

MATH 30A: SUMMARY OF CHAPTERS 3,4,5

3. SUBGROUPS

Definition 3.1. A subgroup of a group G is a subset H which is itself a group under the same operation. This means:

- (1) $e \in H$
- (2) If $h \in H$ then $h^{-1} \in H$ (H is closed under taking inverses.)
- (3) If $h_1, h_2 \in H$ then $h_1 h_2 \in H$ (H is closed under multiplication.)

Theorem 3.2. A subset H of a group G is a subgroup iff it is nonempty and contains gh^{-1} for all $g, h \in H$.

Theorem 3.3. A nonempty subset of a finite group is a subgroup iff it is closed under the operation.

3.1. examples of subgroups. If $g \in G$ then the *centralizer* $C(g)$ of g is a subgroup of G . This is defined to be the set of all elements of G which commute with g :

$$C(g) = \{h \in G \mid gh = hg\}$$

The *center* $Z(G)$ of G is a subgroup. This is defined to be the set of all elements of the group which commute with every other element:

$$Z(G) = \{g \in G \mid gh = hg \forall h \in G\}$$

For example, the center of $GL(2, \mathbb{R})$ consists of the scalar multiples of the identity matrix:

$$Z(GL(2, \mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \neq 0 \right\}$$

3.2. cyclic subgroups. For any $g \in G$ the cyclic subgroup of G generated by g is the set of all integer powers of g :

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

In an additive group this is the set of all integer multiples of g :

$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$$

The *order* of g is the smallest positive integer n so that $g^n = e$. This is written $n = |g|$ or $n = o(g)$. This is also the order of the subgroup generated by g :

$$|g| = |\langle g \rangle|$$

4. CYCLIC GROUPS

A *cyclic group* is a group which is generated by one element:

$$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

The order of a cyclic group is equal to the order of the generator:

$$|G| = |g| = n$$

Here is the key theorem:

Theorem 4.1. $g^k = e$ iff k is a multiple of the order of g .

Proof. $k = qn + r$ where $0 \leq r < n$ is the remainder when k is divided by n . Then

$$g^k = g^{qn+r} = g^{nq}g^r = e^qg^r = g^r$$

This cannot be equal to e unless $r = 0$ since g^n is the smallest positive power of g equal to e . \square

Two powers of the generator are equal iff the difference of the powers is divisible by this order n .

$$g^i = g^j \iff i \equiv j \pmod{n}$$

An element g^k of $G = \langle g \rangle$ is a generator iff k is relatively prime to the order.

The order of g^k is equal to n/d where $d = \gcd(n, k)$. In particular, $|g^k| = n/d$ divides $|g| = n$.

Theorem 4.2. Every subgroup H of a cyclic group $G = \langle g \rangle$ is cyclic and the order of H divides the order of G .

Proof. H is a cyclic subgroup generated by g^k where k is the smallest positive integer so that $g^k \in H$. Then all the other elements of H must be powers of g^k and the order of H is given by

$$|H| = |g^k| = \frac{n}{d}$$

which divides $n = |g| = |G|$. \square

5. PERMUTATION GROUPS

Definition 5.1. If X is any set then the set of all bijections $\phi : X \rightarrow X$ forms a groups under composition of functions. This group is call the (full) permutation group of X . It is also called the symmetry group of X . I call it $\text{Perm}(X)$.

Definition 5.2. The symmetric group S_n is the group of permutations of the n "letters" $1, 2, \dots, n$.

Theorem 5.3. S_n has $n!$ elements.

array notation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

means $\sigma(1) = 3, \sigma(2) = 5, \sigma(3) = 1, \sigma(4) = 2, \sigma(5) = 4$. Nobody uses this notation.

cycle notation

$$\sigma = (13)(254)$$

means $\sigma(1) = 3, \sigma(3) = 1, \sigma(2) = 5, \sigma(5) = 4, \sigma(4) = 2$. $\alpha = (13)$ and $\beta = (254)$ are cycles. They are *disjoint* since they don't have any letters in common in their notation.

Definition 5.4. If a_1, a_2, \dots, a_k are distinct number between 1 and n then the permutation

$$\alpha = (a_1 a_2 \dots a_k) \in S_n$$

is called a k -cycle. This notation means that $\alpha(a_i) = a_{i+1}$ for $i = 1, 2, \dots, n-1$ and $\alpha(a_n) = a_1$.

Lemma 5.5. Disjoint cycles commute.

Theorem 5.6. Every permutation σ is a product of disjoint cycles. Furthermore these cycles are unique and can be multiplies in any order.

For example,

$$\sigma = (13)(254) = (254)(13)$$

This is called the *cycle decomposition* of σ .

Theorem 5.7. The order of a permutation is equal to the least common multiple of the lengths of the cycles in its cycle decomposition.

5.1. Even and odd permutations. 2-cycles (ab) are called *transpositions*. If $b = a + 1$ then (ab) is called an *adjacent transposition*.

Theorem 5.8. *Every permutation of n can be written as a product of adjacent transpositions.*

Definition 5.9. *A permutation σ is called even or odd if it can be written as a product of an even, resp. odd, number of transpositions. The sign of a permutation is 1 for even permutations and -1 for odd permutations.*

The sign of a permutation of n is also given by the following explicit formula:

$$\operatorname{sgn}(\sigma) = \operatorname{sgn} \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i))$$

In other words, σ is even (or odd) if there are an even (or odd) number of pairs $i < j$ which get reversed ($\sigma(i) > \sigma(j)$).

The even permutations form a subgroup A_n of S_n called the *alternating group* on n letters. A_n has $n!/2$ elements. For example, the groups of rotations of the regular tetrahedron gives the alternating group A_4 if we label the four vertices of the tetrahedron 1,2,3,4 and write rotations as permutations of the corners.

Theorem 5.10. *Even cycles are odd permutations and odd cycles are even permutations.*

Proof. Every k -cycle can be written as a product of $k-1$ transpositions:

$$(123 \cdots k) = (12)(23)(34) \cdots (k-1, k)$$

□

Problem. Write the dihedral group D_5 as a permutation group of the corners 1, 2, 3, 4, 5 of the regular pentagon.