Exam Problem 2021

Problem 3

For p a prime and n a positive integer, we let $\mathbb{F}_{p^n}$ be the field with p^n elements, with $\mathbb{F}_p$ denoting $\mathbb{Z}_p$.

3a

Determine if $\mathbb{F}_2[x]/\langle x^4+1\rangle$ is an integral domain.

3b

Show that $f(x) = x^4 + x^3 + 1$ is irreducible in $\mathbb{F}_2$. Explain why $f(x)$ admits a zero θ in the field $\mathbb{F}_{16}$, seen as an extension of $\mathbb{F}_2$ with degree $[\mathbb{F}_{16} : \mathbb{F}_2] = 4$. Prove that $f(x)$ is a primitive polynomial in $\mathbb{F}_2[x]$, meaning that θ is a generator of the multiplicative group of units $\mathbb{F}_{16}^*$.

3c

Assume known that $x^4 + x + 1$ is irreducible in $\mathbb{F}_2$. With $f(x)$ as in part 3b, explain why there is an isomorphism of fields

$$\mathbb{F}_2[x]/\langle x^4+x^3+1\rangle \cong \mathbb{F}_2[x]/\langle x^4+x+1\rangle.$$

3a) R comm ring w/ unity

Then R/I integral domain

$\Updownarrow$

I is a prime ideal

(if $ab \in I$ then a or $b \in I$.)

$\mathbb{F}_2[x]/\langle x^4+1\rangle$ is an integral domain $\Longleftrightarrow$

x^4+1 is irreducible / $\mathbb{F}_2$.

However $1 \in \mathbb{F}_2$ is a zero of x^4+1

Therefore x^4+1 factors over $\mathbb{F}_2$ as $(x+1)f(x)$ for some $f(x) \in \mathbb{F}_2[x]$. Hence x^4+1 is <u>not</u> irreducible and $\mathbb{F}_2[x]/\langle x^4+1 \rangle$ is <u>not</u> an integral domain.

3b

Show that $f(x) = x^4 + x^3 + 1$ is irreducible in $\mathbb{F}_2$. Explain why $f(x)$ admits a zero θ in the field $\mathbb{F}_{16}$, seen as an extension of $\mathbb{F}_2$ with degree $[\mathbb{F}_{16} : \mathbb{F}_2] = 4$. Prove that $f(x)$ is a primitive polynomial in $\mathbb{F}_2[x]$, meaning that θ is a generator of the multiplicative group of units $\mathbb{F}_{16}^*$.

Claim $f(x) = x^4 + x^3 + 1$ is irreducible in $\mathbb{F}_2$.

Case 1 $f(x) \stackrel{?}{=} g(x)h(x)$ where $\deg g(x) = 1$ $\deg h(x) = 3$.

$f(0) \neq 0$ and $f(1) = 1+1+1 \neq 0$ $\Rightarrow$ $f(x)$ has no zeros in $\mathbb{F}_2$

$\Rightarrow \nexists$ a factorisation $f(x) = g(x)h(x)$ where $\deg g = 1$, $\deg h = 3$.

Case 2 $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ $a,b,c,d \in \mathbb{F}_2$

$= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$.

$bd = 1 \Rightarrow b = d = 1$ $a+c=1$ but $ad+bc = 0 \Rightarrow a+c=0$

contradiction

$\Rightarrow$ no such factorisation exists and $f(x)$ is irred. over $\mathbb{F}_2$.

We know $E = \mathbb{F}_2[x] / \langle x^4 + x^3 + 1 \rangle$ is a field since $f(x)$ is irred. over $\mathbb{F}_2$

moreover $\theta = x + \langle x^4 + x^3 + 1 \rangle \in E$ is a zero of $f(x)$

(Recall: $f(\theta) = \theta^4 + \theta^3 + 1 = (x + \langle x^4 + x^3 + 1 \rangle)^4 + (x + \langle x^4 + x^3 + 1 \rangle)^3 + 1$

$= x^4 + x^3 + 1 + \langle x^4 + x^3 + 1 \rangle$

$= \langle x^4 + x^3 + 1 \rangle = 0$ in E)

Now $[E : \mathbb{F}_2] = \deg f(x) = 4$ so $|E| = 2^4 = 16$.

By the uniqueness theorem for finite fields $E \cong \mathbb{F}_{16}$. identify $\theta \in E$ with an element of $\mathbb{F}_{16}$ under the isomorphism.

$|\mathbb{F}_{16}^*| = 15$ moreover $\mathbb{F}_{16}^* = E^*$ is a cyclic group.

<u>claim</u> $\operatorname{ord} \theta = 15$

The possible orders of θ are $1, 3, 5$ or 15.

$$E = \{ a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 \quad a_i \in \mathbb{F}_2 \}.$$

$$\theta \neq 1 \qquad \theta^3 \neq 1 \qquad \theta^5 = \underbrace{(\theta^3 + 1)}\theta = \theta^4 + \theta = \theta^3 + 1 + \theta \neq 1$$

since $\theta^4 + \theta^3 + 1 = 0$ in E

Hence, $\operatorname{ord}\theta = 15$ and θ generates $\mathbb{F}_{16}^* \cong E^*$.

3d

It is known that the Galois group $Gal(\mathbb{F}_{16}/\mathbb{F}_2)$ is a cyclic group of order 4 generated by the Frobenius automorphism σ_2. Use this to write a splitting of $f(x)$ from part 3b into linear terms in $\mathbb{F}_{16}$. If needed, you can use without proof that an irreducible polynomial of degree 4 in $\mathbb{F}_2[x]$ divides $x^{2^4} - x$ in $\mathbb{F}_2[x]$.

Want to factor $f(x) = (x+\alpha_1) \cdots (x+\alpha_4)$.

Recall θ was a zero of $f(x)$. $\theta \in E \cong \mathbb{F}_{16}$.

Frobenius automorphism $\sigma_2 : \mathbb{F}_{16} \longrightarrow \mathbb{F}_{16}$

$$a \longmapsto a^2$$

σ_2 fixes $\mathbb{F}_2$

From last time $\Rightarrow$ $\sigma_2(\theta)$, $\sigma_2 \circ \sigma_2(\theta)$, ... are zeros of $f(x)$.

Claim $\theta, \theta^2, \theta^4, \theta^8$ are distinct zeros of $f(x) = x^4+x^3+1$

$$\theta^4 = \theta^3+1$$

$$\begin{aligned}
\theta^8 &= (\theta^3+1)(\theta^3+1) \\
&= \theta^6 + \cancel{2\theta^3} + 1 \\
&= (\theta^3+1)\theta^2+1 \\
&= \theta^5+\theta^2+1 \\
&\quad \theta(\theta^3+1)+\theta^2+1 \\
&\quad \theta^4+\theta+\theta^2+1 \\
&\quad \theta^3+\cancel{1}+\theta+\theta^2\cancel{+1} \\
&= \theta^3+\theta^2+\theta.
\end{aligned}$$

Check $f(\theta^3+\theta^2+\theta) = 0$ in E.

Isomorphism Extensions §49

Recall Let $F \leq E$. $\alpha, \beta \in E$ are conjugate over F if

$\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$.

α, β conjugate over F $\iff$ $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ is an isomor.

$$\begin{aligned} a &\mapsto a \quad a \in F \\ \alpha &\mapsto \beta \end{aligned}$$

Question Can $\psi_{\alpha,\beta}$ be extended to an automorphism $\psi : E \to E$?

$$\begin{tikzcd} & E & \\ F(\alpha) \arrow[u, dash] \arrow[rr] & & F(\beta) \arrow[ul, dash] \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$\Rightarrow$ $\psi(b) = \psi_{\alpha,\beta}(b)$ $\forall\ b \in F(\alpha)$

$x^2 - 2 = \operatorname{irr}(\pm\sqrt{2}, \mathbb{Q})$

Example $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ $\psi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2})$ extends to

$E = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6}\}$

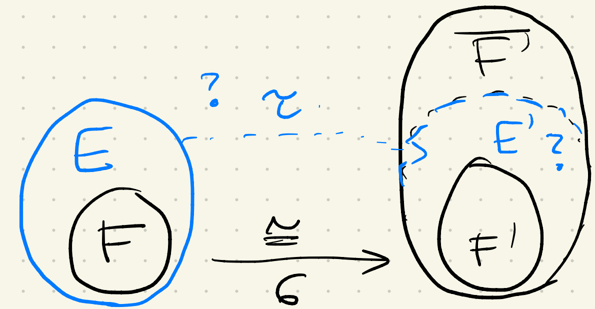
$$\tau_1 : E \longrightarrow E \qquad\qquad \tau_2 : E \to E$$
$$\sqrt{3} \mapsto \sqrt{3} \qquad\qquad \sqrt{3} \mapsto -\sqrt{3}$$

Recall: For α alg over F. Every $\psi: F(\alpha) \to F' \leq \overline{F}$ must map α to a conjugate β of α over F. (Corollary 48.5)

The conjugates of $\sqrt{3}$ over $\mathbb{Q}$ are $\pm\sqrt{3}$ since $\operatorname{irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3$.

Thm 49.3 Iso Ext'n Thm

Let E be an alg ext. of F and $\sigma : F \to F'$ be a field isomorphism. Then σ can be extended to an isomorphism $\tau : E \to E' \leq \overline{F'}$ (so that $\tau(a) = \sigma(a)\ \forall\, a \in F$).



Proof Idea To extend σ: Find $\alpha \in E$, $\alpha \notin F$. First extend to $F(\alpha)$. Let $p(x) = \operatorname{irr}(\alpha, F) = a_0 + a_1 x + \dots + x^n \in F[x]$.

Let β be a zero of $q(x) = \sigma(a_0) + \sigma(a_1)x + \dots + x^n \in F'[x]$

Define $\tau_\alpha : F(\alpha) \to F'(\beta)$

$a \mapsto \sigma(a) \quad a \in F$

$\alpha \mapsto \beta$.

$$\begin{tikzcd} E \arrow[r, dashed, "\tau ?"] & ? \\ F(\alpha) \arrow[r, dashed, "\tau_\alpha"] & F'(\beta) \\ F \arrow[u, dash] \arrow[r, "\sigma"] & F' \end{tikzcd}$$

Continue this procedure + use Zorn's lemma if E is infinite degree / F. $\boxtimes$

Corollary 49.4 $E \leq \overline{F}$ is alg. extn of F and $\alpha, \beta \in E$ conjugate then $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ can be extended to an isomorphism $\tau : E \to E' \leq \overline{F}$.

Example $e^{4\pi i/3} 2^{1/3} \notin E = \mathbb{Q}(2^{1/3}, i) \dashrightarrow E' \neq E$ ← isomorphism not an automorphism

$$\psi_{2^{1/3},\, e^{4\pi i/3} 2^{1/3}} : \mathbb{Q}(2^{1/3}) \longrightarrow \mathbb{Q}(e^{4\pi i/3} 2^{1/3}).$$

$$\operatorname{irr}(\underbrace{2^{1/3}}_{\alpha}, \mathbb{Q}) = \operatorname{irr}(\underbrace{e^{4\pi i/3} 2^{1/3}}_{\beta}) = x^3 - 2 \Rightarrow \alpha, \beta, \gamma \text{ conjugate}$$

$$K = \mathbb{Q}(2^{1/3}, e^{2\pi/3} 2^{1/3}, \underbrace{e^{4\pi i/3} 2^{1/3}}_{\gamma}) \longrightarrow K$$ ← extension of ψ. to K is an automorphism

$$\psi : \mathbb{Q}(2^{1/3}) \longrightarrow \mathbb{Q}(e^{4\pi i/3} 2^{1/3})$$

"Splitting field" of $x^3 - 2$

Corollary 49.5 The algebraic closure of a field is unique up to isomorphism.

Proof idea extend $id : F \to F$ to $\begin{array}{c}\overline{F}\\ | \\ F\end{array}$

⚠ Implicitly used this to shorten proof of uniqueness of finite fields (Thm 33.12)

Def 49.9 Let E be a finite field extension of F ($[E:F] < \infty$). The # of isomorphisms of E onto a subfield of $\overline{F}$ leaving F fixed is the index of E over F, denote $\{E:F\}$.

identity map

$\{E:F\}$ = # of extensions of $id: F \to F$ to $\tau: E \to \tau[E]$ isomorphism where $\tau[E] \leq \overline{F}$

Thm $\{E:F\}$ is finite if $[E:F] < \infty$

See exercise 49.13

Example (See Example 49.11)

$$\begin{tikzcd}
\mathbb{Q}(2^{1/3}, i) \arrow[rr] \arrow[d, dash] & & \overset{\overline{\mathbb{Q}}}{?} \\
\mathbb{Q}(2^{1/3}) \arrow[rr] \arrow[rr, bend left] \arrow[rr, bend right] \arrow[d, dash] & & \mathbb{Q}(2^{1/3}) \quad \mathbb{Q}(e^{2\pi i/3}2^{1/3}) \quad \mathbb{Q}(e^{4\pi i/3}2^{1/3}) \arrow[d, dash] \\
\mathrm{id} : \mathbb{Q} \arrow[rr] & & \mathbb{Q}
\end{tikzcd}$$

$$\{a_0 + a_1 2^{1/3} + a_2 2^{2/3}\} = \mathbb{Q}(2^{1/3})$$
$$a_0, a_1, a_2 \in \mathbb{Q}$$

$$\{\mathbb{Q}(2^{1/3}) : \mathbb{Q}\} = 3$$
$$\parallel \leftarrow \text{Notice}$$
$$[\mathbb{Q}(2^{1/3}) : \mathbb{Q}]$$

Exercise

$$\{\mathbb{Q}(2^{1/3}, i) : \mathbb{Q}(2^{1/3})\}$$
$$\{\mathbb{Q}(2^{1/3}, i) : \mathbb{Q}\}?$$

$$\begin{tikzcd}
K = \mathbb{Q}(2^{1/3}, e^{2\pi i/3}2^{1/3}, e^{4\pi i/3}2^{1/3}) \arrow[rr] \arrow[d, dash] & & ? \\
\mathrm{id} : \mathbb{Q} \arrow[rr] & & \mathbb{Q}
\end{tikzcd}$$