2. Augmented groups and torsion numbers

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **48 (2002)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **10.08.2024**

2. AUGMENTED GROUPS AND TORSION NUMBERS

Torsion numbers for knots and links arise as a special case of a general group-theoretical quantity described below. We see that many knot-theoretic results remain valid in the broader context.

Let G be a finitely generated group and $\chi\colon G \to \mathbf{Z}$ any epimorphism. The pair (G, χ) is called an *augmented group*. Two augmented groups, (G_1, χ_1) and (G_2, χ_2), are *equivalent* if there exists an isomorphism $\phi\colon G_1 \to G_2$ such that $\chi_2 \circ \phi = \chi_1$.

For any augmented group (G, χ), the abelianization of ker χ is a module $\mathcal{M}$ over the ring $\mathcal{R}_1 = \mathbf{Z}[t, t^{-1}]$ of Laurent polynomials. Since $\mathcal{R}_1$ is Noetherian, $\mathcal{M}$ is finitely generated, expressible as

$$\mathcal{M} \cong \mathcal{R}_1^N / \mathcal{A}\mathcal{R}_1^M, \tag{2.1}$$

where $\mathcal{A}$ is an $N \times M$-matrix over $\mathcal{R}_1$, for some positive integers M, N. By adjoining zero columns if needed, we can assume that $M \geq N$.

For any natural number r, we define $\mathcal{M}_r$ to be the quotient module

$$\mathcal{M}_r = \mathcal{M}/(t^r - 1)\mathcal{M}.$$

It is clear that $\mathcal{M}_r$ is finitely generated as an abelian group. Hence it decomposes as

$$\mathcal{M}_r \cong \mathbf{Z}^{\beta_r} \oplus T\mathcal{M}_r,$$

where $T\mathcal{M}_r$ denotes the torsion subgroup of $\mathcal{M}_r$. We define the r^{th} *torsion number* of (G, χ) to be the order b_r of $T\mathcal{M}_r$. We say that b_r is *pure* if the Betti number β_r vanishes.

Clearly b_r and β_r depend only on the module $\mathcal{M}$, which in turn depends only on the equivalence class of (G, χ). Although our motivation is group-theoretic, we note that torsion and Betti numbers can be associated as above to any finitely generated $\mathcal{R}_1$-module $\mathcal{M}$. The difference is a matter only of perspective, for it can be easily seen that any such $\mathcal{M}$ arises from an augmented group (G, χ).

The elementary ideals E_i of $\mathcal{M}$ form a sequence of invariants of (G, χ). The ideal E_i is generated by the $(N-i) \times (N-i)$ minors of the matrix $\mathcal{A}$ of (2.1). Since $\mathcal{R}_1$ is a unique factorization domain, each E_i is contained in a unique minimal principal ideal; a generator is the i^{th} *characteristic polynomial* $\Delta_i(t)$ of (G, χ), well defined up to multiplication by units in $\mathcal{R}_1$. We are primarily interested in $\Delta_0(t)$, which we abbreviate by Δ.

An important class of augmented groups arises in knot theory. For any knot k in the 3-sphere S^3 the fundamental group $G = \pi_1(S^3 - k)$ is finitely presented and has infinite cyclic abelianization. Abelianization provides a surjection $\chi\colon G \to \mathbf{Z}$. (More precisely, there are two choices. The ambiguity, which is harmless, can be eliminated by orienting the knot.) The module $\mathcal{M}$ is isomorphic to the first homology group of the infinite cyclic cover of $S^3 - k$, and it has a presentation marix $\mathcal{A}$ that is square (that is, $M = N$). The quotient module $\mathcal{M}_r$ is isomorphic to the homology group $H_1(M_r, \mathbf{Z})$ of the r-fold cyclic cover M_r of S^3 branched over k. The 0th characteristic polynomial Δ is commonly called the Alexander polynomial of k. (See [Li97] or [Ro76].)

DEFINITION 2.1. The *cyclotomic order* $\gamma = \gamma(\Delta)$ is the least common multiple of those positive integers d such that the dth cyclotomic polynomial Φ_d divides Δ. If no cyclotomic polynomial divides Δ then $\gamma = 1$.

PROPOSITION 2.2 (cf. Theorem 4.2 of [Go72]). *For any augmented group (G, χ) the sequence $\{\beta_r\}$ of Betti numbers satisfies $\beta_{r+\gamma} = \beta_r$, where γ is the cyclotomic order of Δ.*

Proof. We adapt an argument of D. W. Sumners that appears in [Go72]. Since $\Pi = \mathbf{C}[t, t^{-1}]$ is a principal ideal domain, the tensor product $\mathcal{M} \otimes_{\mathbf{Z}} \mathbf{C}$ decomposes as a direct sum $\oplus_{i=1}^{n} \Pi/(\pi_i)$, for some elements $\pi_i \in \Pi$ such that $\pi_i \mid \pi_{i+1}$, $1 \le i < n$. (For $0 \le i < n$, the product $\pi_1 \cdots \pi_{n-i}$ is the same as Δ_i up to multiplication by units in Π.) Likewise,

$$\mathcal{M}_r \otimes_{\mathbf{Z}} \mathbf{C} \cong \oplus_{i=1}^{n} \Pi/(\pi_i, t^r - 1)\,.$$

Each factor $\Pi/(\pi_i)$ can be expressed as $\oplus_j \Pi/((t - \alpha_j)^{e(\alpha_j)})$, where $e(\alpha_j)$ are positive integers, α_j ranging over the distinct roots of π_i. Since

$$((t-\alpha)^{e(\alpha)}, t^r - 1) = \begin{cases} (t-\alpha) & \text{if } \alpha^r = 1\,, \\ \Pi & \text{otherwise}, \end{cases} \cdot$$

we see that

$$\beta_r = \dim_{\mathbf{C}} \mathcal{M}_r \otimes_{\mathbf{Z}} \mathbf{C} = \sum_{i=1}^{n} l_i\,,$$

where l_i is the number of distinct roots of π_i that are also rth roots of unity. Hence $\beta_r = \beta_{(\gamma, r)}$, and so $\beta_{r+\gamma} = \beta_{(\gamma, r+\gamma)} = \beta_{(\gamma, r)} = \beta_r$. □

In view of Proposition 2.2 it is natural to consider a subsequence of torsion numbers b_{r_k} such that β_{r_k} is constant. We prove that $\{b_{r_k}\}$ is a *division sequence* in the sense that b_{r_k} divides b_{r_l} whenever r_k divides r_l.

LEMMA 2.3. *Assume that $\phi\colon \mathcal{N} \to \mathcal{N}'$ is an epimorphism of finitely generated modules over a PID. If $\mathcal{N}$ and $\mathcal{N}'$ have the same rank, then ϕ restricts to an epimorphism $\phi\colon T\mathcal{N} \to T\mathcal{N}'$ of torsion submodules.*

Proof. It is clear that ϕ induces an epimorphism $\overline{\phi}\colon \mathcal{N}/T\mathcal{N} \to \mathcal{N}'/T\mathcal{N}'$. Since $\mathcal{N}$ and $\mathcal{N}'$ have the same rank, $\overline{\phi}$ is an isomorphism. If $y \in T\mathcal{N}'$, then there exists an element $x \in \mathcal{N}$ such that $\phi(x) = y$. If $x \notin T\mathcal{N}$, then x represents a nontrivial element of the kernel of $\overline{\phi}$, a contradiction. Thus ϕ restricts to an epimorphism of torsion submodules. □

PROPOSITION 2.4. *Let (G, χ) be an augmented group. If b_{r_k} is a subsequence of torsion numbers for which the corresponding Betti numbers β_{r_k} are constant, then $\{b_{r_k}\}$ is a division sequence.*

Proof. If r divides s, then clearly there exists a surjection $\phi\colon \mathcal{M}_s \to \mathcal{M}_r$. Since $\beta_r = \beta_s$, Lemma 2.3 implies that ϕ induces a surjection of torsion submodules, and consequently b_r divides b_s. □

Given an augmented group (G, χ) such that $\mathcal{M}$ has a square matrix presentation (2.1), the pure torsion numbers b_r can be computed by the following formula familiar to knot theorists.

PROPOSITION 2.5. *Assume that (G, χ) is an augmented group such that $\mathcal{M}$ has a square matrix presentation. If b_r is a pure torsion number, then it is equal to the absolute value of*

$$\prod_{\zeta^r=1} \Delta(\zeta)\,. \tag{2.2}$$

The quantity (2.2) is equal to the resultant $\mathrm{Res}(\Delta, t^r - 1)$. In general, if $f(t) = a_0t^n + \cdots + a_{n-1}t + a_n$ and $g(t) = b_0t^m + \cdots + b_{m-1}t + b_m$ are polynomials with integer coefficients and zeros $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$, respectively, then the *resultant* of f and g is

$$\mathrm{Res}(f, g) = (a_0^m b_0^n) \prod_{i,j} (\alpha_i - \beta_j) = a_0^m \prod_i g(\alpha_i) = (-1)^{mn} b_0^n \prod_j f(\beta_j)\,.$$

Clearly, $\mathrm{Res}(f_1 f_2, g) = \mathrm{Res}(f_1, g)\,\mathrm{Res}(f_2, g)$ and $\mathrm{Res}(f, g) = (-1)^{mn}\,\mathrm{Res}(g, f)$. The resultant has an alternative definition as the determinant of a certain matrix formed from the coefficients of f and g (cf. [La65]). In particular, the resultant of integer polynomials is always an integer.

In the case that G is a knot group, formula (2.2) was given by R. Fox [Fo56]. A complete proof is contained in [We80]. The proof of Proposition 2.5 can be fashioned along similar lines. We will prove a more general result in Section 3.

In [Le33] D. H. Lehmer investigated resultants $\mathrm{Res}(f, t^r - 1)$, where $f(t) \in \mathbf{Z}[t]$. As he observed, it follows from a theorem of Lagrange that the sequence $\{\mathrm{Res}(f, t^r - 1)\}$ satisfies a linear homogeneous recurrence relation in r with constant coefficients.

The general linear recurrence relation is easy to find. Assume that $f(t) = c_0 t^d + \cdots + c_{d-1}t + c_d$ has roots $\alpha_1, \ldots, \alpha_d$. Form the polynomials

$$\begin{aligned} f_0(t) &= t - 1\,, \\ f_1(t) &= \frac{1}{c_0} f(t) = \prod_{i=1}^{d} (t - \alpha_i)\,, \\ f_2(t) &= \prod_{i>j=1}^{d-1} (t - \alpha_i\alpha_j)\,, \\ &\vdots \\ f_d(t) &= t - \alpha_1\alpha_2 \cdots \alpha_d = t - (-1)^d \frac{c_d}{c_0}\,. \end{aligned}$$

It is not necessary to find the roots of f in order to determine $f_0, \ldots, f_d$. The coefficients of these polynomials are integers obtained rationally in terms of the coefficients of f. Lehmer gives explicit formulas for $d < 6$ ([Le33], p. 472–3). If $t^m + A_1 t^{m-1} + \cdots + A_m$ is the least common multiple of $f_0, \ldots, f_d$, then $\mathrm{Res}(f, t^r - 1)$, which we abbreviate by $R(f, r)$, satisfies the homogeneous linear recurrence with characteristic polynomial $p(t) = c_0^m t^m + c_0^{m-1} A_1 t^{m-1} + \cdots + A_m$; that is,

$$c_0^m R(f, r+m) + c_0^{m-1} A_1 R(f, r+m-1) + \cdots + A_m R(f, r) = 0\,. \tag{2.3}$$

It is easy to see that the degree m of the characteristic equation (2.3) is not greater than 2^d. These facts were rediscovered by W. Stevens [St00]. Stevens proved that when f is a reciprocal polynomial (that is, $c_i = c_{d-i}$ for $i = 0, 1, \ldots, d$) this degree m can be bounded from above by $3^{d/2}$.

We remark that the sign of $\mathrm{Res}(f, t^r - 1)$ is either constant or alternating. For in the product

$$\mathrm{Res}(f, t^r - 1) = c_0^m \prod_i (\alpha_i^r - 1)\,,$$

a pair of conjugate complex roots contributes a factor $(\alpha_i^r - 1)(\overline{\alpha}_i^r - 1) = |\alpha_i^r - 1|^2$, while the real factors have constant or alternating sign. It follows that $|\mathrm{Res}(f, t^t - 1)|$ satisfies a linear recurrence of the same order as $\mathrm{Res}(f, t^r - 1)$; in the alternating sign case, simply modify the characteristic polynomial by changing the sign of alternate terms.

EXAMPLE 2.6. The Alexander polynomial of the figure-eight knot (the knot 4_1 in tables) is $\Delta(t) = t^2 - 3t + 1$. Since neither root has modulus one, all of the torsion numbers of k are pure. The polynomials f_i are $f_0(t) = f_2(t) = t - 1$ and $f_1(t) = \Delta(t)$. The least common multiple is $t^3 - 4t^2 + 4t - 1$, and hence b_r satisfies: $b_{r+3} - 4b_{r+2} + 4b_{r+1} - b_r = 0$. Using the initial conditions $b_0 = 0, b_1 = 1, b_2 = 5$, other values can now be quickly computed.

The torsion numbers for the figure-eight knot produce some surprisingly large prime factors. According to calculations done with Maple, b_{1361} is the square of a prime with 285 digits.

Lehmer, who considered this example in [Le33], albeit for much smaller values of r, was interested in producing new prime numbers. He observed that the factors of $R(f, r)$ satisfy a severe arithmetical constraint, and he proposed that if $R(f, r)$ grows with a relatively small exponential growth rate, then these numbers will likely display large prime factors. Lehmer did not give any proof of the assertion about prime factors, but rather used it heuristically. A survey of Lehmer's efforts together with new results in these directions can be found in [EEW00].

DEFINITION 2.7. Assume that

$$f(t) = c_0 t^d + \cdots + c_{d-1} t + c_d = c_0 \prod_{i=1}^{d} (t - \alpha_i)$$

is a polynomial with complex coefficients, $c_0 \neq 0$. The *Mahler measure* of f is

$$M(f) = |c_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

The empty product is assumed to be 1, so that the Mahler measure of a nonzero constant polynomial $f(t) = c_0$ is $|c_0|$. By convention, the Mahler measure of the zero polynomial is zero.

Clearly, Mahler measure is multiplicative; that is, $M(fg) = M(f)M(g)$, for $f, g \in \mathbf{C}[t]$. The following is proved in [GS91] and [Ri90]. We sketch the argument.

PROPOSITION 2.8. *Let f be a polynomial with integer coefficients. The subsequence $R(f, r_k)$ of nonvanishing resultants has exponential growth rate $M(f)$; that is,*

$$\lim_{r_k \to \infty} |\mathrm{Res}(f, t^{r_k} - 1)|^{1/r_k} = M(f).$$

Sketch of proof. Let $f(t) = c_0 t^d + \cdots + c_{d-1}t + c_d$. Assume that $c_0 \neq 0$ and that $\alpha_1, \ldots, \alpha_d$ (not necessarily distinct) are the roots of f. Then

$$|\mathrm{Res}(f, t^r - 1)|^{1/r} = |c_0| \prod_{i=1}^{d} |\alpha_i^r - 1|^{1/r}.$$

The condition that the resultant does not vanish is equivalent to the statement that no root α_i is an r^{th} root of unity. Consider the subsequence of natural integers r for which this is the case. Note that if $|\alpha_i| < 1$, then the factor $|\alpha_i^r - 1|^{1/r}$ converges to 1 as r goes to infinity. On the other hand, if $|\alpha_i| > 1$, then for sufficiently large r we have

$$\frac{1}{2}|\alpha_i|^r \leq |\alpha_i|^r - 1 \leq |\alpha_i^r - 1| \leq |\alpha_i|^r + 1 \leq 2|\alpha_i|^r.$$

Taking r^{th} roots we see that $|\alpha_i^r - 1|^{1/r}$ converges to $|\alpha_i|$.

When some root α_i lies on the unit circle the nonzero values of $|\alpha_i^r - 1|$ can fluctuate wildly. In this case the analysis is more subtle. González-Acuña and Short use results of A. Baker [Ba77] and A.O. Gelfond [Ge35] to obtain estimates. In [GS91] it is shown that if $|\alpha_i^r| \neq 1$, then

$$C\exp\{-(\log r)^6\} < |\alpha_i^r - 1| \leq 2,$$

where C is a positive constant that depends only on f. As in the case that $|\alpha_i| < 1$ we have that $|\alpha_i^r - 1|^{1/r}$ converges to 1.

The conclusion of Proposition 2.8 follows. □

The following is immediate from Propositions 2.8 and 2.5.

COROLLARY 2.9. *Assume that the finitely generated $\mathcal{R}_1$-module $\mathcal{M}$ has a square matrix presentation. Then the subsequence of $\{b_r\}$ consisting of pure torsion numbers has exponential growth rate equal to $M(\Delta)$.*

We can extend the conclusion of Proposition 2.8 to the entire sequence of resultants by using results from the theory of algebraic dynamical systems. Only the essential elements of the theory are sketched below. Readers unfamiliar with dynamical systems might refer to [EW99].

In brief, to a finitely generated $\mathcal{R}_1$-module we associate a compact space and a homeomorphism σ from the space to itself. The fixed points of σ^r form a closed subspace consisting of exactly b_r connected components. Topological techniques are available to compute the exponential growth rate of b_r, and it coincides with $M(\Delta)$.

THEOREM 2.10. *Assume that the finitely generated $\mathcal{R}_1$-module $\mathcal{M}$ either (i) has a square presentation matrix; or (ii) is torsion-free as an abelian group. Then the sequence $\{b_r\}$ of torsion numbers has exponential growth rate equal to $M(\Delta)$.*

Proof. Let $\mathcal{M}^\wedge$ denote the Pontryagin dual $\mathrm{Hom}(\mathcal{M}, \mathbf{T})$; that is, the topological group of homomorphisms ρ from $\mathcal{M}$ to the additive circle group $\mathbf{T} = \mathbf{R}/\mathbf{Z}$. Here $\mathcal{M}$ has the discrete topology, and $\mathcal{M}^\wedge$ the compact-open topology. Multiplication by t in $\mathcal{M}$ induces a homeomorhism σ of $\mathcal{M}^\wedge$ defined by $\sigma(\rho)(a) = \rho(ta)$, for any $\rho \in \mathcal{M}^\wedge$ and all $a \in \mathcal{M}$. The dual of $\mathcal{M}_r = \mathcal{M}/(t^r - 1)\mathcal{M}$ is the subspace $\mathrm{Fix}(\sigma^r) = \{\rho \in \mathcal{M}^\wedge \mid \sigma^r \rho = \rho\}$, the set of points of $\mathcal{M}^\wedge$ with *period* r.

Since $\mathcal{M}_r = \mathbf{Z}^{\beta_r} \oplus T\mathcal{M}_r$, the dual $\mathcal{M}_r^\wedge$ is homeomorphic to $\mathbf{T}^{\beta_r} \times T\mathcal{M}_r$. This follows from two facts: $\mathbf{Z}^\wedge$ is isomorphic to $\mathbf{T}$; and $A^\wedge$ is isomorphic to A for any finite abelian group. Hence the number of connected components of $\mathcal{M}_r^\wedge$ is equal to the cardinality of $T\mathcal{M}_r$, which by definition is the torsion number b_r. Each component is a torus of dimension β_r, a beautiful fact but one that we will not use here.

The number of connected components of $\mathcal{M}_r^\wedge$ is the same as the number N_r of connected components of $\mathrm{Fix}(\sigma^r)$. Theorem 21.1(3) of [Sc95] states that the exponential growth rate of N_r is equal to the topological entropy of σ. (The proof of this deep result uses a definition of topological entropy in terms of *separating sets*. For an elementary discussion of the theorem see [EW99].)

Further, if $\mathcal{M}$ has a presentation (2.1) with square matrix $\mathcal{A}$, then the topological entropy of σ is equal to $M(\Delta)$. (See Example 18.7(1) of [Sc95].) Thus if the hypothesis (i) is satisfied, then we are done.

If $\mathcal{M}$ is torsion-free as an abelian group, then again the topological entropy of σ is equal to $M(\Delta)$ by Lemma 17.6 of [Sc95]. □

The hypotheses of Theorem 2.10 cannot be dropped, as the following example illustrates.

EXAMPLE 2.11. Consider the augmented group (G, χ) such that

$$G = \langle x, a \mid x^{-2}a^2xa^{-6}xa^2,\ x^{-3}axa^{-4}xa^4xa^{-1}\rangle,$$

and $\chi\colon G \to \mathbf{Z}$ maps $x \mapsto 1$ and $a \mapsto 0$. A straightforward calculation shows that $\mathcal{M} \cong \mathcal{R}_1/(2f, (t-1)f)$, where $f(t) = t^2 - 3t + 1$. The Alexander polynomial Δ is $\gcd(2f, (t-1)f) = f$, and it has Mahler measure greater than 1. However, the topological entropy of the homeomorphism σ is zero by Corollary 18.5 of [Sc95]. As in the proof of the theorem above, it follows that the torsion numbers b_r have trivial exponential growth rate; that is, $\limsup_{r\to\infty} b_r^{1/r} = 1$.

3. EXTENDED FOX FORMULA AND RECURRENCE

Let (G, χ) be an augmented group, and $\mathcal{A}$ the $N \times M$ presentation matrix for the $\mathcal{R}_1$-module $\mathcal{M}$ as in (2.1). For any positive integer r we can obtain a presentation matrix for the finitely generated abelian group $\mathcal{M}_r$ by replacing each entry $q(t)$ of $\mathcal{A}$ by the $r \times r$ block $q(C_r)$, where C_r is the companion matrix of $t^r - 1$,

$$C_r = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

We call the resulting $rN \times rM$ matrix $\mathcal{A}(C_r)$. The proof is not difficult. The torsion number b_r is equal to the absolute value of the product of the nonzero elementary divisors of $\mathcal{A}(C_r)$.

Assume first that $\mathcal{M}$ is a cyclic module. Then $\mathcal{A}$ is the 1×1 matrix $(\Delta(t))$, and the $r \times r$ matrix $(\Delta(C_r))$ presents $\mathcal{M}_r$. The Betti number β_r is the number of zeros of Δ that are r^{th} roots of unity. When it vanishes the matrix $(\Delta(C_r))$ is nonsingular. Then all elementary divisors of the matrix are nonzero, and their product is equal (up to sign) to the product of the eigenvalues, which is the determinant. Fox's formula (Proposition 2.5) follows by choosing a basis for $\mathbf{C}^r$ that diagonalizes the companion matrix C_r; we