

9 Subgroups

A *subgroup* of a group G is defined to be a subset H of G which contains the neutral element $e = 1$ and is also closed under multiplication and inverse. The notation is $H \leq G$.

Theorem 9.1. *A subset $H \subseteq G$ is a subgroup iff*

1. H is nonempty and
2. $HH^{-1} \subseteq H$, i.e., $gh^{-1} \in H$ for all $g, h \in H$.

Examples of subgroups are:

1. $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$ for any $g \in G$
2. The *center* $Z(G)$ of G . This is the set of all elements of G which are *central* (which commute with all other elements).
3. $\{A \in GL_n(\mathbb{R}) \mid Ae_1 = e_1\}$. (This is supposed to be obvious and is an example of a general philosophy that symmetries which preserve some property or equation form a group.)

The main theorem about subgroups is Lagrange's theorem that the order of a subgroup divides the order of the group. This comes from the partition of G into "cosets."

A (*left*) *coset* of H is defined to be a set of the form gH for some $g \in G$. In class I tried to explain to you that the element g is not unique. For example, if $h \in H$ then $eH = hH$ and

$$gH = (gh)H$$

Thus, there are many ways to write the same set.

The statement that the cosets of H form a partition of G is written as follows.

Lemma 9.2. 1. *The cosets gH of H in G are either disjoint or equal.*

2. *G is a union of cosets: $G = \bigcup gH$*

3. *Every coset gH has the same number of elements. More precisely, there is a bijection $f : g_1H \rightarrow g_2H$ between any two cosets.*

Proof. (1) Suppose that g_1H and g_2H are not disjoint. Then they have a common element $x = g_1h_1 = g_2h_2$. This equation can be written as

$$g_2^{-1}g_1 = h_2h_1^{-1} = h_3 \in H$$

or: $g_1 \in g_2H$ which implies that

$$g_1H \subseteq g_2HH = g_2H.$$

A similar argument shows that $g_2H \subseteq g_1H$. Therefore, $g_1H = g_2H$.

(2) Since $e \in H$ every $g \in G$ is an element of the coset gH .

(3) A bijection

$$f : g_1H \rightarrow g_2H$$

is given by $f(x) = g_2g_1^{-1}x$. (The inverse map is given by $f^{-1}(y) = g_1g_2^{-1}y$.)

□

The number of distinct cosets gH of H in G is called the *index* of H in G and is denoted $|G : H|$.

Theorem 9.3 (Lagrange). *If G is a finite group and $H \leq G$ then $|H|$ divides $|G|$ and the quotient is equal to the index:*

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

This follows from the lemma about cosets and the elementary counting principle:

Lemma 9.4. *Suppose that a set S is a disjoint union of n subsets*

$$S = S_1 \cup S_2 \cup \cdots \cup S_n$$

all of the same size: $|S_i| = m$ for all i . Then $|S| = nm$.

Proof. By induction on n .

□

We also went through the following problem:

Problem: Show that every subgroup of a cyclic group is cyclic.

First we decided that the way to begin this problem is the following. We are given a cyclic group G . This means

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

for some $g \in G$ (g is called a *generator* for G). Next we should take an arbitrary subgroup $H \subseteq G$. We need to show that H is cyclic. This means we need to find a generator for H .

Now we have to think. Think about similar problems that we did in the past. The greatest common divisor is similar since it is a single generator of the ideal generated by two other elements. The gcd was defined to be the smallest positive integer in the ideal.

So, let j be the smallest positive integer so that $g^j \in H$. (If no such j exists then $H = \{e\} = \langle e \rangle$ is cyclic.) Then we claim that $H = \langle g^j \rangle$ and thus is cyclic. The proof of this claim is by contradiction. Suppose not. Then there is an element $h \in H$ which is not in $\langle g^j \rangle$. This means that $h = g^i$ where i is not divisible by j . Use the division algorithm:

$$i = jq + r, \quad 0 < r < j$$

But then H contains

$$g^i(g^j)^{-q} = g^{i-jq} = g^r$$

which contradicts the minimality of j . Thus $H = \langle g^j \rangle$ is cyclic.

Homework: p.133 #37, 38, 44, p.142 #48, 51, 53(i).