UNIVERSITY OF SOUTH CAROLINA

MATH-546 Algebraic Structures I — Exam 2 Practice

Problems

Problem 1:

Let $G = \mathbb{Z}_8 \times \mathbb{Z}_6$.

a. Find the order of $([3]_8, [4]_6)$. Justify.

b. Let H denote the subgroup generated by $([3]_8, [4]_6)$ and let K denote the subgroup generated by $([1]_8, [0]_6)$. Prove that $K \subseteq H$.

c. What is $|K|$? Justify.

Answer 1:

a. $o([3]_8) = 8$
$o([4]_6) = 3$
$o(([3]_8, [4]_6)) = \operatorname{lcm}(8, 3) = 24$

b. $([1]_8, [0]_6) = 3([3]_8, [4]_6) \Rightarrow \langle([1]_8, [0]_6)\rangle \subseteq H$

c. $\langle([1]_8, [0]_6)\rangle = \mathbb{Z}_8 \times \{0\}$ and $|K| = 8 \cdot 1 = 8$

Problem 2:

List all the subgroups of S_3. Explain why your list is complete (i.e., there are no other subgroups).

Answer 2:

$\{(1)\}$
$\{(1), (1\ 2)\}$
$\{(1), (1\ 3)\}$
$\{(1), (2\ 3)\}$
$\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$
S_3

The order of S_3 is 6 so any subgroup must be of order 1, 2, 3 or 6. There can only be one subgroup of order 1 and only one of order 6. Subgroups of order 2 or 3 must be cyclic since 2 and 3 are prime. All elements of S_3 are included above so there are no missing generators.

Problem 3:

List all the possible orders of elements in S_6. For each possible order, give two different examples of elements of S_6 that have that order (or state that there is only one such element). Explain why there are no other possible orders.

Answer 3:

The order of a permutation is the least common multiple of the lengths of the disjoint cycles into which it can be decomposed. We look at all possible sets of disjoint cycles; there are 11 (see *Integer Partition* in Wikipedia).

form of disjoint cycles	order
$(a\ b\ c\ d\ e\ f)$	6
$(a\ b\ c\ d\ e)\,(f)$	5
$(a\ b\ c\ d)\,(e\ f)$	4
$(a\ b\ c\ d)\,(e)\,(f)$	4
$(a\ b\ c)\,(d\ e\ f)$	3
$(a\ b\ c)\,(d\ e)\,(f)$	6
$(a\ b\ c)\,(d)\,(e)\,(f)$	3
$(a\ b)\,(c\ d)\,(e\ f)$	2
$(a\ b)\,(c\ d)\,(e)\,(f)$	2
$(a\ b)\,(c)\,(d)\,(e)\,(f)$	2
$(a)\,(b)\,(c)\,(d)\,(e)\,(f)$	1

The identity (1) is the only permutation of order 1.
Order 2: (1 2) and (1 2)(3 4).
Order 3: (1 2 3) and (1 2 3)(4 5 6).
Order 4: (1 2 3 4) and (1 2 3 4)(5 6).
Order 5: (1 2 3 4 5) and (1 2 3 4 6).
Order 6: (1 2 3 4 5 6) and (1 2 3 4 6 5)

Problem 4:

Let G be a group with $|G| = 25$. Assume that G is not cyclic. Prove that every $x \in G$ has order equal to 1 or 5.

Answer 4:

If G is not cyclic then there is no element of order 25. The order of every element must divide the order of the group. The only remaining divisors of 25 are 1 and 5. So every element has order 1 or 5.

Problem 5:

a. Give an example of a group G with $|G| = 16$ such that G is abelian but not cyclic.

b. Give an example of a group G with $|G| = 24$ such that G is not abelian.

c. Give an example of a group G with $|G| = 12$ such that G is not abelian.

   Explain why your examples have the required properties.

Answer 5:

a. $\mathbb{Z}_4 \times \mathbb{Z}_4$

b. $S_3 \times \mathbb{Z}_4$ or S_4

c. $S_3 \times \mathbb{Z}_2$

S_3 is not abelian and has order 6. The order of direct products is the product of the orders.

Problem 6:

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 8 & 7 & 1 & 4 & 9 & 11 & 3 & 2 & 10 & 6 & 12 \end{pmatrix}$$

Write the decomposition of σ into disjoint cycles and find the order of σ.

Answer 6:

$\sigma = (1\ 5\ 4)\,(2\ 8\ 3\ 7\ 11\ 6\ 9)$
$o(\sigma) = 3 \cdot 7 = 21$

Problem 7:

Consider the following elements of S_5:

$$\sigma = (1\,2\,3\,4), \quad \tau = (2\,3\,5)$$

Write each of the following as a composition of disjoint cycles:

$$\sigma^{-1}, \quad \sigma^3, \quad \sigma\tau, \quad \sigma\tau\sigma^{-1}.$$

Answer 7:

$\sigma^{-1} = (4\ 3\ 2\ 1) = (1\ 4\ 3\ 2)$
$\sigma^3 = (1\ 4\ 3\ 2)$
$\sigma\tau = (1\ 2\ 3\ 4)(2\ 3\ 5) = (1\ 2\ 4)(3\ 5)$
$\sigma\tau\sigma^{-1} = (1\ 2\ 3\ 4)(2\ 3\ 5)(4\ 3\ 2\ 1) = (3\ 4\ 5)$

Problem 8:

Recall that for a group G, the center of G is the set

$$Z(G) := \{x \in G \mid ax = xa \ \forall a \in G\}.$$

Prove that $Z(S_3) = \{e\}$.

Answer 8:

The elements of S_3 are cycles of length 1, 2 or 3.

The 1-cycle element is the identity and clearly $e \in Z(S_3)$.

Let $(a\ b)$ and $(a\ c)$ be distinct elements of S_3 then $(a\ b)(a\ c) = (a\ c\ b)$ but $(a\ c)(a\ b) = (a\ b\ c)$ and so no cycles of length 2 are in $Z(S_3)$.

Let $(a\ b\ c)$ be an arbitrary 3-cycle in S_3: $(a\ b\ c)(a\ b) = (a\ c)$ but $(a\ b)(a\ b\ c) = (b\ c)$ and none of the 3-cycle elements are in $Z(S_3)$.

Problem 9:

Let $H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq S_4$. Verify that H is a subgroup of S_4.

Answer 9:

First note that H has the identity plus all possible products of disjoint 2-cycles in S_4 and can be represented as $(a\ b)\,(c\ d)$ for distinct a, b, c, d. And second, remember that $(a\ b) = (b\ a)$.

Identity and associativity are given.

Each element is its own inverse:

$$(a\ b)\,(c\ d)\,(a\ b)\,(c\ d) = (a\ b)\,(a\ b)\,(c\ d)\,(c\ d) = e$$

Closure: Multiplication of any element by the identity or by itself yields the same element or the identity, respectively. Let $(a\ b)\,(c\ d)$ be an arbitrary element of H, not e; and a different element, not e, will be of the form $(a\ c)(b\ d)$. Multiplying, we get

$$(a\ b)\,(c\ d)\,(a\ c), (b\ d) = (a\ d)\,(b\ d)$$

which is also in H.

Problem 10:

a. Does S_7 have an element that has order equal to 12? Give an example or explain why it does not exist.

b. Does S_7 have an element of order equal to 15? Give an example or explain why it does not exist.

Answer 10:

a. $o((1\ 2\ 3\ 4)(5\ 6\ 7)) = 12$

b. The integer partitions of 7 have to have a length of 15 or of both 3 and 5; both not possible with 7.

Theoretical Questions

Question 1:

Using Lagrange's Theorem, prove that if G is a group with $|G|$ equal to a prime number, then G is cyclic.

Answer :

If $p = |G|$ is prime then subgroups must have order 1 or p. Let $x \in G$ and consider the subgroup generated by x. If $x \neq e$ then $|\langle x \rangle| = 15$ and therefore $\langle x \rangle = G$ and so G is cyclic.

Question 2:

Using Lagrange's Theorem, prove that if p is a prime number and a is an integer not divisible by p, then

$$[a^{p-1}]_p = [1]_p$$

Answer :

Since p is prime, every element of $\mathbb{Z}_p \smallsetminus \{[0]\}$ has a multiplicative inverse.

So $|\mathbb{Z}_p^*| = p - 1$ and every subgroup of $\mathbb{Z}_p^*$ has an order that divides $p - 1$.

Consider $A = \langle [a]_p \rangle \subseteq \mathbb{Z}_p^*$. Let $n = |A|$. Then $[a]^n = [a^n] = [1]$ and since there is an integer m such that $nm = p - 1$ and therefore $[a^{p-1}] = [a^{nm}] = [(a^n)^m] = [1^m] = [1]$