Exersise 4.1

We have the root $\alpha = \sqrt[4]{-2} = \zeta_8\sqrt[4]{2}$ and every other root is of the form $\zeta_4^n\alpha$ where $\zeta_4 = i, \zeta_8 = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$ are roots of unity. Thus the splitting field is

$$\mathbb{Q}(i, \zeta_8, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$$

We get the equality since $\zeta_8 = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} \in \mathbb{Q}(i, \sqrt[4]{2})$

We have that the minimal polynomial of $\sqrt[4]{2}$ (over both $\mathbb{Q}$ and $\mathbb{Q}(i)$) is

$$x^4 - 2 = (x - \sqrt[4]{2})(x - i\sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2})$$

The reason this is minimal is because it has no roots in $\mathbb{Q}$ and combining any two of the linear factors does not yield a polynomial in $\mathbb{Q}[x]$ since the constant term will be of the form $\pm\sqrt{2}$ or $\pm i\sqrt{2}$.

Letting K be the splitting filed we have that any $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ is fully determined by $\varphi(\sqrt[4]{2})$ and $\varphi(i)$. When fixing i we have that the group of automorphisms is cyclic.

$$\mathrm{Gal}(K/\mathbb{Q}(i)) = C_4$$

Where we have the generator g Defined by $g(\sqrt[4]{2}) = i\sqrt[4]{2}$. Notice that

$$g(\sqrt[4]{2}) = i\sqrt[4]{2}, g^2(\sqrt[4]{2}) = -\sqrt[4]{2}, g^3(\sqrt[4]{2}) = -i\sqrt[4]{2}, g^4(\sqrt[4]{2}) = \sqrt[4]{2}$$

The orbit of g contains all possible automorphisms. Over $\mathbb{Q}$ we can permute the roots of $x^2 + 1$. We have the automorphism f sending $i \to -i$ while fixing $\sqrt[4]{2}$. Notice we have

$$f \circ g = g^3 \circ f, f^2 = \mathrm{id}$$

The first equality comes from evaluating at the roots $f \circ g(\sqrt[4]{2}) = f(i\sqrt[4]{2}) = -i\sqrt[4]{2}$, $f \circ g(i) = f(i) = -i$. Since $\mathrm{Gal}(K/\mathbb{Q})$ is the group generated by f and g we can conclude

$$\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$$

where D_8 is the order 8 dihedral group

Exersise 4.2

Exersise 4.3

If there was an infinite number of roots of unity in K then for each $N > 0$ there must be a n such that $n > N$, and $\zeta_n \in K$ (since there are only be finitely many roots of unity of degree less than N). Thus we have

$$[K : \mathbb{Q}] \geq [\zeta_n : \mathbb{Q}] = \varphi(n)$$

The Euler Phi function is bounded below (this is a commonly known lower bound)

$$\varphi(n) \geq \frac{\sqrt{n}}{\sqrt{2}}$$

Thus we would contradict finiteness of $[K : \mathbb{Q}]$ since it is bounded fromm below by a number that for large choice of N becomes arbitrarily large.

$$[K : \mathbb{Q}] \geq \varphi(n) \geq \frac{\sqrt{n}}{\sqrt{2}} \geq \frac{\sqrt{N}}{\sqrt{2}}$$

Exersise 4.4

We have that $K = \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$ is an extentsion of $\mathbb{Q}$. We have the chain of extentsions

$$\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_{mn})$$

$$\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_{mn})$$

This yields

$$[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : K] = [\mathbb{Q}(\zeta_{nm}) : K] = [\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_m)][\mathbb{Q}(\zeta_m) : K]$$

Thus if we show it is the case that $[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_n)] = \varphi(m)$ and $[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_m)] = \varphi(n)$ then it must be the case that $[\mathbb{Q}(\zeta_m) : K] = \varphi(m)$. From the following fact this means that $K = \mathbb{Q}$:

$$[\mathbb{Q}(\zeta_m) : K][K : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) \Rightarrow [K : \mathbb{Q}] = 1$$

Therefore all we must show is $[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_n)] = \varphi(m)$ (since labeling is arbitrary this will imply $[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}(\zeta_m)] = \varphi(n)$).
We have that

$$\varphi(mn) = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_m)][\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_m)]\varphi(m)$$

Since m and n are relatively prime, we have that $\varphi(mn) = \varphi(m)\varphi(n)$ and thus dividing by $\varphi(m)$on both sides yields the desired result

$$[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_m)] = \varphi(n)$$

Exersise 4.5

We can use strong induction, first establishing a base case:
For $n = 1$ we have

$$\Phi_1(-x) = -x - 1 = -\Phi_2(x)$$

for $n = 3$:

$$\Phi_3(-x) = x^2 - x + 1 = \Phi_6(x)$$

For the inductive step we use the well established identity:

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

We can reorder the product for $2n$ since each divisor of n must be odd:

$$x^{2n} - 1 = \prod_{d|2n} \Phi_d = \prod_{d|n} \Phi_d(x)\Phi_{2d}(x)$$

We also have the factorization $x^{2n}-1 = (x^n-1)(x^n+1)$. Since n is odd, $x^n+1 = -((-x)^n-1)$:

$$= -(x^n - 1)((-x)^n - 1) = -\prod_{d|n} \Phi_d(x) \prod_{d|n} \Phi_d(-x)$$

So we have

$$\prod_{d|n} \Phi_d(x)\Phi_{2d}(x) = -\prod_{d|n} \Phi_d(x) \prod_{d|n} \Phi_d(-x)$$

From our inductive hypothesis, for each $d < n, d \neq 1$ we have $\Phi_d(-x) = \Phi_{2d}(x)$, thus we can divide on both sides

$$\Phi_{2n}(x)\Phi_1(x) \prod_{d|n} \Phi_d(x) \prod_{d|n, 1<d<n} \Phi_d(-x) = -\prod_{d|n} \Phi_d(x) \prod_{d|n} \Phi_d(-x)$$

$$\Phi_{2n}(x)\Phi_1(x) = -\Phi_2(-x)\Phi_n(-x)$$

Since $\Phi_1(x) = -\Phi_2(-x)$ we get our equality

$$\Phi_{2n}(x) = \Phi_n(-x)$$

Exersise 4.6

(a) We have

$$n! = |\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}]$$

If f were reducible, then f can be factored as such $f(x) = g(x)h(x)$ where $\deg(h), \deg(g) \geq 1$. Letting H be the splitting field of h over $\mathbb{Q}$ we have

$$[K : \mathbb{Q}] = [K : H][H : \mathbb{Q}]$$

We know that $[H : \mathbb{Q}] \leq \deg(h)!$ and $[K : H] \leq \deg(g)!$. Since $n = \deg(h) + \deg(g)$ and $\deg(h), \deg(g) \geq 1$, it is the case

$$n! > \deg(h)! \deg(g)! \geq [K : H][H : \mathbb{Q}] = n!$$

Which is a contradiction. Thus f cannot be be factored

(b) Any automorphism $\varphi \in \text{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is fully determined by $\varphi(\alpha)$. If it was the case that φ was not the identity, then it must be the case $\varphi(\alpha) = \beta$ where $\beta \neq \alpha$ is a root of f. Thus $\beta \in \mathbb{Q}(\alpha)$. Then it would be the case that letting $h(x) = (x-\alpha)(x-\beta) \in \mathbb{Q}(\alpha)[x]$, that $h(x)|f(x) \Rightarrow f(x) = h(x)g(x)$. From this we have the following

$$n! = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

We have that $K/\mathbb{Q}(\alpha)$ is the splitting field of g and so $[K : \mathbb{Q}(\alpha)] \leq \deg(g)!$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = n$. Since $\deg(g) = \deg(f) - 2 = n - 2$ we are led to the contradiction

$$n! \leq n \cdot (n-2)!$$

Thus the only possible automorphism is the identity

(c) If $\alpha^n = a \in \mathbb{Q}$ then the minimal polynomial of α would have to be

$$x^n - a$$

So $f(x) = x^n - a$ since f is the minimal polynomial of α.
All other roots of f would be of the form $\alpha\zeta_n^k$ for some k, and this will not yield a Galois group isomorphic to S_n. The Galois group would be the direct product of cycic groups generated by the two automorphisms that send $\alpha \to \alpha\zeta_n$ and $\zeta_n \to \zeta_n^p$ (where p has order $\varphi(n)$ in $(\mathbb{Z}/n)^*$)