Galois Theory Mock Exam

1. (a) <u>Eisenstein's Criterion</u>

Let $f(X) = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$.
If $\exists$ prime p s.t. • $p \nmid a_n$ • $p \mid a_i$ $(0 \leq i \leq n-1)$ • $p^2 \nmid a_0$
then f is irreducible over $\mathbb{Q}$.

b) <u>Converse:</u> Let $f(X) \in \mathbb{Z}[X]$, $f(X) = \sum_{i=0}^{n} a_iX^i$.
If f is irred over $\mathbb{Q}$ then $\exists$ prime p s.t. $p \nmid a_n$, $p \mid a_i$ $(0 \leq i \leq n-1)$, $p^2 \nmid a_0$.

False: eg $X^2+1 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$ but no such p exists.

c) (i) $f(X) = 3X^5 + 6X^4 + 18X^3 + 12X + 2$

Take $p = 2$ & use Eisenstein $\Rightarrow$ f irred over $\mathbb{Q}$.

ii) $g(x) = 3X^5 + 6X^4 + 18X^3 + 12X + 4$

Can't apply Eisenstein (would need $p=2$ but $2^2 \mid 4$).
Can we apply an adjustment to g?

$$X^5 g\left(\tfrac{1}{X}\right) = \underbrace{4X^5 + 12X^4 + 18X^2 + 6X + 3}_{\text{Irreducible by Eisenstein using } p=3} = g_1, \text{ say}$$

Any factorization of g would lead to a factorization of g_1, impossible. So g irred. over $\mathbb{Q}$.

iii) Tutorial question.

$h(x) = \dfrac{X^p - 1}{X - 1}$. Let $h_1(X) := h(X+1)$;

then $h_1(X) = \frac{1}{X}\left((X+1)^p - 1\right) = \sum_{i=0}^{p-1} \binom{p}{i} X^{p-i-1}$.

Now $p \mid \binom{p}{i}$ for $1 \leq i \leq p-1$. So can apply

Eisenstein to see that h_1 is irredubible.
If $h = uv$ is a proper factorization of h,

$$h_1(X) = u(X+1)\,v(X+1),$$

a proper factorization of h_1 - impossible
So h irred. over $\mathbb{Q}$.

2. a) Splitting field of f over F : an extension K of F st f splits completely over K & does not split completely over any proper subfield of K.

b) Since $\alpha \in K$ and $F \subseteq K$, $F(\alpha) \subseteq K$; subfield by defn.

Clearly f does not split over any proper subfield, as $F(\alpha)$ is smallest containing F and root α.

Why does f split over $F(\alpha)$?

Over $F(\alpha)$, $f(X) = (X-\alpha)\,g(X)$ where $g(X)$ has degree 1.
So $g(X) = (X-\beta) \in F(\alpha)[X]$, ie $\beta \in F(\alpha)$,
ie f splits over $F(\alpha)$.

c) Let $f \in F[X]$ and let K be its splitting field over F.
Then $Gal(f)$ is $Gal(L:K)$, the set of all automorphisms of L which fix K pointwise.

d) $f = (x^2-2)(x^2+1)$.

Splitting field for f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, i)$.

$$\begin{array}{l} \mathbb{Q}(\sqrt{2},i) \\ \quad | \quad 2 \\ \mathbb{Q}(\sqrt{2}) \\ \quad | \quad 2 \\ \mathbb{Q} \end{array}$$

Degree of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is 2; min poly x^2-2, ($\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$)

Degree of $\mathbb{Q}(\sqrt{2})(i)$ over $\mathbb{Q}(\sqrt{2})$ is 2; min poly x^2+1 ($\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$).

By Tower Law, degree of $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$ is 4.

Gal(f) has order 4.

Let $\sigma \in$ Gal(f); σ maps roots to roots so

$$\sqrt{2} \mapsto \pm\sqrt{2}$$
$$i \mapsto \pm i$$

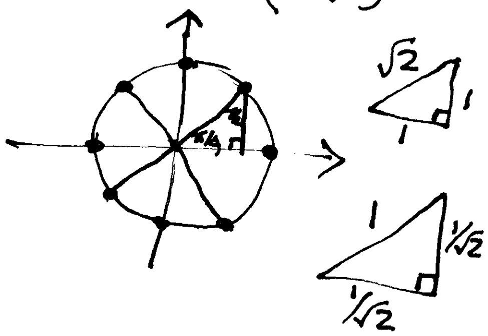
4 options: identity and 3 maps of deg 2.

Gal(f) $\cong K_4$.

$g = (x^4+1)$

Root ξ of g satisfies $\xi^4 = -1 = e^{k\pi i}$, k odd

$$\xi = e^{\frac{\pi i}{4}}, e^{\frac{3\pi i}{4}}, e^{\frac{5\pi i}{4}}, e^{\frac{7\pi i}{4}}$$



primitive 8th roots of 1

$$e^{\frac{\pi i}{4}} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} = \frac{1}{2}(\sqrt{2}+i\sqrt{2})$$

$$e^{\frac{3\pi i}{4}} = \frac{1}{2}(\sqrt{2}-i\sqrt{2}), \quad e^{\frac{5\pi i}{4}} = \frac{1}{2}(-\sqrt{2}+\sqrt{2}i)$$

$$e^{\frac{7\pi i}{4}} = \frac{1}{2}(-\sqrt{2}-\sqrt{2}i)$$

Splitting field is $\mathbb{Q}(\sqrt{2}, i)$.

Same situation as above.

Clearly isomorphic; both are $\mathbb{Q}(\sqrt{2}, i)$.

(4)

3. a) FTGT - bookwork

b) $f = X^4 - 5$

E = splitting field of f over $\mathbb{Q}$

$G = \mathrm{Gal}(E:\mathbb{Q})$.

(i) f is irreducible over $\mathbb{Q}$ by Eisenstein (take $p=5$).

If $f(\beta)=0$, $\beta^4 = 5$

$$\left(\frac{\beta}{5^{1/4}}\right)^4 = 1$$

ie $\frac{\beta}{5^{1/4}} \in \{1,-1,i,-i\}$

So roots are $5^{1/4}, -5^{1/4}, i5^{1/4}, -i5^{1/4}$

Clearly f splits in $\mathbb{Q}(\alpha, i)$ (where $\alpha = 5^{1/4}$), since all roots lie in this field.

To show: f does not split in a smaller field.

Clearly $i \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

Also, $\alpha = 5^{1/4} \notin \mathbb{Q}(i)$ since $5^{1/4}$ is irrational.

So $\mathbb{Q}(\alpha, i)$ is smallest over which f splits.

(ii) Tower Law: for fields $F \subseteq K \subseteq L$,

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

We have splitting field $\mathbb{Q}(\alpha, i)$ over $\mathbb{Q}$:

$$[\mathbb{Q}(\alpha,i):\mathbb{Q}] = \underbrace{[\mathbb{Q}(\alpha,i):\mathbb{Q}(\alpha)]}_{\substack{\text{degree 2, min} \\ \text{poly } X^2+1\text{, since} \\ \mathbb{Q}(\alpha)\subseteq\mathbb{R}\not\ni i}}\underbrace{[\mathbb{Q}(\alpha):\mathbb{Q}]}_{\substack{\text{degree 4,} \\ \text{min poly } X^4-5\text{,} \\ \text{irred by Eisenstein}}} \text{ by Tower Law}$$

So $[E:\mathbb{Q}]=8$.

By theory, $|Gal(E:\mathbb{Q})| = [E:\mathbb{Q}]$
if $E:\mathbb{Q}$ is a Galois extension.

Normal? E is a splitting field by defn
Separable? Char 0

So $|Gal(f)| = |Gal(E:\mathbb{Q})| = [E:\mathbb{Q}] = 8$.

iii) $\sigma(\alpha)=i\alpha \Rightarrow \sigma(-\alpha)=-i\alpha$, ~~so~~
$\sigma(i\alpha)=\sigma(i)\sigma(\alpha)=ii\alpha=-\alpha \Rightarrow \sigma(-i\alpha)=\alpha$
Thus σ permutes the roots of f so
$\sigma \in Gal(E:\mathbb{Q})$.

$\tau(\alpha)=\alpha \Rightarrow \tau(-\alpha)=-\alpha$.
$\tau(i\alpha)=-i\alpha \Rightarrow \tau(-i\alpha)=i\alpha$

τ permutes the roots of f, so $\tau \in Gal(E:\mathbb{Q})$.

iv)

	id	τ	σ					
α	α	α	$i\alpha$	$i\alpha$	$-\alpha$	$-\alpha$	$-\alpha i$	$-i\alpha$
i	i	$-i$	i	$-i$	i	$-i$	i	$-i$
(k,l) s.t. elt is $\sigma^k\tau^l$	$(0,0)$	$(0,1)$	$(1,0)$	$(3,1)$	$(2,0)$	$(2,1)$	$(3,0)$	$(1,1)$.

All images covered, so
each aut has this form.

v) $\alpha \cdot \tau\sigma\tau^{-1} = \alpha\sigma\tau^{-1} = (i\alpha)\tau^{-1} = -i\alpha$

$i \cdot \tau\sigma\tau^{-1} = (-i)\sigma\tau^{-1} = (-i)\tau^{-1} = i.$

So $\tau\sigma\tau^{-1} = \sigma^3 = \sigma^{-1}$!

vi) Group is D_8.

Subgroups of D_8 of order 2 $\longleftrightarrow$ subfields of index 4.

Elt^s of order 2 are $\sigma^i\tau$, $0 \le i \le 3$ and σ^2.

By the Fundamental Th^m, the 5 subgroups of order 2 generated by these elements yield precisely 5 subfields of order 4.

$\tau\sigma = \sigma^{-1}\tau$ by v) so

$$\sigma^{-1}\sigma^i\tau\sigma = \sigma^{i-1} \cdot \sigma^{-1}\tau$$
$$= \sigma^{i-2}\tau$$
$$\neq \sigma^i\tau.$$

$\sigma^{-1}\sigma^2\sigma = \sigma^2$, $\tau^{-1}\sigma^2\tau = \sigma^2$

So $\langle\sigma^2\rangle$ only normal subgroup.

Hence by Fundamental Th^m there is a unique normal extension.

vii) $\mathbb{Q}(i\sqrt{5})$ is a degree 2 extension of $\mathbb{Q}$, so an index 4 subfield of E, so corresponds to a subgroup of order 4.

$i\sqrt{5} = i\alpha^2$.

$(i\alpha^2)\sigma = -i\alpha^2$ so fixed by σ^2.

$(i\alpha^2)\tau = -i\alpha^2$ so fixed by $\sigma\tau, \sigma^3\tau$.

Group is $\{1, \sigma\tau, \sigma^2, \sigma^3\tau\}$.

Q4 a) Bookwork.

b) Bookwork.

c) Bookwork.

d) $K = \mathbb{Q}(\epsilon)$.

ϵ has minimum polynomial dividing $X^n - 1$, so $G = Gal(K:\mathbb{Q})$ sends ~~ϵ~~ to other n^{th} roots of unity.

Since K is generated by ϵ over $\mathbb{Q}$, to define an element of G it suffices to specify the image of ϵ.

Let $\sigma, \tau \in Gal(K:\mathbb{Q})$, and s'pose

$$\sigma : \epsilon \mapsto \epsilon^i$$
$$\tau : \epsilon \mapsto \epsilon^j.$$

Then $\sigma\tau(\epsilon) = \epsilon^{i+j} = \tau\sigma(\epsilon)$,

so $\sigma\tau = \tau\sigma$ and G is abelian.

e) $E = \mathbb{Q}(\epsilon, \alpha)$; $K = \mathbb{Q}(\epsilon)$.

E is the splitting field for $X^n - 2$ over $\mathbb{Q}$, so is Galois over $\mathbb{Q}$.

The roots of $x^n - 2$ are
$$\alpha, \varepsilon\alpha, \ldots, \varepsilon^{n-1}\alpha.$$
Elements of $Gal(E:K)$ must fix ε, so to describe an element of $H \in Gal(E:K)$ it suffices to define image of α.

Let $\sigma \in H$, $\alpha\sigma = \varepsilon^i\alpha$
$$\tau \in H, \alpha\tau = \varepsilon^j\alpha$$
Then
$$\alpha\sigma\tau = \varepsilon^{i+j}\alpha = \alpha\tau\sigma,$$
so $\sigma\tau = \tau\sigma$ & H is abelian.

Since K is a splitting field for $x^n - 1$, K is normal over $\mathbb{Q}$, so $Gal(E:K)$ is a normal subgp of $Gal(E:\mathbb{Q})$ that is abelian, and
$$\frac{Gal(E:\mathbb{Q})}{Gal(E:K)} \cong Gal(K:\mathbb{Q})$$

is also abelian, so $Gal(E:\mathbb{Q})$ is a group with an abelian normal subgroup and abelian quotient, so is soluble.