Algebra/Group

March 1, 2019

Contents

1 Summary

When I am reading this book, I find it is so easy for me to forget the concepts that I was learn before. Because the amount of them are incredible. So, I record some important concepts and their definition here.

2 Logical Prerequisites

2.1 map

If $f : A \mapsto B$ is a mapping of one set into another, we write

$$x \mapsto f(x)$$

to denote the effect of f on an element x of A.

2.2 injective

We say that f is **injective** if $x \neq y$ implies $f(x) \neq f(y)$.

2.3 surjective

We say f is **surjective** if given $b \in B$ there exists $a \in A$ such that $f(a) = b$.

2.4 bijective

We say f is **bijective** if it is both surjective and injective.

2.5 restriction of map

We say the restriction of f to A' is a map of A' into B denoted by $f|A'$.

2.6 composite map

If $f : A \mapsto B$ and $g : B \mapsto C$ are maps, then we have a composite map $g \circ f$ such that $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

2.7 image of f

Let $f : A \mapsto B$ be a map, and B' a subset of B. By $f^{-1}(B')$ we mean the subset of A consisting of all $x \in A$ such that $f(x) \in B'$. We call it the **inverse image** of B'. We call $f(A)$ the image of f.

2.8 commutative

()

3 Monoids

3.1 law of composition

A mapping $S \times S \to S$ is sometimes called a **law of composition** (of S into itself).

3.2 associative

$(xy)z = x(yz)

3.3 unit element

$e \in S$, and $ex = x = xe$ for all $x \in S$. Then e is a unit element.

3.4 monoid

a **monoid** is a set G, with a law of composition which is associative, and having a unit element.

3.5 commutativity

$xy = yx$.

3.6 commutative (or abelian)

If the law of compositive of G is commutative, we also say that G is **commutative (or abelian)**.

3.7 almost all

All but a finite number.

3.8 submonoid

By a **submonoid** of G, we shall mean a subset H of G containing the unit element e, and such that, if $x, y \in H$ then $xy \in H$ (we say that H is **closed** under the law of composition). It is then clear that H is itself a monoid, under the law of composition indeuced by that of G.

4 Group

4.1 group

A **group** G is a monoid, such that for every element $x \in G$, there exists an element $y \in G$ such that $xy = yx = e$.

4.2 inverse

An **inverse** for x is an element $y \in G$ such that $xy = yx = e$. Sometimes y is denoted by x^{-1}.

4.3 direct product

$G_1 \times G_2 = \{(x, y) | \forall x \in G_1, \forall y \in G_2\}$

4.4 generators

Let G be a group and S a subset of G. We shall say that S **generates** G, or S is a set of *generators* for G, if every element of G can be expressed as a product of element in S or a inverse of element in S.

4.5 homomorphism

A (monoid/group)-**homomorphism** of G into G' is a mapping $f : G \mapsto G'$ such that $f(xy) = f(x)f(y)$.

4.6 isomorphism

A homomorphism $f : G \mapsto G'$ is called an **isomorphism** if there exists a homomorphism $g : G' \mapsto G$ such that $f \circ g$ and $g \circ f$ are the identity mappings. This is sometimes denoted by $G' \approx G$.

4.7 automorphism

A isomorphism from G to G.

4.8 endomorphism

A homomorphism from G to G.

4.9 power map

The map $x \mapsto x^n$ is called the n-th **power map**.

4.10 kernel

Let $f : G \mapsto G'$ be a group-homomorphism. We define the **kernel** of f to be the subset of G consisting of all x such that $f(x) = e'$.

4.11 embedding

A homomorphism $f : G \mapsto G'$ which establish an isomorphism between G and its image in G' will also be called an embedding.

4.12 left (right) coset

A **left coset** of H in G is a subset of G of type aH, for some element $a \in G$.

4.13 coset representative

An element of aH is called a **coset representative** of aH.

4.14 index

The number of (left) coset of H in G is called the (left) **index** of H in G, and is denoted by $(G : H)$. The index of the trivial subgroup $\{e\}$ is called the **order** of G ($(G : 1)$).

5 Normal Subgroups

5.1 normal subgroup

Let G be a group and H is a subgroup of G. If H satisfies $H \subset xHx^{-1}$ for all the $x \in G$. Then H is a normal subgroup of G.

5.2 canonical map

If H is a normal subgroup of G. Then, the constructed map $f : G \to G/H$ is called **canonical map**. And G/H is called the **factor group** of G by H. canonical map is often denoted by φ.

5.3 normalizer

Let S be a subset of G and let $N = N_s$ be the set of all elements $x \in G$ such that $xSx^{-1} = S$. Then N is called the **normalizer** of S.

5.4 centralizer

Let S be a subset of G. **Centralizer** C is the set of all the elements in G such that $\forall x \in S, \forall y \in C, yxy^{-1} = x$. The centralizer of G itself is called **center** of G.

5.5 tower

Let G be a group. A sequence of subgroups $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m$ is called a **tower** of subgroups.

5.6 normal tower

a tower is said to be normal if each G_{i+1} is normal in G_i.

5.7 abelian tower

a tower is said to be abelian if it is normal and if each factor group G_i/G_{i+1} is abelian.

5.8 cyclic tower

a tower is said to be cyclic if it is normal and if each factor group G_i/G_{i+1} is cyclic.

5.9 refinement of a tower

a refinement of a tower is a tower which can be obtained by inserting a finite number of subgroups in the given tower.

5.10 solvable group

a group is said to be solvable if it has abelian tower, whose last element is the trivial subgroup({e}).

5.11 commutator

a **commutator** in G is a group element os the form $xyx^{-1}y^{-1}$. with $x, y \in G$.

5.12 commutator subgroup

a commutator subgroup C^C of G is a subgroups generates by the commutators.

5.13 simple group

a group is said to be **simple** if it is non-trivial.

6 Cyclic Groups

6.1 cycilc group

Let G be a group. G is cyclic if there exists an element a of G such that every element x of G can be written in the form a^n for some $n \in Z$. a is called the generator of G.

6.2 exponent of an element

Let G be a group. For $a \in G$, if $a^m = e$, then we say m is a exponent of a. If all the elements in G has the exponent m, then we say that G as exponent m.

6.3 period of an element

d is the smallest positive exponent of a. Then d is called the period of a.

7 Operations Of A Group On A Set

7.1 operation/action of group G on set S.

An operation of G on S is a homomorphism:

$$\pi : G \to Perm(S)$$

. We then call S a \$G\$-set

7.2 conjugation

$G \to Aut(G)$ is called a conjugation. its kernel is called the **center** of G.

7.3 conjugate

A, B are two subsets of G. we say that they are **conjugate** if there exists $x \in G$ such that $B = xAx^{-1}$.

7.4 morphism of \$G\$-set / \$G\$-map

Let S, S' be two \$G\$-sets, and $f : S \to S'$ a map. We say that f is a **morphism** of \$G\$-sets, or a \$G\$-map if $f(xs) = xf(s)$ for $x \in G$ and $s \in S$.

7.5 iostropy

The set of elements $x \in G$ such that $xs = s$ is obviously a subgroup of G, called the *isotropy*. (denoted by G_s).

7.6 faithful / fixed point (P28)

7.7 orbit

Let G operate on a set S. Let $s \in S$. The subset of S consisting of all elements xs (with $x \in G$) is denoted by G_S, and is called the **orbit** of s under G.

7.8 transitive

an operation of G on S is said to be **transitive** if there is only one orbit.

8 Sylow Subgroups

8.1 p-group

a finite group whose order is a power of p.

8.2 p-subgroup

Let G be a finite group and H is a subgroup of it. we call h a p-subgroup os G if H is a p-group.

8.3 p-Sylow subgroup

We call H a p-Sylow subgroup if the order of H is p^n and if p^n is the hightest power of p deviding the order of G.

9 Direct Sums and Free Abelian Groups

9.1 direct sum

Let $\{a_i\}_{i \in i}$ be a family of abelian groups. we define their **direct sum**

$$A = \bigoplus_{i \in I} A_i$$

to be the subset of the direct product $\prod a_i$ consisting of all families $(x_i)_{i \in i}$ with $x_i \in a_i$ such that $x_i = 0$ for all but a finite nunber of indices i.

9.2 basis

Let A be an abelian group. Let $\{e_i\}(i \in I)$ be a family of elements of A. We say that this family is a **basis** for A if the family and if every element of A has a unique expression as a linear combination

$$x = \sum x_i e_i$$

with $x_i \in Z$ and almost all $x_i = 0$.

9.3 free abelian group

An abelian group is said to be **free** if it has a basis.

9.4 free abelian group generated by S

We shall denote $Z\langle S \rangle$ also by $F_{ab}(S)$, and call $F_{ab}(S)$ the **free abelian group generated by** S. we call elements of S its **free generators**.