6.1: 1 (d). Show that $\sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$.

Solution: Let $\alpha = \sqrt{2}+\sqrt{3}$. Then $\alpha^2 = 2 + \sqrt{3}$ and so $\alpha^2 - 2 = \sqrt{3}$. Hence $\alpha^4 - 4\alpha^2 + 4 = (\alpha^2 - 2)^2 = (\sqrt{3})^2 = 3$. Thus $\alpha^4 - 4\alpha^2 + 1 = 0$ and so $\alpha = \sqrt{2}+\sqrt{3}$ is a root of $f(x) = x^4 - 4x^2 + 1$.

6.1: 1 (f). Show that $\sqrt[6]{2}+\sqrt[6]{2}$ is algebraic over $\mathbb{Q}$.

Solution: Let $\alpha = \sqrt[6]{2}+\sqrt[6]{2}$. Then $\alpha - \sqrt[6]{2} = \sqrt[6]{2}$. Hence $\alpha^3 - 3\sqrt[6]{2}a^2 + 6\sqrt[6]{2} - 2\sqrt[6]{2} = (\alpha - \sqrt[6]{2})^3 = (\sqrt[6]{2})^3 = 2$. Therefore $\alpha^3 + 6\alpha - 2 = 3\sqrt[6]{2}a^2 + 2\sqrt[6]{2} = (3\alpha^2 + 2\sqrt[6]{2})$, and so $\alpha^6 + 12\alpha^4 - 4\alpha^3 + 36\alpha^2 - 24\alpha + 4 = (\alpha^3 + 6\alpha - 2)^2 = (3\alpha^2 + 2\sqrt[6]{2})^2 = (9\alpha^4 + 12\alpha^2 + 4) + 2 = 18\alpha^4 + 24\alpha^2 + 8$. Hence $\alpha^6 - 6\alpha^4 - 4\alpha^3 + 12\alpha^2 - 24\alpha - 4 = 0$ and so $\alpha = \sqrt[6]{2}+\sqrt[6]{2}$ satisfies $f(x) = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$.

6.1: 3 (a). Show that $f(x) = x^3 + 3x + 3$ is irreducible over $\mathbb{Q}$.

Solution: Eisenstein’s irreducibility criterion is satisfied for the prime $p = 3$.

6.1: 3 (b). Let $u$ be a root of $f(x)$. Express $u^{-1}$ and $(1+u)^{-1}$ in the form $a + bu + cu^2$, where $a, b, c \in \mathbb{Q}$.

Solution: Since $x^3 + 3x + 3 = x(x^2 + 3) + 3$, we have $1 = \frac{1}{3}(x^3 + 3x + 3) - \frac{1}{3}x(x^2 + 3)$. Thus $u^{-1} = -1 - \frac{1}{3}u^2$. We also have $x^3 + 3x + 3 = (x + 1)(x^2 - x + 4) - 1$, and so $1 = (x + 1)^3$. (Thus $(1 + u)^{-1} = 4 - u + u^2$.)

6.1: 4. Show that the intersection of any collection of subfields of a given field is again a subfield.

Comments: The main problem is with notation. You can’t assume that you have a finite set; in fact, you cannot assume that the set is countable. You need to assume that the fields are indexed by some set $I$.

Let $\{F_\gamma \mid \gamma \in I\}$ be a collection of subfields of $K$. Set $F = \bigcap_{\gamma \in I} F_\gamma = \{x \in K \mid x \in F_\gamma \forall \gamma \in I\}$. Then we need to show that $F$ is a field, and the proof is quite routine.

Note that you do not need to use this notation. For example, to check closure under addition and multiplication, you can simply say let $x, y$ belong to the intersection of the subfields. Then $x$ belongs to each subfield, and so does $y$, so $x + y$ and $xy$ must belong to each subfield. Therefore $x + y$ and $xy$ belong to the intersection of all of the subfields. The rest of the proof is similar.

6.2: 1 (d). Find the degree and a basis for the field extension $\mathbb{Q}(\sqrt{2}, \sqrt[6]{2})$ over $\mathbb{Q}$.

Solution: Since $\sqrt[6]{2}$ satisfies $f(x) = x^3 - 2$, and $f(x)$ is irreducible over $\mathbb{Q}$, we have $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 3$. Similarly, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ since the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$. Corollary 6.2.6 implies that $[\mathbb{Q}(\sqrt{2}, \sqrt[6]{2}) : \mathbb{Q}] \leq 6$, but since this degree is divisible by both 2 and 3, it must be equal to 6. The proof of Theorem 6.2.4 then shows that we can use as a basis the products of the elements $1, \sqrt{2}, \sqrt[6]{2}$ in a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, and the elements $1, \sqrt{2}$ which form a basis for $\mathbb{Q}(\sqrt[6]{2}, \sqrt{2})$ over $\mathbb{Q}(\sqrt{2})$. Thus $\{1, \sqrt{2}, \sqrt[6]{2}, \sqrt{2}, \sqrt{2} \sqrt[6]{2}, \sqrt[6]{2} \sqrt{2} \}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt[6]{2})$ over $\mathbb{Q}$.

6.2: 3. Let $F$ be a finite extension of $K$ such that $[F : K] = p$, a prime number. If $u \in F$ but $u \notin K$, show that $F = K(u)$.

Solution: Since $K \subseteq K(u) \subseteq F$, by Theorem 6.2.4 we have $[F : K] = [F : K(u)] [K(u) : K]$. Because $[F : K]$ is prime, either $[K(u) : K] = 1$ or $[F : K(u)] = 1$. The first case implies $K(u) = K$ and contradicts $u \notin K$. Therefore $[F : K(u)] = 1$ and so $F = K(u)$.

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

Solution: If $a = b$, then $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$, and so we may assume that $a \neq b$. Since $\sqrt{a}, \sqrt{b} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$, we have $\sqrt{a} + \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$, and so $\mathbb{Q}(\sqrt{a} + \sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Since $(\sqrt{a} + \sqrt{b})(\sqrt{a} - \sqrt{b})/(a - b) = 1$, we have $\sqrt{a} - \sqrt{b} = (a - b)/(\sqrt{a} + \sqrt{b})^{-1} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$ and so $\sqrt{a} = 1/2((\sqrt{a} + \sqrt{b}) + (\sqrt{a} - \sqrt{b})) \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$ and $\sqrt{b} = (\sqrt{a} + \sqrt{b}) - \sqrt{a} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Hence $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a} + \sqrt{b})$, and so $\mathbb{Q}(\sqrt{a} + \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. 