Homework 5 Solutions

Enrique Treviño

February 26, 2016

1 Chapter 5

Problem 1. (**Exercise 1**)
Suppose that G is a finite group with an element g of order 5 and an element h of order 7. Why must $|G| \geq 35$?

Solution 1. Let $|G| = n$. Since $\langle g \rangle$ is a subset of G, then $|g| \mid n$. Therefore $5 \mid n$. Similarly $|h| \mid n$, so $7 \mid n$. Since $5 \mid n$ and $7 \mid n$, then $35 \mid n$. Since n is a positive integer, then $n \geq 35$.

Problem 2. (**Exercise 3**)
Prove or disprove: Every subgroup of the integers has finite index.

Solution 2. To turn in.

Problem 3. (**Exercise 5**)
List the left cosets of the subgroups in each of the following.

(a) $\langle 8 \rangle$ in $\mathbb{Z}_{24}$

(b) $\langle 3 \rangle$ in $U(8)$

(c) $3\mathbb{Z}$ in $\mathbb{Z}$

(d) A_4 in S_4

(e) A_n in S_n

(f) D_4 in S_4

Solution 3.

(a) The cosets are: $\{0, 8, 16\}, \{1, 9, 17\}, \{2, 10, 18\}, \{3, 11, 19\}, \{4, 12, 20\}, \{5, 13, 21\}, \{6, 14, 22\}, \{7, 15, 23\}$.

(b) To turn in.

(c) One coset is $H = 3\mathbb{Z}$. Since $1 \notin 3\mathbb{Z}$, then $1H$ is a different coset. $1H = \{3n + 1 | n \in \mathbb{Z}\}$, (i.e., $1H = \{1, 4, 7, 10, 13, \ldots\} \cup \{-2, -5, -8, \ldots\}$). Since $2 \notin (H \cup 1H)$, then $2H$ is a different coset. $2H = \{3n + 2 \mid n \in \mathbb{Z}\}$, i.e., $2H = \{2, 5, 8, 11, \ldots\} \cup \{-1, -4, -7, \ldots\}$. Since these three cosets partition $\mathbb{Z}$, there are no more cosets.

(d) To turn in.

(e) If $n \geq 2$, then A_n is half the size of S_n, so $[S_n : A_n] = 2$. Therefore there are only two cosets. One coset is A_n and the other coset is what is left, i.e., the other coset is $S_n \setminus A_n = \{\sigma \in S_n \mid \sigma \notin A_n\} = \{\sigma \in S_n \mid \sigma \text{ is an odd permutation }\}$. So one coset is the even permutations and the other is the odd permutations.

If $n = 1$, then $A_1 = S_1$, so the only coset is A_1.

(f) To turn in.

Problem 4. (**Exercise 8**)
Use Fermat's Little Theorem to show that if $p = 4n+3$ is prime, there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.

Solution 4. Let $G = \mathbb{Z}_p^\times$, i.e., G is the multiplicative group modulo p. Suppose $x^2 \equiv -1 \pmod{p}$. Then $x \not\equiv 0 \pmod{p}$, therefore $x \in G$.

Since $x^2 \equiv -1 \pmod{p}$, then $x^4 \equiv 1 \pmod{p}$. If $x \equiv 1 \pmod{p}$, then $x^2 \equiv 1 \pmod{p}$. Then $1 \equiv -1 \pmod{p}$, so $2 \equiv 0 \pmod{p}$, so $p = 2$. But since $p = 4n+3$, $p \neq 2$. Therefore $x \not\equiv 1 \pmod{p}$. Since $x \not\equiv 1 \pmod{p}$ and $x^2 \not\equiv 1 \pmod{p}$ and $x^4 \equiv 1 \pmod{p}$, then the order of x in G is 4. By Langrange's theorem $4 \mid |G|$. But the order of G is $p - 1 = 4n + 2$. $4n + 2$ is not a multiple of 4, therefore we've reached a contradiction. Therefore no $x \in G$ satisfies $x^2 \equiv -1 \pmod{p}$.

Solution using Fermat's little theorem: Above I included a solution using group theory. Now, let's just use Fermat's little theorem.

Suppose that $x^2 \equiv -1 \pmod{p}$. Then $x \not\equiv 0 \pmod{p}$, therefore by Fermat's little theorem $x^{p-1} \equiv 1 \pmod{p}$. Therefore

$$x^{p-1} \equiv x^{4n+2} \equiv (x^2)^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{p}.$$

Therefore $1 \equiv -1 \pmod{p}$, so $2 \equiv 0 \pmod{p}$, so $p \mid 2$, so $p = 2$. Since $p \neq 2$, then there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.

Problem 5. (**Exercise 11**)
Let H be a subgroup of a group G and suppose that $g_1, g_2 \in G$. Prove that the following conditions are equivalent.

(a) $g_1 H = g_2 H$

(b) $H g_1^{-1} = H g_2^{-1}$

(c) $g_1 H \subseteq g_2 H$

(d) $g_2 \in g_1 H$

(e) $g_1^{-1} g_2 \in H$

Solution 5. I will include the proof that (b) implies (d). To turn in you have to prove (a) implies (c).

Suppose $Hg_1^{-1} = Hg_2^{-1}$. We want to show $g_2 \in g_1 H$. Since $e \in H$ and $g_1^{-1} = eg_1^{-1}$, then $g_1^{-1} \in Hg_1^{-1}$. Since $Hg_1^{-1} = Hg_2^{-1}$, then $g_1^{-1} \in Hg_2^{-1}$. Therefore there exists $h \in H$ such that $g_1^{-1} = hg_2^{-1}$. Therefore

$$\begin{aligned} g_1(g_1^{-1})g_2 &= g_1(hg_2^{-1})g_2 \\ g_2 &= g_1 h. \end{aligned}$$

Therefore $g_2 \in g_1 H$. This proves that $Hg_1^{-1} = Hh_2^{-1}$ implies $g_2 \in g_1 H$. Now let's prove the reverse direction.

Suppose $g_2 \in g_1 H$. Then there exists an $h \in H$ such that $g_2 = g_1 h$. Therefore $g_1^{-1} g_2 = h$, so $g_1^{-1} = hg_2^{-1}$.

We want to prove that $Hg_1^{-1} = Hg_2^{-1}$. Let $x \in Hg_1^{-1}$. Then there exists $h' \in H$ such that $x = h' g_1^{-1}$. So $x = h'(hg_2^{-1}) = (h'h)g_2^{-1}$. Since $h'h \in H$ because H is a subgroup of G, then $h'hg_2^{-1} \in Hg_2^{-1}$, so $x \in Hg_2^{-1}$. Therefore $Hg_1^{-1} \subseteq Hg_2^{-1}$.

Now, suppose that $x \in Hg_2^{-1}$. Therefore there exists $h'' \in H$ such that $x = h'' g_2^{-1}$. Since $g_2 = g_1 h$, then $g_2^{-1} = h^{-1} g_1^{-1}$. Therefore $x = h'' h^{-1} g_1^{-1}$. Since $h'' h^{-1} \in H$, then $x \in Hg_1^{-1}$. Therefore $Hg_2^{-1} \subseteq Hg_2^{-1}$. Therefore $Hg_1^{-1} = Hg_2^{-1}$.

This proves that (b) and (d) are equivalent.

Problem 6. (**Exercise 17**)
Suppose that $[G : H] = 2$. If a and b are not in H, show that $ab \in H$.

Solution 6. To turn in.

Problem 7. (**Exercise 18**)
If $[G : H] = 2$, prove that $gH = Hg$.

Solution 7. To turn in.

Problem 8. (**Exercise 22**)
Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes. Prove that

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Solution 8. Let's prove that $\phi(mn) = \phi(m)\phi(n)$ if $\gcd(m,n) = 1$. Let $a \le m$ be relatively prime to m. Now consider $\{a, a+m, a+2m, \ldots, a+(n-1)m\}$. All of these numbers are relatively prime to m because a is relatively prime to m and $m|km$. If we look modulo n, then since m and n are relatively prime $\{a, a+m, a+2m, \ldots, a+(n-1)m\} \equiv \{0, 1, 2, \ldots, n-1\} \pmod{n}$ (in a different order). Therefore there are $\phi(n)$ numbers relatively prime to n in $\{a, a+m, a+2m, \ldots, a+(n-1)m\}$. Since there are $\phi(m)$ possibilities for a and for each a there are $\phi(n)$ numbers $\le mn$ relatively prime to m and n, then there are $\phi(m)\phi(n)$ numbers relatively prime to mn, so $\phi(mn) = \phi(m)\phi(n)$.

Now let's calculate $\phi(p^k)$. Among the numbers $1, 2, 3, \ldots, p^k$ the only numbers relatively prime to p^k are $p, 2p, 3p, \ldots, p^{k-1}p$. Therefore $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$. Since ϕ satisfies that $\phi(ab) = \phi(a)\phi(b)$ whenever $\gcd(a,b) = 1$, then if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, we have:

$$\begin{aligned}
\phi(n) &= \phi(p_1^{e_1})\phi(p_2^{e_2})\cdots\phi(p_k^{e_k}) \\
&= p_1^{e_1}\left(1 - \frac{1}{p_1}\right)p_2^{e_2}\left(1 - \frac{1}{p_2}\right)\cdots p_k^{e_k}\left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

Alternative Solution: Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Consider the following sets:

- $A_{p_1} = \{m \le n : p_1|m\}$,
- $A_{p_2} = \{m \le n : p_2|m\}$,
- $\cdots$,
- $A_{p_k} = \{m \le n : p_k|m\}$.

If $gcd(m,n) \ne 1$, then m is divisible by p_i for some i, so $m \in A_{p_i}$. Therefore

$$\phi(n) = n - |A_{p_1} \cup A_{p_2} \cup \cdots \cup A_{p_k}|.$$

Now

$$|A_{p_{i_1}} \cap A_{p_{i_2}} \cap \cdots A_{p_{i_r}}| = \frac{n}{p_{i_1}p_{i_2}\cdots p_{i_r}}.$$

Therefore by inclusion-exclusion:

$$\begin{aligned}
\phi(n) &= n - |A_{p_1}| - \ldots - |A_{p_k}| + |A_{p_1} \cap A_{p_2}| + \ldots + (-1)^r|A_{p_{i_1}} \cap A_{p_{i_2}} \cap \cdots A_{p_{i_r}}| + \ldots + (-1)^k|A_{p_1} \cap \cdots A_{p_k}| \\
&= n - \frac{n}{p_1} - \frac{n}{p_2} - \ldots - \frac{n}{p_k} + \frac{n}{p_1p_2} + \ldots + (-1)^r\frac{n}{p_{i_1}p_{i_2}\cdots p_{i_r}} + \ldots + \frac{n}{p_1p_2\cdots p_k} \\
&= n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \frac{1}{p_1p_2} + \ldots + (-1)^r\frac{1}{p_{i_1}p_{i_2}\cdots p_{i_r}} + \ldots + (-1)^k\frac{1}{p_1p_2\cdots p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

Problem 9. (**Exercise 23**)
Show that

$$n = \sum_{d|n} \phi(d)$$

for all positive integers n.

Solution 9. Let $m \in \{1, 2, 3, \ldots, n\}$. Let $\gcd(m, n) = d$. Then $m = dm'$ and $n = dn'$ where $\gcd(m', n') = 1$ and $m' \leq n'$. Note that $n' = n/d$ and that $d|n$. Now consider all numbers m such that $\gcd(m, n) = d$. The numbers satisfy that m/d is relatively prime with n/d and less than or equal to n/d. Also, as long as those requirements are satisfied, then $(m, n) = d$. Therefore there are

$$\phi\left(\frac{n}{d}\right)$$

numbers m satisfying that $\gcd(m, n) = d$ whenever $d|n$. Since every number $m \in \{1, 2, 3 \ldots, n\}$ has a gcd with n that divides n, then if for each $d|n$ we count all numbers that have gcd d with n, we get n. This is because we are partitioning the set $\{1, 2, \ldots, n\}$ into the gcd that each number has with n. Therefore

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = n.$$

But if $d|n$, then $\frac{n}{d}|n$ as well, so

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d).$$

The conclusion follows.

Alternative phrasing of the solution:
Consider the relation $\sim$ on the set $\{1, 2, 3, \ldots, n\}$, where $a \sim b$ if $\gcd(a, n) = \gcd(b, n)$. It is not hard to show that $\sim$ is an equivalence relation. Therefore $\sim$ partitions the set $\{1, 2, 3, \ldots, n\}$. Let C_d be the equivalence class of the number d. Then $C_d = \{m \leq n : \gcd(m, n) = d\}$. $C_d = \emptyset$ whenever $d \not| n$, therefore C_d partitions $\{1, 2, 3, \ldots, n\}$ whenever d ranges over the divisors of n. Therefore

$$n = \sum_{d|n} |C_d|.$$

As proven above

$$|C_d| = \phi\left(\frac{n}{d}\right).$$

The proof concludes the same way as the original proof.

One more solution:
Let

$$g(n) = \sum_{d|n} \phi(d).$$

Our goal is to show that $g(n) = n$. We will prove that g is multiplicative, i.e., that if $\gcd(a, b) = 1$, then $g(ab) = g(a)g(b)$. Let $d|ab$. We're going to need to prove that there exist unique $d_1|a$ and $d_2|b$ such that $d = d_1 d_2$. Let $d_1 = \gcd(a, d)$ and $d_2 = \gcd(b, d)$. Then d_1 and d_2 are unique. Now let's show that $d_1 d_2 = d$. Since $d_1 = \gcd(a, d)$, then $1 = \gcd\left(\frac{a}{d_1}, \frac{d}{d_1}\right)$. Now $\frac{d}{d_1}|\frac{ab}{d_1}$ and $\frac{d}{d_1}$ is relatively prime so by Exercise 27 in Chapter 2 (done in HW 1), then $\frac{d}{d_1}|b$. Since a and b are relatively prime, then $\gcd\left(\frac{d}{d_1}, b\right) = \gcd(d, b) = d_2$. But since $\frac{d}{d_1}|b$, then $\gcd\left(\frac{d}{d_1}, b\right) = \frac{d}{d_1}$. Therefore $\frac{d}{d_1} = d_2$. Therefore $d = d_1 d_2$.

Okay, so we have proven that if $d|ab$ and $\gcd(a, b) = 1$, then there exist unique $d_1|a$ and $d_2|b$. Therefore

$$g(ab) = \sum_{d|ab} \phi(d) = \sum_{\substack{d_1|a \\ d_2|b}} \phi(d_1 d_2) = \sum_{d_1|a} \sum_{d_2|b} \phi(d_1 d_2).$$

Now, since $\gcd(a,b) = 1$ and $d_1|a$ and $d_2|b$, then $\gcd(d_1,d_2) = 1$. Since $\phi(ab) = \phi(a)\phi(b)$ whenever $\gcd(a,b) = 1$, then $\phi(d_1d_2) = \phi(d_1)\phi(d_2)$. Therefore

$$g(ab) = \sum_{d_1|a}\sum_{d_2|b}\phi(d_1d_2) = \sum_{d_1|a}\sum_{d_2|b}\phi(d_1)\phi(d_2) = \left(\sum_{d_1|a}\phi(d_1)\right)\left(\sum_{d_2|b}\phi(d_2)\right) = g(a)g(b).$$

Now,

$$\begin{aligned}
g(p^k) = \sum_{d|p^k}\phi(d) &= \phi(1) + \phi(p) + \phi(p^2) + \ldots + \phi(p^k) \\
&= 1 + p\left(1 - \frac{1}{p}\right) + p^2\left(1 - \frac{1}{p}\right) + \ldots + p^k\left(1 - \frac{1}{p}\right) \\
&= 1 + p\left(1 - \frac{1}{p}\right)\left(1 + p + p^2 + \ldots + p^{k-1}\right) \\
&= 1 + (p-1)\left(\frac{p^k - 1}{p - 1}\right) = 1 + (p^k - 1) = p^k.
\end{aligned}$$

Since $g(p^k) = p^k$ and $g(ab) = g(a)g(b)$ whenever $\gcd(a,b) = 1$, then $g(n) = n$. The proof is complete.