

Index

- A_n , 85
- $\deg(f)$, 145
- $\operatorname{div}(n)$, 8
- f^F , 195
- \mathbb{F}_p , 118
- \mathbb{F}_{p^n} , 171
- $\langle g \rangle$, 73
- $\gcd(m, n)$, 9
- gH , 61
- $\operatorname{GL}_2(\mathbb{R})$, 57
- L , group of linear isometries, 58
- $n(\sigma)$, 83
- \mathbb{N} , 3
- $O_2(\mathbb{R})$, 57
- $\varphi_\alpha : R[X] \rightarrow R$, 150
- $\varphi(x)$, 17
- $\langle r_1, \dots, r_n \rangle$, 115
- R^* , 112
- $R[X]$, 145
- $R[X]/\langle f \rangle$, 165
- $R[X_1, \dots, X_n]$, 187
- S/\sim , 224
- S_n , 78
- $V(f)$, 151
- $V(f_1, \dots, f_m)$, 214
- $V(I)$, 214
- $[x]_d, [x]$, 5
- \mathbb{Z} , 3
- $\mathbb{Z}[i]$, 114
- $\mathbb{Z}/n\mathbb{Z}$, 52, 117
- $\mathbb{Z}[\sqrt{-5}]$, 127
- action of a group on a set, 92
- alternating group A_n , 85
 - simplicity of A_n , $n \geq 5$, 86
- Artin conjecture, 159
- associated elements, 126
- associativity
 - in groups, 51
 - of composition of maps, 54
- basis of a vector space, 231
- Berlekamp's algorithm for factoring
 - polynomials, 176
- Bernoulli numbers, 137
- binomial coefficients modulo a prime, 146
- birthday problem, 30
- Brun, V., 21
- bubble sort, 82
- Buchberger, B., 187
- Buchberger's algorithm, 209
 - example of, 208
 - terminates, 209
- Buchberger's S -criterion, 208
- Burnside's formula, 96
- Carmichael numbers, 27
- center of a group, 98
- centralizer of group element, 98
- characteristic of a ring, 121
- Chinese remainder theorem, 16
 - group version, 77
 - 30-riddle, 14
- commutative ring, 112
- composition table, 53
 - example with $\mathbb{Z}/4\mathbb{Z}$, 53
 - example with $(\mathbb{Z}/8\mathbb{Z})^*$, 67
- congruence modulo an integer, 6

- conjugacy classes, 98
 - in the symmetric group, 98
 - cycle types for, 98
- conjugation, 98
- cosets, 61
- cycle, 79
- cycle type, 98
- cyclic group, 74
- cyclotomic polynomial, 154

- degree of non-zero polynomial, 145
- derivative of a polynomial, 153
- determinant, 68
- Dickson, L. E., 191
- Dickson's lemma, 191
- dimension of a vector space, 232
- division algorithm, 194
 - examples of, 195
 - remainder in, 194
- division with remainder
 - integers, 5
 - polynomials, 148
 - of several variables, 194
- divisor in rings, 126
- domain, 113
 - Euclidean, 130
 - principal ideal, 115

- Electronic Frontier Foundation, 20
 - \$100 000 prize, 20
- elimination, Gaussian, 215
 - of variables, 215
- equivalence class, 224
- equivalence relation, 223
- Euclid, 8
- Euclidean algorithm, 9
 - and Fibonacci numbers, 12
 - binary, 43
 - complexity, 12
 - extended, 11
 - in Euclidean domains, 131
 - strikes again, 134
- Euclidean domain, 130
 - Euclidean algorithm in, 131
 - is principal ideal domain, 131
- Euler φ -function, 17
 - on a product, 18
- Euler's theorem
 - group theoretic proof, 76
 - on congruences, 18
 - on quadratic residues, 38
- extension field, 113

- factoring algorithms
 - Berlekamp's, 176
 - $(p - 1)$ -algorithm, 33
 - ρ -algorithm, 31
- factoring challenges, 2
- Feit–Thompson theorem, 88
- Fermat, P., 26
- Fermat's last theorem, 26, 137
- Fermat's little theorem, 26
- Fermat's two-square theorem, 132
 - algorithm for, 135
- field, 113
 - extension, 113
 - finite, 170
 - of fractions, 124
 - subfield, 113
- finitely generated vector space, 230
- fixed point of group action, 93
- Freshman's Dream, 122

- Gauss, C. F., 2, 5, 38, 41, 144, 158
- Gaussian elimination, 186
- Gaussian integers, 114, 132
 - Euclidean domain, 133
- Gauss's lemma on quadratic residues, 40
- generator, 74
- GIMPS – Great Internet Mersenne Prime Search, 20
- greatest common divisor (gcd)
 - in rings, 126, 130
 - in \mathbb{Z} , 9
- Gröbner basis, 196
 - existence of, 199
 - minimal, 212
 - reduced, 212
 - every ideal has one, 212
 - example of, 213
- group, 50
 - abelian, 51
 - action of, 92
 - Burnside's lemma, 96
 - conjugacy class, 98
 - fixed point, 93
 - orbit, 93
 - stabilizer, 93
 - alternating, 85
 - classification of finite groups, 88
 - composition in, 51
 - generator in, 74
 - homomorphism for, 68
 - kernel, 68

infinite non-abelian, 57
 isomorphism for, 68
 monster, 88
 p -group, 100
 powers of elements in, 72
 product of groups, 76
 simple, 86
 sporadic, 88
 Sylow p -subgroup, 102
 symmetric, 78

 Hamilton, W. R., 113
 Hilbert, D., 198
 Hilbert's basis theorem, 200
 controversy with Gordan, 199
 Hironaka, H., 187
 homomorphism
 of groups, 68
 of rings, 119

 ideal, 115
 as equations, 214
 generated by elements, 115
 in polynomial rings, 161
 in \mathbb{Z} , 115
 maximal, 118
 non-principal (example of), 127
 prime, 118
 principal, 115
 image
 of a group homomorphism, 68
 of a ring homomorphism, 119
 index of a subgroup, 64
 index theorem, 63
 induction, 3
 inverse element in a group, 51
 inverse of a product, 56
 inversions, 83
 number of, 83
 irreducible element, 126
 irregular prime numbers, 138
 isometry, 57
 isomorphic groups, 68
 isomorphism
 of groups, 68
 of rings, 119
 isomorphism theorem for
 groups, 71
 example with $\mathbb{R}/2\pi\mathbb{Z}$, 71
 example with S_3 , 72
 isomorphism theorem for rings, 120

Jensen, J. L. W., 138

 kernel
 of a group homomorphism, 68
 of a ring homomorphism, 119
 Knuth, D., 12, 29
 Kronecker, L., 3

 Lagrange, J. L., 50
 index theorem of, 63
 least common multiple, 23
 Legendre symbol, 36
 lexicographic order, 189, 193
 graded, 189
 graded reverse, 218
 linear combination in vector space, 231
 linear map, 230
 linearly independent set of vectors, 231
 Lucas, 20

 Maple, 156
 mathematical induction, 3
 maximal ideal, 118
 Mersenne, M., 20
 minimal element, 228
 minimal Gröbner basis, 212
 monic polynomial, 145
 multiplicity of root, 151

 natural numbers, 3
 neutral element in a group, 51
 Newton's method, 137
 Nicely, T., 21
 normalizer of a subgroup, 98

 orbit of group action, 93
 order of an element in a group, 73
 example with S_3 , 73
 ordering
 lexicographic, 189
 partial, 223, 228
 minimal element of, 228
 term, 189
 total, 228
 well, 228
 ordering of \mathbb{Z} , 3
 orthogonal group, 57

 p -group, 100
 partial order, 223
 partition, 225
 Pentium FDIV bug, 21

- permutation, 78
 - as homomorphism, 85
 - even, 85
 - inversion of, 83
 - odd, 85
 - product of simple transpositions, 84
 - sign of, 85
- Pollard, J. M., 33
- polynomial
 - cyclotomic, 154
 - formal definition of, 144, 187
 - in one variable, 145
 - in several variables, 187
 - S -, 206
- prime element, 127
- prime ideal, 118
- prime number, 19
 - astronomical, 26
 - infinitely many prime numbers, 20
 - irregular, 138
 - largest known, 20
 - Mersenne prime number, 20
 - proving primality of without factoring, 26
- primitive root
 - and decimal expansions, 159
 - complex, 155
 - in a ring, 158
 - modulo a prime, 159
- principal ideal domain, 115
 - unique factorization in, 129
- product groups, 76
- pseudoprime, 27
 - strong, 28

- quadratic reciprocity, 41
 - proof of, 167
- quadratic residues, 36
- quaternions, 113
- quotient group, 65
- quotient ring, 116
 - of \mathbb{Z} , 117

- Rabin, M., 29
- reduced Gröbner basis, 212
 - every ideal has one, 212
 - example of, 213
- relation, 223
 - antisymmetric, 223
 - equivalence
 - construction of \mathbb{Q} , 227
 - construction of \mathbb{Z} , 226
 - reflexive, 223
 - symmetric, 223
 - transitive, 223
- remainder in division algorithm, 194
- repeated squaring, 7
- representative, 224
- Riemann hypothesis, 37 (footnote)
- ring, 112
 - commutative, 112
 - homomorphism
 - kernel of, 119
 - isomorphism, 119
 - isomorphism theorem for, 120
- ring homomorphism, 119
- root
 - in extension field, 166
 - in polynomial, 151
 - multiplicity of, 151
- RSA challenge, 2
- RSA cryptosystem, 7
 - explained, 24
- RSA-2048, 2

- S -polynomial, 206
- Schur, I., 156
- sign
 - of homomorphism, 85
 - of permutation, 85
- solving equations, 215
- stabilizer, 93
- Steinitz exchange lemma, 231
- strong pseudoprime, 28
- subfield, 113
- subgroups, 61
 - normal, 65
- subring, 112
- Sylow p -subgroup, 102
- Sylow theorems, 102
- symmetric group, 78
- symmetric polynomials, 186
 - algorithm using Gröbner bases, 200
- system of polynomial equations, 214

- term ordering, 189
 - graded lexicographic, 189
 - graded reverse lexicographic, 218
 - infinitely many on \mathbb{N}^2 , 190
 - is a well order, 192
 - lexicographic, 189
 - through geometry, 190

Cambridge University Press

978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases

Niels Lauritzen

Index

[More information](#)

240

Index

total ordering, 228

transposition, 80

simple, 80

twin primes, 21

unique factorization

into integers (natural numbers), 22

into irreducible elements, 126

short proof of, 23

unique factorization domain, 126

unique ring homomorphism $\mathbb{Z} \rightarrow R$, 120

unit, 112

vector spaces over arbitrary
 fields, 231

finitely generated, 231

Wagstaff, S., 138

well ordering, 228

natural numbers, 3

Wiles, A., 27, 138

Wilson's theorem, 45, 133,
 152

zero divisor, 112