Welcome back

When you're connected by zoom:

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 15.8, 16.1–16.2; for Wed: 16.3–16.4.
- Exam 2: Due Wed Apr 08; PS08: Due Mon Apr 13. (But all deadlines are elastic.)

Last: Five finite field facts

Theorem

p prime, $q = p^r$, K a field of order q.

1. *Elements of K are roots of $x^q - x$.*
2. *$K^\times$ is cyclic of order $q - 1$.*
3. *There exists a field of order q, and all fields of order q are isomorphic.* called $\mathbb{F}_q$
4. *K contains a subfield of order $p^k \Leftrightarrow k$ divides r.*
5. *Irreducible factors of $x^q - x$ over $\mathbb{F}_p$ are irreducibles in $\mathbb{F}_p[x]$ whose degrees divide r.*

Example: Computing in $\mathbb{F}_{16}$

$m(x) = x^4 + x + 1$ irreducible over $\mathbb{F}_2$. Let α be a root of $m(x)$, so $\mathbb{F}_{16} = \mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/(m(x))$.

$16 = 2^4$ deg $m = 4$

$\beta = \alpha^3 + \alpha$

$\gamma = \alpha^2 + \alpha + 1$ $\quad 2\alpha = 0$

min $m(x)$, deg $= 3$

$\beta + \gamma = (\alpha^3 + \alpha) + (\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + 1$

$\beta\gamma = (\alpha^3 + \alpha)(\alpha^2 + \alpha + 1)$

$= \alpha^5 + \alpha^4 + \alpha^3 + \alpha^3 + \alpha^2 + \alpha$

$= \alpha^5 + \alpha^4 + \alpha^2 + \alpha$

$= (\alpha^2 + \alpha) + (\alpha + 1) + \alpha^2 + \alpha = \alpha + 1$

$\alpha^4 + \alpha + 1 = 0$

$\alpha^4 = \alpha + 1$

$\alpha^5 = \alpha^2 + \alpha$

Questions about Ch. 15, PS07, Practice exam?

15.8: Primitive elements

Useful technical tool: (for pfs Ch.16)

Theorem

If $\text{char}(F) = 0$ *and* K/F *finite, then* $K = F(\alpha)$ *for some* $\alpha \in K$.

α called a **primitive** element for K/F.

Since any finite extension obtained by adjoining finite list, ETS:

Idea of proof. $F(\alpha, \beta) = F(\gamma)$ for $\gamma = \beta + c\alpha$ for all but finitely many $c \in F$. □

So primitive element in practice would look something like:

$$\alpha = c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 + \cdots + c_n\alpha_n$$

i.e., a random lin comb of alpha_1, ..., alpha_n.

Galois theory in a nutshell

Ch. 16

Suppose K/F is the **splitting field** of a polynomial $f(x) \in F[x]$; i.e., an irreducible

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$$

think $F = \mathbb{Q}$

and $K = F(\alpha_1, \dots, \alpha_n)$.

- **Galois theory** relates the field theory properties of K/F (e.g., degree) and the group-theoretic properties of the group of field automorphisms of K fixing F.
- These automorphisms must permute $\alpha_1, \dots, \alpha_n$ and are therefore isomorphic to a transitive subgroup of S_n.
- Signature problem: When can $\alpha_1, \dots, \alpha_n$ be written as a function of the coefficients of $f(x)$ in an expression using only kth roots (generalizing quadatic formula)? If so, $f(x) = 0$ is **solvable by radicals**.

$\sqrt{}, \sqrt[3]{}, \sqrt[4]{}, \dots$

(None of the above proven/solved yet, but this is the goal.)

Conventions in Artin: Cycles and left permutations

We can mostly avoid multiplying explicit permutations, but just to set conventions, permutations will be written in cycle form and multiplied as **left** actions, i.e., from right to left like functions. Random example:

$\alpha = (123)$

$\beta = (145)(23)$

$\alpha\beta = (1452)(3)$

"3 goes through 2 to 3"

last first "1 goes through 4 to 4"

16.1: Elementary symmetric functions

Suppose

$$\prod_{i=1}^{n}(x-u_i) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots \pm s_{n-1}x \mp s_n.$$

Then

elt symm fns relate roots of a polynomial to its coefficients.

$$s_1 = \sum_i u_i = u_1 + \cdots + u_n,$$

$$s_2 = \sum_{i<j} u_iu_j = u_1u_2 + u_1u_3 + \cdots + u_{n-1}u_n,$$

$$s_3 = \sum_{i<j<k} u_iu_ju_k = u_1u_2u_3 + \ldots,$$

$$\vdots$$

$$s_n = u_1u_2\ldots u_n$$

one monomial for each unordered pair {i,j}

unchanged if you permute indices 1,...,n

are the **elementary symmetric functions** in the u_i.

Ex: s_2 for $n=4$

$$s_2 = \sum_{i<j} u_i u_j$$ ← sets of size 2 in $\{1,2,3,4\}$.

$$(x-u_1)(x-u_2)(x-u_3)(x-u_4)$$

2^4 monomials, each from choosing either x or u_i in each line of the product over there <---.

$$= \rightarrow x^2 \cdot u_2 u_4 = u_2 u_4 x^2$$

The x^2 terms come from choosing x twice and u_i twice. So each x^2 term comes from a set {i,j} of size 2 inside {1,2,3,4}.

$$\text{So } s_2 x^2 = (u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4) \cdot x^2$$

Symmetric polynomials in general

R a ring.

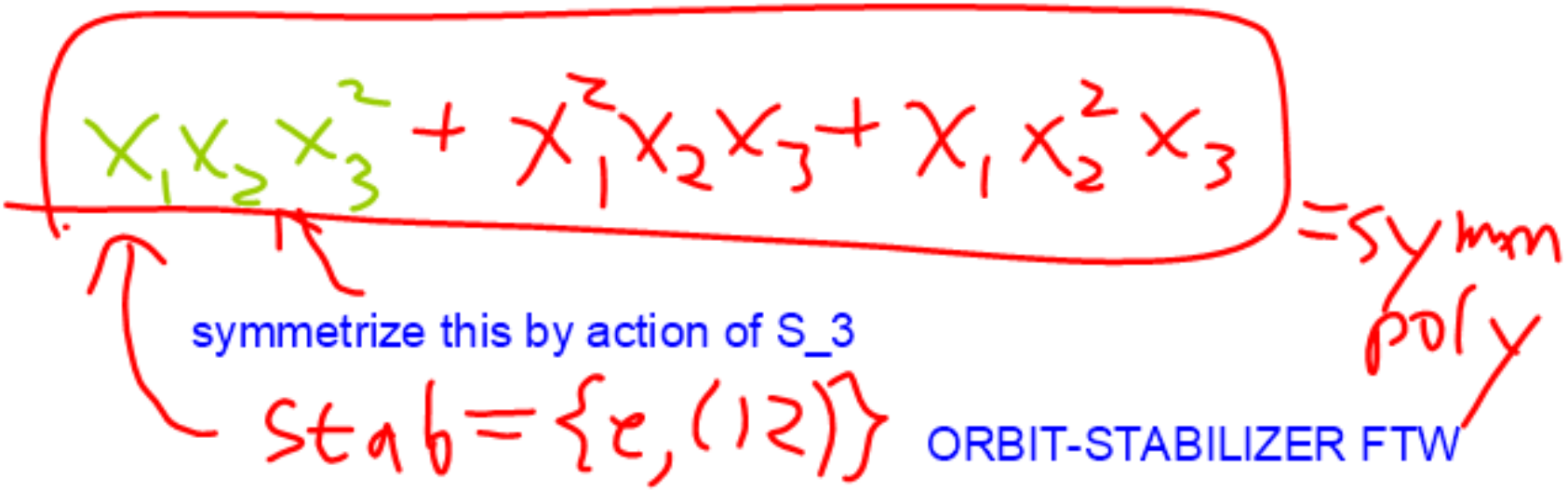
Definition

Note that permutations in S_n act on monomials in $R[u_1, \ldots, u_n]$ by permuting the indices. Action extends to all elements of $R[u_1, \ldots, u_n]$.

To say that $f(u_1, \ldots, u_n) \in R[u_1, \ldots, u_n]$ is a **symmetric polynomial** means that f is fixed by every $\sigma \in S_n$.

Example: Elementary symmetric functions.

Random 3-variable example by symmetrizing:



The Symmetric Functions Theorem

Theorem

If $g(u_1, \ldots, u_n) \in R[u_1, \ldots, u_n]$ is a symmetric polynomial, then g can be written (uniquely) as a polynomial in the elementary symmetric functions $s_1, \ldots, s_n$.

Proof: Boils down to finding a systematic method for rewriting g.

Ex: $u_1^2 u_2 u_3 + u_1 u_2^2 u_3 + u_1 u_2 u_3^2$ in

$s_1 = u_1 + u_2 + u_3$, $s_2 = u_1 u_2 + \cdots$, $s_3 = u_1 u_2 u_3$

A systematic method for rewriting symmetric polynomials

Random example from before ($n = 3$):

$u_1^2 u_2 u_3 + u_1 u_2^2 u_3 + u_1 u_2 u_3^2$

1. Set $u_n = 0$, get a symmetric polynomial g° in $n-1$ variables.
2. Write g° as a polynomial $Q(s_1^\circ, \ldots, s_{n-1}^\circ)$.
3. $g(u_1, \ldots, u_n) - Q(s_1, \ldots, s_{n-1})$ must equal $s_n h$, where h is a symmetric polynomial of smaller degree than g, lather rinse repeat.

1. $g^\circ = 0$ / 2. $Q = 0$

3. $g = s_3(u_1 + u_2 + u_3) = s_3 s_1$

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

$x_3 = 0$ $\quad g^0 = x_1 x_2^2 + x_1^2 x_2 = (x_1 x_2)(x_1 + x_2)$

$= s_2^0 s_1^0 (\text{in } 2 \text{ vars})$

$Q = s_1 s_2$

$= (x_1 + x_2 + x_3)(x_1 x_2 + x_1 x_3 + x_2 x_3)$

$= x_i x_j^2 \text{ terms } (6 \text{ terms})]g$

$+3 x_1 x_2 x_3$

$g - Q = -3 x_1 x_2 x_3 = -3 s_3$

$$g = s_1 s_2 - 3 s_3$$

Try this yourself at home!
(See Artin 16.1 for examples.)

Corollary of the Symmetric Functions Theorem

This is the main reason we care about symmetric polynomials in this course.

Corollary

Suppose $f(x) \in F[x]$,

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$$

and $K = F(\alpha_1, \dots, \alpha_n)$. *If* g *is a symmetric polynomial in* n *variables, then* $g(\alpha_1, \dots, \alpha_n) \in F$.

Proof. If g is an elementary symmetric function,

16.2: The discriminant

Suppose

$$\prod_{i=1}^{n}(x-u_i) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots \pm s_{n-1}x \mp s_n$$

in $\mathbb{Z}[u_1, \ldots, u_n]$.
Discriminant is defined to be

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

- By Symmetric Functions Thm, D can be written as an integer polynomial in $s_1, \ldots, s_n$.
- If $\alpha_1, \ldots, \alpha_n \in K$, $D(\alpha) = 0$ iff some $\alpha_i = \alpha_j$.

Δ in terms of elementary symmetric functions: Degree 2

$$(x - u_1)(x - u_2) = x^2 - s_1 x + s_2.$$

$$D(u) = (u_1 - u_2)^2$$

Δ in terms of elementary symmetric functions: Degree 3

$$(x-u_1)(x-u_2)(x-u_3) = x^3 - s_1x^2 + s_2x - s_3.$$

This discriminant is too complicated to remember. However, after change of variables, can assume polynomial is $x^3 + px + q$, in which case D simplifies to:

$$D(u) = -4p^3 - 27q^2.$$