1. Unitary linear maps

This problem is relevant to quantum computing. Let \( \mathbb{C} \) be the complex numbers, and suppose \( n \geq 1 \). The \( n \)-dimensional vector space \( \mathbb{C}^n \) is the set of all \( n \)-tuples \( \mathbf{a} = (a_1, \ldots, a_n) \) of complex numbers \( a_i \). This becomes a group under addition when we define

\[
\mathbf{a} + \mathbf{b} = (a_1 + b_1, \ldots, a_n + b_n)
\]

for \( \mathbf{b} = (b_1, \ldots, b_n) \). The identity element is \( \mathbf{0} = (0, \ldots, 0) \). We can also multiply elements \( \mathbf{a} \in \mathbb{C}^n \) by scalars \( r \in \mathbb{C} \) by letting

\[
r \cdot \mathbf{a} = (ra_1, \ldots, ra_n).
\]

A map \( f : \mathbb{C}^n \to \mathbb{C}^n \) is \( \mathbb{C} \)-linear if

\[
f(\mathbf{a} + \mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b}) \quad \text{and} \quad f(r \cdot \mathbf{a}) = rf(\mathbf{a})
\]

for all \( \mathbf{a}, \mathbf{b} \in \mathbb{C}^n \) and \( r \in \mathbb{C} \). The complex inner product \( \langle \phantom{\mathbf{a}}, \phantom{\mathbf{b}} \rangle \) on \( \mathbb{C}^n \) is defined by

\[
\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^{n} a_i \overline{b_i}
\]

where \( \overline{b_i} \) is the complex conjugate of \( b_i \).

1. The Unitary group \( U(n) \) is defined as the set of all \( \mathbb{C} \)-linear bijections \( f : \mathbb{C}^n \to \mathbb{C}^n \) such that

\[
\langle f(\mathbf{a}), f(\mathbf{b}) \rangle = \langle \mathbf{a}, \mathbf{b} \rangle
\]

for all \( \mathbf{a}, \mathbf{b} \in \mathbb{C}^n \). Show that \( U(n) \) is a group when we define the group law to be the composition of maps, so that \( (f \circ h)(\mathbf{a}) = f(h(\mathbf{a})) \) for \( f, h \in U(n) \) and \( \mathbf{a} \in \mathbb{C}^n \). Show that \( f(\mathbf{0}) = \mathbf{0} \), and that \( f \) maps \( S = \{ \mathbf{a} : \sum_{i=1}^{n} |a_i|^2 = 1 \} \) bijectively to \( S \).

2. The vector space \( \mathbb{C}^n \) has a basis \( v_1, \ldots, v_n \) such that \( v_1 = (1,0,\ldots,0) \), \( v_2 = (0,1,\ldots,0) \), ..., \( v_n = (0,0,\ldots,0,1) \). To a \( \mathbb{C} \)-linear map \( f : \mathbb{C}^n \to \mathbb{C}^n \) we can associate an \( n \times n \) matrix \( M(f) = (a_{i,j})_{1 \leq i,j \leq n} \) with entries in \( \mathbb{C} \) such that

\[
f(v_j) = \sum_{i=1}^{n} a_{i,j} v_i
\]

for \( j = 1, \ldots, n \). (This corresponds to treating \( v_j \) as a column vector and multiplying \( v_j \) on the left by \( M(f) \) to arrive at \( f(v_j) \).) If \( B = (b_{i,j}) \in \text{Mat}_{n,n}(\mathbb{C}) \) is any \( n \times n \) matrix, define \( B^* = (b_{i,j}^*) \) to be the matrix whose \((i, j)\) entry is \( b_{i,j}^* = \overline{b_{j,i}} \). Call \( B \) a unitary matrix if \( B^* \cdot B \) equals the identity matrix \( I \).

a. Show that a \( \mathbb{C} \)-linear bijection \( f : \mathbb{C}^n \to \mathbb{C}^n \) is in the unitary group \( U(n) \) if and only if its matrix \( M(f) \) is unitary. This means that the map \( f \mapsto M(f) \) gives an isomorphism between the unitary group \( U(n) \) and the group \( \tilde{U}(n) \) of all unitary matrices under multiplication.
Hints: Show that \( \langle v_j, v_i \rangle \) equals 1 (resp. 0) if \( i = j \) (resp. if \( i \neq j \)). Then use the linearity of \( f \) to show \( \langle f(v_j), f(v_i) \rangle \) is the \((i, j)\) entry in the product matrix \( M(f)^* \cdot M(f) \). Then show that \( f \) is unitary if and only if \( \langle f(v_j), f(v_i) \rangle = \langle v_j, v_i \rangle \) for all \( i \) and \( j \), and that this is true if and only if \( M(f)^* \cdot M(f) = I \).

b. Suppose that \( \sigma : \{v_1, \ldots, v_n\} \to \{v_1, \ldots, v_n\} \) is a permutation of \( \{v_1, \ldots, v_n\} \). Show that there is a unique element \( f_\sigma \in U(n) \) such that \( f_\sigma(v_i) = \sigma(v_i) \) for all \( i = 1, \ldots, n \). Prove that the matrix \( M(f_\sigma) \) has exactly one non-zero entry in each row and each column, and each such entry equals 1. Show the map \( \sigma \to f_\sigma \) gives an injective group homomorphism from \( S_n = \text{Perm}(v_1, \ldots, v_n) \) to \( U(n) \).

3. Suppose \( n, m \geq 1 \). The vector space \( \mathbb{C}^n \) has basis \( \{v_1, \ldots, v_n\} \) as above. Let \( \{w_1, \ldots, w_m\} \) be the corresponding basis for \( \mathbb{C}^m \). To each pair \((v_i, w_j)\) we define a symbol \( v_i \otimes w_j \) to stand for this pair. The tensor product \( \mathbb{C}^n \otimes \mathbb{C}^m \) is the vector space of all formal sums

\[
h = \sum_{1 \leq i \leq n, 1 \leq j \leq m} c_{i,j} (v_i \otimes w_j)
\]

in which the \( c_{i,j} \) are in \( \mathbb{C} \). This sum is equal to another one

\[
h' = \sum_{1 \leq i \leq n, 1 \leq j \leq m} c'_{i,j} (v_i \otimes w_j)
\]

if and only if \( c_{i,j} = c'_{i,j} \) for all \( i \) and \( j \). Define

\[
h \pm h' = \sum_{1 \leq i \leq n, 1 \leq j \leq m} (c_{i,j} \pm c'_{i,j}) (v_i \otimes w_j)
\]

and

\[
rh = \sum_{1 \leq i \leq n, 1 \leq j \leq m} rc_{i,j} (v_i \otimes w_j)
\]

for \( r \in \mathbb{C} \). We can define an complex inner product \( \langle , \rangle \) on \( \mathbb{C}^n \otimes \mathbb{C}^m \) by saying that

\[
\langle h, h' \rangle = \sum_{1 \leq i \leq n, 1 \leq j \leq m} c_{i,j} \overline{c'_{i,j}}.
\]

a. Suppose \( f : \mathbb{C}^n \to \mathbb{C}^n \) is a \( \mathbb{C} \)-linear transformation, and that \( f(v_i) = \sum_{k=1}^{n} a_{k,i}v_i \) for some constants \( a_{k,i} \in \mathbb{C} \). Show that there is a unique \( \mathbb{C} \)-linear transformation \( F : \mathbb{C}^n \otimes \mathbb{C}^m \to \mathbb{C}^n \otimes \mathbb{C}^m \) for which

\[
F(v_i \otimes w_j) = f(v_i) \otimes w_j = (\sum_{k=1}^{n} a_{k,i}v_k) \otimes w_j = \text{def} \sum_{k=1}^{n} a_{k,i}(v_k \otimes w_j)
\]

for all \( 1 \leq i \leq n \) and \( 1 \leq j \leq m \).

b. Suppose \( f \) is unitary with respect to the inner product \( \langle , \rangle \) on \( \mathbb{C}^n \) described above. Show that then \( F \) preserves the inner product \( \langle , \rangle \) in the sense that \( [F(h), F(h')] = [h, h'] \) for all \( h, h' \in \mathbb{C}^n \otimes \mathbb{C}^m \). This means that a unitary \( f \) defines an \( F \) which is unitary with respect to \( \langle , \rangle \).

Hints: First show that for all \( h, h_1, h', h'_1 \in \mathbb{C}^n \otimes \mathbb{C}^m \) one has

\[
[h + h_1, h' + h'_1] = [h, h'] + [h, h'_1] + [h_1, h'] + [h_1, h'_1]
\]

and

\[
[rh, h'] = r[h, h'] = [h, rh'] \quad \text{for} \quad r \in \mathbb{C}.
\]
Using this and the fact that $F$ is linear to show $F$ is unitary provided
$$[F(h), F(h')] = [h, h']$$
whenever $h = v_i \otimes w_j$ and $h' = v_{i'} \otimes w_{j'}$ for some pairs $(i, j)$ and $(i', j')$ of subscripts. Prove that in this case $[F(h), F(h')] = [h, h'] = 0$ if $j \neq j'$. Suppose now that $j = j'$. Then show that $[F(h), F(h')] = (f(v_i), f(v_{i'}))$ when $h = v_i \otimes w_j$ and $h' = v_i \otimes w_j$, where $(\cdot, \cdot)$ is the complex inner product on $\mathbb{C}^n$.

**An Example:** Suppose $n = 2$ and $m = 2$. Then $\mathbb{C}^n \otimes \mathbb{C}^m = \mathbb{C}^2 \otimes \mathbb{C}^2$ has basis
$$\{v_1 \otimes w_1, v_2 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_2\}.$$
If $\theta$ is a real number, we can define a $\mathbb{C}$-linear transformation
$$f : \mathbb{C}^n \to \mathbb{C}^n$$
by saying that
$$f(v_1) = \cos(\theta) \cdot v_1 + \sin(\theta) \cdot v_2$$
$$f(v_2) = -\sin(\theta) \cdot v_1 + \cos(\theta) \cdot v_2$$
$$f(a_1 v_1 + a_2 v_2) = a_1 f(v_1) + a_2 f(v_2).$$
To check that this is unitary, we use the usual complex inner product on $\mathbb{C}^n$ given by
$$\langle a_1 v_1 + a_2 v_2, b_1 v_1 + b_2 v_2 \rangle = a_1 \overline{b_1} + a_2 \overline{b_2}.$$
Notice that this inner product has the properties that
$$\langle v_1, v_1 \rangle = \langle v_2, v_2 \rangle = 1 \quad \text{and} \quad \langle v_1, v_2 \rangle = \langle v_2, v_1 \rangle = 0.$$  
To show $f$ is unitary, we have to prove that for all $z, z' \in \mathbb{C}^2$ one has
$$\langle f(z), f(z') \rangle = \langle z, z' \rangle. \quad (1.2)$$
Since $f(z)$ is linear in $z$, and the inner product $\langle z, z' \rangle$ is linear in each of the variables $z$ and $z'$ separately, its enough to check (1.3) when $z = v_i$ and $z' = v_j$ for some $i$ and $j$. One can check this case using (1.2) and the fact that $\cos(\theta)^2 + \sin(\theta)^2 = 1$. Now the transformation
$$F : \mathbb{C}^n \otimes \mathbb{C}^m \to \mathbb{C}^n \otimes \mathbb{C}^m$$
is the one which has
$$F(v_1 \otimes w_j) = (\cos(\theta) \cdot v_1 + \sin(\theta) \cdot v_2) \otimes w_j = \cos(\theta) \cdot (v_1 \otimes w_j) + \sin(\theta) \cdot (v_2 \otimes w_j)$$
and
$$F(v_2 \otimes w_j) = (-\sin(\theta) \cdot v_1 + \cos(\theta) \cdot v_2) \otimes w_j = -\sin(\theta) \cdot (v_1 \otimes w_j) + \cos(\theta) \cdot (v_2 \otimes w_j)$$
for $j = 1, 2$. 


2. Fourier analysis on finite abelian groups

These problems are relevant to the project about multiplying numbers using the discrete Fourier transform. Suppose $G$ is a finite abelian group. The character group $\hat{G}$ is the set whose elements are all group homomorphisms $f : G \to \mathbb{C}^*$, where $\mathbb{C}^* = \mathbb{C} - \{0\}$ is the multiplicative group of all non-zero complex numbers. We will focus on the case in which $n \geq 1$ is an integer and $G = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ is the cyclic group of order $n$ generated by the $n^{th}$ root of unity $\omega = e^{2\pi i/n}$.

4. Show that for each integer $m$ there is an element $e_m \in \hat{G}$ defined by $e_m(\omega^j) = \omega^{jm}$ for all integers $j$. Show that every element of $\hat{G}$ equals $e_m$ for some $m$, and that $e_m = e_{m'}$ if and only if $m \equiv m' \mod n$. Finally, show that the map $\mathbb{Z}/n \to \hat{G}$ defined by $[m] \to e_m$ is an isomorphism of groups, where $[m] = m \mod n$.

5. Let $C(G)$ be the set of all functions $f : G \to \mathbb{C}$. Define an inner product $\langle \ , \ \rangle : C(G) \times C(G) \to \mathbb{C}$ by $\langle f, h \rangle = \sum_{g \in G} f(g)\overline{h(g)}$.

The Fourier transform $\hat{f} : \hat{G} \to \mathbb{C}$ of a function $f : G \to \mathbb{C}$ is defined by $\hat{f}(e_m) = \frac{1}{n} \langle f, e_m \rangle$ for $m = 0, \ldots, n-1$, where $\hat{G} = \{e_0, e_1, \ldots, e_{m-1}\}$ by problem 4. Show that each function $f \in C(G)$ can be written as the particular linear combination $f = \sum_{m=0}^{n-1} \hat{f}(e_m) \cdot e_m$ of the functions $e_m$.

**Hints:** You are trying to show that for each element $\omega^j$ of $G$, the value $f(\omega^j)$ of $f$ at $\omega^j$ equals the sum

$$\sum_{m=0}^{n-1} \hat{f}(e_m) \cdot e_m(\omega^j) = \sum_{m=0}^{n-1} \left( \frac{1}{n} \sum_{\ell=0}^{n-1} f(\omega^\ell) \overline{e_m(\omega^\ell)} \right) \cdot e_m(\omega^j).$$

To simplify the result of writing this out, first prove using geometric series that

$$\sum_{m=0}^{n-1} \omega^{m(j-\ell)} = 0 \quad \text{if} \quad 0 \leq j, \ell \leq n-1 \quad \text{and} \quad i \neq j$$

and

$$\sum_{m=0}^{n-1} \omega^{m(j-\ell)} = n \quad \text{if} \quad j = \ell$$