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: 15.1–15.2; for Wed: 15.3–15.4.
- PS07 due Mon Mar 23.

No office hr today

Questions from Ch. 13?

Any questions?

or PS06?

RC: $\mathbb{F}_p[x]/(x^2-d)$, $x^2-d=(x-a)(x-b)$, $a \neq b$

Like Z/(6) = (Z/(3))x(Z/(2))
Try to do that and then imitate for
F_p[x]/(x^2-d)
e = 1 + (x^2-d) won't work b/c you want an e \neq 1 (mod (x^2-d))

13.7.4: To show P Q ideals are prime, one method is to show N(P) and N(Q) prime, b/c an ideal with a norm that's prime can't factor b/c norm can't factor.

Extension fields

And now for something completely different....

Definition

If K is a field containing a subfield F, we write K/F and say that K is an *field extension* of F, or an *extension field*.

Definition

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.

Examples of finite extensions:

$[\mathbb{C} : \mathbb{R}] = 2$.

$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

$F = \mathbb{F}_2 = \mathbb{F}_3[x]/(x^2 + 1)$ is a field b/c $x^2 + 1$ irred over $\mathbb{F}_3$. Turns out that $|F| = 9$ so $[F : \mathbb{F}_3] = 2$. In fact, all *finite fields* can be constructed in this way.

Extending F by α: algebraic vs. transcendental

Our main tech tool!

Definition

K/F, $\alpha \in K$. α *algebraic* over F means there exists (monic) $f(x) \in F[x]$ such that $f(\alpha) = 0$; if no such $f(x)$ exists, α transcendental.

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

$\mathbb{Q}(e)$?

Ex.: $\sqrt{2}$ vs. π over $\mathbb{Q}$. (Both algebraic over $\mathbb{R}$.)

Open. Is π alg over $\mathbb{Q}$?

Alt description: Consider $\varphi : F[x] \to K$ sending $f(x) \mapsto f(\alpha)$. α transcendental if φ injective; otherwise $\ker \varphi = (g(x))$ for some monic generator $g(x) \in F[x]$. Then TFAE:

↑ b/c $F[x]$ is PID

- g is nonzero monic poly of lowest degree in $F[x]$ s.t. $g(\alpha) = 0$.
- g irreducible in $F[x]$ and $g(\alpha) = 0$.
- $g \in F[x]$, $g(\alpha) = 0$, and $(g(x))$ maximal ideal.
- $g \in F[x]$, $g(\alpha) = 0$, and if $h(\alpha) = 0$, then g divides h.

g is GCD of $\ker \varphi$

Degree of α defined to be $\deg g$.

Notation and examples

Pf ⊗: If $g(x) = f(x)h(x)$ then $f(\alpha)h(\alpha) = g(\alpha) = 0$. D/c K is a field, either $f(\alpha) = 0$ or $h(\alpha) = 0$. So if one has smaller deg, contradiction.

Notn: K/F, $\alpha \in K$; $F(\alpha)$ is the smallest subfield of K containing F and α. $F[\alpha]$ is smallest *subring* of K containing F and α; $F(\alpha)$ is field of fractions of $F[\alpha]$. $F(\alpha_1, \ldots, \alpha_k)$ vs. $F[\alpha_1, \ldots, \alpha_k]$ similar.

Ex.: Irreducible poly for $\sqrt[6]{2}$ over $\mathbb{Q}$ is $x^6 - 2$. $= (x^3 - \sqrt{2})(x^3 + \sqrt{2})$

Irr poly for $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $x^3 - \sqrt{2}$.

smallest field containing Q, sqrt(2)

Working with (computing in) $F(\alpha)$

Theorem

Spose $\alpha \in K/F$, α algebraic over F, f irr poly for α over F. Then $F[x]/(f(x)) \to F[\alpha]$ is an isom, $F[\alpha]$ is a field, $F[\alpha] = F(\alpha)$.

Similar for $F[\alpha_1, \ldots, \alpha_k] = F(\alpha_1, \ldots, \alpha_k)$.

Proof.

$f(x)$ gens ker, ϕ holds by 1IT

$F[\alpha]$ field b/c $f(x)$ irr $\to \langle f(x) \rangle$ max'l. $\to F(x)/\langle f \rangle$ field

Also, if $\deg f = n$, then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ as an F-vector space.

Example: (you pick) $F = \mathbb{R}$, $f(x) = x^2 + 1$, $\alpha = -i$

f irr so $\{1, -i\}$ basis for $F[\alpha]$ & deg 2 $= \{1, \alpha\}$

Constructing field isomorphisms/automorphisms

Definition

An F-isomorphism $K/F \to K'/F$ is an isomorphism $K \to K'$ that is the identity on F. To say that K/F and K'/F are isomorphic means that there exists an F-isomorphism $K/F \to K'/F$.

Theorem

$\alpha \in K/F$ and $\beta \in L/F$, both algebraic. There exists an F-isomorphism $F(\alpha) = F(\beta)$ sending α to β exactly when their irred polys are equal.

Proof.

Why

Let f_α, f_β be irrs. of α, β resp.

$F[x]/(f_\alpha) \leftrightarrow F(\alpha)$

these are isomorphic iff f_alpha=f_beta

$F[x]/(f_\beta) \leftrightarrow F(\beta)$

Usual application: If two alg elements have same irr polynomial, there exists an isomorphism of field extensions.

Examples of F-isomorphisms

α β

Ex.: $\sqrt{2}$, $-\sqrt{2}$ over $\mathbb{Q}$.

Same field, so field AUTOmorphism

There exists an isom of field extensions from Q(sqrt(2)) to Q(-sqrt(2)) sending sqrt(2) to -sqrt(2) b/c both have same irr poly x^2-1.

Ex.: $\sqrt[4]{2}$, $i\sqrt[4]{2}$ over $\mathbb{Q}$.

$\mathbb{Q}(\sqrt[4]{2}) \neq \mathbb{Q}(i\sqrt[4]{2})$ b/c first is real, but field exts are $\mathbb{Q}$-isom

irr x^4-2 over $\mathbb{Q}$

Non-ex.: $\sqrt[4]{2}$, $i\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt{2})$.

Irr of $\sqrt[4]{2}$ is $x^2-\sqrt{2}$

Irr of $i\sqrt[4]{2}$ is $x^2+\sqrt{2}$

} over $\mathbb{Q}(\sqrt{2})$

F-isomorphisms preserve roots

$\varphi : K/F \to K'/F$ an F-isomorphism, $f \in F[x]$.
$\alpha \in K$, $f(\alpha) = 0$, $\varphi(\alpha) = \alpha'$.
Then $f(\alpha') = 0$.
Proof:

α' also root of f. $a_i \in F$

Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$

$0 = f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0$

Apply F-isom φ: $\varphi(\alpha) = \alpha'$, $\varphi(a_i) = a_i$

$0 = \alpha'^n + a_{n-1}\alpha'^{n-1} + \cdots + a_0$

$= f(\alpha')$.

Degree of a field extension

Definition

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 $F \Leftrightarrow \alpha \in F$.

Proof: