

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) $r \leq s \leq n$. So g splits in some $F_g \supseteq K$ where $[F_g:K]$ divides $r!$; so considering now $h(x) \in F_g[x]$, there is some splitting field $F_h \supseteq F_g$ 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 $\frac{(r+s)!}{r!s!} = \binom{r+s}{r} \in \mathbb{N}$. ■

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) ■

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

1 \Rightarrow 2: Immediate from defn.

2 \Rightarrow 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 \Rightarrow 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 $q(x) | p(x)$) and so $F/K(\alpha)$ is Galois & $[F:K(\alpha)] = \{F:K(\alpha)\} = |\text{Gal}(F/K(\alpha))|$.

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

$$\text{Stab}_x = \text{Gal}(K(\alpha)/K) \implies |\text{Gal}(F/K) : \text{Gal}(F/K(\alpha))| = |X| = d.$$

But then

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

So F/K is Galois. \blacksquare

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 non-linear 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) $K \leq E \Rightarrow \text{Aut}(F/E) \subseteq \text{Aut}(F/K)$, and to see $\text{Aut}(F/K) \subseteq \text{Aut}(F/E)$, letting $\sigma \in \text{Aut}(F/K)$

we must have $\sigma \in \text{Sym}(\{u_1, \dots, u_n\})$ and so $\sigma(g(x)) = g(\sigma(x)) = \prod (\sigma(x) - u_i) = \sum v_i \sigma(x)^i$

$$\begin{aligned} & \sigma\left(\sum v_i x^i\right) \\ & \sum \sigma(v_i) \sigma(x)^i \end{aligned}$$

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

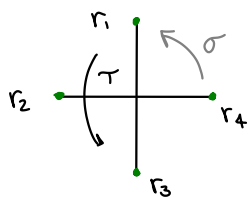


⑤ $f(x) = x^4 - 5$ over

- \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

$$\begin{array}{ll} \tau: F \rightarrow F & \sigma: F \rightarrow F \\ i \mapsto -i & i \mapsto i \\ \omega \mapsto \omega & \omega \mapsto i\omega \end{array}$$

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

⑥

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

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 $[F:\mathbb{Q}] = |\text{Gal}(F/\mathbb{Q})| = 8$.

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

$$[\mathbb{Q}(\omega, \zeta):\mathbb{Q}] = [\mathbb{Q}(\omega, \zeta):\mathbb{Q}(\omega)] [\mathbb{Q}(\omega):\mathbb{Q}]$$

$\swarrow \quad \searrow$
 $\hookrightarrow = 4, \text{ since } \min(\omega, \mathbb{Q}) = x^4 - 5$
 $\hookrightarrow = 2, \text{ since } \mathbb{Q}(\omega) \subseteq \mathbb{R} \text{ but } \zeta \notin \mathbb{R}, \text{ so } \min(\zeta, \mathbb{Q}(\omega)) = x^2 + 1.$

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 $G \not\cong \mathbb{Q}_8$, 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.)

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

$\mathbb{Q}(\omega)$

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

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

Noting that $[\mathbb{Q}(\omega):\mathbb{Q}] = 2$, by the Galois correspondence, $[\text{Gal}(F/\mathbb{Q}) : \text{Gal}(F/\mathbb{Q}(\omega))] = 4$, 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 $\text{order}(\tau)=2$, we have $\langle \tau \rangle \in G$. We also find that σ^2 fixes $\mathbb{Q}(w^2)$, since

$$\sigma^2(a+bw^2) = a+b\sigma(\sigma(w^2)) = a+b\sigma(iw^2) = a+b\sigma(-w^2) = a-b\sigma(w^2) = a-b(iw^2) = a+bw^2$$

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

$$\boxed{\text{Gal}(F/\mathbb{Q}(w)) = \langle \tau, \sigma^2 \rangle.}$$

$$(\cong \mathbb{Z}_2 \times \mathbb{Z}_2)$$

$\mathbb{Q}(iw)$

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

$$\tau\sigma^2(a+b iw) = a+b(-i)(i^2w) = a+b iw.$$

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

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

$$w = 2^{1/3}$$

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

$$\cdot [\mathbb{Q}(w):\mathbb{Q}] = 3, \text{ since } \min(w, \mathbb{Q}) = x^3 - 2.$$

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

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

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

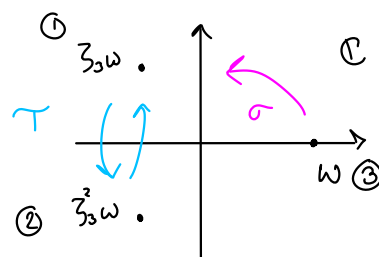
And we can check

$$(12)(123) = (1)(23)$$

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

So G contains a non-abelian subgroup $\langle \tau, \sigma \rangle$ & thus

$$\boxed{G \cong S_3}$$



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

Noting that $x^2 - 5 = (x + w_5)(x - w_5)$ where $w_5 = 5^{1/2}$, the splitting field of $f(x)$ will be

$$L := \mathbb{Q}(w, \zeta_3, w_5) = \mathbb{Q}(2^{1/3}, e^{2\pi i/5})(\sqrt{5}).$$

$$\text{Claim: } [L:\mathbb{Q}] = [L:\mathbb{Q}(w, \zeta_3)][\mathbb{Q}(w, \zeta_3):\mathbb{Q}] = 2 \cdot 6 = 12.$$

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

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 $\sqrt{5} \notin \mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{5})$.

So $G := \text{Gal}(L/\mathbb{Q}) \cong S_3$ as a subgroup by the previous problem, and is thus a nonabelian group of order 12. We can produce a new automorphism γ :

$$\gamma: \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ \sqrt[3]{3} \mapsto \sqrt[3]{3} \\ \omega \mapsto \omega \end{cases}$$

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 $G = \underbrace{\langle \gamma \rangle \times \langle \tau, \sigma \rangle}_{\text{product of subgroups}} \Rightarrow \boxed{G = \langle \gamma \rangle \times \langle \tau, \sigma \rangle \cong \mathbb{Z}_2 \times S_3}$



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 $f(x) = \sum_{j=0}^m a_j x^j$ ($a_m \neq 0 \in K$)
 $f'(x) = m a_m x^{m-1} + \dots + a_1 \equiv 0$. 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 $\text{char}(K) \mid m$. 