Math 115AH, Lecture 1 - HW6

Due on Gradescope by 11:59pm on Thursday, May 16.

What you can use in your proofs: *you may use basic facts which are not "course material", including facts from calculus or basic number theory. If you use such a result, you must clearly state the fact that you are using, although you do not justify it. You may also use any theorems in the textbook or discussed in class, unless the problem is specifically proving a theorem from the text or from class.*

1. **Isomorphisms and quotient spaces.** Let V be a finite-dimensional vector space over a field F, and let $T\colon V \to W$ be a linear transformation.

   (a) **Prove that $V/\operatorname{Ker}(T) \simeq \operatorname{Im}(T)$ by defining a linear transformation $f\colon V/\operatorname{Ker}(T) \to \operatorname{Im}(T)$ and checking that it is an isomorphism.**

   $V/\ker(T)$ is the set of equivalence classes such that for $u, v \in V, u \sim v$ if $u = v + w$ for some $w \in \ker(T)$.
   Let $[v] \in V/\ker(T)$. Since V is finite, by definition $V/\ker(T) \subset V$, so $v \in V$. Define $f([v]) = T(v)$.
   To show that f is an isomorphism, it suffices to show that f is invertible.

   (Injectivity)
   Let $[a], [b] \in V/\ker(T)$. If $f([a]) = f([b])$, then $f([a]) = T(a) = T(b) = f([b])$. If $T(a) = T(b)$, then

   $$T(a) - T(b) = 0$$
   $$T(a - b) = 0$$
   $$a - b \in \ker(T)$$

   So by definition, $[a] = [b]$, and T is injective.

   (Surjectivity)
   Let $w \in \operatorname{Im}(T)$. If f is surjective, there exists $[v] \in V/\ker(T)$ such that $f([v]) = w$. Since $w \in \operatorname{Im}(T), w = T(v)$ for some $v \in V$. By our definition of f, $f([v]) = T(v) = w$. Therefore, each w has a preimage $[v] \in V/\ker(T)$ such that $f([v]) = w$.

   Since f is both injective and surjective, it must be an isomorphism

   (b) **Suppose now that $\operatorname{Im}(T) = W$. Let $\{w_1, \ldots, w_n\}$ is a basis for $\operatorname{Ker}(T)$, and**

   $$\beta = \{w_1, \ldots, w_n, w_{n+1}, \ldots, w_k\}$$

   is a basis for V, where $k > n$. Explain why $\gamma = \{T(w_{n+1}), \ldots, T(w_k)\}$ is a basis for W, and describe the matrix $[T]_\beta^\gamma$.

   From observation, we see that $\dim(\ker(T)) = n, \dim(V) = n + k$.
   By rank-nullity,

   $$\dim(V) = \dim(\operatorname{Im}(T)) + \dim(\operatorname{Ker}(T))$$
   $$n + k = \dim(\operatorname{Im}(T)) + n$$

$$\dim(\text{Im}(T)) = k$$

Since β is a basis, $\{w_{n+1}, ..., w_k\}$ are linearly independent, so we need to show that $\{w_{n+1}, ..., w_k\}$ spans $W = \text{Im}(T)$.
Recall from consequences of the replacement theorem that if β spans V and $W \subset V$, there exists a linearly independent subset $\gamma \subset \beta$ such that $\text{span}(\gamma) = W$.
Suppose for some $v \in \beta$, we apply $T(v)$. Then

$$T(w_1) = T(w_2) = ... = T(w_n) = 0$$

Therefore the vectors $T(w_i) \notin \text{Im}(T)$ for $1 \leq i \leq n \implies$ the only vectors remaining to form a basis for $\text{Im}(T)$ are $\{T(w_{n+1}, ..., T(w_k)\}$
Since $\{w_{n+1}, ..., w_k\} \notin \ker(T), T(w_j) \in \text{Im}(T) \forall n+1 \leq j \leq k$.
Now we know that the a k-dimensional linearly independent subset of β exists and $\gamma = \{T(w_{n+1}, ..., T(w_k)\}$ is k-dimensional, linearly independent, and each $T(w_j) \in \text{Im}(T)$, therefore $\text{span}(\gamma) = W$.

The matrix $[T]_\beta^\gamma$ is the $k \times (n+k)$ matrix such that $[[T]_\beta^\gamma]_j = [T(w_j)]_\gamma$ for $w_j \in \beta$

2. **Invertible functions and matrices.**

(a) **Suppose that both $f\colon X \to Y$ and $g\colon Y \to Z$ are invertible functions. Show that $g \circ f$ is invertible by showing that $f^{-1} \circ g^{-1}$ is an inverse for $g \circ f$. (You may use that function composition is associative in your proof.)**

If f is invertible, then there exists $f^{-1}\colon Y \to X$ such that $f \circ f^{-1} = 1_Y$ and $f^{-1} \circ f = 1_X$
Similarly, if g is invertible, then there exists $g^{-1}\colon Z \to Y$ such that $g \circ g^{-1} = 1_Z$ and $g^{-1} \circ g = 1_Y$
Consider the function $f^{-1} \circ g^{-1}\colon Z \to X$.
Let $z \in Z$, then

$$(f^{-1} \circ g^{-1})(z) = f^{-1}(g^{-1}(z)) = x \quad \text{for some} \quad x \in X$$
$$(f \circ f^{-1})(g^{-1}(z)) = f(x) \quad \text{By associativity}$$
$$(g^{-1}(z)) = f(x)$$
$$(g \circ g^{-1})(z) = (g \circ f)(x)$$
$$z = (g \circ f)(x)$$

Therefore there exists the function $f^{-1} \circ g^{-1}$ which is an inverse for $g \circ f$, so $g \circ f$ is invertible.

(b) **Prove, by induction on n, that if we are given sets $X_0, \ldots, X_n$ and invertible functions $f_i\colon X_{i-1} \to X_i$ for $1 \leq i \leq n$, then**

$$f_n \circ f_{n-1} \circ \ldots \circ f_1\colon X_0 \to X_n$$

is invertible and has inverse

$$f_1^{-1} \circ \ldots \circ f_{n-1}^{-1} \circ f_n^{-1}\colon X_n \to X_0.$$

(You may use that function composition is associative in your proof.)

First check the base case $n = 1$. Then we have the sets X_0, X_1 and $f_1\colon X_0 \to X_1$. Then since f_1 is invertible, there exists $f_1^{-1}\colon X_1 \to X_0$ such that $f \circ f^{-1} = 1_{X_1}$ and $f^{-1} \circ f = 1_{X_0}$

For the inductive step, we want to show that $P_n \implies P_{n+1}$
If P_n is true, then

$$f_n \circ f_{n-1} \circ \ldots \circ f_1 \colon X_0 \to X_n$$

is invertible and has inverse

$$f_1^{-1} \circ \ldots \circ f_{n-1}^{-1} \circ f_n^{-1} \colon X_n \to X_0.$$

Suppose we have an invertible function

$$f_{n+1} \colon X_n \to X_{n+1}$$

$$f_{n+1} \circ f_n \circ \ldots \circ f_1 \colon X_0 \to X_{n+1}$$

Let $v \in X_0$, then $(f_n \circ f_{n-1} \circ \ldots \circ f_1)(v) = w$ for some $w \in X_n$. Since P_n is true,

$$(f_1^{-1} \circ \ldots \circ f_{n-1}^{-1} \circ f_n^{-1})(w) = v$$

Now consider $f_{n+1}(w) = y$ for some $y \in X_{n+1}$. Then

$$(f_{n+1}(f_n \circ f_{n-1} \circ \ldots \circ f_1))(v) = y$$

$$(*)(f_{n+1} \circ f_n \circ f_{n-1} \circ \ldots \circ f_1)(v) = y \quad \text{By associativity}$$

Since f_{n+1} is invertible, there exists f_{n+1}^{-1} such that $f_{n+1}^{-1}(y) = w$. Therefore we substitute and get

$$(f_1^{-1} \circ \ldots \circ f_{n-1}^{-1} \circ f_n^{-1})(f_{n+1}^{-1}(y)) = v$$

Notice this function is from $X_{n+1} \to X_0$ By function composition associativity, this becomes

$$(f_1^{-1} \circ \ldots \circ f_{n-1}^{-1} \circ f_n^{-1} \circ f_{n+1}^{-1})(y) = v$$

Therefore the above function is an inverse for (*), and our initial assumption is true.

(c) **Let $A, B \in \mathrm{Mat}_{n\times n}(F)$ be two invertible matrices. Using the relationship between function composition and matrix multiplication, the previous item in this problem, and Theorems 2.15 and Theorem 2.18 in the textbook, show that $B \cdot A \in \mathrm{Mat}_{n\times n}(F)$ is invertible with inverse given by $A^{-1} \cdot B^{-1}$.**

Consider the linear transformation $L_{B\cdot A}(\vec{x}) = BA\vec{x}$ for $x \in F^n$.
Additionally, let the linear transformations L_B and L_A be $B\vec{x}$ and $A\vec{x}$ respectively for $x \in F^n$.
Since A and B are invertible, we also have $(L_A)^{-1}$ and $(L_B)^{-1}$
Recall that $L_{B\cdot A} = L_B \circ L_A$ and that $C \in M_{n\times n}(F)$ is invertible $\iff$ L_C is invertible and $(L_C)^{-1} = L_{C^{-1}}$
Then

$$L_{B\cdot A}(\vec{x}) = L_B \circ L_A = BA\vec{x}$$

$$((L_B)^{-1})(L_B \circ L_A) = (L_B)^{-1}(BA\vec{x})$$

$$((L_B)^{-1} \circ L_B \circ L_A) = (L_B)^{-1}(BA\vec{x})$$

$$(1_F \circ L_A) = (L_{B^{-1}})(BA\vec{x})$$

$$(1_F \circ L_A) = (B^{-1})(BA\vec{x})$$

$$(L_A)^{-1}(1_F \circ L_A) = (L_A)^{-1}(B^{-1})(BA\vec{x})$$
$$1_F = (L_A)^{-1}(B^{-1})(BA\vec{x})$$
$$1_F = (L_{A_{-1}}(B^{-1})(BA\vec{x})$$
$$1_F = A^{-1}B^{-1}(BA\vec{x})$$
$$1_F = A^{-1}B^{-1}L_{B\cdot A}(\vec{x})$$

We can show that other way easily:
Multiplying the above by A then B, we get:

$$BA = L_{B\cdot A}(\vec{x})$$

$$BAA^{-1}B^{-1} = L_{B\cdot A}(\vec{x})A^{-1}B^{-1}$$
$$B1_FB^{-1} = L_{B\cdot A}(\vec{x})A^{-1}B^{-1}$$
$$BB^{-1} = L_{B\cdot A}(\vec{x})A^{-1}B^{-1}$$
$$1_F = L_{B\cdot A}(\vec{x})A^{-1}B^{-1}$$

$\implies A^{-1}B^{-1}$ is an inverse for $L_{B\cdot A}(\vec{x})$

3. **Textbook 2.4 #19. Note that the textbook writes ϕ_β for the linear transformation of taking β-coordinates, which we call f_β.**
Consider the linear transformation $T\colon M_{2\times 2}(R) \to M_{2\times 2}(R)$ defined by $T(M) = M^t$. Let $\beta = \{E^{11}, E^{12}, E^{21}, E^{22}\}$ be a basis for $M_{2\times 2}(R)$

   (a) **Compute** $[T]_\beta$
   (These are column vectors)
   $[T(E^{11})]_\beta = [E^{11}]_\beta = [1\ 0\ 0\ 0]$
   $[T(E^{12})]_\beta = [E^{21}]_\beta = [0\ 0\ 1\ 0]$
   $[T(E^{21})]_\beta = [E^{12}]_\beta = [0\ 1\ 0\ 0]$
   $[T(E^{22})]_\beta = [E^{22}]_\beta = [0\ 0\ 0\ 1]$
   Therefore $[T]_\beta =$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

   (b) **Verify that** $L_A\phi_\beta(M) = \phi_\beta T(M)$ **for** $A = [T]_\beta$ **and**

$$M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

   $(L_A\phi_\beta)(M) = L_A[M]_\beta$

$$= A[M]_\beta$$
$$= [T]_\beta[M]_\beta$$

$$\phi_\beta T(M) = [T(M)]_\beta = \begin{pmatrix} 1 \\ 3 \\ 2 \\ 4 \end{pmatrix}$$

Then $[T]_\beta[M]_\beta =$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 2 \\ 4 \end{pmatrix} = \phi_\beta T(M)$$

4. **Compute the determinants of the following matrix A. State which row or column you are using to apply the recursive definition of the determinant.**

$$A := \begin{pmatrix} -3 & 4 & 0 & -1 \\ 0 & 9 & -2 & -3 \\ 1 & 1 & 1 & 1 \\ 3 & 0 & 3 & 0 \end{pmatrix}.$$

Iterate across the bottom row since there are two zeroes

$$\det(A) = 3\det\begin{pmatrix} 4 & 0 & -1 \\ 9 & -2 & -3 \\ 1 & 1 & 1 \end{pmatrix} + 3\det\begin{pmatrix} -3 & 4 & -1 \\ 0 & 9 & -3 \\ 1 & 1 & 1 \end{pmatrix}$$

Iterate across top row and first column respectively

$$= 3\left(4\det\begin{pmatrix} -2 & -3 \\ 1 & 1 \end{pmatrix} - \det\begin{pmatrix} 9 & -2 \\ 1 & 1 \end{pmatrix}\right) + 3\left(-3\det\begin{pmatrix} 9 & -3 \\ 1 & 1 \end{pmatrix} + \det\begin{pmatrix} 4 & -1 \\ 9 & -3 \end{pmatrix}\right)$$

$$\begin{aligned} &= 3[4(-2+3) - (9+2) - 3(9+3) + (-12+9)] \\ &= 3[4(1) - (11) - 3(12) + (-3)] \\ &= 3[4 - 11 - 36 + -3] \\ &= 3[-46] \\ &= -138 \end{aligned}$$

5. **Textbook 2.5 #7.**
In $\mathbb{R}^2$, let L be the line $y = mx$, where $m \neq 0$. Find an expression for $T(x, y)$, where

(a) T **is the reflection of** $\mathbb{R}^2$ **about** L

The slope of $L^\perp = -\frac{1}{m}$. Suppose we have the point (x', y'). Then to find the line $L^\perp$ it is on, we use $y - y' = -\frac{1}{m}(x - x')$. To find the intersection of L and $L^\perp$, we need to find a point on both lines. Any point on L is in the form (k, km) for some $k \in \mathbb{R}$. Then k is the midpoint of x' and $T(x')$ and km is the midpoint of y' and $T(y') \implies$

$$T(x') - k = k - x'$$

$$T(x') = 2k - x'$$

Similarly

$$T(y') = 2km - y'$$

Now to solve for k, we know that $T(x', y')$ is on the line $y - y' = -\frac{1}{m}(x - x')$. Then

$$(2k - y') - y' = -\frac{1}{m}((2km - x') - x')$$

$$2km - 2y' = -\frac{2k - 2x'}{m}$$

$$km - y' = -\frac{k - x'}{m}$$

$$-m^2k + my' = k - x'$$

$$x' + my' = k + m^2k$$

$$x' + my' = k(1 + m^2)$$

$$k = \frac{x' + my'}{1 + m^2}$$

Substituting, we get

$$T(x') = 2(\frac{x' + my'}{1 + m^2}) - x'$$

$$= \frac{2x' + 2my'}{1 + m^2} - \frac{x'(1 + m^2)}{1 + m^2}$$

$$= \frac{2x' + 2my' - x'(1 + m^2)}{1 + m^2}$$

$$= \frac{2x' + 2my' - x' - x'm^2)}{1 + m^2}$$

$$T(x') = \frac{x' + 2my' - x'm^2}{1 + m^2}$$

Similarly,

$$T(y') = 2(\frac{x' + my'}{1 + m^2})m - y'$$

$$T(y') = 2(\frac{x' + my'}{1 + m^2})m - \frac{y'(1 + m^2)}{1 + m^2}$$

$$T(y') = \frac{2mx' + 2m^2y' - y' - y'm^2)}{1 + m^2}$$

$$T(y') = \frac{2mx' + m^2y' - y'}{1+m^2}$$

Therefore,

$$T(x,y) = \left(\frac{x + 2my - xm^2}{1+m^2}, \frac{2mx + m^2y - y}{1+m^2}\right)$$

(b) T **is the projection on** L **along the line perpendicular to** L

Consider the point (x', y'). We know that the slope of $L^{\perp} = -\frac{1}{m}$
Therefore,

$$y - y' = -\frac{1}{m}(x - x')$$

We can obtain $T(x', y')$ from $(x' - k, y' - km)$ for some $k \in \mathbb{R}$
Now to solve for k :

$$(y' - km) - y' = -\frac{1}{m}(x' - k) - x'$$

$$-km = -\frac{x' - k - x'm}{m}$$

$$m^2k = x' - k - x'm$$

$$m^2k + k = x' - x'm$$

$$k = \frac{x' - x'm}{m^2+1}$$

Now substitute back in $T(x') = x' - k =$

$$x' - \frac{x' - x'm}{m^2+1}$$

$$= \frac{x'(m^2+1) - x' + x'm}{m^2+1}$$

$$= \frac{x'm^2 + x' - x' + x'm}{m^2+1}$$

$$= \frac{x'm^2 + x'm}{m^2+1}$$

Similarly, $T(y') =$

$$y' - \frac{x' - x'm}{m^2+1}(m)$$

$$= \frac{y'(m^2+1) - m(x' - x'm)}{m^2+1}$$

$$= \frac{y'm^2 + y' - mx' + x'm^2}{m^2+1}$$

Therefore,

$$T(x', y') = (\frac{x'm^2 + x'm}{m^2+1}, \frac{y'm^2 + y' - mx' + x'm^2}{m^2+1})$$

6. **Let** $T\colon \mathrm{Mat}_{2\times 2}(\mathbb{Z}/2\mathbb{Z}) \to \mathrm{Mat}_{2\times 2}(\mathbb{Z}/2)$ **be given by**

$$T(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} a & b \\ 0 & a. \end{pmatrix}$$

(a) Let

$$S = \{E_{11}, E_{12}, E_{21}, E_{22}\}$$

be the standard basis for $\mathrm{Mat}_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$. Let

$$\beta = \{E_{11},\ E_{11}+E_{22},\ E_{12},\ E_{21}\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\}.$$

Compute $[T]_S$ and $[T]_\beta$.

First for $[T]_S$:

$T(E_{11}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = [1\ 0\ 0\ 1]$

$T(E_{12}) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = [0\ 1\ 0\ 0]$

$T(E_{21}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = [0\ 0\ 0\ 0]$

$T(E_{22}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = [0\ 0\ 0\ 0]$

Then $[T]_S =$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

For $[T]_\beta$:

$T(E_{11}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = [0\ 1\ 0\ 0]$

$T(E_{11}+E_{22}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = [0\ 1\ 0\ 0]$

$T(E_{12}) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = [0\ 0\ 1\ 0]$

$T(E_{21}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = [0\ 0\ 0\ 0]$

Then $[T]_\beta =$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(b) **Let $V = \mathrm{Mat}_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$. Compute $Q = [I_V]_S^\beta$ and $Q^{-1} = [I_V]_\beta^S$.**

$Q = [I_V]_S^\beta$:

$$[I_V(E_{11})]_\beta = [E_{11}]_\beta = [1\ 0\ 0\ 0]$$
$$[I_V(E_{12})]_\beta = [E_{12}]_\beta = [0\ 0\ 1\ 0]$$
$$[I_V(E_{21})]_\beta = [E_{21}]_\beta = [0\ 0\ 0\ 1]$$
$$[I_V(E_{22})]_\beta = [E_{22}]_\beta = [-1\ 1\ 0\ 0]$$

Then $Q = [I_V]_S^\beta =$

$$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$Q^{-1} = [I_V]_\beta^S$:

$$[I_V(E_{11})]_S = [E_{11}]_S = [1\ 0\ 0\ 0]$$
$$[I_V(E_{11} + E_{22})]_S = [E_{11} + E_{22}]_S = [1\ 0\ 0\ 1]$$
$$[I_V(E_{12})]_S = [E_{12}]_S = [0\ 1\ 0\ 0]$$
$$[I_V(E_{21})]_S = [E_{21}]_S = [0\ 0\ 1\ 0]$$

Then $Q^{-1} = [I_V]_\beta^S =$

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

(c) **Verify that $Q^{-1}[T]_\beta Q = [T]_S$.**
$Q^{-1}[T]_\beta Q =$

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$= [T]_\beta$$

7. **A *permutation* of the set $\{1, \ldots, n\}$ is a bijective function $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$. We denote the set of all permutations of $\{1, \ldots, n\}$ by S_n.**

Intuitively, we can think of such a permutation as a "shuffle" of the elements in $\{1, \ldots, n\}$. The simplest type of permutations are *transpositions*, which just swap two elements. We can write these down precisely as follows. Given $i, j \in \{1, \ldots, n\}$ with $i \neq j$, let $\sigma_{ij}\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ be the function defined on $k \in \{1, \ldots, n\}$ piecewise by:

$$\sigma_{ij}(k) = \begin{cases} j & \text{if } k = i \\ i & \text{if } k = j \\ k & \text{otherwise.} \end{cases}$$

In otherwords, σ_{ij} swaps i and j and fixes all other elements.

Every permutation can be written as a composition of transpositions: on can obtain any shuffling of $\{1, \ldots, n\}$ by swapping pairs one at a time. In other words, for all $\sigma \in S_n$, there exists a sequence $i_1, i_2, \ldots, i_k$ and $j_1, \ldots, j_k$ such that

$$\sigma = \sigma_{i_k, j_k} \circ \cdots \circ \sigma_{i_2, j_2} \circ \sigma_{i_1, j_1} \tag{1}$$

Such a representation is not unique.

The *sign* of a permutation is defined to be the number of transpositions needed to complete the permutation, taken modulo 2. So, if σ satisfies (1), then

$$\operatorname{sign}(\sigma) = [k] \in \mathbb{Z}/2\mathbb{Z}.$$

It turns out that, while the representation of a given permutation as a composition of transpositions is not unique, the sign is well-defined: if σ can be written as a composition of k transpositions and also as a composition of k' transpositions, then $[k] = [k']$ in $\mathbb{Z}/2\mathbb{Z}$. The sign of a permutation is also equal to the number of pairs (i, j) in $\{1, \ldots, n\} \times \{1, \ldots, n\}$ for which $i < j$ but $\sigma(i) > \sigma(j)$. **(You may use these facts without proof.)**

Another definition of the determinant is the following: given an $n \times n$ matrix A,

$$\det(A) = \Sigma_{\sigma \in S_n} (-1)^{\text{sign}(\sigma)} A_{1\sigma(1)} A_{2\sigma(2)} \ldots A_{n\sigma(n)}, \tag{2}$$

where we make the convention that $(-1)^{[k]} = (-1)^k$ for $[k] \in \mathbb{Z}/2\mathbb{Z}$. It turns out that (2) agrees with the other definitions of the determinant that we have seen, which you will prove in the last part of this problem.

(a) **Consider the permutation $\sigma\colon \{1, 2, 3\} \to \{1, 2, 3\}$ given by $\sigma(1) = 3$, $\sigma(2) = 1$, and $\sigma(3) = 2$. What is $\text{sign}(\sigma)$?**

$\sigma(1, 2, 3) = \sigma_{2,3} \circ \sigma_{1,3}(3, 1, 2)$ (where the subscripts are the indeces)
$\text{sign}(\sigma) = 0$

(b) **Since permutations are bijective maps from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$, their inverses are also bijective maps from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$, i.e., are permutations. Given $\sigma \in S_n$, show that $\text{sign}(\sigma) = \text{sign}(\sigma^{-1})$. (Hint: problem 2 might help!)**

Recall from Problem 2 that if we are given sets $X_0, \ldots, X_n$ and invertible functions $f_i\colon X_{i-1} \to X_i$ for $1 \le i \le n$, then

$$f_n \circ f_{n-1} \circ \ldots \circ f_1 \colon X_0 \to X_n$$

is invertible and has inverse

$$f_1^{-1} \circ \ldots \circ f_{n-1}^{-1} \circ f_n^{-1} \colon X_n \to X_0.$$

In this problem, notice that our $X_0 = ... = X_n = \{1, ..., n\}$. In particular notice that

$$\sigma = \sigma_n \circ \sigma_{n-1} \circ ... \circ \sigma_1 : \{1, ..., n\} \to \{1, ..., n\}$$

and

$$\sigma^{-1} = \sigma_1^{-1} \circ ... \circ \sigma_{n-1}^{-1} \circ \sigma_n^{-1} : \{1, ..., n\} \to \{1, ..., n\}$$

σ^{-1} has the same number of transpositions as σ.
Suppose σ has k transpositions. Then by Problem 2, σ^{-1} also has k transpositions. Therefore $\text{sign}(\sigma) = \text{sign}(\sigma^{-1})$

(c) **Prove that, if σ and τ are two permutations on $\{1, \ldots, n\}$, then $\text{sign}(\sigma \circ \tau) = \text{sign}(\sigma) + \text{sign}(\tau)$, where the right-hand addition takes place in $\mathbb{Z}/2\mathbb{Z}$.**

Let $\sigma = \sigma_n \circ \sigma_{n-1} \circ ... \circ \sigma_1 : \{1, ..., n\} \to \{1, ..., n\}$ and
$\tau = \tau_m \circ \tau_{m-1} \circ ... \circ \tau_1 : \{1, ..., n\} \to \{1, ..., n\}$
Then

$$\sigma \circ \tau = \sigma_n \circ \sigma_{n-1} \circ ... \circ \sigma_1 \circ \tau_m \circ \tau_{m-1} \circ ... \circ \tau_1$$

Therefore $\text{sign}(\sigma \circ \tau) = (n + m) \mod 2$. $\text{sign}(\sigma) = n \mod 2$ and $\text{sign}(\tau) = m \mod 2$. WTS that $(n \mod 2) + (m \mod 2) = (n + m) \mod 2$. This is equivalent to the statement

$$[n] + [m] = [n + m]$$

Recall that addition is defined on $\mathbb{Z}/2\mathbb{Z}$ such that for $[v], [u] \in \mathbb{Z}/2\mathbb{Z}$, $[v] + [u] = [v + u]$. Therefore $\text{sign}(\sigma \circ \tau) = \text{sign}(\sigma) + \text{sign}(\tau)$.

(d) **Using the permutation definition of the determinant, prove that $\det(A) = \det(A^t)$.**
The permutation definition is:

$$\det(A) = \Sigma_{\sigma \in S_n} (-1)^{\text{sign}(\sigma)} A_{1\sigma(1)} A_{2\sigma(2)} \dots A_{n\sigma(n)},$$

Then,

$$\det(A^t) = \Sigma_{\sigma \in S_n} (-1)^{\text{sign}(\sigma)} A_{\sigma(1)1} A_{\sigma(2)2} \dots A_{\sigma(n)n},$$

Recall that σ is a bijection and σ^{-1} is therefore also a bijection and a permutation. Therefore

$$\det(A^t) = \Sigma_{\sigma \in S_n} (-1)^{\text{sign}(\sigma)} A_{\sigma(1)1} A_{\sigma(2)2} \dots A_{\sigma(n)n}$$

$$= \Sigma_{\sigma \in S_n} (-1)^{\text{sign}(\sigma)} A_{1\sigma^{-1}(1)} A_{2\sigma^{-1}(2)} \dots A_{n\sigma^{-1}(n)}$$

These are equivalent because multiplication of entries within the matrices is commutative on the field F and you will still get every permutation possible (because σ and σ^{-1} are a bijections). In one case you are fixing the columns and permuting all the rows, in the other case you are fixing the rows and permuting all the columns.
Lastly, we know that $\text{sign}(\sigma) = \text{sign}(\sigma^{-1})$, so we know that the sign will be the same between the two summatioms for every permutation. Therefore $\det(A) = \det(A^t)$

(e) **Prove, by induction on n, that for any $n \times n$ matrix A and for any $j \in \{1, \dots, n\}$,**

$$\Sigma_{i=1}^{n} (-1)^{i+j} A_{ij} \det(\overline{A_{ij}}) = \Sigma_{\sigma \in S_n} (-1)^{\text{sign}(\sigma)} A_{1\sigma(1)} A_{2\sigma(2)} \dots A_{n\sigma(n)}.$$

Consider first the base case of $n = 1$

$$= (-1)^{1-1} A_{11} = A_{11} = (-1)^0 A_{11} = A_{11}$$

Because that case seems trivial, lets also consider $n = 2$. Then

$$A_{11}A_{22} - A_{21}A_{12} =$$

$$(-1)^{\text{sign}(\sigma_1)} A_{1\sigma_1(1)} A_{2\sigma_1(2)} + (-1)^{\text{sign}(\sigma_2)} A_{1\sigma_2(1)} A_{2\sigma_2(2)}$$

There are two possible permutations:

$$\sigma_1(a, b) = (b, a) \implies \text{sign}(\sigma_1) = 1$$

$$\sigma_2(a, b) = (a, b) \implies \text{sign}(\sigma_2) = 0$$

Therefore we get

$$(-1)^1 A_{12}A_{21} + (-1)^0 A_{11}A_{22}$$
$$= A_{11}A_{22} - A_{12}A_{21}$$

For the inductive step, WTS that $P_n \implies P_{n+1}$ Assume that

$$\Sigma_{i=1}^{n} (-1)^{i+j} A_{ij} \det(\overline{A_{ij}}) = \Sigma_{\sigma \in S_n} (-1)^{\text{sign}(\sigma)} A_{1\sigma(1)} A_{2\sigma(2)} \dots A_{n\sigma(n)}.$$

Then notice that

$$\Sigma_{i=1}^{n+1} (-1)^{i+j} A_{ij} \det(\overline{A_{ij}}) = \Sigma_{i=1}^{n} (-1)^{i+j} A_{ij} \det(\overline{A_{ij}}) + (-1)^{n+1+j} A_{(n+1)j} \det(\overline{A_{(n+1)j}})$$

Additionally,

$$\Sigma_{\sigma \in S_{n+1}} (-1)^{\text{sign}(\sigma)} A_{1\sigma(1)} A_{2\sigma(2)} \dots A_{n+1\sigma(n+1)}$$

$$= (\Sigma_{\sigma \in S_n} (-1)^{\text{sign}(\sigma)} A_{1\sigma(1)} A_{2\sigma(2)} \dots A_{n\sigma(n)}) + (-1)^{\text{sign}(\sigma_{n+1})} A_{1\sigma_{n+1}(1)} A_{2\sigma_{n+1}(2)} \dots A_{n\sigma_{n+1}(n)}$$

Then from assumption, we want to show that

$$(-1)^{n+1+j}A_{(n+1)j}\det(\overline{A_{(n+1)j}}) = (-1)^{\text{sign}(\sigma_{n+1})}A_{1\sigma_{n+1}(1)}A_{2\sigma_{n+1}(2)}\dots A_{n\sigma_{n+1}(n)}$$

σ_{n+1} fixes a row and permutes through all the columns. The key point is that the RHS will include an element from the $n+1$-th row and $n+1$-th column. On the LHS, we are essentially still expanding down the j-th column, and we are calculating for the $n+1$ row. The recursive definition on the LHS finds all the permutations for the $n \times n$ matrix, and then multiplying by the fixed element in the $n+1$ row. These permutations are exactly the same as the ones found on the RHS.
Using the same argument as from part (d), the inversions introduced maintain consistency among signs, therefore the signs are the same for all the permutations.
Therefore, the two sides are equal $\implies P_n \implies P_{n+1}$, and we have proven our assumption.