Solutions to HW3

1. (a) $h(x) = x(x+1)(x^3+x+1)(x^3+x^2+1)$

   (b) $h(x) = (x-0)(x-1)(x-\theta)(x-\theta^2)(x-\theta^3)(x-\theta^4)(x-\theta^5)(x-\theta^6)$

   In (b), note that $h(x)$ is the product of linear factors $x-\alpha$ as α varies over all elements $\alpha \in E$. In general, for any finite field E of order q, the polynomial $h(x) = x^q - x$ factors into q linear factors, one factor $x-\alpha$ for each $\alpha \in E$; thus the roots of $h(x)$ are exactly the elements of E. Since our field has characteristic two, the minus signs reduce to plus signs; but I have written '$-$' to emphasize the pattern which holds in the general case.

   In (a), note that the irreducible factors of $h(x)$ in $F[x]$ are precisely the irreducible monic polynomials of degree dividing $[E:F] = 3$. Again, this is not a coincidence. Also observe the way that σ permutes the elements of E:

   - The root of x is 0, which is fixed by σ; namely $\sigma(0) = 0$.
   - The root of $x+1$ is 1, which is fixed by σ; namely $\sigma(1) = 1$.
   - The roots of x^3+x+1 are cycled by σ, namely $\sigma : \theta \mapsto \theta^2 \mapsto \theta^4 \mapsto \theta$.
   - The roots of x^3+x^2+1 are cycled by σ, namely $\sigma : \theta^3 \mapsto \theta^6 \mapsto \theta^5 \mapsto \theta^3$.

2. (a) If $f(x) = (x-a)(x^3+bx^2+cx+d)$ with $a,b,c,d \in \mathbb{Z}$, then $ad = -2$, so $a \in \{\pm 1, \pm 2\}$. This cannot hold since $f(\pm 1) = -1$ and $f(\pm 2) = 2$. So any nontrivial factorization of $f(x)$ has the form $f(x) = (x^2+ax+b)(x^2-ax+b)$ with $a,b \in \mathbb{Z}$, a form that is required in order to avoid terms of degree 1 or 3 in $f(x)$. But then $f(0) = b^2 = 2$, which is impossible for $b \in \mathbb{Z}$. This shows that $f(x)$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

   (b) Completing the square, then factoring as a difference of squares,

   $$\begin{aligned} f(x) &= x^4 - 4x^2 + 2 = (x^2-2)^2 - 2 = (x^2 - 2 - \sqrt{2})(x^2 - 2 + \sqrt{2}) \\ &= (x^2-\alpha^2)(x^2-\beta^2) = (x-\alpha)(x-\beta)(x+\alpha)(x+\beta). \end{aligned}$$

   (I have listed the four roots in the order that they are permuted by σ.)

   (c) From $\alpha \in E$, we obtain $\sqrt{2} = \alpha^2 - 2 \in E$.

   (d) From $\alpha \in E$, we obtain $\beta = \alpha^3 - 3\alpha \in E$. This is the unique simplest expression for β as a polynomial in α, and it can be obtained in many different ways. In fact, $\alpha\beta = \sqrt{2} = \alpha^2 - 2$, giving $\beta = \alpha - \frac{2}{\alpha} \in E$ directly. But to write this as a polynomial in α, we can divide $\alpha^4 - 4\alpha^2 + 2 = 0$ by α to obtain $\frac{2}{\alpha} = 4\alpha - \alpha^3$. Substitute this into the previous expression for β to obtain $\beta = \alpha^3 - 3\alpha$.

(e) Since $\beta \in E = \mathbb{Q}[\alpha]$, we have $\mathbb{Q}[\beta] \subseteq E$. The reverse inclusion $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\beta]$ can be proved in exactly the same way, either using $\alpha = \frac{\sqrt{2}}{\beta}$ or $\alpha = 3\beta - \beta^3$.

(f) Using (e), observe that $\sigma(\beta) = \sigma(\alpha^3 - 3\alpha) = \sigma(\alpha)^3 - 3\sigma(\alpha) = \beta^3 - 3\beta^3 = -\alpha$. So $\sigma(\sqrt{2}) = \sigma(\alpha\beta) = (\beta)(-\alpha) = -\sqrt{2}$. Alternatively, $\sigma(\sqrt{2}) = \sigma(\alpha^2 - 2) = \beta^2 - 2 = -\sqrt{2}$.

(g) See (f): $\sigma(\beta) = -\alpha$.

(h) This is a cyclic group of order 4 since σ cycles the four roots of $f(x)$ in a 4-cycle as $\alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta \mapsto \alpha$.

(i) Exactly three subfields: $E \supset \mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$. These correspond to the subgroups of $G = \langle\sigma\rangle = \{\iota, \sigma, \sigma^2, \sigma^3\}$, namely $\langle\iota\rangle \subset \langle\sigma^2\rangle \subset G$ respectively. That is, the fixed field of ι is E; the fixed field of σ^2 is $\mathbb{Q}[\sqrt{2}]$; and the fixed field of G is $\mathbb{Q}$.