Exersise 2.1
We have

$$x^5 + x^2 - x - 1 = (x-1)(x+1)(x^3 + x + 1)$$

The roots are

$$\pm 1, \frac{\alpha}{3^{2/3}} - \frac{1}{3^{1/3}\alpha}, \zeta_3^2 \frac{1}{3^{1/3}\alpha} - \zeta_3 \frac{\alpha}{3^{2/3}}, \zeta_3 \frac{1}{3^{1/3}\alpha} - \zeta_3^2 \frac{\alpha}{3^{2/3}}$$

where $\zeta_3 = \frac{1}{2} + \frac{\sqrt{3}}{2}$ is the third root of unity and

$$\alpha = \sqrt[3]{\frac{\sqrt{93} - 9}{2}}$$

(I found these values using wolfram alpha for the roots of $x^3 + x + 1$, then plugged in the values to verify). From this we get the splitting field is

$$\mathbb{Q}(\alpha, \sqrt[3]{3}, \zeta_3)$$

Since $\sqrt[3]{3} = 2(\zeta_3 - 1/2) \in \mathbb{Q}(\zeta_3)$,

$$= \mathbb{Q}(\alpha, \zeta_3)$$

we have

$$[\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ since the degree of the irreducible polynomial is 3. $\zeta_3 \notin \mathbb{Q}(\alpha)$ since $\mathbb{Q}(\alpha) \subset \mathbb{R}$ while $\zeta_3 \notin \mathbb{R}$, so $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)] \geq 2$. Over $\mathbb{Q}$ the irreducible polynomial of ζ_3 is $x^2 + x + 1$, thus we have $2 = [\mathbb{Q}(\zeta_3) : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)]$, So $[\mathbb{Q}(\zeta_3, \alpha) : \mathbb{Q}(\alpha)] = 2$.
Thus

$$[\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}] = 6$$

Exersise 2.2
For any element $a \in D$, since D is finite dimensional over k (lets say of degree n) the $n+1$ vectors $1, a, a^2 \ldots a^n$ are linearly dependent and thus there exists $k_0, k_1, \ldots k_n \in k$ where

$$k_0 + k_1 a + \ldots k_n a^n = 0$$

Thus a is algebraic over k. Since k is algebraically closed, this means $a \in k$. Thus $D \subseteq k$ so $D = k$

Exersise 2.3

Exersise 2.4

($\Leftarrow$) If every irreducible polynomial in $k[x]$ that has root in K splits over K and K is a finite extention of k, let $\alpha_1, \alpha_2 \dots \alpha_n$ be the basis of K over k. Since each are algebraic, each has corresponding minimal polynomials $p_1, p_2, \dots p_n \in k[x]$. Since $p_1 \dots p_n$ is irreducible they split over K. Thus the polynomial $p = \prod p_i$ splits over K. It is the case that K is the splitting field of p over k. We must show that no smaller field extention $K'|k$ splits p. This is true because if $K' \subsetneq K$ as a vector space of k, then K' has a strict subset of the basis of K which means there is $\alpha_i \notin K'$. Since α_i is a root of p, p does not split over K'.

($\Rightarrow$) If K is the splitting field for f and g is any irreducible polynomial over k with roots $\alpha \in K$ and β, we have that $k(\alpha) \cong k(\beta)$. The isomorphism $\sigma : k(\alpha) \to k(\beta)$ fixes k, and thus $f = \sigma(f)$. From the theorem proved in lecture, letting K' be the splitting field of f over $k(\beta)$, we know that σ induces an isomorphism of field extentions

$$K|k(\alpha) \cong K'|k(\beta)$$

Where $K \cong K'$. Since for both K and K', $k \subset K, K'$ and K, K' and they are isomorphic, they are the splitting field of f over k which is unique so they must be equal. Thus $k(\beta) \subset K$ so $\beta \in K$

Exersise 2.5

We can consider the group structure of multiplication over the units of $\mathbb{F}_p$. By Lagrange's Theorem, for any unit $\alpha \in \mathbb{F}_p$, $\alpha^p = \alpha$, thus α is a root of $x^p - x$. Thus all p elements of $\mathbb{F}_p$ (including 0 since $0^p - 0 = 0$) are roots of $x^p - x$. Since $x^p - x$ can have at most p roots (since polynomials have at most their degree number of roots), there can be no multiple roots since it has p distinct roots.

Exersise 2.6

($\Rightarrow$) suppose $\alpha \neq 0$ is a root of multiplicity ≥ 2. We have that $x - \alpha$ divides $x^n - 1$ which yields

$$x^n - 1 = (x - \alpha)(x^{n-1} + \alpha x^{n-2} + \alpha^2 x^{n-3} + \dots \alpha^{n-1})$$

α must be a root of the second polynomial, which means

$$\alpha^{n-1} + \alpha^{n-1} + \dots \alpha^{n-1} = n\alpha^{n-1} = 0$$

Since $\alpha^n = 1, \alpha^{n-1} = \alpha^{-1} \neq 0$. Thus it must be the case that $n = 0 \Rightarrow p|n$

($\Leftarrow$) If $p|n$, we have

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

1 is a root of multiplicity ≥ 2 since 1 is a root of $x - 1$ and a root of $x^{n-1} + \cdots + x + 1$. This is because plugging in 1 we get a sum of n 1s and since the characterstic divides n, that sum is 0