Section 6.3

1. (Problem 2c) Find a splitting field E of $f(x) = x^4 - 6x^2 - 7$ over $\mathbf{Q}$ and compute $[E : \mathbf{Q}]$.

> **Solution:** Notice $f(x) = (x^2 - 7)(x^2 + 1)$. Thus the roots of f in $\mathbf{C}$ are $\pm i$ and $\pm\sqrt{7}$, and we see a splitting field for f over $\mathbf{Q}$, given as a subfield of $\mathbf{C}$, is $E = \mathbf{Q}(\sqrt{7}, i)$. Of course $[\mathbf{Q}(\sqrt{7}) : \mathbf{Q}] = 2$, for instance the minimal polynomial of $\sqrt{7}$ is $x^2 - 7$ (irreducible over $\mathbf{Q}$ by Eisenstein). Next we will compute $[E : \mathbf{Q}(\sqrt{7})]$, but notice that $E = \mathbf{Q}(\sqrt{7}, i) = \big(\mathbf{Q}(\sqrt{7})\big)(i)$, so we should just compute the degree of the minimal polynomial of i over $\mathbf{Q}(\sqrt{7})$. But this minimal polynomial must divide $x^2 + 1$, so the degree of the minimal polynomial is either 1 or 2, so $[E : \mathbf{Q}(\sqrt{7})]$ is 1 or 2, but if the degree is 1 then $i \in \mathbf{Q}(\sqrt{7})$ which is impossible because $i \notin \mathbf{R}$. Thus we see $[E : \mathbf{Q}(\sqrt{7})] = 2$ and then by the tower law we see $[E : \mathbf{Q}] = 4$.

2. (Problem 11) Let $E/L/F$ be fields and $f \in F[x]$. Prove if E is a splitting field for f over F then E is also a splitting field for f over L.

> **Solution:** This is an exercise in being careful about definitions; by definition, because E is a splitting field for f over F, we have a factorization $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$ in $E[x]$, where $a \in F$ and $\alpha_i \in E$, and an equality $E = F(\alpha_1, \ldots, \alpha_n)$.
>
> We need to know the same holds when we replace F by L. Of course we still have $f \in L[x]$ and we have $a \in L$ in the factorization above. The only thing to prove is $E = L(\alpha_1, \ldots, \alpha_n)$. of course $E = F(\alpha_1, \ldots, \alpha_n) \subseteq L(\alpha_1, \ldots, \alpha_n)$, and on the other hand, because $\alpha_i \in E$ for each i and $L \subseteq E$ we find $L(\alpha_1, \ldots, \alpha_n) \subseteq E$, which concludes the proof.

3. (Problem 2) Construct a field of order 27 and find a primitive element.

Solution: We need to construct a field extension of $\mathbf{F}_3$ (where we recall $\mathbf{F}_p$ is just alternative notation for $\mathbf{Z}_p$) of degree 3, so it is enough to find an irreducible polynomial $f \in \mathbf{F}_3[x]$ of degree 3. But degree 3 polynomials over a field are irreducible as long as they have no roots, so we just need some f with no roots, and one can easily check $f(x) = x^3 - x - 1$ works. So we take $E = \mathbf{F}_3[x]/\langle x^3 - x - 1\rangle$.

Now we need to find a primitive element, i.e. an element $\alpha \in E$ which generates E^* as a multiplicative group. Therefore we should have $o(\alpha) = |E^*| = 26$. If we have any such α, then $(\alpha^{13})^2 = 1$ so $\alpha^{13} = \pm 1$, so if we are to have $o(\alpha) = 26$ then we should have $\alpha^{13} = -1$. Conversely, if $\alpha \neq \pm 1$ and $\alpha^{13} = -1$, then using the fact that $26 = 2{\cdot}13$ and $o(alpha) \,|\, 26$, one can deduce that we must have $o(\alpha) = 26$. So we need to find an element $\alpha \in E$ such that $\alpha \neq \pm 1$ and $\alpha^{13} = -1$.

In $E = \mathbf{F}_3[x]/\langle x^3 - x - 1\rangle$, write $\overline{g} = g + \langle x^3 - x - 1\rangle$ for the equivalence class of $g \in \mathbf{F}_3[x]$. Notice then that $\overline{x}^3 = \overline{x} + 1$. From this one can calculate (recalling throughout the calculation that we are in characteristic 3)

$$\begin{aligned}
\overline{x}^{13} &= \overline{x}(\overline{x}^3)^4 = \overline{x}(\overline{x}+1)^4 \\
&= \overline{x}(\overline{x}^4 + 4\overline{x}^3 + 6\overline{x}^2 + 4\overline{x} + 1) \\
&= \cdots \\
&= \overline{x}^3 + 2\overline{x} = \overline{x}^3 - x \\
&= 1.
\end{aligned}$$

So $\overline{x}$ is not the element we want! But it gets us close; notice from $\overline{x}^{13} = 1$ we deduce $(-\overline{x})^{13} = -1$, so because $-\overline{x} \neq \pm 1$ we see $-\overline{x}$ gives us a primitive element.

4. (Problem 8) Find $[\mathrm{GF}(p^n) : \mathrm{GF}(p^m)]$ where $m \,|\, n$.

Solution: Recall if V is a d-dimensional vector space over a field F, say with basis $\{v_1, \dots, v_d\}$, then there is an isomorphism $F^d \to V$ by sending $(a_1, \dots, a_n) \mapsto a_1 v_1 + \cdots + a_d v_d$. [If you are not familiar with this fact, try to prove it yourself! Injectivity will correspond to linear independence of $v_1, \dots, v_d$, and surjectivity will correspond to the fact that they span.]

In the case F is a finite field, we deduce that $|V| = |F|^d$. Therefore, in the case $V = \mathrm{GF}(p^n)$ and $F = \mathrm{GF}(p^m)$ where $m \,|\, n$, we see that

$$p^n = |\,\mathrm{GF}(p^n)| = |\,\mathrm{GF}(p^m)|^d = (p^m)^d = p^{md},$$

and therefore $n = md$, so $[\mathrm{GF}(p^n) : \mathrm{GF}(p^m)] = d = n/m$.