

## Index

- abelian group, 20
- adjoined element, 94
- algebraic integers, 3, 53, 54, 103
  - closure properties, 4, 40, 103
  - congruent, 55
  - decomposable, 55
  - definition, 4, 39
  - divisibility, 54, 105
  - greatest common divisor, 106, 152
  - prime, 54
  - relatively prime, 152
  - units, 54, 106
- algebraic number, 53, 103
  - conjugate, 55
  - definition, 39
  - norm, 54, 111
- Arithmetica*
  - of Diophantus, 8
- Artin, 3, 46
- associates, 85, 106
- associativity
  - of composition, 20
- automorphism
  - of fields, 35
  
- Baker, 42
- basis
  - coordinates with respect to, 108
  - of cyclotomic integers, 140
  - of field, 108
  - of module, 67
- belonging to an exponent, 150
- binomial theorem
  - mod  $p$ , 11, 36
- biquadratic
  - reciprocity, 144
  - residues, 84
- Brahmagupta
  - identity, 18, 26, 28
  
- character
  - biquadratic, 38
  - cubic, 38
  - quadratic, 33
- circle division, 28, 31, 55, 138
- class
  - ideal number, 56
  - modulo a module, 64
  - modulo an algebraic integer, 118
  - modulo an ideal, 97, 122
  - number, 55, 61
  - of Gaussian integers, 84, 86
  - of ideals, 61, 146
  - of rational integers, 84
  - principal, 56
- class group, 19, 20
- class number, 41, 61
  - determination of, 149
  - Dirichlet formula, 42
  - finiteness, 42, 149
  - of cubic field, 149
  - of cyclotomic field, 42, 149
  - of number field, 41
  - of  $\mathbb{Q}(\sqrt{c})$ , 41
  - of quadratic fields, 149
  - of quadratic forms, 14, 56
- commutativity
  - of composition, 20
- complete system
  - of incongruent numbers, 122
  - of representatives, 65
- complex integers, 53, 84
- composite
  - Gaussian integer, 85
  - rational integer, 83
- composition
  - associativity of, 20
  - commutativity of, 20
  - Gauss definition, 20
  - Legendre definition, 20

154

- of forms, 17, 19, 28, 44, 100, 102
- of ideal classes, 146
- congruence
  - higher order, 57
  - modulo a module, 64
  - modulo an algebraic integer, 118
  - modulo an ideal, 97, 121
  - of algebraic integers, 55
  - of Gaussian integers, 85
  - of quadratic integers, 87
  - of rational integers, 84
  - roots of, 137
- conjugate
  - algebraic numbers, 55
  - and norm, 112
  - fields, 110
  - ideals, 97
  - in quadratic field, 89, 116
  - number, 41, 110
  - numbers in quadratic field, 87
  - periods, 143
- construction
  - straightedge and compass, 31, 32
- continued fraction, 4
- continuity, 58
- coordinates
  - with respect to a basis, 108
- correspondence
  - of numbers and ideals, 121
- cubic
  - field, 117
  - reciprocity, 144
- cyclotomic
  - equation, 31, 32, 139
  - field, 139
  - integers, 30, 32, 140
- decomposable numbers, 55
- Dedekind
  - and Weber theory, 46
  - avoidance of symmetric functions, 41
  - class number theorem, 42
  - definition of algebraic integer, 39
  - domain, 5
  - invention of ideals, 3
  - proof of quadratic reciprocity, 37
  - proof of two square theorem, 25
  - section, 44, 58
  - Supplement to Dirichlet, 20
  - theory of ideals, 29, 37
- degree
  - of a field, 54, 108
  - of a form, 56
  - of a prime ideal, 124
- Descartes, 10
- determinant, 71
  - of a quadratic form, 14, 98

*Index*

- Diophantine equation, 8
- Diophantus, 8
  - Arithmetica*, 8
  - identity, 9, 18, 23
- Dirichlet, 56, 149
  - class number formula, 42
  - theorem on primes, 42, 149
  - Vorlesungen*, 5, 21, 40, 45, 53, 61, 84, 87, 98, 102, 119, 125, 135–137, 143, 149
- discriminant, 112
  - determines quadratic field, 117
  - is rational, 113
  - of cyclotomic field, 141
  - of field, 116
  - of Gaussian field, 145
  - of quadratic form, 14
- Disquisitiones*
  - of Gauss, 7, 33, 40
- divisibility
  - by ideal number, 58
  - by  $n^{\text{th}}$  power, 90
  - of algebraic integers, 54, 105
  - of ideals, 60, 98, 120
  - of modules, 63
  - of quadratic integers, 87
  - of rational integers, 83
- divisor, 7
  - behaviour as a, 89
  - ideal, 60
  - of a module, 63
  - of an ideal, 133
- domain, 5
  - Dedekind, 5
- Eisenstein, 40, 144, 149
- elementary transformations, 77
- Elements*
  - of Euclid, 6, 7, 53
- equation
  - cyclotomic, 31, 32, 139
  - Pell, 4, 8
  - Pythagorean, 29
  - $x^3 + y^3 = z^3$ , 30
  - $x^4 + y^4 = z^2$ , 10
  - $x^4 + y^4 = z^4$ , 10
  - $y^3 = x^2 + 2$ , 9, 21
- equivalence
  - of ideal factors, 28
  - of quadratic forms, 13
- equivalent
  - ideal numbers, 56
  - ideals, 146
- Euclid, 53
  - algorithm for gcd, 12, 84
  - Elements*, 6, 7, 53
  - formula for Pythagorean triples, 6, 10

- Euclidean algorithm, 12, 84  
 for quadratic integers, 22  
 in Gaussian integers, 23  
 in  $\mathbb{Z}[\sqrt{-2}]$ , 26
- Euler, 9  
 conjecture on  $x^2 + 5y^2$ , 13, 17  
 conjectured quadratic reciprocity, 16  
 criterion, 17, 37  
 proof of two square theorem, 11
- Fermat, 9  
 and  $x^2 + 5y^2$ , 6  
 conjecture on  $x^2 + 5y^2$ , 13, 17  
 last theorem, 10, 29, 38  
 last theorem for  $n = 3$ , 30  
 last theorem for  $n = 4$ , 29  
 little theorem, 11, 15, 137  
 notes on Diophantus, 10, 29  
 numbers, 31  
 primes, 31  
 two square theorem, 9, 11, 85, 145  
 use of Pythagorean triples, 10
- field  
 automorphism, 35  
 basis of, 108  
 closure properties, 5, 109  
 conjugate, 110  
 cubic, 117  
 cyclotomic, 139  
 definition, 107  
 degree of, 108  
 discriminant of, 116  
 fundamental number of, 116  
 Galois, 111  
 normal, 111, 116  
 of degree  $n$ , 54  
 of finite degree, 5, 39, 41, 106, 108  
 quadratic, 116, 143
- finitely generated module, 67, 95
- forms  
 binary quadratic, 56  
 of degree  $n$ , 56
- fundamental number, 116
- Galois, 61, 94, 137, 138  
 field, 111
- Galois theory, 35, 45
- Gauss, 6, 53, 77, 98, 102, 137, 144  
 complex integers, 84  
 composition of forms, 28  
 definition of composition, 20  
*Disquisitiones*, 7, 33, 40, 77, 84, 100, 127, 144, 149  
 existence of primitive roots, 16  
 proofs of quadratic reciprocity, 37  
 proved quadratic reciprocity, 16  
 sums, 32
- Gaussian integers, 22, 84, 97, 145  
 class, 86  
 composite, 85  
 congruence, 85  
 Euclidean algorithm, 23  
 laws of divisibility, 85  
 norm, 22, 85  
 prime, 85  
 unique prime factorisation, 22, 24, 85  
 units, 23, 85
- Gaussian primes, 23  
 and two square theorem, 24
- greatest common divisor  
 Euclidean algorithm, 84  
 of algebraic integers, 106, 152  
 of ideals, 121, 134  
 of modules, 63  
 of rational integers, 84
- group, 82, 142  
 abelian, 20  
 class, 19, 20
- Hilbert *Zahlbericht*, 38, 46
- ideal, 5, 57, 58  
 class of, 61, 146  
 class representative, 146  
 classes modulo, 122  
 congruence modulo, 97, 121  
 conjugate, 97  
 defining properties, 96  
 divisors of, 60, 133  
 fundamental properties, 59  
 in field of degree  $n$ , 119  
 norm of, 97, 122  
 numbers, 57  
 power of, 125, 150  
 prime, 60, 101, 123  
 prime factors, 56  
 principal, 59, 97, 120
- ideal number  
 class, 56  
 definition, 150  
 equivalent, 56  
 of quadratic field, 90
- ideals  
 divisibility of, 98, 120  
 equivalent, 146  
 greatest common divisor, 121, 134  
 in  $\mathbb{Z}$ , 7, 120  
 least common multiple, 121, 134  
 multiplication of, 60, 98, 125  
 of quadratic integers, 95  
 product of, 43, 44, 60, 125  
 relatively prime, 126, 134  
 unique prime factorisation, 102, 130
- identity

Brahmagupta, 18, 26, 28  
 Diophantus, 9, 18, 23  
   isomorphism, 110  
 Lagrange, 18  
 independent numbers, 71, 108  
 infinite descent, 11  
 infinity  
   horror of, 44  
 integers  
   algebraic, 54, 103  
   complex, 53  
   cubic, 35  
   cyclotomic, 30, 32, 140  
   Gaussian, 22, 84, 97  
   imaginary quadratic, 25  
   in field of degree  $n$ , 113  
   Kummer, 40, 43  
   of  $\mathbb{Q}(\alpha)$ , 5  
   of quadratic field, 102, 116  
   quadratic, 21  
   rational, 4, 83  
 inverse  
   ideal class, 147  
   isomorphism, 110  
   mod  $p$ , 12, 34  
   substitution, 13  
 irrational numbers, 8, 57  
 irreducible  
   equation, 54, 107  
   polynomial, 107  
   system, 107  
 irreducible system, 71  
 isomorphism, 108  
   determined by choice of root, 110  
   fixes rational numbers, 110  
   identity, 110  
   inverse, 110  
   onto number field, 41  
 Jacobi, 144  
 Kronecker, 94  
   abelian group axioms, 21  
   adjoined ideal numbers, 94  
   opposition to infinity, 44  
   theory of fields, 46  
 Kummer, 6, 55, 83, 86, 90, 94, 138, 149  
   ideal factors, 28  
   integers, 40, 43  
   main theorem, 142  
 Lagrange, 6  
   identity, 18  
   proof of two squares theorem, 15  
   reduction process, 41  
 laws of divisibility  
   in Gaussian integers, 85

  in quadratic integers, 86  
   in rational integers, 85, 88  
 least common multiple  
   of ideals, 121, 134  
   of modules, 63  
 Legendre  
   definition of composition, 20  
   notation, 143  
   symbol, 33  
 linear algebra, 41  
 Lipschitz, 44  
 module, 62  
   as a group, 82  
   basis of, 67  
   closure properties, 5  
   congruence modulo, 64  
   divisor of, 63  
   finitely generated, 67, 95  
   multiple of, 63  
   zero, 63  
 modules  
   divisibility of, 63  
   greatest common divisor of, 63  
   least common multiple of, 63  
   multiplication of, 98  
 modulus, 55, 84, 118  
 multiple, 7  
   of algebraic integer, 105  
   of module, 63  
 multiplication  
   of ideals, 60, 98, 125  
   of modules, 98  
 multiplicative property  
   of quadratic character, 34  
 Newton, 40  
 Noether, 3, 46  
 norm  
   and conjugates, 41, 112  
   in field of finite degree, 41  
   in  $\mathbb{Z}[\sqrt{-5}]$ , 27  
   in  $\mathbb{Z}[\sqrt{-c}]$ , 25  
   is rational, 113  
   multiplicative property, 23, 26, 41, 132  
   of algebraic number, 54, 111  
   of Gaussian integer, 22, 85  
   of ideal, 97, 122  
   of principal ideal, 122  
   of quadratic integer, 87  
 normal field, 111, 116  
 number  
   algebraic, 39, 53, 103  
   classes, 55  
   conjugate, 110  
   ideal, 57

- irrational, 8, 57
- order, 127
  - of a group element, 16
  - of quadratic forms, 127
- Pell equation, 4, 8
- periods, 143
  - conjugate, 143
- permutation, 108
- Plimpton 322, 6
- prime, 7
  - divisor property, 7, 22, 23
  - Fermat, 31
  - Gaussian, 23, 85
  - ideal, 101
  - in algebraic integers, 54
  - in  $\mathbb{Q}(\alpha)$ , 5
  - in  $\mathbb{Z}[\sqrt{-2}]$ , 26
  - rational, 83
- prime factors
  - ideal, 56
- prime ideal, 60, 101, 123
  - degree of, 124
  - has principal ideal multiple, 130
  - of quadratic field, 144
- primitive root, 16, 33, 137, 139, 142
- principal
  - class, 56
  - ideal, 59, 97, 120
  - ideal class, 146
- product
  - of ideal classes, 146
  - of ideals, 60, 125
- Pythagoras, 6, 8
  - theorem, 8
- Pythagorean triples, 6
  - and right-angled triangles, 8
  - Euclid's formula, 6, 10
  - primitive, 10
  - used by Fermat, 10
- quadratic
  - character, 33
  - character of  $-1$ , 17, 144
  - character symbol, 33
  - fields, 143
  - reciprocity, 16, 36, 37, 144
- residues, 16, 143
- quadratic field, 116
  - class number, 149
  - conjugate in, 89, 116
  - discriminant of, 117
  - failure of unique prime factorisation, 87
  - ideal number of, 90
  - integers of, 102, 116
  - prime ideals of, 144
  - units, 86
- quadratic forms, 10
  - $2x^2 + 2xy + 3y^2$ , 15, 17, 28
  - $x^2 + 2y^2$ , 12, 15, 26
  - $x^2 + 3y^2$ , 12, 15
  - $x^2 + 5y^2$ , 6, 12, 15, 17, 27
  - $x^2 + y^2$ , 12, 15, 25
  - class number, 14
  - composition of, 17, 19, 100, 102
  - determinant of, 14, 98
  - discriminant of, 14
  - equivalent, 13
  - inequivalent, 14, 15, 27
  - orders of, 127
  - reduced, 14
  - reduction, 41
- quadratic integers, 21
  - and cyclotomic integers, 32
  - congruence, 87
  - divisibility, 87
  - Euclidean algorithm, 22
  - ideals, 95
  - laws of divisibility, 86
  - norm, 87
- rational
  - composite number, 83
  - integers, 4, 53, 83
  - numbers, 107
  - operations, 107
  - prime, 83
  - units, 83
- rational numbers
  - field of, 107
  - fixed by isomorphism, 110
- reciprocity
  - biquadratic, 144
  - cubic, 38, 144
  - laws, 28, 38
  - quadratic, 36, 37, 144
  - reduced quadratic forms, 14
- relatively prime
  - algebraic integers, 152
  - ideals, 126, 134
- representative
  - of ideal class, 146
  - of number class, 65
- representatives
  - complete system, 65
- residues
  - biquadratic, 84
  - quadratic, 143
- Riemann, 45
  - surfaces, 46
- ring, 4
  - closure properties, 5

## root

- of congruence, 137
- of unity, 28, 38
- primitive, 33, 137, 139, 142

## Schönemann, 137

section, 44, 58

Serret, 137

Stark, 42

subfield, 142

substitution, 108

inverse, 13

unimodular, 14

symmetric functions, 41, 113

Newton theorem, 40

## two square theorem, 9

and Gaussian primes, 24

Dedekind proof, 25, 145

Euler proof, 11

Fermat proof, 11

Lagrange proof, 15

## unimodular substitution, 14

## unique prime factorisation

and equivalence of forms, 28

failure in  $\mathbb{Z}[\sqrt{-3}]$ , 30failure in  $\mathbb{Z}[\sqrt{-5}]$ , 5, 27failure in  $\mathbb{Z}[\zeta_{23}]$ , 32

failure in cyclotomic integers, 56

failure in quadratic field, 87

for ideals, 3, 130

in complex integers, 56

in *Disquisitiones*, 7

in Gaussian integers, 22, 24, 85

in rational integers, 22, 56, 84

in  $\mathbb{Z}[\sqrt{-2}]$ , 26in  $\mathbb{Z}[\zeta_3]$ , 30

of ideals, 5, 102

## units

in algebraic integers, 54, 106

in Gaussian integers, 23, 85

in quadratic field, 86

in rational integers, 83

## vector space, 41

## Weber, 45

and Dedekind, 46

## Weil, 13

## zero module, 63