An Unexpected Group

Carl C. Cowen

IUPUI

(Indiana University Purdue University Indianapolis)

Joint Math Meetings, Baltimore, January 17, 2014

Autobiographical talk dating from time of my beginning research,

Autobiographical talk dating from time of my beginning research,

where many of you will be in 2 or 3 years!

Autobiographical talk dating from time of my beginning research,

where many of you will be in 2 or 3 years!

Resulted in reflections on my situation regarding learning mathematics $\cdots$

Questions like:

"How much math do I want to (work hard enough to) know?"

"What kind of math do I want to (work hard enough to) know?"

"How much math do I need to know?"

"What kind of math do I need to know?"

An Unexpected Group:
Observations on the Nature of Mathematics and Success in Learning Mathematics

Carl C. Cowen

IUPUI

(Indiana University Purdue University Indianapolis)

Joint Math Meetings, Baltimore, January 17, 2014

An Unexpected Group:
Observations on the Nature of Mathematics and Success in Learning Mathematics (and Some Math!)

Carl C. Cowen

IUPUI

(Indiana University Purdue University Indianapolis)

Joint Math Meetings, Baltimore, January 17, 2014

Themes:

- Math is unified – Divisions are artificial!
  - Polynomial: an expression (H.S. algebra)
  - Polynomial: a function of a real variable (calculus)
  - Polynomial: an element in a special ring (algebra)
  - Polynomial: a function of a complex variable (complex analysis)
  - Polynomial: defining object for an algebraic curve (algebraic geometry)
  - $\vdots$

Themes:

- Math is unified – Divisions are artificial!
  - Polynomial: an expression (H.S. algebra)
  - Polynomial: a function of a real variable (calculus)
  - Polynomial: an element in a special ring (algebra)
  - Polynomial: a function of a complex variable (complex analysis)
  - Polynomial: defining object for an algebraic curve (algebraic geometry)
  - $\vdots$
  - ALL OF THESE SIMULTANEOUSLY and ALL RELATED!

Themes:

- Math is unified – Divisions are artificial!

  $\Rightarrow$ Need to know *about* everything!

  – Recognize examples of objects – learn later, ask expert, $\cdots$

- **NOT** Need to *know* everything! (Impossible)

Themes:

- Math is unified – Divisions are artificial!

  $\Rightarrow$ Need to know *about* everything!

- **NOT** Need to *know* everything! (Impossible)

- Develop Intuition! Trust Intuition!

Themes:

- Math is unified – Divisions are artificial!

  $\Rightarrow$ Need to know *about* everything!

- **NOT** Need to *know* everything! (Impossible)

- Develop Intuition! Trust Intuition!

  $\Rightarrow$ Take courses, do other things $TO\ GET$ intuition!

  $\Rightarrow$ Work in area where you $HAVE$ intuition!

Themes:

- Math is unified – Divisions are artificial!

  $\Rightarrow$ Need to know *about* everything!

- **NOT** Need to *know* everything! (Impossible)

- Develop Intuition! Trust Intuition!

- Math is growing, Math is changing – THIS IS THE 21^{st} CENTURY!!

Themes:

- Math is unified – Divisions are artificial!

  $\Rightarrow$ Need to know *about* everything!

- **NOT** Need to *know* everything! (Impossible)

- Develop Intuition! Trust Intuition!

- Math is growing, Math is changing – THIS IS THE 21^{st} CENTURY!!

  $\Rightarrow$ Computers will be in your life; Computers will be in your $MATH$ life!

  – Prepare yourself by learning to use computers to help your math.

  $\Rightarrow$ $STOCHASTICITY$ is everywhere!! including in $MATH$!

  – Prepare yourself by learning (more than basic) probability,

  and maybe statistics, too.

At the time of this work, I was an *ANALYST*:

complex analysis and linear algebra in infinite dimensional Euclidean spaces

Except for required courses and *qualifying exams*,

I was fairly successful in avoiding *ALGEBRA* in graduate school,

But, I *was* required to know what a group is!!

At the time of this work, I was an *ANALYST*:

complex analysis and linear algebra in infinite dimensional Euclidean spaces

Except for required courses and *qualifying exams*,

I was fairly successful in avoiding *ALGEBRA* in graduate school,

But, I *was* required to know what a group is!!

The group in the title was unexpected because,

for me, *EVERY* group is unexpected!!

The topic of my talk arises from a problem in analysis: a question

concerning linear transformations on infinite dimensional Euclidean space.

Problem is about polynomials considered as functions of a complex variable:
Solution uses techniques from theory of surfaces in four-dimensional space,

from complex function theory, and from topology to discover a group

then, the answer to the question is stated in terms of properties of the group.

If I had not been forced to learn about groups,

I would probably not have recognized this one when I saw it!!

Be Inspired by the *interconnectivity* of mathematics to become aware of many widely different subdisciplines that you can see in graduate school!

I discovered this group while working on my thesis – naturally, I was very excited about it!

In my first public talk about the result, Joe Doob (an expert in probability and analysis) suggested it might have been discovered before. He was right:

J. F. Ritt: *Transactions of the American Math. Soc.* **23**(1922) 51–66.
Transactions of the American Math. Soc. **25**(1923) 399–448.

A polynomial in one variable with complex coefficients is a object

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_2 z^2 + a_1 z + a_0$$

where the a_j are complex numbers, i.e. a_j is in $\mathbb{C}$ for $j = 0, 1, 2, \cdots, n$.

The set of such polynomials is called by algebraists

the *ring of polynomials in one variable* and the 'z' is a place-holder.

But, we regard $\mathbb{C}[z]$ as set of functions from the complex plane $\mathbb{C}$ into itself!

If z is any number in $\mathbb{C}$, then $p(z)$ is in $\mathbb{C}$ also.

Fundamental Theorem of Algebra:

If p is not constant, for each w in $\mathbb{C}$, there is z in $\mathbb{C}$ so that $p(z) = w$.

In fact, when p has degree n, there are actually n such z's.

This says, as a function,

A polynomial of degree n is an n-to-1 mapping of $\mathbb{C}$ onto itself.

In addition to adding and multiplying polynomials, we can compose them:

If q is a polynomial, and r is a polynomial, then we define the polynomial $q \circ r$ by

$$q \circ r(z) = q(r(z))$$

For example, if $q(z) = z^2 - 2z + 3$ and $r(z) = z^3 - 1$, then

$$\begin{aligned} q(r(z)) &= (z^3 - 1)^2 - 2(z^3 - 1) + 3 = z^6 - 2z^3 + 1 - 2z^3 + 2 + 3 \\ &= z^6 - 4z^3 + 6 \end{aligned}$$

Clearly, if r is polynomial of degree m and q is polynomial of degree n, then $q \circ r$ is a polynomial of degree mn.

Clearly, if r is polynomial of degree m and q is polynomial of degree n,

then $q \circ r$ is a polynomial of degree mn.

Questions:

Can every polynomial of degree mn be written as

the composition of a polynomial of degree m and a polynomial of degree n?

If not, how can we determine whether a given polynomial

CAN or $CANNOT$ be written as such a composition?

If we know $p = q \circ r$ for some q and r,

how do we decide what q and r actually are?

Questions:

Can every polynomial of degree mn be written as

the composition of a polynomial of degree m and a polynomial of degree n?

If not, how can we determine whether a given polynomial

CAN or $CANNOT$ be written as such a composition?

If we know $p = q \circ r$ for some q and r,

how do we decide what q and r actually are?

It is not hard to see that if $m = 1$ or $n = 1$ then the problem is easily

yes and uninteresting:

it is just a change of variables in the domain plane or the range plane,

and we will call polynomials of degree 1 "trivial polynomials".

An Example:

Let $p(z) = z^4 + 2z^3 - 5z^2 - 6z + 5$

Facts about p:

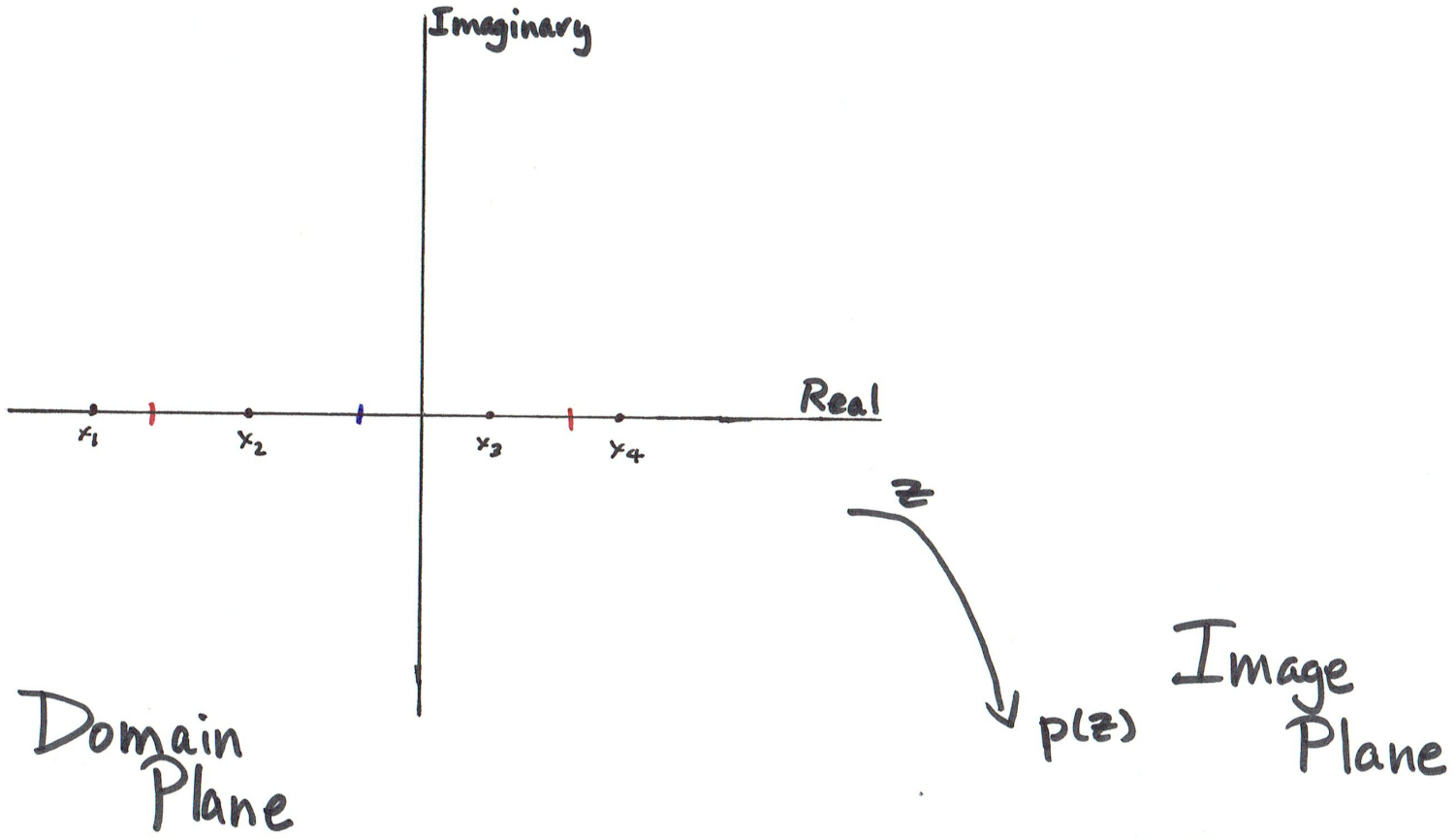
Roots: $x_1 \approx -2.8$, $x_2 \approx -1.6$, $x_3 \approx 0.6$, and $x_4 \approx 1.8$

Derivative:

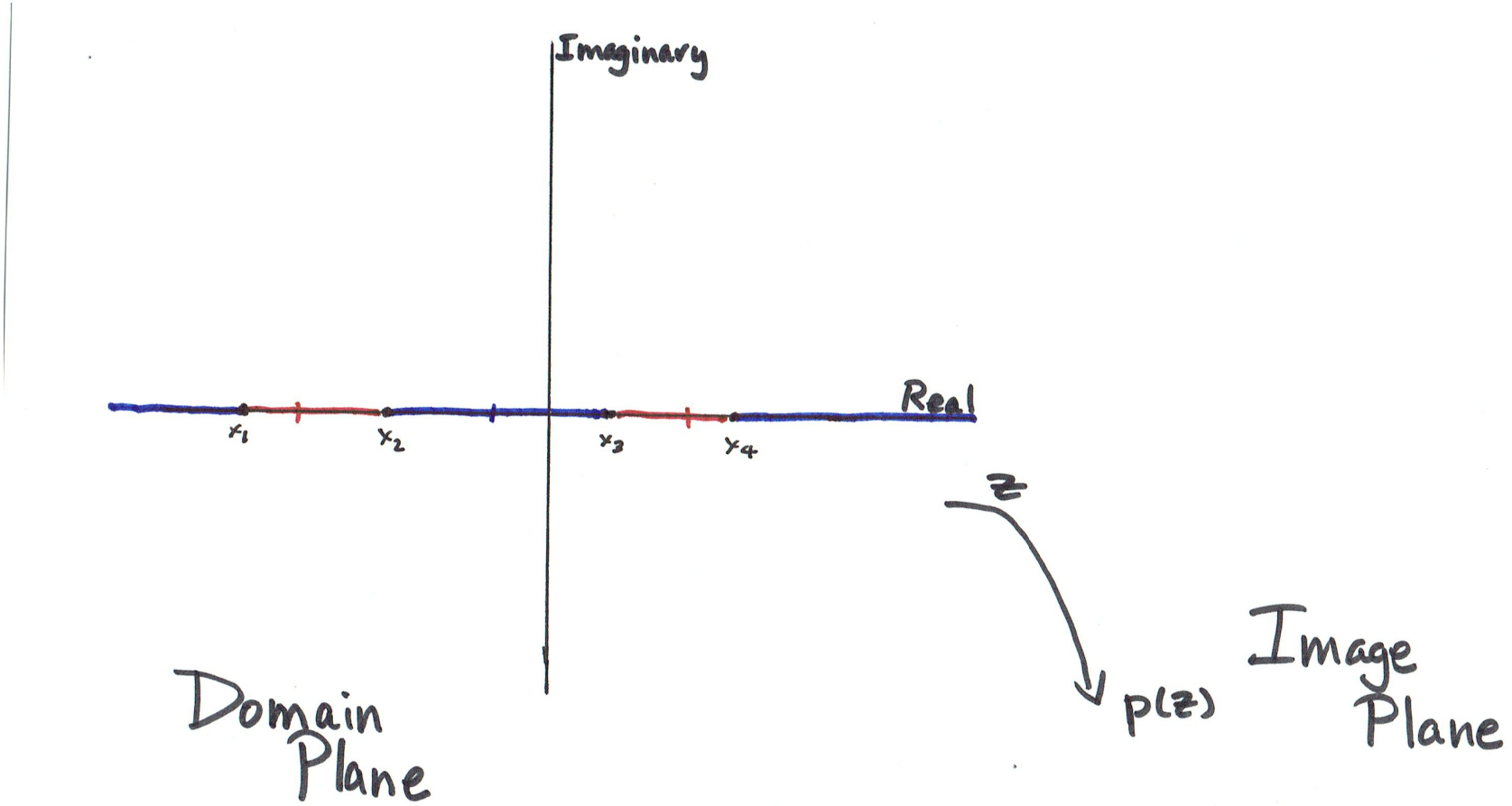
$$p'(z) = 4z^3 + 6z^2 - 10z - 6 = 4(x + \frac{1}{2})(x + \frac{1+\sqrt{13}}{2})(x + \frac{1-\sqrt{13}}{2})$$

Critical points: $-\frac{1}{2}, \qquad -\frac{1+\sqrt{13}}{2} \approx -2.3, \quad \frac{-1+\sqrt{13}}{2} \approx 1.3$

Critical values: $p\left(-\frac{1}{2}\right) = \frac{105}{16}, \quad p\left(-\frac{1+\sqrt{13}}{2}\right) = p\left(\frac{-1+\sqrt{13}}{2}\right) = -4$

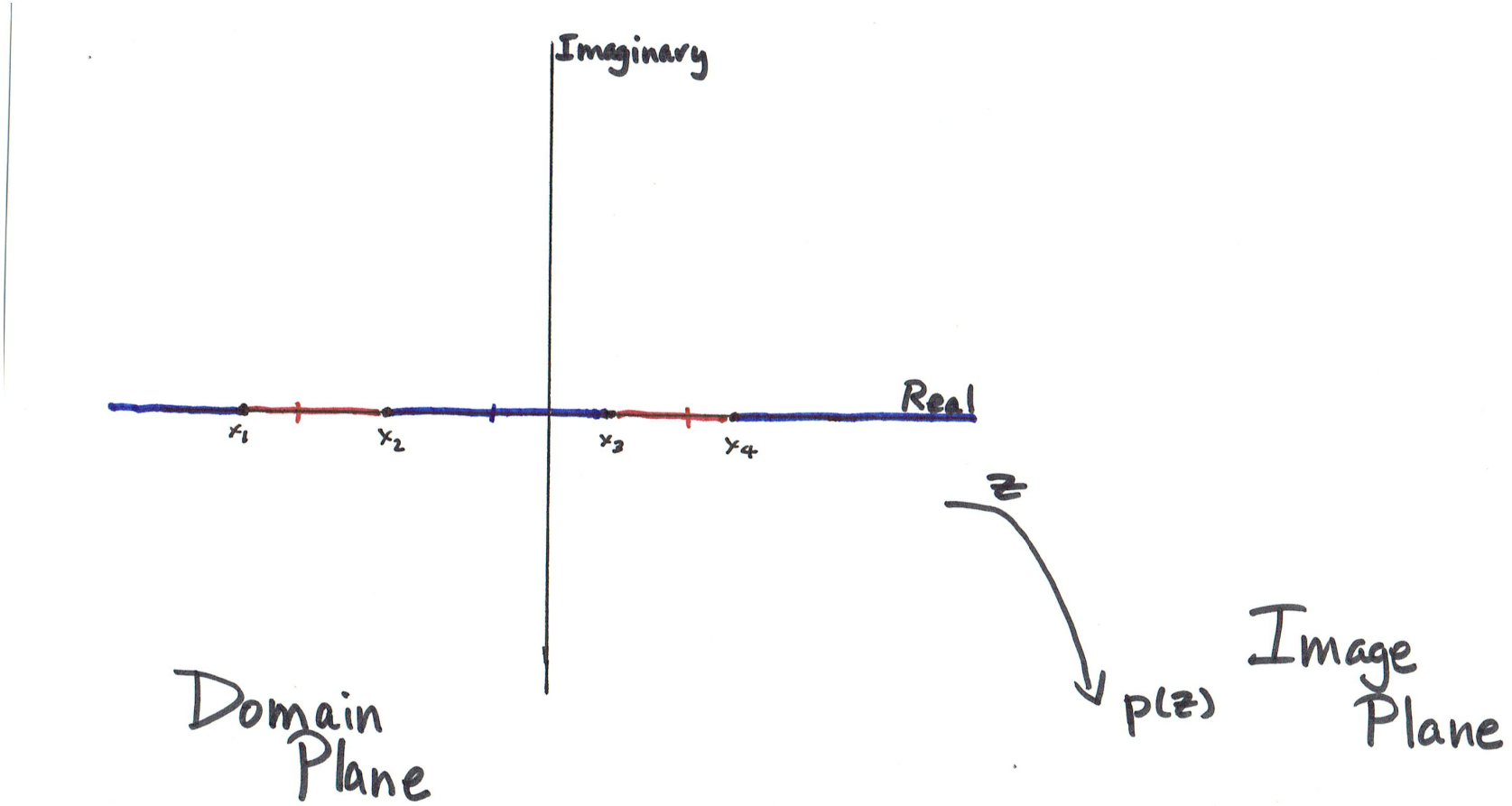


Roots, Critical Points, Critical Values



Roots, Critical Points, Critical Values

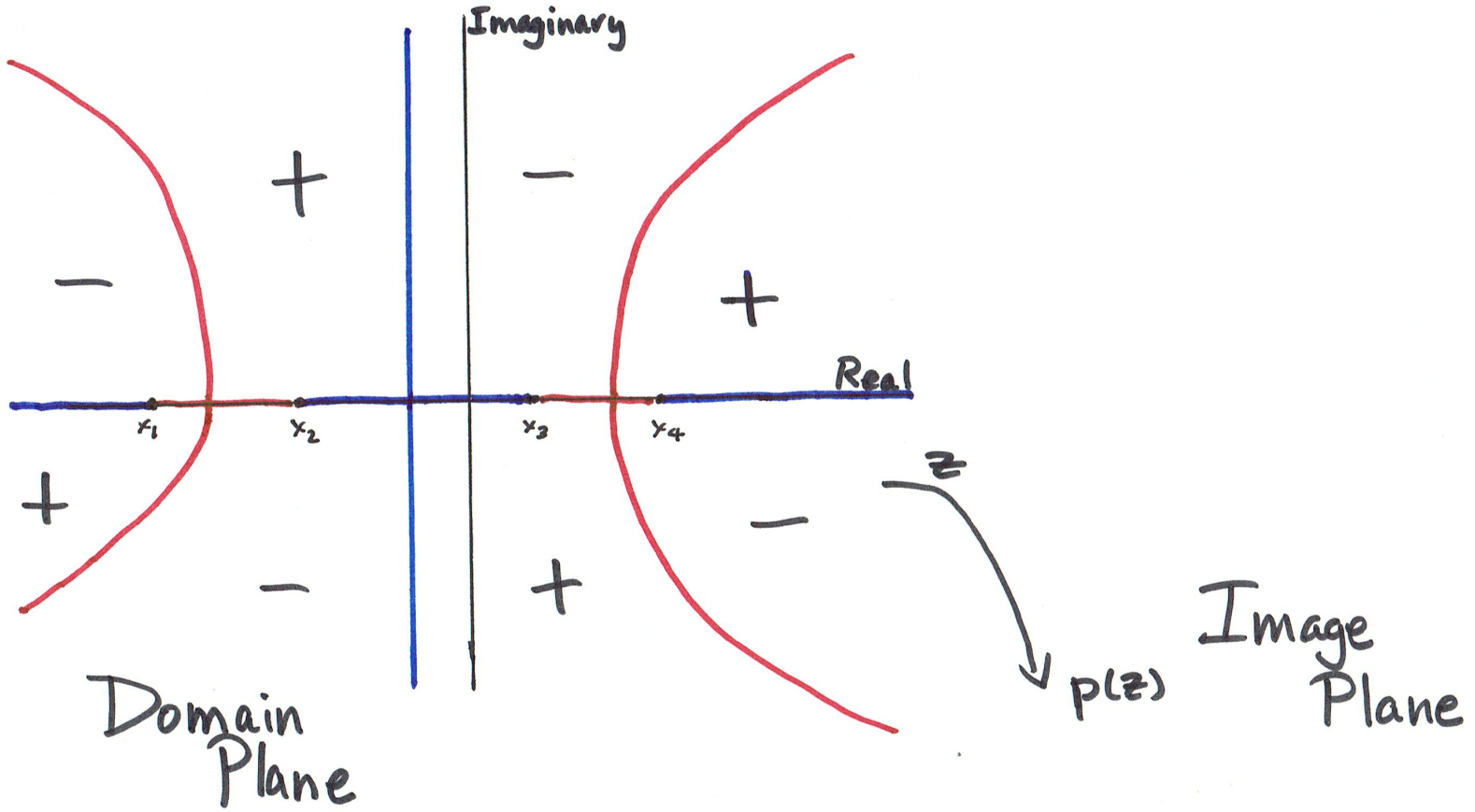
Mapping of Real Axis onto Negative and Positive Real Axis

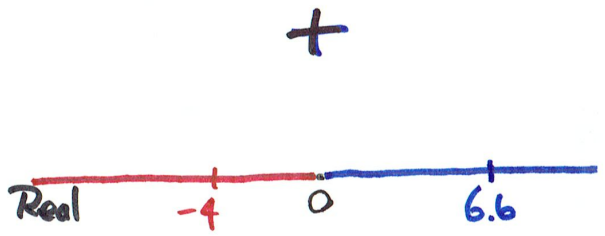


Roots, Critical Points, Critical Values

Mapping of Real Axis onto Negative and Positive Real Axis

Pullbacks (to Real Axis) of Negative and Positive Real Axis





Complete Pullbacks of Negative and Positive Real Axis

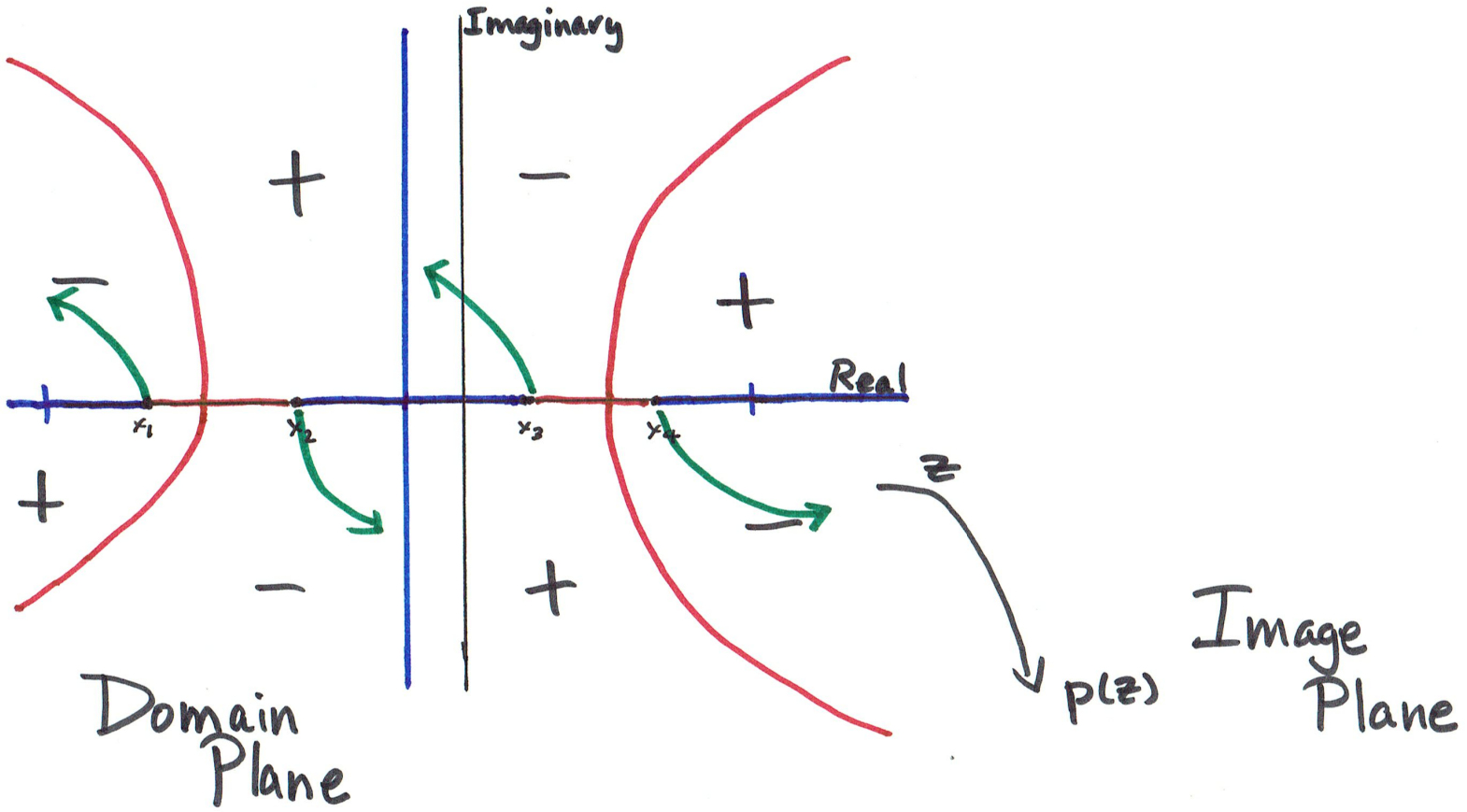
Complete Pullbacks of Upper (+) and Lower (−) Half-planes

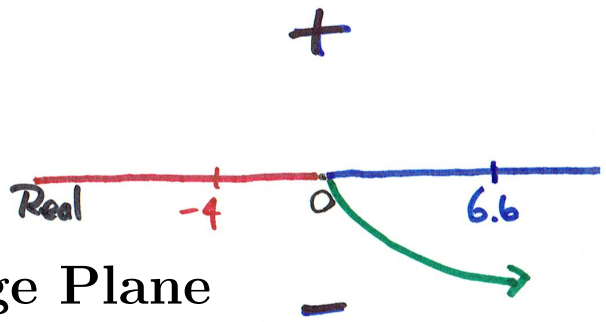
If F is a function or mapping of some 'Domain' onto some 'Image', then the 'Pullback' of a curve or set in the Image is the curve or set that F maps into the set in the Image.

In our case, $p : \mathbb{C} \mapsto \mathbb{C}$ and we are calling the two copies of the complex plane the 'Domain Plane' and the 'Image Plane'.

Because p is a four-to-one map of the plane onto the plane, the Pullback of the upper half-plane in the Image plane is four separate pieces in the Domain plane bounded by curves that are mapped by p onto the real axis.

Inverse image, Lift, and Pullback are closely related ideas that might be used in different contexts.



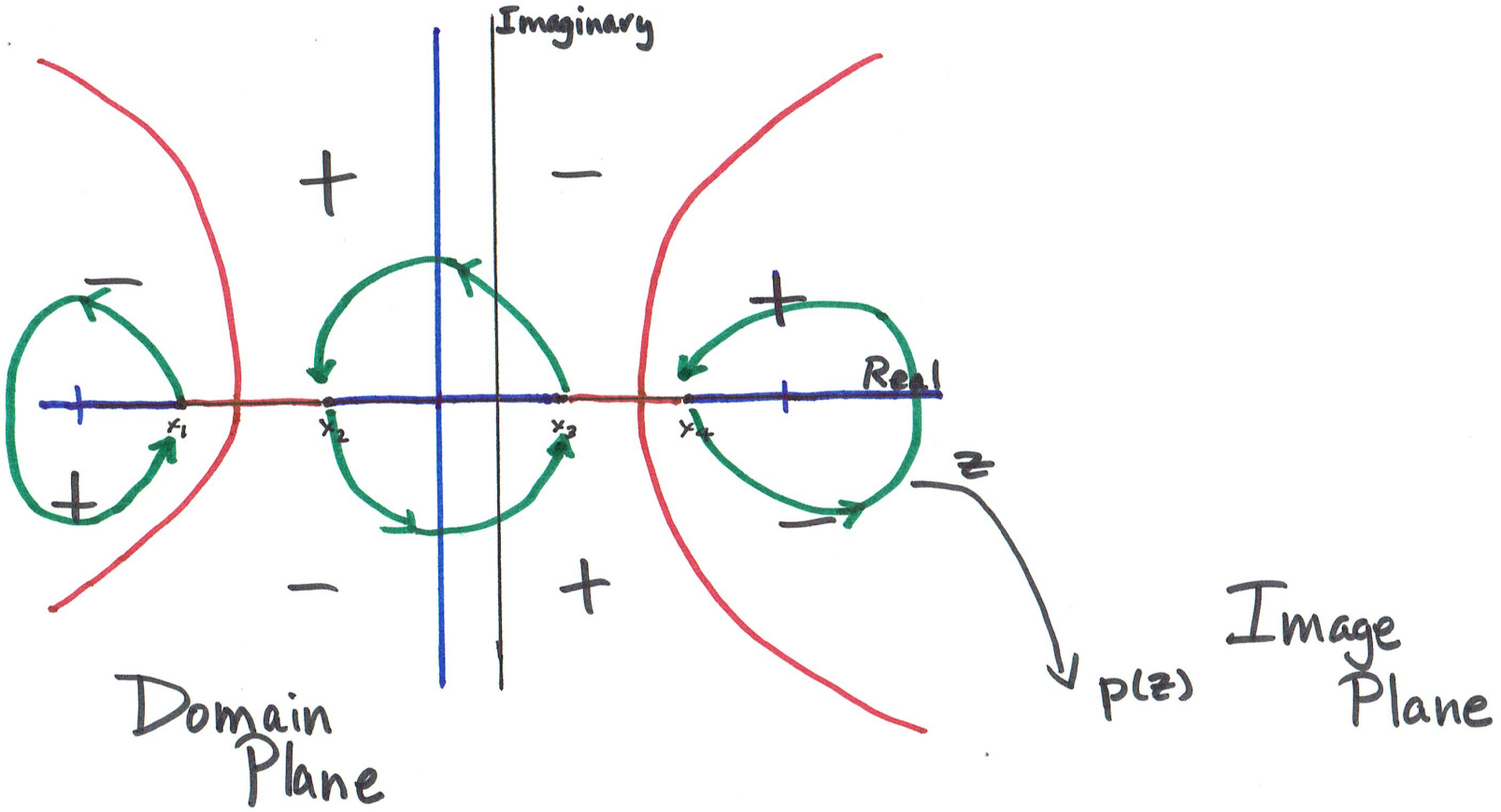


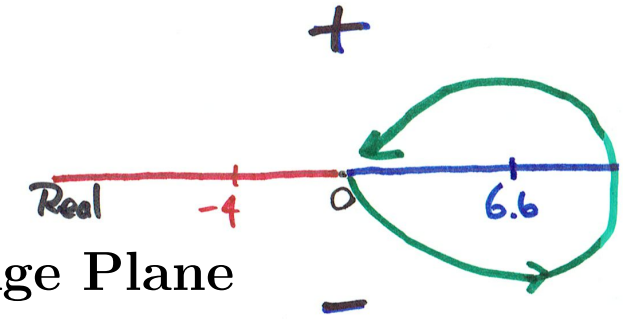
A Path going into lower half-plane of the Image Plane

Four Lifts in the Domain Plane of the Path in the Image Plane

A *Loop* is a path whose beginning point and whose end point are the same point.

A Pullback, or Lift, of a Loop can be a loop or a path with distinct endpoints.





A Loop going into lower half-plane of the Image Plane

Four Lifts in the Domain Plane of the Loop in the Image Plane

In the previous picture, the loop in the Image Plane starts and ends at 0 and goes around the Critical Value $p\left(-\frac{1}{2}\right) = \frac{105}{16}$.

A lift of this loop must have end points that p maps to 0, that is, the end points must be roots of p.

One lift of the loop is a loop with end points x_1 and going around the point of the real axis to the left of x_1 that gets mapped by p to $\frac{105}{16}$ and another is a loop with end points x_4 and going around a point to the right of x_4 that also is mapped by p to $\frac{105}{16}$.

The other two lifts of the loop are paths from x_3 to x_2 and from x_2 to x_3.

The critical observation here is that this loop in the Image Plane, starting and ending at 0, and encircling the critical value 105/16 once counterclockwise, is lifted to paths that give a permutation of the roots x_1, x_2, x_3, and x_4: namely the permutation produced is:

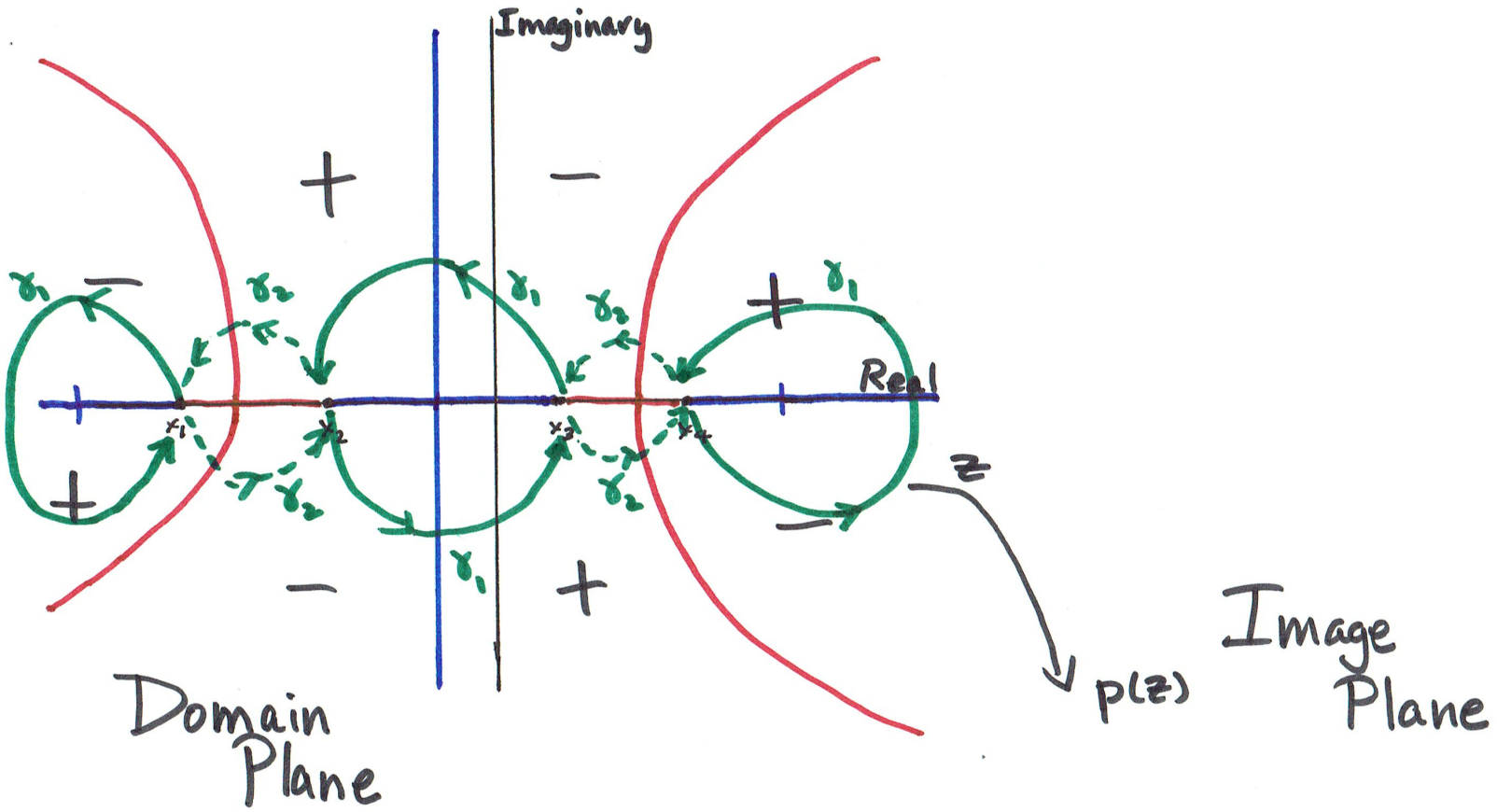
$$x_1 \to x_1 \qquad x_2 \to x_3 \qquad x_3 \to x_2 \qquad x_4 \to x_4$$

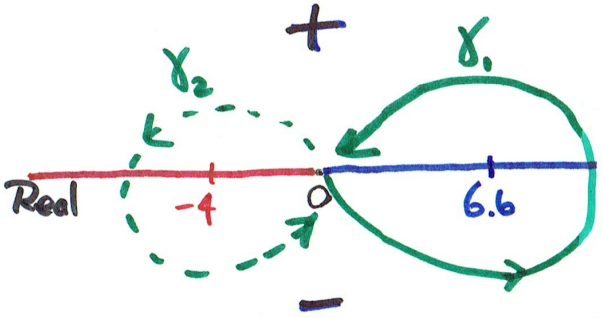
Recall that in algebra, a *Group* is a set G together with an operation $\bullet$ on the set combining order pairs of elements of G to produce an element of G, such that $\bullet$ is associative, there is a special element e such that $e \bullet \zeta = \zeta \bullet e = \zeta$ for each ζ in G, and for each ζ in G, there is is η in G so that $\zeta \bullet \eta = \eta \bullet \zeta = e$.

Easy examples are the integers under addition or the set of invertible $n \times n$ matrices under multiplication.

The integers under multiplication, however, do not form a group because there are not inverses under multiplication for most integers.

A more important example for us is the set of permutations, S_n, of a finite set with n elements.





Labeled Loops at 0 in the Image Plane

Labeled Lifts in the Domain Plane of the Loops in the Image Plane

In this picture, the original loop is labeled γ_1, and we have seen it is associated with a permutation, which we will call γ_1^*, of the roots of p:

$$\gamma_1^* : \qquad x_1 \to x_1 \qquad x_2 \to x_3 \qquad x_3 \to x_2 \qquad x_4 \to x_4$$

In the same way, the loop, γ_2, which has starting and ending point 0 and encircles the critical value -4 once counterclockwise, is lifted to paths that give a permutation of the roots x_1, x_2, x_3, and x_4: namely the permutation produced is:

$$\gamma_2^* : \qquad x_1 \to x_2 \qquad x_2 \to x_1 \qquad x_3 \to x_4 \qquad x_4 \to x_3$$

Similarly, every loop starting and ending at 0, not passing through either critical value, can be associated with a permutation of the zeros of p. These permutations form a group, G_p, which is a subgroup of the group of permutations of the set of roots, in this case, a subgroup of S_4.

For example, starting with loop γ_2, then following it with γ_1, which is a loop going counterclockwise around first -4 and then $105/16$, gives the permutation $(\gamma_2\gamma_1)^* = \gamma_1^*\gamma_2^*$:

$$x_1 \to x_2 \to x_3 \qquad x_2 \to x_1 \to x_1 \qquad x_3 \to x_4 \to x_4 \qquad x_4 \to x_3 \to x_2$$

In this case, computing all possible loops starting at 0, we find the group G_p is isomorphic to the group D_4, the set of symmetries of the square.

Thus, we have seen how a polynomial, p, of degree n, using a set of paths in the plane, can be associated with a group, G_p, that is a subgroup of the group S_n viewed as a group of permutations of the roots of p.

Now, the question is:

What happens if p is a composition of two, non-trivial, polynomials?

If p is a polynomial that is a composition of two polynomials, $p = q \circ r$, then the chain rule says

$$p'(z) = q'(r(z))r'(z)$$

This means that, if $r(z)$ is a critical point of q so that $q'(r(z)) = 0$, then $p'(z) = 0$ and z is a critical point of p.

And, in this case, $w = q(r(z))$ is a critical value of q, that is, $w = q(r(z)) = p(z)$ is a critical value of p.

If p is a polynomial that is a composition of two polynomials, $p = q \circ r$, then the chain rule says

$$p'(z) = q'(r(z))r'(z)$$

This means that, if $r(z)$ is a critical point of q so that $q'(r(z)) = 0$, then $p'(z) = 0$ and z is a critical point of p.

And, in this case, $w = q(r(z))$ is a critical value of q, that is, $w = q(r(z)) = p(z)$ is a critical value of p.

In other words, if p is a composition, $p = q \circ r$, then the set of critical values of q is a subset of the critcal values of p.

If $p = q \circ r$ is a polynomial, the fact that the critical values of q are all critical values of p means that the paths associated with the group G_p allow association of paths to G_q also.

The connection of the paths with the groups allows us to create a homomorphism π of G_p onto G_q. In particular, $G_q = G_p/\ker(\pi)$, so $p = q \circ r$ in a non-trivial way implies G_p has a non-trivial normal subgroup.

If $\mathcal{S}$ is a set, a *partition of* $\mathcal{S}$, is a collection $\mathcal{S}_1, \mathcal{S}_2, \cdots, \mathcal{S}_k$ of disjoint subsets of $\mathcal{S}$ so that $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2 \cup \cdots \cup \mathcal{S}_k$.

If η is a permutation of $\mathcal{S}$ and $\mathcal{S}_1, \mathcal{S}_2, \cdots, \mathcal{S}_k$ is a partition of $\mathcal{S}$, we say η *respects the partition* of $\mathcal{S}$ if $x \in \mathcal{S}_j$ implies $\eta(x) \in \mathcal{S}_j$ for all x in $\mathcal{S}$.

For a given polynomial p, we have associated a group G_p such that each element of G_p is associated with a permutation of the roots of p.

Now, each normal subgroup N of G_p is associated with a partition of the roots of p such that the elements of N respect the partition and the elements of N act transitively each set $\mathcal{S}_j$ in the partition.

Main Theorem:

Let p be a polynomial with distinct roots, let G_p be the group associated with p, and let N be a normal subgroup of G_p. Then N is associated with a partition of the roots of p

$$\{x_1, \cdots x_k\},\ \{x_{k+1}, \cdots x_{2k}\},\ \cdots,\ \{x_{(\ell-1)k+1}, \cdots x_{\ell k}\}$$

for which the degree of p is ℓk. Let r be the polynomial with roots x_1, x_2, $\cdots$, x_k, and q be the polynomial with roots $r(x_k)$, $r(x_{2k})$, $\cdots$, $r(x_{\ell k})$. Then $p = q \circ r$.

Conversely, if $p = q \circ r$, there is a homomorphism $\pi : G_p \mapsto G_q$ so that $G_q \approx G_p/\ker(\pi)$. Constructing $\widetilde{r}$ from $\ker(\pi)$ as above and $\widetilde{q}$ from p and $\widetilde{r}$, gives $p = \widetilde{q} \circ \widetilde{r}$ as a compositional factorization of p that is equivalent to $p = q \circ r$.

Since G_p is a finite group, it has only finitely many normal subgroups. For each normal subgroup, in principle, the calculations in the Main Theorem can be made. For some (non-trivial) normal subgroups, the compositional factorizations might be trivial. But, if any are non-trivial, then p has a non-trivial compositional factorization, and if none are, then p does not have a non-trivial compositional factorization.

Corollary:

If N is a normal subgroup of G_p with the order of N less than the degree of p, then there is a non-trivial factorization of $p = q \circ r$.

Our Example:

We had $p(z) = z^4 + 2z^3 - 5z^2 - 6z + 5$

Roots: $x_1 \approx -2.8$, $x_2 \approx -1.6$, $x_3 \approx 0.6$, and $x_4 \approx 1.8$

From the loops γ_1 and γ_2, we found permutations γ_1^* and γ_2^* that generated G_p which was isomorphic to D_4, the group of symmetries of the square.

In fact, $G_p = \{e,\ \gamma_1^*,\ \gamma_2^*,\ \gamma_1^*\gamma_2^*,\ \gamma_2^*\gamma_1^*,\ \gamma_1^*\gamma_2^*\gamma_1^*,\ \gamma_2^*\gamma_1^*\gamma_2^*,\ \gamma_1^*\gamma_2^*\gamma_1^*\gamma_2^*\}$

The six normal subgroups of G_p are $\{e\}$; G_p; $\mathcal{C} = \{e,\ \gamma_1^*\gamma_2^*\gamma_1^*\gamma_2^*\}$;
$N_1 = \{e,\ \gamma_1^*\gamma_2^*\gamma_1^*\gamma_2^*,\ \gamma_1^*,\ \gamma_2^*\gamma_1^*\gamma_2^*\}$; $N_2 = \{e,\ \gamma_1^*\gamma_2^*\gamma_1^*\gamma_2^*,\ \gamma_2^*,\ \gamma_1^*\gamma_2^*\gamma_1^*\}$;
and $N_3 = \{e,\ \gamma_1^*\gamma_2^*\gamma_1^*\gamma_2^*,\ \gamma_1^*\gamma_2^*,\ \gamma_2^*\gamma_1^*\}$.

Now, the normal subgroup $\{e\}$ acts trivially and the subgroups G_p, N_2, and N_3 act transitively on the set of roots. This means each of these normal subgroups gives a trivial compositional factorization of the polynomial p.

On the other hand, the normal subgroups $\mathcal{C}$ and N_1 each respect the partition $\{x_1, x_4\},\ \{x_2, x_3\}$.

According to the main theorem, we may take

$$r(z) = (z - x_1)(z - x_4) = z^2 + z - 1$$

and, because $r(x_1) = r(x_4) = 0$ and $r(x_2) = r(x_3) = 4$, we may take

$$q(z) = (z - 0)(z - 4) = z^2 - 4z$$

As expected,

$$q(r(z)) = (z^2 + z - 1)^2 - 4(z^2 + z - 1) = z^4 + 2z^3 - 5z^2 - 6z + 5 = p(z)$$

The normal subgroups $\mathcal{C}$ and N_1 each respect the partition

$\{x_1, x_4\},\ \{x_2, x_3\}$.

Also, according to the main theorem, we may take

$$\widetilde{r}(z) = (z - x_2)(z - x_3) = z^2 + z - 5$$

and, because $\widetilde{r}(x_2) = \widetilde{r}(x_3) = 0$ and $\widetilde{r}(x_1) = \widetilde{r}(x_4) = -4$, we may take

$$\widetilde{q}(z) = (z - 0)(z - (-4)) = z^2 + 4z$$

As expected,

$$\widetilde{q}(\widetilde{r}(z)) = (z^2 + z - 5)^2 + 4(z^2 + z - 5) = z^4 + 2z^3 - 5z^2 - 6z + 5 = p(z)$$

To summarize:

Mathematics is deeply unified and interconnected:

Beginning with a problem in complex analysis, using ideas from complex analysis, the theory of Riemann surfaces, and topology, a group is created. Ideas from group theory, involving normal subgroups and their actions, produced a solution the original problem!

To summarize:

Mathematics is deeply unified and interconnected:

Beginning with a problem in complex analysis, using ideas from complex analysis, the theory of Riemann surfaces, and topology, a group is created. Ideas from group theory, involving normal subgroups and their actions, produced a solution the original problem!

Realization: It helps to know about a lot of ideas!

I wouldn't have found this solution if I had not, against my inclination, learned some mathematics others thought important.

To summarize:

Mathematics is deeply unified and interconnected:

Beginning with a problem in complex analysis, using ideas from complex analysis, the theory of Riemann surfaces, and topology, a group is created. Ideas from group theory, involving normal subgroups and their actions, produced a solution the original problem!

Realization: It helps to know about a lot of ideas!

I wouldn't have found this solution if I had not, against my inclination, learned some mathematics others thought important.

Satisfaction!

I was pleased to have used something I had thought impossible to understand to solve an interesting problem.

To summarize:

Mathematics is deeply unified and interconnected:

Beginning with a problem in complex analysis, using ideas from complex analysis, the theory of Riemann surfaces, and topology, a group is created. Ideas from group theory, involving normal subgroups and their actions, produced a solution the original problem!

Realization: It helps to know about a lot of ideas!

I wouldn't have found this solution if I had not, against my inclination, learned some mathematics others thought important.

Satisfaction!

I was pleased to have used something I had thought impossible to understand to solve an interesting problem.

In time, I have forgiven Ritt for doing it first!

References:

- C. C. Cowen, Finite Blaschke products as compositions of other finite Blaschke products, *arXiv* 1207.4010v1, 2012.
- James Rickards, When is a polynomial the composition of other polynomials? *Amer. Math. Monthly* 118(2011), 358–363.
- J. F. Ritt, Prime and composite polynomials, *Trans. Amer. Math. Soc.* 23(1922), 51–66.
- J. F. Ritt, Permutable rational functions, *Trans. Amer. Math. Soc.* 25(1923), 399–448.

THANK YOU!

Slides: `http://www.math.iupui.edu/~ccowen/`