Group Theory

Lecture 11, Sunday January 8, 2023

Ari Feiglin

11.1 p-groups

Notice that if we focus on the conjugate group action and we take I to be a set of representatives of each orbit, then

$$G = \dot{\bigcup_{x\in I}} \operatorname{conj}(x)$$

since the orbits partition the set being acted on (G in this case). Notice that $x \in G$ has an orbit of length 1 if and only if for every $g \in G$ we have $gxg^{-1} = x$ that is $gx = xg$ for all $g \in G$, which is equivalent to $x \in Z(G)$. If we define I' to be the set of representatives of orbits of length larger than 1, we can write the above union as

$$G = \dot{\bigcup_{x\in Z(G)}} G\cdot x \,\dot\cup\, \dot{\bigcup_{x\in I'}} \operatorname{conj}(x) = Z(G) \,\dot\cup\, \dot{\bigcup_{x\in I'}} \operatorname{conj}(x)$$

Using the orbit-stabilizer theorem this means:

$$|G| = |Z(G)| + \sum_{x\in I'} [G : C_G(x)]$$

We summarize this result in the following lemma:

Lemma 11.1.1:

If we define I' to be a set of representatives of orbits of size larger than 1 then:

$$|G| = |Z(G)| + \sum_{x\in I'} [G : C_G(x)]$$

Theorem 11.1.2 (Cauchy's Theorem):

If G is a group whose order is divisible by a prime p, G has an element of order p.

Proof:

If G is abelian then suppose $e \neq g \in G$ let $m = o(g)$. If p divides m then $g^{\frac{m}{p}}$ has order p as required. Else take ${}^{G}\!/\!_{\langle g\rangle}$ which has order $\frac{|G|}{m}$ which must be divisible by p since m is not. Then inductively there must be $h\langle g\rangle \in {}^{G}\!/\!_{\langle g\rangle}$ with order p, so $h^p \in \langle g\rangle$ and therefore the order of h is divisible by p and by above there must be such an element.
If G is not abelian, if $Z(G)$'s order is divisble by p we are finished (since it is abelian). Otherwise there is an $x \notin Z(G)$ such that $p \nmid [G : C_G(x)]$ (since otherwise since the order of G is the sum of the order of $Z(G)$, which is not divisible by p, and the indexes of $C_G(x)$s, which if they are all divisible by p then G cannot be since $Z(G)$ isn't). So p must divide the order of $C_G(x)$, and since $C_G(x) < G$ inductively it has an element of order p.

■

Definition 11.1.3:

A p-group for a prime p is a group where every element's order is a power of p.

Notice that if G is finite, it is a p-group if and only if its order is a power of p. If it is a p group suppose it is divisible by some other prime q, then by Cauchy's theorem it has an element of order q which is a contradiction. And by Lagrange if its order is p then every element must have an order of a power of p.

Definition 11.1.4:

Suppose $\{G_\lambda\}_{\lambda\in\Lambda}$ are sets, then we define the **direct product** and **direct sum** of these sets:

$$\prod_{\lambda\in\Lambda} G_\lambda = \{f\colon \Lambda \longrightarrow \Lambda \mid \forall\lambda\in\Lambda : f(\lambda)\in G_\lambda\}$$

$$\sum_{\lambda\in\Lambda} G_\lambda = \left\{ f\in\prod_{\lambda\in\Lambda} G_\lambda \;\middle|\; f(\lambda) = e_{G_\lambda} \text{ except for a finite number of cases}\right\}$$

Notice that the direct sum and product are non-trivial by the axiom of choice. This is not required if these sets are groups (choose $f(\lambda) = e_{G_\lambda}$). Notice that if these sets are groups then the sum and products are groups themselves under the operation $(f\cdot g)(\lambda) = f(\lambda)\cdot g(\lambda)$.

Proposition 11.1.5:

If P is a p-group acting on X then

$$\mathrm{FP}(X) \equiv |X| \pmod p$$

Proof:

Every cycle must divide the order of P and therefore every other cycle (which is not a fixed cycle) is a non-trivial power of p and is therefore equivalent to 0 modulo p. And since the order of X is the sum of the order of its cycles, this means it is equivalent to the sum of the order of its fixed cycles modulo p, which is equal to $\mathrm{FP}(X)$.

$\blacksquare$

Proposition 11.1.6:

The center of a finite p-group is non-trivial.

Proof:

Let P act on itself through conjugation then since the set of fixed points are $Z(P)$ then

$$|Z(P)| \equiv |P| \equiv 0 \pmod p$$

So $|Z(P)| \neq 1$ and is therefore not trivial.

$\blacksquare$

Proposition 11.1.7:

Every group of order p^2 is abelian.

Proof:

Such a group is a p-group. If P is not abelian, then $\{e\} \neq Z(P) \subset P$, and therefore $|Z(P)| = p$, and therefore $\left|{}^{P}\!/_{Z(P)}\right| = p$ and therefore is cyclic and therefore P is abelian in contradiction.

$\blacksquare$

Theorem 11.1.8:

Suppose P is a finite p-group and $H < P$ then H is a proper subset of its normalizer.

Proof:

We have H act on the set of left cosets of H via $h\cdot(gH) = (hg)H$. We suppose H is a non-trivial subgroup (the case where H is trivial is trivial), and thus its order is a non-trivial power of p. We know that H is necessarily a p-group and therefore

$$\mathrm{FP}(H) \equiv |H| \pmod p \implies \mathrm{FP}(H) \equiv 0 \pmod p$$

Since H is a fixed point in this action, $\mathrm{FP}(f) \geq 1$ so there must be some other fixed point gH for $g \notin H$. So for all $h \in H$ $hgH = gH$ and therefore $g^{-1}Hg \leq H$ as $g^{-1}hg = g^{-1}gh' = h' \in H$ and therefore g is in the normalizer of H but not H.

■

11.2 Sylow's Theorems

Definition 11.2.1:

We use the notation $a^n \parallel b$ to mean a^n is the maximal power of a which divides b. That is $a^n \mid b$ but $a^{n+1} \nmid b$.

Definition 11.2.2:

Suppose G is a group whose group is divisible by a prime p, $P \leq G$ is a p-Sylow subgroup of G if it is a p-group whose index is coprime to p.

Theorem 11.2.3:

If G is a finite group of order divisible by p then it has a p-Sylow group of order $p^t \parallel |G|$.

Proof:

Suppose $p^t \parallel |G|$. Then by Cauchy's theorem there must be an element g of G of order p, then $p^{t-1} \parallel \left| {}^{G}/_{\langle g\rangle} \right|$, by induction there is a p-Sylow subgroup of the form ${}^{P}/_{\langle g\rangle}$ of order p^{t-1}. Then P must be a p-Sylow subgroup of G (since it has order p^t).
If G is not abelian and $p \mid |Z(G)|$ then there is an element $g \in G$ of order p, and the proof continues as above. Otherwise there is $x \notin Z(G)$ (since the order of G is equal to the sum of $Z(G)$ and the centers) such that $p \nmid [G : C_G(x)]$ and therefore $p^t \parallel C_G(x)$ which is an abelian subgroup of G and therefore contains a p-Sylow group of order $p^t \parallel |G|$ by the previous paragraph.

■

If $A, B \leq G$ and $B \subseteq N_G(A)$, then $AB = BA$ since for all $b \in B$, $b \in N_G(A)$ so $bAb^{-1} = A$ and therefore $bA = Ab$ for all $b \in B$ so $AB = BA$. And further, $A \trianglelefteq AB$ since $abAb^{-1}a^{-1} = aAa^{-1} = A$. And by the isomorphism theorems

$${}^{AB}/_{A} \cong {}^{B}/_{A\cap B} \implies |AB| = \frac{|A| \cdot |B|}{|A \cap B|}$$

Such a B is said to *normalize* A (if $B \subseteq N_G(A)$, that is $bAb^{-1} = A$ for every $b \in B$).

Lemma 11.2.4:

Suppose P is a p-Sylow subgroup of G and Q is some p-subgroup of G. If Q normalizes P then $Q \subseteq P$, that is $Q \subseteq N_G(P)$ means $Q \subseteq P$.

Proof:

The order of $|PQ|$ must be a power of p since this is true for $|P|$, $|Q|$, and $|P \cap Q|$, and so PQ is a p-group. Since P is a p-Sylow group it is a maximal p-group, and so $Q \subseteq PQ = P$ as required.

■

Theorem 11.2.5 (Sylow's Second Theorem):

All p-Sylow subgroups are conjugates.

Theorem 11.2.6 (Sylow's Third Theorem):

The number of p-Sylow subgroups is equivalent to 1 modulo p.

We will prove both theorems simultaneously.

Proof:

Let Ω be the set of all p-Sylow subgroups of G, by the first Sylow Theorem, Ω is nonempty (we assume p divides the order of G). G acts on Ω through conjugation. Let $P \in \Omega$, and P also acts on Ω through conjugation and the set of all fixed points are the set of p-Sylow groups Q such that P normalizes Q ($pQp^{-1} = Q$). And so $Q \subseteq P$ and by symmetry $P \subseteq Q$ and so $P = Q$. And so the set of all fixed points includes only P (since P is trivially a fixed point), and since for p-groups $\mathrm{FP}(X) \equiv |X| \pmod p$ we have that

$$|\Omega| \equiv 1 \pmod p$$

which proves the third Sylow Theorem.
Suppose for the sake of contradiction that G's action on Ω is not transitive (there is more than one orbit). Let Ω_0 be one orbit in Ω, then there is a $Q \notin \Omega_0$ which acts on Ω_0 by conjugation which it inherits from G (therefore it is well-defined). But since $Q \notin \Omega_0$ then the action cannot have any fixed points because as explained above the only fixed point would be Q itself which is not in Ω_0. So there are 0 fixed points and therefore:

$$|\Omega_0| \equiv 0 \pmod p$$

But there is a $P \in \Omega_0$ which acts on Ω_0 via conjugation and has a single fixed point itself so

$$|\Omega_0| \equiv 1 \pmod p$$

in contradiction.
So the conjugation of G on Ω must have a single orbit and therefore all p-Sylow subgroups are conjugates.

■

Theorem 11.2.7:

Every p-subgroup is contained within a p-Sylow subgroup.

Proof:

Let Q be some p-subgroup of G then it acts on Ω, and we know $\mathrm{FP}(\Omega) \equiv |\Omega| \equiv 1 \pmod p$, and therefore $\mathrm{FP}(\Omega) \neq \varnothing$. And if $P \in \mathrm{FP}(\Omega)$ then Q normalizes P and is therefore contained in it.

■