Categorical Sylow

1 Basic Category Theory

Skipped. We take our categories to be locally small. Most notably, the equation

$$(f \circ g) \circ h = f \circ (g \circ h)$$

is well defined as written.

2 Two Isomorphic Categories and its Consequences

2.1 The Two Categories

Let G be a group. We define two isomorphic categories. The first Ω_G is the category of subgroups ordered by inclusion. The second $\mathcal{C}$ is the category of isomorphism types of based transitive G-sets. The morphisms are, of course, based G-set morphisms. Let us define two functors which will give us the desired isomorphism. Define

$$\Omega_G \to \mathcal{C}$$

$$H \mapsto G/H$$

where the G-action is left multiplication and the basepoint is H. Next define

$$\mathcal{C} \to \Omega_G$$

$$(X, x_o) \mapsto \mathrm{Stab}_{x_o}$$

Let's first check functoriality of the first mapping. Let $K \subset H$ be subgroups of G, then we get a natural surjective map $G/K \to G/H$ by some slightly more generalized version of first isomorphism theorem showing functorality. Associativity and identity is clear. For functorality of the second mapping, let $\phi : (X, x_o) \to (Y, y_o)$ be a based G-set homomorphism. In this diagram we get the following squares which commute in the first component

$$\begin{array}{ccc} (X, x_o) & \xrightarrow{\phi} & (Y, y_o) \\ {\scriptstyle g}\downarrow & & {\scriptstyle g}\downarrow \\ (X, x_o) & \xrightarrow{\phi} & (Y, y_o) \end{array}$$

If we assume that $g \in \text{Stab}x_o$, this diagram becomes a commutative diagrams of pairs since

$$y_o = \phi(g \cdot x_o) = g \cdot \phi(x_o) = g \cdot y_o$$

This gives us an inclusion $\text{Stab}_{x_o} \subset \text{Stab}_{y_o}$ if such a ϕ exists. Associativity is trivial since you're literally doing nothing. Identity map is clear. It's easy to see that $\Omega_G \to \mathcal{C} \to \Omega_G$ composes to the identity with a moment's thought. For the other composition $\mathcal{C} \to \Omega_G \to \mathcal{C}$ taking

$$(X, x_o) \xrightarrow{\phi} (Y, y_o) \rightsquigarrow G/\text{Stab}_{x_o} \xrightarrow{\pi} G/\text{Stab}_{y_o}$$

Since the objects in $\mathcal{C}$ are isomorphism classes, we want first show on objects we have an isomorphism between (X, x_o) and $(G/\text{Stab}_{x_o}, \text{Stab}_{x_o})$. But this is just the statement that if $G \curvearrowright (X, x_o)$ transitively, then (X, x_o) is a G/Stab_{x_o} torsor since any two ways from x_o to another element differs only by an element of the stabilizer. For morphisms, we are done if we can show if a morphism between (isomophism types of) based transitive G-sets exists, then it is unique. But this is clear; since we must map $x_o \to y_o$ and the action of G commutes with ϕ, this determines the entirety of the mapping by transitivity of G.

2.2 Corollaries

Theorem 2.1. *Every finite group is the subgroup of a permutation group.*

Proof. We have Ω_G is always nonempty since $\{e\} \in \Omega_G$. Using our dictionary, we get

$$G \mapsto (G, e)$$

with the left multiplication as our action. We call this the *regular representation*. This gives a map

$$G \times G \to G$$

$$(g, \gamma) \mapsto g\gamma$$

or equivalently (freezing the first factor to be g)

$$L_g : G \to G$$

$$\gamma \mapsto g\gamma$$

Under the second viewpoint, we get $L_g \in S_G$ since $L_g L_{g^-} = L_e$ so we equivalently get a map

$$G \to S_G$$

$$g \mapsto L_g$$

□

In general, for every subgroup $H \subset G$, our dictionary tells us

$$H \mapsto S_{G/H}$$

where $G \times G/H \to G/H$ is given by left multiplication i.e.

$$(g, \gamma \cdot H) \mapsto g\gamma \cdot H$$

Both statements are useful. For example, this help us tell that groups without many normal subgroups can't have subgroups of small index. Take S_5 for example, we know its only normal subgroup is A_5. The claim is that S_5 has no index 3 or 4 subgroups. If such a subgroup H existed, then we'd get a map $S_5 \to S_{G/H}$ where we'd get nontrivial kernel. Thus, the image of this map must be a transposition. But this is impossible, as the action would not be transitive anymore.

2.3 Sylow's Theorems

Now that we've established this dictionary, we move onto the proof of Sylow's theorems. First, the statement:

Theorem 2.2. *(Sylow) Let G be a finite group and p a prime. Let $|G| = p^t m$ for p not dividing m. Define a Sylow p-group to a subgroup of order p^t. Then, Sylow p-groups*

1. *Always exist.*
2. *Are unique up to conjugation.*
3. *The number of them divide m and is congruent to $1 \mod p$.*

Proof.

1. For existence, it's enough to show for G is a group not a power of p, it contains a proper subgroup of index prime to p. This is essentially an induction argument; let $|G| = (p^t \cdot \alpha) \cdot \beta$ where p does not divide α or $\beta = [G : H]$ for some subgroup H. Then, $|H| = p^t \cdot \alpha$, and we can apply the argument again and again, until $\alpha = 1$, producing the desired Sylow p-subgroup.

   Using the dictionary above, we can reduce this to producing a nontrivial (based, transitive) G-set X with p not dividing $|X|$. By nontrivial here I mean $|X| > 1$ and the action is nontrivial. This follows from orbit-stabilizer as $|G| = |X| \cdot |\text{Stab}_{x_o}|$ by our assumptions. Explicitly, the purported subgroup will be the stabilizer. The assumption that nontrivial assumption is $G \neq \text{Stab}_{x_o}$ i.e. the subgroup we found is proper.

   We can drop the transitivity requirement and add the assumption that G does not act trivially when restricted to each orbit. This is since p does not divide X, p does not divide some orbit as the sum of the carnality of

the orbits is $|X|$. The nontriviality assumption is suitably lifted from the nontriviality assumption previously.

We now begin construction. Take $X \subset \text{Pow}(G)$ such that

$$X = \{S \in X : |S| = p^t\}$$

This has an action of G simply by (left) multiplication. Observe $G \notin X$, by assumption that the cardinality of G is not a power of p. The nontriviality assertion is satisfied by the stronger assertion that no subset is closed under left multiplication other than G itself. It remains to see that p does not divide $|X|$. Let $|G| = p^t m$ with p not dividing m. Then,

$$|X| = \binom{|G|}{p^t} = \binom{p^t m}{p^t} = \frac{p^t m \times ... \times p^t m - (p^t + 1)}{p^t \times ... \times p^t - (p^t + 1)} = \prod_{i=0}^{p^t+1} \frac{p^t m - i}{p^t - i}$$

From here, notice every time $p|p^t m - i$ in the numerator, then $p|i$ under our assumptions, so $p|p^t - i$. Here we used the easy fact that if $\alpha, \beta \in \mathbb{Z}$ such that $\gamma = \frac{\alpha}{\beta} \in \mathbb{Z}$, if $n|\gamma$ then $n|\alpha$, and the definition of a prime number. This means in its reduced form, p does not divide $|X|$. This completes existence.

2. We use the following homework problem as a lemma without proof. The following are equivalent

   (a) Transitive G sets X, Y are isomorphic

   (b) For all $x, y \in X, Y$, Stab_x is conjugate to Stab_y

   (c) For some $x, y \in X, Y$, Stab_x is conjugate to Stab_y

   Using this, we have that $G/P \cong G/Q$ iff P is conjugate to Q via our dictionary. Taking P, Q to be Sylow p-groups, we are left to show that $G/P \cong P/Q$ as based, transitive G-sets. Suppose $|Q| = |P| = p^t$. Consider the action of Q on G/P by left multiplication. If this action by Q is transitive, then $|G| = |G/P| \cdot |\text{Stab}_P(Q)|$. But this tells us $|\text{Stab}_P(Q)| = p^t$ and by order considerations, we have $\text{Stab}_P(Q) = \text{Stab}_P(G) = P$. But since the $\text{Stab}_P(Q) \subset Q$ by order considerations $P = Q$.

   So suppose the action is not transitive. Thus, all the orbits must be of the size p^α with $0 \leq \alpha < t$. But since $|G/P| = m$, we must have some orbit of size 1, else p would divide $|G/P|$. This means we have some coset aP such that $\text{Stab}_{aP}(Q) = Q$. Since $\text{Stab}_{aP}(G) = aPa^-$ by size considerations, $\text{Stab}_{aP}(Q) = \text{Stab}_{aP}(G)$, so $Q = aPa^-$.

3. Let $X = \{P < G : |P| = p^t\}$ Let $G \curvearrowright X$ by conjugation. This is transitive by the uniqueness portion of Sylow, and $|X| = |G|/|\text{Stab}_P(G)|$ where $\text{Stab}_P(G) = \{g \in G | \psi_g(P) = P\}$. We call this the stablizer of this action the *normalizer* of P in G. Let us denote this by $N_P(G)$. Since $P \subset N_P(G)$, p^t divides $|N_P(G)|$. Thus, $|X|$ divides m. $\square$