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. 22. Reading for Wed: Ch. 23.
- Next week: **Groups** are back. Review: Chs. 1, 4, 5, 7 (S_n, A_n, D_n, $C_n \approx \mathbf{Z}_n$).
- PS07 due tonight; PS08 outline due Wed night.
- Problem session Fri Apr 16, 10am–noon.
- Second round of music: `https://forms.gle/v4Xta3E9u3At9sRV8`

Extra office hours today 1-2; regular hours 2-3.

x^2+4 can't be factored over $\mathbb{Q}$
(no real roots)

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

$x^2+4=(x+2i)(x-2i)$

i sufficient to factor

i is also necessary to split x^2+4 b/c we need 2i and the rationals Q to split x^2+4, and any field containing 2i and Q must also contain i.

Simp: $\sqrt{3-2\sqrt{2}}$

Split x^6-7

$\alpha = \sqrt[6]{7}$

$\omega = e^{\frac{2\pi i}{6}}$

$\omega^6 = 1$

$f(x) = x^6 - 7$

$= (x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha) \cdots (x-\omega^5\alpha)$

Most of 1

Pf $f(\omega^i\alpha) = (\omega^i\alpha)^6 - 7$

$= \omega^{6i}\alpha^6 - 7 = 7 - 7 = 0.$

Recall: $\boxed{\text{Thm}}$

$p(x)$ irr over F

p has zero in field $\underbrace{\overset{E \,=}{F[x]/\langle p(x)\rangle}}_{\text{like } \mathbb{Q}(i)}$

And: $[E:F] = \deg p$

Ex Adjoin $\sqrt{3}$ to $F \iff F[x]/\langle x^2-3\rangle$

Recap: Degree of an extension

so E is v.s. over F

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.

Ex $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$

b/c $\sqrt{3}$ is zero of $x^2 - 3$

Theorem (Multiplicativity)

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

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

$$\begin{array}{c} K \\ | \; [K:E] \\ E \\ | \; [E:F] \\ F \end{array} \qquad [K:F]$$

E ≈

Example: Q(sqrt(3)+sqrt(7))

Find deg of E over $\mathbb{Q}$

$$\underset{\alpha}{\underset{\shortparallel}{\sqrt{3}+\sqrt{7}}} \in \mathbb{Q}(\sqrt{3},\sqrt{7},\sqrt{21}) = K$$

$$\underbrace{\text{Know: } [K:\mathbb{Q}] = 4, \text{ basis } \{1,\sqrt{3},\sqrt{7},\sqrt{21}\}}_{\text{previously proven}}$$

$$1 = 1$$

$$\alpha^2 = 3 + \sqrt{21} + 7 = 10 + \sqrt{21}$$

$$\alpha^4 = 100 + 20\sqrt{21} + 21 = 121 + 20\sqrt{21}$$

$$\alpha^4 - 20\alpha^2 = 121 + 20\sqrt{21} - 200 - 20\sqrt{21}$$

$= -79$

$$\boxed{\alpha^4 - 20\alpha^2 + 79 = 0}$$

$\alpha^7 = 10\sqrt{3} + 10\sqrt{7} + 3\sqrt{7} + 7\sqrt{3}$

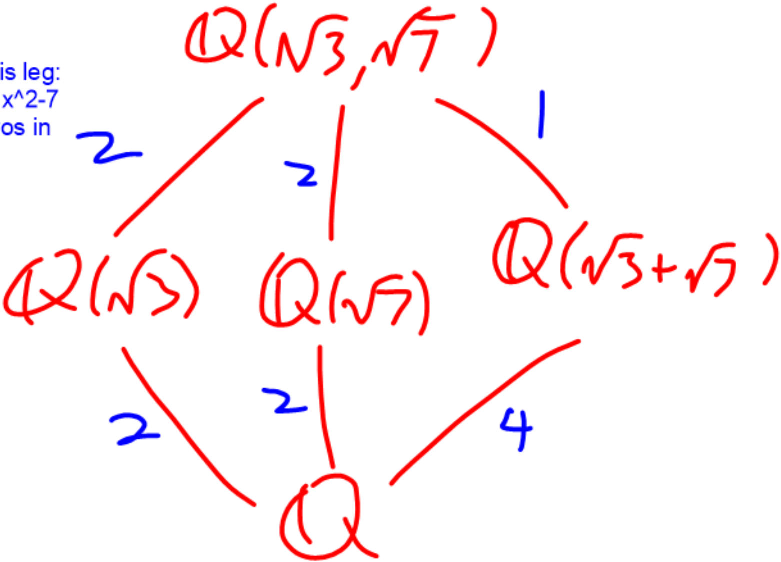
$= 17\sqrt{3} + 13\sqrt{7}$

RREF: $\{1, \alpha, \alpha^2, \alpha^3\}$ lin indep.

So $\text{minpoly}(\alpha) = \alpha^4 - 20\alpha^2 + 79$

$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$

Proof of this leg:
Show that x^2-7
has no zeros in
Q(sqrt(3)).



$$[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}] = 2\cdot 2 = 4$$

$[\mathbb{Q}(\sqrt{3},\sqrt{7}):\mathbb{Q}(\sqrt{3}+\sqrt{7})]$
$= 1$

So $\mathbb{Q}(\sqrt{3},\sqrt{7}) = \mathbb{Q}(\sqrt{3}+\sqrt{7})$

I.e. $\sqrt{3}$ is a rat'l l.c. of powers of $(\sqrt{3}+\sqrt{7})$

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

(without proof)

$\alpha = \sqrt[3]{7}, \quad w = e^{\frac{2\pi i}{3}} \quad (w^3 = 1)$

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha, w) \arrow[dl, dash, "k"'] \arrow[dd, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) & & \mathbb{Q}(w) \\
 & \mathbb{Q} \arrow[ul, dash, "3"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

Min poly of w:

$x^3 - 1 = (x-1)(x^2+x+1)$

w zero of $\underbrace{x^2+x+1}_{\text{irr}}$

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 3k$$

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

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

So 2 div k.

But

$k = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)]$

$=$ deg of min poly of ω over $\mathbb{Q}(\alpha)$

$\leq 2. \quad \Rightarrow k = 2.$

Primitive element theorem

Any extension by finitely many algebraic elements is = some F(c).

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

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: $\boxed{c = a + db}$ 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 $a + b, a - b, ab, ab^{-1} \in K$.

Example: Suppose F in K in L and [L:F]=[L:K]. Prove K=F.

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 subfields" first.