Midterm solutions

1. Let G be a finite group and $H, K \lhd G$ such that $H \cap K = \{1\}$.

   (a) Show that every element of HK can be written uniquely as a product hk for some $h \in H$ and $k \in K$.

   (b) Show that $HK \cong H \times K$.

   (c) Show that for an odd $n \geq 3$, $D_{4n} \cong D_{2n} \times \mathbb{Z}_2$.

   Solution. (a) We know from proof of Lesson Plan 2.2 (xiii) that since $|H \cap K| = 1$, we have $|HK| = |H||K|$, and the assertion follows. (Verify!)

   (b) We know from 3.2 (iv) of the Lesson Plan that $HK \leq G$. Consider the map
   $$\varphi : H \times K \to HK : (h, k) \overset{\varphi}{\mapsto} hk.$$
   Then φ is clearly well-defined since for $(h_1, k_1), (h_2, k_2) \in H \times K$, we have:
   $$(h_1, k_1) = (h_2, k_2) \implies h_1 = h_2 \text{ and } k_1 = k_2 \implies h_1k_1 = h_2k_2.$$
   Moreover, since $H, K \lhd G$, for $h \in H$ and $k \in K$, we have
   $$h(kh^{-1}k^{-1}) \in H \text{ and } (hkh^{-1})k^{-1} \in K,$$
   and so it follows that
   $$hkh^{-1}k^{-1} \in H \cap K.$$
   As $H \cap K = \{1\}$, we have $hkh^{-1}k^{-1} = 1$, which implies that
   $$hk = kh, \forall\, h \in H \text{ and } k \in K. \tag{1}$$
   Now, given $(h_1, k_1), (h_2, k_2) \in H \times K$, we have:
   $$\begin{aligned} \varphi((h_1, k_1)(h_2, k_2)) &= \varphi(h_1h_2, k_1k_2) \\ &= h_1h_2k_1k_2 && \text{(By definition of } \varphi\text{.)} \\ &= h_1k_1h_2k_2 && \text{(By (1) above.)} \\ &= \varphi((h_1, k_1))\varphi((h_2, k_2)), \end{aligned}$$

which shows that φ is a homomorphism. Furthermore, as φ is clearly bijective from 1 (a), we have $HK \cong H \times K$.

(c) Consider the subgroups $H = \langle r^2, s \rangle$ and $K = \langle r^n \rangle = \{1, r^n\}$ of $D_{4n} = \langle r, s \rangle$. Then $H \lhd D_{4n}$ since $[D_{4n} : H] = 2$ (Verify!) and furthermore, as $K = Z(D_{4n})$ (Verify!), we have $K \lhd D_{4n}$. The assertion now follows from 1 (b).

2. Let G be a group and let $g, h \in G$ such that g and h both commute with $[g, h] = ghg^{-1}h^{-1}$. Then show that $(gh)^n = g^n h^n [h, g]^{n(n-1)/2}$.

   Solution. We show this by inducting on n. To begin with, we observe that since g, h both commute with $[g, h]$, it follows that:

   $$h \text{ and } g \text{ both commute with } [g, h]^{-1} = [h, g]. \tag{2}$$

   When $n = 2$, we have:

   $$\begin{aligned} (gh)^2 &= ghgh \\ &= ghg(h^{-1}g^{-1}gh)h && \text{(By definition of } [h, g]) \\ &= g(hgh^{-1}g^{-1})(gh^2) && \text{(By basic group axioms.)} \\ &= g([h, g])(gh^2) && \text{(By definition of } [h, g].) \\ &= g^2h^2[h, g] && \text{(By (2).)} \end{aligned}$$

   Thus, the assertion holds for $n = 2$.

   Now, assuming that the result holds for $n = k$, we prove the assertion for $n = k + 1$. We have:

   $$\begin{aligned} (gh)^{k+1} &= gh(gh)^k \\ &= gh(g^k h^k [h, g]^{k(k-1)/2}) && \text{(By inductive hypothesis.)} \\ &= ghg(g^{k-1} h^k [h, g]^{k(k-1)/2}) && \text{(By basic group axioms.)} \\ &= g[h, g]gh(g^{k-1} h^k [h, g]^{k(k-1)/2}) && \text{(By definition of } [g, h].) \\ &= g^2h[h, g](g^{k-1} h^k [h, g]^{k(k-1)/2}) && \text{(By (2).)} \\ &= g^2hg^{k-1} h^k [h, g]^{k(k-1)/2+1} && \text{(By (2).)} \\ &= g^{\ell+1}hg^{k-\ell} h^k ([h, g]^{k(k-1)/2+\ell}) && \text{(By repeatedly applying (2).)} \\ &= g^{k+1} h^{k+1} ([h, g]^{k(k+1)/2}) && \text{(Taking } k = \ell.) \end{aligned}$$

   Thus, the assertion holds for all k.

3. Let G be a non-abelian group of order p^3, where p is an odd prime.

   (a) Show that $|Z(G)| = p$.

(b) Show that the derived group $[G,G] = Z(G)$.

(c) Show that the map $g \overset{\varphi}{\mapsto} g^p$, for all g, defines a homomorphism $\varphi : G \to Z(G)$.

Solution. (a) By the Class Equation, we have

$$p^3 = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)], \tag{3}$$

where the g_i are representatives of the distinct conjugacy classes of G not contained in $Z(G)$. By Lagrange's Theorem and the fact that $g_i \notin Z(G)$, we have that $[G : C_G(g_i)] = p$ or p^2. Thus, we have that p divides $\sum_{i=1}^{r}[G : C_G(g_i)]$ and since $p \mid p^3$, it follows from (3) that $p \mid |Z(G)|$. Therefore, by Lagrange's theorem, we have $|Z(G)| \in \{p, p^2, p^3\}$.

Clearly, $|Z(G)| \neq p^3$, for this would imply that G is abelian. Suppose that $|Z(G)| = p^2$, then $|G/Z(G)| = p$, and hence $G/Z(G)$ is cyclic, which would imply that G is abelian (see Quiz 2 of MTH 203). Therefore, by elimination we can infer that $|Z(G)| = p$.

(b) Since $|G/Z(G)| = p^2$ (by 3 (a)), and a group of order p^2 is abelian (Verify!), it follows that $G/Z(G)$ is abelian. Thus, by Problem 2(b) of the MTH 203 Final exam we have that $[G,G] \leq Z(G)$. Since, $|Z(G)| = p$ and G is non-abelian, it follows that $Z(G) = [G,G]$.

(c) The map $\varphi : G \to G : g \overset{\varphi}{\mapsto} g^p$ is clearly well-defined (Verify!). Furthermore, for $g, h \in G$, we have:

$$\begin{aligned} \varphi(gh) &= (gh)^p && \text{(By definition of } \varphi.\text{)} \\ &= g^p h^p [h,g]^{p(p-1)/2} && \text{(Since } [h,g] \in Z(G) \text{ and by Problem 2.)} \\ &= g^p h^p, && \text{(Since } [h,g] \in Z(G) \text{ and } |Z(G)| = p.\text{)} \end{aligned}$$

from which it follows that φ is a homomorphism.

Now, for any $g, h \in G$, we have $\varphi([g,h]) = [\varphi(g), \varphi(h)]$, from which it follows that $\varphi([G,G]) \leq [G,G]$. Thus, as $[G,G] \trianglelefteq G$, φ induces a homomorphism

$$\bar{\varphi} : G/[G,G] \to G/[G,G] : g[G,G] \overset{\bar{\varphi}}{\mapsto} g^p[G,G].$$

Since $G/[G,G]$ is an abelian group (as $|G/[G,G]| = p^2$), we have $g^p[G,G] = (g[G,G])^p$. Furthermore, as $G/[G,G]$ is non-cyclic (since

G is non-abelian), it follows from the Lagrange's theorem that every non-trivial element of $G/[G,G]$ has order p. Consequently, we have

$$g^p[G,G] = (g[G,G])^p = [G,G],$$

from which it follows that $g^p \in [G,G]$. Therefore, for any $g \in G$, we have $g^p \in [G,G]$, or in other words, $\varphi(G) \leq [G,G]$.

4. Show that a group G of order 24 is non-simple.

   Solution. The action $G \curvearrowright G/H$ by left-multiplication induces a permutation representation $\psi : G \to S(G/H) \cong S_3$ (since $|G/H| = 3$). By the First Isomorphism Theorem, we have

   $$G/\ker\psi \cong \psi(G).$$

   Since $\psi(G) \leq S(G/H)$, by the Lagrange's theorem, $|G/\ker\psi|$ must divide 6, which implies that

   $$4 \mid |\ker\psi|. \tag{4}$$

   Moreover, for any $g' \in \ker\psi$, we have $\psi(g') = id_{G/H}$, which implies that

   $$gH = g' \cdot (gH) = (g'g) \cdot H,$$

   which implies that $(g'g)g^{-1} = g' \in H$. Thus, it follows that $\ker\psi \leq H$, and so we have

   $$|\ker\psi| \mid 8. \tag{5}$$

   From (4) and (5), we have $|\ker\psi| \in \{4, 8\}$ and thus $\ker\psi$ is a proper normal subgroup of G showing that G is non-simple.