Math 221B, Wed Apr 13

Back Mon!

- Reading for today: 16.1–16.3.
- Reading for ~~Wed Apr 13~~: 16.4–16.5.
- PS08 due in one week(-ish).

(PS07 yesterday)

Mon Apr 18

Symmetric polynomials

R a ring of coefficients.

- S_n (symmetric group on $\{1, \ldots, n\}$) acts on $\{u_1, \ldots, u_n\}$ by permuting indices, and therefore acts on $R[u_1, \ldots, u_n]$.
- To say that $g \in R[u_1, \ldots, u_n]$ is a **symmetric polynomial** means that g is fixed by the action of every $\sigma \in S_n$. Example:

$u_1, u_2 u_3$ e.g.

NB: can get symm poly by taking rand poly & symm

$$g(u_1, u_2, u_3) = u_1^2 u_3 + u_2^2 u_1 + u_3^2 u_2 + u_3^2 u_1 + u_1^2 u_2 + u_2^2 u_3$$

[n] = {1,...,n}

- Key examples: the **elementary symmetric polynomials**:

$\binom{n}{1} s_1 = u_1 + u_2 + u_3 + \cdots + u_n$ terms corresp to subsets of [n] of size 1

$\binom{n}{2} s_2 = u_1 u_2 + u_1 u_3 + \cdots + u_{n-1} u_n$ terms corresp to subsets of [n] of size 2

$\vdots$

$\binom{n}{n} s_n = u_1 u_2 \cdots u_n$ subsets of [n] of size n

The point of the elementary symmetric polynomials

If

$$f(x) = (x - u_1)(x - u_2)\cdots(x - u_n)$$
$$= x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots \pm a_{n-1} x \mp a_n,$$

then:

$a_1 = u_1 + u_2 + \cdots + u_n$

$= s_1(u_1 \ldots u_n)$

$a_2 =$ comes from picking n-2 terms to have x and 2 terms to have u_i

$= u_1u_2 + u_1u_3 + \cdots + u_{k-1}u_n$ $\binom{n}{2}$

$= s_2(u_1 \ldots u_n)$

$a_i = s_i(u_1 \ldots u_n)$

Symmetric polynomials give formula for how coefficients of f are expressed in terms of the roots of f

The Symmetric Functions Theorem

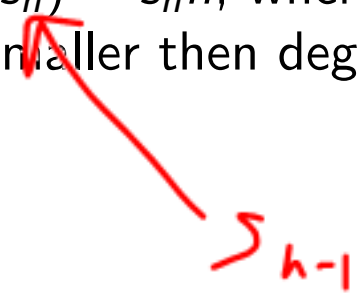
SFT

Theorem

If $g \in R[u_1, \ldots, u_n]$ is symmetric, then g is a polynomial function of the elementary symmetric functions $s_1, \ldots, s_n$.

Methods:

1. Solve for undetermined coefficients by plugging in well-chosen values for $u_1, \ldots, u_n$.
2. Inductively:
   - Let $g^\circ(u_1, \ldots, u_{n-1}) = g(u_1, \ldots, u_{n-1}, 0)$.
   - Solve for g° in terms of the elementary symmetric functions of one fewer variable: $g^\circ = Q(s_1^\circ, \ldots, s_{n-1}^\circ)$.
   - **FACT:** $g - Q(s_1, \ldots, s_n) = s_n h$, where h is a symmetric polynomial of degree smaller then $\deg g$. Can then solve for h by induction.



Ex $g = u_1^2 u_2 + u_2^2 u_3 + u_3^2 u_1 + u_2^2 u_1 + u_3^2 u_2 + u_1^2 u_3$

$s_2 = u_1 u_2 + u_1 u_3 + u_2 u_3$

all possible monomials of *weighted* degree 3 in s_i

$g = a s_3 + b s_1 s_2 + c s_1^3$

$g(1,0,0) = 0 = a \cdot 0 + b \cdot 1 \cdot 0 + c \cdot 1 \quad c = 0$

$s_1(1,0,0) = 1 + 0 + 0 = 1$

$s_2(1,0,0) = 0 + 0 + 0 = 0$ $\quad s_3 = 0$

$g(1,1,0) = 2 \quad s_1(1,1,0) = 2 \quad s_2(1,1,0) = 1$ $\quad s_3 = 0$

$2 = a \cdot 0 + b \cdot 2 \quad \boxed{b = 1}$

g(1,1,1) = 6, s_1(1,1,1)=3, s_2(1,1,1)=3, s_3(1,1,1)=1
=> 6 = a + 9 => a = -3.

Method 2

$g = u_1^2 u_2 + u_2^2 u_3 + u_3^2 u_1 + u_2^2 u_1 + u_3^2 u_2 + u_1^2 u_3$

$g^0 = u_1^2 u_2 + u_2^2 u_1 = (u_1 u_2)(u_1 + u_2)$

$g^0 = s_1^0 s_2^0$

$s_1^0 = u_1 + u_2$

$s_2^0 = u_1 u_2$

lift to n variables

9 terms

$g - s_1 s_2 = g - (u_1 + u_2 + u_3)(u_1 u_2 + u_1 u_3 + u_2 u_3)$

$= g - (g + 3 s_3) = -3 s_3$

$g = s_1 s_2 - 3 s_3$

Why do we care about this right now?

Theorem

For $f \in F[x]$, suppose

$$f(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots \pm a_{n-1} x^{1} \mp a_n$$
$$= (x - \alpha_1) \cdots (x - \alpha_n).$$

$\alpha_i \in K/F$

If $g(u_1, \ldots, u_n)$ is symmetric in n variables with coefficients in F, then $g(\alpha_1, \cdots, \alpha_n) \in F$.

Proof:

By SFT, $g = Q(s_1 \ldots s_n)$

$g(\alpha_1 \ldots \alpha_n) = Q(s_1(\alpha_1) \ldots s_n(\alpha_1))$

$= Q(a_1 \ldots a_n) \in F.$

Note: If you like symmetric polynomials, this leads to a whole field, algebraic combinatorics; see Zhang

The discriminant

We will eventually describe the symmetries of the roots of a given cubic or quartic polynomial in terms of the values of various symmetric polynomials of those roots. Most prominently:

Definition

Suppose

$$P(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots \pm s_{n-1} x \mp s_n$$
$$= (x - u_1)(x - u_2) \cdots (x - u_n).$$

The **discriminant** of P is defined to be

$$D(u) = \prod_{i<j} (u_i - u_j)^2$$
$$= (u_1 - u_2)^2 (u_1 - u_3)^2 \ldots (u_{n-1} - u_n)^2.$$

D(u) is symmetric because it's really defined only in terms of the subsets of [n], and those subsets are preserved by S_n. So D(u) = poly fn of coeffs.

Properties of the discriminant

- Since $D(u)$ is symmetric, by SFT, $D(u) = \Delta(s_1, \ldots, s_n)$ for some polynomial $\Delta(z_1, \ldots, z_n)$.
- Therefore, if f is a polynomial with coefficients in F, then discriminant of f is a function of coefficients of f (and in particular, has value in F).
- If $\alpha_1, \ldots, \alpha_n \in K$, then $D(\alpha) = 0$ iff $\alpha_i = \alpha_j$ for some $i < j$.
- For $n = 2$, we have

$$D(u_1, u_2) = (u_1 - u_2)^2 \qquad s_1 = u_1 + u_2$$
$$s_2 = u_1 u_2$$
$$= u_1^2 - 2u_1u_2 + u_2^2$$
$$= s_1^2 - 4s_2 \qquad P = x^2 - s_1 x + s_2$$
$$= b^2 - 4c \qquad = x^2 + bx + c$$

Discriminant from HS algebra!

Discriminant of a cubic, special case

D = disc in terms of roots; Delta = disc in terms of coeffs of f

Formula for discriminant of cubics and quartics is much more complicated, but we can figure out the special cases we need.

Example: After a change of variables, every cubic looks like $f(x) = x^3 + px + q$, whose discriminant is

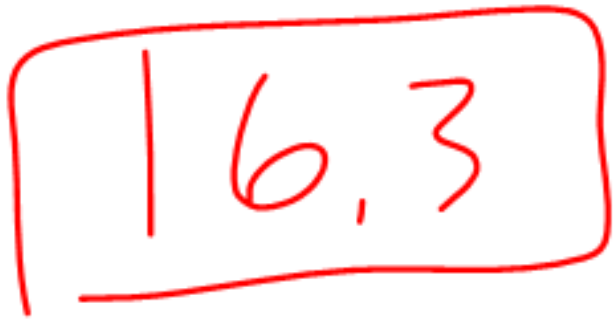
$$\Delta = -4p^3 - 27q^2.$$

So if $f(x) = x^3 + px + q$ has roots $\alpha_1, \alpha_2, \alpha_3$, we have

$$\Delta = -4p^3 - 27q^2 = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

Something analogous, but more complicated, happens in 4 variables.

Definition of splitting field



$f \in F[x]$. To say that K/F is a **splitting field** for f over F means:

- $f = (x - \alpha_1) \dots (x - \alpha_n)$ over K, and
- $K = F(\alpha_1, \dots, \alpha_n)$.

Existence of splitting fields

- Every $f(x) \in F[x]$ has some splitting field K/F, with $[K : F] < \infty$.
- For any L/F, there exists some splitting field K/F such that $F \subseteq L \subseteq K$.

Splitting Theorem

Definition

To say that K/F is **normal** means that if $g(x)$ is irreducible in $F[x]$ and g has one root in K, then g splits completely in K.

Theorem

Suppose K/F is a splitting field of $f(x) \in F[x]$. Then K/F is normal; i.e., if an irreducible $g(x) \in F[x]$ has one root in K, then it splits completely in K.

Not every extension is normal:

The Galois group of an extension

Definition

An F-**isomorphism** $\sigma : K/F \to K'/F$ is an isomorphism that is the identity on F. If $K = K'$, then σ is an F-**automorphism**.

Definition

$\mathrm{Gal}(K/F)$ is the group of all F-automorphisms of K/F.

Definition

For a finite extension K/F, to say that K/F is a **Galois extension** means that $\mathrm{Gal}(K/F) = [K : F]$.

Examples: $\mathbf{C}/\mathbf{R}$

$\mathbf{Q}(\sqrt{2})/\mathbf{Q}$