Practice Final Exam Solutions

1.) Let p be prime and F field, $\operatorname{char} F = p$. Show $f(x) = x^{p^n} - x$ over F has distinct zeros.

pf:
For $f(x) = x^{p^n} - x$ $f'(x) = p^n x^{p^n - 1} - 1 \equiv -1$ since $\operatorname{char} F = p$

so f and f' don't have any common factor of positive deg. so by Prev. Thm f doesn't have any multiple zeros in any extn of F. □

2.) Let p be prime and $F = \mathbb{Z}_p(t)$. Let $f(x) = x^p - t$. Show $f(x)$ is irred. over F and has multiple zero in $K = F[x]/(x^p - t)$.

pf:
TS show irred. of $f(x)$, we'll show it has no zeros in F. since $\frac{h(t)}{k(t)}$ is a zero of $f(x)$ w/ $\frac{h(t)}{k(t)} \in F$. w/ $\deg h = m$, $\deg k = n$ Th $f\left(\frac{h}{k}\right) = 0 \Rightarrow \left(\frac{h(t)}{k(t)}\right)^p = t$

$\Rightarrow (h(t))^p = t(k(t))^p$ since $\mathbb{Z}_p$ is finite $\Rightarrow F$ is perfect field

so $h(t^p) = t\,k(t^p) \Rightarrow \deg h(t^p) = pm$ and $\deg(k(t^p)) = p^n$

but by $\uparrow$ $\Rightarrow pm = pn + 1 \Rightarrow p \mid 1$ contra so no zeros in F.

Now $f'(x) = px^{p-1}$ as t constant. But $p \mid p \Rightarrow f'(x) = 0$. so f and f' have common factor $\Rightarrow$ has multiple zero in some extension namely in $F[x]/\langle f(x)\rangle$. □

3.) find min. poly of $\alpha = \sqrt{-1} + \sqrt{3}$ over $\mathbb{Q}$.

pf:
set $\alpha = \sqrt{-1} + \sqrt{3}$ so $\alpha^2 = (\sqrt{-1} + \sqrt{3})^2 = -1 + 2\sqrt{-3} + 3 \Rightarrow \alpha^2 - 2 = 2\sqrt{3}$

$\Rightarrow (\alpha^2 - 2)^2 = (2\sqrt{-3})^2 = 4(-3) \Rightarrow \alpha^4 - 2\alpha^2 + 4 = -12$ or $\alpha^4 - 6\alpha^2 + 16 = 0$

so $p(x) = x^4 - 2x^2 + 16$ for irred. use ~~substitution~~ rat'l root thm. ~~⊗~~

4⊗ $\Rightarrow p(x)$ has no linear factors so it can't have cubic. A direct check shows $p(x)$ has no quadratic factors either. □

4.) find min. poly of $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$.

pf:
set $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$ Th $\alpha^3 = (\sqrt[3]{2} + \sqrt[3]{4})^3 = 2 + 3\sqrt[3]{4}\sqrt[3]{4} + 3\sqrt[3]{2}\sqrt[3]{16} + 4$

$\Rightarrow \alpha^3 = 6 + 3\cdot 2\sqrt[3]{2} + 3\cdot 2\sqrt[3]{4} = 6(1 + \sqrt[3]{2} + \sqrt[3]{4}) = 6(1 + \alpha)$

so $\alpha^3 - 6\alpha - 6 = 0 \Rightarrow p(x) = x^3 - 6x - 6$. for irred. use Eisenstein w/ $p = 2$ or 3 Th $3 \nmid 1$, $3 \mid 6$, $3^2 \nmid 6$ □.

5.) let a be complex # over $\mathbb{Q}$ that is algebraic. show $\sqrt{a}$ is algebraic over $\mathbb{Q}$.

pf:
since a algebraic $\Rightarrow \exists\, p(x) \in \mathbb{Q}[x]$ s.t. $p(a)=0$ set $p(x) = c_m x^m + \cdots + c_0$
then consider $q(x) = c_m x^{2m} + c_{m-1} x^{2m-2} + \cdots + c_0$ then $q(\sqrt{a}) = c_m a^m + \cdots + c_0 = p(a) = 0$
so $\sqrt{a}$ algebraic. in general set $q(x) = c_m x^{2^n m} + \cdots + c_0$ then $q(\sqrt[2^n]{a}) = p(a) = 0$. ☐

6.) let F be a field and α, β transc. over F. Prove either $\alpha\beta$ or $\alpha+\beta$ are trans.

pf:
suppose both $\alpha\beta$, $\alpha+\beta$ are algebraic over F then $\exists$ some algebraic ext E of F s.t. $\alpha\beta, \alpha+\beta \in E$ Notice $f(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$ in E
$\Rightarrow \alpha, \beta \in E \Rightarrow \alpha, \beta$ are algebraic contradiction. so at one of $\alpha\beta$, $\alpha+\beta$ must be trans. ☐

7.) let $p(x) = x^3 - 2$. Over $\mathbb{Q}$. Do the Galois Analysis.

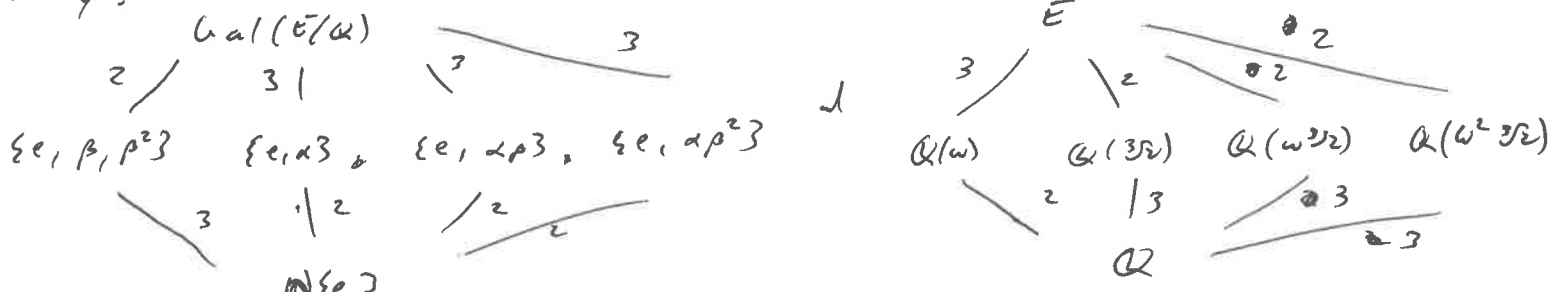
pf:
$p(x)$ is irred. over $\mathbb{Q}$ via Eisenstein w/ $p=2$ as $2 \mid 2$, $2 \nmid 1$ and $2^2 \nmid 2$.
know one root is $a = \sqrt[3]{2}$. since $a^3 = 2$. the other roots come from $x^3 - 1$
namely ω, ω^2 from $x^3 - 1 = (x-1)(x^2+x+1)$ the quadratic. know if ω is one of the ω^2 is the other. so the roots to $p(x)$ are $a, a\omega, a\omega^2$ Claim $E = \mathbb{Q}(a, \omega)$
is the splitting field since $a, a\omega, a\omega^2 \in E$ and $p(x)$ is irred over $\mathbb{Q}$ and $\mathbb{Q}(\omega)$
and x^2+x+1 irred over $\mathbb{Q}$ and $\mathbb{Q}(a)$. still $\omega^2 \in E$ since $\omega \in E$.
Th $[E:\mathbb{Q}] = [E:\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}] = 3 \cdot 2 = 6$ so $|Gal(E/\mathbb{Q})| = 6$. need to construct automorphisms $\varphi: E \to E$ that fix $\mathbb{Q}$. Consider:

$e: \begin{cases} \omega \mapsto \omega \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{cases}$, $\alpha: \begin{cases} \omega \mapsto \omega^2 \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{cases}$, $\beta: \begin{cases} \omega \mapsto \omega \\ \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \end{cases}$. Then $\beta^2: \begin{cases} \omega \mapsto \omega \\ \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \end{cases}$

and $\beta^3 = e$ as $\omega^3 = 1$. Then $\alpha\beta: \begin{cases} \omega \mapsto \omega^2 \\ \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \end{cases}$ and $(\alpha\beta)^2 = e$

Finally $\alpha\beta^2: \begin{cases} \omega \mapsto \omega^2 \\ \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \end{cases}$ and $(\alpha\beta^2)^2 = e$. so found all six elements

so $Gal(E/\mathbb{Q}) = \{e, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\}$. $\Rightarrow Gal(E/\mathbb{Q}) \cong \mathbb{Z}_6$ or S_3
but $(\alpha\beta)(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$ and $(\beta\alpha)(\sqrt[3]{2}) = \omega\sqrt[3]{2} \Rightarrow \alpha\beta \neq \beta\alpha \Rightarrow$ non Abelian so $Gal(E/\mathbb{Q}) \cong S_3$
finally:



8.) Let $p(x) = x^4 - 7x^2 + 10$. Do the Galois Analysis.

pf:

Notice $p(x) = (x^2 - 2)(x^2 - 5)$ both factors are irred. using Eisenstein w/ prime 2 and 5 respectively. Can see roots are easily $\pm\sqrt{2}$ and $\pm\sqrt{5}$. Claim: $E = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ is the splitting field since $x^2 - 2$ is irred. over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$ and similarly $x^2 - 5$ is irred. over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$ thus $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$ so $|Gal(E/\mathbb{Q})| = 4$

need to construct the automorph. $\varphi : E \to E$ that fix $\mathbb{Q}$. Consider:

$e : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}$, $\alpha : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{5} \mapsto \oplus\sqrt{5} \end{cases}$, $\beta : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$ then $\alpha\beta : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$

and $\alpha^2 = \beta^2 = (\alpha\beta)^{**2} = e$ so this is all of them. so $Gal(E/\mathbb{Q}) = \{e, \alpha, \beta, \alpha\beta\}$

Since $|Gal(E/\mathbb{Q})| = 2^2$ and 2 is prime we know ~~all~~ groups of order p^2 p-prime are Abelian. so $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, but all the elmts have order 2 so $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ □.

9.) Let p - odd prime. Let $g(x) = x^p - 1$. Do Galois analysis.

pf:

Notice $g(x) = (x-1)(x^{p-1} + x^{p-2} + \dots + 1)$ into 2 irreducible factors. 1^{st} factor is done so irred. and by shifting $x \mapsto x+1$ use Eisenstein w/ prime p. All the roots of $g(x)$ are the p^{th} roots of unity: $1, \omega, \omega^2, \dots, \omega^{p-1}$ so splitting field is $E = \mathbb{Q}(\omega)$ so $[E : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = p-1$ so $|Gal(E/\mathbb{Q})| = p-1$ need to construct the automorph. $\varphi : E \circlearrowleft$ w/ φ fixing $\mathbb{Q}$. Consider:

$e : \omega^k \to \omega^k$ for $k = 1, \dots, p-1$ and $\alpha_k : \omega \mapsto \omega^k$ for $k = 2, \dots, p-1$ then $e, \alpha_2, \dots, \alpha_{p-1}$ are all the automorphisms

So $Gal(E/\mathbb{Q}) = \{e, \alpha_2, \dots, \alpha_{p-1}\}$. Notice now $\alpha_k(\omega^i \omega^l) = \alpha_k(\omega^{i+l}) = \omega^{k(i+l)} = \omega^{ki}\omega^{kl}$
$= \alpha_k(\omega^i)\,\alpha_k(\omega^l)$

so this is a natural correspondence w/ $\mathbb{Z}_{p-1}$ w/ mapping $k \mapsto \alpha_k$ for if $\overset{i,l}{a} \in \mathbb{Z}_{p-1}$
$(\alpha_j \circ \alpha_l)(\omega) = \alpha_j(\omega^l) = \alpha_j(\omega^i)^l = \omega^{il} = \alpha_{jl}(\omega)$. so $\uparrow$ is a homom.

but if $j \neq l$ then $\omega^i \neq \omega^l$ so $\uparrow$ and by def. it's onto so $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_{p-1}$

then $Gal(E/\mathbb{Q}) = \langle a \rangle$

$\langle a \rangle$
$\langle a^2 \rangle$
$\vdots$
$\langle a^{p-2} \rangle$
$\{e\}$

E
$\mathbb{Q}(\omega^{p-2})$
$\vdots$
$\mathbb{Q}(\omega^3)$
$\mathbb{Q}(\omega^2)$
$\mathbb{Q}$

□