# Solutions to Final Exam of Math 3121

**Problem 1.**(15 points) Determine if the following maps are homomorphisms of groups (no reasons needed).
(1). $\Phi : \mathbb{R} \to \mathbb{R}, \quad \Phi(a) = a^8$
(2). $\Phi : \mathbb{R}^* \to \mathbb{R}^*, \quad \Phi(a) = 8a$
(3). $\Phi : \mathbb{R}^* \to \mathbb{R}^*, \quad \Phi(a) = a^8$
(4). $\Phi : GL(n, \mathbb{R}) \to \mathbb{R}, \quad \Phi(A) = \log |Det(A)|$.
(5). $\Phi : \mathbb{C}^* \to \mathbb{R}^*, \quad \Phi(z) = |z|$.

**Answer:** (1) No. (2) No. (3) Yes. (4) Yes. (5) Yes.

**Problem 2.**(15 points) Determine if each of the following maps is a ring homomorphism (no reasons needed).
(1). $\Phi : \mathbb{R} \to \mathbb{R}$ given by $\Phi(x) = -x$.
(2). $\Phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ given by $\Phi((a, b)) = b$.
(3). $\Phi : \mathbb{C} \to \mathbb{C}$ given by $\Phi(a + bi) = a - bi$.
(4). $\Phi : \mathbb{Z} \to \mathbb{Z}_2$ given by $\phi(a) = 1$ for $a$ odd, and $\phi(a) = 0$ for $a$ even.
(5). $\Phi : M_2(\mathbb{R}) \to M_2(\mathbb{R})$,

$$\Phi(A) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

**Answer:** (1) No. (2) Yes. (3) Yes. (4) Yes. (5) Yes.

To prove $\Phi$ in (5) is a ring homomorphism, we note that $\Phi(A) = CAC^{-1}$, where $C = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. $\Phi(A + B) = C(A + B)C^{-1} = CAC^{-1} + CBC^{-1} = \Phi(A) + \Phi(B)$, and $\Phi(AB) = CABC^{-1} = (CAC^{-1})(CBC^{-1}) = \Phi(A)\Phi(B)$.

**Problem 3.** (20 points). Multiple choice (each problem has only one correct answer, no reasons needed).
(1). Which of the following is a field?
(a). $\mathbb{Z}_{30}$ . (b). $\mathbb{Z}$. (c) $\mathbb{Z}_{19}$. (d). None of above **Answer:** (c)

(2). Which of the following rings is an integral domain?
(a). $\mathbb{Z} \times \mathbb{Z}$ . (b). $\mathbb{Z}_{2018}$. (c) $\mathbb{Z}$. (d). None of above **Answer:** (c)

(3). What is the remainder of $9^{62}$ when divided by 26?

(a) 3, (b). 9, (c). 17 (d). None of above **Answer:** (a)

(4). Which of the following is **not** a subgroup of the permutation group $S_5$?
(a). The set of all $\sigma \in S_5$ such that $\sigma(5) = 5$.
(b). The set of all $\sigma \in S_5$ such that $\sigma(1) = 1$.
(c). The set of all $\sigma \in S_5$ such that $\sigma^{120} = e$.
(d). The set of all $\sigma \in S_5$ such that $\sigma^2 = e$.

**Answer:** (d). Because the set is not closed. The transpositions $(1, 2)$ and $(1, 3)$ both satisfy $\sigma^2 = e$, but $(1, 2)(1, 3)$ does not.

**Problem 4** (10 points). Find a group homomorphism $\Phi : S_3 \to S_4$ that is injective (just write down your map, no reasons needed).

**Answer:** For $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix} \in S_3$, $\Phi(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & 4 \end{pmatrix}$.

**Problem 5** (10 points). Let $F$ be a finite field with $q$ elements. Prove that $a^q = a$ for all $a \in F$.

**Answer:** Let $F^* = F - \{0\}$. Because $F$ is a field, $F^*$ is a group under multiplication. $|F^*| = q - 1$. So for every $a \in F^*$, $a^{q-1} = 1$. This implies $a^q = a$. For $a = 0$, it is clear that $a^q = a$. This proves $a^q = a$ for all $a \in F$.

**Problem 6** (15 points). Let $G$ be an abelian group, $n$ be a positive integer.
(1). Prove that $f : G \to G$ given by $f(a) = a^n$ is a group homomorphism.
(2). Assume $G$ is finite and $|G|$ is relatively prime to $n$, prove that $f$ is an isomorphism.

**Answer:** (1). $f(ab) = (ab)^n$. Because $G$ is abelian, $(ab)^n = a^n b^n = f(a)f(b)$. This proves $f(ab) = f(a)f(b)$, so $f$ a group homomorphism.
(2). It is enough to prove $Ker(f) = \{e\}$. If $a \in Ker(f)$, then $a^n = e$. We also have $a^{|G|} = e$. Since $n$ and $|G|$ are relatively prime, there are $s, t \in \mathbb{Z}$ such that $sn + t|G| = 1$. $a = a^1 = a^{sn+t|G|} = (a^n)^s (a^{|G|})^t = e$. This prove $Ker(f) = \{e\}$. So $f$ is 1-1. Because $G$ is finite, so $f$ is also onto. This proves $f$ is an isomorphism.

**Problem 7** (15 points). Let $R$ be a ring with unity 1, $a \in R$ satisfies $a^7 = 0$.

(1). Prove that $H = \{1 + a^2xa^5 \mid x \in R\}$ is a group under multiplication.
(2). Assume $R$ is finite, prove that $|H|$ is a divisor of $|R|$.

**Answer:** (1). For $1 + a^2xa^5 \in H, 1 + a^2ya^5 \in H$ ,

$$(1+a^2xa^5)(1+a^2ya^5) = 1+a^2xa^5+a^2ya^5+a^2xa^5a^2ya^5 = 1+a^2(x+y)a^5 \in H$$

This proves $H$ is closed under the multiplication. $1 = 1 + a^20a^5 \in H$, so $H$ contains the identity 1. For every $1+a^2xa^5 \in H$, then $1+a^2(-x)a^5 \in H$, we have $(1+a^2xa^5)(1+a^2(-x)a^5) = 1+a^2(x+(-x))a^5 = 1$. So every element in $H$ has an inverse in $H$. This proves $H$ is group under the multiplication.

(2). Consider $A = \{a^2xa^5 \mid x \in G\}$. One checks directly that $A$ is a group under $+$. So $A$ is a subgroup of the additive group $R$. By Lagrange Theorem, $|A|$ is a divisor of $R$. It remains to prove $|A| = |H|$. Let $T : A \to H$ be the map given by $T(u) = 1 + u$. It is clear that $T$ is a bijection, so $|A| = |H|$.

Second method for (2). Consider the map $f : R \to H$ given by $f(x) = 1 + a^2xa^5$. We note that $f(x + y) = f(x)f(y)$. So $f$ is a group homomorphism. It is clear that $f$ is onto, i.e., $f(R) = H$. By Homomorphism theorem, $R/Ker(f)$ is isomorphic to $f(R) = H$. so $|R/Ker(f)| = |H|$, so $|R|/|Ker(f)| = |H|$. This proves $|H|$ is a divisor of $|R|$.