

## Index

- FDeclareExtensionField, 53, 91  
 FDeclareField, 33, 52, 90  
 FDeclareSplittingExtensionField,  
   92  
 FDeclareSplittingField, 92  
 FFactor, 55, 94  
 FFindFactor, 58  
 FFindFactorRt, 58, 96  
 FGaloisGroup, 137  
 FGaloisResolvent, 141  
 FInvert, 33, 54, 93  
 FMakeTower, 59, 97  
 FMap, 100  
 FMapIsIsoQ, 99  
 FMinPoly, 57, 96  
 FPolynomialExtendedGCD, 57, 95  
 FPolynomialGCD, 57, 95  
 FPolynomialOrbit, 141  
 FPolynomialQuotient, 56, 94  
 FPolynomialRemainder, 56, 94  
 FRootNumber, 57, 96  
 FSimplifyE, 33, 54, 93  
 FSimplifyP, 55, 94  
 FSubstituteInGaloisResolvent, 143  
 Factor [*Mathematica*], 13  
 NSolve [*Mathematica*], 12  
 N [*Mathematica*], 13  
 PolynomialExtendedGCD [*Mathematica*],  
   15  
 PolynomialGCD [*Mathematica*], 14  
 PolynomialQuotient [*Mathematica*], 14  
 PolynomialRemainder [*Mathematica*], 14  
 Root [*Mathematica*], 13, 89  
 RootOf [*Maple*], 13, 89  
 factor [*Maple*], 13  
 fsolve [*Maple*], 12  
 gcd [*Maple*], 14  
 gcdex [*Maple*], 14  
 quo [*Maple*], 14  
 rem [*Maple*], 14  
 action, group, 17  
   adjoined, 25  
   affine translation, 44  
 Algebra, Fundamental Theorem of, 12  
 algebraic closure, 179  
 algebraic element, 85, 179  
 algebraic extension, 85, 179  
 algebraic number, 22  
 algebraic number, degree of, 23  
 algebraic number, representation of by an  
   arithmetic combination, 25  
 Algorithm, Division, 7  
 Algorithm, Division, for integral domains, 20  
 Algorithm, Euclidean, 9  
 arithmetic combination, 25  
 associated polynomial, 22  
 associates, 10  
 automorphism, field, 16  
 automorphism, Frobenius, 190  
 automorphisms, independence of, 157  
 characteristic of a field, 19  
 circle, constructible, 165  
 closure, algebraic, 179  
 coefficient, leading, 6  
 combination, arithmetic, 25  
 combination,  $K[X]$ -linear, 9  
 conjugacy class of subgroups, 130  
 conjugate element, 105  
 conjugate number, 42  
 conjugate subgroup, 130  
 constant, 6  
 constant polynomial, 6

206 **Index**

- constructible circle, 165
- constructible number, 166
- constructible point, 165
- criterion, Eisenstein irreducibility, 21
- criterion, mod  $p$  irreducibility, 20
- cyclotomic extension, 153
- cyclotomic polynomial, 154
  
- Dedekind's Lemma, 160
- degree of an algebraic number, 23
- degree of a polynomial, 6
- derivative, 50
- discriminant, 115, 125, 139
- discriminant resolvent, 125
- Division Algorithm, 7
- Division Algorithm for integral domains, 20
- division, polynomial, 7
- divisor, greatest common, 9, 11
- domain, integral, 10
- domain, principal ideal, 11
- domain, unique factorization, 10
  
- Eisenstein irreducibility criterion, 21
- element, algebraic, 85, 179
- element, conjugate, 105
- element, primitive, 64, 84
- element, separable, 181
- elementary symmetric polynomial, 121
- Euclidean Algorithm, 9
- evaluation, 25
- evaluation homomorphism, 32, 68, 69
- exponent of a group, 174, 189
- extension of isomorphism, 78
- extension, algebraic, 85, 179
- extension, cyclotomic, 153
- extension, field, 26
- extension, finite, 85
- extension, Galois, 104, 184
- extension, generated field, 25, 84
- extension, normal, 103, 182
- extension, radical, 171
- extension, separable, 181
- extension, simple, 64, 84
- extension, splitting, 66, 71, 181
- extension, transcendental, 85
  
- factor, linear, 12
- factor, polynomial, 6
- field automorphism, 16
- field extension, 26
- field extension, algebraic, 85, 179
- field extension, generated, 25, 84
- field extension, normal, 103, 182
- field extension, separable, 181
- field extension, simple, 64, 84
- field extension, splitting, 66, 71, 181
- field generated by an algebraic number, 25, 43
- field generated by several algebraic numbers, 63
- field monomorphism, 16
- field of rational functions, 85
- field operations, 25
- field, characteristic of, 19
- field, fixed, 107
- field, Galois, 189
- field, intermediate, 108
- field, multiply generated, 63
- field, number, 86
- field, perfect, 185
- field, splitting, 66, 71, 181
- finite extension, 85
- finitely generated field extension, 84
- First Isomorphism Theorem for rings, 15
- fixed field, 107
- form, reduced, 26, 30, 87
- Frobenius automorphism, 190
- Frobenius map, 185
- Fundamental Theorem of Algebra, 12
  
- Galois extension, 104, 184
- Galois field, 189
- Galois group, 105
- Galois resolvent, 117
- GCD, 9, 11
- generated field, 25
- generated field extension, 84
- generated group, 17
- generated ideal, 24, 67
- generation by an algebraic number, 43
- greatest common divisor, 9, 11
- group action, 17
- group, exponent of, 174, 189
- group, Galois, 105
- group, generated, 17
- group, permutation, 17
- group, solvable, 174
- group, symmetric, 17
  
- homomorphism, evaluation, 32, 68, 69
- homomorphism, trivial, 16
  
- ideal, 11
- ideal, generated, 24, 67
- identities, Newton's, 121
- independence of automorphisms, 157

## Index

207

- integral domain, 10
- integral domains, Division Algorithm for, 20
- intermediate field, 108
- inverse Galois problem, 106
- Irrationalities, Natural, Theorem on, 128
- irreducibility criterion, Eisenstein, 21
- irreducible element, 10
- irreducible polynomial, 6
- isomorphism, extension of, 78
  
- Kronecker's Theorem, 178
  
- Law, Tower, 50
- leading coefficient, 6
- least common multiple, 20
- Lemma, Dedekind's, 160
- linear factor, 12
- linear polynomial, 12
  
- map, Frobenius, 185
- minimal polynomial  $m_\alpha$  of  $\alpha$ , 23
- mod  $p$  irreducibility criterion, 20
- monic, 6
- monomial occurrence, 122
- monomorphism, field, 16
- multiple, least common, 20
- multiplicity of a root, 40
- multivariate polynomial, 67
  
- Natural Irrationalities, Theorem on, 128
- Newton's identities, 121
- normal extension, 103, 182
- number field, 86
- number of operations, 36
- number, algebraic, 22
- number, algebraic, representation of by an arithmetic combination, 25
- number, conjugate, 42
- number, constructible, 166
- number, root, 89
- number, transcendental, 23, 86
  
- occurrence, monomial, 122
- operations, field, 25
- orbit, 17
- orbit of a polynomial, 117
- over, 6, 23, 25, 26, 42, 63, 71, 78, 105
  
- perfect field, 185
- permutation, 17
- permutation group, 17
- permutation representation, 17
  
- point, constructible, 165
- polynomial, 5
- polynomial division, 7
- polynomial factor, 6
- polynomial orbit, 117
- polynomial quotient, 7, 20
- polynomial remainder, 7, 20
- polynomial ring, 5
- polynomial ring in  $n$  variables, 67
- polynomial solvable by radicals, 172
- polynomial stabilizer, 117
- polynomial, associated, 22
- polynomial, constant, 6
- polynomial, cyclotomic, 154
- polynomial, elementary symmetric, 121
- polynomial, irreducible, 6
- polynomial, linear, 12
- polynomial, minimal, 23
- polynomial, monic, 6
- polynomial, multivariate, 67
- polynomial, quotient, 20
- polynomial, reducible, 6
- polynomial, remainder, 20
- polynomial, separable, 180
- polynomial, split, 72
- polynomial, symmetric, 120
- prime subfield, 19, 87
- primitive element, 64, 84
- Primitive Element, Theorem of the, 186
- primitive root of unity, 152
- principal ideal domain, 11
- problem, inverse Galois, 106
- problem, subfield immersion, 59, 97
- product, semidirect, 161
  
- quotient polynomial, 7, 20
- quotient, polynomial, 7, 20
  
- radical extension, 171
- rational functions, field of, 85
- Rational Root Theorem, 20
- reduced form, 26, 30, 87
- reducible polynomial, 6
- reduction modulo  $m_{\alpha, K}$ , 28
- remainder polynomial, 7, 20
- remainder, polynomial, 7, 20
- representation of a number by an arithmetic combination, 25
- representation, permutation, 17
- resolvent, discriminant, 125
- resolvent, Galois, 117
- ring generated by an algebraic number, 26

## 208 Index

- ring, polynomial, in  $n$  variables, 67
- ring, polynomial, in one variable, 5
- root number, 89
- root of unity, 152
- root, multiplicity of, 40
  
- semidirect product, 161
- separable element, 181
- separable extension, 181
- separable polynomial, 180
- simple extension, 64, 84
- solvable by radicals, polynomial, 172
- solvable group, 174
- split polynomial, 72
- splitting field, 66, 71, 181
- stabilizer, 17
- stabilizer of a polynomial, 117
- subfield immersion problem, 59, 97
- subfield, prime, 19, 87
- subgroup, conjugate, 130
  
- subgroup, transitive, 135
- symmetric group, 17
- symmetric polynomial, 120
  
- Theorem of the Primitive Element, 186
- Theorem on Natural Irrationalities, 128
- Theorem, First Isomorphism, for rings, 15
- Theorem, Fundamental, of Algebra, 12
- Theorem, Kronecker's, 178
- Theorem, Rational Root, 20
- Tower Law, 50
- transcendental, 23
- transcendental extension, 85
- transcendental number, 86
- transitive subgroup, 135
- translation, affine, 44
- trivial homomorphism, 16
  
- unique factorization domain, 10
- unity, primitive root of, 152
- unity, root of, 152