

Revêtements, permutations, et quelques problèmes posés par Sacha Zvonkine

Gareth Jones

University of Southampton, UK

January 28, 2016

Polynomials and monodromy groups

One can regard a polynomial $f(z) \in \mathbb{C}[z]$ as a branched covering $\mathbb{C} \rightarrow \mathbb{C}$, or $S^2 \rightarrow S^2$ where we identify the 2-sphere S^2 with the extended complex plane $\mathbb{C} \cup \{\infty\}$ by stereographic projection. .

If $\deg f = n$ then $|f^{-1}(w)| = n$ for all except finitely many w (the **critical values** of f), where $|f^{-1}(w)| < n$ (i.e. $f'(z) = 0$).

Thus f is an n -sheeted covering, branched over these critical values, where two or more sheets come together at a critical point.

Lifting a small loop around a critical value w gives a permutation g_w of the sheets (more precisely, of the fibre $\Phi := f^{-1}(w_0)$ over some non-critical base-point $w_0 \in \mathbb{C}$), called the **monodromy permutation** for f at w . These permutations g_w generate the **monodromy group** G of f , the group of all permutations of Φ induced by lifting closed paths in \mathbb{C} avoiding the critical values.

Example 1

Let

$$w = f(z) = z^n,$$

with $n \geq 2$. There is one critical value in \mathbb{C} , namely $w = 0$. The fibre over a base-point, such as $w_0 = 1$, is

$$\Phi = f^{-1}(1) = \{z \in \mathbb{C} \mid z^n = 1\} = \{\zeta_n^k \mid k = 0, \dots, n-1\},$$

where

$$\zeta_n := e^{2\pi i/n}.$$

If w goes once round the unit circle, starting and finishing at 1, then $z = w^{1/n}$ goes from ζ_n^k to ζ_n^{k+1} ($k \in \mathbb{Z}_n$). Thus the monodromy permutation g_0 is an n -cycle, and the monodromy group G is a cyclic group C_n of order n , permuting Φ regularly.

Example 2

Let

$$w = f(z) = z^4 - 2z^2 + 1.$$

Then $f'(z) = 4z(z^2 - 1)$ so the critical points are at the roots $z = 0, \pm 1$ of $f'(z) = 0$, with critical values $w = 1, 0, 0$. Now $w = (z^2 - 1)^2$, so writing

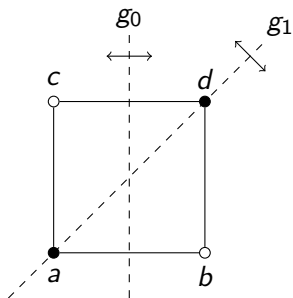
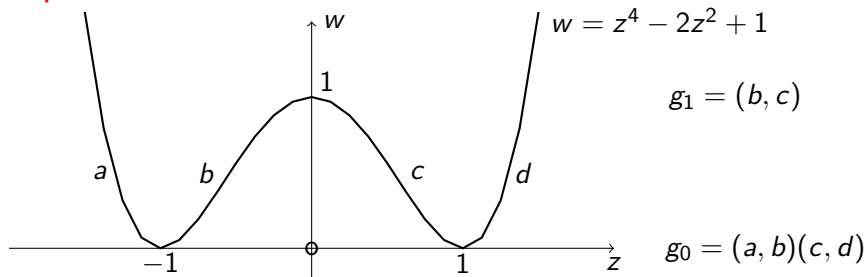
$$z = \sqrt{1 + \sqrt{w}}$$

shows that

- ▶ g_0 is a double transposition (since taking w around 0 multiplies \sqrt{w} by -1), and
- ▶ g_1 is a transposition (since taking w around 1 multiplies z by -1 if $\sqrt{w} \approx -1$, but not if $\sqrt{w} \approx 1$).

In this case $G \cong D_4$, the dihedral group of order 8, acting naturally with degree 4.

Example 2 illustrated



$$G = \langle g_0, g_1 \rangle \cong D_4$$

Monodromy at ∞

For any polynomial f , going once round every critical value $w_1, \dots, w_k \in \mathbb{C}$ in a suitable order is homotopically equivalent to going once round a large circle containing w_1, \dots, w_k , i.e. round a small circle in S^2 enclosing ∞ (with the reverse orientation).

Homotopic paths induce the same monodromy permutations.

If $\deg(f) = n$, then $f(z)$ behaves like z^n near ∞ (see Example 1), so G contains an n -cycle (called a **full cycle**)

$$g_{\infty}^{-1} = g_{w_1} \cdots g_{w_k}.$$

In particular, G is transitive on Φ .

Example 2, revisited Here $g_0 g_1 = (b, c).(a, b)(c, d) = (a, b, d, c)$.

Primitivity

A permutation group is **imprimitive** if it preserves a non-trivial equivalence relation (not the identity or universal relation), permuting the equivalence classes. Otherwise it is **primitive**.

Example 3 If V is a vector space over a field F , then the general linear group $GL(V)$ is transitive on $V \setminus \{0\}$, but imprimitive if $|F| > 2$: define $u \sim v$ if $\langle u \rangle = \langle v \rangle$, or equivalently $v = \lambda u$ for some $\lambda \in F^* = F \setminus \{0\}$.

Every 2-transitive group is primitive, since one can destroy a non-trivial equivalence relation by sending two equivalent points to two inequivalent points. Thus:

Example 4 S_n and A_n are primitive for all n .

Example 5 $GL(V)$ is 2-transitive and hence primitive on the projective geometry $\mathbb{P}(V) = (V \setminus \{0\})/F^*$ formed from the 1-dimensional subspaces of V , inducing the projective general linear group $PGL(V) = GL(V)/\{\lambda I \mid \lambda \in F^*\}$ on $\mathbb{P}(V)$.

Primitivity of monodromy groups

Theorem (Ritt, 1922)

The monodromy group G of a polynomial f is imprimitive if and only if f is a composition of polynomials of lower degrees.

For instance, if $\deg f$ is prime then G is primitive.

In Example 1, with $f(z) = z^n$, $G = C_n$ is primitive if and only if n is prime.

In Example 2, with $f(z) = z^4 - 2z^2 + 1 = (z^2 - 1)^2$, the group $G = D_4$ is imprimitive (2-colour the vertices of a square).

By contrast, a generic (i.e. typical) polynomial of degree n has a primitive monodromy group $G = S_n$.

Ritt's theorem allows us to assume primitivity from now on.

Theorem (Müller, 1995)

Apart from A_n and S_n , the only primitive monodromy groups of polynomials with $k \geq 3$ critical values are the following (with their degrees and the cycle structures of the monodromy generators):

1. $PGL_3(2)$ with $n = 7$, $k = 3$, cycle-structures $2^2 1^3, 2^2 1^3, 2^2 1^3$;
2. $PGL_3(3)$ with $n = 13$, $k = 3$, cycle-structures $2^4 1^5, 2^4 1^5, 2^4 1^5$;
3. $PGL_4(2)$, with $n = 15$, $k = 3$, cycle-structures $2^6 1^3, 2^4 1^7, 2^4 1^7$.

Sacha: "What about the topological conjugacy of the associated polynomials?" He and I worked on this here in Bordeaux, and we published a paper in the Moscow Mathematical Journal, 2002.

(Here, polynomials f_1 and f_2 are **topologically conjugate** if there are orientation-preserving self-homeomorphisms h_1, h_2 of S^2 such that $h_1 \circ f_1 = f_2 \circ h_2$. This is equivalent to f_1 and f_2 having the same monodromy group, with their generating k -tuples equivalent under the action of the k -string braid group B_k on critical values.)

Primitive groups containing a full cycle

Problem Which primitive permutation groups contain a full cycle?

Examples of primitive groups G containing a full cycle:

- (a) Obvious examples: $G = S_n$ for all n , or A_n for all odd n .
- (b) Affine examples: subgroups G of the **affine general linear group**

$$AGL_1(p) := \{t \mapsto at + b \mid a, b \in \mathbb{F}_p, a \neq 0\},$$

containing the translation group $\{t \mapsto t + b\} \cong C_p$, p prime.

- (c) Sporadic examples: $PSL_2(11)$ acting on the $n = 11$ cosets of a subgroup $H \cong A_5$ (known to Galois!), and the Mathieu groups M_{11} for $n = 11$, and M_{23} for $n = 23$, each acting on the n points of the associated Steiner system.

[In fact, any transitive group of prime degree is primitive and contains a full cycle, as in (b) and (c).]

- (d) Projective examples: these are primitive groups $G \leq P\Gamma L_d(q)$ containing Singer cycles.

Identify the d -dimensional vector space $V = (\mathbb{F}_q)^d$ with the additive group of \mathbb{F}_{q^d} ; the multiplicative group $\mathbb{F}_{q^d}^* \cong C_{q^d-1}$ acts linearly on V , and regularly on $V \setminus \{0\}$, inducing a full cycle on the $n = (q^d - 1)/(q - 1)$ points in the projective space

$$\mathbb{P}^{d-1}(\mathbb{F}_q) = \mathbb{P}(V) = (V \setminus \{0\})/\mathbb{F}_q^*.$$

These permutations, and their conjugates in

$$\text{Aut } \mathbb{P}^{d-1}(\mathbb{F}_q) = P\Gamma L_d(q) = PGL_d(q) \rtimes \text{Gal } \mathbb{F}_q,$$

are called **Singer cycles**. Various subgroups $G \leq P\Gamma L_d(q)$ act primitively on $\mathbb{P}^{d-1}(\mathbb{F}_q)$ and contain Singer cycles.

Feit's Theorem

Building on classical results of Galois, Burnside, Schur and Ritt, and using the classification of finite simple groups (asserted around 1979, announced in 1983, finally proved in 2004!) Feit proved:

Theorem (Feit, 1980, CFSG)

The only primitive permutation groups containing a full cycle are the examples given in (a) to (d).

However, his formulation of (d) was rather vague, not specifying which primitive groups $G \leq P\Gamma L_d(q)$ contain Singer cycles.

Theorem (J, 2002)

The groups in (d) are those satisfying $PGL_d(q) \leq G \leq P\Gamma L_d(q)$.

Since $P\Gamma L_2(q)/PGL_d(q) \cong \text{Gal } \mathbb{F}_q \cong C_e$, where $q = p^e$ for some prime p , there is one group G for each divisor of e . This completes the classification of primitive groups containing a full cycle.

Another problem from Sacha

Sacha's work with Fedor Pakovich on polynomials and weighted trees (his talk, later today!) motivated a more general question:

Problem Which primitive groups of degree n contain a cycle of length $m \leq n$ (i.e. with $n - m$ fixed points)?

Theorem (Jordan)

If G is a primitive group of degree n , containing a cycle of prime length $m \leq n - 3$, then $G \geq A_n$ (so $G = A_n$ or S_n).

See Wielandt, *Finite Permutation Groups*, Theorem 13.9.

This theorem is a simple corollary of two theorems in Jordan's papers of 1871 and 1873, though it is not explicitly stated there.

Applying and extending Jordan's Theorem

Jordan's Theorem is often useful in providing particular generating sets for alternating and symmetric groups. For example, Conder (1980) used it to show that if $n \geq 168$ then A_n is a Hurwitz group, that is, it attains Hurwitz's upper bound $84(g - 1)$ for the order of the automorphism group of a Riemann surface of genus $g > 1$.

However, the primality condition on m can be troublesome. After improvements by Rowlinson and Williamson (1974) and Neumann (1975), it was eventually removed. Building on earlier results of Feit (1980) and Müller (1996), and using CFSG, we have:

Theorem (J, 2014)

If G is a primitive permutation group of degree n containing a cycle of length m , then either $G \geq A_n$, or $m \geq n - 2$ and G is known.

Specifically, the 'known' groups $G \neq A_n$ or S_n are as follows:

1. if $m = n$ the cycle is full, so G is as described in cases (b) to (d) of Feit's Theorem;
2. if $m = n - 1$ then (as shown by Müller, 1996)
 - ▶ $AGL_d(q) \leq G \leq A\Gamma L_d(q)$ with $n = q^d$, or
 - ▶ $G = PSL_2(p)$ or $PGL_2(p)$ with $n = p + 1$, or
 - ▶ $G = M_{11}, M_{12}$ or M_{24} with $n = 12, 12$ or 24 ;
3. if $m = n - 2$ then $PGL_2(q) \leq G \leq P\Gamma L_2(q)$ with $n = q + 1$ (J, 2014).

In all cases in (2) and (3) except M_{11} , G is acting naturally, on an affine or projective geometry or a Steiner system, whereas M_{11} is acting on the $n = 12$ cosets of a subgroup $H \cong PSL_2(11)$.

An application

Here is a typical application (with no assumption of primitivity):

Lemma

If G is a transitive permutation group of degree n , containing an m -cycle with m coprime to n and $n/2 < m \leq n - 3$, then $G \geq A_n$.

Proof An easy argument, considering the action of the cycle on equivalence classes, shows that the conditions $m > n/2$ and $\gcd(m, n) = 1$ imply that G is primitive. Since $m \leq n - 3$, the preceding Theorem implies that $G \geq A_n$. \square

This result has recently been applied to algebraic geometry, constructing examples of algebraic varieties called Beauville surfaces from cartesian powers of alternating groups (J, 2015).

Corollary






If $n \geq 9$ there are mutually coprime integers r, s and t such that A_n has generators x and y of orders r and s , with xy of order t .







Proof If n is odd, take a cycle x of length $m = n - 4$, and join the remaining four points to it by a product y of four 2-cycles, so xy is an n -cycle. Then x, y and xy are even permutations of mutually coprime orders $n - 4, 2$ and n . By the Lemma they generate A_n .

If n is even, take a cycle x of length $m = n - 3$, join the remaining three points to it by 2-cycles, and include a fourth 2-cycle in y to transpose two successive elements of the m -cycle. Then xy is an $(n - 1)$ -cycle, with $n - 3, 2$ and $n - 1$ mutually coprime. Being 2-transitive, G is primitive, and since $m < n - 2$, $\langle x, y \rangle = A_n$. \square

Useful fact Up to conjugacy in S_n there are $\Theta(n^3)$ choices for x and y , mutually inequivalent under $\text{Aut } A_n = S_n$. Hence the group $A_n^k = A_n \times \cdots \times A_n$ also has such generators x, y , for $k = \Theta(n^3)$.

Diolch i chi am wrando!

-  M. D. E. Conder, Generators for alternating and symmetric groups, *J. London Math. Soc.* (2) 22 (1980), 75–86.
-  W. Feit, Some consequences of the classification of finite simple groups, in *The Santa Cruz Conference on Finite Groups (Santa Cruz 1979)*, Proc. Sympos. Pure Math. 37, Amer. Math. Soc., Providence RI (1980), pp. 175–181.
-  G. A. Jones, Cyclic regular subgroups of primitive permutation groups, *J. Group Theory* 5 (2002), 403–407.
-  G. A. Jones, Primitive permutation groups containing a cycle, *Bull. Australian Math. Soc.* 89 (2014), 159–165,
-  G. A. Jones and A. Zvonkin, Orbits of braid groups on cacti, *Moscow Math. J.* 2 (2002), 129–162.

-  C. Jordan, Théorèmes sur les groupes primitifs, *J. Math. Pures Appl.* (2) 16 (1871), 383–408.
-  C. Jordan, Sur la limite de transitivité des groupes non alternés, *Bull. Soc. Math. France* 1 (1873), 40–71.
-  P. Müller, Reducibility behavior of polynomials with varying coefficients, *Israel J. Math.* 94 (1996), 59–91.
-  F. Pakovich and A. K. Zvonkin, Minimum degree of the difference of two polynomials over \mathbb{Q} , and weighted plane trees, *Selecta Math. (N.S.)* 20 (2014), 1003–1065.
-  J. F. Ritt, Prime and composite polynomials, *Trans. Amer. Math. Soc.* 23 (1922), 51–66,
-  H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.