Week 3: Polynomials

Lecture notes · Thu Oct 8 / Fri Oct 9

Toolbox. Throughout, p is a polynomial with coefficients in a field ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) or in $\mathbb{Z}$.

1. **Root counting.** A *nonzero* polynomial of degree n has at most n roots (in any field). Hence: if $\deg p, \deg q \le n$ and p, q agree at $n+1$ points, then $p = q$; if p vanishes at infinitely many points, $p \equiv 0$. Factor theorem: $p(a) = 0 \iff (x-a) \mid p(x)$.
2. **Interpolation.** Through any $n+1$ points (x_i, y_i) with distinct x_i passes exactly one polynomial of degree $\le n$ (Lagrange: $\sum_i y_i \prod_{j \ne i} \frac{x-x_j}{x_i-x_j}$). Working move: if p has degree $\le n$ and you know p at $n+1$ points, build an auxiliary polynomial that *vanishes* there, e.g. $q(x) = (x+1)p(x) - x$, and write it as $c\prod(x - x_i)$.
3. **Integer coefficients.** If $p \in \mathbb{Z}[x]$ and $a \ne b \in \mathbb{Z}$, then $(a-b) \mid p(a) - p(b)$. If $p(m) = \pm 1$ at several integers, factor $p(x) \mp 1 = \prod(x - a_i) \cdot q(x)$ with $q \in \mathbb{Z}[x]$ and use that small numbers have few integer divisors. A rational root of a monic $p \in \mathbb{Z}[x]$ is an integer dividing $p(0)$.
4. **Vieta.** If $x^n + c_{n-1}x^{n-1} + \cdots + c_0 = \prod(x - r_i)$ then $e_k(r_1, \ldots, r_n) = (-1)^k c_{n-k}$. Power sums follow, e.g. $\sum r_i^2 = e_1^2 - 2e_2$; every symmetric polynomial in the roots is a polynomial in the coefficients.
5. **Degree and growth.** In a polynomial identity, compare degrees and leading coefficients first; for large $|x|$ the top term dominates. If $r(x) \mid s(x)$ with $s \ne 0$ then $\deg r \le \deg s$, so a nonzero multiple of lower degree is impossible. Formal derivative: $p(x+h) \equiv p(x) + h\,p'(x) \pmod{h^2}$, and a is a repeated root iff $p(a) = p'(a) = 0$.
6. **Locating roots.** Real roots: sign changes plus the intermediate value theorem; n sign changes for a degree-n polynomial pin down *all* its roots. Complex roots: triangle inequality (a root of $z^n + \ldots$ forces the top term to be balanced by the rest); the reciprocal polynomial $x^n p(1/x)$ swaps $|z| < 1$ with $|z| > 1$.

Worked examples (none of these are on the handout).

Example 1 (Vieta and real roots)**.** *If $x^3 + ax^2 + bx + c$ has three real roots, then $a^2 \ge 3b$.*
Let the roots be r, s, t. Vieta gives $r + s + t = -a$, $rs + st + tr = b$. Then $a^2 = (r+s+t)^2 = (r^2+s^2+t^2) + 2b$, and $r^2 + s^2 + t^2 \ge rs + st + tr = b$ because $2(r^2+s^2+t^2) - 2(rs+st+tr) = (r-s)^2 + (s-t)^2 + (t-r)^2 \ge 0$. So $a^2 \ge 3b$. (This needs real *roots: $x^3 - x^2 + x - 1 = (x-1)(x^2+1)$ has $a = -1$, $b = 1$, and $a^2 = 1 < 3 = 3b$.)*

Example 2 (The integer trick)**.** *If $p \in \mathbb{Z}[x]$ takes the value 1 at four distinct integers, then $p(m) \ne -1$ for every integer m.*
Say $p(a_i) = 1$ for distinct integers $a_1, \ldots, a_4$. By the factor theorem applied four times, $p(x) - 1 = (x-a_1)(x-a_2)(x-a_3)(x-a_4)\,q(x)$; each divisor $x - a_i$ is monic, so long division of an integer polynomial by it never leaves $\mathbb{Z}[x]$, and $q \in \mathbb{Z}[x]$. If $p(m) = -1$ then $(m-a_1)(m-a_2)(m-a_3)(m-a_4)\,q(m) = -2$. The four factors $m - a_i$ are distinct nonzero integers dividing 2, so they lie in $\{\pm 1, \pm 2\}$ and their product has absolute value 4, which does not divide 2. Contradiction.

Example 3 (Infinitely many roots)**.** *Find all real polynomials with $p(0) = 0$ and $p(x^2+1) = p(x)^2 + 1$.*
Define $a_0 = 0$, $a_{k+1} = a_k^2 + 1$; this sequence is strictly increasing, so its terms are distinct. Claim: $p(a_k) = a_k$ for all k. Indeed $p(a_0) = 0 = a_0$, and if $p(a_k) = a_k$ then $p(a_{k+1}) = p(a_k^2 + 1) =$

$p(a_k)^2 + 1 = a_k^2 + 1 = a_{k+1}$. *So $p(x) - x$ has infinitely many roots, hence $p(x) = x$, which does satisfy the equation.*

Pitfall. "A degree-n polynomial has n roots" is true over $\mathbb{C}$ with multiplicity, and only for *nonzero* polynomials. When you argue "p and q agree at $n+1$ points, so $p = q$," you must first bound both degrees by n; when you write $q(x) = c\prod(x - x_i)$ you must allow $c = 0$ until you evaluate somewhere else. Over $\mathbb{R}$, a polynomial may have no roots at all, so "the roots are real" is a genuine claim to prove, not a default.

Pitfall. Vieta's signs alternate: for $x^3 + ax^2 + bx + c$ the sum of roots is $-a$, not a. And divisibility depends on the ring: $2x$ divides x^2 in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$; when you need integer quotients, check the divisor is monic or invoke Gauss's lemma.

How to recognize this technique on the exam. The give-away is the *question*:"find all polynomials such that…" (compare degrees, then find infinitely many roots of a difference); "p has integer coefficients and…" (the $a - b \mid p(a) - p(b)$ trick, or factor $p \mp 1$); "$p(k) =$ something for $k = 0, \ldots, n$" (interpolation via an auxiliary vanishing polynomial); "show the roots are real / lie outside the disk" (sign changes, or a triangle-inequality estimate after multiplying by $(1 - z)$ or passing to the reciprocal polynomial); "p divides q" (compare degrees; formal derivative). When stuck, factor over $\mathbb{C}$ and ask what each root must satisfy.

Suggested timing (15 min). 0–3: read the toolbox aloud, emphasizing items 1, 3, 5. 3–9: Examples 2 and 3 on the board (the integer trick, then infinitely many roots). 9–12: Example 1 quickly, as a Vieta reminder. 12–15: the pitfalls and the recognition paragraph; then split into groups on Problems 1–4.