2023 MATH4302 Sample Exam

1.(a): False: $\frac{x^2-1}{x-1}, \frac{x^3-1}{x-1}$ are nontrivial proper factors of $\frac{x^6-1}{x-1}$

(b): True: We've proven on class that $\mathbb{Z}[\sqrt{-1}]$ is a Euclid Domain, and recall that Field $\subseteq$ Euclid Domain $\subseteq$ Principal Ideal Domain $\subseteq$ Unique Factorization Domain $\subseteq$ Integral Domain $\subseteq$ Commutative Ring with Unity

(c): True: $f: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $a \mapsto a^p$ is injective because $x^p=0$ has a unique solution. f is surjective because f is injective and the domain and codomain of f have cardinality p^n

(d) True: Let $l_1, \cdots, l_\mu$ be a basis of L over K.

Let $p_1(x), \cdots, p_\mu(x)$ be the minimal polynomials of $l_1, \cdots, l_\mu$ over K.

$p_1(x), \cdots, p_\mu(x) \in K[x]$ $l_1, \cdots, l_k$ generates L

$\mathrm{Aut}(L/K)$ acts faithfully on the set of roots of $p(x) = p_1(x) \cdots p_\mu(x)$,

so $\mathrm{Aut}(L/K)$ is a finite group.

(e) False: Let $K = \mathbb{F}_p(x,y)$, $L = K(x^{1/p}, y^{1/p})$ be a degree p^2 extension.

For all slope $k \in \mathbb{F}_p(x,y)$, $|\mathbb{F}_p(x,y)| = +\infty$, $K(x^{1/p} + k y^{1/p})$ is an intermediate extension of degree p, where $K(x^{1/p} + k y^{1/p})$ are distinct.

2 (1) Proof: $a=\sqrt{2}+\sqrt{5}$

$a^2-2\sqrt{2}a+2=5$

$\sqrt{2}=\dfrac{a^2-3}{2a}\in\mathbb{Q}(a)$

$a=\sqrt{2}+\sqrt{5}$

$a^2-2\sqrt{5}a+5=2$

$\sqrt{5}=\dfrac{a^2+3}{2a}\in\mathbb{Q}(a)$

(2) Solution: $(a^2-3)^2-8a^2=a^4-14a^2+9$ is a polynomial with root $\sqrt{2}+\sqrt{5}$.

To see why it is irreducible over $\mathbb{Q}$, it suffices to see the degree of $\mathbb{Q}[a]/\mathbb{Q}$ $\cong \mathbb{Q}[\sqrt{2},\sqrt{5}]/\mathbb{Q} \cong \left(\mathbb{Q}[\sqrt{2}][\sqrt{5}]/\mathbb{Q}[\sqrt{2}]\right)\left(\mathbb{Q}[\sqrt{2}]/\mathbb{Q}\right)$ is $2\cdot 2=4$.

(3) Solution: Present L in the form $\mathbb{Q}[\sqrt{2},\sqrt{5}]=\{a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10}: a,b,c,d\in\mathbb{Q}\}$.

Since $\mathbb{Q}[\sqrt{2},\sqrt{5}]=\mathrm{Split}_{\mathbb{Q}}(x^4-14a^2+9)$, $\mathrm{char}(\mathbb{Q})=0$, $\mathbb{Q}[\sqrt{2},\sqrt{5}]/\mathbb{Q}$ is Galois, $|\mathrm{Gal}(\mathbb{Q}[\sqrt{2},\sqrt{5}]/\mathbb{Q})|=[\mathbb{Q}[\sqrt{2},\sqrt{5}]:\mathbb{Q}]=4$, so it suffices to show that the $\mathbb{Q}$-linear maps $f_{0,0}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10})=a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10}$, $f_{1,0}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10})=a-b\sqrt{2}+c\sqrt{5}-d\sqrt{10}$, $f_{0,1}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10})$ $=a+b\sqrt{2}-c\sqrt{5}-d\sqrt{10}$, $f_{1,1}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10})=a-b\sqrt{2}-c\sqrt{5}+d\sqrt{10}$ preserves multiplication. For simplicity, we do the case $f_{1,0}$, and it follows that $\mathrm{Gal}(\mathbb{Q}[\sqrt{2},\sqrt{5}]/\mathbb{Q})=\{f_{0,0},f_{1,0},f_{0,1},f_{1,1}\}\cong\mathbb{Z}_2\times\mathbb{Z}_2$.

$$
\begin{aligned}
&f_{1,0}\left((a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10})(a'+b'\sqrt{2}+c'\sqrt{5}+d'\sqrt{10})\right)\\
&=f_{1,0}\big((aa'+2bb'+5cc'+10dd')\\
&\quad+(ab'+ba'+5cd'+5dc')\sqrt{2}\\
&\quad+(ac'+2bd'+ca'+2db')\sqrt{5}\\
&\quad+(ad'+bc'+cb'+da')\sqrt{10}\big)\\
&=(aa'+2bb'+5cc'+10dd')\\
&\quad-(ab'+ba'+5cd'+5dc')\sqrt{2}\\
&\quad+(ac'+2bd'+ca'+2db')\sqrt{5}\\
&\quad-(ad'+bc'+cb'+da')\sqrt{10}\\
&=(a-b\sqrt{2}+c\sqrt{5}-d\sqrt{10})(a'-b'\sqrt{2}+c'\sqrt{5}-d'\sqrt{10})\\
&=f_{1,0}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10})\,f_{1,0}(a'+b'\sqrt{2}+c'\sqrt{5}+d'\sqrt{10})
\end{aligned}
$$

(4) Solution: According to the Galois correspondence, the following maps are inverses to each other:

i: An intermediate field $K \subseteq M \subseteq L$
$\mapsto$ A subgroup $\mathrm{Aut}(L/K) \supseteq \mathrm{Aut}(L/M) \supseteq \{e\}$

ii: A subgroup $\mathrm{Aut}(L/K) \supseteq H \supseteq \{e\}$
$\mapsto$ An intermediate field $K \subseteq L^H \subseteq L$

In particular, for the case $\mathrm{Aut}(L/K) = \{f_{0,0}, f_{1,0}, f_{0,1}, f_{1,1}\}$,

$$\begin{tikzcd}
 & \{f_{0,0}\} \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
H_{1,0} = \langle f_{1,0} \rangle \arrow[dr, no head] & H_{0,1} = \langle f_{0,1} \rangle \arrow[d, no head] & H_{1,1} = \langle f_{1,1} \rangle \arrow[dl, no head] \\
 & \mathrm{Aut}(L/K) = \{f_{0,0}, f_{1,0}, f_{0,1}, f_{1,1}\} &
\end{tikzcd}$$

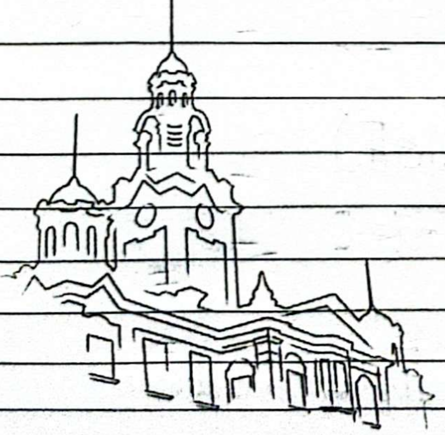
$f_{0,0}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10}) = a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10}$, $L^{f_{0,0}} = \mathbb{Q}[\sqrt{2},\sqrt{5}]$.

$f_{1,0}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10}) = a-b\sqrt{2}+c\sqrt{5}-d\sqrt{10}$, $L^{f_{1,0}} = \mathbb{Q}[\sqrt{5}]$.

$f_{0,1}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10}) = a+b\sqrt{2}-c\sqrt{5}-d\sqrt{10}$, $L^{f_{0,1}} = \mathbb{Q}[\sqrt{2}]$

$f_{1,1}(a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10}) = a-b\sqrt{2}-c\sqrt{5}+d\sqrt{10}$, $L^{f_{1,1}} = \mathbb{Q}[\sqrt{10}]$.

$$\begin{tikzcd}
 & L = \mathbb{Q}[\sqrt{2},\sqrt{5}] \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
M_{1,0} = \mathbb{Q}[\sqrt{5}] \arrow[dr, no head] & M_{0,1} = \mathbb{Q}[\sqrt{2}] \arrow[d, no head] & M_{1,1} = \mathbb{Q}[\sqrt{10}] \arrow[dl, no head] \\
 & K = \mathbb{Q} &
\end{tikzcd}$$



3.(1) Proof: Assume to the contrary that $\mathrm{char}(L) = \overset{\text{in } \mathbb{Z}}{0}$.

That is, the kernel of the ring homomorphism $\sigma: \mathbb{Z} \to L,\ \overset{\text{in } \mathbb{Z}}{n} \mapsto \overset{\text{in } L}{n}$ is trivial.

According to the first isomorphism, $\mathrm{Im}(\sigma) \cong \mathbb{Z}/\mathrm{Ker}(\sigma) \cong \mathbb{Z}$,

so an infinite set $\mathbb{Z}$ is embedded on L, contradiction.

(2) Proof: It suffices to show that $\mathrm{char}(L)$ is a prime number.

Assume to the contrary that $\mathrm{char}(L)$ is not a prime number,

for some $\overset{\text{in } \mathbb{Z}}{s,t \geq 2}$, $\mathrm{char}(L) = \overset{\text{in } \mathbb{Z}}{st}$. As $s \neq 0, \overset{\text{in } L}{t \neq 0}, st = 0$, L contains a zero divisor s, so L is not a field, contradiction. Hence, $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/\mathrm{Ker}(\sigma) \cong \mathrm{Im}(\sigma)$ is embedded on L.

(3) Proof: As $x^{p^n} - x \in \mathbb{F}_p[x]$, it suffices to show that $\mathrm{Root}_{\mathbb{F}_{p^n}}(x^{p^n} - x) \supseteq \mathbb{F}_{p^n}$

and $x^{p^n} - x$ already splits into linear factors over $\mathbb{F}_{p^n}$, having cardinality $|\mathbb{F}_{p^n}| = p^n$ as $\dim_{\mathbb{F}_p} L = n$.

Part 1: $0^{p^n} - 0 = 0 - 0 = 0$, so $0 \in \mathrm{Root}_{\mathbb{F}_{p^n}}(x^{p^n} - x)$

For all $a \in \mathbb{F}_{p^n}^{\times}$, according to Lagrange's theorem, $\mathrm{ord}(a) \mid |\mathbb{F}_{p^n}^{\times}| = p^n - 1$

so $a^{p^n - 1} = a^{\mathrm{ord}(a) \frac{p^n - 1}{\mathrm{ord}(a)}} = 1^{\frac{p^n - 1}{\mathrm{ord}(a)}} = 1$, $a^{p^n} - a = 0$, $a \in \mathrm{Root}_{\mathbb{F}_{p^n}}(x^{p^n} - x)$.

Hence, any proper subfield of $\mathbb{F}_{p^n}$ misses at least one root, thus not the splitting field.

Part 2: $\deg(x^{p^n} - x) = p^n = |\mathbb{F}_{p^n}|$, so $x^{p^n} - x$ has exactly p^n linear factors.

Hence, $\mathbb{F}_{p^n}$ is the smallest field extension of $\mathbb{F}_p$ such that $x^{p^n} - x$ completely splits into linear factors, thus the splitting field.

(4) Proof: An element $a \in \mathbb{F}_{p^n}$ lies in $\mathbb{F}_{p^d}$ $\Rightarrow a = 0$ or $a \in \mathbb{F}_{p^d}^{\times}$

$\Rightarrow 0^{p^d} - 0 = 0 - 0 = 0$, or $a^{p^d - 1} = 1$, $a^{p^d} - a = 0$

$\Rightarrow$ a is a root of $x^{p^d} - x = 0$.

However, $x^{p^d} - x$ has exactly p^d roots in $\mathbb{F}_{p^n}$, so $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ is unique.

4. (1) Proof: I is a nonzero prime ideal of $K[x]$, where K is a field

$\Rightarrow$ I is generated by a prime polynomial $p(x) \in K[x]$, because $K[x]$ is a principal ideal ring

$\Rightarrow$ The prime polynomial $p(x) \in K[x]$ is irreducible, because $K[x]$ is an integral domain

$p(x) \neq \text{const}$, $p(x) = a(x)b(x) \Rightarrow p(x) \mid a(x)b(x)$

$\Rightarrow p(x) \mid a(x)$ or $p(x) \mid b(x) \Rightarrow \frac{a(x)}{p(x)} b(x) = 1$ or $a(x)\frac{b(x)}{p(x)} = 1$

$\Rightarrow$ The irreducible polynomial $p(x) \in K[x]$ generates a maximal ideal I. because $K[x]$ is a principal ideal ring.

$$\langle p(x)\rangle \subsetneqq \langle q(x)\rangle \subseteq K[x]$$

$\Rightarrow q(x) \mid p(x) \Rightarrow q(x) \sim 1$ or $q(x) \sim p(x)$

$\Rightarrow \langle q(x)\rangle = K[x]$ or $\langle q(x)\rangle = \langle p(x)\rangle$, $\langle p(x)\rangle \subsetneqq K[x]$.

(2) Proof: $f(x) \in \bigcap_{\langle p(x)\rangle \in S} \langle p(x)\rangle \Rightarrow$ Infinitely many distinct irreducible polynomial $p(x)$ divides $f(x) \Rightarrow f(x) = 0$ is generic

(3) Proof: Assume to the contrary that $\mathrm{supp}(M)$ is infinite.

As $\mathrm{ann}(M)$ is contained in every $\langle p(x)\rangle \in \mathrm{supp}(M)$, $\mathrm{ann}(M) \subseteq \bigcap_{\langle p(x)\rangle \in \mathrm{supp}(M)} \langle p(x)\rangle$

$= \{0\}$, contradicting to M is torsioned.

(4) Solution:

As $R = K[x]$ is a principal ideal domain, and M is finitely R-generated, for some irreducible polynomials $p_1(x), p_2(x), \cdots, p_k(x)$, not necessarily pairwisely nonassociates, and for some $\alpha_1, \alpha_2, \cdots, \alpha_k \geq 1$, $\beta \geq 0$, $M \cong (R/p_1^{\alpha_1}(x)R) \oplus (R/p_2^{\alpha_2}(x)R) \oplus \cdots \oplus (R/p_k^{\alpha_k}(x)R) \oplus R^{\beta}$. As $\mathrm{supp}(M) = \{xR\}$,

$p_1(x) = p_2(x) = \cdots = p_k(x) = x$, and we are done.

5 (1) Type 1: $(x-\alpha)R$, where $\alpha \in \mathbb{R}$

Type 2: $(x^2-2\alpha x+\alpha^2+\beta^2)R$, where $\alpha \in \mathbb{R}$, $\beta > 0$.

(2) Factorize $x^4+x^3+x^2$ over $\mathbb{R}$: $x^4+x^3+x^2 = x^2(x^2+x+1)$, $\Delta = 1^2-4\cdot 1\cdot 1 = -3 < 0$

Hence, $\operatorname{supp}(M) = \{xR, (x^2+x+1)R\}$.