CAMBRIDGE

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Index
More Information

Index of Definitions

$\mathbb{F}_p$, 298
$\mathbb{F}_q$, 335
Hom, 205
$\mathbb{Z}/n\mathbb{Z}$, 25
b divides *a*, 110

abelian group, 157
action of a group on a set, 237
algebraic
  closure of a field, 320
  element of an extension, 302
  extension, 307
alternating group, 249

basis of a free module, 175

Cartesian product
  of groups, 233
  of rings, 59
center of a group, 272
centralizer, 272
characteristic of a field, 297
cokernel, 183
commutative ring, 52
composite, 13
congruence
  modulo *n*, 23
  modulo an ideal, 83
conjugacy class, 241
constant term of a polynomial, 131
constructible number, 311
content of a polynomial, 141
coset, 84, 166
cycle, 249

degree
  of a polynomial, 131
  of an extension, 299
dihedral group, 242
direct sum of modules, 163
b divides *a*, 4

equivalent matrices, 181
Euclidean domain, 112
exact sequence of modules, 182
extension
  algebraic, 307
  finite, 299
  Galois, 341
  normal, 326
  radical, 362
  simple, 301

faithful action, 239
field, 55
  extension, 295
  fixed, 346
  intermediate, 300
  of fractions, 122
  splitting, 320
finite extension, 299
fixed field, 346
free action, 239
free module, 174
Frobenius homomorphism, 334

Galois
  conjugate, 348
  correspondence, 350
  extension, 341
  group, 340
greatest common divisor
  in $\mathbb{Z}$, 7
  in an integral domain, 110
group, 229
  abelian, 157
  alternating, 249
  dihedral, 242
  Galois, 340
  of permutations, 235
  simple, 275
  symmetric, 235

homomorphism
  of groups, 230
  of modules, 158
  of rings, 64

ideal, 80
  maximal, 106
  prime, 106
  principal, 82
index of a subgroup, 267
integral domain, 53

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

invertible element of a ring, 54
irreducible
  element of an integral domain, 111
  integer, 13
isomorphic, 71, 160, 231
isomorphism, 70, 160, 231

kernel, 79, 165, 254

leading coefficient, 131
linearly independent elements of a module, 175

maximal ideal, 106
minimal polynomial, 303
module, 154
  cyclic, 162
  finitely generated, 162, 183
  finitely presented, 183
  free, 174

normal
  extension, 326
  subgroup, 255
normalizer, 274

operations in $\mathbb{Z}/n\mathbb{Z}$, 27
operations in R/I, 84
orbit, 238
order
  of a group, 202
  of an element of a group, 210

p-group, 271
PID (principal ideal domain), 113
polynomial, solvable by radical, 362
prime
  element of an integral domain, 111
  ideal, 106
  integer, 14
primitive
  polynomial, 141
  root of 1, 362
principal
  ideal, 82
    domain (PID), 113
product of two ideals, 95

quotient
  of a group by a normal subgroup, 259
  of a module by a submodule, 166
  of a ring by an ideal, 84

radical extension, 362
rank, 174
relatively prime, 10
ring, 41
  commutative, 52
  Noetherian, 187

separability degree, 332
separable
  extension, 328
  polynomial, 328
sign of a permutation, 248
simple
  extension, 301
  group, 275
solvable group, 287
splitting field, 320
stabilizer, 270
subgroup, 232
  generated by a subset, 232
  normal, 255
  Sylow, 277
submodule, 161
subring, 61
sum of two ideals, 94
Sylow subgroup, 277
symmetric group, 235

transcendental element of an extension, 302
transitive action, 239
transposition, 249
type of a permutation, 283

unique factorization domain (UFD), 119
unit, 54

zero-divisor, 53

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

CAMBRIDGE
Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Index
More Information

Index of Theorems

$\mathbb{Z}/n\mathbb{Z}$ satisfies the ring axioms, 30
$\mathcal{A}_n$ is simple for $n \geq 5$, 286
$\mathcal{S}_n$ is not solvable for $n \geq 5$, 289
gcd(a, b) is a linear combination of a and b, 8
$|\mathbb{Z}/n\mathbb{Z}| = n$, 26

Abel–Ruffini, 364

binomial, 147

canonical decomposition, 90, 167, 260
Cauchy
  for abelian groups, 215
  general case, 277
Cayley, 240
  –Hamilton, 199
characterization
  of Galois extensions, 348
  of maximal ideals, 108
  of prime ideals, 107
  of splitting fields as finite normal extensions, 326
Chinese Remainder, 97, 197
class equation, 272
classification
  of finite abelian groups, 212
  of finite fields, 334
  of finitely generated modules over Euclidean domains, 195
constructibility
  of a number, 312
  of regular polygons, 373

description of $k[x]/(f(x))$, 135
Dirichlet, on arithmetic progressions, 225
division with remainder, 6

Eisenstein's criterion, 145
Euclidean
  algorithm, 11
  domains are PIDs, 113
Euler–Fermat, 290
existence of
  algebraic closures, 320
  splitting fields, 321

Feit–Thompson, 287
Fermat
  Euler–, 290
  Last Theorem, 129
    for polynomials, 129
  little, 35, 268
  on sums of squares, 217
finitely generated $\Longrightarrow$ finitely presented, over a Noetherian ring, 187
First Isomorphism Theorem
  for groups, 260
  for modules, 168
  for rings, 91
Fundamental
  of Algebra, 137, 370
  of Arithmetic, 15
  of Galois Theory, 351, 355
  on symmetric functions, 358

Galois criterion, 363
Gauss's lemma, 140

Hamilton
  Cayley–, 199
Hilbert's basis, 132, 189

intermediate value, 138

Kronecker–Weber, 375

Lagrange, 267

nonzero prime
  $\Longrightarrow$ irreducible, 112
  if and only if irreducible, in $\mathbb{Z}$, 14

prime number, 19, 36
primitive element, 330

quotients
  of groups by normal subgroups are groups, 258
  of modules by submodules are modules, 167
  of rings by ideals are rings, 85

RSA algorithm, 38

Second Isomorphism Theorem
  for groups, 262
  for modules, 170
simple $\Longleftrightarrow$ finitely many intermediate fields, 306
solvability and radical extensions, 363
structure of $\mathbb{Z}/p\mathbb{Z}$ for p prime, 32
Sylow
  for abelian groups, 224

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

I, 277
II, 277
III, 277
the multiplicative group of a finite field is cyclic, 216
the size of an orbit equals the index of the stabilizer, 270
Third Isomorphism Theorem
for groups, 263
for modules, 169
for rings, 100
unique factorization holds in PIDs, 117
universal property of the field of fractions, 124
vector spaces are free, 190
Weber
Kronecker–, 375

© in this web service Cambridge University Press

Subject Index

(a), 82
(a, b), 7
$(a_1 \dots a_r)$, 249
$(a_1, \dots, a_n)$, 82
$-a$, 49
0_R, 41
1_R, 42
2^A, 392
$A \cap B$, 390
$A \cup B$, 390
$A \smallsetminus B$, 390
A/I, 100
$A/{\sim}$, 22
$A \times B$, 391
C_n, 207
G/K, 254
HK, 262
$I + J$, 94
IJ, 95
$M \oplus N$, 163
R/I, 84, 85
$R[x, y]$, 46
$R[x]$, 46
$R[x_1, \dots, x_n]$, 46
$R \cong S$, 71
$R \times S$, 59
R^*, 54
$R^{\oplus n}$, 163
$S^{-1}R$, 126
$[F : k]$, 299
$[F : k]_s$, 332
$[G : H]$, 267
$\mathbb{C}$, 31, 42, 55, 74, 378
$\mathrm{End}(A)$, 205
$\mathbb{F}_1$, 134
$\mathbb{F}_p$, 298
$\mathbb{F}_q$, 335
$\mathrm{GL}_n(\mathbb{R})$, 234
$\mathrm{Hom}(A, B)$, 205, 231
$\mathbb{N}$, 5, 43, 378
$\mathbb{Q}$, 31, 42, 55, 378
$\mathbb{R}$, 31, 42, 55, 87, 378
$\mathrm{SL}_2(\mathbb{Z})$, 234
$\mathrm{SL}_n(\mathbb{R})$, 266
$\mathrm{Spec}(R)$, 109
$\mathbb{Z}$, 378
$\mathbb{Z}/n\mathbb{Z}$, 25
$\mathbb{Z}[\zeta]$, 131
$\mathbb{Z}[i]$, 62
$\mathbb{Z}^{\geq 0}$, 4
$\mathbb{Z}_n$, 25
$\mathcal{P}(A)$, 392
$\mathcal{S}_A$, 235
$\cap_\alpha$, 390
$\mathrm{coker}\, f$, 183
$\cup_\alpha$, 390
$\deg f$, 131
$\exists$, 383
$\exists!$, 383
$\forall$, 383
$\gcd(a, b)$, 7
$\iff$, 381
$\mathrm{im}\, f$, 78
$\implies$, 381
$\in$, 377
$\ker f$, 79, 165
$\mathrm{lcm}(a, b)$, 95
$|\, G\, |$, 202, 229
$|\, g\, |$, 210
$\notin$, 377
$\overline{\mathbb{Q}}$, 303
$\overline{z}$, 66
$\sim_I$, 83
$\subseteq$, 389
$\wedge$, 379
$a \equiv b \bmod I$, 83
$b - a$, 49
$b \mid a$, 4, 110
$g \circ f$, 393
$n\mathbb{Z}$, 23

Abel, Niels Henrik (1802–1829), 157
  –Ruffini theorem, 364
abelian
  category, 164
  group, 80, 157
absorption property, 80
action, 154, 206, 236

faithful, 239
free, 239
of a group on a set, 237
transitive, 239
additive
cancellation, 50
identity, 30
inverse, 31
notation, 203
algebraic
closure, 320
element of an extension, 302
extension, 307
geometry, 52, 106, 115, 126, 132, 143, 187
numbers, 296, 303
algebraic geometry, 137
algebraically closed field, 137
alternating group, 249
annihilator, 196, 201
ascending chain condition, 116
associative property, 30
Atiyah, Michael (1929–2019), x
automorphism, 73, 235
inner, 265
axioms
abelian group, 80, 157
group, 229
module, 154
ring, 42

basis
of a free module, 175
of a vector space, 190
bijective function, 394
binomial theorem, 147
Boole, George (1815–1864), 57, 382
Boolean
algebra, 382
ring, 57

cancellation, 34, 50, 54, 229
canonical decomposition
for abelian groups, 202
for groups, 253
for modules, 164
for rings, 77
cardinality of a set, 391, 395
Carmichael, Robert Daniel (1879–1967)
number, 40
Cartesian product
of groups, 233
of modules, 163
of rings, 59
of sets, 391
category, xv, 205, 394
abelian, 164
of abelian groups, 202
of field extensions, 298
of groups, 230
of modules, 158
of rings, 68
of sets, 59
Cauchy, Augustin-Louis, (1789–1857)
theorem
for abelian groups, 215
general case, 277
Cayley, Arthur (1821–1895), 240
–Hamilton theorem, 199
theorem, 240
center
of a group, 272
of a ring, 159
centralizer, 272
character of a group, 367
characteristic
of a field, 297
of a ring, 57, 127, 297, 417
polynomial, of a linear transformation, 198
Chinese Remainder Theorem, 97, 197
class equation, 272
closed, with respect to an operation, 30, 41
codomain of a function, 392
cokernel, 183
universal property of, 183
commutative
addition in a ring is, 52
algebra, 52
diagram, 77, 393
group, 230
ring, 30, 31, 52
commutator, 266
subgroup, 266, 292
complement of a set, 390
complex
conjugation, 66, 218
number, 31
composite, 13
composition series, 287
congruence class, 24
congruent
modulo an ideal, 83
modulo an integer, 23
conjugacy class, 241
conjugate, 241
Galois, 348
conjugation, 66, 218
constant
polynomial, 62, 131
term, 131
constructible
complex number, 316, 372
polygon, 373
real number, 311
content of a polynomial, 141

CAMBRIDGE

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Index
More Information

contradiction, 382
contrapositive, 388
coproduct, 164, 233
  universal property of, 163, 172
corollary, 386
correspondence
  Galois, 350
  one-to-one, 69
coset, 84, 166
  left, 254
  right, 255
cycle, 249
  notation, for a permutation, 250
cyclic
  group, 13, 207, 241
  module, 155, 162, 195
cyclotomic
  extension, 357, 374
  polynomial, 147, 374

De Morgan, Augustus (1806–1871)
  laws, 382
Dedekind, Julius Wilhelm Richard (1831–1916)
  lemma, 367
degree
  of a field extension, 299
  of a polynomial, 131
  of an algebraic element, 302
  of separability, 332
derivative of a polynomial, 328
derived series, 292
determinant, 67, 234
diagonal, 62, 74
diagram, commutative, 77
difference set, 390
dihedral group, 242
dimension
  Krull, of a ring, 115
  of a vector space, 163, 174, 190
direct sum
  of abelian groups, 202
  of modules, 163
Dirichlet, Peter Gustav Lejeune (1805–1859)
  theorem, on arithmetic progressions, 225, 357
discriminant of a cubic polynomial, 360
distributive property, 30
division with remainder, 6, 113, 132
divisor, 4
  elementary, 197
  greatest common, 7, 18, 110
  non-zero-, 53
  zero-, 53
domain
  Euclidean, 112
  integral, 53
  of a function, 392
  principal ideal (PID), 113
  unique factorization (UFD), 119

Eisenstein, Ferdinand Gotthold Max (1823–1852)
  criterion, 145, 319
element of a set, 377
elementary
  divisors, 197
  symmetric functions, 358
endomorphism, 205
equivalence
  class, 22, 396
  relation, 22, 396
equivalent matrices, 181
Eratosthenes of Cyrene (276 BC–194 BC)
  sieve, 13
Euclid of Alexandria (~ 300 BC), 11, 19, 389
Euclidean
  algorithm, 11, 114
  domain, 112, 193
  valuation, 113, 219
Euler, Leonhard (1707–1783), 99, 217
  –Fermat theorem, 290
  criterion, 226
  totient function, 99, 207, 373, 374
even permutation, 248
exact sequence
  of groups, 275
  of modules, 182
extension
  cyclotomic, 357, 374
  finite, 299
  Galois, 320, 341
  normal, 326
  of a field, 295
  problem, for groups, 275
  radical, 362
  separable, 328
  simple, 301

factorization, 15
faithful action, 239
Feit, Walter (1930–2004)
  –Thompson theorem, 287, 292
Fermat, Pierre de (1607–1665)
  Euler– theorem, 290
  Last Theorem, 129
    for polynomials, 129
  little theorem, 34
  prime, 314, 376
  theorem on sums of squares, 217
field, 32, 55
  algebraically closed, 137
  extension, 149, 171, 295
    Galois, characterization, 348
  finite, 334
  fixed, 346
  Galois, 342
  intermediate, 300

CAMBRIDGE

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Index
More Information

number, 308
of fractions, 121
universal property of, 121
perfect, 338
splitting, 320
final object, in a category, 75, 171
finite extension, 299
finitely
generated, 169, 183
presented, 182, 183
First Isomorphism Theorem, 401
for groups, 260
for modules, 168
for rings, 91
fixed
field, 346
point of an action, 238
free
action, 239
group, 252
universal property of, 253
module, 163, 174
universal property of, 176
torsion-, 173
Frobenius, Ferdinand Georg (1849–1917)
homomorphism, 334, 345
full subcategory, 231
function, 46, 392
bijective, 394
codomain, 392
composition, 393
domain, 392
identity, 393
image, 392
injective, 394
surjective, 394
target, 392
Fundamental Theorem
of Arithmetic, 15
of Algebra, 137, 370
of Galois Theory, 351, 355
on symmetric functions, 358

Galois, Évariste (1811–1832), 364
congjugates, 348
correspondence, 350
extension, 320, 341
field, 342
Fundamental Theorem, 351, 355
group, 340
inverse problem, 357, 375
Gauss, Johann Carl Friedrich (1777–1855), 62, 310, 373
lemma, 140, 142
Gaussian
elimination, 191
integers, 62, 93, 217
general linear group, 234, 266
Girard, Albert (1595–1632), 217
golden ratio, 354
graph of a function, 392
greatest common divisor, 7, 18
in a commutative ring, 110
in a Euclidean domain, 114
in a PID, 114
group
abelian, 80, 157
alternating, 249
commutative, 230
cyclic, 207, 241
definition, 229
dihedral, 242
divisible, 430
free, 252
Galois, 340
general linear, 234, 266
homomorphism, 230
isomorphism, 231
modular, 234
of permutations, 235
simple, 275
solvable, 286, 363
symmetric, 235

Hamilton, William Rowan (1805–1865)
Cayley– theorem, 199
Hilbert, David (1862–1943)
basis theorem, 132, 189
homological algebra, 223
homomorphic image, 93, 168
of a cyclic group, 208
homomorphism
Frobenius, 334
induced, 90
of R-modules, 158
of abelian groups, 159, 204
of groups, 230
of rings, 64
trivial, 65, 159, 231

ideal, 80
$\Longleftrightarrow$ kernel, 89
generated by a subset of a ring, 82
left, 80, 161
maximal, 106
primary, 119
prime, 106
principal, 82
identity
additive, 30, 41
function, 393
is unique, 48
multiplicative, 42
image, 77
of a function, 392

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

CAMBRIDGE

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Index
More Information

of a homomorphism of groups, 232
of a homomorphism of modules, 163
of a homomorphism of rings, 78
index of a subgroup, 267
indexed set, 379
induced
function, 399
homomorphism, 90
induction, 5
initial object, in a category, 75, 171
injective function, 394
inseparable polynomial, 328
integer, 378
Gaussian, 62, 93, 217
irreducible, 13
prime, 14
integral domain, 29, 53
intermediate
field, 300
value theorem, 138
intersection of sets, 390
invariant factor, 197
inverse
additive, 31, 41, 155
function, 395
Galois problem, 357, 375
is unique, 48
multiplicative, 32, 54
invertible element, in a ring, 54
involution, 271
irreducible
element of an integral domain, 111
integer, 13
isomorphic, 60
fields, 318
groups, 231
modules, 160
rings, 71
sets, 395
isomorphism
of free modules, 179
of groups, 231
of modules, 160
of rings, 70
of sets, 395
theorems
for groups, 260
for modules, 168
for rings, 91, 100

kernel, 79, 165, 254
$\Longleftrightarrow$ ideal (for rings), 89
$\Longleftrightarrow$ normal subgroup (for groups), 259
$\Longleftrightarrow$ submodule (for modules), 167
universal property of, 172
Kronecker, Leopold (1823–1891)
–Weber theorem, 375
Krull, Wolfgang (1899–1971)
dimension, 115

Lagrange, Joseph-Louis (1736–1813)
theorem, 215, 267
leading coefficient, 131
least common multiple, 18, 21, 95
lemma, 386
Lenstra, Arjen Klaas, 39
Lindemann, Carl Louis Ferdinand von (1852–1939), 304
linear
combination, 8, 82
transformation, 47, 197
linearly independent, 175
localization, 126
universal property of, 128
logical connective, 380
long division, 132

Macdonald, Ian Grant, x
Mathematics Subject Classification (MSC), 52
matrices, 44, 177
maximal ideal, 106
Milne, James Stuart, 296
minimal polynomial, 303
of a linear transformation, 198
modular arithmetic, 22, 29
module, 154
cyclic, 162, 195
finitely generated, 162, 183
finitely presented, 183
free, 163
homomorphism, 158
isomorphism, 160
simple, 172
monic polynomial, 131
monomial, 146
morphism in a category, xv, 68, 158, 205
most interesting object in mathematics, 296
multiple, 4, 50
least common, 18, 95
multiplication by scalars, 153
multiplicative
cancellation, 34, 54
inverse, 32, 54
notation, 203
subset, 126

naive set theory, 377
natural number, 5, 43
nilpotent, 58
Noether, Amalie Emmy (1882–1935), 116
Noetherian ring, 116, 119, 128, 132, 187, 200
non-zero-divisor, 53
noncommutative geometry, 53
norm, 219
normal
extension, 326

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

  - series, 287
  - subgroup, 255
    - ⟺ kernel, 259
- normalizer, 274
- Novikov, Pyotr Sergeyevich (1901–1975), 261
- number
  - algebraic, 303
  - Carmichael, 40
  - complex, 31
  - constructible, 311
  - field, 308
  - natural, 5, 43
  - prime, 19
  - rational, 31, 32
  - real, 31
  - theory, 52, 143, 234, 308
- nzd, 53

- object
  - final, 75
  - initial, 75
  - of a category, xv, 68, 158
- odd permutation, 248
- orbit, 238
- order
  - of a group, 202, 229
  - of an element of a group, 210, 242
  - relation, 20
- order relation, 395

- *p*-group, 271
- partition, 22
  - of a number, 224, 437
  - of a set, 397
- perfect field, 338
- permutation
  - even, 248
  - matrix, 247
  - odd, 248
  - sign, 248
  - type, 265, 283
- PID, 113, 196
- polynomial, 45
  - characteristic, 198
  - constant, 62, 131
  - cyclotomic, 147, 374
  - inseparable, 328
  - minimal, 198
  - monic, 131
  - primitive, 141
  - separable, 328
  - solvable by radical, 362
- power set, 392
- presentation of a group, 261
- primary ideal, 119
- prime
  - element of an integral domain, 111
  - factorization, 15
  - Fermat, 314
  - generating large, 36
  - ideal, 106
  - integer, 14
  - numbers, facts about, 19
  - subfield, 298
- primitive
  - element theorem, 330
  - polynomial, 141
  - root of 1, 362
- principal ideal, 82
  - domain, 113, 196
- product
  - of groups, 233
  - of modules, 163
  - of rings, 59
  - of two ideals, 95
  - universal property of, 172
- projection, 60, 89
- proof, 386
  - by contradiction, 388
  - by contrapositive, 387
  - by induction, 5
  - direct, 387
- proposition, 386

- Qín Jiǔsháo (1202–1261), 94
- quadratic residue, 225
- quantifier
  - existential, 383
  - universal, 383
- quotient, 6, 22, 25
  - group, 259
  - module, 166
  - ring, 84
  - set, 396
  - universal property of, 91, 173, 266

- radical extension, 362
- rank, 163
  - of a matrix, 190
  - of a module, 196
- rational
  - number, 32
  - root test, 143
- rational number, 31
- real number, 31
- reducible, 13
- relation, 395
  - equivalence, 396
  - order, 395
- relatively prime, 10, 110, 114
- remainder, 6
- representation theory, 241
- representative, 24
- representative of an equivalence class, 396
- Riemann, Georg Friedrich Bernhard (1826–1866)
  - hypothesis, 19

CAMBRIDGE

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Index
More Information

ring, 30, 31, 41, 51
  axioms, 42
  Boolean, 57, 382
  commutative, 31, 52
  Euclidean domain, 112
  homomorphism, 64
  isomorphic, 71
  isomorphism, 70
  Noetherian, 116, 128, 132, 187, 200
  of functions, 46
  of matrices, 44, 52
  PID, 113
  polynomial, 45, 131
  trivial, 34, 44
  without identity, 42
rng, 42, 43, 80, 103
root of a polynomial, 134
RSA encryption system, 37, 38
Ruffini, Paolo (1765–1822)
  Abel– theorem, 364

Sūnzĭ Suànjīng, 94, 105
Schur, Issai (1875–1941)
  lemma, 172
Second Isomorphism Theorem
  for groups, 262
  for modules, 170
separable
  extension, 328
  polynomial, 328
series
  composition, 287
  normal, 287
set, 377
  cardinality of a, 391, 395
  Cartesian product, 391
  complement, 390
  difference, 390
  element of a, 377
  finite, 378
  indexed, 379
  intersection, 390
  isomorphic, 395
  naive theory of, 377
  partition, 397
  power, 392
  quotient, 396
  subset, 389
  union, 390
Shafarevic, Igor (1923–2017), 357
sign of a permutation, 248
simple
  extension, 301
  group, 275
  module, 172
singleton, 409
singular curve, 111
snake lemma, 185
solvable
  group, 286, 363
solvable polynomial
  by radicals, 361
spectrum of a ring, 109
splitting field, 320
stabilizer, 270
stabilizing chain of ideals, 116
statement, 380
subfield, 75
subgroup, 204, 232
  generated by a subset, 232
  normal, 255
    ⟺ kernel, 259
submodule, 161
  ⟺ kernel, 167
  generated by a subset, 162, 169
subring, 61
subset, 389
subtraction, 49
surjective function, 394
Sylow, Peter Ludwig Mejdell (1832–1918), 276
  subgroup, 277
  theorems, 224, 277
    proofs, 280
symmetric
  function, 358
  group, 235

target of a function, 392
tautology, 382
theorem, 386
Third Isomorphism Theorem
  for groups, 263
  for modules, 169
  for rings, 100
Thompson, John Griggs
  Feit– theorem, 287, 292
torsion, 172, 196
totient function, 99, 373, 374
transcendental, 302
transitive action, 239
transposition, 249
trivial
  R-module, 154
  group, 234
  homomorphism, 65, 159, 231
  orbit, 238
  ring, 34, 44
truth table, 380
type of a permutation, 265, 283

UFD (unique factorization domain), 119
  if R is a UFD, then $R[x]$ is a UFD, 142
union of sets, 390
unique factorization, 15, 117
unit, 54

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

CAMBRIDGE

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Index
More Information

universal property, 23, 317, 399
  of cokernels, 183
  of coproducts, 163, 172
  of free
    groups, 253
    modules, 176
  of kernels, 172
  of localizations, 128
  of products, 172
  of quotients, 91, 173, 266
  of the field of fractions, 121

vector space, 135, 153
Venn, John (1832–1923)
  diagram, 390
Vierergruppe, 258

Weber, Heinrich Martin (1842–1913)
  Kronecker– theorem, 375
well-defined, 28, 399
well-ordering, 5
  principle, 5, 9
witness, 36
word, 252
  problem, 261

Zagier, Don, 217
Zariski, Oscar (1899–1986)
  topology, 109
zero-divisor, 53

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