MA 3419: Galois theory
Selected answers/solutions to the assignment due October 31, 2017

1. We have $\alpha = \beta^3 - \beta$, and $\alpha^3 - \alpha - 1 = 0$. Substituting the expression for α, we obtain $(\beta^3-\beta)^3 - (\beta^3-\beta) - 1 = 0$, or $\beta^9 - 3\beta^7 + 3\beta^5 - 2\beta^3 + \beta - 1 = 0$.

An alternative solution (which is better for more general problems): let $\alpha_1, \alpha_2, \alpha_3$ be all the three roots of $x^3 - x - 1$. We consider the polynomial

$$(x^3 - x - \alpha_1)(x^3 - x - \alpha_2)(x^3 - x - \alpha_3),$$

expand it, and use the Vieta theorem according to which

$$\begin{gathered}\alpha_1 + \alpha_2 + \alpha_3 = 0,\\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -1,\\ \alpha_1\alpha_2\alpha_3 = 1.\end{gathered}$$

This gives the polynomial above.

2. By Tower Law, we have

$$\begin{aligned}m[k(\alpha,\beta)\colon k(\alpha)] = [k(\alpha,\beta)\colon k(\alpha)][k(\alpha)\colon k] = [k(\alpha,\beta)\colon k] =\\ = [k(\alpha,\beta)\colon k(\beta)][k(\beta)\colon k] = [k(\alpha,\beta)\colon k(\beta)]n,\end{aligned}$$

and the statement follows. For $\alpha = \sqrt[3]{2}$ and $\beta = \omega\sqrt[3]{2}$ we have $[k(\alpha)\colon k] = [k(\beta)\colon k] = 3$, but $[k(\alpha,\beta)\colon k(\alpha)] = 2$. (We have $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha,\omega)$, the minimal polynomial of ω over $\mathbb{Q}$ is $x^2 + x + 1$, and this polynomial has no real roots so it cannot split in $\mathbb{Q}(\alpha)$).

3. The roots of $x^4 - 2$ are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$, so the field generated by those roots if $\mathbb{Q}(\sqrt[4]{2}, i)$. Note that $[\mathbb{Q}(\sqrt[4]{2})\colon \mathbb{Q}] = 4$ since $x^4 - 2$ is irreducible by Eisenstein, and this extension contains only real numbers, so $[\mathbb{Q}(\sqrt[4]{2}, i)\colon \mathbb{Q}(\sqrt[4]{2})] = 2$, and hence by Tower Law $[\mathbb{Q}(\sqrt[4]{2}, i)\colon \mathbb{Q}] = 8$. As a basis we can take the elements $1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}, i, i\sqrt[4]{2}, i\sqrt[4]{4}, i\sqrt[4]{8}$; these elements manifestly form a spanning set, and the degree computation shows that they are linearly independent.

4. Since the splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$, each Galois group element is completely determined by the action on $\sqrt[4]{2}$ and on i: $\sqrt[4]{2}$ is sent to $i^l\sqrt[4]{2}$, where $0 \leqslant i \leqslant 3$, and i is sent to $\pm i$. There must be 8 elements in the Galois group, so all these are well defined automorphisms. It is easy to identify this group as the dihedral group D_4, and moreover there is a clear explanation of the isomorphism. Indeed, if we consider in the complex plane the square formed by the roots of $x^4 - 2$, then the Galois group action on the roots is manifestly the group of symmetries of that square: the element σ for which $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\sigma(i) = i$, implements the rotation of the square, while the element τ for which $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$, $\tau(i) = -i$ implements the reflection about the diagonal.

5. Suppose that p is coprime to $[K : k]$. This implies that $x^p - a$ cannot be irreducible over k, or else K contains a subfield $k(\sqrt[p]{a})$ of degree p over k, in contradiction with the tower law. Thus, in $k[x]$ we have $x^p - a = f(x)g(x)$. All roots of $x^p - a$ in its splitting field are of the form $\sqrt[p]{a}\xi$, where ξ is a p-th root of 1. Thus, the constant term of $f(x)$ is $\sqrt[p]{a}^d\zeta$, where $0 < d < p$ is the degree of $f(x)$, and ζ is a p-th root of 1. We have $dx + py = 1$ for some $x, y \in \mathbb{Z}$, so $(\sqrt[p]{a}^d\zeta)^x = \sqrt[p]{a}^{1-py}\zeta^x = \sqrt[p]{a}a^{-y}\zeta^x$ is an element of k, and therefore $\sqrt[p]{a}\zeta^x$ is an element of k, that is $x^p - a$ has a root in k.

6. Yes, since $\mathbb{F}_8$ is normal (it is the splitting field of $x^8 - x$ over $\mathbb{F}_2$) and separable (since every element of a finite field of characteristic p is a p-th power, so a result from class applies). The Galois group of this extension is cyclic of order 3, generated by the automorphism $x \mapsto x^2$. (The degree of the extension is 3, hence the group is cyclic of order 3, hence we just need to find one nontrivial automorphism to generate it).