Rank of a linear transformation.

Let G be a finite abelian group. Let N be the exponent of G and n be the order of G. A function \( f : G \to \mathbb{C} - \{0\} \) is called a character of G if it is a group homomorphism. If f is a character of a finite group, then each function value is a root of unity since all elements of a finite group have finite order. Notice that if \( g \in G \), for any character \( \chi \) of G we have

\[
\chi(g)^N = \chi(g^N) = \chi(e) = 1,
\]

so the values of \( \chi \) lie among the Nth roots of unity. Characters on finite abelian groups were first studied in number theory, since number theory is a source of many interesting finite abelian groups.

A finite abelian group of order n has exactly n distinct characters which are denoted by \( f_1, f_2, ..., f_n \). \( f_1 \) is the trivial representation, that is, \( f_1(g) = 1 \) for all \( g \in G \). It is called the principal character of G; the others are called nonprincipal characters, and \( f_i(g) \neq 1 \) for some \( g \in G \). The set of characters of G form an abelian group under multiplication called the character group.

Let \( \hat{G} \) denote the character group of G. Fix a primitive N-th root \( z \) of unity. Then, for each \( g \in G \) and \( \chi \in \hat{G} \), there is a unique integer \( 1 \leq r \leq N \) such that \( \chi(g) = z^r \). We therefore obtain a pairing

\[
\langle \cdot, \cdot \rangle : G \times \hat{G} \to \mathbb{Q}/\mathbb{Z}
\]

defined by

\[
\langle g, \chi \rangle = \left\{ \frac{r}{N} \right\}
\]

where \( \{r/N\} \) denotes the fractional part of \( r/N \). We may extend the previous pairing to

\[
\langle \cdot, \cdot \rangle : \mathbb{Q}[G] \times \mathbb{Q}[\hat{G}] \to \mathbb{Q}
\]

via linearity in the obvious way

\[
\left\langle \sum_{g \in G} c_g \cdot g, \sum_{\chi \in H} c_\chi \cdot \chi \right\rangle = \sum_{g \in G} \sum_{\chi \in H} c_g \cdot c_\chi \langle g, \chi \rangle.
\]

Here \( \mathbb{Q}[G] \) and \( \mathbb{Q}[\hat{G}] \) are group rings. In particular, both \( \mathbb{Q}[G] \) and \( \mathbb{Q}[\hat{G}] \) are \( \mathbb{Q} \)-vector spaces of dimension \( |G| = |\hat{G}| \).

Let us now define a map \( f : \mathbb{Q}[\hat{G}] \to \mathbb{Q}[G] \) as follows:

\[
f(a) = \sum_{g \in G} \langle g, a \rangle g, \quad \text{for any } a \in \mathbb{Q}[\hat{G}].
\]
We may view $f$ as a linear map between two vector spaces of dimension $|G|$. An important question in some applications in number theory is: what can we say about the kernel of $f$?

The REU students will approach this question by studying the rank of $f$ and determining the dimension of the kernel of $f$. We will work first with finite cyclic groups and, if time permits, we will also consider the general case.