BULLETIN DE LA S. M. F.

DANIEL S. KUBERT

The Z/2 Z cohomology of the universal ordinary distribution

Bulletin de la S. M. F., tome 107 (1979), p. 203-224

<http://www.numdam.org/item?id=BSMF_1979__107__203_0>

Bull. Soc. math. France,
107, 1979, p. 203-224.

THE Z/2 Z COHOMOLOGY OF THE UNIVERSAL ORDINARY DISTRIBUTION

BY

DANIEL S. KUBERT (*)

RÉSUMÉ. — Nous donnons la structure de certains groupes de cohomologie associés à la distribution universelle ordinaire $U^k(N)$ sur $\mathbf{Q}^k/\mathbf{Z}^k$. Le sous-groupe $\pm$ id de $GL_k(\hat{\mathbf{Z}})$ opère sur U^k. Soit $N > 1$ et impaire, ou bien $4 \mid N$. Alors, pour $i = 0, 1$, le groupe $H^i(\pm \text{ id}, U^k(N))$ est un $GL_k(\mathbf{Z}/N\,\mathbf{Z})$-module trivial, de $\mathbf{Z}/2\,\mathbf{Z}$-rang égal à $2^{\nu(N)-1}$, où $\nu(N)$ est le nombre de facteurs premiers distincts de N. Les applications naturelles de $H^i(\pm \text{ id}, U^k(N))$ dans $H^i(\pm \text{ id}, U^k)$ sont injectives. Des résultats semblables sont aussi obtenus quand $N = 2M$, M impair, ainsi que d'autres résultats sur la structure de ces groupes de cohomologie, qui sont importants pour déterminer la 2-torsion dans le groupe des classes de diviseurs cuspidaux sur les courbes modulaires, ainsi que la 2-torsion dans les groupes de classes d'idéaux dans les corps cyclotomiques.

ABSTRACT. — We work out the structure of certain cohomology groups associated to $U^k(N)$, the universal ordinary distribution on $\mathbf{Q}^k/\mathbf{Z}^k$. The subgroup $\pm$ id of $GL_k(\hat{\mathbf{Z}})$ acts on U^k. Let $N > 1$, N odd, or let $4 \mid N$. Then for $i = 0, 1$ the group $H^i(\pm \text{ id}, U^k(N))$ is a trivial $GL_k(\mathbf{Z}/N\,\mathbf{Z})$-module of $\mathbf{Z}/2\,\mathbf{Z}$-rank equal to $2^{\nu(N)-1}$, where $\nu(N)$ is the number of distinct prime factors of N. The natural maps of $H^i(\pm \text{ id}, U^k(N))$ into $H^i(\pm \text{ id}, U^k)$ are injective. Similar results are also obtained when $N = 2M$, with M odd, as well as other results on the structure of such cohomology groups, which are important to determine the 2-torsion in the group of cuspidal divisor classes on modular curves, and 2-torsion in ideal class groups in cyclotomic fields.

In this paper, we continue to develop the ideas of [K 3], where we analysed the structure of the universal ordinary distribution U^k associated with the group $(\mathbf{Q}/\mathbf{Z})^k$. We know that U^k is a $GL_k(\hat{\mathbf{Z}})$-module, and we may, in particular, consider it as a group with $\pm$id acting upon it. We may then calculate the $\pm$id-cohomology of U^k.

(*) Texte reçu le 16 mai 1978.
Supported by N.S.F. grant, Sloan Fellow.
Daniel S. KUBERT, Mathematics Department, Cornell University, Ithaca, N.Y. 14853 (États-Unis).

We use the same notation as in [K 3]. Thus U^k is the injective limit of the level groups $U^k(N)$, and $H^*(\pm\mathrm{id}, U^k)$ is the injective limit of the groups $H^*(\pm\mathrm{id}, U^k(N))$. First we shall study the groups $H^*(\pm\mathrm{id}, U^k(N))$. The method used will be a genezalization of SINNOTT's [S]. Then we shall study the maps between the level groups which will depend on certain relative cohomology groups.

1. The rational distribution

Let k be a positive integer. We define the universal ordinary distribution on $(\mathbf{Q}/\mathbf{Z})^k$ as the free abelian group on $(\mathbf{Q}/\mathbf{Z})^k$ modulo the distribution relations, which are generated by

$$\sum_{Nb=a}(b)-(a), \tag{1.1}$$

with $a, b \in (\mathbf{Q}/\mathbf{Z})^k$, and N any postive integer. We denote the universal ordinary distribution by U^k. It is, in a natural way, a $GL_k(\hat{\mathbf{Z}})$-module, since $GL_k(\hat{\mathbf{Z}})$ leaves invariant the group generated by the distribution relations. We define $U^k(N)$ as the image of $((1/N)\,\mathbf{Z}/\mathbf{Z})^k$ in U^k. There is a canonical model for U^k which we have described in [K 3], and which we called the rational distribution. It is defined as follows.

Let $\mathbf{Q}^k(N)$ be the free $\mathbf{Q}$-vector space generated by the primitive elements of $((1/N)\,\mathbf{Z}/\mathbf{Z})^k$. Then $\mathbf{Q}^k(N)$ is a module over $GL_k(\hat{\mathbf{Z}})$, *via* the action of $GL_k(\mathbf{Z}/N\,\mathbf{Z})$. Let $M \mid N$. Then we have an injection

$$i: \quad \mathbf{Q}^k(M) \to \mathbf{Q}^k(N), \tag{1.2}$$

as $GL_k(\hat{\mathbf{Z}})$-modules, which is defined as follows. If x is a primitive element of $((1/M)\,\mathbf{Z}/\mathbf{Z})^k$ we set

$$i(x) = \sum_{(N/M)\,y=x}(y),$$

where y is a primitive element of $((1/N)\,\mathbf{Z}/\mathbf{Z})^k$. The map is clearly a $GL_k(\hat{\mathbf{Z}})$-morphism.

We define a map

$$r^k(N): \quad U^k(N) \to \mathbf{Q}^k(N),$$

as follows. Given $a \in (1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$, let $f(a)$ be the order of a in $((1/N)\,\mathbf{Z}/\mathbf{Z})^k$. We define

$$X(a) = \{\, b \in \mathbf{Z}^k/N\,\mathbf{Z}^k \text{ such that } b \text{ is primitive, and } (N/f(a))\,b \equiv N\,a \bmod N\,\mathbf{Z}^k \,\}. \tag{1.3}$$

Dividing by N yields a subset of $(1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$, which can be described as

$$\frac{1}{N}X(a) = \left\{ x \in \left(\frac{1}{N}\mathbf{Z}/\mathbf{Z}\right)^k \text{ such that } x \text{ is primitive, and } (N/f(a))\,x = a \right\}.$$

For simplicity, we abbreviate:

$$Z_k(N) = \left(\frac{1}{N}\mathbf{Z}/\mathbf{Z}\right)^k \quad \text{and} \quad Z_k^*(N) = \text{primitive elements in } Z(N).$$

We have a bijection

$$\mathbf{Z}_k^*(N) \to (\mathbf{Z}/N\,\mathbf{Z})^k,$$

obtained by the map $x \longrightarrow N\,x$. Write

$$N = \textstyle\prod_{p \mid N} p^{n(p)}.$$

Then we define an element $s_p(N) \in \mathrm{End}_{\mathbf{Q}}(\mathbf{Q}^k(N))$ by putting

$$s_p(N)(x) = \textstyle\sum(y), \tag{1.4}$$

where the sum is taken over those elements $y \in Z^*(N)$ such that

$$py \equiv x \bmod \frac{1}{p^{n(p)}}\mathbf{Z}^k.$$

Then $s_p(N)$ commutes with the action of $GL_k(\hat{\mathbf{Z}})$. Moreover, if $p \neq q$ are two primes dividing N, then $s_p(N)$, $s_q(N)$ commute.

If X is a subset of $Z^*(N)$ we let

$$s(X) = \textstyle\sum_{x \in X}(x).$$

We define an element $\gamma_p(N) \in \mathrm{End}_{\mathbf{Q}}(\mathbf{Q}^k(N))$ by

$$\gamma_p(N) = \mathrm{id} - \frac{1}{|Z^*(N)|}s_p(N). \tag{1.5}$$

Then we define $r(N)$ by

$$r(N)(a) = \left(\textstyle\prod_{p \mid f(a)} \gamma_p(N)\right).s(X(a)). \tag{1.6}$$

It is shown in [K 3] that $r(N)$ satisfies the distribution relations, and is consistent with injective limits. We thus get a map

$$r: \quad U^k \to \lim_N \mathbf{Q}^k(N),$$

which is in fact an isomorphism of $GL_k(\hat{\mathbf{Z}})$-modules after tensoring with $\mathbf{Q}$ (*see* [K 3]).

Let $C^k(N)$ be the non-split Cartan subgroup of $GL_k(\mathbf{Z}/N\mathbf{Z})$ that we considered in [K 3]. By definition, $C^k(N)$ is isomorphic to the units in the ring $\mathfrak{o}^k(N)$:

$$\mathfrak{o}^k(N) = \prod_{p \mid N} \mathfrak{o}_p^k / N\,\mathfrak{o}_p^k,$$

where $\mathfrak{o}_p^k$ is the ring of integers of the unramified extension of $\mathbf{Q}_p$, of degree k, together with a choice of basis for $\mathfrak{o}^k(N)$ as $\mathbf{Z}/N\mathbf{Z}$-module. Then $C^k(N)$ acts simply transitively on $Z_k^*(N)$ and we may identify the group ring $\mathbf{Q}[C^k(N)]$ with $\mathbf{Q}^k(N)$ as $C^k(N)$-modules. We also write

$$\frac{1}{N}\mathfrak{o}(N)/\mathfrak{o}(N) = \prod \frac{1}{p^{n(p)}}\mathfrak{o}_p/\mathfrak{o}_p.$$

Under the present identification, we now have

(1.7) $X(a) = \{c \in C(N)$ such that $(N/f(a))c_p \equiv (Na)_p \bmod p^{n(p)}\}$,

where $(Na) \in \mathfrak{o}^k(N)$ and $(Na)_p$ is the p-th component. We also define

(1.8) $X_p(N) = \{c = (c_q)_q \in C(N)$ such that if $q \neq p$, then $c_q \equiv p^{-1} \bmod q^{n(q)}\mathfrak{o}_q\}$.

Then we have

$$r(N)a = s(X(a))\prod_{p \mid f(a)}\left(1 - \frac{s(X_p(N))}{|X_p(N)|}\right), \tag{1.9}$$

We fix N and k in what follows. Since $r(N)$ is an isomorphism, by [K 3], we identify $U^k(N)$ with its image under $r(N)$. We shall describe a set of generators for $U^k(N)$ as a $C(N)$-module. We say that $M \mid N$ is admissible if $(M, N/M) = 1$. Then the distribution relations show that $U^k(N)$ is generated as a $\mathbf{Z}$-module by $r(N)\,b$, where $f(b)$ is admissible. For any element $c \in C(N)$ we have

$$cr(N)(b) = r(N)(cb).$$

From this we conclude that the family of elements

$$\left\{ r(N)\frac{1}{M} \text{ for } M \text{ admissible, } M \mid N \right\},$$

generates $U^k(N)$ as a $C(N)$-module. Here $1/M$ means the element with p-component $1/M$ for each $p \mid N$.

Let the integral group ring be $R(N) = \mathbf{Z}[C(N)$, $R_{\mathbf{Q}}(N) = \mathbf{Q}[C(N)]$. Let

$$U_p = s(X(p^{n(p)}/N))R(N) + \left(1 - \frac{s(X_p(N))}{|X_p|}\right)R(N). \tag{1.10}$$

In [K 3], we showed the following Proposition.

PROPOSITION 1.11:

(i) $U^k(N) = \prod_{p \mid N} U_p$.

(ii) $U_p \otimes \mathbf{Q} = R_{\mathbf{Q}}(N)$.

We may reinterpret this Proposition as follows. We identify $R(N)$ with the free $\mathbf{Z}$-module on $Z^*(N)$. Given $p \mid N$, we define an endomorphism t_p of $R(N)$ by

$$t_p(x) = \sum_y (y), \tag{1.12}$$

with the sum taken for $y \equiv x \bmod (1/p^{n(p)})\,\mathbf{Z}^k$ and $y \in Z^*(N)$. Then the endomorphisms t_p commute with $GL_k(\hat{\mathbf{Z}})$, and γ_q, and

$$U_p = t_p R(N) + \gamma_p R(N). \tag{1.13}$$

Set $\bar{N} = \prod p$, where the product is taken over all primes p dividing N. If $r \mid \bar{N}$, set

$$U_r = \prod_{p \mid r} U_p, \qquad U_1 = R(N), \qquad U_{\bar{N}} = U^k(N). \tag{1.14}$$

If $p \nmid r$, it follows that

$$U_{rp} = t_p U_r + \gamma_p U_r. \tag{1.15}$$

2. Structure of $H^*(\pm\mathrm{id}, U^k(N))$

In this section we determine the structure of $H^*(\pm\mathrm{id}, U^k(N))$ as a $GL_k(N)$-module. We make the assumption that either N is odd or $4 \mid N$. When $k = 1$ and N is odd, then $U^k(2N) = U^k(N)$. We will discuss $U^k(2N)$ in general in a latter section. Our analysis follows closely that of SINNOTT in [S].

Let $r \mid \bar{N}$. We define the subgroup C_r of $C^k(N)$ by

$$C_r = c \in C^k(N) \text{ such that } c_p \equiv 1 \bmod p^{n(p)} \text{ if } p \nmid r. \tag{2.1}$$

Then

$$X\left(\frac{p^{n(p)}}{N}\right) = C_p.$$

Set $r' = N/r$. Set

$$A_r^q = H^q(\pm\mathrm{id}, U_r^{C_{r'}}). \tag{2.2}$$

Then A_r^q is a $C(N)$-module, and for $r = \bar{N}$, it is a $GL_k(\hat{\mathbf{Z}})$-module. We have

$$C(N) = C_r \times C_{r'} \qquad \text{for} \quad r \mid \bar{N}. \tag{2.3}$$

We recall the following Lemma.

LEMMA 2.4. — *Let H and K be finite groups. If A is a free $H\times K$-module, then A^H and A/A^H are free K-modules.*

Proof. — *See* [S] for a proof.

LEMMA 2.5. — *If $p \mid N$, $p \nmid r$, then*

$$U_{rp}^{C_p} = s(C_p)\, U_r + \gamma_p\, U_r^{C_p}.$$

Proof. — We have

$$U_{rp} = s(C_p)\, U_r + \left(1 - \frac{s(X_p)}{|X_p|}\right) U_r.$$

Let ε_p be the idempotent of $R_{\mathbf{Q}}(N)$ associated with C_p. Then

$$U_{rp}^{C_p} = \mathrm{Ker}(1-\varepsilon_p) \mid U_{rp}.$$

The endomorphism γ_p may be identified with the element

$$1 - \frac{s(X_p)}{|X_p|},$$

of $R_{\mathbf{Q}}(N)$. But $(1-\varepsilon_p)\, s(C_p)\, U_r = 0$ and $(1-\varepsilon_p)\,\gamma_p = (1-\varepsilon_p)$. So

$$(1-\varepsilon_p)\, U_{rp} = (1-\varepsilon_p)\, U_r,$$

and the Lemma follows.

LEMMA 2.6. — *Let $rs \mid \bar{N}$. Then U_r is free as a C_s-module.*

If $rs \neq \bar{N}$, then U_r is free as a $\pm C_s$-module.

Proof. — We induct on r. When $r = 1$, then $U_r = R(N)$, which is free over any subgroup of $C(N)$.

Suppose now the Theorem is true for r, and let $p \mid \bar{N}$, $p \nmid r$. We prove that the Theorem is true for rp. Let $s \mid \bar{N}$ be such that $(rp, s) = 1$. Set

$$Y = (1-\varepsilon_p)\, U_{rp} = (1-\varepsilon_p)\, U_r.$$

We then have the exact sequences

$$0 \to U_r^{C_p} \to U_r \to Y \to 0 \tag{2.7}$$

$$0 \to U_{rp}^{C_p} \to U_{rp} \to Y \to 0.$$

By induction, U_r is a free $C_p \times C_s$-module. Thus by Lemma 2.4, $U_r^{C_p}$ and Y are free C_s-modules. Since U_r is a free C_p-module, it follows that

$$U_r^{C_p} = s(C_p)\, U_r,$$

and from Lemma 2.5 we have

$$U_{rp}^{C_p} = s(C_p)\, U_r + \gamma_p\, s(C_p)\, U_r.$$

Now $\gamma_p s(C_p) = (1-\lambda_p) s(C_p)$, where $\lambda_p \in C(N)$,

$$\lambda_p \equiv p^{-1} \bmod q^{n(q)} \quad \text{for all } q \neq p.$$

So

$$U_{rp}^{C_p} = U_r^{C_p} \qquad \text{and} \qquad U_{rp} \approx U_r^{C_p} \oplus Y,$$

which is a free C_s-module.

Suppose now that $rps \neq \bar{N}$. By induction, U_r is a free $\pm C_s C_p$-module. Since $\pm C_s \cap C_p = 1$ (here we use the fact that if $2 \mid N$ then $4 \mid N$ and $rps \neq \bar{N}$), we find that $U_r^{C_p}$ and Y are free $\pm C_s$-modules. The Lemma follows from (2.7) and the equality

$$U_{rp}^{C_p} = U_r^{C_p}.$$

COROLLARY 2.8. — *Let* $r \mid \bar{N}$, $s \mid (\bar{N}/r)$, *and* $rs \neq \bar{N}$. *Then*

$$H^q(\pm\mathrm{id}, U_r^{C_s}) = 0 \qquad \textit{for} \quad q = 0, 1.$$

Proof. — From Lemma 2.4 we find that $U_r^{C_s}$ is a free $\pm$id-module, whose cohomology is well known to be trivial.

COROLLARY 2.9:

(i) $C(N)$ *acts trivially on* A_r^q.

(ii) $GL_k(\mathbf{Z}/N\,\mathbf{Z})$ *acts trivially on* $H^q(\pm\mathrm{id}, U^k(N))$.

Proof. — For (i), we need only show that C_p acts trivially on A_r^q, since C_p generates $C(N)$. By definition,

$$A_r^q = H^q(\pm\mathrm{id}, U_r^{C_{r'}}).$$

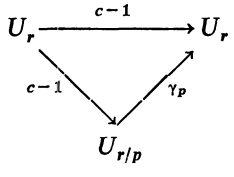
So if $p \nmid r$, the result is obvious. Suppose $p \mid r$. Then

$$U_r = s(C_p)\, U_{r/p} + \gamma_p\, U_{r/p}.$$

Let $c \in C_p$. Then $(c-1)\, s(C_p) = 0$, and $(c-1)\, \gamma_p = c-1$. Thus

$$(c-1)\, U_r \subset U_{r/p},$$

and we have a commutative diagram:



Taking $C_{r'}$-invariants, we see that (i) follows immediately from Corollary 2.8.

To prove (ii), we use (1.15). The group $GL_k(\mathbf{Z}/N\,\mathbf{Z})$ is the direct product of the groups G_p of those elements g such that $g \equiv 1 \bmod (N/p^{n_{(p)}})$. So suppose $g \in G_p$. Then

$$(g-1)\,t_p = 0, \qquad (g-1)\,\gamma_{p_i}^{\frac{p_i}{p}} = g-1.$$

So we have the commutative diagram

$$\begin{array}{ccc} U^k(N) & \xrightarrow{\quad g-1 \quad} & U^k(N) \\ & {\scriptstyle g-1}\searrow \quad \nearrow{\scriptstyle \gamma_p} & \\ & U_{\bar{N}/p} & \end{array}$$

and since $H^q(\pm\mathrm{id}, U_{\bar{N}/p}) = 0$ by Corollary 2.8, (ii) follows.

Thus to determine the structure of $H^q(\pm\mathrm{id}, U^k(N))$, it suffices to determine the order of $H^q(\pm\mathrm{id}, U^k(N))$. By **rank** we shall mean $\mathbf{Z}/2\,\mathbf{Z}$-rank.

PROPOSITION 2.10:

(i) *If* $N > 1$ *then*

$$\operatorname{rank} H^q(\pm\mathrm{id}, U^k(N)) = 2^{\nu-1},$$

where $\nu = \nu(N)$ *is the number of distinct prime factors of* N.

(ii) $H^0(\pm\mathrm{id}, U^k(1)) \approx \mathbf{Z}/2\,\mathbf{Z}$, $H^1(\pm\mathrm{id}, U^k(1)) = 0$.

Proof. — Note that (ii) follows from the fact that $U^k(1)$ is the free $\mathbf{Z}$-module on (0). To prove (i), we used the following Proposition.

PROPOSITION 2.11:

(i) *Let* $r \mid \bar{N}$, $r > 1$. *Then*

$$\operatorname{rank} A_r^q = 2^{\nu(r)-1}.$$

(ii) $A_1^0 = \mathbf{Z}/2\,\mathbf{Z}$ *and* $A_1^1 = 0$.

Proof. — The proof of (ii) is clear since

$$A_1^q = H^q(\pm\mathrm{id}, R(N)^{C(N)}),$$
$$R(N)^{C(N)} = \mathbf{Z}[s(C(N))] \qquad \text{and} \qquad (-1)\,s(C(N)) = s(C(N)).$$

The proof of (i) will follow by induction from the following Lemma.

LEMMA 2.12. — *Let* $rp \mid \bar{N}$, p *prime, and* $r \geqslant 1$. *There is an exact sequence*

$$0 \to A_r^q \to A_{rp}^q \to A_r^{q+1} \to 0.$$

Proof. – We know that $\gamma_p U_r \subset U_{rp}$. So from (2.7) we have the diagram

$$\begin{array}{ccccccccc} 0 & \to & U_r^{C_p} & \to & U_r & \xrightarrow{1-\varepsilon_p} & Y & \to & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \to & U_{rp}^{C_p} & \to & U_{rp} & \xrightarrow[1-\varepsilon_p]{} & Y & \to & 0 \end{array} \tag{2.13}$$

The vertical maps are induced by γ_p. Since

$$(1-\varepsilon_p)\gamma_p = (1-\varepsilon_p),$$

it follows that h is the identity map. Now as in Lemma 6,

$$U_r^{C_p} = U_{rp}^{C_p} = s(C_p)\, U_r \qquad \text{and} \qquad \gamma_p\, U_r^{C_p} = (1-\lambda_p)\, U_r^{C_p},$$

so f is multiplication by $1-\lambda_p$. Set $r' = \bar{N}/rp$. Then, since Lemma 2.6 shows that U_r, U_{rp}, $U_r^{C_p}$ are free $C_{r'}$-modules, we may take $C_{r'}$-invariants to get the diagram

$$\begin{array}{ccccccccc} 0 & \to & U_r^{C_{pr'}} & \to & U_r^{C_{r'}} & \xrightarrow{1-\varepsilon_p} & Y^{C_{r'}} & \to & 0 \\ & & {\scriptstyle 1-\lambda_p}\downarrow & & {\scriptstyle \gamma_p}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \to & U_r^{C_{pr'}} & \to & U_{rp}^{C_{r'}} & \xrightarrow[1-\varepsilon_p]{} & Y^{C_{r'}} & \to & 0 \end{array} \tag{2.14}$$

Taking cohomology, and omitting $\pm\mathrm{id}$ for the sake of typographical brevity, we get

$$\begin{array}{ccccccccccc} H^{q-1}(Y^{C_{r'}}) & \longrightarrow & A_r^q & \to & 0 & \to & H^q(Y^{C_{r'}}) & \longrightarrow & A_r^{q+1} & \to & 0 \\ {\scriptstyle \mathrm{id}}\downarrow & & {\scriptstyle 1-\lambda_p}\downarrow & & \downarrow & & {\scriptstyle \mathrm{id}}\downarrow & & {\scriptstyle 1-\lambda_p}\downarrow & & \\ H^{q-1}(Y^{C_{r'}}) & \longrightarrow & A_r^q & \to & A_{rp}^q & \to & H^q(Y^{C_{r'}}) & \longrightarrow & A_r^{q+1} & & \end{array} \tag{2.15}$$

The zeros occur because $U_r^{C_{r'}}$ is a free $\pm\mathrm{id}$-module. By Corollary 2.9 we know that the maps $1-\lambda_p$ are the zero maps. Thus A_r^q injects into A_{rp}^q, and A_{rp}^q surjects onto $H^q(Y^{C_{r'}})$. The top row shows that $H^q(Y^{C_{r'}})$ is isomorphic to A_r^{q+1}, which completes the proof of the Lemma.

Summarizing, we obtain the following Theorem.

THEOREM 2.16. – *Let N be an integer > 1. Then $H^q(\pm\mathrm{id}, U^k(N))$ is a trivial $GL_k(\mathbf{Z}/N\,\mathbf{Z})$-module of $\mathbf{Z}/2\,\mathbf{Z}$-rank equal to $2^{\nu(N)-1}$, where $\nu(N)$ is the number of prime factors of N.*

3. The relative cohomology groups

In this paper, we wish to determine what happens when we take the injective limit of the groups $H^q(\pm\mathrm{id}, U^k(N))$. Since we take cohomology

only with respect to the group $\pm\mathrm{id}$, we shall often omit this reference to $\pm\mathrm{id}$ for typographical simplicity.

To determine the injective limit, we clearly may restrict our attention again to the cases when N is odd, or when N is divisible by four. We begin with an interpretation of the groups A_r^q.

PROPOSITION 3.1. — *Let* $r \mid \bar{N}$ *and let* $M = \prod_{p \mid r} p^{n(p)}$. *Then*

(i) $U_r^{C_{r'}} = U^k(M) \subset U^k(N)$;

(ii) $A_r^q = H^q(\pm\mathrm{id}, U^k(M))$.

Proof. — Note that (ii) follows immediately from (i). From Lemma 2.6 we know that U_r is a free $C_{r'}$-module, so

$$U_r^{C_{r'}} = s(C_{r'})\, U_r.$$

Now

$$U_r = \prod_{p \mid r} U_p \qquad \text{and} \qquad s(C_{r'}) = \prod_{p \nmid r} s(C_p).$$

So

$$U_r^{C_{r'}} = \prod_{p \mid r} U_p \times \prod_{p \nmid r} s(C_p)\, R(N).$$

Since $s(C_p)\, R(N) \subset U_p$, and since

$$U^k(N) = \prod_{p \mid N} U_p,$$

it is clear that $U_r^{C_{r'}} \subset U^k(N)$. The above decomposition shows, in fact, by immediate inspection, that it is exactly $U^k(M)$.

Proposition 3.1 shows that $U_r^{C_{r'}}$ is actually a $GL_k(\hat{\mathbf{Z}})$-module, and that in Corollary 2.9 we may conclude that $GL_k(\hat{\mathbf{Z}})$ acts trivially on A_r^q.

Let us now reflect on Lemma 2.12. From (2.14) we see that the map from A_r^q to A_{rp}^q arises from the inclusion of $U_r^{C_{pr'}}$ in $U_{rp}^{C_{r'}}$.

In the light of Proposition 3.1, this says that if $p \mid N$, $p \nmid M$, then the inclusion

$$U^k(M) \subset U^k(p^{n(p)} M),$$

induces an injection of cohomology groups. By induction, we may conclude the following.

PROPOSITION 3.2. — *If* M *is an admissible divisor of* N, *then we have an injection*

$$0 \to H^q(\pm\mathrm{id}, U^k(M)) \to H^q(\pm\mathrm{id}, U^k(N)).$$

This Proposition leads one to suspect that not much collapse occurs in passing to the injective limit. Theorem 2.16 suggests that if $M \mid N$, and if M, N have the same prime factors (again we assume that if $2 \mid M$

then $4 \mid M$) then the natural maps on the cohomology groups are isomorphisms. We shall now show that this, in fact, is true.

PROPOSITION 3.3. — *Let $M \mid N$ be such that M, N have the same prime factors. Also assume that if $2 \mid M$, but $4 \nmid M$, then $4 \nmid N$. Then we have an isomorphism*

$$H^q(\pm\mathrm{id},\, U^k(M)) \approx H^q(\pm\mathrm{id},\, U^k(N)).$$

Proof. — The proof follows immediately from the fact that under the conditions of Proposition 3.3, the factor group $U^k(N)/U^k(M)$ can be resolved by a finite chain of acyclic $\pm$id-modules. We may use of the following Lemma.

LEMMA 3.4. — *Let F be a free $(\pm\mathrm{id})$-module, and let G be any $(\pm\mathrm{id})$-module. Then for any positive integer q, we have*

$$H^q(\pm\mathrm{id},\, F \otimes G) = 0.$$

Proof. — We may clearly assume that $F = \mathbf{Z}[\pm\mathrm{id}]$. Then we may represent elements of $F \otimes G$ by

$$z = (\mathrm{id}) \otimes x + (-\mathrm{id}) \otimes y,$$

with $x, y \in G$. The element is 0 if and only if $x = 0$ and $y = 0$. Suppose $z \in F \otimes G$ is such that $(-\mathrm{id})\, z = z$, and z is represented as above. Then

$$(\mathrm{id}) \otimes (x - (-\mathrm{id})\, y) + (-\mathrm{id}) \otimes (y - (-\mathrm{id})\, x) = 0.$$

So $y = (-\mathrm{id})\, x$ and $z = (\mathrm{id}) \otimes x + (-\mathrm{id})\,(\mathrm{id} \otimes x)$, and z is a coboundary. Thus $H^0(F \otimes G) = 0$. A similar argument shows that $H^1(F \otimes G) = 0$.

We now wish to prove Proposition 3.3. By induction we may assume that $p \mid M$ and $N = p\,M$ (here if $p = 2$ then $4 \mid M$). Let

$$N = \prod l^{n(l)}.$$

We define $D(N)$ to be the set of positive divisors of N. Given a subset S of $D(N)$, we define U_S to be the group generated by U_r, where $r \in S$. We say that S is normal if $r \in S$ and $r' \mid r$ imply that $r' \in S$. If $S \subset S'$ are normal, we say the pair (S, S') is normal if for all $r \in S'$, $r' \mid r$, and $r' \neq r$ implies that $r' \in S$. It suffices to show that if S and S' are a normal pair, then there is an isomorphism

$$H^q(U_S) \approx H^q(U_{S'}). \tag{3.5}$$

Indeed, we may produce a sequence $\{ S_i \}$, $i = 1, \ldots, n$ such that

$$S_{i+1} \supset S_i, \qquad S_0 = D(N), \qquad S_n = D(N),$$

and (S_i, S_{i+1}) is a normal pair. We do this as follows. If $S \subset S'$ are each normal, then there exists a sequence $\{S_i\}$ with (S_i, S_{i+1}) normal, such that $S_0 = S$ and $S_n = S'$. If not, there would be a minimal element T under inclusion for which this is not true. Then if we set

$$T' = \{r' \text{ such that } r' \mid r \text{ for } r \in T,\ r' \neq r\},$$

then $T' \cup S$ is normal, and $T' \cup S$ is properly contained in T. So there is a normal chain from S to $T' \cup S$. But $(T' \cup S, T)$ is a normal pair, which yields a contradiction.

To prove (3.5) we may choose S' to be $S \cup (m)$, where, m is such that if $m' \mid m$, $m' \neq m$, then $m' \in S$. This will suffice by induction. Since $M \subset S$, m must be of the form

$$m = \prod_{l \mid m} l^{m(l)},$$

where $m(l) \leqslant n(l)$ and $m(p) = n(p)$.

Let m be a positive integer. We define:

$$D'(m) = \{m' \in D(m) \text{ such that } m' \neq m\},$$
$$U'(m) = U_{D'(m)}.$$

Then we have a surjective homomorphism

$$\rho: \quad U(m)/U'(m) \to U_{S \cup (m)}/U_S. \tag{3.6}$$

We now give a nice description of $U(m)/U'(m)$. We have an isomorphism

$$\mathbf{Z}[C^k(m)] \approx \prod_{l \mid m} \mathbf{Z}[C^k(l^{m(l)})].$$

We define $G_l \subset C^k(l^{m(l)})$ for $l \mid m$ to be

$$G_l = \{c \in C^k(l^{m(l)}) \text{ such that } c \equiv 1 \bmod l^{m(l)-1}\}.$$

We then set

$$V_l = \mathbf{Z}[C^k(l^{m(l)})]/s(G_l)\,\mathbf{Z}[C^k(l^{m(l)})].$$

We now describe a map

$$\mathbf{i}: \quad \otimes_{l \mid m} V_l \to U(m)/U'(m).$$

Let $F^k(m)$ be the free abelian group on $Z^*(m)$. Division by m from $C^k(m)$ to $Z^*(m)$ induces an isomorphism

$$\mathbf{Z}[C^k(m)] \to F^k(m).$$

This gives rise to a natural homomorphism

$$\tilde{\mathbf{i}}: \quad \mathbf{Z}[C^k(m)] \to U(m)/U'(m).$$

From the distribution relations and the fact that the image of i is in $U(m)/U'(m)$, it is immediate that i is trivial on

$$s(G_q) \otimes \otimes_{l \neq q} V_l.$$

Hence $\tilde{\mathbf{i}}$ factors through a homomorphism $\mathbf{i}$ on $\otimes_{l \mid m} V_l$.

PROPOSITION 3.7:

(i) *The map* $\mathbf{i}$ *is an isomorphism.*

(ii) *The map* ρ *is an isomorphism.*

Proof. — It is clear that V_l is torsion free. For, given a coset of G_l, there is only one relation imposed on it, that the sum of its elements in the group ring is zero. Thus $\otimes_{l \mid m} V_l$ is torsion free. Since $C^k(m)$ acts simply transitively on $Z^*(m)$, which generates $U(m)/U'(m)$, we know that $\mathbf{i}$ is surjective.

Thus $\rho \circ i$ is surjective, and it suffices to show that

$$\otimes_{l \mid m} V_l \qquad \text{and} \qquad U_{S \cup (m)}/U_S,$$

have the same $\mathbf{Z}$-rank. Since $\rho \circ i$ is surjective, it is clear that

$$\operatorname{rank} \otimes_{l \mid m} V_l \geqslant \operatorname{rank} U_{S \cup (m)}/U_S.$$

To show the opposite inequality we tensor with $\mathbf{C}$ and examine the character decomposition. The space

$$\mathbf{C} \otimes \otimes_{l \mid m} V_l,$$

has a non-trivial χ-component if and only if χ is a primitive character of $C^k(m)$. On the other hand,

$$U(m) \otimes \mathbf{C} \approx \mathbf{C}[C^k(m)],$$

and therefore has a non-trivial χ-component for each character of $C^k(m)$. Now $U(m) \otimes \mathbf{C}$ injects into $U_{S \cup (m)} \otimes \mathbf{C}$ since $U(m)$ injects into $U_{S \cup (m)}$. Thus $U_{S \cup (m)}$ has non-trivial χ-component if χ is a character of C^k with conductor m. But $U_S \otimes \mathbf{C}$ has trivial χ-component for such a character, and thus

$$\operatorname{rank} U_{S \cup (m)}/U_S \geqslant \operatorname{rank} \otimes_{l \mid m} V_l.$$

This concludes the proof of Proposition 3.7.

To prove Proposition 3.3, it suffices to show that $\otimes_{l \mid m} V_l$ is acyclic. By Lemma 3.4, it is enough to prove that V_p is a free module with respect to the group $\pm \mathrm{id}$. Recall that $m(p) = n(p) > 1$ since $p \mid M$ and

$$N = pM = \prod_{l \mid N} l^{n(l)}.$$

We claim that $-\mathrm{id}$ does not belong to G_p. If $p \neq 2$ then $n(p)-1 > 0$, and

$$-1 \not\equiv 1 \bmod p^{n(p)-1}.$$

If $p = 2$, then $n(p)-1 \geqslant 2$, and again $-1 \not\equiv 1 \bmod p^{n(p)-1}$. That V_p is a free module respect to the group $\pm\mathrm{id}$ now follows immediately from Lemma 2.4. This concludes the proof of Proposition 3.3.

Thus in order to determine what happens as we pass to the injective limit we may restrict our attention to values of N which are either odd and square-free, or 4 times an odd square-free number. We determine the structure of the injective limit of the cohomology groups by analysing the relative cohomology groups using Theorem 2.16.

So in what follows, we assume that N is a square-free odd number, or four times a square-free odd number. Given N, we have defined the group $U'(N)$ as the group generated by the level groups of lower level M, where $M \mid N$ but $M \neq N$. In what follows we modify this definition slightly in the case that $4 \mid N$. We then define $U'(N)$ as the group generated by the groups of level M where $M \mid N$, $M \neq N$, and either M is odd or $4 \mid M$. We also change the definition of G_2 and set $G_2 = C^k(4)$.

In addition, we make a slight alteration of the definitions of $D(N)$ if $4 \mid M$. We set:

$D(N)$ = collection of $M \mid N$ such that either M is odd or $4 \mid M$.

We make the obvious alternations in the definition of a normal subset and normal pair, which is consistent with the above. Then we have the following analogue of Proposition 3.7.

PROPOSITION 3.8:

(i) *There is an isomorphism*

$$\mathbf{i}: \quad \otimes_{p \mid N} V_p \to U(N)/U'(N).$$

(ii) *Let S be a normal subset of $D(N)$, and let $M \mid N$ be such that M is either odd or $4 \mid M$. Suppose $M \notin S$ and also that $(S, S \cup (M))$ is a normal pair. Then there is a natural isomorphism*

$$\rho: \quad U(M)/U'(M) \to U_{S \cup (M)}/U_S.$$

The proof is essentially the same as that for Proposition 3.7, and we leave the details to the reader.

We now calculate the cohomology of $U(N)/U'(N)$. We let $\nu(N)$ be the number of prime factors of N. Let $N > 1$.

PROPOSITION 3.9:

(i) *If* $\nu(N)$ *is odd, then*

$$H^0(\pm\mathrm{id},\, U(N)/U'(N)) = 0, \qquad H^1(\pm\mathrm{id},\, U(N)/U'(N)) \approx \mathbf{Z}/2\,\mathbf{Z}.$$

(ii) *If* $\nu(N)$ *is even, then*

$$H^0(\pm\mathrm{id},\, U(N)/U'(N)) \approx \mathbf{Z}/2\,\mathbf{Z}, \qquad H^1(\pm\mathrm{id},\, U(N)/U'(N)) = 0.$$

Proof. — By our assumption that N is either square-free or four times a square free number, and our redefinition of G_2, we see that $G_p = C^k(p^{n(p)})$ for each $p \mid N$. So

$$V_p = \mathbf{Z}[C^k(p^{n(p)})]/s(C(p^{n(p)}))\,\mathbf{Z}[C(p^{n(p)})].$$

Thus a free $\mathbf{Z}$-basis for V_p consists of the elements of $C(p^{n(p)})$ excluding 1. Set $G'_p = G_p - \{\pm\mathrm{id}\}$. Then G'_p generates a free $(\pm\mathrm{id})$-submodules of V_p which we call V'_p. If W is any $(\pm\mathrm{id})$-module, we obtain and exact sequence

$$0 \to V'_p \otimes W \to V_p \otimes W \to F \to 0.$$

Now by Lemma 3.4,

$$V'_p \otimes \otimes_{q \neq p} V_q$$

is acyclic, and thus $H^*(V_p \otimes W) \approx H^*(F)$. We see that $F \approx \tilde{\mathbf{Z}} \otimes W$, where $\tilde{\mathbf{Z}}$ is $\mathbf{Z}$ thought of as a module over $\pm\mathrm{id}$, with $-\mathrm{id}$ acting through usual multiplication. By induction, we thus see that

$$H^*(\otimes_{p \mid N} V_p) \approx H^*(\otimes^{\nu(N)} \tilde{Z}),$$

where $\otimes^{\nu(N)} \tilde{Z}$ means $\tilde{Z}$ tensored with itself $\nu(N)$ times. Since

$$\otimes^{\nu(N)} \tilde{Z} \begin{cases} \approx \tilde{Z} & \text{if } \nu(N) \text{ is odd,} \\ \approx Z \text{ with trivial action of } -\mathrm{id} & \text{if } \nu(N) \text{ is even,} \end{cases}$$

the Proposition follows.

We conclude this section with a description of these cohomology groups. We may write the set $Z^*(N)$ of primitive elements, which generate $U(N)/U'(N)$, as a product

$$Z^*(N) = \prod_{p \mid N} Z^*(p^{n(p)}).$$

Now we may decompose $Z^*(p^{n(p)})$ as a disjoint union

$$Z^+(p^{n(p)}) \coprod Z^-(p^{n(p)}),$$

where x belongs to $Z^+(p^{n(p)})$ if and only if

$$-x \in Z^-(p^{n(p)}).$$

Then we have the following Proposition.

PROPOSITION 3.10. — *The element* $s(\prod_{p \mid N} Z^+(p^{n(p)}))$ *generates* $H^{\nu(N)}(U(N)/U'(N))$.

We outline the proof and leave the details to the reader. First one shows that the element $s(\prod_{p \mid N} Z^+(p^{n(p)}))$ is a cocycle by using the fact that

$$Z^*(p^{n(p)}) = Z^+(p^{n(p)}) \coprod Z^-(p^{n(p)}),$$

and applying the distribution relations. It is then easy to see that under the map sending $U(N)/U'(N)$ to $\otimes^{\nu(N)} \tilde{\mathbf{Z}}$, the above element goes to a generator, which also generates

$$H^{\nu(N)}(\otimes^{\nu(N)} \tilde{\mathbf{Z}}).$$

4. The injective limit

We shall now calculate the structure of the injective limit of the cohomology groups. From Corollary 2.9, we have the following Proposition.

PROPOSITION 4.1. — $H^q(\pm\mathrm{id}, U^k)$ *is a trivial* $GL_k(\hat{Z})$*-module.*

The basic Theorem is the following.

THEOREM 4.2. — *Let* N *be square-free or four times a square free number. Then:*

(i) $H^q(\pm\mathrm{id}, U(N)) \to H^q(\pm\mathrm{id}, U(N)/U'(N))$ *is surjective.*

(ii) *For each* $M \in D(N)$ *such that* $\nu(M) \equiv q \bmod 2$, *let* α'_M *be the generator of* $H^q(U(M)/U'(M))$. *Let* α_M *be a pull-back of* α'_M *to* $H^q(U(M))$ *(this exists by* (i)). *Then the image of the family* $\{\alpha_M\}$ *in* $H^q(U(N))$ *is a free* $\mathbf{Z}$*-basis for this group.*

Proof. — We use Theorem 2.16. We know that $H^q(U(N))$ has $\mathbf{Z}/2\,\mathbf{Z}$-rank equal to $2^{\nu(N)-1}$. The Theorem is clearly true when $N = 1$. Our method of proof is to form a chain $S_i \subset S_{i+1}$, $S_i \subset D(N)$, where

$$S_0 = U(1), \qquad S_n = D(N),$$

such that (S_i, S_{i+1}) is a normal pair, and such that $S_{i+1} = S \cup (M)$ for some M in $D(N)$. Thus $n = 2^{\nu(N)} - 1$. From the exact sequence

$$\to H^q(U_{S_i}) \to H^q(U_{S_{i+1}}) \to H^q(U(M)/U'(M)) \to,$$

we find that

$$\operatorname{rank} H^q(U_{S_{i+1}}) \leqslant \operatorname{rank} H^q(U_{S_i}) + \operatorname{rank} H^q(U(M)/U'(M)), \tag{4.3}$$

with equality occurring above if and only if $H^q(U_{S_i}) \to H^q(U_{S_{i+1}})$ is injective, and

$$H^q(U_{S_{i+1}}) \to H^q(U(M)/U'(M)),$$

is surjective. From Proposition 3.9 we see that

$$\operatorname{rank} H^q(U_{S_{i+1}}) \leqslant \operatorname{rank} H^q(U_{S_i}) + 1 \qquad \text{if} \quad \nu(M) \equiv q \bmod 2$$

and

$$\operatorname{rank} H^q(U_{S_{i+1}}) \leqslant \operatorname{rank} H^q(U_{S_i}) \qquad \text{if} \quad \nu(M) \equiv q \bmod 2.$$

Thus by induction we find that

$$\operatorname{rank} H^q(U(N)) \leqslant 2^{\nu(N)-1},$$

with equality holding if and only if for each i, the map

$$H^q(U_{S_i}) \to H^q(U_{S_{i+1}}) \quad \text{is injective,}$$

and

$$H^q(U_{S_{i+1}}) \to H^q(U(M)/U'(M)) \quad \text{is surjective.}$$

Since $H^q(U(N))$ has rank $2^{\nu(N)-1}$, we conclude that we must have equality in all cases. When $M = N$, $S_{i+1} = D(N)$, so $U_{S_{i+1}} = U(N)$. This implies part (i) of the Theorem.

We now prove (ii). We actually prove a stronger result by induction. Let S be a normal subset of $D(N)$. We claim that $H^q(U_S)$ has as a free basis the image of the collection $\{\alpha_M\}$, where $M \in S$ and $\nu(M) \equiv q \bmod 2$. This is clearly true for $S = \{1\}$. Suppose that $(S, S \cup (M))$ is a normal pair. Then the above exact sequences say that $H^q(U_S)$ injects in $H^q(U_{S \cup (M)})$, and α_M generates the cokernel. Thus the Theorem follows.

We now have a fairly good description of $H^q(U^k)$. It is trivial as a $GL_k(\hat{\mathbf{Z}})$-module. It is a filtered $\mathbf{Z}/2\,\mathbf{Z}$-vector space with the filtration index consisting of square-free odd numbers, or four times square free odd numbers N such that $\nu(N) \equiv q \bmod 2$. To each such N we may associate a subspace $A^q(N)$ and an element $\alpha_N \in A^q(N)$ such that the elements $\{\alpha_N\}$ give a basis for $H^q(U^k)$.

5. The groups $H^q(\pm\mathrm{id}, U^k(2N))$

In this section, we assume that N is a square-free odd number. Then, by Proposition 3.3, the only group that remains to be considered is the group $H^q(U^k(2N))$. When $k = 1$, $U(2N)$ is identical to $U(N)$, and there is nothing to consider. However, when $k > 1$, $U(2N)$ will properly contain $U(N)$, and $H^q(U^k(2N))$ will not equal $H^q(U^k(N))$.

We begin by analyzing the relative cohomology groups. We define $D(2N)$ to consist of all divisors of $2N$, and we define $U'(2N)$ to be the

group generated by the groups $U(M)$, where M properly divides $2N$. If p is a prime dividing $2N$, we define

$$V_p = \mathbf{Z}[C(p)]/s(C(p))\,\mathbf{Z}[C(p)].$$

Then we have the following Proposition.

PROPOSITION 5.1. — *As a $GL_k(\hat{\mathbf{Z}})$-module, we have an isomorphism*

$$\otimes_{p \mid 2N} V_p \approx U(2N)/U'(2N).$$

The proof is identical to that of Proposition 3.7. We now analyze the above tensor product, in Proposition 5.1. Note that $-\mathrm{id}$ acts trivially on $C(2)$, since $-1 = 1$ as an element of $C(2)$. Let

$$C'(2) = C(2) - \{\mathrm{id}\}.$$

Then we have an isomorphism

$$V_2 \approx \mathbf{Z}[C'(2)],$$

where the right hand side is the free abelian group on $C'(2)$, with $-\mathrm{id}$ acting trivially. So

$$\otimes_{p \mid 2N} V_p \approx \oplus_{x \in C'(2)} (\mathbf{Z} \otimes \otimes_{p \mid N} V_p),$$

where $\mathbf{Z}$ is the abelian group of integers, considered as a trivial $(\pm\mathrm{id})$-module. But

$$\mathbf{Z} \otimes \otimes_{p \mid N} V_p,$$

is isomorphic to $\otimes V_p$ as a $(\pm\mathrm{id})$-module. So using Propositions 3.8 and 3.9, we have the following Proposition.

PROPOSITION 5.2:

$$H^q(U(2N)/U'(2N)) = 0 \quad \text{if} \quad q \not\equiv \nu(N) \bmod 2.$$
$$H^q(U(2N)/U'(2N)) \approx (\mathbf{Z}/2\,\mathbf{Z})[C(2)]/s(C(2))\,(\mathbf{Z}/2\,\mathbf{Z})[C(2)]$$

as $GL_k(\hat{\mathbf{Z}})$-module if $q \equiv \nu(N) \bmod 2$.

The proof of this is clear from the above. As a group,

$$H^q(\otimes_{p \mid 2N} V_p) \approx \oplus_{x \in C'(2)} H^q(U(N)/U'(N)).$$

This fact proves the first statement. If $q \equiv \nu(N) \bmod 2$, it also shows that the second statement is true, considering the objects as vector spaces. To prove the isomorphism as $GL_k(\hat{\mathbf{Z}})$-modules, it is obvious that the subgroup of $GL_k(\hat{\mathbf{Z}})$ which is trivial (mod 2) acts trivially on both

$$(\mathbf{Z}/2\,\mathbf{Z})[C(2)]/s(C(2))\,(\mathbf{Z}/2\,\mathbf{Z})[C(2)]$$

and on

$$\oplus_{x \in C'(2)} H^q(U(N)/U'(N)).$$

This is so in the second case because the group fixes each direct summand which is 1-dimensional by Proposition 3.9. This reduces the question to the action of $GL_k(\mathbf{Z}_2)$. One observes by direct inspection that the action is the same in both cases.

We wish to prove the analogue of Theorem 4.2. We approach it a bit differently. We first prove the following result.

PROPOSITION 5.3. — *We have the following exact sequence:*

$$H^q(U(2N)) \to H^q(U(2N)/U'(2N)) \to 0.$$

We use Theorem 4.2 (i) in the proof. If $q \not\equiv \nu(N) \bmod 2$, then there is nothing to prove. So assume $q \equiv \nu(N) \bmod 2$. Let α'_N be the generator of $H^q(U(N)/U'(N))$, and let α_N be a pull back in $H^q(U(N))$, which exists by Theorem 4.2 (i).

Since $C(2)$ is in natural bijection with $Z^*(2)$, we let $Z'(2)$ be the subset of $Z^*(2)$ corresponding to $C'(2)$. Instead of dealing with elements $x \in C'(2)$, we deal with the corresponding elements, also denoted by x, in $Z'(2)$. Then there is a map

$$t: \quad U(N) \to U(2N),$$

defined by translation. That is, if $y \in Z^*(N)$, define

$$t(x)(y) = (x+y).$$

To show that this map extends to a map from $U(N)$ to $U(2N)$, we must only show that $t(x)$ takes distribution relations to distribution relations. The distribution relations of level N are generated by $\sum_{Mb=a}(b)-(a)$, where $Mf(a) \mid N$, and $f(a)$ is the denominator of a, i. e. the order of a in $(1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$. Then

$$\sum_{Mb=a}(x+b)-(x+a) = \sum_{Mb'=x+a}(b')-(x+a),$$

since M is odd (N is odd, remember), and x has denominator equal to 2, so $Mx = x$. One then sees easily that $t(x)$ maps $H^q(U(N)/U'(N))$ isomorphically onto the x-direct summand of $H^q(U(2N)/U'(2N))$, which is generated by the image of

$$t(x)(\alpha_N) \in H^q(U(2N)).$$

This proves the Proposition.

Suppose then that $(S, S \cup (M))$ is a normal pair, and S, $S \cup (M)$ are contained in $D(2N)$.

Then we have the following Corollary.

COROLLARY 5.4. — *The sequence is exact*

$$0 \to H^q(U_S) \to H^q(U_{S \cup (M)}) \to H^q(U(M)/U'(M)) \to 0.$$

Proof. — The right end of the exact sequence follows from the fact that $U(M)/U'(M)$ is isomorphic to $U_{S \cup (M)}/U_S$, combined with Theorem 4.2 and Proposition 5.3.

To prove the left end of the sequence, we must show that the image of $H^{q-1}(U(M)/U'(M))$ under the boundary map is zero. But replacing q by $q-1$ and using Proposition 5.3, we see that the kernel of the boundary map is the whole group. This proves the Corollary.

We now obtain the new Corollary.

COROLLARY 5.5:

(i) $\operatorname{rank} H^0(\pm\mathrm{id}, U^k(2)) = 2^k - 1$,
$\operatorname{rank} H^1(\pm\mathrm{id}, U^k(2)) = 0$.

(ii) *If* $N > 1$, N *odd, then*

$$\operatorname{rank} H^q(\pm\mathrm{id}, U^k(2N)) = (2^k - 1)\, 2^{\nu(N)-1}.$$

Proof. — The first statement is a simple calculation.

To prove the second statement, by Proposition 3.3 we may assume that N is square-free. One then uses Corollary 5.4 and Proposition 5.2. From Proposition 5.2 we see that if $q \equiv \nu(N) \bmod 2$, then

$$\operatorname{rank} H^q(U(2N)/U'(2N)) = 0.$$

Forming a normal chain from $U(1)$ to $U(2N)$, one may then calculate the rank of $H^q(U(2N))$. One gets a contribution of 1 for each divisor M of N with $\nu(M) \equiv q \bmod 2$, and then $2M$ produces a contribution of $2^k - 2$ to the rank. Thus the total contribution to the rank from such M is $2^k - 1$.

We may actually get the following stronger result.

THEOREM 5.6:

(i) *If* N *is odd* > 1, *then we have an isomorphism*

$$H^q(U^k(2N)) \approx \oplus_{2^{\nu(N)-1}} (\mathbf{Z}/2\mathbf{Z})[Z^*(2)],$$

as a $GL_k(\hat{\mathbf{Z}})$*-module.*

(The direct sum is that of the right hand side, taken $2^{\nu(N)-1}$ times.)

(ii) *The image of* $H^q(U^k(N))$ *in* $H^q(U^k(4N))$ *is equal to the image of* $H^q(U^k(2N))$ *in* $H^q(U^k(4N))$.

Proof. — Again by Proposition 3.3 we may restrict our attention to the case when N is odd and square-free. If α_M is defined as in

Theorem 4.2, then it is easy to see from the proof of Proposition 5.5 that the collection

$$\{\alpha_M, t(x)\alpha_M\}, \qquad x \in Z^*(2), \quad M \mid N,$$

generates $H^q(U^k(2N))$. Fixing M we first claim that the vector spaces generated by the α_M and that generated by $t(x)\alpha_M$ are $GL_k(\hat{\mathbf{Z}})$-modules. The first statement follows from Theorem 2.16. To prove the second we show that if $\sigma \in GL_k(\hat{\mathbf{Z}})$, then

$$t(\sigma x)\alpha_M = \sigma\, t(x)\alpha_M.$$

First, suppose that σ belongs to $GL_k(\mathbf{Z}_2)$. In this case, the equality follows from the definition of $t(x)$ and the definition of the action of σ. Thus suppose $\sigma \equiv \mathrm{id} \bmod 2$. Then

$$\sigma(t(x)\alpha_M) = t(x)\sigma\alpha_M = t(x)(\alpha_M),$$

again by Theorem 2.16. Thus our claim is proved since $\sigma x = x$ in this case.

Next we show that

$$\textstyle\sum_{x \in Z^*(2)} t(x)(\alpha_M) = 0.$$

This is equivalent to showing that

$$\textstyle\sum_{x \in Z^*(2)} t(x)\alpha_M + \alpha_M = \alpha_M.$$

To see this, let 2^* represent multiplication by 2 on $\mathbf{Q}^k/\mathbf{Z}^k$. Choose a cocyle β_M in $U(M)$ which represents α_M. Then the distribution relations imply that

$$\textstyle\sum_{x \in Z^*(2)} t(x)\beta_M + \beta_M = 2^*\beta_M.$$

Modulo coboundaries, using Theorem 2.16, we have

$$\textstyle\sum_{x \in Z^*(2)} t(x)\alpha_M + \alpha_M = \alpha_M,$$

which proves the claim. From this we see that

$$(\mathbf{Z}/2\,\mathbf{Z})(t(x)\alpha_M)_{x \in Z^*(2)} = (\mathbf{Z}/2\,\mathbf{Z})[Z^*(2)]/(\mathbf{Z}/2\,\mathbf{Z})s(Z^*(2)).$$

Thus we have the following equality of $GL_k(\hat{\mathbf{Z}})$-modules:

$$\begin{aligned}&(\mathbf{Z}/2\,\mathbf{Z})(t(x)\alpha_M)_{x \in Z^*(2)} \oplus (\mathbf{Z}/2\,\mathbf{Z})(\alpha_M)\\ &\quad \approx (\mathbf{Z}/2\,\mathbf{Z})[Z^*(2)]/(\mathbf{Z}/2\,\mathbf{Z})s(Z^*(2)) \oplus (\mathbf{Z}/2\,\mathbf{Z}).\end{aligned}$$

But one sees easily that

$$(\mathbf{Z}/2\mathbf{Z})[Z^*(2)]/(\mathbf{Z}/2\mathbf{Z})s(Z^*(2)) \oplus \mathbf{Z}/2\mathbf{Z} \approx \mathbf{Z}/2\mathbf{Z}(Z^*(2)],$$

as a $GL_k(\hat{\mathbf{Z}})$-module. This proves Theorem 5.6 (i).

To prove (ii), we show that the image of $t(x)\alpha_M$ in $H^q(U(4N))$ is 0. Call the image $\overline{t(x)(\alpha_M)}$. Since $H^q(U(4N))$ is a trivial $GL_k(\hat{\mathbf{Z}})$-module, it follows that

$$\overline{t(x)\alpha_M} = \overline{t(x')\alpha_M},$$

for $x, x' \in Z^*(2)$. But since

$$\sum_{x \in Z^*(2)} t(x)\alpha_M = 0,$$

we find that $(2^k-1)\,\overline{t(x)\alpha_M} = 0$. Since 2^k-1 is prime to 2, we find that $\overline{t(x)\alpha_M} = 0$, which proves Theorem 5.6.

BIBLIOGRAPHY

[B] BASS (H.). — Generators and relations for cyclotomic units, *Nagoya math. J.*, t. 27, 1966, p. 401-407.

[G-K] GROSS (B.) and KOBLITZ (N.). — *Jacobi sums and values of* Γ*-functions at rational numbers* (to appear).

[K 1] KUBERT (D.). — A system of free generators for the universal even ordinary $Z(2)$-distribution on $\mathbf{Q}^{2k}/\mathbf{Z}^{2k}$, *Math. Annalen*, t. 244, 1976, p. 21-31.

[K 2] KUBERT (D.). — *The square root of the Siegel group* (to appear).

[K 3] KUBERT (D.). — The universal ordinary distribution, *Bull. Soc. math. France* 107, 1979, p. 179-202.

[S] SINNOTT (W.). — *The index of the Stickelberger ideal* (to appear).