Soltution for the Midterm

M551 – Abstract Algebra

1. Let $H \triangleleft G$.

(a) Show that if G is finite and G/H has an element of order n, for some positive integer n, then G also has an element of order n.

Proof. Let $\bar{g} = gH \in G/H$ with $|\bar{g}| = n$.
If $g^k \in H$, then $\bar{g}^k = (gH)^k = g^k H = H = \bar{1}$ and thus $n \mid k$. In particular, if $k = |g|$ [since $|G| < \infty$], then $g^k = 1 \in H$ and $n \mid k$.
Therefore, $\left|g^{k/n}\right| = k/(k, k/n) = n$.

$\square$

(b) Show that the conclusion of part (a) doesn't always hold if G is infinite.

Proof. Let $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$. Then G/H has an element of order 2, but $\mathbb{Z}$ has only elements of order 1 or infinite order. $\square$

2. Let $H \leq \mathrm{Aut}(N)$, and assume that no non-identity element of H fixes *any* non-identity element of N. [I.e., if $h \neq 1$ and $n \neq 1$, then $h(n) \neq n$.] Let $G \stackrel{\text{def}}{=} N \rtimes H$ and identify N and H with the corresponding subgroups of G.

(a) Show that $H \cap gHg^{-1} = 1$ for all $g \in G - H$.

Proof. Let $g \in G - H$. Since $G = NH$ [with the proper identifications], we have that $g = nh$, with $n \neq 1$, and $gHg^{-1} = nHn^{-1}$.

Now, if $h_2 \in H \cap nHn^{-1}$, then there exists $h_1 \in H$ such that $nh_1n^{-1} = h_2$.

This implies that $nh_1n^{-1}h_1^{-1} = h_2h_1^{-1} \in H$. But, since $N \lhd G$, we have that $h_1n^{-1}h_1^{-1} = n_1 \in N$. In fact, by the construction of the semidirect product, $n_1 = h_1(n^{-1})$. So $nn_1 = h_2h_1^{-1} \in N \cap H = 1$. Thus, $n_1 = h_1(n^{-1}) = n^{-1}$ [and $h_2h_1^{-1} = 1$], and since $n \neq 1$ [and hence $n^{-1} \neq 1$], and with our assumption on the action of H, we must have that $h_1 = 1$. Since we also have $h_2h_1^{-1} = 1$, we get $h_2 = 1$.

Thus, $gHg^{-1} \cap H = nHn^{-1} \cap H = 1$.

□

(b) If G is finite, show that $G = N \cup \left(\bigcup_{g \in G} gHg^{-1} \right)$.

Proof. Again since $G = NH$, we have that $\bigcup_{g \in G} gHg^{-1} = \bigcup_{n \in N} nHn^{-1}$. If $n_1, n_2 \in N$ are such that $n_1Hn_1^{-1} \cap n_2Hn_2^{-1} \neq 1$, then, by (a), $n_1n_2^{-1} \in H \cap N = 1$, i.e., $n_1 = n_2$. So all the sets in $\bigcup_{n \in N} nHn^{-1}$ intersect only at 1, and hence,

$$\left| \bigcup_{g \in G} gHg^{-1} \right| = \left| \bigcup_{n \in N} nHn^{-1} \right| = |N| \cdot (|H| - 1) + 1.$$

[Note that $|nHn^{-1}| = |H|$.]

Moreover, if $m \in N \cap nHn^{-1}$, then $m = nhn^{-1}$ for some $h \in H$. But then, $n^{-1}mn = h \in N \cap H = 1$. So, $h = 1$ and thus $m = 1$. Therefore,

$$\left| N \cup \left(\bigcup_{g \in G} gHg^{-1} \right) \right| = |N| + \left| \bigcup_{g \in G} gHg^{-1} \right| - 1 = |N| \, |H| = |G| \, .$$

Since, clearly $N \cup \left(\bigcup_{g \in G} gHg^{-1} \right) \subseteq G$, we must have equality.

□

3. Prove that if G is nilpotent [possibly *infinite*], and $H < G$, then $H < N_G(H)$.

Proof. We prove by induction on the nilpotency class, say c, of G.

If $c = 1$, then $G = Z(G)$, and so G is abelian. Therefore, for all $H \leq G$, we have $N_G(H) = G$. Thus, if $H < G$, then $H < N_G(H) = G$.

Suppose the statement holds for all nilpotent groups of nilpotency class less than c. Let G be a group of nilpotency class c and $H < G$. If $Z \stackrel{\text{def}}{=} Z(G)$ is not contained in H, then there is an element $x \in Z - H$, which is clearly in $N_G(H)$. Since we always have $H \leq N_G(H)$, this means that $H < N_G(H)$.

So, suppose that $Z \leq H$, and consider $\bar{G} = G/Z$. So, $\bar{G}$ has nilpotency class $(c-1)$. [I showed in class that $Z_k(\bar{G}) = Z_{k+1}(G)/Z$.] Also, since $Z \leq H < G$, we have that $1 \leq \bar{H} \stackrel{\text{def}}{=} H/Z < \bar{G}$ by correspondence. By the induction hypothesis, $\bar{H} \underset{\neq}{\lhd} N_{\bar{G}}(\bar{H}) \leq \bar{G}$, and hence, by correspondence, there exists $N \leq G$ such that $N/Z = N_{\bar{G}}(\bar{H})$ and $H \underset{\neq}{\lhd} N \leq G$. Thus $H < N \leq N_G(H)$. [In fact, using the fact the $N_G(H)$ is the *maximal* subset of G in which H is normal, one can easily prove, using correspondence, that $N = N_G(H)$, but we don't need it here.]

□

4. Let G be a group with $|G| = p(p+1)$, where $p > 2$ is prime. Assume that G has no normal Sylow p-subgroup.

(a) Let $P \in \mathrm{Syl}_p(G)$, $|x| \neq 1, p$, and $S \stackrel{\text{def}}{=} \{1\} \cup \{yxy^{-1} : y \in P\}$. Prove that $|S| = p+1$, and if $z \in S$, then $z^2 = 1$.

Proof. By Sylow's Theorem, we must have that $n_p = (p+1)$. Since $p \nmid (p+1)$, we have that P is cyclic of order p, and hence we have $(p+1)(p-1) = p^2 - 1$ elements of order p in $|G|$, leaving only $(p+1)$ elements for all other possible orders.

Moreover, remember that $n_p = |G : N_G(P)|$, and hence $|N_G(P)| = p$. Since we always have $P \leq N_G(P)$, we must have, in fact, $P = N_G(P)$.

Let now $y_1, y_2 \in P$ such that $y_1 x y_1^{-1} = y_2 x y_2^{-1}$. Then, $x(y^{-1} y_2) = (y_1^{-1} y_2)x$, i.e., $x \in C_G(y_1^{-1} y_2)$. If $y_1 \neq y_2$, then $P = \langle y_1^{-1} y_2 \rangle$ [since every non-identity element of P generates P], and thus $x \in N_G(P)$. But $|x| \neq 1, p$, and hence $x \notin P = N_G(P)$. So, $y_1 x y_1^{-1} = y_2 x y_2^{-1}$ if, and only if, $y_1 = y_2$. Therefore, $|\{yxy^{-1} : y \in P\}| = |P| = p$.

Also, if $yxy^{-1} = 1$ for any $y \in P$, then $x = 1$, which cannot happen since $|x| \neq 1$. Therefore, $|S| = p+1$.

Note that if $|x| = r$, then $|yxy| = r$ for all $y \in G$. So, every non-identity element of S has order r.

But, by our initial remarks [in the first paragraph], observe that a non-identity element of G is either in a Sylow p-subgroup [and hence has order p] or in S [and hence has order r]. But, by Cauchy, since $2 \mid (p+1)$ [since p is odd], there is an element of order 2. This cannot be in a Sylow p-subgroup, since p is odd, and hence it is in S. Therefore, all non-identity elements of S have order 2 [i.e., $r = 2$].

□

(b) Prove that $(p+1) = 2^r$ for some positive integer r, and that G has a normal subgroup of order $(p+1)$.

Proof. By our work in part (a), an element in G has either order 1 [i.e., it's the identity], p [i.e., it's in a Sylow p-subgroup], or 2 [i.e., it's in S]. Hence, by Cauchy, there is no prime divisor for $p(p+1)$ besides p and 2. Since $p \nmid (p+1)$, we must have $(p+1) = 2^r$ for some positive integer r.

So, the Sylow 2-subgroup of G has order $2^r = (p+1) = |S|$. Also, since the elements of such group do not have order p, it must be contained in S, and therefore $S \in \mathrm{Syl}_2(G)$ [since they have the same order]. Since this argument holds for every Sylow 2-subgroup, it's unique, and hence normal.

Thus, G has a normal subgroup of order $(p+1) = 2^r$ [i.e., the Sylow 2-subgroup S].

$\square$