Math 502: Abstract Algebra
Homework 8

Lawrence Tyler Rush
<me@tylerlogic.com>

January 5, 2014
http://coursework.tylerlogic.com/courses/upenn/math502/homework08

1

Let $p(x) = x^3 - x - 1 \in \mathbb{Q}[x]$

(a) Extra Credit: Show that $p(x)$ is irreducible in $\mathbb{Q}[x]$

(b)

(c)

Let $T_n \in \operatorname{End}_{\mathbb{Q}}(V_n)$ be defined by

$$T_n(f(x) + p(x)^n\mathbb{Q}[x]) = x \cdot f(x) + p(x)^n\mathbb{Q}[x] \qquad \forall\ f(x) \in \mathbb{Q}[x]$$

For $n = 1$ The images of the basis elements in part (b) are

$$\begin{aligned} T(1 + p(x)\mathbb{Q}[x]) &= x + p(x)\mathbb{Q}[x] \\ T(x + p(x)\mathbb{Q}[x]) &= x^2 + p(x)\mathbb{Q}[x] \\ T(x^2 + p(x)\mathbb{Q}[x]) &= x^3 + p(x)\mathbb{Q}[x] = (x+1) + p(x)\mathbb{Q}[x] \end{aligned}$$

and so the matrix representation is

$$\begin{pmatrix} & & 1 \\ 1 & & 1 \\ & 1 & \end{pmatrix}$$

For $n = 2$ Since

$$p(x)^2 = x^6 - 2x^4 - 2x^3 + x^2 + 2x + 1$$

then the images of the basis elements in part (b) are

$$\begin{aligned} T(1 + p(x)^2\mathbb{Q}[x]) &= x + p(x)^2\mathbb{Q}[x] \\ T(x + p(x)^2\mathbb{Q}[x]) &= x^2 + p(x)^2\mathbb{Q}[x] \\ T(x^2 + p(x)^2\mathbb{Q}[x]) &= x^3 + p(x)^2\mathbb{Q}[x] \\ T(x^3 - x - 1 + p(x)^2\mathbb{Q}[x]) &= (x^4 - x^2 - x) + p(x)^2\mathbb{Q}[x] \\ T(x(x^3 - x - 1) + p(x)^2\mathbb{Q}[x]) &= (x^5 - x^3 - x^2) + p(x)^2\mathbb{Q}[x] \\ T(x^2(x^3 - x - 1) + p(x)^2\mathbb{Q}[x]) &= (x^6 - x^4 - x^3) + p(x)^2\mathbb{Q}[x] = (x^4 + x^3 - x^2 - 2x - 1) + p(x)\mathbb{Q}[x] \end{aligned}$$

which results in the following matrix representation

$$\left(\begin{array}{ccc|ccc} & & 1 & & & \\ 1 & & 1 & & & \\ & 1 & & & & \\ \hline & & 1 & & & 1 \\ & & & 1 & & 1 \\ & & & & 1 & \end{array}\right)$$

with vertical and horizontal lines to better see the nicities of the matrix.

(d)

For $n = 1$ The characteristic polynomial for the matrix

$$\begin{pmatrix} & & 1 \\ 1 & & 1 \\ & 1 & \end{pmatrix}$$

from above is

$$\det\left(\lambda\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} - \begin{pmatrix} & & 1 \\ 1 & & 1 \\ & 1 & \end{pmatrix}\right) = \lambda^3 - \lambda - 1$$

According to part (a), this polynomial is irreducible, so because the minimal polynomail divides the characteristic polynomial, this polynomial is also the minimal polynomial.

For $n = 2$ The characteristic polynomial for the matrix

$$\begin{pmatrix} & & 1 & & & \\ 1 & & 1 & & & \\ & 1 & & & & \\ & & 1 & & & 1 \\ & & & 1 & & 1 \\ & & & & 1 & \end{pmatrix}$$

from above is

$$\det\left(\lambda\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix} - \begin{pmatrix} & & 1 & & & \\ 1 & & 1 & & & \\ & 1 & & & & \\ & & 1 & & & 1 \\ & & & 1 & & 1 \\ & & & & 1 & \end{pmatrix}\right)$$

which is

$$\begin{aligned} \lambda\big(\lambda(\lambda(\lambda(\lambda^2-1)-1)) - (-1)(-1)(\lambda(\lambda^2-1)-1)\big)(-1)(-1)(-1)(\lambda(\lambda^2-1)-1) \\ \lambda^3(\lambda^3-\lambda-1) - \lambda(\lambda^3-\lambda-1) - (\lambda^3-\lambda-1) \\ (\lambda^3-\lambda-1)(\lambda^3-\lambda-1) \end{aligned}$$

Again because neither of the two factors of the above product are reducible, then the minimal polynomial is simply $\lambda^3 - \lambda - 1$

(e) Extra Credit: Minimal and Characteristic polynomial for T_n

---

Continuing the pattern above, the characteristic polynomial for T_n will be

$$p(x)^n = (x^3 - x - 1)^n$$

and the minimal polynomial will be

$$p(x) = x^3 - x - 1$$

2

(a)

(b) Extra Credit

3

For each $n \in \mathbb{N}$ define an F-linear operator, $\partial^{[n]}$, on $F[x]$ by

$$f(x+t) = \sum_{n \geq 0} \partial^{[n]}(f) \cdot t^n$$

for all $f(x) \in F[x]$. So for an arbitrary m-degree polynomial $f(x) \in F[x]$ defined as

$$\sum_{i=0}^{m} a_i x^i$$

we have, through use of the binomial formula, that

$$f(x+t) = \sum_{i=0}^{m} a_i (x+t)^i = \sum_{i=0}^{m} a_i \sum_{j=0}^{i} \binom{i}{j} x^{i-j} t^j = \sum_{i=0}^{m} \sum_{j=0}^{i} a_i \binom{i}{j} x^{i-j} t^j$$

Rearranging the indexing variables, we can morph the right-hand side of the above equation into

$$\sum_{j=0}^{m} \sum_{i=j}^{m} a_i \binom{i}{j} x^{i-j} t^j$$

which in turn allows us to move the t^j outside the inner summation to obtain

$$f(x+t) = \sum_{j=0}^{m} \left(\sum_{i=j}^{m} a_i \binom{i}{j} x^{i-j} \right) t^j$$

which finally allows us to clearly see the coefficients of $f(x+t)$ and therefore the formulation of $\partial^{[j]}(f)$ to be

$$\partial^{[j]}(f) = \sum_{i=j}^{m} a_i \binom{i}{j} x^{i-j} \tag{3.1}$$

(a) Show that $\partial^{[1]}$ is given by the standard formula for $\frac{d}{dx}$

Letting $f(x) \in F[x]$ be a polynomial of degree m, then the formula in equation 3.1, we have

$$\partial^{[1]}(f) = \sum_{i=1}^{m} a_i \binom{i}{1} x^{i-1} = \sum_{i=1}^{m} a_i i x^{i-1}$$

which is exactly the formula for $f'(x)$.

(b) Show that $n! \cdot \partial^{[n]}(f)$ yields the "n-th derivative of f"

Letting $f(x) \in F[x]$ be a polynomial of degree m, then the formula in equation 3.1, we have

$$\begin{aligned}
n! \cdot \partial^{[n]}(f) &= n! \sum_{i=n}^{m} a_i \binom{i}{n} x^{i-n} \\
&= n! \sum_{i=n}^{m} a_i \frac{i!}{n!(i-n)!} x^{i-n} \\
&= \sum_{i=n}^{m} a_i \frac{i!}{(i-n)!} x^{i-n} \\
&= \sum_{i=n}^{m} a_i i(i-1)(i-2)\cdots(i-(n+1))x^{i-n}
\end{aligned}$$

which is exactly the formula for $f^n(x)$.

(c) Extra Credit

4

(a) Show that $\mathrm{End}_{\mathbf{grp}}(p^{-m}\mathbb{Z}/\mathbb{Z})$ is naturally isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$

Since the ring $p^{-m}\mathbb{Z}/\mathbb{Z}$ is cyclically generated by $\underline{p^{-m}}$, each endomorphism is defined by it's mapping of $\overline{p^{-m}}$. Since each element of $p^{-m}\mathbb{Z}/\mathbb{Z}$ is an integer multiple of $\overline{p^{-m}}$ then let's denote each element of $\mathrm{End}_{\mathrm{grp}}(p^{-m}\mathbb{Z}/\mathbb{Z})$ by

$$\varphi_n(\overline{p^{-m}}) := \overline{np^{-m}}$$

Given this notation, because each φ_n, φ_m are ring homomorphisms, we are immediately afforded both $\varphi_n\varphi_m = \varphi_{nm}$ and $\varphi_n + \varphi_m = \varphi_{n+m}$.

With this, we will define $\phi : \mathrm{End}(p^{-m}\mathbb{Z}/\mathbb{Z}) \to \mathbb{Z}/p^m\mathbb{Z}$ by $\phi(\varphi_n) = \overline{n}$. Thus using the ring homomorphic properties of φ_n and φ_m outlined above and the additive/multiplicative operations on $/p^m\mathbb{Z}$, we have

$$\begin{aligned}
\phi(\varphi_n\varphi_m) &= \phi(\varphi_{nm}) \\
&= \overline{nm} \\
&= \overline{nm} \\
&= \phi(\varphi_n)\phi(\varphi_m)
\end{aligned}$$

and

$$\begin{aligned}
\phi(\varphi_n + \varphi_m) &= \phi(\varphi_{n+m}) \\
&= \overline{n+m} \\
&= \overline{nm} \\
&= \phi(\varphi_n)\phi(\varphi_m)
\end{aligned}$$

and so ϕ is a ring homomorphism.

Now if $\phi(\varphi_n) = \overline{0}$, then $\varphi_n(p^{-m}) = \overline{0p^{-m}} = \overline{0}$, and so $\varphi_n = \varphi_0$. With this we have the injectivity of ϕ. Now because $\mathrm{End}(p^{-m}\mathbb{Z}/\mathbb{Z})$ and $\mathbb{Z}/p^m\mathbb{Z}$ have the same cardinality, then ϕ is bijective. Hence we have that $\mathrm{End}(p^{-m}\mathbb{Z}/\mathbb{Z})$ is isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$.

(b)

For referential reasons, we will number the property each element of $\mathbb{Z}_p$ has

$$a_m \equiv a_n (\bmod p^n\mathbb{Z})\ \forall\ m \geq n \tag{4.2}$$

(b1) **There exists a zero element** The sequence of all zeros, denote it by (0), will be the zero element since:

$$(0) + (x_n)_{n\in\mathbb{N}_{\geq 1}} = (0 + x_n)_{n\in\mathbb{N}_{\geq 1}} = (x_n + 0)_{n\in\mathbb{N}_{\geq 1}} = (x_n)_{n\in\mathbb{N}_{\geq 1}} + (0)$$

Addition is closed For each $(x_n)_{n\in\mathbb{N}_{\geq 1}}, (y_n)_{n\in\mathbb{N}_{\geq 1}} \in \mathbb{Z}_p$ their sum is in $\mathbb{Z}_p$ because of the closure of addition on $\mathbb{Z}/p^n\mathbb{Z}$ and because

$$x_m + y_m \equiv (x_n \bmod p^n\mathbb{Z}) + (y_n \bmod p^n\mathbb{Z}) \equiv (x_n + y_n) \bmod p^n\mathbb{Z}$$

for all $m \geq n$.

Additive inverses The sequence of negatives of the elements of a sequence is the additive inverse since

$$(x_n)_{n\in\mathbb{N}_{\geq 1}} + (-x_n)_{n\in\mathbb{N}_{\geq 1}} = (x_n - x_n)_{n\in\mathbb{N}_{\geq 1}} = (0) = (-x_n + x_n)_{n\in\mathbb{N}_{\geq 1}} = (-x_n)_{n\in\mathbb{N}_{\geq 1}} + (x_n)_{n\in\mathbb{N}_{\geq 1}}$$

Addition is commutative by the following

$$(x_n)_{n\in\mathbb{N}_{\geq 1}} + (y_n)_{n\in\mathbb{N}_{\geq 1}} = (x_n + y_n)_{n\in\mathbb{N}_{\geq 1}} = (y_n + x_n)_{n\in\mathbb{N}_{\geq 1}} = (y_n)_{n\in\mathbb{N}_{\geq 1}} + (x_n)_{n\in\mathbb{N}_{\geq 1}}$$

which is due to the commutative addition of $\mathbb{Z}/p^n\mathbb{Z}$ for each n.

There exists a 1 element which is the sequence of all ones, which we will denote by (1). It is the multiplicative identity by

$$(1)(x_n)_{n\in\mathbb{N}_{\geq 1}} = (1x_n)_{n\in\mathbb{N}_{\geq 1}} = (x_n1)_{n\in\mathbb{N}_{\geq 1}} = (x_n)_{n\in\mathbb{N}_{\geq 1}}(1)$$

Multiplication is closed since

$$x_m y_m \equiv (x_n \bmod p^n\mathbb{Z})(y_n \bmod p^n\mathbb{Z}) \equiv (x_n y_n) \bmod p^n\mathbb{Z}$$

for all $m \geq n$

Multiplication is associative by the following

$$\begin{aligned}
\left((x_n)_{n\in\mathbb{N}_{\geq 1}}(y_n)_{n\in\mathbb{N}_{\geq 1}}\right)(z_n)_{n\in\mathbb{N}_{\geq 1}} &= (x_n y_n)_{n\in\mathbb{N}_{\geq 1}}(z_n)_{n\in\mathbb{N}_{\geq 1}} \\
&= ((x_n y_n) z_n)_{n\in\mathbb{N}_{\geq 1}} \\
&= (x_n(y_n z_n))_{n\in\mathbb{N}_{\geq 1}} \\
&= (x_n)_{n\in\mathbb{N}_{\geq 1}}(y_n z_n)_{n\in\mathbb{N}_{\geq 1}} \\
&= (x_n)_{n\in\mathbb{N}_{\geq 1}}\left((y_n)_{n\in\mathbb{N}_{\geq 1}}(z_n)_{n\in\mathbb{N}_{\geq 1}}\right)
\end{aligned}$$

where we make use of associativity on $\mathbb{Z}/p^n\mathbb{Z}$.

Multiplication distributes over addition by the following

$$\begin{aligned}
(x_n)_{n\in\mathbb{N}_{\geq 1}}\left((y_n)_{n\in\mathbb{N}_{\geq 1}} + (z_n)_{n\in\mathbb{N}_{\geq 1}}\right) &= (x_n)_{n\in\mathbb{N}_{\geq 1}}(y_n + z_n)_{n\in\mathbb{N}_{\geq 1}} \\
&= (x_n(y_n + z_n))_{n\in\mathbb{N}_{\geq 1}} \\
&= (x_n y_n + x_n z_n)_{n\in\mathbb{N}_{\geq 1}} \\
&= (x_n y_n)_{n\in\mathbb{N}_{\geq 1}} + (x_n z_n)_{n\in\mathbb{N}_{\geq 1}} \\
&= \left((x_n)_{n\in\mathbb{N}_{\geq 1}}(y_n)_{n\in\mathbb{N}_{\geq 1}}\right) + \left((x_n)_{n\in\mathbb{N}_{\geq 1}}(z_n)_{n\in\mathbb{N}_{\geq 1}}\right)
\end{aligned}$$

where we make use of the distributive law on $\mathbb{Z}/p^n\mathbb{Z}$.

Multiplication is commutative by the following

$$(x_n)_{n\in\mathbb{N}_{\geq 1}}(y_n)_{n\in\mathbb{N}_{\geq 1}} = (x_n y_n)_{n\in\mathbb{N}_{\geq 1}} = (y_n x_n)_{n\in\mathbb{N}_{\geq 1}} = (y_n)_{n\in\mathbb{N}_{\geq 1}}(x_n)_{n\in\mathbb{N}_{\geq 1}}$$

in which we make use of the commutative property of multiplication on $\mathbb{Z}/p^n\mathbb{Z}$.

Finally, given all the above properties, we have that $\mathbb{Z}_p$ is a commutative ring.

(b2) Let $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ be the n-th component projection map. For $\overline{m} \in \mathbb{Z}/p^n\mathbb{Z}$, define the sequence $(x_n)_{\mathbb{N}_{\geq 1}}$ by $x_n := m \bmod p^n\mathbb{Z}$ for each $n \in \mathbb{N}_{\geq 1}$. Then we will have that $\pi_n((x_n)_{\mathbb{N}_{\geq 1}}) = m(\text{mod} p^n\mathbb{Z}) = \overline{m}$. Hence the map π_n is surjective.

Through use of the additive and multiplicative definitions on both $\mathbb{Z}_p$ and $\mathbb{Z}/p^n\mathbb{Z}$, we obtain

$$\pi_n((x_n)_{\mathbb{N}_{\geq 1}} + (y_n)_{\mathbb{N}_{\geq 1}}) = \pi_n((x_n + y_n)_{\mathbb{N}_{\geq 1}}) = \overline{x_n + y_n} = \overline{x_n} + \overline{y_n} = \pi_n((x_n)_{\mathbb{N}_{\geq 1}}) + \pi_n((y_n)_{\mathbb{N}_{\geq 1}})$$

and

$$\pi_n((x_n)_{\mathbb{N}_{\geq 1}}(y_n)_{\mathbb{N}_{\geq 1}}) = \pi_n((x_n y_n)_{\mathbb{N}_{\geq 1}}) = \overline{x_n y_n} = \overline{x_n}(\overline{y_n}) = \pi_n((x_n)_{\mathbb{N}_{\geq 1}})\pi_n((y_n)_{\mathbb{N}_{\geq 1}})$$

which reveals that π_n is a ring homomorphism in addition to being surjective.

(b3) Let $(x_m) \in \operatorname{Ker} \pi_n$. Then $x_n \equiv 0 \bmod p^n$ implying that x_n is a multiple of p^n. Furthermore given equation 4.2 we have that

$$x_m \equiv 0 \bmod p^n \tag{4.3}$$

for all $m \geq n$. Hence each x_m is a multiple of p^n for $m \geq n$. Likewise, equation 4.2 gives us that $x_n \equiv x_k \bmod p^k$ for all $k < n$, so since x_n is a multiple of p^n it is inherently a multiple of p^k for $k < n$. Thus we have that each $x_k \equiv 0 \bmod p^k$ which also implies that

$$x_k \equiv 0 \bmod p^n \tag{4.4}$$

Hence the fact that $x_n \equiv 0 \bmod p^n$ combined with equations 4.3 and 4.4 implies that $(x_n) \in p^n \cdot \mathbb{Z}_p$. So we have that $\operatorname{Ker} \pi_n \subset p^n \cdot \mathbb{Z}_p$.

Now if $(x_n) \in p^n\mathbb{Z}_p$, then x_n would be a multiple of p^n, i.e. $x_n \equiv 0 \bmod p^n$. So the image of (x_n) under π_n will therefore be $\overline{0} \in \mathbb{Z}/p^n\mathbb{Z}$. Hence $p^n\mathbb{Z}_p \subset \operatorname{Ker} \pi_n$.

With the above two results we conclude that $\operatorname{Ker} \pi_n = p^n\mathbb{Z}_p$.

(c) Extra Credit

(d) Extra Credit

(e) Extra Credit

(f) Extra Credit

(g) Extra Credit

5 Extra Credit