EXERCISES 7

Please submit solutions by 3pm on Thursday 12th April to the pigeonholes in 4W (ground floor).

(W) = Warm-up; (H) = Homework; (A) = Additional.

1. (W) Consider the quaternions $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$.

(1) For $a \in \mathbb{H}$, let $T_a \colon \mathbb{H} \to \mathbb{H}$ be the linear map given by 'multiply on the right by a'. Apply T_i and T_j to each of the basis vectors $1, i, j, k$ in $\mathbb{H}$ and write the result in this basis.

(2) Let $I, J \in \mathrm{End}\,(\mathbb{R}^4)$ be the linear operators that act on the standard basis e_1, e_2, e_3, e_4 of $\mathbb{R}^4$ in the same way that T_i, T_j act on $1, i, j, k$. Show that $I^2 = J^2 = -\mathrm{id}$ and $JI = -IJ$. [Hint: check each identity holds on each standard basis vector of $\mathbb{R}^4$.] Deduce that the subring $\mathbb{R}\mathrm{id} + \mathbb{R}I + \mathbb{R}J + \mathbb{R}(IJ)$ of $\mathrm{End}\,(\mathbb{R}^4)$ is isomorphic to $\mathbb{H}$. This shows that $\mathbb{H}$ is a (noncommutative) ring with 1.

2. (W) For a ring R and for $n \geq 1$, let $S = R[x_1, \ldots, x_{n-1}]$ denote the polynomial ring in $n-1$ variables with coefficients in R. Show that $R[x_1, \ldots, x_n]$ is isomorphic to the polynomial ring $S[x_n]$ in one variable x_n with coefficients in S. [Hint: see Proposition 4.8 in the lecture notes for the idea of the proof.]

3. (W) For $n \geq 2$ and for any integral domain R, show that the ideal in $R[x_1, \ldots, x_n]$ given by

$$I = \big\{ fx_1 + gx_2 \in R[x_1, \ldots, x_n] \mid f, g \in R[x_1, \ldots, x_n] \big\}$$

is not principal.

4. (H) Let $\Bbbk$ be a field and let $n \in \mathbb{N}$. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal.

(1) Show that the quotient ring $\Bbbk[x_1, \ldots, x_n]/I$ is a $\Bbbk$-algebra.

(2) Find an ideal I such that $\Bbbk[x_1, x_2]/I$ has dimension 13, and write the image of the polynomial $f(x_1, x_2) = x_1^7 + x_1^4 x_2^2 + x_2^4 \in \Bbbk[x_1, x_2]$ in the quotient ring in terms of your basis.

5. (H) Let $\Bbbk$ be a field and let $f \in \Bbbk[x]$ be nonconstant. Show that there exists a field extension $\Bbbk \subseteq K$ such that f can be written as a product of polynomials of degree 1 in $K[x]$. [Hint: Use induction on the degree of f, and decompose f as a product of irreducible polynomials.]

6. (A) Let p be a prime and let $q = p^n$ where n is a positive integer. For $x^q - x \in \mathbb{Z}_p[x]$, let K be a field containing all the roots of $x^q - x$. Show that the set S of roots of $x^q - x$ is a subfield of K.

The course website is: `http://people.bath.ac.uk/dmjc20/Alg2B/`

Solutions 7

1. (1) We have

$$T_i(1) = 1 \cdot i = i, \quad T_i(i) = i^2 = -1, \quad T_i(j) = ji = -k, \quad T_i(k) = ki = j$$

and

$$T_j(1) = j, \quad T_j(i) = k, \quad T_j(j) = -1, \quad T_j(k) = -i.$$

(2) We have

$$I(e_1) = e_2, \quad I(e_2) = -e_1, \quad I(e_3) = -e_4, \quad I(e_4) = e_3$$

and

$$J(e_1) = e_3, \quad J(e_2) = e_4, \quad J(e_3) = -e_1, \quad J(e_4) = -e_2.$$

Calculations show that $I^2(e_i) = J^2(e_i) = -e_i$ and thus $I^2 = J^2 = -\mathrm{id}$. Calculations also give that

$$JI(e_1) = J(e_2) = e_4, \quad JI(e_2) = J(-e_1) = -e_3, \quad JI(e_3) = J(-e_4) = e_2, \quad JI(e_4) = J(e_3) = -e_1$$

whereas

$$IJ(e_1) = I(e_3) = -e_4, \quad IJ(e_2) = I(e_4) = e_3, \quad IJ(e_3) = I(-e_1) = -e_2, \quad IJ(e_4) = I(-e_2) = e_1.$$

Thus $JI = -IJ$.

To establish the isomorphism, consider the map

$$\phi\colon \mathbb{R}\mathrm{id} + \mathbb{R}I + \mathbb{R}J + \mathbb{R}(IJ) \longrightarrow \mathbb{H}$$

satisfying $\Phi(a\mathrm{id}+bI+cJ+d(IJ)) = a+bi+cj+dk$. This map is an $\mathbb{R}$-linear isomorphism of vector spaces (not that both are isomorphic to $\mathbb{R}^4$). We'll show now that it preserves the multiplicative structure. Since the domain is a ring, it will follow that the image is also a ring, i.e., $\mathbb{H}$ really is a ring; in fact it's an $\mathbb{R}$-algebra!

Checking that ϕ preserves multiplication means checking that the image of the product of two basis elements is equal to the product of the images of those two basis elements. We know that $\phi(\mathrm{id}) = 1 \in \mathbb{H}$ which is the multiplcative identity, so certainly any product involving id (either on the right or left) is preserved, e.g.,

$$\phi(\mathrm{id} \cdot I) = \phi(I) = i = 1 \cdot i = \phi(\mathrm{id}) \cdot \phi(I).$$

To check the other properties, we use the calculations above. For example, since $I^2 = -\mathrm{id}$, we have

$$\phi(I \cdot I) = \phi(-\mathrm{id}) = -1 = i \cdot i = \phi(I) \cdot \phi(I).$$

and similarly for J in place of I. Also,

$$\phi(I \cdot J) = \phi(IJ) = k = i \cdot j = \phi(I) \cdot \phi(J).$$

and

$$\phi(I \cdot IJ) = \phi(I^2 J) = \phi(-\mathrm{id}J) = -j = i \cdot k = \phi(I) \cdot \phi(IJ).$$

This takes care of all the products of basis elements in which I is the element on the left; now check for yourself those that have J on the left and then IJ on the left.

In short, the basis elements id, I, J, IJ multiply each other in exactly the same way as the basis elements $1, i, j, k$ do in $\mathbb{H}$. Since the ring structure in an $\mathbb{R}$-algebra is completely determined by how the basis elements multiply (see Remark 4.2(2)), we're done.

2. Consider the map $\phi\colon R[x_1,\dots,x_n] \to S[x_n]$ defined by sending $f = \sum_{i_1,\dots,i_n\geq 0} a_{i_1,\dots,i_n} x_1^{i_1}\cdots x_n^{i_n}$ to

$$\phi(f) = \sum_{i_n\geq 0}\left(\sum_{i_1,\dots,i_{n-1}\geq 0} a_{i_1,\dots,i_n} x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}\right) x_n^{i_n}. \tag{0.1}$$

Notice that f and $\phi(f)$ share precisely the same terms, i.e, in passing from f to $\phi(f)$ we haven't done anything (!!!) except gather terms in a particular way. Thus, if we expand the parentheses in $\phi(f)$ then we recover precisely the same terms as those that appear in f. It follows that ϕ is a ring homomorphism because addition and multiplication in both $R[x_1,\dots,x_n]$ and $S[x_n]$ can be understood purely in terms of addition and multiplication term by term.

The map ϕ is surjective because for any polynomial $\sum_{i\geq 0} g_i x_n^i$ in $S[x_n]$, we can multiply each polynomial g_i by x_n^i and sum up to obtain a polynomial $f\in R[x_1,\dots,x_n]$ such that $\phi(f) = \sum_{i\geq 0} g_i x_n^i$. Finally, to see that it's injective, notice that

$$0 = \phi(f) = \sum_{i_n\geq 0} g_{i_n} x_n^{i_n}$$

is the zero polynomial in $S[x_n]$, so all of its coefficients equal zero, i.e., $g_{i_n} = 0 \in R$ for all $i_n \geq 0$. If we substitute these equations into the parentheses from (0.1), we have for each i_n that

$$0 = g_{i_n} = \sum_{i_1,\dots,i_{n-1}\geq 0} a_{i_1,\dots,i_n} x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}$$

in the ring $R[x_1,\dots,x_{n-1}]$. Equate coefficients on the left and right again to see that $a_{i_1,\dots,i_n} = 0$ for all $i_1,\dots,i_n \geq 0$, which in turn forces $f = 0$ as required.

3. Assume there exists $f\in R[x_1,\dots,x_n]$ such that $R[x_1,\dots,x_n]x_1 + R[x_1,\dots,x_n]x_2 = R[x_1,\dots,x_n]f$. Then there exists $g,h\in R[x_1,\dots,x_n]$ such that

$$f = gx_1 + hx_2.$$

Since $x_1 \in R[x_1,\dots,x_n]f$, there exists $r\in R[x_1,\dots,x_n]f$ such that

$$x_1 = rf = r(gx_1 + hx_2) = rgx_1 + rhx_2.$$

Compare coefficients in x_1 on the left and right to see that $1 = rg$ and $0 = rh$. If $r = 0$ then $0 = rg = 1$ which is absurd in an integral domain. Thus $r\neq 0$, in which case the equality $0 = rh$ forces $h = 0$. Thus, $f = gx_1$. This forces everything in the ideal $R[x_1,\dots,x_n]f$ to be divisible by x_1. In particular, the variable x_2 is divisible by x_1, but this is absurd.

4. (1) Write $V := \Bbbk[x_1,\dots,x_n]/I$, and consider the map $\Bbbk\times V\to V$ given by

$$(\lambda, g+I)\mapsto (\lambda g) + I$$

(you might equally well use equivalence class notation $[g]$ in place of coset notation $g+I$). This map is well-defined because if $g+I = h+I$, then $g-h\in I$ and hence $\lambda(g-h)\in I$, giving $\lambda g - \lambda h\in I$, that is, $\lambda g + I = \lambda h + I$ as required.

Since V is a ring, $(V,+)$ is an abelian group, and for $g+I\in V$ and $\lambda,\mu\in\Bbbk$ we have

$$\begin{aligned}
\lambda(\mu(g+I)) &= \lambda(\mu g + I) = \lambda\mu g + I = (\lambda\mu)(g+I),\\
1\cdot(g+I) &= 1g + I = g + I,\\
(\lambda+\mu)(g+I) &= (\lambda+\mu)g + I = (\lambda g + \mu g) + I = \lambda(g+I) + \mu(g+I),\\
\lambda\big((g+I)+(h+I)\big) &= \lambda\big((g+h)+I\big) = (\lambda g + \lambda h) + I = \lambda(g+I) + \lambda(h+I),
\end{aligned}$$

so V is a vector space over $\Bbbk$. In addition, we have

$$(\lambda(g+I)) \cdot (h+I) = (g+I) \cdot (\lambda(h+I)) = \lambda\big((g+I)\cdot(h+I)\big)$$

because each is equal to $(\lambda gh) + I$. Therefore $V := \Bbbk[x_1, \dots, x_n]/I$ is a $\Bbbk$-algebra.

(2) Set $x = x_1$ and $y = x_2$ to make the notation easier. There are many candidates:

- One correct answer is $I = \langle x^{13}, y\rangle$, that is $I = \{gx^{13} + hy \mid g, h \in \Bbbk[x, y]\}$. The point is, the class of a polynomial $f \in \Bbbk[x, y]$ in the quotient ring is such that every term that is divisible by either x^{13} or y equals zero. Therefore, the only terms of f that are nonzero in the quotient ring are scalar multiples of $(1, x, x^2, \dots, x^{12})$, so the quotient ring has dimension 13. In this case, the image of the polynomial f given in the question is $x^7 + I$.
- Similarly, $I = \langle x, y^{13}\rangle$ works equally well, in which case the image of the given polynomial f is $y^4 + I$.
- Another correct answer is the ideal $I = \langle x^4, x^3y, y^4\rangle = \{fx^4 + gx^3y + hy^4 \mid f, g, h \in \Bbbk[x, y]\}$, where a basis for the quotient ring over $\Bbbk$ is $(1, x, x^2, x^3, y, xy, x^2y, y^2, xy^2, x^2y^2, y^3, xy^3, x^2y^3)$. In this example, the image of f is $0 + I$.

There are lots of other correct answers.

5. We prove this by induction on $n = \deg(f)$. If $n = 1$ then f has a root in $\Bbbk$ and we're done by setting $K = \Bbbk$. For $n > 1$, assume that the result holds for smaller values of $\deg(f)$. Let p be an irreducible factor of f, say $f = pg$. Since p is irreducible, the ring

$$F = \Bbbk[x]/\langle p\rangle$$

is a field by Corollary 3.19. By Theorem 4.15, this quotient ring contains $\Bbbk$ as a subfield and has a root a of the polynomial p. Now $f(a) = p(a)g(a) = 0 \cdot g(t) = 0$, so a is also a root of f. We can then factorise f in $F[x]$, say $f = (x - a)h$ for some $h \in F[x]$. As h is of smaller degree than f we can apply the induction hypothesis to get a field K that contains F as a subfield such that h can be written as a product of linear factors $h = c(x - a_1)(x - a_2)\cdots(x - a_{n-1})$ in $K[x]$. Then

$$f = c(x - a_1)\cdots(x - a_{n-1})(x - a)$$

is a factorisation in $K[x]$.

6. Note that $a \in S$ if and only if $a^q = a$. We first show that S is a subring. Since $0^q = 0$, we have $0 \in S$, so S is nonempty. Next, if $a, b \in S$, then $a^q = a$ and $b^q = b$ and hence

$$(ab)^q = a^q b^q = ab$$

where we've used the fact that K is commutative. This shows that $ab \in S$. To show that S is a subring of K, it remains to show that for $a, b \in S$, we have $a - b \in S$. One can tackle this head on, but it's an effort getting the signs right, so instead note first that

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p,$$

where we have used the fact that the characteristic is p and that p divides $\binom{p}{1}, \dots \binom{p}{p-1}$. It follows by induction for $a, b \in S$ that

$$(a+b)^q = (a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b \tag{0.2}$$

and thus $a + b \in S$. Furthermore, for $b \in S$ we have

$$(-b)^q = \begin{cases} (-1)^q b^q = -b & \text{when } q \text{ is odd} \\ b^q = b = -b & \text{otherwise, since the characteristic equals 2 in this case} \end{cases}$$

This shows that $b \in S \Rightarrow -b \in S$. Now, for $a, b \in S$, we have $-b \in S$ and substitute both a and $-b$ into (0.2) to see that $(a - b)^q = a - b$. This shows that $a - b \in S$, so S is indeed a subring.

It remains to show that S is a field, i.e., every non-zero element in S is a unit. But if $0 \neq a \in S$, then

$$0 = a^q - a = a(a^{q-1} - 1)$$

implies that $a^{q-1} = 1$ and thus a is a unit.