Solutions for some homework problems

6.4.10 Let K be a field and let f be a monic polynomial with coefficients in K of degree $d > 0$. Then there exists a splitting field E of K whose degree divides $d!$. We prove this by induction on d. If $d = 1$ f splits in K and there is nothing to prove. Assume the theorem true for all d' less than d. Let us first consider the case in which f is irreducible. Then $K' := K[X]/(f)$ is a field in which f has a root, so the image of f in $K'[X]$ can be written as $(X-u)g$, where g has degree $d-1$. The induction hypothesis says that g has a splitting field F such that $[F : K']$ divides $(d-1)!$. Then $[F : K] = [F : K']d$ which divides $d!$.

Now suppose that f is reducible, say $f = gh$, where g has degree r and h has degree s, with r and s less than d. Then g has a splitting field E, and $a := [E : K]$ divides $r!$, by the induction hypothesis. The image of h in $E[X]$ has a splitting field E', and $b := [E' : E]$ divides $s!$, again by the induction hypothesis. Then f splits in E', and in fact it is clear that it can't split in any smaller field, since the roots of f are the roots of h and g. Now the degree of E' over K is ab, which divides $r!s!$. Since $d = r + s$, we know that $r!s!$ divides $d!$ so ab also divides $d!$.

6.5.4 Compute the splitting fields of $X^4 + 2$ and $X^4 - 2$ over $\mathbf{F}_3$.

In the field $\mathbf{F}_3$, $2 = -1$, so the first polynomial is

$$X^4 - 1 = (X - 1)(X + 1)(X^2 + 1).$$

Evidently the splitting field of this is the same as the splitting field of $X^2 + 1$. This polynomial is irreducible, since -1 is not a square mod 3. In the field $\mathbf{F}_3[X]/(X^2 + 1) = \mathbf{F}_9$, the polynomial $X^2 + 1$ has two roots, i and $-i$, and hence it splits. Note that this field has 9 elements, so its multiplicative group is a cyclic group of order 8. Let u be a generator. Then $u^8 = 1$ but $u^4 \neq 1$. Then if we let $v := u^4$, we see that $v^2 = 1$ but $v \neq 1$, hence $v^2 = -1$. Then $u^4 = -1$ and u is a root of the polynomial $X^4 + 1 = X^4 - 2$. In fact the cyclic group of order 8 has exactly 4 generators, so there are 4 such roots, and our polynomial splits.

6.5.11 Prove that if $a \in \mathbf{F}_p^*$, then the polynomial $f := X^p - X + a$ is irreducible in $\mathbf{F}_p[X]$.

Indeed, suppose that g is a monic irreducible factor of f and consider the field $E := \mathbf{F}_p[X]/(g)$. Recall that the map $\phi\colon E \to E$ defined by $\phi(e) = e^p$ is an automorphism of E over $\mathbf{F}_p$ (the Frobenius automorphism). It follows that ϕ maps roots of g into roots of g: if $e \in E$ and $g(e) = 0$, then $g(e^p)$ is also zero. But if $g(e) = 0$, $f(e) = 0$, hence $e^p = e - a$. Thus $e - a$ is also a root of g. Repeating this argument, we see that $e - a - a = e - 2a$ is a root, and in fact $e - ia$ is a root of g for every i. Since $a \in \mathbf{F}_{\mathbf{p}}^*$, $e - ia \neq e - ja$ if i and j are not congruent modulo p. This means that g has at least p roots, hence has degee at least p, hence $g = f$.

9.1.14 Let $S := \mathbf{Z}[\sqrt{2}]$. Prove S^* is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}$.

We do this using exercise 5.1.4, where it is shown that the only elements of finite order are 1 and -1 and that $u := 1 + \sqrt{2}$ has infinite order. Then it will suffice to show that every element S^* is a power of u times ± 1. If $\alpha := m+n\sqrt{2}$ is an element of S, then $\sigma(\alpha) := m-n\sqrt{2} \in S$, and $\sigma\colon S \to S$ is an automorphism of S. If α is a unit, then so is $\sigma(\alpha)$, and hence so is $N(\alpha) := \alpha\sigma(\alpha) = m^2 - 2n^2$. Hence $m^2 - 2n^2 = \pm 1$. Then $\phi(\alpha) = \pm\alpha^{-1}$, so our claim for α will follow if we prove that $\pm\phi(\alpha)$ or $\pm\alpha$ is a power of u. Thus we may as well assume that m and n are nonnegative. Let F be the set of $\alpha \in S^*$ which are not powers of u and such that m and n are nonnegative. It will suffice to prove that F is empty. If not, choose α from F with m minimal. Since $u^{-1} = -1 + \sqrt{2}$,

$$m' + n'\sqrt{2} := \alpha u^{-1} = (2n - m) + (m - n)\sqrt{2}.$$

Note that $m \geq n$, since otherwise we would have $n^2 > m^2 = 2n^2 \pm 1$, which would imply $n = 0, m = 1$, a contradiction of our assumption that α is not a power of u. Note also that $m \leq 2n$, since otherwise we would have $2n < m$, hence $4n^2 < m^2 = 2n^2 \pm 1$, hence $2n^2 < 1$, which again would imply $n = 0$. Thus m' and n' are still nonnegative. Furthermore $m' = 2n - m < m$ since otherwise we would have $m \leq 2n - m$ hence $m \leq n$, hence $m = n$ and hence $m = 1$ and $\alpha = u$, a contradiction. Since $m' < m$, $\alpha' := m' + n'\sqrt{2}$ is not in F. Since it is a unit of S, it must be a power of u, and since $\alpha = u\alpha'$, α is also a power of u. Contradiction.