CAMBRIDGE

Cambridge University Press
978-0-521-29861-2 - An Introduction to Abstract Algebra, Volume 1 - Second Edition
F. M. Hall
Index
More information

INDEX

Abelian groups, 203–4
Absorption laws, for union and intersection of sets, 34
abstract groups, 207
addition,
  of complex numbers, 80
  of integers, 55
  laws, 171–3
  of natural numbers, 52
  of polynomials, 107
  of rational numbers, 74
  of residues, 90
  of vectors in two dimensions, 131
  of vectors, geometrically, 133
addition tables for finite arithmetics, 94
algebra
  Boolean, 42
  derivation of word, 7
  of sets, 24–50
  of statements, 41–4
algebraic numbers, definition, 79
algebraic structures, 188–9
  types of, 189–90
algorithm, *see* Euclid's algorithm and division algorithm
alternating group, 239
  of degree 4, 240
  of degree 5, 244
'and', in algebra of statements, 42
anti-symmetric law, for inclusion of sets, 34
Argand diagram
  definition, 79
  use in geometry, 142, 145
associates, for polynomials
  definition, 110
  form equivalence classes, 110
Associative laws
  of addition, 171, 172
  of multiplication, 177, 178
  extension to more than 3 elements of group, 201
  for groups, 200
  for rational numbers (addition), 74
  for rational numbers (multiplication), 75
  for union and intersection of sets, 34
  for vectors, geometrically, 134
axes, change of, 154
axioms, *see* postulates

binomial theorem, 69
Boole, *The Laws of Thought*, 8, 42
Boolean algebra, 42
  definition, 44

Cancellation laws
  of addition, 175
  for groups, 202
  for integers, 58
  of multiplication, 183
  for natural numbers, 52
  for polynomials, 107
  for polynomials (restrictions on coefficients), 121
  for residues (not always true), 92
  for sets, 39
Cantor, 52
cardinal numbers, 163
Carroll, Lewis, *Symbolic Logic*, 45, 48
Cartesian geometry
  change of axes, 154
  use of vectors, 136–40
Cayley's theorem, 273–5
centre
  of a group, 262
  is a subgroup, 263
centroids, definition, 137
circle, transformation group of, 228
coefficients of a polynomial, 108–9, 121–3
  definition, 105
Commutative laws
  of addition, 171
  for groups, 203
  of multiplication, 177
  for rational numbers (addition), 74
  for rational numbers (multiplication), 75
  not true for multiplication of quaternions, 82
  for union and intersection of sets, 34
  for vectors, geometrically, 134
complement, of set
  in algebra of statements, 43
  definition and notation, 14
  laws, 37
  relative complement, 40
  representation in Venn diagram, 28
complex, in a group, 271
complex numbers, 79–81
  definition by pairs of real numbers, 80

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-29861-2 - An Introduction to Abstract Algebra, Volume 1 - Second Edition
F. M. Hall
Index
More information

complex numbers (*cont*).
as example of vector multiplication, 142
as a group, 218
isomorphic to vectors, 164
of unit modulus, 221
composite integers, 61
congruences, 86–8
congruence equations, 96–8
consistency theorem, for sets, 40
continuum, definition, 78
co-prime integers, 63
correspondence, 1-1, 160–3
definition, 161
cosets, 276–9
definition of left and right, 277
countable set, *see* denumerable set
counter-example, definition, 6
cross-ratio, 149
the group of, 244
cycles, 257
cyclic groups, 221–5
infinite, 219, 222
of orders 4, 6, 8, 281–3
of prime order, 280
subgroups of, 280–1
transformation groups of one-sided polygons, 227

decimal, repeating decimal as fraction, 83, 85
degree of a polynomial, 105
De Morgan laws, 37
denumerable set
definition, 76
definition in terms of 1-1 correspondence, 163
set of rationals denumerable, 76
set of reals not denumerable, 79
Desargues' theorem, 150
difference of sets
definition, 14
laws, 40
digital root, 101
dihedral groups, 226–30
definition, 229
of order 4, 229
of order 6, 230, 245, 282
of order 8, 283
direct product, 248–50
of subgroups, group as, 266
Distributive laws, 178–81
connecting sum and product, 187
generalised, for sets, 38
for rational numbers, 75
for union and intersection of sets, 34
divisibility
for integers, 61–2
for polynomials, 109
tests, 99–101
division
algebraic definition, 181–4
of integers, 58
of natural numbers, 53
of polynomials, 107, 124
of rational numbers, 75
of residues, 92–4
division algorithm
extension of, 127
for integers, 63
for polynomials, 113
divisor, for integers, 61
dodecahedral (icosahedral) group, 244
duality, for union and intersection of sets, 35

elements of sets, 10
empty set (or null set)
in algebra of statements, 43
definition and notation, 13
laws, 37
uniqueness, 38
equality
general definition, 4
of sets, 12
equivalence classes theorem, 18
equivalence relations, 17–20
and associated polynomials, 110
congruence, 88
definition, 18
in definition of cosets, 277
in definition of integers, 55
in definition of rational numbers, 73
and mappings, 158
Euclidean algorithm
for integers, 64
for polynomials, 114
Euclidean geometry, *see* Cartesian geometry
Euler's extension of Fermat's theorem, 98
proof by Lagrange's theorem, 287
even permutations, 235

factor
for integers, 61
for polynomials, 109
finding polynomial factors, 120

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-29861-2 - An Introduction to Abstract Algebra, Volume 1 - Second Edition
F. M. Hall
Index
More information

factor theorem
  proof, 116
  alternative proofs, 123, 127
Fermat's theorem, 98
  proof by Lagrange's theorem, 287
Fermat's theorem on binary powers, 6
field
  definition, 113
  of scalars, 131
  as a set with the four rules, 170
  as type of algebraic structure, 189
finite arithmetics, 94–6, 93
finite groups, 202
fractions, *see* rational numbers
Frege, 52
Frobenius notation, 270–3
functions, 151–2
  inverse functions, 160
fundamental laws of algebra, brief statement, 33
fundamental theorem of algebra, 7, 80
fundamental theorem of arithmetic, 66

Gauss's theorem, 117–21
Gaussian integers
  definition, 81
  form a group, 219
'Gegenbeispiel', *see* counter-example
generators
  of cyclic groups, 221
  of a group, 250–1
Goldbach's conjecture, 6
greatest common divisor, *see* highest common factor
group
  abstract, 207
  abstract definition, 200–1
  alternating, 239, 240, 244
  as type of algebraic structure, 189
  of cross-ratios, 244
  dodecahedral (icosahedral), 243
  infinite cyclic, 219
  isomorphic, 205
  octahedral (hexahedral), 242
  of a polynomial, 247
  of prime order, 280
  symmetric, 232
  tetrahedral, 240
  Vierergruppe, 207
  see also the paragraphs of ch. 12 for various types of groups

highest common factor
  for integers, 62–5
  for more than two integers, 65
  for polynomials, 112–15
  restrictions on coefficients, 121
homography, 162
homomorphisms, 158

Idempotent laws, for union and intersection of sets, 34
if and only if, 5
image, element in a mapping, 156
image space
  of a function, 152
  of a mapping, 156
implication, 4
inclusion,
  laws, 34
  for sets, 12
  for statements, 42
index of a subgroup, 279
index laws
  for groups, 210
  for natural numbers, 53
induction, 59–61
infinite groups, 202
injection, as a mapping, 159
inner product, 143
integers
  definition from natural numbers, 53–9
  as a group, 218
integral domain, 58
  polynomials as, 108
intersection of sets
  definition and notation, 13
  laws, 34
  representation in Venn diagram, 28
  in algebra of statements, 42
into
  type of mapping, 156
  distinction between into and onto, 160
inverse
  in groups, 200
  existence, 181
  of a product for groups, 208
  right and left inverses, 193
  uniqueness, 182, 201
inverse functions and mappings, 160
inversion, 152
involution, type of mapping, 166
irrational numbers, 77–9
  Dedekind's definition, 78
  proof that $\sqrt{2}$ is irrational, 77
irreducibility of polynomials, 109–12
  definition, 111
  see also 115, 117–21

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-29861-2 - An Introduction to Abstract Algebra, Volume 1 - Second Edition
F. M. Hall
Index
More information

isomorphism, 163–5
  isomorphic groups, 205

Lagrange's theorem, 279–80
Latin squares, 213–14
laws of algebra, *see* fundamental laws of algebra
Laws of Thought, *The*, 8, 42
left coset, 277
left inverse, 193
left unity, 193
Leibniz's theorem, 69
logic
  algebra of statements, 41–4
  logical ideas used in mathematics, 3–6
lowest common multiple
  for integers, 67
  for polynomials, 116

mappings
  definition, 156
  inverse, 160
membership of sets, 12
modulus
  for congruences, 87
  of a vector, 130
multiples
  for integers, 61
  multiples of *r* form a group, 219
multiplication
  of complex numbers, 80
  integers, 58
  laws, 176–8
  of natural numbers, 52
  of polynomials, 107
  of rational numbers, 75
  of residues, 91
  of vectors, 141–4
  of a vector by a scalar, 132
  of a vector by a scalar, geometrically, 134
  see also product
multiplication tables
  for finite arithmetics, 94
  for groups, 204–8

natural numbers, 51–3
  definition, 51
necessary condition, 5
negative
  existence, 174
  of integers, 57
  of polynomials, 107
  uniqueness, 174
neutral element
  of a group, 200
  of integers, 58
  uniqueness, 201
null set, *see* empty set

object, element in a mapping, 156
object space
  of a function, 152
  of a mapping, 156
octahedral (hexahedral) group, 242
odd permutations, 235–6
one to one, type of mapping, 160
only if, *see* if
onto, type of mapping, 160
or, in algebra of statements, 42
order
  of a group, 202–3
  of subgroup, as factor of order of group, 279
  groups of prime order, 280
order of element in a group, 211
  as factor of order of group, 279
ordered pair
  in definition of complex numbers, 80
  in definition of rational numbers, 73
  isomorphic to vectors, 164
  as vector, 131
ordering
  complete, 34
  of integers, 59
  of natural numbers, 52
  not applicable to polynomials, 108
  not applicable to residues, 91
  partial, 34, 49
  of rational numbers, 75
outer product, 144

parallel axis theorem, 150
partial ordering, *see* ordering
Peano, postulates for natural numbers, 52
perfect numbers, 104
permutations
  as groups, 230–9
  as mappings, 159
  even and odd, 235
  sign of, 236
  transpositions, 237
polynomial equation, degree *n*, 60
polynomials
  definition and algebra of, 105–8
  the group of a polynomial, 247
  groups of, 225–6
  mappings of, 158
  as vectors, 145

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-29861-2 - An Introduction to Abstract Algebra, Volume 1 - Second Edition
F. M. Hall
Index
More information

Poretsky's law, 50
postulates, in modern mathematics, 3
powers of an element, 210–13
  subgroup of, 260–1
prime integers, 61
prime factorisation
  of integers, 65–7
  of polynomials, 115
  of polynomials, restrictions on coefficients, 122
prime order, groups of, 280
primitive polynomial, used in proof of Gauss's theorem, 118
primitive roots of unity, 104
Principia Mathematica, 52
product
  inverse of, for groups, 208
  of mappings, 165
  of permutations, 231
  see also multiplication
projection in geometry, 154
  orthogonal, as mapping, 159
projective geometry, 140–1
  1-1 correspondence in, 162
projectivity, 162
proper subgroups, 260
pyramids, transformation groups of, 244

quadrilateral, properties by centroids, 140
quaternions, 81–2
  as a group, 218
  as vectors, 142
quaternion group, 283

rational functions, 123–4
  as a group, 225
rational numbers
  abstract definition, 72–7
  forming a denumerable set, 76
  as a group, 218
real numbers, 77–9
  as a group, 218
  see also irrational number
reciprocation, 153
reductio ad absurdum, used with induction, 61
reflexive law
  for inclusion of sets, 34
  for relations, 17
relations
  equivalence, 17
  for a group, 250–1
relative complement for sets, 40
remainder theorem
  alternative proof, 127
  proof, 116
residues
  definition and algebra, 89–92
  as groups, 196, 197, 221–4
  mappings involving residues, 158
  modulo p as a field, 170
right cosets, 277
right inverse, 193
right unity, 193
ring, as type of algebraic structure, 189
roots, of congruence equation, 97
rules, the four, 169–71
Russell and Whitehead, *Principia Mathematica*, 52

scalar, 130
  multiplication by a vector, 132
  product, 143
sequence as a mapping, 158
sets, 9–50
  elements, 10
  isomorphic, 164
  notation, 11–16
  subsets, 16–17
sign of a permutation, 236
statements, algebra of, 41–4
structures, algebraic, 188–9
  types of, 189–90
subgroups
  definition, 259–60
  generated by a subset, 263
  proper, 260
  trivial, 260
  of vectors, 261
subsets, 16
  definition, 17
  proper, 17
  trivial or improper, 17
subtraction
  algebraic definition, 173–6
  of integers, 58
  of natural numbers, 53
  of polynomials, 107
  of rational numbers, 74
  of residues, 91
  of vectors, 131
  of vectors, geometrically, 134
sufficient condition, 5
syllogisms, 44–6
symbolic logic, 42
  examples from Lewis Carroll, *Symbolic Logic*, 45, 48

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-29861-2 - An Introduction to Abstract Algebra, Volume 1 - Second Edition
F. M. Hall
Index
More information

symmetric groups
definition, 232
of degree 1, 2, 3, 234
of degree 3 ≅ group of cross-ratios, 245
of degree 4, 242
all finite groups ≅ subgroup of, 274
symmetric law for relations, 18

tetrahedral group, 240
tetrahedron, properties by centroids, 140
theory of numbers, some results in, 98–9
transcendental numbers, 79
transformation groups
of equilateral triangle, 197, 230
of polygons, 226–30
of solid figures, 239–44
of triangle ≅ symmetric group of degree 3, 234
transformations in geometry, as functions, 152–5
transitive law
for inclusion of sets, 34
for relations, 18
transpositions, 237
triangle, properties by centroids, 138
trivial subgroups, 260
truth table method, in set theory, 26

union of sets
in algebra of statements, 42
definition and notation, 13
laws, 34
representation in Venn diagrams, 28
unit
for integers, 61
for polynomials, 109
unity
existence, 181
for integers, 58, 61
left and right unities, 193
for polynomials, 107
uniqueness, 181
universal set
in algebra of statements, 43
definition and notation, 14
laws, 37
uniqueness, 38

vectors
as a group, 196, 226
as illustration of direct sums, 248, 266
subgroups of vectors, 261
various isomorphic definitions, 164
vector product, 144
not commutative or associative, 186
Venn diagrams, 28–32
definition, 28
Vierergruppe (four-group), 207, 281
as the dihedral group of order 4, 230
as a direct sum, 249

Whitehead, *see* Russell
Wilson's theorem, 98

zero
cannot divide by zero, 183
existence, 173
in polynomials, 107
uniqueness, 173
in vectors, 131
zero divisors
none for integers, 58
none for polynomials, 107
zeros of a polynomial, 116–17

© Cambridge University Press www.cambridge.org