A Primer on Polynomials : Polys

Jonathan L.F. King
University of Florida, Gainesville 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
13 April, 2017 (at *02:31*)

Preliminaries. An expression such as $k \in \mathbb{N}$ (read as "k is an element of $\mathbb{N}$" or "k in $\mathbb{N}$") means that k is a natural number; a ***natnum***.

$\mathbb{N}$ = natural numbers = $\{0, 1, 2, \dots\}$.

$\mathbb{Z}$ = integers = $\{\dots, -2, -1, 0, 1, \dots\}$. For the set $\{1, 2, 3, \dots\}$ of positive integers, the ***posints***, use $\mathbb{Z}_+$. Use $\mathbb{Z}_-$ for the negative integers, the ***negints***.

$\mathbb{Q}$ = rational numbers = $\{\frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z}_+\}$. Use $\mathbb{Q}_+$ for the positive ***ratnums*** and $\mathbb{Q}_-$ for the negative ratnums.

$\mathbb{R}$ = reals. The ***posreals*** $\mathbb{R}_+$ and the ***negreals*** $\mathbb{R}_-$.

$\mathbb{C}$ = complex numbers, also called the ***complexes***.

Abbrevs. Seq: '*sequence*'. poly(s): '*polynomial(s)*'. irred: '*irreducible*'. Coeff: '*coefficient*' and var(s): '*variable(s)*' and parm(s): '*parameter(s)*'. Expr.: '*expression*'. CoI: '*Constant of Integration*'. LoI: '*Limit(s) of Integration*'.

Fnc: '*function*' (so ratfnc: means rational function, a ratio of polynomials). cty: '*continuity*'. cts: '*continuous*'. diff'able: '*differentiable*'.

Soln: '*Solution*'. Thm: '*Theorem*'. Prop'n: '*Proposition*'. CEX: '*Counterexample*'. eqn: '*equation*'. RhS: '*RightHand Side*' of an eqn or inequality. LhS: '*lefthand side*'. Sqrt or Sqroot: '*square-root*', e.g, "the sqroot of 16 is 4". Ptn: '*partition*', *but* pt: '*point*', as in "a fixed-pt of a map".

FTC: '*Fund. Thm of Calculus*'. IVT: '*intermediate-Value Thm*'. MVT: '*Mean-Value Thm*'. CoV: '*Change-of-Variable*'.

Below we will view various expressions as fncs of a variable, x. As usual, x^0 is a another name for the constant fnc 1.

§Outline

Monomials. Here are examples:

1a: $\quad -6x^2, \quad \sqrt{7} \cdot x^{10}, \quad \pi x, \quad 3, \quad 0\,.$

Here are *non*-examples:

1b: $\quad \sqrt{x}, \quad \mathsf{e}^x, \quad \log(x), \quad \sin(x)\,.$

A ***monomial*** is an expression OTForm Bx^n, where $n \in \mathbb{N}$ and B is a number (in $\mathbb{R}$ or $\mathbb{C}$), called the ***coefficient*** of x^n.

To justify the monomials of (1a), note $x^5 = 1{\cdot}x^5$, $3 = 3{\cdot}x^0$ and $0 = 0{\cdot}x^0$. In contrast, the expressions in (1b) don't look like monomials, although it would take some wrestling to show, for example, that $\sqrt[3]{x} \overset{\text{note}}{=\!=} x^{1/3}$ does not equal some Bx^n. It is easy to show that e^x is not a monomial: e^x has a horizontal asymptote as $x \searrow -\infty$, yet the only monomials with a horiz. asymptote are the constants. And e^x is *not* constant.

Polynomials. Examples:

1c: $\quad -3x^2 + x + 9, \quad \pi \cdot x^{77} - x \cdot \sqrt{\pi + \mathsf{e}}, \quad 4, \quad 0\,.$

A ***polynomial*** is a sum of finitely-many monomials. Thus $4 = 4x^0$ is a polynomial.

Degree. There are two "standard forms" of a polynomial. The ***low-to-high*** form (***LtH***) is

2a: $$f(x) = B_0 + B_1 x + \ldots + B_{N-1}x^{N-1} + B_N x^N .$$

We might stop at the highest N for which $B_N \neq 0$, or we might continue forever, writing the poly as a power-series whose seq. of coeffs is eventually-zero. So a poly $f(x) = \sum_{k=0}^{\infty} B_k x^k$ is a way of describing an *eventually-zero* seq. $\vec{\mathbf{B}} = (B_0, B_1, \ldots)$.

The poly $0 + 0{\cdot}x + 0{\cdot}x^2 + 0{\cdot}x^3 + \ldots$ we will call ***Zip***. In particular, Zip() is the identically-zero function.[♡1]

The ***high-to-low*** form (***HtL***) of a <u>non-zip</u> poly is

2b: $$f(x) = B_N x^N + B_{N-1}x^{N-1} + \ldots + B_1 x + B_0 ,$$

where $\boxed{B_N \neq 0}$. A non-zip poly is ***monic*** if its high-order coeff (also called its ***leading coefficient***) is 1; in (2b), then, this means that $B_N = 1$.

The ***degree*** of a non-zip p, written $\mathrm{Deg}(p)$, is the largest N such that x^N has a non-zero coeff.

Example E1. Consider these polynomials:

$$\begin{aligned} p(x) &:= 0x^2 + 7x + 2 ; \\ q(x) &:= 0x^2 + 0x + 2 ; \\ r(t) &:= 3 + t + t^{19} ; \\ s(y) &:= [y+1][y+2] - y^2 . \end{aligned}$$

Then $\mathrm{Deg}(p) = 1$, $\mathrm{Deg}(q) = 0$, $\mathrm{Deg}(r) = 19$ and $\mathrm{Deg}(s) = 1$; this last, since $s(y)$ equals

$$y^2 + y + 2y + 2 - y^2 \;=\; 3y + 2 ;$$

the latter is its HtL-form. □

A convention is to define $\mathrm{Deg}(\mathrm{Zip}) := -\infty$. This makes the three equalities in (2c), next, work when one or both of the polys is Zip.

[♡1] It is possible for a poly $g{:}\mathbf{F}{\to}\mathbf{F}$ over a <u>finite</u> field $\mathbf{F}$ to be identically-zero, yet have some non-zero coefficients. But over an infinite field, notions "poly g is Zip" and "$\forall x{:}\ g(x) = 0$" are the same. So over an infinite field, while a non-zip polynomial $g(x)$ can be zero for *some* values of x, this cannot happen for *all* values.

2c: Lemma. *The product, sum, and composition of polynomials,*

$$p \cdot q, \quad p + q, \quad p \circ q ,$$

are themselves polynomials. Furthermore

2c1: $\mathrm{Deg}(p \cdot q) = \mathrm{Deg}(p) + \mathrm{Deg}(q)$.

2c2: If p and q have distinct degrees, then $\mathrm{Deg}(p+q)$ equals $\mathrm{Max}\big\{\mathrm{Deg}(p), \mathrm{Deg}(q)\big\}$.

2c3: If neither p nor q is Zip, *then $\mathrm{Deg}(p \circ q)$ equals the product $\mathrm{Deg}(p) \cdot \mathrm{Deg}(q)$.* ♢

As an illustration, let $p(z) := z^2 - z + 3$ and $q(x) := x^{19} + 1$. Then

$$\begin{aligned} [p+q](t) &= t^2 - t + 3 + t^{19} + 1 ; \\ [p \cdot q](t) &= [t^2 - t + 3][t^{19} + 1] ; \\ [p \circ q](t) &= p\big(q(t)\big) = p(t^{19} + 1) \\ &= [t^{19} + 1]^2 - [t^{19} + 1] + 3 \\ &= t^{38} + t^{19} + 3 . \end{aligned}$$

Exercise. The product and composition of monic polynomials is monic. □

Upper-bounding degree. A polynomial p is an "***n-topped polynomial***" if $\mathrm{Deg}(p) < n$. Here are some 3-topped polys:

$$x^2 - 2x, \qquad x + \sqrt{7}, \qquad 17, \qquad \mathrm{Zip} .$$

However $x^3 + x$ is *not* 3-topped.

The *set* of 3-topped polynomials is the set of all $Ax^2 + Bx + C$, as numbers A, B, C vary. Thus this set is a 3-dimensional *vectorspace*.

The zeros of a polynomial

Polynomial p is an ***integral poly***, or an ***intpoly***, or a $\mathbb{Z}$-poly, if each $p()$ coeff is integral, i.e, is an integer. Poly p is called a ***rational polynomial*** (a ***ratpoly***), or a $\mathbb{Q}$-poly, if each coefficient of p is a rational number.

More generally, let Γ be either $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$: We call p a "**Γ-*polynomial*"** IFF each p-coeff is in Γ. For instance, $7x^2 - \boldsymbol{\pi}x$ is a $\mathbb{C}$-poly and an $\mathbb{R}$-poly, but is not a $\mathbb{Q}$-poly, since $\mathbb{Q} \not\ni \boldsymbol{\pi}$.

In any of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$, we can freely *add*, *subtract* and *multiply*; such a set Γ is called a ***ring***. For $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, we can also *divide* by non-zero values, and such an algebraic-system[♡2] is called a ***field***. Henceforth, the symbol $\mathbf{F}$ will mean a general field. I'll speak more about fields in a moment, but first let me say...

Don't Panic! I've designed these notes to be useful for high-school students up to undergraduate seniors (everyone will see some unfamiliar terms). Here is how to skip/substitute parts of the text.

Unfamilar with complex numbers? Then replace every $\mathbb{C}$ with $\mathbb{R}$.

Know $\mathbb{C}$, but not general fields? Then replace every $\mathbf{F}$ with one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Factoring. We now define *reducible* and *irreducible*; I'll apply these words to non-constant polys, i.e, $\text{Deg} \geqslant 1$. The irreducible polynomials play a role similar to the prime numbers; they are the fundamental objects of factoring.

Suppose that p is a non-constant $\mathbb{Q}$-poly. Say that p "factors over $\mathbb{Q}$", or "is **$\mathbb{Q}$-*reducible***", if we can write $p = q \cdot r$, where q and r *are* $\mathbb{Q}$-*polys*, and

$$\text{Deg}(q), \text{Deg}(r) \;<\; \text{Deg}(p)\,.$$

In contrast, p is **$\mathbb{Q}$-*irreducible*** (or "is irreducible over $\mathbb{Q}$") if p cannot be so factored. Define similarly $\mathbf{F}$-irreducible, for $\mathbf{F}$ one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Oftentimes, in factoring p it is convenient to write the factors as monic polys. So if p is non-monic with lead-coeff C, then we may write $p = C \cdot q \cdot r$, with q, r monic polys. E.g,

$$7x^2 - 35x + 70 \quad = \quad 7 \cdot [x-2][x-3]\,.$$

[♡2]Note that $\mathbb{Z}$ is not a field. For example, we can *not* divide 2 into 3, since there is no *integer* n for which $2n = 3$.

Example E2. Consider $p(t) := t^2 - 3$. This p is $\mathbb{R}$-reducible, since

$$p(t) = [t - \sqrt{3}] \cdot [t + \sqrt{3}]\,.$$

But p is $\mathbb{Q}$-*ir*reducible, since $t - \sqrt{3}$ is not a $\mathbb{Q}$-poly. After all, $\sqrt{3}$ is not rational. □

Example E3. Let $p(t) := 3t^4 - 13t^2 + 12$. We can factor this as $p = 3qr$, where

3i: $\quad q(t) := t^2 - 3 \quad$ and $\quad r(t) := t^2 - \frac{4}{3}\,.$

So p is $\mathbb{Q}$-reducible. But q and r are each $\mathbb{Q}$-irred, so $3qr$ is the *fully factored form* –over $\mathbb{Q}$– of p.

Over $\mathbb{R}$, however, p factors further, as

3ii: $\quad 3 \cdot \left[t - \sqrt{3}\right]\left[t + \sqrt{3}\right] \cdot \left[t - \sqrt{\tfrac{4}{3}}\right]\left[t + \sqrt{\tfrac{4}{3}}\right]\,.$ □

Example E4. Is $x^2 + \sqrt{3}$ irreducible over $\mathbb{Q}$?

Trick question! This poly is not a $\mathbb{Q}$-poly at all, so the question is not well-posed. □

Example E5. Polynomial $x^2 + 9$ is irreducible over $\mathbb{R}$. Over $\mathbb{C}$, however, it factors as

$$[x - 3\boldsymbol{i}][x + 3\boldsymbol{i}]\,,$$

where $\boldsymbol{i}^2 = -1$. □

Zeros/Roots of fncs. Consider a fnc $\psi: X \to Y$, where Y is a ring or vectorspace (has a distinguished element $0 \in Y$) and X is an arbitrary set. A point $\mathbf{z} \in X$ is a "***zero*** of ψ" if $\psi(\mathbf{z}) = 0$.

When ψ is a *polynomial* over a field $\mathbf{F}$, it is customary to call $\mathbf{z} \in X$ a ***root*** of ψ. See (5a) for precise defns.

The Quadratic Formula (QF)

Consider a quadratic polynomial

4: $$p(x) \;=\; Ax^2 + Bx + C\,;$$

since $\mathrm{Deg}(p) = 2$, necessarily $A \neq 0$. The ***discriminant***[♡3] of p, written $\mathrm{Discr}(p)$, is the number

$$\mathrm{Discr}(p) \;:=\; B^2 - 4AC\,.$$

Let D henceforth denote this number $\mathrm{Discr}(p)$.

Factor p as $p(x) = A[x-\alpha][x-\beta]$, where $\alpha\,\&\,\beta$ are the two zeros of p. The zeros $\alpha\,\&\,\beta$ of p are

$$\tfrac{1}{2A}[-B + \sqrt{D}] \quad \& \quad \tfrac{1}{2A}\big[-B - \sqrt{D}\big]\,.$$

Now suppose that p is a real poly. When $D > 0$ then p has distinct real zeros. When $D = 0$ then p has one zero, $\alpha = \beta$, of *multiplicity* 2. When $D < 0$ then p has no real zeros; it does, however, have two complex-conjugate zeros.

[♡3] Each non-zip polynomial p has an associated number called its ***discriminant***. This $\mathrm{Discr}(p)$ gives information about the zeros of p. When p is monic of degree N, then

$$\mathrm{Discr}(p) \;:=\; \prod_{j<k} [\alpha_j - \alpha_k]^2\,,$$

where $\alpha_1, \alpha_2, \ldots, \alpha_N$ are the zeros of p, listed with multiplicity. The product is taken over all "N choose 2" many pairs $j{<}k$ of distinct indices. A non-trivial theorem says that this product is a *polynomial* in the *coefficients* of p. E.g, in the quadratic case, the mapping $\mathbf{(}A, B, C\mathbf{)} \mapsto B^2 - 4AC$ is a 3-variable homogeneous polynomial of degree-2. Let's look at this when A is 1.

When p is a monic quadratic polynomial

$$p(t) \;=\; t^2 + Bt + C \;=\; [t-\alpha][t-\beta]\,,$$

then the above definition tells us that $\mathrm{Discr}(p)$ equals $[\alpha-\beta]^2$, which equals $\alpha^2 + \beta^2 - 2\alpha\beta$. On the other hand,

$$B^2 - 4AC \;=\; B^2 - 4C \;=\; [-\alpha-\beta]^2 - 4\alpha\beta\,,$$

which indeed equals $\alpha^2 + \beta^2 - 2\alpha\beta$. So we see, in this case, that $\mathrm{Discr}(p)$ is indeed a polynomial function of p's coefficients A, B, C.

See the **Vandermonde determinant** pamphlet for more on discriminants.

Irreducibility and the QF. When

$$p(x) \quad := \quad Ax^2 + Bx + C$$

is a real poly, then p is reducible over $\mathbb{R}$ IFF $D{:=}\mathrm{Discr}(p)$ is not negative. When $p()$ is a $\mathbb{Q}$-poly, then it is reducible over $\mathbb{Q}$ IFF D is the square of a rational number. That is, expressing D as n/d in lowest common terms with n and d posints, then $p()$ is $\mathbb{Q}$-reducible IFF $n\,\&\,d$ are each perfect squares.

Fully factored form. Let "FFF" abbreviate ***fully-factored form***. Suppose that

$$p(t) \;=\; C_N t^N + C_{N-1} t^{N-1} + \cdots + C_1 t + C_0\,,$$

is a $\mathbb{Q}$-poly of degree N. Say that

$$p() \;=\; C_N \cdot \textstyle\prod_{k=1}^{K} r_k()$$

is "the $\mathbb{Q}$-***FFF*** of p" if each r_k is a monic $\mathbb{Q}$-irreducible polynomial.

For example, the $\mathbb{Q}$-FFF of $3t^4 - 13t^2 + 12$ is

$$3 \cdot [t^2 - 3][t^2 - \tfrac{4}{3}]\,.$$

However, its $\mathbb{R}$-FFF is (3ii).

Multiplicity

Given $\mathbf{z} \in \mathbf{F}$ and non-zip $\mathbf{F}$-poly $p()$, there is a unique pair $M \in \mathbb{N}$ and $\mathbf{F}$-polynomial q st.

5a: $$p(x) \;=\; [x - \mathbf{z}]^M \cdot q(x), \text{ where } q(\mathbf{z}) \neq 0.$$

(I.e, the polynomials on the left and right of (5a) have the same coeff-sequence.) We call this natnum M the ***p-multiplicity*** of $\mathbf{z}$, or the "multiplicity of $\mathbf{z}$ in p", and write it $\boxed{\mathrm{Mult}(p, \mathbf{z})}$. If $M \geqslant 1$ then $\mathbf{z}$ is a ***root*** of p. In contrast, $M{=}0$ means that $\mathbf{z}$ is *not* a p-root; so to speak, "$\mathbf{z}$ has p-multiplicity 0", i.e $\mathrm{Mult}(p, \mathbf{z}) = 0$.

What means "multiplicity" for the 0-poly? Let

5b: $$\mathrm{Mult}(\mathrm{Zip},\, \mathbf{z}) \;:=\; +\infty \quad (\text{for every } \mathbf{z} \in \mathbf{F})\,,$$

since $\text{Zip}(x) = [x-\mathbf{z}]^M \cdot \text{Zip}(x)$ for each posint M.

Lastly, given a subset $\mathcal{S} \subset \mathbf{F}$ define

5c: $\quad {}^{\#}\text{Roots}(p,\, \mathcal{S}) \;:=\; \sum_{\mathbf{z}\in\mathcal{S}} \text{Mult}(p, \mathbf{z})\,;$

we are counting roots in $\mathcal{S}$ *with* multiplicity. Since factoring of non-zip polys is unique,[♡4] we get that

5d: If $p \neq \text{Zip}$ then ${}^{\#}\text{Roots}(p,\, \mathbf{F}) \;\leqslant\; \text{Deg}(p)\,.$

5e: Lemma. *Suppose real-poly p is non-zero on each endpoint of interval $\mathbf{J} := [x_0, x_1] \subset \mathbb{R}$. Then*

$R := {}^{\#}\text{Roots}(p,\, \mathbf{J})$ is even/odd as values $p(x_0), p(x_1)$ have same/opposite signs.

This also holds if R counts distinct roots in $\mathbf{J}$, i.e, ignoring multiplicity. *Proof.* Exercise. ♢

Differentiating a polynomial. Define the ***derivative*** of an $\mathbf{F}$-poly $p(x) = \sum_{\ell=0}^{N} C_\ell x^\ell$ to be

$$p'(x) \;:=\; \sum_{\ell=1}^{N} C_\ell \cdot \left[\ell \cdot x^{\ell-1}\right].$$

In particular, $\text{Zip}' = \text{Zip}$.

Recall that $f^{(M)}$ denotes the M^{th} derivative of fnc f. In particular, $f^{(0)}$ is another name for f.□

6: Derivative root-multiplicity Prop'n. *Over a field $\mathbf{F}$, examine a root $\mathbf{z} \in \mathbf{F}$ of non-zip $\mathbf{F}$-polynomial $p()$. With $M := \text{Mult}(p, \mathbf{z}) \in \mathbb{Z}_+$, then,*

6a: $\quad \text{Mult}(p', \mathbf{z}) \;\geqslant\; M-1\,.$

For the derivative polynomial we have equality

6b: $\quad \text{Mult}(p', \mathbf{z}) \;=\; M-1$

IFF either $\text{Char}(\mathbf{F}) = 0$ or $\text{Char}(\mathbf{F})$ is a prime that does not divide M. ♢

Pf. Factor $p(x) = [x-\mathbf{z}]^M \cdot g(x)$, with $g(\mathbf{z}) \neq 0$. Differentiating establishes (6a), since

6c: $\quad \begin{aligned} p'(x) \;&=\; [x-\mathbf{z}]^{M-1} \cdot s(x)\,, \quad \text{where} \\ s(x) \;&:=\; M\cdot g(x) \,+\, [x-\mathbf{z}]\cdot g'(x)\,. \end{aligned}$

So (6b) iff $s(\mathbf{z}) \neq 0$. Since $s(\mathbf{z}) = M\cdot g(\mathbf{z})$, this is equivalent to $M \nmid \text{Char}(\mathbf{F})$. ♦

See Gallian's text **Contemporary Abstract Algebra**, P.363, for more on the preceding and following results, and for "perfect" fields.

7: Lemma. *For a $\mathbb{C}$-polynomial p, point $\mathbf{z} \in \mathbb{C}$, and $M \in \mathbb{N}$, suppose that*

7a: *Each of these derivatives $p^{(0)}(\mathbf{z})\,,\; p^{(1)}(\mathbf{z})\,,\; p^{(2)}(\mathbf{z})\,,\; \ldots,\; p^{(M-1)}(\mathbf{z})$ equal zero, but $p^{(M)}(\mathbf{z}) \neq 0$.*

Then the p-multiplicity of $\mathbf{z}$ is M. ♢

Proof. WLOG $p \neq \text{Zip}$. Also, ISTShow that if $\text{Mult}(p, \mathbf{z}) = M$ then p has property (7a). The converse is immediate, since p can have (7a) for only *one* value of M.

For two L-times–differentiable fncs α and β, note that the L^{th} derivative equals (Product Rule)

$$[\alpha \cdot \beta]^{(L)} \;=\; \sum_{j+k=L} \binom{L}{j,k} \cdot \alpha^{(j)} \cdot \beta^{(k)}\,,$$

where j and k range over the natnums.

Let $M := \text{Mult}(p, \mathbf{z})$. Factor p as in (5a). For each $j \leqslant M$, this j^{th} derivative w.r.t x is

$$\Big[[x-\mathbf{z}]^M\Big]^{(j)} \;=\; \tfrac{M!}{[M-j]!} \cdot [x-\mathbf{z}]^{M-j}\,.$$

For each $L \leqslant M$, then,

$$p^{(L)}(x) \;=\; \sum_{j+k=L} \binom{L}{j,k} \cdot \tfrac{M!}{[M-j]!} \cdot [x-\mathbf{z}]^{M-j} \cdot g^{(k)}(x)\,.$$

When $L < M$, each exponent $M-j$ is positive, so $p^{(L)}(\mathbf{z}) = 0$. When $L = M$, conversely, $M-j = 0$ implies that $j = M$ and $k = 0$. So $p^{(M)}(\mathbf{z})$ equals

7b: $\quad 1 \cdot M! \cdot 1 \cdot g(\mathbf{z}) \overset{\text{note}}{=\!=} M! \cdot g(\mathbf{z})\,.$

This is not zero, so $p()$ has property (7a). ♦

[♡4] Well... for polynomials over a *field*.

7c: *Remark.* For a poly $p{:}\mathbf{F}\to\mathbf{F}$, the Lemma 7 holds IFF RhS(7*b*) is not zero. So the lemma holds IFF Char($\mathbf{F}$)=0 or $M<$Char($\mathbf{F}$).

When Char($\mathbf{F}$)=0, then poly p is Zip IFF

7d: *there exists a point* $\mathbf{z}\in\mathbf{F}$ *with* <u>*all*</u> *derivatives zero;* $\forall n{\in}\mathbb{N}$: $p^{(n)}(\mathbf{z})=0$.

This fails over fields of characteristic p. E.g, over $\mathbf{F}:=\mathbb{Z}_2$, the non-zip polynomial

$$f(x) \;:=\; x^2[x-1]^2 \;\overset{\text{note}}{=\!=}\; x^4+x^2$$

has $p^{(n)}(\mathbf{z})=0$ for all $\mathbf{z}\in\{0,1\}$ and $n\in\mathbb{N}$. This poly is also an example where the inequality in (6a) is strict. For $\text{Mult}(f,1)=2$. Yet $f'=\text{Zip}$, so $\text{Mult}(f',1)=+\infty$. □

8: Thm. *An irreducibile* $\mathbf{F}$*-polynomial* p *has no repeated roots, if either* Char($\mathbf{F}$) $=0$ *or* $p'\neq$ Zip. ♢

Proof. FTSOC, suppose $\mathbf{z}$ is a p-zero of multiplicity $M{\geqslant}2$. By (6a), $\mathbf{z}$ is a common zero of p' and p; thus $\text{Gcd}(p,p')$ is non-trivial. By irreducibility of p, then, $\text{Gcd}(p,p')$ equals p [times a unit, if you like]. Thus p divides p'. But $\text{Deg}(p')<\text{Deg}(p)$, so the only way this can happen is if $p'=\text{Zip}$.

For the Char($\mathbf{F}$)=0 case, since p is not constant

$$\text{Deg}(p') \;=\; \text{Deg}(p)-1 \;=\; M-1 \;>\; 0\,.$$

So automatically $p'\neq$ Zip. ♦

9: Neg-to-Pos Lemma. *Fix a non-zip* $\mathbb{R}$*-polynomial* p*. At each real root* $\mathbf{z}$ *of* p*, the rational-function* $\mathcal{R}:=\frac{p'}{p}$ *has a simple pole, and changes sign from negative to positive. In particular,*

9a: $$\liminf_{x\nearrow\mathbf{z}} \mathcal{R}(x) \;=\; -\infty \quad \textit{and}$$
$$\limsup_{x\searrow\mathbf{z}} \mathcal{R}(x) \;=\; +\infty\,.$$
♢

Pf. Factor $p(x)=[x-\mathbf{z}]^M\cdot g(x)$ with $M\in\mathbb{Z}_+$ and $g(\mathbf{z})\neq 0$. Then

9b: $$\frac{p'(x)}{p(x)} \;=\; \frac{M}{x-\mathbf{z}}+\frac{g'(x)}{g(x)}\,.$$

Since $g(\mathbf{z})\neq 0$, there exists an open interval $\mathbf{J}\ni\mathbf{z}$ with $g\rfloor_{\mathbf{J}}$ is bounded away from zero. So WELOG

$$-5 \;\leqslant\; \tfrac{g'}{g}\Big|_{\mathbf{J}} \;\leqslant\; 5\,.$$

OTOHand, the map $x\mapsto\frac{1}{x-\mathbf{z}}$ is unbounded as x increases past $\mathbf{z}$, and goes from negative to positive. And $M>0$. ♦

10: de Gua's Thm. *Fix a non-zip real poly* $p()$ *and an* [*possibly half-open, possibly infinite*] *interval* $\mathbf{J}\subset\mathbb{R}$*. Real polys* $A()$ *and* $B()$ *engender a poly*

$$H \;:=\; p'{\cdot}A \;+\; p{\cdot}B\,.$$

If $A\rfloor_{\mathbf{J}}>0$*, then*

10a: $$\#\text{Roots}(H,\mathbf{J}) \;\geqslant\; \#\text{Roots}(p,\mathbf{J})-1\,.$$ ♢

Pf. (We assume $\mathbf{J}$ open; the small modification necessary when a root $\mathbf{z}$ is an endpt of $\mathbf{J}$ is left to the reader.)

List all the <u>distinct</u> p-roots in $\mathbf{J}$ as

$$\mathbf{z}_1 \;<\; \mathbf{z}_2 \;<\; \ldots \;<\; \mathbf{z}_L \quad (\text{possibly } L=0)\,,$$

and let $M_\ell:=\text{Mult}(p,\mathbf{z}_\ell)$. By (6),

$$M_\ell-1 \;\leqslant\; \text{Mult}(p',\,\mathbf{z}_\ell) \;\overset{\text{note}}{\leqslant}\; \text{Mult}(H,\mathbf{z}_\ell)\,.$$

Adding these together,

$$\textstyle\sum_{\ell=1}^{L}\text{Mult}(H,\mathbf{z}_\ell) \;\geqslant\; \#\text{Roots}(p,\mathbf{J})-L\,.$$

So (10a) will follow if, for each $\ell\in[1\,..\,L)$, poly H has a root in open interval $\mathbf{J}_\ell:=(\mathbf{z}_\ell,\mathbf{z}_{\ell+1})$. This will follow from the IVThm if we can show that H changes sign on $\mathbf{J}_\ell$. Since $p()$ is never zero on $\mathbf{J}_\ell$, our $p()$ does *not* change sign. Thus ISTShow

> *For all* $\varepsilon{>}0$ *sufficiently small,* $\mathcal{R}(\mathbf{z}_\ell+\varepsilon)$ *and* $\mathcal{R}(\mathbf{z}_{\ell+1}-\varepsilon)$ *have opposite signs,*

where $\mathcal{R}:=\frac{H}{p}$. So ISTS that our $\mathcal{R}$ fulfills (9a).

Establishing (9a)**.** Fix a p-root $\mathbf{z} \in \mathbf{J}$. From the defn of H,

$$*: \qquad \frac{H}{p} \;=\; \left[\frac{p'}{p}\cdot A\right] \;+\; B\,.$$

By Neg-to-Pos, (9), ratio $\frac{p'}{p}$ satisfies (9a). But $A()$, being cts, is positive on a whole nbhd of $\mathbf{z}$, so product $\frac{p'}{p}\cdot A$ fulfills (9a). Hence so does RhS$(*)$, since polynomial B is bounded near $\mathbf{z}$. ♦

Variation of a tuple. Consider $\vec{\mathbf{a}} = \mathbf{(}a_1, \ldots, a_L\mathbf{)}$, a tuple of reals. Erase each entry which equals zero, giving a possibly-shorter tuple $\vec{\mathbf{b}} = \mathbf{(}b_1, \ldots, b_J\mathbf{)}$ of non-zero reals. Define $\mathrm{Var}(\vec{\mathbf{a}}) := \mathrm{Var}(\vec{\mathbf{b}})$ to be the number of sign-changes in $\vec{\mathbf{b}}$; that is, the number of $j \in [1\,..\,J)$ with $b_j{\cdot}b_{j+1} < 0$.

So $\mathrm{Var}(\mathbf{(}{-}3, {-}4, 0, {-}8\mathbf{)}) = 0$. And $\mathrm{Var}(\vec{\mathbf{a}}) = 2$, where $\vec{\mathbf{a}} := \mathbf{(}3, 0, 0, 4, 0, {-}1, 0, 9, 7, 0\mathbf{)}$. □

11: Descartes's rule-of-signs Thm. *For a non-zip real poly* $p(x) = a_N x^N + \cdots + a_1 x + a_0$, *let*

$$R \;:=\; {}^{\#}\mathrm{Roots}(p, \mathbb{R}_+) \quad \textit{and} \quad V \;:=\; \mathrm{Var}(\vec{\mathbf{a}})\,.$$

Then $V \geqslant R$. *Moreover, the difference* $V - R$ *is even.* ◊

Pf. We induct on V. Since negating p changes neither R nor V, WLOG $a_N > 0$.

CASE: $V = 0$ Every coefficient $a_i \geqslant 0$. For each $x{>}0$, then, $p(x)$ is strictly positive. So $R = 0$.

CASE: $V \geqslant 1$ Since $a_N > 0$, there exist indices $K{>}J$ in $[1\,..\,N]$ with $a_K > 0 > J$, and $a_i = 0$ for each $i \in (J\,..\,K)$.

We apply de Gua's Thm on $\mathbf{J} := \mathbb{Z}_+$, to

$$H(x) \;=\; p'(x){\cdot}x \;+\; p(x){\cdot}\mathrm{B} \;\overset{\text{note}}{=\!=}\; \sum_{\ell=0}^{N} b_\ell x^\ell\,, \quad \text{where } b_\ell := [\ell - \mathrm{B}]{\cdot}a_\ell\,,$$

where $\mathrm{B} := \frac{K+J}{2}$. So de Gua's asserts that

$${}^{\#}\mathrm{Roots}(H, \mathbb{R}_+) \quad \geqslant \quad R{-}1\,.$$

Since $K > \mathrm{B}$, we have, for each $\ell{\geqslant}K$, that $\ell - \mathrm{B} > 0$, so $\mathrm{Sgn}(b_\ell) = \mathrm{Sgn}(a_\ell)$. And $\mathrm{B} > J$ so, for each $\ell{\geqslant}K$, coeffs b_ℓ and a_ℓ have *opposite* signs. Thus $\vec{\mathbf{b}}$ has every variation that $\vec{\mathbf{a}}$ has *except* the one from index J to K. So $\mathrm{Var}(\vec{\mathbf{b}}) = V{-}1$.

Our induction hypothesis applied to H tells us that $V{-}1 \geqslant {}^{\#}\mathrm{Roots}(H, \mathbb{R}_+)$. Thus $V{-}1 \geqslant R{-}1$.

Even difference. Factor the given $p(x)$ as $x^L[a_N x^N + \cdots + a_1 x + a_0]$ with

$$a_N > 0 \;\; \textit{and} \;\; a_0 \neq 0.$$

Neither the number of coeff-variations, nor of positive roots, is changed by redefining

$$p(x) \;:=\; a_N x^N + \cdots + a_1 x + a_0\,.$$

Integer $\mathrm{Var}(\vec{\mathbf{a}})$ is even/odd as a_0 is pos/neg. ${}^{\#}\mathrm{Roots}(p,\, \mathbb{Z}_+)$

Unfinished: as of 13Apr2017 ♦

Defn. For $p(t) = C_0 + C_1 t + C_2 t^2 + \cdots + C_N t^N$, a polynomial over $\mathbb{C}$, its ***complex-conjugate*** is

$$\overline{p}(t) \;:=\; \overline{C_0} + \overline{C_1} t + \overline{C_2} t^2 + \cdots + \overline{C_N} t^N\,. \qquad \square$$

The ***discriminant*** of quadratic [i.e, $A{\neq}0$] polynomial $q(z) := Az^2 + Bz + C$ is

$$12.1\text{:} \quad \mathrm{Discr}(q) \;:=\; B^2 \,-\, 4AC\,.$$

The zeros ["roots"] of q are

$$12.2\text{:} \quad \mathrm{Roots}(q) \;=\; \frac{1}{2A}\Big[{-}B \,\pm\, \sqrt{\mathrm{Discr}(q)}\,\Big]\,.$$

Hence when A,B,C are *real*, then the zeros of q form a complex-conjugate pair. And q has a *repeated root* IFF $\mathrm{Discr}(q)$ is zero.

A monic $\mathbb{R}$-irreducible quadratic has form

$$12.3\text{:} \quad q(x) \;=\; x^2 - Sx + P \;=\; [x - \mathbf{z}]\cdot[x - \overline{\mathbf{z}}]\,,$$

where $\mathbf{z} \in \mathbb{C}{\smallsetminus}\mathbb{R}$. Note $S = \mathbf{z} + \overline{\mathbf{z}} = 2\mathrm{Re}(\mathbf{z})$ is the *Sum* of the roots. And $P = \mathbf{z}\cdot\overline{\mathbf{z}} = |\mathbf{z}|^2$ is the *Product* of the roots. The discriminant of g, $\mathrm{Discr}(g)$, equals

12.4: $S^2 - 4P \overset{\text{note}}{=\!=} [\mathbf{z} - \overline{\mathbf{z}}]^2 \;=\; -4\cdot[\mathrm{Im}(\mathbf{z})]^2\,.$

Completing-the-square yields

12.5: $q(x) \;=\; \left[x - \frac{S}{2}\right]^2 + F^2,$ where $F := |\mathrm{Im}(\mathbf{z})|\,,$

which is easily checked. [Exercise]

13: Fundamental Theorem of Algebra (Gauss and others). *Consider a monic $\mathbb{C}$-polynomial*

$$p(x) \;:=\; x^N + B_{N-1}x^{N-1} + \ldots + B_1 x + B_0\,.$$

Then p factors completely over $\mathbb{C}$ as

$$p(x) \;=\; [x - \mathbf{z}_1]\cdot[x - \mathbf{z}_2]\cdot\ldots\cdot[x - \mathbf{z}_N]\,, \qquad \diamondsuit$$

for a list $\mathbf{z}_1, \ldots, \mathbf{z}_N \in \mathbb{C}$, possibly with repetitions. This list is unique up to reordering.

*If p is a **real** polynomial, i.e $\overline{p} = p$, then p factors over $\mathbb{R}$ as a product of monic $\mathbb{R}$-irreducible linear and $\mathbb{R}$-irred. quadratic polynomials. The product is unique up to reordering.* *Proof.* In appendix, (27).

Division. Fix a field $\mathbf{F}$, e.g $\mathbf{F}$ is one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

We now discuss dividing one poly d (the "divisor") into another poly p (the "dividend").

14: Division Thm. *Consider $\mathbf{F}$-poly p (the dividend) and non-zip $\mathbf{F}$-poly d (the divisor). Then there exists a unique pair of $\mathbf{F}$-polys q and $\mathbf{r}$ (the quotient and remainder) so that*

$$p \;=\; [d\cdot q] + \mathbf{r}\,, \quad \text{where } \mathrm{Deg}(\mathbf{r}) < \mathrm{Deg}(d). \qquad \diamondsuit$$

15: GCD Corollary. *The greatest common divisor poly d of two polynomials p_1, p_2 (not both zip) is a linear combination of them, in the sense that*

$$d() \qquad = \qquad \beta_1()\cdot p_1() \;+\; \beta_2()\cdot p_2()$$

for some "coefficient polynomials" β_1 and β_2. $\diamondsuit$

Polynomial d is written as $\mathrm{Gcd}(p_1, p_2)$.

Rational Functions

Suppose Γ is one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. I'll use the symbol $\Gamma[\![x]\!]$ for the **set** of Γ-polynomials using the variable x. Also $\Gamma(\!(x)\!)$ is used for the **set** of rational functions over Γ, which we introduce next.

Recall that a rational number is a ratio of two *integers*, with the denominator non-zero. Analogously, a ***rational function***, f, is a ratio of two *polynomials* with non-zip denominator . The following,

$$t^4 - t\,; \quad 3\,; \quad \frac{1}{\mathsf{e}\cdot t^6 - \sqrt{3}}\,; \quad \frac{t^2+1}{6t^5 - \boldsymbol{\pi}}\,,$$

are each rational functions of t. In contrast, e^t is not a ***ratfnc*** (rational function) of t.

16: Theorem. *Over a field $\mathbf{F}$, each sum, product, quotient and composition of ratfncs*

$$f + h, \quad f\cdot h, \quad f/h, \quad f\circ h\,,$$

is a ratfnc; the quotient f/h requires that $h \neq$ Zip.

In particular, the set $\mathbf{F}(\!(x)\!)$, of rational functions, is itself a field.[♡5] $\diamondsuit$

Algebraic and Transcendental numbers

A real (or complex) number α is ***algebraic*** if it is a root of *some* non-zip intpoly (equiv., ratpoly) f. Thus

$$\alpha_1 \;:=\; \sqrt[2]{5} \quad \text{and} \quad \alpha_2 \;:=\; \sqrt[4]{17}$$

are algebraic numbers, since α_1 is a root of $x^2 - 5$, and α_2 is a root of $x^4 - 17$. Evidently each rational number P/Q is algebraic, since it is a root of intpoly $Qx - P$.

[♡5] An algebraist would write this field as $\big(\mathbf{F}(\!(x)\!), +, 0, \cdot, 1\big)$, where 0 and 1 denote constant *rational functions*.

Each algebraic number α has an associated posint called its ***degree***; it is written $\mathrm{Deg}(\alpha)$. Writing $\mathbf{d} := \mathrm{Deg}(\alpha)$, then α is a root of some degree-$\mathbf{d}$ intpoly, but is the root of no lower degree (non-zip) intpoly. Evidently, the rational numbers are precisely those numbers of degree 1. As another example, the above α_1 has degree 2, since $\sqrt[2]{5}$ is known to be irrational.

Use $\mathbb{A}$ for the *set* of algebraic numbers in $\mathbb{C}$. We see that $\mathbb{A}$ is stratified into a *hierarchy* by degree. The numbers in the complement, $\mathbb{C} \setminus \mathbb{A}$, *transcend* this hierarchy so –not surprisingly– each such number is said to be ***transcendental***. Although this is not obvious, each of these three numbers

$$\boldsymbol{\pi}, \quad \mathsf{e}, \quad \tau := \sum_{n=1}^{\infty} \frac{1}{b_n}, \text{ where } b_n := 2^{n!},$$

is transcendental.[♡6]

We define the degree of a transcendental number to be ∞. That is to say, the degree of a number $\alpha \in \mathbb{C}$ is the *infimum* of numbers $d \in [1 \,..\, \infty]$ such that α is a zero of some degree-d intpoly.

17: Theorem. *You can add, subtract multiply and divide algebraic numbers, and the result is always algebraic. Specifically, consider two algebraic numbers $\alpha,\beta \in \mathbb{A}$. Then the following hold.*

i: *$\mathrm{Deg}(1/\beta)$ equals $\mathrm{Deg}(\beta)$.*

ii: *The degrees of $\alpha \pm \beta$ and of $\alpha \cdot \beta$ and α/β are upper-bnded by the product $\mathrm{Deg}(\alpha) \cdot \mathrm{Deg}(\beta)$.*

iii: *For an arbitrary rational function $F(x, y)$ with rational coefficients: The degree of $F(\alpha, \beta)$ is upper-bnded by $\mathrm{Deg}(\alpha) \cdot \mathrm{Deg}(\beta)$.*

All assertions involving division by β require β to be non-zero. ◊

A particular implication of the above thm is that the *set* $\mathbb{A}$ of algebraic numbers forms a *field*. This is not obvious.

[♡6]Such a τ is called a *Liouville number*. There is an explanation of Liouville numbers on my Teaching Page.

18: Prop'n. *For α algebraic, let $N := \mathrm{Deg}(\alpha)$. Then there is a unique monic ratpoly $H()$ with $H(\alpha) = 0$. Moreover, H is $\mathbb{Q}$-irreducible.* ◊

Proof. Suppose $H, \widehat{h}$ are degree-N monic ratpolys sending α to zero. Then ratpoly $H - \widehat{h}$ has smaller degree, and $[H - \widehat{h}](\alpha) = 0$, so $H - \widehat{h}$ must be zip.

Irreducibility: FTSOC suppose $H = p \cdot q$, for monic ratpolys of degree $< N$. Then $p(\alpha) \cdot q(\alpha)$ is zero, so WLOG $p(\alpha) = 0$. But p is monic and $\mathrm{Deg}(p) < \mathrm{Deg}(H)$, contradicting the minimal-degreeness of H. ♦

Defn. This minimal-degree monic poly H is called the "***minimal polynomial*** (***min-poly***) of α".

This H is a ratpoly. Sometimes one wants an intpoly. If I say "let H be the minimal *intpoly* of α", then this means that H is the unique minimum-degree intpoly, with leading-coefficient *positive*, and with $\mathrm{Gcd}(H\text{'s coeffs}) = 1$. □

Subfields of $\mathbb{C}$

Fix an $\boldsymbol{\alpha} \in \mathbb{C}$. Let $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$ be the set of complex numbers OTForm $q(\boldsymbol{\alpha})$, where q ranges over all $\mathbb{Q}$-polys. Easily, the set $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$ is what algebraists call a ***ring***; adding or multiplying two numbers in the set keeps you in the set. (That is not a formal defn of "ring".)

19: Lemma. *Suppose that $\boldsymbol{\alpha}$ is an algebraic number of degree N. Then $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$ is an N-dim'al $\mathbb{Q}$-vectorspace, and $\{1, \boldsymbol{\alpha}, \boldsymbol{\alpha}^2, \ldots, \boldsymbol{\alpha}^{N-1}\}$ is a $\mathbb{Q}$-basis.*

Moreover, $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$ is a field, and hence equals $\mathbb{Q}(\!(\boldsymbol{\alpha})\!)$. ◊

Proof. We start by establishing spanning.

The set $\{1,\boldsymbol{\alpha},\ldots,\boldsymbol{\alpha}^{N-1}\}$ ***spans*** $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$**.** Let H be the min-poly of $\boldsymbol{\alpha}$; set $N := \text{Deg}(H)\geqslant 1$. Each element of $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$ has form $f(\boldsymbol{\alpha})$, for some ratpoly f. WLOG $\boxed{\text{Deg}(f)<N}$; for divide H into f to write $f = [H\cdot q]+\mathbf{r}$ where $\text{Deg}(\mathbf{r})<N$. Thus $\mathbf{r}(\boldsymbol{\alpha})=f(\boldsymbol{\alpha})$. Hence $f(\boldsymbol{\alpha})$ is in the $\mathbb{Q}$-span of $\{1,\boldsymbol{\alpha},\ldots,\boldsymbol{\alpha}^{N-1}\}$.

Linear independence of $\{1,\boldsymbol{\alpha},\ldots,\boldsymbol{\alpha}^{N-1}\}$**.** FTSOC, suppose that $\sum_{j=0}^{N-1} B_j\boldsymbol{\alpha}^j = 0$, non-trivially. Let $K\leqslant N-1$ be highest index with $B_K\neq 0$. Dividing the eqn by B_K and renaming, we now have $0=\boldsymbol{\alpha}^K+\sum_{j=0}^{K-1}B_j\boldsymbol{\alpha}^j$. But this says that $\boldsymbol{\alpha}$ is the root of a monic degree-K ratpoly. ⋙

$\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$ ***is a field.*** Fix a non-zero $\omega\in\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$; there is a ratpoly, call it f, with $f(\boldsymbol{\alpha})=\omega$. To show that $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]\ni\frac{1}{\omega}$, we will produce a ratpoly T with

$$\dagger: \qquad f(\boldsymbol{\alpha})\cdot T(\boldsymbol{\alpha}) \;=\; 1\,.$$

Firstly, $f\neq$ Zip, since $\omega\neq 0$. Thus $f\perp H$, since H is irreducible and $\text{Deg}(f)\overset{\text{WLOG}}{<}\text{Deg}(H)$. So there exist [Bézout's lemma] ratpolys S and T with $1=HS+fT$. Evaluating at $\boldsymbol{\alpha}$ yields (†). ♦

20: Thm. *Suppose* $\boldsymbol{\alpha}$ *and* $\boldsymbol{\beta}$ *are roots of an irreducible* $\mathbb{Q}$*-poly,* h*, of degree* $N\geqslant 2$*. Then* $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$ *is field-isomorphic (and vectorspace isomorphic) to* $\mathbb{Q}[\![\boldsymbol{\beta}]\!]$*, via map*

$$\dagger: \qquad \sum_{k=0}^{N-1} q_k\cdot\boldsymbol{\alpha}^k \;\longmapsto\; \sum_{k=0}^{N-1} q_k\cdot\boldsymbol{\beta}^k\,,$$

where the q_k *range over the rational numbers.* ◊

Quadratic extensions

Fix a $\mathbb{Q}$-irreducible quadratic $h(z)=z^2-Sz+P$; so $S,P\in\mathbb{Q}$ with $P\neq 0$. By the Quadratic Formula, there are complex numbers $\boldsymbol{\alpha}$,$\boldsymbol{\beta}$ such that

$$h(z) \;=\; z^2-Sz+P \;=\; [z-\boldsymbol{\alpha}]\cdot[z-\boldsymbol{\beta}]\,.$$

Necessarily, $\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathbb{C}\smallsetminus\mathbb{Q}$ and $\boldsymbol{\alpha}\neq\boldsymbol{\beta}$, since h is irred..

$$*: \quad \text{Thus} \quad \boldsymbol{\alpha}+\boldsymbol{\beta} \;=\; S \qquad \text{(Sum)}$$
$$\text{and} \quad \boldsymbol{\alpha}\cdot\boldsymbol{\beta} \;=\; P\,. \qquad \text{(Product)}$$

Let $\mathbf{F}:=\mathbb{Q}[\![\boldsymbol{\alpha}]\!]\overset{\text{note}}{=\!=}1\cdot\mathbb{Q}+\boldsymbol{\alpha}\cdot\mathbb{Q}$ be this vectorspace (and field). Courtesy $(*)$, note, $\mathbb{Q}[\![\boldsymbol{\beta}]\!]=\mathbf{F}=\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$.

For each $\zeta\in\mathbf{F}$ define $\overline{\zeta}$, its ***"h-conjugate"***. The h***-conjugation*** map $\zeta\mapsto\overline{\zeta}$ is an *involution* (i.e, $\overline{\overline{\zeta}}=\zeta$) which "interchanges $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$". It is determined by

$$\overline{1}:=1, \quad \overline{\boldsymbol{\alpha}}:=\boldsymbol{\beta}, \quad \overline{\boldsymbol{\beta}}:=\boldsymbol{\alpha}\,.$$

For $x,y\in\mathbb{Q}$, then,

$$\overline{x-y\boldsymbol{\alpha}}\overset{\text{def}}{=\!=}x-y\boldsymbol{\beta}=x-y[S-\boldsymbol{\alpha}]=[x-yS]+y\boldsymbol{\alpha}\,.$$

The mapping $\zeta\mapsto\overline{\zeta}$ is special case of (20†), a field automorphism. It engenders a ***norm*** $\mathcal{N}:\mathbf{F}\to\mathbb{Q}$ by

$$21: \quad \mathcal{N}(\zeta):=\mathcal{N}_h(\zeta):=\zeta\cdot\overline{\zeta}\overset{\text{note}}{=\!=}x^2-xyS+y^2P\,,$$

where $\zeta:=x-y\boldsymbol{\alpha}$. This norm is (totally) ***multiplicative*** in that

$$22: \qquad \mathcal{N}(\zeta\cdot z)\overset{\text{def}}{=\!=}\zeta z\overline{\zeta z}\;=\;\mathcal{N}(\zeta)\cdot\mathcal{N}(z)\,,$$

for all $\zeta,z\in\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$.

23: Lemma. $\mathcal{N}(\zeta)=0$ *IFF* $\zeta=0$.

Proof of $(\Rightarrow)$. Write $\zeta:=x-y\boldsymbol{\alpha}$. FTSOC, first suppose that $y\neq 0$. Courtesy (21), then,

$$0 \;=\; \tfrac{1}{y^2}\cdot 0 \;=\; \tfrac{1}{y^2}\cdot\mathcal{N}(\zeta)\overset{\text{note}}{=\!=}h(\tfrac{x}{y})\,.$$

So $\frac{x}{y}$ must be $\boldsymbol{\alpha}$ or $\boldsymbol{\beta}$. But x/y is rational. ⋙

Thus $y=0$. So $\mathcal{N}(\zeta)=x^2$, which forces $x=0$.♦

Note. A corollary is that $\mathbb{Q}[\![\boldsymbol{\alpha}]\!]$ is a field, since

$$1/\zeta \;=\; \overline{\zeta}/\mathcal{N}(\zeta) \;=\; \tfrac{x}{\mathcal{N}(\zeta)}-\tfrac{y}{\mathcal{N}(\zeta)}\boldsymbol{\beta}$$
$$=\; \tfrac{x-yS}{\mathcal{N}(\zeta)}+\tfrac{y}{\mathcal{N}(\zeta)}\boldsymbol{\alpha}\,. \qquad \square$$

Case: S and P are integers. Let $\Gamma := \mathbb{Z}[\![\boldsymbol{\alpha}]\!]$; so $\mathbb{Z}[\![\boldsymbol{\beta}]\!] = \Gamma$, since $S \in \mathbb{Z}$. And the norm $\mathcal{N}(\cdot)$ maps Γ into $\mathbb{Z}$, as (21) shows.

Let $\mathbb{U}_\Gamma$ be the group of units in Γ.

24: Lem. *For $\zeta \in \Gamma$: $\mathcal{N}(\zeta) \in \mathbb{U}_\mathbb{Z}$ IFF $\zeta \in \mathbb{U}_\Gamma$.* ♢

Pf of ($\Rightarrow$). By hypothesis, $u := 1/\mathcal{N}(\zeta)$ is ± 1. And

$$1 \;=\; \mathcal{N}(\zeta) \cdot u \;=\; \zeta \cdot \bar{\zeta} u \,.$$

Thus ζ *is* a Γ-unit, since $\bar{\zeta} u \in \Gamma$ (since $u \in \Gamma$). ♦

Proof of ($\Leftarrow$). Take $\omega \in \Gamma$ with $\zeta\omega = 1$. Thus

$$1 \;=\; \mathcal{N}(1) \;=\; \mathcal{N}(\zeta) \cdot \mathcal{N}(\omega) \,.$$

These last two are integers, so $\mathcal{N}(\zeta)$ is a $\mathbb{Z}$-unit. ♦

25: *Appl.* Let $\boldsymbol{\alpha} := \sqrt{-5}$ and $\Gamma := \mathbb{Z}[\![\boldsymbol{\alpha}]\!]$. So $\mathcal{N}(x + y\boldsymbol{\alpha}) = x^2 + 5y^2$. Note that

$$\dagger: \qquad 2 \cdot 3 \;=\; 6 \;=\; [1 + \boldsymbol{\alpha}][1 - \boldsymbol{\alpha}] \,.$$

Call each of these four numbers $1 \pm \boldsymbol{\alpha}, 2, 3$ a "blip". Let's show that each blip is Γ-irreducible by using its norm,

$$\ddagger: \qquad \mathcal{N}(1 \pm \boldsymbol{\alpha}) = 6 \,; \quad \mathcal{N}(2) = 4 \,; \quad \mathcal{N}(3) = 9 \,.$$

None of $6, 4, 9$ divides another so, by (22), no blip on LhS($\dagger$) divides a blip on RhS($\dagger$), and vice versa. Thus no blip is Γ-prime.

Each blip is Γ-irred. By (22), were a blip to have a nt-factor ζ, its norm would have a nt-$\mathbb{Z}$-factor $\mathcal{N}(\zeta)$. The only *non-negative* nt-factors of $6, 4, 9$ (this norm $\mathcal{N}()$ is non-negative) are $2, 3$. Were $\boxed{x^2 + 5y^2 = 2 \text{ or } 3}$ to have an integer soln, then the corresponding congruence would too, i.e $x^2 \equiv_5 \pm 2$. But the mod-5 squares in $[-2 \,..\, 2]$ are $0, \pm 1$.

Lastly, none of $6, 4, 9$ is a $\mathbb{Z}$-unit (i.e, not ± 1), so (24) says that no blip is a Γ-unit. □

26: *Application.* Let $\boldsymbol{\alpha} := \sqrt{5}$ and $\Lambda := \mathbb{Z}[\![\boldsymbol{\alpha}]\!]$. So $\mathcal{N}(x + y\boldsymbol{\alpha}) = x^2 - 5y^2$. Note

$$\dagger: \qquad 2 \cdot -2 \;=\; -4 \;=\; [1 + \boldsymbol{\alpha}][1 - \boldsymbol{\alpha}] \,.$$

A similar argument shows that each of ± 2, $1 \pm \boldsymbol{\alpha}$ is Λ-irreducible but not Λ-prime. □

More general coefficients

So far, we have considered polys whose coefficients come from a set, Γ, where Γ is either $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$. More generally, we can allow Γ to be a commutative ring. In this more general situation, we need to be careful about the defn of a polynomial.

Consider a sequence $\vec{C} := (C_0, C_1, \dots)$ of points in Γ. This $\vec{C}$ is ***eventually-zero*** if there is a posint N so that $C_k = 0$ for each $k > N$. Formally, a ***Γ-polynomial*** is an eventually-zero sequence $(C_0, C_1, \dots)$ of coefficients from Γ. The polynomial determines an Γ-*function*

$$x \;\mapsto\; \textstyle\sum_{k=0}^{\infty} C_k x^k \overset{\text{note}}{=\!=} \sum_{k=0}^{N} C_k x^k \,.$$

Even for some *fields* $\mathbf{F}$, it is possible for two *different* $\mathbf{F}$-polys to determine the same function! For example, if $\mathbf{F}$ is the field $\{0, 1\}$ having just two elements, then distinct polys x and x^2 determine the same function. And $x + x^2$ is the constant-zero *fnc*, but it is not Zip, since its coeff-seq is $(0, 1, 1, 0, 0, \dots)$.

§A Appendices

We put some proofs here that don't fit into the main text.

Fundamental Theorem of Algebra

A field **F** is ***algebraically closed*** if every monic **F**-polynomial "factors completely"; that is, into a product of linear polynomials. Here we sketch a proof that $\mathbb{C}$ is algebraically closed.

27: Fund. Thm of Algebra. *Every monic $\mathbb{C}$-polynomial*

$$f(z) \;=\; z^N + B_{N-1}z^{N-1} + \cdots + B_1 z + B_0$$

factors as

$$f(z) \;=\; [z - \mathbf{z}_1] \cdot [z - \mathbf{z}_2] \cdot \ldots \cdot [z - \mathbf{z}_N]\,,$$

for a unique multiset $\{\mathbf{z}_1, \ldots, \mathbf{z}_N\}$ of complex numbers. Thanks to the division algorithm, this is equivalent to saying

27′: *Each non-constant [i.e, $N \geqslant 1$] complex polynomial $f()$ has a complex root.* ♢

Sketch of (27′). FTSOC, suppose that

$$\boldsymbol{\mu} \;:=\; \inf_{z\in\mathbb{C}} |f(z)|$$

is positive. As $|z| \to \infty$ note that $|f(z)| \to \infty$, since the high-order term z^N swamps (in absolute-value) the other terms. So there is a sufficiently large closed disk D on which $\inf_{z\in D} |f(z)|$ equals the above $\boldsymbol{\mu}$.

Since $z \mapsto |f(z)|$ is continuous, there exists[♡7] a point $z_0 \in D$ with $f(z_0) = \boldsymbol{\mu}$. Replace f by $z \mapsto f(z - z_0)$, then multiply by $1/\boldsymbol{\mu}$. We now have

†: $f(0) = 1$. *Furthermore, $|f(z)| \geqslant 1$, for all complex z.*

Writing $f(z) = 1 + \sum_{j=1}^N B_j z^j$, let K be the smallest positive exponent with $B_K \neq 0$; this exists, since f is non-constant. Let A be a K^{th}-root of B_K. Replace f by $f(\frac{z}{A})$; this redefines the $(B_j)_{j=1}^N$. We retain (†) and now have

$$f(z) \;=\; 1 + z^K + R(z)\,,$$

where $R(z) := \sum_{j=K+1}^N B_j z^j$, and K is a posint.

Making $|z|$ small. Let $C := \sum_{j=K+1}^N |B_j|$. With a small (positive) $\varepsilon<1$, take z with $|z| = \varepsilon$. So

$$\begin{aligned} |z^K| \;&=\; \varepsilon^K\,. \qquad \text{Yet} \\ \big|R(z)\big| \;&\leqslant\; \varepsilon^{K+1} \cdot C\,. \end{aligned}$$

Pick ε small so that $|R(z)| \leqslant \frac{1}{7}\cdot\varepsilon^K$. Let ζ be a K^{th}-root of –1 and set $z := \varepsilon\zeta$. Thus, here, $f(z)$ equals $1 - \varepsilon^K + R(z)$. Consequently,

$$\begin{aligned} |f(z)| \;&\leqslant\; |1 - \varepsilon^K| + |R(z)| \\ &\leqslant\; 1 - \tfrac{6}{7}\cdot\varepsilon^K\,. \end{aligned}$$

And this contradicts (†).

We conclude that $\inf_{z\in\mathbb{C}} |f(z)|$ is necessarily zero. ♦

[♡7] Since D is closed and bounded, D is compact. And on a non-void compact set, a cts fnc achieves a minimum.

Integrating polynomials

Here we exhibit two tricks, using counting[♡8] ideas.

Bernstein polynomials. Throw $K{+}L{+}1$ darts at the unit-interval $\mathbf{J} := [0,1]$. Condition on x, the landing-spot of the first dart. The probability that the next K darts fall left of x, and the rest right, is $x^K[1{-}x]^L$. So the conditional probability that some K-many of the next $K{+}L$ many darts is

$$\binom{K{+}L}{K,\,L}\cdot x^K\cdot[1{-}x]^L\,.$$

Letting $\mathbf{U}$ be the unconditioned probability gives

$$28{:}\qquad \mathbf{U} \;=\; \binom{K{+}L}{K,\,L}\int_{\mathbf{J}} x^K\cdot[1{-}x]^L\,\mathrm{d}x\,.$$

[♡8]For a natnum n, use "$n!$" to mean "***n factorial***"; the product of all positive-integers less-equal n. So $3! = 3\cdot 2\cdot 1 = 6$ and $5! = 120$. Also $0! = 1$ and $1! = 1$.

The ***binomial coefficient*** $\binom{7}{3}$, read "7 choose 3", means *the number of ways of choosing* 3 *objects from* 7 *distinguishable objects*. If we think of putting these objects in our left pocket, and putting the remaining 4 things in our right pocket, then we write the coefficient as $\binom{7}{3,4}$. [Read as "7 choose 3-comma-4."] Note that $\binom{7}{0} = \binom{7}{0,7} = 1$. Also note this identity:

$$[x+y]^S \;=\; \sum_{j+k=S}\binom{S}{j,k}\cdot x^j y^k\,,$$

where (j,k) ranges over all *ordered* pairs of natural numbers with sum S.

In general, for natnums $S = K_1+\ldots+K_N$, the ***multinomial coefficient*** $\binom{S}{K_1,K_2,\ldots,K_N}$ means the number of ways of partitioning S different things, by putting K_1 of them in pocket 1 and K_2 of them in pocket 2, and so on. Easily

$$\binom{S}{K_1,K_2,\ldots,K_N} \;=\; \frac{S!}{K_1!\cdot K_2!\cdots K_N!}\,.$$

And $[x_1+\cdots+x_N]^S$ indeed equals the sum of

$$\binom{S}{K_1,\ldots,K_N}\cdot {x_1}^{K_1}\cdot {x_2}^{K_2}\cdots {x_N}^{K_N}\,,$$

taken over all natnum-tuples $\vec{K}{=}(K_1,\ldots,K_N)$ that sum to S.

But by permutation symmetry,

$$29{:}\qquad \mathbf{U} \;=\; \tfrac{1}{K+L+1}\,.$$

After all, of the $K{+}L{+}1$ darts, *some* "special" dart ends up having K darts to its left. And the probability that the *first-thrown* dart ends up being special is RhS(29). In consequence

$$30{:}\qquad \begin{aligned}\int_{\mathbf{J}} x^K\cdot[1{-}x]^L\,\mathrm{d}x \;&=\; 1\Big/\Big[\tbinom{K{+}L}{K,\,L}\cdot[K{+}L{+}1]\Big]\\ &=\; K!L!\big/[K{+}L{+}1]!\,.\end{aligned}$$

We now take a different approach to the same problem.

Integration with convolutions. Recall that the one-sided ***convolution*** of two (locally-integrable) fncs $f,g{:}[0,\infty)\to\mathbb{C}$ is the function

$$31{:}\qquad [f\circledast g](t) \;:=\; \int_0^t f(t-x)\cdot g(x)\,\mathrm{d}x\,.$$

Easily, convolution is associative and commutative. Use $f^{\circledast 3}$ for the 3^{rd} convo-power $f\circledast f\circledast f$.

For $K = 0,1,\ldots,$ let $p_K(z) := z^K$; our ***power functions***. Use $\mathbf{1}$ for the constant-one fnc p_0. Induction on natnum K shows that

$$32{:}\qquad \begin{aligned}\mathbf{1}^{\circledast[K+1]} \;&=\; \tfrac{1}{K!}\cdot p_K\,.\quad\text{Hence}\\ p_K \;&=\; K!\cdot\mathbf{1}^{\circledast[K+1]}\,.\end{aligned}$$

For $K\,\&\,L$ natnums, $p_K\circledast p_L \;=\; K!L!\cdot\mathbf{1}^{\circledast[K+L+2]}$, by *associativity of convolution*. Thus

$$33{:}\qquad p_K\circledast p_L \;=\; \tfrac{K!\cdot L!}{[K+L+1]!}\cdot p_{K+L+1}\,.$$

The binomial coeff $\mathbf{M} := \binom{K+L}{K,\,L}$ allows

$$33'{:}\qquad [p_K\circledast p_L](z) \;=\; \frac{z^{K+L+1}}{\mathbf{M}\cdot[K+L+1]}\,.$$

Setting $z := 1$ in $(33')$, makes $(33')$ identical to (30) —as it must!

Several. Consider N and $K_0, K_1, \cdots, K_N$, all natnums. Let $S := \sum_0^N K_j$. From (32a) note that

$$\mathbf{1}^{\circledast[S+N+1]} \;=\; \tfrac{1}{[S+N]!} \cdot p_{S+N} \,.$$

With $\mathbf{M}$ now the multinomial coeff $\binom{S}{K_0,\cdots,K_N}$, the convo-product $p_{K_0} \circledast p_{K_1} \circledast \cdots \circledast p_{K_N}$ equals

$$K_0! \cdot \ldots \cdot K_N! \cdot \mathbf{1}^{\circledast[S+N+1]} \;=\; \tfrac{1}{\mathbf{M}} \cdot \tfrac{S!}{[S+N]!} \cdot p_{S+N} \,.$$

Assigning $\mathbf{B} := \binom{S+N}{S,\,N}$ permits the exposition

$$\text{34:} \qquad [p_{K_0} \circledast \cdots \circledast p_{K_N}](z) \;=\; \frac{z^{S+N}}{\mathbf{M} \cdot \mathbf{B} \cdot N!} \,.$$

Does this denominator have an interesting combinatorial interpretation?

Polynomials in several variables

The ***degree*** of a monomial such as x^4yz^2 is the sum of the exponents; here $\mathrm{Deg}(x^4yz^2) = 4+1+2 = 7$. *However*, to be precise one has to indicate which letters are viewed as the variables, and which are viewed as parameters. For instance (the first line needs $A \neq 0$)

$$\begin{aligned} x &\longmapsto Ax^2 + Bx + C \quad \text{has degree 2;} \\ \mathbf{(}A, x\mathbf{)} &\longmapsto Ax^2 + Bx + C \quad \text{has degree 3;} \\ \mathbf{(}A, B, C\mathbf{)} &\longmapsto Ax^2 + Bx + C \quad \text{has degree 1.} \end{aligned}$$

A ***multivariate polynomial*** is a finite sum of multivariate monomials, and its ***degree*** is the maximum of the degrees of its monomials. E.g

$$f(x,y,z) \;:=\; 2x^4yz^2 + 102y^5z^3 + \text{-}5x^6 + 2007$$

has degree 8. A poly h is said to be "***homogeneous*** of degree N", if *every* h-monomial has degree exactly N. F'irinstance,

$$h(x,y,z) \;:=\; 2x^5yz^3 + 120y^6z^3 - 75x^9$$

is homogeneous of degree 9, but poly $23 + h()$ is not homogeneous, since monomial 23 has degree 0, not 9. Note that Zip is vacuously homogeneous, since it has no monomials.

The product of homogeneous polys is homogeneous but –in general– the sum is not homogeneous.

Now lets view the N^2-positions in an $N \times N$ matrix M as *variables*. Then the matrix-determinant

35: $\mathrm{Det}(\mathsf{M})$ *is a degree-N homogeneous polynomial in N^2 variables. The poly has $N!$ many monomials, half of which (once $N \geqslant 2$) have coefficient +1, and half of which have –1 as coefficient.*

Roots of the Cubic and the Quartic

Here I derive a root-extraction formula for the roots of a cubic polynomial, similar to the QF for a quadratic. Formulas like (40), below, are sometimes called ***Cardano's formula***. [♡9]

First note, for a degree $N \geqslant 1$ (monic) polynomial

$$F(t) \;:=\; t^N + F_{N-1}t^{N-1} + F_{N-2}t^{N-2} + \dots$$

that the linear change-of-variable $\boxed{t =: x - \frac{F_{N-1}}{N}}$ gives a polynomial in x

$$x^N + 0\cdot x^{N-1} + Cx^{N-2} + Dx^{N-3} + \dots$$

with no penultimate term. Such a poly is a called a "***depressed*** degree-N polynomial".

Sum and product. For two mystery numbers U, V, suppose we know their sum and product,

$$\text{36:} \quad U+V \;=:\; S \qquad \text{and} \qquad U\cdot V \;=:\; P\,.$$

Then polynomial $[y-U][y-V] = y^2 - Sy + P$ has U, V as roots. Consequently,

$$\text{36}': \qquad U, V \;=\; \tfrac{1}{2}\Big[S \pm \sqrt{S^2 - 4P}\Big]$$

in some order.

Roots of the depressed cubic

We'll get a formula for the three roots of cubic

$$\text{37:} \quad f(x) \;:=\; x^3 - 3Cx - S\,, \qquad \text{with } C, S \in \mathbb{C},$$

where I have written the x-coefficient as "$-3C$" because I have looked ahead into the proof.

The trick is to write $\boxed{x = \alpha + \beta}$ subject to a constraint on the product $\alpha\cdot\beta$. Computing,

$$f(\alpha+\beta) \;=\; \alpha^3 + \beta^3 - S \;+\; [3\alpha\beta - 3C][\alpha+\beta]\,.$$

[♡9] The history is complicated; see Wikipedia.

The idea is to view α^3 and β^3, as the "mystery" numbers, (36), whose sum and product are known. To make the sum known, *require* that $3\alpha\beta - 3C$ equal 0, i.e

$$\text{38:} \qquad \alpha\cdot\beta \;=\; C\,.$$

This arranges that equality $f(\alpha+\beta)=0$ means

$$\text{39:} \qquad \alpha^3 + \beta^3 \;=\; S\,.$$

Cubing (38) gives

$$\text{39}': \qquad \alpha^3\cdot\beta^3 \;=\; C^3\,.$$

Thus (36) tell us that α^3 and β^3 each have form RhS(36′), with $P := C^3$. Since their sum must be S, by (39), without loss of generality

$$\begin{aligned} \alpha^3 &= \tfrac{1}{2}\Big[S - \sqrt{S^2 - 4C^3}\Big] \quad \text{and} \\ \beta^3 &= \tfrac{1}{2}\Big[S + \sqrt{S^2 - 4C^3}\Big]\,. \end{aligned}$$

Cardano's formula. Let $\boldsymbol{\omega}$ be a primitive cube-root of unity; say, $\boldsymbol{\omega} := \frac{1}{2}[-1 + \sqrt{3}\,\boldsymbol{i}]$.

Let σ be a particular square-root of $S^2 - 4C^3$. Let α_0 be a particular cube-root of $\frac{1}{2}[S-\sigma]$. Let β_0 be *the*[♡10] cube-root of $\frac{1}{2}[S+\sigma]$ satisfying

$$\alpha_0\cdot\beta_0 \;=\; C\,.$$

Then the three roots of (37) are

$$\text{40:} \qquad \begin{aligned} x &= \alpha_0 + \beta_0\,; \\ x &= \boldsymbol{\omega}\alpha_0 + \boldsymbol{\omega}^{-1}\beta_0\,; \\ x &= \boldsymbol{\omega}^{-1}\alpha_0 + \boldsymbol{\omega}\beta_0\,. \end{aligned}$$

[♡10] This β_0 is unique *unless* α_0 is zero. Making the convention that if $C=0$, then the σ we chose is S, we have

$$[\alpha_0 = 0] \iff [C = 0]\,.$$

So when $C = 0$, we can let β_0 be any of the cube-roots of $\frac{1}{2}[S+\sigma]$.

General cubic. To the undepressed-cubic

$$41: \qquad F(t) \;:=\; t^3 - 3Kt^2 - Lt - M\,,$$

the change-of-var $t =: x + K$ produces (37) with

$$C \;:=\; K^2 + \tfrac{L}{3} \quad \text{and} \quad S \;:=\; 2K^3 + M + LK\,.$$

Produce $\sigma, \alpha_0, \beta_0$ as above. Then the three roots of $F()$ are

$$40': \quad \tau_j \;:=\; K + [\boldsymbol{\omega}^j \alpha_0 + \boldsymbol{\omega}^{-j}\beta_0]\,, \qquad \text{for } j = 0, \pm 1.$$

Roots of the Quartic

Let's derive ***Ferrari's formula***, (45), for the roots of a quartic polynomial.

42: Lemma. *Consider complex numbers A, B, C. When do there exist $\Lambda, \Omega \in \mathbb{C}$ such that.*

$$42\dagger: \qquad Ax^2 + Bx + C \;=\; [\Lambda x + \Omega]^2\,,$$

where the equality is as polynomials in x? There exist such $\Lambda, \Omega \in \mathbb{C}$ IFF $B^2 - 4AC$ equals zero.♢

Proof. Condition (42†) says that $A{=}\Lambda^2$ and $C{=}\Omega^2$ and $B{=}2\Lambda\Omega$. Thus $B^2 - 4AC = 0$.

Conversely, now suppose $B^2 = 4AC$ and pick square-roots Λ and Ω such that

$$42\ddagger: \qquad \Lambda^2 \;=\; A \quad \text{and} \quad \Omega^2 \;=\; C\,.$$

Necessarily, $B^2 = [2\Lambda\Omega]^2$. Hence $B = \pm 2\Lambda\Omega$. If the minus-sign, then redefine Ω to be $-\Omega$. ♦

Our goal now is to get a formula for the four complex roots of the depressed quartic

$$43: \qquad q(x) \;:=\; x^4 - Ax^2 - Bx - C\,.$$

Letting $X := x^2$, we rewrite $q(x) \overset{\text{goal}}{=\!=} 0$ as

$$44: \qquad X^2 \;=\; [x^2]^2 \overset{\text{goal}}{=\!=} Ax^2 + Bx + C\,.$$

Each $t \in \mathbb{C}$ produces a perfect square

$$\dagger\text{L}: \quad [X + t]^2 \overset{\text{note}}{=\!=} \text{LhS}(44) + [2tX + t^2]\,.$$

And RhS(44) + $[2tX + t^2]$ equals

$$\dagger\text{R}: \qquad \underbrace{[A + 2t]}_{A_t} \cdot x^2 \;+\; Bx \;+\; \underbrace{[C + t^2]}_{C_t}\,.$$

Since (†L) is always a square, we'd like to choose t so that (†R) is a square.

By lemma 42, we want t st. $B^2 - 4A_tC_t$ equals zero. Multiplying $4A_tC_t - B^2$ by $\frac{1}{8}$ gives

$$F(t) \;:=\; t^3 \;+\; \tfrac{A}{2}t^2 \;+\; Ct \;+\; \tfrac{4AC - B^2}{8}\,.$$

This $F()$, upto a linear change-of-variable, is sometimes called the ***resolvent*** of the quartic polynomial $q()$ from (43).

Ferrari's formula. Use Cardano's formula, (40′), to pick a particular complex number τ st. $F(\tau) = 0$. Now (42‡) hands us numbers Λ and Ω with (†R) equaling $[\Lambda x + \Omega]^2$. But (†L) = (†R). Consequently,

$$44': \qquad [x^2 + \tau]^2 \;=\; [\Lambda x + \Omega]^2\,.$$

The set of x solving (44) is precisely the soln-set to (44′). And this is the union of solutions to

$$\begin{aligned} x^2 + \tau \;&=\; -\Lambda x - \Omega \qquad \text{and} \\ x^2 + \tau \;&=\; \Lambda x + \Omega\,. \end{aligned}$$

I.e, the roots of $x^2 \pm \Lambda x + [\tau \pm \Omega]$. This polynomial's discriminant is

$$\Lambda^2 - 4\tau \mp 4\Omega\,.$$

So we get the four solutions

$$45: \qquad \begin{aligned} x \;&=\; \tfrac{1}{2}\Big[-\Lambda \pm \sqrt{\Lambda^2 - 4\tau - 4\Omega}\Big] \quad \text{and} \\ x \;&=\; \tfrac{1}{2}\Big[+\Lambda \pm \sqrt{\Lambda^2 - 4\tau + 4\Omega}\Big]\,. \end{aligned}$$

§Index for "Primer on Polynomials"

Filename: `Problems/Polynomials/primer.poly.latex`
As of: *Thursday 23Feb2006.* Typeset: *13Apr2017* at *02:31.*