MODEL ANSWERS TO THE NINTH HOMEWORK

1. (i) Easy.
   (ii) First we write down the inverse of $1 - x$. By a formal analogy with geometric series, we guess the answer is
   $$1 + x + x^2 + \ldots.$$
   We check this. We need to compute the product,
   $$(1 - x)(1 + x + x^2 + \ldots).$$
   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
   $$f(x) = a + bx + \ldots,$$
   where $a$ is a unit in $R$. Multiplying through by the inverse of $a$, we might as well assume that
   $$f(x) = 1 + bx + \cdots = 1 - y,$$
   for some power series $y$. Now formally we guess that the inverse is
   $$1 + y + y^2 + \ldots.$$
   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
   $$(1 + y + y^2 + \ldots)(1 - y) = 1,$$
   for the same reasons as before. Thus the inverse of $f$ is $1 + y + y^2 + \ldots$.
   (iii) Easy. Suppose that
   $$f(x) = ax^d + \ldots \quad \text{and} \quad g(x) = bx^d + \ldots$$
   for some $a$ and $b$, where dots indicate higher terms. In this case
   $$f(x)g(x) = abx^{d+e} + \ldots$$
   and since $R$ is an integral domain, $ab \neq 0$. 

(iv) Immediate from (iii).
(v) Define a function
\[ d: F[x] \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\} \]
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
\[
\begin{align*}
f(x) &= ax^d + \ldots \\
&= x^d(a + \ldots) \\
&= x^d u.
\end{align*}
\]
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 \( x^d u \).

2 (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
\[ J = \langle a_1, a_2, \ldots, a_k \rangle, \]
for some $a_1, a_2, \ldots, a_k \in J$. Pick $f_i(x) \in I$ with leading coefficient $a_i$. Let $m$ be the maximum of the degrees of $f_1, f_2, \ldots, f_k$. Now suppose that $p(x)$ is a power series. We may write

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

where $p_0(x)$ is a polynomial of degree less than $m$ (degree as a polynomial) and $p_1(x)$ is a power series of degree at least $m$. Suppose that we can show that the power series $p_1(x)$ lies in the ideal generated by $f_1, f_2, \ldots, f_k$. Let $M$ be the $R$-submodule generated by $1, x, x^2, \ldots, x^{m-1}$. Then $M$ is a finitely generated module over a Noetherian ring $R$. Thus $I \cap M$ is finitely generated. Pick generators $h_1, h_2, \ldots, h_l$. Then

$$p_0(x) = \sum r_i h_i$$

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

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

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 $f_1, f_2, \ldots, f_k$. 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 $r_1, r_2, \ldots, r_k$ such that

$$a = \sum r_i a_i.$$  

Then the coefficient of $x^d$ for

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

is zero by construction and we are done.

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

$$\sum a_f x^f,$$
where the sum ranges over all multi-indexes. As before there is a canonical isomorphism,
\[ R[x_1, x_2, \ldots, x_n] \simeq R[x_1, x_2, \ldots, x_{n-1}][x_n]. \]
The result then follows by a straightforward induction.

3. Let \( M_n \) be the kernel of \( \phi^n \). Note that we have an ascending chain,
\[ M_1 \subset M_2 \subset M_3 \subset \ldots. \]
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 \( m_1, m_2, \ldots, m_n \). As \( \phi \) 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 \( \phi \) must be injective. In this case \( \phi \) must be a bijection, whence an automorphism.

4. (a) We have to define an \( R \)-linear map,
\[ \phi: M \otimes_R N \longrightarrow N \otimes_R M. \]
By the universal property of \( M \otimes_R N \), it suffices to exhibit a bilinear map
\[ f: M \times R N \longrightarrow N \otimes_R M \]
The composition of \( u: N \times R M \longrightarrow N \otimes_R M \) and the map
\[ M \times N \longrightarrow N \times M \text{ which sends } (m, n) \longrightarrow (n, m) \]
will obviously do. The inverse map is constructed similarly. The composition either way is easily seen to be the identity, either because it satisfies the universal property of the identity, or because it is the identity map on generators.
(b) One can prove this as above. Here is a much sneakier way to proceed. Note the canonical isomorphism,
\[ (M \times N) \times R P \simeq M \times (N \times P). \]
On the other hand, given either triple product, one can consider trilinear maps, that is, maps that are linear in all three variables. It is not hard to check that \( M \otimes_R N \otimes_R P \) satisfies the corresponding universal property. Similarly for \( M \otimes_R (N \otimes_R P) \). Thus they are canonically isomorphic.
(c) We are going to show that $M$ satisfies the properties of the tensor product. First we need to exhibit a bilinear map,

$$u: R \times M \longrightarrow M$$

The definition of $u$ is almost forced, send $(r, m)$ to $rm$. This is clearly a bilinear map. Now suppose we are given a bilinear map

$$f: R \times M \longrightarrow N.$$

Define

$$\phi: M \longrightarrow N$$

by sending $m$ to $f(1,m)$. We check that the diagram,

$$\begin{array}{ccc}
R \times M & \xrightarrow{f} & N \\
\downarrow u & & \downarrow \phi \\
M & & \\
\end{array}$$

commutes. Suppose that $(r, m) \in R \times M$. Then

$$\phi \circ u(r, m) = \phi(rm)$$

$$= f(1, rm)$$

$$= rf(1, m)$$

$$= f(r, m),$$

where we applied bilinearity of $f$ twice. Thus the diagram commutes. Finally we check that $\phi$ is $R$-linear. Suppose that $m_1, m_2 \in M$. Then

$$\phi(m_1 + m_2) = f(1, m_1 + m_2)$$

$$= f(1, m_1) + f(1, m_2)$$

$$= \phi(m_1) + \phi(m_2).$$

Now suppose that $r \in R$ and $m \in M$. Then

$$\phi(rm) = f(1, rm)$$

$$= rf(1, m)$$

$$= r\phi(m).$$

Thus $\phi$ is $R$-linear. Thus $M$ satisfies all the properties of a tensor product and the result is clear.

(d) First we define a bilinear map

$$M \times (N \oplus P) \longrightarrow (M \otimes N) \oplus (M \otimes P),$$

by sending $(m, (n, p))$ to $(m \otimes n, m \otimes p)$. It is easy to check that this is bilinear. This gives us a map one way. To get a map the other way, it
suffices, by definition of the direct sum and then of the tensor product and by symmetry, to exhibit a bilinear map

\[ M \times N \longrightarrow M \otimes_R (N \oplus P). \]

For this send \((m, n)\) to \(m \otimes (n, 0)\). Again it is clear that this map is bilinear and that the induced \(R\)-linear maps are inverse to each other.

(e) As \(F \simeq R^n\), this follows immediately from (c) and (d), by induction on \(n\).

5. Let \(d\) be the gcd of \(m\) and \(n\). I claim that

\[ \mathbb{Z}_m \otimes \mathbb{Z}_m \simeq \mathbb{Z}_d. \]

The proof proceeds in two steps. First observe that

\[
\begin{align*}
m(1 \otimes 1) &= m \otimes 1 \\
&= 0 \otimes 1 \\
&= 0.
\end{align*}
\]

Similarly \(n(1 \otimes 1) = 0\). As \(\mathbb{Z}\) is a PID, we may find \(r\) and \(s\) such that

\[ d = rm + sn. \]

Thus

\[
\begin{align*}
d(1 \otimes 1) &= (rm + sn)1 \otimes 1 \\
&= r(m(1 \otimes 1) + s(n(1 \otimes 1)) \\
&= 0.
\end{align*}
\]

Thus \(\mathbb{Z}_m \otimes \mathbb{Z}_m\) is surely isomorphic to a subgroup of \(\mathbb{Z}_d\). It remains to check that no smaller multiple of \(1 \otimes 1\) is zero. The best way to prove this is to use the universal property. Let

\[ f : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_d \]

be the map that sends \((a, b)\) to \(ab\). As \(d\) divides both \(m\) and \(n\), this map is indeed well-defined. On the other it is clearly bilinear. By the universal property, it induces an \(R\)-linear map

\[ \phi : \mathbb{Z}_m \otimes \mathbb{Z}_m \longrightarrow \mathbb{Z}_d. \]

This map sends \(1 \otimes 1\) to \(f(1, 1)\), that is, 1. Hence if \(k(1 \otimes 1) = 0\), then \(k\) is zero in \(\mathbb{Z}_d\) and so \(d\) divides \(k\). The result follows.

6. We first prove that \(M \otimes_R N\) is finitely generated. Suppose that \(x_1, x_2, \ldots, x_m\) and \(y_1, y_2, \ldots, y_n\) are generators of \(M\) and \(N\). Then I
claim that $x_i \otimes y_j$ are generators of $M \otimes N$. Indeed this is generated by elements of the form $m \otimes n$, and so it is enough to observe that if

$$m = \sum r_i x_i \quad \text{and} \quad n = \sum s_i n_i,$$

then

$$m \otimes n = \sum r_i s_j x_i \otimes y_j,$$

where of course we use bilinearity to distribute the sum.

If $R$ is Noetherian then $M \otimes^R N$ is a finitely generated module over a Noetherian ring so that $M \otimes^R N$ is Noetherian.