18. Lagrange Theorem and Classification of groups of small order

18.1. **Lagrange Theorem and its immediate consequences.**

Lagrange Theorem. *Let G be a finite group and H a subgroup of G. Then $|H|$ divides $|G|$.*

We will prove Lagrange Theorem next week. In this lecture we will discuss some of its applications. We start with an immediate corollary:

Corollary 18.1. *Let G be a finite group and $g \in G$. Then*

(A) *$o(g)$ divides $|G|$*
(B) *$g^{|G|} = e$.*

Proof. (A) We know that the order of an element is the order of the cyclic subgroup generated by that element: $o(g) = |\langle g \rangle|$. Thus (A) follows from Lagrange Theorem applied to $H = \langle g \rangle$.

(B) Let $m = o(g)$ and $n = |G|$. Then $g^m = e$ by definition of the order and $n = mk$ for some $k \in \mathbb{Z}$ by (A). Hence $g^n = g^{mk} = (g^m)^k = e$. □

Here is another important consequence.

Theorem 18.2. *Let p be a prime, and let G be a group of order p. Then G is cyclic (hence G is isomorphic to $(\mathbb{Z}_p, +)$ by Lecture 15).*

Proof. Since $|G| = p > 1$, we can choose a non-identity element $a \in G$. By Corollary 18.1(A), $o(a)$ divides p, so $o(a) = 1$ or $o(a) = p$ since p is prime. But $a \neq e$, so $o(a) \neq 1$. Therefore, $o(a) = p$, whence $|\langle a \rangle| = o(a) = p = |G|$. Hence $\langle a \rangle = G$, so G is cyclic. □

18.2. **Classification of groups of small order up to isomorphism.**

Theorem 18.2 shows that for any prime p, there is only one group of order p, up to isomorphism, namely $\mathbb{Z}_p$ (with addition). The next Theorem describes groups or order 4 (which is the smallest composite natural number) up to isomorphism.

Note that there are at least two non-isomorphic groups of order 4: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ (these groups are not isomorphic since $\mathbb{Z}_4$ is cyclic while $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not by HW#7.6).

Theorem 18.3. *Any group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. We already know that a cyclic group of order 4 is isomorphic to $\mathbb{Z}_4$. Thus, it will be sufficient to show that any non-cyclic group of order 4 is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. We will prove the latter by showing that any two non-cyclic groups of order 4 are isomorphic to each other.

First we make an observation about orders of elements in a non-cyclic group of order 4. If $|G| = 4$, then by Corollary 18.1(A) for any $g \in G$ we have $o(g)|4$, so $o(g) = 1, 2$ and 4. If in addition G is non-cyclic, then G cannot have elements of order 4, so all non-identity elements of G must have order 2. Thus, we have

$$g^2 = e \text{ for all } g \in G \qquad (***)$$

(of course this equality also holds if g is the identity element).

Now let us take any two non-cyclic groups of order 4, denote them by G and G'. Let e (respectively e') denote the identity element of G (respectively G'), and let x, y, z (respectively x', y', z') be the three non-identity elements of G (respectively G') listed in an arbitrary order. By (***) we must have $x^2 = y^2 = z^2 = e$ and $(x')^2 = (y')^2 = (z')^2 = e'$, so we can fill a substantial portion of the multiplication table for both G and G':

G	e	x	y	z
e	e	x	y	z
x	x	e		
y	y		e	
z	z			e

G'	e'	x'	y'	z'
e'	e'	x'	y'	z'
x'	x'	e'		
y'	y'		e'	
z'	z'			e'

Note that there is unique way to complete the remainder of those tables using Sudoku property. (For instance, in the multiplication table for G the x-row already contains x and e and y-column contains y and e, so we must have $xy = z$ for the Sudoku property to hold). Thus, multiplication tables for G and G' look as follows:

G	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

G'	e'	x'	y'	z'
e'	e'	x'	y'	z'
x'	x'	e'	z'	y'
y'	y'	z'	e'	x'
z'	z'	y'	x'	e'

It is clear from these multiplication tables that the map $\varphi : G \to G'$ given by $\varphi(e) = e'$, $\varphi(x) = x'$, $\varphi(y) = y'$ and $\varphi(z) = z'$, is an isomorphism. □

Theorem 18.3 has a natural generalization classifying groups of order p^2:

Theorem 18.4. *Let p be a prime. Any group of order p^2 is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.*

The proof of Theorem 18.4 requires more advanced tools.

We finish the lecture by stating (without proof) classification of groups of orders $6, 8, 9$ and 10 up to isomorphism.

Groups of order 6: There are two groups up to isomorphism: $\mathbb{Z}_6$ and S_3. These groups are not isomorphic since $\mathbb{Z}_6$ is abelian while S_3 is not.

Groups of order 8: There are five groups up to isomorphism: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_8 (groups of isometries of a square) and Q_8 (quaternion group – see HW#7). It was proved in HW#7 that D_8 and Q_8 are not isomorphic to each other; also it is clear that D_8 or Q_8 is not isomorphic to any of the first three groups on the list since those groups are abelian while D_8 and Q_8 are not abelian. The groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic to each other by FTFAG, but one can also check this directly by compute the maximal order of an element in each group: the maximal order of an element is 8 for $\mathbb{Z}_8$ (since this group is cyclic), 4 for $\mathbb{Z}_4 \times \mathbb{Z}_2$ (e.g. by the result of Problem 6 in HW#8) and 2 for $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Hence by Corollary 15.4, these three groups are not isomorphic to each other.

Groups of order 9: According to Theorem 18.4 above, there are two groups up to isomorphism: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Groups of order 10: There are two groups up to isomorphism: $\mathbb{Z}_{10}$ and D_{10}, where D_{10} is the group of isometries of a regular pentagon. These groups are not isomorphic to each other since $\mathbb{Z}_{10}$ is abelian while D_{10} is not.

More generally, we have the following classification of groups of order $2p$, where p is prime.

Theorem 18.5. *Let p be a prime. Any group of order $2p$ is isomorphic to $\mathbb{Z}_{2p}$ or D_{2p} (the group of isometries of a regular p-gon).*

Note that the statement of Theorem 18.5 for $p = 3$ does not seem to match what we previously said about groups of order 6. The reason there is no contradiction is that D_6 (the group of isometries of a regular 3-gon AKA equilateral triangle) is isomorphic to S_3. A natural isomorphism $\varphi : D_6 \to S_3$ is given as follows: label vertices of a equilateral triangle Δ by $1, 2$ and 3. Any isometry f of Δ permutes the vertices, so f naturally determines a permutation of the set $\{1, 2, 3\}$ (that is, an element of S_3); we denote this element by $\varphi(f)$. It is easy to check that $\varphi : D_6 \to S_3$ is an isomorphism (the proof of the fact that φ is an injective homomorphism is very similar to the proof of Cayley's theorem, and since $|D_6| = |S_3| = 6$, once we know that φ is injective, it must also be bijective).

One can define analogous map $\varphi_n : D_{2n} \to S_n$ for any $n \geq 3$. The map φ_n will not be an isomorphism unless $n = 3$; however, it will always be an injective homomorphism.

18.3. **Book references.** The general references for the first lecture are [Pinter, Chapter 13] and [Gilbert, 4.4].