Midterm 2- 110AH

Asher Christian 006-150-286

04.12.24

1 Problem 5

Let $HK := \{hk | h \in H, k \in K\}$. Then (clearly) $H/(H \cap K)$ is a subset of $G/(H \cap K)$ and HK/K is a subset of G/K. Show that $f : H/(H \cap K) \to HK/K$ by $h(H \cap K) \to hK$ is a well-defined bijection. In particular, if G is a finite group, then $|HK||H \cap K| = |H||K|$.

1. (i) First to show that f is one-one.

$$\begin{aligned} f(h_1(H \cap K)) &= f(h_2(H \cap K)) \\ \implies h_1 K &= h_2 K \\ h_1 &\equiv h_2 \mod K \\ \implies h_1^{-1} h_2 &\in K \\ \text{Because the domain is } H/(H \cap K)\ h_1, h_2 &\in H \\ \implies h_1^{-1} h_2 &\in H \\ h_1^{-1} h_2 &\in (H \cap K) \\ \implies h_1 &\equiv h_2 \mod (H \cap K) \\ h_1(H \cap K) &= h_2(H \cap K) \end{aligned}$$

   Which shows that if the outputs are the same the inputs must be the same. for onto consider any element $g \in HK$ by definition $g = h_1 k_1$ with $h_1 \in H, k_1 \in K$

$$gK = h_1 k_1 K = h_1 K.$$

   and so

$$f(h_1(H \cap K)) = h_1 K.$$

   and $h_1(H \cap K)$ is in $H/(H \cap K)$ because $h_1 \in H$ so f is onto and thus a bijection.

2. (ii) To prove the equation note that because f is a bijection the number of elements of $H/(H \cap K)$ also known as the index $|H : H \cap K|$ is equal to the number of elements of HK/K which is written as the index $|HK : K|$

which are both less than infinity because G is finite and so every subgroup and coset must be finite.
I now split into two cases. If HK is a subgroup of G or if it is not.
If HK is a subgroup then because $H \cap K$ is a subgroup by lagrange's theorem

$$\begin{aligned} |H| &= |H : H \cap K||H \cap K| \\ |HK| &= |HK : K||K| \\ \frac{|H|}{|H \cap K|} &= \frac{|HK|}{|K|} \\ |HK||H \cap K| &= |H||K| \end{aligned}$$

note that $H \cap K$ is a subgroup because H and K are subgroups and they both contain the identity and if

$$g \in H \cap K \rightarrow g^{-1} \in H \cap K.$$

because H and K are subgroups so they contain their inverses and

$$g_1, g_2 \in H \cap K \rightarrow g_1 g_2 \in H \cap K.$$

This is because H and K are subgroups and contain all combinations of elements within them.
In the second case HK is not a subgroup the same formula still holds. This is because K is a subgroup and so all of the cosets in G are well defined and unique (i.e. a element of G can map to only one coset).
additionally since K is a subgroup all cosets have cardinality K. Lastly each coset defined by $HK/K := \{gK : g \in HK\}$ is disjoint and every element of HK maps to exactly one and elements of HK map to all unique instances of the coset (this is important) because for every coset hK there exists $hk_i \in HK$ for i ranging over the elements in K that maps to every element of the coset hK. This means that the number of representatives for each coset is equal to $|K|$ in HK. Therefore the total number of such cosets is equal to $|HK|/|K|$ which is what we used in the previous part to prove the statement.

2 Problem 6

Suppose that G is a finite group. Show $[G : H \cap K] \leq [G : K][G : H]$ with equality if $[G : H]$ and $[G : K]$ relatively prime.
H and K are subgroups. we know the following facts from lagrange's theorem,

the fact that G is a finite group, and from the previous question.

$$[G : H \cap K] = \frac{|G|}{|H \cap K|}$$
$$(i)\ \ [G : H] = \frac{|G|}{|H|}$$
$$(ii)\ \ [G : K] = \frac{|G|}{|K|}$$
$$|H \cap K| = \frac{|H||K|}{|HK|}$$

now assume for contradiction that the inequality were false and so

$$[G : H \cap K] > [G : H][G : K]$$
$$\frac{|G|}{|H \cap K|} > \frac{|G|^2}{|H||K|}$$
$$\frac{|HK||G|}{|H||K|} > \frac{|G|^2}{|H||K|}$$
$$|HK||G| > |G|^2$$
$$|HK| > |G|$$

this is a contradiction because $|HK| \leq |G|$ for every element of HK is an element of G by definition and this inequality is strict unless H and K generate G. It is clear that for equality to hold $|HK| = |G|$ must hold. The only way for this to happen is if $|HK| = |G|$. By (i) and (ii) if $[G : H]$ and $[G : K]$ are prime then $|H|$ and $|K|$ must be relatively prime and $|H||K|$ must equal $|G|$ Since $|H|$ and $|K|$ are comprime the order of any two elements one from each must be coprime and thus $|H \cap K| = 1$ and so we get

$$[G : H \cap K] = \frac{|G|}{|H \cap K|} = |G| = \frac{|G|^2}{|G|} = \frac{|G|^2}{|H||K|} = [G : H][G : K].$$

3 Problem 11

let p be an odd prime. Prove that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$. [You may use the fact that the polynomial $t^n - 1$ has at most n roots in $(\mathbb{Z}/p\mathbb{Z})[t]$ for any $n > 0$.]

To prove this first prove that if G is a finite abelian group and $a, b \in G$ are such that $|a| = A, |b| = B$ and $lcm(A, B) = C$ then there exists $c \in G$ such that $|c| = C$. we have that for general $n, m \in \mathbb{Z}$ $nm = gcd(n, m)lcd(n, m)$ because

$$n = p_1^{l_1} p_2^{l_2} ... p_n^{l_n}.$$

$$m = p_1^{k_1}...p_n^{k_n}.$$

$$lcm(n,m) = p_1^{\max(l_1,k_1)}...p_n^{\max(l_n,k_n)}.$$

$$gcd(n,m) = p_1^{\min(l_1,k_1)}...p_n^{\min(l_n,k_n)}.$$

$$gcd(n,m)lcm(n,m) = p_1^{l_1+k_1}...p_n^{l_n+k_n} = nm.$$

The final equality is due to the fact that whichever l or k is picked for each p in lcm the opposite will be picked for gcd and in the case where $k_i = l_i$ it does not matter which one is picked.
There are two cases either A, B are mutually prime or not in the first case

$$AB = C.$$

$$(ab)^C = a^C b^C = e.$$

This is because G is abelian and $A|C$ and $B|C$ so $a^C = e = b^C$. if $|ab| \neq C$ it must be equal to $r < C$ and $(ab)^r = e$ so $a^r b^r = e$ set $w = a^r$ then $b^r w = e$ so $w = b^{-r}$ however since w is in the span of both a and r its order must divide A and R. However the gcd of A and R is one so its order must be one. And so $a^r = b^r = e$ both $A|r$ and $B|r$ so r is a common multiple and thus must be greater than C since C is the least common multiple if it doesn't equal C and thus the element (ab) has order C.

In the second case $AB = CG$ for $G = gcd(A, B)$

$$G = p_1^{r_1}...p_n^{r_n}.$$

We know that for each p_i, r_i is the minimum power of p_i and that the particular power occurs in either A or B.
And so by choosing the element for which the power is lower say A we can consider $gcd(\frac{A}{p_i}, B) = \frac{G}{p_i}$ Additionally $lcm(\frac{A}{p_i}, B) = C$ because the maximum l_i or k_i is unchanged. For this to be useful we note that $|(a^{p_i})| = \frac{A}{p_i}$ because $(a^{p_i})^{\frac{A}{p_i}} = a^A = e$ and no smaller power would work because it would result in a power that is smaller than A of a.
Thus we have constructed a way to reduce the gcd while keeping the lcm the same by choosing different elements of the original cycles. Inductively setting $a' = a^{p_i}$ and $b' = b^{p_i}$ for a different i in each step. This process terminates when $G = 1$. In particular when $G = 1$ we have two groups generated by a^{n_1}, b^{n_2} where $n_1 n_2 = gcd(a, b)$. and since $gcd(|a^{n_1}|, |b^{n_2}|) = 1$ from the argument of the gcd = 1 case we have that $|a^{n_1} b^{n_2}| = C = lcm(a^{n_1}, b^{n_2}) = lcm(a, b)$ and thus we have found an element with order C.
By this result we also have that there exists an element that has the order of the least common multiple the order of every element of a set because if we list every element $g_1, g_2, ..., g_n$ we we create g_{i_2} an element with order $lcm(g_1, g_2)$ and g_{i_3} has order $lcm(g_{i_2}, g_3)$ repeating inductively until g_{i_n} which has order equal to the lcm of every element in the group. This follows from the fact taht

the lcm of multiple numbers is well defined and does not depend on order.

To prove the cyclic nature of $\mathbb{Z}/p\mathbb{Z} = Z$ under multiplication first note that Z is finite and abelian for $a * b = b * a$. Assume for contradiction that every element $z \in Z$ has $|z| \neq p-1$. There are $p-1$ elements in Z because it includes congruency classes for every integer up to but not including p and not including 0. Under this assumption there exists some element c of order C where C is the least common multiple of all $z \in Z$. assume that $C \neq p-1$ then we have for all z, $z^C = e$. This means that each z satisfies $t^C - 1 = 0$ however this equation has no more than C roots and which induces a contradiction because there are $p - 1 > c$ such z. This contradiction means that $C = p - 1$ and so the entire group is generated by one element namely c which can be found by the process as mentioned above.

4 Problem A

A. If G is a finite group with order 2n, where n is an odd positive integer then G has a subgroup of order n. (Suggested method: Associate to each g in G the action on G defined by right multiplication by g. This defines an injective homomorphism of G into the group of permutations of the elements of G. Show the image of this homomorphism contains some permutation of odd sign, so that the subgroup consisting of the permutations of even sign has index 2)
First we label each element of G as $g_1, g_2, ...g_{2n}$ for each $g_i \in G$.
Define $\phi_i(g) : G \to G$ by $\phi_i(g) = gg_i$ and $\phi_i = \phi_{g_i}$ (this allows us more flexibility)

1. ϕ_i is onto
   if $h \in G$
   $$\phi_i(hg_i^{-1}) = hg_i^{-1}g_i = h.$$

2. ϕ_i is one-one
   if $\phi_i(g_1) = \phi_i(g_2)$
   $g_1g_i = g_2g_i \implies g_1 = g_2$

3. ϕ_i is a bijection because it is one-one and onto and since it is from G onto itself it is a permutation.

4. $\phi_i \neq \phi_j$ if $j \neq i$.
   assume for contradiction $\phi_i = \phi_j$ then $gg_i = gg_j \implies g_i = g_j$ a contradiction. In fact this relation is even stronger and implies that ϕ_i and ϕ_j must not agree for ANY $g \in G$

5. $S := \{\phi_i : i \in [1, 2n]\}$ is a group. $\phi_i(\phi_j(g)) = gg_jg_i = \phi_{g_jg_i}(g)$ shows that every element stays in the group
   $\phi_{g_i}(\phi_{g_i^{-1}}(g)) = gg_i^{-1}g_i = g = ge = \phi_e(g)$ shows that inverses exist
   $\phi_e(\phi_i(g)) = gg_ie = gg_i = \phi_i(g) = geg_i = \phi_i(\phi_e(g))$ shows that the identity

exists
additionally associativity holds because associativity holds in multiplication (i.e. it does not matter which permutation is calculated first.

6. S has a permutation of odd degree.
   Since $2||G|$, by sylow's first theorem there exists some $h \in H$ such that $|h| = 2 \rightarrow h^2 = e$. consider $\phi_h(g) = gh \neq g$ since $h \neq e$. Additionally $\phi_h(\phi_h(g)) = gh^2 = g$. These together show that every element of ϕ_h is a two-cycle. There are exactly n 2 cycles since there are $2n$ items to be permuted and using the definition of odd degree of number of swaps of elements the degree of ϕ_h is odd since n is odd.

7. Set $A_s := \{\phi \in S; \phi \text{ even}\}$ clearly $|A_s| = n$ because A_s is a subgroup (composition of even permutation is even, contains identity, is subset of a group) and since S is a group, the coset of A_s with any odd permutation (e.x. ϕ_h from previous) must have the same cardinality and be disjoint. Additionally there is only one coset for if ϕ_{h_1}, ϕ_{h_2} both odd assume for contradiction
   $$\phi_{h_1} A_s \neq \phi_{h_2} A_s.$$
   $$A_s \neq \phi_{h_1^{-1}} \phi_{h_2} A_s.$$
   but since $\phi_{h_1^{-1}}$ is odd because the inverse of an odd permutation is odd (their composition must be the identity which is even) $\phi_{h_1^{-1}} \phi_{h_2}$ is even and this implies that
   $$A_s \neq A_s.$$
   a contradiction, thus there is only one left coset of A_s and so $|A_s| = n$

8. Finally $\theta : G \rightarrow S$ defined by $\theta(g) = \phi_g$ is an isomorphism because
   $\theta(e) = \phi_e$ is the identity $\theta(g_1 g_2) = \phi_{g_1 g_2} = \phi_{g_2}(\phi_{g_1})$ but if we define $\phi_i * \phi_j = \phi_j(\phi_i)$ we get $\phi_{g_2}(\phi_{g_1}) = \phi_{g_1} * \phi_{g_2} = \theta(g_1)\theta(g_2)$ and the two sets have the same cardinality and are onto and one-one by their definitions (each g maps to a ϕ_g and each ϕ_g is unique) as shown earlier. Thus finally since A_s is a group of order $|n|$ and θ is an isomorphism, $\theta^{-1}(A_s)$ is a group in G of order n.

5 Problem B

Let G be a group of order 30. According to the previous problem, G has a subgroup of order 15 , which is necessarily normal. Prove that G has another nontrivial normal subgroup $30 = 3 * 5 * 2$ prime factorization. By sylow's first theorem there exists $H \subset G$ s.t. $|H| = 5$. Additionally for each $h \in H$ $|h| = 5$ since the order of h must divide the order of H.
By sylow's second theorem the number of such 5 sylow subgroups must be congruent to 1 mod 5. We also have that the number of 5-sylow subgroups times 5 must be less than G since each 5-sylow group is disjoint and so the

only options are there is one 5-sylow subgroup or there are 6 5-sylow subgroups. Each 5-sylow subgroup is disjoint because the order of each is 5.
and each element is of order 5 since 5 is prime and thus each 5-sylow subgroup is cyclic generated by any element ruling out intersection between them. Therefore if there were 6 5-sylow subgroups they would partition the entire group G. Additionally if there were 6 then every element in G would have to be order 5. Let V normal be the subgroup of order 15 as specified in the problem. We now assume for contradiction that there are 6 5-sylow subgroups. In this case V necessarily contains 3 5-sylow subgroups however since every 5-sylow subgroup is conjugate to each other 5-sylow subgroup let A be a 5-sylow subgroup in V and B be a 5-sylow subgroup not in V. There exists some $x \in G \rightarrow xAx^{-1} = B$ which implies that V is not normal a contradiction because V is normal thus there can only be one 5-sylow subgroup. Since there is only one 5-sylow subgroup it must itself be normal this is because conjugation preserves cardinality and thus any conjugate of the singular 5-sylow subgroup must itself have 5 elements and be a subgroup and since there is only one group with 5 elements (every group with exactly 5 elements is a 5-sylow group) it must conjugate back onto itself. Therefore it is normal and we have found a non-trivial normal subgroup of G.