Homework 6

1 i. Using induction on $[E:F]$,

if $[E:F] = 1$ then $E = F$, so $E = F(1)$.

if $[E:F] > 1$ then $\exists\ \alpha_1 \in E,\ \alpha_1 \notin F$.

consider: $F \subsetneq F(\alpha_1) \subseteq E$.

If $F(\alpha_1) = E$ then we're done.

If not, then $[E : F(\alpha_1)] < [E:F]$,

so by induction $F = F(\alpha_1)(\alpha_2, \alpha_3, \dots, \alpha_n)$

for some set $\{\alpha_2, \dots, \alpha_n\} \subseteq E$.

ii. By part (i) and by Thm 31.4 (in the proof),

E has an F-basis consisting of all products of powers of α_i's, where the exponent of α_i is bounded by the degree of its minimal polynomial. Let $\{1, \beta_1, \beta_2, \dots, \beta_N\}$ be this basis.

Since σ is an isomorphism, its values on $\alpha_1 \dots \alpha_n$ determin its values on $\beta_1 \dots \beta_N$, and since it fixes F, $\sigma(1) = 1$.

since σ is an isomorphism fixing F, it's additive and for any $a \in F$ and β_i, $\sigma(a\beta_i) = \sigma(a)\sigma(\beta_i)$ $= a\sigma(\beta_i)$. Then any F-linear combination of the basis $\{1, \beta_1, \beta_2, \ldots, \beta_N\}$ is determined by the values of σ on the basis, and these values are determined by the values of σ on $\{\alpha_1, \ldots, \alpha_n\}$.

iii) By definition, if τ is an isomorphism then it sends 1 to 1, is F linear, and $\tau(\alpha_i \alpha_j)$ $= \tau(\alpha_i)\tau(\alpha_j)$ $\forall\, 1 \le i, j \le n$

Conversely, if $\tau : E \to F$ is F-linear, sends 1 to 1, and $\tau(\alpha_i \alpha_j) = \tau(\alpha_i)\tau(\alpha_j)$ $\forall\ 1 \le i, j \le n$, we need to prove τ is an isomorphism of rings.

Again, conside the basis $\{1, \beta_1, \ldots, \beta_N\}$ for E over F. Since each β_i is a product of powers of α_i, we know $\tau(\beta_i \beta_j) = \tau(\beta_i)\tau(\beta_j)$ $\forall\ 1 \le i, j \le N$. For an arbitrary $\gamma, \gamma' \in E$ we can write $\gamma = a_0 + a_1\beta_1 + a_2\beta_2 + \ldots + a_N\beta_N$ and $\gamma' = a_0' + a_1'\beta_1 + \ldots + a_N'\beta_N$,

and since τ is F-linear, it fixes F-multiples of 1, and

$$\tau(\gamma+\gamma') = \tau\left((a_0+a_0')+(a_1+a_1')\beta_1+\dots+(a_N+a_N')\beta_N\right)$$

$$= \tau\left(a_0+a_1\beta_1+\dots+a_N\beta_N + a_0'+a_1'\beta_1+\dots+a_N'\beta_N\right)$$

$$= \tau(\gamma)+\tau(\gamma').$$

And

$$\tau(\gamma\gamma') = \tau\left((a_0+a_1\beta_1+\dots+a_N\beta_N)(a_0'+a_1'\beta_1+\dots+a_N\beta_N)\right)$$

$$= \tau\left(\sum_{j=0}^{N}\sum_{k=0}^{N} a_j a_k' \beta_j\beta_k\right) \quad (\text{here } \beta_0=1).$$

$$= \sum_{j=0}^{N}\sum_{k=0}^{N} a_j a_k' \tau(\beta_j\beta_k) \quad \text{by } F\text{-linearity}$$

$$= \sum_{j=0}^{N}\sum_{k=0}^{N} a_j a_k' \tau(\beta_j)\tau(\beta_k) \quad \text{by preceding arg}$$

$$= \left(a_0+a_1\tau(\beta_1)+\dots+a_N\tau(\beta_N)\right)\left(a_0'+a_1'\tau(\beta_1)+\dots+a_N'\tau(\beta_N)\right)$$

$$= \tau(\gamma)\tau(\gamma'),$$

and $\tau(1)=1$ by assumption

So τ is a ring homomorphism. The kernel of τ is a proper ideal ($1 \notin \ker\tau$), and the only proper

ideal in a field is $\{0\}$. So τ is injective, and it's surjective onto its image, so τ is an iiom from E to a subfield of $\overline{F}$.

2. $G = G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is the group

$\{\sigma_{id}, \sigma_1, \sigma_2, \sigma_3\}$, with automorphisms determined by: $\sigma_1 : \begin{matrix} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow \sqrt{3} \end{matrix}$

$\sigma_2 : \begin{matrix} \sqrt{2} \longrightarrow \sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3} \end{matrix}$

$\sigma_3 : \begin{matrix} \sqrt{2} \longrightarrow -\sqrt{2} \\ \sqrt{3} \longrightarrow -\sqrt{3}. \end{matrix}$

with subgroups G,

$\{\sigma_{id}, \sigma_1\}$

$\{\sigma_{id}, \sigma_2\}$

$\{\sigma_{id}, \sigma_3\}$.

$\{\sigma_{id}\}$.

iv. $|G(\mathbb{Q}(w)/\mathbb{Q})| = \{\mathbb{Q}(w) : \mathbb{Q}\} = 4$,

and $\sigma \in G(\mathbb{Q}(w)/\mathbb{Q})$ is determined by $\sigma(w)$ [see problem #1].

$\sigma(w) \in \{w, w^2, w^3, w^4\}$, since it can only be a conjugate of w.

Let σ_1 be defined by $w \longmapsto w^1$

σ_2 by $w \longmapsto w^2$

σ_3 by $w \longmapsto w^3$

σ_4 by $w \longmapsto w^4$.

then the mult. table is.

	σ_1	σ_2	σ_3	σ_4
σ_1	σ_1	σ_2	σ_3	σ_4
σ_2	σ_2	σ_4	σ_1	σ_3
σ_3	σ_3	σ_1	σ_2	σ_2
σ_4	σ_4	σ_3	σ_2	σ_1

4i Since $F(\alpha)$ is a splitting field, we have $|G(F(\alpha)/F)| = [F(\alpha):F]$, which divides $[F(\alpha):F]$ by Thm 51.6.

ii If $f(x)$ has distinct roots $\{\alpha_1, \dots, \alpha_n\}$, with $\alpha_1 = \alpha$, then $\sigma \in G(F(\alpha)/F)$ is determined by $\sigma(\alpha)$.

but $\sigma(\alpha) \in \{\alpha_1, \alpha_2, \dots, \alpha_n\}$, since it must be a conjugate of α.

For any α_i, Thm 48.3 $\Rightarrow \exists\, \psi_{\alpha,\alpha_i} : F(\alpha) \to F(\alpha_i)$, and Thm 49.3 $\Rightarrow$ we can extend ψ_{α,α_i} to an isom from $F(\alpha)$ to a subfield of $\overline{F}$ (in fact we don't need to do this extension), And since $F(\alpha)$ is a splitting field, 50.3 tells us ψ_{α,α_i} is an automorphism of $F(\alpha)$. So $\forall\ 1 \le i \le n$, $\psi_{\alpha,\alpha_i} \in G(F(\alpha)/F)$. So $|G(F(\alpha)/F)| \le n$, and it divides n, so it's equal to n.

5. i $F \leq F(\alpha)$ is separable (Cor 51.10)

and since β is separable over F, and the minimal polynomial of β over $F(\alpha)$ divides the minimal polynomial of β over F, we know β is also seperable over $F(\alpha)$. So $F(\alpha) \leq F(\alpha, \beta)$ is separable.

Then $F \leq F(\alpha) \leq F(\alpha, \beta)$ is a tower of separable extensions, so Thm 51.9 $\Rightarrow F(\alpha, \beta)$ is separable over F. So by Cor 57.10, all elements of $F(\alpha, \beta)$ are separable / F. In particular, $\alpha+\beta$, $\alpha-\beta$, $\frac{\alpha}{\beta}$, $\alpha \cdot \beta$ are separable over F.

ii By (i), the elements of E that are separable over F are closed under addition, subtraction, multiplication, and taking multiplicative inverses. So $\{\alpha \mid \alpha \in E, \alpha \text{ sep. } / F\}$ is a subring of E, and all nonzero elements of this subring have multiplicative inverses. So this is a subfield of E.