MAT301 Groups and Symmetry

Assignment 5 Solutions

1. Consider the following subset of S_4:

$$H := \{e,\ (12)(34),\ (13)(24),\ (14)(23)\}.$$

(a) Show that H is a normal subgroup of S_4. To prove normality you may use the following fact without proof: For every $\sigma, \delta \in S_n$, the permutations δ and $\sigma\delta\sigma^{-1}$ have the same cycle type.

(b) Show that the distinct (left or right because H is normal) cosets of H are H, $(123)H$, $(132)H$, $(12)H$, $(13)H$, and $(23)H$.

(c) Fill in the blanks with one of H, $(123)H$, $(132)H$, $(12)H$, $(13)H$, and $(23)H$. (The operations take place in the quotient group S_4/H.)

(i) $(143)H \cdot (324)H = \ldots\ldots$

(ii) $(1234)H \cdot (12)H = \ldots\ldots$

(d) Show that $S_4/H \simeq S_3$ by defining an isomorphism $S_3 \to S_4/H$.

Solution: (a) First let us check that H is a subgroup. The identity is in H. Moreover, every element of H is its own inverse. In particular, H is closed under taking inverses. To see that H is closed under the operation, note that for i, j, k, l distinct, we have

$$(ij)(kl) \circ (il)(jk) = (ik)(jl).$$

Now we show that H is normal. Let $\delta \in H$ and $\sigma \in S_4$. Note that if $\delta = e$, then $\sigma\delta\sigma^{-1} = e \in H$. Let $\delta \neq e$. Then δ is of cycle type 2,2, and hence $\sigma\delta\sigma^{-1}$ is also of cycle type 2,2. But there are only three elements of cycle type 2,2 in S_4 and H contains all of them. Thus $\sigma\delta\sigma^{-1} \in H$.

(b) This is verified by a straightforward calculation. The cosets are H,

$$(123)H = \{(123), (134), (324), (142)\}, \quad (132)H = \{(132), (234), (124), (143)\},$$

$$(12)H = \{(12), (34), (1324), (1423)\}, \quad (13)H = \{(13), (1234), (24), (1432)\}$$

and

$$(23)H = \{(23), (1342), (1243), (14)\}.$$

(Since every element of S_4 has already appeared in one coset above, we know that there are no more cosets. Alternatively, we know the number of cosets of H is $|S_4|/|H| = 6$, and we have already found 6 distinct cosets.)

(c) (i) $(143)H \cdot (324)H = (32)(41)H = H$ and (ii) $(1234)H \cdot (12)H = (134)H = (123)H$.

(d) Define $\phi : S_3 \to S_4/H$ by $\phi(\sigma) = \sigma H$, where we are thinking of an element $\sigma \in S_3$ as an element of S_4 via its cycle notation. For instance, $\phi((12)) = (12)H$. From (b) it clear that this is an isomorphism. †

2. Consider the subgroups $H = \langle [4] \rangle$ and $K = \langle [-4] \rangle$ of $U(15)$.

(a) Find $|U(15)/H|$ and $|U(15)/K|$.

(b) Find the order of the element $[2]K$ of $U(15)/K$.

(c) Is $U(15)/K$ cyclic?

(d) Find the order of every element of $U(15)/H$. Is $U(15)/H$ cyclic?

† We are being a bit intuitive and informal here. The more formal argument is as follows: First define a map $\iota : S_3 \to S_4$ by sending σ to the permutation of $\{1, 2, 3, 4\}$ that acts like σ on $\{1, 2, 3\}$ and fixed 4. You can check that ι is a homomorphism. Then $\phi : S_3 \to S_4/H$ is the composition of ι and the quotient map $S_4 \to S_4/H$, and being a composition of homomorphisms it is a homomorphism. Bijectivity is immediate from (b).

Solution: (a) Note that $|U(15)| = 8$. Both $H = \{[1], [4]\}$ and $K = \{[1], [-4]\}$ have order 2, hence $|U(15)/H| = |U(15)/K| = 4$.

(b) Note that $([2]K)^n = K$ if and only if $[2]^n \in K$. We have $[2], [2]^2 = [4], [2]^3 = [8] \notin K$, whereas $[2]^4 = [1] \in K$. This $|[2]K| = 4$.

(c) Yes, because it has an element of order 4 (namely $[2]K$).

(d) The elements of $U(15)/H$, i.e. the cosets of H in $U(15)$ are H, $[2]H = \{[2], [8]\}$, $[7]H = \{[7], [13]\}$, and $[-1]H = \{[-1], [-4]\}$. Of course H, as an element of $U(15)/H$, has order 1. We have $[2]^2 = [4] \in H$, $[7]^2 = [4] \in H$, and $[-1]^2 = [1] \in H$, thus $|[2]H| = |[7]H| = |[-1]H| = 2$. The quotient $U(15)/H$ is not cyclic since it has no element of order 4.

3. (a) Let G be an abelian group. Let H be the subset of G consisting of all the elements of finite order. By Problem 1(e) of Assignment 2, H is a subgroup of G (it is sometimes called the *torsion* subgroup of G). Show that the quotient group G/H has no nontrivial element of finite order (i.e. that the only element of finite order in G/H is the identity).

(b) How many elements of order 3 does the quotient group $\mathbb{C}^\times/\mu_4$ have? (Prove your claim.)

Solution: (a) Let $g \in G$ and $gH \in G/H$ be an element of finite order. Then there is a positive integer n such that $(gH)^n = e_{G/H} = H$, i.e. $g^n H = H$. It follows that $g^n \in H$, which means g^n has finite order, i.e. there is a positive integer m such that $(g^n)^m = e$. Then $g^{mn} = e$, so that g itself has finite order, hence $g \in H$ and $gH = H$. (We proved that the only element of finite order in G/H is the identity element, i.e. the element $H \in G/H$.)

(b) Let $z \in \mathbb{C}^\times$. We have

$$(z\mu_4)^3 = e_{\mathbb{C}^\times/\mu_4} \iff z^3\mu_4 = \mu_4 \iff z^3 \in \mu_4 \iff z \in \mu_{12}.$$

Thus the elements of order 3 in $\mathbb{C}^\times/\mu_4$ belong to the subgroup μ_{12}/μ_4 (of $\mathbb{C}^\times/\mu_4$). The subgroup μ_{12}/μ_4 is cyclic group of order 3 (why?), hence it has 2 elements of order 3 (and hence so does $\mathbb{C}^\times/\mu_4$).

4. Let n be a positive integer and p be a prime number. Write $n = p^c m$, where $c \geq 0$ and m are integers and $p \nmid m$ (thus p^c is the highest power of p that divides n). Let G be an abelian group of order n. Let

$$H := \{g \in G : \text{there is } \ell \geq 0 \text{ such that } g^{p^\ell} = e\}.$$

In other words, H consists of all the elements of G whose order is a power of p. Show that $|H| = p^c$. (The subset H defined above is called the p-*part* of G.)

Solution: This is now Proposition 36(a) of the notes. Please see page 93 of the notes for the proof.

5. The goal of this question is to introduce the construction of *direct product* of two groups. Let G and H be any groups. Recall that the Cartesian product $G \times H$ is the set

$$G \times H := \{(g, h) : g \in G \text{ and } h \in H\}.$$

We can use the binary operations on G and H to define a binary operation on $G \times H$: define

$$(g, h) \cdot (g', h') := (gg', hh').$$

(In other words, we multiply elements of $G \times H$ "component-wise".)

(a) Calculate

$$((123), [3]) \cdot ((12), [4])$$

in $S_4 \times \mathbb{Z}/5$. (Remember the operation in $\mathbb{Z}/5$ is addition.)

(b) Back to the general G and H, show that $G \times H$ with the operation defined above is a group with identity (e_G, e_H). (This group is called the *direct product* of G and H.)

(c) Find the order of the element $(g, h) \in G \times H$ in terms of the orders of g and h.

(d) Show that $\mathbb{Z}/m \times \mathbb{Z}/n$ is cyclic if and only if $\gcd(m, n) = 1$.

Solution: (a) In $S_4 \times \mathbb{Z}/5$,

$$\big(\,(123),[3]\,\big)\cdot\big(\,(12),[4]\,\big)=\big(\,(123)(12),[3]+[4]\,\big)=\big(\,(13),[2]\,\big)\,.$$

(b) Let us check associativity:

$$\begin{aligned}\big(\,(g_1,h_1)(g_2,h_2)\,\big)\,(g_3,h_3) &= (g_1g_2,h_1h_2)(g_3,h_3)\\ &= \big(\,(g_1g_2)g_3,(h_1h_2)h_3\,\big)\\ &\overset{\text{associativity in G and H}}{=} \big(\,g_1(g_2g_3),h_1(h_2h_3)\,\big)\\ &= (g_1,h_1)(g_2g_3,h_2h_3)\\ &= (g_1,h_1)\,\big(\,(g_2,h_2)(g_3,h_3)\,\big)\,.\end{aligned}$$

The element (e_G, e_H) satisfies the defining property of the identity element in $G \times H$, as

$$(e_G,e_H)(g,h)=(e_Gg,e_Hh)=(g,h),$$

and similarly, $(g, h)(e_G, e_H) = (g, h)$. Given an arbitrary $(g, h) \in G \times H$, the element (g^{-1}, h^{-1}) of $G \times H$ satisfies the defining property of the inverse of (g, h):

$$(g,h)(g^{-1},h^{-1})=(gg^{-1},hh^{-1})=(e_G,e_H),$$

and similarly $(g^{-1}, h^{-1})(g, h) = (e_G, e_H)$.

(c) This is Proposition 35 of the notes. Please see its proof on page 87.

(d) This is Corollary 7 of the notes. Please see its proof on pages 87 and 88.

6. (a) Let G be an abelian group. Let H and K be subgroups of G with $H \cap K = \{e\}$. Show that the map

$$\phi : H \times K \to G$$

defined by $\phi((h, k)) = hk$ is an injective homomorphism. (The condition $H \cap K = \{e\}$ should come into play for injectivity. To prove that ϕ is a homomorphism you will use the abelian hypothesis.)

(b) Let G be a finite abelian group of order mn, where $\gcd(m, n) = 1$. Let H and K be subgroups of G of orders respectively m and n. Show that $G \simeq H \times K$.

(c) Let G be an abelian group of order $p^a q^b$, where p and q are distinct prime numbers and $a, b \geq 0$ are integers. Show that there are abelian groups H and K of orders p^a and q^b such that $G \simeq H \times K$. (Suggestion: Take H and K to be the p-part and q-part of G.)

Solution: (a) Let us first check that ϕ is a homomorphism. We have

$$\phi\,\big(\,(h_1,k_1)(h_2,k_2)\,\big)=\phi(h_1h_2,k_1k_2)=h_1h_2k_1k_2.$$

On the other hand,

$$\phi(h_1,k_1)\phi(h_2,k_2)=h_1k_1h_2k_2.$$

Since G is abelian, we see that

$$\phi\,\big(\,(h_1,k_1)(h_2,k_2)\,\big)=\phi(h_1,k_1)\phi(h_2,k_2).$$

(Note that this had nothing to do with H and K intersecting trivially. What was important was that G is abelian.)

Now we check injectivity. Let $(h, k) \in \ker(\phi)$. Then $hk = e$, so that $h = k^{-1}$. It follows that The element h of H, being equal to k^{-1}, also belongs to K. Since $H \cap K = \{e\}$, it follows that $h = e$. From $h = k^{-1}$ we see that $k = e$ as well. Thus $(h, k) = (e, e)$ and the kernel of ϕ is trivial.

(b) The assumption that $\gcd(|H|, |K|) = 1$ implies that $H \cap K$ is trivial (as by Lagrange $|H \cap K|$ divides both $|H|$ and $|K|$). By Part (a) the homomorphism $H \times K \to G$ sending $(h, k) \mapsto hk$ is injective. It follows that this map is also surjective as $|H \times K| = |H| \cdot |K| = mn = |G|$.

(c) Let H (resp. K) be the p-part (resp. q-part) of G. By Problem 4, we have $|H| = p^a$ and $|K| = q^b$. Part (b) implies that $H \times K \simeq G$ (the map $(h, k) \mapsto hk$) is an isomorphism).