1. Excercises 6. 1#4 (a) and (b) .

   (a) Show that $\{u, v, w\} = \text{span}\{u + v, u + w, v + w\}$ in any $\mathbb{F}$-vector space V where $2 \neq 0$ in $\mathbb{F}$.

   $\supseteq$: Let $x \in \text{span}\{u+v, u+w, v+w\}$. Then for some $a, b, c \in \mathbb{F}$, $x = a(u+v)+b(u+w)+c(v+w) = (a + b)u + (a + c)v + (b + c)w \in \text{span}\{u, v, w\}$, and $\{u, v, w\} \supseteq \text{span}\{u + v, u + w, v + w\}$

   $\subseteq$: Let $x \in \text{span}\{u, v, w\}$. Then $x = au + bv + cw$ for some $a, b, c \in \mathbb{F}$. Rewrite u, v, w :

$$u = \frac{(u + v) + (u + w) - (v + w)}{2}$$
$$v = \frac{(u + v) + (v + w) - (u + w)}{2}$$
$$w = \frac{-(u + v) + (v + w) + (u + w)}{2}$$
$$x = a\frac{(u + v) + (u + w) - (v + w)}{2} + b\frac{(u + v) + (v + w) - (u + w)}{2} + c\frac{-(u + v) + (v + w) + (u + w)}{2}$$
$$= \frac{a + b - c}{2}(u + v) + \frac{a + c - b}{2}(u + w) + \frac{b + c - a}{2}(v + w).$$

   So we can write x as a linear combination of $\{u+v, u+w, v+w\}$, and $x \in \text{span}\{u+v, u+w, v+w\}$. Therefore $\{u, v, w\} \subseteq \text{span}\{u + v, u + w, v + w\}$ and $\{u, v, w\} = \text{span}\{u + v, u + w, v + w\}$

   (b) Is (a) true if $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$? Support your answer.
   In this case it is not true. Take $\mathbb{Z}_2$ as its own vector space, and let $u = v = w = 1$. Then the sum of any two of these vectors is 0 and span $\{u, v, w\} = \{0, 1\} \neq \{0\} = \text{span}\{u + v, u + w, v + w\}$.

2. Show that $u = \sqrt{2} + \sqrt{3} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ and find its minimal polynomial.

   Solution: Use algebraic trickery on u.

$$\begin{aligned} u &= \sqrt{3} + \sqrt{2} \\ u^2 &= 2\sqrt{6} + 5 \\ u^2 - 5 &= 2\sqrt{6} \\ (u^2 - 5)^2 &= 24 \\ u^4 - 10u^2 + 25 &= 24 \\ u^4 - 10u^2 + 1 &= 0. \end{aligned}$$

   And we have found a polynomial in $\mathbb{Q}$ so that u is a root, and u is algebraic over $\mathbb{Q}$.

   Though this polynomial is monic and has u as a root, we have yet to show that it is irreducible. Eisenstein's criterion fails us since the constant term is 1, no prime can divide it.

   Recall the Modular Irreducibility Theorem (Theorem 4.2.7). It states that if p is a prime not dividing the leading coefficient of a polynomial f in $\mathbb{Z}$, and the reduction of f in $\mathbb{Z}_p[x]$, $\bar{f}$ has no root in $\mathbb{Z}_p$, then f is irreducible in $\mathbb{Q}[x]$.

   Take $p = 3$. Then the reduction of m is $\bar{m} = u^4 - u + 1 = 0$. Check each element,

$$\begin{aligned} \bar{m}(0) &\equiv 0^4 - 0^2 + 1 \equiv 1 \pmod 3 \\ \bar{m}(1) &\equiv 1^4 - 1^2 + 1 \equiv 1 \pmod 3 \\ \bar{m}(2) &\equiv 2^4 - 2^2 + 1 \equiv 1 \pmod 3. \end{aligned}$$

   And so $\bar{m}$ has no roots in $\mathbb{Z}_3$, and by the modular irreducibility theorem m is irreducible in $\mathbb{Q}$.

3. Show that if $u \in \mathbb{C}$ and $u \notin \mathbb{R}$ then $\mathbb{C} = \mathbb{R}(u)$.

   Solution: Let $u \in \mathbb{C} \setminus \mathbb{R}$. Then $u = a + bi$ with $b \neq 0$.

⊆: Let $x \in \mathbb{C}$. Then $x = c + di$, and rewriting, we can also see that $i = \frac{u-a}{b}$, so $x = c + d\left(\frac{u-a}{b}\right) = (c - \frac{a}{b}) + u\left(\frac{d}{b}\right) \in \text{span}\{1, u\} = \mathbb{R}(u)$. so $\mathbb{C} \subseteq \mathbb{R}(u)$

⊃: $\mathbb{C}$ is a field containing both $\mathbb{R}$ and u. Then since $\mathbb{R}(u)$ must be contained in any such field, $\mathbb{R}(u) \subseteq \mathbb{C}$.

Therefore, $\mathbb{C} = \mathbb{R}(u)$.

4. Show that if $u \in \mathbb{E}$ is transcendental in $\mathbb{F}$, then

$$\mathbb{F}(u) = \{f(u)g(u)^{-1} \mid f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0\}.$$

Solution: Let u be transcendental in $\mathbb{F}$. For simplicity, write

$$\mathcal{F} = \{f(u)g(u)^{-1} \mid f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0\}.$$

⊆: If we can show that $\mathcal{F}$ is a field containing $\mathbb{F}, u$, then we can say $\mathbb{F}(u) \subseteq \mathcal{F}$ since $\mathbb{F}(u)$ is contained in every field which contains $\mathbb{F}$ and u.

Then let $a \in \mathbb{F}$. The constant polynomial $a = \frac{a}{1}$ is in $\mathcal{F}$ since, when evaluated at u it is u. So $\mathbb{F}(u) \subseteq \mathcal{F}$ Similarly, the polynomial $\frac{x}{1}$ is simply u when evaluated at u, and $u \in \mathcal{F}$. Finally $\mathcal{F}$ is a field, since it is a field of fractions (Field of Quotients in Nicholson 3.2.5) for the integral domain $\{f(u) : f(x) \in \mathcal{F}[x]\}$.

⊇: Let $a \in \mathcal{F}$. Write

$$f(x) = f_0 + f_1 x + \ldots + f_n x^n$$
$$g(x) = g_0 + g_1 x + \ldots + g_m x^m.$$

Evaluating at u,

$$f(u) = f_0 + f_1 u + \ldots + f_n u^n$$
$$g(u) = g_0 + g_1 u + \ldots + g_m u^m.$$

We know that each term in each polynomial is in $\mathbb{F}(u)$, and so the sum of the terms must be, since $\mathbb{F}(u)$ is closed under $\cdot, +$. And since $g(x) \neq 0$, we know the quotient must also be.

So $a = \frac{f(u)}{g(u)} \in \mathbb{F}(u)$, and $\mathbb{F}(u) \supseteq \mathcal{F}$. Therefore $\mathbb{F}(u) = \mathcal{F}$.