CYCLIC RESULTANTS OF RECIPROCAL POLYNOMIALS - FRIED'S THEOREM

STEFAN FRIEDL

ABSTRACT. This note for the most part retells the contents of [Fr88].

1. Introduction

1.1. **Knot theory.** By a knot we will always mean a simple closed curve in S^3, and we are interested in knots up to isotopy. Interest in knots picked up in the late 19th century, when the physicist Tait was trying to find a catalog of all knots with a small number of crossings. Tait produced a correct list of all knots with up to 9 crossings. One can show using simple combinatorics, that his list is complete, but he had no formal proof, that the list did not have any redundancies, i.e. he could not show that any two knots in the list are in fact non-isotopic.

To a knot $K \subset S^3$ we can associate the knot exterior $X_K := S^3 \setminus \nu K$, where νK denotes an open tubular neighborhood around K. The idea now is to apply methods from algebraic topology to the knot exteriors. A straight forward calculation shows that $H_0(X_K; \mathbb{Z}) = \mathbb{Z}$, $H_1(X_K; \mathbb{Z}) = \mathbb{Z}$ and $H_i(X_K; \mathbb{Z}) = 0$ for $i \geq 2$. It thus looks like homology groups are useless for distinguishing knots. Nonetheless, there's a little opening one can exploit. Namely, the fact that for any knot K we have $H_1(X_K; \mathbb{Z}) = \mathbb{Z}$ means that given any knot K and any $n \in \mathbb{N}$ one can talk of *the n-fold cyclic cover* $X_{K,n}$ corresponding to

$$\pi_1(X_K) \to H_1(X_K; \mathbb{Z}) = \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

In particular, given any $n \in \mathbb{N}$ the group $H_1(X_{K,n}; \mathbb{Z})$ is an invariant of the knot K. This simple idea was exploited by Seifert and Alexander in the 1920s and they showed that these invariants are strong enough to distinguish the knots in Tait's list.

In the systematic study of cyclic covers of knot exteriors Alexander was lead to define a symmetric polynomial $\Delta_K(t) \in \mathbb{Z}[t^{\pm 1}]$ with $\Delta_K(1) = 1$, usually referred to as the *Alexander polynomial of K*, which he obtained from the homology of the infinite cyclic cover of X_K. The precise definition of $\Delta_K(t)$ is of no concern to us, but see [Ro76]. What is is important to us is the following theorem of Fox [Fo56, We79].

Theorem 1.1. *For any K and any n we have*

$$H_1(X_{K,n}; \mathbb{Z}) \cong \mathbb{Z} \oplus A_n(K)$$

Date: July 2, 2015.

whereby $A_n(K)$ *is a group with*

$$|A_n(K)| = \prod_{k=1}^{n} \Delta_K(e^{2\pi i k/n}).$$

Hereby given a group A *we denote by* $|A|$ *the number of elements of* A*, where* $|A| = 0$ *means that* A *is infinite.*

In the following, given a knot K and $n \in \mathbb{N}$ we write

$$b_n(K) := |A_n(K)|.$$

The following question arises:

Question 1.2. *Does the Alexander polynomial contain more information, than the homology groups of the cyclic covers? Put differently, if* J *and* K *are two knots with* $b_n(J) = b_n(K)$ *for all* n*, does that imply, that* $\Delta_J(t) = \Delta_K(t)$*?*

This question is related to a more general question, see [BF15]: does the profinite completion of the knot group, which contains the information on all finite quotients of a knot group, determine the knot itself?

1.2. **Dynamics.** Given a square matrix A we denote by $\chi_A(t) = \det(t\,\mathrm{id} - A)$ the characteristic polynomial of A. We start out with the following lemma.

Lemma 1.3. *Let* A *be an integral* $d \times d$*-matrix with* $\det(A) \neq 0$ *and let* $n \in \mathbb{N}$*. We assume that no eigenvalue of* A *is a root of unity. We write*

$$p_n := \textit{number of points of period } n \textit{ of the map } \cdot A\colon \mathbb{R}^d/\mathbb{Z}^d \to \mathbb{R}^d/\mathbb{Z}^d.$$

Then

$$p_n = \left| \prod_{l=1}^{n} \chi_A(e^{2\pi i l/n}) \right|.$$

Proof. We have to determine the number of elements in the kernel of

$$\cdot(\mathrm{id} - A^n)\colon \mathbb{R}^d/\mathbb{Z}^d \to \mathbb{R}^d/\mathbb{Z}^d.$$

We will first show that this number equals $|\det(A^n - \mathrm{id})|$. We write $B = \mathrm{id} - A^n$. We consider the following diagram

$$\begin{array}{ccccccccc} & & & & \mathbb{R}^d/\mathbb{Z}^d & & & & \\ & & & & \cong \downarrow B & & & & \\ 0 & \longrightarrow & \mathbb{Z}^d/B\mathbb{Z}^d & \longrightarrow & \mathbb{R}^d/B\mathbb{Z}^d & \longrightarrow & \mathbb{R}^d/\mathbb{Z}^d & \longrightarrow & 0, \end{array}$$

where the bottom sequence is exact. It follows that the kernel of the map $\cdot B\colon \mathbb{R}^d/\mathbb{Z}^d \to \mathbb{R}^d/\mathbb{Z}^d$ is isomorphic to $\mathbb{Z}^d/B\mathbb{Z}^d$, i.e. it is a group of order $|\det(B)|$.

Now we denote by $\lambda_1, \dots, \lambda_d$ the eigenvalues of A. Then

$$\begin{aligned} \det(\mathrm{id} - A^n) &= \prod_{k=1}^{d} (1 - \lambda_k^n) \\ &= \prod_{k=1}^{d} \prod_{l=1}^{n} (e^{2\pi i l/n} - \lambda_k) \\ &= \prod_{l=1}^{n} \chi_A(e^{2\pi i l/n}). \end{aligned}$$

□

So we arrive at the following question.

Question 1.4. *Let A be an integral $d \times d$-matrix with $\det(A) \neq 0$. To what degree do the number of periodic points determine A?*

2. Fried's theorem

2.1. **The statement of the theorem.** Let $p = p(t) \in \mathbb{R}[t^{\pm 1}]$ be a polynomial. Given $n \in \mathbb{N}$ we define

$$r_n(p(t)) = \prod_{k=1}^{n} p(e^{2\pi i k/n}) = \text{the resultant of } p(t) \text{ and } t^n - 1$$

and

$$b_n(p(t)) = |r_n(p(t))|.$$

The following theorem was proved by Fried [Fr88].

Theorem 2.1. *Let*

$$p(t) = a_d t^d + \cdots + a_1 t + a_0 \in \mathbb{R}[t^{\pm 1}]$$

be a polynomial. If $p(t)$ is reciprocal, i.e. if $a_i = a_{d-i}$, $i = 0, \dots, d$ with $a_0 = a_d > 0$, and if no root of unity is a zero of $p(t)$, then the numbers $b_n(p(t))$ determine $p(t)$.

Remark.

(1) The assumption that all $b_n(p)$'s are non-zero is necessary, see e.g. [Fr88].
(2) Hillar [Hi05] extended the result to non-reciprocal polynomials, in this case the resultants determine $p(t)$ up to a finite ambiguity.
(3) Hillar–Levine [HL07] showed that a finite number of resultants already determines $p(t)$.

The Alexander polynomial of a knot is reciprocal. We thus obtain the following corollary.

Corollary 2.2. *Let K be a knot such that $\Delta_K(t)$ has no zero that is a root of unity, then the homology groups of the finite cyclic covers of X_K determine the Alexander polynomial.*

2.2. **Group rings of abelian groups.** In the proof of Theorem 2.1 we will need one basic fact about group rings, which we state in this section. In the following let G be a multiplicative abelian group, not necessarily finitely generated. We introduce some definitions:

(1) We denote by $p \to \overline{p}$ the involution induced by $g \mapsto g^{-1}$ for $g \in G$.
(2) Given $r, s \in \mathbb{Z}[G]$ we write $r \sim s$ if $r = \pm gs$ for some $g \in G$.

Lemma 2.3. *Let G be a multiplicative abelian group. If $\beta \in \mathbb{Z}[G]$ satisfies*

$$\beta \sim \prod_{i=1}^{d}(g_i - 1)$$

where $g_1, \dots, g_d \in G$ are elements of infinite order with $g_{d+1-i} = g_i^{-1}$, then β determines the factors $g_i - 1$.

The lemma is proved in detail in [Fr88]. We only sketch a proof.

Sketch of proof. The lemma can easily be reduced to the case that G is finitely generated and torsion-free. The lemma follows from the fact that the group ring of a finitely generated torsion-free group is a unique factorization domain, together with the fact that for $h, k \in G$ of infinite order we have $(h-1) \sim (k-1)$ if and only if $h = k^{\pm 1}$. □

In the following we let $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Given $z \in \mathbb{C}^*$ we denote by $[z]$ the corresponding element in $\mathbb{Z}[\mathbb{C}^*]$. Furthermore, given a non-zero rational function $p(t) \in \mathbb{C}(t)$ with $p(0) \neq 0$ we define

$$\text{divisor}(p(t)) := \sum_{z \text{ zero of } p(t)} [z] - \sum_{z \text{ pole of } p(t)} [z] \ \in \mathbb{Z}[\mathbb{C}^*]$$

where we take the zeros and poles with multiplicities.

2.3. **The proof of Fried's theorem.** The proof provided below follows Fried's exposition quite carefully. Let

$$p(t) = a_d t^d + \dots + a_1 t + a_0 \in \mathbb{R}[t^{\pm 1}]$$

be a reciprocal polynomial with $a_0 = a_d > 0$. We denote by $\lambda_1, \dots, \lambda_d$ the zeros of $p(t)$. Given $n \in \mathbb{N}$ we write

$$\begin{aligned} r_n &= r_n(p(t)) &&= \text{resultant of } t^n - 1 \text{ and } p(t) \\ & &&= a_0^n \cdot \prod_{i=1}^{d}(\lambda_i^n - 1), \\ b_n &= b_n(p(t)) &&= |r_n|. \end{aligned}$$

Now we assume that no zero of $p(t)$ is a root of unity. This implies that all the $b_n(p(t))$ are non-zero. We want to show that the b_n's determine $p(t)$. The key idea will be to study the zeta function

$$B(t) = \exp\Big(\sum_{n\geq 0} b_n \frac{t^n}{n}\Big).$$

This choice is inspired by the example in Section 1.2 and the zeta-function defined in [AM65] in the study of periodic points of a self-automorphism.

Before we study $B(t)$ we first need to determine the relationship between r_n and b_n.

Claim. There exist $\epsilon, \delta \in \{-1, 1\}$ such that the sign of r_n equals $\epsilon \cdot \delta^n$.

Since $p(t)$ is a real polynomial we can write

$$\begin{aligned} r_n &= a_0^n \cdot \prod_{i=1}^{d} (\lambda_i^n - 1) \\ &= \underbrace{a_0^n}_{\text{sign } = 1} \cdot \underbrace{\prod_{\lambda \neq \overline{\lambda}} (\lambda_i^n - 1)(\overline{\lambda_i}^n - 1)}_{\text{sign } = 1} \cdot \underbrace{\prod_{\lambda_i > 1} (\lambda_i^n - 1)}_{\text{sign } = 1} \cdot \underbrace{\prod_{\lambda_i \in (-1,1)} (\lambda_i^n - 1)}_{\text{sign } = -1} \cdot \underbrace{\prod_{\lambda_i < -1} (\lambda_i^n - 1)}_{\text{sign } = (-1)^n} \end{aligned}$$

So ϵ is determined by the number of zeros in $(-1, 1)$ and δ is determined by the number of zeros < -1. This concludes the proof of claim.

By the above claim we have

$$b_n = \epsilon \cdot \delta^n \cdot r_n = \epsilon \cdot (\delta a_0)^n \cdot \prod_{i=1}^{d} (\lambda_i^n - 1).$$

We denote by P the power set of $\{1, \ldots, d\}$. Given $\alpha \in P$ denote by $|\alpha|$ the number of elements in α and we define λ^α to be the product of the λ_i's for which the indices appear in α. Multiplying out all products in the above formula of b_n we see that

$$b_n = \sum_{\alpha \in P} \underbrace{\epsilon(-1)^{d-|\alpha|}}_{=:\eta_\alpha} \cdot \Big(\underbrace{\delta a_0 \lambda^\alpha}_{=:\mu_\alpha}\Big)^n = \sum_{\alpha \in P} \eta_\alpha \cdot \mu_\alpha^n.$$

Finally we consider the power series

$$B(t) = \exp\Big(\sum_{n\geq 0} b_n \frac{t^n}{n}\Big).$$

It follows from the above calculations that

$$\begin{aligned} B(t)=\exp\Big(\sum_{n\geq 0} b_n\frac{t^n}{n}\Big) &= \exp\Big(\sum_{n\geq 0}\sum_{\alpha\in P}\eta_\alpha\mu_\alpha^n\frac{t^n}{n}\Big) \\ &= \exp\Big(\sum_{\alpha\in P}\sum_{n\geq 0}\eta_\alpha\mu_\alpha^n\frac{t^n}{n}\Big) \\ &= \prod_{\alpha\in P}\exp\Big(-\eta_\alpha\underbrace{\sum_{n\geq 0}-\mu_\alpha^n\frac{t^n}{n}}_{=\ln(1-\mu_\alpha t)}\Big) \\ &= \prod_{\alpha\in P}\exp\big(-\eta_\alpha\ln(1-\mu_\alpha t)\big) \;=\; \prod_{\alpha\in P}(1-\mu_\alpha t)^{-\eta_\alpha}. \end{aligned}$$

Summarizing we showed that $B(t)$ is a rational function with divisor

$$\operatorname{divisor}(B(t)) \;=\; \sum_{\alpha\in P}(-\eta_\alpha)\cdot[\mu_\alpha^{-1}] \;=\; \overline{-\sum_{\alpha\in P}\eta_\alpha\cdot[\mu_\alpha]} \in \mathbb{Z}[\mathbb{C}^*].$$

On the other hand, multiplying out in the group ring $\mathbb{Z}[\mathbb{C}^*]$ shows that

$$-\epsilon[\delta a_0]\cdot\prod_{i=1}^{d}([\lambda_i]-[1]) \;=\; \sum_{\alpha\in P}\eta_\alpha\cdot[\mu_\alpha] \in \mathbb{Z}[\mathbb{C}^*].$$

As mentioned above, none of the λ_i's is a root of unity. Put differently, each λ_i is an element of infinite order in $\mathbb{C}^*$.

Now we can conclude the proof of the theorem. The b_n's determine the power series $B(t)$. By the above calculations this shows that the b_n's determine

$$\sum_{\alpha\in P}\eta_\alpha\cdot[\mu_\alpha] \;\sim\; \prod_{i=1}^{d}([\lambda_i]-[1]) \in \mathbb{Z}[\mathbb{C}^*].$$

Our assumption that $p(t)$ is reciprocal shows that we can assume that $\lambda_i=\lambda_{d-i}$, $i=0,\dots,d$. Also, by assumption all λ_i's are elements of infinite order in $\mathbb{C}^*$. It follows from Lemma 2.2 that the b_n's determine the λ_i's. Finally we can solve for a_0 using say b_1.

References

[AM65] M. Artin and B. Mazur, *On periodic points*, Ann. Math. (2) 81, 82–99 (1965).

[BF15] M. Boileau and S. Friedl, *The profinite completion of 3-manifolds groups, fiberedness and the Thurston norm*, preprint (2015).

[Fo56] R. H. Fox, *Free differential calculus II. Subgroups*, Ann. of Math. (2) 64 (1956), 407–419.

[Fr88] D. Fried, *Cyclic resultants of reciprocal polynomials*, Holomorphic dynamics, Proc. 2nd Int. Colloq. Dyn. Syst., Mexico City/Mex. 1986, Lect. Notes Math. 1345, 124–128 (1988).

[Hi05] C. Hillar, *Cyclic resultants*, J. Symb. Comput. 39, No. 6, 653–669 (2005); erratum 40, No. 3, 1126–1127 (2005).

[HL07] C. Hillar and L. Levine, *Polynomial recurrences and cyclic resultants*, Proc. Am. Math. Soc. 135, No. 6, 1607–1618 (2007).

[Ro76] D. Rolfsen, *Knots and links*, Mathematical Lecture Series. 7. Berkeley, Ca.: Publish or Perish, Inc. (1976).

[We79] C. Weber, *Sur une formule de R. H. Fox concernant l'homologie des revêtements cycliques*, Enseign. Math. 25 (1979), 261–272.

Fakultät für Mathematik, Universität Regensburg, Germany