Index

Abel, Niels Henrik, 100
  theorem on genus, 206, 210
Abelian group
  additive notation, 73
  as a $\mathbb{Z}$-module, 172
  axioms, 69
  definition, 69
  finite, 68
  of fractional ideals, 199
absolute value
  of complex number, 39
  multiplicative property, 40
AC. *See* axiom of choice, 122
ACA_0, 125
ACC. *See* ascending chain condition, 114
additive notation, 73
al-Khwarizmi, 26
algebra
  commutative, xii
  linear, xii
  origin of word, 26
algebraic
  curve, 169, 207
  field extension, 90
  function, 184
    definition, 207
    integral, 184
    ring, 188
  function field, 184, 188
    gives Riemann surface, 210
  function theory, 205
  geometry, 27, 57, 188
  integer, 11, 14, 31, 53
    defined by Dedekind, 31, 67
    definition, 93
    factorization of, 95
    is integer over $\mathbb{Z}$, 183
    second definition, 96
    sum and product, 132
    used by Euler, 33
  number, 86, 101
    as fraction of integers, 175
    as matrix, 136
    norm via det, 138, 161
    sum and product, 132
    trace, 161
  number field, 30, 78, 86
    conjugates in, 88
    embedded in $\mathbb{C}$, 142
    integer of, 32, 93, 94, 174
    Kronecker approach, 31
arithmetic comprehension axiom, 125
  algebraic equivalents, 125
Artin, Emil, 150
ascending chain, 110
ascending chain condition, 114
  as “divisor chain theorem,”, 191
  and finite generation, 117
  in Hilbert’s basis theorem, 117
  in a PID, 111
axiom of choice, 115, 122
  for algebraists, 123
  and existence of basis, 128
  and maximal ideals, 123
  and nonmeasurability, 123
  and vector space basis, 123
  and well-ordering, 120, 123
  and Zorn’s lemma, 123

© in this web service Cambridge University Press & Assessment

CAMBRIDGE

Cambridge University Press & Assessment
978-1-316-51895-3 — Algebraic Number Theory for Beginners
John Stillwell
Index
More Information

axioms
  Abelian group, 69
  for determinant, 150
  field, 19, 79
  of infinity, 123
  Peano (for arithmetic), 25, 124
  ring, 15, 79
  for set existence, 124
  vector space, 127, 146

basis
  and axiom of choice, 128
  of field extension, 90
  finite, 128
  Hamel, 129
  independence, 136
    of charpoly, 149, 159
    of det, 136, 149, 159
    of norm, 149
    of trace, 136, 149
  integral, 149, 168, 175
    definition, 176
    existence, 176
  of module, 173, 180
  of vector space, 126
  for $\mathbb{Q}(\alpha)$, 91
Bernoulli, Jakob, 38
Bhaskara II, 25
Binet, Jacques, 170
binomial
  coefficient, 28
    in Chinese mathematics, 28
    and Fermat's little theorem, 29
  theorem, 28
Bourbaki, 123
Brahmagupta, 25
  identity, 58, 66
branch point, 207

$\mathbb{C}$, 70, 99
  Cauchy construction, 102
calculus, 27
  of algebraic functions, 205
  and FTA, 205
Cantor, Georg, 101
  assumed well-ordering, 123
  discovered uncountability, 121
  pairing function, 120
Cardano, Gerolamo, 26
Cauchy, Augustin-Louis
  construction of $\mathbb{C}$, 102
  rebuilt determinant theory, 170

Cayley, Arthur, 148
characteristic polynomial, xii, 149
  definition, 159
  is basis-independent, 149, 159
  is minimal, 162
charpoly. *See* characteristic polynomial, 149
Chinese remainder theorem, 71
choice function, 122
class group, 67, 174
class number, 64
cofactor, 153
Cohen, Paul, 123
commutative algebra, xii
complex number, 39, 55
  absolute value, 39
  multiplication, 40
composition of forms, 66
  associativity, 67
  by Dedekind, 76
congruence, 19
  class, 19
    mod a module, 173
    mod a polynomial, 85, 88
    mod an ideal, 109
  mod a module, 173
  mod a polynomial, 84
  mod an ideal, 104, 109
conjugate, 13
  in algebraic number field, 88, 143
  in cyclotomic field, 164
  of Gaussian integer, 41
  ideal, 191
  multiplicative property, 13, 41
  roots of minimal polynomial, 143
  in $\mathbb{Z}[\sqrt{-2}]$, 51
content, 96
continued fraction, 4
  and Euclidean algorithm, 4
  infinite, 12
countability, 119
Cramer, Gabriel, 145
  rule, 158, 169
cyclotomic
  field, 164, 178
  integer, 102, 179
  polynomial, 98
  reason for name, 98

Dedekind, Richard, xii
  algebraic function theory, 188
  composition of forms, 76
  defined algebraic integers, 31, 103

© in this web service Cambridge University Press & Assessment www.cambridge.org

  - domain, xii
  - ideals, 75
  - induction, 25
  - introduced fractional ideals, 204
  - module concept, 173
  - norm concept, 58
  - on norm and discriminant, 168
  - on Vandermonde deteminant, 169
  - praise for Kummer, 75
  - product theorem, 131
  - realized ideal numbers, 104
  - supplements to Dirichlet, 76
  - theory of algebraic integers, 67, 76, 186
  - theory of ideals, 68
- Dedekind domain, 189, 197
  - in algebraic geometry, 205
  - definition, 193
- Dedekind ring. *See* Dedekind domain, 193
- degree, 84
  - as dimension, 133
  - function, 17
  - of zero polynomial, 16, 84
- del Ferro, Scipione, 26
- dependent choice, 116, 117, 123
- derivative
  - criterion for multiple root, 140
  - of polynomial, 139
  - product rule, 140
- Descartes, René, 27
  - algebraic geometry, 57
  - factor theorem, 22
- det. *See* determinant, 58
- determinant, xii, 126
  - axioms, 150
  - cofactor, 153
  - column expansion, 155
  - computing rules, 154
  - criterion for linear dependence, 156
  - criterion for nonzero solution, 94, 157
  - definition of charpoly, 149
  - definition of norm, 138, 149
  - existence, 153
  - is basis-independent, 136, 149, 159
  - is coefficient of charpoly, 160
  - and linear equations, 145, 156
  - multiplicative property, 58, 66, 149
    - proof, 152
  - and permutations, 152
  - row expansion, 155
  - in study of algebraic integers, 94, 132
  - theory, 149
    - history, 169
  - of transpose, 155
  - uniqueness, 152
  - Vandermonde, 166
- diagonal argument, 122
- differential geometry, 27
- dimension
  - as degree, 133
  - of extension field, 90
    - notation, 131
  - finite, 128
  - of free module, 180
  - invariance under isomorphism, 134
  - relative, 142
  - of a subspace, 132
  - of vector space, 126, 128
- Diophantine equation, 33
  - linear, 6
  - of higher degree, 7
- Diophantus, 26, 33
  - *Arithmetica*, 38, 53, 55
  - chord method, 34, 54
  - identity, 39, 55
    - and multiplicative property, 39
    - and sums of squares, 38, 59
    - as composition of forms, 66
  - tangent method, 54, 55
- direct product
  - of groups, 69
  - of rings, 71
- direct sum, 74
- Dirichlet, Peter Lejeune, 31
  - simplified Gauss, 76
- discriminant, xii, 164
  - criterion for a basis, 167
  - definition, 165
  - Lagrange, 167
  - of quadratic form, 59, 64
  - test for basis, 149
  - of transformed basis, 177
  - trace, in terms of, 165
  - of transformed basis, 166
  - used to find module bases, 171, 176
- division
  - in field, 19
  - ideal, 190
  - and product of ideals, 200
  - property, 2
  - with remainder, 2
  - in a ring, 15
- division property, 2
  - fails in $\mathbb{Z}[\sqrt{-3}]$, 52

division property (Cont.)
  fails in $\mathbb{Z}[\sqrt{-5}]$, 63
  for polynomials, 16
  in $\mathbb{Z}[i]$, 42, 44
  in $\mathbb{Z}[\sqrt{-2}]$, 45, 52
  in $\mathbb{Z}[\zeta]$, 53
division with remainder
  and continued fraction, 4
  and matrices, 5
  in $\mathbb{N}$, 2
divisor, 2
domain, 82
  Dedekind, 189
    definition, 193
  definition, 82
  Euclidean, 17
  finite, 196
  fractions of, 82
  integrally closed, 184
  Noetherian, 194
  principal ideal, 8, 10, 108, 173, 190
duplication of the cube, 133

Eisenstein, Gotthold, 31
  and algebraic integers, 102
  irreducibility criterion, 97
equation
  cubic, 26
  Diophantine, 33
    of higher degree, 7
    linear, 6, 25
    quadratic, 25
  Pell, 13
  polynomial, xi
equivalence
  class, 64, 79
    disjointness, 81
  of fractions, 79
  of quadratic forms, 59, 63
  relation, 64, 79
    reflexivity, 64, 79
    symmetry, 64, 79
    transitivity, 64, 79
Euclid
  algorithm, 3
  ancestor of ACC, 191
  Elements, 1, 11, 24, 101
  formula for Pythagorean triples, 35, 36
  induction, 24, 37
  prime divisor property, 1, 189
  proved infinitude of primes, 2
Euclidean algorithm, 1, 3
  and continued fraction, 4
  by division with remainder, 4
  history, 25
  and irrationality, 11
  for polynomials, 16, 31, 84
  by subtraction, 3
  symbolic form, 6
Euclidean domain, 17
Euler, Leonhard
  conjecture on $x^2 + 5y^2$, 60
  phi function, 73
  solution of $y^3 = x^2 + 3$, 50
  on sums of squares, 46
  used algebraic integers, 31, 33
extension field, 89
  algebraic, 90
  basis, 90, 91
  dimension, 90

factor
  of ideal, 104
  of polynomial, 22
  of sum of squares, 45
  theorem, 22
    for multivariable polynomials, 23, 166
    for polynomials over a ring, 22
Fermat, Pierre de
  conjecture on $x^2 + 5y^2$, 60
  and Diophantine equations, 33
  last theorem, 33
  last theorem for $n = 4$, 36
  little theorem, 20, 29, 49
    and binomial coefficients, 29
  and Pell equation, 25
  primes, 24
  on primes of form $x^2 + ky^2$, 59
  proof using Pythagorean triples, 206
  theorems on primes, 60
  two square theorem, 33, 49
    Lagrange proof, 65
Ferrari, Lodovico, 100
Fibonacci
  numbers, 4
  proved Diophantus identity, 39
field, 1, 19, 30
  algebraic number, 30, 86
  of algebraic functions, 184
  axioms, 19, 79
  called Körper by Dedekind, 30
  cyclotomic, 164, 178

CAMBRIDGE

Cambridge University Press & Assessment
978-1-316-51895-3 — Algebraic Number Theory for Beginners Algebraic Number Theory for Beginners
John Stillwell
Index
More Information

  - extension, 89
    - dimension, 131
  - finite, 19, 30
    - as quotient, 112
  - of fractions, 82
  - isomorphism, 87
- Fontana, Niccolò, 26
- four-group, 69
- fraction
  - of a domain, 82, 183
  - field, 82
- fractions, 79
  - product, 80
  - sum, 80
- free module, 171
  - basis, 180
  - definition, 180
  - rank, 178
    - definition, 180
- FTA *see* fundamental theorem of algebra, 86
- fundamental theorem
  - of algebra, 86, 99, 140
    - and calculus, 205
    - provable in RCA_0, 125
  - of arithmetic, 1, 9
  - of finite Abelian groups, 68

- Galois, Evariste, xi, 100
  - discovered finite fields, 30
  - group, xi
- Gauss, Carl Friedrich
  - composition of forms, 67
  - on determinants, 169
  - *Disquisitiones*, 62, 76
  - lemma, 96
  - proofs of FTA, 100
  - theorem on primitive root, 70
  - theory of quadratic forms, 62
- Gaussian elimination, 144
  - and computation of det, 155
- Gaussian integer, 40
  - conjugate, 41
  - division property, 42, 44
  - norm, 41
- Gaussian prime, 41
  - classification, 47
  - factorization
    - existence, 41
    - uniqueness, 42–44
- gcd. *See* greatest common divisor, 3
- generator of ideal, 108
- generators and relations, 179
- generators of module, 172, 179
- genus, 206
  - and rational functions, 209
  - of Riemann surface, 210
  - topological interpretation, 209
- Gödel, Kurt, 123
- Grassmann, Hermann, 25
  - on arithmetic, 25, 146
  - exchange lemma, 130
  - inner product, 145
  - linear geometry, 145
  - on outer product and det, 170
- greatest common divisor, 1, 3, 9
  - in Dedekind domain, 201
  - of ideals, 190
  - of polynomials, 16, 84
  - in $\mathbb{Z}[\sqrt{-5}]$, 191
- group, xi, 64
  - Abelian, 69, 127
  - cyclic, 69, 70
  - direct product, 69
  - finite Abelian, 68
  - Galois, xi
  - solvable, xii

- Halmos, Paul, 148
- Hamel, Georg, 129
- Hilbert, David, 32
  - basis theorem, 116, 117
  - “not mathematics but theology,”, 117
- homomorphism, 104
  - canonical, 111
  - of groups, 112
  - kernel, 111
  - preserves structure, 147
  - of rings, 111
  - of vector spaces, 134
- Horner’s method, 28

- ideal, xii, 68, 71, 104
  - class, 174
  - conjugate, 191
  - definition, 108
  - division, 190
  - fractional, 197
  - gcd, 190
  - generators, 108
  - inverse, 189, 195
    - in Dedekind domain, 197
  - as kernel of homomorphism, 111

© in this web service Cambridge University Press & Assessment www.cambridge.org

- ideal (Cont.)
  - lcm, 191
  - maximal, 112, 113
    - existence, 116
    - inverse of, 197
    - is prime, 192
  - as a module, 173
  - nonprincipal, 108
  - number, 104
    - in $\mathbb{Z}[\sqrt{-5}]$, 106
  - prime, 104, 189
    - definition, 192
    - in Noetherian domain, 194
    - not maximal, 193
    - quotient characterization, 192
    - of $\mathbb{Z}_E$, 196
  - prime factorization, 78
  - principal, 8, 65, 108
    - inverse of, 198
  - product, 194
  - unique prime factorization, 104, 199
  - in $\mathbb{Z}$, 108
  - in $\mathbb{Z}[\sqrt{-5}]$, 106
- induction
  - in Dedekind, 25
  - in Euclid, 24
  - in Grassmann, 25
  - in Pascal, 28
  - in Peano axioms, 25
  - and well-ordering, 24
- infinity
  - axioms of, 123
  - countable, 119
  - of prime numbers, 3
  - uncountable, 121
- inner product, 145
- integer, 5
  - algebraic, 11, 14, 31, 53
    - defined by Dedekind, 31
    - definition, 93
    - factorization of, 95
    - second definition, 96
  - of algebraic number field, 32, 78, 93, 94, 174
  - cyclotomic, 102, 179
  - over a domain, 183, 187
  - of a field, 183
  - Gaussian, 40
  - over a ring, 182
    - definition, 183
  - quadratic, 61
- integral
  - algebraic function, 184, 188
  - basis, 149, 168, 175
    - definition, 176
    - existence, 176
  - closure, 184
    - introduced by Noether, 187
  - over ring, 183, 184
    - is transitive relation, 186
- integral domain. *See* domain, 82
- integrally closed, 184
- intermediate value theorem, 100
- inverse
  - additive, 18, 127
  - ideal, 189, 195
    - in Dedekind domain, 197
  - of maximal ideal, 197
  - mod a prime polynomial, 84
  - multiplicative, 19
  - of nonzero ideal, 200
  - of principal ideal, 198
- irrationality, 10
  - discovered by Pythagoreans, 10
  - and Euclidean algorithm, 11
  - of $\sqrt{2}$, 10
    - via continued fraction, 12
  - via unique prime factorization, 11
- irreducible polynomial, 84
  - has no multiple root, 140
- isomorphism
  - of fields, 87
    - into $\mathbb{C}$, 142
  - leaves dimension invariant, 134
  - of vector spaces, 134

- Kaplansky, Irving, 148
- kernel, 111
- Knobloch, Eberhard, 169
- Kronecker, Leopold
  - on Abelian groups, 68, 76
  - avoided actual infinity, 99
  - concept of algebraic number field, 31
  - opposed to Cantor, 101
  - replacement for FTA, 99
  - solution field construction, 101
- Krull, Wolfgang, 114
  - on Dedekind domain properties, 202
  - maximal ideal theorem, 116
- Kummer, Ernst Eduard, 31, 75
  - cyclotomic integers, 102
  - ideal numbers, 75, 104
- Kuratowski, Kazimierz, 123

CAMBRIDGE

Beginners
Cambridge University Press & Assessment
John Stillwell
978-1-316-51895-3 — Algebraic Number Theory for Beginners Algebraic Number Theory for
Index
More Information

- Lagrange, Joseph-Louis
  - discriminant, 64, 167
  - equivalence of quadratic forms, 59
  - lemma, 49
  - solved general Pell equation, 25
  - theorem on polynomials, 22, 49
- Laplace, Pierre-Simon, 169
- lcm. *See* least common multiple, 9
- least common multiple
  - in Dedekind domain, 201
  - of ideals, 191
- Leibniz, Gottfried Wilhelm, 169
- lemma
  - exchange, 130
  - Gauss, 96
  - Lagrange, 49
  - Zorn, 115, 116
- lexicographic order, 119
- linear
  - algebra, xii
    - basis-free, 148
    - history, 144
    - for modules, 173
  - equations, 127
    - and Cramer's rule, 145, 158
    - and det, 156
    - and the determinant, 145
    - Diophantine, 6
    - over domain, 157
    - and Gaussian elimination, 144
    - homogeneous, 157
  - independence, 90
    - of basis elements, 90
    - definition, 128
    - determinant criterion, 156
  - map, 126, 147
    - composition, 136
    - definition, 134
    - injective, 134, 135
    - in Lagrange, 147
    - matrix for, 136
    - of modules, 173
    - surjective, 134, 135
  - space, 145

- matrix, 5, 136
  - for algebraic number, 136
  - for basis change, 159
  - basis-independent properties, 136
  - introduced by Cayley, 148
  - inverse, 148
  - for linear map, 126, 136
    - depends on basis, 136
  - multiplication, 136, 137
  - for quaternion, 139
  - sum and product, 148
  - transpose, 155, 165
- maximal ideal, 112
  - existence, 114, 116
    - and axiom of choice, 123
  - inverse of, 197
  - is prime, 192
  - quotient criterion, 113
  - of $\mathbb{Z}[\sqrt{-5}]$, 114
- minimal polynomial, 86, 97
  - is characteristic, 162
  - and conjugates, 143
- module, 126, 136, 171
  - as Abelian group, 172
  - basis, 173
  - definition, 172
  - free, 171
    - definition, 180
    - rank, 178
  - generators, 172, 179
  - quotient, 173
  - reason for name, 173
- monic polynomial, 31, 93, 97
- Muir, Sir Thomas, 169
- multiplicative property
  - of absolute value, 40
  - of conjugate, 13, 41
  - of det, 58, 66, 149
    - proof, 152
  - goes from det to norm, 138, 161
  - of isomorphism, 163
  - of norm, 39, 57
    - via the σ_I, 163

- $\mathbb{N}$, 2
  - is well ordered, 2, 24
  - a potential infinity, 99
- *Nine Chapters*, 144
- Noether, Emmy, xii
  - and algebraic geometry, 188
  - ascending chain condition, 191
  - and axiom of choice, 119
  - on Dedekind domain properties, 202, 204
  - introduced ACC, 114, 116
  - theory of integers, 187
  - theory of rings, 32
  - urged reading of Dedekind, 77
  - used dependent choice, 116
- Noetherian domain, 194

© in this web service Cambridge University Press & Assessment www.cambridge.org

CAMBRIDGE

Cambridge University Press & Assessment
978-1-316-51895-3 — Algebraic Number Theory for Beginners Algebraic Number Theory for Beginners
John Stillwell
Index
More Information

Noetherian ring, 104, 113
  definition, 114
  equivalent properties, 114
  property of $\mathbb{Z}_E$, 182
nonmeasurability, 123
norm
  and absolute value, 57
  of algebraic integer, 57
  of algebraic number, 161
  of complex number, 39
  in cyclotomic field, 164
  as determinant, 58, 149
  of Gaussian integer, 41
  is basis-independent, 149
  is multiplicative, 39, 57, 161
  as product of conjugates, 57, 58
  relative, 161
  in terms of σ_i, 163
number
  algebraic, 86, 101
  complex, 39, 55
  ideal, 104
  integer, 5
  irrational, 10
  natural, 2
  rational, 10

Pascal, Blaise
  theorems on binomial coefficients, 28
  triangle, 28
  used induction, 28
Peano, Giuseppe, 25
  axioms for arithmetic, 25, 124
  axioms for vector spaces, 146
Pell equation, xii, 13, 75
  and continued fractions, 25
  general, 25
  and $\sqrt{2}$, 25
permutation, 152
  even or odd, 153, 169
  transposition, 153
PID. *See* principal ideal domain, 108
polynomial
  characteristic, xii, 149, 159
  content, 96
  cyclotomic, 98
  derivative, 139
  factor, 22
  as integral rational function, 184
  irreducible, 31, 84
  minimal, 86, 97
    and conjugates, 143
  monic, 31, 93, 97
  number of roots, 22
  prime, 84
  ring, 15, 83
    multivariable, 84
    $R[x]$, 17
    unique prime factorization, 84
prime, 2
  Gaussian, 41
  ideal, 104, 189
    definition, 192
    divisor property, 194
    indivisibility, 201
    in Noetherian domain, 194
    which is not maximal, 193
    quotient characterization, 192
    of $\mathbb{Z}_E$, 196
  in a ring, 15
  natural number, 1
  of form $x^2 + ky^2$, 60
  of $\mathbb{Z}[\sqrt{-2}]$, 48
  polynomial, 84
prime divisor property, 6
  defines prime ideal, 189, 192
  for ideals, 194
  in $\mathbb{Q}[x]$, 16
  in $\mathbb{Z}$, 8, 192
  of natural numbers, 1
prime factorization
  existence, 2
  in $\mathbb{Z}[i]$, 41
  uniqueness, 9
prime polynomial. *See* irreducible polynomial, 84
primitive element, 92
  theorem, 139
    proof, 140
primitive root, 70
principal ideal, 65, 88
  definition, 108
  domain, 8, 10, 108, 173, 180, 190
  inverse of, 198
  notation, 108, 112
  shape, 174
  of $\mathbb{Z}[\sqrt{-5}]$, 174
product of ideals, 194
Pythagorean
  discovery of irrationality, 10
  equation, 75

© in this web service Cambridge University Press & Assessment

  - theorem, 44, 52
    - and inner product, 146
  - triples, 34, 206
    - Euclid’s formula, 35
    - primitive, 36

- $\mathbb{Q}$, 10
- $\mathbb{Q}[x]$, 15
  - has unique prime factorization, 17
- quadratic form, 59
  - composition, 66
  - discriminant, 59
  - equivalence, 59, 63
  - and quadratic integers, 61
  - reduced, 64
- quaternion, 139
- quotient, 2
  - of algebraic integers, 83
  - of modules, 173
  - of ring by ideal, 71, 88, 104
    - definition, 111

- $\mathbb{R}$, 70, 99
  - completeness of, 101
  - has no zero divisors, 82
  - is uncountable, 101, 121
  - as vector space over $\mathbb{Q}$, 128
- rank of free module, 178
  - analogous to dimension, 180
  - definition, 180
- rational
  - function, 184
  - number, 10
    - as equivalence class of fractions, 79
  - points
    - on circle, 34
    - on ellipse, 36
    - on hyperbola, 35
- RCA_0, 125
- reflexivity, 64, 79
- remainder, 2
- Riemann surface
  - branch point, 207
  - as covering, 207, 209
  - from a function field, 210
  - genus, 210
  - point of, 210
  - sheets, 207
- Riemann, Bernhard
  - and rational functions, 206
  - sphere, 208
- Riemann-Hurwitz formula, 210
- ring, xii, 1, 30
  - of algebraic functions, 188
  - of algebraic integers, 32, 93, 94, 103
  - axioms, 15, 79
  - finite, 21
  - homomorphism, 111
  - of integers of a field, 183
  - integral over another, 184
  - integral over subring, 185
  - Noetherian, 104, 113
    - definition, 114
    - equivalent properties, 114
  - nonzero, 114
  - polynomial, 15, 83
    - multivariable, 84
  - quotient by ideal, 71, 88, 104
    - definition, 111
  - $R[x]$, 17
  - with zero divisors, 83
  - $\mathbb{Z}[i]$, 40
- Rothe, Heinrich August, 169

- scalar, 127
- Schönemann, Theodor, 97
- Seki, Takakazu, 169
- Solovay, Robert, 123
- solution field, 87
- solvability, xii
  - of linear Diophantine equation, 7
- span, 90, 128
- Steinitz, Ernst, 130
- Stevin, Simon, 16
- straightedge and compass, 133
- submodule, 173
  - of free $\mathbb{Z}$-module, 181
- subspace
  - definition, 132
  - dimension, 132
  - of vector space, 126
- symmetry
  - of equivalence relation, 64, 79
  - of rectangle, 69

- Tartaglia. *See* Fontana, Niccolò, 26
- theorem
  - binomial, 28
  - Chinese remainder, 71
  - Dedekind product, 131
  - factor, 22
  - Fermat two square, 33, 49, 65

© in this web service Cambridge University Press & Assessment www.cambridge.org

CAMBRIDGE

Cambridge University Press & Assessment
978-1-316-51895-3 — Algebraic Number Theory for Beginners Algebraic Number Theory for Beginners
John Stillwell
Index
More Information

theorem (Cont.)
  Fermat's last, 33
  Fermat's little, 20, 29, 49
  fundamental
    of algebra, 86, 99, 125, 140
    of arithmetic, 1, 9
    of finite Abelian groups, 68
  Hilbert basis, 116
  intermediate value, 100
  Lagrange
    on polynomials, 22, 49
  primitive element, 139, 140
  Pythagorean, 44, 52
  well-ordering, 123
trace, xii, 149
  of algebraic number, 161
  in cyclotomic field, 164
  definition, 160
  is basis-independent, 136, 149, 161
  is coefficient of charpoly, 160
  relative, 161
  in terms of σ_i, 163
transitivity
  of equivalence relation, 64, 79
  of relation "integral over,", 186
transpose of matrix, 155, 165
transposition, 153

uncountability, 101, 121
  of $\mathbb{R}$, 121
unimodular map, 64
unique prime factorization, xii
  assumed by Euler, 31
  and class number, 65
  fails in $\mathbb{Z}[\sqrt{-5}]$, 61, 105
  holds in PIDs, 109
  of ideals, 104, 189, 199
  Kummer's replacement, 75
  may require ideals, 104
  in $\mathbb{N}$, 1, 9
  for polynomials, 84
  and principal ideals, 65
  in $\mathbb{Q}[x]$, 17
  of sum of squares, 46
  in $\mathbb{Z}$, 9
  in $\mathbb{Z}[i]$, 43, 44
  in $\mathbb{Z}[\sqrt{-2}]$, 45
  in $\mathbb{Z}[\sqrt{2}]$, 19
  in $\mathbb{Z}[\zeta]$, 53
unit, 15
  of $\mathbb{Z}[i]$, 44
  of $\mathbb{Z}[\sqrt{-2}]$, 51
  of $\mathbb{Z}[\sqrt{2}]$, 15

Vandermonde, Alexandre-Théophile, 166
  founded determinant theory, 169
vector, 127
vector space, 93, 126
  as Abelian group, 127
  axioms, 127, 146
  basis, 126
    and axiom of choice, 123, 128
  concept in Grassmann, 145
  definition, 127
  dimension, 126, 128
    is well-defined, 130
  finite-dimensional, 130
  homomorphism, 134
  isomorphism, 134
Viète, Francois, 27
  angle property, 56
Vitali, Giuseppe, 123

Weber, Heinrich Martin
  algebraic function theory, 188
Weil, André, 60, 75
well-ordering
  and axiom of choice, 120, 123
  definition, 120
  and induction, 24
  of $\mathbb{N}$, 2
  proved by Zermelo, 123
  theorem, 123
  and Zorn's lemma, 120
Wiles, Andrew, 36
WKL_0, 125

$\mathbb{Z}$, 5
  is principal ideal domain, 8, 10
  is ring, 15
$\mathbb{Z}[i]$, 40
$\mathbb{Z}_E$, 78, 95
  has integral basis, 176
  is Dedekind domain, 197
  is free $\mathbb{Z}$-module, 186
  is Noetherian, 182
  prime ideal factorization, 104
  prime ideals, 186, 196
Zermelo, Ernst, 123
zero divisor, 17, 21, 80, 82
$\mathbb{Z}_n$, 73
Zorn, Max, 115

© in this web service Cambridge University Press & Assessment www.cambridge.org

CAMBRIDGE

Cambridge University Press & Assessment
978-1-316-51895-3 — Algebraic Number Theory for Beginners Algebraic Number Theory for Beginners
John Stillwell
Index
More Information

Zorn’s lemma, 115
  and axiom of choice, 123
  and Hamel basis, 129
  and maximal ideals, 116
  and well-ordering, 120
  statement, 116
$\mathbb{Z}[\sqrt{-2}]$, 45
$\mathbb{Z}[\sqrt{-5}]$, 61
  division property fails, 63
  gcd in, 105, 107
  ideal in, 106
  is Noetherian, 118
  maximal ideals, 113
  nonprincipal ideal, 108, 204
  nonunique prime factorization, 61, 105
  prime ideal, 192
  principal ideals, 174
  quotients of, 113

© in this web service Cambridge University Press & Assessment www.cambridge.org