Angelo Taranto (50/50) 4/5/18

Algebra 2 HW 10

① E/F an algebraic extension, $\sigma: E \hookrightarrow E$ a morphism of fields such that $\sigma|_F = Id_F$. Prove $\sigma: E \xrightarrow{\cong} E$.

pf. $\sigma: E \hookrightarrow E$ is injective because $\ker\sigma \subsetneq E$ is an ideal. We need only show σ is surjective. Let $\alpha \in E$. We have:

$$\begin{array}{ccc} E & \overset{\sigma}{\hookrightarrow} & E \\ | & & | \\ F(\alpha) & \xrightarrow{\cong} & \sigma(F(\alpha)) \\ | & & | \\ F & \longrightarrow & F \\ & \sigma|_F = Id_F & \end{array}$$

Let $p(x) \in F[x]$ be the min'l polynomial of α over F (can be chosen since α is algebraic), with $p(\alpha) = 0$

Let $\underbrace{\{\beta_1, \dots, \beta_k\}}_{= S}$ be the roots of $p(x)$ in E $\rightarrow$ i.e. $\beta_1 = \alpha$ ($k \leq n = \deg p(x)$).

Claim: $\sigma|_S : S \longrightarrow S$, i.e. $\sigma(S) \subset S$.

this is because $p(x) \in F[x]$, $\sigma|_F = Id_F \Rightarrow \sigma(p(x)) = p(x)$

so for $\beta_j \in S$, $\sigma(p(\beta_j)) = \sigma(0) = 0$

$= p(\sigma(\beta_j))$, thus $\sigma(\beta_j) \in S$

σ injective $\Rightarrow \sigma|_S : S \hookrightarrow S$, but S is finite so injective maps are surjective $\Rightarrow \exists \beta_j \in S$ such that $\sigma(\beta_j) = \alpha$. So for any $\alpha \in E$ $\exists \beta \in E$ with $\sigma(\beta) = \alpha$. $\square$

③ E/F a normal extension, K intermediate extension $F \subset K \subset E$ and $\sigma: K \hookrightarrow E$ an embedding s.t. $\sigma|_F = Id_F$. Then σ extends to an automorphism $E \xrightarrow{\cong} E$.

Pf. We have

$$\begin{array}{ccc} E & & E \\ | & & | \\ K & \xrightarrow{\sigma} & \sigma(K) \\ | & & | \\ F & \longrightarrow & F \\ & \sigma|_F = Id_F & \end{array}$$

and E/F normal $\Leftrightarrow$ E is splitting ext'n. of some $\mathcal{P} \subset F[x]$ ($E = SF_F(\mathcal{P})$)

Thus, since $\mathcal{P} \subset F[x] \subset K[x]$ and $\mathcal{P} \subset F[x] \subset \sigma(K)[x]$, $E = SF_K(\mathcal{P})$ and $E = SF_{\sigma(K)}(\mathcal{P})$

Thus E is normal over K and $\sigma(K)$.

Note also that $\sigma(\mathcal{P}) = \mathcal{P}$. Thm. 30.2 then gives that σ extends to an automorphism $\sigma: E \xrightarrow{\cong} E$. $\square$

(4) $F = \mathbb{Q}$, $E = SF_{\mathbb{Q}}(x^2-2) = \mathbb{Q}(\sqrt{2})$, and $K = SF_E(x^2-\sqrt{2}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt{2})$
$= \mathbb{Q}(\sqrt[4]{2})$

Describe $Gal(K/F)$ and prove K/F is not Galois.

Pf.

Note that over $F=\mathbb{Q}$, the minimal polynomial of $\sqrt[4]{2}$ is x^4-2, irreducible by Eisenstein.

$\Rightarrow [K:F] = 4$. In general, $|Gal(K/F)| \leq [K:F]$ (actually, $|Gal(K/F)| \mid [K:F]$) $\Rightarrow |Gal(K/F)| \mid 4$.

All the roots of x^4-2 are $\sqrt[4]{2}$, $\sqrt[4]{2}\omega$, $\underbrace{\sqrt[4]{2}\omega^2}_{= -\sqrt[4]{2}}$, $\sqrt[4]{2}\omega^3$ over $\mathbb{C}$ for $\omega = e^{2\pi i/4}$

But $\sqrt[4]{2}\omega^k \in \mathbb{C}\setminus\mathbb{R}$ for $k \in \{1,2,3\}$ so $\sqrt[4]{2}\omega^k \notin \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$

Thus x^4-2 doesn't split into linear factors over $K[x]$

$\Rightarrow K/F$ not normal $\Rightarrow K/F$ not Galois.

Let $\alpha = \sqrt[4]{2}$ $\Rightarrow K = \mathbb{Q}(\alpha)$. Any $\sigma \in Gal(K/F)$ is determined by $\sigma(\alpha)$ since as a field K is generated by $\{\alpha, \alpha^2, \alpha^3, 1\}$.

Also, $\sigma(x^4-2) = x^4-2$, so $\sigma(\alpha)$ must be a (real) root of x^4-2. Thus we have $\sigma = Id$ or

$\uparrow$

α or $-\alpha$.

$$\sigma = \sigma_1 : K \xrightarrow{\cong} K$$
$$\alpha \mapsto -\alpha$$
$$\Rightarrow \alpha^2 \mapsto \alpha^2$$
$$\alpha^3 \mapsto -\alpha^3$$

$\Rightarrow Gal(K/F) \cong \mathbb{Z}_2$. $\square$

(5) $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $F = \mathbb{Q}$. Is E/F Galois and compute $Gal(E/F)$.

Pf.

$E = SF_{\mathbb{Q}}(x^2-2, x^2-3)$ clearly as these have roots $\pm\sqrt{2}, \pm\sqrt{3}$.

$\Rightarrow E/F$ is normal, and x^2-2, x^2-3 (and any poly.) is separable over $\mathbb{Q}$ $\Rightarrow$ E/F is Galois.

$\Rightarrow |Gal(E/F)| = [E:F]$

We compute $[E:F]$.

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

> 2 since x^2-2 is irred. over $\mathbb{Q}$ by Eisenstein.

We claim x^2-3 is irred. over $\mathbb{Q}(\sqrt{2})$, else $\sqrt{3} = a+b\sqrt{2}$ for some $a,b \in \mathbb{Q}$ $\Rightarrow a^2+2b^2+2ab\sqrt{2} = 3 \Rightarrow \sqrt{2} = \dfrac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$ $\lightning$

Thus $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ so $[E:F] = 4 = |Gal(E/F)|$.

Let S = roots of $p = \{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}$. We need only determine $\sigma \in Gal(E/F)$ on $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$.

A basis of E over F is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} = \{1, \alpha, \beta, \alpha\beta\}$.

$\sigma \in Gal(E/F) \Rightarrow \sigma(x^2-2) = x^2-2$ so $\sigma(\alpha^2-2) = \sigma(\alpha)^2 - 2 = 0$

So $\sigma(\alpha)$ is a root of x^2-2, similarly for β and x^2-3.

So $Gal(E/F)$ cannot interchange α and β.

Thus we have

$$\underset{\displaystyle Id}{\sigma_0} : \begin{array}{l} \alpha \longmapsto \alpha \\ \beta \longmapsto \beta \end{array} \qquad \sigma_1 : \begin{array}{l} \alpha \longmapsto -\alpha \\ \beta \longmapsto \beta \end{array} \qquad \sigma_2 : \begin{array}{l} \alpha \longmapsto \alpha \\ \beta \longmapsto -\beta \end{array} \quad \text{and}$$

$$\sigma_3 : \begin{array}{l} \alpha \longmapsto -\alpha \\ \beta \longmapsto -\beta \end{array}$$

All are involutions $\Rightarrow Gal(E/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. $\square$

(6) $\alpha = \sqrt{2+\sqrt{2}} \in \mathbb{R}$ and $E = \mathbb{Q}(\alpha)$, $F = \mathbb{Q}$. Compute $Gal(E/F)$.

Sol.

$\alpha^2 = 2+\sqrt{2} \Rightarrow (\alpha^2-2)^2 = 2 \Rightarrow \alpha^4 - 4\alpha^2 + 2 = 0$

$[E:F]=4 \longleftarrow$ Thus x^4-4x^2+2 is the minimal polynomial of α, irred. by Eisenstein. The quadratic formula gives $x^2 = 2 \pm \sqrt{2}$ for x a root $\Rightarrow$ the roots are $\sqrt{2+\sqrt{2}}$, $\sqrt{2-\sqrt{2}}$, $-\sqrt{2+\sqrt{2}}$, $-\sqrt{2-\sqrt{2}}$. Let $\alpha = \sqrt{2+\sqrt{2}}$, $\beta = \sqrt{2-\sqrt{2}}$.

note $\alpha\beta = \sqrt{2} \Rightarrow \beta = \dfrac{\sqrt{2}}{\alpha}$ (clearly $\sqrt{2} \in \mathbb{Q}(\alpha)$.)

Very clearly.

$E = SF_{\mathbb{Q}}(x^4-4x^2+2) \longleftarrow$ Thus x^4-4x^2+2 splits in $E = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, -\alpha, \beta, -\beta)$ which is thus normal, automatically separable and thus Galois.

You're the only one to have (correctly) mentioned this!

Hence $|\mathrm{Gal}(E/F)| = [E:F] = 4 \Rightarrow \mathrm{Gal}(E/F) \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$

We show $\mathrm{Gal}(E/F)$ has an element of order 4.

Note: $\alpha\beta = \sqrt{2}$, $\alpha^2 - 2 = \sqrt{2}$, and $\beta = \frac{\sqrt{2}}{\alpha}$

Let $\sigma : E \xrightarrow{\cong} E$ be the map s.t. $\sigma(\alpha) = \beta$

$\Rightarrow \underset{\sigma(\sqrt{2})}{\underset{\parallel}{\sigma(\alpha^2-2)}} = \sigma(\alpha)^2 - 2 = \beta^2 - 2 = -\sqrt{2}$

$\Rightarrow \sigma(\beta) = \frac{\sigma(\sqrt{2})}{\beta} = \frac{-\sqrt{2}}{\beta} = -\sqrt{\frac{2}{2-\sqrt{2}}} = -\sqrt{2+\sqrt{2}} = -\alpha$

Thus $\sigma(\beta) = -\alpha$ and $\sigma(-\beta) = \alpha$

$\Rightarrow \sigma : \alpha \longmapsto \beta \longmapsto -\alpha \longmapsto -\beta \longmapsto \alpha$ so σ has order 4 $\Rightarrow \mathrm{Gal}(E/F) \cong \mathbb{Z}_4$. $\square$