138. An Analytical Proof of the Fundamental Theorem on Finite Abelian Groups

By Tamio ONO

Mathematical Institute, Nagoya University, Nagoya, Japan

(Comm. by Z. SUETUNA, M.J.A., Dec. 12, 1957)

The aim of this note is to give an analytical proof of the following fundamental theorem on finite abelian groups.

Theorem. For any finite abelian group $\mathfrak{G}$, there exists a basis $(t_\nu;\ 1\leqq\nu\leqq m)$ such that for any element t of $\mathfrak{G}$, we have one and only one representation $t=t_1^{r_1}t_2^{r_2}\cdots t_m^{r_m}$, where $1\leqq r_\nu\leqq n_\nu$ $(1\leqq\nu\leqq m)$, n_ν being the order of t_ν.

Proof. Let $\mathfrak{G}$ be a finite abelian group of order n and $\mathfrak{H}$ its group-ring over the complex number field C. The ring $\mathfrak{H}$ may constitute an (n-dimensional) Hilbert space with the inner product $(a, b)=\sum_{s\in\mathfrak{G}}\alpha(s)\overline{\beta(s)}$ $(\overline{\beta(s)}=$the complex conjugate number of $\beta(s))$, where $a=\sum_{s\in\mathfrak{G}}\alpha(s)s$ and $b=\sum_{s\in\mathfrak{G}}\beta(s)s$. Let U_t be a unitary operator defined by $U_ta=\sum_{s\in\mathfrak{G}}\alpha(t^{-1}s)s$ on $\mathfrak{H}$ and $\mathfrak{R}$ be the C^*-algebra generated by $(U_t;\ t\in\mathfrak{G})$. The algebra $\mathfrak{R}$ is homomorphic to $C(\Omega)$, the totality of the complex-valued continuous functions on Ω, where Ω is the character group of $\mathfrak{G}$, which consists of finite points $\{\lambda_\nu;\ 1\leqq\nu\leqq m\}$. In fact, for any element t of $\mathfrak{G}$, it follows from $t^n=1$ that a spectrum of U_t is an n-th root of 1. Hence, the number of characters of $\mathfrak{G}$ is at most n^n. Let $A\to\hat{A}$ be the canonical homomorphism from $\mathfrak{R}$ into $C(\Omega)$. Then, $t\to\hat{U}_t$ $(t\in\mathfrak{G})$ is an isomorphism. In fact, if $t\neq 1$, then U_t has at least one spectrum ζ, where ζ is a primitive r-th root of 1 and r is the order of t. Hence, there exists a maximal ideal $\mathfrak{M}$ of $\mathfrak{R}$ containing $U_t-\zeta$, where $\mathfrak{R}/\mathfrak{M}$ is a cyclotomic field over C, that is $\mathfrak{R}/\mathfrak{M}=C$. Therefore, there exists a character λ of $\mathfrak{G}$ with $\lambda(t)\neq 1$, where λ is the canonical homomorphism from $\mathfrak{R}$ onto $\mathfrak{R}/\mathfrak{M}$. Hence, we may assume without loss of generality that $t=\hat{U}_t(t\in\mathfrak{G})$. Let C_ν be $(t(\lambda_{\nu+1});\ t\in\mathfrak{G},\ t(\lambda_1)=1,\cdots,t(\lambda_\nu)=1)$, which is a finite cyclic group in C, because a subgroup of a cyclic group is again cyclic. Let $\mathfrak{G}_\nu$ be a subgroup of $\mathfrak{G}$, which consists of elements t's of $\mathfrak{G}$ with $t(\lambda_1)=\cdots=t(\lambda_\nu)=1$, and t_ν be an element of $\mathfrak{G}$, whose value at $\lambda_{\nu+1}$ is a generator η_ν of C_ν. In order to prove that, for any element t of $\mathfrak{G}$, there exists the representation stated in the theorem, we need only to prove that $t\in\mathfrak{G}_\nu$ implies $tt_{\nu+1}^{-r_{\nu+1}}\in\mathfrak{G}_{\nu+1}$ for one and only one natural number $r_{\nu+1}$ between 1 and $n_{\nu+1}$. And the number $r_{\nu+1}$ defined by $t(\lambda_{\nu+1})=\eta_{\nu+1}^{r_{\nu+1}}$ satisfies this condition.