Section 6.1

1. (Problem 31a) A linear map $\varphi : V \to W$ between vector spaces over F is a map such that $\varphi(v + v') = \varphi(v) + \varphi(v')$ and $\varphi(av) = a\varphi(v)$ for $a \in F$ and $v, v' \in V$. Prove $\ker \varphi$ and $\operatorname{Im} \varphi$ are subspaces of V and W respectively.

Solution: Of course $0 \in \ker \varphi$ because φ is an abelian group homomorphism. If $v, v' \in \ker \varphi$ then

$$\varphi(v - v') = \varphi(v) - \varphi(v') = 0 - 0 = 0,$$

so $v - v' \in \ker \varphi$ and $\ker \varphi$ is an additive subgroup. Finally if $v \in \ker \varphi$ and $a \in F$ then $\varphi(av) = a\varphi(v) = a \cdot 0 = 0$ so $av \in \ker \varphi$, and this concludes the proof that $\ker \varphi$ is a subspace.

Now let $w, w' \in \varphi$ and $a \in F$. By definition we have $w = \varphi(v)$ and $w' = \varphi(v')$ for some $v, v' \in V$. Then

$$w + w' = \varphi(v) + \varphi(v') = \varphi(v + v') \in \operatorname{Im} \varphi,$$

and $aw = a\varphi(v) = \varphi(av) \in \operatorname{Im} \varphi$. Thus shows $\operatorname{Im} \varphi$ is a subspace.

2. (Problem 26) Let U and W be subspaces of a finite-dimensional vector space V over a field F.

   (a)

   (b) Suppose $U \cap W = \{0\}$. Prove $\dim(U + W) = \dim(U) + \dim(W)$.

Solution: Choose bases $\{u_1, \ldots, u_n\}$ and $\{w_1, \ldots, w_m\}$ of U and W, respectively. We will prove $\{u_1, \ldots, u_n, w_1, \ldots, w_m\}$ is a basis of $U + W$: to see it spans, if $v \in U + W$, then by definition this means $v = u + w$ for some $u \in U$ and $w \in W$. Then we can write $u = a_1u_1 + \cdots + a_nu_n$ for some $a_i \in F$, and $w = b_1w_1 + \cdots + b_mw_m$ for some $b_i \in F$. But then

$$v = u + w = a_1u_1 + \cdots + a_nu_n + b_1w_1 + \cdots + b_mw_m,$$

which shows $v \in \operatorname{span}\{u_1, \ldots, u_n, w_1, \ldots, w_m\}$. Now to show linear independence, suppose

$$a_1u_1 + \cdots + a_nu_n + b_1w_1 + \cdots + b_mw_m = 0.$$

Writing $x = a_1u_1 + \cdots + a_nu_n$, we clearly have $x \in U$ (since each $u_i \in U$), but also $x = (-b_1)w_1 + \cdots + (-b_m)w_m$, which shows us that $x \in W$. So $x \in U \cap W = \{0\}$, and we conclude $x = 0$. But then $a_1u_1 + \cdots + a_nu_n = 0$, so by linear independence we conclude each a_i is zero; similarly we conclude each b_i is zero. This shows $\{a_1, \ldots, a_n, w_1, \ldots, w_m\}$ is linear independent, concluding the proof it is a basis for $U + W$.

(c) Prove in general that $\dim(U+W) = \dim(U) + \dim(W) - \dim(U \cap W)$.

Solution: Let $\{v_1, \dots, v_n\}$ be a basis for $U \cap W$ (so $\dim(U \cap W) = n$). Then $\{v_1, \dots, v_n\}$ is a linearly independent subset of U, so by Theorem 6(2) we can extend it to a basis of U, say $\{v_1, \dots, v_n, u_1, \dots, u_k\}$. Similarly we can extend to a basis of W, say $\{v_1, \dots, v_n, w_1, \dots, w_\ell\}$. In particular $\dim(U) = n + k$ and $\dim(W) = n + \ell$ in our notation.

We now claim that $\{v_1, \dots, v_n, u_1, \dots, u_k, w_1, \dots, w_\ell\}$ is a basis for $U+W$. If we can prove this then we will have

$$\dim(U+W) = n + k + \ell = \dim(U \cap W) + \dim(U) + \dim(W)$$

which gives the result by rearranging. To see that the set spans $U+W$, suppose $v = u + w \in U + W$; because $v_1, \dots, v_n, u_1, \dots, u_k$ span U, we can write

$$u = a_1 v_1 + \cdots + a_n v_n + a_{n+1} u_1 + \cdots + a_{n+k} u_k$$

for some $a_i \in F$. Similarly $w = b_1 v_1 + \cdots + b_n v_n + b_{n+1} w_1 + \cdots + b_{n+\ell} w_\ell$ for some $b_i \in F$. Then because $v = u + w$ we have

$$v = (a_1 + b_1) v_1 + \cdots + (a_n + b_n) v_n + a_{n+1} u_1 + \cdots + a_{n+k} u_k + b_{n+1} w_1 + \cdots + b_{n+\ell} w_\ell$$

which shows $v_1, \dots, v_n, u_1, \dots, u_k, w_1, \dots, w_\ell$ span V. For linear independence, suppose

$$a_1 v_1 + \cdots + a_n v_n + b_1 u_1 + \cdots + b_k u_k + c_1 w_1 + \cdots + c_\ell w_\ell = 0$$

for $a_i, b_i, c_i \in F$. Let $x = -(c_1 w_1 + \cdots + c_\ell w_\ell)$; clearly $x \in W$ because each $w_i \in W$. But on the other hand

$$x = a_1 v_1 + \cdots + a_n v_n + b_1 u_1 + \cdots + b_k u_k \in U,$$

and therefore $x \in U \cap W$. But $\{v_1, \dots, v_n\}$ is a basis for $U \cap W$ so $x = a_1' v_1 + \cdots + a_n' v_n$ for $a_i' \in F$. Then we have the equation

$$(a_1 - a_1') v_1 + \cdots + (a_n - a_n') v_n + b_1 u_1 + \cdots + b_k u_k = 0.$$

By linear independence of $\{v_1, \dots, v_n, u_1, \dots, u_k\}$, we see all coefficients here are zero, in particular the b_i are zero. But then our original equation reduces to

$$a_1 v_1 + \cdots + a_n v_n + c_1 w_1 + \cdots + c_\ell w_\ell = 0$$

which by linear independence of $\{v_1, \dots, v_n, w_1, \dots, w_\ell\}$ implies all a_i and c_i are zero. This completes the proof of linear independence.

Section 6.2

3. (Problem 4b) Show $\sqrt{2}$ is algebraic over $F = \mathbf{Q}(1+i)$ and find its minimal polynomial.

Solution: $\sqrt{2}$ is algebraic over F because it is a root of the polynomial $x^2 - 2 \in F[x]$. We claim this is the minimal polynomial (call it m) as well: we know that $m(x) \mid x^2 - 2$, so $\deg(m) = 1$ or 2, and in the case $\deg(m) = 2$ because both polynmomials are monic we can conclude $m(x) = x^2 - 2$. If $\deg(m) = 1$ then this means $\sqrt{2} \in \mathbf{Q}(1+i)$; one can do a straightforward argument to show that $\{1, 1+i, \sqrt{2}\}$ is linearly independent over $\mathbf{Q}$ to show this is impossible. Here is an alternative approach: because $\mathbf{Q}(\sqrt{2}, 1+i) = \mathbf{Q}(1+i)(\sqrt{2})$, we have $\deg(m) = [\mathbf{Q}(\sqrt{2}, 1+i) : \mathbf{Q}(1+i)]$. But similarly, the minimal polynomial occuring in the solution in part (a) has degree 2 which by a similar remark shows $[\mathbf{Q}(\sqrt{2}, 1+i) : \mathbf{Q}(\sqrt{2})] = 2$. But now we can consider the diagram

$$\begin{tikzcd}
 & \mathbf{Q}(\sqrt{2}, 1+i) \arrow[dl, dash, "2"'] \arrow[dr, dash] & \\
\mathbf{Q}(\sqrt{2}) \arrow[dr, dash, "2"] & & \mathbf{Q}(1+i) \arrow[dl, dash, "2"'] \\
 & \mathbf{Q} &
\end{tikzcd}$$

and Theorem 5 (sometimes called the Tower Law) lets us conclude $[\mathbf{Q}(\sqrt{2}, 1+i) : \mathbf{Q}(1+i)] = 2$, therefore $\deg(m) = 2$ so $m(x) = x^2 - 2$. [Note: clearly this method is overkill for the problem at hand, but it is a useful method to know for future problems.]

4. (Problem 13a) Find $[E : F]$ where $E = \mathbf{Q}(\sqrt{3} + \sqrt{5})$ and $F = \mathbf{Q}(\sqrt{3})$.

Solution: Write $u = \sqrt{3} + \sqrt{5}$. Notice that

$$\sqrt{3} = \frac{u^3 - 14u}{4} \in \mathbf{Q}(u) = E$$

so we actually do have $F \subseteq E$. Also notice that $E = F(u)$. Let $m \in F[x]$ be the minimal polynomial of u over F. By Theorem 4 we know that $[E : F] = \deg(m)$. Also notice that $(u - \sqrt{3})^2 = 5$, so expanding we see that u is a root of the polynomial $f(x) = x^2 - 2\sqrt{3}x - 2 \in F[x]$. By Theorem 3 we conclude that $m \mid f$ in $F[x]$. Therefore we either have $\deg(m) = 1$ or $\deg(m) = 2$. If $\deg(m) = 1$ then $[E : F] = 1$ which implies $E = F$ which implies $\sqrt{5} \in \mathbf{Q}(\sqrt{3})$. But by a very similar argument to Section 6.1 Problem 9(a) we can conclude that $\{1, \sqrt{3}, \sqrt{5}\}$ is linearly independent over $\mathbf{Q}$, rendering $\sqrt{5} \in \mathbf{Q}(\sqrt{3})$ impossible. Thus we conclude $\deg(m) = 2$ and hence $[E : F] = 2$.