Welcome! Everything is fine.

When you're connected by zoom:

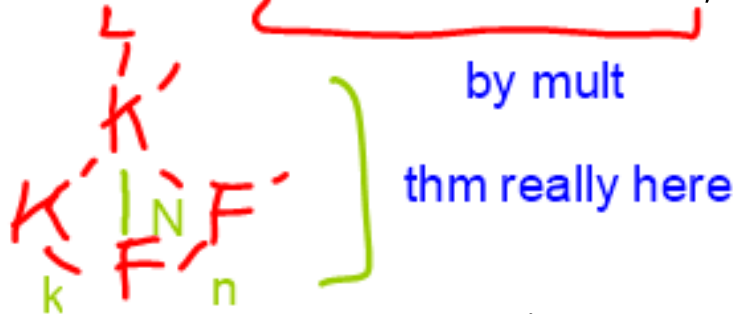
- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 15.4, 15.6; for Wed: 15.7.
- PS07 due Wed Mar 25.
- Exam 2: Take-home, over break or longer.

Consequences of multiplicativity, cont.

Last: For L/K and K/F finite extensions, $[L : F] = [L : K][K : F]$.

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

Diagram:



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

where F' obtained from F by adjoining one element.

[F':F] = degree of beta (as an element) = deg of irr poly of beta over F = n
Since K' = K(beta)
[K':K] = deg of beta (as an elt) = deg of irr poly of beta over K <= n
(Recall: <= n because irr of beta over F factors, and one of those factors becomes irr of beta over K)
So [K':F] = [K':K][K:F] = [K':K] * k <= nk.
(General case follows by applying special case finitely many times, since any finite extension can be obtained by adding elts one at a time.)

Finding the irreducible polynomial

Two methods for finding irr poly of γ over F:

- Keep taking powers of γ and eventually get a linear dependency.

  If gamma algebraic over F, must eventually happen

- Guess other roots of irr poly (symmetrize!) and multiply out $(x - \gamma_i)$ to get irr poly (we hope).

  Only works in special circumstances where we know symmetries of gamma and its friends.

Example

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

irreducible b/c irr over F_2

$\alpha^3 = \alpha^2 + 1$

alpha has deg 3 over Q, so Q(alpha) has dim 3 over Q.
So {1,gamma,gamma^2,gamma^3} is linearly dependent.

$1 \to 1$

$\gamma = 1 + \alpha$

$\gamma^2 = 1 + 2\alpha + \alpha^2$

$\gamma^3 = 1 + 3\alpha + 3\alpha^2 + \alpha^3 = 2 + 3\alpha + 4\alpha^2$

$4\gamma - 4 = 4\alpha^2 + 3\alpha$

$4\gamma^2 - 5\gamma = 4\alpha^2 + 3\alpha - 1$

$4\gamma^2 - 5\gamma + 3 = 4\alpha^2 + 3\alpha + 2 = \gamma^3$

So: $\gamma^3 - 4\gamma^2 + 5\gamma - 3 = 0$

irr b/c no roots in F_2

As a more formal linear algebra problem:

$\gamma^3 = a\gamma^2 + b\gamma + c$ solve a, b, c

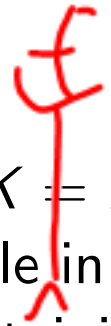
$4\alpha^2 + 3\alpha + 2 = a(\alpha^2 + 2\alpha + 1) + b(\alpha + 1) + c$

Compare coefficients on both sides and do std linear algebra.

Q(alpha) has dim 3 over Q.
{1,gamma,gamma^2} linearly independent, and is therefore a basis for Q(alpha) over Q.
So *any* element of Q(alpha) is a linear comb of 1, gamma, gamma^2.

Skipped: Ruler and compass stuff (15.5) b/c not needed later.

Adjoining roots



Recall: $K = F[x]/(f)$ is a field iff f irreducible. So given an irreducible in $F[x]$, we can (abstractly) construct a finite extension of F containing a root of f:

$[K:F] = \deg f$

Theorem

f irreducible in $F[x]$. Then $K = F[x]/(f)$ is an extension field of F, and image $\overline{x}$ of x in K is a root of f in K. □

use $\alpha, \beta, \ldots$ in place of $\overline{x}$.

Ex: Q(alpha), alpha^3 - alpha - 1 = 0 constructed as Q[x]/(x^3-x-1).
We say Q(alpha) is "Q adjoin a root of x^3-x-1".

Splitting fields

Definition

$f \in F[x]$ *splits* in K means $f(x)$ factors into linear factors over K.

Theorem

I.e., K contains "all roots of f"

F a field, $f \in F[x]$ monic of degree > 0. There exists K/F such that f splits over K.

Proof. Adjoin roots of f until f splits (induction on degree of f).

Example: F = Q, f(x) = x^3 - 2. Construct extension of Q in which f splits.

$F_1 = \mathbb{Q}(\sqrt[3]{2})$; $f(x) = (x - \sqrt[3]{2})(x^2 + 2^{1/3}x + 2^{2/3})$

(b/c $x^3 - y^3 = (x-y)(x^2+xy+y^2)$)

Need more

$\omega = e^{2\pi i/3}$

cube root of unity

$F_2 = F_1(\omega) = F(\sqrt[3]{2}, \omega)$

$f(x) = \underbrace{(x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2})}$

factors from 3 roots of $f(x)$

Check using $1+\omega+\omega^2 = 0$

- (Later: cyclotomic fields.)

Point for now is that f splits over F_2 (but not over F_1).

Divisors and roots vs. extensions

Theorem

$f, g \in F[x]$, $f \neq 0$, K/F.

1. *Division of g by f gives same answer in $F[x]$ or $K[x]$.*
2. $\gcd(f, g)$ *same in $F[x]$ and $K[x]$.*
3. *If f, g have a common root in K, they are not rel prime in $F[x]$. If f, g not rel prime in $F[x]$, there exists an extension in which they have a common root.*
4. *If f irreducible in $F[x]$ and f, g have a common root in K, then f divides g in $F[x]$.*

of F

1. g(x) = q(x)f(x) +r(x) in F[x], and same quotient in K[x] is unique.
2. gcd(f,g) computed using Euclidean algorithm = repeated divison, so by 1.
3. If f, g have common root, gcd(f,g) is not 1 in K[x], so not 1 in F[x].
Conversely: If gcd(f,g)=d(x) (not 1), can extend F by a root of an irr factor of d(x).
4. If f irr, f,g have a common root, then gcd(f,g) is not 1. But since f is irred, gcd(f,g) = f.

The (formal) derivative of a polynomial

Definition F is *any* field, e.g., F=Z/(p).

If

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

in $F[x]$, then define the derivative of f

$$f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 + 0.$$

Product rule still works!! (HW, to be done, but maybe not turned in)

Multiple roots and the derivative

Definition

$\alpha \in K/F$, $f \in F[x]$. α is a multiple root of f means $(x-\alpha)^2$ divides $f(x)$.

Theorem

$\alpha \in K/F$, $f \in F[x]$. α *is a multiple root of* f *iff* $f(\alpha) = 0$ *and* $f'(\alpha) = 0$.

Cor: There exists K in which f has a multiple root iff $\gcd(f, f') \neq 1$.

Proof of Thm:

alpha is root iff f(alpha) = 0 (Root Thm)

Then $f(x) = (x-\alpha)g(x)$

product rule!

So $f'(x) = g(x) + (x-\alpha)g'(x)$

So $f'(\alpha) = g(\alpha)$

alpha mult root of f iff alpha root of g iff f'(alpha) = 0.

Multiple roots of an irreducible

Theorem

$f \in F[x]$ irreducible has multiple roots in an extension of F iff $f' = 0$.

Cor: If characteristic of $F = 0$, then irreducible f has not multiple root in any extension of F.

Proof of Thm: