Complex and Algebraic Numbers

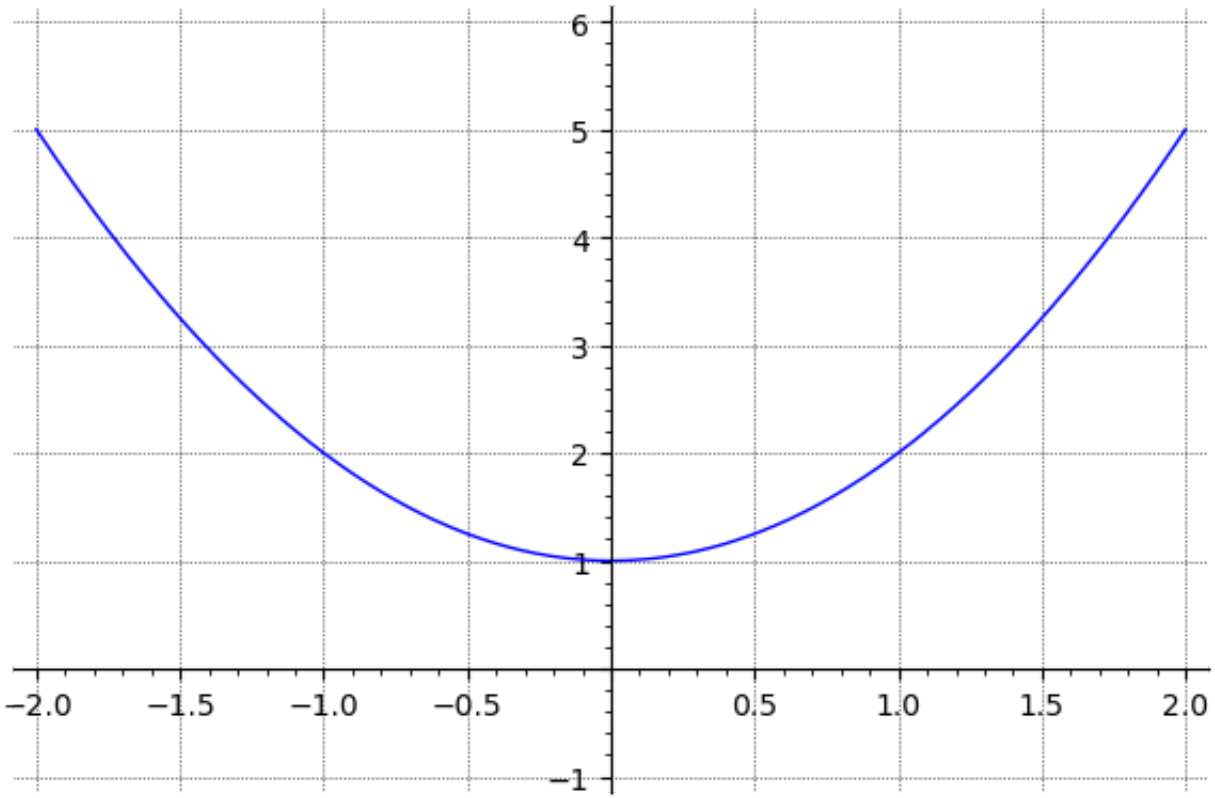
MCS 320 Lecture 5
Introduction to Symbolic Computation
Jan Verschelde, 14 June 2024

Complex and Algebraic Numbers

1. Complex and Algebraic Numbers
   - polynomials without real roots
   - quotients and remainders
2. Algebraic Numbers
   - polynomials without rational roots
   - extending the rational numbers with a root
   - finite field extensions

Polynomials without Real Roots

- $\mathbb{R}$ is the set of all real numbers.
- $x^2 + 1 \neq 0$ for all $x \in \mathbb{R}$, as we can see:



Complex and Algebraic Numbers

1. Complex and Algebraic Numbers
   - polynomials without real roots
   - quotients and remainders
2. Algebraic Numbers
   - polynomials without rational roots
   - extending the rational numbers with a root
   - finite field extensions

Complex Numbers

- $\mathbb{R}$ is the set of all real numbers.
- $x^2 + 1 \neq 0$ for all $x \in \mathbb{R}$.
- $\mathbb{R}[x]$ is the set of all polynomials in x, with coefficients in $\mathbb{R}$.

Consider the division of any $p \in \mathbb{R}[x]$ by $x^2 + 1$:

$$p(x) = q(x)(x^2 + 1) + r(x), \quad \deg(r) < 2, \quad r(x) = r_0 + r_1 x,$$

with quotient q and remainder r.

- $\mathbb{R}[x]/(x^2 + 1)$ is the set of all remainders after division by $x^2 + 1$.
- $\mathbb{C} = \{ a + bI \mid a, b \in \mathbb{R} \}$, $I = \sqrt{-1}$, I is *the imaginary unit*.

$\mathbb{R}[x]/(x^2 + 1)$ is isomorphic with $\mathbb{C}$, the set of all complex numbers:

$$\mathbb{C} \simeq \mathbb{R}[x]/(x^2 + 1).$$

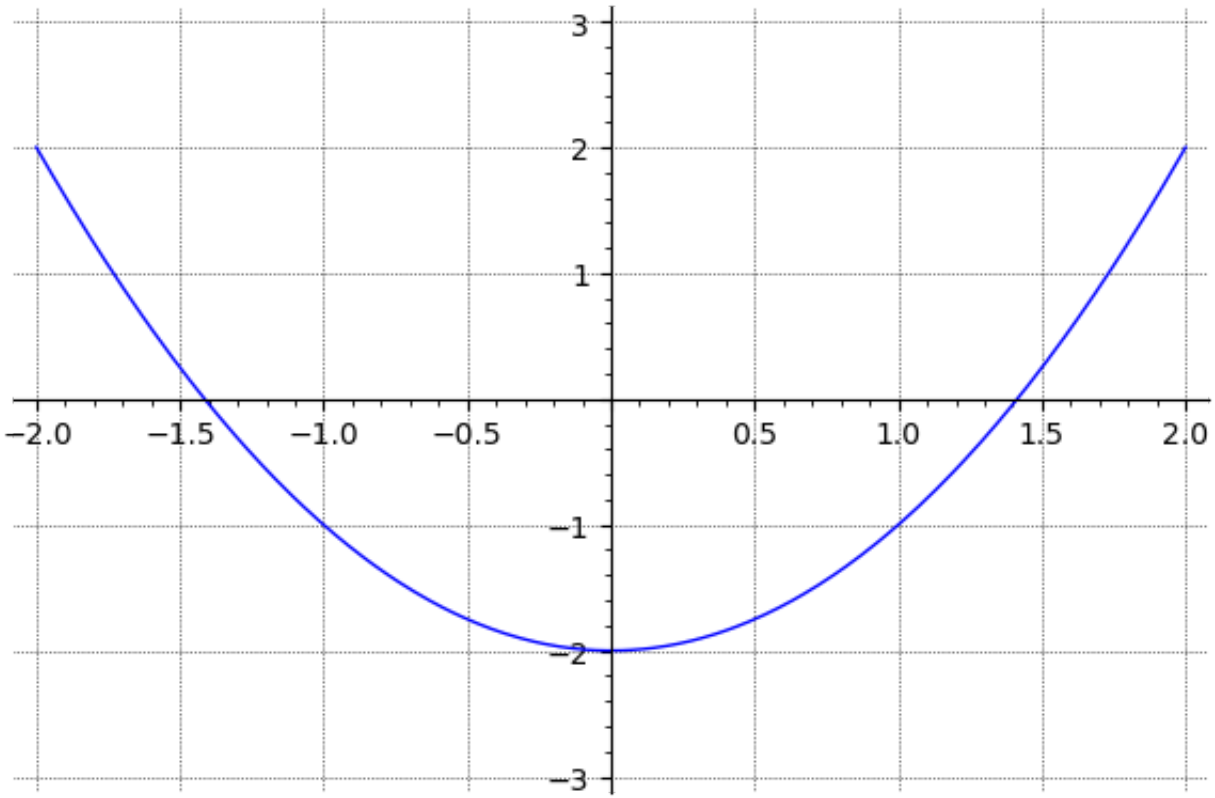
Complex and Algebraic Numbers

1. Complex and Algebraic Numbers
   - polynomials without real roots
   - quotients and remainders

2. Algebraic Numbers
   - polynomials without rational roots
   - extending the rational numbers with a root
   - finite field extensions

Polynomials without Rational Roots

- $\mathbb{Q}$ is the set of all rational numbers.
- $x^2 - 2 \neq 0$ for all $x \in \mathbb{Q}$, as $\sqrt{2} \neq \mathbb{Q}$, $\sqrt{2}$ is *irrational*.



Complex and Algebraic Numbers

1. Complex and Algebraic Numbers
   - polynomials without real roots
   - quotients and remainders

2. Algebraic Numbers
   - polynomials without rational roots
   - extending the rational numbers with a root
   - finite field extensions

extending the rational numbers with a root

- $\mathbb{Q}$ is the set of all rational numbers.
- $x^2 - 2 \neq 0$ for all $x \in \mathbb{Q}$.
- $\mathbb{Q}[x]$ is the set of all polynomials in x, with coefficients in $\mathbb{Q}$.

Consider the division of any $p \in \mathbb{Q}[x]$ by $x^2 - 2$:

$$p(x) = q(x)(x^2 - 2) + r(x), \quad \deg(r) < 2, \quad r(x) = r_0 + r_1 x,$$

with quotient q and remainder r.

- $\mathbb{Q}[x]/(x^2 - 2)$ is the set of all remainders after division by $x^2 - 2$.
- $\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$ is the extension of $\mathbb{Q}$ with $\sqrt{2}$.

$\mathbb{Q}[x]/(x^2 - 2)$ is isomorphic with $\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/(x^2 - 2)$

$a + b\sqrt{2}$ is an *algebraic number*

.

Complex and Algebraic Numbers

1. Complex and Algebraic Numbers
   - polynomials without real roots
   - quotients and remainders

2. Algebraic Numbers
   - polynomials without rational roots
   - extending the rational numbers with a root
   - finite field extensions

finite field extensions

Over $\mathbb{Z}_2 = \{0, 1\}$, working modulo 2:

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

so $x^2 + 1$ factors and is reducible.

The polynomial $x^3 + x + 1 \in \mathbb{Z}_2[x]$ does not factor, it is irreducible.

The extension $\mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field of 8 numbers.

Denote α as a root of $x^3 + x + 1$, then $\alpha^3 = \alpha + 1$.

We can list all 8 elements:

$$\begin{aligned} \mathbb{Z}_2[x]/(x^3 + x + 1) &= \{ a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_2 \} \\ &= \{0, 1, \alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\} \end{aligned}$$

and we also compute the multiplication table.