Algebra I - Homework 8

Pablo Sánchez Ocal

November 21st, 2016

Exercise 1

Prove that $f(x) = x^5 + 6x^4 + 9x^2 - 12 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

We know that $\mathbb{Z}$ is a unique factorization domain and that its field of fractions is $\mathbb{Q}$. Since $f(x)$ is monic, we can apply [1, Lemma 6.13 (p. 163)] and thus it will be irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$. Notice that $p = 3$ is prime and divides $a_0 = -12$, $a_1 = a_3 = 0$, $a_2 = 9$ and $a_4 = 6$ but does not divide $a_5 = 1$, and $p^2 = 9$ does not divide $a_0 = -12$. Thus by Eisenstein's Criterion [1, Theorem 6.15 (p. 164)] we have that $f(x)$ is irreducible in $\mathbb{Q}[x]$, hence it is also irreducible in $\mathbb{Z}[x]$, proving the desired result.

Exercise 2

Prove that $\mathbb{Q}[[x]]$ is a principal ideal domain and describe all its ideals.

First, note that since $\mathbb{Q}$ is a field (and thus every element is a unit), by [1, Proposition 5.9 (p. 155)] the units in $\mathbb{Q}[[x]]$ are the power series with nonzero constant term. Moreover, an element in $\mathbb{Q}[[x]]$ is not a unit if and only if it belongs to $(x) = \{xf(x) : f(x) \in \mathbb{Q}[[x]]\}$ (notice that $(x) \neq \mathbb{Q}[[x]]$ since $1 \notin (x)$):

$\Leftarrow$) Clearly $xf(x)$ has no constant term for every $f(x) \in \mathbb{Q}[[x]]$, thus it is not a unit.

$\Rightarrow$) Let $g(x) = \sum_{i=1}^{\infty} g_i x^i \in \mathbb{Q}[[x]]$ a non unit. Let $f(x) = \sum_{i=0}^{\infty} g_{i+1} x^i \in \mathbb{Q}[[x]]$, we have that $g(x) = xf(x) \in (x)$.

Moreover, considering $f(x), g(x) \in \mathbb{Q}[[x]]$ we have a division algorithm: if both are of finite degree, this is the usual division algorithm as in $\mathbb{Q}[x]$, if at least one is of infinite degree we can consider $h(x) = \sum_{i=0}^{\infty} h_i x^i$ a general power series, and multiply imposing equality(say $f(x) = \sum_{i=0}^{\infty} f_i x^i$ and $g(x) = \sum_{i=0}^{\infty} g_i x^i$):

$$g(x)h(x) = f(x) \iff \sum_{i=0}^{\infty} g_i x^i \sum_{i=0}^{\infty} h_i x^i = \sum_{i=0}^{\infty} \left(\sum_{s+t=i} g_s h_t \right) = \sum_{i=0}^{\infty} f_i x^i,$$

hence imposing equality term by term we can solve:

$$h_0 = \frac{f_0}{g_0}, \quad h_1 = \frac{f_1 - g_1 h_0}{g_0}, \quad h_2 = \frac{f_2 - g_1 h_1 - g_2 h_0}{g_0}, \quad \cdots$$

and since from the equation determining b_j and the one determining b_{j+1} we only add one unknown and we are working with coefficients in $\mathbb{Q}$, we can divide and solve to find the power series $h(x)$. Notice now this is still true if we consider $g_0 = 0 = f_0$, and in this case we will have $h_0 = 0$.

Then, consider I a proper ideal of $\mathbb{Q}[[x]]$:

1. If it has an element $g(x)$ with the smallest degree, then by the above all elements of infinite degree are divisible by it, and if $f(x)$ is an element of finite degree, the usual division algorithm yields $f(x) = q(x)g(x)+r(x)$ and since $r(x) = f(x)-q(x)g(x) \in I$ with $\deg(r) \leq \deg(g)$, we must have $r(x) = 0$ and thus $g(x)$ divides $f(x)$. Hence $I = (g(x))$.

   Notice that in particular I contains all non unit elements of infinite degree.

2. If I has all elements with infinite degree, then by the above they all divide each other, meaning that for any $g(x) \in I$ we have $I = (g(x))$.

   Notice that in particular I contains all non unit elements of infinite degree.

This proves that $\mathbb{Q}[[x]]$ is a principal ideal domain, and characterizes the proper ideals as having form $(g(x))$ with $1 \leq \deg(g) \leq \infty$ and $g(x)$ without constant term (notice the only but important restrictions are that the degree is greater than one, and that it has no constant term, since when the degree is zero or it has a constant term the ideal is the whole $\mathbb{Q}[[x]]$), with the non proper ideals being (1) and (0).

Exercise 3

Prove that $f(x) = x^2 + 3x + 2$ is irreducible in $\mathbb{Z}[[x]]$ but not in $\mathbb{Z}[x]$.

We first notice that $a_0 = 2$ is irreducible in $\mathbb{Z}$, and then applying [1, Proposition 5.9 (p. 155)] we obtain directly that $f(x)$ is irreducible in $\mathbb{Z}[[x]]$.

Moreover, notice that both -2 and -1 are roots of $f(x)$, and using Ruffini's Rule to divide polynomials we obtain that:

$$(x + 2)(x + 1) = x^2 + 3x + 2 = f(x),$$

hence since $x + 2 \in \mathbb{Z}[x]$ and $x + 2 \in \mathbb{Z}[x]$ are not units because they have nonzero first coefficient, we get that $f(x)$ is reducible in $\mathbb{Z}[x]$.

Exercise 4

Let F be a field and $f, g \in F[x]$ with $\deg(g) \geq 1$. Prove that there exist unique polynomials $f_0, \ldots, f_r \in F[x]$ such that $\deg(f_i) < \deg(g)$ for $0 \leq i \leq r$ and $f = f_0 + f_1 g + \cdots + f_r g^r$. To prove this, we will exploit the Division Algorithm [1, Theorem 6.2 (p. 158)].

There are two cases, depending on the degree of f:

1. If $\deg(f) < \deg(g)$, then $f = f + 0g$, that is $r = 0$ and $f_0 = f$, and clearly such f is unique.

2. Suppose $\deg(f) = \deg(g)$, then the division algorithm gives us unique polynomials $q, r \in F[x]$ with $f = qg + r$ and $\deg(r) < \deg(g)$. Moreover, we have (since F has no zero divisors) that $\deg(f) = \deg(qg) = \deg(q) + \deg(g)$, meaning that $\deg(q) = 0 < \deg(g)$. Then $r = 1$, $f_0 = r$, $f_1 = q$.

3. Suppose $\deg(f) > \deg(g)$, then the division algorithm gives us unique polynomials $q_0, r_0 \in F[x]$ with $f = q_0 g + r_0$ and $\deg(r_0) < \deg(g)$. Moreover, we have (since F has no zero divisors) that $\deg(f) = \deg(q_0 g) = \deg(q_0) + \deg(g)$, meaning that $\deg(q_0) < \deg(f)$. Thus, we obtained another polynomial with degree strictly less than the original. Applying the division algorithm to q_0, we obtain unique polynomials $q_1, r_1 \in F[x]$ with $q_0 = q_1 g + r_1$ and $\deg(r_0) < \deg(g)$. By the above, $\deg(q_1) < \deg(q_0)$ and $f = q_1 g^2 + r_1 g + r_0$. As long as $\deg(q_i) > \deg(g)$, we can apply the division algorithm to strictly decrease the degree, meaning that this process will finally come to either a quotient with $\deg(q_k) < \deg(g)$, in which case we apply the first case of this list, or with $\deg(q_k) = \deg(g)$, in which case we apply the second case of this list. In either case, we end up after s steps with the following:

   $$f = r_0 + r_1 g + \cdots + q_{s-1} g^s \Longrightarrow f = f_0 + f_1 g + \cdots + f_s g^s$$

   by defining $f_i = r_i$ when $0 \leq i \leq s-1$ and $f_s = q_{s-1}$. Notice that all the f_i for $0 \leq i \leq s$ are unique since every r_i and q_i for $0 \leq i \leq s$ have uniqueness given by the division algorithm that we applied.

Exercise 5

Let $M_n(R)$ be the ring of matrices over a ring R. We prove that $M_n(R)[x] \cong M_n(R[x])$.

First, we give an idea of the general expression of elements in those rings, and see that we only need a few remarks to almost justify this isomorphism. An element $A(x) \in M_n(R)[x]$ is of the form $A(x) = A_0 + A_1x + \cdots + A_kx^k$ where $A_i \in M_n(R)$ are matrices over the ring R for every $0 \leq i \leq k \in \mathbb{N}$. An element $A \in M_n(R[x])$ has components of the form $A_{ij} = f_{ij}(x) = f_{ij}^0 + f_{ij}^1x + \cdots + f_{ij}^kx^k$ where $f_{ij}^t \in R[x]$ are polynomials over the ring R for every $0 \leq t \leq k \in \mathbb{N}$. We will define a bijective function $\varphi : M_n(R)[x] \longrightarrow M_n(R[x])$ satisfying $\varphi(A(x)B(x)) = \varphi(A(x))\varphi(B(x))$ and $\varphi(A(x) + B(x)) = \varphi(A(x)) + \varphi(B(x))$, and this will prove the desired isomorphism.

First, note that given a matrix $M \in M_n(R)$, we can multiply all its components by the "variable" x^t with $t \in \mathbb{N}$, obtaining what we will denote as $[Ax^t]$:

$$M = \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & & \vdots \\ m_{n1} & \cdots & m_{nn} \end{pmatrix} \quad \Longrightarrow \quad [Mx^t] = \begin{pmatrix} m_{11}x^t & \cdots & m_{1n}x^t \\ \vdots & & \vdots \\ m_{n1}x^t & \cdots & m_{nn}x^t \end{pmatrix}.$$

This gives us a coherent notation for treating matrix multiplication of this form in $M_n(R[x])$, since for $A, B \in M_n(R)$ and $i, j \in \mathbb{N}$ we have (using the usual notation $A = (a_{ij})_{ij}$ for matrices):

$$\begin{aligned}
[Ax^i][Bx^j] &= \begin{pmatrix} a_{11}x^i & \cdots & a_{1n}x^i \\ \vdots & & \vdots \\ a_{n1}x^i & \cdots & a_{nn}x^i \end{pmatrix} \begin{pmatrix} b_{11}x^j & \cdots & b_{1n}x^j \\ \vdots & & \vdots \\ b_{n1}x^t & \cdots & b_{nn}x^j \end{pmatrix} \\
&= \left[\left(\sum_{k=1}^{n} a_{sk}b_{kt}x^{i+j} \right)_{st} \right] = [ABx^{i+j}].
\end{aligned}$$

Now we define:

$$\begin{array}{cccc} \varphi : & M_n(R)[x] & \longrightarrow & M_n(R[x]) \\ & A_0 + \cdots + A_kx^k & \longmapsto & [A_0] + \cdots + [A_kx^k] \end{array}$$

or otherwise stated, $\varphi(Ax^t) = [Ax^t]$ for $A \in M_n(R)$ and $t \in \mathbb{N}$, and then we extend to $M_n(R)[x]$ by linearity over addition: $\varphi(Ax^t + Bx^s) = \varphi(Ax^t) + \varphi(Bx^s)$ for $A, B \in M_n(R)$ and $t, s \in \mathbb{N}$. We can now easily verify that for any $A(x) = A_0 + \cdots + A_kx^k$ and $B(x) = B_0 + B_1x + \cdots + B_sx^s$ elements of $M_n(R)[x]$ we have:

$$\begin{aligned}
&\varphi(A(x) + B(x)) = \varphi(A_0 + \cdots + A_kx^k + B_0 + \cdots + B_sx^s) \\
&= [A_0] + \cdots + [A_kx^k] + [B_0] + \cdots + [B_sx^s] = \varphi(A(x)) + \varphi(B(x)),
\end{aligned}$$

and if me multiply we just have to be a bit more careful:

$$\varphi(A(x)B(x)) = \varphi\left(\sum_{r=0}^{k+s}\sum_{i+j=r} A_iB_jx^r\right) = \sum_{r=0}^{k+s}\sum_{i+j=r}\varphi(A_iB_jx^r) = \sum_{r=0}^{k+s}\sum_{i+j=r}[A_iB_jx^r]$$

$$= \sum_{r=0}^{k+s}\sum_{i+j=r}[A_ix^i][B_jx^j] = \sum_{r=0}^{k+s}\sum_{i+j=r}\varphi(A_ix^i)\varphi(B_jx^j) = \sum_{i=0}^{k}\varphi(A_ix^i)\sum_{j=0}^{s}\varphi(B_jx^j)$$

$$= \varphi(A(x))\varphi(B(x)).$$

Moreover, this ring homomorphism is injective, as if we have that for some $A(x), B(x) \in M_n(R)[x]$:

$$\varphi(A(x)) = \varphi(B(x)) \Longrightarrow [A_ix^i] = [B_ix^i]\,\forall 0 \leq i \leq k$$

$$\Longrightarrow a^i_{st} = b^i_{st}\,\forall 0 \leq s,t \leq n\,\forall 0 \leq i \leq k \Longrightarrow A_i = B_i\,\forall 0 \leq i \leq k$$

$$\Longrightarrow A(x) = B(x),$$

because equality in $M_n(R[x])$ means equality in the coefficients since matrices with different powers of the unknown x cannot be the same when comparing the entries, and this induces equality in the entries of the same coefficients, meaning that the original matrices of the same coefficients were the same, hence that the matrix polynomials we started with were already equal.

Finally, this ring homomorphism is also surjective, since given $F \in M_n(R[x])$ with the polynomial $f_{ij}(x) = f^0_{ij} + \cdots + f^t_{ij}x^t$ as entry (i,j) we can find $k = \max\{\deg(f_{ij}(x)) : 1 \leq i,j \leq n\}$, and then, adding zero coefficients if needed, we can decompose:

$$F = \begin{pmatrix} f_{11}(x) & \cdots & f_{1n}(x) \\ \vdots & & \vdots \\ f_{n1}(x) & \cdots & f_{nn}(x) \end{pmatrix} = \begin{pmatrix} f^0_{11} & \cdots & f^0_{1n} \\ \vdots & & \vdots \\ f^0_{n1} & \cdots & f^0_{nn} \end{pmatrix} + \cdots + \begin{pmatrix} f^k_{11}x^k & \cdots & f^k_{1n}x^k \\ \vdots & & \vdots \\ f^k_{n1}x^k & \cdots & f^k_{nn}x^k \end{pmatrix}$$

$$= \left[\begin{pmatrix} f^0_{11} & \cdots & f^0_{1n} \\ \vdots & & \vdots \\ f^0_{n1} & \cdots & f^0_{nn} \end{pmatrix}\right] + \cdots + \left[\begin{pmatrix} f^k_{11} & \cdots & f^k_{1n} \\ \vdots & & \vdots \\ f^k_{n1} & \cdots & f^k_{nn} \end{pmatrix} x^k\right] = [F_0] + \cdots + [F_kx^k]$$

$$= \varphi(F_0 + \cdots + F_kx^k),$$

that is, we found an element $F(x) = F_0 + \cdots + F_kx^k \in M_n(R)[x]$ such that $\varphi(F(x)) = F$. Thus we have proven that φ is a bijective ring homomorphism, hence $M_n(R)[x] \cong M_n(R[x])$.

References

[1] T. W. Hungerford, *Algebra*.