Solution Sketches

3. ~~B~~ Problems on Fields, Galois Theory

(1) $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$

Note, f factors over $\mathbb{C}$ as $a\left(x - \frac{-b+\sqrt{b^2-4ac}}{2a}\right)\left(x - \frac{-b-\sqrt{b^2-4ac}}{2a}\right)$

(a) $\Rightarrow$ (b) If $\sqrt{b^2-4ac} \in \mathbb{Q}$ then $\frac{-b \pm \sqrt{b^2-4ac}}{2a} \in \mathbb{Q}$ so the above factorization holds over $\mathbb{Q}$ showing f is reducible.

(b) $\Rightarrow$ (c) $\sqrt{b^2-4ac}$ is a root of the poly $x^2 - (b^2-4ac) \in \mathbb{Q}[x]$. Since this is a quadratic poly and $\sqrt{b^2-4ac} \notin \mathbb{Q}$, $[\mathbb{Q}(\sqrt{b^2-4ac}) : \mathbb{Q}] = 2$. As all quadratic extensions of $\mathbb{Q}$ are Galois, $|\mathrm{Gal}(\mathbb{Q}(\sqrt{b^2-4ac}) / \mathbb{Q})| = 2$

(c) $\Rightarrow$ (a) Since $\mathbb{Q}(\sqrt{b^2-4ac}) = \mathbb{Q}\left(\frac{-b+\sqrt{b^2-4ac}}{2a}\right)$, we also have $\left[\mathbb{Q}\left(\frac{-b+\sqrt{b^2-4ac}}{2a}\right) : \mathbb{Q}\right] = 2$, and since $\frac{-b+\sqrt{b^2-4ac}}{2a}$ is a root of f, ~~roots~~ and f is of degree 2, we must have f is irred.

(2) Write $f(x) = \prod_i (x - a_i)$. We assume $\sigma(a_i) = a_i$

Since each coefficient of f looks like $\sum_{i_1 < i_2 < \cdots < i_r} a_{i_1} a_{i_2} \cdots a_{i_r}$ clearly σ fixes each coefficient of f.

~~and therefore~~ Alternately $\sigma(f) = \prod (x - \sigma(a_i)) = \prod (x - a_i) = f$.

~~then~~ We need to know $\sigma\{a_i\} = \{a_i\}$ with multiplicity (for example if $\sigma(a) = b$, $\sigma(b) = a$ and $f(x) = (x-a)(x-a)(x-b)$ we're in trouble.)

But given this $\sigma(f) = \prod (x - \sigma(a_i)) = \underset{\text{in some different order}}{\prod x - a_i} = f$.

(3) $x^4 - 2x^2 + 9$

(4) It is useful to compute over $\mathbb{C}$ that $x^4 - 2 = (x-\alpha)(x+\alpha)(x-\alpha i)(x+\alpha i)$,

over $\mathbb{Q}(\sqrt{2})$: $(x^2-\sqrt{2})(x^2+\sqrt{2})$

$\mathbb{Q}(\sqrt{2}, i)$: $(x^2-\sqrt{2})(x^2+\sqrt{2})$

$\mathbb{Q}(\alpha)$: $(x-\alpha)(x+\alpha)(x^2+\sqrt{2})$

$\mathbb{Q}(\alpha, i)$: $(x-\alpha)(x+\alpha)(x-\alpha i)(x+\alpha i)$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\alpha, i) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & & \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

(5) If $[K:F] = d$, let $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ be a linear basis of K over F. Since $[F(\alpha_i):F] \le d$, α_i is algebraic so is a root of some $g_i(x) \in F[x]$, with $\deg(g_i) \le d$. Let $\sigma \in \mathrm{Aut}_F K$. Since $\sigma(g_i(x)) = g_i(x)$, $g_i(\sigma(\alpha_i)) = \sigma(g_i(\alpha_i)) = 0$ so $\sigma(\alpha_i)$ is also a root of g_i.
As there are only finitely many roots of g_i there are finitely many choices for $\sigma(\alpha_i)$. Thus $|\mathrm{Aut}_F K| < \infty$.
(Note, if $E \supseteq K \supseteq F$ is the smallest Galois extension of F containing K, we can use a similar argument to see $|\mathrm{Gal}(E/F)| < \infty$.)

(6) Yes. Consider

$$\begin{tikzcd}[column sep=small]
 & K \arrow[dl, dash, "C_3"'] \arrow[dr, dash, "C_2"] & \\
E \arrow[dr, dash, "C_2"'] & & L \arrow[dl, dash, "3"] \\
 & F &
\end{tikzcd}$$

Since $[L:F] = 3$ is prime, we know $L = F(\alpha)$ where α satisfies a cubic. Since K/F is Galois, K contains the splitting field of that cubic. Since L/F is NOT Galois (as $C_2 \ntrianglelefteq S_3$) L cannot be the splitting field, and there are no $L \subsetneq L' \subsetneq K$.

(7) Slightly messy

Case 1 $b=0$ a is a cube. So $\alpha^3 = a$

Then $\alpha \in \mathbb{Q}(\rho)$ so $\mathrm{Gal} = \{1\}$

Case 2 $b=0$ a is not a cube. Then $x^3 - a$ splits in $\mathbb{Q}(\alpha, \zeta)$ (and $\alpha \notin \mathbb{Q}(\rho)$)

with $[\mathbb{Q}(\alpha, \rho) : \mathbb{Q}(\rho)] = 3$ so $\mathrm{Gal} = \{\mathbb{Z}/3\mathbb{Z}\}$.

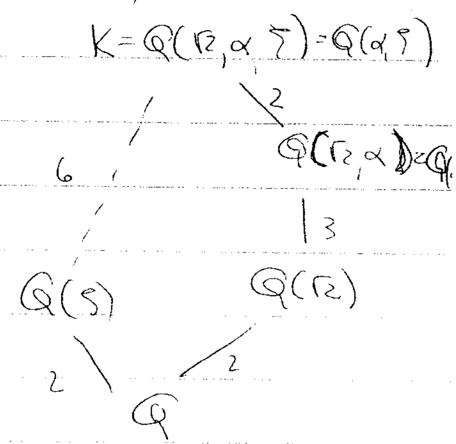
Case 3 $b \neq 0$ then $\alpha^3 = a + b\sqrt{2}$

α is a root of $x^6 - 2a x^3 + (a^2 - 2b^2)$ which we'll assume is irred.

Then $[K : \mathbb{Q}(\rho)] = 6$

and $K = \mathbb{Q}(\alpha, \zeta)$.

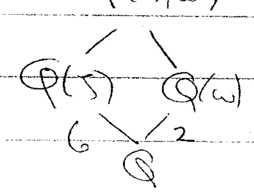
So either $\mathrm{Gal}(K/\mathbb{Q}(\rho)) =$ $\mathbb{Z}/6\mathbb{Z}$ or S_3.



To act transitively on the roots, we need $\mathrm{Gal} = \mathbb{Z}/6\mathbb{Z}$.

(8) 6

$\mathbb{Q}(\rho, \omega) = \mathbb{Q}(21^{st}$ root of unity$)$ since $(3,7)=1$



and we know $[\mathbb{Q}(\rho, \omega) : \mathbb{Q}] = 12$.

(9) The Galois group of $x^n - 1$ over $\mathbb{Q}$ is isom to the group of units $(\mathbb{Z}/n\mathbb{Z})^*$ of order $\varphi(n)$.

Note $\varphi(8) = 4$ $\qquad$ $\varphi(12) = 4$ $\qquad$ $\varphi(9) = 6$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\qquad$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\qquad$ $\mathbb{Z}/6\mathbb{Z}$

(10) Note $[\mathbb{F}_{p^r} : \mathbb{F}_p] = r$.
$\mathbb{F}_{p^r}$ is the splitting field of $x^{p^r} - x = 0$, which has distinct roots so it is Galois.
$\phi \in Gal(\mathbb{F}_{p^r}/\mathbb{F}_p)$. Notice $\phi^r = id$.
If $\phi^k = id$ for any $1 \leq k < r$, then $\mathbb{F}_{p^r}$ would consist of roots of $x^{p^k} - x = 0$ which only has p^k roots.
so $\langle\phi\rangle \cong \mathbb{Z}/r\mathbb{Z}$. Since $\langle\phi\rangle \leq Gal(\mathbb{F}_{p^r}/\mathbb{F}_p)$ and $r = |Gal(\mathbb{F}_{p^r}/\mathbb{F}_p)|$ we are done.

(11) Since $\phi^n = id$ and $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$,
$t^n - 1$ must be the characteristic (and in fact minimal) polynomial of ϕ.
Then the RCF coincides w/ the companion matrix for $t^n - 1$:
$$\begin{bmatrix} 0 & & & 1 \\ 1 & 0 & & \\ & 1 & \ddots & \\ & & 1 & 0 \end{bmatrix}$$

To get the JCF, we need to factor $t^n - 1$ mod p.
* This breaks into cases, but in general, repeated factors contribute to a Jordan block of that size.

(12) (a) $x^4 - 1$ degree $= 2$ $K = \mathbb{Q}(i)$
(b) $x^3 - 2$ degree $= 6$ $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$
(c) $x^4 + 1$ degree $= 4$ $K =$ splitting field for $x^8 - 1$ of degree $\phi(8) = 4$

(13) If $\sigma \in Aut(\mathbb{Q}(\sqrt[3]{2}))$, $\sigma|_{\mathbb{Q}} = id_{\mathbb{Q}}$.
Also $(\sigma(\sqrt[3]{2}))^3 = 2$ forcing $\sigma\sqrt[3]{2} = \sqrt[3]{2}$ and the other roots of $x^3 - 2$ are complex. So $\sigma = id$ and $Aut(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$

(14) (a) true (see fundamental thm)

(b) false Take $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$

L = fixed field of ~~[illegible]~~ complex conjugation $= \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} K \\ | \\ L \\ | \\ F \end{array}$$

(c) false

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}) \\ |\,2 \\ \mathbb{Q}(\sqrt{2}) \\ |\,2 \\ \mathbb{Q} \end{array}$$

not splitting

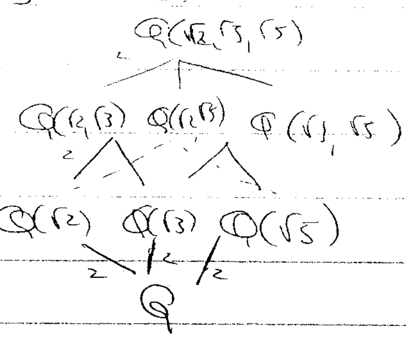
(15) For each matrix to have an inverse we need $a^2+b^2=0$ have no nonzero solutions in $\mathbb{F}$, which holds for $\mathbb{F} = \mathbb{Q}, \mathbb{F}_7$ but not $\mathbb{C}, \mathbb{F}_5$.

(16) $[F(a):F]$, $[F(b):F] < \infty$

$\Rightarrow [F(a,b):F] = [F(a,b):F(b)][F(b):F] < \infty$

and $a+b \in F(a,b)$ so $[F(a+b):F] < \infty \Rightarrow$

$a+b$ is algebraic



(17) sketch: we see $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ is the splitting field of $(x^2-2)(x^2-3)(x^2-5)$,

~~[illegible]~~ $Gal \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$

(18) $\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ is cyclic. Since $2 \mid p-1$

the map $\mathbb{F}_p^* \longrightarrow$ ~~$\mathbb{Z}/\frac{p-1}{2}\mathbb{Z}$~~ $\mathbb{F}_p^*$ is a homom w/ nontrivial kernel
$a \longmapsto a^2$

Then $\frac{p-1}{2}+1$ (don't forget zero) elts have sqrts of order 2.

If $3 \nmid p-1$ $\mathbb{F}_p^* \to \mathbb{F}_p^*$, $a \mapsto a^3$ is onto so all p elts have cube roots.

Else kernel has order 3 so $\frac{p-1}{3}+1$ elts have cube roots

(14) Induct on n in towers.

$n=1$ easy

Given f, let $f(\alpha)=0$ (subcase: f irred) so $[F(\alpha):F] = n$

$$[K:F] = [K:F(\alpha)][F(\alpha):F]$$

Then $f=(x-\alpha)g$ for $\deg g = n-1$ & K is the splitting field of g over $F(\alpha)$. By induction $[K:F(\alpha)] \mid (n-1)!$. Then $[K:F] \mid n!$

In general, if f is not irred write $f = q h^r$ with $q(\alpha)\neq 0$, $h(\alpha)=0$.

Then over $F(\alpha)$, $f = q g^r (x-\alpha)^r$ $\quad [F(\alpha):F] = r$

$\deg(q g^r) = n-r$

so $[K:F] = [K:F(\alpha)][F(\alpha):F] \mid (n-r)!\cdot r \mid n!$