SOLUTIONS TO QUIZ 1

Question 1. If $f(x) \in F[x]$ is a polynomial over a field F and $0 \neq a, b \in F$ are scalars, then $f(x)$ is irreducible if and only if $f(ax+b)$ is irreducible. So to prove irreducibility it is enough to consider an appropriate linear substitution. Let $f(x) = x^4 - 8x^3 + 17x^2 - 4x + 2$. In an attempt to get rid of the coefficient of x^3 we substitute $x+2$. We get that $f(x+2) = x^4 - 7x^2 + 14$ which is irreducible by Eisenstein's criterion with the prime 7.

Question 2. $\alpha = \sqrt[5]{7}$, $K = \mathbb{Q}(\alpha)$.

(a) $[K : \mathbb{Q}] = 5$. The degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is equal to the degree of the minimal polynomial of α over $\mathbb{Q}$. Consider the polynomial $p(t) = t^5 - 7 \in \mathbb{Q}[t]$. It is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with the prime 7, and has α as a root. It follows that $p(t)$ is the minimal polynomial of α over $\mathbb{Q}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg p = 5$.

(b) The extension $K/\mathbb{Q}$ is not normal. It is enough to find an irreducible polynomial in $\mathbb{Q}[t]$ which has a root in K but does not split in K. We take $p(t) = t^5 - 7$ which is irreducible by (a). Let $\zeta = e^{2\pi i/5}$. Then $\zeta^5 = 1$ so the roots of p in $\mathbb{C}$ are $\alpha, \zeta\alpha, \zeta^2\alpha, \zeta^3\alpha, \zeta^4\alpha$. Now $\alpha \in K$ but $\zeta\alpha \notin K$ because $\alpha \in \mathbb{R}$ hence $K = \mathbb{Q}(\alpha) \subset \mathbb{R}$ but $\zeta \notin \mathbb{R}$ so that $\zeta\alpha \notin \mathbb{R}$.

Question 3. (a) Obviously $\sqrt{p} + \sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$ so that $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is a field containing $\mathbb{Q}$ and $\sqrt{p} + \sqrt{q}$. Since $\mathbb{Q}(\sqrt{p} + \sqrt{q})$ is the minimal field with this property, we have $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$. To prove the opposite inclusion, note that

$$(\sqrt{p} + \sqrt{q}) \cdot (\sqrt{p} - \sqrt{q}) = p - q \in \mathbb{Q}$$

hence $\sqrt{p} - \sqrt{q} \in \mathbb{Q}(\sqrt{p} + \sqrt{q})$. But

$$2\sqrt{p} = (\sqrt{p} + \sqrt{q}) + (\sqrt{p} - \sqrt{q}) \in \mathbb{Q}(\sqrt{p} + \sqrt{q})$$
$$2\sqrt{q} = (\sqrt{p} + \sqrt{q}) - (\sqrt{p} - \sqrt{q}) \in \mathbb{Q}(\sqrt{p} + \sqrt{q})$$

hence $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(\sqrt{p} + \sqrt{q})$ so that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

(b) A finite extension is normal if and only if it is a splitting field of a polynomial. I claim that $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is a splitting field of the polynomial $(t^2 - p)(t^2 - q)$ over $\mathbb{Q}$. Indeed, the roots of this polynomial, $\pm\sqrt{p}, \pm\sqrt{q}$, are contained in $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, and this field is generated by the roots ($\sqrt{p}$ and $\sqrt{q}$).

(c) To compute the Galois group of $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$, we use two facts on automorphisms (see the Lemmas in the solution to homework 4). The first is that an automorphism σ on an extension $K(\alpha_1, \dots, \alpha_n)/K$ is determined by its action on generators $\alpha_1, \dots, \alpha_n$. In our case these are $\sqrt{p}$ and $\sqrt{q}$. The second fact is that if L/K is an extension and $\alpha \in L$ is a root of a polynomial in $K[t]$, then any automorphism σ of L/K must carry α to a root of the same polynomial. In our case, considering the polynomials $t^2 - p$

and $t^2 - q$ we see that $\sqrt{p}$ must go to $\pm\sqrt{p}$ and the same for $\sqrt{q}$, so there are at most four automorphisms.

To prove that all four possibilities indeed occur, we consider the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt{p})(\sqrt{q})$. Since $\sqrt{q}, -\sqrt{q}$ are roots of the polynomial $t^2 - q$ and this polynomial is irreducible over $\mathbb{Q}(\sqrt{p})$ (because it is of degree 2 and an easy computation shows that its roots do not lie in $\mathbb{Q}(\sqrt{p})$), there exists an automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}(\sqrt{p}))$ such that $\sigma(\sqrt{q}) = -\sqrt{q}$ (and of course, $\sigma(\sqrt{p}) = \sqrt{p}$). Using the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{q}) \subset \mathbb{Q}(\sqrt{q})(\sqrt{p})$ we deduce the existence of an automorphism τ with $\tau(\sqrt{p}) = -\sqrt{p}$ and $\tau(\sqrt{q}) = \sqrt{q}$. We thus get four automorphisms $id, \sigma, \tau, \sigma\tau$ and the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Question 4. (a) *True.* If K is a field, take $L = K(t)$ the field of rational functions over K. Then L/K is a nontrivial extension.

(b) *True.* For any integer $n \geq 1$, consider the polynomial $p_n(t) = t^n - 2 \in \mathbb{Q}[t]$. Then p_n is irreducible over $\mathbb{Q}$ by Eistenstein's criterion with the prime 2. Take $K = \mathbb{Q}[t]/(p_n(t))$. Then K is a field and $[K : \mathbb{Q}] = \deg p_n = n$.

(c) *False.* Take $K = \mathbb{F}_2$. The polynomial $p(t) = t^2 + t + 1 \in \mathbb{F}_2[t]$ is of degree 2 and has no roots in $\mathbb{F}_2$, so it is irreducible over $\mathbb{F}_2$. Take $L = \mathbb{F}_2[t]/(t^2 + t + 1)$. Then L is a field and $[L : K] = \deg p = 2$. Assume that there exists $\alpha \in L$ such that $\alpha^2 = a \in K$. Since $a^2 = a$ for all $a \in K$, we have $0 = \alpha^2 - a = \alpha^2 - a^2 = (\alpha - a)^2$. It follows that $\alpha = a \in K$ so one cannot have $L = K(\alpha)$ (because $L \neq K$).