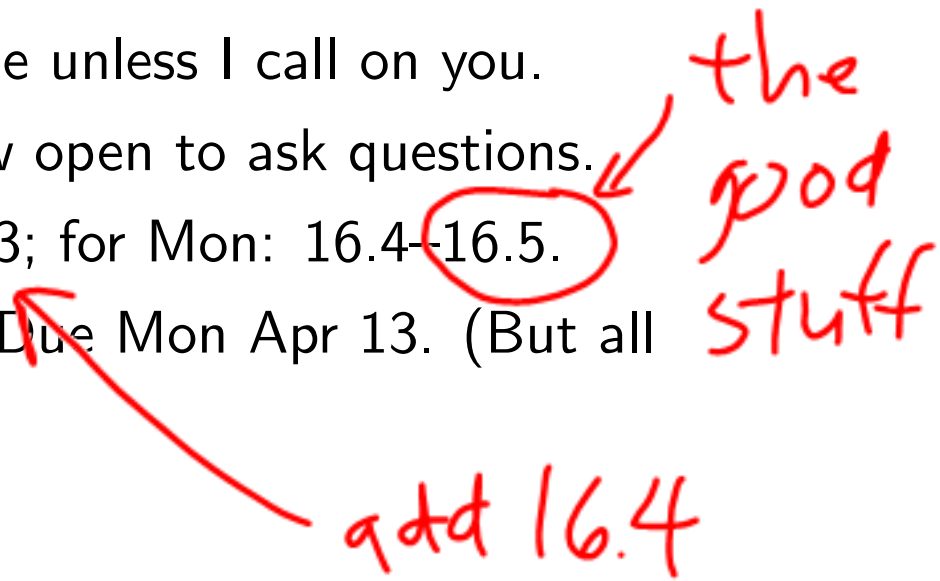
Welcome back

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: 16.2–16.3; for Mon: 16.4–16.5.
- Exam 2: Due today; PS08: Due Mon Apr 13. (But all deadlines are elastic.)

Problem session Fri 10:30 by Zoom



Galois theory in a nutshell

Think: F = Q

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

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

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**.

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

today

16.1: Elementary symmetric functions

point of elt symm fns: express coeffs of a poly as a fn of its roots

$$\prod_{i=1}^{n}(x-u_i) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots \pm s_{n-1}x \mp s_n.$$

Elementary symmetric functions are:

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

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

$$s_3 = \sum_{i<j<k} u_i u_j u_k = u_1u_2u_3 + \ldots,$$

$$\vdots$$

$$s_n = u_1 u_2 \ldots u_n$$

Geh!

not inv't

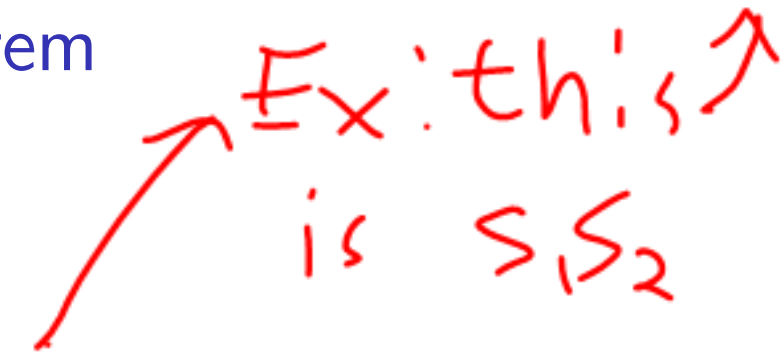
$n=2$:

$u_1^2u_2 + u_1u_2^2$

invariant

$f(u_1,\ldots,u_n)$ **symmetric** when f invariant under S_n.

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 $s_1, \ldots, s_n$.

Main application:

Corollary

Suppose $f(x) \in F[x]$, i.e., K is splitting field of f

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

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

E.g., if F=Q, then plugging the roots of f(x) into the symm poly g gives you a rational number. (!!!!)

Ex.: f(x) = x^2 - 3, so $\alpha_1 = \sqrt{3}$, $\alpha_2 = -\sqrt{3}$

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

$g(\sqrt{3}, -\sqrt{3}) = 3(-\sqrt{3}) + (-\sqrt{3})^2\sqrt{3} = 0$

Try: $\frac{-1 \pm \sqrt{3}}{2}$, etc. Try it yourself!

ω, ω^2, where $\omega^3 = 1$

Pf of corollary: Since g is a symmetric polynomial, by Symm Fns Thm, g is a polynomial function of elementary symmetric functions.
But if you plug $\alpha_1, \ldots, \alpha_n$ into an elementary symmetric function,

you get one of the coefficients of f(x), i.e., an element of F.

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 $\mathbb{Z}[u_1, \ldots, u_n]$.

Expository master's thesis project: symm polynomials and generalizations

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 $s_1, \ldots, s_n$. (b/c D is a symmetric polynomial)
- If $\alpha_1, \ldots, \alpha_n \in K$, $D(\alpha) = 0$ iff some $\alpha_i = \alpha_j$.

Idea: D detects repeated roots.

Δ in terms of elementary symmetric functions: Degree 2

D = disc in u_i (roots); Δ = disc in s_i (coeffs)

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

$x^2 - bx + c$ $\quad s_1 = u_1 + u_2$ $\quad s_2 = u_1 u_2$

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

$$= u_1^2 - 2u_1u_2 + u_2^2$$

$$= (u_1+u_2)^2 - 4u_1u_2 = s_1^2 - 4s_2$$

$$= b^2 - 4c$$

Observe: If D = 0, then quadratic formula becomes x = -b/(2a).

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:

$$D(u) = (u_1-u_2)^2(u_1-u_3)^2(u_2-u_3)^2$$

$$\Delta(p,q) \quad D(u) = -4p^3 - 27q^2.$$

We'll see later that, just as discriminant determines how complicated the quadratic formula is for degree 2, discriminant determines how complicated the cubic and quartic formulas appear in degrees 3 and 4.

16.3: Splitting fields

Definition (f might not be irreducible)

To say that K/F is the **splitting field** of $f(x) \in F[x]$ means

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

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

Straightforward consequences:

- Every $f(x) \in F[x]$ has a splitting field. Pf: Add roots until f factors.
- Every finite extension is contained in a splitting field.

Pf: Finite extension is obtained by adjoining finitely many elts.
Only finitely many min polynomials to consider, so split all of them
(or rather, split their product).

Non-example: Take $K = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$

$f(x) = x^3 - 2$ in $\mathbb{Q}$.

$= (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}\,x + (\sqrt[3]{2})^2)$

factors once but does not split b/c other roots of f are complex. So K is not a splitting field of f, and Splitting Thm (see below) does not apply. (As we'll see, it follows from Splitting Thm that K is not a splitting field of *anything*.)

We'll soon think of non-splitting fields as being "not normal" (pun intended).

The Splitting Theorem

Theorem

So it's not just f that splits in K, it's any poly w/any root in K.

Suppose K/F is a splitting field of $f(x) \in F[x]$. If $g(x) \in F[x]$ is irreducible and has at least one root in K, then $g(x)$ splits in K.

Idea of Proof. Suppose $\beta_1 \in K$, $g(\beta_1) = 0$.

b/c β_1 in K

- Splitting field: $K = F(\alpha_1, \ldots, \alpha_n)$ (α_i the roots of $f(x)$).
- So there exists $p_1(u_1, \ldots, u_n)$ such that $p_1(\alpha_1, \ldots, \alpha_n) = \beta_1$.
- S_n acts on polynomials in n vars. Let orbit of p_1 under that action be $\{p_1, \ldots, p_k\}$, and let $\beta_i = p_i(\alpha_1, \ldots, \alpha_n)$.
- Let

$$h(x) = (x - \beta_1)\ldots(x - \beta_k) = x^k - b_1 p^{k-1} + b_2 p^{k-2} - \ldots.$$

gcd(g,h) ≠ 1

ETS $h(x)$ has coeffs in F, for then, since $g(x)$ has common factor with $h(x)$ and is irreducible over F, g divides h.

- Long story short: Each b_i is a symmetric function of $\alpha_1, \ldots, \alpha_n$, so is a polynomial in coefficients of f (Symmetric Functions Theorem), which are in F.

16.4 Isomorphisms of field extensions

Definition

An F-**isomorphism** $\sigma : K/F \to K'/F$ is an isomorphism fixing F. If $K = K'$, get a F-**automorphism** (symmetry of K/F).

Definition

$G(K/F)$ is the group of all F-automorphisms of K/F, called the **Galois group** of K/F.

Definition

To say a finite extension K/F is a **Galois extension** means that $|G(K/F)| = [K : F]$. (As we'll see, this is largest possible.)

Example: Complex conjugation is an $\mathbb{R}$-automorphism of the extension $\mathbb{C}/\mathbb{R}$, and $\mathbb{C}/\mathbb{R}$ is a Galois extension.
Example: If d square-free, $a + b\sqrt{d} \mapsto a - b\sqrt{d}$ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$, and $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ is Galois.
Example: (to be proven) $\left|G(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})\right| = 1$, so $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not Galois.

First facts about F-isomorphisms

1. $\sigma : K/F \to K'/F$ an F-isomorphism, $f(x) \in F[x]$. If α is a root of f in K, then $\sigma(\alpha)$ is a root of f in K'.
2. Suppose $K = f(\alpha_1, \ldots, \alpha_n)$. An F-isomorphism is determined by the images of $\alpha_1, \ldots, \alpha_n$; in particular, if σ is an automorphism of K/F that fixes $\alpha_1, \ldots, \alpha_n$, then σ is the identity.
3. Suppose $f(x) \in F[x]$ irreducible, α, α' roots of f in $K/F, K'/F$. There exists a unique F-isomorphism $\sigma : F(\alpha) \to F(\alpha')$ such that $\sigma(\alpha) = \alpha'$.

So for example, if $K = f(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f over F and $\alpha_1, \ldots, \alpha_n$ are all of the roots of f, then we can think of elements of $G(K/F)$ as permutations of $\alpha_1, \ldots, \alpha_n$.

More about splitting fields

Theorem

If K_1/F, K_2/F are splitting fields of $f \in F[x]$, then K_1/F and K_2/F are F-isomorphic.

Proof. First show that any L/F contains at most one splitting field of f over F:

Primitive Elt Thm says that $K_1 = F(gamma)$. Let $g(x)$ be irreducible poly of γ over F.
Let $L \supseteq K_2$ contain a root γ' of g, let $K' = F(\gamma')$.

Questions? HW, sample exam, etc.