MTH1001-Algebra

Slides Week 4

The Remainder Theorem and the Factor Theorem.
Ruffini's rule.
Application to factorising $x^n \pm a^n$.
Expanding a polynomial in terms of $x - a$.
GCD for polynomials.
The extended Euclidean algorithm for polynomials, and Bézout's Lemma.

Roots of a polynomial

- We say that $\alpha \in F$ is a *root* (or a *zero*) of $f(x) \in F[x]$ if $f(\alpha) = 0$.
- We say that $g(x) \in F[x]$ divides $f(x) \in F[x]$ if $f(x) = g(x) \cdot h(x)$ for some $h(x) \in F[x]$.
  Equivalently, when dividing $f(x)$ by $g(x)$ gives remainder zero.
- LEMMA (THE REMAINDER THEOREM AND THE FACTOR THEOREM)
  Let F be a field, $0 \neq f(x) \in F[x]$, $\alpha \in F$. Then
  - *$f(\alpha)$ equals the remainder of the division of $f(x)$ by $x - \alpha$;*
  - *α is a root of $f(x) \iff x - \alpha$ divides $f(x)$.*
- PROOF. Dividing $f(x)$ by $(x - \alpha)$, find $f(x) = (x - \alpha) \cdot q(x) + r(x)$, where $\deg(r(x)) < 1$, but then $r(x)$ is a constant, $r(x) = r \in F$.
  - Evaluating on α we find $f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r = r$.
  - The equality $f(x) = (x - \alpha) \cdot q(x) + r$ shows that $x - \alpha$ divides $f(x)$ precisely when $r = 0$; but we already know $r = f(\alpha)$. $\square$

Ruffini's rule

- Dividing a polynomial by a binomial of the form $x - a$, for some constant a, can be done with less writing:
- EXAMPLE. To divide $f(x) = x^4 + 3x^3 - 5x - 10$ by $x - 2$ we write

$$\begin{array}{c|cccc|c} & 1 & 3 & 0 & -5 & -10 \\ 2 & & 2 & 10 & 20 & 30 \\ \hline & 1 & 5 & 10 & 15 & 20 \end{array}$$

  and find $x^4 + 3x^3 - 5x - 10 = (x^3 + 5x^2 + 10x + 15)(x - 2) + 20$.
- According to the Factor Theorem, $f(2) = 20$, the remainder, so this is also a fast method to compute $f(a)$ for some number a.
- Same as writing $x^4 + 3x^3 - 5x - 10 = \big[\big((x+3)x+0\big)x-5\big]x-10$, which is faster to compute.

- EXAMPLE. Divide

$$f(x) = x^3 - 3x^2 + (5 - 2i)x - 4 + 2i,$$

a polynomial with complex coefficients, by $x - 2 - i$.

  - $$\begin{array}{r|rrr|r} & 1 & -3 & 5-2i & -4+2i \\ 2+i & & 2+i & -3+i & 5 \\ \hline & 1 & -1+i & 2-i & 1+2i \end{array}$$

  - So we find

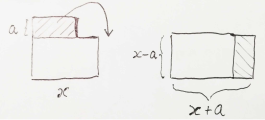
$$f(x) = (x^2 + (-1 + i)x + (2 - i)) \cdot (x - 2 - i) + (1 + 2i)$$

  - This is useful even if we just want to compute

$$f(2 + i) = 1 + 2i$$

An application of the Factor Theorem

- Take $f(x) = x^n \pm a^n$, where $a \neq 0$ is a constant.
  Because $f(a) = a^n \pm a^n$ and $f(-a) = (-1)^n a^n \pm a^n$, we have:
  - $x^n - a^n$ is always divisible by $x - a$;
  - $x^n - a^n$ is divisible by $x + a$ exactly when n is even;
  - $x^n + a^n$ is divisible by $x + a$ exactly when n is odd;
  - $x^n + a^n$ is never divisible by $x - a$.
- EXAMPLE. Good to remember the following:
  - $x^2 - a^2 = (x - a)(x + a)$
  - $x^3 - a^3 = (x - a)(x^2 + ax + a^2)$
  - $x^3 + a^3 = (x + a)(x^2 - ax + a^2)$
  - $x^4 - a^4 = (x-a)(x^3 + ax^2 + a^2x + a^3) = (x+a)(x^3 - ax^2 + a^2x - a^3)$
- Visually, $x^2 - a^2 = (x - a)(x + a)$ means



- EXAMPLE. Factorise the integers 9991 and 9919.
  - $9991 = 100^2 - 3^2 = (100-3)(100+3) = 97 \cdot 103$
  - 97 and 103 are both primes (check: not multiples of $2, 3, 5, 7$)
  - $9919 = 100^2 - 9^2 = (100-9)(100+9) = 91 \cdot 109 = 7 \cdot 13 \cdot 109$
  - 109 is prime but $91 = 10^2 - 3^2 = (10-3)(10+3) = 7 \cdot 13$
- EXAMPLE. Factorise $x^4 - a^4$.
  - We may start with $x^4 - a^4 = (x-a)(x^3 + ax^2 + a^2x + a^3)$, but it's easier to think of 4th powers as squares of squares:
  - $x^4 - a^4 = (x^2)^2 - (a^2)^2 = (x^2 - a^2)(x^2 + a^2) = (x-a)(x+a)(x^2 + a^2).$
  - If $a \in \mathbb{R}$ (and $a \neq 0$) we cannot factorise $x^2 + a^2$ any further in $\mathbb{R}[x]$.
  - In $\mathbb{C}[x]$ we have $x^4 - a^4 = (x-a)(x+a)(x-ai)(x+ai)$.
- EXAMPLE. Factorise $y^5 - z^5$.
  - $y^5 - z^5 = (y-z)(y^4 + y^3z + y^2z^2 + yz^3 + z^4)$
  - We cannot go any further.

- EXAMPLE. Factorise $x^6 - a^6$. Think squares of cubes:
  - $x^6 - a^6 = (x^3)^2 - (a^3)^2 = (x^3 - a^3)(x^3 + a^3) =$
    $= (x-a)(x^2 + ax + a^2)(x+a)(x^2 - ax + a^2).$
  - The two quadratic factors cannot be further factorised in $\mathbb{R}[x]$, having negative discriminant $a^2 - 4a^2 = -3a^2$.
- EXAMPLE. Factorise $x^6 - a^6$. Now think cubes of squares:
  - $x^6 - a^6 = (x^2)^3 - (a^2)^3 = (x^2 - a^2)(x^4 + a^2x^2 + a^4) =$
    $= (x-a)(x+a)(x^4 + a^2x^2 + a^4).$
  - To factorise $x^4 + a^2x^2 + a^4$ transform it with a trick:
    $x^4 + a^2x^2 + a^4 = (x^4 + 2a^2x^2 + a^4) - a^2x^2 =$
    $= (x^2 + a^2)^2 - (ax)^2 = (x^2 - ax + a^2)(x^2 + ax + a^2).$
- EXAMPLE. Factorise $x^6 + a^6$. Think cubes of squares:
  - $x^6 + a^6 = (x^2 + a^2)(x^4 - a^2x^2 + a^4).$
  - $x^4 - a^2x^2 + a^4$ cannot be factorised in $\mathbb{Q}[x]$, but it can in $\mathbb{R}[x]$:
    $x^4 - a^2x^2 + a^4 = (x^4 + 2a^2x^2 + a^4) - 3a^2x^2 =$
    $= (x^2 + a^2)^2 - (\sqrt{3}ax)^2 = (x^2 - a\sqrt{3}x + a^2)(x^2 + a\sqrt{3}x + a^2).$

- EXAMPLE. We have seen that $f(x) = x^n - a^n$ is divisible by $x - a$.
  - In fact, dividing by means of Ruffini's rule we find remainder zero:

$$\begin{array}{c|ccccc|c} & 1 & 0 & 0 & \cdots & 0 & -a^n \\ a & & a & a^2 & \cdots & a^{n-1} & a^n \\ \hline & 1 & a & a^2 & \cdots & a^{n-1} & 0 \end{array}$$

  - and so

$$x^n - a^n = (x-a)(x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1}).$$

  - Of course this can also be verified directly once we know the quotient, but Ruffini's rule quickly produces that quotient.
  - When n is odd (and only then) we get a similar identity

$$x^n + a^n = (x+a)(x^{n-1} - ax^{n-2} + \cdots - a^{n-2}x + a^{n-1})$$

    by applying Ruffini's rule to divide $f(x) = x^n + a^n$ by $x + a$, but it is quicker to deduce it by replacing a with $-a$ in the previous identity.

Expanding a polynomial in terms of $x - a$

- One can use Ruffini's rule repeatedly to expand a polynomial in x into powers of $x - a$, that is, if we like, into *a polynomial in $x - a$*.
- EXAMPLE. To expand $f(x) = x^3 + 2x^2 - x - 3$ into powers of $x - 2$:

$$
\begin{array}{c|rrrrl}
 & 1 & 2 & -1 & -3 & \\
2 & & 2 & 8 & 14 & \\
\hline
 & 1 & 4 & 7 & \mathbf{11} & \Rightarrow \text{new constant term is } 11 \\
2 & & 2 & 12 & & \\
\cline{1-4}
 & 1 & 6 & \mathbf{19} & & \Rightarrow \text{coeff. of } (x-2) \text{ is } 19 \\
2 & & 2 & & & \\
\cline{1-3}
 & 1 & \mathbf{8} & & & \Rightarrow \text{coeff. of } (x-2)^2 \text{ is } 8 \\
2 & & & & & \\
\cline{1-2}
 & \mathbf{1} & & & & \Rightarrow \text{coeff. of } (x-2)^3 \text{ is } 1
\end{array}
$$

and get $x^3 + 2x^2 - x - 3 = 1(x-2)^3 + 8(x-2)^2 + 19(x-2) + 11$.

Greatest common divisor for polynomials

- DEFINITION. Let $f(x), g(x) \in F[x]$. A polynomial $d(x) \in F[x]$ is called *a greatest common divisor* of $f(x)$ and $g(x)$ if
  1. $d(x)$ divides $f(x)$ and $g(x)$, and
  2. if $c(x) \in F[x]$, $c(x) \mid f(x)$, and $c(x) \mid g(x)$, then $c(x) \mid d(x)$.
- A GCD of $f(x)$ and $g(x)$ is denoted by $\big(f(x), g(x)\big)$, and is only unique up to multiplying it by nonzero constants.
- Hence if we find that the GCD of two polynomials is $2x + 3$ then we may as well say that it is $x + \frac{3}{2}$ (choosing the monic GCD).
- If $\big(f(x), g(x)\big) = 1$ then we say that $f(x)$ and $g(x)$ are *coprime*.

The extended Euclidean algorithm for polynomials

- EXAMPLE. We compute the GCD of $x^3 + 2x^2 + x$ and $x^2 + x - 1$:

$$x^3 + 2x^2 + x = (x^2 + x - 1) \cdot (x + 1) + (x + 1)$$
$$x^2 + x - 1 = (x + 1) \cdot x - 1$$

- Since the remainder of the second division is -1, that is the last nonzero remainder, and so $(x^3 + 2x^2 + x, x^2 + x - 1) = 1$.
- Reading the divisions backwards we find:

$$\begin{aligned} 1 &= -(x^2 + x - 1) + (x + 1) \cdot x \\ &= -(x^2 + x - 1) + [(x^3 + 2x^2 + x) - (x^2 + x - 1) \cdot (x + 1)] \cdot x \\ &= (x^3 + 2x^2 + x) \cdot x + (x^2 + x - 1) \cdot [-1 - (x + 1)x] \\ &= (x^3 + 2x^2 + x) \cdot x + (x^2 + x - 1) \cdot (-x^2 - x - 1) \end{aligned}$$

- We have found $u(x) = x$ and $v(x) = -x^2 - x - 1$ such that

$$(x^3 + 2x^2 + x) \cdot u(x) + (x^2 + x - 1) \cdot v(x) = 1.$$

Bézout's Lemma for polynomials

- BÉZOUT'S LEMMA. Let $f(x), g(x) \in F[x]$, where F is a field, and let $d(x) = \big(f(x), g(x)\big)$ be their greatest common divisor. Then there exist polynomials $u(x), v(x) \in F[x]$ such that

$$f(x)\,u(x) + g(x)\,v(x) = d(x).$$

- Fact: If neither $f(x)$ or $g(x)$ is the zero polynomial then the $u(x)$ and $v(x)$ produced by the extended Euclidean algorithm satisfy

$$\deg\big(u(x)\big) < \deg\big(g(x)\big) \qquad \text{and} \qquad \deg\big(v(x)\big) < \deg\big(f(x)\big).$$

- Analogues of Arithmetical Lemmas A–D hold for polynomials, and follow from Bézout's Lemma. In particular, Arithmetical Lemma B: *if the polynomials $f(x)$ and $g(x)$ are coprime, and $f(x)$ divides the product $g(x) \cdot h(x)$, then $f(x)$ divides $h(x)$.*

- EXAMPLE. We compute the monic GCD $d(x)$ of $x^3 - x^2 + x - 6$ and $x^3 + x - 10$:

$$x^3 - x^2 + x - 6 = (x^3 + x - 10) \cdot 1 + (-x^2 + 4)$$
$$x^3 + x - 10 = (x^2 - 4) \cdot x + (5x - 10)$$
$$x^2 - 4 = (x - 2)(x + 2)$$

- The last nonzero remainder is $5x - 10 = 5(x - 2)$, and so $d(x) = (x^3 - x^2 + x - 6, x^3 + x - 10) = x - 2$.
- Reading the divisions backwards we find:

$$\begin{aligned} 5x - 10 &= (x^3 + x - 10) - (x^2 - 4) \cdot x \\ &= (x^3 + x - 10) + [(x^3 - x^2 + x - 6) - (x^3 + x - 10) \cdot 1] \cdot x \\ &= (x^3 - x^2 + x - 6) \cdot x - (x^3 + x - 10) \cdot (x - 1) \end{aligned}$$

- We have found $u(x) = \frac{1}{5}x$ and $v(x) = -\frac{1}{5}(x - 1)$ such that

$$(x^3 - x^2 + x - 6) \cdot u(x) + (x^3 + x - 10) \cdot v(x) = d(x) = x - 2.$$

- Once we have found that $(x^3 - x^2 + x - 6, x^3 + x - 10) = x - 2$, instead of just doing the extended part of the Euclidean algorithm we may first divide both polynomials by their GCD, $x - 2$:

$$x^3 - x^2 + x - 6 = (x-2)(x^2 + x + 3)$$
$$x^3 + x - 10 = (x-2)(x^2 + 2x + 5)$$

- Then the Euclidean algorithm with the quotients is easier:

$$x^2 + x + 3 = (x^2 + 2x + 5) \cdot 1 + (-x - 2)$$
$$x^2 + 2x + 5 = (x+2) \cdot x + 5$$

- Reading the divisions backwards we find:

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

- So we find the same $u(x) = \frac{1}{5}x$ and $v(x) = -\frac{1}{5}(x-1)$.