Math 127
Homework Problem Set 6
Bonus Assignment

Problem 1. Let A, B be two sets, and consider functions $f_1, f_2 : A \to B$.
(a) Suppose that we can find a function $g_1 : B \to A$ such that $g_1 \circ f_1 = \mathrm{id}_A$. Show then that this implies that f_1 is injective.
(b) Suppose that we can find a function $h_2 : B \to A$ such that $f_2 \circ h_2 = \mathrm{id}_B$. Show then that this implies that f_2 is surjective.

[**Note.** Recall that in class we have already discussed that, if a function $f : A \to B$ is bijective, then it has an inverse function.

Now, by considering both parts of this problem together, we can conclude that the converse is also true: if a function $f : A \to B$ has an inverse function $g : B \to A$, which by definition means that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$, then the function f is both injective and surjective, and hence it is bijective.

In other words, a function $f : A \to B$ has an inverse **if and only if** f is bijective.]

Problem 2. Recall the definition of a field homomorphism given in Lecture 45.

If $\mathbb{F}_1 = \big(\{\text{elements in } \mathbb{F}_1\}, +_1, \cdot_1\big)$ and $\mathbb{F}_2 = \big(\{\text{elements in } \mathbb{F}_2\}, +_2, \cdot_2\big)$ are two fields, then a function $f : \mathbb{F}_1 \to \mathbb{F}_2$ is called a *field homomorphism* if f satisfies the following three properties:

1. for every $a, b \in \mathbb{F}_1$, we have that
$$f(a +_1 b) = f(a) +_2 f(b).$$
2. for every $a, b \in \mathbb{F}_1$, we have that
$$f(a \cdot_1 b) = f(a) \cdot_2 f(b).$$

3. $f(1_{\mathbb{F}_1}) = 1_{\mathbb{F}_2}$.

We see that the definition requires the function to respect the operations of field addition and of field multiplication, and also respect the multiplicative unit.

In an analogous way to how we showed the corresponding result for vector space homomorphisms in Lecture 40, show that a field homomorphism respects the other key concepts of a field structure as well. In other words, show that

(i) $f(0_{\mathbb{F}_1}) = 0_{\mathbb{F}_2}$.

(ii) for every $a \in \mathbb{F}_1$, $f(-a) = -f(a)$ *(note that here $f(-a)$ is the image under f of the additive inverse of a in $\mathbb{F}_1$, while $-f(a)$ is the additive inverse of $f(a)$ in $\mathbb{F}_2$).*

(iii) for every non-zero element $a \in \mathbb{F}_1$, $f(a) \neq 0_{\mathbb{F}_2}$ and hence $f(a)$ will have a multiplicative inverse in $\mathbb{F}_2$. Moreover, $(f(a))^{-1} = f(a^{-1})$ *(note that here $f(a^{-1})$ is the image under f of the multiplicative inverse of a in $\mathbb{F}_1$, while $(f(a))^{-1}$ is the multiplicative inverse of $f(a)$ in $\mathbb{F}_2$).*

Problem 3. Let $\mathbb{F}$ be a field, and let A be an invertible matrix in $\mathbb{F}^{n\times n}$. We have stated in class that an element $\lambda \in \mathbb{F}$ is an eigenvalue of A **if and only if** the matrix $A - \lambda I_n$ is **not** invertible.

Observe now that, since $A - 0 \cdot I_n = A$ has been assumed to be invertible, we can be certain that 0 is not an eigenvalue of the given matrix A.

Consider an eigenvalue μ of A (by what we just said, $\mu \neq 0$). Show that μ^{-1} is an eigenvalue of the inverse A^{-1} of A.

Problem 4. Let V be a vector space over a field $\mathbb{F}$, and let u, v, w be vectors in V.
(a) Using the definition of linear span, show that

$$\mathrm{span}(u, v, w) = \mathrm{span}(u - v, v, w).$$

(b) Give an example showing that we can have

$$\mathrm{span}(u, v, w) \neq \mathrm{span}(u - v, v - u, w).$$

(c) What about

$$\mathrm{span}(u, v, w) = \mathrm{span}(u - v, v - w, w - u)\,?$$

Is it always true, or not always? Justify your answer.

Problem 5. Let $\mathcal{P}$ be the space of all real polynomials, that is, polynomials of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$$

where $m \geqslant 0$ and where all the coefficients a_i are real numbers.

Clearly we can add two such polynomials and what we get is again a polynomial from $\mathcal{P}$. More specifically, if $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$ and $q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_s x^s$ are in $\mathcal{P}$, and if we assume that $s \leqslant m$, then we can rewrite $q(x)$ as

$$\begin{aligned} q(x) &= b_0 + b_1 x + b_2 x^2 + \cdots + b_s x^s + 0x^{s+1} + \cdots + 0x^{m-1} + 0x^m \\ &= b_0 + b_1 x + b_2 x^2 + \cdots + b_s x^s + b_{s+1} x^{s+1} + \cdots + b_{m-1} x^{m-1} + b_m x^m \end{aligned}$$

where $b_j = 0$ for all $j > s$, and then we can set

$$p(x) + q(x) := (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_m + b_m)x^m.$$

Analogously we define $p(x) + q(x)$ when $s > m$.

Furthermore, given $r \in \mathbb{R}$ and $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m \in \mathcal{P}$, we can consider the polynomial

$$r \cdot p(x) := (ra_0) + (ra_1)x + (ra_2)x^2 + \cdots + (ra_m)x^m.$$

(a) Show that the space $\mathcal{P}$, together with the addition of polynomials and the scalar multiplication we just stated, is a vector space over $\mathbb{R}$.

(b) Show that the dimension of $\mathcal{P}$ over $\mathbb{R}$ is infinite.

[*Hint.* If you want, you can try to show that, for every $n \geqslant 1$, the set $\{1, x, x^2, \ldots, x^n\}$ is linearly independent, and hence the dimension of $\mathcal{P}$ over $\mathbb{R}$ has to be greater than the cardinality of this set, so it has to be greater than all integers n.]