المحاضرة الثانية

Subgroups and Langrage Theorem

A subgroup of group G is a subset that is a group under the same operation as in G. The following definition will help to make this last phrase precise.

Definition (1): Let $\ast$ be an operation on a set G, and let $S \subseteq G$ be a subset. We say that S is closed under $\ast$ if $x \ast y \in S$ for all $x, y \in S$.

The operation on a group G is a function $*: G \times G \to G$.
(for example, 2 and −2 lie in Z_+, but their sum $-2 + 2 = 0 \notin Z_+$.

Definition (2): A subset H of a group G is a subgroup if:

(i) $I \in H$;
(ii) If $x, y \in H$, then $x y \in H$; that is, H is closed under $\ast$.
(iii) If $x \in H$, then $x^{-1} \in H$.

Proposition (3): Every subgroup $H \leq G$ of a group G is itself a group.

Proof: Axiom (ii) (in the definition of subgroup) shows that H is closed under the operation of G; that is, H has an operation (namely, the restriction of the operation $\ast: G \times G \to G$ to $H \times H \subseteq G \times G$.
This operation is associative:
since the equation $(x y)z = x (yz)$ holds for all $x, y, z \in G$, it holds, in particular, for all $x, y, z \in H$. Finally, axiom (i) gives the identity, and axiom (iii) gives inverses.

It is quicker to check that a subset H of a group G is a subgroup (and hence that it is a group in its own right) than to verify the group axioms for H, for associativity is inherited from the operation on G and hence it need not be verified again.

One can shorten the list of items needed to verify that a subset is, in fact, a subgroup.

Proposition (4): A subset H of a group G is a subgroup if and only if H is nonempty and, whenever $x, y \in H$, then $x y^{-1} \in H$.

Proof: If H is a subgroup, then it is nonempty, for $1 \in H$. If $x, y \in H$, then $y^{-1} \in H$, by part (iii) of the definition, and so $x y^{-1} \in H$, by part (ii).
Conversely, assume that H is a subset satisfying the new condition. Since H is nonempty, it contains some element, say, h. Taking x = h = y, we see that $e = hh^{-1} \in H$, and so part (i) holds. If $y \in H$, then set x = e (which we can now do because $e \in H$), giving $y^{-1} = ey^{-1} \in H$, and so part (iii) holds. Finally, we know that $(y^{-1})^{-1} = y$, by. Hence, if $x, y \in H$, then $y^{-1} \in H$ and so $x y = x (y^{-1})^{-1} \in H$. Therefore, H is a subgroup of G.

Since every subgroup contains e, one may replace the hypothesis "H is nonempty" in Proposition by "$e \in H$".

Note that if the operation in G is added, then the proposition's condition is that H is a nonempty subset of G such that $x, y \in H$ implies $x - y \in H$.

Proposition (5): Let G be a finite group, and $a \in G$. Then the order of a, is the number of elements in (a).

Definition (6): If G is a finite group, then the number of elements in G, denoted by |G|, is called the order of G.

Definition (7): If X is a subset of a group G, such that X generates G, then G is called finitely generated, and G is generated by X.

In particular, If G = ({a}), then G is generated by the subset X = {a}.

Definition (8):

A group G is called cyclic if G = (a); that is G can be generated by only one element say a, and this element is called a generator of G.

Note that we can define cyclic subgroup as follows.

Definition (9): If G is a group and $a \in G$, write

$$(a) = \{a^n : n \in Z_+\} = \{\text{all powers of } a\}$$

(a) is called cyclic subgroup of G generated by a.

Proposition (10): The intersection of any family of subgroups is again subgroup.

Coset of sets:

Definition (1): If H is a subgroup of a group G and a G, then the coset a H is the subset a H of G, where ∈

$$a\,H = \{ah : h \in H\}$$

Of course, $a = ae \in a\,H$. Cosets are usually not subgroups.

The cosets just defined are often called left cosets; there are also right cosets of H, namely, subsets of the form H a {ha| h ∈H}; these arise in further study of groups, but we shall work almost exclusively with (left) cosets.

In particular, if the operation is addition, then the coset is denoted by

$$a + H = \{a + h : h \in H\}.$$

Proposition (2): Let G be a group, and H be a subgroup of G, for any $a, b \in G$ we have the following:

(i) $a\,H = b\,H$ if and only if $b^{-1}a \in H$. In particular, $a\,H = H$ if and only if $a \in H$.

(ii) If $a\,H \cap b\,H \neq \emptyset$, then $a\,H = b\,H$.

(iii) For each $a \in G$: Order of H is equal to the order of aH.

Proof:

(i) It is clear.

(ii) It is clear.

(iii) The function $f: H \rightarrow a\,H$ which is given by $f(h) = ah$, is easily seen to be a bijective [its inverse $a\,H \rightarrow H$ is given by ah r→ $a^{-1}(ah) = h$]. Therefore, H and a H have the same number of elements.

Theorem (3): (Lagrange's Theorem)

If H is a subgroup of a finite group G, then |H | is a divisor of |G|. That is:

$$|G| = [G : H]|H|$$

This formula shows that the index [G : H] is also a divisor of |G|.

Corollary (4): If H is a subgroup of a finite group G, then

$$[G : H] = |G|/|H|$$

Corollary (5): If G is a finite group and $a \in G$, then the order of a is a divisor of |G|.

Corollary (6): If a finite group G has order m, then $a^m = e$ for all $a \in G$.

Corollary (7): If p is a prime, then every group G of order p is cyclic.

Proof: Choose $a \in G$ with $a \neq e$, and let H = (a) be the cyclic subgroup generated by a. By Lagrange's theorem, |H | is a divisor of |G| = p. Since p is a prime and |H | > 1, it follows that |H | = p = |G|, and so H = G.

Lagrange's theorem says that the order of a subgroup of a finite group G is a divisor of G . Is the "converse" of Lagrange's theorem true? That is, if d is a divisor of G, must there exists a subgroup of G having order d? The answer is "no;" We can show that the alternating group A4 is a group of order 12 which has no subgroup of order 6.

References

1. D. M. Burton, Abstract and linear algebra, 1972.

2. Joseph J. Rotman, Advanced Modern Algebra, 2003.

3. John B. Fraleigh, A First Course in Abstract Algebra, Seventh Edition, 2002.

4. Joseph A. Gallian, Contemporary Abstract Algebra, 2010.