
INDEX

- Abel, N.H., 38
 absolute valuation, 234
 active (side condition), 364
 aleatoric (construction of finite fields), 73
 algebraic
 equation, 1
 integers, 22, 246
 number field, 327
 numbers, 1
 ordering, 232
 of a group, 235
 sum, 42
 algebraically
 decomposed, 36
 ordered
 group, 235
 ring, 230
 semiring, 232
 algorithm, 1
 amalgamation (of R -bases), 305
 α -maximal, 304
 antisymmetric *see* skew symmetric
 α -overorder, 303
 archimedean
 ordered, 249
 valuation, 231
 arithmetic radical, 292
 Artin, E., 87, 97
 Artin-Schreier, 104
 generators, 106
 normal form, 39
 theorem of, 79
 associate, 20, 24, 330
 automorphism, 16

 Banach, St., 255
 basic
 parallelotope, 351
 symmetric functions, 30, 48, 50

 basis, 9
 normalized, 237
 of a free module, 177
 of a subset of a factorial monoid, 24
 theorem for finite abelian groups, 285
 Bastida, J.R., 87
 Berlekamp's method, 83–5
 Bernstein, L., 329
 bilinear form, 308
 Blichfeldt, H.F., 199
 blocks of imprimitivity, 144
 Böffgen, R., 455
 Bring-Jerrard normal form, 39
 Buchmann, J., 329

 Cantor, D., 83
 Cayley matrix representation, 163
 Čebotarev *see* Tschebotareff
 ceiling, 411
 principal, 412
 central idempotent, 41
 centralizer, 170
 characteristic, 225
 equation, 34
 polynomial, 17, 34, 55
 Chevalley's
 lemma, 241
 theorem, 243
 Chinese remainder theorem, 45
 Cholesky, 188
 decomposition, 189
 class
 group, 287
 matrix, 414
 computation procedure, 421–3
 number, 378, 380, 384
 semigroup, 289
 Collins, G.E., 319, 325, 347
 comaximal, 306

- common
 - divisor, 27
 - inessential discriminant divisor, 318
 - multiple, 27
- commutative
 - ring, 6
 - constructively given, 6
- companion matrix, 349
- comparable, 248
- complex quadratic field, 329
- conductor, 388
- conjugate, 19, 329
- connecting R -module, 170
- constant polynomial, 10
- convex, 212
 - body theorem of Minkowski, 213
- core algorithm, 323, 324
- cyclic module, 309
- cyclotomic
 - equation, 157
 - field, 159
 - polynomial, 159
 - units, 160
- Dade, E.C., 291, 313
- decomposed, 36
- Dedekind, R., 221, 253, 273
 - criterion, 295
 - domain *see* ring
 - ring, 221, 253, 265–278
 - test, 316, 317
- decomposition of prime ideals, 390
 - in quadratic fields, 393, 394
- degree
 - of an algebraic number field, 327
 - of a polynomial, 10
 - of inertia, 386
 - theorem, 13
 - valuation, 248
- δ -element, 322
- δ -split, 320
- δ -uniform, 321
- dependent (units), 331
- derivation (of a ring), 26, 91–3
- deterministic methods (for constructing finite fields), 77–80
- Deuring, M., 171
- dimension (of a lattice), 187
- Diophantine analysis, 4
- direct sum (of modules), 8
- Dirichlet, P.G.L., 273, 377
 - (Unit) Theorem, 334
- discrete valuation, 251
- discriminant
 - composition formula, 122
 - ideal, 121, 292
 - of an algebraic number field, 329
 - of a lattice, 187
 - of a module, 122
 - of a polynomial, 34, 49, 61, 62
 - of cyclotomic polynomials, 161
- divisible group, 243
- divisibility, 20, 23
- division
 - ring, 235
 - with remainder
 - of integers, 2
 - of polynomials, 10, 11
- divisor cascade, 24
- domain of rationality, 29
- dual
 - basis, 281, 337
 - index rule, 292
- Eisenstein, G., 221, 258
 - extension, 260
 - polynomial, 258
- element = δ -element, 322
- elementary
 - changes, 310
 - divisor, 184
 - form presentation, 284
 - ideal, 284
 - normal form, 184
 - ideals, 282
 - matrices, 178
- equal degree factorization, 81
- equivalence, 20, 23
 - of matrix representations, 165
 - of permutation representations, 142
- equivalent
 - pseudo valuations, 235
- Euclidean
 - algorithm, 3, 4
 - ring, 21
- Euler φ -function, 158
- exponent, 285
 - ideal, 285
- exponential valuation, 248
- factorial
 - monoid, 24
 - ring, 21
- faithful
 - matrix representation, 165
 - permutation representation, 144
- feasible (solution), 364
- Fermat
 - prime numbers, 172
 - 's last theorem, 377
- filtration, 309
- fixed *see* invariant
- formal
 - degree, 57
 - Laurent series, 306
 - power series, 305
- fractional ideals, 264, 265
 - inverse of, 264
 - invertible, 264
- Frobenius automorphism, 82, 153

- fundamental
 - parallelootope, 187
 - unit, 328, 334
- Galois, E., 29, 38, 40, 69, 219
 - correspondence, 19, 90
 - fields, 70
- Gauss, C.F., 15, 20, 29, 44, 46, 69, 70, 71, 172, 173, 384
 - integer ring, 15–22
 - period, 20, 172
- general
 - linear group, 165, 311
 - reduction algorithm, 194, 195
- generalized pseudo valuation, 235
- generator
 - system of invariants, 146
- generic
 - argument, 55
 - element, 52
 - polynomial, 48, 56
- Godwin, H.J., 329
- grading, 309
- Gras, M.N., 329
- greatest common divisor, 3, 27
- group
 - general linear, 165, 311
 - special linear, 166, 311
 - unimodular, 311
- group
 - of an equation, 108
 - of permutation automorphisms, 32
 - of the cyclotomic equation, 157, 158
 - of units, 329
- half
 - module, 143
 - ring, 233
- Hamilton–Cayley equation, 22
- Hasse diagram, 19
- height function, 21
- Hensel, K., 221, 325
 - lemma, 301
- Hermite
 - constants, 198
 - normal form, 179, 311
 - (column, row) reduction, 179
- Hilbert, D., 39, 309
 - theorem, 79, 90
- Hölder, O., 255
- holomorph of a group, 133
- Huppert, B., 141
- hypercube, 174
- ideal
 - class group, 380
 - elementary, 282
 - equivalence procedure, 424
 - fractional, 264, 265
 - group, 379
 - large, 229
 - normal presentation of, 400
 - numbers, 221
 - presentation, 397
 - prime elements, 221
- idempotents, 40
 - central, 41
 - orthogonal, 42
 - primitive, 42
 - central, 43
- identity mapping, 16
- imprimitive permutation representation, 144
- inclusion of normally presented ideals, 403
- indecomposable
 - representation, 143
 - splitting rings, 63–9
- independence of valuations, 251
- independent units, 331
- index, 72
 - discriminant rule, 292
 - ideal, 286, 290
 - multiplicativity, 292
 - of a lattice, 187
 - table, 72
- infinitely larger, 248
- inseparable
 - equation, 35
 - polynomial, 35, 49
- integral
 - basis, 314
 - of quadratic fields, 317, 318
 - of cyclotomic fields, 318
- integral
 - closure, 245–8
 - element, 246
- integrally closed, 246
- intransitive representation, 143
- invariant, 16
- inverse of a normally presented ideal, 401, 402
- invertible R -fractional ideal, 264
- involutionary
 - mapping, 16
 - rule, 292
- Jacobson radical, 307
- Jordan, C., 119, 141
- Klein Four Group \mathfrak{B}_4 , 8, 18
- Knuth, D.E., 4, 85, 183
- Krasner, M., 325
- Kronecker
 - criterion, 247
 - symbol, 10
 - theorem, 157
- Krull, W., 274
 - exponential valuation, 249
 - p -adic, 268
 - valuation, 235, 239
 - ring, 239

- Kuershak, 221
 Kummer, E.E., 220, 253, 273, 377
 extension, 104
- Lagrange, J.L., 97, 104
 operator, 97–9
- Lambek, J., 229
- Lambek–Ushida quotient ring, 230
- Land, R., 296
- Landau, E., 287, 367
- Lang, S., 6, 7, 8, 10, 24, 45, 87, 91
- large ideal, 229
- Lasker, E., 309
- lattice, 187
- leading coefficient, 10
- least common multiple, 27
- left
 module, 7
 regular matrix representation, 163
 unital module, 8
- Lenstra, H.W.Jr., 329
- Lenstra, Lenstra and Lovasz, 177, 200
 reduction = LLL reduction, 200–202
- Lidl, R., 70
- lifting of idempotents, 115–17
- list of cyclotomic polynomials, 344, 345
- LLL reduction *see* Lenstra, Lenstra and Lovasz reduction
- local
 domain, 227
 ring, 227
- localization, 220, 226–9, 303–5
- logarithmic space, 360
- long division *see* division with remainder
- lying (over, under) of ideals, 386
- Mahler, K., 338, 379, 410, 411
- Mäki, S., 329
- main theorem of Galois theory, 87
- matrix representation, 164–9,
 faithful, 165
 improper, 168
 null, 168
 proper, 168
 regular, 164
 sum of, 168
- Matusita, 274
- Matzat, B.H., 455
- maximal
 α -, 304
 order, 22, 278
 purely inseparable
 extension, 96
 subfield, 119
 R -order, 278
 separable overring, 94
- McCauley, 309
- McKay, J. *see* Soicher, L.
- minimal
 basis *see* integral basis
 equation, 17
 polynomial, 17
 splitting ring, 30
- Minkowski, H., 177, 378
 bound = constant 384
 convex body theorem, 213
 mapping, 383
 reduction, 191
- MLLL reduction 209
- Möbius
 inversion formula, 76
 μ -function, 76
- modified division with remainder *see*
 pseudo-division
- module
 connecting R -, 170
 cyclic, 309
 discriminant of, 122
 free R -, 9
 half, 143
 left, 7
 left unital, 8
 Noetherian, 309
 null, 7
 rank of, 9
 relation, 282
 representation, 166
 row, 282
 syzygy, 282
- modulo p independent, 394
- monic, 10
 equation, 13
- multi modular calculus, 46
- multiplicative
 character of a group, 98
 valuation, 231
- multiplier = φ – multiplier, 239
- Newton, I., 257
 polygon, 258
 relations, 51
- Niederreiter, H., 70, 73
- nilideal, 115
- nilradical, 115
- Noether, E., 171, 274, 307
- Noetherian, 309
- non-archimedean pseudo valuation, 231
- non-degenerate, 308
- norm, 16, 34, 53, 55
 of a polynomial, 346
 of an ideal, 291, 381
- normal
 basis, 19, 163
 extension, 68
 presentation of ideals, 400
- normal form
 elementary divisor, 184
 of Hermite, 179, 311
 of monic quadratic equations over \mathbb{Z} , 40
 of Smith, 184

- normalized
 - basis, 237
 - element, 322
 - valuations, 411
- null module, 7
- number of monic irreducible m -th degree polynomials in $\mathbb{F}_q[t]$, 76, 77
- orbit, 143
- order, 22, 278
 - of an algebraic number field, 327
 - ideal, 285
 - rank, 249
- orthogonal
 - (left, right) B -complement, 308
 - idempotents, 42
- Ostrowski, A., 221, 255
- overorder *see* α -overorder
- overring *see* R -ring
- p -adic valuation, 231
- p -adic Krull exponential valuation, 268
- pairwise reduced, 211
- parallelootope
 - basic, 351
 - fundamental, 187
- partial endomorphism, 229
- Peacock, 6
- Peirce decomposition, 40, 41
- Pell's equation, 328
- perfect, 26, 119
- permanence principle, 6
- permutation
 - automorphism, 32
 - matrix, 169
 - representation, 142
- φ -multiplier *see* multiplier
- φ -unit *see* unit
- PID *see* principal ideal domain
- polynomial
 - characteristic, 17, 34, 55
 - constant, 10
 - cyclotomic, 159
 - degree of a , 10
 - discriminant of a , 34, 49, 61, 62
 - Eisenstein, 258
 - generic, 48, 56
 - inseparable, 35, 49
 - minimal, 17
 - primitive, 86
 - principal, 55
 - pseudo Eisenstein, 263
 - separable, 49
- potential list, 70
- power sum, 51
- p -power characteristic, 117
- presentation
 - of gcd, 3
 - of ideals, 397
- prime
 - element, 21
 - ring, 48, 57, 78
- primitive
 - central idempotent, 43
 - element, 140, 173–6
 - extension, 139
 - idempotent, 42
 - permutation groups, 141
 - permutation representation, 144
 - polynomial, 86
 - root, 70
 - root of unity, 344
- principal
 - ceiling, 412
 - equation, 52
 - ideal domain = PID, 266
 - ideal procedure, 424
 - ideal ring, 21
 - polynomial, 55
- product
 - formula for valuations, 235, 411
 - of normally presented ideals, 401
 - valuation, 237
- proper unimodular matrix, 165
- Prüfer ring, 284
- pseudo
 - division, 11
 - Eisenstein polynomial, 263
 - valuations, 231
- purely inseparable
 - element, 117
 - equation, 118
 - extension, 95
- pure quadratic equation, 34
- quadratic supplement, 188
- quotient, 2
 - ring, 7, 222–5
- radical element, 98
- ramification index
 - of ideals, 386
 - of valuations, 275
- ramified, 386
- rank
 - of a lattice, 187
 - of a module, 9
 - rational, 254
- real quadratic field, 329
- reduced
 - discriminant ideal, 292
 - computation, 296
 - integer, polynomial, 314
- reduction, 191–202
 - of Lenstra, Lenstra and Lovasz = LLL, 200–202
 - modified = MLLL, 209
 - of Minkowski, 191
 - pairwise, 211
 - total, 192–5

- of Hermite *see* Hermite (column, row) reduction
- regular
 - matrix representation, 164
 - permutation representation, 144
 - representation, 55
 - trace, 280
- regulator, 361
- relation
 - matrix, 282
 - module, 282
- relative norm, 18
- remainder, 2
- Remak, R., 362
- representation
 - module, 166
 - space, 167
- resultant, 49, 57–61
- R*-fractional ideal *see* fractional ideal
- ring
 - algebraically ordered, 230
 - commutative, 6
 - constructively given, 6
 - Dedekind, 221, 253, 265–78
 - division, 235
 - Euclidean, 21
 - factorial, 21
 - half, 233
 - Krull valuation, 239
 - Lambek-Ushida quotient, 230
 - local, 227
 - of an equation, 13, 14
 - of Gaussian integers, 15–22
 - prime, 48, 57, 78
 - principal ideal, 21
 - Prüfer, 284
 - quotient, 7, 222–5
 - R*-, 9
 - semilocal, 228
 - semisimple, 307
 - simple, 307
 - splitting, 30
 - unital, 6
 - universal splitting, 30
 - valuation, 236
- root, 10
 - estimates, 151, 152
 - finder, 135
- R*-order *see* order
- row
 - equivalence, 283
 - module, 282
- Ruffini, P., 38
- Schreier *see* Artin-Schreier
- Schwarz, St., 81
- semidirect product, 133
- semigroup ring, 167
- semilocal ring, 228
- semiring, 232
- semisimple, 307
- separability, 92
- separable, 35, 49, 93–5
- Shanks, D., 329
- s*-hypercube, 174
- Siegel, C.L., 367
- simple, 307
- Sims, Ch. C., 428
- skew symmetric, 308
- Smith normal form, 184
- Soicher, L. and McKay, J., 429
- solution ring, 14
- Sonn, J., 173
- specialization, 11
- special linear group, 166, 311
- split = δ -split, 320
- splitting
 - field, 36
 - ring, 30
- stabilizer, 144
- standard
 - basis, 30
 - generators, 136
- Stauduhar, R.P., 429
- Steinitz, 287
 - class, 288
- Stender, H.J., 329
- Stirling's formula, 37
- strong independence of valuations, 251
- structural stability, 297–9
- Study numbers, 23
- sublattice, 187
- successive minima, 195
- sum
 - of matrix representations, 168
 - of permutation representations, 142
- symmetric, 308
 - functions, theorem on, 50
 - polynomials, 48
- system of imprimitivity, 144
- syzygy module, 282
- Taussky, O., 167, 291, 313
- torsion
 - element, 22
 - free, 228
 - subgroup (of unit group), 330
 - submodule, 229
- total reduction, 192
- totally
 - complex algebraic number field, 329
 - ramified valuation, 260
 - real algebraic number field, 329
- trace, 16, 34, 53, 55
 - bilinear form, 54
 - radical, 123
 - regular, 280
- Trager, B., 346
- transitive permutation representation, 143
- Trinks, W.,

- equation, 155, 156
- trivial permutation representation, 144
- Tschebotareff, N. 130, 371
 - density theorem, 130
- Tschirnhausen transformation, 38
- uniform = δ -uniform, 321
- unimodular
 - group, 311
 - matrices, 165
- unique factorization ring *see* factorial ring
- unit
 - group, 329
 - matrix I_n , 178
 - φ -, 238
- unital, 6
 - overring, 10
- universal splitting ring, 30
- unramified, 386
- valuation, 231
 - absolute, 234
 - archimedean, 231
 - degree, 248
 - discrete, 251
 - exponential, 248
 - generalized pseudo-, 235
 - Krull, 235, 239
 - exponential, 249
 - p -adic, 268
 - module, 236
 - multiplicative, 231
 - non archimedean pseudo, 231
 - normalized, 411
 - p -adic, 231
 - product, 237
 - pseudo, 231
 - ring, 236
 - Krull, 239
 - totally ramified, 260
- valuations
 - independence of, 251
 - product formula for, 235, 411
 - ramification index of, 275
 - strong independence of, 251
 - weak independence of, 276
- Vandermonde's determinant, 54
- van der Waerden, B.L., 346
 - criterion, 127–9
- Vieta equations, 30
- weak independence (of valuations), 276
- Weierstrass mapping, 78
- Wielandt, H., 141
- Williams, H.C., 329
- Wilson's theorem, 107
- Zassenhaus, H., 83, 141, 173, 291, 313
- zero, 4, 12
- Zimmert, R., 366