# Math 128B, Mon Apr 05

- 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.
- Review session tonight, 3pm (recorded to YouTube).
- **Exam 2 on Wed Apr 07**, on Chs. 15–19 (PS04–06).

Office hours link!

# 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 (single) $a \in E$, we say that $E$ is a **simple** extension of $F$.

# The minimal polynomial of $a \in E$

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

If $a$ transcendental over $F$, then $F(a) \approx F(x)$. Field of rational functions in the variable x

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

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

**Why (algebraic case):** Let $I$ be the set of all $f(x)$ such that $f(a) = 0$.

$f(x) \mapsto f(a)$

$I$ is the kernel of a homomorphism, so $I = \langle p(x)\rangle$ and $p(x)$ is irreducible.

**Ex** (w/o pf)

$F = \mathbb{Q}$

$a = \sqrt{2}$ : min poly is $x^2 - 2$

$$\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/\langle x^2 - 2\rangle$$

---


$\omega = e^{\frac{2\pi i}{3}}$ : min poly $x^2 + x + 1 = \dfrac{x^3 - 1}{x - 1}$

$$\mathbb{Q}(\omega) \simeq \mathbb{Q}[x]/\langle x^2 + x + 1\rangle$$

# 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)

$[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$

Min poly:

$x^3 - 7$

$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$

$x^2 + x + 1$

$(\omega = e^{\frac{2\pi i}{3}})$

$E = \mathbb{Q}(\sqrt[3]{7})$ as a v.s. over $\mathbb{Q}$:

We'll show $\{1, 7^{1/3}, 7^{2/3}\}$ is a basis for $E$ over $\mathbb{Q}$

So: every elt of $E$ written uniquely as

$$a + b \cdot 7^{1/3} + c\, 7^{2/3}$$

$(a, b, c \in \mathbb{Q})$

# A key class of examples

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

basis
span l.i.
l.c.

**Proof:** $I = \langle p(x) \rangle$ $\alpha = x + I$

$n = \deg p(x)$ $\alpha^k = x^k + I$

Claim $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $E$ over $F \Rightarrow [E:F] = n$

$\boxed{\text{Span}}$ For $f(x) + I \in F[x]/I$,

$f(x) = q(x)p(x) + r(x)$ $\deg r < \deg p$

So mod $p(x)$, $f(x)+I = r(x)+I$

$= r(\alpha)$.

I.e. $f(x)+I = c_0 1 + c_1\alpha^1 + \cdots + c_{n-1}\alpha^{n-1}$ for some $c_i \in F$. So $\{1, \ldots, \alpha^{n-1}\}$ spans.

---

l.i. S'pose $c_i \in F$

(*) $c_0 1 + c_1 \alpha^1 + \cdots + c_{n-1}\alpha^{n-1} = 0$

Let $f(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in F[x]$

$f(\alpha)=0$. But $p$ is minpoly of $\alpha$,
so $p(x)$ div $f(x)$, $\deg f < \deg p$
$\Rightarrow f(x)=0$.

(C) $c_0 = 0, c_1 = 0, \ldots, c_{n-1} = 0$

---

$\mathbb{Q}(2) \simeq \mathbb{Q}[x]/\langle x-2\rangle$
$\simeq \mathbb{Q}$

---

$[E:F]=1 \Leftrightarrow E=F$
$(E = F[x]/\langle p(x)\rangle) \Leftrightarrow \deg p = 1$

# Finite extensions are algebraic

$[E:F] = n < \infty$

$\mathbb{Q}(\sqrt[3]{5})$ deg 3 over $\mathbb{Q}$

**Theorem**

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

**Proof:** A $a \in E$

Consider $\{1, a, \ldots, a^n\}$

Has size $n+1$, so lin dep.

So $\exists c_i$ s.t. $c_0 + c_1 a + \cdots + c_n a^n = 0$

(not all 0)

C $\exists f(x) \in F[x]$ s.t. $f(a) = 0$, $f \neq 0$, $\deg f \leq n$.

Ex: $6 - 5\sqrt[3]{5}$ is zero of $f(x)$, $\deg f \leq 3$.

**Theorem (Multiplicativity)**

~~*$K$ finite extension of $E$, $E$ finite extension of $F$. Then*~~

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

To find min poly of $(6-5\sqrt[3]{7})$:

$E=\mathbb{Q}(\sqrt[3]{7})$

$1=1$

$a=6-5\sqrt[3]{7}$

$a^2=36-60\sqrt[3]{7}+25(7^{2/3})$

$a^3=216-3(180)7^{1/3}+3(150)7^{2/3}+25(7)$

$=-659-540(7^{1/3})+450(7^{2/3})$

$= a$

$(1,0,0)$

$(6,-5,0)$

$(36,-60,25)$

$(-659,$
$-540$
$450)$

# ~~Proof~~ of Multiplicativity

Sketch

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

$[K:F] = \underbrace{[K:E]}_{n}\underbrace{[E:F]}_{d}$

MULTIPLICATIVITY

S'pose

$\{\alpha_1, \ldots, \alpha_n\}$ basis for $K$ over $E$

$\{\beta_1, \ldots, \beta_d\}$ " " $E$ over $F$

Want a basis for $K$ over $F$ w/ $nd$ elts.

$$\mathcal{B} = \{\alpha_1\beta_1, \ldots, \alpha_1\beta_d,$$
$$\alpha_2\beta_1, \ldots, \alpha_2\beta_d$$
$$\vdots$$
$$\alpha_n\beta_1, \ldots, \alpha_n\beta_d\}$$

Show $\mathcal{B}$ spans $K$ (over $F$) ✓

lin ind (over $F$).

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

$$\begin{array}{lll} & \mathbb{Q}(\sqrt{3},\sqrt{5}) = K & \\ & \quad 2 \,| & \{1, \sqrt{5}\} \\ 4 & \mathbb{Q}(\sqrt{3}) \supset E & \\ & \quad 2 \,| & \{1, \sqrt{3}\} \\ & \mathbb{Q} = F & \end{array}$$

Basis for $K/F$:

$\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$

So: Every elt of $\mathbb{Q}(\sqrt{3},\sqrt{5})$ is $a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}$ uniquely. $(a,b,c,d \in \mathbb{Q})$

Min poly of $\sqrt{3}+\sqrt{5}=\alpha$

$1=1$

$\alpha = \sqrt{3}+\sqrt{5}$

$\alpha^2 = 3+2\sqrt{15}+5 = 8+2\sqrt{15}$

$\alpha^3 = 3\sqrt{3}+3(3)\sqrt{5}+3\sqrt{3}5+5\sqrt{5}$

$= 18\sqrt{3}+14\sqrt{5}$

$\{1, \alpha^2, \alpha^4\}$ lin dep

$\alpha^4 = 64+32\sqrt{15}+60$

$= 124+32\sqrt{15}$

# 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* 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., $b \in F(c)$.

# Algebraic over algebraic is algebraic

Theorem

*If $K$ is an alg ext of $E$ and $E$ is an alg ext of $F$, then $K$ is an alg ext of $F$.*

**Proof:** Suppose $a \in K$. Because $a$ is algebraic over $E$:

# Subfield of algebraic elements

### Theorem

*$E$ an extension of $F$, $K$ the set of all elements of $E$ that are algebraic over $F$. Then $K$ is a subfield of $E$.*

**Proof:** Need to show that for $a, b \in K$, $b \neq 0$, we have $a + b, a - b, ab, ab^{-1} \in K$.