TOKYO J. MATH.
VOL. 25, NO. 2, 2002

On The Unit Group of The Group Ring $\mathbb{Z}[G]$

Noritsugu ENDO

Chuo University

(Communicated by T. Takakura)

Introduction.

Let G be a commutative group. A formula on the torsion free rank of $\mathbb{Z}[G]$ is given by Higman ([2, Theorem 13.5]). We think about a case where G is a finite commutative group. Then we can define a fundamental system of units in $\mathbb{Z}[G]$ (See Definition 2.2.). We consider the following problem.

PROBLEM A. Given a finite commutative group G, find a specific fundamental system of units in $\mathbb{Z}[G]$.

This is a difficult problem. For example, if G is cyclic of prime order p, then Problem A is equivalent to the problem of find a specific fundamental system of units of the subgroup of $\mathbb{Z}[\zeta]^\times$ consisting of all units which are congruent to 1 modulo $\zeta - 1$, where ζ be a primitive p-th root of unity. Therefore we consider the weaker next problem.

PROBLEM B. Given a finite commutative group G, find a specific system of r independent units of infinite order in $\mathbb{Z}[G]$ or, equivalently, a system of independent units of infinite order which generates a subgroup of finite index.

In the case where G is a cyclic group, an independence system of units in $\mathbb{Z}[G]$ is given by Bass ([1], [2]). In this article, we consider the elementary p-group case $G = (\mathbb{Z}/p)^n$, and we give the direct product decomposition of $\mathbb{Z}[G]^\times$ induced by the structure of the unit group scheme $U(G)$.

ASSERTION 1 (cf. Lemma 2.3). *Let $G = (\mathbb{Z}/p)^n$ and let ζ be a primitive p-th root of unity. We put $\lambda = \zeta - 1$. Then*

$$\mathbb{Z}[G]^\times \xrightarrow{\sim} \{\pm 1\} \times \prod_{i=1}^{n} U_i^{\binom{n}{i}},$$

where $U_i := \{\tilde{u} \in (\mathbb{Z}[\zeta]^{\otimes i})^\times | \tilde{u} \equiv 1^{\otimes i} \bmod \lambda^{\otimes i}\}$.

Moreover we construct an independent system of finite index of the unit group $\mathbb{Z}[G]^\times$ when $G = \mathbb{Z}/p \times \mathbb{Z}/p$.

Received June 26, 2001; revised February 22, 2002

ASSERTION 2 (cf. Theorem 2.4). *Let* $G = \mathbb{Z}/p \times \mathbb{Z}/p$ *and let* $r_1 = \frac{1}{2}(p-3)$. *We take an independent system* $\{u_i | 1 \le i \le r_1\}$ *of the units in the group ring* $\mathbb{Z}[\mathbb{Z}/p]$ *and let* $\overline{u_i}$ *be the image of* u_i *in* $\mathbb{Z}[\zeta]$ *i.e.* $\{\overline{u_i} | 1 \le i \le r_1\}$ *is an independent system of* U_1. *Then* $\{\overline{u_i}_{(j)} | 1 \le i \le r_1, 1 \le j \le p-1\}$ *is an independent system of* U_2. *Here* $\overline{u_i}_{(j)}$ *is an inverse image of* $(1, \cdots, 1, \underset{\hat{j}}{\overline{u_i}}, 1, \cdots, 1)$ *by an injection* $\varphi : \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta] \to \prod_{\sigma \in H} \mathbb{Z}[\zeta]$.

In Section 1, we review the group scheme $U(G)$ and some results. In Sections 2 and 3, we prove the assertions. And in Section 4, we construct a fundamental system of units in the group ring $\mathbb{Z}[G]$ when $p = 5$ and 7.

ACKNOWLEDGMENT. The results in Section 1, which was allowed us to use in this work, are based on N. Suwa. We specify them here. And the author was given some advice from T. Sekiguchi and N. Suwa in finishing this work. He expresses his gratitude for them.

1. Preliminaries.

In this section, we review some results in [3] and [4].

DEFINITION 1.1. Let A be a ring and $a \in A$. We define a group scheme $\mathcal{G}^{(a)}$ over A by $\mathcal{G}^{(a)} = \mathrm{Spec}A[X, 1/(aX+1)]$ with

(1) the multiplication: $X \mapsto aX \otimes X + X \otimes 1 + 1 \otimes X$,
(2) the unit: $X \mapsto 0$,
(3) the inverse: $X \mapsto -X/(aX+1)$.

Moreover, we define an A-homomorphism $\alpha^{(a)} : \mathcal{G}^{(a)} \to \mathbb{G}_{m,A}$ by

$$U \mapsto aX + 1 : A[U, U^{-1}] \to A[X, 1/(aX+1)] .$$

If a is invertible in A, $\alpha^{(a)}$ is an A-isomorphism. If $a = 0$, $\mathcal{G}^{(a)}$ is nothing but the additive group scheme $\mathbb{G}_{a,A}$.

Let B be an A-algebra. Then the multiplication of the group $\mathcal{G}^{(a)}(B) = \{b \in B | 1 + ab \in B^\times\}$ is defined by $b \cdot b' = b + b' + abb'$ for $b, b' \in \mathcal{G}^{(a)}(B)$. Moreover, $\mathcal{G}^{(a)}(B)$ is isomorphic to $\{b \in B^\times | b \equiv 1 \bmod a\} \subset B^\times$.

DEFINITION 1.2. Let G be a finite group. We define a ring scheme $A(G)$ by $A(G) = \mathrm{Spec}\mathbb{Z}[T_g ; g \in G]$ with

(1) the addition: $\alpha^*(T_g) = T_g \otimes 1 + 1 \otimes T_g$,
(2) the multiplication: $\mu^*(T_g) = \sum_{g_1 g_2 = g} T_{g_1} \otimes T_{g_2}$,

where T_g are indeterminates. Then $A(G)$ represents the group algebra of G.

Let $U(G) = \mathrm{Spec}\,\mathbb{Z}[T_g, 1/\det(T_{gh})]$. Then $U(G)$ is an open subscheme of $A(G)$ and represents the unit group of the group algebra of G. If $G = 1$, $U(G)$ is nothing but the multiplicative group $\mathbb{G}_{m,\mathbb{Z}} = \mathrm{Spec}\,\mathbb{Z}[U, 1/U]$.

Let $\varphi : G \to H$ be a homomorphism of finite groups. We denote by $A(\varphi) : A(G) \to A(H)$ and $U(\varphi) : U(G) \to U(H)$ the homomorphism of ring schemes or the homomorphism of group schemes, respectively, induced by φ. These homomorphisms are represented by the homomorphism of rings defined by

$$T_h \mapsto \sum_{\varphi(g)=h} T_g \,.$$

Let $(G_i)_{i\in I}$ be a finite family of finite commutative groups. For $J \subset I$, let $G_J = \prod_{i\in J} G_i$, where $G_\emptyset = 1$. Then the decomposition of the group scheme $U(G_I)$ corresponding to $G_I = \prod_{j\in I} G_j$ is given as follows.

Let $e_i \in \mathrm{End}(U(G_I))$ be defined by the composition of the canonical projection $G_I \to \prod_{j\neq i} G_j$ and the canonical injection $\prod_{j\neq i} G_j \to G_I$. By the definition of e_i, the followings are trivial.

LEMMA 1.3.

$$e_i e_j = \begin{cases} e_i\,, & \text{if } i = j\,, \\ e_j e_i\,, & \text{if } i \neq j\,, \end{cases}$$

for any $i, j \in I$.

Note that the ring structure of $\mathrm{End}(U(G_I))$ is denoted by the addition = the one induced by the multiplication of $U(G_I)$ and the multiplication = the composition of endomorphism.

COROLLARY 1.4. *For any* $i, j \in I$

(1) $(1-e_i)(1-e_j) = \begin{cases} 1-e_i, & \text{if } i = j\,, \\ (1-e_j)(1-e_i), & \text{if } i \neq j\,, \end{cases}$

(2) $e_i(1-e_j) = (1-e_j)e_i\,,$

(3) $e_i(1-e_i) = 0\,.$

REMARK. Let R be a ring. We consider the R-valued points of group scheme $U(G)$. Then

$$(1-e_i)(u) = u(e_i(u))^{-1} \in R[G]^\times$$

for $u \in R[G]^\times$.

Let $\varepsilon_J = (\prod_{i\notin J} e_i)(\prod_{i\in J}(1-e_i))$ for $J \subset I$. Then ε_J are idempotent elements of $\mathrm{End}(U(G_I))$.

LEMMA 1.5. *Under the above notations, we have the following.*

(1) *If* $J \neq K$, *then* $\varepsilon_J \varepsilon_K = 0$,

(2) $\sum_{J\subset I} \varepsilon_J = 1$.

PROOF. We put $I = \{1, 2, \cdots, r\}$.

(1) Since $J \neq K$, we may assume that there is $i \in I$ such that $i \in J$ and $i \notin K$. Then

$$\begin{aligned} \varepsilon_J \varepsilon_K &= e_i(1-e_i)\Big(\prod_{j\notin J} e_j\Big)\Big(\prod_{j\in J\setminus\{i\}}(1-e_j)\Big)\Big(\prod_{k\notin K\cup\{i\}} e_k\Big)\Big(\prod_{k\in K}(1-e_k)\Big) \\ &= 0 \end{aligned}$$

by Lemma 1.3 and Corollary 1.4.

(2) We prove the assertion by the induction on r.

When $r=1$, $e_1+(1-e_1)=1$.

Assume that the assertion is true when $r=k$. If $r=k+1$, then

$$\begin{aligned}\sum_{J\subset I}\varepsilon_J &= e_{k+1}\Big(\sum_{J\subset\{1,2,\cdots,k\}}\varepsilon_J\Big)+(1-e_{k+1})\Big(\sum_{J\subset\{1,2,\cdots,k\}}\varepsilon_J\Big)\\ &=\{e_{k+1}+(1-e_{k+1})\}\Big(\sum_{J\subset\{1,2,\cdots,k\}}\varepsilon_J\Big)\\ &=1\,.\end{aligned}$$

□

By this Lemma, putting $U_J=\operatorname{Im}\varepsilon_J$, we obtain the decomposition $U(G_I)=\prod_{J\subset I}U_J(G_I)$, and the following.

LEMMA 1.6. *If $K\subset J\subset I$, then the canonical projection $G_I=\prod_{i\in I}G_i\to G_J=\prod_{i\in J}G_i$ induces the isomorphism $U_K(G_I)\xrightarrow{\sim}U_K(G_J)$.*

Let $I=\{1,2,\cdots,r\}$, $p_i(i\in I)$ be prime numbers, $G_i=\mathbb{Z}/p_i^{n_i}$ and $G=G_I=\prod_{i\in I}G_i$. Then $\mathbb{Z}[G]$ is isomorphic to $\mathbb{Z}[T_1,T_2,\cdots,T_r]/(T_1^{p_1^{n_1}}-1,T_2^{p_2^{n_2}}-1,\cdots,T_r^{p_r^{n_r}}-1)$ and $U(G)$ is identified with the functor

$$A\mapsto\big(A[T_1,T_2,\cdots,T_r]/(T_1^{p_1^{n_1}}-1,T_2^{p_2^{n_2}}-1,\cdots,T_r^{p_r^{n_r}}-1)\big)^\times\,.$$

Let $\mathbf{I}=\{(k_1,k_2,\cdots,k_r),|\,1\le k_i\le n_i\}$. For $\mathbf{k}=(k_1,k_2,\cdots,k_r)\in\mathbf{I}$, we define the subfunctor $V_{\mathbf{k}}(G)$ of $U(G)$ by

$$A\mapsto\left\{\overline{f(T_1,T_2,\cdots,T_r)}\;\middle|\;\begin{array}{c}f(T_1,T_2,\cdots,T_r)-1-(T_1^{p_1^{k_1-1}}-1)(T_2^{p_2^{k_2-1}}-1)\cdots(T_r^{p_r^{n_r-1}}-1)F(\mathbf{T})\\ \in(T_1^{p_1^{n_1}}-1,T_2^{p_2^{n_2}}-1,\cdots,T_r^{p_r^{n_r}}-1)\\ \text{for some }F(\mathbf{T})\in A[T_1,T_2,\cdots,T_r]\end{array}\right\}$$
$$\subset(A[T_1,T_2,\cdots,T_r]/(T_1^{p_1^{n_1}}-1,T_2^{p_2^{n_2}}-1,\cdots,T_r^{p_r^{n_r}}-1))^\times\,.$$

For example $V_{(1,1,\cdots,1)}(G)=U_I(G_I)$. Then $V_{(1,1,\cdots,1)}(\prod_{i=1}^r\mathbb{Z}/p_i^{n_i})$ is a successive extension of $V_{\mathbf{k}}(\prod_{i=1}^r\mathbb{Z}/p_i^{k_i})$, where $\mathbf{k}=(k_1,k_2,\cdots,k_r)\in\mathbf{I}$.

THEOREM 1.7. *Let $n_1,n_2,\cdots,n_r\in\mathbb{N}_{>0}$, let $p_1,p_2,\cdots,p_r$ be prime numbers and let $\zeta_{p_i^{n_i}}$ be a primitive $p_i^{n_i}$-th root of unity in $\mathbb{C}$, chosen so that $\zeta_{p_i^{n_i}}^p=\zeta_{p_i^{n_i-1}}$. We put $\lambda_{p_i}=\zeta_{p_i^{n_i}}^{p^{n_i-1}}-1$. Then*

$$V_{(n_1,n_2,\cdots,n_r)}\Big(\prod_{i=1}^r\mathbb{Z}/p_i^{n_i}\Big)\xrightarrow{\sim}\prod_{\mathbb{Z}[\zeta_{p_1^{n_1}}]\otimes_{\mathbb{Z}}\cdots\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta_{p_r^{n_r}}]/\mathbb{Z}}\mathcal{G}^{(\lambda_{p_1}\otimes\cdots\otimes\lambda_{p_r})}\,.$$

Here, for an A-algebra B which is finite and locally free over A, and for a B-scheme F, we denote by $\prod_{B/A} F$ the Weil restriction of F. That is to say, for A-algebra R, $\prod_{B/A} F(R) = F(R \otimes_A B)$.

PROOF. Let A be a ring and let

$$f(\mathbf{T}) = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{T}^{\mathbf{i}} = \sum_{i_1, i_2, \cdots, i_r} a_{i_1, i_2, \cdots, i_r} T_1^{i_1} T_2^{i_2} \cdots, T_r^{i_r}$$

$$\in A[T_1, T_2, \cdots, T_r]/(T_1^{p_1^{n_1}} - 1, T_2^{p_2^{n_2}} - 1, \cdots, T_r^{p_r^{n_r}} - 1).$$

We define

$$f(\boldsymbol{\zeta}) \in A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_1^{n_1}}] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_2^{n_2}}] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_r^{n_r}}]$$

by

$$f(\boldsymbol{\zeta}) = \sum_{\mathbf{i}} a_{\mathbf{i}} \boldsymbol{\zeta}^{\mathbf{i}} = \sum_{i_1, i_2, \cdots, i_r} a_{i_1, i_2, \cdots, i_r} \otimes \zeta_{p_1^{n_1}}^{i_1} \otimes \zeta_{p_2^{n_2}}^{i_2} \otimes \cdots \otimes \zeta_{p_r^{n_r}}^{i_r}.$$

If

$$f(\mathbf{T}) \equiv 1 \bmod (T_1^{p_1^{n_1-1}} - 1)(T_2^{p_2^{n_2-1}} - 1) \cdots (T_r^{p_r^{n_r-1}} - 1)$$

for $f(\mathbf{T}) \in (A[T_1, T_2, \cdots, T_r]/(T_1^{p_1^{n_1}} - 1, T_2^{p_2^{n_2}} - 1, \cdots, T_r^{p_r^{n_r}} - 1))^\times$, then $f(\boldsymbol{\zeta}) \in (A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_1^{n_1}}] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_2^{n_2}}] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_r^{n_r}}])^\times$ and $f(\boldsymbol{\zeta}) \equiv 1 \bmod 1 \otimes \lambda_{p_1} \otimes \cdots \otimes \lambda_{p_r}$. Hence we can define a homomorphism

$$\eta_A : V_{(n_1, n_2, \cdots, n_r)}\left(\prod_{i=1}^r \mathbb{Z}/p_i^{n_i}\right)(A) \to \mathcal{G}^{(\lambda_{p_1} \otimes \cdots \otimes \lambda_{p_r})}(A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_1^{n_1}}] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_2^{n_2}}] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_r^{n_r}}])$$

by

$$\eta_A(f(\mathbf{T})) = \frac{f(\boldsymbol{\zeta}) - 1}{1 \otimes \lambda_{p_1} \otimes \cdots \otimes \lambda_{p_r}}.$$

Note that $\zeta_{p_1^{n_1}}^{i_1} \frac{\zeta_{p_1}^{j_1} - 1}{\zeta_{p_1} - 1} \otimes \cdots \otimes \zeta_{p_r^{n_r}}^{i_r} \frac{\zeta_{p_r}^{j_r} - 1}{\zeta_{p_r} - 1}$ $(0 \le i_k \le p_k^{n_k - 1}, 1 \le j_k < p_k)$ form a basis of $\mathbb{Z}[\zeta_{p_1^{n_1}}] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_r^{n_r}}]$ over $\mathbb{Z}$. The injectivity of η_A:

Assume that $\eta_A(f(\mathbf{T})) = 0$. Then $f(\boldsymbol{\zeta}) - 1 = 0$. Since we can represent $f(\mathbf{T}) - 1$ as a linear combination of monomials

$$T_1^{i_1} T_2^{i_2} \cdots T_r^{i_r} (T_1^{j_1 p_1^{n_1-1}} - 1)(T_2^{j_2 p_2^{n_2-1}} - 1) \cdots (T_r^{j_r p_r^{n_r-1}} - 1) \ (0 \le i_k \le p_k^{n_k-1}, 1 \le j_k < p_k)$$

uniquely, $f(\mathbf{T}) - 1 = 0$. Hence η_A is injective.

The surjectivity of η_A:

For any

$$\sum_{\substack{i_1, \cdots, i_r \\ j_1, \cdots, j_r}} a_{i_1, \cdots, i_r, j_1, \cdots, j_r} \otimes \zeta_{p_1^{n_1}}^{i_1} \frac{\zeta_{p_1}^{j_1} - 1}{\zeta_{p_1} - 1} \otimes \cdots \otimes \zeta_{p_r^{n_r}}^{i_r} \frac{\zeta_{p_r}^{j_r} - 1}{\zeta_{p_r} - 1}$$

$$\in \mathcal{G}^{(\lambda_{p_1} \otimes \cdots \otimes \lambda_{p_r})}(A \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_1^{n_1}}] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_2^{n_2}}] \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{p_r^{n_r}}]),$$

we put

$$f(\mathbf{T}) = 1 + \sum_{\substack{i_1,\cdots,i_r\\ j_1,\cdots,j_r}} a_{i_1,\cdots,i_r,j_1,\cdots,j_r} T_1^{i_1} T_2^{i_2}\cdots T_r^{i_r} (T_1^{j_1 p_1^{n_1-1}} - 1)(T_2^{j_2 p_2^{n_2-1}} - 1)\cdots(T_r^{j_r p_r^{n_r-1}} - 1)\,.$$

Then

$$\eta_A(f(\mathbf{T})) = \sum_{\substack{i_1,\cdots,i_r\\ j_1,\cdots,j_r}} a_{i_1,\cdots,i_r,j_1,\cdots,j_r} \otimes \zeta_{p_1{}^{n_1}}^{i_1} \frac{\zeta_{p_1}{}^{j_1} - 1}{\zeta_{p_1} - 1} \otimes\cdots\otimes \zeta_{p_r{}^{n_r}}^{i_r} \frac{\zeta_{p_r}{}^{j_r} - 1}{\zeta_{p_r} - 1}$$

and $f(\mathbf{T}) \in V_{(n_1,n_2,\cdots,n_r)}(\prod_{i=1}^r \mathbb{Z}/p_i^{n_i})(A)$. Hence η_A is surjective.

Therefore η_A is bijective. □

2. The $\mathbb{Z}$-rational points of the group scheme $U(\mathbb{Z}/p \times \mathbb{Z}/p)$.

Let p be a prime number and ζ be a primitive p-th root of unity. Put $\lambda = \zeta - 1$. Then (λ) is a prime ideal of $\mathbb{Z}[\zeta]$ and $(\lambda)^{p-1} = (p)$.

For any commutative group G, there is a formula on the torsion free rank of $\mathbb{Z}[G]^\times$ as follows.

THEOREM 2.1 ([2, Th. 13.5]). *Let G be an arbitrary commutative group and let G_0 be the torsion subgroup of G. Then*

$$\mathbb{Z}[G]^\times = \pm G \times F$$

where F is a free commutative group whose rank is defined as follows:

$$\textit{rank } F = \begin{cases} \frac{1}{2}(|G_0| - 2\ell + m + 1) & \textit{if } G_0 \textit{ is finite}\\ 0 & \textit{if } G_0^4 = 1 \textit{ or } G_0^6 = 1\\ |G_0| & \textit{if } G_0 \textit{ is infinite, } G_0^4 \neq 1 \textit{ and } G_0^6 \neq 1\,. \end{cases}$$

Here m (respectively, ℓ) is the number of cyclic subgroups of G_0 of order 2 (respectively, the number of the cyclic subgroups of G_0).

In particular, if $G = \mathbb{Z}/p \times \mathbb{Z}/p$ for a prime number $p \geq 5$, then $m = 0$ and $\ell = p + 2$. Hence,

$$\operatorname{rank} \mathbb{Z}[G]^\times = \frac{1}{2}(p+1)(p-3)\,.$$

DEFINITION 2.2. Let $r = \operatorname{rank} \mathbb{Z}[G]^\times$. There exists a system of r units $u_1, u_2, \cdots, u_r$ such that every unit of $\mathbb{Z}[G]$ is represented uniquely in the form

$$\pm g u_1^{n_1} u_2^{n_2} \cdots u_r^{n_r} (n_i \in \mathbb{Z},\ \ g \in G)\,.$$

In this case, we call $\{u_1, u_2, \cdots, u_r\}$ a fundamental system of units in $\mathbb{Z}[G]$ and call each u_i a fundamental unit.

Let aug:$\mathbb{Z}[G] \to \mathbb{Z}$ be the homomorphism of $\mathbb{Z}$-algebras defined by $\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$. If $u \in \mathbb{Z}[G]^\times$, then $\operatorname{aug}(u) \in \{\pm 1\}$.

We construct an independent system of finite index of the units of $\mathbb{Z}[G]$ for $G = \mathbb{Z}/p \times \mathbb{Z}/p$ using the rational points of unit group scheme $U(G)$ of group ring scheme $A(G)$.

At first, we give the direct product decomposition of $\mathbb{Z}[G]^\times$ when $G = (\mathbb{Z}/p)^n$

LEMMA 2.3. *Let $G = (\mathbb{Z}/p)^n$ and let ζ be a primitive p-th root of unity. $\lambda := \zeta - 1$. Then*

$$\mathbb{Z}[G]^\times \xrightarrow{\sim} \{\pm 1\} \times \prod_{i=1}^{n} U_i^{\binom{n}{i}},$$

where $U_i := \{\tilde{u} \in (\mathbb{Z}[\zeta]^{\otimes i})^\times | \tilde{u} \equiv 1^{\otimes i} \bmod \lambda^{\otimes i}\}$.

PROOF. Let $I = \{1, 2, \cdots, n\}$. Then

$$U(G) = \prod_{J \subset I} U_J(G)$$

by the direct product decomposition of $U(G)$. And if $\sharp J = k$,

$$U_J(G) \xrightarrow{\sim} \prod_{\mathbb{Z}[\zeta]^{\otimes k}/\mathbb{Z}} \mathcal{G}^{(\lambda^{\otimes k})}$$

by Theorem 1.7. Hence we have

$$U(G) \xrightarrow{\sim} \mathbb{G}_{m,\mathbb{Z}} \times \left(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \right)^{\binom{n}{1}} \times \left(\prod_{\mathbb{Z}[\zeta]^{\otimes 2}/\mathbb{Z}} \mathcal{G}^{(\lambda^{\otimes 2})} \right)^{\binom{n}{2}} \times \cdots \times \left(\prod_{\mathbb{Z}[\zeta]^{\otimes n}/\mathbb{Z}} \mathcal{G}^{(\lambda^{\otimes n})} \right)^{\binom{n}{n}}.$$

Since $U(G) = \mathbb{Z}[G]^\times$ and $\displaystyle\prod_{\mathbb{Z}[\zeta]^{\otimes k}/\mathbb{Z}} \mathcal{G}^{(\lambda^{\otimes k})}(\mathbb{Z}) = U_k$,

$$\mathbb{Z}[G]^\times \xrightarrow{\sim} \{\pm 1\} \times \prod_{i=1}^{n} U_i^{\binom{n}{i}}. \qquad \square$$

Let G be a cyclic group. Then $U_1 = \mathbb{Z}[G]^\times/\{\pm 1\}$ and we obtain the independent system of $\mathbb{Z}[G]^\times$ *i.e.* the independent system of U_1. (cf. [1], [2]) In particular, if the order of G is prime, then we get some results on the fundamental system of $\mathbb{Z}[G]^\times$ (cf. [2]). Let G be a cyclic group of prime order $p > 2$ and let $\phi : \mathbb{Z}[G] \to \mathbb{Z}[\zeta]$ be the homomorphism defined by $g \mapsto \zeta$, where g is a generator of G. For any unit u of $\mathbb{Z}[G]$, $\phi(u) \equiv \pm 1 \bmod (\lambda)$ *i.e.* the restriction of ϕ to $\mathbb{Z}[G]^\times$ is nothing but the isomorphism of Lemma 2.3. Put $\overline{u} = \phi(u)$.

Let $G = \mathbb{Z}/p \times \mathbb{Z}/p$. We have rank $U_2 = \frac{1}{2}(p-3)(p-1)$ by Lemma 2.1. Therefore we can expect to construct independent $\frac{1}{2}(p-3)(p-1)$ units of U_2.

We put $H = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. The isomorphism $\varphi : \mathbb{Q}(\zeta) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta) \xrightarrow{\sim} \prod_{\sigma \in H} \mathbb{Q}(\zeta)$ defined by $\varphi((\sum a_{ij}\zeta^i \otimes \zeta^j)) = \prod_{\sigma \in H}(\sum a_{ij}\zeta^i \sigma(\zeta^j))$ induces an injection $\varphi : \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta] \to \prod_{\sigma \in H} \mathbb{Z}[\zeta]$.

THEOREM 2.4. *Let $G = \mathbb{Z}/p \times \mathbb{Z}/p$ and let $r_1 = \frac{1}{2}(p-3)$. We take an independent system $\{u_i | 1 \le i \le r_1\}$ of the units in $\mathbb{Z}[\mathbb{Z}/p]$ and let $\overline{u_i}$ is image of u_i in $\mathbb{Z}[\zeta]$ i.e. $\{\overline{u_i} | 1 \le$*

$i \le r_1\}$ is an independent system of U_1. Then $\{\overline{u_i}_{(j)} | 1 \le i \le r_1, 1 \le j \le p-1\}$ is an independent system of U_2, where $\overline{u_i}_{(j)} := \varphi^{-1}((1, \cdots, 1, \underset{\hat{j}}{\overline{u_i}}, 1, \cdots, 1))$.

3. The proof of Theorem 2.4.

Let φ be the homomorphism as in section 2. At first, we prove some lemmas for the proof of Theorem 2.4.

LEMMA 3.1. *We employ*

$$\{\zeta\mathbf{e}_1, \zeta^2\mathbf{e}_1, \cdots, \zeta^{p-1}\mathbf{e}_1, \zeta\mathbf{e}_2, \cdots, \zeta^{p-1}\mathbf{e}_{p-1} | \mathbf{e}_i = (0, \cdots, 0, \overset{i}{\check{1}}, 0, \cdots, 0\}$$

and

$$\{\zeta \otimes \zeta, \zeta^2 \otimes \zeta, \cdots, \zeta^{p-1} \otimes \zeta, \zeta \otimes \zeta^2, \cdots, \zeta^{p-1} \otimes \zeta^{p-1}\}$$

as bases of $\mathbb{Z}$-modules $(\mathbb{Z}[\zeta])^{p-1}$ and of $\mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$, respectively. Then the matrix representation A_φ of the injective homomorphism φ is

$$A_\varphi = (A_{ij})_{1 \le i,j \le p-1}$$

where for each i, j, $A_{ij} = (a_{(i-1)(p-1)+k,(j-1)(p-1)+\ell})_{1 \le k,\ell \le p-1} \in M(p-1, \mathbb{Z})$ and

$$a_{(i,k,j,\ell)} := a_{(i-1)(p-1)+k,(j-1)(p-1)+\ell} = \begin{cases} 1, & \text{if } ij + \ell \equiv k \bmod p, \\ -1, & \text{if } ij + \ell \equiv 0 \bmod p, \\ 0, & \text{otherwise}. \end{cases}$$

Then the inverse matrix B of A_φ is as follows:

$$B = (B_{j'i'})_{1 \le i',j' \le p-1}$$

where for each i', j', $B_{j'i'} = (b_{(j'-1)(p-1)+\ell',(i'-1)(p-1)+k'})_{1 \le \ell',k' \le p-1}$ and

$$b_{(j',\ell',i',k')} := b_{(j'-1)(p-1)+\ell',(i'-1)(p-1)+k'} = \begin{cases} \frac{1}{p}, & \text{if } i'j' + \ell' \equiv k' \bmod p, \\ -\frac{1}{p}, & \text{if } k' = \ell' \text{ or else } i'j' = k', \\ -\frac{2}{p}, & \text{if } k' = \ell' \text{ and } i'j' = k', \\ 0, & \text{otherwise}. \end{cases}$$

PROOF. Since $\sum_{j=0}^{p-1} \zeta^j = 0$, it is trivial that A_φ is the matrix of the representation of φ. We prove that

$$\sum_{j,\ell} a_{(i,k,j,\ell)} b_{(j,\ell,i',k')} = \sum_{\substack{j,\ell \\ ij+\ell \equiv k}} b_{(j,\ell,i',k')} - \sum_{\substack{j,\ell \\ ij+\ell \equiv 0}} b_{(j,\ell,i',k')}$$
$$= \delta_{i,i'}\delta_{k,k'}.$$

When $i = i'$ and $k = k'$, then

$$\sum_{\substack{j,\ell \\ ij+\ell\equiv k}} b_{(j,\ell,i,k)} = (p-2)\frac{1}{p}\,,$$

$$\sum_{\substack{j,\ell \\ ij+\ell\equiv 0}} b_{(j,\ell,i,k)} = 2\left(-\frac{1}{p}\right)\,.$$

Hence $\sum_{j,\ell} a_{(i,k,j,\ell)} b_{(j,\ell,i,k)} = 1$.

When $i = i'$ and $k \neq k'$, then

$$\sum_{\substack{j,\ell \\ ij+\ell\equiv k}} b_{(j,\ell,i,k')} = 2\left(-\frac{1}{p}\right)\,,$$

$$\sum_{\substack{j,\ell \\ ij+\ell\equiv 0}} b_{(j,\ell,i,k')} = 2\left(-\frac{1}{p}\right)\,.$$

Hence $\sum_{j,\ell} a_{(i,k,j,\ell)} b_{(j,\ell,i,k')} = 0$.

When $i \neq i'$ and $k = k'$, then

$$\sum_{\substack{j,\ell \\ ij+\ell\equiv k}} b_{(j,\ell,i',k)} = -\frac{1}{p}\,,$$

$$\sum_{\substack{j,\ell \\ ij+\ell\equiv 0}} b_{(j,\ell,i',k)} = \frac{1}{p} + 2\left(-\frac{1}{p}\right)\,.$$

Hence $\sum_{j,\ell} a_{(i,k,j,\ell)} b_{(j,\ell,i',k)} = 0$.

When $i \neq i'$ and $k \neq k'$, then

$$\sum_{\substack{j,\ell \\ ij+\ell\equiv 0}} b_{(j,\ell,i',k')} = \frac{1}{p} + 2\left(-\frac{1}{p}\right)\,.$$

And if we put

$$N = \sharp\{(j,\ell) | ij+\ell \equiv k \bmod p,\, i'j+\ell \equiv k' \bmod p\}\,,$$
$$N' = \sharp\{(j,\ell) | ij+\ell \equiv k \bmod p,\, i'j \equiv k' \bmod p\}\,,$$

then

$$\sum_{\substack{j,\ell \\ ij+\ell\equiv k}} b_{(j,\ell,i',k')} = N\left(\frac{1}{p}\right) + (N'+1)\left(-\frac{1}{p}\right)\,.$$

Hence

$$\sum_{j,\ell} a_{(i,k,j,\ell)} b_{(j,\ell,i',k')} = \frac{N-N'}{p}\,.$$

It is sufficient to prove that $N = N'$. We may assume that $i = 1$. Note that the number of the solutions of congruence equations in j and ℓ for given i', k, k' $j + \ell \equiv k \bmod p$ and $i'j \equiv k' \bmod p$ is one at most. Suppose that $(\alpha, \beta) \in \{(j, \ell) | j + \ell \equiv k \bmod p, i'j + \ell \equiv k' \bmod p\}$. We put γ such that $i'\gamma \equiv -\beta \bmod p$. Since $i \neq i'$, $k \neq k'$ and $\gamma \not\equiv 0, \alpha, \beta$. And

$$\begin{aligned} i'(\alpha - \gamma) &= i'\alpha - i'\gamma \\ &\equiv i'\alpha + \beta \\ &\equiv k' \bmod p\,. \end{aligned}$$

Hence $(\alpha - \gamma, \beta + \gamma) \in \{(j, \ell) | j + \ell \equiv k \bmod p, i'j \equiv k' \bmod p\}$. Conversely, we assume that $(\alpha', \beta') \in \{(j, \ell) | j + \ell \equiv k \bmod p, i'j \equiv k' \bmod p\}$. We put γ' such that $(i' - 1)\gamma \equiv -\beta \bmod p$. Since $i' - 1 \equiv 0, p - 1 \bmod p, \gamma \not\equiv 0, -\alpha', \beta$ '. And

$$\begin{aligned} i'(\alpha' + \gamma') + (\beta' - \gamma') &= i'\alpha' + i'\gamma' + \beta' - \gamma' \\ &\equiv i'\alpha' + (-\beta' + \gamma') + \beta' - \gamma' \\ &\equiv i'\alpha' \\ &\equiv k' \bmod p \end{aligned}$$

Hence $(\alpha' + \gamma', \beta' - \gamma') \in \{(j, \ell) | j + \ell \equiv k \bmod p, i'j + \ell \equiv k' \bmod p\}$. Therefore $N = N'$. □

By the definitions of the elements of A_{ij} (resp. B_{ij}), if $i \cdot j \equiv i' \cdot j' \bmod p$, then $A_{ij} = A_{i'j'}$ (resp. $B_{ij} = B_{i'j'}$). Therefore if we define A_k (resp. B_k) by A_{ij} (resp. B_{ij}) with $1 \leq k \leq p - 1$ and $k \equiv i \cdot j \bmod p$, then

$$A_\varphi = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1,p-1} \\ A_{21} & A_{22} & \cdots & A_{2,p-1} \\ \vdots & \vdots & & \vdots \\ A_{p-1,1} & A_{p-1,2} & \cdots & A_{p-1,p-1} \end{pmatrix} = \begin{pmatrix} A_1 & A_2 & \cdots & A_{p-1} \\ A_2 & A_4 & \cdots & A_{p-2} \\ \vdots & \vdots & & \vdots \\ A_{p-1} & A_{p-2} & \cdots & A_1 \end{pmatrix}$$

$$\left(resp.\ B = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1,p-1} \\ B_{21} & B_{22} & \cdots & B_{2,p-1} \\ \vdots & \vdots & & \vdots \\ B_{p-1,1} & B_{p-1,2} & \cdots & B_{p-1,p-1} \end{pmatrix} = \begin{pmatrix} B_1 & B_2 & \cdots & B_{p-1} \\ B_2 & B_4 & \cdots & B_{p-2} \\ \vdots & \vdots & & \vdots \\ B_{p-1} & B_{p-2} & \cdots & B_1 \end{pmatrix} \right).$$

Moreover, the matrices $A_1, A_2, \cdots, A_{p-1}$ satisfy the following properties.

(1) $|A_i| = 1$ for any $1 \leq i \leq p - 1$.

(2) $A_i A_j = A_j A_i = A_{i+j}$ for any $1 \leq i, j \leq p - 1$. In particular $A_i = A_1^i$.

Moreover, we have the following relation between the determinant of A_φ and the discriminant of $\mathbb{Q}(\zeta)$.

THEOREM 3.2.

$$\det(A_\varphi) = p^{\frac{1}{2}(p-1)(p-2)} = (|\textit{The discriminant of}\, \mathbb{Q}(\zeta)|)^{\frac{1}{2}(p-1)}\,.$$

Here A_φ is the representation matrix of φ in Lemma 3.1.

PROOF. More generally (the discriminant of $\mathbb{Q}(\zeta_n)$)$= \pm p^{p^{n-1}(pn-n-1)}$, where ζ_n is a primitive p^n-th root of unity and we have the sign $-$ if $p^n = 4$ or if $p \equiv 3 \bmod 4$ and we have $+$ otherwise (cf. [6, Prop. 2.1]). Hence, it is sufficient to show that

$$\begin{vmatrix} E_n & E_n & \cdots & E_n \\ M_1 & M_2 & \cdots & M_m \\ M_1^2 & M_2^2 & \cdots & M_m^2 \\ \vdots & \vdots & & \vdots \\ M_1^{m-1} & M_2^{m-1} & \cdots & M_m^{m-1} \end{vmatrix} = \prod_{i<j} |(M_j - M_i)|$$

for $M_1, \cdots, M_m$ are $n \times n$ matrices such that $M_i M_j = M_j M_i$ and E_n is $n \times n$ unit matrix. In fact, if $n = p-1,\ m = p,\ M_1 = \mathbf{0}$ and $M_\ell = A_1^{\ell-1}$ for $2 \leq \ell \leq p$, then

$$\det(A_\varphi) = \Bigg(\prod_{1 \leq i < j \leq p-1} |(A_1^j - A_1^i)| \Bigg) |A_1| \cdots |A_1^{p-1}| .$$

Since $|A_1^m - E_{p-1}| = p$ for $1 \leq m \leq p-1$, it follows that $\det(A_\varphi) = p^{\frac{1}{2}(p-1)(p-2)}$. □

We can get units of $\mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$ as the inverse images of units of $\prod \mathbb{Z}[\zeta]$ by the isomorphism φ. Moreover, we see that the units must be in U_2. Now, we prepare the following lemma.

LEMMA 3.3. *Let $\alpha, \beta \in \{1, 2\}$ and $\alpha \neq \beta$. We put*

$$S_1 = \left\{ \sum a_{i_1 i_2} \zeta^{i_1} \otimes \zeta^{i_2} \in \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta] \,\middle|\, \sum a_{i_1 i_2} \zeta^{i_1} \otimes \zeta^{i_2} \equiv 1 \otimes 1 \bmod \lambda \otimes 1 \right\} \subset \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta] ,$$

$$S_2 = \left\{ \sum a_{i_1 i_2} \zeta^{i_1} \otimes \zeta^{i_2} \in \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta] \,\middle|\, \sum a_{i_1 i_2} \zeta^{i_1} \otimes \zeta^{i_2} \equiv 1 \otimes 1 \bmod 1 \otimes \lambda \right\} \subset \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta] .$$

Then following three conditions are equivalent for

$$\sum_{0 \leq i_1, i_2 \leq p-2} a_{i_1 i_2} \zeta^{i_1} \otimes \zeta^{i_2} = \sum_{1 \leq i'_1, i'_2 \leq p-1} a'_{i'_1 i'_2} \zeta^{i'_1} \otimes \zeta^{i'_2} \in \mathbb{Z}[\zeta] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta] .$$

(1) $S_\alpha \ni \displaystyle\sum_{0 \leq i_1, i_2 \leq p-2} a_{i_1 i_2} \zeta^{i_1} \otimes \zeta^{i_2} = \sum_{1 \leq i'_1, i'_2 \leq p-1} a'_{i'_1 i'_2} \zeta^{i'_1} \otimes \zeta^{i'_2}$.

(2) $\displaystyle\sum_{i_\alpha = 0}^{p-2} a_{i_1 i_2} \equiv \begin{cases} 1 \bmod p & (i_\beta = 0) , \\ 0 \bmod p & (i_\beta \neq 0) . \end{cases}$

(3) $\displaystyle\sum_{i'_\alpha = 1}^{p-1} a'_{i'_1 i'_2} \equiv p - 1 \bmod p$ *for any* i'_β.

PROOF. It is sufficient to prove them for $\alpha = 1, \beta = 2$. (1) $\Rightarrow$ (2) :

$$\sum a_{i_1 i_2}\zeta^{i_1} \otimes \zeta^{i_2} \equiv 1 \otimes 1 \bmod \lambda \otimes 1$$

$$\Leftrightarrow 1 \otimes 1 + (\lambda \otimes 1)\sum c_{i_1 i_2}\zeta^{i_1} \otimes \zeta^{i_2} = \sum a_{i_1 i_2}\zeta^{i_1} \otimes \zeta^{i_2} \text{ for some } c_{i_1 i_2} \in \mathbb{Z}\,.$$

Hence if $i_2 = 0$,

$$\begin{aligned}\sum_{i_1=0}^{p-2} a_{(i_1)0} &= 1 - \sum_{i_1=0}^{p-2} c_{(i_1)0} + \sum_{i_1=0}^{p-3} c_{(i_1)0} - (p-1)c_{(p-2)0} \\ &\equiv 1 \bmod p\,.\end{aligned}$$

And if $i_2 \neq 0$,

$$\begin{aligned}\sum_{i_1=0}^{p-2} a_{i_1 i_2} &= -\sum_{i_1=0}^{p-2} c_{i_1 i_2} + \sum_{i_1=0}^{p-3} c_{i_1 i_2} - (p-1)c_{(p-2)i_2} \\ &\equiv 0 \bmod p\,.\end{aligned}$$

(2) $\Rightarrow$ (1) : Let $\mathbb{Z}[\zeta] \ni \sum_{i=0}^{p-2} a_i\zeta^i$. Assume that $\sum_{i=0}^{p-2} a_i\zeta^i \equiv 0 \bmod (\zeta - 1)$. Since

$$\sum_{i=0}^{p-2} a_i\zeta^i = (\zeta - 1)\left\{a_{p-2}\zeta^{p-3} + (a_{p-2} + a_{p-3})\zeta^{p-4} + \cdots + \left(\sum_{i=1}^{p-2} a_i\right)\right\} + \sum_{i=0}^{p-2} a_i\,,$$

the assumption is equivalent to $\sum_{i=0}^{p-2} a_i \equiv 0 \bmod p$.

(2) $\Leftrightarrow$ (3) : Since $\sum_{i=0}^{p-1} \zeta = 0$, it is obvious. □

For the matrix B, we have equations similar to these in Lemma 3.3(3).

LEMMA 3.4. *Let* $\mathbf{b}_{i,k} = (b_{(i-1)p+k,1} \cdots b_{(i-1)p+k,(p-1)^2})$ *be the* $(i-1)p + k$*-th row of inverse matrix of* A_φ. *We consider* $\sum_{1 \le k \le p-1} \mathbf{b}_{i,k}$ *for any* i. *Then* $p - 1$ *elements of these vectors are* -1 *and others are* 0. *It is similarly about* $\sum_{1 \le i \le p-1} \mathbf{b}_{i,k}$.

We begin to prove Theorem 2.4.

We put

$$S = \left\{(\alpha_i)_{1 \le i \le p-1} \in \left(\prod_{\sigma \in H} \mathbb{Z}[\zeta]\right) \middle|\, \alpha_i \equiv 1 \bmod \lambda^2 \text{ for any } i\right\} \supset \varphi(U_2)\,.$$

At first, we fix an independent unit $u_i \in \{u_i | 1 \le i \le r_1\}$ of $\mathbb{Z}[\mathbb{Z}/p]^\times$. Since $(\lambda)^{p-1} = (p)$, $(\overline{u_i}^p, 1, \cdots, 1) \in S$. As

$$\begin{aligned}\overline{u_i}^p &= 1 + p\sum_{i=0}^{p-2} a_i\zeta^i \\ &= -\zeta - \zeta^2 - \cdots - \zeta^{p-1} + p\sum_{i=1}^{p-1} b_i\zeta^i\,,\end{aligned}$$

and the components of the inverse matrix of A_φ are $\frac{a}{p}$ ($a \in \{1, 0, -1, -2\}$) by Lemma 3.1, $\varphi^{-1}((\overline{u_i}^p, 1, \cdots, 1)) \in \varphi^{-1}(S)$. We put S_1 and S_2 as above. Then by Lemma 3.4 and Lemma 3.3, $\varphi^{-1}((\overline{u_i}^p, 1, \cdots, 1)) \in S_1 \cap S_2$ *i.e.* $\varphi^{-1}((\overline{u_i}^p, 1, \cdots, 1)) \equiv 1 \otimes 1 \bmod \lambda \otimes \lambda$. We obtain the units $\varphi^{-1}((1, \overline{u_i}^p, \cdots, 1)), \cdots, \varphi^{-1}((1, \cdots, 1, \overline{u_i}^p, 1))$ and $\varphi^{-1}((1, \cdots, 1, \overline{u_i}^p))$ similarly. This argument can be applied to any elements of $\{u_i | 1 \leq i \leq r_1\}$. Then we can get $r_1(p-1)$ units. Since $r_1 \times 2 + r_1(p-1) = \frac{1}{2}(p-3)(p+1)$, it is sufficient to prove that these units are independence. Assume that $\prod_{\substack{1 \leq i \leq r \\ 1 \leq j \leq p-1}} \overline{u_{i\,(j)}}^{\alpha_{ij}} = 1 \otimes 1$. Since φ is an injective homomorphism,

$$\varphi\left(\left(\prod_{\substack{1 \leq i \leq r \\ 1 \leq j \leq p-1}} \overline{u_{i\,(j)}}^{\alpha_{i1}}\right)\right) = \left(\prod_{1 \leq i \leq r} \overline{u_i}^{\alpha_{i1}}, \prod_{1 \leq i \leq r} \overline{u_i}^{\alpha_{i2}}, \cdots, \prod_{1 \leq i \leq r} \overline{u_i}^{\alpha_{ir}}, \right) = (1, 1, \cdots, 1).$$

By the independence of units $\{u_1, \cdots, u_r\}$, $\alpha_{ij} = 0$ for any i and j. Hence these $\frac{1}{2}(p-3)(p-1)$ units are independent. □

REMARK. We have to consider the fundamental units u_i satisfying $u_i \equiv 1 \bmod \lambda^2$ for constructing a fundamental system of U_2.

4. Examples.

In this section, we construct a fundamental system of units in the group ring $\mathbb{Z}[G]$ for some groups G. We define

$$\overline{u}_{(n_1, \cdots, n_r)} := \varphi^{-1}(\overline{u}^{n_1}, \cdots, \overline{u}^{n_r})$$

for any units $u \in \mathbb{Z}[\mathbb{Z}/p]^\times$ and integers n_j, where φ is the homomorphism in the section 2. In particular,

$$\overline{u_{i\,(j)}} = \overline{u_i}_{(0, \cdots, 0, \overset{j}{\check{p}}, 0, \cdots, 0)}$$

for a fundamental unit $\overline{u_i}$.

First, let $G = \mathbb{Z}/5 \times \mathbb{Z}/5$.

LEMMA 4.1. *We consider the fixed fundamental unit* $u = g^3 + g^2 - 1 \in \mathbb{Z}[\mathbb{Z}/5]^\times$, *where* g *is a fixed generator of* $\mathbb{Z}/5$ (*cf.* [2, Example 15.4]). *Let* $\phi : \mathbb{Z}[\mathbb{Z}/5] \to \mathbb{Z}[\zeta]$ *be a homomorphism defined by* $g \mapsto \zeta$. *For* $(\phi(u))^i = \sum_{j=1}^{4} a_{(i)j} \zeta^j$, *the following hold.*

(1) *If* $j + j' \equiv 0 \bmod 5$, *then* $a_{(i)j} = a_{(i)j'}$,

(2) $a_{(i)1} \equiv -1 + 2i \bmod 5$ *and* $a_{(i)2} \equiv -1 + 3i \bmod 5$.

PROOF. Note that $u^{-1} = g^4 + g - 1$. Therefore it is sufficient to prove the assertions for $i \geq 1$. Since $\phi(u) = \zeta + 2\zeta^2 + 2\zeta^3 + \zeta^4$, the assertions hold for $i = 1$. We assume that the assertions are true for $i \leq k-1$. Then

$$
\begin{aligned}
(\phi(u))^k &= \Big(\sum_{j=1}^{4} a_{(k-1)j}\zeta^j\Big)(\zeta+2\zeta^2+2\zeta^3+\zeta^4) \\
&= -a_{(k-1)2}\zeta + \{-3a_{(k-1)2}+a_{(k-1)1}\}\zeta^2 + \{-3a_{(k-1)2}+a_{(k-1)1}\}\zeta^3 - a_{(k-1)2}\zeta^4 .
\end{aligned}
$$

Hence

$$
\begin{aligned}
a_{(k)1} &= -a_{(k-1)2} \equiv -1+2k \mod 5 , \\
a_{(k)2} &= -3a_{(k-1)2}+a_{(k-1)1} \equiv -1+3k \mod 5 .
\end{aligned}
$$

□

By Lemma 3.1, we have

$$
A_\varphi = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & A_4 & A_1 & A_3 \\ A_3 & A_1 & A_4 & A_2 \\ A_4 & A_3 & A_2 & A_1 \end{pmatrix} ,
$$

where

$$
A_1 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix} , \quad A_2 = \begin{pmatrix} 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix} ,
$$

$$
A_3 = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_4 = \begin{pmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}
$$

and

$$
B = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 \\ B_2 & B_4 & B_1 & B_3 \\ B_3 & B_1 & B_4 & B_2 \\ B_4 & B_3 & B_2 & B_1 \end{pmatrix} ,
$$

where

$$
B_1 = \begin{pmatrix} -\frac{2}{5} & \frac{1}{5} & 0 & 0 \\ -\frac{1}{5} & -\frac{1}{5} & \frac{1}{5} & 0 \\ -\frac{1}{5} & 0 & -\frac{1}{5} & \frac{1}{5} \\ -\frac{1}{5} & 0 & 0 & -\frac{1}{5} \end{pmatrix} , \quad B_2 = \begin{pmatrix} -\frac{1}{5} & -\frac{1}{5} & \frac{1}{5} & 0 \\ 0 & -\frac{2}{5} & 0 & \frac{1}{5} \\ 0 & -\frac{1}{5} & -\frac{1}{5} & 0 \\ \frac{1}{5} & -\frac{1}{5} & 0 & -\frac{1}{5} \end{pmatrix} ,
$$

$$
B_3 = \begin{pmatrix} -\frac{1}{5} & 0 & -\frac{1}{5} & \frac{1}{5} \\ 0 & -\frac{1}{5} & -\frac{1}{5} & 0 \\ \frac{1}{5} & 0 & -\frac{2}{5} & 0 \\ 0 & \frac{1}{5} & -\frac{1}{5} & -\frac{1}{5} \end{pmatrix} \quad \text{and} \quad B_4 = \begin{pmatrix} -\frac{1}{5} & 0 & 0 & -\frac{1}{5} \\ \frac{1}{5} & -\frac{1}{5} & 0 & -\frac{1}{5} \\ 0 & \frac{1}{5} & -\frac{1}{5} & -\frac{1}{5} \\ 0 & 0 & \frac{1}{5} & -\frac{2}{5} \end{pmatrix} .
$$

By the above matrix and Lemma 4.1,

$$\varphi((\mathbb{Z}[\zeta]\otimes\mathbb{Z}[\zeta])^{\times}) \ni (\overline{u}^a,\overline{u}^b,\overline{u}^c,\overline{u}^d) \Leftrightarrow a+2b+3c+4d \equiv 0 \bmod 5\,.$$

And by Lemma 3.3,

$$\varphi^{-1}((\overline{u}^a,\overline{u}^b,\overline{u}^c,\overline{u}^d)) \equiv 1\otimes 1 \bmod \lambda\otimes\lambda \Leftrightarrow a+b+c+d \equiv 0 \bmod 5 \quad \text{and } a+4b+4c+d \equiv 0 \bmod 5\,.$$

Hence $\{(\overline{u},\overline{u}^2,\overline{u}^3,\overline{u}^4), (1,\overline{u}^5,1,1), (1,1,\overline{u}^5,1), (1,1,1,\overline{u}^5)\}$ forms a generating system of U_2. In fact, for any

$$(\overline{u}^a,\overline{u}^b,\overline{u}^c,\overline{u}^d) \in U_2\,,$$

we can write

$$(\overline{u}^a,\overline{u}^b,\overline{u}^c,\overline{u}^d) = (\overline{u},\overline{u}^2,\overline{u}^3,\overline{u}^4)^a(1,\overline{u}^5,1,1)^{\frac{b-2a}{5}}(1,1,\overline{u}^5,0)^{\frac{c-3a}{5}}(1,1,1,\overline{u}^5)^{\frac{d-4a}{5}}\,.$$

By the conditions, $\frac{b-2a}{5}, \frac{c-3a}{5}, \frac{d-4a}{5} \in \mathbb{Z}$. Therefore we have the following.

EXAMPLE 4.2. Let $G=\mathbb{Z}/5\times\mathbb{Z}/5$ and let $u=g^3+g^2-1$. Then $\overline{u}$ is a fundamental unit of U_1 and

$$\{\overline{u}_{(1,2,3,4)}, \overline{u}_{(2)}, \overline{u}_{(3)}, \overline{u}_{(4)}\}$$

is a fundamental system of U_2.

Secondly, let $G=\mathbb{Z}/7\times\mathbb{Z}/7$. We get the fundamental units $u_1 = g^2-g+1$ *and* $u_2 = -g^5-g^4-g^3+2g+2$ of $\mathbb{Z}[\mathbb{Z}/7]$ by [2, Example 15.5]. Here g is the generator of $\mathbb{Z}/7$. We replace u_1 and u_2 by g^6u_1 and g^3u_2, respectively. Then $\overline{u_1}, \overline{u_2} \equiv 1 \bmod \lambda^2$.

LEMMA 4.3. *For any $n\in\mathbb{Z}$, we put*

$$\overline{u_i}^n = \sum_{j=1}^{6} a_{(n)j}\zeta^j\,.$$

Then $a_{(n)j} = a_{(n)7-j}$ and $a_{(n)3} \equiv 4 - a_{(n)1} - a_{(n)2}$ mod 7.

PROOF. Since $\overline{u_1} = 2\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+2\zeta^6$, $\overline{u_2} = \zeta^2+3\zeta^3+3\zeta^4+\zeta^5$ and $\mathrm{aug}(u_i)=1$, we get the assertion. □

REMARK. For any prime number $p\geq 5$, let $u=\sum_{i=1}^{p-1} a_i\zeta^i$ be a fundamental unit of $\mathbb{Z}[\mathbb{Z}/p]$ such that $a_j = a_{p-j}$ for any j. Then

$$a_{\frac{p-1}{2}} \equiv \frac{p-1}{2} - \left(\sum_{i=1}^{\frac{p-1}{2}-1} a_i\right) \bmod p\,.$$

By Lemma 3.1, we get the matrices

$$A = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 & A_5 & A_6 \\ A_2 & A_4 & A_6 & A_1 & A_3 & A_5 \\ A_3 & A_6 & A_2 & A_5 & A_1 & A_4 \\ A_4 & A_1 & A_5 & A_2 & A_6 & A_3 \\ A_5 & A_3 & A_1 & A_6 & A_4 & A_2 \\ A_6 & A_5 & A_4 & A_3 & A_2 & A_1 \end{pmatrix},$$

where

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_6 = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$B = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 \\ B_2 & B_4 & B_6 & B_1 & B_3 & B_5 \\ B_3 & B_6 & B_2 & B_5 & B_1 & B_4 \\ B_4 & B_1 & B_5 & B_2 & B_6 & B_3 \\ B_5 & B_3 & B_1 & B_6 & B_4 & B_2 \\ B_6 & B_5 & B_4 & B_3 & B_2 & B_1 \end{pmatrix},$$

where

$$B_1 = \begin{pmatrix} -\frac{2}{7} & \frac{1}{7} & 0 & 0 & 0 & 0 \\ -\frac{1}{7} & -\frac{1}{7} & \frac{1}{7} & 0 & 0 & 0 \\ -\frac{1}{7} & 0 & -\frac{1}{7} & \frac{1}{7} & 0 & 0 \\ -\frac{1}{7} & 0 & 0 & -\frac{1}{7} & \frac{1}{7} & 0 \\ -\frac{1}{7} & 0 & 0 & 0 & -\frac{1}{7} & \frac{1}{7} \\ -\frac{1}{7} & 0 & 0 & 0 & 0 & -\frac{1}{7} \end{pmatrix}, \quad B_2 = \begin{pmatrix} -\frac{1}{7} & -\frac{1}{7} & \frac{1}{7} & 0 & 0 & 0 \\ 0 & -\frac{2}{7} & 0 & \frac{1}{7} & 0 & 0 \\ 0 & -\frac{1}{7} & -\frac{1}{7} & 0 & \frac{1}{7} & 0 \\ 0 & -\frac{1}{7} & 0 & -\frac{1}{7} & 0 & \frac{1}{7} \\ 0 & -\frac{1}{7} & 0 & 0 & -\frac{1}{7} & 0 \\ \frac{1}{7} & -\frac{1}{7} & 0 & 0 & 0 & -\frac{1}{7} \end{pmatrix},$$

$$B_3 = \begin{pmatrix} -\frac{1}{7} & 0 & -\frac{1}{7} & \frac{1}{7} & 0 & 0 \\ 0 & -\frac{1}{7} & -\frac{1}{7} & 0 & \frac{1}{7} & 0 \\ 0 & 0 & -\frac{2}{7} & 0 & 0 & \frac{1}{7} \\ 0 & 0 & -\frac{1}{7} & -\frac{1}{7} & 0 & 0 \\ \frac{1}{7} & 0 & -\frac{1}{7} & 0 & -\frac{1}{7} & 0 \\ 0 & \frac{1}{7} & -\frac{1}{7} & 0 & 0 & -\frac{1}{7} \end{pmatrix}, \quad B_4 = \begin{pmatrix} -\frac{1}{7} & 0 & 0 & -\frac{1}{7} & \frac{1}{7} & 0 \\ 0 & -\frac{1}{7} & 0 & -\frac{1}{7} & 0 & \frac{1}{7} \\ 0 & 0 & -\frac{1}{7} & -\frac{1}{7} & 0 & 0 \\ \frac{1}{7} & 0 & 0 & -\frac{2}{7} & 0 & 0 \\ 0 & \frac{1}{7} & 0 & -\frac{1}{7} & -\frac{1}{7} & 0 \\ 0 & 0 & \frac{1}{7} & -\frac{1}{7} & 0 & -\frac{1}{7} \end{pmatrix},$$

$$B_5 = \begin{pmatrix} -\frac{1}{7} & 0 & 0 & 0 & -\frac{1}{7} & \frac{1}{7} \\ 0 & -\frac{1}{7} & 0 & 0 & -\frac{1}{7} & 0 \\ \frac{1}{7} & 0 & -\frac{1}{7} & 0 & -\frac{1}{7} & 0 \\ 0 & \frac{1}{7} & 0 & -\frac{1}{7} & -\frac{1}{7} & 0 \\ 0 & 0 & \frac{1}{7} & 0 & -\frac{2}{7} & 0 \\ 0 & 0 & 0 & -\frac{1}{7} & -\frac{1}{7} & -\frac{1}{7} \end{pmatrix} \text{ and } B_6 = \begin{pmatrix} -\frac{1}{7} & 0 & 0 & 0 & 0 & -\frac{1}{7} \\ \frac{1}{7} & -\frac{1}{7} & 0 & 0 & 0 & -\frac{1}{7} \\ 0 & \frac{1}{7} & -\frac{1}{7} & 0 & 0 & -\frac{1}{7} \\ 0 & 0 & \frac{1}{7} & -\frac{1}{7} & 0 & -\frac{1}{7} \\ 0 & 0 & 0 & \frac{1}{7} & -\frac{1}{7} & -\frac{1}{7} \\ 0 & 0 & 0 & 0 & \frac{1}{7} & -\frac{2}{7} \end{pmatrix}.$$

Then we can get a fundamental system of $\mathbb{Z}[\mathbb{Z}/7 \times \mathbb{Z}/7]^{\times}$.

EXAMPLE 4.4. Let $G = \mathbb{Z}/7 \times \mathbb{Z}/7$, $u_1 = g^2 - g + 1$, $u_2 = -g^5 - g^4 - g^3 + 2g + 2$, and let $u = u_1^4 u_2$. Then $\{\overline{u_1}, \overline{u_2}\}$ is a fundamental system of U_1 and

$$\{\overline{u_i}_{(1,2,3,4,5,6)}, \overline{u}_{(0,1,1,5,4,3)}, \overline{u}_{(0,0,1,4,3,6)}, \overline{u_1}_{(j)}, \overline{u_2}_{(j')} \mid 1 \le i \le 2, 2 \le j \le 6, 4 \le j' \le 6\}$$

is a fundamental system of U_2.

References

[1] H. BASS, The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups, Topology **4** (1966), 391–410.

[2] G. KARPILOVSKY, *Unit groups of group rings*, Longman Scientific and Technical (1989).

[3] T. SEKIGUCHI and N. SUWA, On the structure of the group scheme $\mathbb{Z}[\mathbb{Z}/p^n]^{\times}$, Compositio Math. **97** (1995), 253–271.

[4] N. SUWA and T. SEKIGUCHI, Unit group scheme of commutative ring (in Japanese), Dai2kai Tsudajuku-daigakuseisuuron shinpojiumu Tsudajukudaigaku suugaku.keisankikagakukenkyujo kenkyuushohou **13** (1997), 61–67.

[5] J. P. SERRE, *Algebraic Groups and Class Fields*, GTM**117**, Springer (1988).

[6] L. C. WASHINGTON, *Intoroduction to Cyclotomic Field second edition*, GTM**83**, Springer (1996).

Present Address:
DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE AND ENGINEERING,
CHUO UNIVERSITY, KASUGA, BUNKYO-KU, TOKYO, 112–8551 JAPAN.
e-mail: endo@grad.math.chuo-u.ac.jp