Problem Set 5

Zack Garza

① We'll proceed by induction on $n = \deg f$. The $n=1$ case follows immediately since $\deg f = 1 \Rightarrow$ $f(x) = x - \alpha \in K[x]$, so $\alpha \in K$ and $[K:K] = 1$ which divides $1! = 1$.

If now $\deg f = n$, we have $f(x) = \prod_{i=1}^{\ell} (x-u_i)^{m_i}$ for some $m_i \geq 1$, $1 \leq \ell \leq n$.

- Suppose f is irreducible over K

Then we can write $f(x) = (x-u_1)^{m_1} g(x)$ in $K(u_1)[x]$ where $\deg g \leq n-1$. So let F_g be its splitting field, so $[F_g : K(u_1)]$ divides $(n-1)!$ by hypothesis. But $[K(u_1):K] = n$, so F_g is the splitting field of f and $[F_g:K] = [F_g : K(u_1)][K(u_1):K] = p \cdot n$ where $p \mid (n-1)!$, so $pn \mid n!$

- Suppose f is reducible, then $f(x) = g(x)h(x)$ where $\deg g = r$, $\deg h = s$, $r+s = n$, and in particular, (wlog) $r \leq s < n$. So g splits in some $F_g \geq K$ where $[F_g : K]$ divides $r!$; so considering now $h(x) \in F_g[x]$, there is some splitting field $F_h \geq F_g$ where h splits as well with $[F_h : F_g] \mid s!$

But then F_h is the splitting field for $f(x)$, and $[F_h : K] = [F_h : F_g][F_g : K] := ab$ where $a \mid s!$ & $b \mid r! \Rightarrow ab \mid r!s!$, but $r!s! \mid (r+s)! = n!$ since $\frac{(r+s)!}{r!s!} = \binom{r+s}{r} \in \mathbb{N}$. $\blacksquare$

---

②

a) If u is separable in K, then $f(x) := \min(u, K)$ has distinct roots in its splitting field L. But since $K \subseteq E$, we have $g(x) := \min(u, E) \mid f(x)$. But then g must also have distinct roots in L, otherwise f would have a multiple root, so u is separable over E.

b) Since F/K is separable & $E \subseteq F$, we immediately have E/K separable. To see that F/E is separable, we have:

F/K is separable iff $\forall u \in F$, u is separable over K (defn)

iff $\forall u \in F$, u is separable over E (by (a))

iff F/E is separable. (defn) $\blacksquare$

---

③ Defn: $F \geq K$ is Galois iff F is a separable splitting field, or $[K:F] = \{K:F\} = |Gal(K/F)|$.

1 ⇒ 2: Immediate from defn.

2 ⇒ 3: Since F splits some $f(x)$ & F is separable, $f(x)$ has distinct roots in F. But then any irreducible factor of $f(x)$ can not have a multiple root, so they are all separable as well.

3 ⇒ 2: Let $\{g_i(x)\}$ be the irreducible factors of $f(x)$; then F is the splitting field of $p(x) := \prod_i g_i(x)$, which is separable. Now letting α be a root of p, we have $F/K(\alpha)$ as a splitting field of a separable polynomial (some $q_\alpha(x) \mid p(x)$) and so $F/K(\alpha)$ is Galois & $[F:K(\alpha)] = \{F:K(\alpha)\} = |Gal(F/K(\alpha))|$.

Since F is a splitting field of $q_\alpha(x)$, any $\sigma \in Gal(F/K)$ permutes the roots of $q_\alpha(x)$. Suppose there are d roots, which are distinct, then $[K(\alpha):K] = d$. Since $Gal(F/K) \curvearrowright X := \{\text{roots of } q_\alpha\}$ transitively, we have $|X| = |[Gal(F/K) : Stab_x]|$ by Orbit-stabilizer for any $x \in X$. So pick $x = \alpha$, then

$$Stab_x = Gal(K(\alpha)/K) \implies [Gal(F/K) : Gal(F/K(\alpha))] = |X| = d.$$

But then

$$\begin{aligned}
[F:K] &= [F:K(\alpha)][K(\alpha):K] \\
&= \{F:K(\alpha)\}[K(\alpha):K] && \text{since } F/K(\alpha) \text{ is Galois} \\
&= \{F:K(\alpha)\} \cdot d && \text{since } K(\alpha)/K \text{ is splits a separable } q_\alpha(x) \\
&= \{F:K(\alpha)\} \cdot [Gal(F/K) : Gal(F/K(\alpha))] && \text{by Orbit-Stabilizer} \\
&= |Gal(F/K(\alpha))| \cdot [Gal(F/K) : Gal(F/K(\alpha))] && \text{since } F/K(\alpha) \text{ is Galois} \\
&= |Gal(F/K)|, && \text{since } H \leq G \Rightarrow |H| \cdot [G:H] = |G|
\end{aligned}$$

So F/K is Galois. ■

⑤

a) Noting that $g(x) | f(x)$ and f splits in F, g must split in F as well. (Otherwise, g would have an irreducible nonlinear factor in F and thus f would as well.)

b) The irreducible factors of g are separable in E and F/E is a splitting field for g, so by (3.3) above, F/E is Galois.

c) $K \leq E \Rightarrow Aut(F/E) \subseteq Aut(F/K)$, and to see $Aut(F/K) \subseteq Aut(F/E)$, letting $\sigma \in Aut(F/K)$ we must have $\sigma \in Sym(\{u_1, \cdots, u_n\})$ and so

$$\sigma(g(x)) = g(\sigma(x)) = \prod (\sigma(x) - u_i) = \sum v_i \sigma(x)^i$$

$$\sigma(g(x)) = \sigma\left(\sum v_i x^i\right) = \sum \sigma(v_i) \sigma(x)^i$$

so $\sigma(v_i) = v_i$ & $\sigma \in Aut(F/E)$.

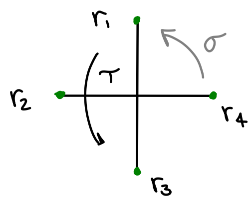
$\blacksquare$

(5) $f(x) = x^4 - 5$ over

- $\mathbb{Q}$
- $\mathbb{Q}(\sqrt{5})$
- $\mathbb{Q}(i\sqrt{5})$

Let $\omega = 5^{1/4}$, $\zeta = e^{2\pi i/4}$, then f splits in $F := \mathbb{Q}(\omega, \zeta)$ as $f(x) = \prod_{j=1}^{4} (x - \omega\zeta^j)$.

We can embed these roots in $\mathbb{C}$ to find some automorphisms of $F/\mathbb{Q}$:



where $r_j = \omega\zeta^j$, so we can define

$$\tau : F \to F \qquad \sigma : F \to F$$
$$i \mapsto -i \qquad i \mapsto i$$
$$\omega \mapsto \omega \qquad \omega \mapsto i\omega$$

Then τ corresponds to the cycle $(1,3)$ in $\mathrm{Sym}(\{r_j\}) \cong S_4$, which has order 2, and σ corresponds to $(1,2,3,4)$, which has order 4; thus $G := \langle \tau, \sigma \rangle \Rightarrow |G| = 8$.

$\mathbb{Q}$

Claim: $G = \mathrm{Gal}(F/\mathbb{Q})$ & $G \cong D_4 = \langle s, r \mid s^2 = r^4 = e,\ (sr)^2 = e \rangle$.

Since F splits $f(x)$ by construction, $F/\mathbb{Q}$ is separable, and since (claim) $[F:\mathbb{Q}] = 8 < \infty$, it is also normal & thus a Galois extension, so we have $[F:\mathbb{Q}] = \{F:\mathbb{Q}\} = \#\mathrm{Gal}(F/\mathbb{Q}) = 8$.

Since $\langle \tau, \sigma \rangle \leq \mathrm{Gal}(F/\mathbb{Q})$, it must be the entire group. To see that $[F:\mathbb{Q}] = 8$, we can note that

$$[\mathbb{Q}(\omega,\zeta):\mathbb{Q}] = \underbrace{[\mathbb{Q}(\omega,\zeta):\mathbb{Q}(\omega)]}_{=2,\ \text{since } \mathbb{Q}(\omega) \subseteq \mathbb{R} \text{ but } \zeta \notin \mathbb{R}, \text{ so } \min(\zeta, \mathbb{Q}(\omega)) = x^2+1.} \underbrace{[\mathbb{Q}(\omega):\mathbb{Q}]}_{=4,\ \text{since } \min(\omega,\mathbb{Q}) = x^4 - 5}$$

We can immediately note that $\tau\sigma = (13)(1234) = (12)(34) \neq (14)(23) = \sigma\tau$, so G is non-abelian.

Moreover, G contains 2 elts of order 2, namely τ & $\sigma\tau$, so $G \not\cong Q_8$, so we must have $G \cong D_4$.

(This follows since they have the same # of generators, satisfy the same relations, & are the same size.)

$$\boxed{\text{So } \mathrm{Gal}(F/\mathbb{Q}) \cong D_4.}$$

$\mathbb{Q}(\omega)$

$\omega = 5^{1/4} \Rightarrow \omega^2 = \sqrt{5}$

$\min(\sqrt{5}, \mathbb{Q}) = x^2 - 5$

Noting that $[\mathbb{Q}(\omega^2):\mathbb{Q}] = 2$, by the Galois correspondence, $[\mathrm{Gal}(F/\mathbb{Q}) : \overbrace{\mathrm{Gal}(F/\mathbb{Q}(\omega))}^{:=G}] = 4$, so we are looking for an index 4 subgroup of $\langle \tau, \sigma \rangle$ that fixes $\mathbb{Q}(\omega)$. Noting that τ corresponds to complex conjugation and order$(\tau)=2$, we have $\langle\tau\rangle \subseteq G$. We also find that σ^2 fixes $\mathbb{Q}(\omega^2)$, since

$$\sigma^2(a+b\omega^2) = a+b\sigma(\sigma(\omega)^2) = a+b\sigma((i\omega)^2) = a+b\sigma(-\omega^2) = a-b\sigma(\omega)^2 = a-b(i\omega)^2 = a+b\omega^2$$

and since order$(\sigma^2)=2$, we have $|\langle\tau,\sigma^2\rangle| = 4$, so $G := \langle\tau,\sigma\rangle$ has index 2 & fixes $\mathbb{Q}(\omega)$, so we must have

$$\boxed{\mathrm{Gal}(F/\mathbb{Q}(\omega)) = \langle\tau,\sigma^2\rangle}$$
$(\cong \mathbb{Z}_2\times\mathbb{Z}_2)$

$\mathbb{Q}(i\omega)$

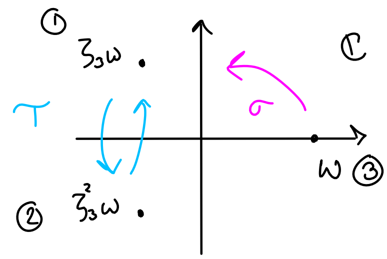
Noting that $[\mathbb{Q}(i\omega):\mathbb{Q}] = 4$ since $\min(i\omega,\mathbb{Q}) = x^4-5$, we look for a subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ of index 4 (& thus order 2) that fixes $\mathbb{Q}(i\omega)$. The subgroup $\langle\tau\sigma^2\rangle$ does the trick, since $\tau\sigma^2(a+bi\omega) = a+b(-i)(i^2\omega) = a+bi\omega$.

$$\boxed{\text{Thus } \mathrm{Gal}(F/\mathbb{Q}(i\omega)) = \langle\tau\sigma^2\rangle \cong \mathbb{Z}_2}$$

$f(x) = x^3-2$ over $\mathbb{Q}$

$\omega = 2^{1/3}$

Factor $f(x) = (x-\omega)(x-\zeta_3\omega)(x-\zeta_3^2\omega)$ where $\zeta_3 = e^{2\pi i/3}$, then $F := \mathbb{Q}(\omega,\zeta_3)$ is the splitting field of $f(x)$, and $[F:\mathbb{Q}] = [F:\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}]$



- $[\mathbb{Q}(\omega):\mathbb{Q}] = 3$, since $\min(\omega,\mathbb{Q}) = x^3-2$.
- $[F:\mathbb{Q}(\omega)] = 2$ since $\min(\zeta_3,\mathbb{Q}(\omega)) = \Phi_3 = x^2+x+1$.

So $[F:\mathbb{Q}] = 6 = |G| := |\mathrm{Gal}(F/\mathbb{Q})| \Rightarrow G \in \{\mathbb{Z}_6, S_3\}$.

We can produce at least two automorphisms fixing $\mathbb{Q}$: $\rightsquigarrow$ $\tau: \begin{cases}\omega \mapsto \omega \\ \zeta_3 \mapsto \zeta_3^2\end{cases} \rightsquigarrow (12)$

And we can check $\sigma: \begin{cases}\omega \mapsto \zeta_3\omega \\ \zeta_3 \mapsto \zeta_3^2\end{cases} \rightsquigarrow (123)$

$$(12)(123) = (1)(23)$$
$$(123)(12) = (13)(2) \neq (12)(123)$$

So G contains a non-abelian subgroup $\langle\tau,\sigma\rangle$ & thus $\boxed{G \cong S_3}$

$f(x) = (x^3-2)(x^2-5)\ /\ \mathbb{Q}$

Noting that $x^2-5 = (x+\omega_5)(x-\omega_5)$ where $\omega_5 = 5^{1/2}$, the splitting field of $f(x)$ will be

$$L := \mathbb{Q}(\omega,\zeta_3,\omega_5) = \mathbb{Q}(2^{1/3}, e^{2\pi i/5})(\sqrt{5}).$$

<u>Claim</u>: $[L:\mathbb{Q}] = [L:\mathbb{Q}(\omega,\zeta_3)][\mathbb{Q}(\omega,\zeta_3):\mathbb{Q}] = 2\cdot 6 = 12$.

The only new content is that $[L:\mathbb{Q}(\omega,\zeta_3)] = 2$, i.e. $\min(\sqrt{5},\mathbb{Q}(\omega,\zeta_3)) = x^2-5$.

The degree could not be higher, since $E \subseteq F \Rightarrow \min(\alpha, F) \mid \min(\alpha, E)$ and $\min(\sqrt{5}, \mathbb{Q}) = x^2 - 5$.
But it could not be 1, since $\sqrt{5} \notin \mathbb{Q}(3^{1/3}, \zeta_3)$.

So $G := \mathrm{Gal}(L/\mathbb{Q}) \geq S_3$ as a subgroup by the previous problem, and is thus a nonabelian group of order 12. We can produce a new automorphism $\gamma: \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ \zeta_4 \mapsto \zeta_4 \\ \omega \mapsto \omega \end{cases}$

Thus $\langle \gamma \rangle$ is a subgroup of order 2, $\langle \gamma \rangle \cap \langle \tau, \sigma \rangle = \{e\}$, and $|\langle \gamma \rangle| \cdot |\langle \sigma, \tau \rangle| = 2 \cdot 6 = 12 = |G|$, and $G = \underbrace{\langle \gamma \rangle \langle \tau, \sigma \rangle}_{\text{product of subgroups}} \Rightarrow \boxed{\begin{aligned} G &= \langle \gamma \rangle \times \langle \tau, \sigma \rangle \\ &\cong \mathbb{Z}_2 \times S_3 \end{aligned}}$ ∎

---

⑥ Suppose f is irreducible & not separable, so $\gcd(f, f') > 1$. Since $\deg f' < \deg f$, and f is irreducible, we have $f'(x) \equiv 0$ in $K[X]$. But if $f(x) = \sum_{j=0}^{m} a_j x^j$ $(a_m \neq 0 \in K)$ $f'(x) = m a_m x^{m-1} + \ldots + a_1 \equiv 0$. So in particular, $m a_m = 0$ in K, forcing $m = 0$ in K and since $m \neq 0 \in \mathbb{N}$, we must have $\mathrm{char}(K) \mid m$. ∎