SOLUTIONS TO QUIZ 2

Question 1. Let $g \in K[t]$ be the minimal polynomial of α over K. Then we know that $[K(\alpha) : K] = \deg g$. On the other hand, α is a root of f, hence by minimality of g we have that g divides f.

If $f = g$ we see immediately that $[K(\alpha) : K] = \deg f$. In the other direction, if $[K(\alpha) : K] = \deg f$ then $\deg g = \deg f$ so that $f = g$ (up to a scalar).

Question 2. Let $\alpha = \sqrt{5} + \sqrt{7}$. We compute in $\mathbb{Q}(\sqrt{5}, \sqrt{7})$:

$$\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \sqrt{5} + \sqrt{7} \\
\alpha^2 &= 12 + 2\sqrt{35} \\
\alpha^4 &= 284 + 48\sqrt{35}
\end{aligned}$$

so we see that $\alpha^4 - 24\alpha^2 + 4 = 0$, so α is a root of the polynomial $t^4 - 24t^2 + 4$.

Since we already know that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5}, \sqrt{7})$ (see, e.g. Quiz 1) and that $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = 4$ we deduce that the degree of the minimal polynomial of α over $\mathbb{Q}$ is 4. Hence $t^4 - 24t^2 + 4$ is the minimal polynomial of α.

Question 3. Let $\alpha = \sqrt{2 + \sqrt{3}}$. Then $\alpha^2 = 2 + \sqrt{3} \in \mathbb{Q}(\sqrt{3})$. First, we show that $\alpha \notin \mathbb{Q}(\sqrt{3})$, hence $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 2$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Indeed, if $\alpha \in \mathbb{Q}(\sqrt{3})$, there were $a, b \in \mathbb{Q}$ such that $(a + b\sqrt{3})^2 = 2 + \sqrt{3}$. Writing the equations, we get

$$\begin{aligned}
a^2 + 3b^2 &= 2 \\
2ab &= 1
\end{aligned}$$

so that $b = 1/2a$. Substituting this, we get that $a^2 + \frac{3}{4a^2} = 2$, or $4a^4 - 8a^2 + 3 = 0$. Solving for a^2, we see that $a^2 = 1 \pm \frac{1}{2}$, which is impossible for $a \in \mathbb{Q}$.

Now $2 + \sqrt{3}$ is a root of the polynomial $t^2 - 4t + 1$ over $\mathbb{Q}$, so α is a root of $f(t) = t^4 - 4t^2 + 1$, and since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, it follows that $f(t)$ is the minimal polynomial of α over $\mathbb{Q}$.

The (other) roots of $f(t)$ are $\pm\sqrt{2 + \sqrt{3}}, \pm\sqrt{2 - \sqrt{3}}$ (because $2 - \sqrt{3}$ is the other root of $t^2 - 4t + 1$). We show that these roots are in $\mathbb{Q}(\alpha)$. Indeed, $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$, so that $1/\alpha$ is a square root of $2 - \sqrt{3}$, and the four roots of $f(t)$ are $\alpha, -\alpha, \alpha^{-1}, -\alpha^{-1}$. It follows that $\mathbb{Q}(\alpha)$ is the splitting field of the separable polynomial $f(t)$ over $\mathbb{Q}$, hence the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois.

The Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ has four elements and acts transitively on the roots, so the two possibilities are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. We know that if L/K is normal and α, β are roots of an irreducible polynomial over

K, there exists an automorphism of L/K moving α to β, so the four automorphisms in $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ are determined by the root of $f(t)$ they map α to.

Define σ, τ by $\sigma(\alpha) = -\alpha$ and $\tau(\alpha) = 1/\alpha$. Then $\sigma^2(\alpha) = \alpha$ and $\tau^2(\alpha) = \alpha$ so that σ, τ are two elements of order 2. It follows that the Galois group is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, consisting of $\{id, \sigma, \tau, \sigma\tau = \tau\sigma\}$.

Question 4. (a) Since α is a root of the polynomial $t^2 - \alpha^2 \in F(\alpha^2)[t]$, we have $[F(\alpha) : F(\alpha^2)] \leq 2$. If the degree were 2, then by multiplicity of degrees, $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$ would be even, a contradiction. Hence the degree is 1, which is equivalent to $\alpha \in F(\alpha^2)$.

(b) Let $1 \leq i \leq n$. As before, since α is a root of the polynomial $t^i - \alpha^i \in F(\alpha^i)[t]$, we have $[F(\alpha) : F(\alpha^i)] \leq i$. Suppose the latter degree is $1 < j \leq i$. Then by multiplicity of degrees, $[F(\alpha) : F] = [F(\alpha) : F(\alpha^i)][F(\alpha^i) : F]$ would be divisible by j, contradicting the assumption that $[F(\alpha) : F]$ is prime to $n!$. Thus we must have $[F(\alpha) : F(\alpha^i)] = 1$ so that $\alpha \in F(\alpha^i)$.

Applying the argument for all $1 \leq i \leq n$, we see that $\alpha \in \bigcap_{i=1}^n F(\alpha^i)$.

(c) Consider $\omega = \exp 2\pi i/3$. Then ω is a third root of unity which is a root of the irreducible polynomial $t^2 + t + 1 \in \mathbb{Q}[t]$. Thus $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ is prime to 3, but $\omega \notin \mathbb{Q}(\omega^3) = \mathbb{Q}$.

Question 6. (a) If α is a root of f, then $\alpha^p - \alpha - a = 0$. Consider $\alpha + 1$. We have $(\alpha+1)^p - (\alpha+1) - a = \alpha^p + 1 - \alpha - 1 - a = \alpha^p - \alpha - a = 0$, hence $\alpha + 1$ is also a root of f. Applying the argument again, we see that $\alpha, \alpha+1, \alpha+2, \ldots, \alpha+(p-1)$ are all roots of f. Since $\deg f = p$ and we found p roots, these are all the roots of f.

(b) Assume that f has no roots in F, and consider the splitting field E of f. By (a), if α is a root of f in E, we have a splitting $f(t) = (t-\alpha)(t-\alpha-1)\cdot\ldots\cdot(t-\alpha-p+1)$ in $E[t]$. If $g(t) \in F[t]$ is a nontrivial factor of f, then we must have (in $E[t]$) $g(t) = \prod_{i \in I}(t - \alpha - i)$ for a subset $I \subsetneq \{0, 1, \ldots, p-1\}$. But the coefficient of $t^{|I|-1}$ in the product $\prod_{i\in I}(t-\alpha-i)$ is equal to minus the sum $\sum_{i\in I}(\alpha + i) = |I|\alpha + \sum_{i\in I} i$.

Since $g(t) \in F[t]$, the coefficient of $t^{|I|-1}$ lies in F, so that $|I|\alpha + \sum_{i \in I} i \in F$. But $\mathbb{F}_p \subset F$, so $|I|\alpha \in F$. Since I is nontrivial, $0 < |I| < p$ and it follows that $\alpha \in F$, contradicting our assumption that f has no roots in F.

(c) Let $L = F[t]/(f)$. Then L has a root α of f (namely, the image of t) and $L = F(\alpha)$. By (a), it has all the other roots $\alpha + i$ for $i \in \mathbb{F}_p$. Hence f splits in L, and from $L = F(\alpha)$ we get that L is the splitting field of f over F, therefore L/F is normal. Since f is of degree p and has p distinct roots in L, it is separable, thus α is separable over F and $L = F(\alpha)$ is separable over F. Thus L/F is Galois.

Since $[L : F] = [F(\alpha) : F] = \deg f = p$ (because f is irreducible by (b)), we get by Galois theorem that $\mathrm{Gal}(L/F)$ is of order p and therefore it is cyclic of order p. A generator σ for $\mathrm{Gal}(L/F)$ is defined by $\sigma(\alpha) = \alpha + 1$.

Question 7. (a) Since α is a root of $t^3 + at + b$, we can divide by $t - \alpha$ and get $t^3 + at + b = (t-\alpha)(t^2 + \alpha t + \alpha^2 + a)$. Now $K(\alpha)/K$ is normal if and only if $t^2 + \alpha t + \alpha^2 + a = 0$ has a solution in $K(\alpha)$; Indeed, if there is a solution, $K(\alpha)$ is the splitting field of $t^3 + at + b$ over K, hence normal over K. If there is no solution, then the irreducible polynomial $t^3 + at + b$ has a solution but does not split in $K(\alpha)$, and $K(\alpha)/K$ is not normal.

Since $\operatorname{char} K \neq 2$, we can use the formula for the solution of a quadratic equation and express the solutions of $t^2 + \alpha t + \alpha^2 + a = 0$ as

$$\frac{-\alpha \pm \sqrt{\alpha^2 - 4(\alpha^2 + a)}}{2}$$

It follows that the solutions are in $K(\alpha)$ if and only if the element $-3\alpha^2 - 4a$ is a square in $K(\alpha)$.