SECTION 39

1. $x^2 - 2x - 1$ **3.** $x^2 - 2x + 2$
5. $x^{12} + 3x^8 - 4x^6 + 3x^4 + 12x^2 + 5$
7. $\mathrm{Irr}(\alpha, \mathbb{Q}) = x^4 - \frac{2}{3}x^2 - \frac{62}{9}$; $\deg(\alpha, \mathbb{Q}) = 4$
9. Algebraic, $\deg(\alpha, F) = 2$
11. Transcendental
13. Algebraic, $\deg(\alpha, F) = 2$
15. Algebraic, $\deg(\alpha, F) = 1$
17. $x^2 + x + 1 = (x - \alpha)(x + 1 + \alpha)$
23. **a.** T **c.** T **e.** F **g.** F **i.** F
25. **b.** $x^3 + x^2 + 1 = (x - \alpha)(x - \alpha^2)[x - (1 + \alpha + \alpha^2)]$
27. The polynomial $\mathrm{irr}(\alpha, F)$ is a generator of the principal ideal of all polynomials in $F[x]$ that have α as a zero. Therefore, irr is the monic polynomial of **minimum degree** that has α as a zero. Also, $\mathrm{irr}(\alpha, F)$ is the only **irreducible** monic polynomial that has α as a zero.

SECTION 40

1. 2, $\{1, \sqrt{2}\}$ **3.** 4, $\{1, \sqrt{3}, \sqrt{2}, \sqrt{6}\}$
5. 6, $\{1, \sqrt{2}, \sqrt[3]{2}, \sqrt{2}(\sqrt[3]{2}), (\sqrt[3]{2})^2, \sqrt{2}(\sqrt[3]{2})^2\}$ **7.** 2, $\{1, \sqrt{6}\}$
9. 9, $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[3]{3}, \sqrt[3]{6}, \sqrt[3]{12}, \sqrt[3]{9}, \sqrt[3]{18}, \sqrt[3]{36}\}$
11. 2, $\{1, \sqrt{2}\}$ **13.** 2, $\{1, \sqrt{2}\}$
19. **a.** F **c.** F **e.** F **g.** F **i.** F
23. *Partial answer:* Extensions of degree 2^n for $n \in \mathbb{Z}^+$ are obtained.

SECTION 41

All odd-numbered answers require proofs and are not listed here.

SECTION 42

1. Yes **3.** Yes **5.** 6 **7.** 0

SECTION 43

1. $\sqrt{2}, -\sqrt{2}$ **3.** $3 + \sqrt{2}, 3 - \sqrt{2}$ **5.** $\sqrt{2} + i, \sqrt{2} - i, -\sqrt{2} + i, -\sqrt{2} - i$
7. $\sqrt{1 + \sqrt{2}}, -\sqrt{1 + \sqrt{2}}, \sqrt{1 - \sqrt{2}}, -\sqrt{1 - \sqrt{2}}$ **9.** $\sqrt{3}$
11. $-\sqrt{2} + 3\sqrt{5}$ **13.** $-\sqrt{2} + \sqrt{45}$
15. $\sqrt{3} + \sqrt{5}$
17. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ **19.** $\mathbb{Q}(\sqrt{3}, \sqrt{10})$ **21.** $\mathbb{Q}$
25. **a.** $3 - \sqrt{2}$ **b.** They are the same maps.
39. Yes

SECTION 44

1. 2 **3.** 4 **5.** 2 **7.** 1 **9.** 2
11. $\sqrt{2} \to \sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{5} \to \sqrt{5}$; and $\sqrt{2} \to \sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{5} \to -\sqrt{5}$
13. $\sqrt{2} \to \sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{5} \to -\sqrt{5}$; $\sqrt{2} \to \sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{5} \to \sqrt{5}$;
$\sqrt{2} \to -\sqrt{2}, \sqrt{3} \to \sqrt{3}, \sqrt{5} \to \sqrt{5}$; $\sqrt{2} \to -\sqrt{2}, \sqrt{3} \to -\sqrt{3}, \sqrt{5} \to -\sqrt{5}$
15. There are six extensions. One for each of the combinations where $\sqrt{3}i$ maps to $\pm\sqrt{3}i$ and $\sqrt[3]{2}$ maps to one of $\alpha_1, \alpha_2, \alpha_3$.

17. **a.** $\mathbb{Q}(\pi^2)$ **b.** $\sqrt{\pi}$ can map to either $\pm\sqrt{\pi}i$.

19. $1 \leq [E : F] \leq n!$

21. Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2})$. Then

$$f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$$

has a zero in E, but does not split in E.

SECTION 45

1. $\alpha = \sqrt[6]{2} = 2/(\sqrt[3]{2}\sqrt{2}).\sqrt{2} = (\sqrt[6]{2})^3$, $\sqrt[3]{2} = (\sqrt[6]{2})^2$. (Other answers are possible.)

3. $\alpha = \sqrt{2} + \sqrt{5}$. $\sqrt{2} = \dfrac{1}{6}\alpha^3 - \dfrac{11}{6}\alpha$, $\sqrt{5} = \dfrac{17}{6}\alpha - \dfrac{1}{6}\alpha^3$. (Other answers are possible.)

7. $f(x) = x^4 - 4x^2 + 4 = (x^2 - 2)^2$. Here $f(x)$ is not an irreducible polynomial. Every irreducible factor of $f(x)$ has zeros of multiplicity 1 only.

SECTION 46

1. 4 **3.** 8 **5.** 4 **7.** 2

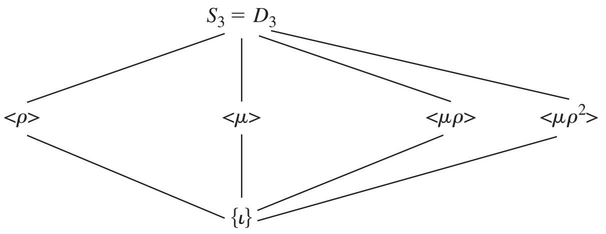
9. The group has two elements, the identity automorphism ι of $\mathbb{Q}(i)$ and σ such that $\sigma(i) = -i$.

11. **b.** Let $\alpha_1 = \sqrt[3]{5}$, $\alpha_2 = \sqrt[3]{5}\dfrac{-1 + i\sqrt{3}}{2}$, and $\alpha_3 = \sqrt[3]{5}\dfrac{-1 - i\sqrt{3}}{2}$.

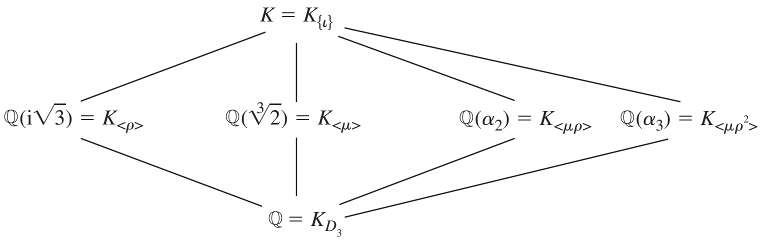
The maps are
ι, where ι is the identity map;
ρ, where $\rho(\alpha_1) = \alpha_2$ and $\rho(i\sqrt{3}) = i\sqrt{3}$;
ρ^2, where $\rho^2(\alpha_1) = \alpha_3$ and $\rho^2(i\sqrt{3}) = i\sqrt{3}$;
μ, where $\mu(\alpha_1) = \alpha_1$ and $\mu(i\sqrt{3}) = -i\sqrt{3}$;
$\mu\rho$, where $\mu\rho(\alpha_1) = \alpha_3$ and $\mu\rho(i\sqrt{3}) = -i\sqrt{3}$;
$\mu\rho^2$, where $\mu\rho^2(\alpha_1) = \alpha_2$ and $\mu\rho^2(i\sqrt{3}) = -i\sqrt{3}$.

c. S_3. The notation in (a) was chosen to coincide with the standard notation for $D_3 \simeq S_3$.

d.



Group diagram


$K = K_{\{\iota\}}$
$\mathbb{Q}(\mathrm{i}\sqrt{3}) = K_{<\rho>}$
$\mathbb{Q}(\sqrt[3]{2}) = K_{<\mu>}$
$\mathbb{Q}(\alpha_2) = K_{<\mu\rho>}$
$\mathbb{Q}(\alpha_3) = K_{<\mu\rho^2>}$
$\mathbb{Q} = K_{D_3}$

Field diagram

13. The splitting field of $(x^3 - 1) \in \mathbb{Q}[x]$ is $\mathbb{Q}(i\sqrt{3})$, and the group is cyclic of order 2 with elements: ι, where ι is the identity map of $\mathbb{Q}(i\sqrt{3})$, and σ, where $\sigma(i\sqrt{3}) = -i\sqrt{3}$.

15. **a.** *F* **c.** *T* **e.** *T* **g.** *F* **i.** *F*

25. *Partial answer:* $G(K/(E \vee L)) = G(K/E) \cap G(K/L)$

SECTION 47

3. $\mathbb{Q}(\sqrt[4]{2}, i)$: $\sqrt[4]{2} + i, x^8 + 4x^6 + 2x^4 + 28x^2 + 1$;
$\mathbb{Q}(\sqrt[4]{2})$: $\sqrt[4]{2}, x^4 - 2$;
$\mathbb{Q}(i\sqrt[4]{2}))$: $i(\sqrt[4]{2}), x^4 - 2$;
$\mathbb{Q}(\sqrt{2}, i)$: $\sqrt{2} + i, x^4 - 2x^2 + 9$;
$\mathbb{Q}(\sqrt[4]{2} + i(\sqrt[4]{2}))$: $\sqrt[4]{2} + i(\sqrt[4]{2}), x^4 + 8$;
$\mathbb{Q}(\sqrt[4]{2} - i(\sqrt[4]{2}))$: $\sqrt[4]{2} - i(\sqrt[4]{2}), x^4 + 8$;
$\mathbb{Q}(\sqrt{2})$: $\sqrt{2}, x^2 - 2$;
$\mathbb{Q}(i)$: $i, x^2 + 1$;
$\mathbb{Q}(i\sqrt{2})$: $i\sqrt{2}, x^2 + 2$;
$\mathbb{Q}$: $1, x - 1$

5. The group is cyclic of order 5, and its elements are

	ι	σ_1	σ_2	σ_3	σ_4
$\sqrt[5]{2} \rightarrow$	$\sqrt[5]{2}$	$\zeta(\sqrt[5]{2})$	$\zeta^2(\sqrt[5]{2})$	$\zeta^3(\sqrt[5]{2})$	$\zeta^4(\sqrt[5]{2})$

where $\sqrt[5]{2}$ is the real 5th root of 2.

7. The splitting field of $x^8 - 1$ over $\mathbb{Q}$ is the same as the splitting field of $x^4 + 1$ over $\mathbb{Q}$, so a complete description is contained in Example 47.7. (This is the easiest way to answer the problem.)

9. **a.** ${s_1}^2 - 2s_2$ **b.** $\dfrac{s_1 s_2 - 3s_3}{s_3}$

SECTION 48

3. **a.** 16 **b.** 400 **c.** 2160

5. 3^0

7. **a.** *T* **c.** *F* **e.** *T* **g.** *T* **i.** *F*

9. $\Phi_1(x) = x - 1$
$\Phi_2(x) = x + 1$
$\Phi_3(x) = x^2 + x + 1$
$\Phi_4(x) = x^2 + 1$
$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
$\Phi_6(x) = x^2 - x + 1$

SECTION 49

1. No. Yes, *K* is an extension of $\mathbb{Z}_2$ by radicals.

3. **a.** *T* **c.** *T* **e.** *T* **g.** *T* **i.** *F* ($x^3 - 2x$ over $\mathbb{Q}$ gives a counterexample.)

APPENDIX

1. $\begin{bmatrix} 2 & 1 \\ 2 & 7 \end{bmatrix}$ **3.** $\begin{bmatrix} -3 + 2i & -1 - 4i \\ 2 & -i \\ 0 & -i \end{bmatrix}$

5. $\begin{bmatrix} 5 & 16 & -3 \\ 0 & -18 & 24 \end{bmatrix}$ **7.** $\begin{bmatrix} 1 & -i \\ 4 - 6i & -2 - 2i \end{bmatrix}$

9. $\begin{bmatrix} 8 & -8i \\ 8i & 8 \end{bmatrix}$ **11.** $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ **13.** -48

This page is intentionally left blank

Index

Abel, Niels Henrik, 21, 150, 191, 385
Abelian extension, 370
Abelian group(s), 20
  finitely-generated, fundamental theorems of, 92, 93
  free, 167
  torsion free, 96, 119
Absolute value, 34
Action
  faithful, 133
  on a group, 132
  transitive, 133
Addition
  modulo 2π, 37
  modulo c, 33
  modulo n, 32, 65
Additive identity, 14
Adjoining elements to field, 321
Al-Tusi Sharaf al-Din, 224
Algebra
  fundamental theorem of, 257, 324
  group, 261
Algebraic closure, 324
Algebraic closure of F in E, 323
Algebraic element over F, 313
Algebraic extension, 319
Algebraic integer, 378
Algebraic number, 314
Algebraic number theory, 294
Algebraic variety, 298
Algebraically closed field, 323, 327
Alphabet, 172
Alternating group on n letters, 84
Antisymmetric law, 324
Arc
  of a diagraph, 72
  of a graph, 308
Arithmetic, fundamental theorem of, 280
Artin, Emil, 225
Ascending central series, 163
Ascending chain condition, 278, 286

Aschbacher, Michael, 127
Associates, 276
Associative operation, 13, 20
Automorphism, 341
  of a field, 345
  Frobenius, 349
  of a group, 68, 118
  group of, 345
  inner, 118
Axiom of choice, 324, 325
Axis of reflection, 105

Banach, Stefan, 268
Basis
  for a finitely-generated abelian group, 176
  for a free abelian group, 167
  Gröbner, 305
  for an ideal, 298
  for a vector space, 270
Bessy, Bernard Frenicle de, 201
Betti number, 92
Bijection, 4
Binary operation, 11
Bit, 237
Bit errors, 239
Blip group, 177
Bloom, David M., 82
Blop group, 177
Boolean ring, 194
Bourbaki, Nicholas, 4, 177, 326
Brahmagupta, 288
Burnside, William, 127, 152
Burnside's formula, 141

Cancellation laws, 23, 196
Cardano, Girolamo, 224, 385
Cardinality, 3, 4
Cartesian product, 2, 88
Cauchy Augustin-Louis, 42
Cauchy's theorem, 136
Cayley, Arthur, 72, 81, 178

Cayley digraph, 72
Cayley's theorem, 79
Cell, 5
Center of a group, 60, 128, 163
Chain(s), 324
Chain condition,
  ascending, 278, 286
  descending, 286
Characteristic of a ring, 198
Chief series, 161
Class
  equivalence, 7
  residue modulo n, 6
Class equation, 156
Closed interval, 8
Closed set under an operation, 12, 37
Closure, algebraic, 323
Code, 238
  polynomial, 241
Code word, 238
Codomain, 3
Coefficients
  of a polynomial, 219
  torsion, 93, 96
Coloring of graph, 308
Commensurable numbers, 223
Commutative operation, 13
Commutative ring, 189
Commutator, 120, 128
Commutator subgroup, 120, 128
Comparable elements, 324
Complex number, 3, 33
  absolute value of, 34
  multiplication of, 34
Composition, function, 12, 14
  associativity of, 14
Composition series, 161
Congruence modulo n, 6
Conjugate elements over F, 345
Conjugate subgroups, 119, 120
Conjugation, 118
Conjugation isomorphism, 345

Consequence, 179
Constant polynomial, 219
Constructible number, 329
Constructible polygon, 380
Content of a polynomial, 237, 281
Contraction, elementary, 173
Correction of bit errors, 239
Correspondence, one-to-one, 4
Coset, 97
  double, 104
  left, 98
  right, 100
Coset group, 97
Crelle, August, 21
Cycle(s), 44
  disjoint, 44, 45
  k-, 44
Cyclic extension, 371
Cyclic group, 56, 61
  elementary properties of, 61
  finite, subgroups of, 66
  structure of, 64
Cyclic linear code, 238
Cyclic subgroup, 55, 61
Cyclotomic extension, 378
Cyclotomic polynomial, 234, 378

Decomposable group, 93
Decryption, 205
Dedekind, Richard, 191, 244
Definitions, 1
Degree
  of α over F, 315
  of an extension, 319
  of a polynomial, 219
Derivative, 340
Descartes, Rene, 218
Descending chain condition, 286
Detection of bit error, 239
Determinant of a square matrix, 28
Diagonal matrix, 28
Diagram, subgroup, 53
Digraph, 72
  arc of, 72
  vertex of, 72
Dihedral group, 46
Dimension of a vector space over F, 272
Direct product, 89
  external, 91
  internal, 91
  of rings, 187
Direct sum, 89
  of vector spaces, 274
Dirichlet, Peter Lejeune, 191
Discrete frieze group, 107
Discriminant of a polynomial, 378
Disjoint cycles, 44, 45
Disjoint sets, 5
Disjoint union of G-sets, 140
Distance between two strings, 238
Distributive law, 185
Division algorithm
  for $\mathbb{Z}$, 62
  for $F[x]$, 228, 286, 300
Division ring, 190
Divisor, 276, 300
  greatest common, 63, 281
  of a polynomial, 234
  of zero, 194
Domain
  Euclidean, 286
  of a function, 3
  integral, 196
  principal ideal, 276
  unique factorization, 276
Double coset, 104
Doubling the cube, 332

Edges of graph, 308
Eisenstein criterion, 233
Element(s), 1
  adjoining to field, 321
  algebraic over F, 313
  comparable, 324
  conjugate over F, 345
  equivalent, 212
  fixed, 342
  idempotent, 19, 31, 193, 199
  identity, 14, 20
  inverse of, 20
  irreducible, 276
  maximal, 325
  nilpotent, 193, 250
  orbit of, 82, 135
  order of, 61
  prime, 280
  primitive, 360
  separable over F, 359
  transcendental over F, 313
Elementary contraction, 173
Elementary symmetric function, 372
Empty set, 1
Empty word, 172
Encryption, 205
  RSA, 206
Endomorphism, 258
Equation, class, 156
Equivalence class, 7
Equivalence relation, 6
Equivalent elements, 212
Errors, bit, 239
Escher M. C., 109
Euclid, 201, 288
Euclidean algorithm, 288
Euclidean domain, 286
Euclidean norm, 286
Euler, Leonard, 21, 34, 202, 381
Euler formula, 34
Euler phi-function, 105, 202
Euler's theorem, 202
Evaluation homomorphism, 120, 189, 221
Even permutation, 83
Extension(s), 311
  abelian, 370
  algebraic, 319
  cyclic, 371
  cyclotomic, 378
  degree of, 319
  finite, 319
  finite normal, 362
  join of, 371
  of a map, 351
  by radicals, 384
  separable, 347, 359
  simple, 315
Extension field, 311
External direct product, 91

Factor, 276, 300
  of a polynomial, 300
Factor group, 113, 115
Factor theorem, 229
Faithful action, 133
Feit, Walter, 127, 152
Fermat, Pierre de, 201
Fermat prime, 381
Fermat's last theorem, 277
Fermat's $p = a^2 + b^2$ theorem, 295
Fermat's theorem, 200
  Euler's generalization of, 202
Ferrari, Lodovico, 385
Ferro, Scipione del, 385
Field, 190
  adjoining elements to, 321
  algebraic closure of, 323
  algebraic closure in E, 323
  algebraically closed, 323, 327
  extension of, 311
  fixed, 365
  Galois, 335
  intermediate, 344
  perfect, 359
  prime, 254
  of quotients, 211, 215
  of rational functions, 221
  separable extension of, 359
  simple extension of, 315
  skew, 190
  splitting, 347, 349, 353
  strictly skew, 190
  subfield of, 190
  tower of, 311
Field extension, 311
  simple, 315
Finite-basis condition, 286
Finite extension, 319
  degree of, 319
Finite generating set, 286
Finite group, 25
Finite presentation, 179
Finite-dimensional vector space, 269
Finitely-generated group, 71
Fixed elements, 342
Fixed field, 365
Fixed point, 110
Free abelian group, 167
  basis for, 167
  rank of, 168
Free generators, 174
Free group, 173
  rank of, 174
Frey, Gerhard, 277
Frieze group, 107

Frobenius, Georg, 150
Frobenius automorphism, 349
Frobenius homomorphism, 249
Function(s), 3
  codomain of, 3
  composite, 12, 14
  composition of, 12, 14
  domain of, 3
  elementary symmetric, 372
  Euler phi-, 105, 202
  image of *A* under, 78
  inverse of, 4
  one-to-one, 4
  onto, 4
  phi-, 105, 202
  polynomial on *F*, 227
  range of, 3
  rational, 221
  symmetric, 372
  trap door, 206
  two-to-two, 9
Fundamental homomorphism theorem, 117, 247
Fundamental theorem of algebra, 257, 324
Fundamental theorem of arithmetic, 280
Fundamental theorem of finitely-generated abelian groups, 170
  invariant factor version of, 93
  primary factor version of, 92
G-set(s), 132
  applications to counting, 140
  applications to finite groups, 136
  disjoint union of, 140
  isomorphic, 139
  orbits of, 135
  sub-, 139
  transitive, 133

Gallian, Joseph A., 108
Galois, Evariste, 162, 191, 337, 379
Galois field, 335
Galois group, 362
Galois theory, 341
  main theorems of, 364
Gauss, Carl F., 21, 92, 292, 334, 337, 379
Gauss's lemma, 282
Gaussian integer, 216, 292
Gaussian norm, 292
General linear group, 22
General polynomial of degree *n*, 372
Generating set, 70, 71
Generator(s), 56, 61, 70, 71
  for a presentation, 179
  free, 174
  of a group, 56, 61
  of a principal ideal, 254
  relation on, 75, 179
  for a vector space, 269
Glide reflection, 106
  nontrivial, 108
Graph, 308
Grassmann, Hermann, 268
Greatest common divisor, 63, 281
Griess, Robert L. Jr., 127
Gröbner basis, 305
Group(s), 20
  abelian, 20
  alternating on *n* letters, 84
  ascending central series of, 163
  automorphism of, 68, 118
  of automorphisms, 345
  blip, 177
  blop, 177
  center of, 60, 128, 163
  commutator in a, 120
  of cosets, 97
  cyclic, 56, 61
  decomposable, 93
  dihedral, 46
  direct product of, 89
  direct sum of, 89
  discrete frieze, 107
  elementary properties of, 23
  endomorphism of, 258
  factor, 115
  finite, 25
  finitely-generated, 71
  free, 173
  free on *A*, 173
  free abelian, 167
  frieze, 107
  Galois, 362
  general linear, 22
  generator(s) of, 56, 61, 70, 71
  indecomposable, 93
  inner automorphism of, 118
  isomorphic, 25, 26
  Klein 4-, 53
  notation and terminology, 39
  octic, 182
  order of, 41
  p-, 137
  permutation, 41, 77, 79
  plane crystallographic, 108
  of a polynomial, 365
  presentation of, 178, 179
  quaternion, 183
  quotient, 115
  regular representation of, 80
  series of, 157
  simple, 126
  solvable, 163
  special linear, 115
  subgroup of, 52
  symmetric on *n* letters, 43
  of symmetries, 105
  torsion, 119
  torsion free, 119
  wallpaper, 108
Group action, 132
Group algebra, 261
Group homomorphism, 77
Group ring, 261
Group table, 25
  properties of, 27
Hamilton, Sir William Rowan, 262, 268
Hamming distance, 238
Hamming weight, 238
Hilbert, David, 186
Hilbert basis theorem, 299
Hölder, Otto, 162, 178
Homomorphism, 113, 188
  evaluation, 120, 189, 221
  Frobenius, 249
  fundamental theorem for, 117, 247
  group, 77
  kernel of, 78, 188, 247
  projection, 246
  of a ring, 188, 245
Homomorphism property, 26

Ideal(s), 244
  ascending chain condition for, 278, 286
  basis for, 298
  descending chain condition for, 286
  finite-basis condition for, 286
  improper, 251
  left, 258
  maximal, 251
  maximum condition for, 286
  minimum condition for, 286
  nilradical of, 250
  prime, 252
  principal, 254
  product of, 258
  proper nontrivial, 251
  quotient of, 258
  radical of, 250
  right, 258
  sum of, 257
  trivial, 251
Idempotent element, 19, 31, 193, 199
Identity element, 14, 20
  left, 25
Image
  of *A*, 78
  inverse, 78
  under a map, 78
Imaginary number, 34
Improper ideal, 251
Improper subgroup, 52, 59
Improper subset, 2
Indecomposable group, 93
Indeterminate, 218
Index of a subgroup, 99
Induced operation, 12, 114
Infinite order, 61
Infinite set, 4
Information rate, 238
Injection, 4
Injection map, 4, 214
Inner automorphism, 118
Integer(s), 2
  algebraic, 378
  Gaussian, 216, 292
  rational, 292
  relatively prime, 64