KSOM ALGEBRA II 2021 MAY–AUG
NOTES AND TUTORIAL PROBLEMS: SYLOW'S THEOREMS

Let G be a finite group and p an arbitrarily fixed prime p. Write $|G| = p^e m$ with $e \geqslant 0$ and m being coprime to p. A subgroup of G of cardinality p^e is called a Sylow p-subgroup of G. Such subgroups

(1) always exist (there is at least one of them),
(2) are all conjugate to one another, and
(3) their number k divides m and leaves remainder 1 on division by p.

These assertions, called Sylow's first, second, and third theorems respectively, will be proved and discussed in the items below.

(1) (Cauchy's theorem; proof by J. H. McKay) Let G be a finite group and p a prime dividing the order of G. Then there exists an element in G of order p. (Hint: Consider $G^p := G \times \cdots \times G$ (p times) and let the cyclic group $C = \langle c \,|\, c^p = 1 \rangle$ of order p act on G^p by $c(g_1, g_2, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1})$. The subset $S = \{(g_1, \ldots, g_p) \,|\, g_1 g_2 \cdots g_p = 1\}$ of G^p is stable under the C-action. Since C is a p-group we have $|S| \equiv |S^C| \bmod p$. Observe that S has cardinality $|G|^{p-1}$ (and so $|S^C| \equiv |S| \equiv 0 \bmod p$). Since $(1, 1, \ldots, 1)$ evidently belongs to S^C, it follows that there is some other element also in S^C. Any element of S^C is of the from $(g, g, \ldots, g)$, with $g^p = 1$.)

(2) (A proof of Cauchy's theorem based on induction and the class equation) Let p be a prime and G a group whose order is divisible by p. We want to show that G has an element of order p. For this, it suffices to find an element x whose order k is divisible by p, for then $x^{p/k}$ has order p. We argue by induction on the order of G that G contains an element whose order is divisible by p. The base case ($|G| = 1$) of the induction being clear, we proceed to the induction step.

Let us first identify two cases when the result holds:

- If there is a proper subgroup whose order is divisible by p, then the induction hypothesis applied to the subgroup gives the result.
- If there is a non-trivial central element x, then too we are done as follows. If x itself has order divisible by p, then of course we are done. If not, then an element whose order is divisible by p exists in the quotient group $G/\langle x \rangle$, and any pre-image in G of such an element also has order divisible by p.

Finally, we argue that one of the above two cases holds. Suppose that the first does not. Then every proper subgroup of G has order coprime to p, or, in other words, every non-singleton orbit of G has cardinality divisible by p. In particular, every non-singleton conjugacy class of G has cardinality divisible by p, and it now follows from the class equation that G has non-trivial centre, so the second case holds. □

(3) Let p be a prime and n an integer. Write $n = p^e m$, where $e \geqslant 0$ and p does not divide m. Show that $\binom{n}{p^e}$ is coprime to p.

(4) Let X be finite set of cardinality coprime to p (where p is some fixed prime) on which a group G acts. Then there is an orbit of X whose cardinality is coprime to p (because X is the disjoint union of its orbits). The isotropy at any point of such an orbit is a subgroup of index coprime to p.

(5) For a subset S and a subgroup H of a group G, we have $HS = S$ if and only if S is a union of right cosets of H.

(6) (Sylow's first theorem) Let G be a finite group and p a prime. Write $|G| = p^e m$ with $e \geqslant 0$ and $(m, p) = 1$. Then G admits a subgroup of order p^e. (Outline of the proof by Wielandt: Consider the left regular action of G on itself and the induced action on the power set of G. The set X of subsets of cardinality p^e of G is stable under this action. By the observations in items (3) and (4) applied to X, we obtain a subgroup H of G of index coprime to p (so p^e divides $|H|$) and such that $HS = S$ for some subset S of G of cardinality p^e. Invoking item (5), we conclude that $|H| \leqslant |S| = p^e \leqslant |H|$, so $|H| = p^e$.)

(7) (Addendum to Sylow's first theorem) A group of order p^e (where p is a prime) admits subgroups of orders p^f for all f, $0 \leqslant f \leqslant e$. Thus, with hypothesis as in item (6), it follows that G admits subgroups of orders p^f for all f, $0 \leqslant f \leqslant e$.

(8) Recall that $|X| \equiv |X^Q| \bmod p$ for a finite p-group Q acting on a finite set X. When the cardinality of X is moreover coprime to p, it follows that X admits an element fixed by Q.

(9) This item gives another proof of Sylow's first theorem. This proof uses the class equation and Cauchy's theorem, the latter proved variously in items (1) and (2) above. Fix hypothesis as in item (6). Proceed by induction on the order of G. The base case being clear (why?), we proceed to the induction step. If G admits a proper subgroup of index coprime to p, then we are done by induction. So assume that the contrary holds. From the class equation it follows that the centre of G has order divisible by p (since every term other than $|\text{centre}(G)|$ on the RHS is divisible by p, and therefore the same is true for this term). Choose a central element x of order p in G (by Cauchy's theorem applied to the centre of G), apply induction to $G/\langle x \rangle$ to get a subgroup of order p^{e-1} of this quotient group, and pull that subgroup back to G.

(10) This item gives a direct proof of the extended version of Sylow's first theorem, namely that, with the hypothesis as in item (6), G admits subgroups of all orders p^f for $0 \leqslant f \leqslant e$. The idea is that Wielandt's proof in item (6) generalises directly. Consider the action of G by left multiplication on the set X of subsets of G of cardinality p^f. An elementary calculation shows that p^{e-f+1} does not divide $|X| = \binom{p^e d}{p^f}$. Thus there exists a subset S of G with p^f elements whose

stabiliser H (that is, the maximal subgroup of G such that $HS \subseteq S$) has order divisible by p^f. And now, it follows as in item (6) that $|H| = p^f$.

(11) (Sylow's second theorem) Let Q be a p-subgroup of a finite group G. Let P be a Sylow p-subgroup of G (whose existence is assured by item (6)). Prove that Q is contained in a conjugate of P. If, in particular, Q is itself a Sylow p-subgroup, then Q must be a conjugate of P. (Hint: Consider the restriction to Q of the natural action of G on the coset space G/P. By invoking the observation made in item (8), we conclude that Q fixes some coset gP. This means $Qg \subseteq gP$ or $Q \subseteq gPg^{-1}$.)

(12) Let P be a Sylow p-subgroup of a finite group G (for some prime p). If P is unique, then it is clearly normal (since any conjugate is a subgroup of the same cardinality and hence equals P). Conversely, if P is normal, then it is unique (by Sylow's second theorem).

(13) Let P and P' be Sylow p-subgroups of a finite group G. If P normalizes P', then $P = P'$. (Hint: Observe that P' is a normal Sylow p-subgroup in its normaliser $N_G(P)$ and is therefore unique (item (12) above). If P normalises P', then P is a Sylow p-subgroup of $N_G(P)$ and so equals P'.)

(14) (Sylow's third theorem) Let p be a prime, G be a finite group, and k the number of Sylow p-subgroups of G. Then k divides m, where $|G| = p^e m$ with $e \geqslant 0$ and m coprime to p, and leaves remainder 1 on division by p. (Hint: Consider the conjugation action of G on itself and the induced action on the power set of G. The set X of Sylow p-subgroups of G is G-stable and we consider it now as a G-set. By Sylow's second theorem (item (11)), it follows that the G-action on X is transitive. The isotropy at P being $N_G(P)$ (=the normaliser in G of P), we may identify X as a G-set with $G/N_G(P)$. Thus $k = |X| = |G/N_G(P)|$. Since $N_G(P) \supseteq P$, it follows that $k = |G/N_G(P)|$ divides $|G/P| = m$. Restricting to P the G-action on X, we observe that P is the unique point that is fixed by P (item (13) above). Since the non-singleton P-orbits of X have cardinalities divisible by p, it follows that $|X| = k \equiv 1 \bmod p$.)

(15) Let G be a finite group with $p_1, \ldots, p_k$ being all the distinct prime divisors of $|G|$. Let P_i be a Sylow p_i-subgroup of G (we are choosing only one for each i out of several choices, possibly). Then $P_1, \ldots, P_k$ generate the group G.

(16) (Characteristic subgroups) A subgroup H of a group G is called characteristic if it is preserved by all automorphisms of G, that is, $\varphi(H) = H$ for every group automorphism φ of G. (In contrast, for a subgroup to be normal, it is enough that it is preserved by all inner automorphisms.) There are many natural characteristic subgroups, e.g., the centre, the commutator.

(17) (Nilpotent groups) Given a group G, consider the following sequence of characteristic subgroups: $\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots$, where $G_0 := \{1\}$ and G_i is inductively defined to be containing G_{i-1} and such that G_i/G_{i-1} is the centre of G/G_{i-1}. The group G is said to be nilpotent if $G_k = G$ for some finite k.

(a) Finite p-groups are nilpotent. This follows from the fact that every finite p-group has non-trivial centre.

(b) Any proper subgroup of a nilpotent group is properly contained in its normaliser.
(c) Subgroups and quotient groups of nilpotent groups are nilpotent.
(d) G need not be nilpotent even if it admits a nilpotent normal subgroup N such that G/N is nilpotent. However, if such an N is also central, then G is nilpotent.

(18) Are the dihedral groups D_n nilpotent?

(19) Let P be a Sylow p-subgroup of a finite group G. Show that $N_G(N_G(P)) = N_G(P)$. (Here $N_G(H)$ denotes the normaliser of a subgroup H.) Deduce that any Sylow subgroup of a finite nilpotent group is normal.

(20) (Structure theorem for finite nilpotent groups) A finite nilpotent group is the direct product of its Sylow subgroups. (Hint: Each Sylow subgroup is normal since G is nilpotent (by a previous item). Let $P_1, \ldots, P_k$ be the Sylow subgroups: there is precisely one for each prime p since the subgroups are normal (by Sylow's second theorem). The subset $P_1 \cdots P_k$ is a subgroup (since the P_i are normal) and $P_1 \cdots P_k = G$ (the Sylow subgroups generate G as observed in a previous item). Finally,

$$P_1 \cdots P_k \simeq P_1 \cdots P_{k-1} \times P_k \simeq P_1 \cdots P_{k-2} \times P_{k-1} \times P_k \simeq \ldots \simeq P_1 \times P_2 \times \cdots \times P_k$$

for $P_1P_2 \simeq P_1 \times P_2$ (since $P_1 \cap P_2$ is empty), $P_1P_2P_3 \simeq P_1P_2 \times P_3$ (since $P_1P_2 \cap P_3$ is empty), etc.)

(21) Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements where p is a prime (e.g., $r = 1$ and $\mathbb{F}_q = \mathbb{Z}/p\mathbb{Z}$) and let $G = GL_n(\mathbb{F}_q)$.
(a) What is the order of a Sylow p-subgroup of G?
(b) Describe any one particular Sylow p-subgroup of G.
(c) How many Sylow p-subgroups does G have?
(d) Show that the subgroup consisting of all invertible upper triangular matrices of G is its own normaliser. (Hint: What is the relevance of this problem to the present context?)

(22) Let G be a subgroup of a finite group K. Suppose that K has a Sylow p-subgroup R.
(a) G has a Sylow p-subgroup P, and $P = G \cap kRk^{-1}$ for some k in K. (Hint: Restrict to G the natural action of K on $X = K/R$. Since $|X|$ is coprime to p, there exists a G-orbit of X that is coprime to p. Let kR be any point on such an orbit and let P be the isotropy at the point kR. We have $Pk \subseteq kR$ or $P \subseteq kRk^{-1}$. Given that P is contained in the p-group kRk^{-1}, it follows that P is a p-group. Given that the index of P is coprime to p, it now follows that P is a Sylow p-subgroup of G.)
(b) (Alternative proof of Sylow's first theorem) Now use the existence of Sylow p-subgroups in the general linear groups $GL_n(\mathbb{F}_p)$ to deduce the existence of such subgroups in any finite group.

(23) Let f be a non-negative integer. We want to now prove that, for any finite group G and any prime p such that p^f divides $|G|$, the number N_f of subgroups

of G of order p^f satisfies $N_f \equiv 1 \bmod p$. As item (7) asserts, $N_f \geqslant 1$. For G such that p^f is the largest power of p that divides $|G|$, this assertion is part of Sylow's third theorem (item (14)). The proof below uses Sylow's third theorem as the input into the base case of an induction, and does not give an independent proof of that theorem.

(a) Let G be a group, Z a subgroup of G of order p, and P a p-subgroup of G that normalises Z. Then P centralises Z. (The automorphism group of Z has order $p-1$. Thus the map from P to Aut Z defining the conjugation action of P on Z is trivial.)

(b) $N_1 \equiv 1 \bmod p$ for any finite abelian p-group G. (The set of all elements of G of order p together with the identity element forms a subgroup. The order of this subgroup is a power of p, say p^f. Given that any two subgroups of order p intersect trivially, we conclude that $N_1 = (p^f - 1)/(p-1)$.)

(c) $N_1 \equiv 1 \bmod p$ for any p-group G. (Consider the conjugation action of G on the set of subgroups of order p. Any non-singleton orbit has cardinality divisible by p. If a subgroup Z of order p forms an orbit by itself, then, by item (23a), it belongs to the centre. Thus we are reduced to the case when G is abelian, which has been handled in item (23b).)

(d) Let G be a group, and P a subgroup of order p^f of G (where p is a prime and f a non-negative integer). Suppose Q is a subgroup of G that contains P and is order p^{f+1}. Then Q normalises P. Thus, any subgroup of order p^{f+1} of G that contains P is contained in $N_G(P)$. (Since Q is a p-group, every proper subgroup H thereof is properly contained in its normaliser $N_Q(H)$. But P is a maximal subgroup Q.) The number of such subgroups equals N_1 of $N_G(P)/P$, which, when G is a finite p-group, is congruent to $1 \bmod p$ (by item (23c)).

(e) Proof by induction on f that $N_f \equiv 1 \bmod p$ for any finite p-group G. (Evidently $N_0 = 1$. And $N_1 \equiv 1 \bmod p$ by item (23c). We now suppose that the claim holds for f and prove that it also holds for $f+1$. Fix G such that p^{f+1} divides $|G|$. Let $P_1, \ldots, P_s$ be all the subgroups of order p^f (of G); and let $Q_1, \ldots, Q_t$ be all the subgroups of order p^{f+1}. Our goal is to show that $t \equiv 1 \bmod p$.
For each j, $1 \leqslant j \leqslant s$, let t_j be the number of those $Q_1, \ldots, Q_t$ that contain P_j; for each i, $1 \leqslant i \leqslant t$, let s_i be the number of those $P_1, \ldots, P_s$ that are contained in Q_i. We then have

$$\sum_{j=1}^{s} t_j = \sum_{i=1}^{t} s_i$$

By item (23d), it follows that each t_j is congruent to 1 modulo p. On the other hand, the induction hypothesis tells us that s and all the s_i are congruent to 1 modulo p. Thus the LHS in the above display is congruent to 1 modulo p and the RHS to t modulo p.)

(f) As the final step in the proof, we now prove the following. Given a finite group G, a prime p, and f an integer such that p^f divides the order of G, the number N_f of subgroups of G of order p^f satisfies $N_f \equiv 1 \bmod p$. (If f is maximal such that p^f divides $|G|$, then the result follows from Sylow's third theorem. We therefore suppose that f is less than maximal, and proceed by a downwards induction on f. As in the previous item, let $Q_1, \ldots, Q_t$ be all the subgroups of (of G) order p^{f+1} and $P_1, \ldots, P_s$ be all the subgroups of order p^f. Let $t_1, \ldots, t_s$ and $s_1, \ldots, s_t$ be defined as above. We have:

$$\sum_{j=1}^{s} t_j = \sum_{i=1}^{t} s_i$$

By item (23e), the s_i are all congruent to 1 modulo p, and so the RHS is congruent to t modulo p. By (23d), the t_j are all congruent to 1 modulo p, and so the LHS is congruent to s modulo p. Now, by the induction hypothesis, t is congruent to 1 modulo p. And we conclude that s too is congruent to 1 modulo p.)

(24) (Frattini Argument) Let G be a finite group, N a normal subgroup, and P a Sylow p-subgroup of N (for some prime p). Show that $G = N \cdot N_G(P)$. (For g an element of G, consider ${}^gP := gPg^{-1}$. Since N is normal, we have ${}^gP \subseteq {}^gN = N$. Given that ${}^gP$ is a Sylow p-subgroup of N, it follows, from Sylow's second theorem (applied to N), that there exists n in N such that ${}^gP = {}^nP$, which means $n^{-1}g$ belongs to $N_G(P)$, and we have $g = n(n^{-1}g) \in N \cdot N_G(P)$.)