Warm-up (not to be handed in)

[DF], §13.3, exercise 1, §13.4, exercises 1, 2, 3, §13.5, exercises 1, 2, 7, 8, 9.

1. Exercises to be handed in


Solution. \( f(x) = x^3 + x^2 - 2x - 1 \) reduces to \( f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x] \) modulo 2. \( f(x) \) is irreducible because it has no roots in \( \mathbb{F}_2 \). Therefore \( f(x) \) is irreducible and \( [Q(\alpha) : Q] = 3 \). If \( \alpha \) is constructible then there exists a tower of extensions

\[ K_0 = Q \subset K_1 \subset \cdots \subset K_r \]

with \( \alpha \in K_r \) and \( [K_i : K_{i-1}] = 2 \) for all \( i \). It follows that 3 = \([Q(\alpha) : Q]\) divides \([K_r : Q]\) = 2^r. Contradiction.

Exercise 2. Do [DF], §13.4, exercise 5.

Solution. Suppose that every irreducible polynomial in \( \mathbb{F}[x] \) with a root in \( K \) splits over \( K \). Since \( K/F \) is finite, there exist \( \alpha_1, \ldots, \alpha_r \in K \) which generate (or even span) \( K \) over \( F \). Let \( p_i \) be the minimum polynomial of \( \alpha_i \). Then \( K \) is the splitting field of \( p_1 p_2 \cdots p_r \) over \( F \).

Suppose that \( K \) is a splitting field of \( f(x) \in \mathbb{F}[x] \) over \( F \) and \( p(x) \in \mathbb{F}[x] \) is an irreducible polynomial with a root \( \alpha \in K \). Let \( E \) be the splitting field of \( p(x) \) over \( K \). Let \( \beta \in E \) be any root. We have \( F(\alpha) \cong F[x]/(p(x)) \cong F(\beta) \). This isomorphism extends to an isomorphism \( \sigma : E \to E \) by Theorem 27, because \( E \) is the splitting field over \( F(\alpha) \) respectively \( F(\beta) \) of the polynomial \( p(x)f(x) \). Since \( K \) is the splitting field of \( f(x) \), we have \( \sigma(K) = K \). In particular \( \sigma(\alpha) = \beta \in K \). This shows that \( p(x) \) splits over \( K \).


solution.

(a). If \( K_1 \) and \( K_2 \) are the splitting fields over \( F \) of \( f_1(x) \) and \( f_2(x) \) respectively then \( K_1 K_2 \) is clearly the splitting field of \( f_1(x)f_2(x) \).

(b). Suppose that \( p(x) \in F[x] \) is irreducible with a root in \( K_1 \cap K_2 \). Using the previous exercise, we see that \( p(x) \) splits in \( K_1 \) but also splits in \( K_2 \). In other words: all roots of \( p(x) \) lie in \( K_1 \cap K_2 \). Again, using the previous exercise, this implies that \( K_1 \cap K_2 \) is a splitting field over \( \mathbb{F} \).

Solution. Let \( f(x) = x^p - x + a \). Note that \( f(x+1) = (x+1)^p - (x+1) + a = x^p + 1 - x - 1 + a = f(x) \). In particular, if \( \alpha \) is a root of \( f(x) \), then so is \( \alpha + 1 \). Let \( p(x) \) be an irreducible factor of \( f(x) \). Then \( p(x+1) \) is also an irreducible factor. So

\[
q(x), q(x+1), \ldots, q(x+p-1)
\]

are all irreducible factors of \( f(x) \). If they are not all distinct, then \( q(x) = q(x+r) \) for some \( r \neq 0 \). If \( \alpha \) is a root of \( q \) then so are \( \alpha + r, \alpha + 2r \), and so forth. This shows that \( q \) has at least \( p \) distinct roots, \( q(x) = f(x) \) and \( f(x) \) is irreducible and separable. Otherwise, \( q(x)q(x+1) \cdots q(x+p-1) \) divides \( f(x) \), so \( q(x) \) must have degree 1. But clearly \( f(x) \) does not have any roots in \( \mathbb{F}_p \) because

\[
f(\beta) = \beta^p - \beta + a = a \quad \text{for all } \beta \in \mathbb{F}_p.
\]


Solution. Let \( E \) be the splitting field of \( f(x) = f_1(x) \cdots f_r(x) \) over \( K \) where \( f_1, \ldots, f_r \) are distinct and irreducible. Let \( E' \) the field which is generated by the roots of \( f(x) \) over \( F \). Then \( E' \) is a splitting field of \( f(x) \) over \( F \). If \( i \neq j \) then \( f_i(x) \) and \( f_j(x) \) do not have a common root (otherwise \( f_i(x) \) divides \( f_j(x) \) and vice versa, so they would have to be the same). Since \( F \) is perfect, each \( f_i \) has only simple roots. Therefore \( f(x) \) has only simple roots so it is separable. So \( f(x) \) also has only simple roots in \( E \) (because \( E \) contains \( E' \)). If \( f(x) \) had a multiple irreducible factor in its factorization over \( K \), then it also would have a multiple root in \( E \). This is not the case, so \( f(x) \) has no repeated irreducible factor over \( K \).

Hard Exercises (optional, for extra credit)

Exercise 6. Let \( \zeta \) be a 17-th root of unity. Define

\[
\alpha_1 = \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^{-1} + \zeta^{-2} + \zeta^{-4} + \zeta^{-8},
\]

\[
\alpha_2 = \zeta + \zeta^4 + \zeta^{-1} + \zeta^{-4},
\]

and \( \alpha_3 = \zeta + \zeta^{-1} \). Prove that \( \mathbb{Q}(\zeta)/\mathbb{Q}(\alpha_3), \mathbb{Q}(\alpha_3)/\mathbb{Q}(\alpha_2) \mathbb{Q}(\alpha_2)/\mathbb{Q}(\alpha_1), \mathbb{Q}(\alpha_1)/\mathbb{Q} \) are all quadratic field extensions. Conclude that it is possible to construct a regular 17-gon with compass and straightedge.

Harm Derksen, 3067EH, 763 2309
Office hours: MWF 3-4pm.
http://www.math.lsa.umich.edu/~hderksen/math594.w06/index.html