Solutions to Final Exam for Math 3121, 2022

Problem 1.(15 points) Determine if the following maps are homomorphisms of groups (no reasons needed).
(1). $\Phi : \mathbb{R}^* \to \mathbb{R}^*, \quad \Phi(a) = 2022a$
(2). $\Phi : \mathbb{R} \to \mathbb{R}, \quad \Phi(a) = 2022a$
(3). $\Phi : \mathbb{C}^* \to \mathbb{C}^*, \quad \Phi(a) = a^{2022}$
(4). $\Phi : \mathbb{R} \to GL(2, \mathbb{R}), \quad \Phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & e^a \end{pmatrix}.$
(5). $\Phi : \mathbb{C}^* \to \mathbb{R}^*, \quad \Phi(a + bi) = a^2 + b^2.$

Answer: (1) No (2) Yes (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). $\Phi : \mathbb{Z} \to \mathbb{R}$ given by $\Phi(x) = -x$.
(2). $\Phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ given by $\Phi(a, b) = a + b$.
(3). $\Phi : \mathbb{C} \to \mathbb{C}$ given by $\Phi(a + bi) = a - bi$.
(4). $\Phi : \mathbb{C} \to M_2(\mathbb{R})$ given by $\Phi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.
(5). $\Phi : M_2(\mathbb{R}) \to M_2(\mathbb{R})$, $\Phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 11b \\ \frac{1}{11}c & d \end{pmatrix}$.

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

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). $\mathbb{Z}_{33}$ (b). $\mathbb{Z}$ (c). $\mathbb{Z}_{13}$ (d). $M_2(\mathbb{R})$

(2). Let G be a finite group, $a \in G$ has order 19, which of the following statement is **false** ?
(a). a^{-1} has order 19.
(b). a^2 has order 19.
(c). If $a^n = e$, n is a positive integer, then 19 is a divisor of n.

(d). If $a^n = e$, n is a positive integer, then $n = 19$.

(3). If $\Phi : G \to G'$ is a **surjective** group homomorphism of finite groups, $b_1, b_2 \in G'$, which of the following statements is true?
(a) $\phi^{-1}(b_1) = \phi^{-1}(b_2)$, (b). $\phi^{-1}(b_1)$ is a subgroup of G, (c). $\phi^{-1}(b_1)$ and $\phi^{-1}(b_2)$ have the equal number of elements (d). None of above

(4). If R is a commutative ring with unity 1, $a \in R$, $a \neq 0$ is NOT a 0-divisor, which of the following is **not** correct?
(a) $ab = 0$ implies that $b = 0$. (b) a^{2022} is not a 0-divisor.
(c) a^{-1} exists. (d) $-a$ is not a 0-divisor.

(5). Which of the following sets is **not** a subring of $M_2(\mathbb{R})$?
(a). $S = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R}\}$. (b). $S = \{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid a, c, d \in \mathbb{R}\}$
(c). $S = \{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}\}$ (d). $S = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{R}\}$

Answer: (1) c (2) d (3) c (4) c (5) d

Problem 4 (5 points). Find an example of an **infinite** commutative ring that is **not** an integral domain. (just write down your example, no reasons needed).

Answer: There are many correct answers. Here are some examples: $\mathbb{Z} \times \mathbb{Z}$, $C[0, 7]$.

Problem 5 (5 points). Suppose H is a finite subgroup of $\mathbb{C}^*$, prove that $H = U_n$ for some positive integer n.

Proof. Suppose $|G| = n$, by the corollary of Lagrange theorem, for every element $a \in G$, $a^n = 1$, so $G \subset U_n$. Since $|G| = |U_n| = n$, so $G = U_n$.

Problem 6 (5 points). Let R be a ring with unity 1, $a \in R$ be a unit with multiplicative inverse a^{-1}. Prove that the map $\Phi : R \to R$ given by $\Phi(x) = axa^{-1}$ is an isomorphism of rings.

Proof.

$$\Phi(x+y) = a(x+y)a^{-1} = axa^{-1} + aya^{-1} = \Phi(x) + \Phi(y)$$

$$\Phi(xy) = axya^{-1} = axa^{-1}aya^{-1} = (axa^{-1})(aya^{-1}) = \Phi(x)\Phi(y)$$

This proves Φ is a ring homomorphism. It remains to prove Φ is a bijection. Let $\Psi : R \to R$ be the map given by $\Psi(x) = a^{-1}xa$. We check $\Phi \circ \Psi$ and $\Psi \circ \Phi$ are the identity map:

$$(\Phi \circ \Psi)(x) = \Phi(\Psi(x)) = \Phi(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$$

$$(\Psi \circ \Phi)(x) = \Psi(\Phi(x)) = \Psi(axa^{-1}) = a^{-1}(axa^{-1})a = x$$

Problem 7 (15 points). Let G be a finite group with order $|G| = 800$. Suppose H and K are subgroups of G with $|H| = 25$ and $|K| = 32$. Prove that every element $a \in G$ can be expressed as $a = hk$ for unique $h \in H$ and unique $k \in K$.

Proof. Step 1. We first prove that $H \cap K = \{e\}$. Since H and K are subgroups of G, so $H \cap K$ is a subgroup of G. Since $H \cap K \subset H$, by Lagrange theorem, $|H \cap K|$ is a divisor of $|H| = 25$. Since $H \cap K \subset K$, by Lagrange theorem, $|H \cap K|$ is a divisor of $|K| = 32$. This proves $|H \times K|$ is a common divisor of 25 and 32, so $|H \times K| = 1$, $H \cap K = \{e\}$.
Step 2. We consider the map $f : H \times K \to G$ given by $f(h, k) = hk$. We prove that f is one-to-one. Suppose $f(h_1, k_1) = f(h_2, k_2)$, so $h_1k_1 = h_2k_2$, $h_2^{-1}h_1 = k_2k_1^{-1}$. $h_2^{-1}h_1 \in H$, $h_2^{-1}h_1 = k_2k_1^{-1} \in K$. So $h_2^{-1}h_1 \in H \cap K$, by Step 1, $h_2^{-1}h_1 = e$, $h_1 = h_2$. Similarly $k_2k_1^{-1} = e$, $k_1 = k_2$. This proves f is one-to-one.
Step 3. Since $|H \times K| = |H| \cdot |K| = 25 \cdot 32 = 800 = |G|$, since f is one-to-one, f is onto. This proves g is a bijection.

Problem 8 (20 points). Let R be a finite commutative ring with unity 1, $1 \neq 0$. Let G be the set

$$G = \{x \in R \,|\, x \neq 0, x \text{ is NOT a 0 divisor}\}$$

(1) Prove that G is closed under the multiplication.
(2) Prove that G is a group under the multiplication.
(3) If a is an element in R satsifying $a^n = 0$ for some positive integer n, prove that $(1+a)^{|G|} = 1$.

Proof. (1) If $x, y \in G$, that is, $x \neq 0, y \neq 0$, and x, y are not 0 divisors, so $xy \neq 0$. We now prove that xy is not a 0 divisor. Suppose xy is a 0 divisor, we can find $a \neq 0$ such that $xya = 0$. $x(ya) = 0$. Since x is not a 0 divisor, $ya = 0$. Since y is not a 0 divisor, $a = 0$, which contradicts to the assumption $a \neq 0$. This proves xy is not a 0 divisor. So $xy \in G$.

(2) It is clear that $1 \in G$. It remains to prove that every $x \in G$ has an multiplicative inverse. We consider the infinite sequence $x, x^2, x^3, \ldots$. Since R is a finite set, there exists positive integers $m > n$ such that $x^m = x^n$. So $x^n(x^{m-n} - 1) = 0$. Since x^{m-n} is not a 0 divisor, $x^{m-n} - 1 = 0$, $x^{m-n} = 1$. This proves $xx^{m-n-1} = 1$, so x^{m-n-1} is the multiplicative inverse of x. This proves G is a group under the multiplication.

(3) We have $(1+a)(1-a+a^2-\cdots+(-1)^{n-1}a^{n-1}) = 1-(-a)^n = 1-(-1)^n a^n = 1$. This proves that $(1+a)$ is a unit. So $1+a \in G$. By the corollary of Lagrange theorem, $(1+a)^{|G|} = 1$.