GENERATORS AND RELATIONS FOR CYCLOTOMIC UNITS

HYMAN BASS

To the memory of TADASI NAKAYAMA

1. Introduction

We prove here an unpublished conjecture of Milnor which gives a complete set of multiplicative relations between the numbers

$$e'(\zeta) = 1 - \zeta,$$

where $\zeta \neq 1$ ranges over complex roots of unity. Information of this type is useful in certain areas of topology as well as in number theory.

2. Statement of the theorem

Clearly

$$\text{(A)} \qquad e'(\zeta^{-1}) = -\zeta^{-1}e'(\zeta).$$

Suppose $\zeta^n \neq 1$. In

$$t^n - 1 = \prod_{\eta^n = 1} (t - \eta)$$

substitute ζ^{-1} for t to obtain

$$\zeta^{-n} - 1 = \prod_{\eta^n = 1} \zeta^{-1}(1 - \zeta\eta),$$

and then multiply by ζ^n, yielding

$$\text{(B)} \qquad e'(\zeta^n) = \prod_{\eta^n = 1} e'(\eta\zeta) \qquad \text{if } \zeta^n \neq 1.$$

MILNOR'S CONJECTURE. *All multiplicative relations, modulo torsion, between the* $e'(\zeta)$, *are consequences of* (*A*) *and* (*B*) *above.*

The following theorem is slightly more precise.

THEOREM 1. *Let* U'_m *denote the multiplicative group generated by all* $e'(\zeta)$

Received June 30, 1965.

$=1-\zeta$ *with* $\zeta^m=1$, $\zeta\neq 1$. *Let* U_m *equal* U'_m *modulo its torsion subgroup, and denote by* $e(\zeta)$ *the image in* U_m *of* $e'(\zeta)$. *Let us, moreover, write* U_m *additively. Then a set of defining relations between the generators* $e(\zeta)$ *of* U_m *is: For all* $\zeta\neq 1$ *such that* $\zeta^m=1$

$(A)_m$ $$e(\zeta^{-1})=e(\zeta)$$

and,

$(B)_m$ *if* n *divides* m *and* $\zeta^n\neq 1$ *then* $e(\zeta^n)=\sum_{\eta^n=1} e(\eta\zeta)$.

3. U_m as a Galois Module

We shall apply the following useful lemma extracted from Artin-Tate ([1], Ch. I).

LEMMA (Dirichlet, Artin-Tate). *Let* K/k *be a finite galois extension of number fields with group* G, *and let* S *be a finite set of primes of* k *containing all archimedean primes. Let* K_S *denote the group of* S*-units, i.e., elements of absolute value one at all primes of* K *not above one in* S. *Then* K_S *is a finitely generated* G*-module, and there is a* G*-isomorphism*

$$\mathbf{Q}\otimes_{\mathbf{Z}}(K_S\oplus\mathbf{Z})\cong\mathbf{Q}\otimes_{\mathbf{Z}}(\bigoplus_{\mathfrak{p}\in S} M_{\mathfrak{p}}).$$

Here G *acts trivially on* $\mathbf{Z}$ *and* $\mathbf{Q}$, *and* $M_{\mathfrak{p}}$ *is the* $\mathbf{Z}[G]$*-module defined by the permutation representation of* G *on the set of* $\mathfrak{P}$ *above* $\mathfrak{p}$.

Proof. Let E be a real vector space with the primes $\mathfrak{P}$ which lie above one of S as a basis, and let $L: K_S\to E$ be the Dirichlet map. Thus $L(a)=\sum_{\mathfrak{P}}(\log|a|_{\mathfrak{P}})\mathfrak{P}$, where $|\ |_{\mathfrak{P}}$ is the normalized absolute value at $\mathfrak{P}$. From the Dirichlet Unit Theorem, ker L is the torsion subgroup of K_S, and im L is a lattice of maximal rank in the product formula hyperplane: $\sum x_{\mathfrak{P}}=0$. G permutes the $\mathfrak{P}$'s and hence operates on E, and we now observe that L is a G-homomorphism:

$$\begin{aligned} L(\sigma a) &= \textstyle\sum_{\mathfrak{P}}(\log|\sigma a|_{\mathfrak{P}})\mathfrak{P} \\ &= \textstyle\sum_{\mathfrak{P}}(\log|\sigma a|_{\sigma\mathfrak{P}})\sigma\mathfrak{P} \\ &= \textstyle\sum_{\mathfrak{P}}(\log|a|_{\mathfrak{P}})\sigma\mathfrak{P} \\ &= \sigma L(A). \end{aligned}$$

If $x=\sum_{\mathfrak{P}}\mathfrak{P}$ then $\mathbf{Z}x$ is a G-submodule of E, with trivial action, and

$L(K_S)\oplus\mathbf{Z}x$ is a lattice of maximal rank in E. Hence the natural map

$$\mathbf{R}\otimes_{\mathbf{Z}}(L(K_S)\oplus\mathbf{Z}x)\rightarrow E$$

is an isomorphism of G-modules.

If $M=\sum_{\mathfrak{P}}\mathbf{Z}\mathfrak{P}$ then $\mathbf{R}\otimes_{\mathbf{Z}}M\rightarrow E$ is similarly a G-isomorphism. Hence $\mathbf{Q}\otimes_{\mathbf{Z}}M$ and $\mathbf{Q}\otimes_{\mathbf{Z}}(L(K_S)\oplus\mathbf{Z}x)\cong\mathbf{Q}\otimes_{\mathbf{Z}}(K_S\oplus\mathbf{Z})$ are $\mathbf{Q}[G]$-modules which become isomorphic after scalar extension from $\mathbf{Q}$ to $\mathbf{R}$. They are therefore already isomorphic, and the lemma is proved.

We now apply the lemma to $\mathbf{Q}_m$, the field generated by all primitive m^{th} roots of unity. Let $\Phi(m)=\mathrm{Gal}(\mathbf{Q}_m/\mathbf{Q})$. If ζ is a primitive m^{th} root of unity, $\mathbf{Q}'_m=\mathbf{Q}(\zeta+\zeta^{-1})$ is the real subfield, and $\Phi'(m)=\Phi(m)/$(complex conjugation) is its galois group over $\mathbf{Q}$. The cardinality of $\Phi(m)$ is $\varphi(m)$ (Euler φ), and that of $\Phi'(m)$ is $\varphi(m)/2$ if $m>2$.

COROLLARY. *Let V'_m denote the group of units in the ring of integers of $\mathbf{Q}_m$. Then $\mathbf{Q}\otimes_{\mathbf{Z}}(V'_m\oplus\mathbf{Z})$ is a free $\mathbf{Q}[\Phi'(m)]$-module on one generator.*

Proof. Let S be the archimedean prime of $\mathbf{Q}$. $\Phi(m)$ permutes the archimedean primes of $\mathbf{Q}_m$ transitively, with complex conjugation generating the isotropy group of each. The corollary is now immediate from the lemma.

We require next some classical facts about cyclotomic units.

LEMMA. *Let ζ be a primitive m^{th} root of unity, $m>1$.* (1) (see [2], Lemma 7.3). *If $N=N_{\mathbf{Q}_m/\mathbf{Q}}$ then $Ne(\zeta)=1$ if m is not a prime power and $Ne(\zeta)=p$ if m is a power of the prime p.*

(2) (see [2], §7 and Corollary to Theorem 4) *$N: U'_m\rightarrow\mathbf{Q}^*$ is a homomorphism whose image is generated by positive powers of the primes dividing m, and whose kernel is $U'_m\cap V'_m$ and has finite index in V'_m.*

The preceding lemma and corollary yield:

THEOREM 2. *As a $\Phi(m)$-module*

$$\mathbf{Q}\otimes_{\mathbf{Z}}U_m\cong\mathbf{Q}[\Phi'(m)]\oplus\mathbf{Q}^{\Pi(m)-1}.$$

Here $\Phi(m)$ acts trivially on $\mathbf{Q}$, and $\Pi(m)$ is the number of prime divisors of m. In particular U_m is a free abelian group of rank $\varphi(m)/2+\Pi(m)-1$.

4. The prime power case

THEOREM 3. *Suppose $q=p^n$ with p prime, $n>0$. Then Theorem 1 is valid* *for $m = q$. Moreover*

$$U_q \cong \mathbf{Z}[\Phi'(q)]$$

as a $\Phi(q)$-module, and $e(\zeta)$ is a generator for any primitive q^{th} root of unity, ζ.

Proof. If $\zeta_1 = \zeta^p$ is a primitive p^{ith} root of unity with $i < n$ then relations $(B)_q$ yield $e(\zeta_1) = \sum_{\eta^p=1} e(\eta\zeta)$, and each $\eta\zeta$ here is a primitive $p^{i+1}th$ root of unity. By induction, then, $(B)_q$ implies U_q is generated by the $e(\zeta)$ with ζ a primitive q^{th} root of unity. Since $\Phi(q)$ permutes the latter transitively it follows that any of them generates U_q as $\Phi(q)$-module. Choosing such a generator yields an epimorphism $\mathbf{Z}[\Phi(q)] \to U_q$. Relations $(\mathrm{A})_q$ imply this factors through the quotient, $\mathbf{Z}[\Phi'(q)]$, of $\mathbf{Z}[\Phi(q)]$. Theorem 2 above shows that $\mathbf{Z}[\Phi'(q)]$ and U_q are free abelian of the same rank, so an epimorphism is an isomorphism.

5. The general case

Let $\overline{U}_m$ be an abelian group with generators $\bar{e}(\zeta)$ subject only to relations $(\mathrm{A})_m$ and $(\mathrm{B})_m$. Let $\overline{U}_m \to U_m$ be the epimorphism sending $\bar{e}(\zeta)$ to $e(\zeta)$. Theorem 1 asserts this is an isomorphism, and Theorem 3 proves it for m a prime power.

If $\sigma \in \Phi(m)$ we let σ operate on $\overline{U}_m$ by $\sigma\bar{e}(\zeta) = \bar{e}(\sigma\zeta)$. This is clearly compatible with $(\mathrm{A})_m$ and $(\mathrm{B})_m$, and it makes $\overline{U}_m \to U_m$ a homomorphism of $\Phi(m)$-modules.

Suppose m has prime factorization $m = p_1^{n_1} \cdots p_r^{n_r} = q_1 \cdots q_r$ where $q_i = p_i^{n_i}$ and $r > 1$. Let $m_i = m/q_i$, $1 \le i \le r$. We assume by induction on r that $\overline{U}_{m_i} \to U_{m_i}$ is an isomorphism. It follows, in particular, that $\overline{U}_{m_i}$ can be identified with a submodule of $\overline{U}_m$. As such we have $\overline{U}_m^{(1)} = \sum_{1 \le i \le r} \overline{U}_{m_i} \subset \overline{U}_m$, which maps onto $U_m^{(1)} = \sum_{1 \le i \le r} U_{m_i} \subset U_m$.

The following technical lemma generalizes Theorem 3.

Lemma. *Let N_i denote the "norm element" (i.e., the sum of the group elements) in $\mathbf{Z}[\Phi(q_i)]$, and let $M_i = \mathbf{Z}[\Phi(q_i)]/\mathbf{Z}N_i$. We have $\Phi(m) = \prod_{1 \le i \le r} \Phi(q_i)$ so $M' = \bigotimes_{i \le i \le r} M_i$ is a $\Phi(m)$-module. Let $M = \mathbf{Z}[\Phi'(m)] \otimes_{\mathbf{Z}[\Phi(m)]} M'$, i.e., M' reduced by complex conjugation. Then $\overline{U}_m \to U_m$ induces an isomorphism $\overline{U}_m/\overline{U}_m^{(1)} \to U_m/U_m^{(1)}$ and the latter are isomorphic to M as $\Phi(m)$-modules.*

Proof. Let Ψ_m denote the group of m^{th} roots of unity and Φ_m the primitive

m^{th} roots. Suppose $m = p^n m'$ with p a prime not dividing m'. Then $\Psi_m = \Psi_{p^n} \times \Psi_{m'}$ as groups, and $\Phi_m = \Phi_{p^n} \times \Phi_{m'}$ as sets.

If $\eta \in \Psi_{p^n}$ and $\zeta \in \Psi_{m'}$, not both 1, then $\bar{e}(\eta\zeta)$ is a typical generator of $\bar{U}_m$. Suppose $\eta \in \Phi_{p^i}$ with $0 < i < n$, so $\eta = \eta_1^p$ for some $\eta_1 \in \Phi_{p^{i+1}}$. Likewise, we can write $\zeta = \zeta_1^p$ with $\zeta_1 \in \Psi_{m'}$ since p doesn't divide m'. Then from $(\mathrm{B})_m$ $\bar{e}(\eta\zeta) = \bar{e}((\eta_1\zeta_1)^p) = \sum_{\nu\in\Psi_p} \bar{e}((\nu\eta_1)\zeta_1)$, and each $\nu\eta_1 \in \Phi_{p^{i+1}}$ since $\eta_1 \in \Phi_{p^{i+1}}$ and $i \geq 1$.

Now let $\zeta' \neq 1$ be any element of Ψ_m. Letting p above range over the prime divisors of the order of ζ, and applying the remark of the last paragraph to each, we deduce easily that $\bar{U}_m$ is generated by the elements $e(\zeta)$ where ζ has order $\prod_{i\in I} q_i$ for some $I \subset \{1, \ldots, r\}$. In other words, each prime divides the order of ζ to the same power that it divides m, if at all. In particular, $\tilde{U}_m = \bar{U}_m / \bar{U}_m^{(1)}$ is generated by the images, $\tilde{e}(\zeta)$, of $\bar{e}(\zeta)$, where ζ ranges over Φ_m.

Set theoretically, $\Phi_m = \prod_{1\leq i\leq r} \Phi_{q_i}$, and this decomposition is compatible with the operation of $\Phi(m) = \prod_{1\leq i\leq r} \Phi(q_i)$ on the generators $\tilde{e}(\zeta)$ of $\tilde{U}_m$. Thus we obtain, after fixing some $\zeta \in \Phi_m$, an epimorphism

$$\mathbf{Z}[\Phi(m)] = \bigotimes_{1\leq i\leq r} \mathbf{Z}[\Phi(q_i)] \to \tilde{U}_m.$$

To show that this factors through the quotient, $\bigotimes_{1<i<r} M_i$, we must show that if $m = p^n m'$, p a prime not dividing m', and if $\zeta \in \Phi_{m'}$, then $\sum_{\eta\in\Phi_{p^n}} \tilde{e}(\eta\zeta) = 0$.

For $n = 1$ this follows from

$$\begin{aligned}\sum_{\eta\in\Phi_p} \bar{e}(\eta\zeta) &= \sum_{\eta\in\Psi_p} \bar{e}(\eta\zeta) - \bar{e}(\zeta)\\ &= \bar{e}(\zeta^p) - \bar{e}(\zeta) \in \bar{U}_m^{(1)}.\end{aligned}$$

Moreover, if $n > 1$, then

$$\begin{aligned}\sum_{\eta\in\Phi_{p^n}} \bar{e}(\eta\zeta) &= \sum_{\eta_1\in\Phi_{p^{n-1}}} \sum_{\eta^p=\eta_1} \bar{e}(\eta\zeta)\\ &= \sum_{\eta_1\in\Phi_{p^{n-1}}} \sum_{\nu\in\Psi_p} \bar{e}(\nu\eta_1'\zeta)\\ &= \sum_{\eta_1\in\Phi_{p^{n-1}}} \bar{e}(\eta_1\zeta^p).\end{aligned}$$

Here η_1' is a fixed solution of $(\eta_1')^p = \eta_1$, for each η_1, and, of course, we have invoked relations $(\mathrm{B})_m$ in the last equation. It follows now, by induction on n, that $\sum_{\eta\in\Phi_{p^n}} \tilde{e}(\eta\zeta) = 0$, as claimed, so we have an epimorphism

$$M' = \bigotimes_{1\leq i\leq r} M_i \to \tilde{U}_m.$$

Relations $(A)_m$ imply this factors through $M=$ (M'-reduced-by-complex-conjugation).

We conclude the proof by showing that both epimorphisms

$$M \to \tilde{U}_m \to U_m/U_m^{(1)}$$

are isomorphisms. For this it suffices to show that the rank of $U_m/U_m^{(1)}$ is not less than that of the torsion free module M, and for this we can tensor with $\mathbf{Q}$. Since $\Phi(q_i)$ operates trivially on U_{m_i}, it follows that $\Phi(q_i)$, for some i, operates trivially on each irreducible submodule of $\mathbf{Q}\otimes_{\mathbf{Z}} U_m^{(1)}$. It follows from Theorem 2 that $\mathbf{Q}\otimes_{\mathbf{Z}}(U_m/U_m^{(1)})$ must contain each irreducible $\Phi'(m)$-module for which this is not the case. The latter add up to exactly $\mathbf{Q}\otimes_{\mathbf{Z}} M$, and hence rank $(U_m/U_m^{(1)}) \geq$ rank M, as required.

Proof of Theorem 1: If $I \subset \{1, \ldots, r\}$ let $m_I = \prod_{i \notin I} q_i$. Filter $\bar{U}_m$ by

$$\bar{U}_m^{(j)} = \sum_{\text{card } I=j} \bar{U}_{m_I}.$$

Thus

$$\bar{U}_m = \bar{U}_m^{(0)} \supset \bar{U}_m^{(1)} \supset \cdots \supset \bar{U}_m^{(r-1)} \supset \bar{U}_m^{(r)} = 0.$$

We similarly filter U_m. To show that the (filtration preserving) map $\bar{U}_m \to U_m$ is an isomorphism it suffices to show that it induces isomorphisms

$$\bar{U}_m^{(j)}/\bar{U}_m^{(j+1)} \to U_m^{(j)}/U_m^{(j+1)}, \quad 0 \leq j < r.$$

The lemma above shows this for $j=0$, and that both terms are isomorphic to a certain module, M. Denoting the latter, more precisely, by $M(m)$, we see, from the same lemma, that there is an epimorphism

$$\bigoplus_{\text{card } I=j} M(m_I) \to \bar{U}_m^{(j)}/\bar{U}_m^{(j+1)}.$$

$M(m_I)$ here has the structure of a $\Phi(m)$-module since $\Phi(m_I)$ is, from galois theory, a quotient (and even a direct factor) of $\Phi(m)$. Since $\mathbf{Q}\otimes_{\mathbf{Z}}(\bigoplus_{\text{card } I=j} M(m_I))$ is the sum of those irreducible $\mathbf{Q}[\Phi'(m)]$-modules on which j, but no more, of the $\Phi(q_i)$ operate trivially, and since, by Theorem 2 plus induction, $\mathbf{Q}\otimes_{\mathbf{Z}}$ $(U_m^{(j)}/U_m^{(j+1)})$ must contain each of these irreducible modules, we obtain, as above, the rank inequality necessary to conclude that the epimorphisms

$$\bigoplus_{\text{card } I=j} M(m_I) \to \bar{U}_m^{(j)}/\bar{U}_m^{(j+1)} \to U_m^{(j)}/U_m^{(j+1)}$$

are both isomorphisms. Theorem 1 is thus proved.

Remarks. (1) By introducing a generator for each root of unity, accompanied by relations defining $\mathbf{Q}/\mathbf{Z}$, we can use Theorem 1 in an obvious way to obtain a presentation for U'_m itself, not merely modulo torsion. It would be more interesting, however, to study the extension, $0 \to \text{torsion} \to U'_m \to U_m \to 0$ of $\Phi(m)$-modules.

(2) One could probably push the above arguments further and describe U_m explicitly as a $\Phi(m)$-module, not just modulo extensions. It is undoubtedly much more subtle to analyze the remaining part of the group of units, V'_m/U'_m.

References

[1] E. Artin and J. Tate, *Class Field Theory*, Harvard, 1963.

[2] H. Bass, The Dirichlet Unit Theorem, Induced Characters, and Whitehead Groups of Finite Groups. Topology (to appear).

Columbia University,
New York, N. Y. U.S.A.