Lecture 7

Recall:

Let G be a finite group.

Let x be an element of G, $x \neq 1$. Let $d = \text{ord}(x)$.

Thus $\langle x \rangle = \{1, x, \dots\dots, x^{d-1}\}$.

Suppose $G \neq \langle x \rangle$.

$\exists$ means "there exists"

Thus $\exists\, y \in G$ such that $y \notin \langle x \rangle$.
Then, we saw that the elements $y, yx, \ldots, yx^{d-1}$ are all distinct. Also, if we denote the set $\{y, yx, \ldots, yx^{d-1}\}$ by $y\langle x \rangle$, then $\langle x \rangle \cap y\langle x \rangle = \phi$

ϕ is the symbol for the empty set.

If z is such that $z \notin \langle x \rangle$ and $z \notin y\langle x \rangle$, then the elements $z, zx, \ldots, zx^{d-1}$ are all distinct. Also, if $z\langle x \rangle = \{z, zx, \ldots, zx^{d-1}\}$, then $\langle x \rangle \cap z\langle x \rangle = \phi$ and $y\langle x \rangle \cap z\langle x \rangle = \phi$.

And so on....

... until we run out of group elements.

Now let us write all this more formally.

Notation

Let G be a group and S be any subset of G. Let $y \in G$ be some element. We define yS to be the set of all elements of the form yx, where $x \in S$.

$yS = \{ yx \mid x \in S \}$
Note that if s_1, s_2 are distinct elements of S, then $ys_1 \neq ys_2$.
Indeed, if $ys_1 = ys_2$, then by cancelling y, we get $s_1 = s_2$ — contradiction.

Thus, the function $\varphi : S \longrightarrow yS$ defined by $\varphi(s) = ys$ for $s \in S$, is a one-to-one function.

<u>φ is also onto:</u>

Any element of yS is of the form ys for some $s \in S$.

So $\varphi(s) = ys$

Thus, the function φ gives a <u>bijection</u> from S to yS.

This explains why the elements $y, yx, \ldots, yx^{d-1}$ were all distinct.

Disjointness arguments

Suppose y, z are two elements of G. When can we say that $y\langle x\rangle \cap z\langle x\rangle = \phi$?

Suppose $y\langle x\rangle \cap z\langle x\rangle \neq \phi$.
Then, $yx^i = zx^j$ for some i and j. So $z = yx^{i-j}$.

But $yx^{i-j} \in y\langle x \rangle$.

So we see that $z \in y\langle x \rangle$.

So, we conclude the following:

$\boxed{\text{If } z \notin y\langle x\rangle \text{, then the sets } y\langle x\rangle \text{ and } z\langle x\rangle \text{ are disjoint.}}$

This explains why the sets $\langle x \rangle$, $y\langle x \rangle$, $z\langle x \rangle$, etc. were disjoint.

Suppose $y\langle x \rangle \cap z\langle x \rangle \neq \phi$.
Then we saw that $z = yx^r$ for some r.

Let us look at elements of $z\langle x\rangle$.

$z x^i = y x^r \cdot x^i = y x^{r+i} \in y\langle x\rangle$

So $z\langle x\rangle \subseteq y\langle x\rangle$.

But we also have $y = z \cdot x^{-r}$

So $y x^i = z x^{-r} \cdot x^i = z x^{i-r} \in z\langle x\rangle$.

So $y\langle x\rangle \subseteq z\langle x\rangle$.

So, we see that $y\langle x\rangle = z\langle x\rangle$.

Thus, we have proved that for any two elements y, z in G, we have either

$$y\langle x\rangle \cap z\langle x\rangle = \phi$$

OR

$$y\langle x\rangle = z\langle x\rangle$$

Observe

We did not use the assumption that $\text{ord}(x)$ is finite. So, our conclusion holds for any x.

So, what properties of the set $\langle x \rangle$ did we really use?

We used two properties:

(1) A product of two powers of x is a power of x.

(2) The inverse of a power of x is a power of x.

But any subgroup has such properties, not just $\langle x \rangle$.

Cosets

Let H be a subgroup of G.
If g is any element of G,
the set

$$gH = \{gh \mid h \in H\}$$

is called a <u>left coset</u> of H.

Similarly, the set $Hg = \{hg \mid h \in H\}$ is called a <u>right coset</u> of H.

Proposition Let G be a group and let H be a subgroup of G. Then, given two left cosets g_1H and g_2H of H, either $g_1H \cap g_2H = \emptyset$ OR $g_1H = g_2H$.

Proof Suppose $g_1 H \cap g_2 H \neq \emptyset$.

Then, $g_1 h_1 = g_2 h_2$ for some h_1, h_2 in H.

So $g_1 = g_2 h_2 h_1^{-1}$

Then, for any $h \in H$, we have $g_1 h = g_2 (h_2 h_1^{-1} h) \in g_2 H$.

So $g_1 H \subseteq g_2 H$.

Similarly, $g_2 = g_1 h_1 h_2^{-1}$.

So, for any $h \in H$,

$g_2 h = g_1 (h_1 h_2^{-1} h) \in g_1 H$.

So $g_2 H \subseteq g_1 H$.

So $g_1 H = g_2 H$.

//

Notation

The set of all left cosets of H is denoted by G/H.

So

$$G/H = \{H, aH, bH, cH, \dots\}$$

The set of all right cosets of H is denoted by $H \backslash G$.

Note that every element g of G is contained in some left coset of H, namely gH.

So, the union of all left cosets of H is G.

So, we observe the following:

(1) The union of all left cosets of H is G.

(2) Two distinct left cosets do not intersect.

So, the left cosets of H give a <u>partition</u> of G.

Cardinality of cosets

We saw earlier that there is a 1-1 correspondence from H to gH for any $g \in G$. So, if H is finite, we see that $\boxed{|gH| = |H|}$ for any $g \in G$.

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

Proof As G is a finite set, the set G/H is also finite.

G is the union of all the left cosets of H. Any two distinct cosets are disjoint.

For any coset gH, we have $|gH| = |H|$.

So $|G| = |G/H| \cdot |H|$.

So $|H|$ divides $|G|$.

//

Corollary Let G be a finite group. Then, for any $x \in G$, $\mathrm{ord}(x)$ divides $|G|$.

Proof: Apply the theorem with $H = \langle x \rangle$. //