4] Ivanyos, Gabor; Marek, Karpinski; Saxena, Nitin (2009). "Schemes for Deterministic Polynomial Factoring". *Proc. ISSAC 2009*: 191–198. doi:10.1145/1576702.1576730.

Chapter 59

Fekete polynomial



Roots of the Fekete polynomial for p = 43

In mathematics, a **Fekete polynomial** is a polynomial

$$f_p(t) := \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) t^a$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo some integer $p > 1$.

These polynomials were known in nineteenth-century studies of Dirichlet L-functions, and indeed to Peter Gustav Lejeune Dirichlet himself. They have acquired the name of Michael Fekete, who observed that the absence of real zeroes t of the Fekete polynomial with $0 < t < 1$ implies an absence of the same kind for the L-function

$$L\left(s, \frac{x}{p}\right).$$

This is of considerable potential interest in number theory, in connection with the hypothetical Siegel zero near $s = 1$. While numerical results for small cases had indicated that there were few such real zeroes, further analysis reveals that this may indeed be a 'small number' effect.

59.1 References

- Peter Borwein: *Computational excursions in analysis and number theory.* Springer, 2002, ISBN 0-387-95444-9, Chap.5.

59.2 External links

- Brian Conrey, Andrew Granville, Bjorn Poonen and Kannan Soundararajan, *Zeros of Fekete polynomials*, arXiv e-print math.NT/9906214, June 16, 1999.

Chapter 60

Fibonacci polynomials

In mathematics, the **Fibonacci polynomials** are a polynomial sequence which can be considered as a generalization of the Fibonacci numbers. The polynomials generated in a similar way from the Lucas numbers are called **Lucas polynomials**.

60.1 Definition

These Fibonacci polynomials are defined by a recurrence relation:[1]

$$F_n(x) = \begin{cases} 0, & \text{if } n = 0 \\ 1, & \text{if } n = 1 \\ xF_{n-1}(x) + F_{n-2}(x), & \text{if } n \geq 2 \end{cases}$$

The first few Fibonacci polynomials are:

$$F_0(x) = 0$$

$$F_1(x) = 1$$

$$F_2(x) = x$$

$$F_3(x) = x^2 + 1$$

$$F_4(x) = x^3 + 2x$$

$$F_5(x) = x^4 + 3x^2 + 1$$

$$F_6(x) = x^5 + 4x^3 + 3x$$

The Lucas polynomials use the same recurrence with different starting values:[2] $L_n(x) = \begin{cases} 2, & \text{if } n = 0 \\ x, & \text{if } n = 1 \\ xL_{n-1}(x) + L_{n-2}(x), & \text{if } n \geq 2. \end{cases}$

The first few Lucas polynomials are:

$$L_0(x) = 2$$

$$L_1(x) = x$$

$$L_2(x) = x^2 + 2$$

$$L_3(x) = x^3 + 3x$$

$L_4(x) = x^4 + 4x^2 + 2$

$L_5(x) = x^5 + 5x^3 + 5x$

$L_6(x) = x^6 + 6x^4 + 9x^2 + 2.$

The Fibonacci and Lucas numbers are recovered by evaluating the polynomials at $x = 1$; Pell numbers are recovered by evaluating Fn at $x = 2$. The degrees of Fn is $n - 1$ and the degree of Ln is n. The ordinary generating function for the sequences are:[3]

$$\sum_{n=0}^{\infty} F_n(x)t^n = \frac{t}{1 - xt - t^2}$$

$$\sum_{n=0}^{\infty} L_n(x)t^n = \frac{2 - xt}{1 - xt - t^2}.$$

The polynomials can be expressed in terms of Lucas sequences as

$F_n(x) = U_n(x, -1),$

$L_n(x) = V_n(x, -1).$

60.2 Identities

Main article: Lucas sequence

As particular cases of Lucas sequences, Fibonacci polynomials satisfy a number of identities.

First, they can be defined for negative indices by[4]

$$F_{-n}(x) = (-1)^{n-1}F_n(x),\ L_{-n}(x) = (-1)^n L_n(x).$$

Other identities include:[4]

$F_{m+n}(x) = F_{m+1}(x)F_n(x) + F_m(x)F_{n-1}(x)$

$L_{m+n}(x) = L_m(x)L_n(x) - (-1)^n L_{m-n}(x)$

$F_{n+1}(x)F_{n-1}(x) - F_n(x)^2 = (-1)^n$

$F_{2n}(x) = F_n(x)L_n(x).$

Closed form expressions, similar to Binet's formula are:[4]

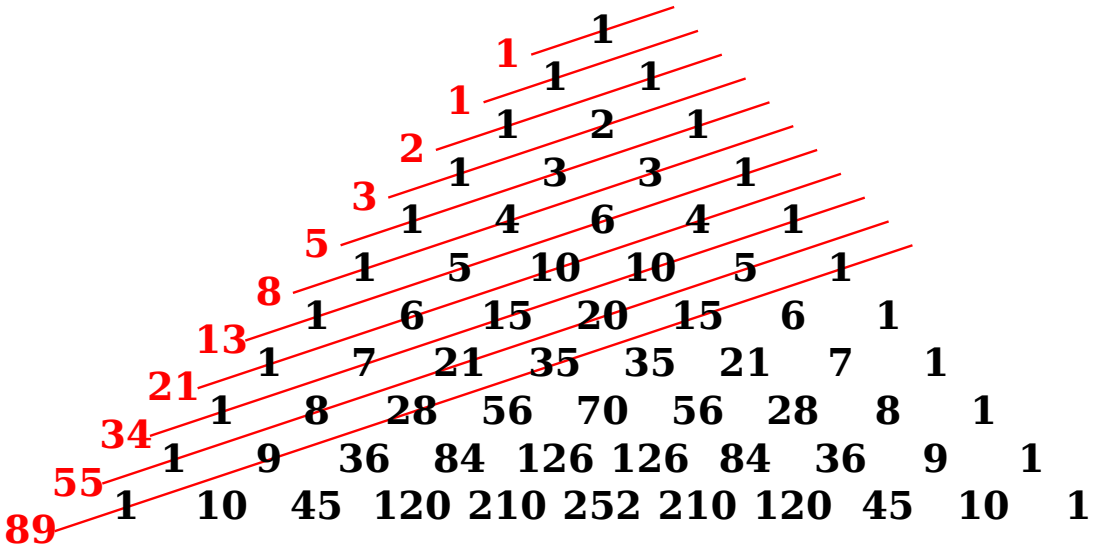
$$F_n(x) = \frac{\alpha(x)^n - \beta(x)^n}{\alpha(x) - \beta(x)},\ L_n(x) = \alpha(x)^n + \beta(x)^n,$$

where

$$\alpha(x) = \frac{x + \sqrt{x^2 + 4}}{2},\ \beta(x) = \frac{x - \sqrt{x^2 + 4}}{2}$$

are the solutions (in t) of

$$t^2 - xt - 1 = 0.$$



The coefficients of the Fibonacci polynomials can be read off from Pascal's triangle following the "shallow" diagonals (shown in red). The sums of the coefficients are the Fibonacci numbers.

60.3 Combinatorial interpretation

If $F(n,k)$ is the coefficient of x^k in $Fn(x)$, so

$$F_n(x) = \sum_{k=0}^{n} F(n,k)x^k,$$

then $F(n,k)$ is the number of ways an $n-1$ by 1 rectangle can be tiled with 2 by 1 dominoes and 1 by 1 squares so that exactly k squares are used.[1] Equivalently, $F(n,k)$ is the number of ways of writing $n-1$ as an ordered sum involving only 1 and 2, so that 1 is used exactly k times. For example F(6,3)=4 and 5 can be written in 4 ways, 1+1+1+2, 1+1+2+1, 1+2+1+1, 2+1+1+1, as a sum involving only 1 and 2 with 1 used 3 times. By counting the number of times 1 and 2 are both used in such a sum, it is evident that $F(n,k)$ is equal to the binomial coefficient

$$F(n,k) = \binom{\frac{n+k-1}{2}}{k}$$

when n and k have opposite parity. This gives a way of reading the coefficients from Pascal's triangle as shown on the right.

60.4 References

[1] Benjamin & Quinn p. 141

[2] Benjamin & Quinn p. 142

[3] Weisstein, Eric W., "Fibonacci Polynomial", *MathWorld*.

[4] Springer

- Benjamin, Arthur T.; Quinn, Jennifer J. (2003). "§9.4 Fibonacci and Lucas Polynomial". *Proofs that Really Count*. MAA. p. 141. ISBN 0-88385-333-7.
- Philippou, Andreas N. (2001), "Fibonacci polynomials", in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4

- Philippou, Andreas N. (2001), "Lucas polynomials", in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Weisstein, Eric W., "Lucas Polynomial", *MathWorld*.

60.5 Further reading

- Hoggatt, V. E.; Bicknell, Marjorie (1973). "Roots of Fibonacci polynomials.". *Fibonacci Quarterly* **11**: 271–274. ISSN 0015-0517. MR 0332645.
- Hoggatt, V. E.; Long, Calvin T. (1974). "Divisibility properties of generalized Fibonacci Polynomials". *Fibonacci Quarterly* **12**: 113. MR 0352034.
- Ricci, Paolo Emilio (1995). "Generalized Lucas polynomials and Fibonacci polynomials". *Rivista di Matematica della Università di Parma*. V. Ser. **4**: 137–146. MR 1395332.
- Yuan, Yi; Zhang, Wenpeng (2002). "Some identities involving the Fibonacci Polynomials". *Fibonacci Quarterly* **40** (4): 314. MR 1920571.
- Cigler, Johann (2003). "q-Fibonacci polynomials". *Fibonacci Quarterly* (41): 31–40. MR 1962279.

60.6 External links

- "Sloane's A162515 : Triangle of coefficients of polynomials defined by Binet form...", *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation.
- "Sloane's A011973 : Triangle of coefficients of Fibonacci polynomials.", *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation.

Chapter 61

Gauss's lemma (polynomial)

This article is about Gauss's lemma for polynomials. For other uses, see Gauss's lemma (disambiguation).

In algebra, in the theory of polynomials (a subfield of ring theory), **Gauss's lemma** is either of two related statements about polynomials with integer coefficients:

- The first result states that the product of two primitive polynomials is primitive (a polynomial with integer coefficients is called *primitive* if the greatest common divisor of its coefficients is 1).
- The second result states that if a non-constant polynomial with integer coefficients is irreducible over the integers, then it is also irreducible if it is considered as a polynomial over the rationals.

This second statement is a consequence of the first (see proof below). The first statement and proof of the lemma is in Article 42 of Carl Friedrich Gauss's *Disquisitiones Arithmeticae* (1801).

61.1 Formal statements

The notion of **primitive polynomial** used here (which differs from the notion with the same name in the context of finite fields) is defined in any polynomial ring $R[X]$ where R is an integral domain: a polynomial P in $R[X]$ is primitive if the only elements of R that divide all coefficients of P at once are the invertible elements of R. In the case where R is the ring $\mathbf{Z}$ of the integers, this is equivalent to the condition that no prime number divides all the coefficients of P. The notion of irreducible element is defined in any integral domain: an element is irreducible if it is not invertible and cannot be written as a product of two non-invertible elements. In the case of a polynomial ring $R[X]$, this means that a non-constant irreducible polynomial is one that is not a product of two non-constant polynomials *and* which is primitive (because being primitive excludes precisely non-invertible constant polynomials as factors). Note that an irreducible element of R is still irreducible when viewed as constant polynomial in $R[X]$; this explains the need for "non-constant" above, and in the irreducibility statements below.

The two properties of polynomials with integer coefficients can now be formulated formally as follows:

- **Primitivity statement:** The set of primitive polynomials in $\mathbf{Z}[X]$ is closed under multiplication: if P and Q are primitive polynomials then so is their product PQ.
- **Irreducibility statement:** A non-constant polynomial in $\mathbf{Z}[X]$ is irreducible in $\mathbf{Z}[X]$ if and only if it is both irreducible in $\mathbf{Q}[X]$ and primitive in $\mathbf{Z}[X]$.

These statements can be generalized to any unique factorization domain (UFD), where they become

- **Primitivity statement:** If R is a UFD, then the set of primitive polynomials in $R[X]$ is closed under multiplication.

- **Irreducibility statement:** Let R be a UFD and F its field of fractions. A non-constant polynomial in $R[X]$ is irreducible in $R[X]$ if and only if it is both irreducible in $F[X]$ and primitive in $R[X]$.

The condition that R is a UFD is not superfluous. In a ring where factorization is not unique, say $pa = qb$ with p and q irreducible elements that do not divide any of the factors on the other side, the product

$$(p + qX)(a + qX) = pa + (p + a)qX + q^2X^2 = q(b + (p + a)X + qX^2)$$

shows the failure of the primitivity statement. For a concrete example one can take

$$R = \mathbb{Z}[\sqrt{-5}], \quad p = 1 + \sqrt{-5}, \quad a = 1 - \sqrt{-5}, \quad q = 2, \quad b = 3.$$

In this example the polynomial $3 + 2X + 2X^2$ (obtained by dividing the right hand side by $q = 2$) provides an example of the failure of the irreducibility statement (it is irreducible over R, but reducible over its field of fractions $\mathbf{Q}[\sqrt{-5}]$). Another well known example is the polynomial $X^2 - X - 1$, whose roots are the golden ratio $\varphi = (1+\sqrt{5})/2$ and its conjugate $(1-\sqrt{5})/2$ showing that it is reducible over the field $\mathbf{Q}[\sqrt{5}]$, although it is irreducible over the non-UFD $\mathbf{Z}[\sqrt{5}]$ which has $\mathbf{Q}[\sqrt{5}]$ as field of fractions. In the latter example the ring can be made into an UFD by taking its integral closure $\mathbf{Z}[\varphi]$ in $\mathbf{Q}[\sqrt{5}]$ (the ring of Dirichlet integers), over which $X^2 - X - 1$ becomes reducible, but in the former example R is already integrally closed.

61.2 Proofs of the primitivity statement

An elementary proof of the statement that the product of primitive polynomials over $\mathbf{Z}$ is again primitive can be given as follows.

Proof: Suppose the product of two primitive polynomials $f(x)$ and $g(x)$ is not primitive, so there exists a prime number p that is a common divisor of all the coefficients of the product. But since $f(x)$ and $g(x)$ are primitive, p cannot divide either all the coefficients of $f(x)$ or all those of $g(x)$. Let arx^r and bsx^s be the first (i.e., highest degree) terms with a coefficient not divisible by p, respectively in $f(x)$ and in $g(x)$. Now consider the coefficient of x^{r+s} in the product. Its value is given by

$$\sum_{i+j=r+s} a_i b_j.$$

This sum contains a term $arbs$ which is not divisible by p (because p is prime, by Euclid's lemma), yet all the remaining ones are (because either $i > r$ or $j > s$), so the entire sum is not divisible by p. But by assumption *all* coefficients in the product are divisible by p, leading to a contradiction. Therefore, the coefficients of the product can have no common divisor and are thus primitive. This completes the proof.

A cleaner version of this proof can be given using the statement from abstract algebra that a polynomial ring over an integral domain is again an integral domain. We formulate this proof directly for the case of polynomials over a UFD R, which is hardly different from its special case for $R = \mathbf{Z}$.

Proof: Let S,T be primitive polynomials in $R[X]$, and assume that their product ST is not primitive, so that some noninvertible element d of R divides all coefficients of ST. There is some irreducible element p of R that divides d, and it is also a prime element in R (since R is a UFD). Then the principal ideal pR generated by p is a prime ideal, so R/pR is an integral domain, and $(R/pR)[X]$ is therefore an integral domain as well. By hypothesis the projection $R[X] \to (R/pR)[X]$ sends ST to 0, and also at least one of S,T individually, which means that p divides all of its coefficients, contradicting primitivity.

The somewhat tedious bookkeeping in the first proof is simplified by the fact that the reduction modulo p kills the uninteresting terms; what is left is a proof that polynomials over an integral domain cannot be zero divisors by consideration of the leading coefficient of their product.

61.2.1 A variation, valid over arbitrary commutative rings

Gauss's lemma is not valid over general integral domains. However there is a variation of Gauss's lemma that is valid even for polynomials over any commutative ring R, which replaces primitivity by the stronger property of co-

maximality (which is however equivalent to primitivity in the case of a Bézout domain, and in particular of a principal ideal domain). Call a polynomial P in $R[X]$ *co-maximal* if the ideal of R generated by the coefficients of the polynomial is the full ring R (when R is a UFD that is not a PID, then co-maximality is much more restrictive than primitivity). The variation of Gauss's lemma says: the product of two co-maximal polynomials is co-maximal.

Proof: Let S,T be co-maximal polynomials in $R[X]$, and assume that their product ST is not co-maximal. Then its coefficients generate a proper ideal I, which by Krull's theorem (which depends on the axiom of choice) is contained in a maximal ideal m of R.Then R/m is a field, and $(R/m)[X]$ is therefore an integral domain. By hypothesis the projection $R[X]\to(R/m)[X]$ sends ST to 0, and also at least one of S,T individually, which means that its coefficients all lie in m, which contradicts the fact that they generate the whole ring as an ideal.

61.2.2 A proof valid over any GCD domain

Gauss's lemma holds over arbitrary GCD domains. There the *content* $c(P)$ of a polynomial P can be defined as the greatest common divisor of the coefficients of P (like the gcd, the content is actually a class of associate elements). The primitivity statement can be generalized to the statement that the content of a product ST of polynomials is the product $c(S)c(T)$ of their contents; in fact this is equivalent to the primitivity statement since $c(S)c(T)$ is certainly a common divisor of the coefficients of the product, so one can divide by $c(S)$ and $c(T)$ to reduce S and T to primitive polynomials. However the proof given above cannot be used when R is a GCD domain, since it uses irreducible factors, which need not exist in such R. Here is a proof that is valid in this context.[1]

We proceed by induction on the total number of nonzero terms of S and T combined. If one of the polynomials has at most one term, the result is obvious; this covers in particular all cases with fewer than 4 nonzero terms. So let both S and T have at least 2 terms, and assume the result established for any smaller combined number of terms. By dividing S by $c(S)$ and T by $c(T)$, we reduce to the case $c(S) = c(T) = 1$. If the content $c = c(ST)$ is not invertible, it has a non-trivial divisor in common with the leading coefficient of at least one of S and T (since it divides their product, which is the leading coefficient of ST). Suppose by symmetry that this is the case for S, let L be the leading term of S, and let $d = \gcd(c,c(L))$ be the mentioned common divisor (here the content $c(L)$ of L is just its unique coefficient). Since d is a common divisor of ST and LT, it also divides $(S - L)T$, in other words it divides its content, which by induction (since $S - L$ has fewer terms than S) is $c(S - L)c(T) = c(S - L)$. As d also divides $c(L)$, it divides $c(S) = 1$, which gives a contradiction; therefore $c(ST)$ is invertible (and can be taken to be 1).

61.3 Proof of the irreducibility statement

We prove the irreducibility statement in the setting of a GCD domain R. As mentioned above a non-constant polynomial is irreducible in $R[X]$ if and only if it is primitive and not a product of two non-constant polynomials in $F[X]$. Being irreducible in $F[X]$ certainly excludes the latter possibility (since those non-constant polynomials would remain non-invertible in $F[X]$), so the essential point left to prove is that if P is non-constant and irreducible in $R[X]$ then it is irreducible in $F[X]$.

Note first that in $F[X]\backslash\{0\}$ any class of associate elements (whose elements are related by multiplication by nonzero elements of the field F) meets the set of primitive elements in $R[X]$: starting from an arbitrary element of the class, one can first (if necessary) multiply by a nonzero element of R to enter into the subset $R[X]$ (removing denominators), then divide by the greatest common divisor of all coefficients to obtain a primitive polynomial. Now assume that P is reducible in $F[X]$, so $P = ST$ with S,T non-constant polynomials in $F[X]$. One can replace S and T by associate primitive elements S', T', and obtain $P = \alpha S'T'$ for some nonzero α in F. But $S'T'$ is primitive in $R[X]$ by the primitivity statement, so α must lie in R (if α is written as a fraction a/b, then b has to divide all coefficients of $aS'T'$, so b divides $c(aS'T') = a$, which means $\alpha = a/b$ is in R) and the decomposition $P = \alpha S'T'$ contradicts the irreducibility of P in $R[X]$.

61.4 Implications

The first result implies that the *contents* of polynomials, defined as the GCDs of their coefficients, are multiplicative: the content of the product of two polynomials is the product of their individual contents.

The second result implies that if a polynomial with integer coefficients can be factored over the rational numbers, then there exists a factorization over the integers. This property is also useful when combined with properties such

as Eisenstein's criterion.

Both results are essential in proving that if R is a unique factorization domain, then so is $R[X]$ (and by an immediate induction, so is the polynomial ring over R in any number of indeterminates). For any factorization of a polynomial P in $R[X]$, the statements imply that the product Q of all irreducible factors that are not contained in R (the non-constant factors) is always primitive, so $P = c(P)Q$ where $c(P)$ is the contents of P. This reduces proving uniqueness of factorizations to proving it individually for $c(P)$ (which is given) and for Q. By the second statement the irreducible factors in any factorization of Q in $R[X]$ are primitive representatives of irreducible factors in a factorization of Q in $F[X]$, but the latter is unique since $F[X]$ is a principal ideal domain and therefore a unique factorization domain.

The second result also implies that the minimal polynomial over the rational numbers of an algebraic integer has integer coefficients.

61.5 Notes

[1] Adapted from: R. Mines, F. Richman, W. Ruitenburg *A course in constructive algebra*, Universitext, Springer-Verlag, 1988

Chapter 62

Gauss–Lucas theorem

In complex analysis, a branch of mathematics, the **Gauss–Lucas theorem** gives a geometrical relation between the roots of a polynomial P and the roots of its derivative P'. The set of roots of a real or complex polynomial is a set of points in the complex plane. The theorem states that the roots of P' all lie within the convex hull of the roots of P, that is the smallest convex polygon containing the roots of P. When P has a single root then this convex hull is a single point and when the roots lie on a line then the convex hull is a segment of this line. The Gauss–Lucas theorem, named after Carl Friedrich Gauss and Félix Lucas is similar in spirit to Rolle's theorem.

62.1 Formal statement

If P is a (nonconstant) polynomial with complex coefficients, all zeros of P' belong to the convex hull of the set of zeros of P.[1]

62.2 Special cases

It is easy to see that if $P(x) = ax^2 + bx + c$ is a second degree polynomial, the zero of $P'(x) = 2ax + b$ is the average of the roots of P. In that case, the convex hull is the line segment with the two roots as endpoints and it is clear that the average of the roots is the middle point of the segment.

For a third degree complex polynomial P (cubic function) with three distinct zeros, Marden's theorem states that the zeros of P' are the foci of the Steiner inellipse which is the unique ellipse tangent to the midpoints of the triangle formed by the zeros of P.

For a fourth degree complex polynomial P (quartic function) with four distinct zeros forming a concave quadrilateral, the zeros of P' lie in two of the three triangles formed by the zeros of P. [2]

In addition, if a polynomial of degree n of real coefficients has n distinct real zeros $x_1 < x_2 < \cdots < x_n$, we see, using Rolle's theorem, that the zeros of the derivative polynomial are in the interval $[x_1, x_n]$ which is the convex hull of the set of roots.

The convex hull of the roots of the polynomial $p_n x^n + p_{n-1}x^{n-1} + \cdots p_0$ particularly includes the point $-\frac{p_{n-1}}{n \cdot p_n}$.

62.3 Proof

Over the complex numbers, P is a product of prime factors

$$P(z) = \alpha \prod_{i=1}^{n} (z - a_i)$$

where the complex numbers $a_1, a_2, \ldots, a_n$ are the – not necessary distinct – zeros of the polynomial P, the complex number α is the leading coefficient of P and n is the degree of P. Let z be any complex number for which $P(z) \neq 0$

. Then we have for the logarithmic derivative

$$\frac{P'(z)}{P(z)} = \sum_{i=1}^{n} \frac{1}{z - a_i}.$$

In particular, if z is a zero of P' and still $P(z) \neq 0$, then

$$\sum_{i=1}^{n} \frac{1}{z - a_i} = 0$$

or

$$\sum_{i=1}^{n} \frac{\overline{z} - \overline{a_i}}{|z - a_i|^2} = 0.$$

This may also be written as

$$\left(\sum_{i=1}^{n} \frac{1}{|z - a_i|^2} \right) \overline{z} = \left(\sum_{i=1}^{n} \frac{1}{|z - a_i|^2} \overline{a_i} \right).$$

Taking their conjugates, we see that z is a weighted sum with positive coefficients that sum to one, or the barycenter on affine coordinates, of the complex numbers a_i (with different mass assigned on each root whose weights collectively sum to 1).

If $P(z) = P'(z) = 0$, then $z = 1 \cdot z + 0 \cdot a_i$, and is still a convex combination of the roots of P .

62.4 See also

- Marden's theorem
- Bôcher's theorem
- Sendov's conjecture
- Rational root theorem
- Routh–Hurwitz theorem
- Hurwitz's theorem (complex analysis)
- Descartes' rule of signs
- Rouché's theorem
- Sturm's theorem
- Properties of polynomial roots
- Gauss's lemma (polynomial)
- Polynomial function theorems for zeros
- Content (algebra)

62.5 Notes

[1] Marden (1966), Theorem (6,1).

[2] A. Rüdinger (2014), http://arxiv.org/abs/1405.0689

62.6 References

- Morris Marden, *Geometry of Polynomials*, AMS, 1966.

62.7 External links

- Lucas–Gauss Theorem by Bruce Torrence, the Wolfram Demonstrations Project.

Chapter 63

Generalized Appell polynomials

In mathematics, a polynomial sequence $\{p_n(z)\}$ has a **generalized Appell representation** if the generating function for the polynomials takes on a certain form:

$$K(z,w) = A(w)\Psi(zg(w)) = \sum_{n=0}^{\infty} p_n(z)w^n$$

where the generating function or kernel $K(z,w)$ is composed of the series

$$A(w) = \sum_{n=0}^{\infty} a_n w^n \quad \text{with } a_0 \neq 0$$

and

$$\Psi(t) = \sum_{n=0}^{\infty} \Psi_n t^n \quad \text{and all } \Psi_n \neq 0$$

and

$$g(w) = \sum_{n=1}^{\infty} g_n w^n \quad \text{with } g_1 \neq 0.$$

Given the above, it is not hard to show that $p_n(z)$ is a polynomial of degree n .

Boas–Buck polynomials are a slightly more general class of polynomials.

63.1 Special cases

- The choice of $g(w) = w$ gives the class of Brenke polynomials.
- The choice of $\Psi(t) = e^t$ results in the Sheffer sequence of polynomials, which include the general difference polynomials, such as the Newton polynomials.
- The combined choice of $g(w) = w$ and $\Psi(t) = e^t$ gives the Appell sequence of polynomials.

63.2 Explicit representation

The generalized Appell polynomials have the explicit representation

$$p_n(z) = \sum_{k=0}^{n} z^k \Psi_k h_k.$$

The constant is

$$h_k = \sum_P a_{j_0} g_{j_1} g_{j_2} \cdots g_{j_k}$$

where this sum extends over all partitions of n into $k+1$ parts; that is, the sum extends over all $\{j\}$ such that

$$j_0 + j_1 + \cdots + j_k = n.$$

For the Appell polynomials, this becomes the formula

$$p_n(z) = \sum_{k=0}^{n} \frac{a_{n-k} z^k}{k!}.$$

63.3 Recursion relation

Equivalently, a necessary and sufficient condition that the kernel $K(z,w)$ can be written as $A(w)\Psi(zg(w))$ with $g_1 = 1$ is that

$$\frac{\partial K(z,w)}{\partial w} = c(w)K(z,w) + \frac{zb(w)}{w}\frac{\partial K(z,w)}{\partial z}$$

where $b(w)$ and $c(w)$ have the power series

$$b(w) = \frac{w}{g(w)}\frac{d}{dw}g(w) = 1 + \sum_{n=1}^{\infty} b_n w^n$$

and

$$c(w) = \frac{1}{A(w)}\frac{d}{dw}A(w) = \sum_{n=0}^{\infty} c_n w^n.$$

Substituting

$$K(z,w) = \sum_{n=0}^{\infty} p_n(z) w^n$$

immediately gives the recursion relation

$$z^{n+1}\frac{d}{dz}\left[\frac{p_n(z)}{z^n}\right] = -\sum_{k=0}^{n-1} c_{n-k-1} p_k(z) - z\sum_{k=1}^{n-1} b_{n-k}\frac{d}{dz}p_k(z).$$

For the special case of the Brenke polynomials, one has $g(w) = w$ and thus all of the $b_n = 0$, simplifying the recursion relation significantly.

63.4 See also

- q-difference polynomials

63.5 References

- Ralph P. Boas, Jr. and R. Creighton Buck, *Polynomial Expansions of Analytic Functions (Second Printing Corrected)*, (1964) Academic Press Inc., Publishers New York, Springer-Verlag, Berlin. Library of Congress Card Number 63-23263.
- William C. Brenke, *On generating functions of polynomial systems*, (1945) American Mathematical Monthly, **52** pp. 297–301.
- W. N. Huff, *The type of the polynomials generated by f(xt) φ(t)* (1947) Duke Mathematical Journal, **14** pp. 1091–1104.

Chapter 64

Gould polynomials

In mathematics the **Gould polynomials** *Gn*(*x*; *a*,*b*) are polynomials introduced by H. W. Gould and named by Roman in 1984.[1] They are given by [2]

$$\exp(xf(t)) = \sum_n G_n(x;a,b)t^n/n!$$

where

$$f(t) = \sum_{k\geq 1} \frac{1}{b}\binom{-(b+ak)/b}{k-1}\frac{t^k}{k!}$$

64.1 References

[1] Roman, Steven (1984), *The umbral calculus*, Pure and Applied Mathematics **111**, London: Academic Press Inc. Harcourt Brace Jovanovich Publishers, ISBN 978-0-12-594380-2, MR 741185, Reprinted by Dover, 2005

[2] Gould, H. W. (1961), "A series transformation for finding convolution identities", *Duke Math. J.* Volume 28, Number 2, 193-202.

Chapter 65

Grace–Walsh–Szegő theorem

In mathematics, the **Grace–Walsh–Szegő coincidence theorem**[1][2] is a result named after John Hilton Grace, Joseph L. Walsh, Gábor Szegő.

65.1 Statement

Suppose $f(z_1, ..., zn)$ is a polynomial with complex coefficients, and that it is

- symmetric, i.e. invariant under permutations of the variables, and
- multi-affine, i.e. affine in each variable separately.

Let A be any simply connected open set in the complex plane. If either A is convex or the degree of f is n, then for any $\zeta_1, \ldots, \zeta_n \in A$ there exists $\zeta \in A$ such that

$$f(\zeta_1, \ldots, \zeta_n) = f(\zeta, \ldots, \zeta).$$

65.2 Notes and references

[1] "A converse to the Grace–Walsh–Szegő theorem", *Mathematical Proceedings of the Cambridge Philosophical Society*, August 2009, 147(02):447–453. DOI:10.1017/S0305004109002424

[2] J. H. Grace, "The zeros of a polynomial", *Proceedings of the Cambridge Philosophical Society* 11 (1902), 352–357.

Chapter 66

List of polynomial topics

This is a **list of polynomial topics**, by Wikipedia page. See also trigonometric polynomial, list of algebraic geometry topics.

66.1 Terminology

- Degree: The maximum exponents among the monomials.
- Factor: An expression being multiplied.
- Linear factor: A factor of degree one.
- Coefficient: An expression multiplying one of the monomials of the polynomial.
- Root (or zero) of a polynomial: Given a polynomial p(x), the x values that satisfy p(x) = 0 are called roots (or zeroes) of the polynomial p.
- Graphing
  - End behaviour –
  - Concavity –
  - Orientation –
  - Tangency point –
  - Inflection point – Point where concavity changes.

66.2 Basics

- Polynomial
- Coefficient
- Monomial
- Polynomial long division
- Synthetic division
- Polynomial factorization
- Rational function
- Partial fraction

    - Partial fraction decomposition over R
- Vieta's formulas
- Integer-valued polynomial
- Algebraic equation
- Factor theorem
- Polynomial remainder theorem

66.2.1 Elementary abstract algebra

See also ***Theory of equations*** *below.*

- Polynomial ring
- Greatest common divisor of two polynomials
- Symmetric function
- Homogeneous polynomial
- Polynomial SOS (sum of squares)

66.3 Theory of equations

- Polynomial family
    - Quadratic function
    - Cubic function
    - Quartic function
    - Quintic function
    - Sextic function
    - Septic function
- Completing the square
- Abel–Ruffini theorem
- Bring radical
- Binomial theorem
- Blossom (functional)
- Root of a function
- *n*th root (radical)
    - Surd
    - Square root
    - Methods of computing square roots
    - Cube root
    - Root of unity
    - Constructible number
    - Complex conjugate root theorem

- Algebraic element
- Horner scheme
- Rational root theorem
- Gauss's lemma (polynomial)
- Irreducible polynomial
  - Eisenstein's criterion
  - Primitive polynomial
- Fundamental theorem of algebra
- Hurwitz polynomial
- Tschirnhaus transformation
- Galois theory
- Discriminant of a polynomial
  - Resultant
- Elimination theory
  - Gröbner basis
  - Regular chain
  - Triangular decomposition
- Sturm's theorem
- Descartes' rule of signs

66.4 Calculus with polynomials

- Delta operator
- Bernstein–Sato polynomial

66.5 Polynomial interpolation

- Lagrange polynomial
- Runge's phenomenon
- Spline (mathematics)

66.6 Weierstrass approximation theorem

- Bernstein polynomial

66.7 Linear algebra

- Characteristic polynomial
- Minimal polynomial
- Invariant polynomial

66.8 Named polynomials and polynomial sequences

- Abel polynomials
- Additive polynomials
- Appell sequence
- Askey–Wilson polynomials
- Bell polynomials
- Bernoulli polynomials
- Bernstein polynomial
- Bessel polynomials
- Binomial type
- Caloric polynomial
- Charlier polynomials
- Chebyshev polynomials
- Cyclotomic polynomials
- Ehrhart polynomial
- Exponential polynomials
- Favard's theorem
- Fibonacci polynomials
- Hahn polynomials
- Heat polynomial — see caloric polynomial
- Heckman–Opdam polynomials
- Hermite polynomials
- Kravchuk polynomials
- Laguerre polynomials
- Laurent polynomial
- Littlewood polynomial
- Legendre polynomials
    - Spherical harmonic
- Macdonald polynomials
- Meixner polynomials
- Newton polynomial
- Orthogonal polynomials
- Orthogonal polynomials on the unit circle
- Racah polynomials
- Rook polynomial

- Schur polynomials
- Sheffer sequence
- Touchard polynomials
- Wilkinson's polynomial
- Wilson polynomials
- Zernike polynomials

66.9 Knot polynomials

- Alexander polynomial
- HOMFLY polynomial
- Jones polynomial

66.10 Algorithms

- Karatsuba multiplication
- Lenstra–Lenstra–Lovász lattice basis reduction algorithm (for polynomial factorization)
- Lindsey–Fox algorithm
- Schönhage–Strassen algorithm

66.11 Text and image sources, contributors, and licenses

66.11.1 Text

- **Abel polynomials** *Source:* https://en.wikipedia.org/wiki/Abel_polynomials?oldid=623595158 *Contributors:* SimonP, Michael Hardy, Charles Matthews, Waltpohl, Jason Quinn, Marcos, Rich Farmbrough, C S, Oleg Alexandrov, YurikBot, Light current, SmackBot, Doctormatt, Hannes Eder, Vanish2, David Eppstein, LordAnubisBOT, Safemariner, Kiensvay, Addbot, Citation bot, Citation bot 1, R. J. Mathar, BG19bot and Anonymous: 1
- **Abel–Ruffini theorem** *Source:* https://en.wikipedia.org/wiki/Abel%E2%80%93Ruffini_theorem?oldid=663884746 *Contributors:* AxelBoldt, XJaM, Nealmcb, Michael Hardy, Dominus, Schneelocke, RodC, Charles Matthews, Dcoetzee, Fibonacci, Psychonaut, Marc Venot, Giftlite, Nsh, Tbjablin, Anythingyouwant, Icairns, Mh, Edudobay, Ben Standeven, Geschichte, Andrewpmk, Gene Nygaard, Oleg Alexandrov, Simetrical, Rjwilmsi, Salix alba, FlaBot, VKokielov, Roboto de Ajvol, YurikBot, RobotE, Dmharvey, Crasshopper, LamilLerran, RDBury, BeteNoir, Eskimbot, Nbarth, Colonies Chris, Javalenok, Zchenyu, Lambiam, BigDom, Mets501, Rlinfinity, CRGreathouse, Myasuda, Stormwyrm, Doctormatt, Paddles, JamesBWatson, Albmont, Kutu su~enwiki, Sue Gardner, Ttwo, Inquam, VolkovBot, Mike4ty4, Quantpole, EverGreg, Wing gundam, JackSchmidt, Cheesefondue, Thegeneralguy, He7d3r, Sandrobt, Marc van Leeuwen, MystBot, Addbot, Tide rolls, Arbitrarily0, Ettrig, Legobot, Luckas-bot, Yobot, TaBOT-zerem, AnomieBOT, VanishedUser sdu9aya9fasdsopa, IRP, Xqbot, Lunae, Swordsmankirby, Trappist the monk, Duoduoduo, WikitanvirBot, Slawekb, ZéroBot, Cf. Hay, Anita5192, Helpful Pixie Bot, Brad7777, Comfr, Nigellwh, Stamptrader, Boazka, Denziloe, Loraof, Boazkat and Anonymous: 51
- **Actuarial polynomials** *Source:* https://en.wikipedia.org/wiki/Actuarial_polynomials?oldid=450910129 *Contributors:* R.e.b. and Headbomb
- **Additive polynomial** *Source:* https://en.wikipedia.org/wiki/Additive_polynomial?oldid=659261624 *Contributors:* Michael Hardy, Evercat, Charles Matthews, Giftlite, Drbreznjev, Oleg Alexandrov, Linas, R.e.b., Crisco 1492, SmackBot, RDBury, Stootoon, LokiClock, Nusumareta, Quondum, Escspeed, Idonotwanttoknow and Anonymous: 5
- **Alexander polynomial** *Source:* https://en.wikipedia.org/wiki/Alexander_polynomial?oldid=660968921 *Contributors:* Michael Hardy, Zoicon5, Hyacinth, Giftlite, Oskar Sigvardsson, Gonzalo Diethelm, Bender235, C S, Dfeldmann, Rjwilmsi, R.e.b., Crasshopper, Orthografer, Pred, Keegan, Tesseran, Lambiam, Knotted, Smackbot, CmdrObot, Ranicki, Myasuda, Biblbroks, Headbomb, Turgidson, Pbroks13, Policron, Typometer, Rybu, S2000magician, Phyte, Alexbot, Sun Creator, Triathematician, Addbot, Frobitz, Tassedethe, Luckas-bot, Jim1138, Citation bot, Quebec99, SUL, Jonesey95, RjwilmsiBot, Enyokoyama, Rjasonparsley and Anonymous: 21
- **Algebraic equation** *Source:* https://en.wikipedia.org/wiki/Algebraic_equation?oldid=668906732 *Contributors:* Charles Matthews, Reilly, Pmanderson, Lectonar, WadeSimMiser, YurikBot, Smaines, Ethan Mitchell, SmackBot, RDBury, Jprg1966, Silly rabbit, SchfiftyThree, Tsca.bot, Cronholm144, Chetvorno, Thijs!bot, RobHar, Mathglot, Daniel5Ko, Policron, Uhai, Oshwah, WikiWonki222, SieBot, Toddst1, NuclearWarfare, Thingg, DumZiBoT, Addbot, Fluffernutter, LaaknorBot, Luckas-bot, Ciphers, Piano non troppo, Materialscientist, Xqbot, Isheden, Raulshc, Erik9bot, Louperibot, Prcnarhet arthas, Krassotkin, Duoduoduo, EmausBot, WikitanvirBot, D.Lazard, ClueBot NG, Wcherowi, Lokhinvar, Guy vandegrift, AvocatoBot, YFdyh-bot, Frosty, Bigdrt, Nigellwh, Ginsuloft, RC711, Loraof and Anonymous: 39
- **Algebraic variety** *Source:* https://en.wikipedia.org/wiki/Algebraic_variety?oldid=667996517 *Contributors:* AxelBoldt, Zundark, Paul Ebermann, Edward, Michael Hardy, TakuyaMurata, Karada, Loren Rosen, Charles Matthews, Dysprosia, Rvollmert, MathMartin, Giftlite, Mporter, Gene Ward Smith, Fropuff, Dratman, Waltpohl, Cambyses, Klemen Kocjancic, Nparikh, Gauge, Pt, Msh210, Jinhyun park, Eric Kvaalen, Linas, Pdn~enwiki, BD2412, Salix alba, Mathbot, YurikBot, Wavelength, KSmrq, Archelon, Crasshopper, Kompik, Orthografer, Kier07, KarlSchwede, SmackBot, RDBury, Eskimbot, Wikikris, Juliusross~enwiki, Michiexile, Lesnail, Vanished user 9i39j3, Titus III, JoeBot, CmdrObot, 345Kai, Thijs!bot, Andri Egilsson, GromXXVII, JamesBWatson, TomyDuby, Shiznick, Mistercupcake, VolkovBot, Camrn86, LokiClock, Marcosaedro, Hesam7, Arcfrk, AlleborgoBot, SieBot, ToePeu.bot, Iamthedeus, JackSchmidt, OKBot, Anchor Link Bot, Marsupilamov, Franklin.vp, Vanished user tj23rpoij4tikkd, Erodium, DumZiBoT, Dthomsen8, D.M. from Ukraine, Addbot, LaaknorBot, Luckas-bot, Yobot, AnomieBOT, Citation bot, Citation bot 1, ElNuevoEinstein, 777sms, EmausBot, John of Reading, WikitanvirBot, D.Lazard, Puffin, Anita5192, ClueBot NG, Uni.Liu, Teika kazura, IluvatarBot, Mark L MacDonald, Cerabot~enwiki, Jochen Burghardt, Mauricebench, Hamoudafg, Danneks, Monkbot, Diptaishik, KasparBot and Anonymous: 50
- **All one polynomial** *Source:* https://en.wikipedia.org/wiki/All_one_polynomial?oldid=637871756 *Contributors:* Oyd11, Charles Matthews, Robbot, Giftlite, CryptoDerk, Oleg Alexandrov, Hathawayc, RDBury, Vanish2, David Eppstein, GL1zdA, Addbot, Yobot, Spectral sequence, Jamesx12345 and Anonymous: 3
- **Almost linear hash function** *Source:* https://en.wikipedia.org/wiki/Almost_linear_hash_function?oldid=656184755 *Contributors:* Michael Hardy, Intgr, QuiteUnusual, Erel Segal and AManWithNoPlan
- **Alternating polynomial** *Source:* https://en.wikipedia.org/wiki/Alternating_polynomial?oldid=630333379 *Contributors:* AxelBoldt, Michael Hardy, Giftlite, Rich Farmbrough, Nbarth, Marc van Leeuwen, Thinking of England, RjwilmsiBot, ManiacParisien and Anonymous: 3
- **Angelescu polynomials** *Source:* https://en.wikipedia.org/wiki/Angelescu_polynomials?oldid=626764132 *Contributors:* R.e.b., Yobot and Trappist the monk
- **Appell sequence** *Source:* https://en.wikipedia.org/wiki/Appell_sequence?oldid=542564562 *Contributors:* Michael Hardy, Linas, Norm mit, David Eppstein, Policron, Anonymous Dissident, Addbot, Luckas-bot, Yobot, Citation bot, RjwilmsiBot, ZéroBot, Snotbot and Anonymous: 3
- **Bell polynomials** *Source:* https://en.wikipedia.org/wiki/Bell_polynomials?oldid=670565180 *Contributors:* SimonP, Michael Hardy, Docu, Giftlite, Gene Ward Smith, Rich Farmbrough, Dfeldmann, Blair Azzopardi, Stolee, GregorB, Mathbot, Maxal, Bluebot, Mhym, Druseltal2005, Cpastern, David Eppstein, Lantonov, AJRobbins, Addbot, DOI bot, Luckas-bot, Yobot, Ptbotgourou, Drilnoth, Charvest, Auclairde, MathFacts, Citation bot 1, PigFlu Oink, RjwilmsiBot, Mveil4483, ZéroBot, R. J. Mathar, Confluent, Manoguru, ChrisGualtieri, Deltahedron, Trompedo and Anonymous: 9
- **Bernoulli polynomials** *Source:* https://en.wikipedia.org/wiki/Bernoulli_polynomials?oldid=663252610 *Contributors:* Zundark, Michael Hardy, Dominus, Fredrik, Moink, Giftlite, Alberto da Calvairate~enwiki, MarkSweep, Lemontea, Bender235, ZeroOne, Eric Kvaalen, Oleg Alexandrov, Linas, Rjwilmsi, R.e.b., Mathbot, Michael Slone, SmackBot, Eskimbot, Silly rabbit, William Ackerman, Michael Ross, Druseltal2005, Francos, OMERZEN~enwiki, A. Pichler, CRGreathouse, Vyznev Xnebara, Thijs!bot, Headbomb, RobHar, Vanish2, Cuzkatzimhut, Xeno onex, LokiClock, SieBot, LeadSongDog, Alexbot, Jsondow, DumZiBoT, Kiensvay, Addbot, LaaknorBot, Haklo,

Lightbot, Wirkstoff, Luckas-bot, Kilom691, KamikazeBot, Citation bot, Citation bot 1, Trappist the monk, N4m3, Slawekb, ZéroBot, WilliamADon and Anonymous: 22

- **Bernstein polynomial** *Source:* https://en.wikipedia.org/wiki/Bernstein_polynomial?oldid=654087214 *Contributors:* Michael Hardy, Nixdorf, Meekohi, Med, Jitse Niesen, Phil Boswell, Robbot, Jaredwf, Peak, MathMartin, Giftlite, Andris, Peter M Gerdes, Tsirel, Ncik~enwiki, Forderud, Oleg Alexandrov, Linas, CyrilleDunant, R.e.b., FlaBot, Eubot, Japaget, YurikBot, Pmdboi, Zvika, RDBury, Tom Lougheed, Slaniel, DHN-bot~enwiki, AdamSmithee, Gala.martin, A. Pichler, James pic, Verdy p, Salgueiro~enwiki, JAnDbot, Magioladitis, MoA)gnome, Policron, Cobi, LokiClock, TXiKiBoT, Alexbot, 1ForTheMoney, MystBot, Addbot, SpBot, Yobot, Charvest, Tal physdancer, RedBot, Toolnut, 777sms, Ybungalobill, Johnnyaug, ChuispastonBot, Gareth Griffith-Jones, Vkn13, Deltahedron and Anonymous: 30
- **Bernstein–Sato polynomial** *Source:* https://en.wikipedia.org/wiki/Bernstein%E2%80%93Sato_polynomial?oldid=616702529 *Contributors:* Michael Hardy, Charles Matthews, Giftlite, Linas, Rjwilmsi, R.e.b., WriterHound, Nobs01, Deville, Headbomb, Turgidson, Jakob.scholbach, Robin S, Yobot, AnomieBOT, Unara, Citation bot, LilHelpa, Info21, Citation bot 1, Helpful Pixie Bot, EulerGauss2518833, Anrnusna and Anonymous: 7
- **Binomial** *Source:* https://en.wikipedia.org/wiki/Binomial?oldid=669471978 *Contributors:* Zundark, Tedernst, Michael Hardy, AugPi, Andres, Pollinator, Robbot, Cdang, Romanm, Jleedev, Giftlite, Pne, Bob.v.R, Icairns, Wroscel, Discospinster, Rich Farmbrough, Paul August, Shanes, Brim, Frodet, Wtmitchell, Mikeo, Blaxthos, Oleg Alexandrov, MFH, Gerbrant, Mathbot, Margosbot~enwiki, Shao, Fresheneesz, Michael Slone, Stephenb, Jatopian, Light current, SmackBot, RDBury, Maksim-e~enwiki, Ashenai, Federalist51, Gilliam, Skizzik, SchfiftyThree, Can't sleep, clown will eat me, OhioFred, Sayama, 16@r, Mets501, JForget, AntiVandalBot, Wayiran, Sterrys, Magioladitis, JNW, David Eppstein, Matyos1, Policron, Idioma-bot, Philip Trueman, TXiKiBoT, Anonymous Dissident, Aymatth2, Eleniel, Dogah, SieBot, Philomantis, Msrasnw, Denisarona, DEMcAdams, ClueBot, Arakunem, SoxBot III, Dark Mage, Mitch Ames, Addbot, Fieldday-sunday, MrOllie, MrVanBot, West.andrew.g, Tide rolls, Luckas-bot, Yobot, AnomieBOT, GB fan, Maddie!, GrouchoBot, RibotBOT, Dalegab, Erik9bot, LucienBOT, Mingcc, Pinethicket, Callanecc, Vrenator, Clarkcj12, EmausBot, ZéroBot, Derekleungtszhei, D.Lazard, Mr Molestah, ChuispastonBot, ClueBot NG, Movses-bot, Helpful Pixie Bot, LukeTurao, Mario Castelán Castro, Esquivalience and Anonymous: 100
- **Boas–Buck polynomials** *Source:* https://en.wikipedia.org/wiki/Boas%E2%80%93Buck_polynomials?oldid=575796953 *Contributors:* R.e.b., TexasAndroid, Headbomb, David Eppstein and Yobot
- **Bollobás–Riordan polynomial** *Source:* https://en.wikipedia.org/wiki/Bollob%C3%A1s%E2%80%93Riordan_polynomial?oldid=635684217 *Contributors:* Michael Hardy, Rjwilmsi, MZMcBride, R.e.b., Leutha, Headbomb, Faizhaider, Reedy Bot, Yobot, LilHelpa, BG19bot, FoCuSandLeArN, Brirush and Anonymous: 1
- **Bombieri norm** *Source:* https://en.wikipedia.org/wiki/Bombieri_norm?oldid=603849297 *Contributors:* Michael Hardy, Charles Matthews, Giftlite, Xezbeth, Pt, Shenme, Arthena, Rjwilmsi, Gaius Cornelius, Alaibot, Pbroks13, JackSchmidt, Raffalli, Sandrobt, Citation bot, Citation bot 1, Darij, Kiefer.Wolfowitz, Trappist the monk, RjwilmsiBot, Helpful Pixie Bot, Monkbot and Anonymous: 7
- **Boole polynomials** *Source:* https://en.wikipedia.org/wiki/Boole_polynomials?oldid=448803332 *Contributors:* R.e.b., Headbomb and Omnipaedista
- **Bracket polynomial** *Source:* https://en.wikipedia.org/wiki/Bracket_polynomial?oldid=607500646 *Contributors:* Michael Hardy, Charles Matthews, Hyacinth, Fropuff, ArnoldReinhold, Momotaro, C S, MarSch, BradBeattie, Stifle, Knotted, Horoball, Alexbot, Triathematician, Addbot, LaaknorBot, Qetuth, Mabulak and Anonymous: 5
- **Bring radical** *Source:* https://en.wikipedia.org/wiki/Bring_radical?oldid=663700319 *Contributors:* Michael Hardy, Zocky, Charles Matthews, Giftlite, Dissident, Pyrop, Lejean2000, C S, JW1805, Rjwilmsi, Salix alba, Fish and karate, RussBot, KSmrq, Wimt, Trovatore, Closedmouth, Lunch, SmackBot, Bluebot, Meni Rosenfeld, Kuru, Cronholm144, Robofish, Mets501, Ksoileau, Fear of ISMs, Stormwyrm, Ntsimp, Battery electric factory flat truck Resident Super Expert Elite, M910292, Headbomb, Nadav1, Rokhan, David Eppstein, Infovarius, Weston.pace, Addbot, Thoughtmeister, Tassedethe, Lightbot, Balabiot, Yobot, AnomieBOT, Citation bot, Wvitale, Citation bot 1, Double sharp, Trappist the monk, RjwilmsiBot, EmausBot, LucasBrown, D.Lazard, Snotbot, Helpful Pixie Bot, Itzuvit, Edisonabcd, Hmainsbot1, Ï¿½, Rmn pl, Footmath, Loraof and Anonymous: 41
- **Bézout matrix** *Source:* https://en.wikipedia.org/wiki/B%C3%A9zout_matrix?oldid=621229043 *Contributors:* Zundark, Charles Matthews, Jitse Niesen, LutzL, Gene Nygaard, Oleg Alexandrov, Pierremenard, Linas, Julien Tuerlinckx, BD2412, Rjwilmsi, R.e.b., Mlouns, DRLB, Headbomb, Cello3141, Qwfp, Addbot, Luckas-bot, Yobot, AnomieBOT and Anonymous: 3
- **Caloric polynomial** *Source:* https://en.wikipedia.org/wiki/Caloric_polynomial?oldid=553985040 *Contributors:* Michael Hardy, Daniele.tampieri, StAnselm, Jianluk91 and Anonymous: 1
- **Casus irreducibilis** *Source:* https://en.wikipedia.org/wiki/Casus_irreducibilis?oldid=669200053 *Contributors:* Michael Hardy, Charles Matthews, Gene Ward Smith, EmilJ, Oleg Alexandrov, Silly rabbit, Lambiam, Albmont, David Eppstein, Someone Roger, Addbot, Yobot, AnomieBOT, Citation bot, Norbirt, Citation bot 1, Duoduoduo, Helpful Pixie Bot, Benblumsmith, Itc editor and Anonymous: 5
- **Cavalieri's quadrature formula** *Source:* https://en.wikipedia.org/wiki/Cavalieri'{}s_quadrature_formula?oldid=605937527 *Contributors:* Michael Hardy, Chinju, Wavelength, Nbarth, Headbomb, R'n'B, SchreiberBike, Citation bot, JmCor, Khazar2, Monkbot and Anonymous: 10
- **Characteristic polynomial** *Source:* https://en.wikipedia.org/wiki/Characteristic_polynomial?oldid=671694001 *Contributors:* AxelBoldt, Zundark, Patrick, Michael Hardy, Suisui, Charles Matthews, Dysprosia, McKay, Aleph4, RedWolf, Tobias Bergemann, Giftlite, Mobius, CryptoDerk, Karol Langner, Jacob grace, CSTAR, Vivacissamamente, Shahab, Zaslav, Pt, Rgdboer, Obradovic Goran, Caesura, Oleg Alexandrov, Conskeptical, Catfive, BD2412, JYOuyang, Hadaso, Algebraist, YurikBot, Alex Bakharev, Crasshopper, SmackBot, Eskimbot, MalafayaBot, Nbarth, Colonies Chris, Mhym, Radagast83, Lhf, DDima, PhiJ, Inquisitus, CBM, Blindman shady, Magioladitis, Albmont, Email4mobile, Ortensia, Lantonov, Fylwind, Cuzkatzimhut, JohnBlackburne, Mggm1982, Wikiisawesome, Mongrel73, Michel.machado, Ivan Štambuk, Brech~enwiki, JackSchmidt, AlanUS, Yoda of Borg, ClueBot, OpenScience, Bender2k14, SchreiberBike, Aprock, Marc van Leeuwen, SilvonenBot, MystBot, Addbot, LarryJeff, Arbitrarily0, Luckas-bot, Yobot, Twri, Mr Sketchy, Undsoweiter, FrescoBot, Cdibuduo, Jujutacular, Dinamik-bot, RenamedUser01302013, Netheril96, Straightontillmorning, D.Lazard, ClueBot NG, Chester Markel, Dlituiev, Katherine Pendleton and Anonymous: 59
- **Coefficient** *Source:* https://en.wikipedia.org/wiki/Coefficient?oldid=672827553 *Contributors:* The Anome, Rade Kutil, Heron, Michael Hardy, Silverfish, Ffransoo, Charles Matthews, SchmuckyTheCat, Bkell, Hadal, Michael Snow, Tobias Bergemann, Marc Venot, Giftlite, Bovlb, Eequor, Mormegil, Discospinster, Paul August, Rgdboer, Sam Korn, Jumbuck, Msh210, Alansohn, Gene Nygaard, Crosbiesmith, WadeSimMiser, Magister Mathematicae, MarSch, Jameshfisher, Fresheneesz, TheGreyHats, Chobot, Roboto de Ajvol, YurikBot,

RobotE, Pip2andahalf, Michael Slone, GeeJo, Shreshth91, S.L.~enwiki, Nucleusboy, Mad Max, DavidHouse~enwiki, Bota47, Haemo, Spliffy, SmackBot, Maksim-e~enwiki, Skizzik, IMacWin95, Octahedron80, Sidious1701, Cybercobra, Decltype, Amtiss, Cronholm144, Mets501, Igoldste, Hynca-Hooley, Iokseng, ST47, Biblbroks, UberScienceNerd, Epbr123, Braveorca, Escarbot, AntiVandalBot, Oddity-, Res2216firestar, JAnDbot, Bongwarrior, A Hauptfleisch, Granburguesa, JaGa, Hdt83, MartinBot, Tgeairn, Pharaoh of the Wizards, Lantonov, Enuja, Jarry1250, Signalhead, VolkovBot, Someguy1221, Broadbot, Maxim, Dogah, Xanstarchild, Paolo.dL, JackSchmidt, Denisarona, ClueBot, Deviator13, Gene93k, Uncle Milty, Niceguyedc, UKoch, DragonBot, Excirial, CrazyChemGuy, Estirabot, Thingg, DumZiBoT, Hotcrocodile, Marc van Leeuwen, Stickee, Gggh, CalumH93, Addbot, Proofreader77, Atethnekos, Fgnievinski, Ronhjones, Wikimichael22, Fluffernutter, AndersBot, Tide rolls, דוד שי, Zorrobot, Legobot, Luckas-bot, Yobot, SwisterTwister, Tempodivalse, Ciphers, Speller26, IRP, Piano non troppo, Darolew, Materialscientist, E2eamon, Capricorn42, Renaissancee, Mgtrevisan, 33rogers, LucienBOT, Bkerkanator, I dream of horses, Uknighter, Vrenator, ی‌کی‌وی‌لی‌ع, Diannaa, DARTH SIDIOUS 2, EmausBot, WikitanvirBot, RA0808, Darkfight, ZéroBot, John Cline, Chharvey, D.Lazard, ChuispastonBot, ClueBot NG, Gareth Griffith-Jones, Wcherowi, Helpful Pixie Bot, DBigXray, Mark Arsten, Peru Serv, Gunn1t, Omulae, GoShow, Makecat-bot, Lugia2453, Frosty, Cmckain14, Neitiznot, Tango303, Hollylilholly, Graceracer525, Carlos881, MinnieBeachBum1382 and Anonymous: 196

- **Coefficient diagram method** *Source:* https://en.wikipedia.org/wiki/Coefficient_diagram_method?oldid=668548926 *Contributors:* Mdd, Oleg Alexandrov, Marudubshinki, Encyclops, Whitejay251, Dogears, Seh444, R'n'B, Yobot, Sci-cdm, Loraof and Anonymous: 5
- **Complex conjugate root theorem** *Source:* https://en.wikipedia.org/wiki/Complex_conjugate_root_theorem?oldid=607163243 *Contributors:* Michael Hardy, Giftlite, Pmanderson, Oleg Alexandrov, Woohookitty, Uncle G, Gaius Cornelius, Lunch, InverseHypercube, N Shar, EdJohnston, CharlotteWebb, Haseldon, Jmathews1t, Anonymous Dissident, Zwahls21, Geometry guy, SchreiberBike, Lhopitalified, Yobot, Quebec99, Jujutacular, Brad7777, Vanischenu, Ashvin narayanan and Anonymous: 12
- **Complex quadratic polynomial** *Source:* https://en.wikipedia.org/wiki/Complex_quadratic_polynomial?oldid=648048597 *Contributors:* Michael Hardy, Dcljr, Giftlite, Discospinster, Rich Farmbrough, El C, Mdd, GregorB, Bruce1ee, Daverocks, RussBot, Ospalh, SmackBot, Adam majewski, Myasuda, AndrewHowse, Doctormatt, Yrodro, Alaibot, David Eppstein, Philg88, KylieTastic, Funandtrvl, Fractalizator, Gpap.gpap, Mild Bill Hiccup, Addbot, Fgnievinski, Yobot, Yngvadottir, EmausBot, Fly by Night, Jimothylad, Helpful Pixie Bot, Raj8990kal, Jbomb1234, Brad7777, Prashant05me, ChrisGualtieri, Rishab021, KennyMagee and Anonymous: 13
- **Constant function** *Source:* https://en.wikipedia.org/wiki/Constant_function?oldid=656805803 *Contributors:* TakuyaMurata, Glenn, Jitse Niesen, David Shay, Saltine, Tobias Bergemann, Giftlite, Jason Quinn, Abdull, Mormegil, Paul August, Khakbaz, Oleg Alexandrov, Prophile, Dpv, Chobot, YurikBot, Kompik, Pred, SmackBot, Incnis Mrsi, PJTraill, Octahedron80, Gracenotes, CRGreathouse, AndrewHowse, Mhaitham.shammaa, JAnDbot, David Eppstein, JaGa, MartinBot, TheSeven, Austinmohr, VolkovBot, Caiguanhao, לירן, OKBot, ClueBot, Addbot, LaaknorBot, SpBot, Peti610botH, Xario, PV=nRT, Luckas-bot, Sz-iwbot, RibotBOT, Joxemai, Zero Thrust, RedBot, MondalorBot, Mz7, ZéroBot, Quondum, Lanthanum-138, Helpful Pixie Bot, Daviddwd, BG19bot, MusikAnimal, Lfahlberg, Makecat-bot, PC-XT, WillemienH and Anonymous: 26
- **Constant term** *Source:* https://en.wikipedia.org/wiki/Constant_term?oldid=607877610 *Contributors:* Andre Engels, Ixfd64, Giftlite, Horatio, TexasAndroid, SmackBot, Lambiam, Jim.belk, Happy-melon, Mhaitham.shammaa, JohnBlackburne, Dreamfall, Aitias, SoxBot III, Marc van Leeuwen, Dawynn, Fgnievinski, Wikimichael22, Tide rolls, Legobot, Math Champion, Isheden, Erik9bot, Techhead7890, EmausBot, ClueBot NG, Gilderien, Wiki13 and Anonymous: 15
- **Content (algebra)** *Source:* https://en.wikipedia.org/wiki/Content_(algebra)?oldid=667372231 *Contributors:* Joriki, A. Pichler, MyUsername, RobHar, Vanish2, JoergenB, J.delanoy, Nn123645, ClueBot, Pichpich, Addbot, RjwilmsiBot, D.Lazard, Monkbot and Anonymous: 4
- **Continuant (mathematics)** *Source:* https://en.wikipedia.org/wiki/Continuant_(mathematics)?oldid=647635282 *Contributors:* Michael Hardy, Giftlite, Maxal, Glenn L, Janmarthedal, Vanish2, Addbot, AnomieBOT, Qetuth, Deltahedron and Anonymous: 5
- **Cubic function** *Source:* https://en.wikipedia.org/wiki/Cubic_function?oldid=672590676 *Contributors:* Stevertigo, Michael Hardy, Dcljr, Strebe, AugPi, Charles Matthews, Dino, Jitse Niesen, Saltine, Frazzydee, Chuunen Baka, Donarreiskoffer, Robbot, Tosha, Jpo, Giftlite, BenFrantzDale, Nova77, Alberto da Calvairate~enwiki, Agro r, Kundor, Haham hanuka, LutzL, Lectonar, PAR, Oleg Alexandrov, 2004-12-29T22:45Z, Tabletop, Eatsaq, Koassim, Zzyzx11, Gisling, Graham87, MauriceJFox3, Rjwilmsi, Volfy, Mathbot, RexNL, Mark J, Wars, Fephisto, Scythe33, Turidoth, Krishnavedala, DVdm, Roboto de Ajvol, Wavelength, Eraserhead1, MathMan64, Biolinker, Airbete~enwiki, Mgnbar, Haihe, SamuelRiv, Arthur Rubin, Gesslein, Cmglee, AndrewWTaylor, SmackBot, Jagged 85, Nbarth, ACupOfCoffee, Tavianator, Lhf, Meni Rosenfeld, Titus III, Olin, Jim.belk, BillFlis, Newone, Jbolden1517, SkyWalker, Hacktivist, INVERTED, Myasuda, Ntsimp, MC10, Verdy p, Nein~enwiki, Hugozam, Headbomb, Bobblehead, BigJohnHenry, Seaphoto, Михајло Анђелковић, John.d.page, Mhaitham.shammaa, TK-925, Jrw@pobox.com, Lklundin, JAnDbot, Sangwinc, JamesBWatson, Pixel ;-), Anaxial, Glrx, R'n'B, Laurusnobilis, KIAaze, Policron, Heero Kirashami, Fylwind, Celtic Minstrel, VolkovBot, Pleasantville, Dmcq, SieBot, Ttony21, ClueBot, Admiral Norton, Binksternet, Mod.torrentrealm, Bobathon71, Justin W Smith, LizardJr8, Terets, Byafet, He7d3r, KyuubiSeal, Mprager, Kiensvay, N.Mori, YouRang?, Addbot, GardinerNeDay, חצרוני, CarsracBot, TStein, Lightbot, Kiril Simeonovski, Zorrobot, Martenjan, Zoho, Yobot, Roviury, Halothane, AnomieBOT, Murugesh108, GaussianV, ArthurBot, LilHelpa, Mthw2vc, RibotBOT, Seeleschneider, Gabiteodoru, Tubk02, Canned Soul, Geometryfan, Doraemonpaul, Tobby72, Aliotra, Sag2000, D'ohBot, HugoMeder, Citation bot 1, Wandering-teacher, Alidev, Jujutacular, Double sharp, Duoduoduo, Vmohanaraj, EmausBot, Skysmurf, Syncategoremata, Tommy2010, TeleComNasSprVen, ZéroBot, Knight1993, Jt6195, D.Lazard, Mathkt, Don hinson, Donner60, Scientific29, Michaelnikolaou, Adsmt, Nickalh50, Jrsanthosh, CharlieEchoTango, Kanidhappuli, Mikhail Ryazanov, ClueBot NG, Versatranitsonlywaytofly, Lanthanum-138, Rurik the Varangian, Dipan.pal.10, Helpful Pixie Bot, Kidd Varrow, ServiceAT, GKFX, CitationCleanerBot, Pokajanje, Frivolous Consultant, Rmehtany, ?????, Tentinator, Michaeljiz, Alexvong1995~enwiki, Zlk1214, BethNaught, Ruchira S Gamage, Duckfar, Loraof, Cohengar, User000name and Anonymous: 239
- **Cyclotomic polynomial** *Source:* https://en.wikipedia.org/wiki/Cyclotomic_polynomial?oldid=672438323 *Contributors:* AxelBoldt, Zundark, Michael Hardy, Oyd11, Tosha, Giftlite, Herbee, Elroch, EmilJ, Salix alba, HardDiet, Maxal, Glenn L, SmackBot, RDBury, Chris the speller, SMP, WAREL, LDH, Bruno321, CBM, Headbomb, RobHar, Magioladitis, JamesBWatson, David Eppstein, JoergenB, JadeNB, Acabre, Policron, DavidCBryant, VolkovBot, LokiClock, Tomaxer, Dmcq, JP.Martin-Flatin, Excirial, Watchduck, Marsupilamov, He7d3r, SchreiberBike, DumZiBoT, Virginia-American, Addbot, Fyrael, דניאל ב., Yobot, Charleswallingford, AnomieBOT, DemocraticLuntz, Citation bot, Anne Bauval, Lefschetz, Howard McCay, FrescoBot, Lunae, Aperisic, Alpenfrauchen, AvicBot, D.Lazard, Uni.Liu, Frietjes, Helpful Pixie Bot, Raoxiaojia, Justincheng12345-bot, Jag426, Stephan Alexander Spahn, Spectral sequence, Tristanhands, Jose Brox, DaedulusPromethean, K9re11, Cactus(uk) and Anonymous: 60
- **Degree of a polynomial** *Source:* https://en.wikipedia.org/wiki/Degree_of_a_polynomial?oldid=672615417 *Contributors:* Michael Hardy, DniQ, Charles Matthews, Gandalf61, Tobias Bergemann, Giftlite, BenFrantzDale, Leflyman, Jason Quinn, MacGyverMagic, Icairns,

Trevor MacInnis, Rich Farmbrough, Andros 1337, Mecanismo, Eric Shalov, El C, Oleg Alexandrov, Mindmatrix, Georgia guy, Mandarax, Algebraist, YurikBot, Hairy Dude, Grubber, Gaius Cornelius, 48v, Goffrie, CWenger, Bo Jacoby, SmackBot, Oli Filth, Octahedron80, Nbarth, AdamSmithee, Lambiam, Nat2, Cyberstrike2000x, GoCooL, Nhinchey, Blehfu, JForget, Rudjek, Daniel, Marek69, Smiddle, VoABot II, Usien6, CaptainP, Brandon Hixson, MartinBot, TomS TDotO, Jfsportz, Oleg Nitz, Tbone762, Alan012, Rekinser, Doug, Jugurtha3, Logan, StevenJohnston, SieBot, Ceroklis, SLMarcus, Smsarmad, Flyer22, Yerpo, OKBot, Denisarona, ClueBot, Bender2k14, SchreiberBike, Tarunsaxena, Marc van Leeuwen, Addbot, Download, Luckas-bot, Guy1890, AnomieBOT, Shadowjams, Dougofborg, FrescoBot, Pinethicket, Serols, Double sharp, Greatpopcorn, SaintNULL, Jowa fan, Techhead7890, DaveMudstain, Quondum, D.Lazard, Tolly4bolly, Card Zero, TYelliot, Gary Dee, ClueBot NG, KlappCK, Hypergraph, Lanthanum-138, Widr, MaximalIdeal, Sqzx, MusikAnimal, Kodiologist, ChrisGualtieri, Spencerleet, SassyLilNugget, Cadillac000, Kharkiv07, Nateowami, GeoffreyT2000, TuringMachine001, Lvance9174 and Anonymous: 127

- **Delta operator** *Source:* https://en.wikipedia.org/wiki/Delta_operator?oldid=607145000 *Contributors:* AxelBoldt, Tarquin, Patrick, Michael Hardy, Charles Matthews, Robbot, Oleg Alexandrov, Linas, Jeargle, AlainD, Jakob.scholbach, Daniele.tampieri, Tbone762, Marc van Leeuwen, Addbot, Luckas-bot, Yobot, Unara, SaschaWolff and Anonymous: 5
- **Denisyuk polynomials** *Source:* https://en.wikipedia.org/wiki/Denisyuk_polynomials?oldid=450913898 *Contributors:* R.e.b. and Headbomb
- **Derivation of the Routh array** *Source:* https://en.wikipedia.org/wiki/Derivation_of_the_Routh_array?oldid=671148042 *Contributors:* Michael Hardy, Giftlite, Mdd, Bgwhite, Dspradau, SmackBot, Zaxxonal, CRGreathouse, Phatom87, Alaibot, Magioladitis, Mreiki, Maralia, Sdrtirs, Yobot, AnomieBOT, LilHelpa, Locobot, SPKirsch, BG19bot and Anonymous: 8
- **Descartes' rule of signs** *Source:* https://en.wikipedia.org/wiki/Descartes'{}_rule_of_signs?oldid=667957539 *Contributors:* Michael Hardy, Charles Matthews, Chuunen Baka, Gandalf61, Auric, Magic Window, Tosha, Giftlite, Gazpacho, Bender235, Lou Crazy, Alansohn, Dzordzm, Adam Field, Chenxlee, Salix alba, Spacepotato, Alethiareg, Palladinus, DavidMcKenzie, Haihe, SmackBot, Sinblox, Jeekc, Silly rabbit, SashatoBot, Mets501, GNB, Blademasterx, A. Pichler, Reywas92, Mglg, Colin Rowat, Nishantsah, Jeepday, Lechatjaune, Geometry guy, ClueBot, Mild Bill Hiccup, Addbot, Pdebart, Tide rolls, PV=nRT, Fraggle81, Estudiarme, Vroo, Citation bot, JimVC3, Raffamaiden, Adavis444, FrescoBot, 777sms, Duoduoduo, Bento00, Alph Bot, Ripchip Bot, EmausBot, 478jjjz, Puffin, Gareth Griffith-Jones, Helpful Pixie Bot, FHGJ, Snstrand, Pratyya Ghosh, Deltahedron, Viewmont Viking, EFZR090440, Loraof, Metazoan-Marek, Thorthugnasty, User000name, Pj.spaenlehauer and Anonymous: 48
- **Dickson polynomial** *Source:* https://en.wikipedia.org/wiki/Dickson_polynomial?oldid=672065010 *Contributors:* Michael Hardy, Giftlite, Touriste, Darkoneko, Rjwilmsi, R.e.b., Arthur Rubin, SmackBot, Vanish2, David Eppstein, JackSchmidt, Yobot, Citation bot, Ting ganZ, Jonespoll, JonnyHallid, Etaittunpe, Citation bot 1, Xnn, RjwilmsiBot, John of Reading, R. J. Mathar, Wcherowi, Zieve, Helpful Pixie Bot, Deltahedron and Anonymous: 3
- **Difference polynomials** *Source:* https://en.wikipedia.org/wiki/Difference_polynomials?oldid=340989871 *Contributors:* Michael Hardy, Paul August, Linas, CBM, Adolphus79 and 1ForTheMoney
- **Discriminant** *Source:* https://en.wikipedia.org/wiki/Discriminant?oldid=672777882 *Contributors:* AxelBoldt, Zundark, Michael Hardy, Wshun, Den fjättrade ankan~enwiki, Charles Matthews, Dino, Dysprosia, Robbot, Jwpurple, Georg Muntingh, Tosha, Giftlite, BenFrantzDale, Calmofthestorm, Discospinster, Paul August, DcoetzeeBot~enwiki, Bender235, Gauge, Erik456, Gary, Trhaynes, Rodii, Mindmatrix, CyrilleDunant, Marudubshinki, Salix alba, FlaBot, Mathbot, McAusten, Petrvs~enwiki, Glenn L, Imnotminkus, King of Hearts, Chobot, Dylan Thurston, DVdm, Dmharvey, Gene.arboit, Michael Slone, Danuthaiduc, Sir48, Zephalis, Hirak 99, LarryLACa, SmackBot, Thunderboltz, Bluebot, Nbarth, Hdgcfcf, Akriasas, Coredesat, Asyndeton, Robertwb, Igoldste, Valoem, 345Kai, MaxEnt, Doctormatt, SpK, Thijs!bot, Pmagyar, Knakts, RobHar, Eleuther, Wang ty87916, Lklundin, 01001, VoABot II, Xiahou, VolkovBot, Hellohihihihi, Davidsevilla, Jobu0101, Anonymous Dissident, Arcfrk, SieBot, Dawn Bard, Cwkmail, Svick, The sunder king, DavidHobby, ClueBot, DionysosProteus, Southrop, Supertouch, Mild Bill Hiccup, Lexa122, Excirial, Alexbot, Estirabot, Alexey Muranov, Ncsinger, Qwfp, RMFan1, Gonfer, Deineka, Addbot, MrOllie, Sanawon, Tide rolls, Ajstern, Zorrobot, Luckas-bot, THEN WHO WAS PHONE?, Halothane, Naderra, AnomieBOT, Dans595, Unara, Materialscientist, DannyAsher, Xqbot, Σ, Jujutacular, Mean as custard, RjwilmsiBot, Rhythms06, Jowa fan, EmausBot, Tommy2010, TuHan-Bot, David2121~enwiki, Chharvey, Sbealing, D.Lazard, Electron0511, ClueBot NG, Chester Markel, Johnma97, Helpful Pixie Bot, MusikAnimal, Comfr, ChrisGualtieri, Deltahedron, SBareSSomErMig, Pokajanje, SucreRouge, Weux082690, Fowlslegs, GeoffreyT2000, Loraof, Jerry08baddog, Batman's butler and Anonymous: 122
- **Divided power structure** *Source:* https://en.wikipedia.org/wiki/Divided_power_structure?oldid=634640958 *Contributors:* Charles Matthews, Number 0, Mdd, GeeJo, SmackBot, Nbarth, RobHar, Fetchcomms, David Eppstein, Schepler, Sharlaon, Tide rolls, Cfranc, Keegscee, Deltahedron and Anonymous: 7
- **Division polynomials** *Source:* https://en.wikipedia.org/wiki/Division_polynomials?oldid=607146039 *Contributors:* Michael Hardy, Caramdir~enwiki, Giftlite, RussBot, JosephSilverman, JamesBWatson, Mild Bill Hiccup, Frobitz, Robert.Harker, PV=nRT, Yobot, Omnipaedista, Blugan, TLange, Isarra (HG) and Anonymous: 6
- **Ehrhart polynomial** *Source:* https://en.wikipedia.org/wiki/Ehrhart_polynomial?oldid=672075346 *Contributors:* AxelBoldt, Michael Hardy, Charles Matthews, McKay, Giftlite, Vanished user 1234567890, NickSchweitzer, Oleg Alexandrov, Rjwilmsi, Sango123, Masnevets, Dea13, SmackBot, Bluebot, Mattbeck, Akriasas, Headbomb, Paxinum, Turgidson, David Eppstein, Tomaxer, Arcfrk, JerroldPease-Atlanta, ClueBot, Dthomsen8, Addbot, Yobot, Citation bot, Twri, Flandre~enwiki, Helpful Pixie Bot, BG19bot, Enyokoyama, Alexcrussell, StevenCollazos, Monkbot, Alexander Craig Russell and Anonymous: 8
- **Eisenstein's criterion** *Source:* https://en.wikipedia.org/wiki/Eisenstein'{}s_criterion?oldid=657213897 *Contributors:* Michael Hardy, Revolver, Charles Matthews, Dysprosia, Ktotam, Marc Venot, Giftlite, Brequinda, Klemen Kocjancic, Gauge, El C, EmilJ, Obradovic Goran, Oleg Alexandrov, Stolee, Ryan Reich, Chenxlee, Rjwilmsi, YurikBot, Michael Slone, Danlaycock, Matikkapoika~enwiki, KnightRider~enwiki, Reedy, Melchoir, Lambiam, Valoem, Wafulz, Stebulus, Mon4, Thijs!bot, LaGrange, RobHar, WelcomeToDie, SpecZ, Albmont, Steve Checkoway, SieBot, AlphaPyro, PipepBot, Marc van Leeuwen, Addbot, Whyiseverythingused, Luckas-bot, Yobot, Calle, Anythingapplied, Cpryby, Duoduoduo, EmausBot, ZéroBot, D.Lazard, Nicelbole, Spectral sequence, Parkerf and Anonymous: 28
- **Equally spaced polynomial** *Source:* https://en.wikipedia.org/wiki/Equally_spaced_polynomial?oldid=662175323 *Contributors:* Charles Matthews, Giftlite, CryptoDerk, Phantomsteve, Geach, Vanish2, Mogism and Anonymous: 1
- **Equioscillation theorem** *Source:* https://en.wikipedia.org/wiki/Equioscillation_theorem?oldid=663181132 *Contributors:* Michael Hardy, Andrewman327, Bruguiea, Katharineamy, Nikthestunned, Ryan Vesey, Brad7777, Qetuth, EdvinW and Anonymous: 2
- **Exponential polynomial** *Source:* https://en.wikipedia.org/wiki/Exponential_polynomial?oldid=655156047 *Contributors:* Michael Hardy, Giftlite, Oleg Alexandrov, Chenxlee, Bhny, SmackBot, CBM, JaGa, Deltahedron and Anonymous: 1

- **External ray** *Source:* https://en.wikipedia.org/wiki/External_ray?oldid=672565621 *Contributors:* Michael Hardy, Schneelocke, Charles Matthews, Giftlite, Dfeldmann, Uncle G, Rjwilmsi, Malcolma, SmackBot, Adam majewski, Bluebot, Saganatsu, Lasserempe, JebJoya, David Eppstein, JaGa, Sfan00 IMG, Auntof6, Sun Creator, Yobot, FrescoBot, BattyBot, C.D. Tondela and Anonymous: 10
- **Faber polynomials** *Source:* https://en.wikipedia.org/wiki/Faber_polynomials?oldid=536981105 *Contributors:* Jftsang, R.e.b., Headbomb and Helpful Pixie Bot
- **Factor theorem** *Source:* https://en.wikipedia.org/wiki/Factor_theorem?oldid=660950746 *Contributors:* Michael Hardy, Barak~enwiki, Charles Matthews, Chuunen Baka, UtherSRG, Giftlite, Wronkiew, Discospinster, Rich Farmbrough, Tooto, Mairi, La goutte de pluie, Arthena, Bsadowski1, LOL, Mpatel, Jacj, Magister Mathematicae, MarSch, Celestianpower, Wknight94, SmackBot, BeteNoir, Iain.dalton, Fredvanner, David Radcliffe, Lambiam, Balrog30, AntiVandalBot, 28bytes, Geometry guy, Wikiisawesome, ClueBot, La Pianista, Qwfp, RMFan1, Kiensvay, Addbot, Static shock1994, Erik9bot, Kurosuke88, Ebony Jackson, S243a, Dashed, Ripchip Bot, Slawekb, ClueBot NG, Wcherowi, Helpful Pixie Bot, Brad7777, Lugia2453, Password12344, PeanutBuddhaJellyTime and Anonymous: 51
- **Factorization of polynomials** *Source:* https://en.wikipedia.org/wiki/Factorization_of_polynomials?oldid=672304279 *Contributors:* Bryan Derksen, Michael Hardy, Ciphergoth, Charles Matthews, Phil Boswell, Gene Ward Smith, Fintor, Masv~enwiki, J.Voss, Natalya, Wedesoft, Rjwilmsi, R.e.b., Grblpi, Ian Pitchford, YurikBot, Baccala@freesoft.org, SmackBot, Adam majewski, Tamfang, ArglebargleIV, MvH, Luke Maurits, JdH, CRGreathouse, Stubbscroll, Porqin, Loren.wilton, ClueBot, Bender2k14, Addbot, Legobot, Drpickem, Luckas-bot, Yobot, Becky Sayles, AnomieBOT, RandomAct, Citation bot, TLange, Kiefer.Wolfowitz, Duoduoduo, RjwilmsiBot, D.Lazard, EdoBot, ClueBot NG, Dipdapdingy, CitationCleanerBot, Deltahedron, Mogism, 2Powers, Monkbot, Mario Castelán Castro, Loraof, Davidparks21 and Anonymous: 47
- **Factorization of polynomials over finite fields** *Source:* https://en.wikipedia.org/wiki/Factorization_of_polynomials_over_finite_fields?oldid=671097723 *Contributors:* Michael Hardy, Bearcat, Tobias Bergemann, MathKnight, Hydrox, Pontus, Sperril, Walkie, Efnar, MvH, Headbomb, Asmeurer, JoergenB, R'n'B, Demokratickid, JL-Bot, Jan1nad, Mild Bill Hiccup, Arjayay, Rcampbell1, Marc van Leeuwen, Jncraton, Yobot, DutchCanadian, AnomieBOT, LilHelpa, Stbuehler, FrescoBot, TLange, Sławomir Biały, Masahiro Sakai, John of Reading, D.Lazard, SilentBobxy2, Crypto2010, AALProject2010, Amdeberhan, Joechem77, Helpful Pixie Bot, Zieglerk, Teddyktchan and Anonymous: 23
- **Fekete polynomial** *Source:* https://en.wikipedia.org/wiki/Fekete_polynomial?oldid=658837541 *Contributors:* Michael Hardy, Charles Matthews, Jitse Niesen, Giftlite, Jgbustos, SmackBot, Vyznev Xnebara, Vanish2, GirasoleDE, Addbot, Lightbot, דוד ש, Kilom691 and Anonymous: 4
- **Fibonacci polynomials** *Source:* https://en.wikipedia.org/wiki/Fibonacci_polynomials?oldid=604226493 *Contributors:* SimonP, Michael Hardy, Charles Matthews, Gandalf61, Herbee, Wwoods, Vsmith, Oleg Alexandrov, Jb-adder, Maxal, YurikBot, Laurentius, SmackBot, RDBury, Vanish2, Kateshortforbob, J.delanoy, Excirial, Murdernacho, Addbot, Kilom691, Citation bot, GrouchoBot, Merak2007, RjwilmsiBot, ZéroBot, R. J. Mathar, E4master, Helpful Pixie Bot, SoylentPurple, Qetuth, Kleanupguy11, ChrisGualtieri, K9re11 and Anonymous: 8
- **Gauss's lemma (polynomial)** *Source:* https://en.wikipedia.org/wiki/Gauss'{}s_lemma_(polynomial)?oldid=667372077 *Contributors:* Zundark, Michael Hardy, Charles Matthews, Giftlite, 3mta3, Blahma, Oleg Alexandrov, Joriki, Simetrical, BillC, Lockley, Mathbot, Salvatore Ingala, Thesm, Algebraist, RussBot, FF2010, Nicholas Jackson, SmackBot, Chris the speller, JCSantos, SMP, Lhf, CRGreathouse, Dcravenel, Hardmath, Asmeurer, Magioladitis, Albmont, Johnbibby, GermanX, Gentlemath, Plclark, Shuhab, Marc van Leeuwen, Virginia-American, Addbot, Opa, Mdg583, TaBOT-zerem, Andreesakia, Point-set topologist, Rghthndsd, Erik9bot, DrilBot, MastiBot, Anikbak, GoingBatty, D.Lazard, ClueBot NG, O.Koslowski, Kappaenne and Anonymous: 20
- **Gauss–Lucas theorem** *Source:* https://en.wikipedia.org/wiki/Gauss%E2%80%93Lucas_theorem?oldid=636166541 *Contributors:* Michael Hardy, Charles Matthews, Giftlite, Pmanderson, EmilJ, Woohookitty, Linas, Sodin, Chobot, Zvika, RDBury, Twas Now, A. Pichler, Pascal.Tesson, Thijs!bot, Escarbot, JaGa, Haseldon, Pleasantville, M.schwed, Sidawang, Addbot, Luckas-bot, Yobot, Anne Bauval, Jujutacular, Jowa fan, EmausBot, HiW-Bot, ZéroBot, Brad7777 and Anonymous: 12
- **Generalized Appell polynomials** *Source:* https://en.wikipedia.org/wiki/Generalized_Appell_polynomials?oldid=544095145 *Contributors:* Michael Hardy, Icairns, Linas, R.e.b., Harryboyles, Trassiorf, OrenBochman, Svick, SchreiberBike and Addbot
- **Gould polynomials** *Source:* https://en.wikipedia.org/wiki/Gould_polynomials?oldid=483515384 *Contributors:* R.e.b., Headbomb, Katharineamy, Omnipaedista and DoctorKubla
- **Grace–Walsh–Szegő theorem** *Source:* https://en.wikipedia.org/wiki/Grace%E2%80%93Walsh%E2%80%93Szeg%C5%91_theorem?oldid=618164131 *Contributors:* Michael Hardy, David Eppstein, Yobot and K9re11
- **List of polynomial topics** *Source:* https://en.wikipedia.org/wiki/List_of_polynomial_topics?oldid=654049846 *Contributors:* Michael Hardy, Charles Matthews, Dysprosia, Jaredwf, MathMartin, Marc Venot, Giftlite, Brockert, Reilly, D6, ZeroOne, Calair, Aranel, Spalding, 3mta3, Oleg Alexandrov, BD2412, Chenxlee, Salix alba, R.e.b., Mathbot, Hillman, Baccala@freesoft.org, RDBury, Fplay, Silly rabbit, DRLB, Lambiam, Vanished user 9i39j3, Syrcatbot, Paddles, Thijs!bot, The Transhumanist, Absolutely Insane, Smcinerney, Barraki, Larry R. Holmgren, Kimble9t, Good Olfactory, Addbot, Gchesi, Verbal, Jujutacular, Gamewizard71, M.Moreno-Maza, Danparrish and Anonymous: 12

66.11.2 Images

- **File:6furcation.gif** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/4e/6furcation.gif *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Adam majewski
- **File:Ambox_important.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/b4/Ambox_important.svg *License:* Public domain *Contributors:* Own work, based off of Image:Ambox scales.svg *Original artist:* Dsmurat (talk · contribs)
- **File:Bernoulli_polynomials.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/67/Bernoulli_polynomials.svg *License:* CC-BY-SA-3.0 *Contributors:* Transferred from en.wikipedia to Commons. *Original artist:* The original uploader was Linas at English Wikipedia
- **File:Bernstein_Approximation.gif** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a6/Bernstein_Approximation.gif *License:* Public domain *Contributors:* Transferred from en.wikipedia; transferred to Commons by User:Georg-Johann using CommonsHelper. *Original artist:* Original uploader was James pic at en.wikipedia

- **File:BinomialTheorem.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/0f/BinomialTheorem.png *License:* Public domain *Contributors:* Danilo Guanabara Fernandes *Original artist:* Danilo Guanabara Fernandes
- **File:Blue_6_2_Knot.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/bc/Blue_6_2_Knot.png *License:* Public domain *Contributors:* Own work *Original artist:* Jim.belk
- **File:Commons-logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/4a/Commons-logo.svg *License:* ? *Contributors:* ? *Original artist:* ?
- **File:Cot(theta).svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f9/Cot%28theta%29.svg *License:* Public domain *Contributors:*
- -cot(theta).jpg *Original artist:*
- derivative work: Phatom87 (talk)
- **File:Cr_orbit_3.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/ff/Cr_orbit_3.png *License:* CC BY-SA 3.0 *Contributors:* This graphic was created with gnuplot. *Original artist:* Adam majewski
- **File:Critical_orbit_3d.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/07/Critical_orbit_3d.png *License:* CC BY-SA 3.0 *Contributors:* Own work by uploader in Maxima and Gnuplot *Original artist:* Adam majewski
- **File:Cubic_graph_special_points.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d4/Cubic_graph_special_points.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Cmglee
- **File:Discriminant_of_cubic_polynomials..png** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/81/Discriminant_of_cubic_polynomials..png *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Salix alba
- **File:Edit-clear.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/f/f2/Edit-clear.svg *License:* Public domain *Contributors:* The *Tango! Desktop Project*. *Original artist:*
  The people from the Tango! project. And according to the meta-data in the file, specifically: “Andreas Nilsson, and Jakub Steiner (although minimally).”
- **File:Elliptic_curve2.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/0c/Elliptic_curve2.png *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Oscarpettersson
- **File:Erays.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f8/Erays.png *License:* CC BY-SA 3.0 *Contributors:* Own work by uploader in Maxima and Gnuplot with help of many people (see references) *Original artist:* Adam majewski
- **File:Exponential_Parameter_Space_Detail_PSP_Rays.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/39/Exponential_Parameter_Space_Detail_PSP_Rays.png *License:* Public domain *Contributors:* Own work *Original artist:* L rempe - Dr. L. Rempe
- **File:Folder_Hexagonal_Icon.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/48/Folder_Hexagonal_Icon.svg *License:* Cc-by-sa-3.0 *Contributors:* ? *Original artist:* ?
- **File:Graph_of_cubic_polynomial.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/15/Graph_of_cubic_polynomial.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Krishnavedala
- **File:Graphical_interpretation_of_the_complex_roots_of_cubic_equation.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/ae/Graphical_interpretation_of_the_complex_roots_of_cubic_equation.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Olin
- **File:Iray.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/b5/Iray.png *License:* CC BY-SA 3.0 *Contributors:* Own work by uploader in Maxima and Gnuplot with help of many people (see references) *Original artist:* Adam majewski
- **File:Jung200.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/35/Jung200.png *License:* CC BY-SA 3.0 *Contributors:* Own work : translation of maple code by G. A. Edgar; Help : G. A. Edgar and Richard J. Fateman, Robert P. Munafo and Richard J. Fateman.[#cite_note-1 [1]] See also : Bifurcation of Dynamic Rays in Complex Polynomials of Degree Two, Atela, P., Ergod Th & Dynam Sys (1991) 12, 401-423 *Original artist:* Adam majewski
- **File:Jung50e.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/60/Jung50e.png *License:* CC BY-SA 3.0 *Contributors:* Own work with help of : Richard J. Fateman and G. A. Edgar *Original artist:* Adam majewski
- **File:Kauffman_bracket2.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/13/Kauffman_bracket2.png *License:* CC-BY-SA-3.0 *Contributors:* Transferred from en.wikipedia; transferred to Commons by User:Serguei S. Dukachev using CommonsHelper. *Original artist:* Original uploader was Horoball at en.wikipedia
- **File:Lebesgue_Icon.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/c9/Lebesgue_Icon.svg *License:* Public domain *Contributors:* w:Image:Lebesgue_Icon.svg *Original artist:* w:User:James pic
- **File:MandelbrotLambda.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/04/MandelbrotLambda.jpg *License:* Public domain *Contributors:* I created this image entirely by myself. *Original artist:* JDSperling (talk)
- **File:Miimcr.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/2e/Miimcr.png *License:* GFDL *Contributors:* self-made, below *Original artist:* Adam majewski
- **File:Niccolò_Tartaglia.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/0b/Niccol%C3%B2_Tartaglia.jpg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Nuvola_apps_edu_mathematics_blue-p.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/3e/Nuvola_apps_edu_mathematics_blue-p.svg *License:* GPL *Contributors:* Derivative work from Image:Nuvola apps edu mathematics.png and Image:Nuvola apps edu mathematics-p.svg *Original artist:* David Vignoni (original icon); Flamurai (SVG convertion); bayo (color)
- **File:OEISicon_light.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d8/OEISicon_light.svg *License:* Public domain *Contributors:* Own work *Original artist:* Watchduck (a.k.a. Tilman Piesk)
- **File:Omar_Kayyám_-_Geometric_solution_to_cubic_equation.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/5e/Omar_Kayy%C3%A1m_-_Geometric_solution_to_cubic_equation.svg *License:* Public domain *Contributors:* Own work *Original artist:* Pieter Kuiper

- **File:Parabolic_Segment.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/be/Parabolic_Segment.svg *License:* Public domain *Contributors:* http://en.wikipedia.org/wiki/Image:Parabolic_Segment.png *Original artist:* en:User:Jim.belk (original); Pbroks13 (talk) (redraw)
- **File:PascalTriangleFibanacci.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/bf/PascalTriangleFibanacci.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* RDBury
- **File:Polynome_de_fekete_43.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/ab/Polynome_de_fekete_43.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Kilom691
- **File:Polynomialdeg3.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a3/Polynomialdeg3.svg *License:* Public domain *Contributors:* Polynomialdeg3.png *Original artist:* N.Mori
- **File:Quartic_Discriminant.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/2b/Quartic_Discriminant.png *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Salix alba
- **File:Question_book-new.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/9/99/Question_book-new.svg *License:* Cc-by-sa-3.0 *Contributors:*
  Created from scratch in Adobe Illustrator. Based on Image:Question book.png created by User:Equazcion *Original artist:* Tkgd2007
- **File:Rubik'{}s_cube_v3.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/b6/Rubik%27s_cube_v3.svg *License:* CC-BY-SA-3.0 *Contributors:* Image:Rubik'{}s cube v2.svg *Original artist:* User:Booyabazooka, User:Meph666 modified by User:Niabot
- **File:Second_dilate_of_a_unit_square.png** *Source:* https://upload.wikimedia.org/wikipedia/en/1/14/Second_dilate_of_a_unit_square.png *License:* CC-BY-SA-3.0 *Contributors:*
  I used http://www.quickmath.com/webMathematica3/quickmath/graphs/inequalities/advanced.jsp#c=plot_advancedgraphinequalities&v1=3x+%2B+4y+%3C%3D+20000&v2=3x+%2B+2y+%3C%3D+4000&v3=x+%3E%3D+0&v4=y+%3E%3D+0&v7=x&v8=y&v9=0&v10=2000&v11=0&v12=4000&v13=forest-green&v14=purple&v15=forest-green&v16=dark-turquoise and Paint. *Original artist:* StevenCollazos
- **File:Skein_(HOMFLY).svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/c3/Skein_%28HOMFLY%29.svg *License:* Public domain *Contributors:*
- Skein_(HOMFLY).png *Original artist:*
- derivative work: Pbroks13 (talk)
- **File:Tan(theta).jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/38/Tan%28theta%29.jpg *License:* Public domain *Contributors:* Transferred from en.wikipedia to Commons by Phatom87 using CommonsHelper. *Original artist:* Zaxxonal at English Wikipedia
- **File:Text_document_with_red_question_mark.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a4/Text_document_with_red_question_mark.svg *License:* Public domain *Contributors:* Created by bdesham with Inkscape; based upon Text-x-generic.svg from the Tango project. *Original artist:* Benjamin D. Esham (bdesham)
- **File:Translation_to_english_arrow.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/8a/Translation_to_english_arrow.svg *License:* CC-BY-SA-3.0 *Contributors:* Transferred from en.wikipedia; transferred to Commons by User:Faigl.ladislav using CommonsHelper. *Original artist:* tkgd2007. Original uploader was Tkgd2007 at en.wikipedia
- **File:Trigonometric_interpretation_of_a_cubic_equation_with_three_real_roots.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/07/Trigonometric_interpretation_of_a_cubic_equation_with_three_real_roots.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Olin
- **File:Twisted_cubic_curve.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/89/Twisted_cubic_curve.png *License:* CC BY 3.0 *Contributors:* Own work *Original artist:* Claudio Rocchini
- **File:Wiki_constant_function_175_200.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d3/Wiki_constant_function_175_200.png *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Lfahlberg
- **File:Wiki_letter_w.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/6/6c/Wiki_letter_w.svg *License:* Cc-by-sa-3.0 *Contributors:* ? *Original artist:* ?
- **File:Wiki_letter_w_cropped.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1c/Wiki_letter_w_cropped.svg *License:* CC-BY-SA-3.0 *Contributors:*
- Wiki_letter_w.svg *Original artist:* Wiki_letter_w.svg: Jarkko Piiroinen
- **File:Wikibooks-logo-en-noslogan.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/df/Wikibooks-logo-en-noslogan.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* User:Bastique, User:Ramac et al.
- **File:Wikibooks-logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikibooks-logo.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* User:Bastique, User:Ramac et al.
- **File:Wikinews-logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/24/Wikinews-logo.svg *License:* CC BY-SA 3.0 *Contributors:* This is a cropped version of Image:Wikinews-logo-en.png. *Original artist:* Vectorized by Simon 01:05, 2 August 2006 (UTC) Updated by Time3000 17 April 2007 to use official Wikinews colours and appear correctly on dark backgrounds. Originally uploaded by Simon.
- **File:Wikiquote-logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikiquote-logo.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Wikisource-logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/4c/Wikisource-logo.svg *License:* CC BY-SA 3.0 *Contributors:* Rei-artur *Original artist:* Nicholas Moreau
- **File:Wikiversity-logo-Snorky.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1b/Wikiversity-logo-en.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Snorky
- **File:Wiktionary-logo-en.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f8/Wiktionary-logo-en.svg *License:* Public domain *Contributors:* Vector version of Image:Wiktionary-logo-en.png. *Original artist:* Vectorized by Fvasconcellos (talk · contribs), based on original logo tossed together by Brion Vibber
- **File:X_cubed_plot.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/94/X_cubed_plot.svg *License:* CC-BY-SA-3.0 *Contributors:* Original version self-made using gnuplot. Present version HandSVG *Original artist:* Qualc1

66.11.3 Content license

- Creative Commons Attribution-Share Alike 3.0