Lecture 1: Polynomials and Sequences

ECON 2127/8014

Semester 2, 2009

23 July 2009

Complex numbers

Let $\mathbb{R}$ denote the set of real numbers. A complex number is a number of the form $a + bi$, where $a, b \in \mathbb{R}$, and

$$i := \sqrt{-1},$$

or equivalently, $i^2 = -1$.

We use $\mathbb{C}$ to denote the set of complex numbers.

If $z = a + bi$, then

a is the real part of z, denoted by $\operatorname{Re} z$,

b is the imaginary part of z, denoted by $\operatorname{Im} z$,

$\bar{z} := a - bi$ is the complex conjugate of z.

Check that $z\bar{z} = a^2 + b^2$!

Polynomials

Let $\mathbb{F}$ denote either $\mathbb{R}$ or $\mathbb{C}$. (Note that $\mathbb{R} \subset \mathbb{C}$!)

Definition

- A function $p : \mathbb{F} \to \mathbb{F}$ is called a polynomial with coefficients in $\mathbb{F}$, if there exist numbers $a_0, a_1, \ldots, a_m \in \mathbb{F}$, such that

  $$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m$$

  for all $z \in \mathbb{F}$.
- If $a_m \neq 0$, we say that p has degree m.
- A number $\lambda \in \mathbb{F}$ is a root of a polynomial p if

  $$p(\lambda) = 0.$$

We use $\mathscr{P}(\mathbb{F})$ to denote the set of all polynomials with coefficients in $\mathbb{F}$.

Proposition

Suppose $p \in \mathscr{P}(\mathbb{F})$ has degree $m \geq 1$ and $\lambda \in \mathbb{F}$. Then λ is a root of p iff there exists a polynomial $q \in \mathscr{P}(\mathbb{F})$ with degree $m-1$ such that

$$p(z) = (z - \lambda)q(z)$$

for all $z \in \mathbb{F}$.

Proof. [⇐] If $p(z) = (z - \lambda)q(z)$ for some polynomial q, then

$$p(\lambda) = (\lambda - \lambda)q(\lambda) = 0,$$

so λ is a root of p.
[⇒] Suppose λ is a root of p, and we can write p as

$$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m.$$

Since $p(\lambda) = 0$,

$$0 = a_0 + a_1\lambda + a_2\lambda^2 + \cdots + a_m\lambda^m.$$

Subtracting the last two equations yields

$$p(z) = a_1(z - \lambda) + a_2(z^2 - \lambda^2) + \cdots + a_m(z^m - \lambda^m).$$

For $j = 2, \ldots, m$, we have

$$z^j - \lambda^j = (z - \lambda)q_{j-1}(z),$$

where $q_{j-1}(z) = \lambda^{j-1} + \lambda^{j-2}z + \cdots + \lambda z^{j-2} + z^{j-1}$ is a polynomial with degree $j - 1$. (Check!) Then

$$p(z) = (z - \lambda)\underbrace{\left(a_1 + a_2q_1(z) + \cdots + a_mq_{m-1}(z)\right)}_{q(z)},$$

with q a polynomial of degree $m - 1$. ■

Corollary

If $p \in \mathscr{P}(\mathbb{F})$ has degree $m \geq 0$, then p has at most m distinct roots in $\mathbb{F}$.

Proof. By induction on m. Look it up! □

Theorem (Division Algorithm)

Suppose $p, q \in \mathscr{P}(\mathbb{F})$, with $p \neq 0$. Then there exist polynomials $s, r \in \mathscr{P}(\mathbb{F})$ such that

$$q = sp + r$$

and $deg(r) < deg(p)$.

$\Rightarrow$ Polynomial long division

Theorem (Fundamental Theorem of Algebra)

Every non-constant polynomial with complex coefficients has a root.

Factorization

Corollary

If $p \in \mathscr{P}(\mathbb{C})$ is a non-constant polynomial, then p has a unique factorization (except for the order of the factors) of the form

$$p(z) = c(z - \lambda_1) \dots (z - \lambda_m),$$

where $c, \lambda_1, \dots, \lambda_m \in \mathbb{C}$.

Proof. We use induction on m to show that a factorization of the required form exists. If $m = 1$, $p(z) = a_0 + a_1 z$, so $\lambda = -a_0/a_1$ is a root, and $p(z) = a_1(z + a_0/a_1)$ is the (unique) required factorization.
Inductive hypothesis: Assume that $m > 1$ and that the desired factorization exists and is unique for all polynomials of degree $m - 1$.
Inductive step: We show that the inductive hypothesis implies that the required factorization exists and is unique for all polynomials of degree m: Let $p \in \mathscr{P}(\mathbb{C})$ have degree m.

By the fundamental theorem of algebra, p has a root λ, so we can write p as $p(z) = (z - \lambda)q(z)$, where q has degree $m - 1$. The inductive hypothesis implies that q has the required factorization, which yields a factorization for p of the required form.

To show that the factorization is unique, note that c must be equal to the coefficient of z^m, and assume that there are two such factorizations, so

$$(z - \lambda_1) \ldots (z - \lambda_m) = (z - \tau_1) \ldots (z - \tau_m).$$

Since the left-hand side of the equation is equal to 0 when $z = \lambda_1$, one of the τ's must equal λ_1, so we can set $\tau_1 = \lambda_1$. Dividing by $(z - \lambda_1)$ for $z \neq \lambda_1$, yields

$$(z - \lambda_2) \ldots (z - \lambda_m) = (z - \tau_2) \ldots (z - \tau_m).$$

This equation must also hold for $z = \lambda_1$ (otherwise, the polynomial defined by subtracting the right side of the equation from the left side is not equal to zero at $z = \lambda_1$ and has an infinite number of roots given by all $z \neq \lambda_1$). Thus, the inductive hypothesis implies that except for the order, the λ's and τ's must be the same. ■

Proposition

If $p \in \mathscr{P}(\mathbb{R})$ and $\lambda \in \mathbb{C}$ is a root of p, then so is $\bar{\lambda}$.

Proof. We can write p as

$$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m,$$

with $a_0, a_1, a_2, \ldots, a_m \in \mathbb{R}$. Since $\lambda \in \mathbb{C}$ is a root,

$$0 = a_0 + a_1 \lambda + a_2 \lambda^2 + \cdots + a_m \lambda^m.$$

Taking the conjugate of both sides yields

$$0 = a_0 + a_1 \bar{\lambda} + a_2 \bar{\lambda}^2 + \cdots + a_m \bar{\lambda}^m,$$

which is equivalent to saying that $\bar{\lambda}$ is a root of p. ∎

Proposition

If $\alpha, \beta \in \mathbb{R}$, there exists a polynomial factorization of the form

$$x^2 + \alpha x + \beta = (x - \lambda_1)(x - \lambda_2),$$

with $\lambda_1, \lambda_2 \in \mathbb{R}$ if and only if $\alpha^2 \geq 4\beta$.

Recall that the roots of a polynomial $ax^2 + bx + c$ with $a, b, c \in \mathbb{R}$, can be calculated using the formula

$$\lambda_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

These roots are real if $b^2 - 4ac \geq 0$.

Theorem

If $p \in \mathscr{P}(\mathbb{R})$ *is a non-constant polynomial, then* p *has a unique factorization (except for the order of the factors) of the form*

$$p(x) = c(x-\lambda_1)\dots(x-\lambda_m)(x^2+\alpha_1 x+\beta_1)\dots(x^2+\alpha_M x+\beta_M),$$

$c, \lambda_1, \dots, \lambda_m \in \mathbb{R}$ *and* $(\alpha_1, \beta_1), \dots, (\alpha_M, \beta_M) \in \mathbb{R}^2$ *with* $\alpha_j < 4\beta_j$ *for each* j*.*

Proof. (Idea) p has a unique factorization of the form

$$p(z) = c(z - \lambda_1)\dots(z - \lambda_m),$$

with $c, \lambda_1, \dots, \lambda_m \in \mathbb{C}$. Since complex roots come in conjugate pairs $\lambda, \bar{\lambda}$, we can combine $(x - \lambda)(x - \bar{\lambda})$ to get a term of the form $(x^2 + \alpha x + \beta)$, with $\alpha, \beta \in \mathbb{R}$. $\square$

Sequences

Let $\mathbb{N}_+ := \{1, 2, 3, \ldots\}$.

Definition

A real-valued *sequence* s is a function $s : \mathbb{N}_+ \to \mathbb{R}$.

Note:

- We denote the values of a sequence by $s(n)$ or s_n.
- We often write a sequence s as $(s_n)_{n \in \mathbb{N}_+}$, or (s_n).
- The image of a sequence (s_n) is the set $\{s_n \mid n \in \mathbb{N}_+\}$.

Examples:

- $s_n = \frac{1}{n}$
- $s_n = (-1)^n$
- $s_n = \frac{1}{q^n}$, where $q \in \mathbb{R}$

Subsequences

Let $n : \mathbb{N}_+ \to \mathbb{N}_+$ be an increasing function (sequence?), i.e., a function having the property that $n(k) < n(m)$ whenever $k < m$.

Given any sequence s, we can define a new sequence (t_k) by

$$t_k = t(k) = [s \circ n](k) = s(n(k)) = s(n_k) = s_{n_k}.$$

Definition

A *subsequence* of a sequence s is a sequence $(s_{n_k})_{k \in \mathbb{N}_+}$ defined as above by some increasing function n.

Note that $\{s_{n_k} \mid k \in \mathbb{N}_+\} \subseteq \{s_n \mid n \in \mathbb{N}_+\}$.

Example: The sequence $(1/k^2)$ is a subsequence of $(1/n)$ by letting $n(k) = k^2$.

Limits

Definition

A real-valued sequence (s_n) *converges* to a number $s \in \mathbb{R}$, if for each $\epsilon > 0$, there exists a number N, such that $n > N$ implies that $|s_n - s| < \epsilon$.

Note:

- If (s_n) converges to s, we write $\lim_{n\to\infty} s_n = s$, or $s_n \to s$.
- s is called the *limit* of (s_n).
- A sequence (s_n) *diverges* if it has no limit.
- The value of N depends on ϵ!

Proposition

A convergent sequence (s_n) has a unique limit.

Proof. (by contradiction) We assume that (s_n) has two distinct limits, s and t, and derive a contradiction.

If $\lim s_n = s$ and $\lim s_n = t$, then for any $\epsilon > 0$, there exists a number N_1, so that

$$n > N_1 \text{ implies that } |s_n - s| < \frac{\epsilon}{2},$$

and there exists a number N_2, so that

$$n > N_2 \text{ implies that } |s_n - t| < \frac{\epsilon}{2}.$$

For $n > \max\{N_1, N_2\}$, the triangle inequality implies that

$$|s - t| = |(s - s_n) + (s_n - t)| \leq |s - s_n| + |s_n - t| \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Thus, $|s - t| < \epsilon$ for every $\epsilon > 0$, which implies that $s = t$, a contradiction to the assumption that s and t are distinct. ■

Proposition

If a sequence (s_n) converges, then every subsequence converges to the same limit.

Proof. If $(s_{n_k})_{k \in \mathbb{N}_+}$ is a subsequence of (s_n), then $n_k \geq k$ for every k. (Prove this using induction!)
Let $s = \lim s_n$ and choose any $\epsilon > 0$. Then there exists an N so that $n > N$ implies $|s_n - s| < \epsilon$. $k > N$ implies that $n_k > N$, and thus that $|s_{n_k} - s| < \epsilon$. ■

Claim

$lim \frac{1}{n^2} = 0$.

Proof. We need to find, for every $\epsilon > 0$, a corresponding N so that $|1/n^2 - 0| < \epsilon$ for all $n > N$. Consider any $\epsilon > 0$. Then $1/n^2 < \epsilon$ whenever $n > 1/\sqrt{\epsilon}$. Thus, the required condition holds if we set $N = 1/\sqrt{\epsilon}$. ■

Claim

The sequence defined by $a_n = (-1)^n$ *does not converge.*

Proof. (by contradiction) Assume $\lim a_n = a$ for some a. We need to find one ϵ for which this assumption yields a contradiction.

Let $\epsilon = 1$. Since we assumed that a_n converges, there must exist an N so that $|(-1)^n - a| < 1$ for all $n > N$. For even n, this yields $|1 - a| < 1$, for odd n, $|-1-a| < 1$. By the triangle inequality,

$$2 = |1-(-1)| = |1-a+a-(-1)| \leq |1-a|+|a-(-1)| < 1+1 = 2,$$

which yields a contradiction since $2 < 2$ is not possible. ■

Limit theorems

Let $s_n \to s$ and $t_n \to t$, and let $k \in \mathbb{R}$. Then

- $\lim(ks_n) = ks$;
- $\lim(s_n + t_n) = s + t$;
- $\lim(s_n t_n)$=st;
- If $s_n \neq 0$ for all n, and $s \neq 0$, then $\lim 1/s_n = 1/s$;
- If there exists an N so that $s_n \leq t_n$ for all $n > N$, then $s \leq t$;
- If $s = t$ and there exists an N so that $s_n \leq r_n \leq t_n$ for all $n > N$, then $r_n \to s$.

Bounded and monotone sequences

Definition

Let (s_n) be a real-valued sequence and define $S := \{s_n \mid n \in \mathbb{N}_+\}$.

- (s_n) is *bounded* if S is a bounded set, i.e., if there exists a constant M such that $|s_n| \leq M$ for all n.
- (s_n) is *non-decreasing* if $s_n \leq s_{n+1}$ for all n.
- (s_n) is *non-increasing* if $s_n \geq s_{n+1}$ for all n.
- (s_n) is *monotone* if it is either non-decreasing or non-increasing.
- A number M such that $s_n \leq M$ for all n is called an *upper bound* of S. The *supremum* of S, denoted by $\sup S$, is the least upper bound of S.
- A number m such that $s_n \geq m$ for all n is called an *lower bound* of S. The *infimum* of S, denoted by $\inf S$, is the greatest lower bound of S.