Welcome! Everything is fine.

When you're connected by zoom:

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 15.3–15.4; for Mon: 15.6.
- PS07 due Mon Mar 23.

Wed Mar 25 OK

Degree of a field extension

Definition

K is a field ext of F

For K/F, K is an F-vector space. We define the *degree* $[K : F]$ to be the dimension of K as an F-vector space. To say K/F is finite means that $[K : F]$ is finite.

Degree 1:

- K/F has deg 1 $\Leftrightarrow F = K$.
- α has deg 1 over $F \Leftrightarrow \alpha \in F$.

deg of an elt \alpha over F is the degree of irr poly of \alpha in F[x], i.e., irr f(x)\in F[x] s.t. f(\alpha)=0.

Proof:

is one particular

[K:F] = 1 <-> K has dim 1 as v.s. over F <-> {1} F-basis for K <-> K=F

\alpha has deg 1 over F <-> irr poly of \alpha has deg 1, so (x-a), a\in F

<-> irr poly of \alpha is (x-\alpha), \alpha\in F.

Degree 2 extensions

so quadratic formula works

Suppose $2 \neq 0$ in F (characteristic of F is not 2).

Theorem

If $[K : F] = 2$, then $K = F(\delta)$ where $\delta^2 = d \in F$. Conversely, if $\delta^2 = d \in F$ and $\delta \notin F$, then $[F(\delta) : F] = 2$.

Proof. of (1) . .

[K:F] = 2 means that any two elements of K lin ind over F are a basis for K. Since [K:F]>1, there exists some \alpha in K s.t. \alpha is not a F-multiple of 1, so {1,\alpha} is linearly independent and therefore an F-basis for K. But {1,\alpha,\alpha^2} is linearly dependent over F, so we must have:

$a \neq 0$ $a\alpha^2 + b_0\alpha + c_0 = 0 \Rightarrow \alpha^2 + b\alpha + c = 0$ } lin dep over F-alg rel'n

for some b,c\in F. The quadratic formula then gives \alpha = (-b+/-sqrt(b^2-4c))/2, so K = F(\delta), where \delta = sqrt(b^2-4c).

$$\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2} \qquad \delta = \sqrt{b^2-4c} \qquad K = F(\delta)$$

Degrees of elements vs. degrees of extensions

Fortunately: Degree of elt: degree of its irreducible polynomial
Degree of extension of F: dim of extension over F

Theorem

If α algebraic over F, degree of α equal to $[F(\alpha) : F]$.

Proof.

Spose \alpha algebraic over F. Then there exists some irr f(x)\in F[x] s.t.

$f(\alpha)=0$. If $\deg f = n$, we know

$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is F-basis for $F(\alpha)$

basis w/ n elts

$= F[\alpha]$.

So dim of F(\alpha) over F is n.

Recall: If $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, in $F(\alpha)$ use $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$ to compute

Note:

If $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$,

then $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0$

Use ↗ to compute in $F(\alpha)$:

1. Do all computations in terms of polynomials in \alpha.
2. Use above relation to reduce any term of deg >= n to terms of smaller degree, so we end up with poly of deg <n, which is a unique expression for elt of F(\alpha), since

$\{1, \alpha, \ldots, \alpha^{n-1}\}$

is F-linearly independent.

Degrees are multiplicative

Theorem

If $F \subseteq K \subseteq L$ a tower of fields. Then

$$[L : F] = [L : K][K : F].$$

dim of L as K-v.s.

dim of L as F-v.s.

dim of K as F-v.s.

Proof. Let:

$\{\beta_1, \ldots, \beta_n\}$ a basis for L as a K-vector space. So n = [L:K]

$\{\alpha_1 \ldots, \alpha_s\}$ a basis for K as a F-vector space. So s = [K:F]

Enuf to show $\{\alpha_i \beta_j\}$ is basis for L over F.

Span: If $\gamma \in L$, $\gamma = \sum b_j \beta_j \quad (b_j \in K)$ b/ beta_j span L

$= \sum (\sum a_{ij} \alpha_i) \beta_j \quad (a_{ij} \in F)$ b/c alpha_i span K

$= \sum\sum a_{ij} \alpha_i \beta_j$

Lin ind: If

$$\sum \left(\sum a_{ij}\alpha_i\right)\beta_j = 0$$

b/c beta_j are linearly independent, $\sum a_{ij}\alpha_i = 0$

b/c alpha_i are linearly independent, all $a_{ij} = 0$.

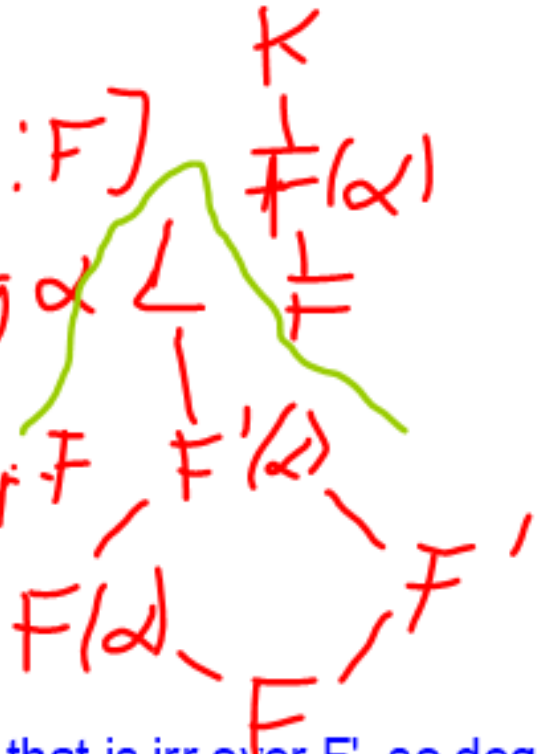
Yay linear algebra ☺

Consequences of multiplicativity

1. If $[K : F] = n$, $\alpha \in K$, then α algebraic over F, degree of α divides n.
2. $F \subseteq F' \subseteq L$. If $\alpha \in L$ alg over F, α alg over F'; deg over $F \geq$ deg over F'. (Maybe not divides)
3. Adjoining finitely many alg elts gives a finite extension.
4. For K/F, elements of K algebraic over F is a subfield of K.

Pf 1: $n = [K:F] = [K:F(\alpha)][F(\alpha):F]$

(2) If $f(\alpha) = 0$, f irr over F, then $f(\alpha) = 0$, $f \in F[x]$



So irr poly of alpha over F' is a factor of f(x) that is irr over F', so degree smaller.

Pf of 3: WTS: Adjoining finitely many alg elements to F gives finite extension of F.
Proof goes by adding elements algebraic over F, one at a time.
We know this true for adding one element, since [F(alpha):F] = deg of alpha.
But after adding one element, we get:

Adj α_1: Get $F(\alpha_1)$ alg over F
$\alpha_2 \cdots \alpha_k$ still alg over $F(\alpha_1)$

Proceeding by induction, we add on elements one at a time and get a finite extension each time.

By multiplicativity of degree, end result still has finite degree.

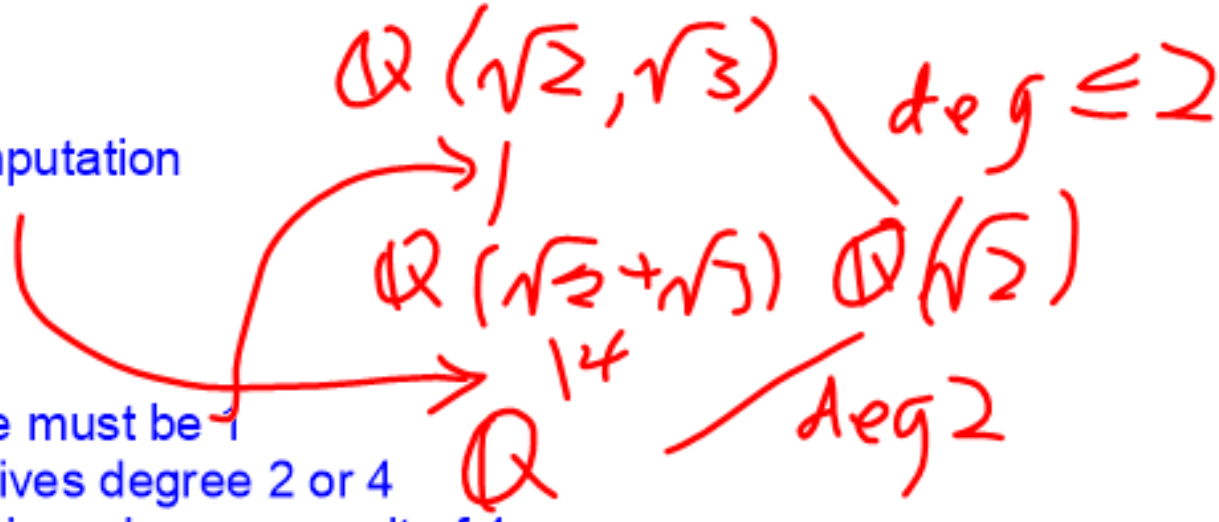
From Gallian: How to prove

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})\ ?$$

One method: Set containment both ways and mult of degree.

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \quad \checkmark$$

Can show by computation that this deg = 4:



So this degree must be 4
b/c RH path gives degree 2 or 4
and LH path gives degree a mult of 4.

Consequences of multiplicativity, cont.

- L/F extension, K/F and F'/F finite extensions in between, K' generated by K and F'. $[K' : F] = N$, $[K : F] = k$, $[F'/F] = n$. Then k and n divide N, $\leq kn$.

Diagram:

Proof of $\leq kn$ in special case. Suppose $F' = F(\beta)$.

Finding the irreducible polynomial

We'll start here on Mon.

Two methods for finding irr poly of γ over F:

- Keep taking powers of γ and eventually get a linear dependency.
- Guess other roots of irr poly (symmetrize!) and multiply out $(x - \gamma_i)$ to get irr poly (we hope).

Example

$K = \mathbb{Q}(\alpha)$, $\alpha^3 - \alpha^2 - 1 = 0$. Find irreducible for $\gamma = 1 + \alpha$ over $\mathbb{Q}$.