Math Class: Review Notes

Spencer Martz

October 2, 2024

1 Basics of Groups

A group is a set G, closed under a binary operation * that satisfies the following properties:

G1 : Associativity: $a * (b * c) = (a * b) * c$

G2 : Identity: $\exists e \in G$ s.t. $\forall a \in G,\ a * e = e * a = a$

G3 : Inverse: $\forall a \in G,\ \exists a'$ s.t. $a * a' = a' * a = e$

The set and operation that form a group can be denoted explicitly by $< G, * >$, but often just G is used. A group is said to be "Abelian", named after Neils Henrik Abel, if it's operation is commutative.

1.1 Basic Results

a. Function composition, multiplication, addition are associative. Multiplication and addition are also commutative.

b. The identity element of a group is unique. The inverse of an element is also unique.

c. $(a * b)' = b' * a'$

2 Definitions, Notations, and First Concepts

- A subgroup of a group $< G, * >$ is a subset $H \subseteq G$, which also forms a group $< H, * >$. This is denoted by $H \leq G$.

  One need only show that this subgroup contains the identity, and is closed under the operation as well as inverses. It inherits the associativity propery from it's superset group. Every group is a subgroup of itself. If the subgroup is not equal to the whole group, it is called a proper subgroup. Every group has the "trivial subgroup", $\{e\}$.

- A group is finite if it's underlying set is finite. A group is finitely generated if there is a finite set of elements which can generate it. (Here, generate means to use the group operation on the generating elements, in all possible combinations). All finite groups are finitely generated.

- A homomorphism is a function $\phi G \to G'$, where G and G' are groups, and the following property holds:
$$\forall a, b \in G, \quad \phi(a \cdot b) = \phi(a) \cdot' \phi(b) \tag{1}$$

- An isomorphism is a bijective homomorphism. We say two groups are isomorphic (and consider them "essentially the same") if there is an isomorphism between them.

- We denote the image of a function on a set S by f(S).

- The kernel of a function $\phi : G \to G'$, denoted $\ker(\phi)$, is the set of all elements which map to the identity under phi: $\{a \in G | \phi(a) = e'\}$

  The kernel of a function is similar to the null space of a linear function, particularly for homomorphic ones, but it is not the same.

- If $< G, * >, < H, \cdot >$ are groups, the direct product of G and H, $G \times H$, is the cartesian product of G and H with the operation $(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$. This product is commutative and associative upto isomorphism.

3 Examples of Abelian groups

3.1 Standard examples:

- The most standard group is $\mathbb{Z}$ under addition. $\mathbb{Q}$ is also a group under addition, as are $\mathbb{R}$ and $\mathbb{C}$, but not $\mathbb{N}$. However, none of these are groups under multiplication as they fail the inverse condition.
- The set of all n by m matrices is a group under addition.

3.2 Other, less standard examples

a. $U_n = \{z \in C : z^n = 1\}$, forms a group under multiplication, called the nth roots of unity.

b. $U = \{z \in C : |z| = 1\}$, the circle group, is also a group under multiplication.

4 Examples of Non-Abelian Groups

4.1 The dihedral group, D_n

The dihedral group is the set of symmetry preserving transformations (specifically, rotation and reflection) on a regular n-gon. Usually,ρ denotes a rotation by $2pi/n$ radians, and μ represents a reflection about a line of symmetry. It's order is 2n, since n unique orientations arise from rotation, each of which produce another unique orientation under reflection.

4.2 The Symmetric and Alternating Groups: S_n, A_n

- Under the operation of composition, the permutations on n objects form a group, denoted S_n and called the symmetric group. In general, permutation composition is not commutative. Thus S_n is not Abelian. Note that $|S_n| = n!$.
- There is also $A_n = \{\sigma \in S_n \text{ s.t. } sgn(\sigma) = 1\}$, called the alternating group. We have $|A_n| = |S_n|/2$.

5 Cyclic Groups

A group G is said to be cyclic if it is generated by one element a, called a generator., In other words, each element of G may be created by repeatedly "cycling" a, that is, applying the group operation:

$$G =< a >= \{a, a * a, a * a * a, \dots\} \tag{2}$$

In light of this definition, we define the order of an element of G, $|a| = | < a > |$ to be the size of the cyclic (sub)group generated by a. The order of some element $b = a^s \in G$ where $|G| = n$ is $|b| = \frac{n}{d}$, $d = (n, s)$ The fundamental example of a cyclic group is Z, generated by 1.

5.1 Properties of cyclic groups

- All cyclic groups are Abelian.
- Any subgroup of a cyclic group is cyclic.
- Any cyclic group is isomorphic to some $< Z, + >$ or $< Z_n, +_n >$.

5.2 Properties of finite cyclic groups

- $< a^r >$ is isomorphic to $< a > \iff (r, |a|) = 1$
- If $H \leq G$, $|H|$ divides $|G|$
- $Z_m \times Z_n \cong Z_{mn} \iff (m, n) = 1$

  In other words, $Z_n \times Z_m$ is NOT cyclic if $(m, n) \neq 1$.

  We also have: $|(a_1, a_2)| = lcm(|a_1|, |a_2|)$

5.3 Fundamental Theorem of Finitely Generated Abelian Groups

A finitely generated Abelian group G is isomorphic to some direct product of the form:

$$Z_{p_1^{r_1}} \times Z_{p_2^{r_2}} \times \dots Z_{p_n^{r_n}} \times Z \times Z \cdots \times Z \tag{3}$$

where the p_i are primes, not necessarily distinct. The number of Z terms in this product is called the Betti number of G. Any finite group has a Betti number of 0.

6 Properties of Homomorphisms

Let $\phi : G \to G'$ be a homomorphism. Then:

a. $\phi(e) = e'$

b. $\phi(a') = \phi(a)'$

c. If $H \leq G$, $\phi(H) \leq G'$

d. If $H' \leq G'$, $\phi^{-1}(H') \subset G$

e. $\ker(\phi) \triangleleft G$

6.1 Fundamental Theorem of Homomorphisms (or Isomorphism theorem I).

Let G, H be groups, and $\phi : G \to H$ a homomorphism. Let N be a normal subgroup of G, and define $\mu : G \to G/N,\ \mu(g) = gN$. Then if $N \subseteq \ker(\phi)$, there is a unique homomorphism $\gamma : G/N \to H$ that satifies $\phi = \mu \circ \gamma$.

7 Subgroups and Cosets

For a group G and subgroup H, the left coset aH is the set $\{ah : h \in H\}$ and the right coset defined similarly. A subgroup is said to be normal, denoted $H \trianglelefteq G$ if it's left and right cosets and equal. The order of this set is called the index of H in G, and is denoted $(G : H)$. If H is normal, we denote the set of cosets by G/H, called the quotient group of H.

7.1 Lagrange's Theorem

Let $H \leq G, |G| \neq \infty$, then $|G| = (G : H)|H|$.