Exercise 1. Show $\mathbb{Q} [\sqrt{2}] = \{ a + b \sqrt{2} : a, b \in \mathbb{Q} \}$ is a field. The only tricky bit is showing $\frac{1}{a + b \sqrt{2}} \in \mathbb{Q} [\sqrt{2}]$.

$$\frac{1}{a + b \sqrt{2}} = \frac{1}{a + b \sqrt{2}} \cdot \frac{a - b \sqrt{2}}{a - b \sqrt{2}} = \frac{a - b \sqrt{2}}{a^2 + 2b^2}$$

Now let’s try to do this with $\sqrt[3]{2}$. We wish to show that $\mathbb{Q} [\sqrt[3]{2}] = \{ a + b \sqrt[3]{2} + c \sqrt[3]{4} : a, b, c \in \mathbb{Q} \}$ is a field. First we build a bit of “number theory of polynomials.”

Throughout $F$ is a field, $F[x]$ the space of polynomials in $x$ with coefficients in $F$ and $F^\times = F \setminus \{0\}$.

Definition 2. Let $(0 \neq) f \in F[x]$. We define the degree of $f$, notated $\deg(f)$, to be largest power of $x$ whose coefficient is non-zero.

But what about $f = 0$?

Consider what degree should satisfy. For $f, g \in F[x]$ non-zero:

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(f g) = \deg(f) \deg(g)$

By convention we set $\deg(0) = -\infty$. This fits with (1), (2).

Let $F_{\leq k}[x] = \{ a_0 + a_1 x + \ldots + a_k x^k : a_0, a_1, \ldots, a_k, \in F \}$.

Exercise 3. Does the space of all polynomials in $F$ of degree $k$ form a subspace of $F[x]$?

Is $F_{\leq k}$ a subspace? What is its dimension? Find a basis. Is it true that one polynomial from each degree forms a basis?

Definition 4. Let $f, g \in F[x]$. We say $f$ is a divisor of $g$, notated $f \mid g$, if

$$(\exists h \in F[x])(g = f h)$$

Exercise 5. $f \mid 0 \iff \ ?$ – always true

$0 \mid f \iff f = 0$. Does this violate $\frac{0}{0}$ undefined? No, as our definition only involved multiplication.

For what $f \in F[x]$ is it true that $(\forall g \in F[x])(f \mid g)$? Answer: $F^\times$.

Definition 6. Let $u \in F[x]$. We say $u$ is a unit if $u \mid 1$.

Note that the set of units is exactly $F^\times$.

We want to find the objects in $F[x]$ analogous to primes in $\mathbb{Z}$.

Definition 7. Let $f \in F[x]$. We say $f$ is irreducible in $F[x]$ if

$$(\forall g, h \in F[x])(f = gh \implies (g \text{ is a unit or } h \text{ is a unit})).$$

Exercise 8. "Which of the following are irreducible in $\mathbb{Q}[x]$?" Show $x^4 + 1$ and $x^n - 2$ are irreducible but $x^4 + 4$ is not. Try to write $x^4 + 4$ as $f^2 - g^2$.

For what $p$ is $x^2 + 1$ irreducible in $\mathbb{Z}_p[x]$? (this is related to PP17)

Theorem 9 (Division Theorem). Let $f, g \in F[x]$ with $g \neq 0$. The there exists unique $q, r \in F[x]$ such that $f = q \cdot g + r$ and $\deg(r) < \deg(g)$.

Exercise 10. Prove the Division Theorem.
Definition 11. Let \( f, g \in F[x] \). We can define \( d := \gcd(f, g) \) a greatest common divisor of \( f \) and \( g \) if

- \( d \mid f \) and \( d \mid g \)
- \( (\forall h \in F[x])(h \mid f \) and \( h \mid g) \implies h \mid d \)

Theorem 12. Let \( f, g \in F[x] \). There exists a greatest common denominator \( \gcd(f, g) \) unique up to multiplication by units.

Theorem 13. Let \( f, g \in F[x] \) and \( d = \gcd(f, g) \).

\[
(\exists u, v \in F[x])(d = u.f + v.g).
\]

Exercise 14 (PP). Prove theorems (only need Division theorem)

Definition 15. Let \( f, g \in F[x] \). We say \( f \) and \( g \) are relatively prime if and only if \( (\exists u, v \in F[x])(1 = f.u + g.v) \).

Convention is to write \( \gcd(f, g) = 1 \) if relatively prime and \( \gcd(f, g) \neq 1 \) if not.

Exercise 16. Let \( f \) be irreducible. Then \( f \mid g \) or \( \gcd(f, g) = 1 \)

Corollary 17. Let \( f \in F[x] \) be irreducible with \( \deg(f) = k \). Let \( g \in F[x] \) with \( \deg(g) < k \). Then \( \gcd(f, g) = 1 \).

Exercise 18. \( x^3 - 2 \) is irreducible.

Finally to show \( \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\} \) is a field.

Community solution: Let \( p = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}] \). It is sufficient to show there exists \( q \) such that \( pq = 1 \) (as then \( \frac{1}{p} = \frac{q}{pq} = q \)). Define \( f \in \mathbb{Q}[x] \) to be \( f(x) = a + bx + cx^2 \). Since \( \deg(f) < 3 \) and \( x^2 - 3 \) is irreducible, corollary says that there exists \( u, v \in \mathbb{Q}[x] \) such that \( 1 = u.f + v.(x^3 - 2) \). Substituting \( x = \sqrt[3]{2} \) we have \( 1 = u(\sqrt[3]{2}).f(\sqrt[3]{2}) \). Set \( q = u(\sqrt[3]{2}) \), then \( pq = 1 \). □