University of Illinois at Urbana-Champaign

MATH 417 - Introduction to Abstract Algebra

Spring 2022 - Midterm1 - Review questions - Short answers

---

1. Solve the linear equation $9x \equiv 13 \pmod{70}$ in two steps.

   a) Determine integers s and t such that $1 = 9s + 70t$.

   b) Determine the smallest positive integer solution x.

	q	r	s	t
-1		70	0	1
0	7	9	1	0
1	1	7	-7	1
2	3	2	8	-1
3	2	1	-31	4
4		0	70	-9

a) $s = -31, t = 4$. Verification: $1 = 9 \cdot -31 + 70 \cdot 4$, yes.

b) $x \equiv -31 \cdot 13 \pmod{70} \equiv -53 \pmod{70}$. Choose $x = 17$.

Verification: $9 \cdot 17 = 153 \equiv 13 \pmod{70}$, yes.

2. Let $A \leq G$ and $B \leq G$ be subgroups of an abelian group $(G, +)$.

   a) Show that $A + B = \{a + b : a \in A, b \in B\}$ is a subgroup of G.

   b) Show that $A \cap B$ is a subgroup of G.

In both cases: Either use the definition of subgroup (Definition 5.4 on page 50) or verify the three properties that characterize a subgroup (Theorem 5.14 on page 52). The last one will be shorter because it avoids checking associativity.

3. Let $H = 12\mathbb{Z} + 27\mathbb{Z} \subset \mathbb{Z}$ and let $K = 12\mathbb{Z} \cap 27\mathbb{Z} \subset \mathbb{Z}$.

   a) Determine h such that $H = h\mathbb{Z}$..

   b) Determine k such that $K = k\mathbb{Z}$.

a) Use two different arguments to explain separately that $12\mathbb{Z} + 27\mathbb{Z} \subset 3\mathbb{Z}$ and that $12\mathbb{Z} + 27\mathbb{Z} \supset 3\mathbb{Z}$. Conclude that $h = 3$. (In general h is the gcd, but be sure that you can provide the arguments and not just the answer)

b) Use two different arguments to explain separately that $12\mathbb{Z} \cap 27\mathbb{Z} \supset 108\mathbb{Z}$ and that $12\mathbb{Z} \cap 27\mathbb{Z} \subset 108\mathbb{Z}$. Conclude that $k = 108$. (In general k is the lcm, but be sure that you can provide the arguments and not just the answer)

4. Let $S_3 = \{1, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$, with $\rho = (1\,2\,3), \sigma = (1\,2)$.

   a) Show that $\rho\sigma = \sigma\rho^2$.

   b) Reduce the permutation $\rho\sigma\rho^2\sigma\rho\sigma$ to one of the six elements in the set S_3.

   a) $\rho\sigma = (1\,2\,3)(1\,2) = (1\,3)$, $\sigma\rho^2 = (1\,2)(1\,3\,2) = (1\,3)$.

   b) $\rho\sigma\rho^2\sigma\rho\sigma = \rho(\sigma\rho^2)\sigma\rho\sigma = \rho(\rho\sigma)\sigma\rho\sigma = \rho^2\sigma^2\rho\sigma = \rho^2\rho\sigma = \rho^3\sigma = \sigma$.

   (There are other ways to carry out the reduction, no computations needed, only that $\rho\sigma = \sigma\rho^2$)

5. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$.

   a) Determine the number of elements in G of order 1, order 2, and order 4.

   b) Determine the number of subgroups of G of size 4.

   a) Order 1: $1\times$, Order 2: $7\times$, Order 4: $56\times$.

   b) There are seven subgroups of type $\mathbb{Z}_2 \times \mathbb{Z}_2$ (because there are seven subgroups of type $\mathbb{Z}_2 \times \mathbb{Z}_2$ in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$) and 28 of type $\mathbb{Z}_4$ (one for each element of order four and its inverse). Total: 35.

6. Give a permutation $\tau \in S_8$ such that $\tau(1\,3\,5\,7\,2\,4\,6\,8) = (1\,3\,5\,7)(2\,4\,6\,8)$.

   $\tau = (1\,2)$. Verification: yes. (In general a cycle breaks into two parts after multiplication with a carefully chosen transposition).

7. Give a permutation $\sigma \in S_8$ such that $(1\,3\,5\,7) = \sigma(2\,4\,6\,8)\sigma^{-1}$.

   $\sigma = (1\,2)(3\,4)(5\,6)(7\,8)$. Verification: yes.

   (Another solution would be (87654321). In general use for σ a permutation that maps the cycle element-wise to the other cycle, in this case $2 \mapsto 1, 4 \mapsto 3$, $6 \mapsto 5, 8 \mapsto 7$)

8. List the possible cycle structures for a permutation $\sigma \in A_5$.

   $(1)\ 1\times, (1\,2)(3\,4)\ 15\times, (1,2,3)\ 20\times, (1,2,3,4,5)\ 24\times$. Total : $60 = |A_5|$.

9. Select all pairs of isomorphic groups among the following three groups.

$$\mathbb{Z}_{14} \times \mathbb{Z}_{24} \times \mathbb{Z}_{35}, \qquad \mathbb{Z}_{210} \times \mathbb{Z}_{56}, \qquad \mathbb{Z}_6 \times \mathbb{Z}_{40} \times \mathbb{Z}_{49}.$$

$$\begin{aligned}
\mathbb{Z}_{14} \times \mathbb{Z}_{24} \times \mathbb{Z}_{35} &\simeq \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times Z_5 \times \mathbb{Z}_7. \\
\mathbb{Z}_{210} \times \mathbb{Z}_{56} &\simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_8 \times \mathbb{Z}_7. \\
\mathbb{Z}_6 \times \mathbb{Z}_{40} \times \mathbb{Z}_{49} &\simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_{49}.
\end{aligned}$$

   The first two are isomorphic (matching factorizations). The third group is not isomorphic to the first two (the subgroups $\mathbb{Z}_7 \times \mathbb{Z}_7$ and $\mathbb{Z}_{49}$ of order 49 do not match)

10. Prove using only the group axioms that each element in a group G has a unique inverse in G.

    Assume that $ba = ab = e$ and $ca = ac = e$. Then $c = ce = c(ab) = (ca)b = eb = b$.