Homework 7.

1. i) If $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$,

then WLOG we can assume $n \geq m$, and by writing

$b_{m+1} = b_{m+2} = \dots = b_n = 0$ we can re-write

$g(x) = \sum_{j=0}^{n} b_j x^j$. Then

$$D(f(x) + g(x)) = D\left(\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{n} b_j x^j\right)$$

$$= D\left(\sum_{i=0}^{n} (a_i + b_i) x^i\right)$$

$$= \sum_{i=1}^{n} i \cdot (a_i + b_i) x^{i-1}$$

$$= \sum_{i=1}^{n} i a_i x^{i-1} + \sum_{j=1}^{n} j b_j x^{j-1}$$ and since $b_j = 0$ for $j \geq m+1$,

$$= \sum_{i=1}^{n} i a_i x^{i-1} + \sum_{j=1}^{m} j b_j x^{j-1}$$

$$= D\left(\sum_{i=0}^{n} a_i x^i\right) + D\left(\sum_{j=0}^{m} b_j x^j\right)$$

$$= D(f(x)) + D(g(x)).$$

ii) $$D(f(x)g(x)) = D\left(\sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j x^j\right)$$

$$= D\left(\sum_{i=0}^{m+n}\left(\sum_{k=0}^{i} a_k b_{i-k}\right)x^i\right)$$

$$= \sum_{i=1}^{m+n} i\left(\sum_{k=0}^{i} a_k b_{i-k}\right)x^{i-1}$$

$$= \sum_{i=0}^{n+m-1}(i+1)\left(\sum_{k=0}^{i+1} a_k b_{i+1-k}\right)x^i$$

$$= \sum_{i=0}^{n+m-1}\cancel{(i+1)}\left(\sum_{k=0}^{i+1}(k+i+1-k)a_k b_{i+1-k}\right)x^i$$

$$= \sum_{i=0}^{n+m-1}\left(\left(\sum_{k=0}^{i+1} k a_k b_{i+1-k}\right)+\left(\sum_{k=0}^{i+1}(i+1-k)a_k b_{i+1-k}\right)\right)x^i$$

no nonzero terms are dropped here.

$$= \sum_{i=0}^{n+m-1}\left(\sum_{k=1}^{i+1} k a_k b_{i+1-k}\right)x^i + \sum_{i=0}^{n+m-1}\left(\sum_{k=0}^{i}(i+1-k)a_k b_{i+1-k}\right)x^i$$

$$= \sum_{i=1}^{n} i a_i x^{i-1}\cdot\sum_{j=0}^{m} b_j x^j + \sum_{i=0}^{n} a_i x^i \sum_{j=1}^{m} j b_j x^{j-1}$$

$$= D(f(x))\,g(x) + f(x)\,D(g(x))$$

iii) α is a root of $f(x)$ with multiplicity $m>1$

$\iff$

$(x-\alpha)^m \mid f(x)$

$\iff$ $f(x) = (x-\alpha)^m g(x)$ for some $g(x)$

$$\iff D(f) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m D(g(x))$$

$$= (x-\alpha)^{m-1}\big(m g(x) + (x-\alpha) D(g(x))\big)$$

so if α is a root of $f(x)$ with multiplicity m, then it is a root of $D(f(x))$ with multiplicity $m-1$, and the converse also holds (note: because we have m showing up as a coefficient, it's important that the field F have characteristic 0)

iv. Let F be a field with $\mathrm{char}(F)=0$ and Let $F \subseteq E$ be a finite extension. For any $\alpha \in E$, Let $f(x)$ be the minimal polynomial of α over F. If α is a root of $f(x)$ with multiplicity $m>1$, then α is also a root of $D(f(x))$ $\in F[x]$, which has degree strictly smaller than the degree of $f(x)$, a contradiction. So it must be that $m=1$, hence E is separable over F.

2. Using the proof of the primitive element theorem, $F(\alpha, \beta)$ is equal to $F(\alpha + \gamma\beta)$, as long as $\gamma \in F$, $\gamma \neq \dfrac{\alpha_i - \alpha}{\beta - \beta_j}$ where α_i, β_j are any conjugates of α, β $(\beta_j \neq \beta)$.

i. we need $\sqrt{2} + \gamma\sqrt{5}$, where $\gamma \neq \dfrac{0}{2\sqrt{5}}, \dfrac{2\sqrt{2}}{2\sqrt{5}}$.

so $\gamma = 1$ works, and

$$\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{5}).$$

ii we need $\gamma \neq \dfrac{2i}{\sqrt[3]{2} - w \cdot \sqrt[3]{2}}, \dfrac{2i}{\sqrt[3]{2} - w^2 \cdot \sqrt[3]{2}}, 0.$

where $w = \dfrac{-1 + i\sqrt{3}}{2}$. again, $\gamma = 1$ works, and

$$\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(i + \sqrt[3]{2}).$$

iii Need $\gamma \neq \dfrac{a}{b}$,

where $a = 0, \sqrt[4]{2} - (-\sqrt[4]{2}), \sqrt[4]{2} - i\sqrt[4]{2}, \sqrt[4]{2} - (-i\sqrt[4]{2})$

and $b = \sqrt[6]{2} - \zeta\sqrt[6]{2}, \sqrt[6]{2} - \zeta^2\sqrt[6]{2}, \sqrt[6]{2} - \zeta^3\sqrt[6]{2}$

$\sqrt[6]{2} - \zeta^4\sqrt[6]{2}, \sqrt[6]{2} - \zeta^5\sqrt[6]{2}$, where ζ is a 6^{th} root of 1.

Again, 1 works, so

$$\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2}) = \mathbb{Q}(\sqrt[4]{2} + \sqrt[6]{2}).$$

3. i. True:

If F is algebraically closed, then any finite extension $F \leq E$ is also algebraic, and since F has no proper algebraic extensions, it follows that $E = F$

For any $\alpha \in F$, its min. poly in $F[x]$ is $x - \alpha$, of which α is a root with multiplicity 1. so $E = F$ is separable over F.

ii False: $\mathbb{Q}(\sqrt[3]{2})$ is finite (deg 3) and separable ($\mathbb{Q}$ is perfect), but any automorphism of $\mathbb{Q}(\sqrt[3]{2})$ fixing $\mathbb{Q}$ must send $\sqrt[3]{2}$ to one of its conjugates. But $\omega \cdot \sqrt[3]{2}$ and $\omega^2 \cdot \sqrt[3]{2}$ aren't in the field. So there's only 1 (not 3) elements of $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$

iii) This is true consider a finite extension $E \subseteq L$.

Then since $F \subseteq L$ is finite, L is separable over F. By theorem 51.9, L is separable over E. so E is perfect.

4. i. Since $\deg f(x) = 3$, f is reducible $\iff$ f has a linear factor $\iff$ f has a root in $\mathbb{Z}/2\mathbb{Z}$. But we can just check: $f(1) = 1+1+1 \equiv 1 \bmod 2$

$f(0) = 0+0+1 \equiv 1 \bmod 2$.

and so f has no roots in $\mathbb{Z}/2\mathbb{Z}$. $\begin{cases} \alpha^3 = \alpha+1 \\ \alpha^4 = \alpha^2+\alpha \end{cases}$

ii	0	1	α	$\alpha+1$	α^2+1	$\alpha^2+\alpha$	α^2	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2+1	$\alpha^2+\alpha$	α^2	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	1	$\alpha^2+\alpha+1$	$\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	1	$\alpha^2+\alpha+1$	α
α^2+1	0	α^2+1	1	α^2	$\alpha^2+\alpha+1$	$\alpha+1$	α	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	$\alpha+1$	α	α^2+1	α^2
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	α	α^2+1	$\alpha^2+\alpha$	1
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	$\alpha^2+\alpha$	α^2	1	$\alpha+1$

iii) Plug in the elements of $F(\alpha)$ to $f(x)$. we see that:

$$f(0) = 1$$
$$f(1) = 1$$
$$f(\alpha) = 0$$
$$f(\alpha+1) = \alpha^2 + \alpha$$
$$f(\alpha^2+1) = \alpha$$
$$f(\alpha^2+\alpha) = 0$$
$$f(\alpha^2) = 0$$
$$f(\alpha^2+\alpha+1) = \alpha^2.$$

So the conjugates of α are $\alpha^2+\alpha$ and α^2.

iv) Since $F(\alpha)$ is separable (finite fields are perfect) and a splitting field by iii, we know

$$|G(F(\alpha)/F)| = \{F(\alpha):F\} = [F(\alpha):F] = 3.$$

The auts are determined by

$$\sigma_1(\alpha) = \alpha$$
$$\sigma_2(\alpha) = \alpha^2$$
$$\alpha_3(\alpha) = \alpha^2 + \alpha.$$

Note that $\sigma_2 \circ \sigma_2 = \sigma_3$, $\sigma_3 \circ \sigma_3 = \sigma_2$,

and $\sigma_2 \circ \sigma_3 = \sigma_3 \circ \sigma_2 = \sigma_1$ = identity elt.

so the mult table is

	σ_1	σ_2	σ_3
σ_1	σ_1	σ_2	σ_3
σ_2	σ_2	σ_3	σ_1
σ_3	σ_3	σ_1	σ_2

this is a cyclic group of order 3.