Question 1

(a) We find the splitting field of $f(x) = x^{11} - 2$ by finding the roots. In particular, notice that we have an immediate root of $\sqrt[11]{2}$, and if we suppose ξ_{11} the 11th root of unity, then we have that the roots of this polynomial will be $\sqrt[11]{2}, \xi_{11}\sqrt[11]{2}, \xi_{11}^2\sqrt[11]{2}, \ldots, \xi_{11}^{10}\sqrt[11]{2}$. So, the splitting field will be $\mathbb{Q}(\sqrt[11]{2}, \xi_{11})$. Notice, $\deg_{\mathbb{Q}}\left(\sqrt[11]{2}\right) = 11$ and $\deg_{\mathbb{Q}}(\xi_{11}) = 10$ since 11 is prime. These two are coprime, and thus by a lemma we proved in the previous assignment,

$$[\mathbb{Q}(\sqrt[11]{2}, \xi_{11}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[11]{2}) : \mathbb{Q}][\mathbb{Q}(\xi_{11}) : \mathbb{Q}] = 11 \cdot 10 = 110\,.$$

(b) We find the splitting field of $f(x) = x^4 - x^2 + 4$ by first finding the roots:

$$f(x) = (x^2+2)^2 - 5x^2 = (x^2 + 2 - \sqrt{5}x)(x^2 + 2 + \sqrt{5})$$

$$f(x) = \left(x - \frac{\sqrt{5} - i\sqrt{3}}{2}\right)\left(x - \frac{\sqrt{5} + i\sqrt{3}}{2}\right)\left(x - \frac{-\sqrt{5} - i\sqrt{3}}{2}\right)\left(x - \frac{-\sqrt{5} + i\sqrt{3}}{2}\right).$$

These aren't nice roots, but we only need to adjoin $\sqrt{5}$ and $i\sqrt{3}$ onto $\mathbb{Q}$ to have the splitting field, that is, the splitting field is $\mathbb{Q}(\sqrt{5}, i\sqrt{3})$. To compute $[\mathbb{Q}(\sqrt{5}, i\sqrt{3}) : \mathbb{Q}]$, we notice

$$\deg_{\mathbb{Q}}(\sqrt{5}) = \deg_{\mathbb{Q}}(x^2 - 5) = 2 \quad \deg_{\mathbb{Q}}(\sqrt{3}) = \deg_{\mathbb{Q}}(x^2 + 3) = 2\,.$$

Since these are not coprime, we can't apply our little trick. Instead, we use the fact that $f(x)$ is irreducible over $\mathbb{Q}$. This would imply that any field extension using this polynomial better have degree atleast 4, and since $f(x)$ will split over $\mathbb{Q}(\sqrt{5}, i\sqrt{3})$, it better be atleast degree 4. However, from last assignment, we also have an inequality that says $[\mathbb{Q}(\sqrt{5}, i\sqrt{3}) : \mathbb{Q}] \leq 4$, and thus we would require that $[\mathbb{Q}(\sqrt{5}, i\sqrt{3}) : \mathbb{Q}] = 4$.

So, to see that $f(x)$ is irreducible, we use the mod-3 irreducibility test. Then,

$$\bar{f}(x) = x^4 - x^2 + 1 \quad \bar{f}(0) = 1, \bar{f}(1) = 1, \bar{f}(2) = 1\,.$$

So, we need to check if this factors into degree 2 irreducible polynomials. The irreducible polynomials of $\mathbb{Z}_3[x]$ are

$$x^2 + 2\,,\; x^2 + 1\,,\; x^2 + x + 2\,,\; x^2 - x + 2\,,\; 2x^2 + x + 1\,,\; 2x^2 - x + 1\,.$$

Immediatly, we see that the polynomials with leading coefficient 2 can only multiply one another since the result better be monic, but the product is $x^4 - x + 1$. Similarly, the polynomials with only an x^2 term can only multiply one another since the result with another polynomial would leave them with an extra x^3 term, and they multiply together to $x^4 - 1$. Finally, the remaining two multiply to $x^4 + 4$. Thus, we have irreducibility, and

$$[\mathbb{Q}(\sqrt{5}, i\sqrt{3}) : \mathbb{Q}] = 4\,.$$

(c) We need to find the roots of the polynomial. Notice,

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

So, the extension we consider will be $\mathbb{Q}(\sqrt[4]{2}, i)$. We know this because $\sqrt{i} = e^{i\frac{\pi}{4}} = \frac{1+i}{\sqrt{2}}$, which is a combination of our extensions. This is clearly the minimal such extension as we need atleast these to get our polynomial to split. We notice that the degree can be obtained from using the fact that this is the extension in which the root $\sqrt[4]{2}$ lives, so this is atleast of order 4 by the fact that the minimal polynomial is $x^4 + 2$ since it is irreducible by 2-Eisenstein.

The minimal polynomial for i is $x^2 + 1$, which is irreducible since it is the first cyclotomic polynomial, $\Phi_1(x) \in \mathbb{Q}$, and is of degree 2. So, at most we expect $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] \leq 8$. From the tower theorem,

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] \leq 8$$
$$\iff [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] \leq 4\,.$$

However, we know that these two roots are independent, since $\sqrt[4]{2}$ is trancendental over $\mathbb{Q}(i)$, and so $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = 4 \implies [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$.

Question 2

(a) (i) Suppose $I = R$. Then units will be in I such as 1, and thus $f(x_f) \,|\, 1$, for some $f(x_f) \in I$. But then $f(x_f)$ is a unit and in F, and thus $f(x) \in F[x]$ would be constant. This is a contradiction, and therefore $I \neq R$.

(ii) Assuming the I and R from before, we now have the field extension of F in the form $K_1 = R/M$, where M is the maximal ideal containing I. Suppose $g(x) \in F[x]$ is some polynomial over F. We can assume it monic, since if it is not $\exists\, u \in F$ such that $ug(x)$ is monic. Further, we suppose that it has no roots over F, since otherwise it will have roots over K_1 simply be the fact that $F \subseteq K_1$. So, we now have the monic polynomial $g(x)$ that has no roots over F. Since it is monic, we better have that $\langle g(x_g) \rangle \subset I \subset M$, for some indeterminant x_g, where $R = F[\dots, x_g, \dots]$. In particular, this immediately tells us that if we consider $g(x) \in K_1[x]$, then we have $g(x_g) \in R/M$ and thus $g(x_g) = 0$, and x_g better be a root of $g(x) \in K_1[x]$. All that remains to show is that $x_g \in K_1$. But this comes for free from the fact that $K_1 = R/M$, and this is exactly all polynomials over all the polynomial indeterminants such that they vanish over their respective indeterminants. Thus, we have shown that all polynomials have a root at their respective indeterminant over K_1.

(iii) Suppose $f(x) \in K[x]$, then $\exists\, K_n$, for smallest n, such that $f(x) \in K_n[x]$. By (ii), we have that $f(x)$ has a root in $K_{n+1} \subset K$, and so K is algebraicly closed. Further, $K_0 = F \subset K$, and thus contains F by construction (technically an isomorphic copy).

(b) We see that the closure of $\mathbb{Q}$ cannot be $\mathbb{C}$ since $\mathbb{C}/\mathbb{Q}$ is not algebraic. In particular, notice that we have trancendental numbers, such as $\pi \in \mathbb{C}$, but there is no such polynomial over $\mathbb{Q}[x]$ where π is the root.

Question 3

(a) ($\implies$) Suppose $f(x)$ has a multiple root in some extension, say $f(x) = (x-\alpha)^n q(x) \in K[x]$, where K/F, $q(x) \in K[x]$. Notice,

$$f'(x) = n(x-\alpha)^{n-1}q(x) + (x-\alpha)^n q'(x)$$

where $n > 1$ since it is a multiple root. So, clearly $f(x)$ and $f'(x)$ share a common root, and since they share a common root, we can suppose $\exists\, g(x) \in F[x]$ minimal polynomial of α, and thus we better have that $g(x) \,|\, f(x)$ and $g(x) \,|\, f'(x)$, and since $\deg_F(g(x)) > 1$, we have a positive degree factor between the two.

($\impliedby$) Suppose $f(x)$ and $f'(x)$ share a common factor of positive degree, call it $g(x)$, with $\deg(g(x)) \geq 1$. Then, $\exists h(x) \in F[x]$ such that $f(x) = g(x)h(x)$, and more importantly,

$$f'(x) = g'(x)h(x) + g(x)h'(x)\,.$$

Clearly $g(x) \,|\, g(x)h'(x)$, and thus $g(x) \,|\, g'(x)h(x)$, but since $\deg_F(g'(x)) < \deg_F(g(x))$ and since we can assume $g(x)$ irreducible (since if it is not, we can reduce it until it is and then rename), we must have that $g(x) \,|h(x)$, and thus, $\exists\, q(x) \in F[x]$ such that $h(x) = g(x)q(x)$. Finally, if we suppose K the splitting field of $f(x)$, then

$$f(x) = g(x)h(x) = (g(x))^2 q(x) \to (\dots(x-\alpha_i)\dots)^2 \dots (x-\beta_i)\dots = f(x) \in K[x]\,.$$

Clearly we have atleast one multiple root.

(b) Notice that $f(x) = x^6 - 2$ and so $f'(x) = 6x^5 = 0 \in \mathbb{Z}_3[x]$. Ofcourse, since $f'(x) = 0$, we better have that $f(x)$ and $f'(x)$ satisfy our lemma (they share a common divisor in $F[x]$ of positive degree) and hence $f(x) = x^6 - 2$ will most definitely have a multiple root in some field extension.

(c) ($\implies$) By the contrapostive, suppose that $f'(x) = 0$, then clearly we have a common factor between $f(x)$ and $f'(x)$ of $f(x)$, since $f(x)$ is irreducible. By the previous lemma, $f(x)$ will have atleast one multiple root in a field extension, and thus is not seperable.

($\impliedby$) Suppose $f'(x) \neq 0$, well then since $f(x)$ is irreducible they will not share any common factors of positive degree, and by **(a)** we will know that $f(x)$ is seperable.

(d) If F is characteristic zero, then for any polynomial $f(x)$, we must have that $f'(x) = 0 \iff f(x) = c \in F$. That is, in characterstic zero fields polynomials have vanishing derivatives when they are constant. However, all irreducible polynomials have postive degree, hence no irreducible polynomial will have vanishing derivatives, and thus from the previous lemma, all irreducible polynomials will be seperable.

Question 4

(a) Suppose $p \nmid n$, then since $f(x) = x^n - c$, we have that $f'(x) = nx^{n-1}$ is non-zero in $\mathbb{Z}_p[x]$. Further, notice that all of the roots of $f'(x)$ are zeros and all the roots of $f(x)$ are "nth roots" of c. So, since $c \neq 0$, $f(x)$ and $f'(x)$ will not share any positive degree factors, since if they did, that would imply they share roots, which they clearly do not. Thus, by the lemma before, since the polynomial and it's derivative do not share a common factor of positive degree, we expect $f(x) = x^n - c$ to be separable, and hence will have n distinct roots.

(b) By Fermat's little theorem, we can see that $c \equiv c^p \in \mathbb{Z}_p$, so

$$f(x) = x^n - c = x^n - c^p$$

but since $p \,|\, n$, where we let $p^k \cdot m = n$ for some $m \in \mathbb{Z}$ and $p \nmid m$. By freshman's dream,

$$f(x) = x^{p^k m} - c^p = (x^m - c)^{p^k}$$

and since $p \nmid m$ by construction, $x^m - c$ from our previous lemma gives us m distinct roots which are repeated p^k times. So, the number of distinct roots for this polynomial in the extension will be the factors of n left after removing all possible powers of p.