Final Exam

(1) Let $B = \{b_i\}_{i \in I}$ be a basis for F.

Then $F \cong \bigoplus_{i \in I} \mathbb{Z} b_i$. Since $\bigcap_{n=1}^{\infty} n(\mathbb{Z} b_i) = 0$,

$$\bigcap_{n=1}^{\infty} nF = \bigcap_{n=1}^{\infty} n \bigoplus_{i \in I} \mathbb{Z} b_i \underset{(A)}{\subseteq} \bigcap_{n=1}^{\infty} \bigoplus_{i \in I} n\mathbb{Z} b_i \underset{(B)}{\subseteq} \bigoplus_{i \in I} \bigcap_{n=1}^{\infty} n\mathbb{Z} b_i = 0. \quad //$$

(A) If $\sum_{i \in I} k_i b_i$, where $k_i \in \mathbb{Z}$, and all by finitely many $k_i \neq 0$, then $n \sum_{i \in I} k_i b_i = \sum_{i \in I} n k_i b_i$.

(B) If $\sum_{i \in I} k_i b_i \in \left(\bigoplus_{i \in I} n\mathbb{Z} b_i\right) \cap \left(\bigoplus_{i \in I} m\mathbb{Z} b_i\right)$ Then $\forall i$, $k_i \in n\mathbb{Z} b_i \cap m\mathbb{Z} b_i$.

Thus $\bigcap_{n=1}^{\infty} nF = 0$.

② (a) $\mathbb{Q} \oplus \mathbb{Z}$ is flat

ISTS $\mathbb{Q}$ and $\mathbb{Z}$ are flat.

- Since $\mathbb{Z}$ is free as a $\mathbb{Z}$-module, $\mathbb{Z}$ is projective and hence flat.
- Let $0 \longrightarrow M \longrightarrow N$ be an exact seqn. of $\mathbb{Z}$-module.

  Since localization is flat, $0 \longrightarrow \mathbb{Q} \otimes M \longrightarrow \mathbb{Q} \otimes N$ is an exact sequence (of $\mathbb{Q}$-modules, but also of $\mathbb{Z}$-modules).

  Hence $\mathbb{Q}$ is flat as a $\mathbb{Z}$-module.
- $\Rightarrow$ $\mathbb{Q} \oplus \mathbb{Z}$ is flat.

(b) • $\mathbb{Q} \oplus \mathbb{Z}$ is not projective because $\mathbb{Q}$ is not projective:

If $\mathbb{Q}$ were projective, then $F = \mathbb{Q} \oplus C$ where F is a free $\mathbb{Z}$-module.

But $\mathbb{Q} = n\mathbb{Q}$, so $\mathbb{Q}$ cannot be viewed as a submodule of F.

- $\mathbb{Q} \oplus \mathbb{Z}$ is not injective because $\mathbb{Z}$ is not injective, since $\mathbb{Z}$ is not divisible.

(3) Since is skew symmetric, $A^T = -A$.

Therefore $A^2 = -A^TA$

- A^TA is symmetric: $(A^TA)^T = A^TA^{TT} = A^TA$.
- Since A is invertible, $A \in Mat_{n\times n}(\mathbb{R})$ for some n.

Let $v \in \mathbb{R}^n$, where $v \neq 0$. Let $w = Av \neq 0$ as A is invertible.

Then $v^T(A^TA)v = (Av)^T(Av) = w \cdot w > 0$.

Therefore $v^T(-A^TA)v = -w\cdot w < 0$,

so $A^2 = -A^TA$ is negative definite.

(4) Recall $\mathbb{F}_m = \mathbb{F}_{p^k} = \{\text{roots of } x^{p^k} - x = 0\}$.

Observe $x^{p^k} - x = x(x^{p^k-1} - 1) = x \prod_{n | p^k} \Phi_n(x)$.

Since $d \mid p^k - 1$, $\Phi_d(x)$ splits over $\mathbb{F}_{p^k}$ (since $x^{p^k}-x$ splits here).

Finally, the roots of $\Phi_d(x)$ are precisely the elements of $\mathbb{F}_{p^k}^\times$ (a cyclic group) of order d; there are $(p^k-1)/d$ elements α where $\alpha^d = 1$; $\varphi(d)$ of these have order d.

(5) $\alpha = \sqrt{1+\sqrt{2}}$

(a) $\alpha^2 = 1+\sqrt{2} \Rightarrow \alpha^2 - 1 = \sqrt{2} \Rightarrow (\alpha^2-1)^2 = 2$

$\Rightarrow \alpha$ is a root of $(x^2-1)^2 - 2 = x^4 - 2x^2 + 1 - 2 = x^4 - 2x^2 - 1 =: f(x)$

Check that $f(x)$ is irreducible over $\mathbb{Q}$:

- By the Rational Root Theorem, the only possible linear factors of $f(x)$ are $(x+1)$ and $(x-1)$.

  But $f(-1) = 1-2-1 = -2 = f(1)$, $\neq 0$.

- Check for quadratic factors with α as a root:

  Since $f(x)$ is an even function, $-\alpha$ is also a root, $m_{-\alpha,\mathbb{Q}}(x) = m_{\alpha,\mathbb{Q}}(x)$. So if $m_{\alpha,\mathbb{Q}}(x) \neq f(x)$, then $m_{\alpha,\mathbb{Q}}(x) = (x-\alpha)(x+\alpha) = x^2 - 2\alpha x - \alpha^2 \in \mathbb{Q}[x]$.

  Clearly, $-2\alpha \notin \mathbb{Q}[x]$. Therefore $f(x)$ is irreducible (and monic), so $m_{\alpha,\mathbb{Q}}(x) = x^4 - 2x^2 - 1$.

(b) From $(\alpha^2-1)^2 = 2$, we see that if γ is a root of $f(x)$, then $\gamma^2 - 1 = \pm\sqrt{2} \Rightarrow \gamma^2 = 1 \pm \sqrt{2} \Rightarrow \gamma = \pm\sqrt{1 \pm \sqrt{2}}$.

Let $\beta = \sqrt{1-\sqrt{2}}$. Then the roots of $m_{\alpha,\mathbb{Q}}(x) = \{\pm\alpha, \pm\beta\}$, so the splitting field of $m_{\alpha,\mathbb{Q}}(x)$ is

$$\mathbb{Q}(\alpha,\beta) = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}\right).$$

This is Galois because it's the splitting field of a separable polynomial. No subfield $K \subsetneq \mathbb{Q}(\alpha,\beta)$ can be the Galois closure of $\mathbb{Q}(\alpha)$, since the irreducible $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$ with root $\alpha \in K$ does not split over K.

Therefore $\mathbb{Q}(\alpha,\beta)$ is the Galois closure of $\mathbb{Q}(\alpha)$.

⑥ Let $f(x)=x^4+1$.

(a) Recall $f(x)$ is irreducible in $\mathbb{Z}[x]$ because $(x+1)^4+1$ is Eisenstein at $p=2$.

Over $\mathbb{F}_3[x]$, $f(x)=x^4+1=x^4-2$.

Since $f(0), f(1), f(-1) \neq 0$, there are no linear factors.

We just need to check for quadratic factors.

$$(x^2+ax+b)(x^2+\alpha x+\beta)$$

$$= x^4 + \underbrace{(a+\alpha)}_{a=-\alpha}x^3 + (b+\beta+a\alpha)x^2 + (\underbrace{a\beta+b\alpha}_{a=-\alpha})x + \underbrace{b\beta}_{\substack{b=\beta \\ \text{either } 1 \text{ or } 2}}$$

Consider $b=\beta=2$, $a=1$, $\alpha=-1$.

Thus $(x^2+x-1)(x^2-x-1)=x^4+1$.

Since $f(x)$ has no linear factors, these quadratic factors are irreducible.

(b) $\mathrm{Gal}(f(x)/\mathbb{Q})$

Note $(x^4+1)(x^4-1)=x^8-1$. The roots of $f(x)$ are the primitive 8^{th} roots of unity. The splitting field is $\mathbb{Q}(\zeta_8)$, a degree 4 extension of $\mathbb{Q}$. The Galois group is of order 4. Since the automorphism $\sigma: \mathbb{Q}(\zeta_8) \longrightarrow \mathbb{Q}(\zeta_8)$ fixing $\mathbb{Q}$ is determined by $\sigma(\zeta_8)$, which must be another root of $f(x)$, we can check if there are any automorphisms of order 4:

- If $\sigma(\zeta)=\zeta$, then $|\sigma|=1$.
- If $\sigma(\zeta)=\zeta^3$, then $\zeta \mapsto \zeta^3 \mapsto \zeta^9=\zeta$, so $|\sigma|=2$.
- If $\sigma(\zeta)=\zeta^{-1}$, then $|\sigma|=2$.
- If $\sigma(\zeta)=\zeta^{-3}$ then $\zeta \mapsto \zeta^{-3} \mapsto \zeta^9=\zeta$ so $|\sigma|=2$.

Therefore $\mathrm{Gal}(f(x)/\mathbb{Q}) \cong C_2 \times C_2$.

(c) Over $\mathbb{F}_3$, we saw that $f(x) = \underbrace{(x^2+x-1)}_{g(x)}\underbrace{(x^2-x-1)}_{h(x)}$

Let α be a root of $g(x)$. Then $\mathbb{Q}(\alpha)$ is a splitting field of $g(x)$.

Note $[\mathbb{F}_3(\alpha):\mathbb{F}_3]=2$. So the elements of $\mathbb{F}_3(\alpha)$ are of the form

$\{a+b\alpha \mid a,b \in \mathbb{F}_3\}$, where $\alpha^2=1-\alpha$.

Compute
$$h(a+b\alpha) = (a+b\alpha)^2-(a+b\alpha)-1$$
$$= a^2+2ab\alpha+b^2(1-\alpha)-a-b\alpha-1$$
$$=(a^2+b^2-a-1)+(2ab-b^2-b)\alpha.$$

If $b\neq 0$, then $a^2+b^2-a-1 = a^2+1-a-1 = a^2-a=0 \Rightarrow a=1$.

Then $2ab-b^2-b = 2b-b^2-b = b-b^2=0 \Rightarrow b=1$.

So $h(1+\alpha) = (1+\alpha)^2-(1+\alpha)-1$
$$=1^2+2\alpha+\alpha^2-1-\alpha-1$$
$$=\alpha^2+\alpha-1=0$$

$\Rightarrow h(x)$ also splits over $\mathbb{F}_3(\alpha)$.

$\Rightarrow f(x)$ splits over $\mathbb{F}_3(\alpha)$. So $\mathrm{Gal}(f(x)/\mathbb{F}_3) \cong C_2$.