Root Loops Supplement: Quick facts and slow questions

Sean Howe (seanpkh@gmail.com)

1. Electronic resources

This document, as well as the Mathematica notebook used in the demonstrations (and a version of it that will run in Wolfram's free CDF player software), are available online at `web.stanford.edu/~seanpkh/rootloops`. This document is a supplement to the lecture and demonstrations, and is not meant to stand alone.

2. The Complex Numbers

The *complex numbers*, $\mathbb{C}$, is the Euclidean plane $\mathbb{R}^2$ equipped with the usual addition of points

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

and multiplication given in polar coordinates by

$$(r_1, \theta_1) \cdot (r_1, \theta_2) = (r_1 r_2, \theta_1 + \theta_2).$$

We write $i = (0,1) \in \mathbb{C}$, $1 = (1,0) \in \mathbb{C}$, so that $(a, b) = a + bi$.

Exercise C1. Explain why $i^2 = -1$.

Multiplication and addition of complex numbers behaves formally like multiplication and addition of real numbers (associativity, distributivity, etc.), thus

Exercise C2. $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

Exercise C3. Every $z \neq 0 \in \mathbb{C}$ has exactly two square roots, i.e. complex numbers ζ such that $\zeta^2 = z$.

Exercise C4. The solutions to $z^2 + ax + b = 0$ in $\mathbb{C}$ are given by the quadratic formula. There are exactly two when $b^2 - 4c \neq 0$, and one when $b^2 - 4c = 0$.

Exercise C5. Let t be a non-zero complex number. Describe the solutions $z \in \mathbb{C}$ to the equation $z^n = t$.

Theorem (The fundamental theorem of algebra)**.**

v1 *Every nonzero complex polynomial* $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0$ *with* $a_i \in \mathbb{C}$ *has a root* $\zeta \in \mathbb{C}$ *(i.e* $f(\zeta) = 0$.*)*

v2 *Every degree* n *monic polynomial* $f(z) = z^n + a_{n-1} z^{n-1} + \ldots + a_0$ *factors into linear terms*

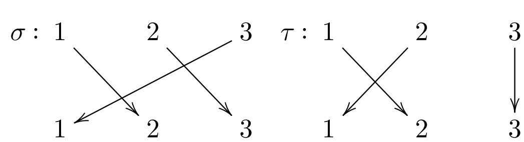
$$f(z) = (z - \zeta_1)^{k_1} \cdot \ldots \cdot (z - \zeta_m)^{k_m}$$

with $\zeta_i \neq \zeta_j$ *for* $i \neq j$ *and* $k_1 + \ldots + k_m = n$.

The ζ_i are the *roots* of $f(z)$, i.e. the solutions to $f(z) = 0$. The number k_i is the *multiplicity* of the root ζ_i. We say $f(z)$ has *repeated roots* if any of the roots have multiplicity larger than 1.

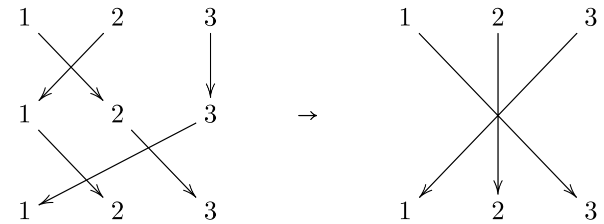
3. Permutations

A *permutation* of a set X is a way to rearrange the elements of X. We can write it using arrows, for example consider the following permutations σ and τ of $\{1, 2, 3\}$:



Exercise P1. How many permutations are there of the set $\{1, 2, \ldots, n\}$?

If we have two permutations σ and τ, we get a new permutation by first rearranging via τ, then rearranging via σ. We write $\sigma\tau$ for this new permutation. In diagrams, $\sigma\tau$ is given by stacking the diagram for σ beneath the diagram for τ, and then following the arrows while forgetting the middle row. For our examples of σ and τ as above, we compute their product $\sigma\tau$:



Exercise P2. Compute the product in the opposite order, $\tau\sigma$ (where τ and σ are the example permutations found above).

The *identity* permutation e is the permutation which leaves all the elements in the same place. Given a permutation σ, we also get an *inverse* permutation σ^{-1} by reversing the arrows.

Exercise P3. For any permutation σ, $\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$.

A *permutation group* is a set G of permutations of a set X such that:

(1) $e \in G$
(2) If $\sigma \in G$, then $\sigma^{-1} \in G$
(3) If $\sigma \in G$ and $\tau \in G$, then $\sigma\tau \in G$.

Exercise P4. What are all the permutation groups of the set $\{1,2\}$? Of the set $\{1,2,3\}$?

It is often convenient to have a more compact notation for writing permutations. We write permutations in *cycle notation*: e.g., the permutation $(13)(254)$ of $\{1,2,3,4,5\}$ sends 1 to 3, 3 to 1, 2 to 5, 5 to 4, and 4 to 2 – each number gets sent to the one to the right of it, and an end parenthesis tells you to loop back around to the corresponding start parenthesis.

Exercise P5. Write the example permutations σ and τ of $\{1,2,3\}$ from above, as well as their product, in cycle notations. Write the remaining permutations of $\{1,2,3\}$ in cycle notation. Compute a few products and inverses in cycle notation without drawing the diagrams.

Exercise P6. Consider all of the permutations of the vertices of a square given by the Euclidean symmetries of the square (i.e. rotations and reflections preserving the square). Is this a permutation group? How many permutations are in it? Write all of these permutations in cycle notation.

4. Root loops

We consider family of polynomials $f_t(z)$ depending on a complex parameter $t \in \mathbb{C}$. For example,

$$f_t(z) = z^3 + tz - 1.$$

If we plug in $t = 0$, we get $z^3 - 1$; if we plug in $t = 1$, we get $z^3 + z - 1$.

The following result should be visualized using the Root Loops mathematica notebook or CDF file:

Theorem (The fundamental theorem of Root Loops)**.** *Let $f_t(z)$ be a family of polynomials depending on a complex parameter t, and let γ be a loop in $\mathbb{C}$ starting at a complex number t_0, and such that $f_t(z)$ has no repeated roots along the loop. Then, following the roots of $f_t(z)$ as t moves along γ induces a permutation of the roots of $f_{t_0}(z)$.*

Exercise RL1. Convince yourself that if we consider all of the permutations of the roots of $f_{t_0}(z)$ given by loops γ, this is a permutation group. **Hint:** What happens when you make a new loop by following one loop, then another? What happens when you follow a loop backwards? What happens if you follow the "trivial loop", where the parameter t doesn't move at all?

The permutation group described in the previous exercise is the *Root Loop Group* of the family of polynomials $f_t(z)$.

The Big Question[1]: Which permutation groups arise as the Root Loop Group of a family of polynomials?

This question can be explored using the Root Loops Mathematica notebook / CDF document. Here are some more specific questions to get you started:

Exploration questions [some of these might be difficult!]:

(1) Describe the Root Loop Group for the family $f_t(z) = z^n - t$. (Take $t_0 = 1$).

(2) If you squish, squeeze, or bend a loop by a small amount, it does not change the induced permutation of the roots. Can you explain why?

(3) Can you find a non-constant family (i.e. depending non-trivially on t, i.e. not something like $f_t(z) = z^2 - 1$) such that the Root Loop Group contains only the identity permutation?

(4) Can you find a simple polynomial for every degree n whose Root Loop Group contains every permutation of the roots?

(5) Can you find a polynomial whose Root Loop Group is the group of permutations of the vertices of a regular n-gon given by symmetries of the plane? [As a first step, you might ask how big is this permutation group, and what permutations are in it!]

(6) The Root Loop Group depends on the choice of t_0 (in a quite literal sense – the elements of the Root Loop Group are permutations of the set of roots of $f_{t_0}(z)$). However, this dependence is fairly benign, which is why we have not emphasized it – can you make this precise?

(7) A permutation group is *transitive* if for any two elements x and y of the set, there is a permutation in the group sending x to y. Can you explain algebraically in terms of the family of polynomials $f_t(z)$ what it means for the Root Loop Group to be transitive?

(8) For any polynomial of the form $f_t(z) = g(z) - t$, e.g. $f_t(z) = z^3 - z - t$, the Root Loop Group is transitive. Can you explain this with a geometric argument? That is, can you give a way to construct for any two roots ζ_1, ζ_2 of $f_{t_0}(z)$, a loop which sends ζ_1 to ζ_2?

(9) What Root Loop Group are you most likely to get for a "random" family of polynomials, whatever that means? For example, if you try many examples in the Root Loops program, what do you seem to find?

(10) Find some polynomials with interesting Root Loop Groups, where you may interpret the word "interesting" however you like!

[1]This is also known as the *inverse Galois problem* for the field $\mathbb{C}(t)$. The answer, it turns out, is always yes, though we won't explain that here!