Algebra II. Exercise 13.
Solutions.

1. By multiplying the equation

$$\frac{1}{\sqrt[3]{2}} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

by the number $\sqrt[3]{2}$ we obtain $1 = a\sqrt[3]{2} + b\sqrt[3]{4} + c \cdot 2$, from which we see that $a = b = 0$ and $c = 1/2$. Thus

$$\frac{1}{\sqrt[3]{2}} = \frac{1}{2} \cdot \sqrt[3]{4}.$$

In a similar manner,

$$\frac{\sqrt[3]{2} - 1}{\sqrt[3]{2} - \sqrt[3]{4}} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

$$\Leftrightarrow \sqrt[3]{2} - 1 = a\sqrt[3]{2} + b\sqrt[3]{4} + 2c - a\sqrt[3]{4} - 2b - 2c\sqrt[3]{2}$$

$$\Leftrightarrow \begin{cases} -2b + 2c & = -1 \\ a - 2c & = 1 \\ -a + b & = 0 \end{cases}$$

from which we can solve $a = b = 0$ and $c = -1/2$. Thus

$$\frac{\sqrt[3]{2} - 1}{\sqrt[3]{2} - \sqrt[3]{4}} = -\frac{1}{2} \cdot \sqrt[3]{4}.$$

2. Suppose that L is a finite extension of a field K. We prove that L is finitely generated and algebraic with respect to K.

Denote $[L : K] = n$ and let $\{x_1, ..., x_n\}$ be a basis for L with respect to K. We prove that $L = K(x_1, ..., x_n)$:

Because L is a field, which contains $K, x_1, ..., x_n$, then $K(x_1, ..., x_n) \subset L$. On the other hand, if $a \in L$, then $a = \sum_i a_i x_i$ for some $a_i \in K$, and clearly $a \in K(x_1, ..., x_n)$. Thus $L \subset K(x_1, ..., x_n)$. We have proved that L is finitely generated.

Then we prove that L is algebraic: Let $a \in L$. Because L is finite dimensional as a K-vector space, then the set $(a^i)_{i\in\mathbb{N}}$ cannot be free, and we see that

$$0 = \sum_{i=0}^{k} b_i a^i$$

for some $b_i \in K$, and at least one of the coefficients b_i is $\neq 0$. Thus

$$f = \sum_{i=0}^{k} b_i X^i \quad (\neq 0)$$

is a polynomial, which has a as a root. Hence a is algebraic with respect to K.

3. a) In Example 12.6 (6.6) it was proved that $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, thus $\mathbb{Q}(i)$ is two dimensional as a $\mathbb{Q}$-vector space. In a similar manner we first see that

$$\mathbb{Q}(\sqrt{2}) = \{\frac{a + b\sqrt{2}}{c + d\sqrt{2}} \mid a, b, c, d \in \mathbb{Q};\ c \neq 0 \text{ or } d \neq 0\},$$

and then we see that

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2} \in \mathbb{Q}[\sqrt{2}].$$

Thus $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, which also is two dimensional as a $\mathbb{Q}$-vector space. From this it follows that they are isomorphic as $\mathbb{Q}$-vector spaces (as an isomorphism one can choose for example the linear map for which $1 \mapsto 1$ and $\sqrt{2} \mapsto i$).

Then we prove the latter claim. Suppose the contrary that there exists a field isomorphism $f\colon \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$; denote $f(i) = a + b\sqrt{2},\ a, b \in \mathbb{Q}$. Because $f(1) = 1$, then $f(-1) = -1$ and

$$-1 = f(-1) = f(i^2) = f(i)^2 = (a + b\sqrt{2})^2,$$

which is a contradiction, since $a + b\sqrt{2} \in \mathbb{R}$. Thus a field isomorphism cannot exist.

b) As in item a) we can prove that $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Suppose the contrary that there exists a field isomorphism $f\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$; denote $f(\sqrt{2}) = a + b\sqrt{3}$. Because $f(1) = 1$, then $f(2) = 2$, and we obtain

$$2 = f(2) = f((\sqrt{2})^2) = f(\sqrt{2})^2 = (a + b\sqrt{3})^2 = a^2 + 2ab\sqrt{3} + 3b^2.$$

Hence $a = 0$ or $b = 0$. If $b = 0$, then $a^2 = 2$, which is a contradiction, because $a \in \mathbb{Q}$. On the other hand, if $a = 0$, then $3b^2 = 2$, from which it follows that b^2 is an even number and then also b is even. Then we have $4|3b^2$, that is, $4|2$, which is a contradiction. Both alternatives lead to a contradiction, and thus a field isomorphism cannot exist.

4. a) Let $a \in K(A)$. By Proposition 12.7 (6.7) we have $a \in K(a_1, ..., a_n)$ for some $a_1, ..., a_n \in A$. Because $a_1, ..., a_n$ are algebraic with respect to K, we have that $K(a_1, ..., a_n)$ is a finite extension of K by Proposition 13.8 (7.8), so it is an algebraic extension by Proposition 13.7 (7.7). Thus the element a is algebraic with respect to K. Because the element $a \in K(A)$ was arbitrary, we have that $K(A)/K$ is an algebraic extension.

b) The minimal polynomial of the element $\sqrt[n]{2}$ with respect to $\mathbb{Q}$ is $X^n - 2$ (this is an irreducible polynomial by Eisenstein's criterion). Thus every element of the set A is algebraic with respect to $\mathbb{Q}$, so by item a) we have that $\mathbb{Q}(A)/\mathbb{Q}$ is an algebraic extension.
For every n we have

$$[\mathbb{Q}(A) : \mathbb{Q}] = [\mathbb{Q}(A) : \mathbb{Q}(\sqrt[n]{2})] \cdot [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = [\mathbb{Q}(A) : \mathbb{Q}(\sqrt[n]{2})] \cdot n,$$

hence $[\mathbb{Q}(A) : \mathbb{Q}] \geq n$ for every $n \in \mathbb{N}$. Thus $[\mathbb{Q}(A) : \mathbb{Q}] = \infty$.
Then we prove that the extension $\mathbb{Q}(A)$ is not finitely generated. Assume the contrary that $\mathbb{Q}(A) = \mathbb{Q}(B)$ for some finite set $B \subset \mathbb{Q}(A)$. Because all elements of B are algebraic, we have that $\mathbb{Q}(B)$ is a finite extension by Proposition 13.8 (7.8). This is a contradiction, because by what we proved above, $\mathbb{Q}(A)$ is an infinite extension.

5. a) The map $\tau_b\colon R[X] \to R[X]$ is an evaluation homomorphism, which maps the indeterminate X to the element $X + b$. Thus it is an R-algebra homomorphism, especially a ring homomorphism. It has the inverse map τ_{-b}, so it is an isomorphism.
A ring isomorphism maps units to units, because $\sigma(a)^{-1} = \sigma(a^{-1})$. If $f = gh$ in the ring $R[X]$, then $\tau_b(f) = \tau_b(g)\tau_b(h)$. Now the factorization of the

polynomial f is trivial $\Leftrightarrow$ g or h is a unit $\Leftrightarrow$ $\tau_b(g)$ or $\tau_b(h)$ is a unit $\Leftrightarrow$ the factorization of the polynomial $\tau_b(f)$ is trivial. Thus f is irreducible, if and only if $\tau_b(f)$ is irreducible.

b) Consider the polynomial

$$\tau_1(X^p-1) = (X+1)^p-1 = \left(\sum_{i=0}^{p} \begin{pmatrix} p \\ i \end{pmatrix} X^i\right)-1 = \sum_{i=1}^{p} \begin{pmatrix} p \\ i \end{pmatrix} X^i = X\cdot\sum_{i=0}^{p-1} \begin{pmatrix} p \\ i+1 \end{pmatrix} X^i.$$

The binomial coefficient appearing in the formula is

$$\begin{pmatrix} p \\ i+1 \end{pmatrix} = \frac{p(p-1)\cdots(p-i)}{1\cdot 2\cdots(i+1)}.$$

Because p is a prime number, no factor of the denominator divides p, unless $p = i+1$, that is, $i = p-1$.

Thus the coefficient $\begin{pmatrix} p \\ i+1 \end{pmatrix}$ is divisible by p always, when $0 \leq i < p-1$.

Moreover $\begin{pmatrix} p \\ 1 \end{pmatrix} = p$ is not divisible by p^2. Thus by the Eisenstein criterion, the polynomial

$$h = \sum_{i=0}^{p-1} \begin{pmatrix} p \\ i+1 \end{pmatrix} X^i$$

is irreducible. Now

$$X^p - 1 = \tau_{-1}(X\cdot h) = (X-1)\cdot g,$$

where

$$g = \tau_{-1}(h) = 1 + X + ... + X^{p-1}$$

is irreducible by item a).

6. a) By one of the preliminary exercises we have that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$. As in Example 12.6 (6.6) we see that every element in the extension $\mathbb{Q}(\sqrt{2})(i)$ can be written in the form $(a+bi)/(c+di)$, where $a, b, c, d \in \mathbb{Q}(\sqrt{2})$. Moreover

$$\frac{1}{c+di} = \frac{1}{c^2+d^2}(c-di),$$

so the set $\{1, i\}$ generates the $\mathbb{Q}(\sqrt{2})$-vector space $\mathbb{Q}(\sqrt{2})(i)$. Furthermore we know that $i \notin \mathbb{Q}(\sqrt{2})$, so $\{1, i\}$ is free. Thus $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2$, and by Proposition 12.3 (6.3) we have

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

b) Denote $\omega = e^{2\pi i/5}$. Now ω is a root of the polynomial $X^5 - 1$, so we know that $\min(\mathbb{Q}, \omega) | X^5 - 1$. Now

$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1),$$

and according to the previous exercise the polynomial $g = X^4 + X^3 + X^2 + X + 1$ is irreducible. Because ω is not a root of the polynomial $X - 1$, it has to be a root of g. Because g is irreducible, we have $g = \min(\mathbb{Q}, \omega)$ and thus $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(g) = 4$.

c) Denote $\omega = e^{\pi i/3} = \frac{1}{2} + \frac{\sqrt{3}}{2} i$. Because $i, \omega \in \mathbb{Q}(i, \sqrt{3})$, then $\mathbb{Q}(i, \omega) \subset \mathbb{Q}(i, \sqrt{3})$. On the other hand, from the equation $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2} i$ we can solve $\sqrt{3} = i - 2i\omega$, thus $i, \sqrt{3} \in \mathbb{Q}(i, \omega)$ and hence $\mathbb{Q}(i, \sqrt{3}) \subset \mathbb{Q}(i, \omega)$. Thus $\mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(i, \omega)$. Analogously as in item a) we now obtain that

$$[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$