**1** Answer the following:

a. Find $u \in \mathbb{R}$ such that $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

b. Describe how you would find all $w \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ such that $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

**Solution** a. One such value of $u$ would be $u = \sqrt{2} + \sqrt[3]{5}$. By calculating the various powers of $\sqrt{2} + \sqrt[3]{5}$, it's easy to see that $\{1, \sqrt{2}, \sqrt[3]{5}, \sqrt[3]{5^2}, \sqrt{2}\sqrt[3]{5}, \sqrt{2}\sqrt[3]{5^2}\}$ is a basis for $\mathbb{Q}(u)$, which is the same basis as for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$, so they are the same.

b. I would look at linear combinations of the basis elements, and check to see if their powers can give me the rest of the basis elements.

---

**2** If $a, b \in K$ are algebraic over $F$ and are of degree $m, n$, respectively, with $\gcd(m, n) = 1$, show that $[F(a, b) : F] = mn$.

**Solution** We have:

$$[F(a, b) : F] = [F(a, b) : F(a)]m = [F(a, b) : F(b)]n$$

$$\begin{tikzcd}[column sep=small]
 & F(a,b) \arrow[dl, dash] \arrow[dr, dash] & \\
F(a) \arrow[dr, dash, "m"'] & & F(a) \arrow[dl, dash, "n"] \\
 & F &
\end{tikzcd}$$

Because $\gcd(m, n) = 1$, we know that $mn \mid [F(a, b) : F]$; indeed, we can just look at the prime decomposition of $m$ and $n$, and note that $m, n \mid [F(a, b) : F]$. Hence, $[F(a, b) : F] \geq mn$.

Since $F \subseteq F(a)$, we also know that $b$ is algebraic over $F(a)$ with degree at most $n$, so $[F(a, b) : F(a)] \leq n$. Hence, $[F(a, b) : F] \leq mn$, which shows that $[F(a, b) : F] = mn$.

---

**3** If $|F| = q < \infty$, show:

a. There exists a prime $p$ such that $\operatorname{char} F = p$.

b. $q = p^n$ for some $n$.

c. $a^q = a$ for all $a \in F$.

d. If $b \in K$ is algebraic over $F$, then $b^{q^m} = b$ for some $m > 0$.

**Solution** a. First note that $\operatorname{char} F > 1$, or else $F$ would only have 1 element, which is impossible since $F$ must have $0 \neq 1 \in F$.

Suppose the characteristic of $F$ is not prime, and let $n, m$ be two prime divisors of $\operatorname{char} F$. Also, for $k \in \mathbb{Z}$, we identify $k \in F$ via $k = \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}}$.

By assumption, there exists $k \in \mathbb{Z} \setminus \{0\}$ so that $knm = \operatorname{char} F$. But this means that

$$knm = 0 \implies nm = 0,$$

but $n, m \neq 0$, since $n, m < \operatorname{char} F$. This implies that $F$ is not an integral domain, which contradicts the definition of a field. Hence, $\operatorname{char} F$ is prime.

b. We have a natural embedding $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$, where $k \mapsto \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}}$. Because of this and the fact that $p$ is prime, we can think of $\mathbb{Z}/p\mathbb{Z}$ as a subfield of $F$. Hence, we can consider $F$ as a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. Now pick a basis $\mathfrak{B}$ for the vector space. Then if $|\mathfrak{B}| = n$, we have

$$q = |F| = |\mathbb{Z}/p\mathbb{Z}|^{|\mathfrak{B}|} = p^n$$

as required.

c. Notice that the units $F^\times$ form a group under multiplication with $|F^\times| = q-1$, since $F^\times = F \setminus \{0\}$. By Lagrange, $a^{q-1} = 1 \implies a^q = a$ for all $a \in F^\times$. 0 clearly satisfies the equation, so the equation holds for all $a \in F$.

d. Because $b$ is algebraic over $F$, $F(b)$ is finite dimensional over $F$, which is finite dimensional over $\mathbb{Z}/p\mathbb{Z}$, so $F(b)$ is finite dimensional over $\mathbb{Z}/p\mathbb{Z}$. Specifically,

$$[F(b) : \mathbb{Z}/p\mathbb{Z}] = [F(b) : F][F : \mathbb{Z}/p\mathbb{Z}] \coloneqq mn.$$

Let $\mathfrak{B}$ be a basis for $F(b)$ over $\mathbb{Z}/p\mathbb{Z}$, so that $|\mathfrak{B}| = mn$. Hence,

$$|F(b)| = |\mathbb{Z}/p\mathbb{Z}|^{|\mathfrak{B}|} = p^{mn} = q^m.$$

Thus, by (c), $b^{q^m} = b$ for all algebraic $b \in K$.

---

**4** Let $u$ be a root of $f = t^3 - t^2 + t + 2 \in \mathbb{Q}[t]$ and $K = \mathbb{Q}(u)$.

a. Show that $f = m_{\mathbb{Q}}(u)$.

b. Express $(u^2 + u + 1)(u^2 - u)$ and $(u-1)^{-1}$ in the form $au^2 + bu + c$ for some $a, b, c \in \mathbb{Q}$.

**Solution** a. By the rational root theorem, the only possible roots in $\mathbb{Q}$ are $\pm 1$ and $\pm 2$. A quick check shows that $f$ is irreducible over $\mathbb{Q}[t]$.

Now suppose otherwise, and assume that $g \coloneqq m_{\mathbb{Q}}(u)$ has a strictly lower degree than $f$. Since $\mathbb{Q}[t]$ is a Euclidean domain, it follows that $f = qg + r$ for some $g, r \in \mathbb{Q}[t]$. Since $u$ is a root for both polynomials, we see that $r(u) = 0$ also. But $\deg(r) < \deg(g)$, and because $g$ is the minimal polynomial, it follows that $r = 0$, so $g \mid f$.

Hence, we can write $f = (t-a)g$, but this implies that $f$ is reducible, which is a contradiction. Thus, $f = m_{\mathbb{Q}}(u)$.

b. Notice that $u^3 - u^2 + u + 2 = 0 \implies u^3 = u^2 - u - 2$. Expanding,

$$(u^2 + u + 1)(u^2 - u) = u^4 - u = u^3 - u^2 - 2u - u = u^3 - u^2 - 3u = -4u - 2.$$

We solve $(au^2 + bu + c)(u-1) = 1$:

$$1 = au^3 + bu^2 + cu - au^2 - bu - c = bu^2 + (c - a - b)u - (c + 2a).$$

Then $a = -1/3, b = 0, c = -1/3$, so

$$-\frac{u^3}{3} - \frac{1}{3} = (u-1)^{-1}.$$

---

**5** Let $\zeta = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6} \in \mathbb{C}$. Show that $\zeta^{12} = 1$ but $\zeta^r \neq 1$ for $1 \leq r < 12$. Show also that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ and find $m_{\mathbb{Q}}(\zeta)$.

**Solution** We can write $\zeta = e^{i\pi/6}$. Then $\zeta^{12} = e^{2\pi i} = 1$. For $1 \leq r < 12$, $\zeta^r \neq 1$: we need $\cos\frac{r\pi}{6} = 1$, which first happens when $r = 12$.

We claim that $m_{\mathbb{Q}}(\zeta) = t^4 - t^2 + 1$. First,

$$m_{\mathbb{Q}}(\zeta)(\zeta) = \zeta^4 - \zeta^2 + 1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} - \cos\frac{\pi}{3} - i\sin\frac{\pi}{3} + 1 = 0.$$

Next, we need to show that this is irreducible over $\mathbb{Q}$. By the rational root theorem, the only possible roots in $\mathbb{Q}$ are $\pm 1$, but it's easy to see that these both fail. Hence, $t^4 - t^2 + 1$ is irreducible, and is thus the minimal polynomial.

Lastly, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg m_Q(\zeta) = 4$, so we're done.

**6** Let $K = F(u)$, $u$ be algebraic over $F$, and the degree of $u$ be odd. Show that $K = F(u^2)$.

**Solution** It's clear that $F(u^2) \subseteq F(u)$. Notice that

$$[F(u) : F] = \big[F(u) : F(u^2)\big]\big[F(u^2) : F\big].$$

We also know that $\{1, u\}$ span $F(u)/F(u^2)$, so $\big[F(u) : F(u^2)\big] \leq 2$. But by assumption, $2 \nmid [F(u) : F]$, which implies that $\big[F(u) : F(u^2)\big] = 1$. Hence, $[F(u) : F] = \big[F(u^2) : F\big]$, so $F(u^2) = F(u)$, as required.

---

**7** Let $u$ be transcendental over $F$ and $F < k \subseteq F(u)$. Show that $u$ is algebraic over $k$.

**Solution** First notice $F(u) = F(u, u^2, \ldots)$, since $u$ is transcendental. Thus, because $k$ strictly contains $F$, $k$ must contain at least one of the $u^n$. Thus, $t^n - u^n \in k[t]$, and $u$ is clearly a root of this polynomial. Hence, $u$ is algebraic over $k$.

---

**8** If $f = t^n - a \in F[t]$ is irreducible, $u \in K$ is a root of $f$, and $n/m \in \mathbb{Z}$, show that $[F(u^m) : F] = n/m$. What is $m_F(u^m)$?

**Solution** Since $f$ is irreducible, $f = m_F(u)$. Since $n/m \in \mathbb{Z}$, we have

$$0 = f(u) = u^n - a = (u^m)^{n/m} - a.$$

We claim that $m_F(u^m) = t^{n/m} - a$. Suppose otherwise, and that there exists $g = b_k t^k + \cdots + b_0$ such that $g(u^m) = 0$ and $k < n/m$. Then $u$ is a root of $g(t^m)$, but $\deg g(t^m) = mk < n$, which contradicts the minimality of $f$. Hence, $m_F(u^m) = t^{n/m} - a$, which also shows that $[F(u^m) : F] = n/m$, as required.

---

**9** If $a^n$ is algebraic over a field $F$ for some $n > 0$, show that $a$ is algebraic over $F$.

**Solution** Since $a^n$ is algebraic over $F$, there exists a polynomial $f \in F[t]$ so that $f(a^n) = 0$. Then $g(t) := f(t^n) \in F[t]$, and $g(a) = f(a^n) = 0$, so $a$ is algebraic over $F$ also.