

# Precalculus

## , Factorization of polynomials: overview

Todor Milev

2019

# Outline

## 1 Factorization overview

Recall that  $i^2 = -1$ ,  $\sqrt{-1} = i$ .

## Example (Polynomial factorizations)

$$2x^2 + 3x - 5 = (2x + 5)(x - 1) = 2 \left(x - \left(-\frac{5}{2}\right)\right)(x - 1)$$

$$x^2 + 1 = x^2 - (-1) = x^2 - i^2 = (x + i)(x - i)$$

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

$$\begin{aligned} x^4 + 1 &= \left(x^2 - \sqrt{2}x + 1\right) \left(x^2 + \sqrt{2}x + 1\right) \\ &= \left(x - \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right) \left(x - \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right) \\ &\quad \left(x - \left(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right) \left(x - \left(-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right) \end{aligned}$$

## Theorem (The Fundamental Theorem of Algebra)

*Every polynomial can be factored into product of linear terms*

$$p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = a_0(x - x_1) \cdots (x - x_n),$$

*where  $x_1, \dots, x_n$  are the (not necessarily different) roots of  $p(x)$ .*

- Every pol. of deg.  $n$  can be factored as product of  $n$  linear factors.
- $x_1, \dots, x_n$  may be complex numbers. Reminder: complex numbers are of the form  $p + qi$ , where  $i^2 = -1$  and  $\sqrt{-1} = i$ .
- While we can find  $x_1, \dots, x_n$  with arbitrary precision, there may not exist a formula involving radicals for computing each  $x_1, \dots, x_n$ .

## Corollary

*Every real polynomial can be factored into a product of real linear terms and real quadratic terms with no real roots, i.e., factors of form*

- $(x - r)$ , where  $r$  is real and
- $ax^2 + bx + c$  with  $b^2 - 4ac < 0$  where  $a, b, c$  are real.

$$a_0x^n + a_1x^{n-1} + \dots + a_n = a_0(x - x_1) \dots (x - x_n)$$

=prod. real quadratics no roots & lin. terms.

## Example

$$2x^2 + 3x - 5 = (2x + 5)(x - 1) = 2\left(x - \left(-\frac{5}{2}\right)\right)(x - 1)$$

real roots

$$x^2 + 1 = x^2 - (-1) = x^2 - i^2 = (x - (-i))(x - i)$$

complex roots

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$$

$$= (x - 1)(x - (-1))(x - i)(x - (-i))$$

mixed roots

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

$$= \left(x - \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right) \left(x - \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right)$$

$$\left(x - \left(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right) \left(x - \left(-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right)$$

complex roots

# Factoring polynomials in practice

- In theory every polynomial can be factored.

$$a_0x^n + a_1x^{n-1} + \dots + a_n = a_0(x - x_1) \dots (x - x_n)$$

- Theory guarantees numerical approximations for roots  $x_1, \dots, x_n$ .
- Can we find algebraic formulas for  $x_1, \dots, x_n$ ?
- No, if using finitely many operations  $+$ ,  $-$ ,  $*$ ,  $/$ ,  $\sqrt[n]{\phantom{x}}$ .
- First (advanced) proof by Norwegian Niels Henrik Abel(1824) based on work of Italian Paolo Ruffini(1799).
- Yes, with extra operations. Difficult: google Galois Theory to get started.

# What does factorization mean?

- Based on context, “to factor a polynomial” means one of:
  - Factor the polynomial over the rational numbers. Use integers/quotients, but no  $\sqrt{\phantom{x}}$ .
  - Factor the polynomial over the real numbers. Use radicals and/or numerical approximations, no use of  $i = \sqrt{-1}$ .
  - Fully factor the polynomial using complex numbers.

These poly's are equal	Type of factorization
$x^4 + 1$	factored over rationals
$(x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$	factored over the reals
$\left( x - \left( \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \right) \right) \left( x - \left( -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \right) \right)$ $\left( x - \left( \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \right) \right) \left( x - \left( -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \right) \right)$	full complex factorization

# Factorization over the rationals

- Suppose we want to factor a polynomial using only rational numbers (no  $\sqrt[n]{\phantom{x}}$  or numerical approximations).
- No guarantee to get:

$$a_0x^n + a_1x^{n-1} + \dots + a_n = a_0(x - x_1) \dots (x - x_n)$$

- A factorization using rationals may have arbitrarily large factors.
- Efficient algorithms for factoring using rationals exist.
  - Kronecker algorithm (German Leopold Kronecker (1823-1891)).
  - Methods based on finite fields.
    - Cantor-Zassenhaus factorization algorithm.
  - Lenstra-Lenstra-Lovász algorithm.
- Above methods require computer; no rational roots assumption.
- If we assume rational roots there are practical algorithms by hand.