Next Exam Wed Mar 28

Part 2: Polynomials in one variable.

Given R = comm. ring with 1 we define

$$R[x] = \left\{ \sum_{k=0}^{\infty} a_k x^k \;:\; a_k \in R,\ a_k = 0 \text{ a.e.} \right\}.$$

Then $R[x]$ is a ring with

$$\left(\sum a_k x^k\right) + \left(\sum b_k x^k\right) := \sum (a_k + b_k) x^k$$

$$\left(\sum a_k x^k\right)\left(\sum b_k x^k\right) := \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k$$

i.e. $(a_0 + a_1 x + \cdots)(b_0 + b_1 x + \cdots)$

$$= (a_0 b_0) + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \text{etc} \ldots$$

Remarks:

(1) $\exists$ natural embedding $R \hookrightarrow R[x]$

We say $R \subseteq R[x]$ is a ring extension.

(2) The elements $1, x, x^2, x^3, \ldots$ are linearly independent over R, i.e.

$$\sum a_k x^k = 0 \iff a_0 = a_1 = \cdots = 0$$

all coeffs. are zero.

Corollary: $\sum a_k x^k = \sum b_k x^k \iff a_k = b_k \ \forall k$.

Proof:

$$\sum a_k x^k = \sum b_k x^k \iff \sum (a_k - b_k) x^k = 0$$

$$\iff a_k - b_k = 0 \quad \forall k$$ ∎

Think of $R[x]$ as an ∞-dimensional "vector space" over R.
(actually a "free R-module")

(3) Clearly $R^\times \subseteq R[x]^\times$.
The converse is not always true.

e.g. in $\mathbb{Z}/(4)[x]$ we have

$$(\bar{2}x + \bar{1})(\bar{2}x + \bar{1}) = \bar{4}x^2 + \bar{4}x + \bar{1} = \bar{1}$$

Hence $\bar{2}x + \bar{1} \in (\mathbb{Z}/(4)[x])^\times$

However: if R is an integral domain then $(R[x])^\times = R^\times$ (HW 3)

Q: What is the ring structure of $R[x]$?

DEF: Given $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ with $a_n \neq 0$ we say f has degree n and leading coefficient a_n.

- We say $f(x)$ is MONIC if its leading coefficient is 1

Proposition 11.2.9:
Given $g, f \in R[x]$ with f MONIC, $\exists\, q, r \in R[x]$ such that

- $g(x) = q(x) f(x) + r(x)$
- $r \equiv 0$ OR $\deg(r) < \deg(f)$.

Proof by example:
Consider $g(x) = 2x^3 + 3x + 1$, $f(x) = 1x + 1$ (monic) } in $\mathbb{Z}[x]$.

$$2x^2 - 2x + 5$$

$x+1 \;\big|\; 2x^3 + 0x^2 + 3x + 1$

$2x^3 + 2x^2 + 0 + 0$

$0 - 2x^2 + 3x + 1$

$-2x^2 - 2x + 0$

$0 + 5x + 1$

$5x + 5$

$0 - 4$

$\Rightarrow (2x^3 + 3x + 1) = (2x^2 - 2x + 5)(x+1) + (-4)$

↑ quo ↑ rem

Note: $\deg(-4) < \deg(x+1)$

$0 \qquad 1$

Try to divide x^2+1 by $2x+1$ in $\mathbb{Z}[x]$

$\frac{1}{2}x - \frac{1}{4}$

$2x+1 \;\big|\; x^2 + 0x + 1$

$x^2 + \frac{1}{2}x + 0$

$0 - \frac{1}{2}x + 1$

$-\frac{1}{2}x - \frac{1}{4}$

$0 + \frac{5}{4}$

Can't be done since $2x+1$ is not monic

However, if we think $x^2+1,\ 2x+1 \in \mathbb{Q}[x]$

Then

$$(x^2+1) = \left(\frac{1}{2}x - \frac{1}{4}\right)(2x+1) + \frac{5}{4}.$$

$\frac{1}{2}x - \frac{1}{4}$ ↑ quo; $\frac{5}{4}$ ↑ rem.

This works because $2 \in \mathbb{Q}$ is a unit.

Conclusion: Actually we can divide by $f(x) \in R[x]$ if f has a unit leading coefficient.
(i.e. f is associate to a monic poly.)

Corollary: If F is a field, then $F[x]$ is a Euclidean Domain

Proof: Every nonzero poly is assoc. to a monic poly, so we can divide. ☒

Corollary: $F[x]$ is a UFD.

i.e. Every poly $f(x)$ can be written uniquely as

$$f(x) = k\, a_1(x)\, a_2(x) \cdots a_n(x)$$

k: nonzero constant; $a_1(x) \cdots a_n(x)$: monic irreducibles

Exam 1 out of 15 points.

Ave 12 $\quad A = \geq 11$

Med. 12 $\quad B = \leq 10$

St Dev 3.6

Recall: Given comm ring R with 1 we get a ring extension $R \subseteq R[x]$ where

$$R[x] := \left\{ \sum_{i=0}^{\infty} a_i x^i : a_i \in R,\ a_i = 0 \text{ a.e.} \right\}.$$

$R[x]$ is an ∞-dimensional "vector space" over R with "basis" $1, x, x^2, \ldots$.

Division Theorem: Given $f, g \in R[x]$, if g has unit leading coefficient, then $\exists\ q, r$ such that

$$f(x) = q(x)\, g(x) + r(x)$$

with $\deg(r) < \deg(g)$ OR $r = 0$.

Cor: If F is a field, then $F[x]$ is Euclidean, hence PID, hence UFD.

Other Corollary (Descartes' Factor Theorem):
Let R be comm. with 1, $f(x) \in R[x]$, $\alpha \in R$.
Then

$$\underbrace{f(\alpha) = 0}_{\text{"evaluation"}} \iff (x-\alpha) \mid f(x) \text{ in } R[x].$$

Proof: ($\Leftarrow$) Suppose $f(x) = (x-\alpha)g(x)$
Then $f(\alpha) = (\alpha-\alpha)g(\alpha) = 0 \cdot g(\alpha) = 0$. ✓

($\Rightarrow$) Suppose $f(\alpha) = 0$. Divide $f(x)$ by (monic) $x-\alpha$ to get.

$$f(x) = q(x)(x-\alpha) + \underbrace{k}_{\text{constant or zero.}}$$

Evaluate at $x = \alpha$ to get

$$0 = f(\alpha) = q(\alpha) \cdot 0 + k = k$$

$$\Rightarrow f(x) = q(x)(x-\alpha)$$ ∎

Def: Say $\alpha \in R$ is a root of $f(x) \in R[x]$ if $(x-\alpha) \mid f(x)$. The multiplicity of the root is max k such that

$$(x-\alpha)^k \mid f(x).$$

Theorem: Let R = integral domain.
Then a polynomial $f(x) \in R[x]$ of degree n has at most n roots (counting multiplicity) in any domain extension $R \subseteq S$.

Proof: Given $f(x) \in R[x] \subseteq S[x]$.
If $f(x)$ has 0 roots, done ✓
Else consider $\alpha \in S$ with $(x-\alpha)^k \| f(x)$ ← highest power

Hence $f(x) = (x-\alpha)^k g(x)$.
with $g(x) \in S[x]$ of degree $n-k$., $g(\alpha) \neq 0$.

Suppose $f(\beta) = 0$ for $\beta \neq \alpha$, so
$0 = f(\beta) = (\beta-\alpha)^2 g(\beta)$.
Since $(\beta-\alpha)^2 \neq 0$, $g(\beta) = 0$.
(Every other root of f is a root of g)

By induction, g has $\leq n-k$ roots,
counting multiplicity

$\Rightarrow$ f has $\leq k + (n-k) = n$ roots ∎

Translation: Given $f(x) \in R[x]$, $\deg(f) = n$.
If $f(\alpha) = 0$ for $n+1$ distinct α
then $f \equiv 0$.

Polynomials are "Rigid"

DEF: Given $f \in R[x]$ of deg. n and $R \subseteq S$.
We say f splits over S if it has
n roots in S.

We say R is algebraically closed
if every $f \in R[x]$ splits over R.

Big Theorem (Fundamental Theorem of Algebra):
The field $\mathbb{C}$ is algebraically closed.

Eg. Consider $x^4+1 \in \mathbb{Q}[x]$.
Has no roots in $\mathbb{Q}$ or $\mathbb{R}$.
Has 4 roots in $\mathbb{C}$, $\left\{\frac{1}{\sqrt{2}}(\pm 1 \pm i)\right\}$.

Irreducible factorizations

$x^4+1 = x^4+1$ irred over $\mathbb{Q}$

$= (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$ over $\mathbb{R}$.

$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$ "splits" over $\mathbb{C}$.

$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \left(\frac{1}{\sqrt{2}}(\pm 1 \pm i)\right)$.

Explanation: To solve $x^4 + 1 = 0$.

$x^4 = -1 \implies |x|^4 = 1 \implies |x| = 1$

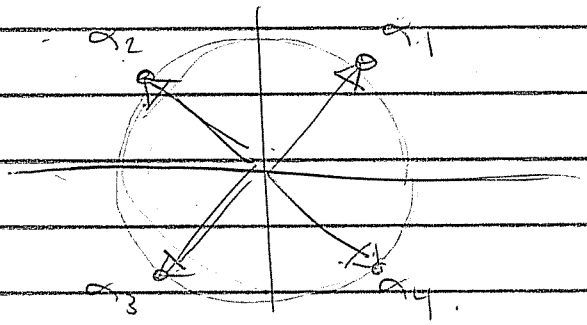
$\implies x = e^{i\theta}$

$x^4 = -1 = e^{-i\pi} \implies e^{i4\theta} = e^{-i\pi + 2\pi ik} \quad \forall k \in \mathbb{Z}$.

$\implies 4\theta = \pi + 2\pi k$

$\theta = \frac{\pi}{4} + \frac{\pi}{2} k \quad \forall \in k \in \mathbb{Z}$.

exactly 4 angles



$x^4 + 1 = \prod_{i=1}^{4} (x - \alpha_i)$

Note: $(x - \alpha_1)(x - \alpha_2)$

$= (x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2)$

$= (x^2 - \sqrt{2}x + 1)$

etc.

HW 3 due Wed Mar 7

Exam 2 Wed Mar 28

Let R be comm with 1.

Recall (Factor Theorem).

Given $f \in R[x]$ and $\alpha \in R$ we have

"$f(\alpha) = 0$" $\iff$ $(x-\alpha) \mid f(x)$.

Corollary: If R is a domain and $f \in R[x]$ has $\deg(f) = n$ then f has $\leq n$ roots counting multiplicity.

Remarks:

(1) "Domain" is needed since $x^2 - 1$ has 4 roots in $\mathbb{Z}/(8)$, $x = 1, 3, 5, 7$.

(2) "Commutative" is needed since $x^2 + 1$ has ∞ many roots in $\mathbb{H}$.

$(ai + bj + ck)^2 = -1 \quad \forall\ a, b, c \in \mathbb{R}$.

DEF: Say R is algebraically closed if $\deg(f) = n \Rightarrow f$ has exactly n roots in R. (every polynomial "splits")

Note: alg. closed $\Rightarrow$ field.
Since $\forall\ 0 \neq a \in R$ the poly $ax - 1$ has a root.

Theorem (FTA): $\mathbb{C}$ is alg. closed.

New Topic: What does "$f(\alpha)$" mean?

(comm.!)
Given rings $R \subseteq S$ and $\alpha \in S$, $\exists!$ homomorphism $\varphi_\alpha : R[x] \to S$ s.t.

- $\varphi_\alpha(r) = r \quad \forall r \in R$ (coeffs. are fixed)
- $\varphi_\alpha(x) = \alpha$. ($x \rightsquigarrow \alpha$).

φ_α is called "evaluation at α" and we write $\varphi_\alpha(f(x)) = "f(\alpha)"$.

Q: When is $\varphi_\alpha : R[x] \to S$ injective?

DEF: If φ_α is injective say α is "transcendental over R". Otherwise say α is "algebraic over R".

i.e.:

α alg. over $R \iff \ker \varphi_\alpha \neq 0$.

$(\exists\, f(\alpha) = 0)$.

Ex.

π trans. / $\mathbb{Q}$ (Lindemann, 1882).

π alg. / $\mathbb{R}$ $(f(x) = x - \pi \in \mathbb{R}[x])$.

$\sqrt{2}$ alg. / $\mathbb{Q}$ $(f(x) = x^2 - 2 \in \mathbb{Q}[x])$.

Claim: $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{R}$ is alg. / $\mathbb{Q}$.

$$\alpha^2 = 2 + 2\sqrt{6} + 3.$$
$$\alpha^2 - 5 = 2\sqrt{6}.$$
$$\alpha^4 - 10\alpha^2 + 25 = 24.$$
$$\alpha^4 - 10\alpha^2 + 1 = 0 \quad \checkmark$$

DEF: Let $R[\alpha] := \operatorname{im} \varphi_\alpha$.

We can identify $R \subseteq R[\alpha]$ by

$$\begin{array}{ccccc} R[x] & \xrightarrow{\varphi_\alpha} & R[\alpha] & \hookrightarrow & S \\ \uparrow & & \uparrow & & \\ R & \xrightarrow{\varphi_\alpha} & R & & \end{array}$$

Claim: $R[\alpha]$ is the smallest subring of S containing R & α.

Proof: Suppose $R \subseteq R' \subseteq S$ with $\alpha \in R'$.
Then since R' is a ring we have
$\operatorname{im} \varphi_\alpha = R[\alpha] \subseteq R'$. //

Say $R[\alpha]$: "R adjoin α".

Examples:

(1) $\varphi_\pi : \mathbb{Q}[x] \to \mathbb{R}$ is injective
hence
$$\mathbb{Q}[\pi] = \operatorname{im} \varphi_\pi \approx \mathbb{Q}[x]/(0) \approx \mathbb{Q}[x]$$

$\mathbb{Q}[\pi] \approx \mathbb{Q}[x]$
π acts just like a variable.

Note: $e \approx 2.71828$ is also trans. / $\mathbb{Q}$.

Hence $\mathbb{Q}[\pi] \approx \mathbb{Q}[x] \approx \mathbb{Q}[e]$

π & e are algebraically indistinguishable over $\mathbb{Q}$.

"$\mathbb{Q}$ can't tell the difference between π and e". ($\mathbb{R}$ can).

HW 3 due Wed Mar 7

Recall: Given $R \hookrightarrow S$ and $\alpha \in S$, $\exists!$ evaluation homomorphism $\varphi_\alpha : R[x] \to S$ such that
- $\varphi_\alpha|_R = \iota$
- $\varphi_\alpha(x) = \alpha$.

DEF: $R[\alpha] := \operatorname{im} \varphi_\alpha$.

FACT: If $R \subseteq R' \subseteq S$ and $\alpha \in R'$, then $R[\alpha] \subseteq R'$.
($R[\alpha]$ is the smallest subring of S containing $R \cup \{\alpha\}$.
Say $R[\alpha]$ = "R adjoin α")

Alternatively:

(Q: Is S really necessary?)

$$R[\alpha] = \bigcap_{R \cup \{\alpha\} \subseteq R' \subseteq S} R'$$

= the subring of S "generated by" R and α.

DEF: $\ker \varphi_\alpha = 0 \iff \alpha$ "transcendental over R"
$\ker \varphi_\alpha \neq 0 \iff \alpha$ "algebraic over R."

Examples:

(1) $\pi \in \mathbb{R}$ is trans. / $\mathbb{Q}$ (Lindemann, 1882).

$\Rightarrow \ker \varphi_\pi = 0$

$\Rightarrow \mathbb{Q}[\pi] = \operatorname{im} \varphi_\pi \tilde{=} \mathbb{Q}[x]/\ker \varphi_\pi = \mathbb{Q}[x]$

$\mathbb{Q}[\pi] \tilde{=} \mathbb{Q}[x]$.

(π is just like x)

$\Rightarrow \mathbb{Q}[\pi]$ is ∞-dim vector space over $\mathbb{Q}$ with basis $1, \pi, \pi^2, \cdots$.

(2) $\sqrt{2} \in \mathbb{R}$ is algebraic / $\mathbb{Q}$

Since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is PID.

$\Rightarrow \mathbb{Q}[\sqrt{2}] = \operatorname{im} \varphi_{\sqrt{2}} \tilde{=} \dfrac{\mathbb{Q}[x]}{\ker \varphi_{\sqrt{2}}} = \dfrac{\mathbb{Q}[x]}{(f_{\sqrt{2}})}$

for some unique monic $f_{\sqrt{2}} \in \mathbb{Q}[x]$.

DEF: $f_{\sqrt{2}}$ is called THE minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$.

Guess: $f_{\sqrt{2}}(x) = x^2 - 2$.

How can we prove this?

General Method:

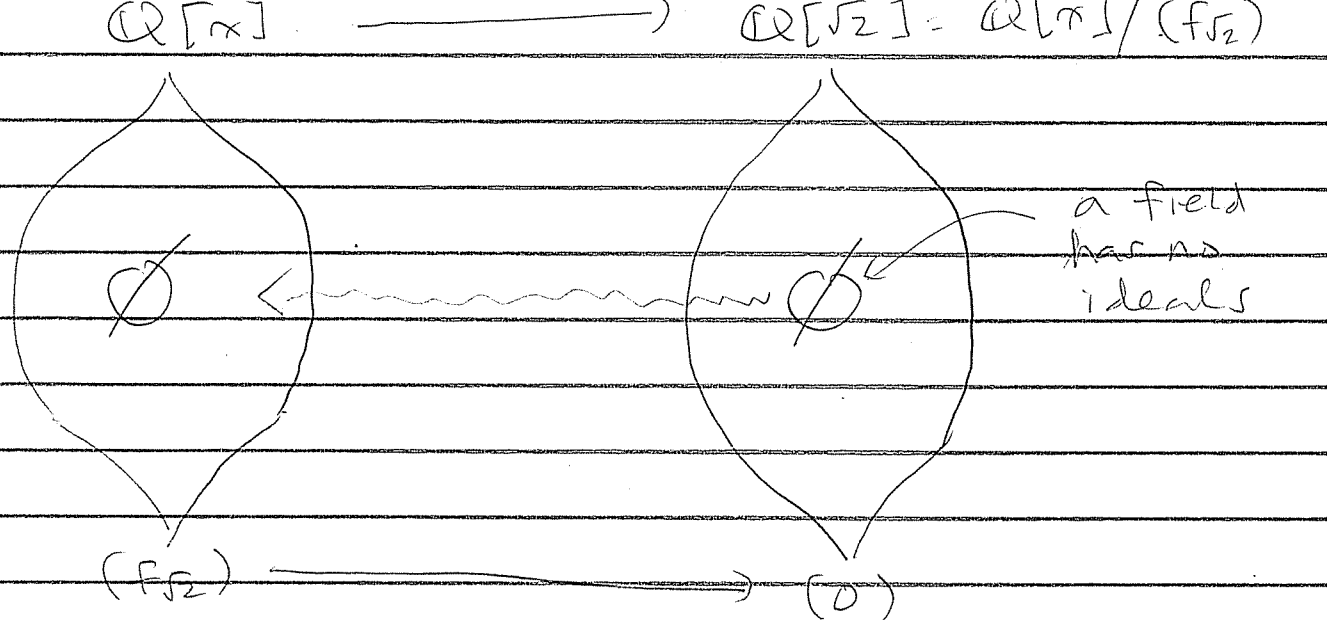
Claim 1: $f_{\sqrt{2}}$ is irreducible / $\mathbb{Q}$.

Proof: Note that $\mathbb{Q}[\sqrt{2}]$ is actually a field because

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2+2b^2}$$

$$= \left(\frac{a}{a^2+2b^2}\right) + \left(\frac{-b}{a^2+2b^2}\right)\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Now use Correspondence:



$\Longrightarrow \nexists\ g \in \mathbb{Q}[x]$ with $(f_{\sqrt{2}}) < (g) < \mathbb{Q}[x]$.

$\Longrightarrow f_{\sqrt{2}}$ is irreducible ▨

Claim 2: $f_{\sqrt{2}}(x) = x^2 - 2$

Proof: Note that "conjugation" $\overline{a+b\sqrt{2}} := a - b\sqrt{2}$ is a field automorphism $\mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{2}]$.

Check: $\overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta}$, $\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$.

Now take any $g \in \ker \varphi_{\sqrt{2}}$ (i.e. $g(\sqrt{2}) = 0$).
Then we also have

$$g(-\sqrt{2}) = g(\overline{\sqrt{2}}) = \overline{g(\sqrt{2})} = \bar{0} = 0.$$

Apply Factor Theorem over $\mathbb{Q}[\sqrt{2}]$ to get

$$g(x) = (x+\sqrt{2})(x-\sqrt{2})\,h(x) \quad (\text{for } h(x) \in \mathbb{Q}[\sqrt{2}][x])$$
$$g(x) = (x^2-2)\,h(x)$$

Then $g,\ x^2-2 \in \mathbb{Q}[x] \Longrightarrow h(x) \in \mathbb{Q}[x]$.

Hence $x^2 - 2 \mid g$ in $\mathbb{Q}[x]$

↳

In particular, $f_{\sqrt{2}} \in \ker \varphi_{\sqrt{2}}$ (by def.)

$\Rightarrow x^2 - 2 \mid f_{\sqrt{2}}$ in $\mathbb{Q}[x]$

Then $f_{\sqrt{2}}$ monic irred $\Rightarrow f_{\sqrt{2}} = x^2 - 2$

Conclusion: (where's $\mathbb{R}$?)

$$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[x]/(x^2-2)$$

But the same argument shows

$$\mathbb{Q}[-\sqrt{2}] = \mathbb{Q}[x]/(x^2-2) = \mathbb{Q}[\sqrt{2}]$$

"$\pm\sqrt{2}$ are indistinguishable over $\mathbb{Q}$".

So let's just say

$$\mathbb{Q}[\gamma] = \mathbb{Q}[x]/(x^2-2) \text{ where } \gamma^2 - 2 = 0.$$

we don't care what γ "is".

HW 3 due Wed Mar 7

Continue Example $\varphi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}$.

$$\mathbb{Q}[\sqrt{2}] = \operatorname{im} \varphi_{\sqrt{2}} \cong \frac{\mathbb{Q}[x]}{\ker \varphi_{\sqrt{2}}} = \frac{\mathbb{Q}[x]}{(f_{\sqrt{2}})}$$

for some unique monic $f_{\sqrt{2}} \in \mathbb{Q}[x]$ called THE min. poly. of $\sqrt{2}$ over $\mathbb{Q}$.

Claim 1: $f_{\sqrt{2}} \in \mathbb{Q}[x]$ is irreducible.

Proof: $\mathbb{Q}[\sqrt{2}]$ is a field $\Rightarrow (f_{\sqrt{2}}) \subseteq \mathbb{Q}[x]$ maximal ideal $\Rightarrow$ $f_{\sqrt{2}}$ irreducible ☐

Claim 2: $f_{\sqrt{2}}(x) = x^2 - 2$.

Proof: Let $g \in \ker \varphi_{\sqrt{2}}$ so $g(\sqrt{2}) = 0$. Then also $g(-\sqrt{2}) = 0$. Hence $g(x) = (x-\sqrt{2})(x+\sqrt{2})h(x)$
$= (x^2-2)h(x)$ for some $h \in \mathbb{Q}[x]$.
In particular $(x^2-2) \mid f_{\sqrt{2}}$.
Then $f_{\sqrt{2}}$ irred $\Rightarrow f_{\sqrt{2}} = x^2 - 2$ ☐

Get

$$\mathbb{Q}[\sqrt{2}] \cong \frac{\mathbb{Q}[x]}{(x^2-2)} \cong \mathbb{Q}[-\sqrt{2}].$$

algebraically indistinguishable

Claim 3: $\mathbb{Q}[\sqrt{2}]$ is a 2D vector space / $\mathbb{Q}$ with basis $\{1, \sqrt{2}\}$.

Proof: • $\{1, \sqrt{2}\}$ SPANS $\mathbb{Q}[\sqrt{2}] = \operatorname{im} \varphi_{\sqrt{2}} \cong \mathbb{Q}[x]/(x^2-2)$.

Every elt. of $\mathbb{Q}[x]/(x^2-2)$ looks like $g(x) + (x^2-2)$ for some $g(x) \in \mathbb{Q}[x]$.
Divide g by (x^2-2) to get

$$g + (x^2-2) = r - q(x^2-2) + (x^2-2)$$
$$= r + (x^2-2)$$

where $\deg(r) < 2$ or $r = 0$
(i.e. $r(x) = a + bx$ for $a, b \in \mathbb{Q}$).

Now apply the (surjective) natural map.

$$\mathbb{Q}[x]/(x^2-2) \xrightarrow{\varphi_{\sqrt{2}}} \mathbb{Q}[\sqrt{2}].$$

$$a + bx + (x^2-2) \longmapsto a + b\sqrt{2}.$$

SPAN. ✓

- $\{1, \sqrt{2}\}$ lin. ind. over $\mathbb{Q}$.

Suppose $a1 + b\sqrt{2} = 0$ for $a, b \in \mathbb{Q}$.
Then $a + bx \in \ker \varphi_{\sqrt{2}} = (x^2 - 2)$.

$\Rightarrow$ $a + bx = (x^2 - 2)h(x)$ for some $h \in \mathbb{Q}[x]$.

$\Rightarrow$ $a + bx = 0 \in \mathbb{Q}[x]$

$\Rightarrow$ $a = b = 0$
since $\{1, x\}$ are lin. ind. over $\mathbb{Q}$ ▽

Terminology:

Since $\mathbb{Q}[\sqrt{2}]$ is a field we write

$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ = the field generated by $\mathbb{Q} \cup \{\sqrt{2}\}$

Let $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] := \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$.
as a $\mathbb{Q}$-vector space

End of Example (2). ///

General Story:

The general story works best over fields.

Let $F \hookrightarrow K$ be fields and suppose $\alpha \in K$ is algebraic / F.

Prop 1: Choose monic $f_\alpha \in \ker \varphi_\alpha$ of smallest degree. (well-ordering). Then f_α is irreducible.

Proof: If not then $f_\alpha(x) = g(x)h(x) \in F[x]$ with $0 < \deg(g), \deg(h) < \deg(f_\alpha)$.
But $f_\alpha(\alpha) = g(\alpha)h(\alpha) = 0$
$\Rightarrow g(\alpha) = 0$ or $h(\alpha)$. contradiction. ☒

f_α is called the min. poly. of α / F.

Prop 2: $F[\alpha] = F(\alpha)$.

Proof: $F[\alpha]$, $F(\alpha)$ are smallest ring, field containing $F \cup \{\alpha\}$. Hence, $F[\alpha] \subseteq F(\alpha)$.

Since f_α is irred / F and $F[x]$ is PID, $(f_\alpha) \subseteq F[x]$ is a maximal ideal.

$\Rightarrow \mathbb{Q}[\alpha] \approx \mathbb{Q}[x]/(f_\alpha)$ is a field.

$\Rightarrow F(\alpha) \subseteq F[\alpha]$ ☒

HW 3 due Wed. Mar 7

Consider fields $F \hookrightarrow K$ and $\alpha \in K$ algebraic over F.

Recall

Prop 1: $F[x]$ PID $\Rightarrow \ker \varphi_\alpha = (f_\alpha)$ for unique monic $f_\alpha \in F[x]$. Note that f_α is irred over F since $f_\alpha(x) = g(x)h(x) \Rightarrow f_\alpha(\alpha) = g(\alpha)h(\alpha) = 0$ $\Rightarrow$ WLOG $g(\alpha) = 0 \Rightarrow g \in \ker \varphi_\alpha = (f_\alpha)$. $\Rightarrow (g) \subseteq (f_\alpha)$. But $g \mid f_\alpha \Rightarrow (f_\alpha) \subseteq (g)$ Hence g, f_α are associate ///.

f_α is THE min. poly. of α / F.

Prop 2: Then f_α irred $\Rightarrow (f_\alpha) \subseteq F[x]$ maximal $\Rightarrow F[\alpha] \cong F[x]/(f_\alpha)$ is a field $\Rightarrow F[\alpha] = F(\alpha)$.

Warning: If α is transcendental / F then $F[\alpha] \subsetneq F(\alpha)$.

$\wr$ ||

$F[x]$ not a field

$F(\alpha) \cong F(x)$ = field of fractions of $F[x]$

= "rational functions"

☆ **Prop 3**: Thus $F(\alpha)$ is an F-vector space. If $\deg(f_\alpha) = n$ then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)/F$.

SPAN?

Pf: Every elt of $F[x]/(f_\alpha)$ is $g + (f_\alpha)$. Divide g by f_α to get $g + (f_\alpha) = r - q f_\alpha + (f_\alpha) = r + (f_\alpha)$ where $\deg(r) < \deg(f_\alpha)$ or $r = 0$.

Consider isom. $F[x]/(f_\alpha) \xrightarrow{\overline{\varphi}_\alpha} F(\alpha)$.

Every elt has form $\overline{\varphi}_\alpha(r + (f_\alpha))$
$= \varphi_\alpha(r) = r(\alpha) \in \operatorname{span}\{1, \ldots, \alpha^{n-1}\}$ ✓.

INDEPENDENT?

Sp. $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$ where
$0 \neq g(x) = \sum_{i=0}^{n-1} a_i x^i \in F[x]$ $(\deg(g) < n)$.

Then $g(\alpha) = 0 \Rightarrow g \in \ker \varphi_\alpha = (f_\alpha) \Rightarrow f_\alpha \mid g$.
$\Rightarrow n = \deg(f_\alpha) \leq \deg(g) < n$ ✗

Hence $g = 0$ i.e. $a_0 = a_1 = \cdots = a_{n-1} = 0$. ✓

Hence $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a BASIS. ☒

Get $\boxed{[F(\alpha) : F] = \dim_F F(\alpha) = \deg(f_\alpha).}$

Ex $\sqrt[3]{2} \in \mathbb{R} \supseteq \mathbb{Q}$.

Note $x^3 - 2$ is irred / $\mathbb{Q}$ (HW 3.6(a))

Then $x^3 - 2 \in \ker \varphi_{\sqrt[3]{2}} = (f_{\sqrt[3]{2}})$

$\Rightarrow f_{\sqrt[3]{2}}(x) = x^3 - 2$.

$\Rightarrow \mathbb{Q}(\sqrt[3]{2})$ has $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$

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

a "cubic" extension of $\mathbb{Q}$.

HW 3.6(b).

Compute $(1 + 2(\sqrt[3]{2}) + (\sqrt[3]{2}))^{-1}$ in $\mathbb{Q}(\sqrt[3]{2})$.

Ex. $i \in \mathbb{C} \supseteq \mathbb{R}$ has min. poly. $x^2 - 1$.

$\Rightarrow \mathbb{R}[x]/(x^2-1) \cong \mathbb{R}(i) = \mathbb{C}$.

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

a "quadratic" field extension

Ex. $[\mathbb{R} : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{R} = \infty$

in fact uncountable.

Theorem (The Tower Law)

Given fields $F \subseteq K \subseteq L$ we have

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

In particular, $[L:F] < \infty$ implies $[L:K], [K:F] < \infty$.

Proof: Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis for K/F; $\beta_1, \ldots, \beta_n$ basis for L/K.

Claim: $\{\alpha_i \beta_j : 1 \le i \le m, 1 \le j \le n\}$ is a basis for L/F.

SPAN? Given $\gamma \in L$ let $\gamma = b_1\beta_1 + \cdots + b_n\beta_n$ with $b_1, \ldots, b_n \in K$.

Let $b_j = a_{1j}\alpha_1 + a_{2j}\alpha_2 + \cdots + \alpha_{mj}\alpha_m$ with $a_{ij} \in F$.

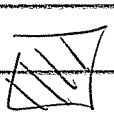
Then $\gamma = \sum_j \left(\sum_i a_{ij}\alpha_i \right)\beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j)$. ✓

INDEPENDENT? Sp. $\sum_{i,j} a_{ij}(\alpha_i\beta_j)$

$= \sum_j \left(\sum_i a_{ij}\alpha_i \right)\beta_j = 0$.

Since β's are independent / K we get $\sum_i a_{ij}\alpha_i = 0 \quad \forall j$.

Since α's are ind. over F we get $a_{ij} = 0 \quad \forall i, j$



HW 3 due Wed.

Now: Galois Theory.

Summary so far.

Given fields $F \subseteq K$ and $\alpha \in K$ consider evaluation $\varphi_\alpha : F[x] \to K$ $(x \rightsquigarrow \alpha)$.

Say α algebraic / F if $\ker \varphi_\alpha \neq 0$. Then $\ker \varphi_\alpha = (f_\alpha)$ where f_α is the minpoly.

$$F[x]/(f_\alpha) \cong F[\alpha] = F(\alpha). \quad \text{a field.}$$

$$[F(\alpha) : F] = \dim_F F(\alpha) = \deg(f_\alpha).$$

If α is transcendental / F $(\ker \varphi_\alpha = 0)$.

$$F[x] \cong F[\alpha] \subsetneq F(\alpha) \cong F(x).$$

$= $ field of "rational functions"

Thm (The Tower Law).
Given fields $F \subseteq K \subseteq L$ have

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

Applications:

(1) The field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Let $\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{R} \supseteq \mathbb{Q}$.

Q: Find minpoly of $\alpha / \mathbb{Q}$.

$$\alpha^2 = 2 + 2\sqrt{6} + 3$$

$$\alpha^2 - 5 = 2\sqrt{6}$$

$$\alpha^4 - 10\alpha + 25 = 24$$

$$\alpha^4 - 10\alpha + 1 = 0$$

$\Rightarrow f_\alpha(x) \mid g(x) := x^4 - 10x + 1$ in $\mathbb{Q}[x]$.

$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f_\alpha) \leq 4$.

Q: Is $g(x) = x^4 - 10x + 1$ irred. $/\mathbb{Q}$?

[Remark: Proving irreducibility/primality can be HARD.]

Note. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\alpha)$.

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

$$\leq 4 \qquad ? \qquad 2$$

But if $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})] = 1$ Then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$

$\Rightarrow \alpha \in \mathbb{Q}(\sqrt{2}) \Rightarrow \exists\, a, b \in \mathbb{Q}$ with

$$\sqrt{2} + \sqrt{3} = a + b\sqrt{2}.$$

$$\sqrt{3} = a + (b-1)\sqrt{2}$$

$$3 = a^2 + 2(b-1)^2 + 2a(b-1)\sqrt{2}.$$

$\Rightarrow \sqrt{2} \in \mathbb{Q}$ ✗. Hence $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})] \geq 2$.

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

$\Rightarrow f_\alpha(x) = x^4 - 10x^2 + 1$.

(Corollary: This is irred / $\mathbb{Q}$).

[Remark: If $f \in F[x]$ has $\deg(f) \leq 3$. Then

f irred / $F \iff f$ has NO root $\in F$.

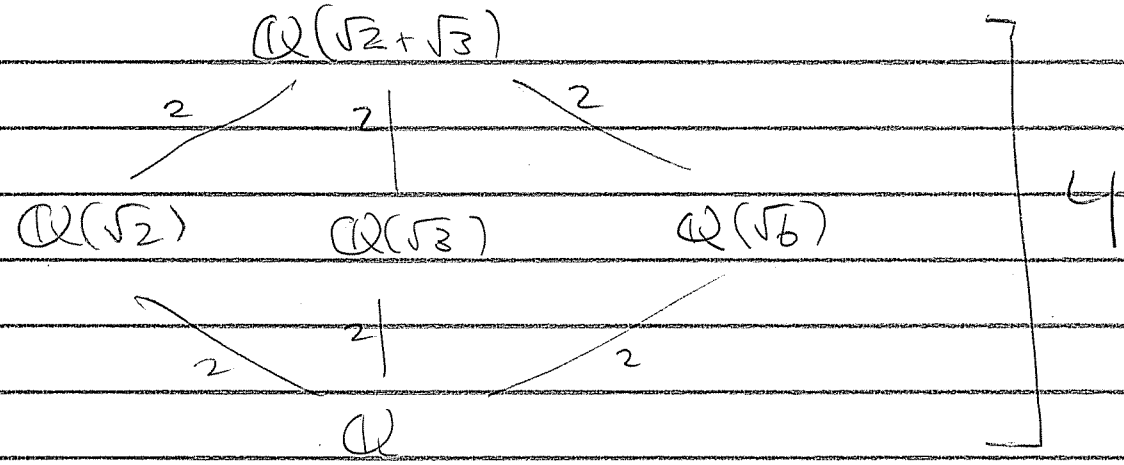
(easier to check).

for $\deg(f) \geq 4$, this fails.

eg $f(x) = x^4 + 4 \in \mathbb{R}[x]$ has NO roots in $\mathbb{R}$. BUT

$$x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2).$$]

Picture:



Remarks:

- Note $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ span $\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}$.
  Since $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}+\sqrt{3}) = 4$, They are a BASIS.

- Minpoly of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}(\sqrt{6})$?
  Answer: $x^2 - (5+2\sqrt{6})$.

- Q: $\exists$ other fields between $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})$
  A: No, but we can't prove it yet.

- Observation: Lattice of fields $\mathbb{Q} \to \mathbb{Q}(\sqrt{2}+\sqrt{3})$
  $\cong$ Lattice of subgroups of $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.
  $= \{1, a, b, ab\}$ where $a^2 = 1$, $b^2 = 1$, $(ab)^2 = 1$