MODEL ANSWERS TO THE SIXTH HOMEWORK

1. Suppose that m and n are in M. Then

$$\begin{aligned}\phi(m+n) &= r(m+n)\\ &= rm+rn\\ &= \phi(m)+\phi(n).\end{aligned}$$

Thus ϕ is additive. Now suppose that $s \in R$. Then

$$\begin{aligned}\phi(sm) &= r(sm)\\ &= (rs)m\\ &= s(rm)\\ &= s\phi(m).\end{aligned}$$

Thus ϕ is R-linear.
2. Let N be a submodule of M. Then N is an additive subgroup of M and so it is non-empty and closed under addition. It is also closed under multiplication by definition of the inherited rule for multiplication.
Now suppose that N is non-empty and closed under addition and scalar multiplication. As N is non-empty and closed under addition, it follows that it is an additive subgroup. The other axioms obviously hold in N, since they hold in the larger set M.
Thus N is a submodule.
3. Let K be the kernel of ϕ. As ϕ is a homomorphism of the underlying additive groups, it follows that K is an additive subgroup. Suppose that $r \in R$ and $k \in K$. We have

$$\begin{aligned}\phi(rk) &= r\phi(k)\\ &= r\cdot 0\\ &= 0.\end{aligned}$$

Thus $rk \in K$. It follows that K is closed under scalar multiplication. Therefore K is a submodule.
4. Let M_i be a collection of submodules of an R-module M and let N be their intersection. Then N is an additive subgroup as each M_i is an additive subgroup. Suppose that $r \in R$ and $n \in N$. Then for every $i \in I$, $n \in M_i$. As M_i is an R-module, it follows that $rn \in M_i$. As this is true for every i, in fact $rn \in N$. Thus N is closed under scalar multiplication and so it is a submodule.

5. Let M_i, $i \in I$ be the set of all submodules of M that contain X. Then N, the intersection of every M_i is a submodule of M, which contains X. As $N \subset M_i$ it is clearly the smallest such submodule.
6. Let F be the set of all functions from X to M. We need to define a rule of addition and scalar multiplication. Suppose that f and g are elements of F. Define $f + g$ as the pointwise sum, so that

$$(f + g)(x) = f(x) + g(x).$$

Similarly, given $r \in R$ and $f \in F$, define rf as the pointwise product,

$$(rf)(x) = r(f(x)).$$

It is an easy matter to check that with this rule of addition and scalar multiplication, F becomes an R-module.
7. Let $H = \mathrm{Hom}_R(M, N)$ be the set of all R-module homomorphisms. Then H is a subset of F, the set of all functions from M to N. It suffices to prove that H is non-empty and closed under addition and scalar multiplication.
First note that the zero map, which sends every element of M to the zero element of N, is R-linear. Thus H is certainly non-empty. Suppose that f and g are elements of H. We need to prove that $f+g$ is R-linear. Let m and n be elements of M and r and s be elements of R. We have

$$\begin{aligned}(f + g)(rm + sn) &= f(rm + sn) + g(rm + sn)\\ &= rf(m) + sf(n) + rg(m) + sg(n)\\ &= rf(m) + rg(m) + sf(m) + sf(n)\\ &= r(f + g)(m) + s(f + g)(n).\end{aligned}$$

Thus $f + g$ is indeed R-linear. It is equally easy and just as formal to prove that rf is R-linear. Thus H is closed under addition and scalar multiplication and so H is an R-module.
8. Since the arbitrary intersection of ideals is an ideal, it suffices to prove that I is an ideal, in the case that X contains one point x. Clearly $0 \in I$. Thus I is non-empty. Suppose that i and j are elements of I. Then

$$\begin{aligned}(i + j)x &= ix + jx\\ &= 0 + 0 = 0.\end{aligned}$$

Thus $i + j \in I$ and I is closed under addititíon. Now suppose that $r \in R$ and $i \in I$. Then

$$\begin{aligned} ri(x) &= r(ix) \\ &= r0 \\ &= 0. \end{aligned}$$

Thus $ri \in I$ and I is an ideal. Here is another way to conclude that I is an ideal. Let

$$\phi \colon R \longrightarrow \mathrm{Hom}_R(M, M)$$

be the natural map which sends an element R to the R-linear map, $m \longrightarrow rm$. It is easy to see that ϕ is R-linear. Replacing M by the module generated by X, note that an element $r \in R$ is in I if and only if $\phi(r)$ is the zero map. Thus I is the kernel of ϕ. It also follows that I is also the annihilator of $\langle X \rangle$.

9. (i) Easy.

(ii) First we write down the inverse of $1 - x$. By a formal analogy with geometric series, we guess the answer is

$$1 + x + x^2 + \dots.$$

We check this. We need to compute the product,

$$(1 - x)(1 + x + x^2 + \dots).$$

The constant term is clearly 1. In degree n, there are two terms, one coming from x^n from the second bracket and 1 from the first, which gives coefficient 1, and the second one coming from x^{n-1} from the second bracket and $-x$ from the first, which gives coefficient -1. In total we then have $0 = 1 - 1$.

In general, then, suppose that we have

$$f(x) = a + bx + \dots,$$

where a is a unit in R. Multiplying through by the inverse of a, we might as well assume that

$$f(x) = 1 + bx + \dots = 1 - y,$$

for some power series y. Now formally we guess that the inverse is

$$1 + y + y^2 + \dots.$$

The only subtle thing to be careful of is that this involves an infinite sum, which does not a priori make sense. On the other hand, note that to compute the coefficient of x^n, (after substituting for y) we only need the first $n+1$ terms. Thus each coefficient can be computed using only finitely many terms and so the sum does make sense. With this said, it is then clear that

$$(1 + y + y^2 + \dots)(1 - y) = 1,$$

for the same reasons as before. Thus the inverse of f is $1+y+y^2+\dots$.
(iii) Easy. Suppose that

$$f(x) = ax^d + \dots \qquad \text{and} \qquad g(x) = bx^d + \dots$$

for some a and b, where dots indicate higher terms. In this case

$$f(x)g(x) = abx^{d+e} + \dots$$

and since R is an integral domain, $ab \neq 0$.
(iv) Immediate from (iii).
(v) Define a function

$$d\colon F[\![x]\!] - \{0\} \longrightarrow \mathbb{N} \cup \{0\}$$

by sending a power series to its degree. We have to check two things. The first follows immediately from (iii).
Now we have to check that if $f(x)$ and $g(x)$ are two power series, then we may find $q(x)$ and $r(x)$ such that

$$g(x) = q(x)f(x) + r(x),$$

where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $f(x)$. There are two cases. If the degree of $g(x)$ is less than the degree of $f(x)$ there is nothing to do; take $q(x) = 0$ and $r(x) = g(x)$. In this case the fact that $r(x)$ has degree less than $f(x)$ is clear.
Otherwise I claim that $f(x)$ divides perfectly into $g(x)$. To see this, note that we have

$$\begin{aligned} f(x) &= ax^d + \dots \\ &= x^d(a + \dots) \\ &= x^d u. \end{aligned}$$

Here as $a \neq 0$ and F is a field, a is a unit. Thus u is a unit. But then by the same token, $g(x) = x^e v$, where e is the degree of g and v is a unit. Thus

$$g(x) = q(x)f(x),$$

where $q(x) = x^{e-d}vw$ and w is the inverse of u. Thus we have a Euclidean Domain.
(vi) Follows from (v), as every Euclidean Domain is a UFD. Note though, that much more is true. The only prime element of $F[\![x]\!]$ is x and the factorisation of f above is given by $x^d u$.

10. (ii) Define $R[\![x_1, x_2, \dots, x_n]\!]$ as for the polynomial ring, but erasing any mention of finiteness conditions, so that a general element of $R[\![x]\!]$ is of the form

$$\sum a_I x^I,$$

where the sum ranges over all multi-indices. As before there is a canonical isomorphism,

$$R[\![x_1, x_2, \dots, x_n]\!] \simeq R[\![x_1, x_2, \dots, x_{n-1}]\!][\![x_n]\!].$$

The result then follows by a straightforward induction.

Challenge Problems:

10 (i) We follow the proof of Hilbert's Basis Theorem, although there are some twists to the story. Let $I \subset R[\![x]\!]$ be an ideal. Let $J \subset R$ be the set of leading coefficients (that is, the coefficients of the lowest non-zero term), union zero.

I claim that J is an ideal. It is non-empty as it contains 0. If a and b are in J, then we may find $f(x)$ and $g(x)$ in I such that $f(x)$ has leading term ax^d and $g(x)$ has leading term bx^e. Multiplying by an appropriate power of x, we may assume that $d = e$. As $f + g \in I$, it follows that $a + b \in J$. Similarly $ra \in J$. Thus J is an ideal.

As R is Noetherian, we have

$$J = \langle a_1, a_2, \dots, a_k \rangle,$$

for some $a_1, a_2, \dots, a_k \in J$. Pick $f_i(x) \in I$ with leading coefficient a_i. Let m be the maximum of the degrees of $f_1, f_2, \dots, f_k$.

Note that there is a R-module homomorphism

$$\pi \colon R[\![x]\!] \longrightarrow R[x],$$

which sends a power series $p(x)$ to the polynomial of degree less than m, obtained by setting all of the coefficients of $p(x)$ of degree at least m to zero. The image M of π is the set of all polynomials of degree less than m. M is the R-submodule generated by 1, x, x^2, $\dots$, x^{m-1}. As R is Noetherian, M is Noetherian, as it is finitely generated. If N is the image of I then N is a submodule of M. Thus N is finitely generated. Pick generators and let $h_1, h_2, \dots, h_l$ be the inverse image of these generators in $R[\![x]\!]$. Then $h_1, h_2, \dots, h_l$ are power series of degrees at most $m - 1$.

Now suppose that $p(x)$ is a power series. As $\pi(p(x))$ is a polynomial of degree at most $m - 1$ belonging to N, it follows that we may write

$$p(x) = p_0(x) + p_1(x),$$

where $p_0(x)$ is a power series of degree less than m, a linear combination of $h_1, h_2, \dots, h_l$ and $p_1(x)$ is a power series of degree at least m. It suffices to prove that $p_1(x)$ is in the ideal generated by $f_1, f_2, \dots, f_k$, since then $f_1, f_2, \dots, f_k$ and $h_1, h_2, \dots, h_l$ clearly generate I. Thus we may as well assume that $f(x)$ has degree at least m. We define a sequence of polynomials, $p_1^{(j)}(x)$, $p_2^{(j)}(x)$, $\dots$, $p_k^{(j)}(x)$, such that if we put

$$r^{(j)}(x) = f(x) - \sum_i p_i^{(j)}(x) f_i(x),$$

then as we increase j, the degree of r goes up and the initial coefficients of $p_i^{(j)}(x)$, stabilise. Supposing that we can do this, taking the limit (in the obvious sense), then the polynomials become power series and the degree of r goes to infinity, which is the same as to say that in fact f is a linear combination of the $f_1, f_2, \dots, f_k$. By induction on the degree, it suffices to increase the degree of r by one, that is, to kill the leading coefficient of f. Suppose that the leading coefficient of f is a. Then $a \in J$. Pick $r_1, r_2, \dots, r_k$ such that

$$a = \sum r_i a_i.$$

Then the coefficient of x^d for

$$f(x) - \sum_i r_i x^{d-d_i} f_i(x)$$

is zero by construction and we are done.

11. Let M_n be the kernel of ϕ^n. Note that we have an ascending chain,

$$M_1 \subset M_2 \subset M_3 \subset \dots.$$

As M is Noetherian, this chain must stabilise, so that $M_n = M_{n+1}$ for some n. Now suppose that M_1 is not trivial. We will define $m_n \in M_n - M_{n-1}$ recursively, so that $\phi(m_n) = m_{n-1}$. This will obviously be a contradiction. By assumption, there is $m_1 \in M_1$, such that $m_1 \neq 0$. Suppose we have defined $m_1, m_2, \dots, m_n$. As ϕ is surjective, there is an $m_{n+1} \in M$ such that $\phi(m_{n+1}) = m_n$. As $m_n \in M_n$, it is immediate that $m_{n+1} \in M_{n+1}$ but not in the smaller subset. This completes the construction and the contradiction.

Thus M_1 is the trivial module and ϕ must be injective. In this case ϕ must be a bijection, whence an automorphism.