Exersise 5.1

We can define

$$\alpha = \frac{1}{\mathrm{Tr}(\theta)}\left(\beta\theta + (\beta+\beta^{\sigma})\theta^{\sigma} + \dots \left(\sum_{i=0}^{k}\beta^{\sigma^i}\right)\theta^{\sigma^k} + \dots + \left(\sum_{i=0}^{n-2}\beta^{\sigma^i}\right)\theta^{\sigma^{n-2}}\right)$$

Where $\theta \in K$ is chosen so that $\mathrm{Tr}(\theta) \neq 0$ (this can always be done since $\sigma, \sigma^2, \dots \sigma^n$ are linearly independent)

We have that

$$\alpha^{\sigma} = \frac{1}{\mathrm{Tr}(\theta)}\left(\beta^{\sigma}\theta^{\sigma} + (\beta^{\sigma}+\beta^{\sigma^2})\theta^{\sigma^2} + \dots \left(\sum_{i=0}^{k}\beta^{\sigma^{i+1}}\right)\theta^{\sigma^k} + \dots + \left(\sum_{i=0}^{n-2}\beta^{\sigma^{i+1}}\right)\theta^{\sigma^{n-1}}\right)$$

Notice that

$$\mathrm{Tr}(\beta) = \sum_{i=0}^{n-1}\beta^{\sigma^i} = 0 \Rightarrow \sum_{i=0}^{n-2}\beta^{\sigma^{i+1}} = -\beta$$

Pairing up terms we have the following cancelation

$$\alpha - \alpha^{\sigma} = \frac{1}{\mathrm{Tr}(\theta)}\left(\beta\theta + (\beta+\beta^{\sigma}-\beta^{\sigma})\theta^{\sigma} + \dots \left(\beta + \sum_{i=1}^{k}\beta^{\sigma^i} - \beta^{\sigma^i}\right)\theta^{\sigma^k} + \dots + \beta\theta^{\sigma^{n-1}}\right)$$

$$= \beta\frac{\mathrm{Tr}(\theta)}{\mathrm{Tr}(\theta)} = \beta$$

Thus we have

$$\alpha - \alpha^{\sigma} = \beta$$

Exersise 5.2

Since K/k is Galois, we know that K is Galois over the intermediate field $k' = K \cap \ell \supseteq k$ as well since it is still the splitting field of the same seperable polynomial f over k. Letting $\alpha_1, \alpha_2, \dots \alpha_n \notin K \cap \ell$ be the roots of f not in k' we have that

$$K = k'(\alpha_1, \alpha_2, \dots \alpha_n)$$

When considering the extension $K\ell/\ell$ we have that

$$K\ell = \ell(\alpha_1, \alpha_2, \dots \alpha_n)$$

Since $K = k'(\alpha_1, \dots \alpha_n) \subseteq \ell(\alpha_1, \dots \alpha_n)$ and $\ell \subseteq \ell(\alpha_1, \dots \alpha_n)$ which leads to $K\ell \subseteq \ell(\alpha_1, \dots \alpha_n)$ while conversly $\ell(\alpha_1 \dots \alpha_n) \subseteq K\ell$ since $\alpha_1 \dots \alpha_n \in K$

Thus $K\ell$ is the splitting field of f over ℓ and thus Galois
We have the isomorphism

$$\Phi : \mathrm{Gal}(K\ell/\ell) \to \mathrm{Gal}(K/k')$$

$$\varphi \to \varphi|_K$$

Φ is injective since every automorphism in both $\mathrm{Gal}(K\ell/\ell)$ and $\mathrm{Gal}(K/k')$ is fully determined by the image of $\alpha_1 \dots \alpha_n$ so if $\varphi|_K = \psi|_K$ then they must act the same way on $\alpha_1 \dots \alpha_n$ and thus must be the same automorphisms to begin with
Φ is surjective as follows:
We have that $H = \mathrm{im}(\Phi)$ is a subgroup of $\mathrm{Gal}(K/k')$. If we show that the fixed field of H is precisely k' then from the correspondence of Galois theory it must be the case $\mathrm{im}(\Phi) = \mathrm{Gal}(K/k')$
We have that for any $\alpha \in K \setminus k'$, we have that $\alpha \notin \ell$ and thus there is an isomorphism

$$\varphi : \ell(\alpha) \to \ell(\beta)$$

$$\alpha \to \beta$$

where $\beta \neq \alpha$ is another root of the minimal polynomial of α over ℓ. Since $K\ell$ is a splitting field this isomorphism extends to a automorphism

$$\psi : K\ell/\ell$$

Thus we have $\psi|_K \in H$ is a automorphism which does not fix α. Thus it must be the case the fixed field is k'

We have that

$$|\mathrm{Gal}(K\ell/\ell)| = |\mathrm{Gal}(K/K \cap \ell)|$$

so

$$[K\ell : \ell] = [K : K \cap \ell]$$

multiplying on both sides by $[\ell : k][K \cap \ell : k]$

$$[K\ell : \ell][\ell : k][K \cap \ell : k] = [K : K \cap \ell][\ell : k][K \cap \ell : k]$$

$$[K\ell : k][K \cap \ell : k] = [K : k][\ell : k]$$

Exersise 5.3

We have the isomorphism

$$\Phi : \mathrm{Gal}(K_1K_2/k) \to \mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k)$$

$$\varphi \to (\varphi|_{K_1}, \varphi|_{K_2})$$

Φ is injective as follows. Since, K_1, K_2, K_1K_2 are splitting fields,

$$K_1 = k(\alpha_1 \dots \alpha_n), K_2(\beta_1 \dots \beta_m)$$

$$K_1K_2 = k(\alpha_1 \dots \alpha_n, \beta_1, \dots \beta_m)$$

We have that $\varphi \in \mathrm{Gal}(K_1K_2/k)$ is completely determined by the image of $\alpha_1 \dots \alpha_n, \beta_1 \dots \beta_m$, yet every element in $\mathrm{Gal}(K_1/k)$ and $\mathrm{Gal}(K_2/k)$ is determined by the images of $\alpha_1 \dots \alpha_n$ or $\beta_1 \dots \beta_m$ respectively. Thus if $(\varphi|_{K_1}, \varphi|_{K_2}) = (\psi|_{K_1}, \varphi|_{K_2})$ then it must be the case that $\varphi = \psi$ since they act the same way on $\alpha_1 \dots \alpha_n, \beta_1 \dots \beta_n$
Φ is surjective as follows:
We have that $H = \mathrm{im}(\Phi)$ is a subgroup of $\mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k)$. If we define the following groups

$$H_1 = H \cap (\mathrm{Gal}(K_1/k) \times \{\mathrm{id}\})$$

and

$$H_2 = H \cap (\{\mathrm{id}\} \times \mathrm{Gal}(K_2/k))$$

If we show

$$H_1 = \mathrm{Gal}(K_1/k) \times \{\mathrm{id}\}$$
$$H_2 = \{\mathrm{id}\} \times \mathrm{Gal}(K_2/k)$$

then we have shown

$$H = \mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k)$$

and thus Φ is surjective.
Under the canonacal isomorphism H_1, H_2 are subgroups of $\mathrm{Gal}(K_1/k), \mathrm{Gal}(K_2/k)$ respectively. Thus if we show that they each have fixed field k, then we have shown that each is isomorphic to their respective Galois group and thus be able to conclude that Φ is surjective. To show that the fixed field of H_1 is k, consider any $\alpha \in K_1 \backslash k$. There exists the isomorphism

$$\varphi : k(\alpha) \to k(\beta)$$

$$\alpha \to \beta$$

where $\beta \neq \alpha$ is a root of the same minimal polynomial over k. Since K_1K_2 is a splitting field of $k(\alpha)$ this isomorphism extends to an automorphism $\psi \in \mathrm{Gal}(K_1K_2/k)$. We have that

$$(\psi|_{K_1}, \mathrm{id}) \in H_1$$

And thus H_1 does not fix α so the fixed field of H_1 must be k. The argument for H_2 is the same with the appropriate relabeling

Exersise 5.4

We will define

$$\widetilde{K} = \bigcup_{\varphi \in \mathrm{Aut}(\overline{k}/k)} \varphi(K)$$

We have that $\widetilde{K}$ is Galois by the fact that the fixed field of $\mathrm{Aut}(\widetilde{K}/k)$ is k. The reason for this is because for any $\alpha \in \widetilde{K} \setminus k$, there exists an automorphism

$$\varphi : k(\alpha) \to k(\beta)$$

which extends to

$$\phi \in \mathrm{Aut}(\overline{k}/k)$$

that sends α to some other root β of the minimal polynomial of α and thus does not fix α. Thus $\phi|_{\widetilde{K}} \in \mathrm{Aut}(\widetilde{K}/k)$ is an automorphism that does not fix α

We have that for any Galois extension K'/k with $K \subseteq K'$ if there exists $\alpha \in \widetilde{K} \setminus K'$, from how $\widetilde{K}$ was constructed, there exists $\varphi \in \mathrm{Aut}(\overline{k}/k)$ and $\beta \in K \setminus k$ so that $\alpha = \varphi(\beta)$. This would lead to a contradiction since α and β must be roots of the same minimal polynomial $m(x) \in k[x]$ yet $\beta \in K'$ while $\alpha \notin K'$ so $m(x)$ does not split over K' which means K' is not a splitting field so not Galois.

Exersise 5.5

We have that $\mathbb{F}_{p^n}^*$ is a cyclic group. The reason for this is because by our classification of finite abelian groups

$$\mathbb{F}_{p^n}^* \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \ldots \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1|n_2|\ldots n_k$. However if $k > 1$ then the polynomial $x^{n_2} - x$ would have more than n_2 roots which is not possible. Thus if we let θ be a generator of $\mathbb{F}_{p^n}^*$ we have

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$$

We have that there exists an irreducible polynomial of degree n over $\mathbb{F}_p$ for any $n > 0$ we can construct the splitting field of $x^{p^n} - x$ and use that it is a simple extension to conclude

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\theta) \cong \mathbb{F}_p[x]/(m_\theta(x))$$

where m_θ is the minimal polynomial of θ. We have that m_θ is the desired polynomial:

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \deg(m_\theta)$$

Exersise 5.6

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois since it is the splitting field of the cyclotomic polynomial (which is irreducible and thus seperable)

$$\Phi_n(x)$$

We know that every automorphism $\varphi \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is fully determined by mapping ζ_n to another primitive root of unity. Thus the Galois group is isomorphic to the group of units in $\mathbb{Z}/n\mathbb{Z}$

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$