Lecture 8 : Cosets, subgroups of $\mathbb{Z}$

Consider the group $G = D_6$.

The elements are:

$$\begin{matrix} 1 & \rho & \rho^2 & \rho^3 & \rho^4 & \rho^5 \\ \tau & \rho\tau & \rho^2\tau & \rho^3\tau & \rho^4\tau & \rho^5\tau \end{matrix}$$

We have the relations $\rho^6 = 1$, $\tau^2 = 1$, $\rho\tau = \tau\rho^{-1}$.

Left cosets of $H = \{1, \tau\}$

1	ρ	ρ^2	ρ^3	ρ^4	ρ^5
τ	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$	$\rho^4\tau$	$\rho^5\tau$

Right cosets of $H = \{1, \tau\}$

1	ρ	ρ^2	ρ^3	ρ^4	ρ^5
τ	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$	$\rho^4\tau$	$\rho^5\tau$

So, we observe that

(1) Both left and right cosets give partitions of the group.

(2) Right cosets of a group may be very different from the left cosets.

Subgroups of $\mathbb{Z}$

We know that if m is any integer, the set

$$m\mathbb{Z} = \{ mx \mid x \in \mathbb{Z} \}$$

is a subgroup of $\mathbb{Z}$.

Are there any other subgroups of $\mathbb{Z}$?

Recall

Well-ordering principle

Any non-empty set of positive integers has a smallest member.

Non-examples

1) Consider the set $\mathbb{R}$ of all real numbers. This has no smallest element.

2) Consider the set of all positive real numbers. It has a lower bound but no smallest element.

A small generalization.

Let $S \subseteq \mathbb{Z}$ be a non-empty subset that has a lower bound, i.e. there exists some $x_0 \in \mathbb{Z}$ such that $x \geq x_0 \ \forall \ x \in S$.

Then S has a smallest element.

Proof

Let $T = \{x - x_0 + 1 \mid x \in S\}$

Then T consists of positive integers. Also, T is non-empty. So, T has a smallest element z. Then $z = y - x_0 + 1$ for some $y \in S$.

We claim that y is the smallest element of S.

If not, suppose there exists some $x \in S$, $x < y$.

Then, $x - x_0 + 1 < y - x_0 + 1 = z$.

But $x - x_0 + 1 \in T$ and z is the smallest element of T. — contra.

Conclusion

So, the well-ordering principle applies to non-empty subsets of non-negative integers as well.

Division algorithm

Let $a, b \in \mathbb{Z}$, $b > 0$. Then, there exist unique integers q, r such that $a = bq + r$ and $0 \leq r < b$.

Warning Note the conditions on r carefully. We have $0 \leq r$ and $r < b$.

Proof

Consider the set

$S = \{ a - bm \mid m \in \mathbb{Z},\ a - bm \geq 0 \}$

We claim that S is non-empty.

Case 1 Suppose $a \geq 0$.

Then $a = a - b \cdot 0 \in S$.

Case 2 $a < 0$.

Then $a - b(2a) = a(1-2b)$.

As $b \geq 1$, $2b \geq 2$ and so $1-2b < 0$.

As $a < 0$, $a(1-2b) > 0$.

So $a - b(2a) \in S$.

So, in this case also, S is non-empty.

So, S has a smallest element, which we denote by r. As $r \in S$, there exists some $q \in \mathbb{Z}$ such that $a - bq = r$.

If $r \geqslant b$, $r - b \geqslant 0 \implies a - bq - b \geqslant 0$

But this means $a - b(q+1) \in S$.

But $a - b(q+1) < r$ — contra.

So, existence is proved

Uniqueness

Suppose we have two pairs (q_1, r_1) and (q_2, r_2) with the required property.

So, $a = b q_1 + r_1$ and

$$a = b q_2 + r_2.$$

If $r_1 = r_2$, then $b q_1 = b q_2 \Rightarrow q_1 = q_2$.

So, if possible, let $r_1 \neq r_2$.

Suppose $r_1 < r_2$. So $r_2 - r_1 > 0$

Then, $bq_1 - bq_2 = r_2 - r_1$.

So $b(q_1 - q_2) = r_2 - r_1$

As $b > 0$ and $r_2 - r_1 > 0$, we see that $q_1 - q_2 > 0$. So

$q_1 - q_2 \geq 1 \implies r_2 - r_1 = b(q_1 - q_2) \geq b$.

But $r_2 < b$ and $r_1 \geqslant 0$

So $r_2 - r_1 < b$ — contra.

So, $r_1 \neq r_2$ is impossible.

Thus, $r_1 = r_2$ and so $q_1 = q_2$.

This completes the proof.

Theorem Any subgroup H of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for some $m \geq 0$.

Proof Let H be a subgroup of $\mathbb{Z}$.

Let $S = \{x \mid x \in H, \; x > 0\}$.

<u>Case 1</u> Suppose $S = \phi$.

Thus, all elements of H are non-positive.

If $\exists\ x \in H$ such that $x < 0$, then $-x > 0$. But $-x \in H$

$\Rightarrow -x \in S$ — contra.

So, H has no negative elements.

So, $H = \{0\}$.

So, we can take $m = 0$.

<u>Case 2</u> Suppose $S \neq \phi$.

Then, S has a smallest element, which we denote by m. We claim that $H = m\mathbb{Z}$.

Indeed, suppose $x \in H$ is any element.

By division algorithm, $\exists\ q, r \in \mathbb{Z}$ such that $x = qm + r$, $0 \le r < m$.

Then, as $x \in H$ and $qm \in H$, $r = x - qm \in H$.

If $r > 0$, $r \in S$.

But $r < m$ and m is the smallest element of S. — contra.

So, $r = 0$.

Thus, $x = q \cdot m$. $\Rightarrow$ $x \in m\mathbb{Z}$

Thus, $H \subseteq m\mathbb{Z}$

But $m\mathbb{Z} \subseteq H$ $\Rightarrow$ $H = m\mathbb{Z}$.

This completes the proof. //

Cosets of subgroups of $\mathbb{Z}$

Let H be a subgroup of $\mathbb{Z}$.

Assume $H \neq \{0\}$.

Thus, there exists $m > 0$ such that $H = m\mathbb{Z}$.

Any coset of H is of the form $a + m\mathbb{Z}$, $a \in \mathbb{Z}$.

When is $a + m\mathbb{Z} = b + m\mathbb{Z}$.

$a+m\mathbb{Z} = b+m\mathbb{Z} \iff a \in b+m\mathbb{Z}$

$\iff a = b + md$ for some integer d

$\iff a-b = md$ for some integer d

$\iff m$ divides $a-b$.

Use division algorithm.

Let $q_1, r_1 \in \mathbb{Z}$ such that

$a = mq_1 + r_1$, $\quad 0 \leq r_1 < m$

and $q_2, r_2 \in \mathbb{Z}$ such that

$b = mq_2 + r_2$, $\quad 0 \leq r_2 < m$.

Then, $a - b = m(q_1 - q_2) + (r_1 - r_2)$

So m divides $a-b$

$\iff$ m divides $r_1 - r_2$.

If $r_1 > r_2$, $0 \leq r_1 - r_2 < m$ and so m cannot divide $r_1 - r_2$.

Similarly, if $r_2 > r_1$, $0 \leq r_2 - r_1 < m$ and so m cannot divide $r_2 - r_1$. So m cannot divide $r_1 - r_2 = -(r_2 - r_1)$.

So, m divides $r_1 - r_2 \iff r_1 = r_2$.

Thus, we have proved,

$\boxed{a + m\mathbb{Z} = b + m\mathbb{Z}$ if and only if a and b leave the same remainder when divided by m.$}$

So, the cosets of $m\mathbb{Z}$ are
$m\mathbb{Z}$, $1+m\mathbb{Z}$, $\ldots$, $(m-1)+m\mathbb{Z}$.
The collection of all these cosets is $\mathbb{Z}/m\mathbb{Z}$.
Note that, in this case, the left and right cosets are the same.

Example

$m = 5$ (Each column is a coset of $5\mathbb{Z}$)

-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$