THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2024-25
Tutorial 7 solutions
24th October 2024

- The tutorial solutions are written for reference and proofs will be sketched briefly. You should try to fill in the details as an exercise. The solutions for Homework optional questions can be found in Homework solutions, which would be released after the deadlines. Please send an email to echlam@math.cuhk.edu.hk if you have any further questions.

1. Since P is normal in G, we have that $P \cap H \trianglelefteq H$, therefore by second isomorphism theorem $[H : P \cap H] = [PH : P]$. Now since P is a Sylow p-subgroup, $[G : P]$ must be coprime with p, therefore $[PH : P]$, as a factor of $[G : P]$ must also be coprime with p. This establishes $P \cap H$ as a p-subgroup inside H with $[H : P \cap H]$ coprime with p, thus it is a Sylow p-subgroup.

2. Let G be a group of order 56, we have $n_7 \equiv 1 \mod 7$, so $n_7 = 1$ or 8. If $n_7 = 1$ then the unique Sylow 7-subgroup is proper normal and we are done. Otherwise suppose that $n_7 = 8$, since distinct cylic subgroups of prime order must intersect trivially, the eight Sylow 7-subgroups would consist of a total of $6 \cdot 8 = 48$ distinct elements of order 7. The remaining elements of G has order dividing 8. Since it is impossible for the Sylow 2-subgroup of order 8 to have any element of order 7, the remaining 8 elements in G should constitute the Sylow 2-subgroup. Therefore it is necessarily unique and hence normal. In either cases, G is not simple.

3. Let G be a simple group of order 168, by simplicity there must be more than one Sylow 7-subgroup. And since $n_7 \equiv 1 \mod 7$, we can deduce that $n_7 = 8$. We argue as before, the Sylow 7-subgroups are cylic and intersect trivially. So there are $6 \cdot 8 = 48$ elements of order 7. Any element of order 7 is clearly contained in some Sylow 7-subgroup, so this accounts for all elements of order 7.

4. Let G be a group of order 231, then $n_{11} \equiv 1 \mod 11$ so n_{11} can only be 1. Let H be the unique Sylow 11-subgroup, we already know that it is normal. Let $g \in G$, define $\varphi_g : H \to H$ by $\varphi_g(h) = ghg^{-1}$. Then φ_g is an automorphism of $H \cong \mathbb{Z}_{11}$. Recall that for prime p, we have $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, therefore the homomorphism $\varphi : G \to \mathrm{Aut}(\mathbb{Z}_{11})$ by $\varphi(g) = \varphi_g$ must be trivial, as $|G|/|\ker\varphi| = 1, 2, 5$ or 10 implies that $G = \ker\varphi$. This implies that for any $g \in G, h \in H$, $\varphi_g(h) = ghg^{-1} = h$, so $gh = hg$. We have $H \leq Z(G)$ so that $11 = |H| \leq |Z(G)|$.

5. This result (or the consequence thereof) is known as Cayley normal 2-complement theorem. It says that if G has cyclic Sylow 2-subgroup, then it has an index two subgroup.

   (a) Let P be a cyclic Sylow 2-subgroup, and pick $s \in P$ a generator. The statement is just saying that $\phi(s) \in S_G = S_{2^r m}$ by $\phi(s) : g \mapsto sg$ is an odd permutation. To see why, let's restrict the left regular action to $P = \langle s \rangle$ acting on G. The orbits of this action are given by $P \cdot x = \{y \in G : s^k \cdot x = y\}$. In other words, x, y are in the same orbit if and only if they are in the same right P-coset.

Therefore G is partitioned into $[G : P] = m$ an odd number of orbits. The action of $P = \langle s \rangle$ on each orbit is cyclic, in terms of $\phi(s) \in S_G$, this says that multiplying by s is given by m disjoint cycles of length 2^r. But since a cycle of length 2^r can be written as a product of $2^r - 1$ transpositions. We can write $\phi(s)$ as product of $(2^r - 1)m$ many transpositions. Hence, $\phi(s)$ is an odd permutation and $\psi(s) = 1$.

(b) $\psi(s) = 1$ implies that $\psi : G \to \mathbb{Z}_2$ is surjective, so $\ker(\psi)$ is a proper normal subgroup. But G is simple, this forces that $\ker(\psi) = 1$ and so $\psi : G \to \mathbb{Z}_2$ is an isomorphism.

6. (a) Suppose that p^n is the highest power of a prime p that divides $|G|$, then there are at most p^n many elements having order dividing p^n by the condition. If P is a Sylow p-subgroup of order p^n then all elements have order dividing p^n and it already accounts for all possible g with such orders. Therefore it is necessarily unique.

(b) Suppose that P is not cyclic, then all elements of P have order dividing p^{n-1}. But this would imply that there are p^n many elements of order dividing p^{n-1}, which is a contradiction.

(c) All Sylow p-subgroups are unique and cyclic, by a proposition of lecture 5, we know that G is isomorphic to the direct product of cyclic groups that are coprime in order. Therefore it is also cyclic. (Recall that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if $\gcd(m, n) = 1$.)

7. (a) $n_r \equiv 1 \mod r$, but we have $p, q < r$, so $n_r = 1$ or possibly pq if $pq \equiv 1 \mod r$. If $n_r \neq 1$, then there are pq many Sylow r-subgroups which are all cyclic and therefore there are $pq(r-1)$ many elements of order r.

Likewise for n_q, by $p < q$ we cannot have $n_q = p$, but n_q can possibly be $1, r, pr$. So if $n_q \neq 1$, there are at least r many Sylow q-subgroups, so there are at least $r(q-1)$ many elements of order q.

Same argument for n_p implies that n_p could be $1, q, r, qr$. So for $n_p \neq 1$ we have at least $q(p-1)$ many elements of order p.

(b) Suppose that all n_p, n_q, n_r are not 1, then by part (a) there are at least the following number of distinct elements in G:

$$\begin{aligned} pq(r-1) + r(q-1) + q(p-1) + 1 &= pqr - pq + qr - r + pq - q + 1 \\ &= pqr + (q-1)(r-1) \\ &> pqr = |G| \end{aligned}$$

This is clearly a contradiction. So at least one of n_p, n_q, n_r is 1, and there is a unique Sylow subgroup N that is normal. Then N is cyclic, and G/N has order pq, qr or pr, which is solvable by a result in lecture 5.

8. (a) Consider the homomorphism $\varphi : G/P \to \mathrm{Aut}(P)$ defined by $gP \mapsto \varphi_g : P \to P$ by $\varphi_g(x) = gxg^{-1}$. This is well-defined because if $gP = g'P$, then there is some $p \in P$ so that $g' = gp$, then $\varphi_{g'}(x) = g'xg'^{-1} = gpxp^{-1}g^{-1}$. But P is cyclic, hence abelian, so that $pxp^{-1} = x$, thus $\varphi_{g'} = \varphi_g$. Now $P \cong \mathbb{Z}_{2^n}$ and so $|\mathrm{Aut}(P)| = 2^{n-1}$ in bijection with the odd numbers from 1 to 2^n. But then $|G/P| = m$ is odd, so φ must be trivial because the only odd factor of 2^{n-1} is 1.

Now let $aP \in G/P$ is a generator of G/P and $b \in P$ be a generator of P. If $g \in G$ is any element, $g \in gP$ clearly, and thus $g = (aP)^i = a^iP$ for some i. So that

$g = a^i p$ for some $p \in P$, which in turn can be expressed as $g = a^i b^j$. It suffices to prove that a commutes with b, then for any $g, h \in G$, we have $g = a^i b^j$ and $h = a^k b^l$ for some integers i, j, k, l, then $gh = hg = a^{i+k} b^{j+l}$. Now we know that a, b commutes because $\varphi_a(b) = aba^{-1} = b$.

(b) First note that since G/P is cyclic of order m, $(aP)^m = a^m P = P$ implies that $a^m \in P$, so we have $a^m = b^s$ for some positive integer s. Now since m and 2^n are coprime, the equation $s \equiv c2^n \mod m$ is always solvable. Therefore $a^m = b^{c2^n + md} = b^{md}$ for some integers c, d. This implies that $a^m b^{-md} = (ab^{-d})^m = e$, denote $\tilde{a} = ab^{-d}$, note that $\tilde{a}P = aP$

By the same argument as in part (a), we have that any $g \in G$ can be expressed as $\tilde{a}^i b^j$. We claim that $\tilde{a}b$ is a generator of G, i.e. we will show that for any $i, j \in \mathbb{Z}$ there exists some $k \in \mathbb{Z}$ so that $\tilde{a}^i b^j = \tilde{a}^k b^k$. This is equivalent to the equations

$$\begin{aligned} i &\equiv k \mod m \\ j &\equiv k \mod 2^n \end{aligned}$$

Since m and 2^n are coprime, by Chinese remainder theorem, the above system is always solvable for any $i, j \in \mathbb{Z}$. Since G is generated by one element, it is cyclic.

Alternative argument: $H = \langle \tilde{a} \rangle$ and P have coprime orders, therefore $H \cap P = \{e\}$. G is abelian, so H, P are both subgroups. By Q5 of tutorial 4, we know that $G = HP$ is in fact isomorphic to $H \times P$. Then we may conclude by noting that product of cyclic groups of coprime orders is again isomorphic to a cyclic group.