Useful Facts From Finite Group Theory

Alex Provost

May 28, 2015

Any group is tacitly assumed to be finite unless otherwise stated.

1 Orbit-stabilizer, class equation

Any group G acts on itself by conjugation: $g \cdot h = g^{-1}hg$. The orbits $\mathcal{O}(h) = \{g^{-1}hg : g \in G\}$ are the conjugacy classes, and the stabilizers $G_h = \{g \in G : gh = hg\} = C_G(h)$ are exactly the *centralizers*. (Note that for singleton sets, centralizers and normalizers coincide, and so $G_h = C_G(h) = N_G(h)$.) Now, note the following two general things (unrelated to our particular choice of action):

Remark 1. Being in the same orbit is an equivalence relation, so the orbits partition G. Thus in particular $|G| = \sum_{i=1}^{s} |\mathcal{O}(h_i)|$ for some choice of representative $h_1, \dots, h_s$ of each orbit.

Remark 2. There is a natural bijection $\mathcal{O}(h) \cong G/G_h$ for any $h \in G$: the correspondence is given by $g \cdot h \leftrightarrow gG_h$. (Note that G_h need not be normal in G and so G/G_h might not be a group.)

Denote the center of G by $Z(G) = \{h \in G : \forall g \in G, gh = hg\}$.

Proposition 1.1. *We have $h \in Z(G)$ if and only if $|\mathcal{O}(h)| = 1$ (for our particular choice of action, namely action by conjugation).*

Proof. Indeed $h \in Z(G) \iff gh = hg$ for all $g \in G \iff \mathcal{O}(h) = \{g^{-1}hg : g \in G\} = \{h\}$. □

Thus the elements which belong to the center of G correspond exactly to the singleton conjugacy classes of G (the singleton orbits).

Now the class equation is just a restatement of the remarks above together with Proposition 1.1:

Proposition 1.2 (Class equation)**.** *Let $h_1, \dots, h_s$ be representatives of the non-singleton conjugacy classes of G. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{s} [G : C_G(h_i)].$$

Remark 3 (Counting orbits). A similar argument can be used to compute the number of orbits of an arbitrary action of a group G on a set X. In this case, let $x_1, \ldots, x_s \in X$ be a complete set of representatives for the orbits. (Hence we which to determine the number s.) For $g \in G$, write $X^g = \{x \in X : g \cdot x = x\}$ for the set of points fixed by g, and note the symmetry relation

$$\sum_{g \in G} |X^g| = |\{(g, x) \in G \times X : g \cdot x = x\}| = \sum_{x \in X} |G_x|.$$

But each $|G_x|$ is just $|G|/|\mathcal{O}(x)|$, and so the above sum is just

$$|G| \sum_{x \in X} 1/|\mathcal{O}(x)| = |G| \sum_{i=1}^{s} |\mathcal{O}(x_i)|/|\mathcal{O}(x_i)| = |G|s.$$

Hence the number of orbits is exactly the "average number of points fixed by G,"

$$s = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

2 Applications of the class equation

The class equation has the following immediate application, which is frequently useful. Recall that a *p-group* is a group of order p^n, where p is prime.

Proposition 2.1. *Any p-group G has nontrivial center.*

Proof. Since each index $[G : C_G(h_i)]$ appearing in the class equation is ≥ 2 and divides $|G| = p^n$, then necessarily p divides $[G : C_G(h_i)]$. Since p also divides $|G|$, it follows that p divides the sum $|G| - \sum_{i=1}^{s} [G : C_G(h_i)] = |Z(G)|$. $\square$

Proposition 2.2. *If $G/Z(G)$ is cyclic, then G is abelian (thus a fortiori $G/Z(G)$ is trivial).*

Proof. Let $hZ(G)$ be a generator for the cyclic group $G/Z(G)$. Let $g_1, g_2 \in G$ be arbitrary elements. Since the cosets $h^i Z(G)$ partition G, we can write $g_1 = h^k z_1$ and $g_2 = h^l z_2$ for some $k, l \in \mathbb{N}$ and some $z_1, z_2 \in Z(G)$. Then

$$g_1 g_2 = h^k z_1 h^l z_2 = z_1 h^{k+l} z_2 = z_2 h^{l+k} z_1 = h^l z_2 h^k z_1 = g_2 g_1$$

since z_1 and z_2 commute with everything. Hence G is abelian. $\square$

These two results give us the following

Proposition 2.3. *A group G of order p^2 for some prime p is necessarily abelian.*

Proof. We must show that $Z(G) = G$. By Lagrange's theorem, the only possibilities for $|Z(G)|$ are $1, p, p^2$. By Proposition 2.1, $|Z(G)| \neq 1$ since G is a p-group. If $|Z(G)| = p$, then $|G/Z(G)| = p$. This implies that $G/Z(G)$ is cyclic; thus G is abelian by Proposition 2.2. $\square$

3 Sylow's theorem

Sylow's theorem lets us extract information about the structure of p-subgroups inside a group G given only the data $|G|$.

Theorem 3.1 (Sylow). *Let G be a group of order $p^k m$, where p doesn't divide m. A subgroup of order p^k in G is then called a* Sylow p-subgroup. *The following statements hold:*

(1) Sylow p-subgroups exist;

(2) Any two Sylow p-subgroups are conjugate in G (hence isomorphic);

(3) The number of Sylow p-subgroups $n_p \equiv 1 \mod p$. Moreover $n_p = [G : N_G(P)]$ for any Sylow p-subgroup P; hence, by Euclid's lemma, n_p divides m.

Corollary 3.2. *A Sylow p-subgroup is normal in G if and only if it is the unique Sylow p-subgroup in G, i.e., $n_p = 1$.*

Let us look at some examples. First, recall the following:

Proposition 3.3. *A subgroup H of index 2 in G is normal.*

Proof. The left and right cosets partition G, so $G = H \sqcup gH = H \sqcup Hg$ for any $g \notin H$. This implies that $gH = Hg$ for all $g \in G$ as desired. □

Proposition 3.4. *Any group G of order 30 has a normal subgroup of order 15.*

Proof. By the above proposition, any subgroup of order 15 is automatically normal. Thus it suffices to show that such a subgroup exists. Now $30 = 2 \cdot 3 \cdot 5$; in particular, by Sylow's theorem (or the weaker theorem of Cauchy), subgroups of order 3 and 5 exist. If either of them if normal in G, then their product is a subgroup of order 15 and we are done.

So suppose that $n_3 > 1$ and $n_5 > 1$ (cf. Corollary 3.2). By the divisibility relation in Sylow's theorem, n_3 must divide 10 and n_5 must divide 6. Also, we must have $n_3 \equiv 1 \mod 3$ and $n_5 \equiv 1 \mod 5$. Thus the only possibility is $n_3 = 10$ and $n_5 = 6$. By Lagrange's theorem, distinct Sylow 5-subgroups must intersect in the identity (since the intersection of subgroups is a subgroup and 5 is prime). Hence the 6 Sylow 5-subgroups yield 4 distinct non-identity elements each for a total of 24 elements of order 5. Similarly, the 10 Sylow 3-subgroups provide in total $10 \cdot 2 = 20$ elements of order 3, a contradiction since G only has order 30. □