Lecture 6

Abel groups. Subgroups. Cyclic groups

We remind the following definition

Def. If $G = (A, \circ)$ is a group, and $\forall a, b \in A$

$$a \circ b = b \circ a,$$

then G is an abelian group.

Def. If $A_1 \subset A$ is a subset of A, and $G_1 = (A_1, \circ)$ is also a group, then G_1 is called a subgroup of group $G = (A, \circ)$.

Here we test the properties of groups:

1. $\forall a, b \in A_1 \Rightarrow a \circ b \in A_1$.

2. A_1 contains a neutral element $e \in A_1$ (of group A, also).

3. $\forall a \in A_1$ there exists an inverse element $a' \in A_1$, such that $a \circ a' = e$.

Example. $G_1 = (2\mathbb{Z}, +)$ is a subgroup of $G = (\mathbb{Z}, +)$.

$2\mathbb{Z} = 0 + 2\mathbb{Z}$

1. $2k, 2l \in 2\mathbb{Z}$, if $k, l \in \mathbb{Z}$.
$2k + 2l = 2(k+l) \in 2\mathbb{Z}$

2. $e = 0 \in 2\mathbb{Z}$

3. $-2k = (2k)' \in 2\mathbb{Z}$.

Def. The order of a group $G = (A, \circ)$ is the number of its elements

$$E(A) = |A|.$$

If $E(A) < \infty$, then the group G is finite, otherwise the group G has infinite order.

The order of a subgroup of an infinite group can be finite or infinite.

Example 1. A group $G = (\mathbb{Z}, +)$ and its subgroup $G_1 = (2\mathbb{Z}, +)$ both are infinite.

Example 2.

Take a group $G=(\mathbb{R},\cdot)$.

Show that

$G_2=(\{-1,1\},\cdot)$ is a subgroup of G.

The order of G_2 is finite and equal to 2.

Order of group elements

Def. Let $G=(A,\circ)$ is a group and let $g\in A$.

$$g^m=\overbrace{g\circ g\circ\dots\circ g}^{m},\quad m\in\mathbb{N}$$

Recursive definition

$$g^m=g\circ g^{m-1},\quad g^1=g.$$

$g^0 = e$ (it is a definition)

It is clear that

$$g^1 = g \circ g^0 = g \circ e = g$$

Def.

$g^{-m} = (g')^m$, where g' is inverse element of g:

$g' \circ g = e$.

Theorem.

$$g^m \circ g^n = g^{m+n}, \quad m, n \in \mathbb{Z}$$

(can be negative)

For the proof lets consider three cases

1) $m, n > 0$ 2) $m > 0, n < 0$, 3) $m < 0$, $n < 0$

Let's take $m > 0$, $n < 0$.

$n = -k$, $k > 0$. and assume that $k > m$.

$$g^m \circ g^n = \underbrace{g \circ \cdots \circ g}_{m} \circ \underbrace{(g' \circ g' \circ \cdots \circ g')}_{k}$$

$$= \underbrace{g' \circ \cdots \circ g'}_{k-m} = g^{-(k-m)}$$

$$= g^{m-k} = g^{m+n}. \quad \blacktriangleright$$

If $G = (A, \circ)$ is a group, and $a \in A$, then $G_1 = (\{a^m : m \in \mathbb{Z}\}, \circ)$ is a subgroup of group G. (Give a proof).

G_1 the subgroup generated by g and is denoted by (g).

Def. If $G = (g)$ for some $g \in G$, then G is called cyclic and g is called a generator of G.

Def. Let $g \in G$. If there is a positive integer a with $g^a = e$, where e is a neutral element, then the smallest such integer a is called the order of g.

It is denoted $\operatorname{order}_G g \; (= E(g))$

Example We determine the order of $2 + 13\mathbb{Z}$ in

k	1	2	3	4	5	6	7	8	9	10
$2^k \bmod 13$	2	4	8	3	6	12	11	9	5	10

11	12
7	1

Now we determine the order of element $4 + 13\mathbb{Z}$.

k	1	2	3	4	5	(6)
$4^k \bmod 13$	4	3	12	9	10	1

Multiplicative Group of Residues

The following result is very important in cryptography

Th. The set of all invertible residue classes modulo m is a finite abelian group with respect to multiplication.

This group is called the multiplicative group of residues modulo m and is denoted

$$(\mathbb{Z}/m\mathbb{Z})^*.$$

Its order is denoted by $\varphi(m)$, where φ is called the Euler φ-function.

The residue class $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ if and only if the congruence

$$ax \equiv 1 \mod m$$

is solvable.

We know that this statement is valid if

$$\gcd(a, m) = 1.$$

Th. For any cyclic group (g) the order of its generator $g \in A$ (i.e. $G = (A, \circ) = (g)$) is equal to the order of this group

$$E(g) = E(G).$$

◀ The proof is very simple and we skip it. ▶

Example 1.

$$E(\mathbb{Z}/13\mathbb{Z}) = 12$$

and the order of element $g = 2 + 13\mathbb{Z}$ is also $E(2+13\mathbb{Z}) = 12$, We know that $(g) = \mathbb{Z}/13\mathbb{Z}$.

Values of Euler φ-function

m	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4

Example 1.

$$(\mathbb{Z}/12\mathbb{Z})^* = \{1+12\mathbb{Z},\ 5+12\mathbb{Z},\ 7+12\mathbb{Z},\ 11+12\mathbb{Z}\}.$$

Ex 2. (Th).

If p is a prime number, then

$$\varphi(p) = p-1.$$

Questions?

1. How to find the number of generators of a cyclic group $(\mathbb{Z}/m\mathbb{Z})^*$.
2. How to find one (or all) generators.

We determine the order of powers.
G is multiplicatively written with neutral element 1.

Th.1. If $g \in G$ is of finite order e, and if n is an integer, then order

$$E(g^n) = \frac{e}{\gcd(e,n)}.$$

Example

$$G = (\mathbb{Z}/13\mathbb{Z})^*$$

$$E(2+13\mathbb{Z}) = 12$$

Then $E(2^2+13\mathbb{Z}) = \frac{12}{\gcd(12,2)} = \frac{12}{2} = 6.$

We had the table showing

$$E(4+13\mathbb{Z}) = 6$$

Homework: test (computation).

$$E(8+13\mathbb{Z}) = E(2^3+13\mathbb{Z})$$

Th. If G is finite and cyclic, then G has exactly $\varphi(|G|)$ generators and they are of order $|G|$.

Proof. From Th 1 we get that $k \in G$ is a generator if

$$\gcd(k, |G|) = 1.$$

This indicates that the number of generators of G is exactly $\varphi(|G|)$.

Examples 1.

$G = (\mathbb{Z}/13\mathbb{Z})^* \Rightarrow |G| = 12$

$= \{a + 13\mathbb{Z}, \} \cdot a = \{1, 2, \dots, 12\}$.

The set of generators? Find it

The number of generators $\varphi(12) = 4$.

Example 2.

Subgroup generated by $4 + 13\mathbb{Z}$ has order 6

$\{k + 13\mathbb{Z}, \quad k = 1, 4, 3, 12, 9, 10\}$.

Next we formulate the Fermat's Little Theorem.

Th F. If $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Example. Take $a = 5$, $m = 4$.

$$\varphi(4) = 2$$

$$5^2 = 25 \equiv 1 \mod 4.$$

We get second algorithm how to compute inverse mod m element (the first one was the extended euclidean algorithm).

$$a^{\varphi(m)} = a^{\varphi(m)-1} \cdot a \equiv 1 \bmod m.$$

$a^{\varphi(m)-1}$ is the inverse of a.

$a^{\varphi(m)-1} + m\mathbb{Z}$.

Example.

$a = 5, \quad m = 4.$

We find: $\varphi(4) = 2$

inverse

$\Rightarrow \quad 5' = 5^{\varphi(4)-1} = 5$

$$5 \cdot 5 = 25 \equiv 1 \bmod 4.$$

T. Let $m_1, \dots, m_n$ be pairwise coprime positive integers, $m = \prod_{i=1}^{n} m_i$.

Then $\varphi(m) = \varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_n)$.