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We prove here an unpublished conjecture of Milnor which gives a complete set of multiplicative relations between the numbers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

(A) \[ e'(\zeta^{-1}) = -\zeta^{-1}e'(\zeta). \]

Suppose \( \zeta^n \neq 1 \). In

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

substitute \( \zeta^{-1} \) for \( t \) to obtain

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

and then multiply by \( \zeta^n \), yielding

(B) \[ e'(\zeta^n) = \prod_{\eta^n = 1} e'(\etaζ) \quad \text{if} \quad \zeta^n \neq 1. \]

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^n = 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 \( \zeta^n = 1 \)

\[(A)_m \quad e(\zeta^{-1}) = e(\zeta)\]

and,

\[(B)_m \quad \text{if } n \text{ divides } m \text{ and } \zeta^n \neq 1 \text{ then } e(\zeta^n) = \sum_{\eta=1}^{m} e(\eta \zeta).\]

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

\[
\mathbb{Q} \otimes \mathbb{Z}(K_S \oplus \mathbb{Z}) \cong \mathbb{Q} \otimes \mathbb{Z}(\bigoplus_{\mathfrak{p} \in S} M_{\mathfrak{p}}).
\]

Here \( G \) acts trivially on \( \mathbb{Z} \) and \( \mathbb{Q} \), and \( M_{\mathfrak{p}} \) is the \( \mathbb{Z}[G] \)-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 \( L : K_S \rightarrow E \) be the Dirichlet map. Thus \( L(a) = \sum_{\mathfrak{p}} (\log |a|_{\mathfrak{p}}) \mathfrak{p} \), where \( | \cdot |_{\mathfrak{p}} \) 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:

\[
L(\sigma a) = \sum_{\mathfrak{p}} (\log |\sigma a|_{\mathfrak{p}}) \mathfrak{p} \\
= \sum_{\mathfrak{p}} (\log |a|_{\mathfrak{p}}) \sigma \mathfrak{p} \\
= \sum_{\mathfrak{p}} (\log |a|_{\mathfrak{p}}) \sigma \mathfrak{p} \\
= \sigma L(A).
\]

If \( x = \sum_{\mathfrak{p}} \mathfrak{p} \) then \( Zx \) is a \( G \)-submodule of \( E \), with trivial action, and
$L(K_s) \oplus \mathbb{Z}x$ is a lattice of maximal rank in $E$. Hence the natural map

$$R \otimes \mathbb{Z}(L(K_s) \oplus \mathbb{Z}x) \to E$$

is an isomorphism of $G$-modules.

If $M = \sum \mathbb{Z}\mathfrak{p}$ then $R \otimes \mathbb{Z}M \to E$ is similarly a $G$-isomorphism. Hence $\mathbb{Q} \otimes \mathbb{Z}M$ and $\mathbb{Q} \otimes \mathbb{Z}(L(K_s) \oplus \mathbb{Z}x)$ are $\mathbb{Q}[G]$-modules which become isomorphic after scalar extension from $\mathbb{Q}$ to $R$. They are therefore already isomorphic, and the lemma is proved.

We now apply the lemma to $\mathbb{Q}_m$, the field generated by all primitive $m^{th}$ roots of unity. Let $\Phi(m) = \text{Gal}(\mathbb{Q}_m/\mathbb{Q})$. If $\zeta$ is a primitive $m^{th}$ root of unity, $\mathbb{Q}'_m = \mathbb{Q}(\zeta + \zeta^{-1})$ is the real subfield, and $\Phi'(m) = \Phi(m)/(\text{complex conjugation})$ is its galois group over $\mathbb{Q}$. The cardinality of $\Phi(m)$ is $\varphi(m)$ (Euler $\varphi$), 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 $\mathbb{Q}_m$. Then $\mathbb{Q} \otimes \mathbb{Z}(V'_m \oplus \mathbb{Z})$ is a free $\mathbb{Q}[\Phi'(m)]$-module on one generator.

**Proof.** Let $S$ be the archimedean prime of $\mathbb{Q}$. $\Phi(m)$ permutes the archimedean primes of $\mathbb{Q}_m$ 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 $\zeta$ be a primitive $m^{th}$ root of unity, $m > 1$. (1) (see [2], Lemma 7.3). If $N = N_{\mathbb{Q}_m/\mathbb{Q}}$ 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) $N : U'_m \to \mathbb{Q}^*$ 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

$$\mathbb{Q} \otimes \mathbb{Z}U'_m \cong \mathbb{Q}[\Phi'(m)] \oplus \mathbb{Q}^{\Pi(m)-1}.$$  

Here $\Phi(m)$ acts trivially on $\mathbb{Q}$, 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,

\[ U_q \cong \mathbb{Z}[[\Phi(q)]] \]

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

**Proof.** If \( \zeta_i = \zeta^b \) is a primitive \( p_i^{n_i} \)th root of unity with \( i < n \) then relations (B) yield \( e(\zeta_i) = \sum_{\nu \neq 1} e(\nu \zeta) \), and each \( \nu \zeta \) here is a primitive \( p_i^{n_i+1} \)th root of unity. By induction, then, (B) implies \( U_q \) is generated by the \( e(\zeta) \) with \( \zeta \) a primitive \( q^n \)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 \( \mathbb{Z}[[\Phi(q)]] \to U_q \). Relations (A) imply this factors through the quotient, \( \mathbb{Z}[[\Phi(q)]]/\mathbb{Z}[[\Phi(q)]] \). Theorem 2 above shows that \( \mathbb{Z}[[\Phi(q)]] \) and \( U_q \) are free abelian of the same rank, so an epimorphism is an isomorphism.

5. The general case

Let \( \bar{U}_m \) be an abelian group with generators \( \bar{e}(\zeta) \) subject only to relations (A) \( m \) and (B) \( m \). Let \( \bar{U}_m \to U_m \) 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 \( \sigma \) operate on \( \bar{U}_m \) by \( \sigma \bar{e}(\zeta) = \bar{e}((\sigma \zeta)) \). This is clearly compatible with (A) \( m \) and (B) \( m \), and it makes \( \bar{U}_m \to U_m \) 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 \( m_i = m/q_i, \ 1 \leq i \leq r \). We assume by induction on \( r \) that \( \bar{U}_{m_i} \to U_{m_i} \) is an isomorphism. It follows, in particular, that \( \bar{U}_m \), can be identified with a submodule of \( \bar{U}_m \). As such we have \( \bar{U}_m = \sum_{i=1}^r \bar{U}_{m_i} \subset \bar{U}_m \), which maps onto \( U_m = \sum_{i=1}^r U_{m_i} \subset U_m \).

The following technical lemma generalizes Theorem 3.

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

**Proof.** Let \( \mathcal{F}_m \) denote the group of \( m^\text{th} \) roots of unity and \( \Phi_m \) the primitive
$m^{th}$ roots. Suppose $m = p^n m'$ with $p$ a prime not dividing $m'$. Then $\mathcal{F}_m = \mathcal{F}_{p^n} \times \mathcal{F}_{m'}$ as groups, and $\Phi_m = \mathcal{F}_{p^n} \times \Phi_{m'}$ as sets.

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

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

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

$$\mathbb{Z} \left[ \Phi(m) \right] = \bigotimes_{1 \leq i \leq r} \mathbb{Z} \left[ \Phi(q_i) \right] \rightarrow \tilde{U}_m.$$ 

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

For $n = 1$ this follows from

$$\sum_{\eta \in \mathcal{F}_{p^n}} \tilde{e}(\eta \zeta) = \sum_{\eta \in \mathcal{F}_{p^n}} \tilde{e}(\eta \zeta) - \tilde{e}(\zeta) = \tilde{e}(\zeta^p) - \tilde{e}(\zeta) \in \tilde{U}_m^{(1)}.$$ 

Moreover, if $n > 1$, then

$$\sum_{\eta \in \mathcal{F}_{p^n}} \tilde{e}(\eta \zeta) = \sum_{\eta \in \mathcal{F}_{p^{n-1}}} \sum_{\eta \in \mathcal{F}_{p^{n-1}}} \tilde{e}(\eta \zeta) = \sum_{\eta \in \mathcal{F}_{p^{n-1}}} \tilde{e}(\nu \eta \zeta) = \sum_{\eta \in \mathcal{F}_{p^{n-1}}} \tilde{e}(\eta \zeta^p).$$

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

$$M' = \bigotimes_{1 \leq i \leq r} M_i \rightarrow \tilde{U}_m.$$
Relations \((A)_m\) imply this factors through \(M = (M'\text{-reduced-by-complex-conjugation})\).

We conclude the proof by showing that both epimorphisms

\[ M \rightarrow \overline{U}_m \rightarrow U_m/U_m^{(1)} \]

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 \(U_m\), 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 \(I \subseteq \{1, \ldots, r\}\) let \(m_i = \prod_{i \in I} q_i\). Filter \(\overline{U}_m\) by

\[ \overline{U}_m^{(j)} = \sum_{\text{card } I = j} \overline{U}_{m_i}. \]

Thus

\[ \overline{U}_m = \overline{U}_m^{(0)} \supset \overline{U}_m^{(1)} \supset \cdots \supset \overline{U}_m^{(r-1)} \supset \overline{U}_m^{(r)} = 0. \]

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

\[ \overline{U}_m^{(j)} / \overline{U}_m^{(j+1)} \rightarrow U_m^{(j)} / U_m^{(j+1)}, \quad 0 \leq j < r. \]

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

\[ \bigoplus_{\text{card } I = j} M(m_i) \rightarrow \overline{U}_m^{(j)} / \overline{U}_m^{(j+1)}. \]

\(M(m)\) here has the structure of a \(\Phi(m)\)-module since \(\Phi(m)\) is, from galois theory, a quotient (and even a direct factor) of \(\Phi(m)\). Since \(\mathbf{Q} \otimes \mathbf{Z} \left( \bigoplus_{\text{card } I = j} M(m_i) \right)\) 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

\[ \bigoplus_{\text{card } I = j} M(m_i) \rightarrow \overline{U}_m^{(j)} / \overline{U}_m^{(j+1)} \rightarrow U_m^{(j)} / U_m^{(j+1)} \]

are both isomorphisms. Theorem 1 is thus proved.
Remarks. (1) By introducing a generator for each root of unity, accompanied by relations defining $\mathbb{Q}/\mathbb{Z}$, 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


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