# Solutions to Final Exam for Math 3131, Spring 2022, **Version 1**

**Problem 1.**(10 points) Find group homomorphisms satisfying the required conditions (no need to give reasons).
(1). $\Phi : \mathbb{R}^\times \to \mathbb{R}^\times$, $\Phi(\mathbb{R}^\times)$ has two elements.
(2). $\Phi : GL_{10}(\mathbb{R}) \to \mathbb{Z}_2 = \{0, 1\}$, $\Phi$ is surjective.
(3). $\Phi : \mathbb{C}^\times \to \mathbb{C}^\times$, $\Phi(t) = t$ for $|t| = 1$ and $\Phi(2) = 4$.
(4). $\Phi : S_3 \to GL_3(\mathbb{R})$, $\Phi$ is injective.
(5). $\Phi : U_{30} \to U_5$, $\Phi$ is surjective.

**Answer:** (1) $\Phi(x) = \begin{cases} 1 & \text{for } x > 0 \\ -1 & \text{for } x < 0 \end{cases}$ (2) $\Phi(A) = \begin{cases} 0 & \text{for } \det A > 0 \\ 1 & \text{for } \det A < 0 \end{cases}$
(3) $\Phi(z) = |z|^2$.
(4) The idea is that every $\sigma \in S_3$ gives a linear isomorphism of $\mathbb{R}^3$ by permuting the 3 coordinates. For $\sigma \in S_3$, $\Phi(\sigma)$ is the unique isomorphism of $\mathbb{R}^3$ that maps to $e_i$ to $e_{\sigma(i)}$, where $e_1, e_2, e_3$ is the standard basis for $\mathbb{R}^3$.
(5) $\sigma(z) = z^6$.

**Problem 2.** (10 points) Find ring homomorphisms satisfying the required conditions (no need to give reasons).
(1). $\Phi : \mathbb{R}[x] \to \mathbb{R}[x]$, $\Phi$ is injective but NOT surjective.
(2). $\Phi : \mathbb{Z}[x] \to \mathbb{Z}[i]$, $\Phi$ is surjective.
(3). $\Phi : \mathbb{C} \to \mathbb{C}$, $\Phi$ is NOT the identity map.
(4). $\Phi : \mathbb{Q}[x] \to \mathbb{R}$, $\Phi$ is injective.
(5). Let $F_{49}$ be a finite field with 49 elements, find a ring homomorphism $\Phi : F_{49} \to F_{49}$ such that $\Phi$ is NOT the identity map.

**Answer:** (1). $\Phi(f(x)) = f(x^2)$. Many other answers are possible. (2). $\Phi(f(x)) = f(i)$. Many other answers are possible. (3). $\Phi(z) = \bar{z}$. (4) $\Phi(f(x)) = f(\pi)$. (5) $\Phi(a) = a^7$.

**Problem 3** (15 points) Give a brief answer to each of the following problems

(no reasons needed)
(1) Determines if each of the rings $\mathbb{Z}$, $\mathbb{C}[x]$, $C[2,7]$ is an integral domain.
(2) If $a$ in a group $G$ has order 100, what is the order of $a^6$?
(3) Give an infinite chain of ideals $I_1, I_2, \ldots$ in $C[2,7]$ such that for each $i$, $I_i \subsetneqq I_{i+1}$.
(4) List all the finite abelian groups of order 196 up to isomorphism.
(5) Give an example of $\mathbb{R}[x]$-module $M$ such that $M$ has dimension 10 as a vector space over $\mathbb{R}$.

**Answer:** (1) $\mathbb{Z}$ and $\mathbb{C}[x]$ integral domains, $C[2,7]$ is not. (2) $a^6$ has order 50. (3) Let $S_n$ be the following subset of $[2,7]$, $S_n = [2, 2+\frac{1}{n}]$, let

$$I_n = \{f \in C[2,7] \mid f(x) = 0 \text{ for all } x \in S_n\}$$

Since $S_{n+1} \subset S_n$, so $I_n \subset I_{n+1}$. It is easy to find $f(x) \in I_n$ but $f(x) \notin I_{n+1}$.
(4) $196 = 2^2 \times 7^2$, there are 4 groups: ,

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_7, \;\; \mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_7, \;\; \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{49}, \;\; \mathbb{Z}_4 \times \mathbb{Z}_{49}$$

(5) $\mathbb{R}[x]/(x^{10})$, Many other answers are possible.

**Problem 4.**(10 points) Let $G$ be a group, $N \subset G$ be a normal subgroup. Suppose the quotient group $G/N$ has finite order $n$, prove that for all $a \in G$, $a^n \in N$.

**Proof.** Let $\pi : G \to G/N$ be the canonical homomorphism, that is, $\pi(a) = aN$. $Ker(\pi) = N$. Since $|G/N| = n$, so $(aN)^n = 1$, that is, $a^n N = 1$, so $a^n \in Ker(\pi) = N$.

**Problem 5.**(10 points) Let $I = \{f(x) \in \mathbb{R}[x] \mid f(1) = f(2) = 0\}$, it is clear that $I$ is an ideal of $\mathbb{R}[x]$, prove that the quotient ring $\mathbb{R}[x]/I$ is isomorphic to $\mathbb{R} \times \mathbb{R}$.

**Proof.** Let $\Phi : \mathbb{R}[x] \to \mathbb{R} \times \mathbb{R}$ be the map given by $\Phi(f) = (f(1), f(2))$. It is clear that $\Phi$ is a ring homomorphism and $Ker(\Phi) = I$. The map $\Phi$ is a $\mathbb{R}$-linear map, $\Phi(x-1) = (0,1)$, $\Phi(2-x) = (1,0)$. Since $(0,1),(1,0)$ is a basis for $\mathbb{R}^2$, so $\Phi$ is onto. We apply the homomorphism theorem to have $\mathbb{R}[x]/I = \mathbb{R}[x]/Ker(\Phi)$ is isomorphic to $Im(\Phi) = \mathbb{R}^2$.

**Problem 6.**(15 points) Let $R$ be a commutative ring, $a \in R$ is called a nilpotent element if $a^n = 0$ for some positive integer $n$. Let $N$ be the set of all nilpotent elements in $R$.
(1) Prove that $N$ is an ideal of $R$.
(2) Prove that $1 + N$ given by

$$1 + N = \{1 + a \,|\, a \in N\}$$

is a group under the multiplication.
(3) Suppose $R$ is finite, prove that $|N|$ is a common divisor of $|R|$ and $|R^\times|$, where $R^\times$ is the set of all units in $R$.

**Proof.** (1). Obviously $0 \in N$. If $a \in N$, it is clear that $-a \in N$. For $a, b \in N$, so $a^m = 0, b^n = 0$ for some positive integers $m, n$.

$$(a+b)^{m+n} = \sum_{j=0}^{m+n} \binom{m+n}{j} a^j b^{m+n-j} \tag{1}$$

For any $0 \le j \le m+n$, either $j \ge m$ or $m+n-j \ge n$. If $j \ge m$, $a^j = 0$ since $a^m = 0$, if $m+n-j \ge n$, $b^{m+n-j} \ge 0$ since $b^n = 0$. So all the terms in the right hand side of (1) are 0. This proves $a + b \in N$. So $N$ is a subgroup of the additive group $R$.

If $a \in N$, $b \in R$, so $a^m = 0$ for some positive integer $m$, $(ab)^m = a^m b^m = 0b^m = 0$, so $ab \in N$. This proves $N$ is an ideal.

(2). Since $0 \in N$, so $1 = 1 + 0 \in 1 + N$. If $1 + a, 1 + b \in 1 + N$, $a, b \in N$, $(1+a)(1+b) = 1 + (a + b + ab)$, by (1), $a + b + ab \in N$, so $1 + N$ is closed under the multiplication. For $1 + a \in N$, $a^m = 0$,

$$(1+a)(1 - a + a^2 + \cdots + (-1)^{m-1}a^{m-1}) = 1 - (-a)^m = 1.$$

By (1), $-a+a^2+\cdots+(-1)^{m-1}a^{m-1} \in N$, so $1-a+a^2+\cdots+(-1)^{m-1}a^{m-1} \in 1+N$. This proves every element in $1+N$ has a multiplicative inverse in $1+N$. This completes the proof that $1+N$ is a group under the multiplication.

(3). Since $N$ is an additive subgroup of $R$, by Lagrangian theorem, $|N|$ is a divisor of $|R|$. By (2), $1+N$ is a subgroup of $R^\times$, by Lagrangian theorem, $|1+N|$ is a divisor of $|R^\times|$. Since the map $N \to 1+N$, $a \mapsto 1+a$ is a bijection, so $|N| = |1+N|$ is a divisor of $|R^\times|$.

**Problem 7.**(15 points) Let $n$ be a positive integer, $G$ be the group of $n \times n$ upper triangular invertible real matrices (so $G$ is a subgroup of $GL_n(\mathbb{R})$), let $G$ operate on $\mathbb{R}^n$ by the matrix multiplication, how many orbits does this group operation have? write a detailed proof for your answer.

**Proof.** An element $g \in GL_n(\mathbb{R})$ is upper triangular iff $g_{ij} = 0$ for all $i > j$, where $g_{ij}$ denotes the $(i,j)$-entry of $g$.

For each non-zero vector $a = (a_1, a_2, \ldots, a_n)^T \in \mathbb{R}^n$, let $L(a)$ be the largest index $i$ such that $a_i \neq 0$. Since the $k$-th component of $ga$ is

$$(ga)_k = \sum_{j=1}^{n} g_{kj}a_j = \sum_{j \geq k} g_{kj}a_j$$

This formula implies that $L(ga) = L(a)$ for all $g \in GL_n(\mathbb{R})$ and $a \neq 0$. Next we verify that for $L(a) = k$, $a$ is in the orbit of $e_k$. Pick $g \in G$ which has $k$-the column $a$, $ge_k = a$.

In summary, we have proved that all the non-zero vectors $a$ with $L(a) = k$ form the orbit $Ge_k$. So we have $n+1$ orbits: $\{0\}, Ge_1, Ge_2, \ldots, Ge_n$.

**Problem 8.**(15 points) Let $F$ be a field, $K$ is a finite extension of $F$ with degree $[K : F] = d$. Suppose $f(x) \in F[x]$ is an irreducible polynomial with $\deg(f)$ relatively prime to $d$. Prove $f(x)$ is also an irreducible polynomial over $K$.

**Proof.** Let $p(x)$ be an irreducible factor of $f(x)$ in $K[x]$. Then $L = K[x]/(p(x))$ is a field extension of $K$, $\alpha = x + (p(x)) \in L$ is a root of $p(x)$. We have the chain of field extensions

$$F \subset K \subset L$$

So we have

$$[L : F] = [L : K]\,[K : F] = d \deg(p).$$

Since $\alpha$ is a root of $p(x)$, so it is also a root of $f(x)$, $F[\alpha]$ is isomorphic to $F[x]/(f(x))$, so $[F[\alpha] : F] = \deg(f)$. The chain $F \subset F[\alpha] \subset L$ implies that $\deg(f) = [F[\alpha] : F]$ is a divisor of $[L : F] = d \deg(p)$, since $\deg(f)$ and $d$ are relatively prime, so $\deg(f)$ is a divisor of $\deg(p)$, but $\deg(p) \leq \deg(f)$, so $\deg(p) = \deg(f)$. So $p(x) = f(x)$ up to a non-zero scalar. It is proves $f(x)$ is irreducible over $K$.