

Homework 7 Solutions.

§6.1 #12. Assuming that π is transcendental over \mathbb{Q} , show that either $\pi + e$ or $\pi \cdot e$ is transcendental over \mathbb{Q} .

Proof. Suppose, by way of contradiction that

- $\pi + e$ is algebraic over \mathbb{Q} with degree m , and that
- $\pi \cdot e$ is algebraic over \mathbb{Q} with degree n .

Then we have $[\mathbb{Q}(\pi + e, \pi \cdot e) : \mathbb{Q}] \leq mn$. Now, consider $f(x) = x^2 + (\pi + e)x + \pi \cdot e \in \mathbb{Q}(\pi \cdot e, \pi + e)[x]$. Observe that its roots are π and e . Therefore, we have

$$[\mathbb{Q}(\pi, e, \pi \cdot e, \pi + e) : \mathbb{Q}(\pi \cdot e, \pi + e)] = [\mathbb{Q}(\pi, e) : \mathbb{Q}(\pi \cdot e, \pi + e)] \leq 2.$$

It follows that

$$[\mathbb{Q}(\pi, e) : \mathbb{Q}] = [\mathbb{Q}(\pi, e) : \mathbb{Q}(\pi \cdot e, \pi + e)] \cdot [\mathbb{Q}(\pi \cdot e, \pi + e) : \mathbb{Q}] \leq 2mn.$$

Since $\pi \in \mathbb{Q}(\pi, e)$, we see that $[\mathbb{Q}(\pi) : \mathbb{Q}] \leq 2mn$, which implies that π is algebraic over \mathbb{Q} , a contradiction. \square

§6.2 #1. Find the degree and a basis for each of the given field extensions.

(a) $\mathbb{Q}(\sqrt{3})$ over \mathbb{Q} .

Solution: The minimal polynomial of $\sqrt{3}$ over \mathbb{Q} is $f_{\sqrt{3}}(x) = x^2 - 3$. (It is monic and irreducible (3-Eisenstein) with $\sqrt{3}$ as a root.) Hence, we have $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$; a basis is $\{1, \sqrt{3}\}$.

(b) $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ over \mathbb{Q} .

Solution: Part (a) implies that $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. We claim that $\pm\sqrt{7} \notin \mathbb{Q}(\sqrt{3})$. To see this, suppose on the contrary that $\sqrt{7} \in \mathbb{Q}(\sqrt{3})$. Since $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}[\sqrt{3}]$, there exists $a, b \in \mathbb{Q}$ with $\sqrt{7} = a + b\sqrt{3}$. We suppose that $a, b \neq 0$. The case when one of a or $b = 0$ is similar. Squaring gives $49 = a^2 + 2ab\sqrt{3} + 3b^2$, from which it follows that $\sqrt{3} = \frac{49 - (a^2 + 3b^2)}{2ab} \in \mathbb{Q}$, a contradiction. Hence, $x^2 - 7$ is irreducible over $\mathbb{Q}(\sqrt{3})$; it is the minimal polynomial over $\mathbb{Q}(\sqrt{3})$, so we conclude that $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}(\sqrt{3})] = 2$, and that $\{1, \sqrt{7}\}$ is a basis for $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ over $\mathbb{Q}(\sqrt{3})$. We compute

$$[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4;$$

The extension $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ has basis $\{1, \sqrt{3}, \sqrt{7}, \sqrt{3} \cdot \sqrt{7} = \sqrt{21}\}$ over \mathbb{Q} .

(c) $\mathbb{Q}(\sqrt{3} + \sqrt{7})$ over \mathbb{Q} .

Solution: Problem #9 below asserts that $\mathbb{Q}(\sqrt{3} + \sqrt{7}) = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. An alternative approach is as follows. One can verify that $\alpha = \sqrt{3} + \sqrt{7}$ satisfies $f(x) = x^4 - 20x^2 + 16$. It remains to show that $f(x)$ is irreducible over \mathbb{Q} . One can use the Rational Root Theorem to verify that $f(x)$ has no linear factors in $\mathbb{Q}[x]$, and hence, no cubic factors in $\mathbb{Q}[x]$. To show that $f(x)$ has no quadratic factors in $\mathbb{Q}[x]$, we suppose that $\exists a, b, c, d \in \mathbb{Q}$ with

$$f(x) = (x^2 + ax + b)(x^2 + cx + d).$$

Comparing coefficients yields:

$$a + c = 0; \quad b + ac + d = -20; \quad ad + bc = 0; \quad bd = 16.$$

We deduce that $c = -a$; it follows that $ad + bc = a(d - b) = 0$. Therefore, we have either $a = 0$ or $b = d$.

- $a = 0$. If $a = 0$, then $c = -a = 0$. Furthermore, we find that $b + d = -20$. Substituting in $bd = 16$ gives $b(-b - 20) = -b^2 - 20b = 16$, which implies that $b^2 + 20b + 16 = 0$. One can now use the Rational Root Theorem to show that no such $b \in \mathbb{Q}$ exists.
- $b = d$. If $b = d$, then $b = \pm 4$. If $b = 4$, we have $b + ac + d = 8 - a^2 = -20$ which gives $a^2 = 28$; no such $a \in \mathbb{Q}$ exists. If $b = -4$, we have $b + ac + d = -8 - a^2 = -20$ which gives $a^2 = 12$; again, no such $a \in \mathbb{Q}$ exists.

We conclude that $f(x)$ is irreducible. Hence, it is the minimal polynomial of α over \mathbb{Q} . We now have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. A basis for $\mathbb{Q}(\alpha)$ over \mathbb{Q} is $\{1, \alpha, \alpha^2, \alpha^3\}$.

(d) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ over \mathbb{Q} .

Solution: We observe that

$$\begin{aligned} 2 &= [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \\ 3 &= [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]. \end{aligned}$$

Since $\gcd(2, 3) = 1$, we find that $6 \mid [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}), \mathbb{Q}]$, so $6 \leq [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. On the other hand, we note that

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

We conclude that $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

To write down a basis, note that

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 6,$$

so we have $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ with basis $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$, and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ with basis $\{1, \sqrt{2}\}$. Therefore, a basis for the degree 6 field over \mathbb{Q} is obtained by multiplying the bases together:

$$\{1, \sqrt{2}, \sqrt[3]{2}, \sqrt[3]{2}^2, \sqrt{2}\sqrt[3]{2}, \sqrt{2}\sqrt[3]{2}^2\}$$

Alternatively, one could take for a basis:

$$= \{1, 2^{1/6}, 2^{1/3}, 2^{1/2}, 2^{2/3}, 2^{5/6}\}.$$

§6.2 #3. Find the degree of $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$ over \mathbb{Q} .

Solution: We observe:

$$3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) : \mathbb{Q}]$$

$$4 = [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) : \mathbb{Q}].$$

Since $\gcd(3, 4) = 1$, we see that $3 \cdot 4 = 12 \mid [\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) : \mathbb{Q}]$. It follows that $12 \leq [\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) : \mathbb{Q}]$. On the other hand, we compute

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 3 \cdot 4 = 12.$$

Therefore, we conclude that $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}) : \mathbb{Q}] = 12$.

§6.2 #4. Let F be a finite extension of K such that $[F : K] = p$ is prime. If $u \in F \setminus K$, show that $F = K(u)$.

Proof. We first note that $K \subseteq K(u) \subseteq F$. Since $u \notin K$, we have $K \neq K(u)$, so $[K(u) : K] > 1$. But also, we have $[K(u) : K] \mid [F : K] = p$. Now, $[K(u) : K] \neq 1$, implies that $[K(u) : K] = p$. Multiplicativity of degrees in towers gives $[F : K(u)] = 1$; hence we conclude that $F = K(u)$. \square

§6.2 #5. Let $f(x)$ be an irreducible polynomial in $K[x]$. Show that if F is an extension field of K such that $\deg(f(x))$ is relatively prime to $[F : K]$, then $f(x)$ is irreducible in $F[x]$.

Proof. Without loss of generality, suppose that $f(x)$ is monic. (If not, we divide $f(x)$ by an appropriate $c \in K \setminus \{0\}$ (a unit) to make it monic.) Let u be a root of the polynomial $f(x)$. Then $f(x) = f_{K,u}(x)$ is the minimal polynomial of u over K . We compute $[F(u) : K]$ in two ways:

$$[F(u) : F] \cdot [F : K] = [F(u) : F] = [F(u) : K(u)] \cdot [K(u) : K].$$

It follows that $[K(u) : K] \mid [F(u) : F] \cdot [F : K]$. By hypothesis, $\deg(f_{K,u}(x)) = [K(u) : K]$ is relatively prime to $[F : K]$. Therefore, we have $[K(u) : K] \mid [F(u) : F]$; we note that $[K(u) : K] \leq [F(u) : F]$. But $K \subseteq F$ implies that $f_{F,u}(x) \mid f_{K,u}(x)$ in $F[x]$, so $\deg(f_{K,u}(x)) = [K(u) : K] \geq [F(u) : F] = \deg(f_{F,u}(x))$. Hence, we have $\deg(f_{F,u}(x)) = \deg(f_{K,u}(x))$. Since $f_{F,u}(x) \mid f_{K,u}(x)$ and both polynomials are monic, we conclude that $f_{K,u}(x) = f_{F,u}(x)$. I.e., as the minimal polynomial of u over F , $f(x) = f_{K,u}(x)$ is irreducible over F . \square

§6.2 #7. Let $F \supseteq K$ be fields, and let R be a ring such that $F \supseteq R \supseteq K$. If F is an algebraic extension of K , show that R is a field. What happens if we do not assume that F is algebraic over K ?

Proof. Suppose that $R \neq K$, and let $r \in R \setminus K$. Then $r \neq 0$. Since $r \in R \subseteq F$, r is algebraic over K : let $f_{K,r}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in K[x]$ be the minimal polynomial of r over K . Since $f_{K,r}(x)$ is irreducible, we have $a_0 \neq 0$. Therefore, $f_{K,r}(r) = 0$ implies that

$$r \cdot \left(\left(\frac{-1}{a_0} \right) r^{n-1} + \cdots + \left(\frac{-a_1}{a_0} \right) \right) = 1.$$

Note that $a_0^{-1} \in K \subseteq R$. Hence, r^{-1} exists in R , so R is a division ring. It lies in F , so it is commutative. We conclude that R is a field. \square

§6.2 #9. For any positive integers a, b , show that $\mathbb{Q}(\sqrt{a} + \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.

Proof. Let $K := \mathbb{Q}(\sqrt{a}, \sqrt{b})$, and let $L := \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Suppose that $a = b$. Then $K = \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(2\sqrt{a}) = L$. Hence, we may assume that $a \neq b$.

First, note that $\sqrt{a}, \sqrt{b} \in K$. Therefore, we have $\sqrt{a} + \sqrt{b} \in K$. It follows that $L \subseteq K$.

Next, we show that $\sqrt{a}, \sqrt{b} \in L$. We observe that

$$\sqrt{ab} = \frac{(\sqrt{a} + \sqrt{b})^2 - (a + b)}{2} \in L.$$

Therefore, since $a \neq b$, we have

$$\frac{b(\sqrt{a} + \sqrt{b}) - \sqrt{ab}(\sqrt{a} + \sqrt{b})}{b - a} = \sqrt{b} \in L$$

$$\frac{a(\sqrt{a} + \sqrt{b}) - \sqrt{ab}(\sqrt{a} + \sqrt{b})}{a - b} = \sqrt{a} \in L.$$

We conclude that $K \subseteq L$. \square

§6.2 #10. Let F be an extension field of K . Let $a \in F$ be algebraic over K , and let $t \in F$ be transcendental over K . Show that $a + t$ is transcendental over K .

Proof. Suppose, by way of contradiction, that $b := a + t$ is algebraic over K . Note that since a and $t \in F$, we have $b = a + t \in F$. The set of all elements of F which are algebraic over K form a field; therefore, since $a, b \in F$, it follows that $b - a = t$ is algebraic over K . But this contradicts the hypothesis that t is transcendental over K . \square