Practice Final Exam Solutions

1.) Construct a field w/ 27 elements.

pf:

Consider $p(x) = x^3 + 2x^2 + 1$ over $\mathbb{Z}_3$ then $p(0) = 1$, $p(1) = 1$, $p(2) = 2$ so $p(x)$ is irreducible over $\mathbb{Z}_3$. Thus $\langle p(x) \rangle$ is a maximal ideal in $\mathbb{Z}_3[x]$ as $\mathbb{Z}_3$ is a field. So $\mathbb{Z}_3[x]/\langle p(x)\rangle$ is a field and by div. alg.

if $f(x) \in \mathbb{Z}_3[x]/\langle p(x)\rangle$ $f(x) = p(x)g(x) + r(x)$ w/ deg $r(x) <$ deg $p(x)$ so $r(x) = ax^2 + bx + c$

$\therefore$ $\mathbb{Z}_3[x]/\langle p(x)\rangle = \{ax^2 + bx + c + \langle p(x)\rangle : a, b, c \in \mathbb{Z}_3\}$ so # elements are $3^3 = 27$. $\square$

2.) let $f(x) \in \mathbb{Z}_m[x]$. What criteria is needed on $f(x)$ and m s.t. $\mathbb{Z}_m[x]/\langle f(x)\rangle$ field w/ m^n elements.

pf:

1st need $f(x)$ to be irreducible over a field F then $F[x]/\langle f(x)\rangle$ is a field as $\langle f(x)\rangle$ will be maximal $\therefore$ 1st need $\mathbb{Z}_m$ to be a field so m must be prime then to get m^n elements need $f(x)$ to have degree n as $\mathbb{Z}_m[x]/\langle f(x)\rangle$ will consist of polys w/ degree $n-1$ or less meaning n coefficients w/ m choices for each so m^n elements. $\square$

3.) Show $\mathbb{Q}(4-i) = \mathbb{Q}(1+i)$

pf:

need to show $\mathbb{Q}(4-i) \subseteq \mathbb{Q}(1+i)$ and vice versa. Notice $4-i = 5-(1+i) \Rightarrow 4-i \in \mathbb{Q}(1+i)$ so any $a + b(4-i) \in \mathbb{Q}(1+i)$ for $a, b \in \mathbb{Q}$ $\Rightarrow \mathbb{Q}(4-i) \subseteq \mathbb{Q}(1+i)$. Similarly notice $1+i = 5-(4-i) \in \mathbb{Q}(4-i) \Rightarrow 1+i \in \mathbb{Q}(4-i)$ so any $a + b(1+i) \in \mathbb{Q}(4-i)$ for $a, b \in \mathbb{Q}$ $\therefore \mathbb{Q}(1+i) \subseteq \mathbb{Q}(4-i)$. Thus $\mathbb{Q}(4-i) = \mathbb{Q}(1+i)$. $\square$

4.) let $a, b \in \mathbb{Q}$, $a \neq 0$. show $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ iff $\exists c \in \mathbb{Q}$ s.t. $a = bc^2$.

pf:

($\Rightarrow$) S'pose $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$. if $\sqrt{a} \in \mathbb{Q}$ then $\sqrt{b} \in \mathbb{Q}$ since generic elts of $\mathbb{Q}(\sqrt{a})$ are $c_1 + c_2\sqrt{a}$ and generic elts of $\mathbb{Q}(\sqrt{b})$ are $d_1 + d_2\sqrt{b}$ for $c_1, c_2, d_1, d_2 \in \mathbb{Q}$ so pick $c = \frac{\sqrt{a}}{\sqrt{b}}$

if $\sqrt{a} \notin \mathbb{Q}$ get $\sqrt{b} \notin \mathbb{Q}$ in a similar fashion. So must have $\sqrt{a} = r + s\sqrt{b}$ for $r, s \in \mathbb{Q}$

s'pose $r \neq 0 \Rightarrow a = (r + s\sqrt{b})^2 = r^2 + s^2 b + 2rs\sqrt{b} \Rightarrow \sqrt{b} \in \mathbb{Q}$ contradiction $\Rightarrow r = 0$

so $\sqrt{a} = s\sqrt{b} \Rightarrow c = s = \frac{\sqrt{a}}{\sqrt{b}}$.

($\Leftarrow$) if $\exists c \in \mathbb{Q}$ s.t. $a = bc^2$ then $\sqrt{a} = |c|\sqrt{b}$ so this $\Rightarrow \sqrt{a} \in \mathbb{Q}(\sqrt{b})$ and $\sqrt{b} = \frac{1}{|c|}\sqrt{a}$ $\Rightarrow \sqrt{b} \in \mathbb{Q}(\sqrt{a})$. Similar to #3 since $\sqrt{a} \in \mathbb{Q}(\sqrt{b})$ then $c_1 + c_2\sqrt{a} \in \mathbb{Q}(\sqrt{b})$ for $c_1, c_2 \in \mathbb{Q}$ and since $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ get $d_1 + d_2\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ for $d_1, d_2 \in \mathbb{Q}$. then $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a})$. $\square$

5.) let F field and $p(x)=x^3+x+1$ irred. over F. express a^{-1} in terms of basis elmts in $F(a)$ where $p(a)=0$.

pf:

In $F(a)$ know the basis is $\{1,a,a^2\}$ and $a^3+a+1=0$ since $p(a)=0$ but $a^3+a=-1$ so $a(a^2+1)=-1 \Rightarrow a^{-1}=-(a^2+1)=-a^2-1 \in F(a)$. then if $k\in\mathbb{Z}$ $a^{-k}=(a^{-1})^k=(-a^2-1)^k=(-1)^k(a^2+1)^k=(-1)^k\sum_{j=0}^{k}\binom{k}{j}a^{2k-2j}\in F(a)$ since $a^3=-a-1$ so the powers of 3 and above in a^{2k-2j} reduce. so this says $a^{-k}\in F(a)$ always. ◻

6.) let $f(x)\in F[x]$ be nonconst. let $a\in E$ ext of F and $f(a)$ is algebraic over F. Prove a is algebraic over F.

pf:

Notice since $f(a)$ is algebraic over F, then $\exists\, p(x)\in F[x]$ nonzero s.t. $p(f(a))=0$. then $(p\circ f)(x)$ is a nonzero poly. over F. but $(p\circ f)(a)=p(f(a))=0 \Rightarrow a$ is algebraic over F. ◻

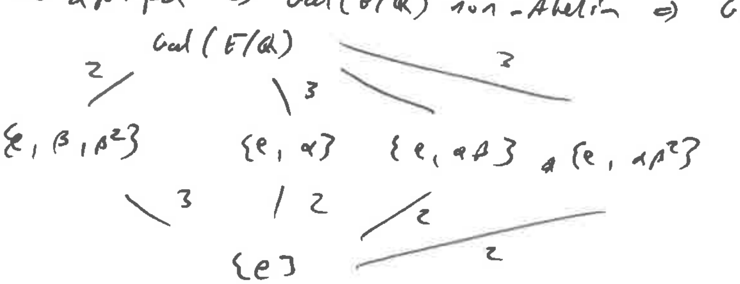
7.) let $p(x)=x^3-2$. Do the Galois analysis.

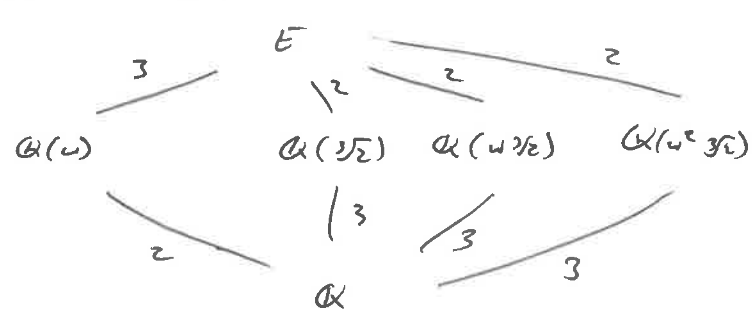
pf:

1st note $p(x)$ is irreducible by Eisenstein's criteria w/ prime $=2$ as $2\nmid 1$, $2|2$ and $2\nmid 4$. know one of the roots is $a=\sqrt[3]{2}$ as $(\sqrt[3]{2})^3-2=0$. the other roots come from x^3-1 namely the two complex roots of unity i.e. $\omega=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$ and $\omega=-\frac{1}{2}-i\frac{\sqrt{3}}{2}=\omega^2$ so the 3 roots are $a, a\omega, a\omega^2$ so the splitting field is $E=\mathbb{Q}(\sqrt[3]{2},\omega)$ as $\omega^2\in E$ don't need to add it. Then $[E:\mathbb{Q}]=[E:\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}]=3\cdot 2=6$ so $|Gal(E/\mathbb{Q})|=6$. need to construct the automorphisms that fix $\mathbb{Q}$. (i.e. permute the roots)

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 $Gal(E/\mathbb{Q})=\{e,\alpha,\beta,\beta^2,\alpha\beta,\alpha\beta^2\}$ notice $(\alpha\beta)(\sqrt[3]{2})=\alpha(\omega\sqrt[3]{2})=\omega^2\sqrt[3]{2}$, $(\beta\alpha)(\sqrt[3]{2})=\beta(\sqrt[3]{2})=\omega\sqrt[3]{2}$
so $\alpha\beta\neq\beta\alpha \Rightarrow Gal(E/\mathbb{Q})$ non-Abelian $\Rightarrow Gal(E/\mathbb{Q})\cong S_3$.





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

pf:

1st notice $p(x) = (x^2-2)(x^2-5)$ is reducible into 2 irreducible factors via Eisenstein's criterion w/ prime 2 1st factor and 5 for 2nd factor.

can easily see the roots to be $\sqrt{2}, -\sqrt{2}, \sqrt{5}, -\sqrt{5}$ so the splitting field is $E = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ as $-\sqrt{2}, -\sqrt{5} \in E$. so $[E:\mathbb{Q}] = [E:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2 \cdot 2 = 4$

so $|Gal(E/\mathbb{Q})| = 4$ need to construct the automorphisms that fix $\mathbb{Q}$ (i.e. permute the roots)

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

there are no others as $\sqrt{2}$ and $\sqrt{5}$ don't mix as roots. notice $(\alpha\beta)(\sqrt{5}) = \alpha(-\sqrt{5}) = -\sqrt{5} = \beta(\sqrt{5}) = (\beta\alpha)(\sqrt{5})$ and similarly $(\alpha\beta)(\sqrt{2}) = (\beta\alpha)(\sqrt{2})$ so $\alpha\beta = \beta\alpha \Rightarrow Gal(E/\mathbb{Q})$ is Abelian. and $\alpha^2 = e$, $\beta^2 = e$ and $(\alpha\beta)^2 = e$ so all elements have order 2 except identity $\Rightarrow Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$$\begin{tikzcd}
 & Gal(E/\mathbb{Q}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\{e, \alpha\} \arrow[dr, dash, "2"'] & \{e, \beta\} \arrow[d, dash, "2"] & \{e, \alpha\beta\} \arrow[dl, dash, "2"] \\
 & \{e\} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & E \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{10}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

□

9.) p odd prime let $q(x) = x^p - 1$. Do Galois Analysis.

pf:

1st notice $q(x) = (x-1)(x^{p-1} + x^{p-2} + \dots + 1)$ is reducible into 2 irreducible factors. 1st is linear 2nd via Eisenstein's Criterion using a shift of $x+1$ w/ prime p. recall the roots to q are the p^{th} primitive roots of unity ω, w/ all roots $1, \omega, \omega^2, \dots, \omega^{p-1}$ so the splitting field is $E = \mathbb{Q}(\omega)$ as $\omega^2, \dots, \omega^{p-1} \in E$. so $[E:\mathbb{Q}] = [\mathbb{Q}(\omega):\mathbb{Q}] = p-1$

$\Rightarrow |Gal(E/\mathbb{Q})| = p-1$ need to construct the automorphisms that fix $\mathbb{Q}$ (i.e. permute the roots)

consider: ~~eimg~~ $e: \omega^k \mapsto \omega^k$ for $k = 1, \dots, p-1$ then $\alpha_k: \omega \mapsto \omega^k$ $k = 2, \dots, p-1$ notice $\alpha_k(\omega^j\omega^l) = \alpha_k(\omega^{j+l}) = \omega^{k(j+l)} = \omega^{kj}\omega^{kl} = \alpha_k(\omega^j)\alpha_k(\omega^l)$

so α_k ~~for~~ e and are all the field automorphisms. next pick $j, l \in \mathbb{Z}_{p-1}$ then $(\alpha_j \alpha_l)(\omega) = \alpha_j(\omega^l) = (\alpha_j(\omega))^l = (\omega^j)^l = \omega^{jl} = \alpha_{jl}(\omega)$ $\Rightarrow$ ~~the~~ mapping $k \mapsto \alpha_k$ which goes from $\mathbb{Z}_{p-1}$ onto $Gal(E/\mathbb{Q})$ is a grp homom. if $j \neq l$ then $\omega^j \neq \omega^l$ so its 1-1. thus an isom.

$\Rightarrow Gal(E/\mathbb{Q}) \cong \mathbb{Z}_{p-1}$

$$\begin{tikzcd}
Gal(E/\mathbb{Q}) = \langle a \rangle \arrow[d, dash] \\
\langle a^2 \rangle \arrow[d, dash, dotted] \\
\langle a^{p-2} \rangle \arrow[d, dash] \\
\{e\}
\end{tikzcd}
\qquad
\begin{tikzcd}
E \arrow[d, dash] \\
\mathbb{Q}(\omega^{p-2}) \arrow[d, dash, dotted] \\
\mathbb{Q}(\omega^2) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

□