ENTREGA 1. EEAA. GRUPO M3 (19-20).
CARLOS ANDRADAS Y ANDONI DE ARRIBA.

Fecha límite: 4-X-2019.

Entregar en la hora de problemas en mano o enviar por correo: andonide@ucm.es.

Problema 1. Sean $(A,+,\cdot)$ un anillo y $(\mathrm{End}((A,+,\cdot)),+,\circ)$ sus endomorfismos con la suma definida por $+ : \mathrm{End}((A,+,\cdot)) \times \mathrm{End}((A,+,\cdot)) \longrightarrow \mathrm{End}((A,+)); (f,g) \mapsto f+g$, donde $(f+g)(a) := f(a)+g(a)$ para cada $a \in A$[1], y el producto definido por la composición usual. Se trata de probar que, en general, este satisface **todas** las propiedades de los anillos unitarios **salvo dos** (una está explicada a pie de página). ¿Qué pasa si el anillo A es de Boole?

Solución: En primer lugar, debemos comprobar que se tienen todas las propiedades que cumple un anillo unitario, **sin olvidar ninguna**.

(1) ¿Es la **suma** de endomorfismos una operación **cerrada**? **NO**. En efecto, hay que dar un **contraejemplo**. Si tomamos el anillo $A = \mathbb{Z}$ y sus endomorfismos con las operaciones arriba definidas, tomando en particular $f, g = \mathrm{Id}$ la identidad en $\mathbb{Z}$ usual y $a = 2 \in \mathbb{Z}$ un cierto entero, vemos que

$$(f+g)(a \cdot a) = (f+g)(4) := \mathrm{Id}(4) + \mathrm{Id}(4) = 8,$$

mientras que

$$(f+g)(a \cdot a) = ((f+g)(a)) \cdot ((f+g)(a)) := ((2\mathrm{Id})(2)) \cdot ((2\mathrm{Id})(2)) = 16.$$

Luego, en general, la suma de endomorfismos no es un nuevo endomorfismo, ya que este puede no preservar el producto dado en el anillo A.

(2) ¿Es la **composición** de endomorfismos una operación **cerrada**? **SI**. En efecto, vamos a **demostrar**lo. Se trata de probar que, dados $f, g \in \mathrm{End}(A)$ arbitrarios, entonces $f \circ g \in \mathrm{End}(A)$. En otras palabras, probemos que este preserva la suma y el producto dados en A. Sean $a, b \in A$ arbitrarios. Entonces, por un lado,

$$(f \circ g)(a+b) := f(g(a+b)) = f(g(a)+g(b)) = f(g(a)) + f(g(b)) =:$$
$$=: (f \circ g)(a) + (f \circ g)(b);$$

mientras, por otra parte,

$$(f \circ g)(a \cdot b) := f(g(a \cdot b)) = f(g(a) \cdot g(b)) = f(g(a)) \cdot f(g(b)) =:$$
$$=: (f \circ g)(a) \cdot (f \circ g)(b).$$

En conclusión, queda demostrado que la composición de endomorfismos es un nuevo endomorfismo.

(a) ¿Es **asociativa la suma**? SI (formalmente, pues hemos visto que la suma de endomorfismos no tiene porqué serlo). En efecto, se tiene que $(f+g)+h = f+(g+h)$ para cualesquiera $f, g, h \in \mathrm{End}(A)$ dado que, si tomamos $a \in A$ arbitrario, es

$$((f+g)+h)(a) := (f+g)(a) + h(a) := (f(a)+g(a)) + h(a) =$$
$$= f(a) + (g(a)+h(a)) =: f(a) + (g+h)(a) =: (f+(g+h))(a).$$

[1] ¡OJO! La suma de endomorfismos así definida NO es endomorfismo de anillos; esto es, en general, se tiene que $f+g \notin \mathrm{End}((A,+,\cdot))$, pues puede ser que $(f+g)(ab) \neq (f+g)(a)(f+g)(b)$ para ciertos $a, b \in A$.

(b) ¿Es **conmutativa la suma**? SI (formalmente, pues hemos visto que la suma de endomorfismos no tiene porqué serlo). En efecto, se tiene que $f+g=g+f$ para cualesquiera $f,g\in \mathrm{End}(A)$ dado que, si tomamos $a\in A$ arbitrario, es

$$(f+g)(a):=f(a)+g(a)=g(a)+f(a)=:(g+f)(a).$$

(c) ¿Existe el **elemento neutro** para la suma? SI. El homomorfismo constantemente nulo; es decir, la aplicación dada por $0_{\mathrm{End}(A)}:A\to A; a\mapsto 0$, es el elemento neutro para la suma. En efecto, pues, por una parte, este **es un endomorfismo** (esto es, se tiene que $0_{\mathrm{End}(A)}\in \mathrm{End}(A)$) dado que, para todo $a,b\in A$ que tomemos, se tiene que

$$0=:0_{\mathrm{End}(A)}(a+b)=0_{\mathrm{End}(A)}(a)+(0_{\mathrm{End}(A)})(b):=0$$

y

$$0=:0_{\mathrm{End}(A)}(a\cdot b)=0_{\mathrm{End}(A)}(a)\cdot 0_{\mathrm{End}(A)}(b):=0;$$

pero, además, este verifica la **condición de elemento neutro** (a saber, que $f+0_{\mathrm{End}(A)}=0_{\mathrm{End}(A)}=0_{\mathrm{End}(A)}+f$ para todo $f\in\mathrm{End}(A)$), ya que para todo endomorfismo $f\in\mathrm{End}(A)$ se tiene que

$$\left(f+0_{\mathrm{End}(A)}\right)(a):=f(a)+0_{\mathrm{End}(A)}(a)=f(a)=$$
$$=0_{\mathrm{End}(A)}(a)+f(a)=:\left(0_{\mathrm{End}(A)}+f\right)(a),$$

para todo $a\in A$ que consideremos.

(d) ¿Existe el **elemento opuesto** para la suma? NO, pues, si queremos que se cumpla la **condición de elemento opuesto**, dado $f\in\mathrm{End}(A)$ arbitrario, el elemento opuesto de este homomorfismo debe ser la aplicación $g:A\to A; a\mapsto g(a)=-f(a)$. En efecto, pues, dados $a\in A$ arbitrario, se tiene que

$$0=0_{\mathrm{End}(A)}(a)=f(a)+(-f(a))=:f(a)+g(a)=:(f+g)(a)=$$
$$=(g+f)(a):=g(a)+f(a):=(-f(a))+f(a)=0_{\mathrm{End}(A)}(a)=0.$$

Luego, como el **elemento opuesto** para f en los endomorfismos de A es **único**, si este existe, debe ser g. Sin embargo, en general, este resulta **no** ser un **endomorfismo**. En efecto, basta dar el **contraejemplo** siguiente: supongamos que en el anillo $\mathbb{Z}$ se tiene el homomorfismo identidad Id usual, que, según lo que acabamos de probar, si tiene opuesto, este debe ser $g=-\mathrm{Id}$. Pero este no es homomorfismo de anillos, ya que no preserva productos, pues tomando $a=1\in\mathbb{Z}$ vemos que

$$1=(-1)\cdot(-1)=:g(1)\cdot g(1)=g(a)\cdot g(a)\neq g(a\cdot a)=g(1):=-1.$$

(e) ¿Es **asociativo el producto**? SI. En efecto, se tiene que $(f\circ g)\circ h=f\circ(g\circ h)$ para cualesquiera $f,g,h\in\mathrm{End}(A)$ dado que, si tomamos $a\in A$ arbitrario, es

$$((f\circ g)\circ h)(a):=(f\circ g)(h(a)):=f(g(h(a)))=:$$
$$=:f((g\circ h)(a))=:(f\circ(g\circ h))(a).$$

(f) ¿Es **distributivo el producto con respecto a la suma**? SI (formalmente, pues hemos visto que la suma de endomorfismos no tiene porqué serlo). En efecto, se tiene que $(f+g)\circ h=f\circ h+g\circ h$ y $f\circ(g+h)=f\circ g+f\circ h$ para cualesquiera $f,g,h\in\mathrm{End}(A)$ dado que, si tomamos $a\in A$ arbitrario, por un lado es

$$((f+g)\circ h)(a):=(f+g)(h(a)):=f(h(a))+g(h(a))=:$$
$$=:(f\circ h)(a)+(g\circ h)(a);$$

mientras que, por el otro, tenemos que

$$(f\circ(g+h))(a):=f((g+h)(a)):=f(g(a)+h(a))=f(g(a))+f(h(a))=:$$
$$=:(f\circ g)(a)+(f\circ h)(a).$$

(g) ¿Existe el **elemento identidad** para la suma? SI. El homomorfismo identidad; es decir, la aplicación $\mathrm{Id}_A\colon A \longrightarrow A; a \mapsto a$, es el elemento identidad para el producto. En efecto, pues, por una parte, este **es un endomorfismo** (esto es, se tiene que $\mathrm{Id}_A \in \mathrm{End}(A)$) dado que, para todo $a, b \in A$ que tomemos, se tiene que

$$a + b =: \mathrm{Id}_A(a + b) = \mathrm{Id}_A(a) + \mathrm{Id}_A(b) := a + b$$

y

$$a \cdot b =: \mathrm{Id}_A(a \cdot b) = \mathrm{Id}_A(a) \cdot \mathrm{Id}_A(b) := a \cdot b;$$

pero, además, este verifica la **condición de elemento identidad** (a saber, que $\mathrm{Id}_A \circ f = f = f \circ \mathrm{Id}_A$ para todo $f \in \mathrm{End}(A)$), ya que para todo endomorfismo $f \in \mathrm{End}(A)$ se tiene que

$$(\mathrm{Id}_A \circ f)(a) := \mathrm{Id}_A(f(a)) = f(a) = f(\mathrm{Id}_A(a)) =: (f \circ \mathrm{Id}_A)(a).$$

para todo $a \in A$ que consideremos.

Si **ahora suponemos** que A es un **anillo de Boole**, se puede probar que **se corrige la no existencia del elemento opuesto para la suma**. En efecto, pues, bajo lo que ya se ha probado, dados $a, b \in A$ arbitrarios, se tiene para $f \in \mathrm{End}(A)$ arbitrario que

$$(-f)(a + b) := -f(a + b) = -(f(a) + f(b)) = (-f)(a) + (-f)(b),$$

lo cual es cierto sin imponer ninguna condición sobre A siempre, pero con respecto al producto en A tenemos que

$$(-f)(a \cdot b) := -f(a \cdot b) = -f(a) \cdot f(b);$$

mientras que, por otro lado, obtenemos

$$(-f)(a) \cdot (-f)(b) := (-f(a)) \cdot (-f(b)) = f(a) \cdot f(b),$$

donde, como en general no es cierto que $-f(a)f(b) = f(a)f(b)$ en todo anillo (como ya hemos visto), no era posible demostrar que este es un endomorfismo de A. Sin embargo, cuando A es un anillo de Boole, puesto que $a = -a$ para cada $a \in A$ como ya se vio, esto sí que es cierto trivialmente. Nos preguntamos ahora: ¿Se corrige también el que la suma no sea cerrada en este caso? Si intentamos imponer que se corrija esta condición, vemos que para la suma en A no hay problemas en ningún anillo, pues

$$(f + g)(a + b) := f(a + b) + g(a + b) = f(a) + f(b) + g(a) + g(b) =: (f + g)(a) + (f + g)(b),$$

para cualesquiera $f, g \in \mathrm{End}(A)$ y $a, b \in A$ que consideremos, pero para el producto en A nos encontramos que, por un lado, se tiene que

$$(f + g)(a \cdot b) := f(a \cdot b) + g(a \cdot b) = f(a) \cdot f(b) + g(a) \cdot g(b),$$

mientras que, por otro lado, obtenemos que

$$\begin{aligned}(f + g)(a) \cdot (f + g)(b) &:= (f(a) + g(a)) \cdot (f(b) + g(b)) = \\ &= f(a) \cdot f(b) + f(a) \cdot g(b) + g(a) \cdot f(b) + g(a) \cdot g(b),\end{aligned}$$

donde, como en general no es cierto que $f(a) \cdot g(b) + g(a) \cdot f(b) = 0$ en todo anillo (como ya hemos visto), no era posible demostrar que la suma es un endomorfismo de A. En particular, si se corrige esto, también se arreglamos la otra condición. Pero estas no son equivalentes como puede verse en los anillos de Boole, pues la respuesta a esta pregunta que se ha hecho es que NO. Para verlo, es necesario dar un **contraejemplo**. En nuestro anillo de Boole favorito $A = \mathbb{Z}_2$ es imposible encontrarlo, por lo que es necesario pasar al siguiente nivel. Se sabe que los anillos de Boole finitos están caracterizados por su cardinal, que es una potencia de 2. Así pues, el siguiente anillo de Boole tiene que tener cardinal 4. Vamos a definir este de manera abstracta como

$$A := \{0, 1, x, y\}.$$

En este anillo, el 0 es, como sabe esperar, el elemento neutro para la suma, mientras que el 1 se corresponde con el elemento identidad para el producto, siendo así las operaciones no triviales en A que nos quedan por definir

$$x+1=y \iff x+y=1 \iff y+1=x,$$

pues $x\cdot y=0$ (estos deben ser divisores de cero), y además son $x^2=x$ y $y^2=y$ por definición en anillo de Boole (y se sigue que $2x=0=2y$). Tenemos así operaciones cerradas bien definidas en A que nos dan un anillo de Boole con cardinal 4. Si tomamos la aplicación $f\equiv \mathrm{Id}_A$ (endomorfismo de anillos en A) y $g\colon A\longrightarrow A$ definido por $g(0)=g(x)=0$ y $g(1)=g(y)=1$, donde g es también endomorfismo de anillos en A (se debe escribir que g preserva todas las suma y productos entre los elementos de A). Sin embargo, para $a=1$ e $b=x$ es

$$f(a)\cdot g(b)+f(b)\cdot g(a)=1\cdot 0+x\cdot 1=x\neq 0.$$

Una manera de dar sentido a este ejemplo es tomando el anillo cociente

$$A=\frac{\mathbb{Z}_2[x,y]}{(x^2-x,y^2-y,x+y+1,x\cdot y)}.$$

Se tiene así que g es la aplicación inducida por el homomorfismo evaluación $(x,y)=(0,1)$. Esta está bien definida, pues aplicada al ideal del cociente es nula, y es homomorfismo.

CONCLUSIONES: En general, no se dan contraejemplos para los axiomas que no se cumplen. **Es necesario darlos**. Cuando queremos probar que una afirmación es cierta, se demuestra; y, cuando queremos ver que esta es falsa, basta dar un contraejemplo para algún caso particular, demostrando que efectivamente no se cumple la afirmación dada.

Problema 2. Sea A un anillo conmutativo y unitario.

(1) Probar que los elementos nilpotentes de A forman un ideal (llamado *nilradical* de A).
(2) Un *ideal* $\mathfrak{a}$ propio de A se dice *radical* si, para todo $a\in A$, se cumple que, si existe $n\in\mathbb{Z}^+$ tal que $a^n\in\mathfrak{a}$, entonces $a\in\mathfrak{a}$. Probar que un ideal $\mathfrak{a}$ propio de A es radical si, y sólo si, el nilradical de $A/\mathfrak{a}$ es trivial. Deducir que todo ideal primo de A es radical. Encontrar un ejemplo de ideal NO primo que sea radical en $\mathbb{Z}$.
(3) Dado $\mathfrak{a}$ un ideal de A arbitrario, se define su *radical* como el conjunto

$$\sqrt{\mathfrak{a}}=\{a\in A\mid \exists\ n\in\mathbb{N} \text{ tal que } a^n\in\mathfrak{a}\}.$$

Demostrar que el radical de un ideal es el menor ideal radical que contiene a $\mathfrak{a}$.

Solución:

(1) Sea $\mathrm{Nil}(A)$ el nilradical de A. Por definición,

$$\mathrm{Nil}(A):=\{x\in A\mid \exists n\in\mathbb{N} \text{ t.q. } x^n=0\}.$$

Veamos que este es un ideal de A.
- Este es no vacío dado que $0\in\mathrm{Nil}(A)$ trivialmente.
- Sean $x,y\in\mathrm{Nil}(A)$ arbitrarios. Por definición, tenemos que existen $n,m\in\mathbb{N}$ tales que $x^n=0=y^n$. Sea $k:=n+m\in\mathbb{N}$. Por el **Teorema del Binomio de Newton**, como A es anillo conmutativo y unitario, tenemos que

$$(x-y)^k=\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}x^jy^{k-j}.$$

Veamos que bajo nuestras hipótesis esto es cero. En efecto,

- si $j \geq n$ tenemos que $x^j = 0$ y, por tanto, es
$$(-1)^{k-j}\binom{k}{j}x^j y^{k-j} = 0.$$
- si $j < n$ entonces es $k - j = m + n - j \geq m$. Por tanto $y^j = 0$ de donde se sigue que
$$(-1)^{k-j}\binom{k}{j}x^j y^{k-j} = 0.$$

En resumen, se tiene que $(x - y)^k = 0$.

- Sean $x \in \mathrm{Nil}(A)$ y $a \in A$ arbitrarios. Por definición, tenemos que existe $n \in \mathbb{N}$ tal que $x^n = 0$. Así, como A es conmutativo, llegamos a que
$$(ax)^n = a^n x^n = 0,$$
luego $ax \in \mathrm{Nil}(A)$.

En conclusión, se ha demostrado que $\mathrm{Nil}(A)$ es un ideal de A.

(2) La primera parte es inmediata por las definiciones de ideal radical y nilradical. En efecto, tenemos que $\mathrm{Nil}(A/\mathfrak{a}) = \{[0]\}$ por definición si, y sólo si, se tiene que, para todo $x + \mathfrak{a} \in A/\mathfrak{a}$ tal que exista $n \in \mathbb{N}$ con $(x + \mathfrak{a})^n = x^n + \mathfrak{a} = \mathfrak{a}$ entonces $x + \mathfrak{a} = \mathfrak{a}$. En otras palabras, si, para todo $x \in A$ tal que exista $n \in \mathbb{N}$ con $x^n \in \mathfrak{a}$ entonces $x \in \mathfrak{a}$. Pero esto último es la definición de ideal radical para $\mathfrak{a}$. Ahora, sabemos que los ideales primos $\mathfrak{p}$ de A están caracterizados por los cocientes $A/\mathfrak{p}$ que sean dominios de integridad. Ahora bien, como en todo dominio íntegro NO se tienen elementos nilpotentes no triviales (pues, de lo contrario, tendríamos divisores de cero entre manos), tenemos que el ideal primo $\mathfrak{p}$ del que partimos es radical en virtud de la equivalencia que se acaba de probar. El ideal $6\mathbb{Z}$ no es primo como bien sabemos, ya que en el cociente $\mathbb{Z}_6$ tenemos que $[2]_6 \cdot [3]_6 = [0]_6$ (y, por tanto, no es un dominio íntegro). Sin embargo, este es radical, ya que, si tenemos $x \in \mathbb{Z}$ para el que existe $n \in \mathbb{N}$ con $x^n \in 6\mathbb{Z}$ (esto es, se tiene $k \in \mathbb{Z}$ con $x^n = 6k$), como 6 es libre de cuadrados, necesariamente $x = 6k'$ con $k' \in \mathbb{Z}$. En efecto, pues $x = up_1^{r_1} \cdots p_m^{r_m}$ con $u \in \{\pm 1\}$ unidad; $m, r_1, \ldots, r_m \in \mathbb{N}$ y $p_1, \ldots, p_m$ irreducibles ordenados de menor a mayor (números primos), por lo que $x^n = u^n p_1^{nr_1} \cdots p_m^{nr_m} = 6k$ donde, como 6 es libre de cuadrados, necesariamente $p_1 = 2$ y $p_2 = 3$ con $r_1, r_2 \geq 1$. Luego $x \in 6\mathbb{Z}$.

(3) Tenemos que probar un total de cuatro cosas:

(i) $\sqrt{a}$ es ideal.
(ii) $\sqrt{a}$ es radical.
(iii) $\sqrt{a}$ contiene a $\mathfrak{a}$.
(iv) $\sqrt{a}$ es el menor[2] verificando (i)-(iii).

Que $\sqrt{a}$ es ideal radical es evidente (pues para ver que es ideal basta reciclar la prueba dada para $\mathrm{Nil}(A)$ con el anillo $A/\mathfrak{a}$ y que este es radical se tiene por la propia definición). Ahora, que contiene a $\mathfrak{a}$ es trivial, pues todo $a \in \mathfrak{a}$ verifica que existe $n \in \mathbb{N}$ tal que $x^n \in \mathfrak{a}$ (para $n = 1$). Finalmente, veamos que es el menor verificando todo esto. En otras palabras, supongamos que $I \subseteq A$ es otro ideal de A radical que contiene a $\mathfrak{a}$. Se trata de probar que entonces $\sqrt{a} \subseteq I$. En efecto, sea $x \in \sqrt{a}$ arbitrario. Por definición, existe $n \in \mathbb{N}$ tal que $x^n \in \mathfrak{a}$. Como I contienen a $\mathfrak{a}$ por hipótesis, entonces $x^n \in I$. Pero como I es también ideal radical, necesariamente $x \in I$ por definición. En resumen, queda probado que $\sqrt{a}$ es un ideal radical que contiene a $\mathfrak{a}$ que, de hecho, es el menor verificando todo esto.

[2]Se entiende que va referido en el sentido de la inclusión.

CONCLUSIONES: En general, **da la impresión** de que hay problemas a la hora de interactuar con la definición de ideal radical. Puede resultar de ayuda, cuando a uno le introducen un nuevo concepto, pensar qué estamos definiendo en anillos que manejamos muy bien (por ejemplo, en $\mathbb{Z}$). Un grupo incluye como opción en nilradical trivial que este sea el total, lo cual está muy bien visto de la manera que estaba redactado el ejercicio (para que no haya dudas por tanto, vamos a suponer que tenemos ideales propios). No olvidéis que para tener un **ideal**, este tiene que ser **no vacío** (en general, se ha olvidado probar esto aunque sea una tontería). Otro grupo olvida ver que la suma es cerrada (¿Por qué?)Hay problemas también a la hora de decidir cuál es "el camino fácil" para realizar algunas pruebas. Es importante tener en mente todas las nociones equivalentes que se van probando (a veces ayuda pasar al cociente en cierto tipo de ideales...). Una vez más, cuando uno da un contraejemplo, debe explicarse que, efectivamente, este lo es. Finalmente, muchas personas se hacen un lio en la última parte (gente va incluso más allá probando que $\sqrt{a}$ es la intersección de todos los ideales radicales que contienena $\mathfrak{a}$), y dejan sin demostrar alguna de las cuatro cosas que deben demostrarse para concluir correctamente el ejercicio.

Problema 3. Consideremos $f\colon A \longrightarrow B$ un epimorfismo de anillos y $\mathfrak{a}$ un ideal de A.

(1) Probar que la imagen por f de $\mathfrak{a}$ es ideal en B.

Supongamos ahora que f es biyectiva y sea $\mathfrak{b} = f(\mathfrak{a})$.

(2) Probar que se tiene el isomorfismo $A/\mathfrak{a} \cong B/\mathfrak{b}$.
(3) Deducir que f establece una biyección entre los ideales de A y los de B; y que, en esta biyección, los ideales primos, maximales y radicales de A[3] se corresponden con los ideales primos, maximales y radicales, respectivamente, de B.

Solución:

(1) Sea $f(\mathfrak{a}) := \{b \in B \mid \exists\ a \in \mathfrak{a} \text{ t.q. } f(a) = b\} \subseteq B$. Veamos que es ideal. En efecto,
- es obvio que este no es vacío, pues $f(0_A) = 0_B \in f(\mathfrak{a})$ por ser f un homomorfismo de anillos, donde $\mathfrak{a}$ es un ideal (que por tanto contiene al neutro en A).
- Sean $x, y \in f(\mathfrak{a})$ arbitrarios. Por definición, existen $x', y' \in \mathfrak{a}$ tales que $x = f(x')$ e $y = f(y')$. Tenemos entonces que
$$x + y = f(x') + f(y') = f(x' + y').$$
Luego, existe $x' + y' \in \mathfrak{a}$ (por ser este ideal) tal que $x + y = f(x' + y')$. Esto es, se ha probado que $x + y \in f(\mathfrak{a})$.
- Sean $x \in f(\mathfrak{a})$ y $b \in B$ arbitrarios. Por definición, existe $x' \in \mathfrak{a}$ tal que $x = f(x')$. Además, como f es sobreyectiva, tenemos que existe $a \in A$ tal que $f(a) = b$. Por tanto,
$$bx = f(a)f(x') = f(ax') \quad \text{y} \quad xb = f(x')f(a) = f(x'a).$$
Esto es, por definición existen $ax', x'a \in \mathfrak{a}$ (por ser este ideal) para los que es $bx = f(ax')$ y $xb = f(x'a)$. En otras palabras, se ha probado que $bx, xb \in f(\mathfrak{a})$.

En conclusión, se ha demostrado que $f(\mathfrak{a})$ es un ideal de B.

[3]Se sobreentiende que para esta parte se suponen sobre A y B todas las condiciones necesarias para que estas tres nociones tengan sentido. A saber, que estos dos son anillos conmutativos y unitarios (pues, de lo contrario, no tiene sentido hablar de ideales radicales).

(2) Vamos a considerar el epimorfismo canónico

$$\begin{array}{rccc} \pi_B\colon & B & \longrightarrow & \frac{B}{\mathfrak{b}} \\ & b & \mapsto & \pi(b) := b + \mathfrak{b} \end{array}.$$

Sea $g := \pi_B \circ f\colon A \longrightarrow B/\mathfrak{b}$. Este vuelve a ser epimorfismo, pues es composición de dos epimorfismos. Calculemos su núcleo, teniendo en cuenta que f es isomorfismo.

$$\ker g := \{a \in A \mid g(a) = 0_B + \mathfrak{b}\} =$$

$$= \{a \in A \mid \pi_B(f(a)) = f(0_A) + f(\mathfrak{a})\} = \{a \in A \mid \pi_B(f(a)) \in f(\mathfrak{a})\} =$$

$$= \left\{a \in A \mid \pi_{f^{-1}(B)}(a) \in \mathfrak{a}\right\} = \{a \in A \mid \pi_A(a) \in \mathfrak{a}\} = \ker \pi_A = \mathfrak{a}.$$

Aplicando en estas circunstancias el **Primer Teorema de Isomorfía** a la aplicación g que hemos definido, obtenemos que

$$\frac{A}{\ker g} \cong \mathrm{Im} g \iff \frac{A}{\mathfrak{a}} \cong \frac{B}{\mathfrak{b}},$$

el cual se trata del isomorfismo deseado. Este resultado también nos dice que este viene dado explícitamente por la aplicación

$$\begin{array}{rccc} \widetilde{g}\colon & \frac{A}{\mathfrak{a}} & \longrightarrow & \frac{B}{\mathfrak{b}} \\ & a + \mathfrak{a} & \mapsto & f(a) + \mathfrak{b}. \end{array}.$$

(3) Es obvio que f nos determina una correspondencia entre los ideales de A y B. En efecto, como f es biyectiva, tenemos que un ideal $\mathfrak{a}$ de A cumple que $(f^{-1} \circ f)(\mathfrak{a}) = \mathfrak{a}$. Sea $\mathfrak{b} = f(\mathfrak{a})$ el correspondiente ideal de B. Tenemos entonces que $\mathfrak{a} = f^{-1}(\mathfrak{b})$ viene unívocamente determinado por un ideal de B. Como los papeles de A y B son intercambiables, hemos demostrado que f establece una biyección entre los ideales de A y B. Veamos ahora que esta **preserva primalidad, maximalidad y radicalidad**, suponiendo sin mucho esfuerzo que estamos antes anillos conmutativos y unitarios (para que estos tres conceptos estén bien definidos):

- Para el caso de **ideales primos**, podemos usar directamente la caracterización por cocientes. A saber, sabemos que $\mathfrak{p}$ es ideal primo si, y sólo si, el anillo cociente $A/\mathfrak{p}$ es dominio de integridad. Así, como tenemos que $A/\mathfrak{p} \cong B/f(\mathfrak{p})$, donde $f(\mathfrak{p})$ ideal en B está unívocamente determinado por $\mathfrak{p}$ como hemos visto, al preservarse el ser dominio de integridad mediante isomorfismos, todo esto es equivalente a que $f(\mathfrak{p})$ sea ideal primo de B.
- Para el caso de **ideales maximales**, bajo las hipótesis que hemos impuesto sobre los anillos, podemos utilizar la caracterización por cocientes. A saber, como $\mathfrak{m}$ es ideal maximal si, y sólo si, el anillo cociente $A/\mathfrak{m}$ es cuerpo, bajo el isomorfismo $A/\mathfrak{m} \cong B/f(\mathfrak{m})$ dado, donde $f(\mathfrak{m})$ ideal en B está unívocamente determinado por $\mathfrak{m}$ ideal inicial, como el ser cuerpo se preserva mediante isomorfismos, todo esto es equivalente a que $f(\mathfrak{m})$ sea ideal maximal de B.
- Para el caso de **ideales radicales**, bajo las condiciones que hemos puesto a nuestros anillos y en virtud de lo que se ha probado en el ejercicio anterior, podemos usar la caracterización por el nilradical del cociente. A saber, como $\mathfrak{r}$ es ideal radical si, y sólo si, el nilradical del anillo cociente $A/\mathfrak{r}$ es trivial, bajo el isomorfismo $A/\mathfrak{r} \cong B/f(\mathfrak{r})$ dado, donde $f(\mathfrak{r})$ es un ideal en B que está unívocamente determinado por $\mathfrak{r}$ anterior, al preservarse el ser elemento nilpotente mediante isomorfismos (pues depende únicamente de la estructura del anillo), todo esto es equivalente a que $f(\mathfrak{r})$ sea ideal radical de B.

Con todo esto, podemos dar por concluida la resolución del apartado.

CONCLUSIONES: Se resuelve el ejercicio haciendo muchas veces más de lo necesario. Por ejemplo, no hace falta argumentar las cosas en el último apartado en las dos direcciones porque los papeles de A y B son intercambiables (ser isomorfismo es relación de equivalencia). No es necesario definir el isomorfismo entre los cocientes (basta probar su existencia), y hay gente que no prueba todo lo necesario (bien definida, homomorfismo y biyectivo). Emplear resultados ya conocidos sobre isomorfía facilita mucho el trabajo. En algunos casos, parece no estar claro lo que significa "ser isomorfo" en anillos. A saber, que la estructura de un anillo (suma y producto) viene unívocamente determinada por cualquier objeto que sea isomorfo. Para la última parte, como se han definido ideales radicales sólo en anillos conmutativos y unitarios (fuera no sabemos si esta noción tiene sentido en principio), podemos suponer que estamos en este caso. De esta manera, puede uno razonar sobre los cocientes.

Problema 4**.**

(1) Usando que todo subconjunto no vacío de los enteros positivos tiene un elemento mínimo (**Teorema del Buen Orden**) y el **Teorema de la División**, probar que todo ideal de $\mathbb{Z}$ es principal; esto es, está generado por los múltiplos de un elemento.
(2) Utilizando el **Ejercicio** 13 de la primera **Hoja de Problemas**, deducir que un ideal propio de $\mathbb{Z}$ es primo si, y sólo si, es maximal. Concluir que los ideales primos de $\mathbb{Z}$ (distintos del trivial) son aquellos generados por un número primo.

Solución:

(1) Sea $\mathfrak{a} \subseteq \mathbb{Z}$ un ideal. Si $\mathfrak{a}$ es trivial, se tiene que $\mathfrak{a} = (0)$ o $\mathfrak{a} = \mathbb{Z} = (1)$. Supongamos que $\mathfrak{a}$ es propio y sea $n \in \mathbb{Z}$ el elemento mínimo de $\{m : m \in \mathfrak{a}, m > 0\} \subseteq \mathbb{N}$ (**Teorema del Buen Orden**). Comprobemos que $\mathfrak{a} = n\mathbb{Z}$. Esto es, cualquier elemento de $\mathfrak{a}$ es un múltiplo de n. Sea $m \in \mathfrak{a}$ arbitrario, por el **Teorema de División**, se tiene que existen dos enteros únicos $q, r \in \mathbb{Z}$ con $0 \leq r \leq n-1$ de forma que $m = qn + r$. Si tenemos que $r = 0$ hemos terminado. En caso contrario, se tendría que $r = m - qn \in \mathfrak{a}$. En otras palabras, tendríamos que r es un entero positivo menor que n perteneciente al ideal. Esto es imposible por construcción, luego forzosamente $r = 0$ y $\mathfrak{a} = n\mathbb{Z}$.
(2) Sea $n\mathbb{Z} \subseteq \mathbb{Z}$ un ideal propio. Sabemos que $n\mathbb{Z}$ es primo si, y sólo si, el cociente $\mathbb{Z}_n$ es un dominio de integridad. Por otro lado, el ideal $n\mathbb{Z}$ es maximal, si y sólo si, el cociente $\mathbb{Z}_n$ es cuerpo. Todo se reduce por tanto a comprobar que $\mathbb{Z}_n$ es dominio si, y sólo si, es cuerpo. Ahora bien, esto es consecuencia directa del **Ejercicio** 13 de la primera **Hoja de Problemas**; ya que $\mathbb{Z}_n$ es un anillo conmutativo, unitario (pues es el cociente de un anillo conmutativo y unitario) y finito. En conclusión, tenemos que este es dominio íntegro si, y sólo si, es cuerpo. Dicho de otra forma, el ideal $n\mathbb{Z}$ es primo si, y sólo si, es maximal. Sea ahora $n\mathbb{Z}$ un ideal de $\mathbb{Z}$. Hemos probado que este es primo si, y sólo si, es maximal. Por definición, el ideal $n\mathbb{Z}$ es maximal si, y sólo si, para cualquier otro ideal $m\mathbb{Z}$ con $n\mathbb{Z} \subseteq m\mathbb{Z}$ se tiene que $m\mathbb{Z} = n\mathbb{Z}$ ó $m\mathbb{Z} = \mathbb{Z}$. Nótese que la condición $n\mathbb{Z} \subseteq m\mathbb{Z}$ es equivalente a que $m|n$ y que $m\mathbb{Z} = n\mathbb{Z}$ ó $m\mathbb{Z} = \mathbb{Z}$ es equivalente a decir que $m = n$ ó $m = 1$. Esto equivale a que para todo entero positivo m con $m|n$ se tenga que $m = n$ ó $m = 1$ (definición de que n sea primo).

CONCLUSIONES: No ha habido grandes dificultades en la resolución de este ejercicio en general, salvo quizás pocos casos en los que se lía la gente en las pruebas (haciendo incluso más de lo necesario, pues las cosas probadas en clase no hace falta probar).