2024 MATH 4302 Sample Exam.

1. (1) True. By "R is a UFD $\Rightarrow R[x]$ is a UFD",
$\mathbb{Z}[x]$ is a UFD, $x-1$ is irreducible $\Rightarrow x-1$ is prime.

Alternatively, by Taylor's theorem, $f(x) = \sum_{n=0}^{+\infty} a_n (x-1)^n$,
so $x-1 \mid f(x)g(x) \Rightarrow a_0 b_0 = 0 \Rightarrow a_0 = 0$ or $b_0 = 0$ as $\mathbb{Z}$ is an integral domain.

While, every maximal ideal I of $R[x]$ is in the form $\langle p(x), J \rangle$,
where $p(x)$ is an irreducible polynomial in $(R/J)[x]$, J is maximal in R.
So we still have the freedom to quotient $J = \langle 2 \rangle$.

(2) True. For some prime element $p=5$ in the UFD $\mathbb{Z}$,
$p \nmid 1, p \mid 0, p \mid 0, p \mid 0, p \mid 0, p \mid -5, p^2 \nmid -5$, x^5-5 is irreducible over $\mathbb{Z}[x]$
It follows from Gauss's lemma that x^5-5 is irreducible over $\mathbb{Q}[x]$.
As $\mathbb{Q}[x]$ is a PID, $\langle x^5-5 \rangle$ is maximal, $\mathbb{Q}[x]/\langle x^5-5 \rangle$ is a field.

(3) True. There exists $(x-1)(x+15)^3 \in \mathbb{Z}[x]$ that annihilate every $(f(x), g(x)) \in M$.

(4) False. x^2+x+1 has negative discriminant $\Delta = -3$, so it has no root in $\mathbb{R} \supseteq \mathbb{Q}$,
thus, the quadratic polynomial x^2+x+1 is irreducible over $\mathbb{R} \supseteq \mathbb{Q}$.
$(x^2)^2 + x^2 + 1 = x^4 + x^2 + 1 = (x^2+x+1)(x^2-x+1)$ is reducible over $\mathbb{Z} \subseteq \mathbb{Q}$.

(5) True. Assume to the contrary that $f(x) = g(x)h(x)$, $\deg g(x) > 0$, $\deg h(x) > 0$
is reducible over K. Apply the evaluation homomorphism $\varepsilon: K[x] \to K[x]$,
$l(x) \mapsto l(x^2)$, we see that $f(x^2) = g(x^2)h(x^2)$, $\deg g(x^2) > 0$, $\deg h(x^2) > 0$
is reducible over K.

(2)

1) Solution: Define:

$f_{3,1}(x) = (x-3)^1(x-5)^2$

$f_{3,2}(x) = (x-3)^0(x-5)^2$

$f_{5,1}(x) = (x-3)^2(x-5)^1$

$f_{5,2}(x) = (x-3)^2(x-5)^0$

Step1: For any linear combination $C_{3,1}f_{3,1}(x)+C_{3,2}f_{3,2}(x)+C_{5,1}f_{5,1}(x)+C_{5,2}f_{5,2}(x)$, evaluate at $x=3,5$ respectively, we obtain $C_{3,2}=C_{5,2}=0$.

Divide both sides by $(x-3)(x-5)$, and then evaluate at $x=3,5$ respectively, we obtain $C_{3,1}=C_{5,1}=0$

Hence, $f_{3,1}(x), f_{3,2}(x), f_{5,1}(x), f_{5,2}(x)$ is linearly independent in the $4=\deg((x-3)^2(x-5)^2)$-dimensional space, it is a basis.

Step2:

$(x-3)f_{3,1}(x) = 0 \qquad T(f_{3,1}(x)) = 3f_{3,1}(x)$

$(x-3)f_{3,2}(x) = f_{3,1}(x) \qquad T(f_{3,2}(x)) = f_{3,1}(x) + 3f_{3,2}(x)$

$(x-5)f_{5,1}(x) = 0 \qquad T(f_{5,1}(x)) = 5f_{5,1}(x)$

$(x-5)f_{5,2}(x) = f_{5,1}(x) \qquad T(f_{5,2}(x)) = f_{5,1}(x) + 5f_{5,2}(x)$

$$T = \left(\begin{array}{cc|cc} \overbrace{3 \quad 1}^{\text{minimal polynomial } (x-3)^2} & & 0 & 0 \\ 0 & 3 & 0 & 0 \\ \hline 0 & 0 & 5 & 1 \\ 0 & 0 & \underbrace{0 \quad 5}_{\text{minimal polynomial } (x-5)^2} & \end{array}\right)$$ is in Jordan Normal Form under this basis.

2) Solution: Define:

$g_{3,1}(x) = x^0(x-5)^2$

$g_{3,2}(x) = x^1(x-5)^2$

$g_{5,1}(x) = x^0(x-3)^2$

$g_{5,2}(x) = x^1(x-3)^2$

Step1: $g_{3,1}(x) = f_{3,2}(x)$; $f_{3,1}(x) = -3g_{3,1}(x) + g_{3,2}(x)$

$g_{3,2}(x) = f_{3,1}(x) + 3f_{3,2}(x)$; $f_{3,2}(x) = g_{3,1}(x)$

$g_{5,1}(x) = f_{5,2}(x)$; $f_{5,1}(x) = -5g_{5,1}(x) + g_{5,2}(x)$

$g_{5,2}(x) = f_{5,1}(x) + 5f_{5,2}(x)$; $f_{5,2}(x) = g_{5,1}(x)$

Hence, $g_{3,1}(x), g_{3,2}(x), g_{5,1}(x), g_{5,2}(x)$ is also a basis of the $4=\deg((x-3)^2(x-5)^2)$-dimensional space.

Step2:

$$x g_{3,1}(x) = x^1(x-5)^2 = g_{3,2}(x)$$

$$x g_{3,2}(x) = x^2(x-5)^2 = (6x-9)(x-5)^2 = -9g_{3,1}(x) + 6g_{3,2}(x)$$

$$x g_{5,1}(x) = x^1(x-3)^2 = g_{5,2}(x)$$

$$x g_{5,2}(x) = x^2(x-3)^2 = (10x-25)(x-3)^2 = -25g_{5,1}(x) + 10g_{5,2}(x)$$

minimal polynomial $(x-3)^2$

$$T = \left(\begin{array}{cc|cc} 0 & -9 & 0 & 0 \\ 1 & 6 & 0 & 0 \\ \hline 0 & 0 & 0 & -25 \\ 0 & 0 & 1 & 10 \end{array}\right)$$ is an rational canonical form under this basis.

minimal polynomial $(x-5)^2$

3. 1) Solution:

Assume to the contrary that $\mathbb{Q}(\alpha)$ contains $\sqrt[3]{2}$.

That is, $\mathbb{Q}(\alpha)/\mathbb{Q}$ has an intermediate extension $\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

By Tower theorem, $3 = \deg(x^3-2) = [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] \mid [\mathbb{Q}(\alpha):\mathbb{Q}]$

$= \deg(x^5+2x^4+4x^3-6x+2$, irreducible by Eisenstein criterion modulo prime 2$) = 5$, which is a contradiction.

$x^2+1=0$ $\quad$ $x^3-5=0$

2) Proof: First, $K = \mathbb{Q}[i, \sqrt[5]{11}, \sqrt[3]{5}, \sqrt{37}]$ is a finite extension over $\mathbb{Q}$.

$x^5-11=0$ $\quad$ $x^2-37=0$

Second, $K[\beta] \subseteq \mathrm{Split}_K\left(-x^{19} + i\sqrt[5]{11}x^4 + \frac{\sqrt[3]{5}+191}{\sqrt{37}+1}x^3 + 1\right)$ is a finite extension over K. By Tower Theorem, $K[\beta]$ is a finite extension over $\mathbb{Q}$.

Third, as $K[\beta]$ is a finite extension over $\mathbb{Q}$, $\beta \in K[\beta]$ is algebraic over $\mathbb{Q}$.

4. Proof: As a corollary of Eisenstein's criterion, the minimal polynomial of $e^{\frac{2\pi i}{p}}$ over $\mathbb{Q}$ is $\frac{x^p-1}{x-1}$, so $[\mathbb{Q}[e^{\frac{2\pi i}{p}}]:\mathbb{Q}]=p-1$.

As $\frac{2\pi}{p}$ is constructable, $\mathbb{Q}[e^{\frac{2\pi i}{p}}]/\mathbb{Q}$ is a tower of degree 2 extensions, by tower theorem, $p-1=[\mathbb{Q}[e^{\frac{2\pi i}{p}}]:\mathbb{Q}]=2^n$ for some $n\geq 0$.

5. (1) Let R be a principal ideal domain. For any finitely generated module M over R, for some prime elements $p_1,\cdots,p_k$ in R (not necessarily pairwise nonassociates), an integer $r\geq 0$, and positive integers $n_1,\cdots,n_k$, such that:

$$M\cong R^r\oplus R/\langle p_1^{n_1}\rangle\oplus\cdots\oplus R/\langle p_k^{n_k}\rangle.$$

(2) Proof: Suppose G is a finite Abelian group. Identify G with a finite module over the principal ideal domain $\mathbb{Z}$. Hence, for some prime elements $p_1,\cdots,p_k$ in R (not necessarily pairwise nonassociates), an integer $r\geq 0$, and positive integers $n_1,\cdots,n_k$, such that:

$$G\cong\mathbb{Z}^r\oplus\mathbb{Z}/p_1^{n_1}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p_k^{n_k}\mathbb{Z}.$$

Observation 1: G is finite, so r must be 0;

Observation 2: For each prime number $p_e\geq 2$, combine all the similar terms $\mathbb{Z}/p_{e,1}^{n_{e,1}}\mathbb{Z}$, $\mathbb{Z}/p_{e,2}^{n_{e,2}}\mathbb{Z}$, $\mathbb{Z}/p_{e,3}^{n_{e,3}}$, $\cdots$, such that $n_{e,1}\geq n_{e,2}\geq n_{e,3}\geq\cdots$

Hence, we obtain the Classification theorem of finite Abelian groups:

$$G\cong\overbrace{\left(\mathbb{Z}/p_{1,1}^{n_{1,1}}\mathbb{Z}\oplus\mathbb{Z}/p_{1,2}^{n_{1,2}}\mathbb{Z}\oplus\cdots\right)}^{p_1\text{ part}}\oplus\overbrace{\left(\mathbb{Z}/p_{2,1}^{n_{2,1}}\mathbb{Z}\oplus\mathbb{Z}/p_{e,2}^{n_{e,2}}\oplus\cdots\right)}^{p_2\text{ part}}\oplus\cdots$$

(3) Proof: Assume to the contrary that a finite subgroup H of $K^\times$ is not cyclic.
According to the classification theorem of finite Abelian groups, for some prime number $p \geq 2$, $\mathbb{Z}_p \times \mathbb{Z}_p$ is embedded in $K^\times$.
Assume that the embedded image of $\mathbb{Z}_p \times \mathbb{Z}_p$ in $K^\times$ is $\{a^k b^l : 1 \leq k, l \leq p\}$.
We see that $(a^k b^l)^p = (a^p)^k (b^p)^l = 1^k 1^l = 1$, so a polynomial $x^p - 1$ of degree p has $p^2 > p$ roots, contradicting to the assumption that K is a field.

(4) Proof: Let L/K be a finite field extension.
As $L^\times$ is a finite subgroup of $L^\times$, it is cyclic.
Take a generator g of $L^\times$, we see that $L = \mathrm{Split}_K(x^{|L|} - x)$
$= \mathrm{Split}_K\left(x \prod_{k=0}^{|L|-1} (x - g^k)\right) = K[g]$ is simple.

7. Proof: It is clear that $q(\alpha) = 0$. To see why it is the minimal polynomial of α over K:

Step 1: We show that $q(x) \in K[x]$.

According to Vieta's theorem, $q(x) = \sum_{t=0}^{r} x^{r-t} (-1)^t \sum_{k_1, \cdots, k_t} \alpha_{k_1} \cdots \alpha_{k_t}$,
where each $\sum_{k_1, \cdots, k_t} \alpha_{k_1} \cdots \alpha_{k_t} \in L^G = K$ by the Galois correspondence.
Hence, $q(x) \in K[x]$

Step 2: We show that $q(x)$ is irreducible over K.

As $G * \alpha = \{\alpha_1, \alpha_2, \cdots, \alpha_r\}$, every $f(x) \in K[x]$ with $f(\alpha) = 0$ must satisfy $f(\alpha_2) = \cdots = f(\alpha_r) = 0$, because there is a relative field automorphism sending α_1 to α_j. Hence $q(x)$ is of minimal degree, it is irreducible over K.

8. 1): Proof. Take a nonzero element $1 \in M$,
and extend it to a basis $1, \alpha$ of M over $\mathbb{Q}$.

As $\alpha^2 \in M = \mathrm{span}_{\mathbb{Q}}\{1, \alpha\}$, for some $a, b \in \mathbb{Q}$, $\alpha^2 + a\alpha + b = 0$.

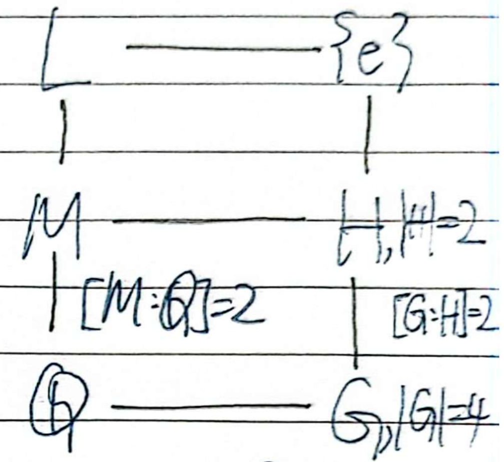
Hence, $M = \mathbb{Q}[\alpha] = \mathbb{Q}\left[\frac{-a \pm \sqrt{a^2-4b}}{2}\right] = \mathbb{Q}[\sqrt{a^2-4b}]$.

by clearing the content of a^2-4b and simplifying the radical,
a^2-4b be comes a square-free positive integer, because otherwise
5 $M = \mathbb{Q}$, contradicting to our assumption that $[M:\mathbb{Q}] = 2$.

8.2) Proof: Assume that $G = Gal(L/\mathbb{Q})$.

As $L/\mathbb{Q}$ is Galois, $|G| = [L:\mathbb{Q}] = 4$.

Case 1: If $L \subseteq \mathbb{R}$, then according to Cauchy's theorem, G has a subgroup H of order 2. According to Galois correspondence, for some intermediate field extension $\mathbb{Q} \subseteq M \subseteq L$, then index $[M:\mathbb{Q}] = [G:H] = 4/2 = 2$, so $\mathbb{Q} \subseteq M \subseteq L \subseteq \mathbb{R}$ is a real quadratic extension of $\mathbb{Q}$.



Case 2: If $L \not\subseteq \mathbb{R}$, then according to primitive element theorem, $L = \mathbb{Q}[\alpha]$ for some $\alpha \in L \setminus \mathbb{Q}$. Assume that the irreducible polynomial of α over $\mathbb{Q}$ is $f(x)$. As $L/\mathbb{Q}$ is Galois, $f(x)$ completely splits, so $\bar{\alpha} \in R_f \subseteq L = \mathbb{Q}[\alpha]$, $\alpha + \bar{\alpha}, \alpha\bar{\alpha} \in \mathbb{Q}[\alpha] \cap \mathbb{R}$. We see that $\mathbb{Q}[\alpha] / \mathbb{Q}[\alpha+\bar{\alpha}, \alpha\bar{\alpha}]$ is a degree 2 extension, so by tower theorem, $\mathbb{Q}[\alpha+\bar{\alpha}, \alpha\bar{\alpha}]$ is real quadratic over $\mathbb{Q}$.