Lecture 10

We have seen (Tutorial 2) that the intersection of two subgroups is a subgroup.

This is true for <u>any</u> collection of subgroups (even infinite collection).

Theorem Let G be a group. Let $\mathcal{S}$ be a set of subgroups of G. Then, the intersection of all subgroups in $\mathcal{S}$ is a subgroup of G.

Proof: Let $K = \bigcap_{H \in \mathcal{S}} H$.

Identity: $1_G \in H$ for all $H \in \mathcal{S}$

So $1_G \in \bigcap_{H \in \mathcal{S}} H = K$.

Closure under inverses:

Let $x \in K$. So, for any $H \in \mathcal{S}$, $x \in H$. As H is a subgroup, $x^{-1} \in H$.

Thus, $x^{-1} \in H$ for all $H \in \mathcal{S}$.

So $x^{-1} \in \bigcap_{H \in \mathcal{S}} H = K$.

Closure under the binary operation:

Let $x, y \in K$. We want to show that $xy \in K$.

For any $H \in \mathcal{S}$, we have $x, y \in H$. As H is a subgroup, this implies that $xy \in H$.

Thus, $xy \in H$ for all $H \in \mathcal{S}$.

So, $xy \in \bigcap_{H \in \mathcal{S}} H = K$.

Thus K is a subgroup. //

Subgroup generated by a set.

Let G be a group and let S be a subset of G.

We define $\langle S \rangle$ to be the intersection of all subgroups of G which contain S.

By the previous theorem, $\langle S \rangle$ is a subgroup of G.

If H is any subgroup of G which contains S, then $\langle S \rangle \subseteq H$. (Because $\langle S \rangle$ is the intersection of all such subgroups.)

Thus, $\langle S \rangle$ is the <u>smallest subgroup</u> containing S.

What does $\langle S \rangle$ look like?

Let M be the set of all elements of G which can be written in the form

$$x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r}$$

where

- r is a positive integer
- $x_1, x_2, \ldots x_r \in S$ (not necessarily distinct)

- $m_1, m_2, \cdots, m_r \in \mathbb{Z}$

It is easy to set that M is a subgroup of G.

<u>Exercise</u> Write a proof of this statement.

Also, if H is any subgroup of G containing S, H contains every element of the form $x_1^{m_1} \cdot \ldots \cdot x_r^{m_r}$ where $x_1, x_2 \ldots x_r \in S$.

Thus $M \subseteq H$ for any such subgroup H.

Thus, $M \subseteq \langle S \rangle$ (as $\langle S \rangle$ is the intersection of such subgroups).

However, M is a subgroup containing S. So $\langle S \rangle \subseteq M$.

So, $M = \langle S \rangle$.

For example, if $S = \{a\}$,

$$\langle S \rangle = \langle a \rangle = \{1, a, a^{-1}, a^2, a^{-2}, \cdots\}$$
$$= \{a^n \mid n \in \mathbb{Z}\}$$

If $S = \{a, b\}$, $\langle S \rangle$ is the set of elements of all products of the form $a^{m_1} b^{n_1} a^{m_2} b^{n_2} \cdots a^{m_r} b^{m_r}$ where r is a positive integer and $m_i, n_i \in \mathbb{Z}$ for all i.

So, a typical element may look like $a^2 b^{-3} a b^{-2}$.

Note that we may not be able to collect all the a's and b's together <u>in general</u>. In special cases we may be able to do so.

For example, in the dihedral group D_n, we have the relation $\tau\rho = \rho^{-1}\tau$ which allows us to rewrite every expression in the form $\rho^m\tau^n$.

An even simpler situation arises if $ab = ba$, i.e. a and b commute.

In that case any element of the form $a^{m_1} b^{n_1} \cdots a^{m_r} b^{n_r}$ can be written as $a^{m_1+m_2+\cdots+m_r} b^{n_1+n_2\cdots+n_r}$

__Definition__ A group G is said to be __commutative__ or __abelian__ if for any $x, y \in G$, we have $xy = yx$.

__Example__: $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ are abelian.

D_n is not abelian for any $n \geq 3$.

Exercise: Prove the following.

Theorem Let $(G, +)$ be an abelian group. Let $S \subseteq G$. Then $\langle S \rangle$ is equal to the set of all elements of the form $n_1 x_1 + n_2 x_2 + \cdots + n_r x_r$ where $x_1, x_2, \ldots, x_r \in G$ and $n_1, n_2, \ldots, n_r \in \mathbb{Z}$.

Example:

Consider the group $(\mathbb{Z}, +)$.

Let $a, b \in \mathbb{Z}$.

Then

$\langle a, b \rangle = \{am + bn \mid m, n \in \mathbb{Z}\}$.

But $\langle a, b \rangle$ is a subgroup of $\mathbb{Z}$. So $\langle a, b \rangle = \langle d \rangle$ for some $d \geq 0$.

What is the relation between d and the pair $\{a, b\}$?

$a \in \langle a, b \rangle = \langle d \rangle \implies d \mid a.$

Similarly, $d \mid b.$

Let $g = \gcd(a,b)$. Then, $d \mid g.$

But $g \mid a$ and $g \mid b \implies g \mid am+bn$

for <u>all</u> $m, n \in \mathbb{Z}.$

As $d \in \langle a, b \rangle$, there exist integers r, s such that $d = ar + bs$.

So $g \mid ar + bs = d$.

So, $d \mid g$ and $g \mid d$. As $g \geqslant 0$ and $d \geqslant 0$, we see that $d = g$.

So, we have proved:

Theorem Let a, b be two integers. Then, there exist integers r, s such that

$$\gcd(a,b) = ar + bs.$$

Question: How do we find these integers r, s? (Next lecture.)

Cyclic groups

A group G is said to be **cyclic** if there exists an element $a \in G$ such that $G = \langle a \rangle$.

Example: $\mathbb{Z}$ is cyclic.

$\mathbb{Z}/m\mathbb{Z}$ is cyclic for any $m > 0$.

Structure of cyclic groups

Let G be a cyclic group.

Suppose $G = \langle a \rangle$.

We have two possibilities:

- $\mathrm{ord}(a)$ is not finite.
- $\mathrm{ord}(a)$ is finite.

Case 1: ord(a) is not finite

This means that there does not exist any positive integer m such that $a^m = 1$.

Consider the sequence (extending in both directions):

$$\ldots\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\ldots$$

We claim that all these elements are distinct.

In other words, we claim that if i, j are <u>distinct</u> integers, then $a^i \neq a^j$.

Suppose this is not true.

Then, there exist integers i, j such that $i < j$ and $a^i = a^j$.

Then $a^{j-i} = 1$.

As $j-i > 0$, this contradicts our assumption that $\mathrm{ord}(a)$ is not finite.

Let $\varphi : \mathbb{Z} \to G$ be the function defined by $\varphi(n) = a^n$.

We have proved above that φ is a one-to-one function.

φ is onto as $G = \langle a \rangle$.

Thus, φ is a 1-1 correspondence.

Also, $\varphi(m+n) = a^{m+n}$

$$= a^m \cdot a^n$$

$$= \varphi(m) \cdot \varphi(n).$$

Thus, φ is a group isomorphism.

Case 2: $\mathrm{ord}(a) = m$ for some $m \in \mathbb{Z}$

Lemma: Suppose $a^n = 1$ for some integer n. Then, $m \mid n$.

Proof: Using the division algorithm, we write $n = mq + r$ where $0 \leq r < m$.

Then $1 = a^n = a^{mq+r} = (a^m)^q \cdot a^r$

$$= 1 \cdot a^r = a^r.$$

But $r < m$, so $a^r = 1$ is impossible unless $r = 0$. This completes the proof.

Suppose i and j are distinct integers such that $a^i = a^j$. Then $a^{i-j} = 1$. So $m \mid i-j$, i.e. $i \equiv j \pmod{m}$.

Conversely, if $i \equiv j \pmod{m}$

then $i = j + mx$ for some $x \in \mathbb{Z}$.

So $a^i = a^{mx+j}$

$= (a^m)^x \cdot a^j = a^j$.

$\boxed{\text{Thus } a^i = a^j \text{ if and only if } i \text{ and } j \text{ lie in the same coset of } m\mathbb{Z}.}$

We define

$\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \langle a \rangle$ by

$\varphi(\overline{n}) = a^n.$

This is well-defined because if $\overline{n_1} = \overline{n_2}$, then $n_1 \equiv n_2 \pmod{m}$ and so $a^{n_1} = a^{n_2}.$

Also, if $\varphi(\overline{n_1}) = \varphi(\overline{n_2})$, we have seen that $n_1 \equiv n_2 \pmod m$, i.e. $\overline{n_1} = \overline{n_2}$.

So φ is a one-to-one function.

φ is also onto: Indeed, for any $n \in \mathbb{Z}$, $\varphi(\overline{n}) = a^n$.

Thus φ is a 1-1 correspondence.

$$\varphi(\bar{n}_1 + \bar{n}_2) = a^{n_1+n_2}$$
$$= a^{n_1} \cdot a^{n_2}$$
$$= \varphi(\bar{n}_1) \cdot \varphi(\bar{n}_2)$$

Thus, φ is a group isomorphism.

Summary

Let $G = \langle a \rangle$.

- If $\mathrm{ord}(a)$ is not finite G is isomorphic to $\mathbb{Z}$.
- If $\mathrm{ord}(a) = m$, $m \in \mathbb{Z}$, then G is isomorphic to $\mathbb{Z}/m\mathbb{Z}$