Exercises from Dummit and Foote Chapter 13 on Field Theory

Wesley Basener

July 22, 2025

Problem 1.1. Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.

Proof. The polynomial $p(x)$ is monic and all non leading terms are divisible by 3 with the constant term not divisible by 3^2. So, by Eisenstein's criterion, the polynomial is irreducible.

By the Euclidean property, there are polynomials $a(x)$ and $b(x)$ such that

$$a(x)(1 + x) + b(x)(x^3 + 9x + 6) = 1$$

Mapping this polynomial to $Q(\theta)$ yields,

$$a(\theta)(1 + \theta) = 1$$

So $a(\theta)$ is the inverse of $(1 + \theta)$.

We can find $a(\theta)$ with the Euclidean algorithm (D&F p275). Doing so gives us

$$(x^3 + 9x + 6) = (x + 1)(x^2 - x + 10) - 4$$

Hence, the inverse of $\theta + 1$ is $\frac{1}{4}(\theta^2 - \theta + 10) = \frac{1}{4}\theta^2 - \frac{1}{4}\theta + \frac{5}{2}$. This can be verified with

$$(\theta + 1)(\frac{1}{4}\theta^2 - \frac{1}{4}\theta + \frac{5}{2}) = \frac{1}{4}(\theta^3 - 9\theta + 10) = \frac{1}{4}(\theta^3 + 9\theta + 6) + 1 = 1$$

□

Problem 1.2. Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let θ be a root. Compute $(1 + \theta)(1 + \theta + \theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

Proof. This polynomial is again irreducible by Eisenstein. Multiplying out the given product yields

$$(1 + \theta)(1 + \theta + \theta^2) = 1 + 2\theta + 2\theta^2 + \theta^3$$

Dividing by $\theta^3 + \theta + 1$ yields a remainder of $2\theta^2 + \theta$. //TODO □

Problem 1.3. Show that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$.

Proof. The polynomial is congruent to 1 mod 2 whenever it is evaluated at 1 and 0. Hence, it has no roots in $\mathbb{F}_2$ and is irreducible there.

We immediately have that $\theta^3 = \theta + 1$. We can also see that $\theta = \theta^3 + 1$ so $\theta^2 = \theta^6 + 1$. Dividing the base polynomial by this renders θ^2 as a remainder, so their is no reduced form of θ^2. θ is obviously itself and $\theta^0 = 1$.

For θ^n where $n > 3$, we can factor n into a sum of 3s and some b equal to either 1 or 2 as $n = 3a + b$ yielding $\theta^n = (\theta)^{3a} \cdot \theta^b = (\theta + 1)^a \cdot \theta^b$. Repeating the process for a and factoring when needed will eventually terminate with a polynomial of degree less than 3. □

Problem 1.5. Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[x]$. Prove that α is an integer.

Proof. Let $a, b \in \mathbb{Z}$ be such that $\frac{a}{b} = \alpha$ is fully reduced. By the rational roots theorem, b divides the leading term of the polynomial, which is 1. So, b is either 1 or -1. In either case, α is an integer. $\square$

Problem 1.6. Show that if α is a root of $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, then $a_n\alpha$ is a root of $x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + ... + a_n^{n-2}a_1 x + a_n^{n-1}a_0$.

Proof. Evaluating the later polynomial yields

$$a_n^n\alpha^n + a_n^{n-1}a_{n-1}\alpha^{n-1} + a_n^{n-1}a_{n-2}\alpha^{n-2} + ... + a_n^{n-1}a_1\alpha + a_n^{n-1}a_0 = a_n^{n-1}(a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0)$$

Which is just a_n^{n-1} times the original polynomial evaluated at its root. Thus, $a_n\alpha$ is a root of the given polynomial. $\square$

Problem 1.7. Prove that $x^3 - nx + 2$ is irreducible for $n \neq -1, 3, 5$.

Proof. Suppose it is reducible, then we can rewrite the polynomial as $x^3 - nx + 2 = (x-\theta)(x^2+ax+b)$ for some root θ. By Gauss's lemma, we can assume a, b, and θ are integers. From this, we can infer that $a = \theta$, which allows us to rewrite the equation as $(x-a)(x^2+ax+b)$. We can further infer that $ab = -2$ and $a^2 - b = n$. Since a and b are integers, the only options for their values are $(a = 1, b = -2), (a = -1, b = 2), (a = 2, b = -1)$, and $(a = -2, b = 1)$. These result in n being equal to $-1, -1, 5$, and 3 respectively. Hence, if n is not one of these options, the polynomial is irreducible. $\square$

Problem 2.1. Let $\mathbb{F}$ be a finite field of characteristic p. Prove that $\mathbb{F} = p^n$ for some positive integer n.

Proof. The field $\mathbb{F}$ is an extension of its prime subfield $(1_\mathbb{F})$. By theorem 17, $\mathbb{F}$ being finite implies that it is a extended from $1_\mathbb{F}$ by a finite number or elements $\alpha_1, \alpha_2, ..., \alpha_i$. Each element has finite dimension $k_1, k_2, ..., k_j$. Hence, by lemma 16 and theorem 14, the field has degree $n = k_1 k_2 ... k_j$, and any element can be represented as a linear sum $a_1\beta_1 + a_2\beta_2 + ... + a_n\beta_n$, with $a_1, ..., a_n \in (1_\mathbb{F})$ and each β_l being powers of roots of polynomials with solutions $\alpha_1, ..., \alpha_i$. Since their are p choices for each a_l, it is easy to see that there are p^n unique choices for any element in $\mathbb{F}$. $\square$

Problem 2.2. Let $g(x) = x^2 + x - 1$ and let $h(x) = x^3 - x + 1$. Obtain fields of $4, 8, 9$, and 27 elements by adjoining a root of $f(x)$ to the field F where $f(x) = g(x)$ or $h(x)$ and $F = \mathbb{F}_2$ or $\mathbb{F}_3$. Write down the multiplication tables for the fields with 4 and 9 elements and show that the nonzero elements form a cyclic group.

Proof. By proposition 11, the fields $\mathbb{F}_2/(g(x)), \mathbb{F}_2/(h(x)), \mathbb{F}_3/(g(x))$, and $\mathbb{F}_3/(h(x))$ are of order $4, 8, 9$, and 27 respectively.

Letting α be a root for $g(x)$, the multiplication tables of the first and third fields are

	1	α	$1+\alpha$
1	1	α	$1+\alpha$
α	α	$1+\alpha$	1
$1+\alpha$	$1+\alpha$	1	α

	1	2	α	2α	$1+\alpha$	$2+\alpha$	$1+2\alpha$	$2+2\alpha$
1	1	2	α	2α	$1+\alpha$	$2+\alpha$	$1+2\alpha$	$2+2\alpha$
2	2	1	2α	α	$2+2\alpha$	$1+2\alpha$	$2+\alpha$	$1+\alpha$
α	α	2α	$1+\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$	7	8
2α	2α	1	3	4	5	6	7	8
$1+\alpha$	$1+\alpha$	1	3	4	5	6	7	8
$2+\alpha$	$2+\alpha$	1	3	4	5	6	7	8
$1+2\alpha$	$1+2\alpha$	1	3	4	5	6	7	8
$2+2\alpha$	$2+2\alpha$	1	3	4	5	6	7	8

$\square$

Problem 2.3. Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.

Proof. The minimal polynomial is the irreducible monic polynomial of minimal degree with $1+i$ as a root. Since there is obviously no degree 1 polynomial with such a root, we start by solving the quadratic equation for $1+i$

$$(1+i)^2 + b(1+i) + c = 0 \rightarrow 2i + bi + b + c = 0$$

The equation is solved by setting $b = -2$ and $c = 2$. Hence, the minimal polynomial is $x^2 - 2x + 2x$ $\square$

Problem 2.5. Let $F = \mathbb{Q}(i)$. Prove that $x^3 - 2$ and $x^3 - 3$ are irreducible over F.

Proof. Both of these follow from Eisenstein's criterion, since 2 and 3 are not squares. $\square$

Problem 2.7. Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ [one inclusion is obvious, for the other consider $(\sqrt{2}+\sqrt{3})^2$ etc.]. Conclude that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$.

Proof. Since any element of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ contains a rational number, $\sqrt{2}$, $\sqrt{3}$, it is obviously a s subset of the field generated by these elements, namely $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ Thus, we have $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

For the other inclusion, consider $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$. Hence, subtracting this from $11(\sqrt{2}+\sqrt{3})$ yields $2\sqrt{3}$. From there, it is obvious that $\sqrt{2}$ and $\sqrt{3}$ are in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

By theorem 14, we have $4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}]$.

To find the minimal polynomial, we first note that we are looking for a fourth degree term. Raising $(\sqrt{2}+\sqrt{3})$ to the fourth power gives us $49 + 20\sqrt{6}$. Raising it to the second gives $5 + 2\sqrt{6}$. So, to cancel the $\sqrt{6}$ out, we set the x^4 coeficient to 1 and x^2's coefficient to -10. Setting the constant to 1 leaves us with

$$(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 0$$

Hence, the minimal polynomial for this term is $x^4 - 10x^2 + 1$. $\square$

Problem 2.9. Let F be a field of characteristic $\neq 2$. Let a, b be elements of the field F with b not a square in F. Prove that a necessary and sufficient condition for $\sqrt{a+\sqrt{b}} = \sqrt{m} + \sqrt{n}$ for some m and n in F is that $a^2 - b$ is a square in F. Use this to determine when the field $\mathbb{Q}(\sqrt{a+\sqrt{b}})(a, b \in \mathbb{Q})$ is biquadratic over $\mathbb{Q}$.

Proof. The term $\sqrt{a+\sqrt{b}}$ is a root of the polynomial $x^4 - 2ax^2 - b + a^2$.

First, suppose $\sqrt{m} + \sqrt{n} = \sqrt{a+\sqrt{b}}$. Then, $\sqrt{m} + \sqrt{n}$ is a root of the polynomial and the term $(\sqrt{m}+\sqrt{n})^4 + 2a(\sqrt{m}+\sqrt{n})^2$ must be in $\mathbb{Q}$. So $2a$ must be such that the roots in the following expression cancel.

$$4\sqrt{nm^3} + 4\sqrt{nm^3} + m^2 + n^2 + 6nm + 2a(n + \sqrt{nm} + m)$$

To do this, we solve for a in the equation $2a(2\sqrt{nm}) = -4\sqrt{nm^3} - 4\sqrt{mn^3}$. The solution is of course $m + n = a$. Plugging this result in for a in the previous equation yields

$$4\sqrt{nm^3} + 4\sqrt{nm^3} + m^2 + n^2 + 6nm + 2a(n + \sqrt{nm} + m) = -m^2 + 2mn - n^2 = -(m-n)^2$$

Ultimately, we have

$$-(m-n)^2 + a^2 - b = 0$$

whenever $\sqrt{m} + \sqrt{m} = \sqrt{a+\sqrt{b}}$. Hence, $a^2 - b$ is a square.

Now suppose that $a^2 - b$ is a square. Then, let $m = \frac{2a-1}{2}$ and $n = \frac{1}{2}$. We have $\square$

Problem 2.11. **(a)** Let $\sqrt{3+4i}$ denote the square root of the complex number $3+4i$ that lies in the first quadrant and let ,$\sqrt{3-4i}$ denote the square root of $3-4i$ that lies in the fourth quadrant. Prove that $[\mathbb{Q}(\sqrt{3+4i} + \sqrt{3-4i}) : \mathbb{Q}] = 1$.

(b) Determine the degree of the extension $\mathbb{Q}(\sqrt{1+\sqrt{-3}} + \sqrt{1-\sqrt{-3}})$ over $\mathbb{Q}$.

Proof. (a) This is the same as proving $\sqrt{3+4i} + \sqrt{3-4i}$ is a rational number. Using Euler's identity

$$\sqrt{3+4i} + \sqrt{3-4i}$$
$$=$$
$$\sqrt{5}(\cos(\arctan(\frac{4}{3})) + i\sin(\arctan(\frac{4}{3})))^{\frac{1}{2}} + \sqrt{5}(\cos(\arctan(\frac{4}{3})) + i\sin(\arctan(\frac{4}{3})))^{\frac{1}{2}}$$
$$=$$
$$2\sqrt{5}\cos(\frac{1}{2}\arctan(\frac{4}{3}))) = \sqrt{20}\cos(\frac{1}{2}\arctan(\frac{4}{3})))$$

Next, we factor the trigonometric functions with the identies $\cos(\frac{\theta}{2}) = \pm\sqrt{\frac{1+\cos(\theta)}{2}}$ and $\cos(\arctan(\theta)) = \frac{1}{\sqrt{1+\theta^2}}$.

$$\sqrt{20}(\cos(\frac{1}{2}\arctan(\frac{4}{3})) = \pm\sqrt{20}\sqrt{\frac{1+\cos(\arctan(\frac{4}{3}))}{2}}$$
$$=$$
$$\pm\sqrt{20}\sqrt{\frac{1+\frac{1}{1+(\frac{4}{3})^2}}{2}} = \pm\sqrt{10+\frac{90}{25}}$$
$$=$$
$$\pm\sqrt{\frac{340}{25}} = \pm\sqrt{16} = \pm 4$$

Hence, $\mathbb{Q}(\sqrt{1+\sqrt{-3}} + \sqrt{1-\sqrt{-3}}) \cong \mathbb{Q}$ and the degree of the extension is 1. $\square$

(b). We work in a similar manner to reduce the expression. By Euler's identity we have

$$\sqrt{1+\sqrt{-3}} + \sqrt{1-\sqrt{-3}}$$
$$=$$
$$\sqrt{2}(\cos(\arctan(\sqrt{3})) + i\sin(\arctan(\sqrt{3})))^{\frac{1}{2}} + \sqrt{2}(\cos(\arctan(\sqrt{3})) - i\sin(\arctan(\sqrt{3})))^{\frac{1}{2}} = \sqrt{2}(\cos(\frac{1}{2}\arctan(\sqrt{3})) + i\sin(\frac{1}{2}\text{ar}$$
$$=$$
$$2\sqrt{2}\cos(\frac{1}{2}\arctan(\sqrt{3}))$$

Using the same identities as before,

$$= 2\sqrt{2}\sqrt{\frac{1+\frac{1}{\sqrt{1+\sqrt{3}^2}}}{2}} = \sqrt{4+\frac{4}{\sqrt{4}}} = \sqrt{6}$$

Hence, this extension is obviously of degree 2. $\square$

Problem 1.13. Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ where $\alpha_i^2 \in Q$ for $i = 1, 2, ..., n$. Prove that $\sqrt[3]{2} \notin F$.

Proof. Since each α_i^2 is in $\mathbb{Q}$, $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = 2$ for each i. So the degree of $\mathbb{Q}(\alpha_1)$ will be 1 or 2. The degree of $\mathbb{Q}(\alpha_1, \alpha_2)\mathbb{Q}(\alpha_1)(\alpha_2)$ will either be $1, 2$, or $2 \cdot 2$. By induction, the degree of $F = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ will be 2^i for some $1 \leq i \leq n$. Hence, the degree of F is not a divisible by 3.

By corollary 15, if $\mathbb{Q}(\sqrt[3]{2})$ is in F, then the degree of $\mathbb{Q}(\sqrt[3]{2})$ must divide $[F : Q] = 2$. However, the degree of $\mathbb{Q}(\sqrt[3]{2})$ is 3. Therefore, $\sqrt[3]{2}$ it is not contained in F. $\square$

Problem 1.15. A field F is said to be formally real if -1 is not expressible as a sum of squares in F. Let F be a formally real field, let $f(x) \in F[x]$ be an irreducible polynomial of odd degree and let α be a root of $f(x)$. Prove that $F(\alpha)$ is also formally real. [Pick α a counterexample of minimal degree. Show that $-1 + f(x)g(x) = (p_1(x))^2 + ... + (p_m(x))^2$ for some $p_i(x), g(x) \in F[x]$ where $g(x)$ has odd degree $<$ deg$f$. Show that some root β of g has odd degree over F and $F(\beta)$ is not formally real, violating the minimality of α.]

Proof. Suppose α is a minimal degree counterexample for some field F. (It is possible to choose a minimal degree counterexample for any field F because any root α has finite degree.) By definition, $p_1(\alpha)^2 + ... + p_n(\alpha)^2 = -1$ for each $p_i(\alpha)$ being in $F(\alpha)$. Let $q(x) = (p_1(x))^2 + ... + (p_n(x))^2$. Since $q(x) \cong -1 \mod f(x)$, there is a $g(x)$ such that $-1 + f(x)g(x) = q(x)$. Since $\deg q(x) = \deg g(x) \cdot \deg f(x)$ is even, $\deg g(x)$ must be odd. Since each term in $q(\alpha)$ is the square of a term in $F(\alpha) \cong F[x]/(f(x))$, $q(x)$ has degree at most $2(\deg f - 1)$. Hence, $g(x)$ has degree at most $2(\deg f - 1) - \deg f = \deg f - 2$. So $\deg g < \deg f$.

Let $g'(x)$ be the minimal irreducible odd degree factor of $g(x)$ and denote its root by β. Let $p_i'(x)$ be the remainder after dividing $p_i(x)$ be $g(x)$. Then in $F(\beta)$, the term $p_n'(\beta)^2 + ... + p_1'(\beta)^2 = -1$, which is a contradiction. Therefore, $F(\alpha)$ is formally real for all odd degree roots α. □

Problem 2.17. Let $f(x)$ be an irreducible polynomial of degree n over a field F. Let $g(x)$ be any polynomial in $F[x]$. Prove that every irreducible factor of the composite polynomial $f(g(x))$ has degree divisible by n.

Proof. If α is a root of $f(x)$, then the roots of $g(x) - \alpha$ are roots of $f(g(x))$. If β is a root of $g(x) - \alpha$, then it will have degree $n \leq \deg g$. Hence, β will have degree $n \cdot \deg f$ in $f(g(x))$, which obviously divides $\deg f$. □

Problem 2.19. Let K be an extension of F of degree n.

(a) For any $\alpha \in K$ prove that α acting by left multiplication on K is an F-linear transformation of K.

(b) Prove that K is isomorphic to a subfield of the ring of $n \times n$ matrices over F, so the ring of $n \times n$ matrices over F contains an isomorphic copy of every extension of F of degree n.

Proof. (a) Let a, b be elements of K and c be an element of F; $\alpha \cdot (a + bc) = \alpha \cdot (a) + c\alpha \cdot (b)$. □

Problem 4.1. Determine the splitting field and its degree over $x^4 - 2$.

Proof. This polynomial can be factored as $(x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$. Hence, its roots are $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. So the splitting field is isomorphic to $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$. Since the polynomial is irreducible in $\mathbb{Q}$ by Eisenstein, this extension is degree 4. □

Problem 4.3. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.

Proof. Using the quadratic formula on $x^2 + x + 1$ yields $\frac{-1 \pm i\sqrt{3}}{2}$ So the roots of the original polynomial are $\pm\sqrt{\frac{-1 \pm i\sqrt{3}}{2}}$. And the splitting field is hence $\mathbb{Q}(\sqrt{\frac{-1+i\sqrt{3}}{2}}, \sqrt{\frac{-1-i\sqrt{3}}{2}})$.

Using Wolfram Alpha to find different forms of $\sqrt{\frac{-1+i\sqrt{3}}{2}}, \sqrt{\frac{-1-i\sqrt{3}}{2}}$, we see that the roots of the polynomial can also be written as $\pm\frac{1}{2} \pm \frac{i\sqrt{3}}{2}$. Hence, the cutting field is isomorphic to $\mathbb{Q}(i\sqrt{3})$, and the field is hence a two degree extension.

Remark 1. *Since I have already done a few problems involving reduction of complex numbers, I decided to use Wolfram Alpha to simplify terms. However, while using wolfram alpha, I discovered that the polynomial $x^4 + x^2 + 1$ can be factored in $\mathbb{Q}$ as $(x^2 + x + 1)(x^2 - x + 1)$. This is reminiscent of example 4 on page 534 of the book. Sometimes, the degree of a splitting field is lower than expected.*

□

Problem 4.5. Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. [Use Theorems 8 and 27.]

Proof. Suppose K is a splitting field of F, and that $f'(x) \in F[x]$ is an irreducible polynomial with a root α in K. And let $f(x)$ be a polynomial in $F[x]$ with root α which is split by K. Let β be any root of $f'(x)$. By theorem 8, we can extend the identity isomorphism to conclude $F(\alpha) \cong F(\beta)$. From the division algorithm in $F(\alpha)$, we can conclude that there is a $g(x)$ in $F(\alpha)[x]$ such that $f(x) = (x-\alpha)^n g(x)$, where n is the order of α in $f(x)$. (note that there is no remainder since $(x-\alpha)^n$ divides $f(x)$.) Since □

Problem 5.1. Prove that the derivative D_x of a polynomial satisfies $D_x(f(x)+g(x)) = D_x(f(x))+D_x(g(x))$ and $D_x(f(x)g(x)) = D_x(f(x))g(x) + D_x(g(x))f(x)$ for any two polynomials $f(x)$ and $g(x)$.

Proof. Let $f(x) = f_m x^m + f_{m-1}x^{m-1} + ... + f_1 x + f_0$ and $g(x) = g_n x^n + g_{n-1}x^{n-1} + ... + f_1 x + f_0$. The derivative of $f(x) + g(x)$ is then $m f_m x^{m-1} + ... + f_1 + n g_n x^{n-1} + ... + g_1$, which is obviously $D_x(f(x)) + D_x(g(x))$. For $f(x)g(x)$, we can rewrite the product as $\Sigma_{i=0}^n \Sigma_{j=0}^m g_i f_j x^{i+j}$. The derivative of this is

$$\Sigma_{i=0}^n \Sigma_{j=0}^m (i+j) g_i f_j x^{i+j-1} = \Sigma_{i=0}^n \Sigma_{j=0}^m (i g_i x^{i-1}) f_j x^j + g_i x^i (j f_j x^{j-1}) =$$

Distributing the sumations leads us to

$$\Sigma_{i=0}^n i g_i x^{i-1} \Sigma_{j=0}^m f_j x^j + \Sigma_{i=0}^n g_i x^i \Sigma_{j=0}^m j f_j x^{j-1}$$

Which is of course the equivalent to $D_x(g(x))f(x) + g(x)D_x(f(x))$. □

Problem 5.3. Prove that d divides n if and only if $x^d - 1$ divides $x^n - 1$. [Note that if $n = qd + r$ then $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$.]

Proof. Suppose d divides n. Then, for any α a root of $x^d - 1$, $\alpha^n - 1 = (\alpha^{dq} - 1 = 1^q - 1 = 1 - 1 = 0$. So $x^n - 1$ has all of $x^d - 1$ roots. Furthermore, since both polynomials are separable, all of $x^d - 1$ roots show up exactly once in its factorization. From this we can conclude that $x^d - 1$ factors out of $x^n - 1$. Now, suppose $x^d - 1$ divides $x^n - 1$. Then any root α of $x^d - 1$ is also a root of $x^n - 1$. As noted in the hint, we can rewrite $x^n - 1$ as $(x^{qd+r} - x^r) + (x^r - 1)$. At α, this must evaluate to 0. So, we have $0 = (\alpha^{qd+r} - \alpha^r) + (\alpha^r - 1) = (\alpha^{qd}\alpha^r - \alpha^r) + (\alpha^r - 1) = (\alpha^r - \alpha^r) + (\alpha^r - 1) = (\alpha^r - 1)$. Hence $x^r - 1$ must be zero for any root of $x^d - 1$. Since there are $d > r$ distinct roots for $x^d - 1$, this can only be true if $x^r - 1$ is identically 0. Therefore, $r = 0$ and $d|n$. □

Problem 5.5. For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. [For the irreducibility: One approach - prove first that if a is a root then $a + 1$ is also a root. Another approach - suppose it's reducible and compute derivatives.]

Proof. Suppose for the sake of contradiction that $\alpha \in \mathbb{F}_p$ is a root of the polynomial. Then $(\alpha+1)^p - (\alpha+1) + a$ can be rewritten by the Frobenius endomorphism theorem to $\alpha^p + 1^p - \alpha + 1 + a = \alpha^p + \alpha + a$. Hence, $\alpha + 1$ is also a root. By induction, this means that every element of the field is a root of the polynomial. Hence, a is a root and $0 = a^p - a + a = a^p$. This is a contradiction since a is nonzero and fields are integral domains. Therefore, the polynomial is irreducible in $\mathbb{F}_p$. It follows from proposition 37 that the polynomial is also separable. □

Problem 5.7. Suppose K is a field of characteristic p which is not a perfect field: $K \neq K^p$. Prove there exist irreducible inseparable polynomials over K. Conclude that there exist inseparable finite extensions of K.

Proof. Let a be an element of K such that $\alpha = a^{\frac{1}{p}} \notin K$. The field $K(\alpha)$ is still of characteristic p. So we have $(x-\alpha)^p = x^p - \alpha^p = x^p - a$. Hence, $x^p - a$ is inseparable, as well as being obviously irreducible in K. Therefore, $K(\alpha)$ is a finite inseparable extension of K. To see that there are multiple irreducible inseparable polynomials in K and multiple inseparable extensions of K, note that $a + a \neq a$ is also not perfect since $(a+a)^{\frac{1}{p}} = \alpha + \alpha \notin K$. □

Problem 5.9. Show that the binomial coefficient $\binom{pn}{pi}$ is the coefficient of x^{pi} in the expansion of $(1+x)^{pn}$. Working over $\mathbb{F}_p$ show that this is the coefficient of $(x^p)^i$ in $(1+x^p)^n$ and hence prove that $\binom{pn}{pi} = \binom{n}{i}($ mod $p)$.

Proof. By the binomial theorem, the coefficient of x^{pi} is $\binom{pn}{pi}$. In $\mathbb{F}$, we can rewrite $(1+x)^{pn}$ as $(1+x^p)^n$. Hence, $\binom{pn}{pi}$ is also the coefficient of $(x^p)^i$ in the expansion. □