MTH1001-Algebra

Slides Week 5

Tips for checking polynomial calculations.
Irreducible polynomials.
Finding roots and factorisations of quadratic polynomials.
Unique factorisation of polynomials.
The maximum number of roots of a polynomial.
Polynomial interpolation.
Complex roots: the Fundamental Theorem of Algebra.
Roots and factorisations of polynomials with real coefficients.

Tips for checking polynomial calculations

- It is very easy to do mistakes in doing polynomial calculations.
- An obvious way of checking a polyn. division is multiplying the second polyn. by the quotient and then add the remainder.
- A partial check is substituting numbers for x (choosing them easy).
  - EXAMPLE. Suppose we have found, by long division,

$$x^4 - 3x^2 + x - 5 = (x^2 + x + 3) \cdot (x^2 - x - 5) + (9x + 10).$$

  - Now we do a few checks, substituting some numbers for x:

$$\begin{aligned} x = 0: &\quad -5 = 3 \cdot (-5) + 10 \\ x = 1: &\quad (1 - 3 + 1 - 5) = (1 + 1 + 3) \cdot (1 - 1 - 5) + (9 + 10) \\ x = -1: &\quad (1 - 3 - 1 - 5) = (1 - 1 + 3) \cdot (1 + 1 - 5) + (-9 + 10) \end{aligned}$$

  - A nonzero value for x is often enough to reveal a calc. error.
  - In case of longer calculations, such as the ext. Eucl. alg., first check the final result, and then, if wrong, check each intermediate step.

Irreducible polynomials

- DEFINITION. A non-constant polynomial $f(x) \in F[x]$
  - is *reducible* in $F[x]$ (or *over* F) if $f(x) = g(x)\,h(x)$, for some $g(x)$ and $h(x)$ non-constant polynomials in $F[x]$,
  - is *irreducible* (rather than *prime*) in $F[x]$ if it is not reducible.
- Equivalently, a non-constant $f(x) \in F[x]$ is irreducible in $F[x]$ if it has no *proper* divisors $g(x)$ (that is, with $0 < \deg(g) < \deg(f(x))$).
- The constant polynomials are neither reducible nor irreducible.
- Polynomials of degree 1 are, clearly, always irreducible.
- EXAMPLE. $x^2 + 1$ is irreducible as a polynomial in $\mathbb{R}[x]$, but not as a polynomial in $\mathbb{C}[x]$, because $x^2 + 1 = (x - i)(x + i)$.

Quadratic polynomials

- Finding the roots of $ax^2 + bx + c$ (with $a \neq 0$) is the same as finding the solutions of the equation $ax^2 + bx + c = 0$.
-
  - Equivalent to $4a^2x^2 + 4abx = -4ac$.
  - *completing the square* we get $4a^2x^2 + 4abx + b^2 = b^2 - 4ac$,
  - which is $(2ax + b)^2 = b^2 - 4ac$.
-
  - If the *discriminant* $\Delta = b^2 - 4ac$ is not a square in F (meaning it has no square root in F), then $ax^2 + bx + c$ has no root in F.
  - If Δ is a square in F, then $(2ax + b)^2 - (\sqrt{\Delta})^2 = 0$, hence $(2ax + b - \sqrt{\Delta}) \cdot (2ax + b + \sqrt{\Delta}) = 0$.
  - In this case $ax^2 + bx + c$ has roots given by the familiar formula $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, which coincide when $b^2 - 4ac = 0$.
- $ax^2 + bx + c$ is reducible precisely when $b^2 - 4ac$ is a square in F.

- EXAMPLE. A quadratic polynomial $ax^2 + bx + c \in \mathbb{R}[x]$ (hence assuming $a \neq 0$) is irreducible exactly when $b^2 - 4ac < 0$.
- EXAMPLE. The polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}$, but reducible over $\mathbb{R}$, because $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, and $\sqrt{2} \notin \mathbb{Q}$, which means that $\sqrt{2}$ is irrational (we'll see later why).
- EXAMPLE. Because any number in $\mathbb{C}$ has square roots in $\mathbb{C}$, every quadratic polynomial in $\mathbb{C}[x]$ is reducible (and so it factorises as a product of two polynomials of degree one).

Unique factorisation for polynomials

- THEOREM. *Every non-constant polynomial over a field F is a product of irreducible polynomials, in an* essentially *unique way.*
- *Essentially* means the factorisation is only unique up to permuting factors and multiplying them by non-zero constants.
- EXAMPLE. $2x^2 + 10x + 12 = 2(x+2)(x+3) = (2x+4)(x+3) = (x+2)(2x+6) = (3x+6)\left(\frac{2}{3}x + 2\right)$, and so on.
- EXAMPLE. In $\mathbb{Q}[x]$ (or $\mathbb{R}[x]$) we have

$$\begin{aligned} x^4 - 5x^2 + 4 = (x^2-1)(x^2-4) &= (x^2-3x+2)(x^2+3x+2) \\ &= (x^2-x-2)(x^2+x-2) \end{aligned}$$

  - This does not contradict the Unique Factorisation Theorem because those quadratic factors are not irreducible over $\mathbb{Q}$.
  - In fact, $x^4 - 5x^2 + 4 = (x-1)(x+1)(x-2)(x+2)$.

The maximum number of roots of a polynomial

- THEOREM. *A polynomial of degree $n \geq 0$ has at most n distinct roots in a field F.*
- PROOF (INFORMAL).
  - If $f(x)$ has a root α, then by the Factor Theorem $f(x) = (x - \alpha) \cdot g(x)$, with $g(x)$ of degree $n - 1$.
  - If $f(x)$ has another root $\beta \neq \alpha$, then $0 = f(\beta) = (\beta - \alpha) \cdot g(\beta)$, hence $g(\beta) = 0$, so β is a root of $g(x)$.
  - Then by the Factor Theorem $g(x) = (x - \beta) \cdot h(x)$, and so $f(x) = (x - \alpha) \cdot (x - \beta) \cdot h(x)$, with $h(x)$ of degree $n - 2$.
  - And so on, but in this way we cannot find more than n distinct roots. (The procedure may stop before finding n distinct roots if some root is repeated, or if we get some factor of f which has no roots in F.) $\square$

- COROLLARY. *A polynomial $f(x)$ of degree $< n$ is uniquely determined by the values it takes on n distinct elements of F.*
- PROOF. Suppose we know the values

  $$f(b_1) = c_1, \quad f(b_2) = c_2, \quad \dots \quad f(b_n) = c_n,$$

  for some distinct $b_1, \dots, b_n$.

  - Let $g(x)$ be any polynomial of degree $< n$ which also satisfies

    $$g(b_1) = c_1, \quad g(b_2) = c_2, \quad \dots \quad g(b_n) = c_n.$$

  - Then either $h(x) = f(x) - g(x)$ is zero, or $\deg(h(x)) < n$, and

    $$h(b_1) = 0, \quad h(b_2) = 0, \quad \dots \quad h(b_n) = 0.$$

  - So $h(x)$, which has degree $< n$, has at least n roots. This contradicts the Theorem, unless $h(x) = 0$, hence $g(x) = f(x)$. □
- EXAMPLE. If $\deg(f) < 2$ (hence of degree 1 or constant), then knowing $f(b_1)$ and $f(b_2)$ for some $b_1 \neq b_2$ is sufficient to determine f uniquely. (Note the graph is a straight line.) We actually need two values, just $f(b_1)$ would not be enough.

Polynomial interpolation

- The Corollary proves the *uniqueness* part of the following.
- INTERPOLATION THEOREM. *Given distinct* $b_1, \dots, b_n \in F$ *(a field as usual), and arbitrary* $c_1, \dots, c_n \in F$*, there* exists *a* unique *polynomial* $f(x) \in F$ *of degree* $< n$ *such that*
$$f(b_1) = c_1, \quad f(b_2) = c_2, \quad \dots \quad f(b_n) = c_n.$$
- A proof of *existence* is the Notes (optional) and includes a method to find $f(x)$. Or proceed directly as follows.
- EXAMPLE. Find the unique polynomial $f(x)$ of degree < 3 such that $\quad f(-2) = 7, \quad f(0) = 3, \quad f(1) = 1.$
  - Set $f(x) = ax^2 + bx + c$. Then $4a - 2b + c = 7, \quad c = 3,$ $a + b + c = 1$. Solving the system we find $a = 0$, $b = -2$, $c = 3$.
  - Hence $f(x) = -2x + 3$, actually of degree 1 (could have been 2).

The Fundamental Theorem of Algebra

- FUNDAMENTAL THEOREM OF ALGEBRA. (Argand, 1806)
  Every non-constant polynomial in $\mathbb{C}[x]$ has at least one root in $\mathbb{C}$.
- COROLLARY. The irreducible polynomials in $\mathbb{C}[x]$ are precisely those of degree one.
- COROLLARY. Every non-constant polynomial in $\mathbb{C}[x]$ is a product of polynomials of degree one.
- The fact that a root exists *does not mean* that there is a formula for finding it (or finding all roots, like for quadratics):
  - formulas for cubics and quartics known since 16th century;
  - no formula exists (using only the four operations, and radicals) for quintics and higher degree (proved by Abel and Ruffini, 1824).
- EXAMPLE. No complex root of $x^5 - x - 1$ can be be written using rational numbers and applying algebraic operations and radicals.

- EXAMPLE. Consider the polynomial $x^5 - x - 1 \in \mathbb{R}[x]$.
  - One can find a root numerically, roughly 1.167.
  - Applying Ruffini's Rule we find (approximately!)

	1	0	0	0	−1	−1
1.167		1.167	1.362	1.590	1.856	1
	1	1.167	1.362	1.590	0.856	0

$$x^5 - x - 1 \approx (x - 1.167)(x^4 + 1.167x^3 + 1.362x^2 + 1.590x + 0.856).$$

  - The factor of degree 4 has at least one root in $\mathbb{C}$. Continuing in this way one eventually finds the complete complex factorisation
$$x^5 - x - 1 \approx (x - 1.167)\,(x - 0.181 + 1.083\,i)(x - 0.181 - 1.083\,i) \cdot (x + 0.764 + 0.352\,i)(x + 0.764 - 0.352\,i).$$
  - The complete factorisation in $\mathbb{R}[x]$ is
$$x^5 - x - 1 \approx (x - 1.167)(x^2 - 0.362x + 1.207)(x^2 + 1.529x + 0.709).$$

Complex conjugation

- For a complex number in standard notation $\alpha = s + it$ (so $s, t \in \mathbb{R}$), its conjugate is $\overline{\alpha} = s - it$. Hence $\overline{\overline{\alpha}} = \alpha$.
- α is real exactly when $\overline{\alpha} = \alpha$. In fact, its real and imaginary parts are $s = \Re(\alpha) = (\alpha + \overline{\alpha})/2$ and $it = \Im(\alpha) = (\alpha - \overline{\alpha})/2$.
- Because $\alpha\overline{\alpha} = (s + it)(s - it) = s^2 + t^2 = |\alpha|^2$, we have

$$\frac{1}{\alpha} = \frac{1}{s + it} = \frac{s - it}{s^2 + t^2} = \frac{\overline{\alpha}}{|\alpha|^2}$$

- The main two properties of complex conjugation are

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}, \qquad \overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}.$$

- They say that conjugation $\alpha \mapsto \overline{\alpha}$ is a *field automorphism* of $\mathbb{C}$.
- Other properties follow: $\overline{\alpha - \beta} = \overline{\alpha} - \overline{\beta}$ and $\overline{\alpha/\beta} = \overline{\alpha}/\overline{\beta}$.
- Also, $\overline{\alpha^2} = \overline{\alpha}^{\,2}$ and, more generally, $\overline{\alpha^n} = \overline{\alpha}^{\,n}$.

Complex roots of a polynomial with real coefficients

- LEMMA. *If a complex number $\alpha = s + it$ is a root of a polynomial $f(x) \in \mathbb{R}[x]$, then its conjugate $\overline{\alpha} = s - it$ is a root as well.*
- PROOF. Write $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$, hence $a_j \in \mathbb{R}$.
  - For any complex number α (a root or not) we have

$$
\begin{aligned}
f(\overline{\alpha}) &= a_n \, \overline{\alpha}^{\,n} + \cdots + a_2 \, \overline{\alpha}^{\,2} + a_1 \, \overline{\alpha} + a_0 \\
&= a_n \, \overline{\alpha^n} + \cdots + a_2 \, \overline{\alpha^2} + a_1 \, \overline{\alpha} + a_0 \quad (\text{because } \overline{\alpha^n} = \overline{\alpha}^{\,n}) \\
&= \overline{a_n \, \alpha^n} + \cdots + \overline{a_2 \, \alpha^2} + \overline{a_1 \, \alpha} + \overline{a_0} \quad (\text{because } \overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}) \\
&= \overline{a_n \, \alpha^n + \cdots + a_2 \, \alpha^2 + a_1 \, \alpha + a_0} \quad (\text{because } \overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}) \\
&= \overline{f(\alpha)}.
\end{aligned}
$$

  - In particular, if $f(\alpha) = 0$, then $f(\overline{\alpha}) = \overline{f(\alpha)} = 0$. □

- Hence non-real complex roots of a polynomial with real coefficients come in conjugate pairs, α and $\bar{\alpha}$.

Combining pairs of conjugate roots

- For any complex number $\alpha = s + it$, the polynomial

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$$

  has real coefficients, because $\alpha + \overline{\alpha} = 2s$ and $\alpha\overline{\alpha} = s^2 + t^2$.
- If $\alpha \notin \mathbb{R}$ then $(x - \alpha)(x - \overline{\alpha})$ is irreducible in $\mathbb{R}[x]$. It has negative discriminant: $(\alpha + \overline{\alpha})^2 - 4\alpha\overline{\alpha} = (\alpha - \overline{\alpha})^2 = (2it)^2 = -4t^2 < 0$.
- THEOREM. *The irreducible polynomials in $\mathbb{R}[x]$ are those of degree one, and the polynomials $ax^2 + bx + c$ with $b^2 - 4ac < 0$.*
- COROLLARY. *Every non-constant polynomial in $\mathbb{R}[x]$ is a product of polynomials of degree one and two.*
- Hence $f(x) \in \mathbb{R}[x]$ of odd degree has always at least one real root. (This is actually easier to prove directly, as in Calculus.)

- EXAMPLE. Take $f(x) = 4x^4 + 20x^3 + 30x^2 - 40x + 26$.
  - Suppose we know a root $-3+2i$. Then $x+3-2i$ is a factor of $f(x)$.
  - Hence we divide $f(x)$ by $x+3-2i$ using Ruffini's rule:

	4	20	30	-40	26
$-3+2i$		$-12+8i$	$-40-8i$	$46+4i$	-26
	4	$8+8i$	$-10-8i$	$6+4i$	0

  - $f(x) = (x+3-2i) \cdot [4x^3 + (8+8i)x^2 + (-10-8i)x + (6+4i)]$.
  - Then the conjugate $-3-2i$ is a root of the cubic factor. Divide:

	4	$8+8i$	$-10-8i$	$6+4i$
$-3-2i$		$-12-8i$	$12+8i$	$-6-4i$
	4	-4	2	0

  - So $f(x) = (x+3-2i)(x+3+2i)(4x^2-4x+2)$, and now it is easy:
  - $f(x) = (x+3-2i)(x+3+2i)(2x-1-i)(2x-1+i)$ in $\mathbb{C}[x]$.
  - $f(x) = (x^2+6x+13)(4x^2-4x+2)$ in $\mathbb{R}[x]$.