

Homework 1 Solutions

1. Field trip.

Recall that for a prime p , $\mathbb{F} = \mathbb{Q}^2$ (pairs of rational numbers) is a field with the notions of addition and multiplication defined as

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{and} \quad (a, b) \cdot (c, d) = (ac + pbd, ad + bc).$$

- (a) What are the additive and multiplicative identities? What is the multiplicative inverse of (a, b) for $(a, b) \neq 0_{\mathbb{F}}$?

Solution: Additive identity is $(0, 0)$. Multiplicative identity is $(1, 0)$. Given $(a, b) \neq 0_{\mathbb{F}}$, we can solve for its multiplicative inverse (c, d) as follows. If $b = 0$ then we need $(ac, ad) = (1, 0)$ which yields $c = 1/a$ and $d = 0$ (which is legal since $a \neq 0$). If $b \neq 0$ then we need $(ac + pbd, ad + bc) = (1, 0)$ which solves to $c = -a/(pb^2 - a^2)$ and $d = b/(pb^2 - a^2)$. Note that this is legal since $\sqrt{p}$ is irrational, so $pb^2 - a^2 \neq 0$.

- (b) Does everything still go through for $p = 6$? How about $p = 4$?

Solution: Yes for $p = 6$ but no for $p = 4$, because we can no longer guarantee that $pb^2 - a^2 \neq 0$. For example, $(2, 1)$ has no inverse.

- (c) When p is such that $\mathbb{F}$ defined above is a field, the set

$$S = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$$

can be thought of as a vector space over the field $\mathbb{Q}$. What is its dimension? What is a basis for it?

Solution: Dimension is 2. $\{1, \sqrt{p}\}$ is a basis.

2. Basis Basics.

If $S = \{v_1, \dots, v_n\}$ is a basis for V , then we know that any $v \in V$ is in the span of S and so can be written as $a_1v_1 + \dots + a_nv_n$ for some $a_1, \dots, a_n$.

- (a) Prove this decomposition is unique.

Solution: Suppose not. This means there is some v such that $v = a_1v_1 + \dots + a_nv_n = a'_1v_1 + \dots + a'_nv_n$ where for some i we have $a_i \neq a'_i$. Subtracting, we get $(a_1 - a'_1)v_1 + \dots + (a_n - a'_n)v_n = 0$, a contradiction since the coefficients are not all zero.

- (b) Give an example of a case of a non-unique decomposition (i.e., multiple ways of writing v as a linear combination of vectors in S) when S is *not* a linearly independent set.

Solution: Lets consider vectors $v_1 = (1, 0), v_2 = (0, 1), v_3 = (1, 1) \in \mathbb{R}^2$. We can then write the vector $(2, 2)$ as $2v_1 + 2v_2$ or as $2v_3$.

3. Linear equations.

Let $A \in \mathbb{F}_2^{m \times n}$ be a matrix with entries in the field $\mathbb{F}_2$ and let $m < n$ (m rows and n columns). Let all rows of A be linearly independent in the vector space $\mathbb{F}_2^n$ over the field $\mathbb{F}_2$.

- (a) What is the dimension of the space $\ker(A)$?

Solution: Since the rows of A are linearly independent, the row-rank is m , which means the column-rank is m , which means the dimension of the image is m . So, by the rank-nullity theorem, the dimension of the kernel is $n - m$.

- (b) How many vectors $x \in \mathbb{F}_2^n$ satisfy the system of equations $Ax = 0$? (Note that here 0 denotes the zero vector in $\mathbb{F}_2^m$.)

Solution: The number of vectors in the kernel is the number of distinct linear combinations of kernel basis elements. Since the kernel has dimension $n - m$, the number of distinct linear combinations is 2^{n-m} .

- (c) Let $b \in \mathbb{F}_2^m$ be such that the system of equations $Ax = b$ has at least one solution, say x_0 . Show that $\{x - x_0 \mid Ax = b\} = \ker(A)$. What is the total number of solutions to the system $Ax = b$?

Solution: If $Ax = b$ then $A(x - x_0) = 0$, so $x - x_0 \in \ker(A)$. This means that $\{x - x_0 \mid Ax = b\} \subseteq \ker(A)$. In the other direction, if $x' \in \ker(A)$ then $A(x' + x_0) = b$, so any $x' \in \ker(A)$ can be written as $x - x_0$ such that $Ax = b$. So the two sets are equal. Since $f(x) = x - x_0$ is a 1-1 function, this means that there are 2^{n-m} solutions to $Ax = b$.

For this problem you may use the fact that for a matrix $A \in \mathbb{F}^{m \times n}$ for any field $\mathbb{F}$, if $R \subseteq \mathbb{F}^n$ denotes the set of its rows and $C \subseteq \mathbb{F}^m$ denotes the set of its columns, then

$$\dim(\text{Span}(R)) = \dim(\text{Span}(C)).$$

The quantity $\dim(\text{Span}(R))$ is called the row-rank of A and $\dim(\text{Span}(C))$ is called the column-rank of A .

4. Inner Products.

Consider the vector space $\mathbb{R}[x]$ of polynomials in a single variable x with coefficients in $\mathbb{R}$. Define the function $\mu : \mathbb{R}[x] \times \mathbb{R}[x] \rightarrow \mathbb{R}$ as

$$\mu(P, Q) = \text{degree}(P \cdot Q) \quad \text{for all } P, Q \in \mathbb{R}[x],$$

where $P \cdot Q$ denotes the product of the two polynomials P and Q (which is another polynomial). Is the function μ an inner product? Justify your answer.

Solution: No, it is not an inner product, because it fails linearity. For example, if $P = x$ and $Q = x^2$ then $\mu(P, Q) = 3$. But $\mu(P, 2Q) = 3 \neq 2\mu(P, Q)$.

5. Eigenvalues.

Let V be a finite dimensional vector space over a field $\mathbb{F}$ and $\alpha, \beta : V \rightarrow V$ be linear operators. Show that for every $\lambda \in \mathbb{F}$ (including $0_{\mathbb{F}}$), λ is an eigenvalue of $\alpha\beta$ if and only if λ is an eigenvalue of $\beta\alpha$. Here, $\alpha\beta$ denotes the linear transformation $\alpha \circ \beta$ defined as $\alpha\beta(v) = \alpha(\beta(v)) \forall v \in V$ (and $\beta\alpha$ is defined similarly).

Solution: Suppose λ is an eigenvalue of $\alpha\beta$. This means there is some $v \in V \setminus \{0_V\}$ such that $\alpha(\beta(v)) = \lambda v$. So, $\beta(\alpha(\beta(v))) = \beta(\lambda v) = \lambda\beta(v)$. In the case that $\beta(v) \neq 0_V$, this means that $\beta(v)$ is an eigenvector of eigenvalue λ for the linear transformation $\beta\alpha$. In the case that $\beta(v) = 0_V$ (which implies $\lambda = 0$) we can consider two cases: (a) $\text{im}(\alpha) = V$, which means $\alpha^{-1}(v)$ exists and is an eigenvector of eigenvalue 0 for $\beta\alpha$, or (b) $\text{im}(\alpha) \neq V$, which means there is some nonzero vector $w \in \ker(\alpha)$, and so w is an eigenvector of eigenvalue 0 of $\beta\alpha$.

The same argument shows that any eigenvector of $\beta\alpha$ must also be an eigenvector of $\alpha\beta$.