SOLUTION SHEET 6:

(1) Let $F = \mathbb{F}_{p^e}$ for some prime p and natural number $e>0$. Let $\sigma \in Aut_F(\bar{F})$ be a non-trivial automorphism of finite order n. By taking powers of σ we may assume that n is prime. Let $x \in \bar{F}$ such that $\sigma(x) \neq x$.

Then $\mathbb{F}_{p^e}(x) = \mathbb{F}_{p^{e \cdot r}}$ for some $r>0$. As $\mathbb{F}_{p^e} \subseteq \mathbb{F}_{p^{e \cdot r}}$ is normal, σ restricts to an automorphism σ' of $\mathbb{F}_{p^{e\cdot r}}$. Note that σ' is non trivial as $x \in \mathbb{F}_{p^{e\cdot r}}$ thus the order of σ' is also n. Let K be the fixed field of σ and notice that $[\mathbb{F}_{p^e}(x) : \mathbb{F}_{p^e}(x) \cap K] = n$ because $\mathbb{F}_{p^e}(x) \cap K = \mathbb{F}_{p^e}(x)^{\langle\sigma'\rangle}$.

Let $m = r \cdot \ell$ and $E = \mathbb{F}_{p^{e \cdot m}} \supseteq \mathbb{F}_{p^e}(x)$. Then $\sigma_{|E}$ is once again a non-trivial automorphism. Moreover $[E : E \cap K] = n$ as before. But $\mathbb{F}_{p^e}(x)$ is the only subfield of E with $[E : \mathbb{F}_{p^e}(x)] = n$ this shows that $\mathbb{F}_{p^e}(x) = E \cap K$
$\Rightarrow x \in K$ which is contradiction. This shows that every non-trivial element in $Aut_F(\bar{F})$ has infinite order.

Now lets show that $Aut_F(\bar{F})$ is abelian. Let $\sigma, \delta \in Aut_F(\bar{F})$ and suppose that there exists $x \in \bar{F}$ such that $(\sigma\delta - \delta\sigma)(x) \neq 0$.
Consider the field extension $F \subseteq F(x)$. As before $\sigma_{|F(x)}, \delta_{|F(x)} \in Gal(F(x)/F)$
But $Gal(F(x)/F)$ is cyclic (so abelian) thus

$$(\sigma_{|F(x)}\delta_{|F(x)} - \delta_{|F(x)}\sigma_{|F(x)})(x) = 0$$ which is a contradiction.

(2)(i) We can write

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \_\_ \times \mathbb{Z}/n_k\mathbb{Z} \quad \text{for } n_i \in \mathbb{N}.$$

by Dirichlet's theorem there exist a prime number p_i such that $p_i = k_i \cdot n_i + 1$ for some $k_i \in \mathbb{N}$ i.e. $n_i \mid p_i - 1$. As $(\mathbb{Z}/p_i\mathbb{Z})^\times$ is a cyclic group of order $p_i - 1$ there exists a subgroup H_i of order k_i and we have $\mathbb{Z}/n_i\mathbb{Z} \cong (\mathbb{Z}/p_i\mathbb{Z})^\times / H_i$ and

$$G \cong (\mathbb{Z}/p_1\mathbb{Z})^\times/H_1 \times \_\_ \times (\mathbb{Z}/p_k)^\times/H_k$$

Note that

$$\prod_{i=1}^k (\mathbb{Z}/p_i\mathbb{Z})^\times \cong (\mathbb{Z}/p_1 \cdots p_k)^\times$$ thus G is a quotient group of $A := (\mathbb{Z}/p_1 \cdots p_k)^\times$ and we write $G \cong A/H$ for some $H \trianglelefteq A$.
Define $m := p_1 \cdots p_k$ and let ξ be an mth root of unity.
Then $Gal(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and $\mathbb{Q} \subseteq \mathbb{Q}(\xi)$ is Galois.
Take $H \trianglelefteq Gal(\mathbb{Q}(\xi)/\mathbb{Q})$ as above. Then $\mathbb{Q} \subseteq \mathbb{Q}(\xi)^H$ is Galois and $Gal(\mathbb{Q}(\xi)^H/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times/H = A/H \cong G$ and we are done.

(ii) Note that by Dirichlets theorem there exists infinitely prime p_i such that $p_i = k_i \cdot n_i + 1$. This shows that there are infinitely many extensions $\mathbb{Q} \subseteq L'$ such that $Gal(L'/\mathbb{Q}) \cong G$. By the primitive element theorem, write $K = \mathbb{Q}(\alpha)$ and define $L = L'(\alpha)$. Notice that $K \subseteq L$ is normal indeed $\mathbb{Q} \subseteq L'$ is normal so L' is the splitting field of a polynomial therefore $L'(\alpha)$ is the splitting field of the same polynomial. It is clearly separable as characteristic is 0. Therefore $\mathbb{Q}(\alpha) \subseteq L'(\alpha)$ is Galois. Moreover it can be seen that $Gal(L'(\alpha)/\mathbb{Q}(\alpha)) \xrightarrow{\cong} Gal(L'/\mathbb{Q})$ hence we are done.

$$\sigma \longmapsto \sigma_{|L'}$$

(3) Let $\overline{K}$ be an alg. closure of K. Then $\overline{K}$ is given by the union of all the intermediate finite extensions $K \subseteq L \subseteq \overline{K}$. For such an extension L we have that $\mathrm{Gal}(L/K) = \langle \sigma_L \rangle$ as $\mathrm{Gal}(L/K)$ is cyclic. Define

$$\bar{\sigma} \in \mathrm{Aut}_K(\overline{K}) \quad \text{by} \quad \bar{\sigma}_{|L} = \sigma_L. \text{ Let us show that } \overline{K}^{\bar{\sigma}} = K.$$

Let $x \in \overline{K}$ such that $\bar{\sigma}(x) = x$. As $K \subseteq K(x)$ is a finite extension

$x = \bar{\sigma}(x) = \sigma_{K(x)}(x) \Rightarrow x \in K(x)^{\sigma_{K(x)}} = K$.

Caution: One should show that $\bar{\sigma}$ is well defined, that is for $x \in L \cap L'$ where L, L' are finite extensions of K we should show that $\sigma_L(x) = \sigma_{L'}(x)$. As every Galois group is cyclic and thus abelian we have that $K \subseteq K(x)$ is also a cyclic extension.

Then $\sigma_L(x) = \sigma(x) = \sigma_{L'}(x)$.

(4)(i) The containment $\mathrm{im}\,T \subseteq K$ is clear as $T(\ell)$ is fixed by the action of $Gal(L/K)$ and $K \subseteq L$ is Galois. The additivity is a consequence of $g \in G$ being field homomorphisms.

(ii) In this case write $T(\ell) = \sum_{g\in G} g(\ell) = \sum_{i=0}^{n-1} \sigma^i(\ell) = \ell + \sigma(\ell) + \sigma^2(\ell) + \_ + \sigma^{n-1}(\ell)$
Now it is clear that $\mathrm{im}(\sigma - id_L) \subseteq \ker(T)$. Suppose that $\ell \in \ker T$ and let
$x = \ell + (\ell + \sigma(\ell)) + (\ell + \sigma(\ell) + \sigma^2(\ell)) + \_ + (\ell + \sigma(\ell) + \_ + \sigma^{n-1}(\ell))$.
then $x - \sigma(x) = (\ell - \sigma(\ell)) + (\ell - \sigma^2(\ell)) + \_ + (\ell - \sigma^{n-1}(\ell)) + (\ell - \ell)$
$= n.\ell - (\ell + \sigma(\ell) + \sigma^2(\ell) + \_ + \sigma^{n-1}(\ell)) = n.\ell$
Thus taking $\frac{-x}{n}$ works.

(5) Suppose that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\omega)$ where ω is an nth root of unity for some n.
Note that $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ is Galois. Moreover $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ is Abelian.
As $\mathbb{Q}(\sqrt[3]{2})$ is an intermediate extension $\exists H \leqslant Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ such that
$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\omega)^H$. But as $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ is Abelian H is normal which implies that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is Galois. This is a contradiction.

(6) Suppose that there is a non-real root $z \in \mathbb{C} \setminus \mathbb{R}$. Then $\bar{z}$ is also a root.
This shows that $\bar{\cdot}$ acts non-trivially on the roots of f thus has order 2 in $Gal(L/\mathbb{Q})$. However $Gal(L/\mathbb{Q}) \cong C_3$ which do not contain an element of order 2.

(7) (i) Let F be the normal closure of $L(\alpha)$ of K. This is obtained by adjoining $L(\alpha)$ all the roots of the minimal polynomial of α over K.
Let us show that $L(\alpha)^{norm} = L(\alpha, \sigma(\alpha))$.

First of all note that the polynomial $H(x) = (x^2 - \beta)(x^2 - \sigma(\beta))(x^2 - \sigma^2(\beta))$ is in $K[x]$. Indeed all of its coefficients are invariant under the action of $Gal(L/K)$. Therefore $m_{\alpha,K} \mid H(x)$ and the roots of $m_{\alpha,K}$ are contained in $\{\pm\alpha, \pm\sigma(\alpha), \pm\sigma^2(\alpha)\}$ which are the roots of $H(x)$. Moreover note that the only roots of $m_{\alpha,K}$ can't be α and $-\alpha$ as $\beta \notin K$ therefore either $\sigma(\alpha) \in L(\alpha)^{norm}$ or $\sigma^2(\alpha) \in L(\alpha)^{norm}$. In both cases by the identity,

$$\alpha^2 \sigma(\alpha)^2 \sigma^2(\alpha)^2 = \beta\sigma(\beta)\sigma^2(\beta) = 1$$ we have that
$\alpha, \sigma(\alpha) \in L(\alpha)^{norm}$. by the same identity we have that all the roots of $H(x)$ are contained in $L(\alpha, \sigma(\alpha))$. This shows that $L(\alpha, \sigma(\alpha)) = L(\alpha)^{norm}$.

Now let us compute $Gal(L(\alpha,\sigma(\alpha))/K)$. First of all
$$[L(\alpha,\sigma(\alpha)):K] = [L(\alpha,\sigma(\alpha)):L(\alpha)].[L(\alpha):L].[L:K]$$
$$= [L(\alpha,\sigma(\alpha)):L(\alpha)]. \quad 2 \quad . \quad 3$$
Moreover $\sigma(\alpha)$ is a root of $x^2 - \sigma(\beta)$ and $L(\alpha) \neq L(\alpha)^{norm} = L(\alpha, \sigma(\alpha))$
therefore $[L(\alpha,\sigma(\alpha)):L(\alpha)] = 2$ and $|Gal(L(\alpha,\sigma(\alpha))/K)| = 12$.

As $L(\alpha)/K$ is not Galois (as it is not normal) $Gal(L(\alpha,\sigma(\alpha))/K)$ is not abelian.

Now the 2-Sylow group is normal as L/K is Galois. Looking at the classification of finite groups of order 12 we see that $Gal(L(\alpha,\sigma(\alpha))/K) \cong A_4$.

(ii) We think of L as an intermediate extension, $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(\zeta_7)$

Recall that $Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = (\mathbb{Z}/7\mathbb{Z})^\times = \mathbb{Z}/6\mathbb{Z}$ and it is generated by $\sigma: \zeta_7 \to \zeta_7^3$. Then L is given by the fixed field of $\{id, \sigma^3\}$.

And $Gal(L/\mathbb{Q}) = Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})/\{id, \sigma^3\} = \{id, \sigma, \sigma^2\}$.

It remains to show that $\overbrace{(\zeta_7 + \zeta_7^6).(\zeta_7^3 + \zeta_7^4).(\zeta_7^2 + \zeta_7^5)}^{(*)} = 1$

$(*) = (\zeta_7^4 + \zeta_7^5 + \zeta_7^2 + \zeta_7^3)(\zeta_7^2 + \zeta_7^5) = (\zeta_7^6 + 1 + \zeta_7^4 + \zeta_7^5 + \zeta^2 + \zeta_7^3 + 1 + \zeta_7)$

Now we know that ζ_7 is a root of $x^6 + x^5 + x^4 + x^3 + x^2 + 1$ therefore the above expression is indeed equal to 1.