Exercise 0.1 (1)**.** *Proof.* (1) A left $\mathbb{Z}$-module is by definition already an abelian group. We must check that the module structure doesn't add any additional structure, or more specifically, that every abelian group has a unique $\mathbb{Z}$-module structure which is the one described below.
Now, we are given a map $\mathbb{Z} \times M \to M$ by $(n, x) \mapsto n \cdot x$ where M is some abelian group. Since by part (2) of the definition of being a module, i.e., $(r + s) \cdot x = r \cdot x + s \cdot x$, we have

$$n \cdot x = \underbrace{1 \cdot x + \ldots + 1 \cdot x}_{n \text{ times}} = \underbrace{x + \ldots + x}_{n \text{ times}}$$

where the second equality follows from (4) in the definition: $\mathbb{1}_R \cdot x = x$. This tells us how to give any abelian group M a $\mathbb{Z}$-module structure and that this must be unique. Simply define a map $\mathbb{Z} \times M \to M$ by

$$(n, x) \mapsto n \cdot x = \underbrace{x + \ldots + x}_{n \text{ times}}.$$

This is indeed an element of M since groups are closed under addition. Now we check that this map satisfies the axioms for a module.

$$n(x + y) = \underbrace{(x + y) + (x + y) + \ldots + (x + y)}_{n \text{ times}} = \underbrace{x + \ldots + x}_{n \text{ times}} + \underbrace{y + \ldots + y}_{n \text{ times}}$$

The others are checked similarly.

(2) For $R = k$ a field, we have that the distribute laws are precisely those of (1) and (2) from the definition of a module in the notes, and $\alpha(\beta x) = (\alpha\beta)x$ and $1 \cdot x = x$ are precisely axioms (3) and (4). Furthermore, we by assumption have that M is an abelian group.

(3) Suppose M is a $k[t]$-module. Then, in particular, M inherits a k-multiplication making it into a k-vector space, but the question is whether it has additional structure. If we know what (t, x) is mapped to, then by axiom (3), we know what $t^2 x = t(tx)$ will be, and likewise $t^k x$ for any $k \in \mathbb{N}$. Consider M as a k-vector space with basis $\mathcal{B} = \{v_\alpha \mid \alpha \in I\}$ for some indexing set I. Now, we claim that $t\mathcal{B} = \{tv_\alpha \mid \alpha \in I\}$ is also a basis. Suppose $\sum c_\alpha t v_\alpha = 0$ as a finite sum in M. By axiom (1), we then also have $t\left(\sum c_\alpha v_\alpha\right) = 0$. Now, $\alpha x = 0 \iff \alpha = 0 \vee x = 0$ in a vector space, so $t = 0$ or $\sum c_\alpha v_\alpha = 0$. Now, if $t = 0$, then M simply reduces to a k-vector space with no additional structure. However, if $t \neq 0$, then by linear independence, $c_\alpha = 0$ for all α, so $t\mathcal{B}$ is again a basis. By induction then, $t^k\mathcal{B}$ will be a basis. We can define a linear map $T \colon M \to M$ by $v_\alpha \mapsto tv_\alpha$ on the basis and extend it linearly. Then we indeed have

$$\left(\sum_{n=0}^{m} c_n t^n\right) x = \sum_{n=0}^{m} c_n t^n x = \sum_{n=0}^{m} c_n T^n x$$

so the action of any element of $k[t]$ on some $x \in M$ is uniquely determined by the linear map T. So we have an injective map

$$\{k[t]\text{-modules}\} \to \{(V, T) \mid V \text{ is a } k\text{-vector space and } T \in \mathrm{End}_k(V)\}.$$

by sending $M \mapsto (V, T)$ where V is M considered as a vector space over K and T is the map $v \mapsto tv$.

Conversely, given a pair (M, T), we can make M into a k-module by letting $\left(\sum c_n t^n\right) x = \sum c_n T^n(x)$. This clearly satisfies the axioms for the map in the definition of a module.

(4) Suppose M is a $k\,[G]$-module where $k\,[G]$ is a k-algebra associated to a group G. Then M inherits a vector space structure from k. Now, the map $k\,[G] \times M \to M$ sends $(g, x) \mapsto gx$ which is invertible since $g^{-1}\,(g \cdot x) = \left(g^{-1}g\right) \cdot x = 1 \cdot x = x$. Furthermore, since $g\,(x + y) = gx + gy$ by the axioms of a module, the map $T_g(x) = gx$ is a group automorphism, so $g \mapsto T_g$ is a map $\rho \colon G \to \mathrm{Aut}(V)$. Furthermore, we have $\rho(g + g')(x) = T_{g+g'}(x) = (g + g')x = gx + g'x = \rho(g)(x) + \rho(g')(x)$. Thus ρ is in fact a group homomorphism.

Conversely, any such pair M and a group homomorphism $\rho \colon G \to \mathrm{Aut}(V)$ defines a $k\,[G]$-module by $\left(\sum c_g g\right) \cdot x = \sum c_g \rho(g)(x)$.

$\square$

Exercise 0.2 (2)**.** Let M be a $k[t]/\left(t^n\right)$-module. Then M is in particular a k-vector space. Now, if $\mathcal{B} = \{v_\alpha\}$ is a basis for M as a k-vector space, then $t\mathcal{B}, \ldots, t^{n-1}\mathcal{B}$ are bases for M as k-vector spaces, so the map $T \colon M \to M$ sending $x \to tx$ is a linear automorphism, but since $t^n = 0$, we get $T^n = 0 \in \mathrm{Hom}_k\,(M, M)$. So a $k[t]/\left(t^n\right)$-module consists of a pair (M, T) of a k-vector space M and a nilpotent map T of index k.
A $k[t, t^{-1}]$-module consists similarly of a k-vector space and an invertible linear automorphism of the k-vector space.

Exercise 0.3 (5)**.** *Proof.* We have $r \cdot (x + y) = \varphi(r)(x + y) = \varphi(r)x + \varphi(r)y = r \cdot x + r \cdot y$, $(r + s) \cdot x = \varphi(r + s)x = \varphi(r)x + \varphi(s)x = r \cdot x + s \cdot x$, $r \cdot (s \cdot x) = r \cdot \varphi(s)x = \varphi(r)\varphi(s)x = \varphi(rs)x = (rs) \cdot x$, and lastly, $1_R \cdot x = \varphi(1_R)x = 1_S x = x$ (where we assume that $\varphi \neq 0$) $\square$

Exercise 0.4 (6)**.** *Proof.*

(1) When $R = \mathbb{Z}$, we have $a \cdot x = \underbrace{x + \ldots + x}_{a \text{ times}}$, so

$\varphi(a \cdot x + y) = \varphi\left(\underbrace{x + \ldots + x}_{a \text{ times}}\right) + \varphi(y) = \varphi(y) + \sum_{i=1}^{a} \varphi(x)$, so again, no additional structure is preserved besides φ being a group homomorphism. Converse is the same.

(2) Suppose $\varphi \colon M \to N$ is a k-linear homomorphism where M and N are k-modules. Then first, M and N can be considered as k-vector spaces. If we consider them as such, we have for $\alpha, \beta \in k$ and $x, y \in M$ that $\varphi\,(\alpha x + \beta y) = \varphi(\alpha x) + \varphi(\beta x) = \alpha\varphi(x) + \beta\varphi(x)$, where the first equality follows from φ being a homomorphism of the underlying abelian groups, and the second equality follows from the additional assumption on R-maps that we can draw the scalar out.

(3) Suppose φ is a $k[t]$-linear homomorphism from (V, T) to (W, S). We then have $\varphi\left(\sum c_n T^n x\right) = \varphi\left(\left(\sum c_n t^n\right) x\right) = \sum c_n t^n \varphi(x) = \sum c_n S^n \varphi(x)$, so it follows from the previous subexercise, that φ is a vector space homomorphism with the property $\varphi\,(T(x)) = S\,(\varphi(x))$ for all $x \in V$.

$\square$

Exercise 0.5 (8)**.** *Proof.* This follows from the same being true for maps of sets which φ, in particular, is. $\square$

Exercise 0.6 (10)**.** *Proof.* By exercise 6.(a), a $\mathbb{Z}$-linear homomorphism is simply a homomorphism of the underlying abelian groups.So we easily find that

(1) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$ is in bijection with the integers, $\mathbb{Z}$.
(2) Similar. Bijection with $\mathbb{Z}/m$.
(3) Similarly, bijection with the underlying set of A.
(4) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}) = \{0\}$ since for any $\mathbb{Z}$-linear homomorphism $\varphi\colon \mathbb{Z}/m \to \mathbb{Z}$, we have $m \cdot \varphi(1) = 0$ and hence $\varphi(1) = 0$, so $\varphi = 0$.
(5) If $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $n = q_1^{\beta_1} \cdots q_t^{\beta_t}$, then

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n) &= \mathrm{Hom}_{\mathbb{Z}}\left(\oplus_i \mathbb{Z}/\left(p_i^{\alpha_i}\right), \oplus_j \mathbb{Z}/\left(q_j^{\beta_j}\right)\right) \\ &= \bigoplus_{i,j} \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/\left(p_i^{\alpha_i}\right), \mathbb{Z}/\left(q_j^{\beta_j}\right)\right)\end{aligned}$$

Now if $p \neq q$, then the Hom set is trivial. If $p_i = q_j$ then we must have that $\varphi\left(p_i^{\alpha_i}\right) = 0$, thus $\beta_j \leq \alpha_i$. If $\beta_j \leq \alpha_i$, then $\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/\left(p_i^{\alpha_i}\right), \mathbb{Z}/\left(q_j^{\beta_j}\right)\right) \approx \mathbb{Z}/\left(q_j^{\beta_j}\right)$, so

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n) \approx \bigoplus_{\substack{p_i = q_j \\ \beta_j \leq \alpha_i}} \mathbb{Z}/\left(q_j^{\beta_j}\right)$$

(6) Suppose $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$, then suppose $\varphi\left(\frac{a}{b}\right) = m$. Then $n\varphi\left(\frac{a}{bn}\right) = m$ so $n \mid m$ for all $n > 1$. Thus $m = 0$, so as $\frac{a}{b}$ was arbitrary, $\varphi = 0$. Hence $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$.

$\square$

Exercise 0.7 (11)**.** *Proof.* Since k is algebraically closed, we have that V decomposes as the direct sum of its generalized eigenspaces. So we now claim that $M_{\lambda_i} = k[t]/(t-\lambda_i)^{e_i}$. But $M_{\lambda_i} = \left\{x \in V \mid \exists k > 0\colon (t-\lambda_i)^k x = (T-\lambda_i)^k x = 0\right\}$. Now, M_{λ_i} is cyclic with generator x and has basis $x, (T-\lambda_i)x, \ldots, (T-\lambda_i)^{k-1}x$. Define now a map $M_{\lambda_i} \to k[t]/(t-\lambda_i)^k$ by $(T-\lambda_i)^r x \mapsto (t-\lambda_i)^r$ which is clearly a linear isomorphism. Thus the decomposition follows.

$\square$

Exercise 0.8 (12)**.** *Proof.* We have that $R[t]/\left(t^2+1\right) \approx \{a_0 + a_1 t \mid a_0, a_1 \in \mathbb{R}\}$, and on the other hand, $t^2 \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = -\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$, so we have that $\left(\mathbb{R}^2, T\right) \approx \mathbb{R}[t]/\left(t^2+1\right)$ by $ct^n x \mapsto ct^n$.
Irreducibility of t^2+1 follows from Eisenstein. $\square$

Exercise 0.9 (14)**.** *Proof.* Suppose M is finitely generated by the set $\{x_1, \ldots, x_n\} \subset M$. Define $\varphi\colon R^n \to M$ by $\varphi(r_1, \ldots, r_n) = r_1 x_1 + \ldots + r_n x_n$. By definition of a generating set, φ is surjective, and it is clear that it is an R-homomorphism.
Conversely, if $\varphi\colon \mathbb{R}^m \to M$ is a surjective homomorphism, then since $\{e_1, \ldots, e_m\}$ generates $\mathbb{R}^m$, $\{\varphi e_1, \ldots, \varphi e_m\}$ generates M. $\square$

Exercise 0.10 (15)**.** By exercise 14, there is a surjective R-homomorphism $\varphi\colon R \to M$, so by the first isomorphism theorem, $M \approx R/\ker\varphi$. Conversely, if $M \approx R/I$ then M is cyclic as it is generates by the inverse of $\overline{1} \in R/I$ which generates R/I.

Exercise 0.11 (16)**.** To show surjectivity, we must show that for any $m \in M$, there is an R-map $\varphi\colon R \to M$ with $\varphi(1) = m$. But R is cyclic, generated by $1 \in R$. By prop 2.34 in Rotman, we can extend a function $\tilde{\varphi}\colon \{1\} \to M$ mapping $1 \mapsto m$ to an R-map $\varphi\colon R \to M$ with $\varphi(1) = m$. Hence the map $\mathrm{Hom}_R(R, M) \to M$ by $f \mapsto f(1)$ is surjective. Since R is generated by 1 and any functions are uniquely determined by their values on the generating set, we get that the map is also injective. Lastly, we must check that it is an R-map. Let $\psi(f) = f(1)$. Then $\varphi(rf) = (rf)(1) = rf(1) = r\psi(f)$ since $\mathrm{Hom}_R(R, M)$ has the structure of a group ring.

Exercise 0.12 (17)**.** Suppose M is an R-module which has a basis X. Then let $\mu\colon X \to M$ be the inclusion. Now for any function $X \to N$ for N another R-module, we have that it extends uniquely by linearity to a function $M \to N$. Namely, if $f\colon X \to N$ is the function, then the R-map $\tilde{f}\colon M \to N$ must be

$$\tilde{f}\left(\sum_{x\in X} c_x x\right) = \sum_{x\in X} c_x f(x)$$

which is clearly R-linear.
Conversely, suppose M is a free R-module on the set X, given with the map $\mu\colon X \to M$. We claim that $\mu(X)$ is an R-linarly independent set which generates M, i.e., a basis. To show that it generates M, first note that the inclusion $X \to \langle X\rangle$ gives a map $f\colon M \to \langle X\rangle$ such that

$$\begin{tikzcd} X \arrow[r, "\mu"] \arrow[dr, "\iota"'] & M \arrow[d, "f"] \\ & \langle X\rangle \end{tikzcd}$$

commutes. But by extending linearly, a map on X can be extended to $\langle X\rangle$, so μ extends to a map $\tilde{\mu}\colon \langle X\rangle \to M$ such that

$$\begin{tikzcd} X \arrow[r, "\mu"] \arrow[dr, "\iota"'] & M \arrow[d, shift left, "f"] \\ & \langle X\rangle \arrow[u, shift left, "\tilde{\mu}"] \end{tikzcd}$$

commutes. Then $f\tilde{\mu}\iota = f\mu = \iota$, which, by the universal of freeness of $\langle X\rangle$ on X, gives that $f\tilde{\mu} = \mathbb{1}_{\langle X\rangle}$. Likewise, $\tilde{\mu}f\mu = \tilde{\mu}\iota = \mu$, so by universality of freeness of M on X, we get $\tilde{\mu}f = \mathbb{1}_M$. Thus f is indeed an isomorphism.

Exercise 0.13 (20)**.**

(1) Let U be the set of all $f(N)$ for $f\colon M \to R$ an R-map. We order U by inclusion, so $f(N) \le g(N)$ iff $f(N) \subset g(N)$. Suppose $f_1(N) \le f_2(N) \le \ldots$ is a tower. By theorem 1.12 in the notes, every submodule of a free R-module is free, so N is free. Suppose $v_1, \ldots, v_k$ is a basis for N. Then let $f_1(v_{i_1}), \ldots, f_1(v_{i_r})$ be a basis for $f_1(N)$. Now, for all i, $f_i(N)$ has dimension at most k, so adjoining repeatedly certain $f_j\left(v_{i_{j_t}}\right)$, we obtain a basis for $f_i(N)$ for all $i \ge K \in \mathbb{N}$ for some K. Then $f_K(N)$ is an upper bound. By Zorn's lemma, there thus exists a maximal element $u(N)$ for some map $u\colon M \to R$.

(2) If $a_1 = 0$ then $u(N) = \{0\}$, so every $f\colon M \to R$ would have to vanish on N. However, if $N \neq 0$, then choosing a basis as above, $v_1, \dots, v_k$, we can define a map $\tilde{g}\colon \{v_1, \dots, v_k\} \to R$ by $v_i \mapsto 1_R$ and then extending linearly to a map $g\colon N \to R$ which is nontrivial, hence $g(N) \neq 0$, and then we can extend this again to a map on M by mapping the rest of M to 0. Hence $a_1 \neq 0$.

(3) Since $\pi_i \in \operatorname{Hom}_R(M, R)$, we have that $\pi_i(N) \subset u(N) = (a_1)$, so in particular, $\pi_i(e_1') = a_1\alpha_i$ for some $\alpha_i \in R$.

(4) If $e_1' = c_1x_1 + \ldots + c_nx_n$, then $a_1\alpha_i = \pi_i(e_1') = c_i$, so $e_1' = a_1\sum_i \alpha_i x_i = a_1e_1$.

(5)
$$a_1u(e_1) = u(a_1e_1) = u(e_1') = a_1$$
hence $a_1(u(e_1) - 1) = 0$ and since $a_1 \neq 0$ and R is an integral domain, we have $u(e_1) = 1$. Now, define $\varphi(x) = (x - u(x)e_1, u(x))$. Then $(0,0) = \varphi(x) = (x - u(x)e_1, u(x))$ if and only if $u(x) = 0$ and hence $x = 0$. So φ is injective. Now suppose $(x, y) \in \ker u \oplus R$. Then $u(ye_1) = y$ and $ye_1 - u(ye_1)e_1 = 0$, so $\varphi(ye_1) = (0, y)$. Meanwhile, $x \in \ker u$, so $\varphi(x) = (x, 0)$. Hence $\varphi(x + ye_1) = (x, y)$, so φ is surjective. Lastly, $\varphi(x + x') = (x + x' - u(x + x')e_1, u(x + x')) = (x - u(x)e_1, u(x)) + (x' - u(x')e_1, u(x')) = \varphi(x) + \varphi(x')$ and $\varphi(rx) = (rx - u(rx)e_1, u(rx)) = (r(x - u(x)e_1), ru(x)) = r(x - u(x)e_1, u(x)) = r\varphi(x)$, so φ is an R-map. Thus $M \approx \ker u \oplus R$.

(6) We can repeat the above process on $M' \cap N$ to decompose M' into $M'' \oplus R$ with some isomorphism $\varphi\colon M' \approx M'' \oplus R$ with $\varphi(x) = (x - u'(x)e_2, u'(x))$ where $u'(e_2) = 1$ and $\alpha_2 e_2 \in M' \cap N$. Thus,
$$M \approx \tilde{M} \oplus \underbrace{R \oplus \ldots \oplus R}_{n \text{ times}}$$
under the isomorphism
$$x \mapsto \Big(x - u(x)e_1 - u^{(1)}(x)e_2 - \ldots - u^{(n-1)}(x)e_n, u^{(1)}(x), u^{(2)}(x), \ldots, u^{(n-1)}(x)\Big).$$
How can we show that $a_1e_1, \dots, a_ne_n$ are now linearly independent? Suppose $\sum a_ie_i = 0$. Then this is mapped under the isomorphism to
$$0 = \Big(\sum a_ie_i - a_1e_1 - \ldots - a_ne_n, a_1, \ldots, a_n\Big)$$
so $a_i = 0$ for all i.

Exercise 0.14 (21)**.** A free module F of rank n is isomorphic to R^n, so we get from the first isomorphism theorem that
$$M \approx R^n / (\langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \ldots \oplus \langle a_m \rangle) \approx R^k \oplus R/(a_1) \oplus \ldots \oplus R/(a_m)$$
where $\ker \varphi = \langle a_1e_1, \dots, a_ne_n \rangle$ as in the previous exercise.
Apply the Chinese Remainder Theorem