

# Exercises from Dummit and Foote Chapter 13 on Field Theory

Wesley Basener

June 24, 2025

**Problem 1.1.** Show that  $p(x) = x^3 + 9x + 6$  is irreducible in  $\mathbb{Q}[x]$ . Let  $\theta$  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

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

Polynomial gives us

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

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

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

□

**Problem 1.3.** Show that  $x^3 + x + 1$  is irreducible over  $\mathbb{F}_2$  and let  $\theta$  be a root. Compute the powers of  $\theta$  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  $\theta^2$  as a remainder, so there is no reduced form of  $\theta^2$ .  $\theta$  is obviously itself and  $\theta^0 = 1$ .

For  $\theta^n$  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  $\theta^n = (\theta^3)^a \cdot \theta^b = (\theta + 1)^a \cdot \theta^b$ . Repeating the process for  $a$  and factoring when needed will eventually terminate with a polynomial of degree less than 3. □

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

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

*Proof.* I'm gonna come back to this later. □

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

**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  $x^2 - 2x + 2$   $\square$

**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 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  $x^4$  coefficient 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  $\sqrt{m} + \sqrt{n} = \sqrt{a + \sqrt{b}}$ . 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

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

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

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

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

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

$$\begin{aligned} & \sqrt{1+\sqrt{-3}} + \sqrt{1-\sqrt{-3}} \\ &= \\ & \sqrt{2}(\cos(\arctan(\sqrt{3})) + i \sin(\arctan(\sqrt{3})))^{\frac{1}{2}} + \sqrt{2}(\cos(\arctan(\sqrt{3})) - i \sin(\arctan(\sqrt{3})))^{\frac{1}{2}} = \sqrt{2}(\cos(\frac{1}{2} \arctan(\sqrt{3})) + i \sin(\frac{1}{2} \arctan(\sqrt{3}))) \\ &= \\ & 2\sqrt{2} \cos(\frac{1}{2} \arctan(\sqrt{3})) \end{aligned}$$

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. □

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

*Proof.* Since each  $\alpha_i^2$  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  $F = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$  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  $[F : \mathbb{Q}] = 2$ . However, the degree of  $\mathbb{Q}(\sqrt[3]{2})$  is 3. Therefore,  $\sqrt[3]{2}$  it is not contained in  $F$ . □

**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  $\alpha$  be a root of  $f(x)$ . Prove that  $F(\alpha)$  is also formally real. [Pick  $\alpha$  a counterexample of minimal degree. Show that  $-1 + f(x)g(x) = (p_1(x))^2 + \dots + (p_m(x))^2$  for some  $p_i(x), g(x) \in F[x]$  where  $g(x)$  has odd degree  $< \deg f$ . Show that some root  $\beta$  of  $g$  has odd degree over  $F$  and  $F(\beta)$  is not formally real, violating the minimality of  $\alpha$ .]

*Proof.* Suppose  $\alpha$  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  $\alpha$  has finite degree.) By definition,  $p_1(\alpha)^2 + \dots + p_n(\alpha)^2 = -1$  for each  $p_i(\alpha)$  being in  $F(\alpha)$ . Let  $q(x) = (p_1(x))^2 + \dots + (p_n(x))^2$ . Since  $q(x) \cong -1 \pmod{f(x)}$ , 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  $\beta$ . Let  $p'_i(x)$  be the remainder after dividing  $p_i(x)$  by  $g(x)$ . Then in  $F(\beta)$ , the term  $p'_n(\beta)^2 + \dots + p'_1(\beta)^2 = -1$ , which is a contradiction. Therefore,  $F(\alpha)$  is formally real for all odd degree roots  $\alpha$ .  $\square$

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

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

- (a) For any  $\alpha \in K$  prove that  $\alpha$  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  $F$ ;  $\alpha \cdot (a + bc) = \alpha \cdot a + c\alpha \cdot b$ .  $\square$

**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.  $\square$

**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.  $\square$

**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  $\alpha$  in  $K$ . And let  $f(x)$  be a polynomial in  $F[x]$  with root  $\alpha$  which is split by  $K$ . Let  $\beta$  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  $\alpha$  in  $f(x)$ . (note that there is no remainder since  $(x - \alpha)^n$  divides  $f(x)$ .) Since  $\square$

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

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

Distributing the summations leads us to

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

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

**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  $\alpha$  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  $\alpha$  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  $\alpha$ , 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  $d|n$ .  $\square$

**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.  $\square$

**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  $(a + a)^{\frac{1}{p}} = \alpha + \alpha \notin K$ .  $\square$

**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  $\binom{pn}{pi} \equiv \binom{n}{i} \pmod{p}$ .

*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.  $\square$