MODEL ANSWERS TO THE SECOND HOMEWORK

1. (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.
(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-indexes. 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.
2. Let M_n be the kernel of ϕ^n. Note that we have an ascending chain,

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

Suppose that $M_1 \neq 0$. We will define $m_n \in M_n - M_{n-1}$ recursively, so that $\phi(m_n) = m_{n-1}$. 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 M_n. Thus we have a strictly increasing sequence of submodules of M. This contradicts the fact that M is Noetherian.
Thus M_1 is the trivial module and ϕ must be injective. In this case ϕ must be a bijection, so that it is an automorphism.
3. Let I be the ideal generated by S. As $S \subset I$ we surely have

$$V(I) \subset V(S).$$

On the other hand, if $f \in I$ then we may find $f_1, f_2, \ldots, f_i \in S_0$ and $g_1, g_2, \ldots, g_k \in k[x_1, x_2, \ldots, x_n]$ such that

$$f = \sum f_i g_i.$$

If $a = (a_1, a_2, \ldots, a_n) \in V(S)$ then $f_i(a) = 0$ so that $f(a) = 0$. It follows that

$$V(S) \subset V(I) \qquad \text{so that} \qquad V(I) = V(S).$$

By Hilbert's basis theorem we may find $h_1, h_2, \ldots, h_k \in I$ such that

$$I = \langle h_1, h_2, \ldots, h_k \rangle.$$

As above,

$$V(I) = V(h_1, h_2, \ldots, h_k).$$

On the other hand, for each j we may find $f_i^{(j)} \in S$, $1 \leq i \leq p_j$ such that h_j is a linear combination, with coefficients in $k[x_1, x_2, \ldots, x_n]$, of $f_i^{(j)} \in S$, $1 \leq i \leq p_j$. Let S_0 be the set of all polynomials, $f_i^{(j)}$, $1 \leq j \leq k$ and $1 \leq i \leq p_j$.
Then $S_0 \subset S$ and

$$V(S_0) = V(I) = V(S).$$