Exercise 16.

1. Let $(\mathcal{M}_{\mathbf{u},\mathbf{v}}(\varphi))_{i,j} = \lambda_{i,j}$ where $\lambda_{i,j}$ is the unique element of R such that
$$\varphi(u_j) = \lambda_{1,j}v_1 + ... + \lambda_{i,j}v_i + ... + \lambda_{m,j}v_m.$$
It is immediate to check that $(\varphi(u_1), ..., \varphi(u_n)) = (v_1, ..., v_m)\mathcal{M}_{\mathbf{u},\mathbf{v}}(\varphi)$.
Suppose now that $\mathcal{M}' \neq \mathcal{M}_{\mathbf{u},\mathbf{v}}(\varphi)$ and let $a_{i,j} = (\mathcal{M}')_{i,j} \neq (\mathcal{M}_{\mathbf{u},\mathbf{v}}(\varphi))_{i,j}$ for some $i \in \{1, ..., m\}$ and $j \in \{1, ...n\}$. It follows that the j-th entry of $(v_1, ..., v_m)\mathcal{M}'$ is
$$z = ... + a_{i,j}v_i + ...$$
which can't be equal to $\varphi(u_j)$, since the i-th coordinate of $\varphi(u_j)$ w.r.t. the base $\mathbf{v}$ is $(\mathcal{M}_{\mathbf{u},\mathbf{v}}(\varphi))_{i,j}$ and the coordinates are unique.

2. Follows immediately from the distributivity and scalar multiplication compatibility of the matrix multiplication (together with the trivial observation that $\theta_A(\mathbf{0}) = A\mathbf{0} = \mathbf{0}$).

3. The proof that $\kappa_{\mathbf{u}}$ is a morphism is immediate. The sujectivity follows trivially by the fact that $\mathbf{u}$ is a basis and by definition of basis every element can be written as a sum of elements of the basis. The injectivity follows immediately from the fact that by definition of basis the elements of the basis are linearly independent.

4. Surjectivity: it's sufficient to define φ properly (immediate).
Injectivity: immediate.
Morphism: for the addition it's immediate, for the composition it's boring (works thanks to definition of multiplication of matrices).

Exercise 17.

Proof.

- ($\Longrightarrow$) Suppose that M is free. Suppose towards a contradiction that $\mathrm{rk}(M) > 1$. Then let x_1, x_2 be two elements of a basis. Since by hypothesis M is a subset of the quotient field, $x_1 = ab^{-1}$ and $x_2 = cd^{-1}$ for some $a, b, c, d \in R$. Then $(bc)ab^{-1} + (-da)cd^{-1} = 0$, contradiction.

- ($\Longleftarrow$) If $M = \langle x \rangle$ then $\{x\}$ is a base for M. In fact, obviously x generates all M. It is also linearly independent since $\lambda x = 0 \Rightarrow \lambda = 0$ for all $\lambda \in R$, because K is a field, and hence a domain (and the scalar operation is defined as the internal multiplication of K, restricted to the elements of R).

$\square$

Exercise 18.

Proof.

1. Thanks to Exercise 17, it is sufficient to show that $M = \langle 2, 1+\sqrt{-5}\rangle$ is not cyclic. Observe that M is also an ideal over R. It's trivial to see that if M is a cyclic R-module, then it must be a principal ideal of R as well. Our aim is therefore to show that M is not a principal ideal. Suppose towards a contradiction that $M = (g)$, i.e. M is the principal ideal generated by some $g \in M$. Of course $2, 1+\sqrt{-5} \in M$, therefore $2 = \lambda g$ and $1+\sqrt{-5} = \mu g$ for some $\lambda, \mu \in \mathbb{Z}[\sqrt{-5}]$. Consider now the standard norm $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$. We have that $g|2$ and $g|1+\sqrt{-5}$, thus $N(g)|4$ and $N(g)|6$, and so $N(g)|6-4=2$. Write now g as $a+b\sqrt{-5}$ with $a, b \in \mathbb{Z}$. This means that $a^2+5b^2|2$, thus $b=0$ and $a^2|2$, so $a = \pm 1$. Thus, $g = \pm 1$, and this means that M is the full $\mathbb{Z}\sqrt{-5}$ ring.
   Therefore we can write 1 as a combination of 2 and $1+\sqrt{-5}$, i.e.
   $$1 = 2(c+d\sqrt{-5}) + (1+\sqrt{-5})(e+f\sqrt{-5})$$
   which by computations means $2c+e-5f = 1$ and $2d+e+f = 0$, with $c, d, e, f \in \mathbb{Z}$. Taking classes modulo 2 we obtain $[e]+[f] = 1$ and $[e]+[f] = 0$, which is impossible.

2. Let $M' = \langle (2, 1+\sqrt{-5}), (1-\sqrt{-5}, 2)\rangle$. Suppose towards a contradiction that $(2, 1+\sqrt{-5}) = k(1-\sqrt{-5}, 2)$ for some $k \in \mathbb{Z}\sqrt{-5}$. Then
   $$\begin{cases} 2 = k - k\sqrt{-5} \\ 1+\sqrt{-5} = 2k \end{cases}$$
   which means that $2 = [1+\sqrt{-5} - (1+\sqrt{-5})(\sqrt{-5})]/2$, i.e. $2 = 6/2 = 3$, contradiction (note that we did the calculation in $\mathbb{Q}(\sqrt{-5})$, but if the vectors are independent in $\mathbb{Q}(\sqrt{-5})$, then they have to be independent in $\mathbb{Z}\sqrt{-5}$ as well).

   First observe that, since $2, 1+\sqrt{-5}, 1-\sqrt{-5} \in M$, it follows immediately that $M' \subseteq M \times M$.

   For the other inclusion, observe that $(1-\sqrt{-5})(2, 1+\sqrt{-5}) - 2(1-\sqrt{-5}, 2) = (0, 2)$. So $(0, 2) \in M'$. By the same argument we obtain that $(2, 0) \in M'$.

   Then it's immediate to see that $(0, 1+\sqrt{-5})$ and $(1-\sqrt{-5}, 0)$ are also in I.

   So we proved that $(2, 0), (1-\sqrt{-5}, 0), (0, 2), (0, 1+\sqrt{-5}) \in M'$, which trivially implies $M \times M \subseteq M'$.

   Hence $M \times M = M'$, i.e. it is the free R-module of rank 2 generated by $(2, 1+\sqrt{-5})$ and $(1-\sqrt{-5}, 2)$.

□

Exercise 19.

Proof.

1. Observe that $0 \to \ker \pi \to M \xrightarrow{\pi} F \to 0$ is an exact short sequence. Then $g : F \to M$,

$$\lambda_{i_1}\pi(x_{i_1}) + ... + \lambda_{i_n}\pi(x_{i_n}) \mapsto \lambda_{i_1}x_{i_1} + ... + \lambda_{i_n}x_{i_n}$$

is a morphism s.t. $\pi \circ g = \mathrm{id}_F$. Therefore, the sequence is a split short exact sequence, and thus $M \simeq \ker \pi \oplus F \simeq \ker \pi \oplus (\oplus_{i \in I} Rx_i)$.
If $\pi : M \to F$ is an R-module epimorphism onto a free module F, we can always find a family $(x_i)_{i\in I}$ in M whose image $\pi(x_i)_{i\in I}$ is a basis of F. In fact, if $(b_i)_{i\in I}$ is a basis of F (and the Axiom of Choice holds), it is sufficient to choose $(y_i)_{i\in I}$ s.t. $y_i = \pi^{-1}(b_i)$.

2. Let $(x_i)_{i\in I}$ be a basis of M/N. Let $\pi : M \to M/N$ the canonical projection. Then, thanks to the first point, we have

$$M = \ker \pi \oplus (\oplus_{i\in I} Rx_i).$$

Since $\ker \pi = N$, the $(x_i)_{i\in I}$ let us extend every basis of N to a basis of M.

□

Exercise 20.

Proof.

1. A module over a field is a vector space. So M is a finite-dimension vector space and N is a vector subspace of M. Thus N has a basis (and we don't need the Axiom of Choice).

2. If $(b_i)_{i\in I}$ is a basis of M, then the vector subspaces of M are precisely the ones generated by any subset of $\{b_i : i \in I\}$. So the conclusion follows immediately.

3. Every module morphism over a field is a linear map. Therefore the statement becomes the well-known linear algebra result (since the dimension of M is finite).

4. Same of above.

Suppose now that R is not a field.

1. Doesn't necessarily hold. In fact, let $I \lhd R$ be an ideal. Since $\forall a, b\ [ba+(-a)b = 0]$, in order to be free (as a module), I must (at least) be generated by just one element, i.e. I must be principal. So if R is not a PID, then the statement doesn't hold for sure.

2. Doesn't necessarily hold. Let R be a domain and let $p \in R$ be a prime element. Then the ideal $I = pR$ cannot be a direct summand of R. Indeed, if there was an R-module isomorphism $R \cong I \oplus M$ for some R-module M, then we would have an injection $R/I \cong M \hookrightarrow R$, which is impossible as the source is a non-zero torsion R-module, while R is not, since it is a domain by hypothesis.

3. Doesn't necessarily hold. Consider $\varphi : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto 2n$.

4. Doesn't necessarily hold. Consider the ring $M = R = \mathbb{Z}_4$ and the morphism $f : x \mapsto 2x$. Then M is free and finitely generated, because $\{1\}$ is a basis, and $\ker f = \operatorname{ran} f = \{0, 2\}$ is not even free, since $2 \cdot 2 = 0$, thus it has no basis.

$\square$