§5. Universal Kubert functions

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **29 (1983)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.09.2024**

§5. Universal Kubert functions

The results in this section are either due to Kubert, or are minor variations on results of Kubert.

Let $A \subset \mathbf{Q}/\mathbf{Z}$ be a subgroup, and let s be a fixed integer. A function

$$f : A \to V$$

to a rational vector space will be called a *Kubert function* if it satisfies

$$(*'_s) \qquad f(ma) = m^{s-1} \sum_{0}^{m-1} f(a+k/m)$$

for every integer m such that $1/m$ belongs to A. It will be convenient to say that f is *universal* if every $\mathbf{Q}$-linear relation between the values $f(a)$ follows from these Kubert relations.

Let $U_s(A)$ be the additive group with one generator $u(a)$ for each element of A, and with defining relations $(*'_s)$. *Then evidently f is universal if and only if the induced mapping*

$$u(a) \mapsto f(a)$$

from $U_s(A) \otimes \mathbf{Q}$ to V is injective.

We are primarily interested in the case where A is the entire group $\mathbf{Q}/\mathbf{Z}$. However, it is very useful to consider finite subgroups of $\mathbf{Q}/\mathbf{Z}$, and requires no extra work to consider arbitrary subgroups.

Note that every automorphism of A gives rise to an automorphism of $U_s(A)$. We will use the notation $\mathrm{Hom}(A, A)^{\bullet}$ for the automorphism group of A, identifying it with the group of invertible elements in the ring $\mathrm{Hom}(A, A)$ consisting of all homomorphisms from A to itself.

THEOREM 2. *The complex vector space $U_s(A) \otimes \mathbf{C}$ splits, under the action of the automorphism group of A, into a direct sum of 1-dimensional eigenspaces, with just one eigenspace corresponding to each continuous character*

$$\chi : \mathrm{Hom}(A, A)^{\bullet} \to \mathbf{C}^{\bullet}.$$

Furthermore, any inclusion $A \subset A' \subset \mathbf{Q}/\mathbf{Z}$ gives rise to an embedding $U_s(A) \otimes \mathbf{C} \subset U_s(A') \otimes \mathbf{C}$.

Proofs will be given at the end of this section.

If $A = A_m$ is the cyclic group of order m, note that $\mathrm{Hom}(A, A)$ can be identified with the ring $\mathbf{Z}/m\mathbf{Z}$, and $\mathrm{Hom}(A, A)^{\bullet}$ is an abelian group of order $\varphi(m)$. *In general, $\mathrm{Hom}(A, A)^{\bullet}$ is to be topologized as the inverse limit of these groups*

$$\operatorname{Hom}(A_m, A_m)^\cdot = (\mathbf{Z}/m\mathbf{Z})^\cdot$$

as A_m *varies over all finite subgroups of* A. Similarly, the character group of $\operatorname{Hom}(A, A)^\cdot$ is the direct limit of the corresponding Dirichlet character groups $\operatorname{Hom}((\mathbf{Z}/m\mathbf{Z})^\cdot, \mathbf{C}^\cdot)$.

One interesting consequence of Theorem 2 is the following statement, which is reminiscent of Galois theory.

COROLLARY. *If* $A \subset A' \subset \mathbf{Q}/\mathbf{Z}$, *then* $U_s(A) \otimes \mathbf{Q}$ *can be identified with the subspace of* $U_s(A') \otimes \mathbf{Q}$ *which is fixed by all automorphisms of* A' *over* A.

A proof is easily supplied. □

Here is another consequence.

LEMMA 8. *If* $A = A_m$ *is cyclic of order* m, *then the rational vector space* $U_s(A_m) \otimes \mathbf{Q}$ *has dimension* $\varphi(m)$. *For* $m > 2$ *this splits as the direct sum of even and odd parts with respect to the involution*

$$u(a) \mapsto u(-a)\,,$$

where each of these summands has dimension $\varphi(m)/2$.

Proof. This follows immediately from the corresponding statement for $U_s(A) \otimes \mathbf{C}$. The two summands have equal dimension since there are as many even characters $(\chi(-1) = 1)$ as odd characters $(\chi(-1) = -1)$ modulo m. □

If $s \neq 1$, then Lemma 8 could also be derived from the following more explicit statement.

LEMMA 9. *If* $s \neq 1$, *and if* $A = A_m$ *is cyclic of order* m, *then* $U_s(A) \otimes \mathbf{Q}$ *has a basis consisting of the* $\varphi(m)$ *elements* $u(k/m)$ *with* k *relatively prime modulo* m.

However, this statement definitely fails for $s = 1$.

Another complication when $s = 1$ is that Lemma 7 fails, so that we must also consider "punctured" Kubert functions, which are not defined at zero.

Definition. Let $U_s(A-0)$ be the universal group with one generator $u(a)$ for each $a \neq 0$ in A, and with defining relations

$$u(ma) = m^{s-1} \sum_{0}^{m-1} u(a + k/m)$$

for all m and a with $ma \neq 0$ and $1/m \in A$.

If $s \neq 1$, then the proof of Lemma 7 can be used to show that the kernel and cokernel of the natural maps

$$U_s(A_m - 0) \to U_s(A_m)$$

are finite groups of order prime to m. Taking the direct limit over m, it follows that

$$U_s(\mathbf{Q}/\mathbf{Z} - 0) \cong U_s(\mathbf{Q}/\mathbf{Z}).$$

However, for $s = 1$ the situation is different.

LEMMA 10. *The kernel of the natural homomorphism*

$$U_1(A - 0) \to U_1(A)$$

is a free abelian group freely generated by the elements

$$u(1/p) + u(2/p) + \ldots + u((p-1)/p),$$

as p *ranges over all primes with* $1/p \in A$. *The cokernel of this homomorphism is free cyclic, generated by* $u(0)$.

A proof is easily supplied, using formula (10) of §4 to prove that there are no relations between these generators. □

The precise structure of $U_s(A)$ can be given as follows.

LEMMA 11. *If* $s \leqslant 1$, *or if* A *is finite, then the group* $U_s(A)$ *is free abelian. In any case,* $U_s(A)$ *is torsion free, and any inclusion* $A \subset A'$ *gives rise to an embedding of* $U_s(A)$ *into* $U_s(A')$.

If $s \geqslant 2$, it is interesting to note that $U_s(\mathbf{Q}/\mathbf{Z})$ is actually a vector space over the rational numbers. For this lemma asserts that it is torsion free, and the relations $(*_s)$ clearly imply that it is divisible.

The proof of Theorem 2 will be based on the following. Let s be any complex number and let $\chi : \mathrm{Hom}(A, A)^{\bullet} \to \mathbf{C}^{\bullet}$ be a continuous character.

LEMMA 12. *There is one and, up to a constant multiple, only one function*

$$f = f_\chi : A \to \mathbf{C}$$

satisfying $(*_s')$ *and satisfying* $f(ua) = \chi(u)f(a)$ *for every* u *in* $\mathrm{Hom}(A, A)^{\bullet}$ *and every* a *in* A.

Proof. To fix our ideas, let us consider only the case $A = \mathbf{Q}/\mathbf{Z}$, so that $\mathrm{Hom}(A, A) = \varprojlim \mathbf{Z}/m\mathbf{Z}$ is the profinite completion $\hat{\mathbf{Z}}$ of the integers. The general case is completely analogous.

Since χ is continuous, there exists an integer $m \neq 0$ so that χ is identically equal to 1 on the congruence class $1 + m\hat{\mathbf{Z}}$ intersected with $\hat{\mathbf{Z}}^{\bullet}$. The collection of all m with this property forms an ideal $\mathscr{F}$ called the *conductor* of χ. Evidently χ is equal to the composition

$$\hat{\mathbf{Z}}^{\cdot} \to (\mathbf{Z}/\mathscr{F})^{\cdot} \to \mathbf{C}^{\cdot}$$

for some Dirichlet character modulo $\mathscr{F}$, and $\mathscr{F}$ is the unique largest ideal with this property. We will use the same symbol χ for this character on $(\mathbf{Z}/\mathscr{F})^{\cdot}$. *If k is any integer relatively prime to $\mathscr{F}$, it follows that $\chi(k)$ is a well defined root of unity.*

Any fraction in $\mathbf{Q}/\mathbf{Z}$ with denominator n can be written as u/n for some unit u in $\hat{\mathbf{Z}}^{\cdot}$. In view of the identity

$$f(u/n) = \chi(u) f(1/n),$$

we need only compute the values $f(1/n)$ in order to determine f completely.

Note that the unit u in this equation is well defined modulo $n\hat{\mathbf{Z}}$. If n belongs to the ideal $\mathscr{F}$, then it follows that the root of unity $\chi(u)$ is uniquely determined. However, if $n \notin \mathscr{F}$, then we can choose $u \equiv 1 \bmod n$ with $\chi(u) \neq 1$. *This proves that $f(1/n) = 0$ whenever n is not in the ideal $\mathscr{F}$.*

The proof will show that f is some constant multiple of the expression

$$f(1/n) = n^{-s} \prod_{p|n} (p - p^s \bar{\chi}(p))/(p-1) \qquad \text{for} \qquad n > 0, n \in \mathscr{F}.$$

Here $\bar{\chi}(p)$ is a well defined root of unity if the prime p is a unit modulo $\mathscr{F}$, and is to be set equal to zero otherwise.

First consider the Kubert identity

$$(\bigstar) \qquad p^{1-s} f\left(\frac{1}{n}\right) = \sum_{0}^{p-1} f\left(\frac{1+kn}{pn}\right)$$

for $n \in \mathscr{F}$.

Case 1. If $p \mid n$, then each $1 + kn$ is a unit modulo pn, with $\chi(1+kn) = 1$. Hence this equation reduces simply to

$$p^{-s} f\left(\frac{1}{n}\right) = f\left(\frac{1}{pn}\right).$$

Case 2. If n is not a multiple of p, then there is exactly one k_0 between 1 and $p - 1$ so that $1 + k_0 n$ is some multiple, say lp, of p. Then

$$f\left(\frac{1+k_0 n}{np}\right) = f\left(\frac{l}{n}\right) = \chi(l) f\left(\frac{1}{n}\right),$$

where $\chi(l) = \bar{\chi}(p)$ since $lp \equiv 1 \bmod \mathscr{F}$. Thus the Kubert identity takes the form

$$(p^{1-s} - \bar{\chi}(p)) f\left(\frac{1}{n}\right) = (p-1) f\left(\frac{1}{pn}\right).$$

Evidently this completes the proof that f is uniquely defined up to multiplication by a constant.

To prove that the function f defined in this way satisfies all of the Kubert identities, we must also consider the case where n does *not* belong to the ideal $\mathscr{F}$, so that $f(1/n) = 0$. If pn does belong to $\mathscr{F}$, then the units $1 + kn$ modulo pn, in the argument above, range precisely over the kernel of the homomorphism

$$(\mathbf{Z}/pn\mathbf{Z})^{\bullet} \to (\mathbf{Z}/n\mathbf{Z})^{\bullet} .$$

Since χ is non-trivial on this kernel, by the definition of $\mathscr{F}$, it follows that

$$\sum \chi(1+kn) = 0 ,$$

taking the sum over all k between 0 and $p - 1$ with $1 + kn$ prime to p. Thus both sides of the required equation ($\bigstar$) are zero. Since every other Kubert identity follows from one of these by applying an automorphism to $\mathbf{Q}/\mathbf{Z}$, this completes the proof. □

Proof of Theorem 2. If $A = A_m$ is a finite group of order m, then $U_s(A) \otimes \mathbf{C}$ is finite dimensional, so it certainly splits under the action of the commutative group $\text{Hom}(A, A)^{\bullet}$ into a direct sum of 1-dimensional spaces. According to Lemma 12, there is exactly one of these spaces for each character χ mod m, so the conclusion follows.

The general case now follows by passing to a direct limit over finite subgroups of A. (For any integer n, note that there are only finitely many characters χ whose conductor contains n, hence only finitely many χ with $f_{\chi}(1/n) \neq 0$.) This completes the proof. □

Proof of Lemma 9. It will be convenient to consider the various vector spaces $U_s(A_m) \otimes \mathbf{Q}$ as subspaces of $U_s(\mathbf{Q}/\mathbf{Z}) \otimes \mathbf{Q}$. This is permissible by the Corollary above (or by Lemma 11)).

Let W_m be the rational vector space spanned by all elements

$$u(a) \in U_s(\mathbf{Q}/\mathbf{Z}) \otimes \mathbf{Q}$$

such that a has denominator precisely m, and hence generates the cyclic group A_m. We will show that $W_m \subset W_{pm}$. Assuming this for the moment, it follows inductively that

$$W_m = U_s(A_m) \otimes \mathbf{Q} .$$

Hence the $\varphi(m)$ generators of W_m must be linearly independent, as was to be proved.

Suppose then that a generates A_m. If $p \mid m$, then the Kubert identity

$$u(a) = p^{s-1} \sum_{0}^{p-1} u((a+k)/p) ,$$

where each $(a+k)/p$ has denominator precisely pm, proves that $u(a) \equiv 0 \bmod W_{pm}$. On the other hand, if p is prime to m, then the relation

$$u(pa) - p^{s-1}u(a) = p^{s-1}\sum_{1}^{p-1} u(a+k/p)$$

proves that

$$u(pa) \equiv p^{s-1}u(a) \bmod W_{pm}.$$

Choosing $r \geqslant 1$ so that $p^r \equiv 1 \bmod m$, it follows that

$$u(a) = u(p^r a) \equiv p^{r(s-1)}u(a) \bmod W_{pm}.$$

Since $s \neq 1$, this proves that $u(a) \equiv 0 \bmod W_{pm}$, as required. □

Proof of Lemma 11. For any $a \in \mathbf{Q}/\mathbf{Z}$ let a_p be the p-primary component of a. Thus $a = \sum a_p$, where the denominator of a_p is a power of p. Represent each a_p as a rational in the interval $0 \leqslant a_p < 1$.

Definition. We will say that a is *reduced* if $0 \leqslant a_p < 1 - p^{-1}$ for every prime p.

Then for $s \leqslant 1$ we will prove explicitly that $U_s(A)$ is a free abelian group, with one free generator $u(a)$ for each reduced element a of A. Evidently it suffices to check that $U_s(A)$ is generated by these elements. For a simple counting argument shows that the number of reduced elements in any finite subgroup $A_m = m^{-1}\mathbf{Z}/\mathbf{Z}$ is equal to the rank

$$\varphi(m) = m\prod_{p|m}(1-p^{-1})$$

of $U_s(A_m)$.

Suppose that a is not reduced, say $1 - p^{-1} \leqslant a_p < 1$ for some prime p. Then the identity

$$p^{1-s}u(pa) = u(a) + u(a-1/p) + \dots + u\big(a - (p-1)/p\big)$$

shows that $u(a)$ is a linear combination of $u(pa)$, where pa has strictly smaller denominator than a, and elements $a - k/p$ which are reduced at the prime p and have q-primary component unchanged for $q \neq p$. A straightforward induction now completes the proof in the case $s \leqslant 1$.

If $s \geqslant 2$, this argument shows only that the reduced generators form a basis for the rational vector space $U_s(A) \otimes \mathbf{Q}$. To prove that $U_s(A_m)$ is free abelian, we will show that the tensor product $U_s(A_m) \otimes \mathbf{Z}_q$ is generated by $\varphi(m)$ elements for any prime q. This will show that there cannot be any torsion.

As free generators, we will choose all elements $u(a)$ where $a = \sum a_p$ is "reduced" at all primes p other than q. *However, we require that the q-primary component a_q should have denominator equal to the highest power of q dividing m.*

The proof that these elements generate over $\mathbf{Z}_q$ proceeds as above for $p \neq q$, and proceeds as in the proof of Lemma 9 when $p = q$. Details are easily supplied. □

§6. On Q-linear relations

S. Chowla and P. Chowla have suggested the following conjecture in a private communication to the author. Let $a_1, a_2, \ldots$ be a sequence of integers which is periodic, $a_n = a_{n+p}$, for some prime p. Then

$$\sum_1^\infty a_n/n^2 \neq 0 \tag{11}$$

except in the special case

$$a_1 = \ldots = a_{p-1} = a_p/(1-p^2).$$

If we use the Hurwitz function

$$\zeta_2(k/p) = p^2(k^{-2} + (k+p)^{-2} + \ldots),$$

then the inequality (11) can be written as

$$\sum_1^p a_k \, \zeta_2(k/p) \neq 0;$$

and the exceptional case corresponds to the Kubert relation

$$\zeta_2(1) = p^{-2} \sum_1^p \zeta_2(k/p).$$

Thus the Chowlas' conjecture is true if and only if the real numbers

$$\zeta_2(1/p), \ldots, \zeta_2((p-1)/p)$$

are linearly independent over the rational numbers. More generally, for any $m \geqslant 2$ one might conjecture that the $\varphi(m)$ real numbers $\zeta_2(k/m)$, where k varies over all relatively prime integers between 1 and $m - 1$, are $\mathbf{Q}$-linearly independent. Using Lemma 9, a completely equivalent statement would be the following.

Conjecture: Every $\mathbf{Q}$-linear relation between the real numbers $\zeta_2(x)$, where x is rational with $0 < x \leqslant 1$ is a consequence of the Kubert relations $(*_{-1})$.

In fact, since $\zeta_2(x+1) \equiv \zeta_2(x) \bmod \mathbf{Q}$ for positive rational x, it might be more natural to sharpen this conjecture by taking the values of ζ_2 modulo $\mathbf{Q}$. *In other words, it is conjectured that the mapping*

$$\mathbf{Q}/\mathbf{Z} \to \mathbf{R}/\mathbf{Q}$$

induced by ζ_2 *is a "universal" function satisfying* $(*_{-1})$. It follows easily from Theorem 3 below that the corresponding conjecture for the even part,

$$\zeta_2(x) + \zeta_2(1-x) = \pi^2/\sin^2 \pi x,$$

of ζ_2 is indeed true; but the odd part of ζ_2 seems difficult to work with.