

Turn in problems 54, 55, 57, 58, 59, 60, 61, 62, 63, 64, 65.

**Problem 54.** If  $f \in \mathbb{K}[X]$  (with  $\mathbb{K}$  field) has degree  $n$  and  $\mathbb{F}$  is a splitting field of  $f$  over  $\mathbb{K}$ , prove that  $[\mathbb{F} : \mathbb{K}] \mid n!$ .

*Proof.* If  $f$  has a degree 1 over  $\mathbb{K}$ , then it has only one zero  $a$  whose minimal polynomial must have degree 1.  $1 = [\mathbb{K}(a) : \mathbb{K}] = [\mathbb{F} : \mathbb{K}] \mid 1!$ . If  $f$  has degree 2 over  $\mathbb{K}$ , then it has at most two distinct zeros. Suppose  $f$  is reducible. Then it splits into two linear factors over  $\mathbb{K}$  and so  $\mathbb{F} \cong \mathbb{K} \implies [\mathbb{F} : \mathbb{K}] = 1 \mid 2!$ . Otherwise  $f$  is irreducible, and so the minimal polynomial for a zero  $a_1$  of  $f$  must be of the form  $\frac{f(x)}{\ell}$  for some  $\ell \in \mathbb{K}$ , and therefore both zeros  $a_1$  and  $a_2$  share the same minimal polynomial  $x^2 + bx + c = (x - a_1)(x - a_2) \in \mathbb{K}[x]$ . So then  $x^2 - (a_1 + a_2)x + a_1a_2 = x^2 + bx + c \implies a_2 = -b - a_1 \in \mathbb{K}(a)$  and so  $\mathbb{F} \cong \mathbb{K}(a) \implies [\mathbb{F} : \mathbb{K}] \in \{1, 2\}$  both of which divide  $2!$ . Suppose  $[\mathbb{F} : \mathbb{K}] \mid d!$  if  $\mathbb{F}$  is the splitting field of any degree  $d$  polynomial  $f$  over  $\mathbb{K}$  for all  $1 \leq d < m$  for some  $m \geq 2$ . Consider the statement for a degree  $m$  polynomial  $f$  over  $\mathbb{K}$ .

If  $f$  is reducible, then  $f(x) = P(x)Q(x)$  for some non-constant degree  $p$  and  $(m - p)$  polynomials  $P$  and  $Q$  over  $\mathbb{K}$ . Let  $\mathbb{F}_P$  be the splitting field of  $P$  over  $\mathbb{K}$  and  $\mathbb{F}_Q$  be the splitting field of  $Q$  over  $\mathbb{F}_P$ . Since  $\deg_{\mathbb{K}}(P(x)) = p$ ,  $\deg_{\mathbb{F}_P}(Q(x)) = \deg_{\mathbb{K}}(Q(x)) = m - p < m$ , we have that  $[\mathbb{F}_Q : \mathbb{F}_P] \mid (m - p)!$  and  $[\mathbb{F}_P : \mathbb{K}] \mid p!$ . Well,  $\mathbb{F}_Q = (\mathbb{F}_P)(\alpha \mid Q(\alpha) = 0) \cong (\mathbb{K}(a \mid P(a) = 0))(b \mid Q(b) = 0) = \mathbb{K}(\alpha \mid P(\alpha) = 0 \text{ or } Q(\alpha) = 0) \cong \mathbb{F}$ . So finally,  $\mathbb{F}_Q \supseteq \mathbb{F}_P \supseteq \mathbb{K} \implies [\mathbb{F} : \mathbb{K}] = [\mathbb{F}_Q : \mathbb{K}] = [\mathbb{F}_Q : \mathbb{F}_P][\mathbb{F}_P : \mathbb{K}] \mid p!(m - p)! \mid m!$  (via  $\binom{p}{m} = \frac{m!}{p!(m - p)!}$ ). So  $[\mathbb{F} : \mathbb{K}] \mid m!$ .

If  $f$  is irreducible, then for any zero  $a$  of  $f$ ,  $[\mathbb{K}(a) : \mathbb{K}] = m$  and by the division algorithm we have  $f(x) = (x - a)Q(x)$  over  $\mathbb{K}(a)$  where  $Q$  has degree  $m - 1$ . Since  $Q$  has degree less than  $m$ , the splitting field  $\mathbb{F}_Q$  of  $Q$  over  $\mathbb{K}(a)$  must be such that  $[\mathbb{F}_Q : \mathbb{K}(a)] \mid (m - 1)!$  and since  $\mathbb{F}_Q = (\mathbb{K}(a))(\alpha \mid Q(\alpha) = 0) = \mathbb{K}(\alpha \mid x - \alpha = 0 \text{ or } Q(\alpha) = 0) \cong \mathbb{F}$  we have that  $[\mathbb{F} : \mathbb{K}] = [\mathbb{F}_Q : \mathbb{K}] = [\mathbb{F}_Q : \mathbb{F}_P][\mathbb{F}_P : \mathbb{K}]$  divides  $m(m - 1)! = m!$ .

Thus, by induction,

If  $\mathbb{F} \supseteq \mathbb{K}$  is the splitting field of a degree  $n \in \mathbb{Z}^+$  polynomial over  $\mathbb{K}$ , then  $[\mathbb{F} : \mathbb{K}] \mid n!$ .

□

**Problem 55.** If  $K \subseteq F$  is a field extension,  $F$  is algebraically closed, and  $E$  is the set of all elements of  $F$  that are algebraic over  $K$ , prove that  $E$  is an algebraic closure of  $K$ .

**Problem 57.** If  $[F : K] = 2$ , then  $K \subseteq F$  is a normal extension.

**Problem 58.** If  $d$  is a nonnegative rational number, then  $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))$  is the identity or is isomorphic to  $\mathbb{Z}_2$ .

**Problem 59.** What is the Galois group of  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  over  $\mathbb{Q}$ ?

**Problem 60.** Assume  $K$  is a field of characteristic 0. Let  $G$  be the subgroup of  $\text{Aut}_K(K(X))$  generated by the  $K$ -automorphism induced by  $X \mapsto X + 1$ . Prove that  $G$  is an infinite cyclic group. What is the fixed field  $E$  of  $G$ ? What is  $[K(X) : E]$ ?

We prepare for the next problem by proving a bunch of useful stuff.

**Lemma 1.** *If  $\mathbb{K}$  is a field and  $f(x) \in \mathbb{K}[x]$ ,  $f(x)$  has some repeated zero  $\alpha$  if and only if  $\alpha$  is also a zero of  $f'(x)$ , the formal derivative of  $f(x)$  over  $\mathbb{K}$ .*

*Proof.* (  $\implies$  ) If  $\alpha$  is a repeated zero of  $f(x)$ , then  $f(x) = (x - \alpha)^2 g(x) \in \overline{\mathbb{K}}[x]$  for some  $g(x)$  over an algebraic closure  $\overline{\mathbb{K}}$  of  $\mathbb{K}$ . So then  $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x) \implies f'(\alpha) = 0$ . (  $\impliedby$  ) On the other hand if  $f(\alpha) = f'(\alpha) = 0$ , then  $f(x) = (x - \alpha)q(x) \in \overline{\mathbb{K}}[x]$  for some  $q(x)$  over  $\overline{\mathbb{K}}$ . Therefore,  $f'(x) = q(x) + (x - \alpha)q'(x)$  and so  $f'(\alpha) = q(\alpha) = 0 \implies q(\alpha) = 0$  since  $q(x) = 0$  implies that  $f(x) = 0$ , a contradiction. So then  $q(\alpha) = 0 \implies (x - \alpha) \mid q(x) \in \overline{\mathbb{K}}[x] \setminus \overline{\mathbb{K}} \implies f(x) = (x - \alpha)^2 h(x)$  for some  $h(x) \in \overline{\mathbb{K}}[x]$  where  $q(x) = (x - \alpha)h(x)$ . So  $\alpha$  is a repeated zero of  $f(x)$ . □

**Theorem 2.**  *$\mathbb{K}$  is a finite field*

$$\implies \text{Char } \mathbb{K} = p > 0 \text{ for some prime } p \quad (1)$$

$$\iff \mathbb{K} \text{ is some } n\text{-dimensional } \mathbb{k}_p\text{-vector space where } n \in \mathbb{Z}^+ \text{ and } \mathbb{k}_p \cong \mathbb{Z}_p \quad (2)$$

$$\iff \mathbb{K} \text{ is a splitting field of } f_{p,n}(x) = x^{(p^n)} - x \text{ over } \mathbb{k}_p \text{ where } n \in \mathbb{Z}^+ \text{ and } \mathbb{k}_p \cong \mathbb{Z}_p \quad (3)$$

*Proof.* (1) We can't have  $\text{Char } \mathbb{K} = 0$  otherwise  $\mathbb{K}$  would be infinite, so  $\text{Char } \mathbb{K} = p > 0$ . Suppose  $p$  is not prime. (We typically just denote an  $n$ -sum of 1's  $n := \sum_{i=1}^n 1$  in the context of our fields.) So  $p = ab = 0$  for some  $1 \leq a, b < p$ . But then  $p = ab = 0$  for some  $a, b \neq 0$  and then  $\mathbb{K}$  has zero divisors, a contradiction. So  $\text{Char } \mathbb{K} = p > 0$  for some prime  $p$ .

(2) (  $\implies$  ) Since (1)  $\implies \text{Char } \mathbb{K} = p > 0$  for some prime  $p$ , we have that  $\mathbb{k}_p = \langle 1_{\mathbb{K}} \rangle_+ \cong \langle 1_{\mathbb{Z}_p} \rangle_+ = \mathbb{Z}_p$ , a finite field because  $p$  is prime, via  $1_{\mathbb{K}} \leftrightarrow 1_{\mathbb{Z}_p}$ . So then  $\mathbb{k}_p \subseteq \mathbb{K}$  is a subfield, and immediately by the field axioms we have that  $\mathbb{K}$  is a  $\mathbb{k}_p$ -vector space. Additionally, since  $\mathbb{K}$  is finite, it must also be finite dimensional over  $\mathbb{k}_p$ . Therefore,  $\mathbb{K}$  is an  $n$ -dimensional  $\mathbb{k}_p$ -vector space for some  $n \in \mathbb{Z}^+$  and  $\mathbb{k}_p \cong \mathbb{Z}_p$ . (  $\impliedby$  ) If  $\mathbb{K}$  is an  $n$ -dimensional  $\mathbb{k}_p$ -vector space where  $n \in \mathbb{Z}^+$  and  $\mathbb{k}_p \cong \mathbb{Z}_p$ , then  $|\mathbb{K}| = p^n$  and so  $\mathbb{K}$  is finite.

(3) (  $\implies$  ) By (2) we have that  $|\mathbb{K}| = p^n$  for some  $n \in \mathbb{Z}^+$  and then for any  $a \in \mathbb{K}^* = \mathbb{K} \setminus \{0\}$ , the multiplicative group of  $\mathbb{K}$ , we have that  $|a|$  divides  $|\mathbb{K}^*| = p^n - 1$ . Therefore,  $a^{p^n-1} = 1 \implies a^{p^n} = a$ . Therefore, every  $a \in \mathbb{K}$  is a zero of  $f_{p,n}(x) = x^{(p^n)} - x \in \mathbb{k}_p[x]$ . Now,  $f'_{p,n}(x) = p^n x^{p^n-1} - 1 = -1$  since  $\text{Char } \mathbb{K} = p$  and so by **Lemma 1**,  $f'_{p,n}(\alpha) = -1 \neq 0$  for all zeros  $\alpha$  of  $f_{p,n}(x) \implies f_{p,n}(x)$  has no repeated zeros. So then since  $f_{p,n}(x)$  has at most  $p^n$  zeros which are all distinct, in fact  $\mathbb{K}$  must be exactly all distinct zeros of  $f_{p,n}(x)$ . Suppose  $f_{p,n}(x)$  splits completely in a smaller field  $\mathbb{M}$  where  $|\mathbb{M}| < |\mathbb{K}|$ . But then  $\mathbb{K} = \{\alpha \in \overline{\mathbb{K}} \mid f_{p,n}(\alpha) = 0\} \subseteq \mathbb{M} \implies |\mathbb{M}| \geq |\mathbb{K}|$  for some algebraic closure  $\overline{\mathbb{K}}$  of  $\mathbb{K}$ , a contradiction. So then  $\mathbb{K}$  is a splitting field of  $f_{p,n}(x)$  over  $\mathbb{k}_p$ . (  $\impliedby$  ) If  $\mathbb{K}$  is a splitting field of  $f_{p,n}(x) = x^{(p^n)} - x$  over  $\mathbb{k}_p \cong \mathbb{Z}_p$ , then it is generated by finitely many algebraic elements over  $\mathbb{k}_p$  which means it is algebraic over  $\mathbb{k}_p$  and therefore a finite extension of the finite field  $\mathbb{k}_p$  which means it is finite field itself. □

Now, we prepare some Corollaries.

**Corollary 3.** If  $\mathbb{K}$  is a finite field of characteristic  $p > 0$ , then inside a fixed algebraic closure  $\overline{\mathbb{K}}$

$$\mathbb{k}_p = \langle 1 \rangle_+ \cong \mathbb{Z}_p \text{ is the prime subfield of } \mathbb{K} \quad (1)$$

$$\text{There exists a unique extension } \mathbb{K}_m \supseteq \mathbb{K} \text{ with } [\mathbb{K}_m : \mathbb{K}] = m \in \mathbb{Z}^+ \quad (2)$$

$$\text{There exists a unique subfield } \mathbb{k}_{p,d} \subseteq \mathbb{K} \text{ with } [\mathbb{k}_{p,d} : \mathbb{k}_p] = d \text{ for each divisor } d \text{ of } [\mathbb{K} : \mathbb{k}_p] \quad (3)$$

*Proof.* (1) Suppose there exists some subfield  $\mathbb{M} \subseteq \mathbb{k}_p$  smaller than  $\mathbb{k}_p$ , so  $|\mathbb{M}| < |\mathbb{k}_p|$ . But then  $0, 1 \in \mathbb{M} \implies \mathbb{k}_p = \langle 1 \rangle_+ \subseteq \mathbb{M} \implies |\mathbb{M}| \geq |\mathbb{k}_p|$ , a contradiction. So  $\mathbb{k}_p$  must be the prime subfield of  $\mathbb{K}$ .

(2) By **Theorem 2.**,  $\mathbb{K}$  has dimension  $n$  over  $\mathbb{k}_p$  for some  $n \in \mathbb{Z}^+$ . Now, for some  $m \in \mathbb{Z}^+$  let  $f_{p,n,m}(x) = x^{(p^n)^m} - x \in \mathbb{K}_p$  and  $\mathbb{K}_m = \{\alpha \in \overline{\mathbb{K}} \mid f_{p,n,m}(\alpha) = 0\}$ . Observe.

For any  $\alpha, \beta \in \mathbb{K}_m$  with  $\beta \neq 0$ ,  $f_{p,n,m}(\alpha - \beta) = (\alpha - \beta)^{p^{nm}} - (\alpha - \beta) = (\sum_{i=0}^{p^{nm}} \binom{p^{nm}}{i} \alpha^{p^{nm}-i} (-\beta)^i) - (\alpha - \beta) = (\alpha^{p^{nm}} + (-\beta)^{p^{nm}}) - (\alpha - \beta)$  since  $\binom{p^{nm}}{0} = \binom{p^{nm}}{p^{nm}} = 1$  and  $p \mid \binom{p^{nm}}{i}$  for all  $0 < i < p^{nm}$  (I am uninterested in proving this part.) and since  $p = 0$  we get that in fact  $f_{p,n,m}(\alpha - \beta) = (\alpha^{p^{nm}} - \beta^{p^{nm}}) - (\alpha - \beta) = \alpha - \beta - (\alpha - \beta) = 0$ . Note that this holds for  $p = 2$  since  $-\alpha = \alpha$  in a field with characteristic 2. Therefore,  $\alpha - \beta \in \mathbb{K}_m$ . Next,  $f_{p,n,m}(\alpha\beta^{-1}) = (\alpha\beta)^{p^{nm}} = \alpha^{p^{nm}}\beta^{-p^{nm}} - (\alpha\beta^{-1}) = \alpha(\beta^{p^{nm}})^{-1} - \alpha\beta^{-1} = \alpha(\beta)^{-1} - \alpha\beta^{-1} = 0 \implies \alpha\beta^{-1} \in \mathbb{K}_m$ .

So  $\mathbb{K}_m$  is a subfield of  $\overline{\mathbb{K}}$  in which  $f_{p,n,m}(x)$  splits completely. Suppose there is a smaller such field  $\mathbb{M}$  that  $f_{p,n,m}(x)$  splits completely over, so  $|\mathbb{M}| < |\mathbb{K}_m|$ . But then  $\mathbb{K}_m = \{\alpha \in \overline{\mathbb{K}} \mid f_{p,n,m}(\alpha) = 0\} \subseteq \mathbb{M} \implies |\mathbb{M}| \geq |\mathbb{K}_m|$ , a contradiction. So  $\mathbb{K}_m$  must be a splitting field of  $f_{p,n,m}(x)$  over  $\mathbb{k}_p$ . Finally,  $a^{(p^n)} = a$  for all  $a \in \mathbb{K}$ . Suppose that for any  $a \in \mathbb{K}$ ,  $a^{(p^n)^c} = a$  for some  $c \geq 1$ . Then,  $a^{(p^n)^{c+1}} = (a^{(p^n)^c})^{p^n} = (a)^{p^n} = a$ . Therefore, by induction  $a^{(p^n)^c} = a$  for all  $c \geq 1$ . So then every element  $a \in \mathbb{K}$  is a zero of  $f_{p,n,m}(x) = x^{(p^n)^m} - x$  and  $\mathbb{K}_m \supseteq \mathbb{K} \supseteq \mathbb{k}_p$ . So then we have  $[\mathbb{K}_m : \mathbb{k}_p] = [\mathbb{K}_m : \mathbb{K}][\mathbb{K} : \mathbb{k}_p] = nm = [\mathbb{K}_m : \mathbb{K}]n \implies [\mathbb{K}_m : \mathbb{K}] = m$ . Suppose some other distinct extension  $\mathbb{E}_m \supseteq \mathbb{K}$  of degree  $m$  over  $\mathbb{K}$  exists. Well, it has order  $p^{nm}$  and all of its elements must be zeros of  $f_{p,n,m}(x)$  via  $|\mathbb{E}_m^*| = p^n - 1$ , and then since  $\mathbb{K}_m - \mathbb{E}_m \neq \emptyset$  we have that  $|\mathbb{K}_m \cup \mathbb{E}_m| > p^{nm}$  and so  $f_{p,n,m}(x)$  has more than  $p^{nm}$  distinct zeros, a contradiction. So  $\mathbb{K}_m$  is the unique extension with  $[\mathbb{K}_m : \mathbb{K}] = m$  with respect to the closure  $\overline{\mathbb{K}}$ .

(3) By (2), we immediately get that there exists a unique extension  $\mathbb{k}_{p,d} \supseteq \mathbb{k}_p$  with  $[\mathbb{k}_{p,d} : \mathbb{k}_p] = d$  for each divisor  $d \mid n$  which is a splitting field for  $f_{p,m,d}(x) = x^{p^d} - x$  over  $\mathbb{k}_p$ . For any such divisor  $d \mid n$ ,  $a^{p^d} = a$  for all  $a \in \mathbb{k}_{p,d}$ . So then since  $d \mid n$ ,  $n = dq$  for some  $q \in \mathbb{Z}^+$  and therefore by the induction earlier replacing  $\mathbb{K}$  with  $\mathbb{k}_{p,d}$  we get that  $a^{p^n} = a^{p^{dq}} = a$  for all  $a \in \mathbb{k}_{p,d}$ . Therefore every element in  $\mathbb{k}_{p,d}$  is a zero of  $f_{p,n}(x) = x^{p^n} - x$  over  $\mathbb{k}_p$ , and since  $\mathbb{K}$  is a splitting field for  $f_{p,n}(x)$  in fact we have that  $\mathbb{K} \supseteq \mathbb{k}_{p,d} \supseteq \mathbb{k}_p$ . So then for each divisor  $d \mid n$ ,  $\mathbb{k}_{p,d}$ , the splitting field of  $f_{p,d}$  over  $\mathbb{k}_p$ , is a unique subfield of  $\mathbb{K}$  with  $[\mathbb{k}_{p,d} : \mathbb{k}_p] = d$ .

□

Alright now let's do the problem. I just wanted to prove this all myself instead of looking over the notes.

**Problem 62.** Let  $k$  be a finite field of characteristic  $p > 0$ .

- (a) Prove that for every  $n > 0$  there exists an irreducible polynomial  $f \in k[X]$  of degree  $n$ .
- (b) Prove that for every irreducible polynomial  $P \in k[X]$  there exists  $n \geq 0$  such that  $P$  divides  $X^{p^n} - X$ .

*Proof.* Fix some algebraic closure  $\overline{\mathbb{K}} \supseteq \mathbb{K}$ . Every object that follows is contained in  $\overline{\mathbb{K}}$ . By our theorems, if  $\mathbb{K}$  is a finite field of characteristic  $p > 0$ ,  $p$  is prime and  $\mathbb{K}$  is an  $n$ -dimensional  $\langle 1 \rangle_+ = \mathbb{k}_p$ -vector space for some  $n \in \mathbb{Z}^+$ . Also, there exists a unique extension  $\mathbb{K}_m$  of  $\mathbb{K}$  with  $[\mathbb{K}_m : \mathbb{K}] = m$  for each  $m \in \mathbb{Z}^+$ . Finally, both  $\mathbb{K}$  and  $\mathbb{K}_m$  are unique splitting fields of  $f_{p,n} = x^{p^n} - x$  and  $f_{p,n,m} = x^{p^{nm}} - x$ , respectively, over  $\mathbb{k}_p$  with respect to  $\overline{\mathbb{K}}$ . Suppose that for all  $\alpha \in \mathbb{K}_m$ , the degree of  $\alpha$  over  $\mathbb{K}$  is strictly less than  $[\mathbb{K}_m : \mathbb{K}] = m$ . Any  $\alpha$  must belong to  $\mathbb{K}(\alpha) \subseteq \mathbb{K}_m$  and  $[\mathbb{K}(\alpha) : \mathbb{K}] = d$  for some divisor  $0 < d < nm$  of  $[\mathbb{K}_m : \mathbb{k}_p] = nm$ . Well, by our theorems this must be the unique subfield  $\mathbb{k}_{p,d}$  of order  $p^d$ . Therefore,

$$\mathbb{K}_m = \bigcup_{\substack{d|nm \\ 0 < d < nm}} \mathbb{k}_{p,d} \implies |\mathbb{K}_m| = p^{nm} = \left| \bigcup_{\substack{d|nm \\ 0 < d < nm}} \mathbb{k}_{p,d} \right| \leq \sum_{\substack{d|nm \\ 0 < d < nm}} p^d < \sum_{i=0}^{nm-1} p^i = \frac{p^{nm} - 1}{1 - p} < p^{nm},$$

a contradiction. (Another contradiction is just the fact that then every  $\alpha \in \mathbb{K}_m$  belongs to  $\mathbb{k}_{p,d}$  for the largest  $d < nm$  that divides  $nm$  and is less than  $m$ , but  $|\mathbb{K}_m|$  is strictly less than  $p^{nm}$ . We did not prove directly that all these subfields are nested, so I didn't do that.) Therefore, there exists an element  $\alpha_m \in \mathbb{K}_m$  with degree  $m$  over  $\mathbb{K}$ , and so there exists a monic irreducible polynomial of  $\alpha_m$  over  $\mathbb{K}$  with degree  $m$ , that is  $\mathbb{K}_m = \mathbb{K}(\alpha_m)$ .

Now, consider any irreducible polynomial  $P(x) \in \mathbb{K}[x]$ . It must have some degree  $q \in \mathbb{Z}^+$ , and some zero  $\alpha$  with the minimal polynomial  $P_\alpha(x) = \frac{P(x)}{a} \in \mathbb{K}[x]$  where  $a \in \mathbb{K}$  is the leading coefficient of  $P(x)$ . So then  $\alpha$  has degree  $q$  over  $\mathbb{K}$  and  $[\mathbb{K}(\alpha) : \mathbb{K}] = q$ . Therefore, by our theorems,  $\mathbb{K}(\alpha) = \mathbb{K}_q \subseteq \overline{\mathbb{K}}$ , the splitting field of  $f_{p,n,q}(x) = x^{p^{nq}} - x$  over  $\mathbb{k}_p$ . Well,  $\alpha \in \mathbb{K}_q \implies |\alpha|$  divides  $|\mathbb{K}_q^*| = p^{nq} - 1$  and so  $\alpha^{p^{nq}-1} = 1 \implies \alpha^{p^{nq}} = \alpha \implies f_{p,n,q}(\alpha) = (\alpha)^{p^{nq}} - \alpha = 0$ . So  $\alpha$  is a zero of  $f_{p,n,q}(x) = x^{p^{nq}} - x$  over  $\mathbb{k}_p$ , which is also a polynomial over  $\mathbb{K}$ .

□

**Problem 63.** Let  $p$  be a prime and  $\mathbb{F}_q$  (with  $q = p^s$ ) be the finite field with  $q$  elements. Let  $f \in \mathbb{F}_q[X]$  be an irreducible polynomial. Prove that  $f$  is irreducible in  $\mathbb{F}_{q^m}[X]$  if and only if  $m$  and  $\deg f$  are relatively prime.

*Proof.* Let  $f(x)$  be an irreducible polynomial over  $\mathbb{F}_{p^n}$  with degree  $\deg f(x) = d$  for some prime  $p$  and some  $n \geq 1$ . Also, let  $f_{p,N}(x) = x^{p^N} - x$  over  $\mathbb{F}_p$  for any  $N \in \mathbb{Z}^+$  and recall that every element of  $\mathbb{F}_{p^{nN}}$ , the splitting field of  $f_{p,N}(x)$ , is a zero of  $f_{p,N}(x)$ .

Now, since  $f(x)$  is irreducible over  $\mathbb{F}_{p^n}$ , any zero  $\alpha$  of  $f(x)$  has the minimal polynomial  $p_\alpha(x) = \frac{f(x)}{c}$  over  $\mathbb{F}_{p^n}$  where  $c$  is the leading coefficient of  $f(x)$  and so it has degree  $d$  over  $\mathbb{F}_{p^n}$ . That is,  $\mathbb{F}_{p^n}(\alpha) = \mathbb{F}_{p^{nd}}$ . So then  $\alpha$  is a zero of  $f_{p,nd}(x)$ , and we also have that  $d$  is smallest integer such that  $\alpha^{p^{nd}} = \alpha$ . Furthermore,  $\alpha^{nk} = \alpha \iff d \mid k$ .

( $\implies$ ) If  $f(x)$  is irreducible over  $\mathbb{F}_{p^{nm}}$ , then  $\alpha$  has degree  $d$  over both  $\mathbb{F}_{p^n}$  and  $\mathbb{F}_{p^{nm}}$ . So  $\alpha = k_1 = k_2$  is the smallest integer such that  $\alpha^{p^{nk_1}} = \alpha^{p^{nmk_2}} = \alpha$ . Additionally, the previous equalities hold for any multiples  $k_1, k_2 \geq 1$  of  $d$ . Suppose  $g = \gcd(d, m) > 1$ , then  $\frac{d}{g} = \ell_d < d$ ,  $\frac{m}{g} = \ell_m < m$ . Observe.

$$m\ell_d = m \frac{d}{g} = \frac{m}{g} d = d\ell_m \implies \alpha^{p^{nm\ell_d}} = \alpha^{p^{nm(\frac{d}{g})}} = \alpha^{p^{nd(\frac{m}{g})}} = \alpha^{p^{nd\ell_m}} = \alpha.$$

But then there is a smaller positive integer  $k_2 = \ell_d < d$  such that  $\alpha^{nmk_2} = \alpha$ , a contradiction. So we must have that  $\gcd(d, m) = 1$ .

( $\impliedby$ ) On the other hand, if  $\gcd(d, m) = 1$ , recall that  $d$  is the smallest positive integer  $d = k_1$  such that  $\alpha^{p^{nk_1}} = \alpha$  for any zero  $\alpha$  of  $f(x)$ . So for any  $k_2 \geq 1$  such that  $\alpha^{p^{nmk_2}} = \alpha$ , we must have that  $d \mid mk_2$ . Suppose we have such a  $k_2$  less than  $d$ . But then  $\gcd(d, m) = 1$  and  $d \mid mk_2 \implies d \mid k_2$  and  $k_2 < d$ , which is impossible. So the smallest such  $k_2 = d$ , which is also the degree of  $\alpha$  over  $\mathbb{F}_{p^{nm}}$ . Since degree of any zero  $\alpha$  of  $f(x)$  is  $d$  over  $\mathbb{F}_{p^{nm}}$ ,  $f(x)$  must be irreducible over  $\mathbb{F}_{p^{nm}}$ . (Otherwise we have some minimal polynomial of degree less than  $d$  which can be pulled out of  $f(x)$  over  $\mathbb{F}_{p^{nm}}$ ).

□

**Problem 64.** Prove that  $E = \mathbb{F}_2[X]/(X^4 + X^3 + 1)$  is a field with 16 elements. What are the roots of  $X^4 + X^3 + 1$  in  $E$ ?

*Proof.* Let  $p(x) = x^4 + x^3 + 1 \in \mathbb{F}_2$ .  $p(0) = p(1) = 1 \neq 0$ , so  $p(x)$  has no zeros in  $\mathbb{F}_2$  and therefore no linear factors over  $\mathbb{F}_2$ , which means it can't factor into a linear and cubic. Suppose  $p(x)$  is reducible. Then must split into two irreducible quadratics over  $\mathbb{F}_2$ . These quadratics must have a non-zero constant and leading coefficient, which must then be  $1 \in \mathbb{F}_2$ , otherwise  $x$  would divide them along with  $p(x)$  or they wouldn't be quadratic at all. So then a factor  $p(x)$  could only be  $x^2 + x + 1$  or  $x^2 + 1$ . However, notice that  $x^2 + 1$  has 1 as a zero, so  $x - 1$  divides it, and would have to then divide  $p(x)$ . Therefore, we must have that  $p(x)$  has only one possible (repeated) factor:  $x^2 + x + 1$ . Well, since  $\text{Char } \mathbb{F}_2 = 2$ , we have Freshman's dream for multiples of 2 and so  $(x^2 + x + 1)^2 = ((x^2) + (x + 1))^2 = x^4 + x^2 + 2x + 1 = x^4 + x^2 + 1 \neq x^4 + x^3 + 1 = p(x)$ , a contradiction. So  $p(x)$  must be irreducible over  $\mathbb{F}_2$ .

Since  $p(x)$  is monic and irreducible,  $\langle p(x) \rangle$  is a maximal ideal, and so  $\mathbb{E} = \mathbb{F}_2[x]/\langle x^4 + x^3 + 1 \rangle$  is a field extension that is also a 4-dimensional  $\mathbb{F}_2$ -vector space. Therefore  $|\mathbb{F}_2[x]/\langle x^4 + x^3 + 1 \rangle|^{2^4} = 16$ . Now we will just use the shorthand  $x := [x]$  since we work in  $\mathbb{E}$  for the remainder of this proof.

$\mathbb{E} = \text{Span}\{1, x, x^2, x^3\}$ . Now, since  $x^4 + x^3 + 1 = 0$  in this field,  $x^4 = -x^3 - 1 = x^3 + 1$ , and obviously  $x$  is a root of  $p(x) = x^4 + x^3 + 1$  over  $\mathbb{E}$ . Then, recall that since  $\mathbb{E} \cong \mathbb{F}_{2^4}$ , a finite field with characteristic 2, we must have that the Frobenius endomorphism  $\varphi_2(x) = x^2$  is an automorphism in  $\text{Aut}_{\mathbb{F}_2}(\mathbb{F}_{2^4})$ . So then it permutes roots of any  $f(x) \in \mathbb{F}_2$  in any extension of  $\mathbb{F}_2$  to each other. Therefore, the orbit  $\langle x \rangle \varphi_2 = \{x\} \cup \{x^2\} \cup \{x^4 = x^3 + 1\} \cup \{x^8 = (x^4)^2 = (x^3 + 1)^2 = x^6 + 1 = (x^3 + x^2 + x + 1) + 1 = x^3 + x^2 + x\} \cup \dots = \{x, x^2, x^3 + 1, x^3 + x^2 + x\}$  must be all roots of  $p(x)$  over  $\mathbb{E}$ , since they are four distinct elements and  $p(x)$  has at most four distinct roots.

□

Here's the computation used to find  $x^6$ .  $x^4 = x^3 + 1 \implies x^5 = x(x^4) = x(x^3 + 1) = x^4 + x = x^3 + x + 1 \implies x^6 = x(x^5) = x(x^3 + x + 1) = x^4 + x^2 + x = (x^3 + 1) + x^2 + x = x^3 + x^2 + x + 1$

**Problem 65.** Prove that an algebraic extension of a perfect field is a perfect field.

*Proof.* Let  $\mathbb{K}$  be a perfect field. If  $\mathbb{K}$  has characteristic 0, then so does any extension of it since they share 1, and so any algebraic extension of  $\mathbb{K}$  must be perfect.

If  $\mathbb{K}$  has characteristic  $p > 0$ . Since  $\mathbb{K}$  is perfect, every irreducible polynomial  $f(x)$  over  $\mathbb{K}$  has no repeated roots in some splitting field  $\mathbb{F}_{f(x)}$  of  $f(x)$ . That is, the minimal polynomial of any algebraic element has no repeated linear factors in  $\mathbb{F}_{P(x)}$ .

Therefore, if  $\mathbb{E}$  is some algebraic extension of  $\mathbb{K}$ , then any  $\alpha \in \mathbb{E}$  is algebraic over  $\mathbb{K}$ . Its minimal polynomial  $P_{\alpha, \mathbb{K}}(x)$  over  $\mathbb{K}$  has no repeated roots some splitting field  $\mathbb{F}_{P(x)}$  of  $P(x)$ . Now, since  $\alpha$  is a zero of  $P_{\alpha, \mathbb{K}}(x)$  which also belongs to  $\mathbb{E}[x]$ , the minimal polynomial  $P_{\alpha, \mathbb{E}}(x)$  of  $\alpha$  over  $\mathbb{E}$  must divide  $P_{\alpha, \mathbb{K}}(x)$  over  $\mathbb{E}$ . Therefore,  $P_{\alpha, \mathbb{E}}(x)$  must split completely over  $\mathbb{F}_{P(x)}$  into distinct linear factors as well, since otherwise  $P_{\alpha, \mathbb{K}}(x)$  is divisible by some repeated linear factor of  $P_{\alpha, \mathbb{E}}(x) \mid P_{\alpha, \mathbb{K}}(x) \in \mathbb{F}_{P(x)}[x]$ , a contradiction. So every minimal polynomial over  $\mathbb{E}$  is separable. Since every irreducible polynomial over  $\mathbb{E}$  is simply some minimal polynomial of one of its zeros, which we proved is separable, scaled by some  $c \in \mathbb{E}$ , every irreducible over  $\mathbb{E}$  is also separable. Therefore,  $\mathbb{E}$  is perfect.

□



**Problem 66.** Show that the extension  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$  is Galois. Find its Galois group.