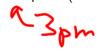
Math 128B, Wed Mar 24

- ▶ 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.
- ► Exam 2 on Wed Apr 07, on Chs. 15–19 (PS04–06). Review session Mon Apr 05 (recorded to YouTube).





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
$$f(x) = a_n x^n + \dots + a_2 x^2 + a_1 x + a_0 \in F[x]$$
, we define algebraic derivative $f'(x) = n a_n x^{n-1} + \dots + 2 a_2 x + a_1$.

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 .

Computed in F[x]

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 are all powers of x^p = terms of the form x^k

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.

OTOHit nto (matp), then (cxn)= cnxn-1 = 0 (c#0) So gry terms not cxtp give f + 0. $\frac{1}{\pm x \cdot p} = 5$ (x20+3x10+x5+4)=20x19+30x1+5x7 = 0+0+0=0

Perfect fields

Definition

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

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

Theorem

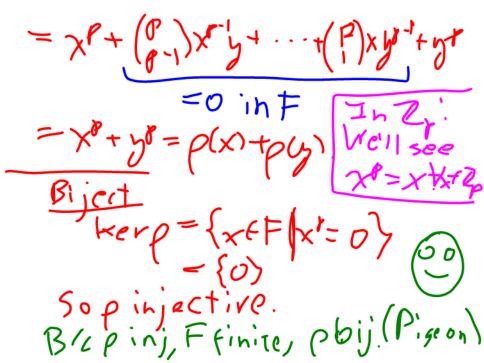
 $F^p=F$ as if-then: If y in F, then y = x^p for some x in F.

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. and σ w. of F)

 $\frac{t_{lomon}}{\rho(x+y)} = (xy)^p = x^p y^p = \rho(x)\rho(y)$ $\rho(x+y) = (x+y)^p \qquad p = charf$ sop=0



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.

$$f(x) = b_{kp} x^{kp} + \cdots + b_{0}^{p} x^{0} + b_{0}^{p}$$

$$= (b_{kp} x^{k+1} - \cdots + b_{p} x + b_{0})^{p}$$

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

contradicting the fact that f is irreducible.



0 h/y t.f. 5 2 Lder, we'll ser! I unique field order pt tor all primes p, t 21. Called GF(pt)(#Zpt) Constructed like field order 125. (pertect : Zs(t) portet, chars)

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, \ldots, a_t are distinct elements of E.

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

Algebraic vs. transcendental extensions

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

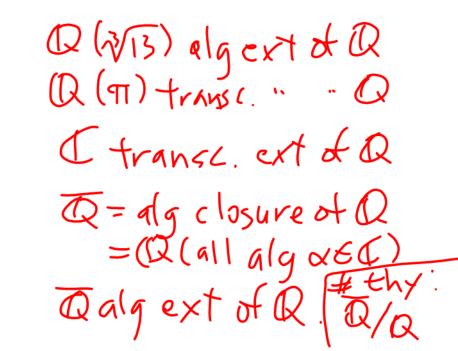
If f(a) = 0 for some nonzero $f(x) \in F[x]$, we say a is algebraic over F; otherwise, we say a is **transcendental** over F.

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.

EFQ, E=C 7813 alg. 6/2 ((x)=x3-13+Q[x] ~~~ (3/5)=0. TT transc. overa (TteP) Q(11) F=Q(TS) E=Q(T)
T algebraic over F b/c
zero of x5-TS. Rand



The minimal polynomial of $a \in E$

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

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



If a algebraic over F, there exists a monic $p(x) \in F[x]$ such that:

- $ightharpoonup F(a) \approx F[x]/\langle p(x)\rangle;$
 - ▶ p(x) is the monic polynomial of smallest degree such that p(a) = 0;
 - \triangleright 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: (,
$$Q(\eta) \approx Q(x)$$
 $\frac{\pi}{2\pi^4+8}$ 2. $Q(3/3) \approx Q(x)/(x^3-13)$

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 **Q**

Primitive element theorem

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

Theorem

F a field with 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., $b \in F(c)$.