STUDY GUIDE: ABSTRACT ALGEBRA

PHIL MAYER

1. Groups

Definition 1.1. $*$ is a **binary operation** if and only if $* : S \times S \to S$ is one-to-one and onto.

Definition 1.2. $(G, *)$ is a **group** if and only if $*$ is associative, has an identity in the set G, each $g \in G$ has an inverse in G, and G is closed under the operation.

Definition 1.3. A group G is **abelian** (or commutative) if and only if $\forall a, b \in G$, $ab = ba$.

Groups have the following properties:

(1) Cancellation law: $\forall a, b, c \in G, ab = ac \implies b = c$.

(2) Solution uniqueness: "linear" equations of the form $ax = b$ have a unique solution in G.

(3) Uniqueness of identity: $e \in G$ is the only valid identity.

(4) Uniqueness of inverses: each $a \in G$ has a unique inverse $a^{-1} \in G$.

(5) Inverse of a product: $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

2. Subgroups and Cyclic Groups

Definition 2.1. $H \subset G$ is a **subgroup** of G if and only if H is closed under G's binary operation, is associative, its identity is in H, and for each $h \in H$, $h^{-1} \in H$. We denote H as a subgroup of G by $H \leq G$.

Definition 2.2. G is said to be a **cyclic group** generated by $a \in G$ if and only if $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Theorem 2.3. *Any subgroup of a cyclic group is cyclic. This is a general statement that is difficult to prove, so below we will show that any subgroup of* $(\mathbb{Z}, +)$ *is cyclic.*

Proof. Suppose $H \leq G$ on addition.
Case: if $H = \{0\}$, then 0 generates H, so H is trivially cyclic.
Case: if $H \neq \{0\}$, then we want to show $\exists d \in H$ such that $\langle d \rangle = H$.

Since $H \neq \{0\}$, H contains a least positive integer d since all non-empty subsets of $\mathbb{Z}$ have a least element.
By closure of H, $\langle d \rangle \subset H$. Now we need to show $H \subset \langle d \rangle$.
So let $h \in H$. We want $h = cd$ for some $c \in \mathbb{Z}$.
Divide h by d: then we have a quotient q and remainder r such that $h = dq + r$ with $0 \leq r < d$.
Observe $r \in H$ since $r = h - dq$ and $h, dq \in H$ by closure.
But since d is the smallest integer in H and $r < d$, $r = 0$.
So $h = dq \implies h \in \langle d \rangle$.
Then $H \subset \langle d \rangle$, so $H = \langle d \rangle$.
$\therefore$ H is cyclic. □

Theorem 2.4. *There is exactly one cyclic subgroup of $\mathbb{Z}_n$ for each divisor d of n, generated by $\frac{n}{d}$.*

Theorem 2.5. *Some element $l \in \mathbb{Z}$ is a generator for $\mathbb{Z}_n$ if and only if* $\gcd(\{l, n\}) = 1$.

Theorem 2.6. *Integers $l, k \in \mathbb{Z}$ generate the same subgroup of $\mathbb{Z}_n$ if and only if* $\gcd(\{l, n\}) = \gcd(\{k, n\})$.

Theorem 2.7. *Let $p \in \mathbb{P}$, the prime numbers. Then $\mathbb{Z}_p$ has $p - 1$ generators and two distinct subgroups: $\{0\}$ and $\mathbb{Z}_p$.*

Theorem 2.8. *Let G be a cyclic group generated by a. If the order of G is infinite, then $G \cong (\mathbb{Z}, +)$. If G is finite with order n, then $G \cong (\mathbb{Z}_n, +)$.*

3. Permutation Groups

Definition 3.1. A **permutation** is a one-to-one, onto function that rearranges a set. Composition of functions is well-known to be associative, have an identity, have inverses, and be closed.

Theorem 3.2. *Let $A \neq \varnothing$ and call S_A the collection of all permutations on a set A. Then S_A is a group under function composition.*

Theorem 3.3. *If $n \geq 2$, then the collection of all even permutations of $\{1, \dots, n\}$ forms a subgroup A_n of the symmetric group S_n of order $\frac{n!}{2}$.*

Proof. It can be shown that A_n is closed, has identity $e = (1,2)(1,2)$, and all inverses have an even number of elements.
To show $|A_n| = \frac{n!}{2}$, we need to show $|A_n| = |B_n|$ by constructing a one-to-one, onto function between them.
So let $f : A_n \to B_n$ by $f(\sigma) = \sigma(1,2)$. Then show one-to-one and onto. □

Theorem 3.4. *No permutation in S_n can be expressed as both a product of an even and an odd number of transpositions.*

4. Cosets

Definition 4.1. Let $a \in G$ and suppose $H \leq G$. Then the **left coset** of H in G is the set $aH = \{ah \mid h \in H\}$.

Cosets have the following key properties:

(1) $|aH| = |bH|$ for all cosets aH, bH of H. Can be proven by constructing a one-to-one and onto function between.

(2) $aH = bH$ or $aH \cap bH = \varnothing$.

(3) H is always a trivial coset of itself.

Theorem 4.2 (The Theorem of LaGrange)**.** *Suppose G is a finite group and $H \leq G$. Then $|H|$ divides $|G|$.*

Proof. Let G be a finite group and suppose H is a subgroup of G.
Now decompose G into a union of its left cosets. Assume there are r. Then we have:

$$G = \bigcup_{i=1}^{r} a_i H$$

Expanded out, $|G| = |a_1 H \cup a_2 H \cup \cdots \cup a_r H|$.
Now recall that for two general sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$.
But since $a_i H \cap a_j H = \varnothing \ \forall i \neq j$, $|G| = |a_1 H| + |a_2 H| + \cdots + |a_r H|$.
Then since all cosets have the same order, $|G| = r|H|$.
$\therefore$ $|H|$ divides $|G|$. □

Definition 4.3. The **index** of H in G, $[G : H]$, is the number of distinct costs of H in G.

Corollary 4.4 (The Theorem of LaGrange)**.** $\frac{|G|}{|H|} = [G : H]$

5. Homomorphisms and Isomorphisms

Definition 5.1. The function $\phi : G \to G'$ is a **homomorphism** from G to G' if and only if $\phi(ab) = \phi(a)\phi(b) \ \forall a, b \in G$.

Definition 5.2. $\phi : G \to G'$ is an **isomorphism** from G to G' if and only if ϕ is a one-to-one, onto homomorphism.

Recall that ϕ is one-to-one if and only if $\forall x_1, x_2 \in G$ where $\phi(x_1) = \phi(x_2)$, we have $x_1 = x_2$.
ϕ is onto if and only if $\forall g' \in G'$, $\exists g \in G$ such that $g' = \phi(g)$.

Theorem 5.3. *Assume $f : G \to G'$ is a homomorphism. Then:*

(1) $f(e) = e'$

(2) $f(a^{-1}) = f(a)^{-1}$

(3) *If* $H \leq G$*, then* $f(H) \leq G'$

(4) *If* $K \leq G'$*, then* $f^{-1}(K) \leq G$

Definition 5.4. Let $f : G \to G'$ be a homomorphism. Then the **kernel** of f, $\ker(f)$, is the set of elements of G which are sent to the identity in G'. So $\ker(f) = \{a \in G \mid; f(a) = e'\}$.

Theorem 5.5. $\ker(f) \leq G$ *and* $\frac{|G|}{|\ker(f)|} = |$*image of* G *under* $f|$

6. Factor Groups

Definition 6.1. $H \leq G$ is **normal**, denoted $H \lhd G$, if and only if $aH = Ha\ \forall a \in G$, or equivalently, $a^{-1}h_1a = h_2$ for $h_1, h_2 \in H$.

Theorem 6.2. $H \lhd G$ *if and only if* $[G : H] = 2$*.*

Theorem 6.3. *Let* $H \leq G$*. Then the left coset multiplication* $(aH)(bH) = (ab)H$ *is well-defined if and only if* $H \lhd G$*. The cosets form a group under multiplication:* G/H*.*

Theorem 6.4 (The Fundamental Theorem of Homomorphisms)**.** *The theorem relates factor groups, normal subgroups, and kernels of homomorphisms in three parts:*

(1) *If* $f : G \to G'$ *is an onto homomorphism, then* $\ker(f) \lhd G$ *and* $G/\ker(f)$ *is a group.*

(2) *If* $H \lhd G$ *and* $f : G \to G/H$ *by* $f(g) = gH$*, then* f *is a homomorphism.*

(3) *If* $f : G \to G'$ *is an onto homomorphism, then* $G/\ker(f) \cong G'$*.*