Subgroups

Definition: A subset H of a group G is a subgroup of G if H is itself a group under the operation in G.

Note: Every group G has at least two subgroups: G itself and the subgroup $\{e\}$, containing only the identity element. All other subgroups are said to be proper subgroups.

Examples

1. GL(n,R), the set of invertible $n \times n$ matrices with real entries is a group under matrix multiplication. We denote by SL(n,R) the set of $n \times n$ matrices with real entries whose determinant is equal to 1. SL(n,R) is a proper subgroup of GL(n,R) . (GL(n,R), is called the general linear group and SL(n,R) the special linear group.)

2. In the group D_4, the group of symmetries of the square, the subset $\{e,r,r^2,r^3\}$ forms a proper subgroup, where r is the transformation defined by rotating $\frac{\pi}{2}$ units about the z-axis.

3. In Z_9 under the operation +, the subset {0, 3, 6} forms a proper subgroup.

Problem 1: Find two different proper subgroups of S_3.

We will prove the following two theorems in class:
Theorem: Let H be a nonempty subset of a group G. H is a subgroup of G iff
  (i) H is closed under the operation in G and
  (ii) every element in H has an inverse in H.

For finite subsets, the situation is even simpler:

Theorem: Let H be a nonempty *finite* subset of a group G. H is a subgroup of G iff H is closed under the operation in G .

Problem 2: Let H and K be subgroups of a group G.
(a) Prove that $H \cap K$ is a subgroup of G.
(b) Show that $H \cup K$ need not be a subgroup

Example: Let Z be the group of integers under addition. Define H_n to be the set of all multiples of n. It is easy to check that H_n is a subgroup of Z. Can you identify the subgroup $H_n \cap H_m$? Try it for $H_6 \cap H_9$.

Note that the proof of part (a) of Problem 2 can be extended to prove that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup.

Cyclic Groups and Subgroups

We can always construct a subset of a group G as follows:
Choose any element a in G. Define $\langle a \rangle = \{a^n \mid n \in Z\}$, i.e. $\langle a \rangle$ is the set consisting of all powers of a.

Problem 3: Prove that $\langle a \rangle$ is a subgroup of G.

Definition: $\langle a \rangle$ is called the cyclic subgroup generated by a. If $\langle a \rangle = G$, then we say that G is a cyclic group. It is clear that cyclic groups are abelian.

For the next result, we need to recall that two integers a and n are relatively prime if and only if gcd(a, n)=1. We have proved that if gcd(a, n)=1, then there are integers x and y such that $ax + by = 1$. The converse of this statement is also true:

Theorem: Let a and n be integers. Then gcd(a, n)=1 if and only if there are integers x and y such that $ax + by = 1$.

Problem 4: (a) Let $U_n = \{a \in Z_n \mid \gcd(a,n)=1\}$. Prove that U_n is a group under multiplication modulo n. (U_n is called the group of units in Z_n.)
(b) Determine whether or not U_n is cyclic for n= 7, 8, 9, 15.

We will prove the following in class.
Theorem: Let G be a group and $a \in G$.
(1) If a has infinite order, then $\langle a \rangle$ is an infinite subgroup consisting of the distinct elements a^k with $k \in Z$.
(2) If a has finite order n, then $\langle a \rangle$ is a subgroup of order n and $\langle a \rangle = \{e = a^0, a^1, a^2, \ldots, a^{n-1}\}$.

Theorem: Every subgroup of a cyclic group is cyclic.

Problem 5: Find all subgroups of U_{18}.

Note: When the group operation is addition, we write the inverse of a by $-a$ rather than a^{-1}, the identity by 0 rather than e, and a^k by ka. For example, in the group of integers under addition, the subgroup generated by 2 is $\langle 2 \rangle = \{2k \mid k \in Z\}$.

Problem 6: Show that the additive group $Z_2 \times Z_3$ is cyclic, but $Z_2 \times Z_2$ is not.

Problem 7: Let G be a group of order n. Prove that G is cyclic if and only if G contains an element of order n.

The notion of cyclic group can be generalized as follows. : Let S be a nonempty subset of a group G. Let $\langle S \rangle$ be the set of all possible products, in every order, of elements of S and their inverses.
We will prove the following theorem in class.
Theorem: Let S be a nonempty subset of a group G.

(1) $\langle S \rangle$ is a subgroup of G that contains S.

(2) If H is a subgroup of G that contains S, then H contains $\langle S \rangle$.

(3) $\langle S \rangle$ is the intersection of all subgroups of G that contain S.

The second part of this last theorem states that $\langle S \rangle$ is the smallest subgroup of G that contains $\langle S \rangle$. The group $\langle S \rangle$ is called the subgroup of G generated by S.
Note that when S = $\{a\}$, $\langle S \rangle$ is just the cyclic subgroup generated by a. In the case when $\langle S \rangle = G$, we say that G is generated by S, and the elements of S are called generators of G.

Example: Recall that we showed that every element in D_4 could be represented by r^k or ar^k for k=0, 1, 2, 3, where r is the transformation defined by rotating $\frac{\square}{2}$ units about the z-axis, and a is rotation / / units about the line y=x in the x-y plane. Thus D_4 is generated by S =$\{a, r\}$.

Problem 8: Show that U_{15} is generated by {2, 13}.