BULLETIN DE LA S. M. F.

DANIEL S. KUBERT

The universal ordinary distribution

Bulletin de la S. M. F., tome 107 (1979), p. 179-202

<http://www.numdam.org/item?id=BSMF_1979__107__179_0>

Bull. Soc. math. France,
107, 1979, p. 179-202.

THE UNIVERSAL ORDINARY DISTRIBUTION

BY

DANIEL S. KUBERT (*)

RÉSUMÉ. — Soit k un entier positif. Soit U^k le groupe abélien libre sur $\mathbf{Q}^k/\mathbf{Z}^k$, modulo le sous-groupe des relations de « distribution », définies plus loin. On appelle U^k la distribution ordinaire universelle de dimension k. Nous développons les propriétés fondamentales de U^k, qui trouvent des applications dans la théorie des nombres algébriques et la théorie des fonctions modulaires. Soit $U^k(N)$ le sous-module engendré par l'image de $(1/N)\mathbf{Z}^k/\mathbf{Z}^k$ dans U^k. Notons par $Z_k^*(N)$ l'ensemble des éléments primitifs d'ordre N dans $(1/N)\mathbf{Z}^k/\mathbf{Z}^k$. Parmi d'autres résultats, nous montrons que $U^k(N)$ est un $\mathbf{Z}$-module libre de rang égal à la cardinalité de $Z_k^*(N)$. De plus, $U^k(N)\otimes\mathbf{Q}$ est isomorphe (comme $GL_k(\mathbf{Z}/N\mathbf{Z})$-module) au $\mathbf{Q}$-espace vectoriel libre sur l'ensemble $Z_k^*(N)$. On développe également la théorie des distributions de Bernoulli, ainsi qu'un autre modèle pour la distribution universelle ayant sa source dans un travail récent de Sinnott.

ABSTRACT. — Let k be a positive integer. Let U^k be the free abelian group on $\mathbf{Q}^k/\mathbf{Z}^k$ modulo the group of distribution relations (defined below). We call U^k the universal ordinary distribution of dimension k. We work out some of the basic structure theory for U^k, having applications in algebraic number theory and the theory of modular functions. Let $U^k(N)$ be the submodule generated by the image of $(1/N)\mathbf{Z}^k/\mathbf{Z}^k$ in U^k. Let $Z_k^*(N)$ denote the set of elements primitive of order N in $(1/N)\mathbf{Z}^k/\mathbf{Z}^k$. Then among other things, we show that $U^k(N)$ is a free $\mathbf{Z}$-module of rank equal to the cardinality of $Z_k^*(N)$. Furthermore $U^k(N)\otimes\mathbf{Q}$ is isomorphic to the free $\mathbf{Q}$-vector space on the set $Z_k^*(N)$, as a $GL_k(\mathbf{Z}/N\mathbf{Z})$-module. The theory of Bernoulli distributions is also developed as well as another model for the universal distribution having its source in recent work of Sinnott.

Let k be a positive integer. Let M be the abelian group $(\mathbf{Q}/\mathbf{Z})^k$. Let f be a function from M to an abelian group A which satisfies the identity

$$\textstyle\sum_{Nb=m} f(b) = f(m),$$

for all $m \in M$ and all positive integers N. We say then that f is an ordinary distribution from M to A.

(*) 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).

Given M there is an abelian group U_M and a map

$$\delta: \quad M \to U_M,$$

which is the universal distribution for M. In other words, if $f: M \to A$ is a distribution, there exists a homomorphism $f_*: U_M \to A$ such that the following diagram commutes:

$$\begin{tikzcd} M \arrow[rr, "\delta"] \arrow[dr, "f"'] & & U_M \arrow[dl, dashed, "f_*"] \\ & A & \end{tikzcd}$$

It is obvious how to construct U_M. One simply takes the free abelian group on M, modulo the distribution relations.

The motivation for this study comes from the fact that ordinary distributions arise naturally in number theory when $k = 1$, and in the theory of modular forms when $k = 2$. Let $\mathbf{Q}^{ab}$ be the maximal abelian extension of $\mathbf{Q}$, which by Kronecker's Theorem is generated by all roots of unity. Let $A = (\mathbf{Q}^{ab})^*/\mathbf{Q}^*$, so A is an abelian group under multiplication. We define

$$f: \quad \mathbf{Q}/\mathbf{Z} \to A,$$

by $f(0) = 1$, and for $x \in \mathbf{Q}/\mathbf{Z}$, $x \neq 0$, we let $f(x) = 1 - e^{2\pi i x}$. The identity

$$\prod\nolimits_{\zeta^N = 1} (1 - \zeta X) = 1 - X^N,$$

shows that f is an ordinary distribution (*see* [B]).

Another distribution when $k = 1$ comes from the Bernoulli polynomial $\mathbf{B}_1(X) = X - (1/2)$. If $x \in \mathbf{R}$, we let $\langle x \rangle$ be the unique number such that

$$0 \leqslant \langle x \rangle < 1 \qquad \text{and} \qquad x \equiv \langle x \rangle \bmod \mathbf{Z}.$$

Let $A = Q$, and put $f(x) = \mathbf{B}_1(\langle x \rangle)$. Then f is an ordinary distribution from $\mathbf{Q}/\mathbf{Z}$ to $\mathbf{Q}$. MAZUR uses this to obtain a measure theoretic approach to p-adic L-functions (*see* [M]).

A third distribution when $k = 1$ comes from the p-adic gamma function which has been used by GROSS and KOBLITZ to prove a version of Deligne's conjecture for periods of Fermat surfaces (*see* [G]).

In the case $k = 2$, the Siegel functions generate a natural ordinary distribution. Let $a = (a_1, a_2) \in \mathbf{Q}^2$ and $a \notin \mathbf{Z}^2$.

Define g_a by the q-expansion

$$g_a = -q_\tau^{(1/2)\, B_2(a_1)} e^{2\pi i a_2 (a_1 - 1)/2} (1-q_z) \prod_{n=1}^{\infty} (1-q_\tau^n q_z)(1-q_\tau^n / q_z),$$

where $z = a_1 \tau + a_2$, $q_\tau = e^{2\pi i \tau}$, and $B_2(X) = X^2 - X + (1/6)$ (*see* [L], p. 251).

It is easy to see that if $a \equiv a' \bmod \mathbf{Z}^2$, then $g_a = g_{a'}$ modulo constants. Let A be the group generated by the functions g_a modulo constants. Then we define a map

$$g: \ (\mathbf{Q}/\mathbf{Z})^2 \rightarrow A,$$

by $g(a) = g_a$, which is well-defined by the above remark. It is then easy to check that g is an ordinary distribution.

Let U^k denote the universal distribution associated with $(\mathbf{Q}/\mathbf{Z})^k$. Then U^k is naturally a $GL_k(\hat{\mathbf{Z}})$-module, where $\hat{\mathbf{Z}}$ is the completion of $\mathbf{Z}$ under the ideal topology, and

$$\hat{\mathbf{Z}} \approx \prod_p \mathbf{Z}_p.$$

The module structure is derived from the natural action of $GL_k(\hat{\mathbf{Z}})$ on $(\mathbf{Q}/\mathbf{Z})^k$, and the fact that $GL_k(\hat{\mathbf{Z}})$ takes the group of distribution relations into itself.

We shall determine exactly the structure of U^k as a group, and we show that U^k is free. We also give a canonical system of free generators. We also determine precisely the structure of $\mathbf{Q} \otimes U^k$ as a $GL_k(\hat{\mathbf{Z}})$-module.

In the present paper, we first produce free generators for $U^k(N)$.

Next we give two examples of universal distributions on $(\mathbf{Q}/\mathbf{Z})^k$. The first one arises from a classical construction of Stickelberger elements, and the second is related to some ideas of SINNOTT [S].

In the paper which immediately follows the present one, we calculate the cohomology groups of U^k as a module over the group $\{\pm \text{id}\}$. We are motivated to do this for the following reasons. First in the case when $k = 2$, we have shown in [K 2] that the calculation of the unit group in the modular function field involves the determination of $H^0(\pm \text{id}, U^2)$. More precisely, it had been shown earlier that the Siegel units given above have rank equal to the rank of the full set of modular units. In [K 2], we show that the group of units modulo the Siegel units is in fact a $\mathbf{Z}/2\,\mathbf{Z}$-vector space, which injects naturally into $H^0(\pm \text{id}, U^2)$, and which maps onto $H^0(\pm \text{id}, U^2(\mathrm{N}))$ when N is odd.

In [S], SINNOTT calculates the index of the Stickelberger ideal for composite N. He finds that this index equals the odd part of the class number of the cyclotomic field of conductor N times half the square root of the order of $H^1(\pm \text{id}, U^1(N))$. He also calculates the index of the units in the cyclotomic field of conductor N modulo the circular units, and finds this index to be the even part of the class number times a power of 2, again closely related to the order of $H^0(\pm \text{id}, U^1(N))$.

The group $H^0(\pm \text{id}, U^1(N))$ also represents an obstruction in [6] to getting the field of definition predicted by DELIGNE for certain periods of Fermat surfaces, thus providing another motivation for its study.

1. Free generators for $U^k(N)$

In this section, we show how to produce a set of free generators for $U^k(N)$. Let $F^k(N)$ be the free abelian group

$$\frac{1}{N}\mathbf{Z}^k/\mathbf{Z}^k = \left(\frac{1}{N}\mathbf{Z}/\mathbf{Z}\right)^k.$$

We let F^k be the free abelian group on $\mathbf{Q}^k/\mathbf{Z}^k$, so we have an injection for each positive integer N:

$$0 \to F^k(N) \to F^k. \tag{1.1}$$

Let D^k be the subgroup of F^k generated by the distribution relations. Set

$$\mathrm{D}_N^k = F^k(N) \cap D^k.$$

We define a related group $D^k(N)$ as the group generated by elements

$$\textstyle\sum_{Mb=a}(b)-(a), \qquad \text{with } M \mid N, \text{ and } a \in \frac{M}{N}\mathbf{Z}^k/\mathbf{Z}^k. \tag{1.2}$$

Thus $D^k(N) \subset D_N^k$. We will show that, in fact, $D^k(N) = D_N^k$. We define $U^k(N) = F^k(N)/D_N^k$, so we have a surjective map

$$F^k(N)/D^k(N) \to U^k(N) \to 0. \tag{1.3}$$

For $M \mid N$ define

$$Z_k^*(M) = \left\{ x \in \frac{1}{M}\mathbf{Z}^k/\mathbf{Z}^k \text{ such that } x \text{ has order } M \right\}. \tag{1.4}$$

Thus $Z_k^*(M)$ is the set of primitive elements in $(1/M)\mathbf{Z}^k/\mathbf{Z}^k$. When k is fixed, we often omit the subscript k and write simply $Z^*(M)$.

We now exhibit explicit generators for $F^k(N)/D^k(N)$ whose cardinality is equal $Z_k^*(N)$. We shall see later that $U^k(N)$ has free rank at least equal to this cardinality, so we can conclude that our generators are free, that therefore

$$D^k(N) = D_N^k,$$

and finally that $U^k(N)$ is a free $\mathbf{Z}$-module of rank $|Z_k^*(N)|$.

Let $N = \prod p^{n(p)}$ be the prime power decomposition of N. We say that M is an admissible divisor of N if $(M, N/M) = 1$. This means that if p divides M, then $p^{n(p)}$ divides M. Using k-tuples to describe elements of $\mathbf{Q}^k/\mathbf{Z}^k$, we denote by $e(N)$ the element

$$e(N) = \left(\frac{1}{N}, 0, \ldots, 0\right). \tag{1.5}$$

Note that $Z^*(M)$ is naturally the direct product of the sets

$$Z^*(p^{n(p)}), \qquad \text{where} \quad p \mid M.$$

Let $Z^*(M, p)$ be the subset of elements of $Z^*(M)$ with p-component equal to $e(p^{n(p)})$. Let

$$T^*(M) = Z^*(M) - \bigcup_{p \mid M} Z^*(M, p) \qquad \text{if} \quad M \neq 1, \tag{1.6}$$

$$T^*(1) = \{0\}.$$

Then let

$$T(N) = \bigcup_M T^*(M) \text{ where } M \text{ is admissible, } \; M \mid N. \tag{1.7}$$

The Theorem we wish to prove is the following.

THEOREM 1.8.

(i) *The cardinality of* $T(N)$ *is* $|Z_k^*(N)|$.

(ii) $T(N)$ *is a free basis for* $U^k(N)$.

From (i) and the lower bound, we shall obtain for the rank of $U^k(N)$, to prove (ii), it suffices to prove the following Proposition.

PROPOSITION 1.9. – $T(N)$ *generates* $F(N)/D(N)$.

We see immediately that

$$T(N) = \prod_{p \mid N} [Z^*(p^{n(p)}) - \{e(p^{n(p)})\} \cup \{0\}].$$

Thus the first part of the Theorem follows immediately.

We now prove Proposition 1.9. Set $A(N) = F(N)/D(N)$. Let $B(N)$ be the group generated by the image of $T(N)$ in $A(N)$. We say that an element $t \in (1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$ is *available* if the image of (t) in $F(N)/D(N)$ belongs to $B(N)$. We must show that each element of $(1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$ is available. We induct on the number of prime factors of N. Suppose first that $N = p^n$, where p is prime. The only element of $Z^*(M)$ which is not available is $e(p^n)$. But since by the distribution relations

$$\textstyle\sum_{t \in Z^*(N)} (t) = 0,$$

we see that $e(p^n)$ is available. If $M \mid N$ and $M \neq 1$, and $t \in Z^*(M)$, then

$$t = \textstyle\sum_{s \in Z^*(N),\,(N/M)\,s=t} (s),$$

so t is available. Finally (0) is available, because $(0) \in T(N)$. Thus the Proposition is proved in the prime power case.

Let $A'(N)$ be the group generated by the elements (t) for $t \in Z^*(M)$, where M is admissible.

LEMMA 1.10. $A(N) = A'(N)$.

Proof. – Let M be an admissible divisor of N. Let E be a positive integer dividing M and having the same prime factors as M. Then

$$(t) = \textstyle\sum_{s \in Z^*(M),\,(M/E)\,s=t} (s).$$

This proves the Lemma.

So by the Lemma, we must show that $B(N) = A'(N)$. By induction we know that M is admissible divisor of N, $M \neq N$, then

$$A'(M) = B(M) \subset B(N).$$

Hence it suffices to show that if $t \in Z^*(N)$, then $t \in B(N)$. Set

$$W(N) = \textstyle\bigcup_{p \mid N} Z^*(N, p).$$

We must show that if $t \in W(N)$ then $t \in B(N)$, since these are the elements excised from $Z^*(N)$. Given $t \in W(N)$, let $V(t)$ be the set of primes p such that $t \in Z^*(N, p)$. Set

$$v(t) = |V(t)|.$$

We induct on $v(t)$ to show that each t is available. Define

$$W_i = \{t \in W(N) \text{ such that } v(t) = i\}. \tag{1.11}$$

Then

$$W(N) = \coprod_{i=1}^{s} W_i$$

is the disjoint union. We make use of the following Lemma.

LEMMA 1.12. – *Given $t \in W(N)$ and p such that $t \in Z^*(N, p)$. Set*

$$Y = y \in Z^*(N) \text{ such that } p^{n(p)} y = p^{n(p)} t.$$

Suppose that $Y - \{ t \}$ is available. Then t is available.

Proof. – Let Y_p be the set of $p^{n(p)-1}$ multiples of elements of Y. Then the distribution relations show that

$$Y_p - \{ p^{n(p)-1} t \},$$

is available. Write $N = p^{n(p)} M$. By induction, $z = p^{n(p)} t$ is available, and so is $w \in Z^*(M)$ for which $pw = z$. Now by the distribution relations,

$$\sum_{s \in Y_p} (s) + (w) = z.$$

We conclude that $p^{n(p)-1} t$ is available. But then using the obvious distribution relation, we see that t is available.

Suppose now that $t \in W_1$. There is a unique p such that $t \in Z^*(N, p)$. We claim that if $y \in W(N)$ and $p^{n(p)} y = p^{n(p)} t$, then $y = t$. To see this, since $p^{n(p)} y = p^{n(p)} t$, we may write the partial fraction decomposition

$$t = \sum_{q \mid N, q \neq p} a(q) + e(p^{n(p)}), \qquad y = \sum_{q \mid N, q \neq p} a(q) + a(p).$$

Since $t \in W_1$, we have $a(q) \neq e(q^{n(q)})$ for $q \neq p$. So if $y \in W(N)$, then $a(p) = e(p^{n(p)})$ implies $y = t$. Applying Lemma 1.12, we conclude that W_1 is available.

Suppose $t \in W^r$, and by induction that W_s is available for $s < r$. Choose p such that $t \in Z^*(N, p)$. Let Y be as in Lemma 1.12. Then

$$Y \cap \coprod_{i \geqslant r} W_i = t.$$

Indeed, suppose y is in the intersection on the left hand side. We have

$$t = \sum_{q \neq p} a(q) + e(p^{n(p)}) \qquad \text{and} \qquad y = \sum_{q \neq p} a(q) + a(p).$$

Thus $v(y) \leqslant v(t)$, with equality if, and only if, $a(p) = e(p^{n(p)})$, which implies that $y = t$, as claimed.

Applying Lemma 1.12 shows that W^r is available, and concludes the proof of Proposition 1.9 and Theorem 1.8.

2. The Cartan group

Let k be a positive integer. Given a prime number p, there is a unique unramified extension of $\mathbf{Q}_p$ of degree k, which we denote by $\mathbf{Q}_p^k$. We denote the integers of $\mathbf{Q}_p^k$ by $\mathfrak{o}_p^k$, or also $\mathfrak{o}_p$. The units $\mathfrak{o}_p^*$ form a group $C_p^k = C_p$, which is the non-split unramified Cartan group of degree k associated with the prime p, the Cartan group for short. Given a positive integer n, we define

$$\mathfrak{o}^k(p^n) = \mathfrak{o}_p^k / p^n \mathfrak{o}_p^k. \tag{2.1}$$

We set

$$C^k(p^n) = \mathfrak{o}_p^* / (1 + p^n \mathfrak{o}_p^k), \tag{2.2}$$

and we call $C^k(p^n)$ the non-split Cartan group of level p^n. We have

$$C^k(p^n) = (\mathfrak{o}^k(p^n))^*. \tag{2.3}$$

Let N be a positive integer,

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

Set

$$\mathfrak{o}^k(N) = \prod_{p \mid N} \mathfrak{o}^k(p^{n(p)}) \quad \text{and} \quad C^k(N) = \mathfrak{o}_N^* = \prod_{p \mid N} C^k(p^{n(p)}). \tag{2.4}$$

The groups $C^k(N)$ clearly form a projective system and we denote by C^k the projective limit, which is the non-split Cartan group of degree k. Clearly,

$$C^k = \prod_p C_p^k. \tag{2.5}$$

If k is fixed in the course of a discussion, we will often omit the superscript k.

There is a natural isomorphism

$$\mathfrak{o}^k(N) \approx \prod_{p \mid N} \frac{1}{N} \mathfrak{o}_p^k / \mathfrak{o}_p^k,$$

as an $\mathfrak{o}^k(N)$-module, with 1 going to the element with coordinate $1/N$ at each prime p under the natural map. As a group,

$$\prod_{p \mid N} \frac{1}{N} \mathfrak{o}_p^k / \mathfrak{o}_p^k \text{ is isomorphic to } \left(\frac{1}{N} \mathbf{Z}/\mathbf{Z}\right)^k.$$

The group $C^k(N)$ corresponds under this isomorphism to the primitive elements of $((1/N)\,\mathbf{Z}/\mathbf{Z})^k$, i. e. to $Z_k^*(N)$. In particular, the order of $C^k(N)$ equals the number of primitive elements of $((1/N)\mathbf{Z}/\mathbf{Z})^k$, and we may consider that $C^k(N)$ acts simply transitively on $Z_k^*(N)$.

Let L be a field and fix k. Denote by $L^k(N)$ the free L-vector space generated by the primitive elements of $((1/N)\,\mathbf{Z}/\mathbf{Z})^k$. Then $L^k(N)$ is a module over $GL_k(\hat{\mathbf{Z}})$, which factors through $GL_k(\mathbf{Z}/N\,\mathbf{Z})$. Let $M \mid N$. Then we have an injection

$$0 \to L^k(M) \xrightarrow{i} L^k(N) \tag{2.6}$$

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

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

where the sum is taken over primitive elements y in $((1/N)\,Z/Z)^k$ such that $(N/M)\,y = x$. The map is clearly a $GL_k(\hat{\mathbf{Z}})$-morphism. We wish to identify this map with a map on the Cartan group rings. Let $L\,[C^k(N)]$ be the group ring of $C^k(N)$. If $M \mid N$, we have an injection of C^k-modules

$$0 \to L[C^k(M)] \xrightarrow{i} L[C^k(N)], \tag{2.7}$$

given by

$$i(x) = \sum\nolimits_{y \equiv x \bmod M}(y),$$

where $x \in C^k(M)$ and $y \in C^k(N)$. Maps (2.6) and (2.7) are identical under the isomorphism of $\mathfrak{o}^k(N)$ with $\prod_{p \mid N}(1/N)\,\mathfrak{o}_p^k/\mathfrak{o}_p^k$.

Denote by $L\langle C^k\rangle$ the injective limit of $L\,[C^k(N)]$. We shall construct ordinary distributions from $(\mathbf{Q}/\mathbf{Z})^k$ to $L\langle C^k\rangle$, i. e. homomorphisms from U^k to $L\langle C^k\rangle$. Let

$$\varphi:\ \mathbf{Q}/\mathbf{Z} \to L$$

be a map such that if $M \mid N$ and $a \in (1/M)\,\mathbf{Z}/\mathbf{Z}$, then

$$N^{k-1}\sum\nolimits_{(N/M),\,b=a}\varphi(b) = M^{k-1}\,\varphi(a). \tag{2.8}$$

(This may be called a distribution of weight $k-1$.) We shall construct an associated distribution Φ with values in $L\langle C^k\rangle$, i. e. a map

$$\Phi:\ U^k \to L\langle C^k\rangle$$

as follows. Let

$$\lambda:\ \prod\nolimits_p \mathfrak{o}_p^k \to \prod\nolimits_p \mathbf{Z}_p$$

be a surjective homomorphism. Then we have naturally derived surjective homomorphisms

$$\lambda_N : \mathfrak{o}^k(N) \to \mathbf{Z}/N\mathbf{Z}$$

which satisfy an obvious consistency property. If $x \in (1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$, we may consider $Nx \in \mathfrak{o}^k(N)$ as seen above. Set

$$\Phi(x) = \textstyle\sum_{c \in C^k(N)} \varphi\left(\frac{1}{N}\lambda_N(cNx)\right)c^{-1}. \tag{2.9}$$

We must first check that this map is consistent and then that the distribution relations are satisfied. So suppose $x \in (1/M)\,\mathbf{Z}^k/\mathbf{Z}^k$, where $M \mid N$. We must show

$$\textstyle\sum_{c \in C^k(N)} \varphi\left(\frac{1}{N}\lambda_N(cNx)\right)c^{-1} = \sum_{d \in C^k(M)} \varphi\left(\frac{1}{M}\lambda_M(dMx)\right)d^{-1}. \tag{2.10}$$

as elements of the injective limit.

To see this, fix d, and let $\{c\}$ be such that $c \bmod M = d$. Then in the group ring,

$$d^{-1} = \textstyle\sum_{c \bmod M = d} c^{-1}.$$

Now $\lambda_N(cNx) = \lambda_M(cNx)$, considering cNx as an element of $\mathfrak{o}^k(M)$, and

$$\lambda_M(cNx) = \frac{N}{M}\lambda_M(cMx) = \frac{N}{M}\lambda_M(dMx),$$

which proves (2.10). We now show that the distribution relations are satisfied. Let $x \in (1/M)\,\mathbf{Z}^k/\mathbf{Z}^k$. We wish to show that if $M \mid N$, then

$$\textstyle\sum_{(N/M)\,y = x} \Phi(y) = \Phi(x). \tag{2.11}$$

But

$$\textstyle\sum_{(N/M)\,y = x} \Phi(y) = \sum_{(N/M)\,y = x} \sum_{c \in C^k(N)} \varphi\left(\frac{1}{N}\lambda_N(cNy)\right)c^{-1}.$$

Now

$$\frac{N}{M}\cdot\frac{1}{N}\lambda_N(cNy) = \frac{1}{N}\lambda_N(cNx) \bmod \mathbf{Z}.$$

Furthermore λ_N maps $\mathfrak{o}^k(N)$ onto $\mathbf{Z}/N\mathbf{Z}$. If $z \in (1/N)\,\mathbf{Z}/\mathbf{Z}$ is such that

$$(N/M)\,z = \frac{1}{N}\lambda_N(cNx),$$

then there exists y such that $(1/N)\,\lambda_N(c\,N\,y) = z$. It is clear from the elementary divisor Theorem that the number of such y is equal to $(N/M)^{k-1}$. So

$$\begin{aligned}\textstyle\sum_{(N/M)\,y=x}\Phi(y) &= \textstyle\sum_{c\in C^k(N)}(N/M)^{k-1}\sum_{(N/M)\,z=(1/N)\,\lambda_N(cNx)}\varphi(z)\,c^{-1}\\ &= \textstyle\sum_{c\in C^k(N)}\varphi\left(\frac{1}{N}\lambda_N(c\,N\,x)\right)c^{-1} \quad \text{by } (2.8)\\ &= \Phi(x).\end{aligned}$$

In the next section we exhibit functions φ satisfying (2.8).

3. Bernoulli distributions

The following relation is equivalent to (2.8).

$$N^{k-1}\textstyle\sum_{Nb=a}\varphi(b) = \varphi(a). \tag{3.1}$$

simply by replacing N/M by N. We consider the special case when $L = R$ is the field of real numbers. We also consider functions φ which satisfy (3.1) for $a \in \mathbf{R}/\mathbf{Z}$. Choosing $t \in [0, 1)$, we may rewrite (3.1) as

$$N^{k-1}\textstyle\sum_{r=0}^{N-1}\varphi\left(\frac{t}{N}+\frac{r}{N}\right) = \varphi(t), \tag{3.2}$$

PROPOSITION 3.3. – *Let $\varphi(t)$ be of class $C^{(k+1)}$ on $[0, 1)$, and assume that φ satisfies* (3.2) *for all positive integers N. Then there is a constant α such that*

$$\varphi(t) = \alpha\,\mathbf{B}_k(t),$$

where $\mathbf{B}_k(X)$ is the k-th Bernoulli polynomial.

Proof. – The polynomial $\mathbf{B}_k(X)$ is defined by the series

$$\frac{ue^{uX}}{e^u-1} = \sum \mathbf{B}_k(X)\frac{u^k}{k!}.$$

It is a classical fact that $\mathbf{B}_k(t)$ satisfies (3.2), and can easily be shown from the above definition (*see* for instance [L], p. 230). If φ satisfies (3.2) for a certain integer k, then φ' satisfies (3.2) for $k-1$. By induction, $\varphi'(t) = \alpha\,B_k(t)$, so φ' is uniquely determined up to an additive constant. Since $\mathbf{B}_k(t)$ satisfies (3.2), and since for any number $c \neq 0$ the function

$\mathbf{B}_k(t)+c$ does not satisfy (3.2), the Proposition follows if we prove it for $k=1$. Differentiating twice, we get

$$N^{-2}\sum_{r=0}^{N-1}\varphi''\left(\frac{t}{N}+\frac{r}{N}\right)=\varphi''(t).$$

Since φ'' is bounded on $[0, 1)$ by assumption, letting $N\to\infty$ we conclude that $\varphi''(t)=0$ for all t. So φ'' is linear. Since $\mathbf{B}_1(t)$ satisfies (3.2) while $\mathbf{B}_1(t)+c$ does not, the Proposition is proved.

We wish to find a function φ such that the associated distribution Φ gives an isomorphism from U^k to its image. The Bernoulli distribution does not accomplish this since the polynomial $\mathbf{B}_k(t)$ is odd (resp. even) as k is odd (resp. even) under the map $x\mapsto 1-x$. As we have seen in [K 1], $\mathbf{B}_k(t)$ essentially yields the universal even or odd distribution, depending on the parity of k. Proposition 3.2 says that we must loosen the smoothness conditions on φ to accomplish this.

Let L now be the field of complex numbers $\mathbf{C}$. Let φ be an L^2-function from $\mathbf{R}/\mathbf{Z}$ to $\mathbf{C}$. I am indebted to D. ROHRLICH for the following Lemma.

LEMMA 3.4. — *Let* $\varphi\in L^2([0, 1))$, *and suppose* φ *satisfies* (3.2) *for all positive integers* N. *Let* $a(N)$ *be the* N*-th Fourier coefficient of* φ. *Then:*

$$a_0=0,\qquad a(N)=\frac{a(1)}{N^k},\qquad a(-N)=\frac{a(-1)}{N^k}$$

for all integers $N>0$.

Proof. — For $c\in\mathbf{Z}$, set

$$\hat{\varphi}(c)=\int_0^1\varphi(t)e^{-2\pi ict}\,dt.$$

By (3.2) we have

$$\hat{\varphi}(c)=N^{k-1}\int_0^1\sum_0^{N-1}\varphi\left(\frac{t}{N}+\frac{j}{N}\right)e^{-2\pi ict}\,dt$$

$$=N^k\int_0^1\sum_0^{N-1}\varphi\left(\frac{t}{N}+\frac{j}{N}\right)e^{-2\pi ict}\,d\left(\frac{t}{N}\right).$$

Set $t'=t/N$. Then

$$\hat{\varphi}(c)=N^k\int_0^1\sum_0^{N-1}\varphi\left(t'+\frac{j}{N}\right)e^{-2\pi icNt'}\,dt'$$

$$=N^k\sum_0^{N-1}\int_0^{1/N}\varphi\left(t'+\frac{j}{N}\right)e^{-2\pi icNt'}\,dt'$$

$$=N^k\int_0^1\varphi(t')e^{-2\pi icNt'}\,dt'.$$

Putting $c = 0$, $N \neq 1$, we see that $a(0) = 0$. Putting $c = 1$, we get $a(N) = a(1)/N^k$. Putting $c = -1$, we get $a(-N) = a(-1)/N^k$, which proves the Lemma.

So the family of L^2-functions satisfying (3.2) for fixed k is essentially one-dimensional. It is easy to see that

$$\mathbf{B}_k(t) = \frac{(-1)^{(k/2)-1}k!}{(2\pi)^k}\sum_{n=1}^{\infty}\left(\frac{e^{2\pi int}}{n^k} + \frac{e^{-2\pi int}}{n^k}\right) \quad \text{if } k \text{ is even,} \tag{3.5}$$

$$\mathbf{B}_k(t) = \frac{(-1)^{(k+1)/2}k!}{i(2\pi)^k}\sum_{n=1}^{\infty}\left(\frac{e^{2\pi int}}{n^k} - \frac{e^{-2\pi int}}{n^k}\right) \quad \text{if } k \text{ is odd.}$$

Let

$$G_k(t) = \sum_{n=1}^{\infty}\frac{e^{2\pi int}}{n^k} \quad \text{for } k > 1, \tag{3.6}$$

$$G_1(t) = \log(1 - e^{2\pi it}),$$

where the log is the principal branch, and $0 < t < 1$. If $k > 1$, we check easily that $G_k(t)$ satisfies (3.2), namely

$$\sum_{j=0}^{N-1} G_k\left(\frac{t}{N} + \frac{j}{N}\right) = \sum_{j=0}^{N-1}\sum_{n=1}^{\infty}\frac{e^{2\pi i(t/N + j/N)n}}{n^k}$$

$$= \sum_{n=1}^{\infty}\frac{e^{2\pi itn/N}}{N^k}\sum_{j=0}^{N-1} e^{2\pi ijn/N}$$

$$= \sum_{N \mid n} N\frac{e^{2\pi itn/N}}{n^k}$$

$$= \frac{1}{N^{k-1}}\sum_{n=1}^{\infty}\frac{e^{2\pi int}}{n^k} = \frac{1}{N^{k-1}}G_k(t).$$

For $k = 1$, we have the representation

$$G_1(t) = \log(1 - e^{2\pi it}) = \sum_{n=1}^{\infty}\frac{e^{2\pi int}}{n}, \tag{3.7}$$

which is valid by the Abel summation formula for $0 < t < 1$. By considering $\exp G_1(t) = 1 - e^{2\pi it}$, it is easy to see that $G_1(t)$ satisfies (3.2) for $0 < t < 1$. The corresponding relation to that for $t = 0$ is

$$\sum_{r=0}^{N-1} G_1\left(\frac{r}{N}\right) = \log N. \tag{3.8}$$

So $G_1(t)$ will not strictly produce a distribution. We might say it produces a modified distribution. We may however produce a function φ satisfying (3.1) for each $a \in \mathbf{Q}/\mathbf{Z}$ by choosing $u \in \hat{\mathbf{Z}}^*$, setting $\varphi(0)$ to any arbitrary value, and

$$(3.9) \qquad \varphi(a) = G_1(ua) - G_1(a) \qquad \text{for} \quad a \in \mathbf{Q}/\mathbf{Z}, \quad a \neq 0.$$

Using (3.9) one can then construct the universal distribution for $k = 1$ from the function $G_1(t)$. We shall leave the details to the reader, and give the Theorem here only for $k > 1$.

THEOREM 3.10. — *Let Φ_k be the distribution associated with the function $G_k(t)$ for $k > 1$. Then:*

(i) *The map Φ_k gives an isomorphism of $U^k(N)$ with its image, as $C^k(N)$-modules.*

(ii) *Let $\Phi_k(N)$ be the image of $U^k(N)$ under Φ_k. Then*

$$\Phi_k(N) \otimes \mathbf{C} = \mathbf{C}\left[C^k(N)\right].$$

Proof. — Since $U^k(N)$ has a set of generators $T^k(N)$ of cardinality $|Z_k^*(N)| = |C^k(N)|$, it suffices to prove that $\Phi_k(N)$ has free rank $|C^k(N)|$, and thus it suffices to prove (ii). This is equivalent to showing that for each character χ of $C^k(N)$, the χ-component of $\Phi_k(N) \otimes C$ is non-trivial, since $\Phi_k(N)$ is a $C^k(N)$-module by construction. By (2.10), the χ-component is

$$(3.11) \qquad S(\Phi, \chi) = \sum_{c \in C^k(N)} \bar{\chi}(c)\, \varphi\left(\frac{1}{N} \lambda_N(c N x)\right).$$

But from [KL], we find that for each χ, the sum $S(\Phi, \chi)$ is non-zero if, and only if, for each character ψ of $(\mathbf{Z}/N\mathbf{Z})^*$, we have

$$(3.12) \qquad \sum_{c \in (\mathbf{Z}/f\mathbf{Z})^*} \psi(c)\, \varphi\left(\frac{c}{f}\right) \neq 0,$$

where f is the conductor of ψ. In our case, $k > 1$, we have

$$\varphi\left(\frac{c}{f}\right) = \sum_{n=1}^{\infty} \frac{e^{2\pi i c n/f}}{n^k}.$$

Hence

$$\sum_{c \in (\mathbf{Z}/f\mathbf{Z})^*} \psi(c)\, \varphi\left(\frac{c}{f}\right) = \sum_{c \in (\mathbf{Z}/f\mathbf{Z})^*} \psi(c) \sum_{n=1}^{\infty} \frac{e^{2\pi i c n/f}}{n^k}$$
$$= \sum_{n=1}^{\infty} \sum_{c} \frac{\psi(c)\, e^{2\pi i c n/f}}{n^k}.$$

By standard properties of Gauss sums, we know that

$$\sum_c \psi(c)\, e^{2\pi i c n/f} \begin{cases} = 0 & \text{if } (n, f) \neq 1, \\ \neq 0 & \text{if } (n, f) = 1. \end{cases}$$

so

$$\sum_{n=1}^{\infty} \sum_c \frac{\psi(c)\, e^{2\pi i c n/f}}{n^k} = S(\chi) \sum_{(n, f)=1} \frac{\bar{\psi}(n)}{n^k}$$

where

$$S(\psi) = \sum_c \psi(c)\, e^{2\pi i c/f} \quad \text{and} \quad \sum_{(n, f)=1} \frac{\bar{\psi}(n)}{n^k} = L(k, \bar{\psi}) \neq 0,$$

by the product expression for the L-series. This proves the Theorem.

4. The rational distribution

In this section, we present another model for the universal distribution, taking its values in $\mathbf{Q}\langle C^k \rangle$, and which we therefore call the rational distribution. For the case $k = 1$, the image of the distribution appears in SINNOTT [S], although it is not identified as such.

We will define maps

$$r^k(N): \ \frac{1}{N}\mathbf{Z}^k/\mathbf{Z}^k \to \mathbf{Q}[C^k(N)],$$

which will be $GL_k(\hat{\mathbf{Z}})$-morphisms, after a choice of basis for $\mathfrak{o}^k(N)$. We have a natural bijection

$$\frac{1}{N}\mathfrak{o}^k(N)/\mathfrak{o}^k(N) \to \mathfrak{o}^k(N)/N\,\mathfrak{o}^k(N),$$

obtained by $x \mapsto Nx$. A choice of basis identifies $\mathfrak{o}^k(N)$ with $\mathbf{Z}^k/N\,\mathbf{Z}^k$, which then becomes a $C^k(N)$-module.

Let $a \in (1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$. Let $f(a)$ be the order of a in $(1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$. Define

$$(4.1) \qquad \frac{1}{N}X(a) = \left\{ x \in \frac{1}{N}\mathbf{Z}^k/\mathbf{Z}^k \text{ such that } x \right.$$
$$\left. \text{is primitive and } (N/f(a))\,x = a \right\}.$$

In terms of the Cartan group, we can then write

$$(4.2) \qquad X(a) = \{c \in C^k(N) \text{ such that } (N/f(a))\, c_p \equiv (N\,a)_p \bmod p^{n(p)}\},$$

where $(N\,a)_p$ is the p-th coordinate of $N\,a$, for $p \mid N$.

Let $N = \prod q^{n(q)}$. For $p \mid N$ define the set $X_p(N)$ by

$$(4.3) \qquad X_p(N) = \{c = (c_q)_q \in C^k(N) \text{ such that if } q \neq p \text{ then } c_q \equiv p^{-1} \bmod q^{n(q)} \mathfrak{o}_q\}.$$

If X is a subset of $C^k(N)$, we define

$$(4.4) \qquad s(X) = \textstyle\sum_{x \in X} (x).$$

We now define $r^k(N) = r(N)$ by

$$(4.5) \qquad r(N)(a) = s(X(a)) \textstyle\sum_{p \mid f(a)} \left(1 - \dfrac{s(X_p(N))}{|X_p(N)|}\right),$$

so that $r(N)(a) \in \mathbf{Q}[C(N)]$. We first show that $r(N)$ is a $GL_k(N)$-map.

PROPOSITION 4.6. — *Let* $\gamma \in GL_k(N)$. *Then*

$$r(N)(\gamma\, a) = \gamma(r(N)(a)).$$

Proof. — It is clear that $f(\gamma\, a) = f(a)$. Set

$$\varepsilon = \textstyle\prod_{p \mid f(a)} \left(1 - \dfrac{s(X_p(N))}{|X_p(N)|}\right).$$

Multiplication by ε is an element of $\mathrm{End}(\mathbf{Q}^k(N))$. Then

$$r(N)(a) = \varepsilon(s(X(a))) \qquad \text{and} \qquad r(N)(\gamma\, a) = \varepsilon(s(X(\gamma\, a))).$$

From (4.1), it is clear that $s(X(\gamma\, a)) = \gamma\, s(X(a))$. So it suffices to show that

$$\gamma\varepsilon = \varepsilon\gamma \quad \text{for all } \gamma \in GL_k(N).$$

Let

$$(4.7) \qquad \varepsilon_p(N) = 1 - \frac{s(X_p(N))}{|X_p(N)|}.$$

It then suffices to show that $\gamma\varepsilon_p(N) = \varepsilon_p(N)\,\gamma$, or that

$$s(X_p(N))\,\gamma(c) = \gamma(s(X_p(N))\, c) \qquad \text{for} \quad c \in C^k(N).$$

Now $s(X_p(N))\,c = s(X)$, where

$$X = \{x \in C^k(N) \text{ such that } x_q = p^{-1} c_q \text{ for all } q \neq p\},$$

$$\gamma X = \{x \in C^k(N) \text{ such that } x_q = p^{-1}(\gamma c_q) \text{ for all } q \neq p\}.$$

Thus $\gamma \varepsilon_p(N) = \varepsilon_p(N)\gamma$, and the Proposition follows.

Next we show that the maps $\gamma(N)$ are compatible with the injective limits. If $M \mid N$, we let $i : \mathbf{Q}[C(M)] \to \mathbf{Q}[C(N)]$ be the map of (2.7):

PROPOSITION 4.8. — *If $M \mid N$, the following diagram commutes.*

$$\begin{tikzcd}
\frac{1}{M}\mathbf{Z}^k/\mathbf{Z}^k \arrow[r, "r(M)"] \arrow[d] & \mathbf{Q}[C^k(M)] \arrow[d] \\
\frac{1}{N}\mathbf{Z}^k/\mathbf{Z}^k \arrow[r, "r(N)"'] & \mathbf{Q}[C^k(N)].
\end{tikzcd}$$

Proof. — Let $c_1, c_2 \in C^k(M)$. Set

$$N = \textstyle\prod_p p^{n(p)} \quad \text{and} \quad M = \prod_p p^{m(p)}.$$

Then

$$i(c_1\, c_2) = \frac{C(M)}{C(N)}\, i(c_1)\, i(c_2). \tag{4.9}$$

If g is the number of distinct prime factors of $f(a)$, we have

$$i(r(M)(a)) = \left(\frac{|C(M)|}{|C(N)|}\right)^g i(s(X_M(a)) \textstyle\prod_{p \mid f(a)} i\left(1 - \dfrac{s(X_p(M))}{|X_p(M)|}\right).$$

Now $i(s(X_M(a)) = s(X_N(a))$ because

$$(M/f(a))\,x_p \equiv (M\,a)_p \bmod p^{m(p)},$$

is equivalent with

$$(N/f(a))\,x_p \equiv (N\,a)_p \bmod p^{n(p)}.$$

But $i(1) = \sum(c)$, where the sum is taken for $c \equiv 1 \bmod M$,

$$i(s(X_p(M)) = s(X_p(N))\, i(1) \frac{|X_p(M)|}{|X_p(N)|}.$$

So

$$\textstyle\prod_{p \mid f(a)} i\left(1 - \dfrac{s(X_p(M))}{|X_p(M)|}\right) = \prod_{p \mid f(a)} i(1)\left(1 - \dfrac{s(X_p(N))}{|X_p(N)|}\right).$$

But

$$s(X_N(a))\,i(1) = |\,i(1)\,|\,s(X_N(a)) = \frac{|\,C(N)\,|}{|\,C(M)\,|}\,s(X_N(a)),$$

which proves the Proposition.

PROPOSITION 4.10. — *The maps* $r(N)$ *define a distribution. Precisely, let* $f(a) = N$ *and* $M \mid N$. *Then*

$$\sum_{Mb=Ma} r(N)(b) = r(N)(M\,a).$$

Proof. — By induction we may assume that $M = q$ is prime. We distinguish the cases $q \mid (N/q)$ and $q \nmid (N/q)$.

First suppose $q \mid (N/q)$. In this case, each b such that $qb = qa$ is primitive, i. e. has order N. So

$$\sum_b r(N)(b) = \sum_b s(X(b)) \prod_{p \mid N}\left(1 - \frac{s(X_p)}{|\,X_p\,|}\right).$$

Set $a' = qa$. Since $q \mid (N/q)$, it follows that $p \mid f(a')$ if, and only if, $p \mid N$. So

$$r(N)(a') = s(X(qa)) \prod_{p \mid N}\left(1 - \frac{s(X_p)}{|\,X_p\,|}\right).$$

So we need only show that

$$X(qa) = \bigcup_{qb=qa} X(b).$$

Since b is primitive, we have $X(b) = \{\, N\,b \,\}$, and

$c \in X(qa)$ if and only if $c_p = N\,a_p$ for $p \neq q$ and $qc_q = q\,N\,a_q$.

But this is equivalent to $qc/N = qa$. So

$$\sum_b s(X(b)) = s(X(q(a))),$$

and the Proposition is proved in this case.

Next suppose $q \nmid (N/q)$. If $qb = qa$ then $b_p = a_p$ for $p \neq q$ and $q(b_q - a_q) \in \mathfrak{o}_q$. Since $q \nmid (N/q)$, it follows that $qa_q \in \mathfrak{o}_q$. Define $\bar{b}$ to be the element such that $\bar{b}_q = 0$, and if $q \neq p$, then $\bar{b}_q = a_q$. Thus if $qb = qa$ and b does not equal $\bar{b}$, we see that $b_q \notin \mathfrak{o}_q$, and that $f(b) = f(a) = N$. Now

$$\sum_{qb=qa} r(N)(b) = \sum_{b \neq \bar{b}} r(N)(b) + r(N)(\bar{b}).$$

If $b \neq \bar{b}$ we have

$$r(N)(b) = (N\,b) \prod_{p \mid N}\left(1 - \frac{s(X_p)}{|\,X_p\,|}\right).$$

Therefore

$$\textstyle\sum_{b \neq b} r(N)(b) = (\sum_{b \neq \bar{b}} (N\, b)) \prod_{p \mid N} \left(1 - \frac{s(X_p)}{|X_p|}\right)$$

$$\textstyle = (\sum_{b \neq \bar{b}} (N\, b)) \prod_{p \neq q} \left(1 - \frac{s(X_p)}{|X_q|}\right)$$

$$\textstyle - \frac{1}{|X_q|} (\sum_{b \neq \bar{b}} s(X_q)(N\, b)) \prod_{b \neq \bar{b}} \left(1 - \frac{s(X_p)}{|X_p|}\right).$$

Set $a' = qa$. Then $f(a') = f(\bar{b}) = N/q$. Furthermore,

$$X(\bar{b}) = \{ c \in C(N) \text{ such that } qc_p = N\, a_p \bmod p^{n(p)} \text{ if } p \neq q$$
$$\text{and } qc_q = 0 \bmod q \}$$

$$\textstyle r(N)(\bar{b}) = s(X(\bar{b})) \prod_{p \neq q} \left(1 - \frac{s(X_p)}{|X_p|}\right).$$

Now from the above,

$$\textstyle s(X_q) \sum_{b \neq \bar{b}} (N\, b) = |X_q| \, s(X(\bar{b})).$$

So

$$\textstyle \frac{1}{|X_q|} (\sum_{b \neq \bar{b}} s(X_q)(N\, b)) \prod_{p \neq q} \left(1 - \frac{s(X_p)}{|X_p|}\right) = r(N)(\bar{b}),$$

and thus

$$\textstyle \sum_{qa = qb} r(N)(b) = (\sum_{b \neq \bar{b}} (N\, b)) \prod_{p \neq q} \left(1 - \frac{s(X_p)}{|X_n|}\right).$$

It is immediate from the Definitions that

$$\textstyle s(X(a')) = \sum_{b \neq \bar{b}} (N\, b).$$

Since

$$\textstyle r(N)(a') = s(X(a')) \prod_{p \neq q} \left(1 - \frac{s(X_p)}{|X_p|}\right),$$

The Proposition is proved in this case also.

THEOREM 4.11. — *The maps $r(N)$ define the universal distribution, and we have*

$$r(N)\, U(N) \otimes \mathbf{Q} = \mathbf{Q}[C(N)].$$

Proof. — Let $V(N) = r(N)\, U(N)$ and $V_{\mathbf{Q}}(N) = \mathbf{Q} \otimes V(N)$. Then $V(N)$ is a $C(N)$-module. Recall that a divisor M of N is called admissible if $(M, N/M) = 1$. Then the distribution relations show that $V(N)$ is generated as a $\mathbf{Z}$-module by $r(N)\,b$, where $f(b) = M$, M admissible. Since for any element $c \in C(N)$ we have

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

we conclude that the elements $r(N)(1/M)$ with admissible divisors M of N generate $V(N)$ as a $C(N)$-module. Here $1/M$ means the element with p-component $1/M$ for each $p \mid N$,

$$\frac{1}{M} \in \frac{1}{p^{n(p)}}\mathfrak{o}_p/\mathfrak{o}_p.$$

Put $R(N) = \mathbf{Z}[C(N)]$ and $R_{\mathbf{Q}}(N) = \mathbf{Q}[C(N)]$. Let

$$(4.12) \qquad V_p = s(X(p^{n(p)}/N))\,R(N) + \left(1 - \frac{s(X_p)}{|X_p|}\right) R(N).$$

Then we claim that

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

We first see that

$$|X_p| = |X_p|\left(1 - \frac{s(X_p)}{|X_p|}\right) + s(X_p),$$

so it suffices to show that

$$s(X_p) \in s(X(p^{n(p)}/N))\,R(N).$$

Let $\lambda \in C(N)$ be such that $\lambda_q \equiv p^{-1} \bmod q^{n(q)}$ for $q \neq p$. Now

$$X(p^{n(p)}/N) = \{c \in C(N) \text{ such that } c_q \equiv 1 \bmod q^{n(q)} \text{ for } q \neq p\}.$$

So $\lambda X(p^{n(p)}/N) = X_p$ and $s(X_p) \in s(X(p^{n(p)}/N))\,R(N)$. Thus the following Proposition will prove the Theorem.

PROPOSITION 4.13. – $V(N) = \prod_{p \mid N} V_p$.

Proof. – The proof here follows as in SINNOTT [S]. Set

$$V_N = \prod_{p \mid N} V_p, \qquad \text{and} \qquad \bar{N} = \prod_{p \mid N} p.$$

Also let

$$\gamma_p = 1 - \frac{s(X_p)}{|X_p|}.$$

As an $R(N)$-module, V_N is generated by the following elements:

$$\prod_{q \mid (\bar{N}/\bar{M})} s\left(X\left(\frac{q^{n(q)}}{N}\right)\right) \prod_{p \mid \bar{M}} \gamma_p \quad \text{for all divisors } \bar{M} \mid \bar{N}.$$

But it is easy to see that

$$\prod\nolimits_{q \mid (\bar{N}/\bar{M})} s\left(X\left(\frac{q^{n(q)}}{N}\right)\right) = s\left(X\left(\frac{1}{M}\right)\right)$$

where $M = \prod_{p \mid \bar{M}} p^{n(q)}$ and M is admissible. Moreover,

$$\prod\nolimits_{p \mid \bar{M}} \gamma_p = \prod\nolimits_{p \mid M} \gamma_p,$$

which proves the Proposition and thus also Theorem 4.11.

We now summarize our knowledge about $U^k(N)$.

THEOREM 4.14.

(i) *$U^k(N)$ is a free **Z**-module of rank $|C^k(N)|$.*

(ii) *$U^k(N) \otimes \mathbf{Q}$ is isomorphic to the free **Q**-vector space on $Z_k^*(N)$ as a $GL_k(\mathbf{Z}/N\mathbf{Z})$-module.*

(iii) $\dot{D}^k(N) = D_N^k$.

(iv) *The map $\Phi_k(N)$, $k \geqslant 2$, is an isomorphism of $U^k(N)$ with its image as a $C^k(N)$-module.*

(v) *The map $r_k(N)$, $k \geqslant 1$, is an isomorphism of $U^k(N)$ with its image, as a $GL_k(\mathbf{Z}/N\mathbf{Z})$-module.*

Finally, we draw some conclusion about the universal even and odd ordinary distribution. We define U_+^k to be the quotient module of U^k obtained from the relations

$$(x)-(-x)=0, \qquad x \in \mathbf{Q}^k/\mathbf{Z}^k.$$

We define U_-^k to be the quotient module of U^k obtained from the relations

$$(x)+(-x)=0, \qquad x \in \mathbf{Q}^k/\mathbf{Z}^k.$$

Let $U_+^k(N)$ (resp. $U_-^k(N)$) be the groups generated by the image of $(1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$ in U_+^k (resp. U_-^k). We have the following Corollary.

COROLLARY 4.15.

(i) *$U_+^k(N) \otimes \mathbf{Q}$ has rank equal to $(1/2)\,|C^k(N)|$.*

$U_-^k(N)$ has rank equal to $(1/2)\,|C^k(N)|$ if $N > 2$.

(ii) *If $N = 2$, then rank $U_+^k(N) \otimes \mathbf{Q} = 2^k - 1$, and*

$$\operatorname{rank} U_-^k(N) \otimes \mathbf{Q} = 0.$$

If $N = 1$, then

$$\operatorname{rank} U_+^k(N) \otimes \mathbf{Q} = 1 \qquad \text{and} \qquad \operatorname{rank} U_-^k(N) \otimes \mathbf{Q} = 0.$$

(iii) *We have isomorphisms as* $\mathbf{Z}/2\,\mathbf{Z}$*-vector spaces:*

$$U^k_+\,(\text{torsion}) \approx H^1(\pm\text{id},\, U^k),$$

$$H^k_-\,(\text{torsion}) \approx H^0(\pm\text{id},\, U^k).$$

Proof. — Statements (i) and (ii) follow directly from Theorem 4.17 (ii). To prove (iii) we use Theorem 4.17 (i). Suppose

$$\bar{u} \in U^k_+(N), \qquad n\bar{u} = 0.$$

Let u belong to $U^k(N)$ such that the image of u in $U^k_+(N)$ is $\bar{u}$. Then, since nu is a relation, we have

$$n((u)+(-u)) = 0,$$

where $-u$ represents the action of -1 as an element of $GL_k(\hat{\mathbf{Z}})$ on u. Since $U^k(N)$ is torsion free, we must have $(u)+(-u) = 0$, or $u \in Z^1(\pm\text{ id},\, U^k(N))$. Then $\bar{u} = 0$ if and only if u is a boundary. The argument is similar for U^k_- (torsion). This proves Corollary 4.15.

When $k = 1$, the resultats of Corollary 4.15 (i) and (ii) were previously obtained by BASS [B] and YAMAMOTO [Y] in the even and odd casse respectively. In the case $k = 2$, the calculation of $H^0(\pm\text{ id},\, U^k)$ has an intepretation in the theory of modular forms (*see* [K 2]). We will calculate these cohomology groups in a following paper.

Appendix

The following broader notion has also proved useful in certain applications, e. g. Bernoulli polynomials on $\mathbf{Q}/\mathbf{Z}$, and also [Ma], [Mi]. Let A be an abelian group and let

$$g:\ \mathbf{Q}^k/\mathbf{Z}^k \to A,$$

be a map. We say that g is a distribution of weight w (a positive integer), if for each positive integer N we have

$$\textbf{(A1)} \qquad N^w \textstyle\sum_{Nb=a} g(b) = g(a).$$

For $k = 1$, the Bernoulli polynomial $B_w(X)$ yields a distribution of weight $w-1$. One may clearly speak of the universal distribution on $\mathbf{Q}^k/\mathbf{Z}^k$ of weight w, and we denote it by $U^{k,\,w}$. We may also speak of the level groups $U^{k,w}(N)$. There is a rational isomorphism of $U^{k,w}(N)$ into the group ring $\mathbf{Q}[C^k(N)]$ given by

$$\text{(A 2)} \qquad r^{k,w}(N)(a) = f(a)^{-w} s(X(a)) \prod\nolimits_{p \mid f(a)} \left(1 - p^w \frac{s(X_p(N))}{|X_p(N)|}\right),$$

where $a \in (1/N)\,\mathbf{Z}^k/\mathbf{Z}^k$. We have the following analogue of Theorem 4.17.

THEOREM :

(i) *$U^{k,w}(N)$ is a free $\mathbf{Z}$-module of rank $|C^k(N)|$.*

(ii) *$U^{k,w}(N) \otimes \mathbf{Q}$ is isomorphic to the free $\mathbf{Q}$-vector space on $Z_k^*(N)$ as a $GL_k(\mathbf{Z}/N\,\mathbf{Z})$-module.*

The proof is as follows. By **(A 2)** we see as before that $U^{k,w}(N)$ has free rank at least $|C^k(N)|$. The Theorem will therefore follow if we can show that $U^{k,w}(N)$ is generated as an abelian group by at most $|C^k(N)|$ elements. It is clear from **(A 1)** that the elements we chose in Section 1 in the case $w = 0$ will no longer generate $U^{k,w}(N)$ for $w > 0$. We now proceed as follows. Define

$$\text{(A 3)} \qquad \langle a \rangle = \sum\nolimits_{(N/f(a))\,b = a} (b),$$

so

$$\text{(A 4)} \qquad (N/f(a))^w \langle a \rangle = (a).$$

We prove the following, distribution law" for $\langle a \rangle$.

LEMMA. — *Let p be a prime such that p divides $N/f(a)$.*

(i) *If $p \mid f(a)$, then*

$$\sum\nolimits_{pb = a} \langle b \rangle = \langle a \rangle.$$

(ii) *If $p \nmid f(a)$, then*

$$\sum\nolimits_{pb = a,\, f(b) = pf(a)} \langle b \rangle = \langle a \rangle - p^w \langle p^{-1} a \rangle.$$

Proof. — For (i), we have

$$\begin{aligned} \sum\nolimits_{pb = a} \langle b \rangle &= \sum\nolimits_b \sum\nolimits_{(N/p)\,f(a)\,c = b} (c) \\ &= \sum\nolimits_{(N/f(a))\,c = a} (c) = \langle a \rangle. \end{aligned}$$

For (ii), we have

$$\begin{aligned} \sum\nolimits_{pb = a,\, f(b) = pf(a)} \langle b \rangle &= \sum\nolimits_b \sum\nolimits_{(N/p)\,f(a)\,c = b} (c) \\ &= \sum\nolimits_{(N/f(a))\,c = a} (c) - \sum\nolimits_{(N/p)\,f(a)\,c = p^{-1}a} (c) \\ &= \langle a \rangle - p^w \sum\nolimits_{(N/f(a))\,d = p^{-1}a} (d) \quad \text{by } \textbf{(A 1)} \\ &= \langle a \rangle - p^w \langle p^{-1} a \rangle. \end{aligned}$$

We may now proceed as in Section 1 to show that the family of elements $\{\langle a \rangle\}$ with $a \in T(N)$ generates $U^{k,w}(N)$ by using the distribution relations for $\langle a \rangle$. This completes the proof of the Theorem.

One special feature when $w > 0$ is that $U^{k,w}(N) \otimes \mathbf{Q}$ has as a $\mathbf{Q}$-basis the elements (x), where $x \in Z_k^*(N)$. This may be proved easily by induction. We must only show that the elements of exact denominator N/p belong to the $\mathbf{Q}$-vector space generated by $Z_k^*(N)$. This is obvious from the distribution relations if $(N/p, p) \neq 1$. Suppose $p \nmid (N/p)$. Let $x \in Z_k^*(N/p)$. Then modulo the distribution relations and the image of $Z_k^*(N)$ in $U^{k,w}(N)$, the element (x) is congruent to $p^w(p^{-1}x)$, where

$$(p^{-1}x) \in Z_k^*(N/p).$$

Let v be the order of p in $(\mathbf{Z}/(N/p)\,\mathbf{Z})^*$. Then by induction we see that (x) is congruent to $p^{wv}(x)$ modulo the image of $Z_k^*(N)$ in $U^{k,w}(N)$. So $(p^{wv}-1)(x)$ belongs to the group generated by $Z_k^*(N)$ in $U^{k,w}(N)$. Since $w > 0$, we have $p^{wv}-1 \neq 0$, and the result follows by tensoring with $\mathbf{Q}$. The corresponding statement when $w = 0$ is not true.

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. 224, 1976, p. 21-31.

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

[K-L] Kubert (D.) and Lang (S.). — Distributions on toroidal groups, *Math. Z.*, t. 148, 1976, p. 33-51.

[Ma] Mazur (B.). — *Analyse p-adique*, Bourbaki report, 1972.

[Mi] Milnor (J.). — *Notes on volume in hyperbolic space* (to appear).

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

[Y] Yamamoto (K.). — The gap group of multiplicative relationships of gaussian sums, "*Symposia Mathematica*, 15", p. 427-440. — London, Academic Press, 1975.