

MATH 731, FALL 2008
HOMEWORK SET 1 sample solutions

A. Let A, B be arbitrary sets and let $f : A \rightarrow B$ be a function. Prove that the following statements are equivalent.

(1) f is onto.

(2) f is right invertible, that is, there exists $g : B \rightarrow A$ with $f \circ g = \text{id}_B$.

(3) f is right cancellable, that is, if $g, h : B \rightarrow C$ are any functions with $g \circ f = h \circ f$, then $g = h$.

Proof. (1) \Rightarrow (2). For each $b \in B$, pick an element a_b in A with $f(a_b) = b$. Such elements exist since f is onto. Define $g : B \rightarrow A$ by $g(b) = a_b$. This is a function with $f \circ g = \text{id}_B$.

(2) \Rightarrow (3). Suppose $f' : B \rightarrow A$ satisfies $f \circ f' = \text{id}_B$ and suppose $g \circ f = h \circ f$, where $g, h : B \rightarrow C$. Then $g = g \circ f \circ f' = h \circ f \circ f' = h$.

(3) \Rightarrow (1). Suppose f is right cancellable but not onto, say $b \in B \setminus \text{im } f$. Choose any $y \neq b$ and let $C = \{b, y\}$. Define $g : B \rightarrow C$ by $g(x) = y$ for all $x \in B$ and define $h : B \rightarrow C$ by $h(b) = b$ and $h(x) = y$ for all $x \in B, x \neq b$. Clearly g, h are not equal, but equally clearly, $g \circ f = h \circ f$. This contradicts the statement that f is right cancellable.

Note: “cancelable” is the more common American spelling.

B. (i) Show that a group G is Abelian if and only if the map $\phi : G \rightarrow G$ defined by $\phi(g) = g^{-1}$ is a group homomorphism.

Proof. If G is Abelian, then $\phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \phi(g)\phi(h)$, so ϕ is a homomorphism.

Conversely, suppose ϕ is a homomorphism. Then for any $g, h \in G$, we have $gh = \phi((gh)^{-1}) = \phi(h^{-1}g^{-1}) = (h^{-1})^{-1}(g^{-1})^{-1} = hg$.

(ii) Determine for which fields F the map $\phi : F \rightarrow F$ defined by $\phi(0) = 0$ and $\phi(x) = x^{-1}$ for $x \neq 0$ is a field homomorphism.

Proof. The answer is that ϕ is a homomorphism if and only if F has 2, 3, or 4 elements, i.e., F is one of the fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$.

If $F = \mathbb{F}_2$ or \mathbb{F}_3 , then the map ϕ is just the identity, so naturally, it is a homomorphism. If $F = \mathbb{F}_4$, then F has 4 elements $0, 1, a, 1 + a$, where a satisfies $a^{-1} = a^2 = a + 1$. In this case $\phi(x) = x^2$ for all $x \in F$, and it is not hard to see that this is a homomorphism (the Frobenius endomorphism).

Suppose F is a field for which ϕ is a homomorphism. As long as $x \neq 0, -1$, we have $(x + 1)^{-1} = \phi(x + 1) = \phi(x) + \phi(1) = x^{-1} + 1$. Clearing fractions yields $x = (x + 1)^2$, or $x^2 + x + 1 = 0$. This polynomial can have at most two roots in F , so F can have at most 4 elements ($0, -1$, and the roots of $x^2 + x + 1 = 0$). Thus the only possibilities are the ones described in the previous paragraph.

C. Let V be a vector space and let $\pi : V \rightarrow V$ be a linear operator. We say π is an **internal projection** if $\pi^2 = \pi$. (The word “internal” is often omitted.)

(i) Let $\pi : V \rightarrow V$ be an internal projection. Prove that $V = \text{im } \pi \oplus \text{ker } \pi$.

Proof. Given $v \in V$, set $w = \pi(v)$ and $w' = v - \pi(v)$. It is obvious that $v = w + w'$ and that $w \in \text{im } \pi$. Furthermore, $\pi(w') = \pi(v) - \pi^2(v) = \pi(v) - \pi(v) = 0$, so $w' \in \text{ker } \pi$. Suppose $u \in \text{im } \pi \cap \text{ker } \pi$, so $u = \pi(v)$. Then $0 = \pi(u) = \pi^2(v) = \pi(v) = u$. This proves $V = \text{im } \pi \oplus \text{ker } \pi$.

(ii) Suppose W, W' are subspaces of V with $V = W \oplus W'$. Prove that there is an internal projection $\pi : V \rightarrow V$ with $\text{im } \pi = W$, $\pi|_W = \text{id}_W$, and $\text{ker } \pi = W'$.

Proof. Define $\pi(v) = w$, where $v = w + w'$ is the unique representation of v with $w \in W$, $w' \in W'$. This defines a function, and if $v \in W$, then $v = w$, so $\pi(v) = v$. Thus $\pi^2 = \pi$. Plainly $\text{im } \pi = W$ and $\text{ker } \pi = W'$.

To see that π is linear, note that $cv = cw + cw'$ and cw, cw' are in W, W' , so $\pi(cv) = cw = c\pi(v)$. Given v_1, v_2 , if we write them $v_i = w_i + w'_i$ as above, then $w_1 + w_2 \in W$, $w'_1 + w'_2 \in W'$. Thus $v_1 + v_2 = (w_1 + w_2) + (w'_1 + w'_2)$ is in the right form and so we have $\pi(v_1 + v_2) = w_1 + w_2 = \pi(v_1) + \pi(v_2)$.

D. Let V be a vector space over the field F and let U, W be subspaces. Prove that $\dim(U + W) + \dim(U \cap W) = \dim U + \dim W$.

Proof. Define $\phi : U \oplus W \rightarrow V$ by $\phi((u, w)) = u + w$. (This \oplus is external.) Clearly $\text{im } \phi = U + W$, while $\text{ker } \phi = \{(u, -u) \mid u \in U \cap W\}$. Thus $\text{ker } \phi \cong U \cap W$ via $(x, -x) \mapsto x$.

The Dimension Formula now gives us $\dim U + \dim W = \dim(U \oplus W) = \dim \text{im } \phi + \dim \text{ker } \phi = \dim(U + W) + \dim(U \cap W)$.

Here is an alternative proof. Let \mathcal{A} be a basis for $U \cap W$. Extend \mathcal{A} to bases $\mathcal{A} \cup \mathcal{B}$ for U and $\mathcal{A} \cup \mathcal{C}$ for W . We claim $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ is a basis for $U + W$.

It's easy to see that $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ spans $U + W$. To see that it's linearly independent, suppose we have a relation $\sum_{a \in \mathcal{A}} \alpha_a a + \sum_{b \in \mathcal{B}} \beta_b b + \sum_{c \in \mathcal{C}} \gamma_c c = 0$ for some sets of scalars, α, β, γ . Then $\sum_{c \in \mathcal{C}} \gamma_c c = -\sum_{a \in \mathcal{A}} \alpha_a a - \sum_{b \in \mathcal{B}} \beta_b b \in U$, so $\sum_{c \in \mathcal{C}} \gamma_c c \in U \cap W$. This means $\sum_{c \in \mathcal{C}} \gamma_c c = \sum_{a \in \mathcal{A}} \alpha'_a a$ for some scalar set α' . Linear independence of $\mathcal{A} \cup \mathcal{C}$ implies that each $\gamma_c = 0$. This means $\sum_{a \in \mathcal{A}} \alpha_a a + \sum_{b \in \mathcal{B}} \beta_b b = 0$, and so linear independence of $\mathcal{A} \cup \mathcal{B}$ means each α_a and each β_b is 0. This proves $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ is linearly independent.

We now have $\dim(U + W) + \dim(U \cap W) = |\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}| + |\mathcal{A}| = 2|\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}|$. We also have $\dim U + \dim W = |\mathcal{A} \cup \mathcal{B}| + |\mathcal{A} \cup \mathcal{C}| = 2|\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}|$.

E. Find all 2×2 matrices A over \mathbb{R} satisfying $A^2 = -I$.

Proof. We know A satisfies the polynomial $x^2 + 1$. Since this polynomial is irreducible, it must be the minimal polynomial of A . The characteristic polynomial is a multiple of the minimal polynomial, the characteristic polynomial must also be $x^2 + 1$.

The trace of A is the additive inverse of the coefficient of x , namely 0, and the determinant of A is the constant coefficient, namely 1. Thus $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, where $-a^2 - bc = 1$, i.e., $a^2 + bc = -1$.

One can check that any such matrix satisfies $A^2 = -I$, so the set of all matrices of the form $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ with $a^2 + bc = -1$ is the answer.