ALGEBRAIC COMBINATORICS II, HOMEWORK 1
DUE JULY 25 AT 5:30PM

Some ground rules:

- Feel free to use English, Chinese, or both, in your solutions.
- Write your argument as clear as possible, and make sure the writing in your submission is clear.
- Feel free to use results that are proved in class. If you'd like to use other results, you have to prove them before using them.
- You're encouraged to work together on the assignments. In your solutions, you should acknowledge the students with whom you worked, and should **write solutions on your own**.

Problems:

(1) Prove the following statements.

(a) Prove that any set with a binary operator $(S, \circ)$ has at most one identity element.

(b) Let $(S, \circ, e)$ be a set with an associative binary operator and an identity element. Prove that any element in S has at most one inverse. *(Does the statement still hold without the "associativity" assumption on $(S, \circ)$?)*

(c) Let $f\colon G \to H$ be a group homomorphism. Prove that:

(i) it preserves the identity: $f(e_G) = e_H$;

(ii) it preserves the inverses: $f(g^{-1}) = f(g)^{-1}$ for any $g \in G$.

(2) Let n be a positive integer. Euler's function $\varphi(n)$ counts the numbers in $\{1, 2, \ldots, n\}$ that are relatively prime to n.

Let G be a group that is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Prove that there are exactly $\varphi(n)$ elements in G that have order n.

(3) The next two problems concern isometries of $\mathbb{R}^n$. In this course, we always equip $\mathbb{R}^n$ with the standard Euclidean metric, i.e. for $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{y} = (y_1, \ldots, y_n)$ we have

$$d(\vec{x}, \vec{y}) = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}.$$

Let $\mathrm{O}(n, \mathbb{R})$ be the set of isometries of $\mathbb{R}^n$ that preserve the origin $\vec{0} \in \mathbb{R}^n$, i.e.

$$\mathrm{O}(n, \mathbb{R}) = \left\{ T\colon \mathbb{R}^n \to \mathbb{R}^n \mid T \text{ is an isometry and } T(\vec{0}) = \vec{0} \right\}.$$

Prove that for any isometry $f\colon \mathbb{R}^n \to \mathbb{R}^n$, there exist $T \in \mathrm{O}(n, \mathbb{R})$ and $\vec{v} \in \mathbb{R}^n$ such that

$$f(\vec{x}) = T(\vec{x}) + \vec{v} \text{ holds for any } \vec{x} \in \mathbb{R}^n.$$

In other words, any isometry of $\mathbb{R}^n$ can be written as a composition of an origin-preserving isometry and a translation.

(4) In this problem, you'll prove that any origin-preserving isometry of $\mathbb{R}^n$ is *linear*. We say a function $T\colon \mathbb{R}^n \to \mathbb{R}^n$ is *linear* if for any $\vec{x}, \vec{y} \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$ we have $T(\vec{x}+\vec{y}) = T(\vec{x})+T(\vec{y})$ and $T(\lambda\vec{x}) = \lambda T(\vec{x})$.

Let $g\colon \mathbb{R}^n \to \mathbb{R}^n$ be an origin-preserving isometry, i.e. an isometry with $g(\vec{0}) = \vec{0}$.

(a) Denote the *inner product* of $\vec{x} = (x_1, \dots, x_n)$ and $\vec{y} = (y_1, \dots, y_n)$ by

$$\langle \vec{x}, \vec{y} \rangle = x_1 y_1 + \cdots + x_n y_n.$$

In particular, $\langle \vec{x}, \vec{x} \rangle = x_1^2 + \cdots + x_n^2 = d(\vec{x}, \vec{0})^2$. Denote $||\vec{x}|| \coloneqq d(\vec{x}, \vec{0}) = \sqrt{\langle \vec{x}, \vec{x} \rangle}$. Prove that

$$\langle \vec{x}, \vec{y} \rangle = \frac{1}{2}\left(||\vec{x}||^2 + ||\vec{y}||^2 - ||\vec{x}-\vec{y}||^2\right),$$

and prove that g preserves the inner product, i.e. $\langle g(\vec{x}), g(\vec{y}) \rangle = \langle \vec{x}, \vec{y} \rangle$ for any $\vec{x}, \vec{y} \in \mathbb{R}^n$.

(b) It is easy to show that the inner product on $\mathbb{R}^n$ satisfies the following properties: (you don't have to prove these properties in your homework)

- (symmetric) $\langle \vec{x}, \vec{y} \rangle = \langle \vec{y}, \vec{x} \rangle$.
- (linearity in the first component) $\langle \vec{x}_1 + \vec{x}_2, \vec{y} \rangle = \langle \vec{x}_1, \vec{y} \rangle + \langle \vec{x}_2, \vec{y} \rangle$ and $\langle \lambda\vec{x}, \vec{y} \rangle = \lambda \langle \vec{x}, \vec{y} \rangle$. Note that it is also linear in the second component since it is symmetric.
- (positive definiteness) $\langle \vec{x}, \vec{x} \rangle > 0$ for any $\vec{x} \neq \vec{0}$.

Using the above properties, along with what we proved in (a) that g is inner-product preserving, prove that $||g(\vec{x}+\vec{y}) - g(\vec{x}) - g(\vec{y})||^2 = 0$ and $||g(\lambda\vec{x}) - \lambda g(\vec{x})||^2 = 0$, then conclude that g is linear.