8. Let $f(X) \in k[X]$ be a polynomial of degree n. Let K be its splitting field. Show that $[K : k]$ divides $n!$.

   Proof. Induct on n. This is trivial if $n = 0$, since the splitting field of the constant polynomial is k, which has degree 1, and 1 divides $0! = 1$. So suppose $n > 0$ and the proposition holds for all polynomials of degree at most n. Let f have degree $n + 1$.

   If f is irreducible, then $E = k[X]/(f(X))$ has degree $n + 1$ over k, and f has at least one linear factor $X - \alpha$ over E, where $\alpha = \overline{X}$. By induction, the splitting field of $\frac{f(X)}{X-\alpha}$ over E (which equals that of f over k) is an extension of degree dividing $n!$, since $\frac{f(X)}{X-\alpha}$ has degree at most n. Thus, the degree of K over k divides $(n + 1)!$.

   Suppose now that f is reducible, meaning $f(X) = h(X)g(X)$ where $\deg(h) = r$ and $\deg(g) = s$. By induction, the splitting field K_h of h over k has degree dividing $r!$, and the splitting field of g over K_h has degree dividing the degree of g over K_h, which is less than s, so the degree of K_g over K_h divides $s!$. This latter extension gives the field K, however. So the degree of K over k divides $s!r!$. The degree of the original polynomial f was $n = s + r$, and it is always true that $s!r! \mid (s + r)!$, since this quotient counts the number of ways to choose r items from a set of $s + r$. Thus, $[K : k] \mid s!r! \mid (s + r)! = n$. □

9. Find the splitting field of $X^{p^8} - 1$ over the field $\mathbf{Z}/p\mathbf{Z}$.

   Proof. This is simply $\mathbb{F}_p$, since $X^{p^8} - 1 = (X - 1)^{p^8}$ splits completely over this field. In the case where p is odd, this factorization holds because $(-1)^{p^8} = -1$. If $p = 2$, then $-1 = 1$ in $\mathbb{F}_p$. So this factorization holds for all p. □

10. Let α be a real number such that $\alpha^4 = 5$.

    (a) Show that $\mathbf{Q}(i\alpha^2)$ is normal over $\mathbf{Q}$.

    Proof. The minimal polynomial of $i\alpha^2$ over $\mathbf{Q}$ is $X^2 + 5$, which splits completely as $(X + i\alpha^2)(X - i\alpha^2)$ over this extension. Since this polynomial is irreducible, it does not split over any smaller extension (the only other is $\mathbf{Q}$), so this is the splitting field of $X^2 + 5$, hence is normal. □

    (b) Show that $\mathbf{Q}(\alpha + i\alpha)$ is normal over $\mathbf{Q}(i\alpha^2)$.

    Proof. $\alpha + i\alpha$ satisfies $X^4 + 20$, since $(\alpha + i\alpha)^4 = \alpha^4(1 + i)^4 = -20$. However, over $\mathbf{Q}(i\alpha^2)$ this has a factor of $X^2 + 2i\alpha^2$, which is the minimal polynomial of $\alpha + i\alpha$ over $\mathbf{Q}(i\alpha^2)$. However, this polynomial is irreducible, so $\mathbf{Q}(\alpha + i\alpha)$ is the splitting field of $X^2 + 2i\alpha^2$ over $\mathbf{Q}(i\alpha^2)$. □

    (c) Show that $\mathbf{Q}(\alpha + i\alpha)$ is not normal over $\mathbf{Q}$.

    Proof. The minimum polynomial of $\alpha + i\alpha$ over $\mathbf{Q}$ is $X^4 + 20$, whose roots are $\pm\alpha \pm i\alpha$. However, $\mathbf{Q}(\alpha + i\alpha)$ does not contain $\alpha - i\alpha$. If it did, then it would also contain α, and thus i as well. Since α has degree 4 over $\mathbf{Q}$, $\alpha \in \mathbf{Q}(\alpha + i\alpha)$ would mean $\mathbf{Q}(\alpha) = \mathbf{Q}(\alpha + i\alpha)$, and so $i \in \mathbf{Q}(\alpha) \subseteq \mathbf{R}$, a contradiction. So this extension is not normal. □

11. Describe the splitting fields of the following polynomials over $\mathbf{Q}$, and find the degree of each such splitting field.

    I will give the splitting fields as subfields of $\mathbf{C}$.

    (a) $X^2 - 2$
    $\mathbf{Q}(\sqrt{2})$, degree 2.

    (b) $X^2 - 1$
    $\mathbf{Q}$, degree 1.

    (c) $X^3 - 2$
    $\mathbf{Q}(\sqrt[3]{2}, \omega)$ where $\omega = \frac{-1+\sqrt{-3}}{2}$, degree 6.

Proof. The roots are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$. $X^3 - 2$ is irreducible over $\mathbf{Q}$, so $\mathbf{Q}(\sqrt[3]{2})$ has degree 3. The minimum polynomial for ω is $X^2 + X + 1$, which is also irreducible over $\mathbf{Q}(\sqrt[3]{2})$, and so the total extension has degree $2 \cdot 3 = 6$. $\square$

(d) $(X^3 - 2)(X^2 - 2)$
$\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)$, degree 12.

Proof. This is simply the compositum of the fields from (a) and (c). Since $\sqrt{2} \notin \mathbf{Q}(\sqrt[3]{2}, \omega)$, the total degree must be $2 \cdot 6 = 12$. $\square$

(e) $X^2 + X + 1$
$\mathbf{Q}(\omega)$, degree 2.

Proof. The only roots are $\pm\omega$, which are not in $\mathbf{Q}$. $\square$

(f) $X^6 + X^3 + 1$
$\mathbf{Q}(\zeta_9)$ where $\zeta_9 = e^{\frac{2\pi i}{9}}$, degree 6.

Proof. The roots of this polynomial are the primitive 9th roots of unity, which are ζ_9^k for k relatively prime to 9. This is because each of these cubes to a primitive cube root of unity, and $X^6 + X^3 + 1 = (X^3)^2 + (X^3) + 1$. $\square$

(g) $X^5 - 7$
$\mathbf{Q}(\sqrt[5]{7}, \zeta_5)$, $\zeta_5 = e^{\frac{2\pi i}{5}}$, degree 20.

Proof. The roots are $\zeta_5^k \sqrt[5]{7}$ for $0 \leq k \leq 4$. $\sqrt[5]{7}$ has degree 5 over $\mathbf{Q}$ and ζ_5 has degree 4. For $1 \leq k \leq 4$, $\zeta_5^k \notin \mathbf{R}$, so this element has degree 4 over $\mathbf{Q}(\sqrt[5]{7})$ as well. Thus, the extension has degree $4 \cdot 5 = 20$. $\square$

12. Let K be a finite field with p^n elements. Show that every element of K has a unique p-th root in K.

Proof. This is simply a restatement of the fact that the Frobenius endomorphism φ is an automorphism. Recall that $(\alpha+\beta)^p = \alpha^p + \beta^p$ in K (prove using the binomial theorem, p divides $\binom{p}{m}$ if $1 \leq m \leq p-1$). Obviously $(\alpha\beta)^p = \alpha^p\beta^p$. Since $1 \mapsto 1$, the kernel is nonzero. So this map is an embedding. Since K is finite, it is an isomorphism. $\square$

13. If the roots of a monic polynomial $f(X) \in k[X]$ in some splitting field are distinct, and form a field, then $\operatorname{char}(k) = p$ and $f(X) = X^{p^n} - X$ for some $n \geq 1$.

Proof. Let K be the field formed by these roots. K must be finite, since f has finitely many roots. By the uniqueness of finite fields, $K = \mathbb{F}_{p^n}$ for some $n \geq 1$ and some p, which is its characteristic. We know then that

$$f(X) = \prod_{\alpha \in K} (X - \alpha) = \prod_{\alpha \in \mathbb{F}_{p^n}} (X - \alpha) = X^{p^n} - X.$$

$\square$