Advance GROUP THEORY NOTES

FOR 3 days

Note: Don't confuse **distinct** with disjoint.

Thm 5.43: If G is a p-group having a unique subgroup of order p and more that one cyclic subgroup of index p, then $G \cong Q$, the quaternions.

Proof: If A is a subgp. of G of index p, then $A \trianglelefteq G$, by Theorem 5.39. Thus, if $x \in G$, then $xA \in G/A$, a group of order p, and so $x^p \in A$. Let $A = \langle a \rangle$ and $B = \langle b \rangle$ be two distinct subgps of index p, and let $D = A \cap B$.

As mentioned above, $A, B \trianglelefteq G$, ~~def~~ then D, which is the intersection of two normal subgps, is normal in G.

The underlined portion shows that the subset,

$$G^p = \{x^p : x \in G\}$$

is contained in A as well as B. Therefore

$G^p \subseteq A \cap B = D$. ......(1)

Since A and B are two dintict maximal subgroups, we claim the following result, Claim 1: $G = AB$.

As $A, B \trianglelefteq G \Rightarrow AB \leq G$.

Enough to show that: $|G| = |AB|$.

As A and B are distinct so there exist an element, $x \neq e$, such that $x \in A$ but $x \notin B$.

As $A \leq G$ and G is a p-group, so $|A| \mid |G|$ and therefore A will also be a p-group.

~~Now $p \mid |A|$, and using Cauchy's theorem we know that A has an element of order p~~

Now, we know, using Lagrange's theorem, that

$o(x) \mid |A|$ & $o(x) \neq 1$

$\Rightarrow o(x) \geq p$

Now cosider the cyclic group generated by x namely $\langle x \rangle$.

Using the argument above we have that,

$$|\langle x \rangle| = o(x) \geq p$$

Since A is cyclic, it follows that every subgroup of A is normal, and so $\langle x \rangle$ is normal in A.

This is unnecessary

Consider, the set,

$$\langle x \rangle B \subseteq AB.$$

The last inclusion is evident as $\langle x \rangle \subset A$.

We thus have,

$$|\langle x \rangle B| \leq |AB| \quad \text{.....(i)}$$

but $|\langle x \rangle B| = \dfrac{|\langle x \rangle| \, |B|}{|\langle x \rangle \cap B|}$

As $x \notin B \Rightarrow \langle x \rangle \notin B$ so,

$$|\langle x \rangle B| = |\langle x \rangle| \, |B| = |\langle x \rangle| \cdot \frac{|G|}{p} \geq |G| \quad \text{---(ii)}$$

(because $|\langle x \rangle| \geq p$)

Equations (i)&(ii) gives us,

$$|AB| \geq |\langle x \rangle B| \geq |G|$$

Because $AB \leq G$, we can not have that $|AB| > |G|$, therefore,

$$|AB| = |G|$$

and this ~~will~~ proves our claim. Hence $G = AB$.

Using the formula for the order of product of two subgroups,

$$|G| = |AB| = \frac{|A| \, |B|}{|A \cap B|} = \frac{|G|}{p} \cdot \frac{|G|}{p \cdot |A \cap B|}$$

(A and B were index p subgroups)

$$\Rightarrow \frac{|G|}{|A \cap B|} = p^2 \Rightarrow [G : A \cap B] = p^2$$

Hence, $|G/D| = \frac{|G|}{|A \cap B|} = p^2$, making G/D an abelian group.

As G/D is abelian; by one of the theorems proved, in connection with commutator subgroup, in class we have ~~tell us~~ that $G' \leq D$.

As $G = AB$, each $g \in G$ is a product of xy, where $x \in A$ & $y \in B$. Since $A = \langle a \rangle$ and $B = \langle b \rangle$, it gives us that $x = a^r$ & $y = b^s$ so $g = a^r b^s$; but every element of D is simultaneously a power of a and a power of b, and so it commutes with each $x \in G$. How?

Lets see. Take any $\alpha \in D \Rightarrow \alpha \in A$ & $\alpha \in B$.

$\Rightarrow \alpha = a^m = b^n$

$\Rightarrow a'\alpha = \alpha a'$ and $b'\alpha = \alpha b'$ $\forall a' \in A$ and $\forall b' \in B$.

If $g \in G$ then $g = a^r b^s$, where $a^r \in A$ and $b^r \in B$

Take an arbitrary elt. of D and call it α'

$\alpha' g = \alpha' a^r b^s = a^r \alpha' b^s = a^r b^s \alpha' = g\alpha'$ $\forall g \in G$.

(as $a^r \in A$ and $b^r \in B$)

This shows that,

Every elt. of D commutes with every elt. of G resulting in following: $D \leq Z(G)$. Hence,

$G' \leq D \leq Z(G)$ (first inclusion is already proved)

$\Rightarrow G' \leq Z(G) \Rightarrow$ if $[x,y] \in G'$ then $[x,y] \in Z(G)$.

Therefore if $[x,y] \in G'$ then

$[x,y]$ commutes with every elt. of G.

Now using lemma 5.42 (if you have written it as 5.41 then make the correction) we have,

$[y,x]^p = [y^p, x]$. But ~~using~~ the underlined result on page 1 gives us that $y^p \in D \leq Z(G)$ ---(*)

and therefore $y^p g = g y^p \quad \forall g \in G$.

Hence,

$[y,x]^p = [y^p, x] = y^p x y^{-p} x^{-1} = 1$ (using *)

Again using lemma 5.42, but this time the second part, we have,

$(xy)^p = [y,x]^{p(p-1)/2} x^p y^p$.

As p is prime so there are only two possibilities, either $p=2$ or p is odd.

We'll start with the second case. Assume that p is odd then p divides $p(p-1)/2$, ~~and~~ therefore

$(xy)^p = ([y,x]^p)^{p-1/2} x^p y^p = x^p y^p$

(as $[y,x]^p = 1$)

Exercise: Let G be a finite group such that, for some fixed integer $n>1$, $(xy)^n = x^n y^n$, $\forall x, y \in G$. If $G[n] = \{z \in G \mid z^n = 1\}$ and $G^n = \{x^n \mid x \in G\}$, then both $G[n]$ and G^n are normal subgps of G and

$$|G^n| = [G : G[n]].$$

Proof will be given later.

As we already have that, for p odd prime,

$$(xy)^p = x^p y^p \quad , \quad \forall x, y \in G$$

so we can use the above exercise.

If $G[p] = \{x \in G \mid x^p = 1\}$ and $G^p = \{x^p \mid x \in G\}$, then using the exercise (above) we have that both these subsets are normal subgroups and

$[G : G[p]] = |G^p|$. Thus,

$$|G[p]| = [G : G^p] = [G : D][D : G^p] \geq p^2$$

(because $[G : D] = p^2$ & $[D : G^p] \geq 1$).

Since $G[p] \leq G \Rightarrow |G[p]| \mid |G|$

$\Rightarrow G[p]$ is a p-group

Now we know that if H is a p-group with order p^n then for every $r \leq n$, H contains a subgp. of order p^r. (This comes from the theory of p-group. In case you don't understant refer to the section of p-gp. in Rotman's book)

As $G[p]$ is a p-group with order $\geq p^2$, so using the argument just stated we conclude that $G[p]$ contains a subgroup of order p^2, call it E. Since E is abelian and $E \leq G[p]$ we conclude that E is elementary abelian. (because $E \leq G[p] = \{x \mid x^p = 1\}$)

So all elts. except identity in E have order p, implying that E contains more that one subgroup of order p. (If $a', b' \in E$ then $\langle a' \rangle, \langle b' \rangle \leq E$ of order p)

This ~~Which~~ contradicts the assumption of the theorem, hence p can not be an odd prime.

Therefore, $p = 2$.

When $p=2$, the commutator identity gives,

$$(xy)^4 = [y,x]^6 x^4 y^4 \quad , \quad \forall x, y \in G.$$

As $p=2$, so $[y,x]^2 = 1$ (we saw that $[y,x]^p = 1$).

$\Rightarrow [y,x]^6 = 1$

Hence,

$$(xy)^4 = x^4 y^4 \quad \forall x, y \in G.$$

using the exercise again we have that,

$$|G[4]| = [G:G^4] = [G:D][D:G^4] = 4[D:G^4] \quad \cdots (2)$$

(as $[G:D] = p^2$ and $p=2$, is concluded)

Now $A/D = A/A\cap B \cong AB/B = G/B$, for A and B are distinct maximal subgps. of G. Because $p=2$, so A & B are index 2 subgps of G. Hence

$$[A:D] = [G:B] = 2.$$

<u>Result:</u> Cyclic groups have a unique subgp. of any order).

As $[G:D] = 2^2 \Rightarrow |D| = \frac{|G|}{2^2} = \frac{|G|}{4}$ ... (iii)

Also $A = \langle a \rangle$ and A is an index 2 subgroup.

This means that $o(a) = |\langle a \rangle| = |A| = \frac{|G|}{2}$,

which implies that

$$o(a^2) = \frac{o(a)}{2} = \frac{|G|}{4} \quad \text{(iv)}$$ (First equality is an easy ex.)

using (iii) & (iv) we see that, A has two subgroups of order $\frac{|G|}{4}$ but due to the result mentioned above, this is not possible.

So, $D = \langle a^2 \rangle$

Using eq (1) on page 1 we have that

$$G^2 \leq \langle a \rangle \cap \langle b \rangle = D = \langle a^2 \rangle, \text{ so}$$

$G^4 \leq \langle a^4 \rangle$ and we can also notice that

$\langle a^4 \rangle \leq G^4$

Let $t \in \langle a^4 \rangle \Rightarrow t = a^{4t_1} = (a^{t_1})^4 \in G^4$

This implies that, $\langle a^4 \rangle \leq G^4$

Combining the previous two observations we have,

$G^4 = \langle a^4 \rangle$.

Hence, $[D : G^4] = |\langle a^2 \rangle : \langle a^4 \rangle| = 2$

Using eq (2) on page 7 we have,

$|G[4]| = 4\,[D : G^4] = 8$.

This implies that $G[4] \cong \mathbf{Q}$ (the quaternion group)

Reason: There are five groups of order 8 and no other group except $\mathbf{Q}$ has 7 elts. of order 4.
Also it has a unique subgp. of order 2.

Claim: $a^4 = 1$

Let us assume that $a^4 \neq 1$, then

$D = \langle a^2 \rangle$ has order ≥ 4 $(O(a^2) \mid |G| \} = p^n)$
call is $\langle u \rangle$ and $\langle u \rangle \leq D$

As subgp. of a cyclic group is cyclic, $\langle u \rangle$ is cyclic. Off course

$\langle u \rangle \leq G[4]$ (as forall $x' \in \langle u \rangle$, $(x')^4 = e$)

Take an element v of $G[4]$ different from u, then

$\langle v \rangle \leq G[4] \cong \mathbf{Q}$. Since $\langle u \rangle \leq D \leq Z(G)$, the group $H = \langle u \rangle \langle v \rangle$ is abelian. (every elt. of $\langle u \rangle$ commutes with every elts. of G)

Also $H \leq G[4]$ $\{$ as $\langle u \rangle$ and $\langle v \rangle$ are subgroup of $G[4]$ and $\langle u \rangle$ is normal in $G[4]$ as it is of index 2 $\}$

Because $u \neq v$ we notice that

$$|\langle u\rangle \cap \langle v\rangle| \leq 2 \quad \text{(exercise)}$$

This means,

$$|H| = \frac{|\langle v\rangle||\langle u\rangle|}{|\langle u\rangle \cap \langle v\rangle|} \geq 8 = |G[4]|$$

$\Rightarrow$ $H = G[4]$

Not possible as H is abelian but $G[4]$ is non-abelian.

Hence a contradiction. This means $a^4 = 1$.

Thus $|D| = |\langle a^2\rangle| = 2$, and

$$[G:D] = 4$$

implies, $|G| = 4|D| = 8$

~~Therefore~~ As $G[4] \leq G$ and $|G| = |G[4]|$

We have that

$$G = G[4] \cong Q$$