(iii) Always try the Degree Theorem. And remember that degrees of minpols give degrees of simple extensions. It's tempting to think that $[K(\alpha):K(\alpha^2)]$ must be 2, so how can n be odd?

Since $\alpha^2 \in K(\alpha^2)$, α is a zero of the polynomial $t^2 - \alpha^2$ over $K(\alpha^2)$. Let m be the minimum polynomial of α over $K(\alpha^2)$. Then $\partial m = 1$ or 2.

By the Degree Theorem,

$$\begin{aligned} n = [K(\alpha):K] &= [K(\alpha):K(\alpha^2)][K(\alpha^2):K] \\ &= \partial m \times [K(\alpha^2):K] \end{aligned}$$

and so ∂m divides n. But n is odd, so ∂m cannot be 2, so $\partial m = 1$. Thus $[K(\alpha):K(\alpha^2)] = 1$, and so $K(\alpha) = K(\alpha^2)$.

(iv) By (iii), n must be even. Take the simplest case, $n = 2$ — no good, because then $= K$ or $K(\alpha)$. So try $n = 4$.

Let $\alpha = \sqrt[4]{2}$. The minimum polynomial of α over $\mathbf{Q}$ is $t^4 - 2$, so $n = 4$ and $[\mathbf{Q}(\alpha):\mathbf{Q}] = 4$. But $\alpha^2 = \sqrt{2}$ and $[\mathbf{Q}(\sqrt{2}):\mathbf{Q}] = 2$, so $\mathbf{Q}$ is a proper subset of $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{2})$ is a proper subset of $\mathbf{Q}(\sqrt[4]{2})$.

Question 9

(i) We've done lots of examples like this. It's a question of proving that the four obvious automorphisms really *are* automorphisms, and that there are no more.

The name x is to save writing.

$\mathbf{Q}(\sqrt{5}) \subsetneq \mathbf{R}$, so $i \notin \mathbf{Q}(\sqrt{5})$, so i has minimum polynomial $t^2 + 1$ over $\mathbf{Q}(\sqrt{5})$; the other zero of this is $-i$. By the Automorphism Theorem, there is a $\mathbf{Q}(\sqrt{5})$-automorphism σ of $\mathbf{Q}(\sqrt{5}, i)$ such that $\sigma(i) = -i$.

The standard element of $\mathbf{Q}(\sqrt{5}, i)$ is

$$x = a + b\sqrt{5} + ci + d\sqrt{5}i \quad (a, b, c, d \in \mathbf{Q}),$$

and σ maps x to

$$a + b\sqrt{5} - ci - d\sqrt{5}i.$$

Since $\mathbf{Q}(\sqrt{5}) \neq \mathbf{Q}(\sqrt{5}, i)$, we also know that $\sqrt{5} \notin \mathbf{Q}(i)$, so a similar argument gives a $\mathbf{Q}(i)$-automorphism τ of $\mathbf{Q}(\sqrt{5}, i)$ such that $\tau(\sqrt{5}) = -\sqrt{5}$. Now $\tau(x) = a - b\sqrt{5} + ci - d\sqrt{5}i$. Since σ and τ both fix every element of $\mathbf{Q}$, they are in G; thus so is their product $\sigma\tau$, and

$$\sigma\tau(x) = a - b\sqrt{5} - ci + d\sqrt{5}i.$$

G always contains the identity id, and $id(x) = x$.

Each element of G is determined by its effect on i and on $\sqrt{5}$. But each of these must map to a zero of their own minimum polynomial over $\mathbf{Q}$. There are 2 zeros in each case, so there are at most $2 \times 2 = 4$ $\mathbf{Q}$-automorphisms of $\mathbf{Q}(\sqrt{5}, i)$. We have found 4, so there are no more. Thus

$$G = \{id, \sigma, \tau, \sigma\tau\}.$$

(ii) The answers are quite straightforward, but remember that 'find' means some working has to be shown.

If $\sigma(x) = x$ then

$$ci + d\sqrt{5}i = -ci - d\sqrt{5}i$$

so $2(ci + d\sqrt{5}i) = 0$, giving $c = d = 0$. Hence

$$\begin{aligned} \{id, \sigma\}^\dagger &= \{a + b\sqrt{5} : a, b \in \mathbf{Q}\} \\ &= \mathbf{Q}(\sqrt{5}). \end{aligned}$$

Similarly, $\{id, \tau\}^\dagger = \mathbf{Q}(i)$.

The other non-trivial proper subgroup of G is $\{id, \sigma\tau\}$.

If $\sigma\tau(x) = x$ then

$$b\sqrt{5} + ci = -b\sqrt{5} - ci$$

so $b = c = 0$. Hence

$$\begin{aligned} \{id, \sigma\tau\}^\dagger &= \{a + d\sqrt{5}i : a, d \in \mathbf{Q}\} \\ &= \mathbf{Q}(\sqrt{5}i). \end{aligned}$$

Don't forget the bottom and the top!

$1^\dagger = \mathbf{Q}(\sqrt{5}, i)$, because the identity fixes everything.

If $x \in G^\dagger$ then $\sigma(x) = x$ and $\tau(x) = x$, so $x \in \mathbf{Q}(\sqrt{5}) \cap \mathbf{Q}(i) = \mathbf{Q}$. But $\mathbf{Q} \subseteq G^\dagger$, so $G^\dagger = \mathbf{Q}$.