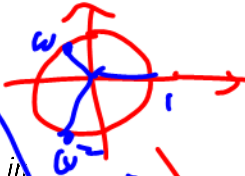
Math 128B, Mon Mar 22

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: Ch. 20. Reading for Wed: Ch. 21.
- PS06 due tonight. Late deadline Fri Mar 26.
- **Exam 2 on Wed Apr 07**, on Chs. 15–19 (PS04–06). Review session Mon Apr 05 (recorded to YouTube).

Recap



$\omega^3 = 1$

Theorem

F a field, $p(x) \in F[x]$ irreducible. Then p has a zero in $F[x]/\langle p(x)\rangle$. $= F(\alpha)$, α root of $p(x)$.

Definition

$f(x) \in F[x]$, $\deg f = k > 0$.

some ext of F

- To say f **splits** in E means that

$$f(x) = a(x - a_1)\cdots(x - a_k)$$

  for some $a_1, \ldots, a_k \in E$

- If also $E = F(a_1, \ldots, a_k)$, we say that E is a **splitting field for f over F**.

Example: If $\omega = e^{2\pi i/3}$, $\alpha = \sqrt[3]{7}$, then splitting field of $x^3 - 7$ over $\mathbf{Q}$ is $\mathbf{Q}(\alpha, \alpha\omega, \alpha\omega^2) = \mathbf{Q}(\alpha, \omega)$.

$x^3 - 7 = (x-\alpha)(x-\alpha\omega)(x-\alpha\bar{\omega})$

Why do we care about splitting fields?

The basic question of the entire semester is:

$$\textit{Solve } f(x) = a_n x^n + \cdots + a_1 x + a_0 = 0 \textit{ over } F.$$

IDEA: Instead of looking at the (finite) solution set $\cancel{a_1, \ldots, a_k}$ to $f(x) = 0$, study the splitting field $\cancel{F(a_1, \ldots, a_k)}$.

$\alpha_1 \cdots \alpha_k$

$F(\alpha_1 \ldots \alpha_k)$

We can use then algebraic structures like fields, vector spaces (!), and finite groups (!?!) to learn more about $\cancel{F(a_1, \ldots, a_k)}$, and therefore, about $\cancel{a_1, \ldots, a_k}$

$F(\alpha_1 \ldots \alpha_k)$

$\alpha_1 \ldots \alpha_k$.

Our next goal

Show that we can replace each "a splitting field" with "**the** splitting field."

I.e., we will show that every polynomial in $F[x]$ has a splitting field ~~in $F[x]$~~, and that any two splitting fields of $f(x)$ over F are isomorphic.

over F

Existence of splitting fields

Theorem
$f(x) \in F[x]$, $\deg f > 0$. *Then there exists a splitting field E for $f(x)$ over F.*

Why:

- Construct $F(\alpha)$, α zero of $f(x)$.
- Over $F(\alpha)$, $f(x) = g(x)(x-\alpha)$
- Induction on degree ($\deg g = \deg f - 1$)
  $\Rightarrow \exists$ ext in which f factors
- Then $E = F(\alpha_1, \ldots, \alpha_k)$.

Ex. $F = \mathbb{Q}$, $f(x) = x^3 - 7$ $\quad \alpha = \sqrt[3]{7}$, $\omega = e^{\frac{2\pi i}{3}}$

Over $\mathbb{Q}(\alpha)$:

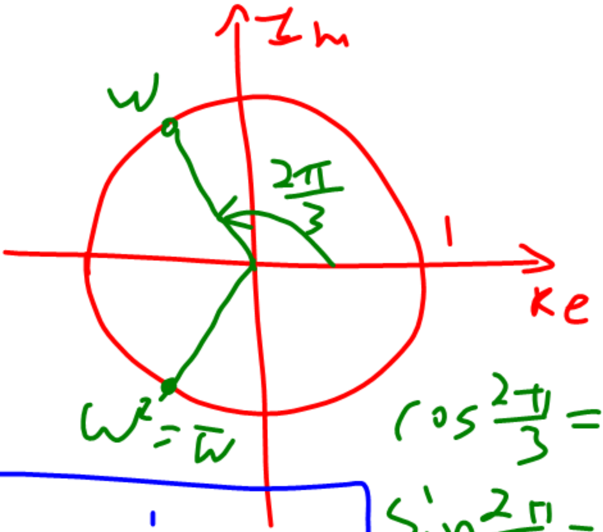
$$f(x) = (x-\alpha)(x^2 + \alpha x + \alpha^2)$$

Over $\mathbb{Q}(\alpha, \alpha\omega) = \mathbb{Q}(\alpha, \omega)$: $\left(\omega = \frac{\alpha\omega}{\alpha}\right)$

$$f(x) = (x-\alpha)(x-\alpha\omega)(x-\alpha\omega^2)$$

$\mathbb{Q}(\alpha, \omega)$ is sp. field for f.

$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$; $\omega^2 = \overline{\omega}$



$\cos \frac{2\pi}{3} = -\frac{1}{2}$

$\sin \frac{2\pi}{3} = \frac{\sqrt{3}}{2}$

This says:

$\mathbb{Q}(\alpha) \approx \mathbb{Q}(\alpha\omega)$

Adjoining one root (towards uniqueness of splitting fields)

Theorem

F a field, $p(x) \in F[x]$ irreducible over F. If E is an extension of F, $a \in E$, and $p(a) = 0$, then

$$F(a) \approx F[x]/\langle p(x) \rangle .$$

Point: The structure of this field is independent of which zero you pick!

Claim 1: Kernel of substitution homomorphism $\varphi : F[x] \to F(a)$ given by $\varphi(f(x)) = f(a)$ is: $\ker\varphi = \langle p(x) \rangle$

$p(a)=0$, so $p \in \ker\varphi$

$\ker\varphi$ ideal of $F[x] \Rightarrow \ker\varphi = \langle g(x) \rangle$

So $g(x)$ div $p(x) \Rightarrow g(x)$ is assoc of $p(x)$

or g is a unit

~~**Claim 2:** Image of φ is:~~

If g is a unit, $\langle g(x) \rangle = F[x]$, which is impossible b/c nonzero const polys aren't in $\ker\varphi$.

So g is an assoc of $p(x)$

$\Rightarrow \ker\varphi = \langle p(x) \rangle$.

<u>Claim 2</u>: $\operatorname{Im}\varphi = F(a)$

Plug in a, so $\operatorname{im}\varphi \subseteq F(a)$

But $\varphi(x) \mapsto a$, and $\operatorname{im}\varphi$ is a field, so $F(a) \subseteq \operatorname{im}\varphi$.

1IT $\quad F(a) \cong F[x]/\langle p(x) \rangle$

Uniqueness of splitting fields

From previous result:

Corollary

$p(x) \in F[x]$ irreducible over F. If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F, then $F(a) \approx F[x]/\langle p(x)\rangle \approx F(b)$.

Long story short, carefully applying the above corollary repeatedly (or inductively) gives:

Corollary

Any two splitting fields of $f(x) \in F[x]$ are isomorphic.

A thing you weren't even worried about, but. . .

Suppose $f(x)$ irreducible over F, E splitting field of $f(x)$ over F.

Weird question: Is it possible that $f(x)$ has repeated roots in E?

irred in $F[x]$

Example: Consider $E = \mathbf{Z}_5(t)$, $F = \mathbf{Z}_5(t^5)$, $f(x) = x^5 - t^5$.

$t^5 \in F$

$\frac{f(x)}{g(x)}$ $(f, g \in \mathbb{Z}_5[t])$

Same, but $f, g \in \mathbb{Z}_5[t^5]$

Observe:

$(x-t)^5 = x^5 - 5x^4t + 10x^3t^2 - 10x^2t^3 + 5xt^4 - t^5$

$= x^5 - t^5$

So $f(x)$ has one zero, t, mult 5 in E.

Surprise! The derivative

If $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \in F[x]$, we define

(e.g. $F = \mathbb{Z}_5$)

$$f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

Fact: Sum rule, constant multiple rule, and product rule all work for derivative in $F[x]$.

Theorem: $f(x) \in F[x]$. Then TFAE:

1. f has a multiple zero in some extension E of F.
2. $\gcd(f(x), f'(x))$ has degree ≥ 1.

<u>Pf</u> (1) $\Rightarrow$ (2)

If $f(x) = (x-\alpha)^2 g(x)$ in $E[x]$

then $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$

So $(x-\alpha)$ is a CD of f, f' in $E[x]$.

$\Rightarrow$ gcd(f, f') in $F[x]$ can't be 1;

b/c if gcd$(f, f') = 1$

$\Rightarrow$ $p(x)f(x) + q(x)f'(x) = 1$

and $x - \alpha$ would divide

both sides, contra.

When do irreducibles have multiple zeros?

Suppose $f(x)$ irreducible over F.

- If char $F = 0$, then f has no multiple zeros.
- If char $F = p$, then f has multiple zeros iff $f(x) = g(x^p)$ for some $g \in F[x]$.

Proof:

Perfect fields

Definition

F is **perfect** when either char $F = 0$ or char $F = p$ and $F^p = F$.

Theorem

Let F be a finite field of characteristic p. Then F is perfect.

Proof: Follows from fact of independent interest:

> *Claim: The map $\rho : F \to F$ given by $\rho(x) = x^p$ is an automorphism of F.*

No multiple zeros over a perfect field

Theorem

If F is perfect and $f(x) \in F[x]$ irreducible, then f does not have multiple zeros in any extension of F

Proof: Characteristic 0 case done, so suppose char $F = p$ and F is perfect.

What happens over imperfect fields?

Theorem

$f(x)$ irreducible over F and E the splitting field of f over F. Then all zeros of f have the same multiplicity.

Corollary

$f(x)$ irreducible over F and E the splitting field of f over F. Then there exists n such that

$$f(x) = (x - a_1)^n \dots (x - a_t)^n,$$

where $a_1, \dots, a_t$ are distinct elements of E.

Example, again: $E = \mathbf{Z}_5(t)$, $F = \mathbf{Z}_5(t^5)$, $f(x) = x^5 - t^5$.