Math 128B, Wed Mar 24

- 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. 21.
- **Exception 2 on Wed Apr 07**, on Chs. 15–19 (PS04–06). Review session Mon Apr 05 (recorded to YouTube).

3pm

Recap: A thing you weren't even worried about

$$\begin{array}{c} E \\ | \\ F \end{array}$$

Suppose $f(x)$ irreducible over F, E splitting field of $f(x)$ over F.
Is it possible that $f(x)$ has repeated roots in E?

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

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

algebraic derivative

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

1. f has a multiple zero in some extension E of F.
2. $\underbrace{\gcd(f(x), f'(x))}_{\text{Computed in } F[x]}$ has degree ≥ 1.

Why: B/c of the product rule!

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 $g \in F[x]$.

(Nonzero terms of f are all powers of x^p
= terms of the form x^{kp})

Proof:

In general (char p or char 0), f ' will have smaller degree than f, so the only way that gcd(f,f ') can have degree >= 1 is if f ' = 0.

Char 0: Irred has deg ≥ 1, so $f' \neq 0$.

Char p: $(cx^{kp})' = c(kp\,x^{kp-1}) = 0$

So if $f(x) = g(x^p)$, $f' = 0$.

$p = 0$ in F

OTOH, if $n \not\equiv 0 \pmod p$, then

$$(cx^n)' = cnx^{n-1} \neq 0$$

$(c \neq 0)$

So any terms not cx^{kp} give $f' \neq 0$.

Ex. $p=5$

$$(x^{20}+3x^{10}+x^5+4)' = 20x^{19}+30x^9+5x^4$$
$$= 0+0+0 = 0$$

Perfect fields

I.e., every element of F is a pth power of something in F.

Definition

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

F^p=F as if-then: If y in F, then y = x^p for some x in 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. (Frob. autom. of F)

Homom $\rho(xy) = (xy)^p = x^p y^p = \rho(x)\rho(y)$

$\rho(x+y) = (x+y)^p$

$p = \operatorname{char} F$

so $p = 0$ in F

$$= x^p + \underbrace{\binom{p}{p-1} x^{p-1} y + \cdots + \binom{p}{1} x y^{p-1}}_{=0 \text{ in } F} + y^p$$

$$= x^p + y^p = \rho(x) + \rho(y)$$

$$\boxed{\text{In } \mathbb{Z}_p\text{: We'll see } x^p = x \ \forall x \in \mathbb{Z}_p}$$

<u>Biject</u>

$$\ker \rho = \{x \in F \mid x^p = 0\} = \{0\}$$

So ρ injective.

B/c ρ inj, F finite, ρ bij. (Pigeon)

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.

S'pose $f' = 0$. Then

$f(x) = a_{kp}x^{kp} + a_{(k-1)p}x^{(k-1)p} + \cdots + a_p x^p + a_0$

B/c F perfect, each $a_i = b_i^p$ for $b_i \in F$

So

$$f(x)$$

$$= b_{kp}^{p} x^{kp} + \cdots + b_p^{p} x^{p} + b_0^{p}$$

$$= \left(b_{kp} x^{k} + \cdots + b_p x + b_0\right)^{p}$$

$$= (g(x))^{p}$$

contradicting the fact that f is irreducible.

Later, we'll see: only f.f.s

$\exists$ unique field order p^k for all primes p, $k \geq 1$.

Called $GF(p^k)$ ($\neq \mathbb{Z}_{p^k}$)

Constructed like field order 125.

(∞ perfect: $\mathbb{Z}_5(t)$ perfect, char 5)

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

$$(x^5 - t^5) = (x - t)^5$$

Algebraic vs. transcendental extensions

E extension of a field F, $a \in E$.

If $f(a) = 0$ for some nonzero $f(x) \in F[x]$, we say a is **algebraic** over F;
otherwise, we say a is **transcendental** over F.

If every $a \in E$ is algebraic over F, we say E is an **algebraic extension** of F;
otherwise we say E is a **transcendental extension** of F.

If $E = F(a)$ for some $a \in E$, we say that E is a **simple** extension of F.

single

Ex $F = \mathbb{Q}$, $E = \mathbb{C}$

$\sqrt[3]{13}$ alg. b/c $f(x) = x^3 - 13 \in \mathbb{Q}[x]$ and $f(\sqrt[3]{13}) = 0$.

π transc. over $\mathbb{Q}$ ($\pi + e$?)

e " " $\mathbb{Q}$

$F = \mathbb{Q}(\pi^5)$ $E = \mathbb{Q}(\pi)$

$$\begin{array}{c} \mathbb{Q}(\pi) \\ | \\ \mathbb{Q}(\pi^5) \end{array}$$

π algebraic over F b/c zero of $x^5 - \pi^5$.

$\mathbb{Q}(\sqrt[3]{13})$ alg ext of $\mathbb{Q}$

$\mathbb{Q}(\pi)$ transc. " " $\mathbb{Q}$

$\mathbb{C}$ transc. ext of $\mathbb{Q}$

$\overline{\mathbb{Q}}$ = alg closure of $\mathbb{Q}$

= $\mathbb{Q}$(all alg $\alpha \in \mathbb{C}$)

$\overline{\mathbb{Q}}$ alg ext of $\mathbb{Q}$.

$\#$ thy: $\overline{\mathbb{Q}}/\mathbb{Q}$

The minimal polynomial of $a \in E$

$$\begin{array}{c} a \in E \\ | \\ F(a) \\ | \\ F \end{array}$$

Theorem: E extension of F, $a \in E$.

1. If a transcendental over F, then $F(a) \approx F(x)$.

2. If a algebraic over F, there exists a monic $p(x) \in F[x]$ such that: l.c. $= 1$
   - $F(a) \approx F[x]/\langle p(x) \rangle$;
   - $p(x)$ is the monic polynomial of smallest degree such that $p(a) = 0$;
   - $p(x)$ is irreducible over F; and
   - If $f(x) \in F[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $F[x]$.

Example: 1. $\mathbb{Q}(\pi) \approx \mathbb{Q}(x)$ $\dfrac{\pi^5+3\pi-7}{2\pi^4+8}$

2. $\mathbb{Q}(\sqrt[3]{13}) \approx \mathbb{Q}[x]/\langle x^3-13 \rangle$

Proof of minimal polynomial (algebraic case)

Degree of an extension

E an extension of F.

Recall that the whole point of abstract vector spaces is that E is a v.s. over F. To say that E has **degree** n over F, written $[E : F] = n$, means that $\dim E = n$ as a v.s. over F.

If $[E : F]$ is finite, then we say E is a **finite extension of** F; otherwise, E is an **infinite extension of** F.

Examples: (without proof)

A key class of examples

If $p(x)$ irreducible over F, $E = F[x]/\langle p(x) \rangle$, then $[E : F] = \deg p(x)$.

Proof:

Finite extensions are algebraic

Theorem

If E is a finite extension of F, then E is an algebraic extension of F.

Proof:

Theorem (Multiplicativity)

K finite extension of E, E finite extension of F. Then

$$[K : F] = [K : E][E : F] < \infty.$$

Proof of Multiplicativity

Example: $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ and $\mathbf{Q}(\sqrt{3} + \sqrt{5})$

Example: Splitting field of $x^3 - 7$ over $\mathbf{Q}$

Primitive element theorem

Generalizing $\mathbf{Q}(\sqrt{3}+\sqrt{5})$:

Theorem

F a field with $\operatorname{char} F = 0$ *(and therefore F infinite). If a, b algebraic over F, then there exists $c \in F(a, b)$ such that $F(c) = F(a, b)$.*

Idea of proof: $c = a + db$ for (basically) random $d \in F$ works.

- If $p(x)$ is min poly of a over F, $q(x)$ is min poly of b over F, and $r(x) = p(c - dx)$, there are only finitely many $d \in F$ that allow $q(x)$ and $r(x)$ to have common zeros other than b. Avoid those.
- That implies that the (irreducible) min poly $s(x)$ of b over $F(c)$ has only one zero, and because $F(c)$ has char 0, must have $s(x) = x - b$ (no repeated zeros in an irreducible), i.e., $b \in F(c)$.