Introduction to Group Theory - Notes

Dom Hutchinson

March 20, 2018

Contents

1 Symmetries

Definition 1.01 - *Permutation*
A *permutation* of a set, G, is a bijection $f : G \to G$.
N.B. - Since the composition of two bijections is also a bijection, then the composition of two permutations is a permutation.

Definition 1.02 - *Symmetries of a Polygon*
A *symmetry* of an n-sided polygon is a permutation of the vertices which preserves adjacency. So if the vertices, u, v, are adjacent then the permutation f is a symmetry if $f(u)$ & $f(v)$ are adjacent.

Remark 1.03 - *Symmetries*
When dealing with symmetries of a shape then they can only be rotations or reflections.

Definition 1.04 - *Identity*
The trivial symmetry, which maps an element to itself, is known as the identity.

Remark 1.05 - *Multiple Composition*
Let R, S & T be permutations. Then $(RS)T$ means do T, then S, then R. So

$$(RS)T = R(ST)$$

Remark 1.06 - *One-Line Notation*
Let $S = \{a_1, \dots, a_n\}$ be a set and $\sigma : S \to S$ be a permutation.
One-Line notation denotes the result of σ by

$$\begin{pmatrix} \sigma(a_1) & \dots & \sigma(a_n) \end{pmatrix}$$

So if σ maps $1 \to 2, 2 \to 3, \dots, n \to 1$ then it can be denoted by

$$\begin{pmatrix} 2 & 3 & \dots & n & 1 \end{pmatrix}$$

Remark 1.07 - *Two-Line Notation*
Let $S = \{a_1, \dots, a_n\}$ be a set and $\sigma : S \to S$ be a permutation.
Two-Line notation denotes the result of σ by

$$\begin{pmatrix} a_1 & \dots & a_n \\ \sigma(a_1) & \dots & \sigma(a_n) \end{pmatrix}$$

So if σ maps $1 \to 2, 2 \to 3, \dots, n \to 1$ then it can be denoted by

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$$

Remark 1.08 - *Cycle Decomposition Notation*
Let $S = \{a_1, \dots, a_n\}$ be a set and $\sigma : S \to S$ be a permutation.
Cycle Decomposition Notation denotes σ as the product of disjoint cycles.
Each element in a cycle goes the position of the element after it in the list, the last element goes to the position of the first.
$()$ denotes no variation. The operation of σ is denoted by

$$\begin{pmatrix} a_1 & \sigma(a_1) & \sigma(\sigma(a_1)) & \dots & \sigma(\dots\sigma(a_1)\dots) \end{pmatrix}$$

2 Groups

Definition 2.01 - *Binary Operation*
A *binary operation* on a set X is a fuction from $X \times X \to X$.

Remark 2.02 - *Asteriks Notation*
Binary operations are general denoted by an $*$.

$$f(x, y) = x * y$$

Remark 2.03 - *Set of Permutations*
A set of permutations have a binary operation for composition.
Let f, g, h be permutations of a set X and $x \in X$

$$f(x) \times g(x) \to h(x)$$

Definition 2.04 - *Commutative*
A binary operation, $*$, on a set X is commutative if order of input doesn't affected the outcome.

$$x * y = y * x, \forall\ x, y \in X$$

Defintion 2.05 - *Group*
A group is a set, G, with an associated binary operation, $*$, such that

i) It is *associative*, $(x * y) * z = x * (y * z)\ \forall\ x, y, z \in G$;

ii) It as an *identity element*, $\exists\ e \in G$ such that $x * e = x = e * x$;

iii) For all $x \in G\ \exists\ x^{-1} \in G$ st $xx^{-1} = e = x^{-1}x$.

Remark 2.06 - *Group Notation*
The group of set G and binary operation $*$ is denoted by $(G, *)$.

Definition 2.07 - *Abelian Group*
An *Abelian group*, $(G, *)$ is one where $*$ is commutative.

Definition 2.08 - *Commute*
If $x, y \in G$ satisfy $x * y = y * x$ then it is said that x & y commute.

Remark 2.08 - *Multiplicty Notation*
Multiplicity notation is used to simplify equations with a single binary operator, by not writting $*$.

$$x * y = xy$$

3 Elementary Consequences of the Definition

Proposition 3.1 - *Right Cancellation*
If $a, b, x \in G$ and

$$ax = bx => a = b$$

Proposition 3.2 - *Left Cancellation*
If $a, b, x \in G$ and

$$xa = xb => a = b$$

Proposition 3.3 - *Uniqueness of Identity*
If $a, x, e \in G$ with e as the identity of G then

$$ax = a => e = x$$

Proposition 3.4 - *Uniqueness of Inverses*
If $x, y, e \in G$ with e as the identity of G then

$$xy = e => x = y^{-1} \;\&\; y = x^{-1}$$

Proposition 3.5 - *Inverse of Inverse*
Let $x \in G$ then

$$(x^{-1})^{-1} = x$$

Proposition 3.6 - *Composite Inverses*
Let $x, y \in G$ then

$$(xy)^{-1} = y^{-1}x^{-1}$$

Definition 3.7 - *Caley Table*
Let e, x, y be all the elements of G then the result of all compositions can be displayed in a Caley Table.

	e	x	y
e	e	x	y
x	x	xx	yx
y	y	xy	yy

The operation of the column is done first, then the operation of the row.
N.B. - All values in any given column or row are unique, so all elements of G appear exactly once.

Definition 3.8 - *Powers of Elements*
If $n > 0$ then x^n means $x * \cdots * x$ n times.

$$x^{-n} = (x^n)^{-1} = (x^{-1})^n, \quad x^0 = e$$

Definition 3.9 - *Composition of Powers*
For $m, n \in \mathbb{Z}$

$$x^m x^n = x^{m+n}$$

4 Dihedral Groups

Definition 4.01 - *Order*
The *order* of a group G is the number of elements in G.
N.B. - Order of G is denoted by $|G|$.

Definition 4.02 - *Dihedral Groups*
The dihedral group D_{2n} is the group of symmetries of a regular n-sided polygon, with $n \geq 3$.
N.B. - $|D_{2n}| = 2n$.

Proposition 4.03 - *Elements of Dihedral Group*
Let a describe a rotation by $\frac{2\pi}{n}$ and b a reflection thenAn External

$$D_{2n} = \{e, a, a^2, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b\}$$

N.B. - $a^n = e = b^2, \quad a^{-1} = a^{n-1}, b = b^{-1}$.

Proposition 4.04 - *Reflections & Rotations*
Let a denote a rotation and b denoted a reflection then

$$ab = ba^{-1}$$

5 Subgroups

Definition 5.01 - *Subgroup*
A subgroup of a group G is a group formed of a subset of G with the same associated operation.
N.B. - H being a subgroup of G is denoted by $H \leq G$.

Definition 5.02 - *Non-Trivial Subgroup*
A subgroup H of G is non-trivial if $H \neq \{e\}$.

Definition 5.03 - *Proper Subgroup*
A subgroup H of G is a proper subgroup if $H \neq G$.

Theorem 5.04 - *Subgroup*
A subset H of a group G is a subgroup iff

i) It is closed under binary operation $x, y \in H => xy \in H$;

ii) It has an identity element $\exists\ e \in H$ st $xe = x\ \forall\ x \in H$;

iii) All elements have an inverse $\forall\ x \in H\ \exists\ x^{-1} \in H$ st $xx^{-1} = e$.

Proposition 5.05 - *Pairs of Subgroups*
Let G, H, K be groups with $H \leq G$ & $K \leq G$ then $H \cap K \leq G$.

6 Order of Elements

Definition 6.01 - *Order of an Element*
Let $x \in G$ such that $x^n = e$, then the order of x is the smallest such n.

$$ord(x) = n$$

N.B. - If there is no such n then $ord(x) = \infty$.

Proposition 6.02 - *Uniqueness of Powers*
Let $x \in G$ with $ord(x) = \infty$ then

$$x^i \neq x^j\ \forall\ i \neq j$$

Theorem 6.03 - *Order Elements in a Finite Group*
Every element of a finite group has finite order.

Theorem 6.04 - *Properties of Order of an Element*
Let $x \in G$ such that $ord(x) = n < \infty$ then if

i) $x^i = e \iff n|i$;

ii) $x^i = x^j \iff i \equiv j(modn)$;

iii) $x^{-1} = x^{n-1}$;

iv) The powers of x less than n are all distinct.

Proposition 6.05 - *Order of Powers of Elements*
let $x \in G, i \in \mathbb{Z}$.

i) If $ord(x) = \infty$ then $ord(x^i) = \infty$ if $i \neq 0$;

ii) If $ord(x) = n < \infty$ then $ord(x^i) = \dfrac{n}{gcd(n,i)}$.

7 Cyclic Groups & Cyclic Subgroups

Definition 7.01 - *Generating Cyclic Groups*
Let G be a group and $x \in G$.
We define a cyclic group generated by x

$$\langle x \rangle = \{x^i : i \in \mathbb{Z}\} \leq G$$

.
Theorem 7.02 - *Cyclic Subgroup*
Let $x \in G$ then $\langle x \rangle$ is a subgroup of G.

Definition 7.03 - *Cyclic Group*
A group G is cyclic if $G = \langle x \rangle$ for some $x \in G$.
N.B. - Here x is called the generator of G.

Theorem 7.04 - *Abelian Cyclic Groups*
Every cyclic group is abelian.

Theorem 7.05 - *Finding Cyclic Groups*
Let G be a group with $|G| = n < \infty$.
G is cyclic iff $\exists\ x \in G$ such that $ord(x) = n$.

Theorem 7.06 - *Subgroups of Cyclic Groups*
Every subgroup of a cyclic group is also a cyclic group.

8 Groups from Modular Arithmetic

Definition 8.01 - *Congruence Class*
Let $n \in \mathbb{N}$ then $a \equiv b(mod\ n)$ means $n|a-b$.
There are n *congruence classes* $[0], [1], \dots, [n-1]$ where every integer is in exactly one of these classes.

$$[x] = \{y \in \mathbb{Z} : x \equiv y(mod\ n) = \{\dots, a-n, a, a+n, a+2n, \dots\}$$

Definition 8.02 - *Congruence groups*
Let $n \in \mathbb{N}$ then we denoted a congruence group of n by

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = [0], [1], \dots, [n-2], [n-1]$$

N.B - Addition and multiplication are valid binary operations for congruence groups.

Definition 8.03 - *Properties of Congruence Groups*
Let $[a], [b] \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ for some $n \in \mathbb{N}$ then

$$[a] + [b] = [a+b], [a].[b] = [a.b]$$

Theorem 8.04 - *Abelian Congurence Groups*
Let $n \in \mathbb{N}$ then $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is an abelian group.

Theorem 8.05 - *Cyclic Abelian Congurence Groups*
The group $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right) = \langle [1] \rangle$, so it is a cyclic group.
The group $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \cdot\right)$ is never a group for $n > 1$ as $[0][x] = [0] \neq [1] = e$.