Abstract Notes

James McFeeters

March 11, 2017

1 Basic Group Properties

1.1 Definition of a Group

Binary relation: If G is a set, $*$ is a binary relation on G if $a * b \in G$ for all $a, b \in G$.

Group Let G be a set. G is a group if there exists a binary relation on G that satisfies the following properties for all $a, b, c \in G$:

1. $a(bc) = (ab)c$ (associative)
2. There exists an identity element $e \in G$.
3. Every element has an inverse

Identity: An element e is an identity of G if $ae = ae = a$ for all $a \in G$.

Inverse: Let G be a group and let $a \in G$. By the inverse of a we mean an element $b \in G$ such that $ab = ba = e$.

Abelian group: If $ab = ba$ for all $a, b \in G$, then the group is called abelian. (Abelian groups are those for which the commutative property holds.)

Order: The order of G, denoted $|G|$, refers to the number of elements in G.
The order of an element a, denoted $|a|$, is the smallest positive integer n such that $a^n = e$.

Cyclic groups: A cyclic group is one which can be generated by just one element of the group using the operation of the group. The group generated by an element a is denoted $\langle a \rangle$

1.2 Basic Theorems / Properties

Prop. 1: The identity is unique.

Prop. 2: Suppose $a, b, x \in G$ where G is a group. If $ax = bx$ then $a = b$, and if $xa = xb$ then $a = b$. (The right and left cancellation laws hold.)

Prop. 3: The inverse of any element $a \in G$ is unique.

Socks-shoes property: For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$. Because you put on your socks, then your shoes: ab. Then to reverse the operation, you take off your shoes, then your socks: $b^{-1}a^{-1}$

2 (.*)morphisms

2.1 Definitions

Isomorphism: G and $\bar{G}$ are said to be isomorphic if there exists a one-to-one and onto function $\phi : G \mapsto \bar{G}$ such that $\phi(ab) = \phi(a)\phi(b)$.

Automorphism: An isomorphism $\phi : G \mapsto G$ is called an automorphism of G.

2.2 Theorems

Proposition: Suppose $\phi : G \mapsto \bar{G}$ is an isomorphism. Then:

1. $\phi(e) = \bar{e}$
2. $\phi(a^{-1}) = (\phi(a))^{-1}$
3. $\phi(a^s) = (\phi(a))^s$ for any integer s.

In re 3: We write a^{-k} where k is a positive integer to denote $\underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{k \text{ times}}$

3 Groups and Subgroups

3.1 Definitions

Subgroup: Let G be a group. If a subset H of G is a group under the operation of G, then H is a subgroup of G.
Let H be a subgroup of G. If $H \neq G$ and $H \neq \{e\}$, then H is called a *proper subgroup* of G.

3.2 Theorems

Any subgroup of a cyclic group is itself cyclic.

4 Cosets:

4.1 Definition

Left and right cosets: Let G be a group and let H be a subgroup of G. We define left and right cosets of H in G as follows:
Let $a \in G$, then

$$\text{the set } \; aH = \{ah \mid h \in H\} \; \text{ is called a left coset of } H \text{ in } G$$

and

$$\text{the set } \; Ha = \{ha \mid h \in H\} \; \text{ is called a right coset of } H \text{ in } G$$

The element a is called the coset representative of aH or Ha

Index: The index of a subgroup H in G id the number of distinct left cosets of H in G, denoted $|G : H|$

4.2 Theorems and Properties

1. $a \in aH$
2. $aH = H \iff a \in H$
3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$
4. $aH = bH \iff a \in bH$
5. $aH = bH$ or $aH \cap bH = \varnothing$

6. $aH = bH \iff a^{-1}b \in H$

7. $|aH| = |bH| = |H|$

8. $aH = Ha \iff H = aHa^{-1}$

9. aH is a subgroup of $G \iff a \in H$

Lagrange's Theorem: If H is a subgroup of a finite group G, then $|H| \mid |G|$.
Also, the number of distinct left/right cosets of H in G is $\frac{|G|}{|H|}$

Corollaries:

1. $|G : H| = \frac{|G|}{|H|}$

2. $|a| \mid |G|$ for all $a \in G$

3. Groups of prime order are cyclic.

4. $a^{|G|} = e$ (since the order of the group must be a multiple of the order of the element)

Theorem: Suppose G is a group and H and K are subgroups of G.
$|HK| = \dfrac{|H||K|}{|H \cap K|}$
Where $HK = \{hk \mid h \in H \text{ and } k \in K\}$

5 Disorganized Notes

Lagrange's Theorem: If H is a subgroup of a finite group G, then $|H| \mid |G|$.

5.0.1 Order of an Element

The order of an element a, denoted $|a|$, is the smallest positive integer n such that $a^n = e$.

$\langle a \rangle$ = the group generated by a.

Prop. 1: If $a\ inG$, then $|a| \mid |G|$

Prop. 2: Take $\mathbb{Z}_p^*$ where p is prime. Then $|\mathbb{Z}_p^*| = p - 1$

5.0.2 Stabilizer

The stabilizer of i in G is the set of elements of G that fix i.
Denoted $\mathrm{stab}_G(i)d$.

Prop: $\mathrm{stab}_G(i)$ is a subgroup of G.

5.0.3 Orbit

The orbit of i in G is the set of all $g(i)$ where $g \in G$. Denoted $\mathrm{orb}_G(i)$

Theorem: $|G| = |\mathrm{stab}_G(i)||\mathrm{orb}_G(i)|$

5.0.4 Normal Subgroup

Let G be a group. A subgroup N is called a normal subgroup of G if $gN = Ng$ for all $g \in G$. This does not mean that $gn = ng$ for all $n \in N$. It does mean that $gn = n_1 g$ for some $n_1 \in N$.

5.0.5 Index of a Subgroup

Let H be a subgroup of G. Then the index of H in G is the number of distinct left (or right) cosets of H in G.
index $= \frac{|G|}{|H|}$

5.0.6 External Direct Product

Let G_1 and G_2 be two groups. The external direct product is defined as $G_1 \oplus G_2 = \{(x, y)|x \in G_1, y \in G_2\}$.
And the product is defined by $(x, y)(x_1, y_1) = (xx_1, yy_1)$.
Observe that if G_1 and G_2 are abelian, then $G_1 \oplus G_2$ is abelian.

5.0.7 Internal Direct Product

Suppose H and K are normal subgroups of G. G is called the internal direct product of H and K if $G = HK$ and $H \cap K = \{e\}$

Theorem: Let G be an abelian group of order n. Suppose p is a prime and $p|n$. Then there exists an element $g \in G$ that is of order p.

5.0.8 Center of G:

$Z(G) = \{g \in G|gh = hg \text{ for all } h \in G\}$

Prop: $Z(G)$ is a normal subgroup of G.

Theorem: $Z(G)$ is a normal subgroup of G.

5.0.9 Homeomorphism

A homeomorphism is a mapping

$$\begin{aligned} \phi : & G \mapsto G' \\ & e \mapsto e' \end{aligned}$$

if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$

5.0.10 Kernel

The kernel of ϕ is the set of all elements in G that are mapped to e'. Denoted $\ker \phi = \{g \mid g \in G, \phi(g) = e'\}$

Prop: $\ker \phi$ is a normal subgroup of G.

Theorem: Suppose $\phi : G \mapsto G'$ is an onto homeomorphism. Then $G/\ker\phi$