MATH 433

Applied Algebra

Lecture 29: Lagrange's Theorem (continued). Classification of subgroups. Quotient group.

Lagrange's Theorem

Definition. Let H be a subgroup of a group G. A **coset** (or **left coset**) of the subgroup H in G is a set of the form $aH = \{ah : h \in H\}$, where $a \in G$.

Proposition The cosets of the subgroup H in G form a partition of the set G.

Definition. The number of elements in a group G is called the **order** of G and denoted $o(G)$. Given a subgroup H of G, the number of cosets of H in G is called the **index** of H in G and denoted $[G : H]$.

Theorem (Lagrange) If H is a subgroup of a finite group G, then $o(G) = [G : H] \cdot o(H)$. In particular, the order of H divides the order of G.

Corollaries of Lagrange's Theorem

Corollary 1 If G is a finite group, then the order of any element $g \in G$ divides the order of G.

Corollary 2 Any group G of prime order p is cyclic.

Corollary 3 If G is a group of prime order, then it has only 2 subgroups: the trivial subgroup and G itself.

Corollary 4 The alternating group $A(n)$, $n \geq 2$, consists of $n!/2$ elements.

Proof: Indeed, $A(n)$ is a subgroup of index 2 in the symmetric group $S(n)$. The latter consists of $n!$ elements.

Corollary 5 If G is a finite group, then $g^{o(G)} = e$ for all $g \in G$.

Corollary 6 (Fermat's Little Theorem) If p is a prime number then $a^{p-1} \equiv 1 \bmod p$ for any integer a that is not a multiple of p.

Proof: $a^{p-1} \equiv 1 \bmod p$ means that $[a]_p^{p-1} = [1]_p$.
a is not a multiple of p means that $[a]_p$ is in G_p, the multiplicative group of invertible congruence classes modulo p. It remains to recall that $o(G_p) = p - 1$ and apply Corollary 5.

Corollary 7 (Euler's Theorem) If n is a positive integer then $a^{\phi(n)} \equiv 1 \bmod n$ for any integer a coprime with n.

Proof: $a^{\phi(n)} \equiv 1 \bmod n$ means that $[a]_n^{\phi(n)} = [1]_n$.
a is coprime with n means that the congruence class $[a]_n$ is in G_n. It remains to recall that $o(G_n) = \phi(n)$ and apply Corollary 5.

Classification of subgroups

- Subgroups of $(\mathbb{Z}_{10}, +)$.

The group is cyclic: $\mathbb{Z}_{10} = \langle[1]\rangle = \langle[3]\rangle = \langle[7]\rangle = \langle[9]\rangle$. Therefore any subgroup of $\mathbb{Z}_{10}$ is also cyclic. There are three proper subgroups: the trivial subgroup $\{[0]\}$ (generated by [0]), a cyclic subgroup of order 2 $\{[0], [5]\}$ (generated by [5]), and a cyclic subgroup of order 5 $\{[0], [2], [4], [6], [8]\}$ (generated by either of the elements [2], [4], [6], and [8]).

- Subgroups of $(G_{15}, \times)$.

The group consists of 8 congruence classes modulo 15: $G_{15} = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$. It is Abelian. However G_{15} is not cyclic since it contains a non-cyclic subgroup $\{[1], [4], [11], [14]\} = \{[1], [4], [-4], [-1]\}$. The other proper subgroups of G_{15} are cyclic: $\{[1]\}$, $\{[1], [4]\}$, $\{[1], [11]\}$, $\{[1], [14]\}$, $\{[1], [2], [4], [8]\}$, $\{[1], [4], [7], [13]\}$.

Theorem Let G be a cyclic group of finite order n. Then for any divisor d of n there exists a unique subgroup of G of order d, which is also cyclic.

Proof: Let g be the generator of the cyclic group G. Take any divisor d of n. Since the order of g is n, it follows that the element $g^{n/d}$ has order d. Therefore a cyclic group $H = \langle g^{n/d} \rangle$ has order d.

Now assume H' is another subgroup of G of order d. The group H' is cyclic since G is cyclic. Hence $H' = \langle g^k \rangle$ for some $k \in \mathbb{Z}$. Since the order of the element g^k is d while the order of g is n, it follows that $\gcd(n, k) = n/d$. We know that $\gcd(n, k) = an + bk$ for some $a, b \in \mathbb{Z}$. Then $g^{n/d} = g^{an+bk} = g^{na}g^{kb} = (g^n)^a(g^k)^b = (g^k)^b \in \langle g^k \rangle = H'$. Consequently, $H = \langle g^{n/d} \rangle \subset H'$. However H and H' both consist of d elements. Thus $H' = H$.

- Subgroups of $S(3)$.

The group consists of 6 permutations: $S(3) = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. It is not Abelian. All proper subgroups of $S(3)$ are cyclic: $\{\mathrm{id}\}$, $\{\mathrm{id}, (1\ 2)\}$, $\{\mathrm{id}, (1\ 3)\}$, $\{\mathrm{id}, (2\ 3)\}$, and $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$.

- Subgroups of $A(4)$.

The group consists of 12 permutations:

$$A(4) = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2),\\ (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}.$$

It is not Abelian. The cyclic subgroups are $\{\mathrm{id}\}$, $\{\mathrm{id}, (1\ 2)(3\ 4)\}$, $\{\mathrm{id}, (1\ 3)(2\ 4)\}$, $\{\mathrm{id}, (1\ 4)(2\ 3)\}$, $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$, $\{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\}$, $\{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}$, and $\{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\}$.
Also, $A(4)$ has one non-cyclic subgroup of order 4: $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Quotient group

Let's recall the construction of the group $(\mathbb{Z}_n, +)$. The elements are congruence classes $a + n\mathbb{Z}$ modulo n and the operation is defined by $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$. Observe that congruence classes $a + n\mathbb{Z}$ are also cosets of the subgroup $n\mathbb{Z}$ in the group $\mathbb{Z}$.

Now consider an arbitrary group G (with multiplicative operation) and a subgroup H of G. Let G/H denote the set of all cosets gH of the subgroup H in G. We try to define an operation on G/H by the rule $(aH)(bH) = (ab)H$. Assume that this operation is well defined (it need not be). Then it makes G/H into a group, which is called the **quotient group** of G by the subgroup H. Indeed, the closure axiom and associativity will hold in G/H since they hold in G. Further, the identity element will be $eH = H$ and the inverse of gH will be $g^{-1}H$.

Question. When the operation on G/H is well defined?