Problem Set #3 (Solutions)

1. Proof: According to L/K is a finite normal extension. $\exists F \in K[x]$ s.t. L is splitting field for F over K.
Let L° be a splitting field extension for f over L. We have L°/L is normal. $\forall F \in K[x]$. $\forall F$ splits in L°. Suppose $L' \subseteq L^\circ$ and $\forall F$ splits in L', according to f splits in L'. $f \in L[x]$ and L° is the splitting field extension for f over L, we have $L^\circ \subseteq L'$. Thus $L' = L^\circ$. This proves L° is splitting field for $\forall F$ over K. Thus L°/K is normal.
f is irreducible in $K[x]$. According to it splits in L°.
Let $\alpha, \beta \in L^\circ$ s.t. $g(\alpha) = 0$. $h(\beta) = 0$. Obviously α and β are roots of f.
Suppose $\deg g \leq \deg h$. According to f irred in $K[x]$ and L° spl. fld. ext
$\exists \sigma : L^\circ \xrightarrow{\cong} L^\circ$, $\sigma(\alpha) = \beta$, $\sigma|_K = \mathrm{id}_K$.
According to L°/K is finite and normal, and $\sigma \in \mathrm{Aut}(L^\circ/K)$ and L/K normal, we have $\sigma(L) = L$. $\sigma|_L \in \mathrm{Aut}(L/K)$.
Let m_α and m_β be the minimal polynomial of α and β in L. According to g, h irred. and monic we have $g = m_\alpha$, $h = m_\beta$.
$\sigma(g)(\beta) = \sigma(g(\alpha)) = \sigma(0) = 0$ which means $m_\beta \mid \sigma g$, $h \mid \sigma g$,
According to $\deg \sigma g = \deg g \leq \deg h$. g, h monic, irreducible.
We have $h = \sigma(g)$.
If it is the case $\deg g \geq \deg h$, repeat what we have done and consider σ^{-1}. $\square$

(2) Suppose L/K is a Galois extension, $G = \mathrm{Aut}(L/K)$, $\alpha \in L$. Show that $L = K(\alpha)$ if and only if the images of α under the elements of G are distinct.

($\Rightarrow$) Suppose $L = K(\alpha)$. Then since the automorphisms in G fix K, they are completely determined by their action on α, and $g_1(\alpha) = g_2(\alpha) \iff g_1 = g_2$ for $g_1, g_2 \in G$.

($\Leftarrow$) Suppose the images of α under G are distinct but $K(\alpha) \subsetneq L$. Then since L/K is a Galois extension, $K(\alpha) = \mathrm{Inv}\, H$ for some nontrivial subgroup H of G, and there is some $h \in H$, h not the identity element, such that $h(\alpha) = \alpha$, contradicting the assumption that all images are distinct, since $h \in G$.

3. Suppose the matrix is not invertible. Then the corresponding homogeneous system of equations (let the ith row contain all the $\sigma_i(\beta_j)$) has a nontrivial solution. In particular, there exist constants $a_j \in K$ for some i, not all of which are zero, such that

$$\sum_{j=1}^{n} a_j \sigma_i(\beta_j) = \sum \sigma_i(a_j \beta_j) = 0.$$

Because σ_i is an automorphism, this means $\sum a_j \beta_j = 0$, a contradiction, as the β_j are a basis. This shows that the determinant is nonzero if the β_j form a basis.

Conversely, assume the the β_j are not a basis. Then some K-linear combination of them is zero, and taking σ_i of this combination for each i gives a a system of linear equations with matrix $\{\sigma_i(\beta_j)\}$ with a nontrivial solution, so the determinant of the matrix is zero. This contradiction proves the theorem.

4. Claim: $\mathbb{Q}(\sqrt[4]{2}, i)$ is the SFE for f over $\mathbb{Q}$

$f = (x-\sqrt[4]{2})(x-\sqrt[4]{2})(x-(-\sqrt[4]{2}))(x-(-2\sqrt[4]{2}))$ splits in $\mathbb{Q}(\sqrt[4]{2}, i)$ and for L' s.t. f splits in L', and it must contain $\sqrt[4]{2}$ and $\frac{i\sqrt[4]{2}}{\sqrt[4]{2}} = i$, so $L' \geq \mathbb{Q}(\sqrt[4]{2}, i)$

Thus $\mathbb{Q}(\sqrt[4]{2}, i)$ is the SFE for f over $\mathbb{Q}$.

Suppose: $\eta \in Aut(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$, η is determined by $\eta(\sqrt[4]{2}) = i^k \cdot \sqrt[4]{2}$ $k = 0, 1, 2, 3$

so $|Gal_{\mathbb{Q}}(f)| = |Aut(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = 8$. $Gal_{\mathbb{Q}}(f) \cong D_4$ $\eta(i) = i$.

$x^4 - 2 = (x^2+x-1)(x^2-x-1)$ in $\mathbb{Z}_3[x]$. x^2+x-1, x^2-x-1 irred in $\mathbb{Z}_3[x]$

Let $L_1 := \mathbb{Z}_3[x]/(x^2+x-1)$, we have $x^2+x-1 = (x-\alpha)(x-(-\alpha-1))$ and
($\alpha \leftrightarrow x$)

$x^2-x-1 = (x-(-\alpha))(x-(\alpha+1))$

So x^4-2 split in L_1. L_1 is the splitting field of x^4-2 over $\mathbb{Z}_3$

$|Gal_{\mathbb{Z}_3}(f)| = |Aut(\mathbb{Z}_3(\alpha)/\mathbb{Z}_3)| = 2$. $Gal_{\mathbb{Z}_3}(f) \cong \mathbb{Z}_2$.

$x^4-2 = (x-2)(x-5)(x^2+4)$ x^2+4 is irreducible in $\mathbb{Z}_3[x]$.

Let $L_2 := \mathbb{Z}_3[x]/(x^2+4)$, we have $x^2+4 = (x+\beta)(x-\beta)$
($\beta \leftrightarrow x$)

x^4-2 splits in L_2. L_2 is the splitting field of x^4-2 over $\mathbb{Z}_3$

$|Gal_{\mathbb{Z}_3}(f)| = |Aut(\mathbb{Z}_3(\beta)/\mathbb{Z}_3)| = 2$. $Gal_{\mathbb{Z}_3}(f) \cong \mathbb{Z}_2$.

5. Given a group G, embed it into $S_{|G|}$. Look at $R = \mathbb{Q}[x_1, x_2, \ldots x_{|G|}]$ and let F be its field of fractions. Given $\sigma \in G$, we define μ with $\mu(x_i) \to x_{\sigma(i)}$. This fixes $\mathbb{Q}$. Given $\sigma_1, \sigma_2 \in G$ and their corresponding μ_1, μ_2, we have $\mu_1 \circ \mu_2(x_i) = x_{\sigma_1 \circ \sigma_2(i)}$ and so the μ_i form a group isomorphic to G. We now have $(F/\mathrm{Inv}F) \cong G$, which is what we wanted to show.
(Aut)

6. a. I assume that K has characteristic zero. Then M is a ~~/~~ normal, separable, ~~/~~ finite extension of both K and L, and so is a Galois extension of both.

Consider the fixed field of some Sylow 2-subgroup P of G. Then its fixed field M^P/K has odd degree by the Galois correspondence. Fix some $\alpha \in M^p$ but not in K. Its minimal polynomial has odd degree and has some root r in K. Then polynomial long division by $x - r$ shows that the minimal polynomial is not irreducible, a contradiction.

b. Suppose $n > 1$. We know that $|H| = 2^{n-1}$ from the above result and the Galois correspondence. From Sylow theory, we know H contains a subgroup with order 2^{n-2}, so it contains a subgroup with index 2. Then M^H/L has degree 2. Fix some element α in M^H but not L. Then its minimal polynomial must have degree 2, and we have found an irreducible quadratic in $L[x]$.

c. Adjoining a root of this irreducible quadratic gives a an extension of degree 2 over L. But because the characteristic is not two, we may complete the square and take square roots to get the roots of the polynomial. Since $L^2 = L$, it is impossible for a polynomial of degree 2 to be irreducible. This contradiction shows L is algebraically closed.

d. It's easy to see that $\mathbb{C}/\mathbb{R}$ is such an extension and therefore algebraic closed. It is clearly of degree two, as i has minimal polynomial $x^2 + 1$ and $\mathbb{C} = \mathbb{R}(i)$. Every polynomial of odd degree has a real root because complex roots come in conjugate pairs, and one can use polar form to directly find the square root of any given complex number. So by the prior part, $\mathbb{C}$ is algebraically closed.

(7) [p. 243 #1 Jacobson] (a) Show that in the FToGT correspondence, the subfield corresponding to the intersection of two subgroups H_1 and H_2 is the subfield generated by $\mathrm{Inv}\,H_1$ and $\mathrm{Inv}\,H_2$.

Let M be the subfield generated by $\mathrm{Inv}\,H_1$ and $\mathrm{Inv}\,H_2$. Then $M = \bigwedge M_\alpha$ where $M_\alpha \supset \mathrm{Inv}\,H_1$ and $M_\alpha \supset \mathrm{Inv}\,H_2$

$\underline{M \subset \mathrm{Inv}(H_1 \wedge H_2)}$

Since $\mathrm{Inv}(H_1 \wedge H_2) \supset \mathrm{Inv}\,H_1, \mathrm{Inv}\,H_2$, $\mathrm{Inv}(H_1 \wedge H_2)$ is a qualified M_α and M is contained in it.

$\underline{M \supset \mathrm{Inv}(H_1 \wedge H_2)}$

For all α and $i = 1, 2$, $\mathrm{Gal}\left(E/M_\alpha\right) \subset \mathrm{Gal}\left(E/\mathrm{Inv}\,H_i\right) = H_i$;

$\Rightarrow \mathrm{Gal}\left(E/M_\alpha\right) \subset H_1 \wedge H_2 \;\forall \alpha$

$\Rightarrow \mathrm{Gal}(E/M) \subset H_1 \wedge H_2$

$\Rightarrow M \supset \mathrm{Inv}(H_1 \wedge H_2)$

$\Rightarrow M = \mathrm{Inv}(H_1 \wedge H_2)$.

(b) The intersection of two intermediate fields K_1 and K_2 corresponds to the subgroup generated by $\mathrm{Gal}(E/K_1)$ and $\mathrm{Gal}(E/K_2)$.

Let H be the subgroup generated by $G_1 = \mathrm{Gal}(E/K_1)$ and $G_2 = \mathrm{Gal}(E/K_2)$. On one hand, $\mathrm{Gal}(E/K_1 \wedge K_2)$ contains G_1 and G_2, so $\underline{K_1 \wedge K \subset \mathrm{Inv}\,H}$. But since $H \supset G_1$ and $H \supset G_2$, $K_1 = \mathrm{Inv}\,G_1 \supset \mathrm{Inv}\,H$ and $K_2 = \mathrm{Inv}\,G_2 \supset \mathrm{Inv}\,H$. Thus $\underline{K_1 \wedge K_2 \supset \mathrm{Inv}\,H}$, and so $K_1 \wedge K_2 = \mathrm{Inv}\,H$

8. We have

$$(r^2-2)^3+(r^2-2)^2-2(r^2-2)-1=(r^3-r^2-2r+1)(r^3+r^2-2r-1)=0.$$

Since $\mathbb{Q}(r)$ is a field that contains two of the roots, it contains the third (-1/rr'), so the field is a splitting field for the polynomial in the problem and hence normal. If we can show the polynomial is irreducible, then it is separable by the derivative test, and the extension will have degree 3, forcing the Galois group to be $\mathbb{Z}_3$.

Suppose it factored over $\mathbb{Q}$ as $(x-a)(x^2+bx+c)$. Equating coefficients gives $-ac=-1$, so $ac=1$ and $c=1/a$. This reduces the factorization to $(x-a)(x^2+bx+1/a)$. Examining the x term gives $-2=-ab+1/a$, and the x^2 term gives $1=b-a$. So $b=a+1$, and $-2=-a(a+1)+1/a$. Then $-2a=-a^3-a^2+1$, and the rational root test shows this has no rational roots, and the polynomial is irreducible.

9. Let $\sigma: \bar{E} \to \bar{E}$, $t \mapsto t+1$, so $\sigma(t^p-t)=(t+1)^p-(t+1)=t^p+1-(t+1)=t^p-t$.
so $\mathrm{Inv}G \supseteq \mathbb{Z}_p(t^p-t)$.
Since $\sigma^p=\mathrm{id}$, $|G|=p$. $[\bar{E}:\mathrm{Inv}G]=p$, $[\bar{E}:\mathbb{Z}_p(t^p-t)]=p$.
Since $x^p-x-(t^p-t) \in \mathbb{Z}_p(t^p-t)[x]$ is irreducible, we get. $\mathrm{Inv}G=\mathbb{Z}_p(t^p-t)$
by the tower law. So $F=\mathbb{Z}_p(t^p-t)$ and $[\bar{E}:F]=p$.

(10) $K = \mathbb{Q}(\sqrt{2},\sqrt{3}) \subset L = \mathbb{Q}(\sqrt{2},\sqrt{3},u)$, $u^2 = \alpha := (9-5\sqrt{3})(2-\sqrt{2})$.

Here $u \in K$, $\left(N_{K/\mathbb{Q}(\sqrt{3})}(u)\right)^2 = N_{K/\mathbb{Q}(\sqrt{2})}(\alpha) = (9-5\sqrt{3})(9+5\sqrt{3})(2-\sqrt{2})^2$
$= 6(2-\sqrt{2})^2$
$\Rightarrow$ 6 is a square in $\mathbb{Q}(\sqrt{2})$ ✱.

One easily checks that $1, \alpha, \alpha^2, \alpha^3$ are independent $\Rightarrow$

$K = \mathbb{Q}(\alpha) \Rightarrow L = \mathbb{Q}(u)$, i.e. u is a primitive element.

Clearly $[L:\mathbb{Q}] = 8$ by tower law, and as a quadratic extension tower it is normal $\Rightarrow |\mathrm{Aut}(L/\mathbb{Q})| = 8$, with automorphisms sending u to every other root of its minimal polynomial $f_u(x) = f_\alpha(x^2)$.

Clearly these are just the $\boxed{\pm\sqrt{(9\pm5\sqrt{3})(2\pm\sqrt{2})}}$ (✱) (there are 8 of these) — all in L.

That is: the elements of $\mathrm{Aut}(L/\mathbb{Q})$ are precisely the maps determined by writing elements of L as polynomials in u with $\mathbb{Q}$-coeffs. and sending u to one of the elements (✱).

Let $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$ and $u \mapsto v := \sqrt{(9-5\sqrt{3})(2+\sqrt{2})}$;

since $\sigma(u^2) = \sigma(u)^2 = v^2$, $\sigma|_K$ must be the autom. of $K/\mathbb{Q}$ sending $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$. Now $\sigma(uv) = \sigma(\sqrt{2}(9-5\sqrt{3})) = -\sqrt{2}(9-5\sqrt{3}) = -uv \Rightarrow \sigma(v) = -u$, so σ sends

$$u \longmapsto v \longmapsto -u \longmapsto -v \longmapsto u$$

and $\therefore$ has order 4 (σ is determined by its behavior on u).

Let $\eta \in \mathrm{Aut}(L/\mathbb{Q})$ send $u \mapsto w := \sqrt{(9+5\sqrt{3})(2-\sqrt{2})}$;

since $\eta(u^2) = \eta(u)^2 = w^2$, $\eta|_K$ sends $\sqrt{2} \mapsto \sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$.

$\eta(uw) = \eta\left(\sqrt{6}(2-\sqrt{2})\right) = -\sqrt{6}(2-\sqrt{2}) = -uw \Rightarrow$ η sends $u \mapsto w \mapsto -u \mapsto -w$

& has order 4.

Moreover, $\sigma\eta|_K$ sends $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$ so sends

$u \mapsto \pm t := \pm\sqrt{(9+5\sqrt{3})(2+\sqrt{2})}$ and $ut \mapsto -ut$ hence $\pm t \mapsto -u$

($ut = 2\sqrt{3}$)

giving another 4-cycle. Conclude that σ, η generate $G := \mathrm{Aut}(L/\mathbb{Q})$.

Clearly σ^2, η^2 fix K and send $u \mapsto -u$, so are equal;

whilst $\eta\sigma^3|_K$ also sends $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$, $u \mapsto -u$ ($\eta\sigma^3$:) $\Rightarrow$

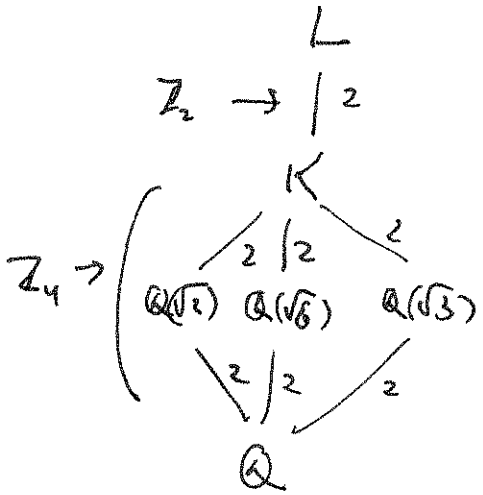
$\eta\sigma^3 = \sigma\eta$. But the quaternion group

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ may be presented as

$$\langle \sigma, \eta \mid \sigma^4 = 1 = \eta^4,\ \sigma^2 = \eta^2,\ \sigma\eta = \eta\sigma^3 \rangle$$

$\Rightarrow$ $\boxed{G \cong Q_8}$.

Remark: One can go a certain distance with the diagram :



which clearly says that G is an Extension

$$\{e\} \to \mathbb{Z}_2 \xrightarrow{\rho} G \xrightarrow{\pi} \mathbb{Z}_2 \times \mathbb{Z}_2 \to \{e\} .$$

Were this split — i.e. if there were a map (homomorphism) $\mu : \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$ with $\pi \circ \mu = id_{\mathbb{Z}_2 \times \mathbb{Z}_2}$ — then G would have to be $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

But it isn't split, as the above proof establishes.