Math 128B, Mon Apr 12

- 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. 23. Reading for Mon: Ch. 23. (Ch. 24)
- Next week: **Groups** are back. Review: Chs. 1, 4, 5, 7 (S_n, A_n, D_n, $C_n \approx \mathbf{Z}_n$).
- PS08 outline due ~~tonight~~ Thu night, full version due Mon.
- Problem session Fri Apr 16, 10am–noon.
- Second round of music: ~~https://forms.gle/v4Xta3E9u3At9sBV8~~

Recap: Degree of an extension

Definition

E an extension of 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.

Definition

E an extension of F, $a \in E$. The **degree** of a over F is $[F(a):F]$.

Theorem (Multiplicativity)

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

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

$$mn \left(\begin{array}{c} K \\ \big| \, m \\ E \\ \big| \, n \\ F \end{array} \right.$$

Key example:

Then if $p(x) \in F[x]$, $\deg p = n$. $\boxed{p \text{ irr}}$

$E = F[x]/\langle p(x) \rangle$

α root of p

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

$[E:F] = n$

$[F(\alpha):F] = n$

Questions?

I.e., degree of an alg elt is = deg of min poly.

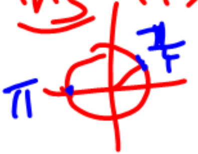
Let E = split field of x^4+1 over $\mathbb{Q}$

Express $E=\mathbb{Q}(\alpha)$, find $[E:\mathbb{Q}]$.

Prove $E=\mathbb{Q}(\sqrt{2}, i)$.

Ans $f(x)=x^4+1$

To factor this 4th degree polynomial, find 4 roots.



$x^4=-1$ $\quad w=e^{\frac{\pi}{4}i}$

$$w^4 = \left(e^{\frac{\pi}{4}i}\right)^4 = e^{\pi i} = -1$$

Note: $w = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, $w^2 = i$

(trig)

$$(e^{i\theta})^2 = e^{2\theta i}$$

$$\boxed{e^z e^w = e^{z+w}}$$

$$(e^{i\theta})^2 = e^{i\theta} e^{i\theta} = e^{i\theta + i\theta} = e^{2\theta i}$$

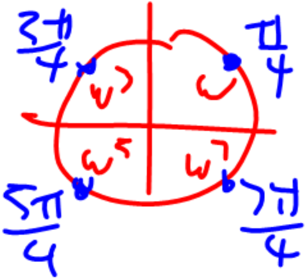
If $\eta^k = 1$, $x^k = (\eta x)^k$

(Like $(-x)^2 = x^2$)

So if $\alpha^4=-1$, $(i\alpha)^4=-1$

b/c $i^4=1$.

$\Rightarrow$ Zeros of x^4+1 are $\omega,\ i\omega,\ i^2\omega,\ i^3\omega$.



$\frac{\pi}{2}=\frac{2\pi}{4}$ Since $i=\omega^2$:

Zeros $=\omega,\ \omega^3,\ \underset{-\omega}{\underset{\parallel}{\omega^5}},\ \underset{-\omega^3}{\underset{\parallel}{\omega^7}}$

$\Rightarrow x^4+1=(x-\omega)(x-\omega^3)(x-\omega^5)(x-\omega^7)$

$\Rightarrow E=\mathbb{Q}(\omega)$

Can I solve $\underbrace{y^2=-1}_{\substack{\mathbb{Q}(i) \\ \text{s.f. of} \\ x^2+1 \text{ over} \\ \mathbb{Q}}}$, $\underbrace{x^2=y}_{\substack{\mathbb{Q}(w) \\ \text{s.f. of} \\ x^2+i \\ \text{over } \mathbb{Q}(i)}}$

$$\begin{tikzcd}
\mathbb{Q}(w) \arrow[d, dash, "?"'] \\
\mathbb{Q}(i) \arrow[d, dash, "2"'] \\
\mathbb{Q}
\end{tikzcd}$$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, i) \arrow[d, dash, "m"'] \arrow[dl, dash, "\ell"'] \\
\mathbb{Q}(\sqrt{2}) \arrow[ddr, dash, "2"'] & \mathbb{Q}(w) \arrow[d, dash, "k"'] \\
 & \mathbb{Q}(i) \arrow[d, dash, "2"] \\
 & \mathbb{Q}
\end{tikzcd}$$

$i \notin \mathbb{Q}$ $\deg(i) > 1$

i zero of x^2+1

so $\deg(i) \le 2$

$\Rightarrow \deg(i) = 2$

a is NOT an element of F <=> deg(a) > 1 <=> [F(a):F] > 1.

$$w^2 = i \Rightarrow i \in \mathbb{Q}(w)$$

$$w = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i, \text{ so } 2w \in \mathbb{Q}(w)$$

$$2w = \sqrt{2} + \sqrt{2} i = (\sqrt{2})\underbrace{(1+i)}_{\in \mathbb{Q}(w)}$$

$$\Rightarrow \frac{2w}{1+i} \in \mathbb{Q}(w) \Rightarrow \sqrt{2} \in \mathbb{Q}(w)$$

$$\Rightarrow \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(w)$$

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(w) \arrow[dl, dash, "2 = l"'] \arrow[dd, dash, "4"] \arrow[dr, dash, "k = 2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

w is zero of $x^2 - i$

$\Rightarrow w$ deg ≤ 2 over $\mathbb{Q}(i)$

$\Rightarrow k \leq 2$.

$2k = 2l \Rightarrow k = l$

$\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{2}, i)$

$\subseteq \mathbb{R}$ $\qquad$ $\not\subseteq \mathbb{R}$

$l > 1$

$k = l = 2$

$w = e^{\frac{\pi}{4}i}$ $\quad w^4 = -1$

w zero of x^4+1

$[\mathbb{Q}(w):\mathbb{Q}] = 4$, $\Lambda \cdot g(w) = 4$

So x^4+1 is min poly of w

<u>Cor</u> x^4+1 is irr over $\mathbb{Q}$.

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:

Why: Consequence of multiplicativity; see text for details.

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 $a + b, a - b, ab, ab^{-1} \in K$.

Why: Consider $F(a,b)$ over F.

Example: Consider the set K of all complex numbers that are algebraic over Q. By the Fundamental Theorem of Algebra, every polynomial equation has a solution in C, so K contains the all solutions to all polynomials equations with rational coeffs.

#thy: Study $K/\mathbb{Q} = \bar{\mathbb{Q}}/\mathbb{Q}$

Finite fields

Recall: Finite field of characteritic p is a vector space over $\mathbf{Z}/(p)$ and therefore has order p^e for some $e \geq 1$. In fact:

Theorem

For each prime p and $e \geq 1$, there exists a unique field of order $q = p^e$, denoted by $GF(q)$; namely, $GF(q)$ is the splitting field of $x^q - x$ over $\mathbf{F}_p$.

Proof: Uses existence and uniqueness of splitting fields.

A common confusion

Note that while $GF(p) \approx \mathbf{Z}_p$, for $e \geq 2$ and $q = p^e$, $GF(q) \not\approx \mathbf{Z}_q$.

Example: $GF(8)$ vs. $\mathbf{Z}_8$.

The multiplicative group of a finite field is cyclic

p prime, $e \geq 1$, $q = p^e$.

Theorem

The group of units of $GF(q)$ is cyclic of order $q - 1$.

Proof: Define the **exponent** of a finite group G to be smallest $n \geq 1$ such that $a^n = 1$ for all $a \in G$.
Let G be the group of units of $GF(q)$, $|G| = q - 1$. From classification of finite abelian groups (!!), the exponent of

$$G \approx \mathbf{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbf{Z}_{p_k^{n_k}}$$

is $\mathrm{lcm}(p_1^{n_1}, \ldots, p_k^{n_k})$. This $= q - 1$ exactly when G is cyclic; otherwise $< q - 1$.
Assume (by way of contradiction) that G is not cyclic.

Example: $GF(9)$

Construction, orders of elements, primitive element, factorizations of $x^9 - x$ and $x^2 + 1$.

Subfields of a finite field

p prime, $e \geq 1$, $q = p^e$.

Theorem

For each divisor d of e, $GF(q)$ has exactly one subfield of order p^d, and those are the only subfields of q.

Exmp: Subfields of $GF(5^{12})$.

Proof of subfields theorem

p prime, $e \geq 1$, $q = p^e$.

Theorem

For each divisor d of e, $GF(q)$ has exactly one subfield of order p^d, and those are the only subfields of q.

Proof: "Only" because $GF(q)$ is a v.s. over a subfield K:

Existence: $K = \left\{\alpha \in GF(q) \mid \alpha^{p^d} = \alpha\right\}$. Suppose $GF(q)^* = \langle\beta\rangle$.

Ruler-and-compass constructions

Suppose we start w/a straightedge, compass, and a unit length:

I.e., from those starting ingredients, we can:

1. Intersect two lines
2. Intersect a circle and a line
3. Intersect two circles

Q: Which lengths can we construct? I.e., which points can we capture as one of those types of intersections?

Constructible fields

Call $\alpha \in \mathbf{R}$ **constructible** if we can construct a segment of length α. Then

Theorem

The set of constructible numbers F is closed under $+$, $-$, $\times$, and reciprocals; i.e., F is a subfield of $\mathbf{R}$.

Proof: Suppose we have a and b constructed. To construct ab:

Square root extensions are possible

Theorem
F is closed under taking square roots.

Only square root extensions are possible

Suppose we follow a sequence of steps $1, \dots, n$ to construct a given length. Let F_k be the field generated by all lengths constructed up through step k (and $F_0 = \mathbf{Q}$). Because each operation involves taking an intersection of two lines, a line and a circle, or two circles, $F_{k+1} \subseteq F_k(\sqrt{a})$ for some $a \in F_k$. By multiplicativity of degree, we see that:

Theorem

$[F_n : \mathbf{Q}] = 2^t$ for some $t \geq 0$.

So for any constructible length a, considering $\mathbf{Q} \subseteq \mathbf{Q}(a) \subseteq F_n$:

A specific non-constructible angle

Let $\theta = \dfrac{2\pi}{18} = 20^\circ$. If we can construct θ, we can construct $\alpha = \cos\theta$, and from trig identities, can show that α is a zero of $p(x) = 8x^3 - 6x - 1$. Can show $p(x)$ is irreducible, so $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$, which means that α is non-constructible.