DIS 5B

1 Polynomials in One Indeterminate

We will now prove a fundamental result about polynomials: every non-zero polynomial of degree n (over a field F) has at most n roots. Think of F as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or GF(p) for a prime p; your proofs should work equally well in each case.

(a) Show that for any $\alpha \in F$, there exists some polynomial $Q(x)$ of degree $n-1$ and some $b \in F$ such that $P(x) = (x-\alpha)Q(x) + b$.

(b) Show that if α is a root of $P(x)$, then $P(x) = (x-\alpha)Q(x)$.

(c) Prove that any polynomial of degree 1 has at most one root. This is your base case.

(d) Now prove the inductive step: if every polynomial of degree $n-1$ has at most $n-1$ roots, where n is an integer ≥ 2, then any polynomial of degree n has at most n roots.

Solution:

(a) Let

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0.$$

We need to show that there is a polynomial

$$Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots b_1 x + b_0$$

and $b \in F$ such that $Q(x)(x-\alpha) + b = P(x)$.

$$\begin{aligned} Q(x)(x-\alpha) + b = b_{n-1}x^n + (b_{n-2} - \alpha b_{n-1})x^{n-1} + (b_{n-3} - \alpha b_{n-2})x^{n-2} \\ + \cdots + (b_0 - \alpha b_1)x - \alpha b_0 + b \end{aligned}$$

Therefore if we set

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= a_{n-1} + \alpha b_{n-1} \\ b_{n-3} &= a_{n-2} + \alpha b_{n-2} \\ &\vdots \\ b_0 &= a_1 + \alpha b_1 \\ b &= a_0 + \alpha b_0 \end{aligned}$$

we get the desired equality.

(b) If α is a root of $P(x)$, $0 = P(\alpha) = (\alpha - \alpha)Q(\alpha) + b = 0 \cdot Q(\alpha) + b = b$ (where we used the theorem for general fields that $a0 = 0$). Hence $P(x) = (x - \alpha)Q(x)$.

(c) **Base case:** Consider a non-zero polynomial $P(x) = a_1 x + a_0$. If there exists a root of the polynomial α, $P(\alpha) = 0$. That is:

$$\begin{aligned} a_1\alpha + a_0 &= 0 \\ a_1\alpha &= -a_0 \end{aligned}$$

Since P has degree 1, $a_1 \neq 0$, so multiplying both sides by a_1^{-1} yields $\alpha = a_1^{-1}(-a_0)$, so there is exactly one possible value for α.

(d) **Inductive step:** Suppose every polynomial of degree $n-1$ has at most $n-1$ roots. Consider a polynomial P of degree n. If P has no roots, then we are done. Otherwise, let α be a root of P. We can then factor $P(x) = (x - \alpha)Q(x)$, where Q has degree $n-1$. By the inductive hypothesis, Q has at most $n-1$ roots. Note that if $P(x) = 0$, then either $x - \alpha = 0$ or $Q(x) = 0$ since F is a field, so the roots of P are precisely α along with the roots of Q, and thus P has at most n roots.

2 Interpolate!

Find the lowest-degree polynomial $P(x)$ that passes through the points $(1,4), (2,3), (5,0)$ modulo 7.

Solution:

First, observe that we don't need to compute Δ_5(x), since it will be multiplied by 0 anyway.

$$\begin{aligned} \Delta_1(x) &\equiv \frac{(x-2)(x-5)}{(1-2)(1-5)} \equiv \frac{x^2 - 7x + 10}{4} \equiv 2 \cdot (x^2 + 3) \equiv 2x^2 + 6 \pmod 7 \\ \Delta_2(x) &\equiv \frac{(x-1)(x-5)}{(2-1)(2-5)} \equiv \frac{x^2 - 6x + 5}{-3} \equiv 2 \cdot (x^2 - 6x + 5) \equiv 2x^2 + 2x + 3 \pmod 7 \\ P(x) &\equiv y_1\Delta_1(x) + y_2\Delta_2(x) \equiv 4 \cdot (2x^2 + 6) + 3 \cdot (2x^2 + 2x + 3) \equiv 14x^2 + 6x + 33 \\ &\equiv \boxed{6x + 5} \pmod 7. \end{aligned}$$

Alternatively, you can graph the points in GF(7) and observe that they all lie on $y = -x + 5$, which is equivalent to $\boxed{6x + 5}$ modulo 7.

3 Secrets in the United Nations

The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination s. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

(a) Propose a scheme that gives private information to the Secretary General and n countries so that s can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: in order for a country to help, all of the country's k representatives must agree. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary General and to each representative of each country.

Solution:

(a) Create a polynomial of degree $n-1$ and give each country one point. Give the Secretary General $n-m$ points, so that if he collaborates with m countries, they will have $n-m+m=n$ points and can reconstruct the polynomial. Without the General, n countries can come together and also recover the polynomial. No combination of the General with fewer than m countries can recover the polynomial.

Alternatively:

Have two schemes, one for the first condition and one for the second.

For the first condition: just one polynomial of degree $\leq n-1$ would do, where each country gets one point. The polynomial evaluated at 0 would give the secret.

For the second condition: one polynomial is created of degree $m-1$ and a point is given to each country. Another polynomial of degree 1 is created, where one point is given to the secretary general and the second point can be constructed from the first polynomial if m or more of the countries come together. With these two points, we have a unique 1-degree polynomial, which could give the secret evaluated at 0.

(b) The scheme in part (a) remains the same, but instead of directly giving each country a point on the $n-1$ degree polynomial to open the vault, construct an additional polynomial for each country that will produce that point.

Each country's polynomial has degree $k-1$, and a point is given to each of the k representatives of the country. Thus, when they all get together they can produce a point for either of the schemes.