Written Homework # 3 Solution

12/01/08

Here is the basis for a solution to the first two problems.

Lemma 1 *Suppose G is a group, p is a positive prime, and G has s cyclic subgroups of order p. Then the number of elements of G of order p is $s(p-1)$.*

PROOF: Suppose that $H_1, \ldots, H_s$ are the subgroups of order p. Then the non-identity elements of these subgroups account for the elements of G of order p by Lagrange's Theorem. Suppose $H_i \cap H_j \neq (e)$. Choose $e \neq a \in H_i \cap H_j$. Then $a \in H_i, H_j$ and has order p. Thus $H_i = (a) = H_j$. Consequently $H_1 \backslash \{e\} \cup \cdots \cup H_s \backslash \{e\}$ describes a partition of the elements of G of order p. □

For a finite group G and positive prime p we let n_p denote the number of Sylow p-subgroups of G. If $|G| = p^n m$, where $n \geq 1$ and $(m, p) = 1$, then $n_p = 1 + kp$ for some non-negative integer k and $n_p \,|\, |G|$. Thus $n_p | m$.

There is a corollary to the proof of the lemma which is stated here for the record. It is generalization of the lemma.

Corollary 1 *Suppose G is a group, d is a positive integer, and G has n_d cyclic subgroups of order d. Then the number of elements of G of order d is $n_d \varphi(d)$, were φ is the Euler phi-function.* □

1. (**20 points**) Most of the basic details are taken care of by Lemma 1. Since p, q divide $|G|$ it follows by the Sylow Theorems that $n_p, n_q \geq 1$. Suppose that no Sylow q-subgroup is normal. Then $n_q > 1$ which means $n_q = 1 + q = p^n$. The number of elements in G of order q is therefore $n_q(q-1) = p^n(q-1) = p^n q - p^n = |G| - p^n$ by Lemma 1.

Let $S \subseteq G$ be the subset of all elements which do not have order q. Then $|S| = p^n$. Let P be a Sylow p-subgroup of G. Then elements of P have order p^ℓ for some $0 \leq \ell \leq n$. Therefore $P \subseteq$S which means $P = S$ since $|S| = p^n = |P|$. Thus P is the only Sylow p-subgroup of G which means that P is normal. We have shown that G is not simple.

2. (**20 points**) We may assume $p < q < r$. Assume that G is simple. Then $n_p, n_q, n_r > 1$. Since $n_p | qr$, $n_q | pr$, and $n_r | pq$ it follows that $n_p \geq q$, $n_q \geq r$ and $n_r = pq$. The number of elements of orders p, q, and r respectively account for

$$\ell = n_p(p-1) + n_q(q-1) + n_r(r-1) \geq q(p-1) + r(q-1) + pq(r-1) = pqr - q - r + rq.$$

Now $1/q + 1/r < 1$ as $2 \leq p < q < r$. Therefore $0 < -r - q + rq$. We have shown that $|G| \geq \ell > |G| - q - r + qr > |G|$, a contradiction. Therefore G is not simple (indeed one of its Sylow subgroups is normal).

3. (**20 points**) Since $p \,|\, |G|$ there is a Sylow p-subgroup for G. Let $e \neq a \in G$. Since $|G|$ is a power of p it follows that (a) as order a power of p by Lagrange's Theorem. By the theory of cyclic groups (a) contains an element of order p.

4. (**20 points**) By assumption $|G : H| \leq n - 1$. Let A be the set of left cosets of H in $G = S_n$ and let $\pi : G \longrightarrow S_A$ be the group homomorphism defined by $\pi(g)(aH) = gaH$ for all $g \in G$ and $aH \in A$. Recall that $\mathrm{Ker}\,\pi \subseteq H$. Since $|G| = n!$ and $|S_A| = |G : H|! \leq (n-1)!$ it follows that π is not injective. Therefore $\mathrm{Ker}\,\pi \neq (e)$.

Note that $\ker \pi \cap A_n$ is a normal subgroup of A_n. Since $n \geq 5$ the group A_n is simple. Therefore $\ker \pi \cap A_n = A_n$ or $\ker \pi \cap A_n = (e)$.

Suppose that $\ker \pi \cap A_n = A_n$. Then $A_n \subseteq \mathrm{Ker}\,\pi \subseteq H$. Since $|G : H| \leq |G : A_n| = 2$ it follows that $|G : H| = 1$, in which case $H = G$, or $|G : H| = 2$, in which case $H = A_n$. (We use the fact that $|G| = |G : H||H|$ for a finite group G and subgroup H.)

We will show that $\ker \pi \cap A_n = (e)$ is not possible which will complete the proof. Suppose the equations holds. Then $|\ker \pi||A_n| = |(\ker \pi)A_n| \leq |G| = 2|A_n|$ which means that $|\ker \pi| \leq 2$. By the first isomorphism theorem

$$|G|/|\mathrm{Ker}\,\pi| = |G/\mathrm{Ker}\,\pi| = |\mathrm{Im}\,\pi| \leq |S_A| \leq (n-1)!.$$

Therefore $n! = |G| \leq 2(n-1)!$, or $n \leq 2$, a contradiction. Thus $\ker \pi \cap A_n \neq (e)$.

5. (**20 points**) This is basically a matter of patience.

(a) Let $P = G_1 \times G_2$ be the "product" of groups and $\pi_i : P \longrightarrow G_i$ for $i = 1, 2$ be defined by $\pi_i((g_1, g_2)) = g_i$ for all $(g_1, g_2) \in P$. For $(g_1, g_2), (g_1', g_2') \in P$ the calculation

$$\pi_i((g_1, g_2)(g_1', g_2')) = \pi_i((g_1 g_1', g_2 g_2')) = g_i g_i' = \pi_i((g_1, g_2))\pi_i((g_1', g_2'))$$

shows that π_i is a homomorphism.

Suppose that P is a group and $\pi_i' : P' \longrightarrow G_i$ are group homomorphisms. Suppose further that $F : P' \longrightarrow P$ is a group homomorphism such that $\pi_i \circ F = \pi_i'$ for $i = 1, 2$. For $a \in P'$ the calculation

$$\pi_i(F(a)) = (\pi_i \circ F)(a) = \pi_i'(a)$$

shows that $F(a) = (\pi_1'(a), \pi_2'(a))$. Therefore there is at most one group homomorphism $F : P' \longrightarrow P$ such that $\pi_i \circ F = \pi_i'$ for $i = 1, 2$.

Define a function $F : P' \longrightarrow P$ by $F(a) = (\pi_1'(a), \pi_2'(a))$ for all $a \in P'$. Thus $\pi_i'(a) = \pi_i(F(a)) = (\pi_i \circ F)(a)$ for all $a \in P'$ which means $\pi_i' = \pi_i \circ F$ for $i = 1, 2$. For $a, a' \in P'$ note that

$$F(aa') = (\pi_1'(aa'), \pi_2'(aa')) = (\pi_1'(a)\pi_1'(a'), \pi_2'(a)\pi_2'(a')) = (\pi_1'(a), \pi_2'(a))(\pi_1'(a'), \pi_2'(a')) = F(a)F(a')$$

and thus F is a group homomorphism.

(b) Suppose that (P, π_1, π_2) and (P', π'_1, π'_2) are products of G_1 and G_2. Then there is a group homomorphism $F : P' \longrightarrow P$ which satisfies $\pi_i \circ F = \pi'_i$ for $i = 1, 2$. Since (P', π'_1, π'_2) and (P, π_1, π_2) are products of G_1 and G_2, there is a group homomorphism $F' : P \longrightarrow P'$ which satisfy $\pi'_i \circ F' = \pi_i$ for $i = 1, 2$. Note $F \circ F' : P \longrightarrow P$ satisfies

$$\pi_i \circ (F \circ F') = (\pi_i \circ F) \circ F' = \pi'_i \circ F' = \pi_i.$$

As $\mathrm{Id}_P : P \longrightarrow P$ satisfies $\pi_i \circ \mathrm{Id}_P = \pi_i$ for $i = 1, 2$ also, by uniqueness $F \circ F' = \mathrm{Id}_P$. Therefore $F' \circ F = \mathrm{Id}_{P'}$. These last two equations establish that F and F' are inverses of each other.