**Exersise 3.1**

The algebraic closure of $\mathbb{F}_p$ is the infinite vectorspace over $\mathbb{F}_p$

$$K = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$$

Where each $\mathbb{F}_{p^n}$ extends $\mathbb{F}_{p^{n-1}}$ as the splitting field of $x^{p^n} - x$: $\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^3} \cdots \subset \mathbb{F}_{p^n} \ldots$. We know that the algebraic closure must contain the splitting field of $x^{p^n} - x$ and thus each $\mathbb{F}_{p^n}$ is contained in the closure. Therefore the algebraic closure necessarily contains $K$. Conversly every algebraic extension of $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is a finite vectorspace over $\mathbb{F}_p$ and thus letting $n = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ it is the case that $\mathbb{F}(\alpha) \cong \mathbb{F}_{p^n}$ and thus is a subfield of $K$. Thus $K$ contains all algebraic extensions of $\mathbb{F}_p$ which means $K$ contains the algebraic closure.

**Exersise 3.2**

We have that $[\mathbb{F}_p(\sqrt{\alpha}) : \mathbb{F}_p] = [\mathbb{F}_p(\sqrt{\beta}) : \mathbb{F}_p] = 2$. Therefore $|\mathbb{F}_p(\sqrt{\alpha})| = |\mathbb{F}_p(\sqrt{\beta})| = p^2$. As we have established in lecture it is necessarily the case that they are the splitting field of $x^{p^2} - x$ over $\mathbb{F}_p$ and are thus isomorphic to $\mathbb{F}_{p^2}$, so isomorphic to each other.

**Exersise 3.3**

$\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$, and for any $\alpha \in \mathbb{F}_{p^n}$,

$$\alpha^{p^n} - \alpha = F^n(\alpha) - \alpha = 0 \Rightarrow F^n(\alpha) = \alpha \Rightarrow F^n = \mathrm{id}_{\mathbb{F}_{p^n}}$$

Thus $\mathrm{ord}(F)|n$.

If it is the case for $d \geq 1$, $F^d = \mathrm{id}_{\mathbb{F}_{p^n}}$, then for all $\alpha \in \mathbb{F}_{p^n}$, $\alpha^{p^d} = \alpha$ so $\alpha^{p^d} - \alpha = 0$. Since $x^{p^d} - x$ has exactly $p^d$ roots, in order for every element of $\mathbb{F}_{p^n}$ to be a root, it would have to be the case

$$p^n = |\mathbb{F}_{p^n}| \leq p^d \Rightarrow n \leq d$$

Thus $n$ must be the order of $F$

**Exersise 3.4**

As we have established in lecture, every finite field is of the form $\mathbb{F}_{p^n}$ which is the splitting field for the seperable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. Thus since $x^{p^n} - x$ is seperable, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois: $|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$. Since the orbit of $F \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is of size $n$, it must be the case $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathrm{orb}(F)$

**Exersise 3.5**

In the field $\mathbb{F}_{p^m}$ every element is a root of $x^{p^m} - x$. For $n|m$ we will show that any element $\alpha$ in the splitting field of $x^{p^n} - x$ is a root of $x^{p^m} - x$ thus showing that $\mathbb{F}_{p^n}$ is contianed in the splitting field of $x^{p^m} - x$ which is $\mathbb{F}_{p^m}$. Since $n|m$ we have that $p^m = p^n p^n p^n \ldots p^n$ so

$$\alpha^{p^m} = \alpha^{p^n p^n p^n \ldots p^n} = ((\alpha^{p^n})^{p^n} \ldots)^{p^n}$$

Since $\alpha^{p^n} = \alpha$, we get $\alpha^{p^m} = \alpha$ and thus is a root of $x^{p^m} - x$. Thus $\mathbb{F}_{p^n}$ embeds into $\mathbb{F}_{p^m}$. Since $\mathbb{F}_{p^m}$ is still the splitting field of the seperable polynomial $x^{p^m} - x$ over $\mathbb{F}_{p^n}$, it is Galois:

$$[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = |\mathrm{Aut}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})|$$

**Exersise 3.6**

We have that $F$ is not surjective. There is no $f(t) = \frac{p(t)}{q(t)} \in K$ where $F(f) = t$. The reason for this if

$$t = F(f(t)) = \frac{(p(t))^p}{(q(t))^p}$$

Then

$$t(q(t))^p = (p(t))^p \in \mathbb{F}_{p^n}[x]$$

This cannot be the case however since the degree of $(p(t))^p$ is divisible by $p$ while $t(q(t))^p$ is not (it is of the form $kp + 1$)