1. Give complete and precise definitions for the following.

   (a) $\mathbf{F}$ is a field.

   A subset $\mathbf{F} \subseteq \mathbf{C}$ is a field if and only if

   - 1 is an element of $\mathbf{F}$ and
   - if $a, b \in \mathbf{F}$ then $a+b$, $a-b$, ab, and (if $b \neq 0$) a/b are all in $\mathbf{F}$.

   (b) φ is an automorphism of $\mathbf{F}$.

   Let $\mathbf{F}$ be a field. Then a function $\varphi : \mathbf{F} \to \mathbf{F}$ is an automorphism of $\mathbf{F}$ if and only if

   - $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for every $a, b \in F$ and
   - φ is a bijection.

2. Short answer questions. Give brief justifications.

   (a) What is the minimal polynomial of $(1+\sqrt{5})/2$ over $\mathbf{Q}$?

   Let $\theta = (1+\sqrt{5})/2$. Then $\theta - 1/2 = \sqrt{5}/2$, so $(\theta - 1/2)^2 = 5/4$, i.e., $\theta^2 - \theta - 1 = 0$.

   Let $f(x) = x^2 - x - 1$. Then $f(\theta) = 0$. Moreover, $f(x-2) = x^2 - 5x + 5$, which is irreducible over $\mathbf{Q}$ by Eisenstein's criterion with $p = 5$. Therefore, $f(x)$ is also irreducible over $\mathbf{Q}$ and hence $f(x)$ is the minimal polynomial of $(1+\sqrt{5})/2$ over $\mathbf{Q}$.

   (b) Is $\cos(1^\circ)$ algebraic over $\mathbf{Q}$? Why or why not?

   $\cos(1^\circ)$ is algebraic over $\mathbf{Q}$. (Note: "algebraic" is *not* the same as "constructible".) To see this, note that $e^{2\pi i/360} = e^{\pi i/180}$ is algebraic over $\mathbf{Q}$ because it is a root of the polynomial $x^{360} - 1 \in \mathbf{Q}[x]$. Therefore $\mathbf{Q}(e^{\pi i/180})$ is an algebraic extension of $\mathbf{Q}$. As such, any element of $\mathbf{Q}(e^{\pi i/180})$ is algebraic over $\mathbf{Q}$. Finally,

   $$\frac{e^{\pi i/180} + e^{-\pi i/180}}{2} = \frac{\cos(\frac{\pi}{180}) + i\sin(\frac{\pi}{180}) + \cos(\frac{\pi}{180}) - i\sin(\frac{\pi}{180})}{2} = \cos(\tfrac{\pi}{180}) = \cos(1^\circ).$$

   $\mathbf{Q}(e^{\pi i/180})$ is closed under addition and division, so the fact that $e^{-\pi i/180} = 1/e^{\pi i/180}$ implies $\cos(1^\circ) \in \mathbf{Q}(e^{\pi i/180})$, completing the proof.

   Alternatively, we may use a constructablity argument. First, use trigonometric identities to write

   $$\begin{aligned} \cos(3^\circ) &= \cos(1^\circ + 2^\circ) = \cos(1^\circ)\cos(2^\circ) - \sin(1^\circ)\sin(2^\circ) \\ &= \cos(1^\circ)(\cos^2(1^\circ) - \sin^2(1^\circ)) - 2\sin^2(1^\circ)\cos(1^\circ) \\ &= \cos^3(1^\circ) - 3\sin^2(1^\circ)\cos(1^\circ) = 4\cos^3(1^\circ) - 3\cos(1^\circ). \end{aligned}$$

   We saw in homework 4 that that a regular pentagon is constructible, which is equivalent to constructing 72°. We also know that 60° is constructible by the section on trisecting an angle. Since an angle is constructible if and only if its cosine and sine are constructible, we conclude, using the fact that

   $$\cos(12^\circ) = \cos(72^\circ - 60^\circ) = \cos(72^\circ)\cos(60^\circ) - \sin(72^\circ)\sin(60^\circ),$$

   that $\cos(12^\circ)$ is also constructible. Using the half angle formula twice gives

   $$\cos(3^\circ) = \frac{1 - \cos(6^\circ)}{2} = \frac{1 - \frac{1}{2}(1 - \cos(12^\circ))}{2},$$

   which means $\cos(3^\circ)$ is also constructible. By theorem 4 on page 32, this implies that $\cos(3^\circ)$ is algebraic over $\mathbf{Q}$. Let $f(x) \in \mathbf{Q}[x]$ be a nonzero polynomial satisfied by $\cos(3^\circ)$. Then $\cos(1^\circ)$ satisfies the nonzero polynomial $f(4x^3 - 3x)$.

   (c) Is $e^{2\pi i/7}$ constructible? Why or why not?

   Constructing $e^{2\pi i/7}$ is equivalent to constructing a regular 7-gon, which is impossible by lemma 24b since 7 is not a Fermat prime.

(d) True or False: If a polynomial in $\mathbf{Q}[x]$ has no roots in $\mathbf{R}$ then it is irreducible in $\mathbf{Q}[x]$. Explain your answer.

False. Consider the polynomial $f(x) = (x^2+1)^2 \in \mathbf{Q}[x]$, which has no roots in $\mathbf{R}$. This polynomial is not irreducible in $\mathbf{Q}[x]$ since it factors as two polynomials in $\mathbf{Q}[x]$ of lower degree, $(x^2+1)\cdot(x^2+1)$.

3. Suppose that $\mathbf{F}$ is a field, $\mathbf{E}$ is an extension of $\mathbf{F}$, and $[\mathbf{E} : \mathbf{F}] = 2$. Show that there is a $k \in \mathbf{F}$ such that $\mathbf{E} = \mathbf{F}(\sqrt{k})$.

Since $[\mathbf{E} : \mathbf{F}] = 2$, the fields $\mathbf{E}$ and $\mathbf{F}$ are not equal and hence there is some $c \in \mathbf{E}\backslash\mathbf{F}$. Consider the tower of fields $\mathbf{F} \subseteq \mathbf{F}(c) \subseteq \mathbf{E}$. Since $[\mathbf{E} : \mathbf{F}(c)][\mathbf{F}(c) : \mathbf{F}] = [\mathbf{E} : \mathbf{F}] = 2$ and $[\mathbf{F}(c) : \mathbf{F}] \neq 1$, we have $[\mathbf{F}(c) : \mathbf{F}] = 2$ and $[\mathbf{E} : \mathbf{F}(c)] = 1$. The latter degree forces $\mathbf{F}(c) = \mathbf{E}$. $2 = [\mathbf{F}(c) : \mathbf{F}] = \deg_{\mathbf{F}}(c)$, so c satisfies some monic quadratic polynomial $x^2 + bx + d \in \mathbf{F}[x]$. Using the quadratic formula, we have either

$$c = \frac{1 + \sqrt{b^2 - 4ad}}{2} \quad \text{or} \quad c = \frac{1 - \sqrt{b^2 - 4ad}}{2}$$

In either case, $\mathbf{E} = \mathbf{F}(c) = \mathbf{F}(\sqrt{b^2 - 4ad})$. Take $k = b^2 - 4ad$ to complete the proof.

4. (a) Show that $\mathbf{Q}(\sqrt[5]{2}) = \mathbf{Q}(\sqrt[5]{4})$.

First, $\sqrt[5]{4} = \sqrt[5]{2}^2$ so $\sqrt[5]{4} \in \mathbf{Q}(\sqrt[5]{2})$. Since $\mathbf{Q}(\sqrt[5]{4})$ is the smallest field containing both $\mathbf{Q}$ and $\sqrt[5]{4}$, we have $\mathbf{Q}(\sqrt[5]{2}) \supseteq \mathbf{Q}(\sqrt[5]{4})$. On the other hand

$$\sqrt[5]{4}^3 = \sqrt[5]{2^6} = 2\sqrt[5]{2},$$

which implies $\sqrt[5]{2} \in \mathbf{Q}(\sqrt[5]{4})$ and hence $\mathbf{Q}(\sqrt[5]{2}) \subseteq \mathbf{Q}(\sqrt[5]{4})$.

(b) Show that $x^5 - 4$ is irreducible in $\mathbf{Q}[x]$ (Hint: use part a).

$x^5 - 4$ is certainly a polynomial in $\mathbf{Q}[x]$ satisfied by $\sqrt[5]{4}$. The plan here is to show it is the minimal polynomial of $\sqrt[5]{4}$ over $\mathbf{Q}$, from which irreducibility follows by theorem 16. By Eisenstein's criterion at $p = 2$, the polynomial $g(x) = x^5 - 2 \in \mathbf{Q}[x]$ is irreducible over $\mathbf{Q}$. Since $g(\sqrt[5]{2}) = 0$, $g(x)$ is the minimal polynomial of $\sqrt[5]{2}$ over $\mathbf{Q}$. Then using part a we have

$$[\mathbf{Q}(\sqrt[5]{4}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt[5]{2}) : \mathbf{Q}] = 5.$$

Any polynomial in $\mathbf{Q}[x]$ satisfied by $\sqrt[5]{4}$ then must have degree at least 5, which forces $x^5 - 4$ to be the minimal polynomial of $\sqrt[5]{4}$ over $\mathbf{Q}$, and hence irreducible.

5. Suppose a is algebraic over $\mathbf{Q}$, and let $d = [\mathbf{Q}(a) : \mathbf{Q}]$. What are all the possibilities for $[\mathbf{Q}(a^3) : \mathbf{Q}]$? Illustrate your answer with concrete examples.

First, $a^3 \in \mathbf{Q}(a)$ so we have the tower of fields $\mathbf{Q} \subseteq \mathbf{Q}(a^3) \subseteq \mathbf{Q}(a)$. Then

$$d = [\mathbf{Q}(a) : \mathbf{Q}] = [\mathbf{Q}(a) : \mathbf{Q}(a^3)][\mathbf{Q}(a^3) : \mathbf{Q}].$$

Since a satisfies the polynomial $x^3 - a^3 \in \mathbf{Q}(a^3)[x]$, $[\mathbf{Q}(a) : \mathbf{Q}(a^3)] \leq 3$. Therefore $[\mathbf{Q}(a^3) : \mathbf{Q}]$ is either d, $d/2$, or $d/3$.

These three cases are all realizable. For the first, let a be any element of $\mathbf{Q}$. Then $\mathbf{Q} = \mathbf{Q}(a^3) = \mathbf{Q}(a)$ so $[\mathbf{Q}(a) : \mathbf{Q}] = [\mathbf{Q}(a^3) : \mathbf{Q}] = 1$.

For the second case, take $a = \omega$, where ω is a primitive third root of unity. Then from a theorem in lecture, $[\mathbf{Q}(a) : \mathbf{Q}] = \varphi(3) = 2$ where φ is the Euler totient function. In this case $a^3 = 1$, so $\mathbf{Q}(a^3) = \mathbf{Q}$ and $[\mathbf{Q}(a^3) : \mathbf{Q}] = 1$.

For the final case, take $a = \sqrt[3]{2}$ to be the real cube root of 2. In this case, $x^3 - 2$ is irreducible over $\mathbf{Q}$ by Eisenstein at $p = 2$, so $[\mathbf{Q}(a) : \mathbf{Q}] = 3$. However, $a^3 = 1$ so we again have $[\mathbf{Q}(a^3) : \mathbf{Q}] = 1$.