

Index

- Algebraic independence of automorphisms, 92
 Analytic root functions, 68
 Anti-symmetrisation, 241, 246
 Arithmetic lifting property, 76
 Artin symbol, 181
- Beckmann-Black Conjecture, 76
 Belyi's Theorem, 5
 Bilinear form, 211
 Binary form, 27, **217**
 Transformation of, 218
 Black, 157
 Bracket, 222
 Bracket invariants, 224
 of the binary quadratic, 225
 of the binary cubic, 225
 of the binary quartic, 225
 of the binary quintic, 226
 Bracket polynomial, 222
 Brauer type embedding problem, 134, 208
 Bring-Jerrard trinomials, 42
 Brumer's Theorem, 9, 45
 Bucht's Parametrisation, 135
 Buhler, 46
 Buhler and Reichstein, 12, 190, 196
 Burnside, 169
 Burnside's Theorem, 7
- Castelnuovo's Theorem, 6
 Center of algebra, 233
 Character (linear), 220
 Chebyshev polynomial, 179
 Class number, 181
 Commutator of subalgebra, 233
 Completely reducible module, 231
 $C_{p^2} \rtimes C_p$, 128
 Crossed homomorphism, 94
 Additive, 209
 Cubic resolvent, 31
 Cyclic algebra, 166
 Cyclic group of order eight, 56
 as Galois group, 152ff
- Decomposition group, 71
 Dedekind Independence Theorem, 86, 92
 Dedekind's Q_8 -extension, 138
 Dedekind's Theorem, 73
 DeMeyer, 101
 Density Theorem, 232
 Descent-generic polynomial, 21
 Dessins d'enfants, 16
 Diagonal action of group, 220
 Dihedral group, 109
 as Galois group, 170
 of 2-power degree, 127
 Discriminant,
 of binary form, 222
 of trinomial, 26, 80
 Dual space, 18
 Duality, 86
- Embedding along an epimorphism, 207
 Embedding problem, 207
 Epimorphism, 207
 Central, 207
 Non-split, 207
 Equivariant of group action, 220
 Essential dimension, 12, **190ff**
 of abelian groups, 199
 of algebraic group, 196
 of A_n , 194
 of C_7 , 196
 of C_p^n , 12, **194**
 of D_{15} and D_{21} , 205
 of dihedral groups, 199
 of groups of degree up to five, 190
 of H_{p^3} , 205
 of M_2^n , 205
 of p -groups in char. p , 201
 of Q_{2^n} , 204
 of semi-direct products, 196
 of S_n , 194
 Étale algebra, 88
- Factor system, 209
 Faddeyev's Theorem, 139
 Fano plane, 52

- Feit, 175
- First cohomology group, 94
- First Fundamental Theorem, 228
Version two, 229
Version three, 230
Proof, 242–243
- Fractional linear transformation, 219
- Frattni group, 91
- Frobenius group, 169
as Galois group, 175ff
- Furtwängler's Theorem, 7
- G -extension, 1
- $\text{Gal}(-/K)$, *see* Galois group
- Galois algebra, 90ff
- Galois extension, 1
of commutative rings, 85ff
- Galois group, 1
- Galois homomorphism, 95
- Galois theory,
Existence problem of, 1
Inverse problem of, 1
of commutative rings, 83ff
Regular inverse problem of, 3, 76
- Galois' Lemma, 169
- Gaschütz, 117
- Gauss, 182
- General polynomial
for semi-direct product, 174
- Generic dimension, 201ff
of some cyclic groups, 205
- Generic extension, 96
for C_2 , 96
for C_3 , 96
for C_n (n odd), 102ff
for C_p in char. p , 96
for D_q (q prime power), 109ff
for p -group in char. p , 120
for S_n , 98
for wreath product, 173–174
- Generic polynomial, 1
for A_4 , 37, 61
for A_5 , 47
for $C_2 \wr S_n$, 124
for C_3 , 30, 103
for $C_3 \rtimes C_4$, 60
for $C_3 \rtimes Q_8$, 205
for C_4 , 34, 60
for C_5 , 44
for C_7 , 199
for C_9 , C_{11} and C_{13} , 205
for C_n (n odd), 103, 125
over \mathbb{Q} , 104–105
for $C_{p^2} \rtimes C_p$, 167
for C_{p^n} in char. p , 121
for D_{15} and D_{21} , 205
for D_{2^n} in char. two, 123
for D_3 , 111, 117, 125
for $D_{3 \times 3}$, 125
for D_4 , 35, 60
in char. two, 123
for D_5 , 45
for D_5 (over $\mathbb{Q}(\sqrt{5})$), 117
for D_6 , 60
for D_8 , 159
for D_n ($16 \nmid n$), 112
for D_q (q prime power), 111
for F_{20} , 46
for F_{pd} in char. p , 122
for $F_{p\ell}$, 175
for $\text{GL}(n, q)$ in char. p , 19
for H_{27} , 165
for H_{p^3} , 164
for p -group in char. p , 117ff
for Q_8 , 140
for QC , 145
for QD_8 , 150
for S_3 (*see also* D_3), 30
for S_4 , 38
for S_5 , 48
for S_6 , 51
for S_n , 195
for V_4 , 33, 60
for wreath product, 173
non-existence for C_8 , 56
- Geyer and Jensen, 160
- Gröbner's Theorem, 7, 141
- Gross and Zagier, 183
- Group ring, 17
- Groups of degree three, 30
- Groups of degree four, 31
- Groups of degree five, 38
- Groups of degree six, 50
- Groups of degree seven, 51
- Groups of degree eight to ten, 56
- Groups of degree eleven, 57
- Grunwald-Wang, 105
- Hamiltonian quaternions, 127, 132
- Harbater Existence Theorem, 2
- Hashimoto and Miyake, 113ff
- Heisenberg group, 128
- Hermite's Theorem, 48
- Hilbert class field, 181
- Hilbert Class Field Theory, 181ff
- Hilbert Irreducibility Theorem, 63, **70**
- Hilbert Ninety, 91, 94
Additive, 209
for Witt vectors, 120
for Witt vectors, 120

- Hilbert Nullstellensatz, 214
 Hilbert set, 64
 Hilbert's Theorem, 78
 Hilbertian field, 63
 Homogeneous coordinates, 219
 Homogeneous element, 22
 Degree of, 22
- Ideal class group, 181
 Ikeda's Theorem, 108
 Induced algebra, 89
 Inertia group, 72
 Inner product, 246
 Invariant basis, 21
 Invariant Basis Lemma, 21, 93
 Invariant of binary form, 220
 Invariant of group action, 220
 I_{RM} , 84
 Irreducible component, 233
 Irreducible module, 231
- Jordan's Theorem, 58
 Joubert, 51
- $K[G]$, *see* Group ring
 $K[V]$ (commutative tensor algebra), 18
 $K(V)$ (quotient field of $K[V]$), 18
 $K(V)_0$ (degree-0 subfield), 22
 Kemper, 21
 Kemper and Mattig, 19, 21
 Kiming, 141
 Kronecker resolvent, 81
 Kronecker specialisation, 64
 Kronecker's Criterion, 64
 Kronecker-Weber's Theorem, 3
 Kuyk and Lenstra, *see* Whaples' Theorem
- LaMacchia's Theorem, 55
 Lattice, 196ff
 Non-degenerate, 198
 Lefschetz' Theorem, 46
 Lenstra, 196
 Lenstra's Theorem, 10
 Level of field, 135
 Lifting property, 99
 Linear disjointness, 213
 Localised polynomial ring, 96
 Lüroth Problem, 6
 Lüroth's Theorem, 5, 22
- Maeda's Theorem, 7
 Malfatti, 39
 Malle and Matzat, 5, 54
 Maschke's Theorem, 180, 235
 Massy's Theorem, 161
 Matzat et al., 5
- Miyata, 125
 Modular group, 127
 Monier's Lemma, 162
 Monomial group action, *see* Multiplicative group action
 Morse polynomials, 80
 Multiplicative group action, 196
 Multiplicity of projective zero, 219
- Nakayama's Lemma, 83
 No-Name Lemma, 22
 Noether, 204
 Noether Problem, 4, **5ff**
 for A_4 , 36
 for A_5 , *see* Maeda's Theorem
 for C_3 , 30
 for C_4 , 34
 for C_6 , 61
 for D_4 , 35
 for V_4 , 33
 General, 8
 Linear, 8, **18**
 for p -groups in char. p , 117
 Multiplicative, 197
- Normal basis, 91
 Normal factorisation, 218
- Parametric polynomial, 1
 Parametric solution, 109
 p -equivalent, 208
 p -independent, 161, 208
 Polarisation, 230
 Projective class group, 94
 Projective line, 219
 Projective point, 219
- Quadratically equivalent, 208
 Quadratically independent, 208
 Quasi-dihedral extension, 146
 Quasi-dihedral group, 127
 Quaternion algebra, 131
 Split, 132
 Quaternion extension, 128
 Quaternion group, 127
- Rank of module, 84
 Rational extension, 5
 Real part (of quaternion), 132
 Reduction modulo m , 71ff
 Regular extension, 3, **74**
 with Galois group A_n , 78
 with Galois group S_n , 77
 with group C_{2^n} , 107
 Regular point, 68
 Regular polynomial, 224
 Reichstein, 196

- Relative invariant, 228
 - Joint, 229
- Representation of finite group, 17ff
 - Contragredient, 18
 - Cyclic, 18
 - Faithful, 17
 - Permutation, 17
 - Regular, 17
- Representation of linear group,
 - Dimension, 228
 - Homogeneous, 229, 238ff
 - Linear, 228
 - Polynomial, 219, 228
 - Rational, 219
- Residue Theorem, 68
- Resolvent polynomial, 23
 - Linear, 23
- Resultant, 25, 27
 - of binary forms, 245
- Retract-rational extension, 99
- Riemann Existence Theorem, 2
- Rigidity Method, 15
- Ring class field, 182
- Roland, Yui and Zagier, 61
- Roquette-Ohm's Theorem, 187

- Saltman, 98, 173
- Saltman and DeMeyer, 99
- Schertz, 185
- Scholz-Reichardt's Theorem, 4
- Schur Commutator Theorem, 233
- Schur's Lemma, 232
- Schwarz' Mean Value Theorem, 69
- Second Fundamental Theorem, 228
- Section of epimorphism, 209
- 'Seen one, seen them all' Lemma, 207
 - Char. p case, 208
- Semi-dihedral group, *see* Quasi-dihedral group
- Semi-linear group action, 21
- Semi-simple algebra, 231ff
- Serre, 194
- Shafarevich' Theorem, 4
- Shih's Theorem, 4
- Simple algebra, 231
- Simple component, 233
- Simultaneously symmetric polynomials, 223
- Smith's Theorem, 12, **104**
- Soicher and McKay, 25
- Solution to embedding problem, 207
- Square class, 208
- Stably rational extension, 6
- Stem cover of S_n , 15
- Sylvester resultant, *see* Resultant
- Szygies, 226, 228

- Tensor product, 211
 - of algebras, 213
- Thompson's Theorem, 5
- Trace (in Galois extension), 86
- Trace forms, 15
- Trink's PSL(2, 7)-polynomial, 53
- Tschirnhaus transformation, 141

- Unirational extension, 6
 - Non-rational of degree two, 10
 - Non-rational of degree three, 9, **57**

- Vector part (of quaternion), 132
- Vectorial polynomial, 19
- Versal extension, 100
- Von Neumann's Lemma, 236
- Voskresenskii's Theorem, 197
- V^* , *see* Dual space

- Wang, 56
- Weber resolvent, 39ff
- Weber's Theorem, 42
- Weight of invariant, 220
- Weight of relative invariant, 229
- Weyl module, 240
- Whaples' Theorem, 107
- Williamson, 172
- Witt vector, 120
- Witt's Criterion, 128
 - Necessity, 134
 - Sufficiency, 129–131
- Wreath product, 108
 - Generalised, 180

- Yakovlev, 106
- Young diagram, 235
 - Size of, 235
- Young tableau, 235ff

- Zassenhaus, 169