

Index

Note: Numerals in boldface type indicate where a notion or notation is defined.

- $(\)$, **9**
- $1^{m_1} \dots n^{m_n}$, **228**
- $A \times B$, **8**
- $A(m, x)$, **109**
- A_n , **9**
- $C_G(U)$, **7**
- C_n , **8**
- $E(A)$, **36**
- $G|_\Delta$, **9**
- $G \wr H$, **10**
- G' , **8**
- $G(\mathcal{P})$, **201**
- G^Δ , **9**
- $G^{[i]}$, **55**
- $G_{(\Delta)}$, **9**
- G_Δ , **10**
- $H \lesssim G$, **7**
- $H \triangleleft\triangleleft G$, **7**
- $L[i]$, **12**
- $N(k, \Pi, d_1, \dots, d_i)$, **231**
- $N_G(U)$, **7**
- $N_n(x)$, **231**
- $O(f)$, **11**
- $O^\infty(G)$, **8**
- $O_p(G)$, **8**
- $O_\infty(G)$, **8**
- S_n , **9**
- $T_n(x)$, **231**
- $[H, K]$, **8**
- $[a, b]$, **8**
- $\text{Alt}(\Omega)$, **9**
- $\text{Aut}(G)$, **7**
- $\text{Aut}(\mathcal{X})$, **11**
- Δ^g , **9**
- $\text{Diag}(H)$, **129**
- $\text{GF}(q)$, **8**
- $\text{GL}_d(q)$, **8**
- $\text{Inn}(G)$, **7**
- $\Omega(f)$, **11**
- $\Omega_{\mathcal{P}}(\gamma_1, \dots, \gamma_{l-1})$, **205**
- $\text{Out}(G)$, **7**
- $\Pi \wedge \Sigma$, **208**
- $\mathcal{R}(\Pi)$, **209**
- $\text{Soc}(G)$, **8**
- $\text{Sym}(\Omega)$, **9**
- $\mathcal{T}(t)$, **202**
- $\Theta(H)$, **210**
- $\Theta(f)$, **11**
- $\mathcal{X}(V, \mathcal{E})$, **11**
- $\mathcal{X}(\alpha, \beta)$, **212**
- α^g , **9**
- \mathbb{N} , **10**
- \mathbb{R} , **10**
- \mathbb{Z} , **10**
- $\text{fix}(G)$, **117**
- $\langle S \rangle$, **7**
- $\langle U^G \rangle$, **7**
- μ , **94, 228**
- ω^G , **9**
- $O^\sim(f)$, **11**
- $\prod A_i$, **8**
- $\text{supp}(g)$, **9**
- $\varphi((\gamma_1, \dots, \gamma_l))$, **202**
- ξ , **94, 228**
- $\sigma(f)$, **11**
- $\text{OP}(\Omega)$, **207**
- $\text{Prob}(A|B)$, **30**
- Ackerman function, **109, 176**
- automorphism group, **7, 129, 131, 144**
 of a graph, **11, 207**
- backtrack, **53, 169, 201–217**
- base, **50, 55**
 \mathcal{R} -base, **210**
 nonredundant, **55**

- base change, **82**, **97**, 112, 116, 134, 143, 190, 204, 205
- black-box f -recognizable, **192**, 193, 195, 196, 198
- black-box group, **16**, 16–47, 135, 139, 192, 193, 195, 228, 235–244
- block, **9**, 50, 100, 107–110, 112, 113, 121, 142, 190, 214
 maximal, **9**, 144, 146
 minimal, **9**, 101–107, 112
- block homomorphism, **81**
- block system, **9**, 121, 126, 128, 142, 176, 178
 maximal, **9**, 191
 minimal, **9**, 132, 149, 247, 253
- Cayley graph, **12**, 26, 64
 center, **7**, 50, 120, 133
 centralizer, **7**, 53, 117–124, 130, 134, 149, 150, 152, 158, 169, 172, 205, 216
- Chernoff's bound, **31**, 33–35, 37–39
 basic-type application, **32**
- chief series, 49, 155
- closure, **83**, 111
 G -closure, **7**, 23, 38, 44, 83
 normal closure, **7**, 23, 83, 111, 116, 138, 140, 155, 250, 251
- collection, **17**, **165**
- commutator, **8**
- complement, **7**, 182
- composition series, 50, 125–155, 158, 165, 193, 197, 199
- conjugacy class, 172, 214–216
- constructive recognition, 168, **192**, 193, 195, 196, **227**, 235–246
- coordinatization, **167**, 169–171, 173
- core, **8**, 50, 124, 180
 p -core, **8**, 51, 138, 157–159
- coset enumeration, 184–186
- cube, **64**, 67, 69
 nondegenerate, **65**
- cycle type, **228**
- degree
 of a graph or hypergraph, **11**
 of a permutation, **9**
 of a permutation group, **9**
- derived series, **8**, 24, 38, 49, 84, 159
- diagonal subgroup, **129**, 131, 144, 160
- direct product, **8**, 119–122, 129, 141, 147, 216
 projection, **8**, 130
- directed graph, **11**
 out-degree, **11**
 strongly connected, **12**, 112, 251
 underlying graph, **12**, 219
- double coset, 53, 203
- forest, **12**, 219, 249
- Fratini argument, 170, 182
- Frobenius group, **10**, 133, 137, 148, 160
- graph, **11**
 component, **12**, 112
 connected, **12**
- Hall subgroup, 182
- hash function, **22**, 142
- hypergraph, **11**, 87
 uniform, **11**, 87
- labeled branching, **219**, 218–225
 represents a group, **220**
 represents a transversal, **220**
- Las Vegas algorithm, **14**
- local expansion, 72
- lower central series, **8**, 24, 38, 49, 84, 180
- Markov chain, **25**, 27, 215, 217
 aperiodic, **25**, 28, 47, 215
 irreducible, **25**, 28, 215
 period of, **25**, 47
 stationary distribution of, **25**, 28, 215
 transition probability, **25**, 28, 47, 215
- Monte Carlo algorithm, **13**
- nearly linear-time algorithm, **51**
- nearly uniform distribution, **24**, 29
- nilpotent group, 175–182
- nonconstructive recognition, 227
- normalizer, **7**, 134, 137, 142, 154, 170, 211
- orbit, **9**, 18, 36, 49, 60, 65, 102, 112, 120–122, 141, 143, 144, 154, 173, 179, 189, 190, 252
 fundamental, **56**, 83, 97, 99, 182, 204, 223
- orbital graph, **212**, 251
- ordered partition, **207**
 cell of, **207**
 refinement, **208**
- out-degree, **11**
- path, **12**, 219, 252
- perfect group, **8**, 146
- permutation group as black-box group, **93**, 135, 138, 139, 192, 193, 197
- permutation isomorphism, **10**, 95, 119, 127, 128, 140, 142, 146, 173
- polycyclic generating sequence, **162**, 163, 165, 166, 181
- power-conjugate presentation, 165–166
- presentation, 49, 112, 165, 184, 192, 194, 197–200, 227, 236, 237, 244, 247, 250

- primitive group, **9**, 95, 100, 126, 129–149, 160, 225, 251
 product replacement algorithm, **27**
- random prefix, **40**
 random subproduct, **30**, 30–40, 73, 77, 84, 88, 92, 182, 245, 246, 249
 recognition, *see* constructive recognition
 regular graph, **11**
 regular group, **10**, 78, 113, 129, 133, 137, 138, 146, 150, 154, 160, 161
- Schreier generator, **58**, 59, 62, 73, 76–78, 86, 88, 92, 97, 177, 198, 222, 246, 249
 Schreier tree, **56**, 65, 67, 70, 72, 75, 77, 82, 85, 136, 155, 163, 190
 shallow, **114**
 Schreier vector, *see* Schreier tree
 Schreier–Sims algorithm, **59**
 Schur–Zassenhaus theorem, **182**
 search tree, **202**
 semiregular group, **10**, 117, 123, 130
 SGS, **50**, **55**
 construction, 59, 63, 70, 72, 75, 86, 87, 90, 99, 162, 193, 222, 246
 testing, 64, 77, 186, 190, 193
 siftee, **56**
 sifting, **56**
 as a word, **86**, 88, 91, 128, 156, 166, 167, 187
 in a labeled branching, **221**, 223, **224**
 small-base group, **51**
 socle, **8**, 51, 129, 147–149, 152–154, 161
 solvable radical, **8**, 157–159, 216
 solvable residual, **8**, 150, 152
 spreader, **41**
- stabilizer
 pointwise, **9**, 49, 79, 115, 127, 247
 setwise, **10**, 53, 145, 176, 206
 standard word, **93**
 straight-line program, **10**, 192–194, 197, 199, 200, 227, 239, 240, 243, 244, 250
 strong generating set, *see* SGS
 subdirect product, **8**, 130, 160
 subnormal, **7**, 49, 124, 149, 152, 160, 161, 180
 support, **9**
 Sylow subgroup, 50, 95, 125, 157, 161, 167–172, 182, 216
- transitive closure, **219**, 220
 transitive constituent homomorphism, **81**
 transitive group, **9**, 36, 87, 117
 transversal, **8**, 56, 57, 59, 65, 82, 101, 118, 218, 220, 246, 247, 249, 253
- tree, **12**
 breadth-first-search, **19**, 65, 68, 113, 157, 187
 rooted, **12**, 108, 111, 202, 219
 children of a vertex, **12**
 leaf, **12**
 parent of a vertex, **12**
- Union-Find data structure, **108**, 113
 up-to-date SGS data structure, **59**, **70**, 83, 88, 91
 upper central series, **8**, 179–181
- valency, **11**
- walk, **12**, 25, 212, 213, 215
 lazy random, **26**
 wreath product, **10**, 119, 122, 129, 160, 226