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 $\frac{(r+s)!}{r!s!} = \binom{r+s}{r} \in \mathbb{N}$. ■

---

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: $F \geq K$ is <u>Galois</u> iff F is a separable splitting field, or

$[K:F] = \{K:F\} = |Gal(K/F)|$.

<u>1 ⇒ 2</u>: Immediate from defn.

<u>2 ⇒ 3</u>: 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.

<u>3 ⇒ 2</u>: 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 $q_\alpha(x) | p(x)$) 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. ∎

---

④

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

$$\begin{aligned} \sigma(g(x)) &= g(\sigma(x)) = \prod(\sigma(x) - u_i) = \sum v_i \sigma(x)^i \\ &\,\,\| \\ \sigma(\textstyle\sum v_i x^i) & \\ &\,\,\| \\ \textstyle\sum \sigma(v_i)\sigma(x)^i & \end{aligned}$$

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

■