COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 33, No. 1, 1984

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

The Relationship between Arithmetics and Infinite Series of Indecomposable Integral Representations of Finite Groups

by

Makoto ISHIBASHI

(Received April 2, 1983)

§ 1. Introduction

The aim of this paper is to clarify some problems of finite groups in the case of infinite integral representation type, and to construct explicitly infinite series of indecomposable integral representations of finite abelian p-groups. These problems are closely related to unsolved arithmetical problems.

One of the basic problems in the theory of integral representations is to know all the indecomposable representations. Even if it should be settled, we still have to find the full set of direct sum invariants, since the Krull-Schmidt-Azumaya theorem cannot hold in our situation.

The first treatment of integral representations of finite groups was due to F. E. Diederichsen (in 1938) in the case of cyclic group of prime order. The necessary and sufficient conditions for a finite group to have infinitely many indecomposable integral representations has been established (in 1962) by several mathematicians (Berman, Heller-Reiner, Jones, Dade).

The development of integral representation theory has been much influenced by algebraic number theory. In 1978, Reiner almost completely settled the integral representation problem of cyclic group of prime power order p^2. However, it has not been accomplished how to determine explicitly all the indecomposable integral representations of non-cyclic groups with infinite integral representation type (except for the Klein's four group). It should be noted that Berman and Gudivok (in 1964) have established a method, which is used to construct families of integral representations parametrized by several matrices (parameter matrices) and which can be applicable to the construction of indecomposable integral representations of finite p-groups.

The second section is devoted to the notations needed in the rest of this paper, and to a notice in the general integral representation theory of orders. The Berman-Gudivok theory will be described in § 3. Berman-Gudivok used the Jordan normal blocks as parameter matrices for the construction of infinite series of indecomposable integral representations of an abelian group of type (p, p).

The main motivation of this paper is to know another explicit informations of infinite number of indecomposable integral representations.

The fourth section is the heart of the present paper, where we investigate a relation between sizes of parameter matrices and indecomposability of integral representations. We also construct infinite series of indecomposable integral representations, and show how to relate the problem to arithmetical problems (for example Artin's conjecture on primitive roots).

This paper contains the major part of the author's thesis (Rikkyo University, 1983). I would like to express my gratitude to Professor Kinya Honda for his careful reading and guidance during the preparation of this paper. I would also like to express my sincerely thanks to Professor Klaus W. Roggenkamp for informing me of some related papers, and for pointing out an error in §4 in the manuscript of this paper.

§2. Basic preliminaries

Let us recall the basic definitions and notations in the theory of integral representations of orders. Let R be a Dedekind domain whose quotient field K is an algebraic number field, A be a finite-dimensional K-algebra, S be an R-order in A, ${}_SL$ be the category of left S-lattices (i.e. R-torsionfree finitely generated S-modules), and $n(S)$ be the number of isomorphism classes of indecomposable left S-lattices.

DEFINITION 2.1. An R-order S is said to be of finite representation type (resp. infinite representation type) if $n(S)<+\infty$ (resp. $n(S)=+\infty$).

Let P be a prime ideal in R, K_P be the completion field of K at P, R_P be the valuation ring of K_P, and S_P be $R_P\otimes_R S$. Let H_p denote a Sylow p-subgroup of a finite group G. For an object M in the category ${}_SL$, let M_P be the S_P-lattice $S_P\otimes_S M$ ($\cong R_P\otimes_R M$) in ${}_{S_P}L$.

Then the following propositions and theorems are well-known.

PROPOSITION 2.2. *$n(S)<+\infty$ if and only if $n(S_P)<+\infty$ for all prime ideal P in R.*

PROPOSITION 2.3. *Let $P\ni p$ and $p\,|\,|G|$. Then $n((RG)_P)<+\infty$ if and only if $n((RH_p)_P)<+\infty$.*

PROPOSITION 2.4. (i) *If H_p is non-cyclic or $|H_p|\geqq p^3$, then $n((RH_p)_P)=+\infty$.*
(ii) *If H_p is cyclic and $|H_p|\leqq p^2$, then $n((ZH_p)_P)<+\infty$.*

THEOREM 2.5. *$n(ZG)<+\infty$ if and only if H_p is cyclic and $|H_p|\leqq p^2$ for every rational prime divisor p of $|G|$.*

The above Proposition 2.4 (ii), Theorem 2.5 were generalized by Dade, Jacobinski, Drozd-Roiter, and Roggenkamp.

The crucial step of the proof of the necessity in this theorem is the construction of infinite series of indecomposable integral representations. Furthermore, the set of degrees of the above infinitely many indecomposable integral representations is

unbounded in the case of infinite integral representation type.

The complete classification (i.e. complete description of the indecomposable representation modules up to isomorphism, and finding the full set of direct sum invariants) of integral representations of a finite group which has infinite integral representation type, has been considered to be too complicated to treat. In the case of infinite integral representation type, we shall distinguish the representation types into tamely and wildly.

DEFINITION 2.6. (cf. [3]) An R-order S is said to be of wildly representation type if there exist a full subcategory U of ${}_SL$, a field F, and a representation equivalent (i.e. full, dence, isomorphism-reflecting additive) functor T such that $T\colon U\to {}_{F[X,Y]}M$ ($F[X, Y]$ is the polynomial ring of two variables X, Y over F, and ${}_{F[X,Y]}M$ is the category of finitely generated $F[X, Y]$-modules.) Otherwise, S is said to be of tamely representation type.

In the case of wildly representation type, it seems to be quite hopeless to classify completely the indecomposable representations.

An integral R-matrix representation of an R-order S is a ring-homomorphism from S into $M_m(R)$ (the ring of full set of (m, m)-matrices with entries in R). For two objects A, B in ${}_SL$, let $r_1\colon S\to \mathrm{End}_R(A)$ and $r_2\colon S\to \mathrm{End}_R(B)$ be integral R-linear representation of S afforded by A and B, respectively. It is said that r_1 is R-equivalent to r_2 if there exists an R-isomorphism j from A onto B such that $r_1(x)=j^{-1}r_2(x)j$ for all $x\in S$.

The difficulty of integral representation theory arises from the fact that the R-order S is not always of finite representation type and several useful theorems in the ring theory (for example, the Krull-Schmidt-Azumaya theorem) do not hold. However, some of these hold in the case of local integral representations, and hence we can treat some Z_p-representations. Suppose that the class number of R is equal to 1 and $\mathrm{rank}_R A=m$. Then, by the well-known structure theorem of finitely generated torsionfree modules over a Dedekind domain, we have that $M_m(R)\cong \mathrm{End}_R(A)$. In this case, integral matrix representations coincide with integral linear representations.

Let a be a non-square natural number, and P_a be the set

$$\{q;\ \text{rational prime} \mid (Z/qZ)^*=\langle a \bmod q\rangle\}\,.$$

Let p be an odd prime, and P'_p be the set

$$\{q;\ \text{odd prime} \mid q \,||\, p^{q-1}-1,\ (Z/qZ)^*=\langle p \bmod q\rangle\}\,.$$

Remark. If $m \mid n$ (m divides n) and $m^2 \nmid n$ (m^2 does not divide n), then we denote $m\| n$.

In the rest of this paper, we assume the following conditions;

(i) The set P_a is an infinite set.

(ii) The set P'_p is a non-empty set.

Remark. The condition (i) is called Artin's conjecture on primitive roots.

Let C_p be a cyclic group of prime order p, and h be the class number of the cyclotomic field $Q(\zeta_p)$ (ζ_p; a primitive p-th root of unity in the complex number field). Diederichsen began (in 1938) to study systematically the theory of integral representations. His result is that $n(ZC_p)=2h+1$. Furthermore, he tried to construct infinite series of indecomposable integral representations of finite group, but didn't succeeded. In 1933, Latimer-MacDuffee had established a relation between integral matrices and ideals in an order. Let $W(X)$ be a fixed monic polynomial of degree n in $Z[X]$ such that $W(0)\neq 0$, and $W_A(X)$ denotes the minimal polynomial of a matrix A. Their result is that there is a one-to-one correspondence between the Z-similarity classes of (n, n)-matrices A with entries in Z such that $W_A(X)=W(X)$, and the classes of nonsingular ideals in the ring $Z[X]/(W(X))$.

Throughout in this paper, let $\Phi_m(X)$ denote the m-th cyclotomic polynomial ($\deg \Phi_m(X)=\varphi(m)$, where φ is the Euler function), and $(\frac{\cdot}{p})$ denote the Legendre symbol.

§ 3. The method of constructions by Berman-Gudivok

Berman and Gudivok [1] has established a framework of the indecomposable Z_p-matrix representations of finite p-groups. Let $M_{n_1,n_2}(R)=M(n_1, n_2; R)$ denote the full set of (n_1, n_2)-matrices with entries in a ring R. In the case of $n_1=n_2=n$, we briefly write $M_n(R)$, and let E_n be the unit matrix in $M_n(R)$. In the rest of this section, we fix a rational prime number p. For brevity, let $\zeta_r(=\zeta_{p^r})$ be a primitive p^r-th root of unity in C (the field of complex numbers). Then $\mathrm{End}_{Z_p}(Z_p[\zeta_r])\cong M_{\varphi(p^r)}(Z_p)$ with respect to the fixed basis $\{\zeta_r^j;\ 0\leqq j\leqq \varphi(p^r)-1\}$ of $Z_p[\zeta_r]$, where $\varphi(p^r)=p^{r-1}(p-1)$. Thus, there corresponds the matrix

$$\tilde{\zeta}_r=\begin{pmatrix} 0 & 1 & & & & & \\ & 0 & 1 & & & 0 & \\ & & \cdot & \cdot & & & \\ & 0 & & \cdot & \cdot & & \\ & & & & \cdot & \cdot & \\ & & & & & 0 & 1 \\ -1 & * & \cdot & \cdot & \cdot & * & * \end{pmatrix}$$

to the endomorphism of left multiplication by ζ_r of $Z_p[\zeta_r]$. Furthermore, let $\tilde{\zeta}_r^{(n)}$ be the Kronecker product

$$\tilde{\zeta}_r\otimes E_n=\begin{pmatrix} \tilde{\zeta}_r & & 0 \\ & \ddots & \\ 0 & & \tilde{\zeta}_r \end{pmatrix}\in M_{n\varphi(p^r)}(Z_p)\,.$$

Let $\langle c\rangle$ be

$$\begin{pmatrix} 0 & & 0 & a_0 \\ \cdot & & \cdot & \\ \cdot & \cdots & \cdot & a_1 \\ \cdot & & \cdot & \vdots \\ 0 & & 0 & a_{\varphi(p^r)-1} \end{pmatrix} \in N(\varphi(p^r), s; Z_p),$$

where $c=\sum_{j=0}^{\varphi(p^r)-1} a_j\zeta_r^j \in Z_p[\zeta_r]$ $(r, s\in N)$.

We choose suitable $s(\in N)$ to substitute each $\langle c\rangle$ in a block of matrix. For every $B=(c_{ij})\in M(n_1, n_2; Z_p[\zeta_r])$, let $\langle B\rangle$ be $(\langle c_{ij}\rangle)\in M(n_1\varphi(p^r), n_2 s; Z_p)$. The matrix $\langle B\rangle$ is called the blowing up of B.

Let $C_{p^t}=(a)$ be a cyclic group of order $p^t(t\geqq 3)$.

THEOREM 3.1 (Berman-Gudivok Theorem 3.1 in [1]). *Let m_1, m_2, m_3, i, j, k be rational integers such that $1\leqq m_1,\ m_2,\ m_3\leqq t,\ m_1\neq m_2,\ m_1\neq m_3,\ m_2\neq m_3,\ 0\leqq i<\varphi(p^{m_2}),\ 0\leqq j<\varphi(p^{m_3}),\ 0\leqq k<i,\ 0\leqq k<j$, and let r be $\min\{\varphi(p^{m_2})-i,\ \varphi(p^{m_3})-j, i-k, j-k\}$. In the case of $r=\varphi(p^{m_2})-i$ or $r=j-k$, assume that $\varphi(p^{m_2})\neq i+j-k$. For a matrix B (parameter matrix) in $GL_n(Z_p[\zeta_{m_1}])$, let $W_n(B)(a)$ be*

$$\begin{pmatrix} \zeta_{m_1}^{(n)} & \langle(1-\zeta_{m_1})^i E_n\rangle & \langle(1-\zeta_{m_1})^k B\rangle \\ 0 & \zeta_{m_2}^{(n)} & \langle(1-\zeta_{m_2})^j E_n\rangle \\ 0 & 0 & \zeta_{m_3}^{(n)} \end{pmatrix}.$$

Then $W_n(B)$ is a Z_p-representation of C_{p^t}, and $W_n(B)$ is Z_p-equivalent to $W_n(B')$ if and only if B is similar mod $(1-\zeta_{m_1})^r$ *to B' in $GL_n(Z_p[\zeta_{m_1}])$. Furthermore, $W_n(B)$ is Z_p-indecomposable if and only if B is indecomposable* mod $(1-\zeta_{m_1})^r$.

THEOREM 3.2 (A generalization of Berman-Gudivok Theorem 3.2 in [1]). *Let a be a generator of the cyclic group $C_p r$. Let d be $r-3$ $(5\leqq r\in N)$ and $W_n(B_1, \cdots, B_d)(a)$ be the following matrix;*

$$\begin{pmatrix} \zeta_{m_1}^{(n)} & 0 & \langle E_n\rangle & \langle(1-\zeta_{m_1})^{j_1}B_1\rangle & \cdots & \langle(1-\zeta_{m_{d-1}})^{j_{d-1}}B_{d-1}\rangle & \langle B_d\rangle \\ & \zeta_{m_2}^{(n)} & \langle E_n\rangle & \langle E_n\rangle & \cdots & \langle E_n\rangle & \langle E_n\rangle \\ & & \zeta_{m_3}^{(n)} & & 0 & & \\ & & & & \cdots & & \\ & & 0 & & & \zeta_{m_{r-1}}^{(n)} & \\ & & & & & & E_n \end{pmatrix},$$

where $r\geqq m_1>m_2>\cdots>m_{r-1}>0, j_k=\varphi(p^{mk+3})-1$ $(1\leqq k\leqq d-1=r-4)$ and $B_1, \cdots, B_d$ are parameter matrices in $GL_n(Z_p[\zeta_{m_1}])$. Then $W_n(B_1, \cdots, B_d)$ is a Z_p-representation of C_{p^r}, and $W_n(B_1, \cdots, B_d)$ is Z_p-equivalent to $W_n(B_1', \cdots, B_d')$ if and only if there

exists H *in* $GL_n(Z_p[\zeta_{m_1}])$ *such that* $H^{-1}B_vH \equiv B'_v \pmod{(1-\zeta_{m_1})}$ $(1 \leqq v \leqq d)$. *Furthermore* $W_n(B_1, \cdots, B_d)$ *is* Z_p*-decomposable if and only if there exists a suitable invertible matrix* H *in* $GL_n(Z_p[\zeta_{m_1}])$ *such that*

$$H^{-1}B_vH \equiv \begin{pmatrix} S_v & 0 \\ 0 & L_v \end{pmatrix} \pmod{(1-\zeta_{m_1})} \qquad (1 \leqq v \leqq d),$$

where the sizes of square matrices $S_1, \cdots, S_d$ *(resp.* $L_1, \cdots, L_d$*) are equal to each other.*

Proof. To begin with, let us notice that there exists a one-to-one correspondence f such that

$$\begin{array}{ccccc} f(B)=\tilde{B} & \in & R_1 & \subset & M_{n\varphi(p^{m_1})}(Z_p) \\ \uparrow & & f\uparrow\wr & & \wr\| \\ B & \in M_n(Z_p[\zeta_{m_1}]) & \cong & & \mathrm{End}_{Z_p}(M) \\ & & & & \cup \\ & & & & \mathrm{End}_{Z_p[\zeta_{m_1}]}(M) \end{array},$$

where $R_1 = \{X \in M_{n\varphi(m_1)}(Z_p) \mid X\tilde{\zeta}^{(n)}_{m_1} = \tilde{\zeta}^{(n)}_{m_1}X\}$ and M is a free $Z_p[\zeta_{m_1}]$-module of rank n.

Without loss of generality we may assume that $\zeta_m^p = \zeta_{m-1}$ $(m=1, 2, \cdots)$. Since $\zeta'_j = \zeta_i/\zeta_j = \zeta_j^{p^{j-i}-1}$ is a primitive p^j-th root of unity $(\zeta_i = \zeta_j^{p^{j-i}}$, where $0 \leqq i \leqq j \in Z)$ and $\zeta_j^{p-1}\{(\zeta_i/\zeta_j)^{p-1} + \cdots + (\zeta_i/\zeta_j) + 1\} = \zeta_j^{p-1}\Phi_p(\zeta'_j)$, we have

$$\{W_n(B_1, \cdots, B_d(a)\}^p$$

$$= \begin{pmatrix} \tilde{\zeta}^{(n\varphi(p))}_{m_1-1} & 0 & \langle \Phi_p(\zeta'_{m_1})\zeta_{m_1}^{p-1}E_n\rangle & \cdots & \langle \Phi_p(\zeta'_{m_1})\zeta_{m_1}^{p-1}B_d\rangle \\ & \tilde{\zeta}^{(n\varphi(p))}_{m_2-1} & \langle \Phi_p(\zeta'_{m_2})\zeta_{m_2}^{p-1}E_n\rangle & \cdots & \langle \Phi_p(\zeta'_{m_2})\zeta_{m_2}^{p-1}E_n\rangle \\ & & \tilde{\zeta}^{(n\varphi(p))}_{m_3-1} & & 0 \\ & & & \cdots & \\ & 0 & & \tilde{\zeta}^{(n\varphi(p))}_{m_{r-1}-1} & \\ & & & & E_n \end{pmatrix}.$$

Thus the (1,3)-block of the matrix $\{W_n(B_1, \cdots, B_d)(a)\}^{p^{m_1}}$ is

$$\left\langle \Phi_p(\zeta'_1)\Phi_p(\zeta'_2)\cdots\Phi_p(\zeta'_{m_1}) \prod_{j=1}^{m} \zeta_j^{p-1} E_n \right\rangle = 0,$$

because of $\Phi_p(\zeta'_1)=0$. Using the similar method, we see easily that all the blocks except the diagonal blocks of $\{W_n(B_1, \cdots, B_d)(a)\}^{p^r}$ $(r \geqq m_1)$ are zero matrices with suitable sizes, and $\{W_n(B_1, \cdots, B_d)(a)\}^{p^r}$ is a unit matrix. Therefore $W_n(B_1, \cdots, B_d)$ is a Z_p-representation of C_{p^r}. Suppose that $C^{-1}W_n(B_1, \cdots, B_d)(a)\ C = W_n(B'_1, \cdots, B'_d)(a)$, where

$$C = \begin{pmatrix} \tilde{H}_1 & & * \\ & \ddots & \\ 0 & & \tilde{H}_r \end{pmatrix}.$$

By the lemmas with respect to the basis changes of Berman-Gudivok [1], we can take the matrix $W_n(B_1, \cdots, B_d)(a)$ to the following form W';

$$\begin{pmatrix} \zeta_{m_1}^{(n)} & 0 & \langle H_1^{-1}H_3\rangle & \langle (1-\zeta_{m_1})^{j_1}H_1^{-1}B_1H_4\rangle & \cdots & \langle (1-\zeta_{m_1})^{j_{d-1}}H_1^{-1}B_{d-1}H_{r-1}\rangle & \langle H_1^{-1}B_dH_r\rangle \\ & \zeta_{m_2}^{(n)} & \langle H_2^{-1}H_3\rangle & \langle H_2^{-1}H_4\rangle & \cdots & \langle H_2^{-1}H_{r-1}\rangle & \langle H_2^{-1}H_r\rangle \\ & & \zeta_{m_3}^{(n)} & & & & \\ & & & \ddots & & 0 & \\ & & 0 & & & & \\ & & & & & \zeta_{m_{r-1}}^{(n)} & \\ & & & & & & E_n \end{pmatrix}.$$

Now

$$\begin{pmatrix} E_{n\varphi(p^{m_1})} & & & \\ & \ddots & & * \\ & & E_{n\varphi(p^{m_{r-1}})} & \\ 0 & & & E_n \end{pmatrix}^{-1} W' \begin{pmatrix} E_{n\varphi(p^{m_1})} & & & \\ & \ddots & & * \\ & & E_{n\varphi(p^{m_{r-1}})} & \\ 0 & & & E_n \end{pmatrix} = W_n(B_1', \cdots, B_d'),$$

we have

$$H_1^{-1}H_3 \equiv E_n \pmod{(1-\zeta_{m_1})}, \quad H_2^{-1}H_k \equiv E_n \pmod{(1-\zeta_{m_2})} \quad (3 \leqq k \leqq r),$$

$$(1-\zeta_{m_1})^{j_k}H_1^{-1}B_kH_{k+3} \equiv (1-\zeta_{m_1})^{j_k}B_k' \pmod{(1-\zeta_{m_1})^{\varphi(p^{m_{k+3}})}} \quad (1 \leqq k \leqq d-1,\ j_k+1=\varphi(p^{m_{k+3}})),$$

$$H_1^{-1}B_dH_{d+3} \equiv E_n \pmod{(1-\zeta_{m_1})}.$$

Hence $H_1 \equiv H_2 \equiv \cdots \equiv H_r \pmod{(1-\zeta_{m_1})}$. Consequently,

$$(*) \qquad H_1^{-1}B_kH_1 = B_k' \pmod{(1-\zeta_{m_1})} \qquad (1 \leqq k \leqq d).$$

Conversely, if the condition $(*)$ is satisfied, then it follows that $W_n(B_1, \cdots, B_d)$ is Z_p-equivalent to $W_n(B_1', \cdots, B_d')$ by suitable basis changes. Suppose that $W_n(B_1, \cdots, B_d)$ is Z_p-decomposable. By considering the companion representation

$$\begin{pmatrix} \zeta_{m_2}^{(n)} & \langle E_n\rangle \\ 0 & \zeta_{m_3}^{(n)} \end{pmatrix}$$

of $W_n(B_1, \cdots, B_d)$, it decompose as follows;

$$\begin{pmatrix} \zeta_{m_2}^{(n_1)} & \langle E_{n_1}\rangle \\ 0 & \zeta_{m_3}^{(n_1)} \end{pmatrix} \oplus \begin{pmatrix} \zeta_{m_2}^{(n_2)} & \langle E_{n_2}\rangle \\ 0 & \zeta_{m_3}^{(n_2)} \end{pmatrix},$$

where $n=n_1+n_2$, $0<n_1, n_2 \in N$. Thus

$$H_1^{-1}H_3 \equiv \begin{pmatrix} E_{n_1} & 0 \\ 0 & E_{n_2} \end{pmatrix} \pmod{(1-\zeta_{m_1})},$$

$$H_2^{-1}H_k \equiv \begin{pmatrix} E_{n_1} & 0 \\ 0 & E_{n_2} \end{pmatrix} \pmod{(1-\zeta_{m_2})}\ (3 \leqq k \leqq r),$$

$$H_1^{-1}B_kH_{k+3} \equiv \begin{pmatrix} S_k & 0 \\ 0 & L_k \end{pmatrix} \pmod{(1-\zeta_{m_1})}\ (1 \leqq k \leqq d-1=r-4),$$

$$H_1^{-1}B_dH_{d+3} \equiv \begin{pmatrix} S_d & 0 \\ 0 & L_d \end{pmatrix} \pmod{(1-\zeta_{m_1})}.$$

Hence $H_1 \equiv H_2 \equiv \cdots \equiv H_r \pmod{(1-\zeta_{m_1})}$. Therefore,

$$(**) \qquad H_1^{-1}B_vH_1 \equiv \begin{pmatrix} S_v & 0 \\ 0 & L_v \end{pmatrix} \pmod{(1-\zeta_{m_1})}\ (1 \leqq v \leqq d)$$

(i.e. simultaneously decomposable). Conversely, if the condition (**) is satisfied, then it follows that $W_n(B_1, \cdots, B_d)$ is Z_p-decomposable. Q.E.D.

THEOREM 3.3 (Berman-Gudivok Theorem 3.3 in [1]). *For the non-cyclic p-group* $C_p \times C_p = (a) \times (b)$ *and an arbitrary matrix* B *in* $M_n(Z_p[\zeta_1])$, *let* $W_n(B)(a)$, $W_n(B)(b)$ *be the following matrices*

$$\begin{pmatrix} \tilde{\zeta}_1^{(n)} & 0 & 0 & \langle B \rangle \\ & E_{(p-1)n} & E_{(p-1)n} & 0 \\ & & \tilde{\zeta}_1^{(n)} & 0 \\ & 0 & & E_n \end{pmatrix},$$

$$\begin{pmatrix} E_{(p-1)n} & 0 & E_{(p-1)n} & 0 \\ & \tilde{\zeta}_1^{(n)} & 0 & \langle E_n \rangle \\ & & \tilde{\zeta}_1^{(n)} & 0 \\ & 0 & & E_n \end{pmatrix}, \textit{ respectively}.$$

Then $W_n(B)$ *is a* Z_p*-representation of* $C_p \times C_p$, *and* $W_n(B)$ *is* Z_p*-equivalent to* $W_n(B')$ *if and only if* B *is similar* mod $(1-\zeta_1)$ *to* B' *in* $M_n(Z_p[\zeta_1])$. *Furthermore,* $W_n(B)$ *is* Z_p*-indecomposable if and only if* B *is indecomposable* mod $(1-\zeta_1)$.

By virtue of Theorem 3.2 (resp. Theorem 1 in [5]), the description of the Z_p-representations C_{p^r} $(r \geqq 5)$ (resp. $C_p \times C_p$) involves the matrix pair problem (i.e. simultaneous similarity transformation of two parameter matrices). Therefore, it is one of the problems to find indecomposable pair of parameter matrices. In the remark in §4, we will describe an example of indecomposable pair of matrices (in $M_2(Z)$).

§ 4. Infinite series of indecomposable representations

The indecomposable matrices in $M_m(C)$ are similar to the Jordan normal blocks

$$J_{a,m}=\begin{pmatrix} a & 1 & & & \\ & a & 1 & & 0 \\ & & \ddots & \ddots & \\ & & & a & 1 \\ 0 & & & & a \end{pmatrix},$$

which is a well-known fact in linear algebra. For the time being, we shall consider the indecomposability of a matrix L in $M_n(Z)$. Let K be an arbitrary algebraic number field, O_K be the ring of algebraic integers in K (i.e. the integral closure of Z in K), $U(O_K)$ be the group of units in O_K, and define the group $GL_n(O_K)$ as follows;

$$GL_n(O_K)=\{B\in M_n(O_K)\,|\,\det B\in U(O_K)\}\,.$$

If there exists $A\in M_{n_1}(O_K)$, $B\in M_{n_2}(O_K)$ and $C\in GL_n(K)$ (resp. $C\in GL_n(O_K)$) such that

$$C^{-1}LC=\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \quad (n=n_1+n_2)\,,$$

then we say that the matrix L is K-decomposable (resp. O_K-decomposable), otherwise L is said to be K-indecomposable (resp. O_K-indecomposable). If O_K-indecomposable matrix L is not similar to any Jordan normal blocks $J_{v,n}$, where $v\in O_K$ and K is an algebraic number field such that all the eigenvalues of L are contained in O_K, then we can choose an appropriate D in $GL_n(K)$ such that

$$D^{-1}LD=\begin{pmatrix} F & 0 \\ 0 & H \end{pmatrix} \quad \text{for some} \quad F\in M_{n_1}(0_K)\,, \qquad H\in M_{n_2}(O_K)$$

for some $F\in M_{n_1}(O_K)$, $H\in M_{n_2}(O_K)$ (i.e. L is K-decomposable).

One of the basic problems in the integral representation theory is to find all the O_K-indecomposable matrices in $M_n(O_F)$, where $K\,(\subset C)$ is a finite extention field over an algebraic number field F. Another problem is to clarify the forms of the O_K-indecomposable matrices other than the Jordan normal blocks.

We define $A_m(a;\, b_1,\, \cdots,\, b_m)$ to be the matrix in $M_m(Z)$ as follows;

$$\begin{pmatrix} a & b_1 & & & & \\ & a & b_2 & & & 0 \\ & & \ddots & \ddots & & \\ & 0 & & \ddots & & \\ & & & & a & b_{m-1} \\ b_m & 0 & \cdots & & 0 & a \end{pmatrix}.$$

Then the Jordan normal block $J_{a,m}$ can be written as $A_m(a; 1, \cdots, 1, 0)$. The characteristic polynomial $f_{A_m(a;b_1,\cdots,b_m)}(X)$ of the matrix $A_m(a; b_1, \cdots, b_m)$ is

$$(X-a)^m - \prod_{j=1}^{m} b_j \in Z[X].$$

DEFINITION 4.1. For two integral matrices $A=(a_{ij})$, $B=(b_{ij})$ in $M_n(Z)$, we write $A \equiv B \pmod{p}$ if $a_{ij} \equiv b_{ij} \pmod{p}$ for every i, j $(1 \leqq i, j \leqq m)$.

DEFINITION 4.2. An integral matrix $A \in M_m(Z)$ is said to be similar modulo p to a matrix $B \in M_m(Z)$, if there exists a matrix $C \in M_m(Z)$ such that $AC \equiv CB \pmod{p}$ and $p \nmid \det C$. Otherwise we write $A \underset{\text{mod } p}{\not\sim} B$.

PROPOSITION 4.3.

$$J_{a,q} \underset{\text{mod } p}{\not\sim} A_q(a; 1, \cdots, 1),$$

$$J_{a,2^r} \underset{\text{mod } p}{\not\sim} A_{2^r}(a; 1, \cdots, 1, b),$$

where p and q are distinct odd primes, and $b \not\equiv 0 \pmod{p}$.

Proof. Let us compare the multiplicity of eigenvalues.

(1) $f_{J_{a,q}}(X)=(X-a)^q$, $f_{J_{a,2^r}}(X)=(X-a)^{2^r}$.

(2) $f_{A_q(a;1,\cdots,1)}(X)=(X-a)^q-1$, $f_{A_{2^r}(a;1,\cdots,b)}(X)=(X-a)^{2^r}-b$.

The polynomials in (2) are separable over Z/pZ. However, all the roots over Z/pZ of the polynomials in (1) are $\bar{a}$ $(=a \bmod p)$. Thus the above matrices cannot be similar modulo p. Q.E.D.

DEFINITION 4.4. Let F_p $(=Z/pZ)$ be the prime field of characteristic $p>0$. An integral matrix A in $M_m(Z)$ is said to be strongly F_p-indecomposable if the characteristic polynomial $f_A(X)$ is irreducible in $F_p[X]$.

PROPOSITION 4.5. *Let*

$$\prod_{j=1}^{m} b_j \not\equiv 0 \pmod{p}, \qquad a, b_j \in Z \quad (1 \leqq j \leqq m).$$

If $A_m(a; b_1, \cdots, b_m)$ is strongly F_p-indecomposable, then the rational prime divisor of m is 2 or that of $p-1$.

Proof. Suppose that $q \mid m$ for some odd prime q such that G.C.D. $(p-1, q)=1$. Since $b^{p-1} \equiv 1 \pmod{p}$ for every $p \nmid b$, and there exist g, h such that $g(p-1)+hq=1$, we have

$$\prod_{j=1}^{m} b_j \in F_p^{\,q}.$$

Thus

$$f_{A_m(a,b_1,\cdots b_m)}(X) \equiv \{(X-a)^{m'}-b'\}\{(X-a)^{m'(q-1)}+(X-a)^{m'(q-2)}b'+\cdots+b'^{q-1}\} \pmod{p},$$

where

$$m=qm', \quad \text{and} \quad b'^q \equiv \prod_{j=1}^{m} b_j \pmod{p}.$$

Q.E.D.

PROPOSITION 4.6. *Let $y\neq 0$, $2\leq r\in Z$, and let p be a rational prime. If $A_{2^r}(a; 1, \cdots, 1, -y)$ is strongly F_p-indecomposable, then $y\not\equiv \pm 1 \pmod{p}$.*

Proof. If $y\equiv -1 \pmod{p}$, then it is obvious that $f_{A_{2^r}(a;1,\cdots,1,-y)}(X)\equiv (X-a)^{2^r}-1 \pmod{p}$ is reducible.

In the case of $y\equiv 1 \pmod{p}$, we have $f_{A_{2^r}(a;1,\cdots,1,-y)}(X)\equiv (X-a)^{2^r}+1 \pmod{p}$ (the latter polynomial is equal to $\Phi_{2^{r+1}}(X-a)$, which is irreducible in $Q[X]$). Now we prove the reducibility of the cyclotomic polynomial $\Phi_{2^{r+1}}(X)=X^{2^r}+1$ in $F_p[X]$. It is enough to prove that X^4+1 is a reducible polynomial in $F_p[X]$. If $p=2$, then $X^4+1\equiv (X^2-1)(X^2-1) \pmod{2}$. If p is an odd prime, then

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right).$$

We can write as follows;

$$X^4+1=X^4-(-1), \qquad (X^2+1)^2-2X^2, \qquad (X^2-1)^2-(-2)X^2.$$

Consider the three values

$$\left(\frac{-2}{p}\right), \qquad \left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right).$$

At least one of them must be $+1$. Therefore X^4+1 is reducible in $F_p[X]$. Q.E.D.

LEMMA 4.7 (E. Artin). *Let k be a field and n be an integer ≥ 2. Let $a\in k$ and $a\neq 0$. Assume that for all prime numbers p such that $p\,|\,n$ we have $a\notin k^p$, and that in the case of $4\,|\,n$ we have $a\notin -4k^4$. Then X^n-a is irreducible in $k[X]$.*

For the proof, see Lang [6], p. 221–223.

THEOREM 4.8. *Let p, q be distinct odd primes, and a, $r\in N$. Then $A_q(a; 1, \cdots, 1, 1)$ and $A_{2^r}(a; 1, \cdots, 1, -1)$ are Z-indecomposable matrices.*

If

(i) $p\equiv 1 \pmod{4}$ *and* $\left(\frac{y}{p}\right)=-1$

(ii) $p\equiv 7 \pmod{8}$ *and* $\left(\frac{y}{p}\right)=1$ *and* $y\notin F_p^4$ *or*

(iii) $p\equiv 3 \pmod{8}$ *and* $\left(\frac{y}{p}\right)=1$ *and* $y\notin 4F_p^4$,

then the matrices $A_{2^r}(a; 1, \cdots, 1, -y)$ $(r=2, 3, \cdots)$ *are strongly* F_p*-indecomposable.*

Proof. The characteristic polynomial $f_{A_{2^r}(a;1,\cdots,1,-1)}(X)=(X-a)^{2^r}+1$ is equal to $\Phi_{2^{r+1}}(X-a)$, which is irreducible over Q, hence $A_{2^r}(a; 1, \cdots, 1, -1)$ is Z-indecomposable. Suppose that $A_q(a; 1, \cdots, 1, 1)$ is Z-decomposable. Then there exists $B=(b_{ij})$ in $GL_q(Z)$ such that

$$BA_q(a; 1, \cdots, 1, 1) = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1,q-1} & 0 \\ c_{21} & c_{22} & \cdots & c_{2,q-1} & 0 \\ & & & & \\ c_{q-1,1} & c_{q-1,2} & \cdots & c_{q-1,q-1} & 0 \\ 0 & 0 & \cdots & 0 & a+1 \end{pmatrix} B,$$

because $F_{A_q(a;1,\cdots,1,1)}(X)=\{X-(a+1)\}\{(X-a)^{q-1}+\cdots+(X-a)+1\}$, where the second factor is irreducible over Q, and $Q[X]$ is factorial (i.e. unique factorization ring). By the equality of matrices, we write out the components as follows;

$$\begin{pmatrix} ab_{11}+b_{1q} & ab_{12}+b_{11} & \cdots & ab_{1,q-1}+b_{1,q-2} & ab_{1q}+b_{1,q-1} \\ & & \vdots & & \\ ab_{q1}+b_{qq} & ab_{q2}+b_{q1} & \cdots & ab_{q,q-1}+b_{q,q-2} & ab_{qq}+b_{q,q-1} \end{pmatrix}$$

$$= \begin{pmatrix} \sum_{j=1}^{q-1} c_{kj}b_{js} \\ (a+1)b_{q1} \quad \cdots \quad (a+1)b_{qq} \end{pmatrix} \quad \begin{matrix} 1\leq k\leq q-1 \\ 1\leq s\leq q \end{matrix}.$$

Thus we have

$$(a+1)\sum_{j=1}^{q} b_{hj} = \sum_{j=1}^{q-1} c_{hj}\left(\sum_{k=1}^{q} b_{jk}\right) \quad (1\leq h\leq q-1),$$

and $b_{q1}=\cdots=b_{qq}$ (for brevity, we write b). Therefore

$$(c_{ij})\begin{pmatrix} \sum_{k=1}^{q} b_{1k} \\ \vdots \\ \sum_{k=1}^{q} b_{q-1,k} \end{pmatrix} = (a+1)\begin{pmatrix} \sum_{j=1}^{q} b_{1j} \\ \vdots \\ \sum_{j=1}^{q} b_{q-1,j} \end{pmatrix}.$$

Assume that

$$\left(\sum_{k=1}^{q} b_{1k}, \cdots, \sum_{k=1}^{q} b_{q-1,k}\right)=(0, \cdots, 0),$$

then

$$\pm 1=\det B = \begin{vmatrix} 0 & b_{12} & \cdots & b_{1q} \\ & & \cdots & \\ & & \vdots & \\ 0 & b_{q-1,2} & \cdots & b_{q-1,q} \\ qb & b_{q2} & \cdots & b_{qq} \end{vmatrix} = qb \begin{vmatrix} b_{12} & \cdots & b_{1q} \\ & \vdots & \\ b_{q-1,2} & \cdots & b_{q-1,q} \end{vmatrix}$$

This is a contradiction. Hence $a+1$ is an eigenvalue of the matrix (c_{ij}). On the other hand, the number $a+1$ cannot be any roots of $f_{(c_{ij})}(X)$ $(=(X-a)^{q-1}+\cdots+(X-a)+1)$. Therefore $A_q(a; 1, \cdots, 1, 1)$ must be Z-indecomposable.

In order to prove the second half of our theorem, we will apply Lemma 4.7.

In case (i), it follows that

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}=1 .$$

Hence

$$\left(\frac{-y}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{y}{p}\right)=-1 \qquad \text{(i.e., } -y\notin F_p^2\text{)} .$$

Since $-4F_p^4\subseteq(-1)F_p^2=F_p^2$, we have $-y\notin -4F_p^4$. In case (ii), it follows that

$$\left(\frac{-1}{p}\right)=-1 \quad \text{and} \quad \left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}=1 .$$

Hence $-y\notin F_p^2$ and $4F_p^4=F_p^4$. Thus we have $-y\notin -4F_p^4$. In case (iii), it follows that

$$\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=-1 .$$

Hence

$$\left(\frac{-y}{p}\right)=-1 .$$

Consequently, the polynomial $f_{A_{2^r}(a;1,\cdots,1,-y)}(X)=(X-a)^{2^r}-(-y)$ is irreducible in $F_p[X]$ by means of Lemma 4.7. This completes the proof the theorem. Q.E.D.

Applying the Berman-Gudivok theorems to indecomposable $(2^r, 2^r)$-matrices $(r=2,3,4, \cdots)$ constructed in Theorem 4.8, we have obtained infinite series of indecomposable integral representations. Then the corresponding indecomposable ZG-lattices are not necessarily projective ZG-modules in view of the Nakayama's proposition with respect to Z-rank. For example, in the case of Theorem 3.3, since $p\nmid n(3p-2)$ $(n=q$ or $n=2^r)$ and Z-ranks of these lattices are

$n(p-1)+n(p-1)+n(p-1)+n=n(3p-2)$, it follows that these lattices are non-projective.

Remark. Let B_2, B_3 be triangular matrices as defined below;

$$B_2=B_2(a, b)=\begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}\in M_2(Z),$$

where $|a-b|\neq 1$,

$$B_3=B_3(a, b, c)=\begin{pmatrix} a & 1 & 0 \\ 0 & b & 1 \\ 0 & 0 & c \end{pmatrix}\in M_3(Z),$$

where $|a-b|\neq 1$, $|b-c|\neq 1$, $a\neq c$.

Suppose that there exists a

$$Z\text{-matrix}\begin{pmatrix} u & v \\ s & t \end{pmatrix} \text{ in } GL_2(Z)$$

such that

$$B_2\begin{pmatrix} u & v \\ s & t \end{pmatrix}=\begin{pmatrix} u & v \\ s & t \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

Then $s=0$ and $t=v(b-a)$. Hence

$$\pm 1=\det\begin{pmatrix} u & v \\ s & t \end{pmatrix}=\begin{vmatrix} u & v \\ 0 & v(b-a) \end{vmatrix}=uv(b-a).$$

This is a contradiction. Therefore, the matrix B_2 is Z-indecomposable.

By the similar method, assume that

$$\begin{pmatrix} d & u & v \\ e & s & t \\ f & g & h \end{pmatrix} B_3=\begin{pmatrix} a & x & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}\begin{pmatrix} d & u & v \\ e & s & t \\ f & g & h \end{pmatrix} \text{ or } \begin{pmatrix} a & 0 & x \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}\begin{pmatrix} d & u & v \\ e & s & t \\ f & g & h \end{pmatrix}$$

for some

$$\begin{pmatrix} d & u & v \\ e & s & t \\ f & g & h \end{pmatrix}\in GL_3(Z).$$

In the first case, it follows that $e=f=g=0$ and $s=(b-c)t$. Hence

$$\pm 1=\det\begin{pmatrix} d & u & v \\ 0 & s & t \\ 0 & 0 & h \end{pmatrix}=(b-c)tdh.$$

This is a contradiction. In the second case, it follows that $e=f=g=0$ and $d=(a-b)u$. This also implies a contradiction. Thus the matrix B_3 is Z-indecomposable.

While two matrices

$$\begin{pmatrix} m & 1 \\ 0 & m+1 \end{pmatrix}, \quad \begin{pmatrix} m & 1 \\ 0 & m-1 \end{pmatrix}$$

are decomposable by

$$\begin{pmatrix} x & -x \\ 0 & y \end{pmatrix}, \quad \begin{pmatrix} x & x \\ 0 & y \end{pmatrix} \text{ in } GL_2(Z),$$

respectively. In fact

$$\begin{pmatrix} m & 1 \\ 0 & m+1 \end{pmatrix} \underset{z}{\sim} \begin{pmatrix} m & 0 \\ 0 & m+1 \end{pmatrix} \text{ and } \begin{pmatrix} m & 1 \\ 0 & m-1 \end{pmatrix} \underset{z}{\sim} \begin{pmatrix} m & 0 \\ 0 & m-1 \end{pmatrix}.$$

However these two matrices cannot be decomposed simultaneously by any matrix in $GL_2(F_p)$, since $x \not\equiv -x \pmod{p}$ for odd rational prime p such that $p \nmid xy$.

Under the same notations in Theorem 3.1, let P be the prime ideal of $Z_p[\zeta_{p^{m_1}}]$ generated by $1-\zeta_{p^{m_1}}$. Then it follows that $(p)=P^{\varphi(p^{m_1})}$ and $Z_p[\zeta_{p^{m_1}}]/P \cong F_p = Z/pZ$. Thus, (p) is completely ramified in $Z_p[\zeta_{p^{m_1}}]$ over Z_p.

Since $1 \leq r$, we have

$$\begin{array}{ccc} W_n(B) \text{ is } Z_p\text{-indecomposable} & \Longleftrightarrow & B \text{ is indecomposable mod } P^r \\ & & \Uparrow \\ GL_n(F_p) \in \bar{B} \text{ is indecomposable} & \Longleftrightarrow & GL_n(Z_p[\zeta_{p^{m_1}}]/P) \in \bar{B} \text{ is indecomposable} \end{array}$$

($\bar{B}$ denotes the reduction mod P of B)

Therefore, for constructing infinite series of Z_p-indecomposable representations, it is sufficient to find infinitely many number of indecomposable F_p-matrices which are non-similar to each other. For distinct odd primes p, q, let $\Phi_{q^r}(X)$ (the q^r-th cyclotomic polynomial) be $\sum c_j X^j \in Z[X]$ ($c_0 = c_{\varphi(q^r)} = 1$), and let $C_{\varphi(q^r)}$ be the following normal form associated with $\Phi_{q^r}(X)$ (i.e. the companion matrix of $\Phi_{q^r}(X)$);

$$C_{\varphi(q^r)} = \begin{pmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & 0 \\ & & \ddots & \ddots & & \\ & 0 & & & & \\ & & & & 0 & 1 \\ -c_0 & -c_1 & \cdots & & & -c_{\varphi(q^r)-1} \end{pmatrix}.$$

The ideal (p) is unramified in $Q(\zeta_{q^r})$ over Q, since $p \nmid D_{Q(\zeta_{q^r})}$ (discriminant of the field $Q(\zeta_{q^r})$). Let P_i ($1 \leq i \leq g$) be all the prime ideals of $Q(\zeta_{q^r})$ such that $P_i \cap Z = (p)$. Then the order of the element p mod q^r in $(Z/q^rZ)^*$ is $\varphi(q^r)$ if and only if $g=1$ (i.e. (p) remains prime in $Z[\zeta_{q^r}]$) (cf. [2] pp. 327–328). Furthermore, (p) remains prime in $Z[\zeta_{q^r}]$ if and only if the polynomial $\Phi_{q^r}(X)$ is irreducible in $F_p[X]$ (cf. [2] pp. 233–234).

Consequently the Z_p-representation $W_{\varphi(q^r)}(C_{\varphi(q^r)})$ is Z_p-indecomposable if p is a primitive root of Z/q^rZ.

By the assumption (i) in § 2, for an odd prime $p\ (=a)$, there exist infinitely many Z_p-indecomposable representations $W_{\varphi(q^1)}\ (c_{\varphi(q^1)})$, where $q\in P_p$ and $r=1$. While, by the assumption (ii) in § 2, there exist infinitely many Z_p-indecomposable representations $W_{\varphi(q^r)}(C_{\varphi(q^r)})$ $(r=1, 2, 3, \cdots)$ for some odd prime q. Suppose that q, $q'\in P'_p$ and $q\neq q'$, then $W_{\varphi(q'^{r'})}(C_{\varphi(q'^{r'})})(r'=2, 3, \cdots)$ are not Z_p-equivalent to $W_{\varphi(q^r)}(c_{\varphi(q^r)})$ $(r=2, 3, \cdots)$, because of $\varphi(q^r)\neq\varphi(q'^{r'})$.

References

[1] BERMAN, S. D. and GUDIVOK, P. M.; Indecomposable representations of finite groups over the ring of p-adic integers, *Izv. Akad. Nauk. SSSR, Ser. Math.*, **28** (1964), 875–910; (English transl.), *Amer. Math. Soc. Transl.* (2) **50** (1966), 77–113.

[2] BOREVICH, Z. I. and SHAFAREVICH, I. R.; *Number Theory* (English transl.), Academic Press, New York, 1966.

[3] DIETERICH, E.; Darstellungstypen von gruppenringen über vollständigen diskreten bewertungsringen, Dissertation (Universität Bielefeld) (1981).

[4] GUDIVOK, P. M.; Representations of finite groups over number rings, *Izv. Aka. Nauk. SSSR, Ser. Math.*, **31** (1967), 799–834; (English transl.), *Math. USSR. Izv.*, **1** (1967), 773–805.

[5] GUDIVOK, P. M.; On representations of finite groups over a complete discretely valued ring, Proceeding of the Steklov Inst. of Math., 1980, Issue 4, *Algebra, Theory of Numbers and Their Applications* (A.M.S. Transl.), pp. 95–105.

[6] LANG, S.; *Algebra*, Addison Wesley, Reading Mass., 1965.

[7] REINER, I.; A survey of integral representation theory, *Bull. Amer. Math. Soc.*, **76** (1970), 159–227.

[8] REINER, I.; *Maximal Orders*, Academic Press, London, 1975.

[9] ROITER, A. V.; Unbounded dimensionality of indecomposable representations of an algebra with an infinite number of indecomposable representations, *Izv. Akad. Nauk. SSR, Ser. Math.*, **32** (1968), 1275–1283; (English transl.), *Math. USSR. Izv.*, **2** (1968), 1223–1230.

Department of Mathematics
Rikkyo University
Tokyo, 171, Japan