HW 9 Solutions MATH 1250

Sec. 48

32. By Corollary 48.5, if $\tau: F(\alpha) \to \overline{F}$ is an iso$\underline{\text{ism}}$ into a subfield of $\overline{F}$, then $\tau(\alpha)$ is a conj. of α (i.e. a root of irr. poly. of α). Also τ is determined by $\tau(\alpha)$. Since the irr. poly. has degree n, it has at most n roots and

thus there are at most n iso$\underline{\text{ism}}$s.

34. Let $\sigma: E \to E$ be an auto. of E leaving F fixed. Let $\alpha \in E$ & let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_s$ be Conj. of α that lie in E. Pick α_i, $i = 1 \cdots s$.
Then $\sigma(\alpha_i)$ (by Coro. 48.5) is a Conj. of α_i & Since σ is an auto. it should lie in E & hence $\sigma(\alpha_i)$ is one of the α_j's.

i.e. $\sigma: \{\alpha_1, \dots, \alpha_s\} \longrightarrow \{\alpha_1, \dots, \alpha_s\}$. Also σ is a one-to-one function (auto$\underline{\text{ism}}$) so σ gives a permutation of $\{\alpha_1, \dots, \alpha_s\}$.

36. (a) First note that $\zeta^i \neq 1$ for $i < p$. Because otherwise

ζ is a root of $x^i - 1$ and since $\Phi_p(x)$ is irr. $(= \text{irr}(\zeta, \mathbb{Q}))$ then $x^i - 1$ is div. by $\Phi_p(x)$ which is not possible as $\deg \Phi_p(x) = p-1 \geq i$.

Thus all the $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$ are distinct.

Also $\underset{i=1,\dots,p-1}{(\zeta^i)^p - 1} = (\zeta^p)^i - 1 = 1-1=0 \Rightarrow \zeta^i$ are roots of x^p-1

& Since $\zeta^i \neq 1$ they are roots of $\Phi_p(x) = \dfrac{x^p-1}{x-1}$.

& there are $p-1$ of them hence $\zeta, \dots, \zeta^{p-1}$ are all the

roots of $\Phi_p(x)$.

(b) Each auto. $\sigma \in G(\mathbb{Q}(\zeta)/\mathbb{Q})$ is determined by

$\sigma(\zeta)$ which is one of the ζ^i's.

Take $\sigma_1, \sigma_2 \in G(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $\sigma_1(\zeta) = \zeta^i$ and $\sigma_2(\zeta) = \zeta^j$.

Then $\sigma_1(\sigma_2(\zeta)) = \sigma_1(\zeta^j) = (\sigma_1(\zeta))^j = \zeta^{ji}$

$\sigma_2(\sigma_1(\zeta)) = \sigma_2(\zeta^i) = (\sigma_2(\zeta))^i = \zeta^{ij} = \zeta^{ji}$.

$\Rightarrow \sigma_1\sigma_2 = \sigma_2\sigma_1$ (because auto. determined by its value on ζ).

$\Rightarrow G(\mathbb{Q}(\zeta)/\mathbb{Q})$ abelian. By Cor. 48.5 for each $\zeta^i, i=1\dots p-1$

there is an iso. from $\mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta^i)$, $\zeta \longmapsto \zeta^i$

but but $\mathbb{Q}(\zeta^i) = \mathbb{Q}(\zeta)$ so this is an auto. & we have $p-1$ auto.

This finishes Part (b) (by Ex. 32 there cannot be more than $p-1$ automorphisms).

(c) We know by Thm. 30.23 that $B = \{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$ is a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Let $\beta \in \mathbb{Q}(\zeta)$. We can write

$$\frac{\beta}{\zeta} = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2} \quad \text{for } a_i \in \mathbb{Q}.$$

Multiplying by ζ we see that $\beta = a_0\zeta + \cdots + a_{p-2}\zeta^{p-1}$. So these powers of ζ do span $\mathbb{Q}(\zeta)$. They are lin. ind. because a lin. combination of them equal to zero gives a lin. comb. of elements of B equal to $\underline{0}$ (after dividing by ζ). Thus $\{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$ is a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$.

By Thm. 48.3 and Part (a) there exist automorphisms σ_i, $i = 1, \dots, p-1$ in $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\sigma_i(\zeta) = \zeta^i$. Thus if $\beta = a_0\zeta + \cdots + a_{p-2}\zeta^{p-1}$ is fixed by all such σ_i we must have $a_0 = a_1 = \cdots = a_{p-2}$ so $\beta = a_0(\zeta + \cdots + \zeta^{p-1}) = -a_0$ since ζ is a zero of $\Phi_p(x)$. Thus $\beta \in \mathbb{Q} \Rightarrow \mathbb{Q}$ is the fixed field of $G(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Sec. 49

6. The extensions are:

τ_1 given by $\tau_1(i) = i$, $\tau_1(\sqrt{3}) = -\sqrt{3}$, $\tau_1(\alpha_1) = \alpha_1$.

τ_2 given by $\tau_2(i)=i$, $\tau_2(\sqrt{3})=-\sqrt{3}$, $\tau_2(\alpha_1)=\alpha_2$

τ_3 " " $\tau_3(i)=i$, $\tau_3(\sqrt{3})=-\sqrt{3}$, $\tau_3(\alpha_1)=\alpha_3$

τ_4 " " $\tau_4(i)=-i$ $\tau_4(\sqrt{3})=-\sqrt{3}$, $\tau_4(\alpha_1)=\alpha_1$.

τ_5 " " $\tau_5(i)=-i$ $\tau_5(\sqrt{3})=-\sqrt{3}$ $\tau_5(\alpha_1)=\alpha_2$.

τ_6 " " $\tau_6(i)=-i$ $\tau_6(\sqrt{3})=-\sqrt{3}$, $\tau_6(\alpha_1)=\alpha_3$

where $\alpha_1=\sqrt[3]{2}$ $\alpha_2=\sqrt[3]{2}\underbrace{\left(\frac{-1+i\sqrt{3}}{2}\right)}_{e^{2\pi i/3}}$ $\alpha_3=\sqrt[3]{2}\underbrace{\left(\frac{-1-i\sqrt{3}}{2}\right)}_{e^{2\pi i(2/3)}}$

10. Let E be an algebraic ext. of F and let τ be an iso$\underline{\text{ism}}$ of E onto a subfield of $\overline{F}$ that leaves F fixed. Because E is an alg. ext. of F, the field $\overline{F}$ is an alg. ext. of E & is an alg. closure of E. By Thm. 49.3, τ can be extended to an iso$\underline{\text{ism}}$ σ of $\overline{F}$ onto a subfield of $\overline{F}$. If σ is not onto applying Iso. Ext. Thm. to σ^{-1}, can be extended to whole $\overline{F}$ which shows σ was onto in fact.

Sec. 50

4. The splitting field has deg. 6 over $\mathbb{Q}$. Replace $\sqrt[3]{2}$ by $\sqrt[3]{3}$ in Example 50.9.