Pespectives in Mathematical Sciences

Due: Tuesday, June 30, 2020, on NUCT.

Problem 1. Let $\varphi(n)$ be Euler's phi-function that counts the number of integers $0 \leqslant k < n$ such that k and n are relatively prime. Show that

$$\sum_{d\,|n} \varphi(d) = n.$$

Here the sum ranges over all positive integers d that divide n.

The formula in Problem 1 is used to determine the structure of the rational group ring $\mathbb{Q}[C_n]$ of the cyclic group C_n of order n. As we did for $\mathbb{C}[C_n]$ and $\mathbb{R}[C_n]$, we first choose a generator $g \in C_n$ and a primitive nth root of unity $\zeta_n \in \mathbb{C}$ and then, for all $0 \leq k < n$, define $\mathbb{Q}(\zeta_n^k) \subset \mathbb{C}$ to be the sub-$\mathbb{Q}$-vector space spanned by the family $(\zeta_n^{ki})_{0\leq i<n}$ and give it the left $\mathbb{Q}[C_n]$-module structure defined by

$$(\sum_{i=0}^{n-1} a_i g^i) \cdot z = \sum_{i=0}^{n-1} a_i \zeta_n^{ki} z.$$

The left $\mathbb{Q}[C_n]$-module $\mathbb{Q}(\zeta_n^k)$ is simple, since given any $z, z' \in \mathbb{Q}(\zeta_n^k)$, there exists an element $\omega \in \mathbb{Q}[C_n]$ with $\omega \cdot z = z'$. Suppose that

$$\{\zeta_n^{ki} \mid 0 \leqslant i < n\} = \{\zeta_n^{li} \mid 0 \leqslant i < n\} \subset \mathbb{C}.$$

Then we may define a $\mathbb{Q}[C_n]$-linear isomorphism

$$f\colon \mathbb{Q}(\zeta_n^k) \to \mathbb{Q}(\zeta_n^l)$$

to be the unique $\mathbb{Q}$-linear map that takes ζ_n^{ki} to ζ_n^{li}, for all $0 \leqslant i < n$. Moreover, if the set $\{\zeta_n^{ki} \mid 0 \leqslant i < n\}$ has d elements, then d divides n and

$$\{\zeta_n^{ki} \mid 0 \leqslant i < n\} = \{\zeta_d^{i} \mid 0 \leqslant i < d\}$$

with $\zeta_d \in \mathbb{C}$ a primitive dth root of unity. So if we let $\mathbb{Q}(\zeta_d) \subset \mathbb{C}$ be the sub-$\mathbb{Q}$-vector space spanned by $(\zeta_d^i)_{0\leqslant i<d}$ and give it the left $\mathbb{Q}[C_n]$-module defined by

$$(\sum_{i=0}^{n-1} z_i g^i) \cdot z = \sum_{i=0}^{n-1} a_i \zeta_d^i z,$$

then there is a $\mathbb{Q}[C_n]$-linear isomorphism

$$f\colon \mathbb{Q}(\zeta_d) \to \mathbb{Q}(\zeta_n^k)$$

given by the unique $\mathbb{Q}$-linear map that takes ζ_d^i to ζ_n^{ki}. One may show, following Gauss, that the dimension of $\mathbb{Q}(\zeta_d)$ as a $\mathbb{Q}$-vector space is equal to the number $\varphi(d)$ of integers $0 \leq l < d$ such that l and d are relatively prime. So the formula

$$\sum_{d|n} \varphi(d) = n$$

proved in Problem 1 and Theorem 3.5 (i) shows that the simple left $\mathbb{Q}[C_n]$-modules $\mathbb{Q}(\zeta_d)$, where d varies over positive integers that divide n, represent all isomorphism classes of simple left $\mathbb{Q}[C_n]$-modules. Therefore, as a left $\mathbb{Q}[C_n]$-module,

$$\mathbb{Q}[C_n] = \bigoplus_{d|n} \mathbb{Q}(\zeta_d).$$

Finally, we note that $\mathbb{Q}(\zeta_d) \subset \mathbb{C}$ is a subfield, the dth cyclotomic field over $\mathbb{Q}$, and that the endomorphism ring $\mathrm{End}_{\mathbb{Q}[C_n]}(\mathbb{Q}(\zeta_d))^{\mathrm{op}}$ is isomorphic to the field $\mathbb{Q}(\zeta_d)$ for every divisor d of n.

If $n = p$ is a prime number, then we have

$$\mathbb{Q}[C_p] = \mathbb{Q}(\zeta_1) \oplus \mathbb{Q}(\zeta_p),$$

where $\mathbb{Q}(\zeta_1) = \mathbb{Q}$ and $\mathbb{Q}(\zeta_p)$ have dimension 1 and $p-1$, respectively, as $\mathbb{Q}$-vector spaces.