

## Index

---

- $p$ -group, 22
- abelian, 4
- ACCPI: ascending chain condition for
  - principal ideals, 37
- algebra, fundamental theorem of, 85
- algebraic element, 74
- algebraic extension, 77
- algebraic geometry, 184
- algebraic number, 78
- algebraically closed, 170
- algorithm
  - for factorizing polynomials, 49
- associate, 37
- automorphism, 5
  - inner, 5
- automorphism of a field, 80
- axiom of choice
  - equivalence to the existence of maximal proper ideals, 35
- basis
  - existence of, 190
  - for a vector space, 56
  - transcendence, 180
- bijection, 4
- Cantor, 74
- centralizer, 5
- centre, 5
- centre of a group, 140
- chain, 190
- character, 61
- characteristic  $n$ , 29
- characteristic 0, 29
- characteristic polynomial, 65
- choice, axiom of
  - equivalence to the existence of maximal proper ideals, 35
- closure
  - normal, 100
- column, 62
- commutative, 4
- commutative ring with a, 126
- commutative ring with a 1, 25
- commutator, 4
- commute, 4
- conjugacy class, 6
- conjugate, 5
- conjugation, 5
- constant, 26
- constructible, 147
- content of a polynomial, 41
- coset
  - right, left, 6
- cubic polynomial, 47
- cubic resolvent, 154
- cycle
  - of type  $j$ , 12
- cycle type, 12
- cyclic extension, 135
- Dedekind's lemma, 62
- degree, 26
  - of an extension, 71
- dependent, linear, 56
- derivative, 106
- determinant, 62, 76, 116, 168
- differentiation, 106
- dihedral group, 13
- dimension, of a vector space, 55, 58
- discriminant, 125, 144

- eigenvalue, 65
- eigenvector, 65
- Eisenstein's criterion for irreducibility, 94, 118
- elementary symmetric polynomial, 187
- epimorphism, 5
- Euclid's algorithm, 42
- Euclidean domain, 41
- Euclidean function, 41
- evaluation map, 30, 74
- exchange theorem, Steinitz, 57, 181
- extension
  - algebraic, 77
  - degree of, 71
  - field, 70
  - finite, 71
  - generated by a set, 73
  - infinite, 71
  - Kummer, 137
  - normal, 98
  - of monomorphisms, 89
  - separable, 103
  - simple, 72
  - splitting field, 86, 98
- factorization, 36
- Fermat number, 146
- Fermat prime, 146
- field, 32
  - extension, 70
  - finite, 60
  - fixed, 112
  - infinite, 60
  - of fractions, 69
  - prime subfield of, 48
  - splitting, 86
- field of fractions, 33
- finite extension, 71
- finite field, 60
- finite-dimensional vector space, 56
- first isomorphism theorem, 8
- fixed field, 112
- formal power series, 27
- fundamental theorem
  - of algebra, 85
  - of Galois theory, 118
- Galois group of a polynomial, 116
- Galois group of an extension, 112
- Galois theory, fundamental theorem of, 118
- Gauss' lemma, 45, 49
- generated by a set
  - extension, 73
  - ideal, 27
- generic polynomial, 186
- geometry, algebraic, 185
- group, 3
  - alternating, 14
  - cyclic, 5
  - derived, 5
  - exponent, 4
  - finite, 5
  - Galois, 112
  - normal, 6
  - order, 4
  - simple, 140
  - transitive group of permutations, 117
- Hermite's proof that  $e$  is transcendental, 74
- highest common factor, 40
- Hilbert's theorem, 111
- homomorphism, 5
  - ring, 27
- ideal, 27
  - generated by a set, 27
  - principal, 27
  - proper, 27
- image, 6, 55, 59
- independent
  - algebraically, 178
  - linearly, 56
- indeterminate, 26
- index, 6
- infinite extension, 71
- infinite field, 60
- inseparable extension, totally, 111
- inseparable polynomial, 108
- integers
  - ring of, mod  $n$ , 28
- integral domain, 29
- intermediate value theorem, 118
- inverse, 3, 25
- irreducible, 37
- irreducible polynomial
  - an example, 48
  - Eisenstein's criterion, 94
  - localization, 51
- isomorphism, 5
  - ring, 27
  - theorem for rings, 28

kernel, 6  
 of a ring homomorphism, 27  
 Kronecker's factorization algorithm, 49  
 Kummer extension, 137

Lagrange's theorem, 7  
 least common multiple, 41  
 length, 39  
 Lindemann's proof that  $\pi$  is transcendental, 74  
 linear mapping, 55, 59  
 linear subspace, 55  
 linearly dependent, 56  
 linearly independent, 56  
 Liouville  
 shows that transcendental numbers exist, 74  
 theorem on bounded analytic functions, 85  
 localization principle, 52  
 lowest common multiple, 43  
 Lüroth's theorem, 183

matrix, 62, 168  
 unit, 63  
 maximal element, 37, 190  
 minimal polynomial, 74  
 in terms of a determinant, 76  
 monic, 26  
 monic polynomial, 74  
 monomorphism, 5  
 extension of, 89  
 of an algebraic extension, 80  
 ring, 27  
 multiple, least common, 41  
 multiplicative Euclidean function, 43  
 multiplicity, 30  
 multiplicity of a root, 108, 111

natural irrationalities, theorem on, 164  
 Newton's identities, 124  
 nilpotent, 18, 26  
 Noetherian, 36  
 norm, 137  
 normal closure, 100  
 normal extension, 98  
 normalizer, 6  
 null-space, 55  
 number field, 33  
 numerical integral domain, 33

orbit, 11  
 order, 5  
 partial, 190  
 total, 190

partial order, 190  
 pentagon, regular, 161  
 permutation, 4  
 permutations  
 transitive group of, 117  
 polarity, 112  
 polynomial  
 content of, 44  
 cubic, 47  
 cyclotomic, 126  
 elementary symmetric, 187  
 equation, 69  
 generic, 186  
 inseparable, 108  
 minimal, 74  
 monic, 74  
 primitive, 44  
 quadratic, 47  
 quartic, 153  
 quintic, 161  
 symmetric, 188  
*PP*: proper principal ideals, 37  
 prime, 39  
 subfield, 48  
 prime number, 37  
 prime ring, 29  
 primitive polynomial, 44  
 primitive roots of unity, 126  
 principal ideal, 28  
 principal ideal domain, 41  
 proper ideal, 27  
 purely transcendental, 183

quadratic equation, 69  
 quadratic polynomial, 47  
 quartic polynomial, 153  
 quintic polynomial, 161  
 quotient ring, 28

rank, 59  
 relatively prime, 40  
 Rolle's theorem, 118  
 root, 30  
 multiplicity of, 108  
 of a polynomial, 74  
 of unity, 126  
 primitive roots of unity, 126  
 repeated, 106  
 row, 62  
 ruler and compass construction, 180

- self-conjugate, 6
- series
  - central, 17
  - derived, 17
  - group, 17
  - invariant, 17
  - normal, 17
  - subnormal, 17
  - upper central, 18
- signature, 14
- simple, 15
- simple extension, 73
- simple,  $\mathbb{R} : \mathbb{Q}$  is not, 73
- Soicher, Leonard, 162
- soluble, 18
- span, 55
- splitting field extension, 86, 98
- stabilizer, 11, 23
- Steinitz exchange theorem,
  - 57, 181
- subfield
  - prime, 48
- subgroup, 4
- subring, 26
- Sylow  $p$ -subgroup, 22
- Sylow theorems, 22
- symmetric polynomial, 188
  - elementary, 187
- Taylor's formula, 108
- total order, 190
- totally inseparable, 111
- tower law, 72
  - for transcendence degree, 182
- trace, 137
- trajectory, 113
- transcendence
  - basis, 180
  - degree, 181
- transcendental element, 74, 177
- transcendental, purely, 183
- transitive, 12
- transitive group of permutations, 117
- transposition, 12
- triangular, 64
- triangular matrix, 63
- unique factorization, 38
- unique factorization domain, 39
- unit, 25
- unity
  - primitive roots of, 126
  - roots of, 126
- upper bound, 190
- variable, 26
- vector space, 54
  - basis of, 55
  - finite-dimensional, 56
- Vierergruppe, 15
- well-ordered set, 189
- Wilson's theorem, 13, 108
- zero, 30
- Zorn's lemma, 189
  - and the construction of an algebraic closure, 171, 174
  - and the existence of proper maximal ideals, 35