CHAPTER 6 OF ARTIN'S ALGEBRA: "MORE GROUP THEORY"

NOTES AND TUTORIAL SHEET 2B

Abstract. Proofs of Sylow's theorems by means of group actions

Let p be a prime and G a finite group of order $n = p^e m$, where p does not divide m. A subgroup of order p^e of G is called a Sylow p-subgroup. Sylow's theorems are usually stated as follows:

(1) There exists a Sylow p-subgroup.
(2) The Sylow p-subgroups are all conjugate.
(3) The number n_p of Sylow p-subgroups divides m and satisfies $n_p \equiv 1 \bmod p$.

We prove the above theorems and provide some context in the following series of tutorial exercises:

(1) A p-group G satisfies the converse of Lagrange's theorem: that is, for any integer d such that $0 \leqslant d \leqslant e$, where $|G| = p^e$, there exists a subgroup in G of order p^d. (Hint: We have already seen, as a consequence of the class equation, that a p-group has non-trivial centre. Use this and induction on $|G|$.)
(2) Combining item (1) with the first Sylow theorem, one obtains the following (partial) converse to Lagrange's theorem: given a prime power q that divides the order of a finite group G, there exists a subgroup of G of order q. In particular, we get Cauchy's theorem: if a prime p divides the order of a finite group G, there exists an element of order p in G.
(3) Show that $\binom{p^e m}{p^e}$ is not divisible by p (where p is a prime and m an integer coprime to p).
(4) A subgroup H of a finite group G is a Sylow p-subgroup if and only if H is a p-group and the index of H in G is coprime to p. (On the face of it, this appears to be an innocuous characterization of a Sylow p-subgroup, but it plays a crucial role in the proofs below of the first and second Sylow theorems in items (5), (7b) below.)
(5) We now prove the existence of a Sylow p-subgroup (Sylow's first theorem). Let us first explain our strategy.

    Given item (4), we look for a subgroup H that is in some sense large enough (has index coprime to p) and in another sense small enough (is a p-subgroup). To stage this balancing act, we try to realize H as the stabiliser of some point in a suitable G-orbit $\mathscr{O}$. By the counting formula, the index of H in such a case equals the cardinality of $\mathscr{O}$. So we look for an $\mathscr{O}$ which is small enough (has cardinality coprime to p) and is also large enough (its stabiliser is a p-subgroup).

    Consider the action of G by left multiplication on the collection $\mathscr{C}$ of subsets of G of cardinality p^e.

    (a) By item (3), $|\mathscr{C}|$ is coprime to p, so $\mathscr{C}$ has a G-orbit whose cardinality is coprime to p.
    (b) Let U be an element of $\mathscr{C}$ belonging to such an orbit and let H be the stabiliser of U. Then U is the union of right cosets of H (see problem (4b) in Tutorial sheet 2A), and hence $|H|$ divides $|U| = p^e$, so H is a p-group.

    The subgroup H thus has the desired properties.

(6) Show that the second Sylow theorem follows from the following finer claim:

Let K be a subgroup of G and P a Sylow p-subgroup of G. Then there exists a conjugate ${}^gP := gPg^{-1}$ of P (for some g in G) such that $K \cap {}^gP$ is a Sylow p-subgroup of K.

(7) Let us now prove the claim in the previous item. Let P be a Sylow p-subgroup of G.
   (a) Consider G/P with the natural G action on it. We restrict the action to K and decompose G/P into a disjoint union of K-orbits. Since $|G/P| = m$ is not divisible by p, it follows that at least one of these K-orbits has cardinality not divisible by p. Let g in G be such that the K-orbit of the coset gP in G/P has cardinality not divisible by p. Let Q denote the stabiliser in K of the coset gP. We claim that Q is a Sylow p-subgroup of K.
   (b) On the one hand, by the "counting formula" we have
$$|K| = |K\text{-orbit of } gP| \cdot |Q|$$
and so the index of Q in K is coprime to p. On the other hand, the stabiliser of gP in G being gPg^{-1}, we have $Q = K \cap gPg^{-1}$, so Q is a p-group. It follows that Q is a Sylow p-subgroup of K (see item (4) above).

(8) (a) A Sylow p-subgroup of a finite group is unique if and only if it is normal.
   (b) Let P and P' be Sylow p-subgroups of a finite group G. If $P \neq P'$, then P does not normalise P'. (Hint: Suppose that $P \subseteq N_G(P')$. Then P and P' are distinct Sylow p-subgroups of $N_G(P')$, with P' being normal, a contradiction to the previous item.)

(9) Let us now prove Sylow's third theorem.
   (a) The group G acts on the set $\mathscr{S}$ of its Sylow p-subgroups by conjugation. By Sylow's second theorem, this action is transitive. So the number n_p of Sylow p-subgroups is the index in G of the stabiliser of any one particular Sylow p-subgroup, say P. This stabiliser is the normaliser $N_G(P)$ of P in G and contains P. Hence its index divides the index of its subgroup P, which is m.
   (b) Restrict the action on $\mathscr{S}$ in the previous item to the Sylow p-subgroup P. By item (8) the only P-fixed point in $\mathscr{S}$ for this action is P. Now, by the "fixed point theorem for p-group actions" (item (13) in Sheet 1), the cardinality of $\mathscr{S}$ and that of the fixed point set are equal modulo p.

(10) For a Sylow p-subgroup P of a finite group G, we have $N_G(N_G(P)) = N_G(P)$.

(11) Let q be the power of a prime p, and $\mathbb{F}_q$ a finite field with q elements. Put $G = GL(n, \mathbb{F}_q)$ (where n is some positive integer).
   (a) What is the cardinality of a Sylow p-subgroup of G?
   (b) Describe explicitly a Sylow p-subgroup of G.
   (c) What is the number of Sylow p-subgroups in G?