Final exam solution - Ma 5a, Caltech

Instructor: Alexander Yom Din

1. Let \( p \geq 5 \) be a prime.

(a) (5 pt) Show that \( S_p \) has a subgroup of index \( p \).

(b) (20 pt) Show that if \( S_n \) has a subgroup of index \( p \) (where \( n \geq 1 \) is an integer), then \( n = p \).

Solution:

(a) Consider \( H = \{ \sigma \in S_p \mid \sigma(p) = p \} \). The map \( H \to S_{p-1} \) given by \( \sigma \mapsto \sigma|_{\{1, \ldots, p-1\}} \) is clearly an isomorphism so, in particular, \( |H| = (p-1)! \). Thus \( [S_p : H] = \frac{|S_p|}{|H|} = \frac{p!}{(p-1)!} = p \).

(b) Assume that \( S_n \) has a subgroup \( H \) of index \( p \). Clearly, \( n \geq p \geq 5 \) (because \( p = [S_n : H]|S_n| = n! \)). We claim now that the group \( S_n \) has a normal subgroup \( K \) of index \( k \) satisfying \( p \leq k \leq p! \). Indeed, we can take \( K \) to be the kernel of the left regular action map \( S_n \to S(S_n/H) \); We saw this in our study. But we saw in our study that the only normal subgroups of \( S_n \) are \( \{e\}, A_n, S_n \), so having index \( n! \), 2, 1 in \( S_n \) - thus the only possibility is that \( k = n! \), and this forces \( p! = n! \), which forces \( p = n \).

2. (25 pt) Let \( p > q \) be odd primes. Let \( G \) be a group of order \( p^nq^2 \) (where \( n \geq 0 \) is an integer). Show that \([G, G]\) is a \( p \)-group.

Solution:

Denote by \( n_p \) the number of \( p \)-Sylow subgroups of \( G \). We have \( p|n_p - 1 \) and \( n_p|q^2 \). The later condition gives \( n_p \in \{1, q, q^2\} \).

Let us show that \( n_p = 1 \). For this, we rule out \( n_p = q \) and \( n_p = q^2 \).\( n_p = q \) implies \( p|q - 1 \), which in its turn implies \( q > p \) - contradicting the given \( p > q \). \( n_p = q^2 \) implies \( p|q^2 - 1 = (q+1)(q-1) \) thus implying \( p|q-1 \) or \( p|q+1 \). \( p|q-1 \) was already ruled out. \( p|q+1 \) is also impossible.
- it would mean \( p \leq q+1 \) so we would have \( p-1 \leq q < p \), thus \( q = p-1 \), which is impossible since both \( p \) and \( q \) are odd.

Thus, we have \( n_p = 1 \). This means that \( G \) admits a unique \( p \)-Sylow subgroup \( P \), and \( P \) is normal in \( G \). Notice that \( G/P \) is a group of order \( q^2 \), and hence abelian as we studied. Thus, as we studied, \([G,G] \subset P\). So, since \( P \) is a \( p \)-group, so is \([G,G]\).

3. Let \( G \) be a group of order \( 255 = 3 \cdot 5 \cdot 17 \).

   (a) \((13 \text{ pt})\) Let \( P \in Syl_{17}(G) \). Show that \( P \subset Z(G) \). Hint: First show that \( P \) is normal in \( G \), then try to think about the action of \( G \) on \( P \) by conjugation.

   (b) \((5 \text{ pt})\) Show that \( G/P \) is cyclic.

   (c) \((7 \text{ pt})\) Show that \( G \cong \mathbb{Z}/255\mathbb{Z} \).

**Solution:**

(a) Denoting by \( n_{17} \) the number of 17-Sylow subgroups in \( G \), the conditions \( 17 | n_{17} - 1 \) and \( n_{17} | 15 \) clearly imply \( n_{17} = 1 \). Thus, \( P \) is a normal subgroup of \( G \). Consider the homomorphism \( G \to Aut(P) \) given by the conjugation action. Notice that \( P \), being a group of prime order 17, is isomorphic to \( \mathbb{Z}/17\mathbb{Z} \). Thus, as we have studied, \( Aut(P) \cong Aut(\mathbb{Z}/17\mathbb{Z}) \cong (\mathbb{Z}/17\mathbb{Z})^\times \) and so, in particular, \( |Aut(P)| = 16 \). Thus, \( |G| \) and \( Aut(P) \) are coprime. Thus, as we have studied, \( G \to Aut(P) \) must be the trivial homomorphism. This exactly means that \( P \subset Z(G) \).

(b) \( G/P \) is a group of order \( 15 = 3 \cdot 5 \). By what we studied about groups of order \( pq \), since 3 does not divide \( 5 - 1 \), this group is isomorphic to \( \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \), which in its turn is isomorphic, by the Chinese reminder theorem, to \( \mathbb{Z}/15\mathbb{Z} \), hence is cyclic.

(c) Since \( P \subset Z(G) \) and \( G/P \) is cyclic, \( G \) is abelian (Indeed, let \( g \) be a lift to \( G \) of a generator of \( G/P \). Then \( G = \langle g \cup P \rangle \), and since any two generators commute, so do any two elements of \( G \)). By our classification of abelian groups of finite order, clearly \( G \) has no choice but to be isomorphic to \( \mathbb{Z}/255\mathbb{Z} \).

4. (a) \((15 \text{ pt})\) Let \( A \) be an abelian group, and \( B \subset A \) a subgroup. Show that the quotient map \( A \to A/B \) splits if and only if there exists a subgroup \( C \subset A \) such that \( A = B \oplus C \).
(b) (10 pt) Let $A$ be a finite abelian group, and $B \subset A$ a subgroup. Suppose that $gcd(|B|, |A/B|) = 1$. Show that the quotient map $A \to A/B$ splits (i.e., that there exists a homomorphism $s : A/B \to A$ such that $q \circ s = id$). Hint: Think about the primary decomposition.

Solution:

(a) This is a sketch - the student should formalize this in the language that he prefers.

Suppose that $A \to A/B$ splits. Then, as we studied, if we denote by $C$ the image of a splitting homomorphism, we have $A = B \times C$. But in our abelian case, conjugation is trivial, and we obtain $A = B \times C$.

Suppose that $A = B \oplus C$ for some subgroup $C \subset A$. Then as we studied $A \to A/B$ splits (it is ”the same” as the epimorphism in the short exact sequence $0 \to B \to A \to C \to 0$...)

(b) As we studied, since $|B| \cdot |A/B|$ annihilates the whole of $A$, and $|B|, |A/B|$ are coprime, $A = A^{|B|} \oplus A^{|A/B|}$. Clearly $B \subset A^{|B|}$ by Lagrange’s theorem. But also $A^{|B|} \subset B$, because the projection $A^{|B|} \to A \to A/B$ is trivial (since the order of the source group is coprime to the order of the target group). Thus $B = A^{|B|}$. So we obtain $A = B \oplus A^{|A/B|}$, which shows that $B$ admits a complement in $A$, and hence by part (a) that $A \to A/B$ splits.