

Appendix

Category Theory

In this book, we introduced and studied several mathematical structures, viz. semi-groups, groups, rings, and fields. We noticed some common features in the study of these structures. The category theory gives a unified general and abstract setting for all these and many more mathematical structures such as modules, vector spaces, and topological spaces. Quite often, in mathematics, the concrete results are expressed in the language of category theory. This appendix introduces the very basics in category theory for the purpose. The Gödel–Bernays axiomatic system for sets is the most suitable axiomatic system for category theory. As described in Chap. 2, class is a primitive term in this axiomatic system instead of sets. Indeed, sets are simply the members of classes. The classes which are not sets are termed as proper classes.

Definition A category Σ consists of the following:

1. A class $Obj\Sigma$ called the class of objects of Σ .
2. For each pair A, B in $Obj\Sigma$, we have a set $Mor_\Sigma(A, B)$ called the set of morphisms from the object A to the object B . Further,

$$Mor_\Sigma(A, B) \cap Mor_\Sigma(A', B') \neq \emptyset \text{ if and only if } A = A' \text{ and } B = B'.$$

3. For each triple A, B, C in $Obj\Sigma$, we have a map \cdot from $Mor_\Sigma(B, C) \times Mor_\Sigma(A, B)$ to $Mor_\Sigma(A, C)$ called the law of composition. We denote the image $\cdot(g, f)$ by gf . Further, the law of composition is associative in the sense that if $f \in Mor_\Sigma(A, B)$, $g \in Mor_\Sigma(B, C)$ and $h \in Mor_\Sigma(C, D)$, then $(hg)f = h(gf)$.

4. For each $A \in Obj\Sigma$, there is an element I_A in $Mor_\Sigma(A, A)$ such that $fI_A = f$ for all morphisms from A , and $gI_A = g$ for all morphisms to A .

Clearly, for each object A of Σ , I_A is unique morphism, and it is called the identity morphism on A . The category Σ is called a **small category** if $Obj\Sigma$ is a set.

Examples 1. We have the category SET of sets whose objects are sets, and the morphisms from a set A to a set B are precisely the maps from A to B .

2. There is a category GP of groups whose objects are groups, and the morphisms from a group H to a group K are homomorphisms from H to K .

3. SG denotes the category of semigroups all of whose objects are semigroups, and morphisms are semigroup homomorphisms.

4. AB denotes the category of abelian groups whose objects are abelian groups, and morphisms are group homomorphisms.

5. $RING$ denotes the category of rings whose objects are rings, and morphisms are ring homomorphisms.

6. TOP denotes the category of topological spaces whose objects are topological spaces, and the morphisms are continuous maps.

7. A group G can also be treated as a category having a single object G . The elements of the group can be taken as morphisms from G to G , and the composition of the morphisms is the binary operation of G .

Let Σ be a category. A morphism f from A to B is said to be a monomorphism (epimorphism) if it can be left (right) canceled in the sense that $fg = fh$ ($gf = hf$) implies that $g = h$. A morphism f from A to B is said to be an isomorphism if there is a morphism g from B to A such that $gf = I_A$ and $fg = I_B$. Clearly, such a morphism g is unique, and it is called the inverse of f . The inverse of f , if exists, is denoted by f^{-1} .

Remark In the category SET of sets, a morphism f from a set A to a set B is a monomorphism (epimorphism) if and only if it is an injective (surjective) map. Also in the category GP , a morphism f from a group H to a group K is a monomorphism if and only if f is injective (prove it). Clearly, an isomorphism is a monomorphism as well as an epimorphism. However, a morphism which is a monomorphism as well as epimorphism need not be an isomorphism. For example, consider the category $Haus$ of Hausdorff topological spaces. The inclusion map from \mathbb{Q} to \mathbb{R} is a monomorphism as well as an epimorphism (it is an epimorphism because \mathbb{Q} is dense in \mathbb{R}) but it is not an isomorphism.

Let Σ be a category and A be an object of Σ . Then, $Mor_{\Sigma}(A, A)$ is a monoid with respect to the composition of morphisms. The members of $Mor_{\Sigma}(A, A)$ are called the endomorphisms of A . The monoid $Mor_{\Sigma}(A, A)$ is denoted by $End(A)$. An isomorphism from A to A is called an automorphism of A . The set of all automorphisms of A is denoted by $Aut(A)$ which is a group under the composition of morphisms.

Let Σ be a category. We say that a category Γ is a subcategory of Σ if (i) $Obj\Gamma \subseteq \Sigma$, (ii) for each pair $A, B \in Obj\Gamma$, $Mor_{\Gamma}(A, B) \subseteq Mor_{\Sigma}(A, B)$, and (iii) the law of composition of morphisms in Γ is the restriction of the law of composition of morphisms in Σ to Γ . The subcategory Γ is said to be a full subcategory if $Mor_{\Gamma}(A, B) = Mor_{\Sigma}(A, B)$ for all $A, B \in Obj\Gamma$. AB is a full subcategory of GP .

Functors

Definition Let Σ and Γ be categories. A functor F from Σ to Γ is an association which associates with each member $A \in \text{Obj}\Sigma$, a member $F(A)$ of Γ , and to each morphism $f \in \text{Mor}_\Sigma(A, B)$, a morphism $F(f) \in \text{Mor}_\Gamma(F(A), F(B))$ such that the following two conditions hold:

- (i) $F(gf) = F(g)F(f)$ whenever the composition gf is defined.
- (ii) $F(I_A) = I_{F(A)}$ for all $A \in \Sigma$.

Let Σ be a category. Consider the category Σ^o whose objects are same as the objects of Σ , $\text{Mor}_{\Sigma^o}(A, B) = \text{Mor}_\Sigma(B, A)$, and the composition fg in Σ^o is same as gf in Σ . The category Σ^o is called the opposite category of Σ . A functor from Σ^o to the category Γ is called a contravariant functor from Σ to Γ .

If Σ is a category, then the identity map $I_{\text{Obj}\Sigma}$ from $\text{Obj}\Sigma$ to itself defines a functor called the identity functor. Composition of any two functors is again a functor.

Examples 1. Let H be a group. Denote its abelianizer $H/[H, K]$ by $Ab(H)$. Let f be a homomorphism from H to a group K . Then f induces a homomorphism $Ab(f)$ from $Ab(H)$ to $Ab(K)$ defined by $Ab(f)(h[H, H]) = f(h)[K, K]$. This defines a functor Ab from the category GP of groups to the category AB . This functor is called the abelianizer functor.

2. Let H be a group. Denote the commutator $[H, H]$ of H by $Comm(H)$. If f be a homomorphism from H to K , it induces a homomorphism $Comm(f)$ from $Comm(H)$ to $Comm(K)$ defined by $Comm(f)([a, b]) = [f(a), f(b)]$. This defines a functor $Comm$ from the category GP to itself. This functor is called the commutator functor.

3. We have a functor Ω from the category GP of groups to the category SET of sets which simply forgets the group structure and retains the set part of the group. More explicitly, $\Omega(G, o) = G$. Such a functor is called a forgetful functor. There is another such functor from the category $RING$ of rings to the category AB of abelian groups which forgets the ring structure, but retains the additive group part of the ring. There is still another forgetful functor from the category TOP to the category SET which forgets the topological structure, and retains the set part of the space.

4. Let f be a map from a set X to a set Y . Then, f induces a unique homomorphism $F(f)$ from the free group $F(X)$ to the free group $F(Y)$. This gives us the functor F from the category SET to the category GP . This functor is called the free group functor.

5. Let Σ be a category and A be an object of Σ . For each $B \in \text{Obj}\Sigma$, we put $\text{Mor}_\Sigma(A, -)(B) = \text{Mor}_\Sigma(A, B)$, and for each morphism f from B to C , we have a map $\text{Mor}_\Sigma(A, -)(f)$ from $\text{Mor}_\Sigma(A, B)$ to $\text{Mor}_\Sigma(A, C)$ defined by $\text{Mor}_\Sigma(A, -)(f)(g) = fg$. It is easily verified that $\text{Mor}_\Sigma(A, -)$ defined above is a functor from Σ to the category SET of sets. Similarly, we have a contravariant functor $\text{Mor}_\Sigma(-, A)$ from the category Σ to the category SET of sets.

Remark There is a useful important functor, viz, homotopy group functor π_1 from the category TOP^* of pointed topological spaces to the category GP of groups. It has tremendous application in geometry and topology. This functor will be discussed in Algebra 3.

Let F be a functor from a category Σ to a category Γ . The functor F is said to be faithful if for each pair $A, B \in Obj\Sigma$, the induced map $f \mapsto F(f)$ from $Mor_\Sigma(A, B)$ to $Mor_\Gamma(F(A), F(B))$ is injective. The functor F is said to be a full functor if these induced maps are surjective. The forgetful functor from GP to SET is faithful but it is not full. The abelianizer functor Ab is not faithful. A functor F is said to be an isomorphism from the category Σ to the category Γ if there is a functor G from Γ to Σ such that $GoF = I_\Sigma$ and $FoG = I_\Gamma$.

Natural Transformations

Definition Let F and G be functors from a category Σ to a category Γ . A natural transformation η from F to G is a family $\{\eta_A \in Mor_\Gamma(F(A), G(A)) \mid A \in Obj\Sigma\}$ of morphisms in Γ such that the diagram

$$\begin{array}{ccc}
 F(A) & \xrightarrow{\eta_A} & G(A) \\
 \downarrow F(f) & & \downarrow G(f) \\
 F(B) & \xrightarrow{\eta_B} & G(B)
 \end{array}$$

is commutative for all morphisms f in Σ .

Examples 1. Let ν_G denote the quotient homomorphism from G to $G/[G, G]$. Then, the family $\{\nu_G \mid G \in ObjGP\}$ defines a natural transformation ν from the identity functor I_{GP} to the abelianizer functor Ab .

2. For each set X , we have the inclusion map i_X from X to $\Omega(F(X))$ where F is the free group functor, and Ω is the forgetful functor. Evidently, the family $\{i_X \mid X \in ObjSET\}$ of maps defines a natural transformation from the identity functor I_{SET} to the functor $\Omega o F$ on the category SET .

Let F and G be two functors from a category Σ to a category Γ . A natural transformation η from F to G is called a natural equivalence if η_A is an isomorphism from $F(A)$ to $G(A)$ for all $A \in Obj\Sigma$. This is equivalent to say that there is a natural transformation ρ from G to F such that $\rho_A o \eta_A = I_{F(A)}$ and $\eta_A o \rho_A = I_{G(A)}$ for all

objects A of Σ . A functor F from Σ to Γ is called an equivalence from Σ to Γ if there is a functor G from Γ to Σ such that $F \circ G$ and $G \circ F$ are naturally equivalent to the corresponding identity functors. Notice that there is a difference between isomorphism and equivalence between categories. An equivalence need not be an isomorphism.

Let Σ and Γ be categories. Then, $\Sigma \times \Gamma$ represents the category whose objects are pairs $(A, B) \in \text{Obj}\Sigma \times \text{Obj}\Gamma$, and a morphism from (A, B) to (C, D) is a pair (f, g) , where f is a morphism from A to C in Σ , and g is a morphism from B to D in Γ . The composition law is coordinate-wise. This category is called the product category.

Let F be a functor from a category Σ to a category Γ . Let f be a morphism from C to A in Σ , and g be a morphism from B to D in Γ . This defines a map $Mor_{\Gamma}(F(f), g)$ from the set $Mor_{\Gamma}(F(A), B)$ to $Mor_{\Gamma}(F(C), D)$ given by $Mor_{\Gamma}(F(f), g)(h) = ghF(f)$. This defines a functor $Mor_{\Gamma}(F(-), -)$ from the product category $\Sigma \times \Gamma$ to the category SET of sets. Similarly, given a functor G from Γ to Σ , we have a functor $Mor_{\Sigma}(-, G(-))$ to the category SET of sets. We say that F is left adjoint to G , or G is right adjoint to F if there is a natural isomorphism η from the functor $Mor_{\Gamma}(F(-), -)$ to the functor $Mor_{\Sigma}(-, G(-))$. More explicitly, for each object A in Σ and each object B in Γ , we have a bijective map $\eta_{A,B}$ from $Mor_{\Gamma}(F(A), B)$ to the set $Mor_{\Sigma}(A, G(B))$ such that $Mor_{\Sigma}(f, G(g)) \circ \eta_{A,B} = \eta_{C,D} \circ Mor_{\Gamma}(F(f), g)$ for all morphisms (f, g) in $\Sigma \times \Gamma$ (look at the corresponding commutative diagram).

Examples 1. Consider the category SET of sets and the category GP of groups. We have the free group functor F from the category SET to the category GP . More explicitly, for each set X , we have the free group $F(X)$ on the set X . We also have the forgetful functor Ω from GP to SET . From the universal property of free group, every group homomorphism f from $F(X)$ to G determines and is uniquely determined by its restriction to X . This gives us a bijective map $\eta_{X,G}$ from $Hom(F(X), G)$ to $Map(X, \Omega(G))$. It is easy to observe (using the universal property of a free group) that η , thus obtained, is a natural equivalence. Hence, the free group functor F is left adjoint to the forgetful functor Ω .

2. We have the forgetful functor Ω from the category AB of abelian groups to the category GP of groups. We also have the abelianizer functor Ab from GP to AB . It can be easily verified that Ab is left adjoint to Ω .

Products and Coproducts in a Category

Definition Let A and B be objects in a category Σ . A product of A and B in Σ is a triple (P, f, g) , where P is an object of the category Σ , f is morphisms from P to A , and g is a morphism from P to B such that given any such triple (P', f', g') , there is a unique morphism ϕ from P' to P such that $f\phi = f'$ and $g\phi = g'$.

It is easily observed from the definition that if (P, f, g) and (P', f', g') are two products of A and B , then there is an isomorphism ϕ from P' to P with $f\phi = f'$ and

$g\phi = g'$. Thus, if the product exists, then it is unique up to natural isomorphism. The product of A and B is usually denoted by $A \times B$.

In the category SET of sets, the Cartesian product $A \times B$ with the corresponding projection maps is the product in the category SET . Similarly, the direct product $H \times K$ of the groups H and K together with the corresponding projection maps is the product of H and K in the category GP .

Dually, we have the following:

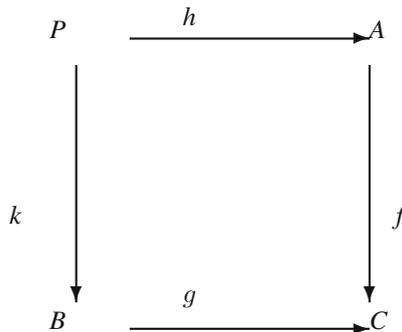
Definition Let A and B be objects in a category Σ . A coproduct of A and B in Σ is a triple (U, f, g) , where U is an object of the category Σ , f is morphisms from A to U , and g is a morphism from B to U such that given any such triple (U', f', g') , there is a unique morphism ϕ from U to U' such that $\phi f = f'$ and $\phi g = g'$.

It is easily observed from the definition that if (U, f, g) and (U', f', g') are two coproducts of A and B , then there is an isomorphism ϕ from U to U' with $\phi f = f'$ and $\phi g = g'$. Thus, if the co-product exists, then it is unique up to natural isomorphism. The coproduct of A and B is denoted by $A \coprod B$.

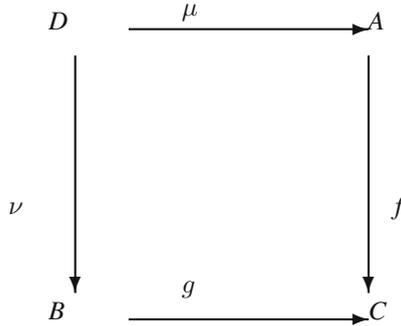
In the category SET of sets, the disjoint union $(A \times \{0\}) \cup (B \times \{1\})$ of A and B with the natural inclusion maps is the coproduct of A and B in the category SET . Similarly, the free product $H \star K$ of the groups H and K together with the natural inclusion maps is the coproduct of H and K in the category GP .

PullBack and Push-out Diagrams

Definition Let Σ be a category. Let $f \in Mor_{\Sigma}(A, C)$, and $g \in Mor_{\Sigma}(B, C)$. A commutative diagram



is said to be a pullback diagram if given any commutative diagram



there exists a unique morphism ϕ from D to P such that $h\phi = \mu$ and $k\phi = \nu$.

Dually, a push-out diagram can be defined by reversing the arrows in the definition. The reader is advised to formulate the definition of push-out diagram.

In general, pullback and push out need not exist in a category. However, they exist in the category SET of sets and also in the category GP of groups: Let f be a morphism from A to C , and g be a morphism from B to C in the category SET/GP . Consider the product $A \times B$ in the category SET/GP . Let $P = \{(a, b) \in A \times B \mid f(a) = g(b)\}$. Let h denote first projection from P to A , and k denotes the second projection from P to B . This gives us a pullback diagram in SET/GP . Similarly, push out also exists in the category SET , and also it exists in the category GP .

Bibliography

1. Cohen, P.J.: Set Theory and Continuum Hypothesis. Dover Publication (2008)
2. Halmos, P.R.: Naive Set Theory. Springer (1914)
3. Kakkar, V.: Set Theory. Narosa Publishing House (2016)
4. Artin, M.: Algebra. Pearson Education (2008)
5. Herstein, I.N.: Topics in Algebra, 2nd edn. Wiley, New York (1975)
6. Jacobson, N.: Basic Algebra I. Freeman, San Francisco, II (1980)
7. Lang, S.: Algebra, 2nd edn. Addison-Wesley, MA (1965)
8. Birkoff, G., MacLane, S.: A survey of Modern Algebra, 3rd edn. Macmillan, New York (1965)
9. Hungerford, T.W.: Algebra, 8th edn. Springer, GTM (2003)
10. Rademacher, H.: Lectures on Elementary Number Theory. Krieger Publishing Co (1977)
11. Serre, J.P.: A Course in Arithmetic. Springer (1977)
12. Robinson, D.J.S.: A Course in The Theory of Groups, 2nd edn. Springer (1995)
13. Rotman, J.J.: An Introduction to the Theory of Groups, 4th edn. Springer, GTM (1999)
14. Suzuki, M.: Group Theory I and II. Springer (1980)
15. Curtis, M.L.: Matrix Groups. Springer (1984)
16. Magnus, W., Karrass, A., Solitar, D.: Combinatorial Group Theory. Wiley, Newyork (1966)
17. Rudin, W.: Principles of Mathematical Analysis, 3rd edn. McGraw Hill (1976)

Index

A

Abelian group, 98
Abelianizer, 165
Absolute value, 68
Affine space, 262
Alternating group, 189
Alternating map, 187
Antisymmetric, 25
Archemidean property, 90
Arithmetic and ideals, 391
Artin-Chevalley, 265
Associates, 71
Associative, 94
Augmentation ideal, 259
Augmentation map, 259
Automorphism, 113
Automorphism group, 117
Axiom of choice, 35
Axiom of existence, 16
Axiom of extension, 13
Axiom of infinity, 20
Axiom of pairing, 17
Axiom of power set, 19
Axiom of regularity, 19
Axiom of specification, 14
Axiom of union, 17

B

Bijjective, 30
Binary operation, 57, 94
Binomial theorem, 223
Borel subgroups, 201
Brauer, 363
Burnside Basis theorem, 373
Burnside, W., 363

C

Caley Theorem, 191
Cardinal numbers, 49
Cartesian product, 22, 34
Cartesian product of groups, 155
Category, 421
Cauchy sequence, 88
Center, 125
Central endomorphism, 167
Central product, 374
Centralizer, 125
Chain, 38
Chain of subgroups, 126
Characteristically simple group, 166
Characteristic of an integral domain, 229
Characteristic subgroup, 166
Chinese remainder theorem, 281
Chinese remainder theorem in rings, 404
Circle group, 100
Class equation, 313
Class number, 320
Classical class equation, 315
C.L.T group, 363
Co-domain, 29
Co-maximal pair, 404
Commutative, 94
Commutative ring, 222
Commutator series, 360
Commutator subgroup, 164
Complement, 16
Complete order, 40
Complex numbers, 91
Composition, 23
Composition length, 343
Composition of maps, 29
Composition series, 339
Congruence on a group, 158

Conjugacy class, 314
 Conjugacy class of a permutation, 184
 Conjugacy problem, 382
 Conjugate, 314
 Consistency of premises, 12
 Constant map, 30
 Continuum hypothesis, 50
 Contradiction, 8
 Coordinate ring, 267
 Core of a subgroup, 172
 Correspondence theorem for groups, 128
 Correspondence theorem for rings, 241
 Correspondence theorem of maps, 36
 Countable set, 50, 61
 Cycle decomposition, 183
 Cycles, 181
 Cyclic group, 134
 Cyclic reduction, 383

D

Decomposition of groups, 353
 Defining relations, 380
 Definition by induction, 57
 Degree of a polynomial, 253
 Dehn fundamental problems, 382
 Dehn, M., 377
 Derivable, 384
 Derived length, 360
 Derived series, 360
 Derived subgroup, 164
 Dihedral group, 102
 Division algorithm, 69, 254
 Division ring, 227
 Divisor function, 125, 270
 Divisors, 387
 Domain, 29

E

Eisenstein Irreducibility Criteria, 417
 Embedding, 67
 Empty set, 16
 Endomorphism, 113
 Equipotent, 49
 Equivalence class, 27
 Equivalence relation, 26
 Equivariant map, 319
 Euclidean Algorithm, 72
 Euclidean Domain, 399
 Euler–Fermat’s theorem, 150
 Euler’s criteria, 293
 Even permutation, 188

Existential quantifier, 7
 External direct product, 104
 Extra special p-group, 374

F

Factor theorem, 257
 Family of sets, 34
 Feit, W., 363
 Fermat prime, 79
 Field, 227
 Field of fractions, 236
 Finite Abelian groups, 335
 Finite set, 37
 First isomorphism theorem, 175
 Fitting Lemma, 354
 Fitting subgroup, 369
 Fixed point set, 313
 Frattini subgroup, 371
 Free group, 379
 Free presentation, 380
 Free product, 386
 Free reduction, 383
 Fully invariant subgroup, 166
 Function, 29
 Fundamental theorem of algebra, 91
 Fundamental theorem of arithmetic, 75
 Fundamental theorem of homomorphism,
 173
 Functor, 423

G

Gauss Lemma, 296, 411
 Gauss Theorem, 411
 Gauss Quadratic Reciprocity, 299
 Gaussian domain, 406
 Gaussian integers, 220
 Generalized continuum hypothesis, 50
 Greatest common divisor (g.c.d.), 71, 388
 Greatest lower bound (g.l.b.), 39
 Group, 98
 Group action, 311
 Group of isometries, 101
 Group of motions, 101
 Group of prime residue classes, 99
 Group of symmetry, 102
 Group of unit Quaternions, 105
 Group ring, 251
 Group with operator, 165
 Groupoid, 94
 Groups of order pq, 329

H

Hall subgroup, 364
 Hall, P., 363
 Higher degree congruence, 279
 Homomorphism, 113
 Hyper surface, 262

I

Ideal of a ring, 242
 Idempotent, 226
 Identity map, 29
 Image, 32
 Inclusion, 30
 Indecomposable group, 157
 Index of a subgroup, 147
 Index set, 34
 Infimum, 39
 Initial segment, 40
 Injective, 30
 Inner automorphism, 118
 Inner conjugation, 314
 Inner conjugation of G on G , 315
 Integers, 62
 Integral domain, 224
 Integral powers, 107
 Intersection, 15
 Invariant subgroup, 159
 Inverse image, 32
 Inverse map, 30
 Irreducibility criteria, 415
 Irreducible elements, 388
 Irreducible integers, 71
 Isomorphism, 113
 Isomorphism problem, 383
 Isotropy group, 312

J

Jordan Holder Theorem, 343

K

Kernel of a homomorphism, 128, 240
 Kernel of a map, 35
 Klein's four group, 100
 Krull–Remak–Schmidt theorem, 170, 353

L

Lagrange theorem, 147
 Largest element, 39
 Lattice, 43
 Least common multiple (l.c.m.), 71, 388

Least element, 39
 Least upper bound (l.u.b), 39
 Left and right cosets, 146
 Legendre symbol, 294
 Limit ordinal, 47
 Linear congruence, 79
 Linear Diophantine Equations, 83
 Local isotropy group, 312
 Logical inference, 9
 Lorentz orthogonal group, 214
 Lower bound, 39
 Lower central series, 365

M

Map, 29
 Maximal element, 39
 Maximal ideal, 244
 Mersenne prime, 79
 Möbius function, 270
 Minimal element, 39
 Mobius inversion formula, 273
 Monoid, 95
 Multiplicative function, 271

N

Natural numbers, 55
 Nilpotency class, 366
 Nilpotent, 226
 Nilpotent group, 366
 Noether 2nd isomorphism theorem, 176
 Nongenerator, 371
 Normal endomorphism, 166
 Normal series, 338
 Normal subgroup, 159
 Normal subgroups of permutation groups, 185
 Normalizer, 125
 Normalizer condition, 370
 Normalizer of a subgroup, 172
 Novikiv and Boon, 383

O

Odd permutation, 188
 Orbit, 312
 Order in \mathbb{N} , 59
 Order isomorphic, 44
 Order of a group, 99
 Order of an element, 134
 Ordered field, 249
 Ordered pair, 22
 Ordinal number, 43

Orthogonal group, 210

P

Partial order, 38
 Partition, 27
 Partition function, 186
 Peano's axioms, 55
 Perfect group, 358
 Perfect number, 277
 Permutation group, 179
 Permutation representation, 190, 311
 Permutations of same form, 184
 Pivot, 203
 Poincare, H., 377
 Polynomial function, 262
 Polynomial ring, 253
 Polynomials in several variable, 262
 Power set, 19
 Presentation of a group, 380
 Prime elements, 388
 Prime ideal, 245
 Prime integer, 71, 75
 Primitive polynomial, 411
 Principal Ideal Domain, 393
 Principal ideals, 391
 Principal series, 339
 Principle of induction, 56
 Product, 35
 Projection, 30
 Proof by induction, 56
 Proper subgroup, 123
 Propositional calculus, 2
 Propositional connectives, 2

Q

Quadratic residue, 290
 Quaternion group, 101
 Quotient field, 236
 Quotient group, 163
 Quotient map, 36
 Quotient ring, 242
 Quotient set, 27

R

Radical ideal, 246
 Radical of a group, 361
 Radical of an ideal, 246
 Rank of a group, 373
 Rational numbers, 86
 Real numbers, 88
 Recursion theorem, 51, 56

Reduced ring, 247
 Reduced row echelon form, 203
 Reflexive, 25
 Regular action, 314
 Regular permutation representation, 314
 Relation, 22
 Remainder, 70
 Remainder theorem, 257
 Residue classes, 79
 Residue classes modulo m , 80
 Restriction, 30
 Ring, 219
 Ring homomorphism, 233
 Ring isomorphism, 233
 Ring of Quaternions, 220
 Ring with identity, 222
 Roots of a polynomial, 257
 Rules of inference, 10
 Russel's paradox, 15

S

Schreier theorem, 340
 Second principle of induction, 60
 Semigroup, 94
 Semigroup of endomorphisms, 117
 Semigroup ring, 251
 Semisimple group, 361
 Sequence, 88
 Set, 13
 Set of generators, 131
 Sharply doubly transitive, 320
 Sharply transitive, 320
 Sign map, 187
 Simple group, 160
 Simplicity of alternating group, 193
 Small category, 421
 Solvable group, 360
 Special linear group, 209
 Special orthogonal group, 211
 Special unitary group, 215
 Stabilizer, 312
 Statement formulas, 3
 Statement variables, 3
 Subgroup, 122
 Subgroup generated by a set, 129
 Subnormal subgroup, 347
 Subring, 238
 Subring generated by a subset, 240
 Subset, 14
 Successor, 19
 Successor set, 20
 Sum of divisors, 270

Supremum, 39
Surjective map, 30
Sylow subgroups, 322
Sylow Theorems, 321
Symmetric, 25
Symmetric group, 101, 179

T

Tautology, 8
Thompson, J.G., 363
Tietze, 377
Tietze transformation, 384
Torsion free group, 135
Torsion group, 135
Total order, 38
Transformation group, 101
Transitive, 25
Transitive action, 319
Transpositions, 181
Transvections, 202
Transversal to a subgroup, 155
Truth functional rules, 3

U

Uncountable, 50
Union, 17
Unipotent, 226
Unipotent subgroup, 227
Unique Factorization Domain (U.F.D), 406

Unit, 226
Unitary group, 215
Units and associates, 387
Universal quantifier, 7
Upper bound, 39
Upper central series, 366

V

von Dyck's Theorem, 380

W

Warning's theorem, 266
Well-order, 40
Well-ordering in \mathbb{N} , 60
Wielandt, 371
Wielandt theorem, 370
Wilson theorem, 110
Witt-Hall identities, 365
Word problem, 382
Words, 378

Z

Zassenhaus Lemma, 340
Zermelo's well-ordering principle, 41
Zero divisors, 224
Zero ring, 220
Zorn's Lemma, 41