# Lecture 6.3: Polynomials and irreducibility

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

# Polynomials

## Definition

Let $x$ be an unknown variable. A polynomial is a function

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \, .$$

The highest non-zero power of $n$ is called the degree of $f$.

We can assume that all of our coefficients $a_i$ lie in a field $F$.

For example, if each $a_i \in \mathbb{Z}$ (not a field), we could alternatively say that $a_i \in \mathbb{Q}$.

Let $F[x]$ denote the set of polynomials with coefficients in $F$. We call this the set of polynomials over $F$.

## Remark

Even though $\mathbb{Z}$ is not a field, we can still write $\mathbb{Z}[x]$ to be the set of polynomials with integer coefficients. Most polynomials we encounter have integer coeffients anyways.

# Radicals

The roots of low-degree polynomials can be expressed using arithmetic and radicals.

For example, the roots of the polynomial $f(x) = 5x^4 - 18x^2 - 27$ are

$$x_{1,2} = \pm\sqrt{\frac{6\sqrt{6}+9}{5}}, \qquad x_{3,4} = \pm\sqrt{\frac{9-6\sqrt{6}}{5}}.$$

**Remark**

The operations of arithmetic, and radicals, are really the "only way" we have to write down generic complex numbers.

Thus, if there is some number that cannot be expressed using radicals, we have no way to express it, unless we invent a special symbol for it (e.g., $\pi$ or $e$).

Even weirder, since a computer program is just a string of 0s and 1s, there are only countably infinite many possible programs.

Since $\mathbb{R}$ is an uncountable set, there are numbers (in fact, "almost all" numbers) that can *never* be expressed algorithmically by a computer program! Such numbers are called "uncomputable."

# Algebraic numbers

## Definition

A complex number is algebraic (over $\mathbb{Q}$) if it is the root of some polynomial in $\mathbb{Z}[x]$. The set $\mathbb{A}$ of all algebraic numbers forms a field (this is not immediately obvious).

A number that is not algebraic over $\mathbb{Q}$ (e.g., $\pi$, $e$, $\phi$) is called transcendental.

Every number that can be expressed from the natural numbers using arithmetic and radicals is algebraic. For example, consider

$$\begin{aligned} x = \sqrt[5]{1+\sqrt{-3}} \quad &\iff \quad x^5 = 1+\sqrt{-3} \\ &\iff \quad x^5 - 1 = \sqrt{-3} \\ &\iff \quad (x^5-1)^2 = -3 \\ &\iff \quad x^{10} - 2x^5 + 4 = 0\,. \end{aligned}$$

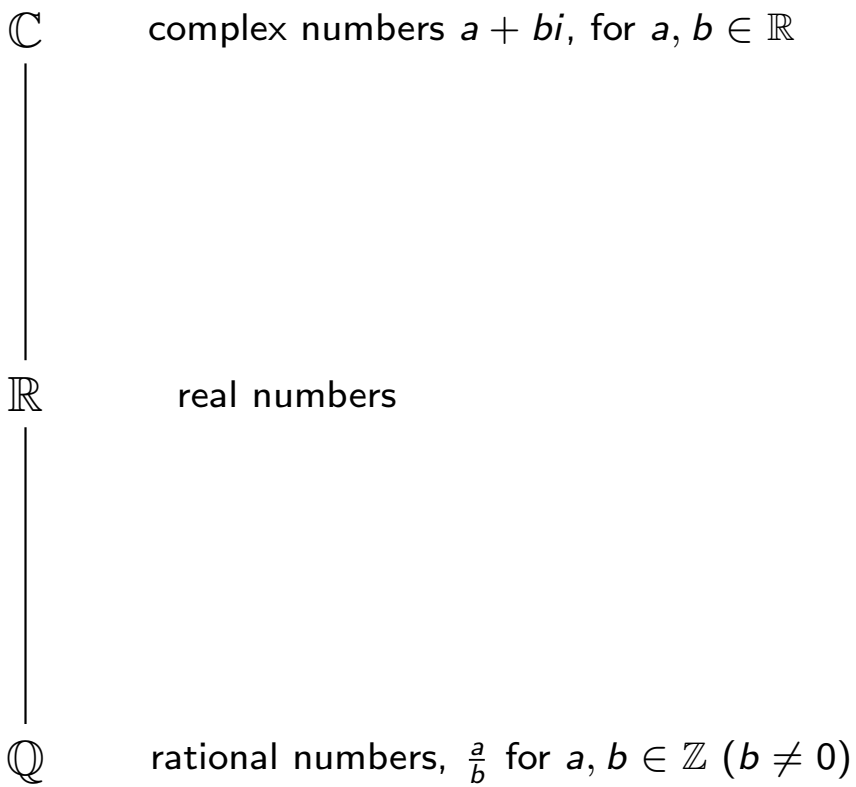
## Question

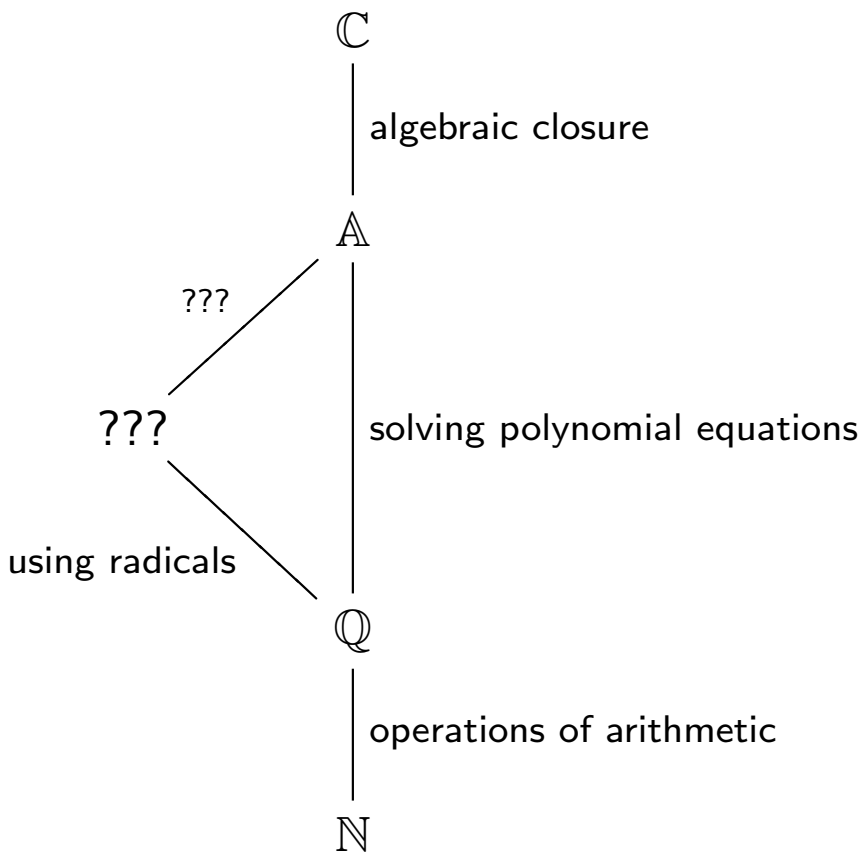
Can *all* algebraic numbers be expressed using radicals?

This question was unsolved until the early 1800s.

# Hasse diagrams

The relationship between the natural numbers $\mathbb{N}$, and the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{A}$, and $\mathbb{C}$, is shown in the following Hasse diagrams.



# Some basic facts about the complex numbers

## Definition

A field $F$ is algebraically closed if for any polynomial $f(x) \in F[x]$, all of the roots of $f(x)$ lie in $F$.

## Non-examples

- $\mathbb{Q}$ is not algebraically closed because $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ has a root $\sqrt{2} \notin \mathbb{Q}$.
- $\mathbb{R}$ is not algebraically closed because $f(x) = x^2 + 1 \in \mathbb{R}[x]$ has a root $\sqrt{-1} \notin \mathbb{R}$.

## Fundamental theorem of algebra

The field $\mathbb{C}$ is algebraically closed.

Thus, every polynomial $f(x) \in \mathbb{Z}[x]$ completely factors, or splits over $\mathbb{C}$:

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n), \qquad r_i \in \mathbb{C}.$$

Conversely, if $F$ is *not* algebraically closed, then there are polynomials $f(x) \in F[x]$ that do *not* split into linear factors over $F$.

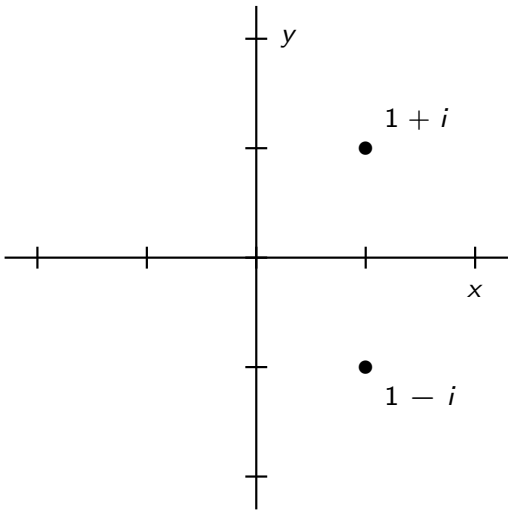
# Complex conjugates

Recall that complex roots of $f(x) \in \mathbb{C}[x]$ come in conjugate pairs: If $r = a + bi$ is a root, then so is $\overline{r} := a - bi$.

For example, here are the roots of some polynomials (degrees 2 through 5) plotted in the complex plane. All of them exhibit symmetry across the $x$-axis.

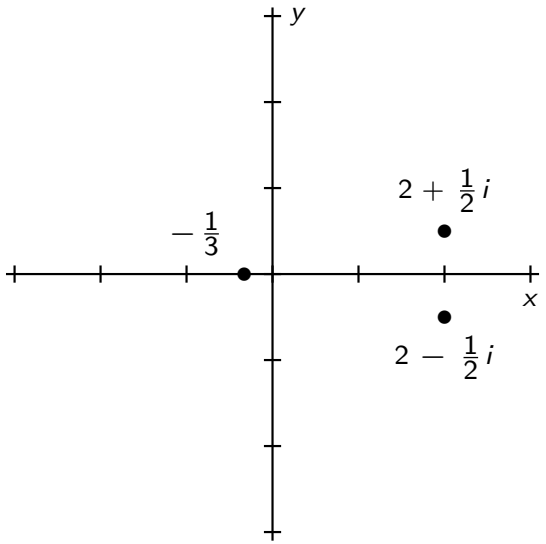
$f(x) = x^2 - 2x + 2$

Roots: $1 \pm i$



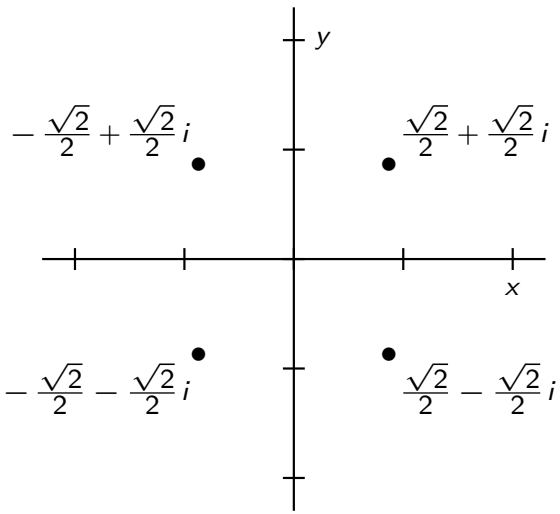

$f(x) = 12x^3 - 44x^2 + 35x + 17$

Roots: $-\frac{1}{3}$, $2 \pm \frac{1}{2}i$



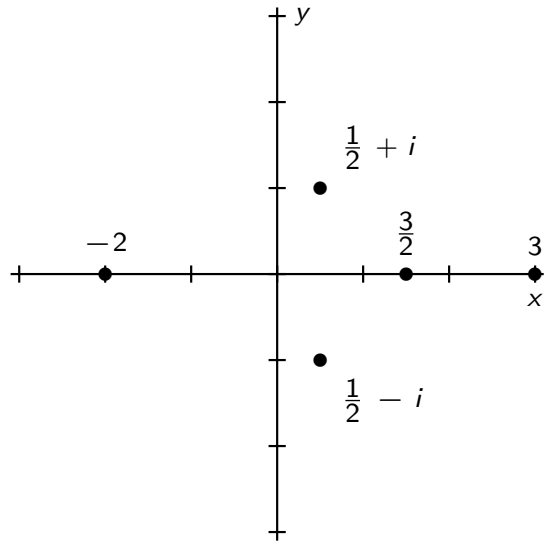

$f(x) = x^4 + 1$

Roots: $\pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}$




$f(x) = 8x^5 - 28x^4 - 6x^3 + 83x^2 - 117x + 90$

Roots: $-2$, $\frac{3}{2}$, $3$, $\frac{1}{2}i \pm i$



# Irreducibility

## Definition

A polynomial $f(x) \in F[x]$ is reducible over $F$ if we can factor it as $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ of strictly lower degree. If $f(x)$ is not reducible, we say it is irreducible over $F$.

## Examples

- $x^2 - x - 6 = (x + 2)(x - 3)$ is reducible over $\mathbb{Q}$.
- $x^4 + 5x^2 + 4 = (x^2 + 1)(x^2 + 4)$ is reducible over $\mathbb{Q}$, but it has no roots in $\mathbb{Q}$.
- $x^3 - 2$ is irreducible over $\mathbb{Q}$. If we could factor it, then one of the factors would have degree 1. But $x^3 - 2$ has no roots in $\mathbb{Q}$.

## Facts

- If $\deg(f) > 1$ and has a root in $F$, then it is reducible over $F$.
- Every polynomial in $\mathbb{Z}[x]$ is reducible over $\mathbb{C}$.
- If $f(x) \in F[x]$ is a degree-2 or 3 polynomial, then $f(x)$ is reducible over $F$ if and only if $f(x)$ has a root in $F$.

# Eisenstein's criterion for irreducibility

## Lemma

Let $f \in \mathbb{Z}[x]$ be irreducible. Then $f$ is also irreducible over $\mathbb{Q}$.

Equivalently, if $f \in \mathbb{Z}[x]$ factors over $\mathbb{Q}$, then it factors over $\mathbb{Z}$.

## Theorem (Eisenstein's criterion)

A polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0 \in \mathbb{Z}[x]$ is irreducible if for some prime $p$, the following all hold:

1. $p \nmid a_n$;
2. $p \mid a_k$ for $k = 0, \ldots, n-1$;
3. $p^2 \nmid a_0$.

For example, Eisenstein's criterion tells us that $x^{10} + 4x^7 + 18x + 14$ is irreducible.

## Remark

If Eisenstein's criterion fails for all primes $p$, that does *not* necessarily imply that $f$ is reducible. For example, $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Q}$, but Eisenstein cannot detect this.

## Extension fields as vector spaces

Recall that a vector space over $\mathbb{Q}$ is a set of vectors $V$ such that

- If $u, v \in V$, then $u + v \in V$ (closed under addition)
- If $v \in V$, then $cv \in V$ for all $c \in \mathbb{Q}$ (closed under scalar multiplication).

The field $\mathbb{Q}(\sqrt{2})$ is a 2-dimensional vector space over $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

This is why we say that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

Notice that the other field extensions we've seen are also vector spaces over $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i : a, b, c, d \in \mathbb{Q}\},$$
$$\mathbb{Q}(\zeta, \sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{4} : a, b, c, d, e, f \in \mathbb{Q}\}.$$

As $\mathbb{Q}$-vector spaces, $\mathbb{Q}(\sqrt{2}, i)$ has dimension 4, and $\mathbb{Q}(\zeta, \sqrt[3]{2})$ has dimension 6.

### Definition

If $F \subseteq E$ are fields, then the degree of the extension, denoted $[E : F]$, is the dimension of $E$ as a vector space over $F$.

Equivalently, this is the number of terms in the expression for a general element for $E$ using coefficients from $F$.

# Minimial polynomials

## Definition

Let $r \notin F$ be algebraic. The minimal polynomial of $r$ over $F$ is the irreducible polynomial in $F[x]$ of which $r$ is a root. It is unique up to scalar multiplication.

## Examples

- $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$, and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
- $i = \sqrt{-1}$ has minimal polynomial $x^2 + 1$ over $\mathbb{Q}$, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.
- $\zeta = e^{2\pi i/3}$ has minimal polynomial $x^2 + x + 1$ over $\mathbb{Q}$, and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.
- $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$, and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

What are the minimal polynomials of the following numbers over $\mathbb{Q}$?

$$-\sqrt{2}\,, \qquad -i\,, \qquad \zeta^2\,, \qquad \zeta\sqrt[3]{2}\,, \qquad \zeta^2\sqrt[3]{2}\,.$$

## Degree theorem

The degree of the extension $\mathbb{Q}(r)$ is the degree of the minimal polynomial of $r$.