ENTREGA 2. EEAA. GRUPO M3 (19-20).
CARLOS ANDRADAS Y ANDONI DE ARRIBA.

Fecha límite: 31-X-2019 antes de las 17:00 horas[1].

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

Problema 1. Buscar la noción de *Anillo Noetheriano*, y responder a las siguientes cuestiones.

Definicion 1. Se dice que un *anillo* A **conmutativo**[2] es *Noetheriano* si satisface cualquiera de los enunciados dados en el **Teorema 2** que, como se va a probar, son dos a dos equivalentes.

(1) Rellenar los huecos en la siguiente demostración.

Teorema 2. *Si A es anillo conmutativo, son equivalentes las afirmaciones siguientes:*
(i) *Todos los ideales de A son finitamente generados.*
(ii) *Todo conjunto no vacío de ideales propios en A tiene un elemento maximal*[3]*.*
(iii) *Toda cadena ascendente de ideales propios*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots \tag{1}$$

es estacionaria[4]*.*

Demostración. En efecto, se procede de manera cíclica:

- $(i) \Longrightarrow (iii)$: Sea
$$I := \bigcup_{j \in \mathbb{N}} I_j.$$
Como los ideales I_j están encadenados, entonces I es un ideal de A. En efecto, la condición de ideal es trivial por verificarse para cada ideal de la unión. Para ver que es además subgrupo aditivo, lo único no sencillo es ver que es cerrado para la diferencia. A saber, dados $x, y \in I$ arbitrarios, se trata de probar que $x - y \in I$. **Aquí es donde entra que los ideales están encajados**. Sabemos que existen $n, m \in \mathbb{N}$ tales que $x \in I_n$ e $y \in I_m$. Supongamos sin pérdidad de generalidad que $m \leq n$. Entonces, tenemos que $I_m \subseteq I_n$ y, por tanto $y \in I_n$. Así, como I_n es ideal, se tiene que $x - y \in I_n \subseteq I$. Luego, **en estas condiciones, la unión de ideales es ideal**. Más aún, este es propio porque los I_j lo son. Por hipótesis, sabemos que I es finitamente generado. Escribimos $I = (a_1, \ldots, a_n)$. Nótese que, tomando m suficientemente grande, es $a_i \in I_m$ para todo $i \in \{1, \ldots, n\}$. En efecto, como existe un mínimo índice $j_i \in \mathbb{N}$ tal que $a_i \in I_{j_i}$ para cada $i \in \{1, \ldots, n\}$ dado, basta tomar $m := \max\{j_1, \ldots, j_n\}$. Luego, tenemos que $I \subseteq I_m$. A saber, se cumple que $I_k = I_m$ cuando $k \geq m$.

[1]Plazo ampliado, a pertición popular, en **una semana**, hasta el **día 8-X-2019 a las 20:00 horas**.

[2]En general, es necesario considerar nociones (naturales) de anillos Noetherianos a izquierda y derecha.

[3]Dado $(P, \leq)$ un conjunto parcialmente ordenado, así como $S \subseteq P$ un subconjunto, se dice que $s \in S$ es un *elemento máximo* en S si para todo $x \in S$ es $x \leq s$. En particular, todo *elemento* máximo es *maximal*. A saber, se tiene que para todo $x \in S$ tal que $s \leq x$ entonces, necesariamente, es $x = s$. El recíproco no es cierto en general, y, de hecho, el elemento máximo, si existe, es único (a diferencia de los elementos maximales que puede haber varios). Por ejemplo, en el conjunto de todos los **ideales** de un anillo, los **maximales** son, valga la redundancia, todos los **elementos** que son **maximales** en dicho conjunto ordenado parcialmente por la inclusión. Pero no siempre se tiene un elemento máximo (este sería el único ideal maximal en caso de no haber más). Los anillos con un único ideal maximal son muy importantes, y se conocen como *anillos locales*.

[4]Una cadena de ideales propios (1) se dice *estacionaria* si existe un entero $m \in \mathbb{Z}$ tal que $I_m = I_{m+1} = \cdots$.

- $(ii) \Longrightarrow (i)$: Si $I \subseteq A$ es ideal propio, sea $\mathcal{F}$ la familia de ideales contenidos en I del tipo $(a_1, \ldots, a_m)$. A saber, $\mathcal{F} = \{(a_1, \ldots, a_m) \mid a_i \in I, \ \forall\, i \in \{1, \ldots, m\}\}$. Por hipótesis, esta familia tiene un elemento maximal, digamos $J := (a_1, \ldots, a_n)$ (con $n \geq m$). Entonces, para todo $a \in I$ arbitrario, se tiene que $J + (a) \in \mathcal{F}$ es un ideal (finitamente generado) contenido en I con $J \subseteq J + (a)$ trivialmente, y, como J es elemento maximal, necesariamente $J + (a) = J$. Por tanto, se tiene que $a \in J$ y así se ha probado que $I = J$ es un ideal finitamente generado.
- $(iii) \Longrightarrow (ii)$: Si $\mathcal{F}$ es una familia no vacía de ideales propios en A que **no contiene** un elemento maximal[5] entonces para cualquier $I_1 \in \mathcal{F}$ existe $I_2 \in \mathcal{F}$ tal que $I_1 \subsetneq I_2$. De esta manera, se puede construir trivialmente una cadena que no es estacionaria inductivamente.

Con esto se concluye la demostración. □

Sea A un DI conmutativo.

(2) Dado $x \in A \backslash A^*$ no nulo tal que no admite factorización en A como producto de irreducibles, probar que existe $y \in A$ que no se factoriza con $(x) \subsetneq (y) \subsetneq A$. Deducir que si A es Noetheriano, entonces es **Dominio de Factorización** (las factorizaciones pueden no ser únicas). Si además todo irreducible de A es primo, entonces A es DFU.

(3) Dar un ejemplo de anillo NO Noetheriano, y de otro que SÍ lo sea; razonando un mínimo los motivos. **Sugerencia:** Lo mejor es usar la condición (i) del **Teorema 2**.

Solución:

(2) Dado que $x \in A \backslash A^*$ no nulo es tal que no se factoriza como producto de irreducibles en A por hipótesis, se tiene, en particular, que x no es un elemento irreducible. Por tanto, han de existir $a, b \in A \backslash A^*$ tales que $x = ab$ (a saber, es reducible). Más aún, al menos uno de estos dos elementos no admite tampoco factorización como producto de irreducibles en A trivialmente; pues, en caso contrario, tendríamos que x también tiene que admitir una factorización de ese tipo (dada por el producto de las otras dos factorizaciones), en contra de la hipótesis. Supongamos sin pérdida de generalidad que es a el elemento que no admite factorización como producto de irreducibles (lo cual podemos hacer porque A es conmutativo). Entonces, es obvio que $(x) \subsetneq (a) \subsetneq A$ pues tanto a como b son no unidades. En efecto, si existe $c \in A$ tal que $a = xc = abc$ se tendría que $a(1 - bc) = 0$ donde, como A es DI por hipótesis, necesariamente $1 = bc$ en contra de que b sea no unidad. Como consecuencia de este resultado, si partimos de un anillo que no es Dominio de Factorización, podemos construir, de manera inductiva, una cadena ascendente de ideales propios principales que nunca se estaciona. Luego, por definición, se tiene que A no puede ser Noetheriano. Por el contrarecíproco, se ha demostrado que todo Anillo Noetheriano es Dominio de Factorización. Supongamos ahora que todo elemento irreducible de A es primo. Veamos que toda factorización en A como producto de irreducibles es única. En efecto, sea $x \in A$ un elemento arbitrario que admite factorización como producto de irreducibles en A. Por defínición, se tiene $x = p_1 p_2 \cdots p_n$ con $n \in \mathbb{N}$ y $p_i \in A$ elementos irreducibles en A para cada $i \in \{1, \ldots, n\}$. Veamos que, si existe otra factorización como producto de irreducibles en A, entonces estas tienen el mismo número de elementos que son dos a dos asociados.

[5] Si supusiéramos que esta familia no contiene un elemento máximo, no podríamos asegurar lo que sigue, pues pueden existir elementos maximales. Por ejemplo, en la familia $\mathcal{F} = \{2\mathbb{Z}, 3\mathbb{Z}\}$ no vacía de ideales propios en $\mathbb{Z}$ (Noetheriano como se va a ver), se tienen dos elementos maximales, pero ninguno de ellos es máximo.

Dicho de otra forma, si tenemos que $q_1q_2\cdots q_m$ es otra factorización en A como producto de irreducibles con m un cierto entero, entonces se trata de probar que $n = m$ y $p_i \sim q_i$ para cada $i \in \{1,\dots,n\}$ tras una reordenación de los elementos en la factorización. En efecto, esto se sigue del hecho de que todo irreducible en A es también primo. Supongamos por tanto que se tiene la igualdad entre estas dos factorizaciones. A saber, es $x = p_1p_2\cdots p_n = q_1q_2\cdots q_m$. Es obvio que $p_i|q_1q_2\cdots q_m$ para cada $i \in \{1,\dots,n\}$ trivialmente. Luego, por la condición de primalidad, existe $j \in \{1,\dots,m\}$ tal que $p_i|q_j$. Vamos a suponer sin pérdida de generalidad que $j = 1$. Por definición, existe $a \in A$ tal que $q_1 = ap_1$. Ahora bien, como q_1 es irreducible, dado que p_1 no es unidad (pues también es irreducible), la única conclusión posible es que a sea unidad y, por tanto, tengamos que p_1 y q_1 son asociados. Así, cancelando términos, se tiene que $p_2\cdots p_n = aq_2\cdots q_m$. Reiterando por tanto este argumento un número finito de pasos, llegamos a que $n = m$ y $p_i \sim q_i$ para cada $i \in \{1,\dots,n\}$. A saber, la factorización es única. Por tanto, todo Anillo Noetheriano en el que los elementos irreducibles sean también primos es DFU. Por ejemplo, como todo DIP es Noetheriano trivialmente (condición (i) del **Teorema 2**, pues en particular todo ideal principal es finitamente generado), y en los DIPs todo irreducible es primo como bien sabemos, hemos obtenido otra forma de demostrar que DIP implica DFU.

(3) Como acabamos de decir, cualquier DIP nos vale como ejemplo de Anillo Noetheriano. Basta tomar por tanto los enteros Gaussianos $\mathbb{Z}[i]$. Ahora, para dar un ejemplo de Anillo NO Noetheriano, lo más sencillo es concentrar los esfuerzos en hacer fallar la condición (i) del **Teorema 2**. A saber, se trata de construir un anillo A que tenga, al menos, un ideal que no sea finitamente generado. Basta tomar un anillo de polinomios con infinitas (numerables) indeterminadas para ello. A saber, por ejemplo, el anillo[6]

$$\mathbb{R}\left[\{x_j\}_{j\in\mathbb{N}}\right],$$

dado que este tiene a

$$I := \left(\{x_j\}_{j\in\mathbb{N}}\right)$$

como ideal, que en ningún caso es finitamente generado (no podemos obtener ninguna indeterminada como producto de las demás).

CONCLUSIONES: En la primera parte, muchos olvidan probar que la unión de ideales es en este caso ideal (en general, esto no es cierto) y hay una errata (sólo una persona se ha percatado), que no es muy importante para esta asignatura puesto que es un asunto de lógica, y es que el elemento ha de ser maximal (no máximo). Algunos cambian la prueba $(ii) \Longrightarrow (i)$ por alguna razón. En el resto de apartados, bastante bien en general (típicos lios en alguna resolución), salvo en los ejemplos (hay gente que los deja en blanco, sin haber preguntado), ya que en algunos casos no se emplean las palabras clave (se dan vueltas innecesarias).

[6]Si tenemos que A es un anillo, entonces el conjunto

$$A\left[\{x_j\}_{j\in\mathbb{N}}\right]$$

de los polinomios en las infinitas (numerables) indeterminadas $\{x_j\}_{j\in\mathbb{N}}$ tiene también estructura de anillo con las operaciones suma y producto usuales

$$\begin{aligned} p\left(\{x_j\}_{j\in\mathbb{N}}\right) + q\left(\{x_j\}_{j\in\mathbb{N}}\right) &:= (p+q)\left(\{x_j\}_{j\in\mathbb{N}}\right); \\ p\left(\{x_j\}_{j\in\mathbb{N}}\right) \cdot q\left(\{x_j\}_{j\in\mathbb{N}}\right) &:= (p\cdot q)\left(\{x_j\}_{j\in\mathbb{N}}\right), \end{aligned}$$

para todo $p, q \in A\left[\{x_j\}_{j\in\mathbb{N}}\right]$.

Problema 2. En el anillo A de los enteros Gaussianos,

(1) estudiar si el ideal $\mathfrak{a}$ generado por $236+160i$ y $35+3i$ es principal, dando un generador del mismo y unos coeficientes para una identidad de Bézout en caso afirmativo.
(2) calcular el máximo común divisor de $-3+35i$ y $160-236i$. ¿Es un elemento primo?
(3) determinar el núcleo y la imagen del **único homomorfismo de anillos unitarios**

$$f\colon \mathbb{Z} \to \frac{A}{\mathfrak{a}}.$$

Describir el anillo $A/\mathfrak{a}$ (dando su estructura) y calcular su cardinal.

Solución:

(1) Como $\mathbb{Z}[i]$ es un DE como ya sabemos (**Ejercicio** 16 **de la Hoja** 2), en particular es un DIP, y por tanto el ideal generado por $236+160i$ y $35+3i$ es principal con todal seguridad. De hecho, el generador es su máximo común divisor, pues

$$\mathfrak{a} = (236+160i)\mathbb{Z}[i] + (35+3i)\mathbb{Z}[i] = \mathrm{mcd}(236+160i, 35+3i)\mathbb{Z}[i].$$

Este se puede calcular por medio del **Algoritmo de Euclides (Extendido)**, y es esto mismo lo que nos proporcionará una identidad de Bézout. Realizamos las sucesivas divisiones, que nos dan los siguientes resultados:

$$\frac{236+160i}{35+3i} = \frac{(236+160i)(35-3i)}{(35+3i)(35-3i)} = \frac{1}{1234}(8740+4892i) =$$

$$= (7+4i) + \frac{1}{1234}(102-44i) \iff (236+160i) = (35+3i)(7+4i) + \boxed{(3-i)};$$

en el siguiente paso

$$\frac{35+3i}{3-i} = \frac{(35+3i)(3+i)}{(3-i)(3+i)} = \frac{1}{10}(102+44i) =$$

$$= (10+4i) + \frac{1}{10}(2+4i) \iff (35+3i) = (3-i)(10+4i) + \boxed{(1+i)};$$

y, finalmente, se tiene que

$$\frac{3-i}{1+i} = \frac{(3-i)(1-i)}{(1+i)(1-i)} = \frac{1}{2}(2-4i) = (1-2i)+0 \iff$$

$$\iff (3-i) = (1+i)(1-2i) + \boxed{0}.$$

Por tanto, como el máximo común divisor es el último resto no nulo que se obtiene tras realizar las sucesivas diviones por medio del **Algoritmo de Euclides**, obtenemos que $\mathrm{mcd}(236+160i, 35+3i) = 1+i$ (único salvo asociados). Esto es,

$$\mathfrak{a} = (236+160i, 35+3i)\mathbb{Z}[i] = (1+i)\mathbb{Z}[i].$$

Además, de las expresiones anteriores se obtiene la identidad de Bézout mediante un proceso de marcha atrás (lo que se conice por **Algoritmo de Euclides Extendido**). A saber, se tiene que

$$(1+i) = (35+3i) - (3-i)(10+4i) =$$

$$= (35+3i) - ((236+160i) - (35+3i)(7+4i))(10+4i) =$$

$$= (55+68i)(35+3i) - (10+4i)(236+160i) \iff$$

$$\iff \boxed{1+i = (55+68i)(35+3i) - (10+4i)(236+160i)}.$$

(2) Podemos observar que

$$-3+35i = i(35+3i) \quad \text{y} \quad 160-236i = -i(236+160i).$$

Esto es, los dos enteros Gaussianos que tenemos entre manos son los mismos dados en el apartado anterior, salvo multiplicación por una unidad en $\mathbb{Z}[i]$. Dicho de otra forma, el máximo común divisor de estos dos elementos es el mismo (salvo asociados) que hemos obtenido antes por la propia definición. Es obvio que este es un elemento primo (que, de hecho, equivale a que sea irreducible porque estamos en un DE), pues su norma es 2 (primo en $\mathbb{Z}$), por lo visto en el **Ejercicio** 1 **ó** 2 **de la Hoja** 2.

(3) Lo primero es observar que, como $\mathbb{Z}[i]$ es DE, entonces, por ser $\mathfrak{a}$ maximal (está generado por un elemento primo en un DE), el anillo cociente $\mathbb{Z}[i]/\mathfrak{a}$ es un cuerpo. Sea ahora $\varphi : \mathbb{Z} \to \mathbb{Z}[i]/\mathfrak{a}; k \mapsto k+\mathfrak{a}$, el único homomorfismo de anillos unitarios que va de $\mathbb{Z}$ a $\mathbb{Z}[i]$. Esto es, este es la composición entre los homomorfismos de anillos

$$f: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}[i] \\ n & \mapsto & f(n) := n \end{array} \quad \text{y} \quad \pi: \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \frac{\mathbb{Z}[i]}{\mathfrak{a}} \\ a+bi & \mapsto & \pi(a+bi) := (a+bi)+\mathfrak{a} \end{array},$$

los cuales sabemos que son únicos por construcción. El núcleo de $\varphi = \pi \circ f$ es

$$\ker \varphi = \ker(\pi \circ f) = \mathbb{Z} \cap \ker(\pi) = \mathbb{Z} \cap \mathfrak{a},$$

dado que f es una aplicación inyectiva y $\ker \pi = \mathfrak{a}$. Veamos que, de hecho, este es $2\mathbb{Z}$. En efecto, es claro que $2\mathbb{Z} \subseteq \ker \varphi$ pues se tiene la identidad $2 = (1-i)(1+i) \in \mathfrak{a}$. Nótese que $2\mathbb{Z}$ es un ideal maximal en $\mathbb{Z}$ (al ser 2 un número primo), luego, por maximalidad, dado que el núcleo de un homomorfismo de anillos es siempre un ideal, se tiene que $\ker \varphi = 2\mathbb{Z}$ ó $\ker \varphi = \mathbb{Z}$. Es claro que $1 \notin \ker \varphi$ porque $1+i$ no es una unidad, por lo tanto necesariamente es $\ker \varphi = 2\mathbb{Z}$. Comprobemos que φ es sobreyectiva. En otras palabras, se tiene que $\mathrm{Im}(\varphi) = \mathbb{Z}[i]/\mathfrak{a}$. Basta ver que existe un entero $k \in \mathbb{Z}$ de forma que $\varphi(k) = i+\mathfrak{a}$. En efecto, visto esto, se tendrá que para cualesquiera $a, b \in \mathbb{Z}$ es $\varphi(a+kb) = (a+ib)+\mathfrak{a}$, por estar ante un homomorfismo de anillos unitario, y, en consecuencia, tendremos que φ será sobreyectiva. Comprobemos por tanto que existe $k \in \mathbb{Z}$ con $\varphi(k) = i$. Pero esto es trivial, pues basta observar que se tiene la igualdad $i+\mathfrak{a} = -1+\mathfrak{a} = \varphi(-1)$ trivialmente, por como viene dado el ideal $\mathfrak{a}$. Por lo tanto, se ha demostrado que φ es sobreyectiva. Ahora, aplicando el **Primer Teorema de Isomorfía**, se concluye que $\mathbb{Z}[i]/\mathfrak{a} \cong \mathbb{Z}_2$ es el cuerpo de 2 elementos[7]. Además, se tiene que

$$\frac{\mathbb{Z}[i]}{\mathfrak{a}} = \{\mathfrak{a}, 1+\mathfrak{a}\}.$$

CONCLUSIONES: Hay personas que no emplean bien el algoritmo de Euclides: recuérdese que si $z/w = A+Bi$ y se toma $q = q_1+iq_2$ como cociente, entonces $|A-q_1|, |B-q_2| \leq 1/2$ (esto tiene que cumplirse). Bastantes en el segundo apartado no ven que estamos ante elementos asociados, y que por tanto nos podemos ahorrar volver a hacer las cuentas (elementos asociados tienen máximo común divisor asociado). Con respecto al último apartado, parece que se tiene miedo a utilizar el **Primer Teorema de Isomorfía** (y cuando se utiliza en muchos de los casos se hace mal), y a escribir $2\mathbb{Z}$ (rara vez aparece esto escrito). En general, conviene repasar este último apartadode nuevo por todos.

[7]Obsérvese que, una vez visto que el cociente es un cuerpo, dado que **el cardinal** de este **es menor o igual que el número de los posibles restos que podemos obtener** al dividir los elementos de $\mathbb{Z}[i]$ entre el generador del denominador; a saber, el cardinal es menor o igual que el del conjunto

$$\left\{z \in \mathbb{Z}[i] : |z|^2 \leq 1\right\} = \{0\} \cup \mathbb{Z}[i]^* = \{0, \pm 1, \pm i\},$$

como todas las unidades coinciden en $\mathfrak{a}$ trivialmente, podemos concluir que tenemos un cuerpo de 2 elementos.

Problema 3. Sea $\varphi : A\backslash\{0\} \to \mathbb{N}$ una aplicación que dota a A con estructura de DE. Demostrar que si $m = \min(\mathrm{Im}(\varphi))$, entonces $A^* = \{z \in A : \varphi(z) = m\}$.

Solución: En primer lugar, nótese que, como $\varphi(A\backslash\{0\}) \subseteq \mathbb{N}$ trivialmente, dado que los naturales están bien ordenados, se tiene que existe $z \in A\backslash\{0\}$ con $\varphi(z) = m$. En otras palabras, el entero m está bien definido. Vamos a comprobar que, por ejemplo, se tiene que $\varphi(1) = m$. En efecto, pues para todo $w \in A\backslash\{0\}$ arbitrario, por las propiedades de los DEs, es

$$\varphi(1) \leq \varphi(w \cdot 1).$$

Luego $\varphi(1) = m = \min(\mathrm{Im}(\varphi))$. Para concluir el resultado, debemos ver que un elemento $w \in A\backslash\{0\}$ es una unidad si, y sólo si, se tiene que $\varphi(w) = \varphi(1)$. Supongamos primero que w es una unidad; a saber, existe $v \in A\backslash\{0\}$ con $vw = 1$. Por las propiedades de los DEs, se tiene que

$$\varphi(w) \leq \varphi(v \cdot w) = \varphi(1) = m = \min(\mathrm{Im}(\varphi)),$$

luego, por la propia elección de m (pues es el mínimo natural dado en la imagen de φ), necesariamente $\varphi(w) = \varphi(1)$. Por otro lado, supongamos que $\varphi(w) = \varphi(1) = m$. Realizando la división, que nos proporciona la estructura de DE dada, siguiendo el correspondiente **Algoritmo de la División**, de 1 entre w nuestro elemento, obtenemos que existen un cociente $q \in A$ y un resto $r \in A$ únicos de tal forma que

$$1 = wq + r,$$

donde, además, se tiene que $r = 0$ o $\varphi(r) < \varphi(w)$. Como $\varphi(w) = \varphi(1) = m = \min(\mathrm{Im}(\varphi))$ por hipótesis, concluimos que forzosamente $r = 0$. A saber, se ha demostrado que $1 = qw$ y, por definición, hemos concluido que w es una unidad.

CONCLUSIONES: En general, bastante bien (alguna persona/grupo de gente sólo prueba una inclusión o se lía en alguna), salvo en algunos casos donde afirman que $1 = \min(\mathrm{Im}(\varphi))$ debido a que φ es multiplicativa. Pero esto último no es cierto, ya que en la definición de DE no se dice en ningún momento que esta aplicación sea multiplicativa. Por ejemplo, en los anillos $\mathbb{K}[x]$ de polinomios, la aplicación grado que dota a este con esta estructura no es multiplicativa y, de hecho, se tiene que $\deg \mathbb{K}^* = 0 \in \mathbb{N}$ (recuérdese que para los algebristas $0 \in \mathbb{N}$).

Problema 4. Sean A un DFU y $\mathbb{K}$ un cuerpo.

(1) Probar que en A todo irreducible es primo[8]. Dado $f \in \mathbb{K}[x_1, \ldots, x_n]$ un polinomio no nulo, deducir que (f) es primo si, y sólo si, el polinomio f es irreducible.

El **objetivo** de este ejercicio es probar que **lo anterior no es cierto**, en general, para **ideales generados por varios polinomios cuando se tienen más de dos indeterminadas**.

(2) Probar que $\left(x^2 + 1, x^2 y\right)$ es primo en $\mathbb{R}[x, y]$ a pesar de que $x^2 y$ no es irreducible.
(3) ¿Es cierta, en general, la otra implicación?[9] Estudiar si los polinomios $x^2 + 1$ e $y^2 + 1$ son irreducibles en $\mathbb{R}[x, y]$. ¿Es el ideal generado por ellos un ideal primo?

Solución:

[8]Obsérvese que esto, junto con lo probado en el apartado (2) del **Problema** 1, nos dice que una condición necesaria y suficiente para tener unicidad en las factorizaciones como producto de irreducibles en los **Dominios de Factorización** es que todo elemento irreducible sea de hecho primo.

[9]Para poder completar la prueba de que lo anterior no es cierto para ideales generados por varios polinomios con dos o más variables, es necesario probar también que existen polinomios irreducibles que generan un ideal no primo, o bien que esta implicación sí que puede darse en general.

(1) Dado A un DFU cualquiera, supongamos que $x \in A$ es un elemento irreducible tal que $x|ab$ en A siendo $a, b \in A$ arbitrarios. Entonces, por definición, existe $c \in A$ tal que $ab = xc$. En consecuencia, debido a la unicidad en A de la factorización en producto de irreducibles, se tiene que x ha de ser un factor irreducible de a ó b (de hecho, sólo de uno). Supongamos sin pérdida de generalidad que x es factor irreducible de a. Tenemos entonces que $a = uxq_1 \cdots q_n$ es la factorización en A como producto de irreducibles para a con $u \in A^*$ y $q_1, \ldots, q_n \in A$ elementos irreducibles para $n \in \mathbb{N}$. Esto es, se tiene que $x|a$ en A por definición, lo cual concluye que x es primo en A. Como bien dabemos, si A es un DFU, entonces $A[x]$ es también un DFU. Por tanto, y dado que $(A[x])[y] \cong A[x, y]$ trivialmente, aplicando inductivamente este argumento $n \in \mathbb{N}$ veces, llegamos a que $A[x_1, \ldots, x_n]$ es un DFU. En particular, tomando $A = \mathbb{K}$ un cuerpo, esto sigue siendo cierto. En consecuencia, dado $f \in \mathbb{K}[x_1, \ldots, x_n]$ un polinomio no nulo arbitrario, se tiene que (f) es ideal primo si, y sólo si, el elemento f es de hecho primo en el anillo dado, que, en virtud de lo que se acaba de demostrar, es equivalente, en nuestro anillo, por ser este DFU (pues que todo primo es irreducible se sabe que es cierto siempre), a que f sea elemento irreducible.

(2) Es obvio que x^2y no es un elemento irreducible, pues puede factorizarse en $\mathbb{R}[x, y]$ como producto de los irreducibles x e y por $x^2y = x \cdot x \cdot y$ con x e y no unidades (pues son indeterminadas). Veamos ahora que el ideal $\left(x^2 + 1, x^2y\right)$ es primo en $\mathbb{R}[x, y]$. Para ello, vamos a definir el homomorfismo de anillos evaluación dado por

$$\begin{array}{rccccc} \varphi\colon & \mathbb{R}[x,y] & \longrightarrow & \frac{\mathbb{C}[y]}{(y)} & \cong & \mathbb{C} \\ & 1 & \mapsto & 1 & \mapsto & 1 \\ & x & \mapsto & i & \mapsto & i \\ & y & \mapsto & y & \mapsto & 0 \end{array}.$$

Este es un homomorfismo de anillos (unitario) claramente sobreyectivo, pues todo $a + bi \in \mathbb{C}$ tiene una preimagen por φ evidente en $\mathbb{R}[x, y]$. Por ejemplo, basta tomar $g(x, y) = a + bx \in \mathbb{R}[x, y]$. De hecho, se demuestra que $\ker \varphi = \left(x^2 + 1, x^2y\right)$. En efecto, por doble inclusión, se tiene que $\supseteq$ es trivial por definición de núcleo, mientras que la otra se sigue de tomar un polinomio $f \in \mathbb{R}[x, y]$ arbitrario, y dividir este entre x^2+1 y x^2y. En efecto, podemos hacer esto porque ambos polinomios son mónicos en la indeterminada correspondiente. Así, dividiendo primero entre $x^2 + 1$ por ejemplo, se tiene que $f(x, y) = q(x, y)\left(x^2 + 1\right) + r(x, y)$, donde el grado de $r(x, y)$ en x es menor que 2. Ahora, dividiendo $r(x, y)$ entre x^2y en $\mathbb{R}[x, y]$ obtenemos que

$$f(x,y) = q(x,y)\left(x^2+1\right) + r(x,y) = q(x,y)\left(x^2+1\right) + q'(x,y)\left(x^2y\right) + r'(x,y),$$

donde el grado de $r'(x, y)$ en x es menor que 2 y el grado en y es menor que 1. A saber, existen $a, b \in \mathbb{R}$ tales que $r(x, y) = a + bx$. Aplicando ahora φ a la igualdad obtenida, como f es un elemento del núcleo, tenemos que

$$0 = \varphi(f) = \varphi(r'(x,y)) = r'(i,y) = a + bx \iff a = b = 0,$$

donde la última equivalencia es cierta porque igualamos por coeficientes. A saber, se ha probado que $r'(x, y) = 0$ y, por tanto, se ha demostrado que $f \in \left(x^2 + 1, x^2y\right)$. Por el **Primer Teorema de Isomorfía** para el homomorfismo φ construido, es

$$\frac{\mathbb{R}[x,y]}{(x^2+1, x^2y)} \cong \frac{\mathbb{C}[y]}{(y)} \cong \mathbb{C}.$$

Ahora bien, es obvio que $\mathbb{C}$ es un cuerpo, luego, por el isomorfismo probado, se tiene que $\left(x^2 + 1, x^2y\right)$ es un ideal maximal en $\mathbb{R}[x, y]$ que, en particular, es primo como se quería demostrar. Esto prueba que, en general, más de dos polinomios que generen un ideal primo no tienen porqué ser irreducibles.

(3) Es obvio que los polinomios x^2+1 y y^2+1 son irreducibles, pues son mónicos de grado 2 sin raíces en los anillos $\mathbb{R}[y]$ y $\mathbb{R}[x]$ que tocan, respectivamente. Veamos, sin embargo, que el ideal generado por ellos no es en ningún caso primo en $\mathbb{R}[x,y]$. Para ello, vamos a definir el homomorfismo de anillos evaluación dado por

$$\begin{array}{rccc} \varphi\colon & \mathbb{R}[x,y] & \longrightarrow & \frac{\mathbb{C}[y]}{(y^2+1)} \\ & 1 & \mapsto & 1 \\ & x & \mapsto & i \\ & y & \mapsto & y \end{array}.$$

Este es un homomorfismo de anillos (unitario) claramente sobreyectivo, pues todo $f(y)=(a+bi)+(c+di)y+\left(y^2+1\right)\in\mathbb{C}[x]/\left(y^2+1\right)$ tiene una preimagen por φ evidente en $\mathbb{R}[x,y]$. Por ejemplo, basta tomar $g(x,y)=(a+bx)+(c+dx)y\in\mathbb{R}[x,y]$. De hecho, se demuestra que $\ker\varphi=\left(x^2+1,y^2+1\right)$. En efecto, por doble inclusión, se tiene que $\supseteq$ es trivial por definición de núcleo, mientras que la otra se sigue de tomar un polinomio $f\in\mathbb{R}[x,y]$ arbitrario, y dividir este entre x^2+1 e y^2+1. En efecto, podemos hacer esto porque ambos polinomios son mónicos en la indeterminada correspondiente. Así, dividiendo primero entre x^2+1 por ejemplo, se tiene que $f(x,y)=q(x,y)\left(x^2+1\right)+r(x,y)$, donde el grado de $r(x,y)$ en la indeterminada x es menor que 2. Ahora, dividiendo $r(x,y)$ entre y^2+1 en $\mathbb{R}[x,y]$ obtenemos que

$$f(x,y)=q(x,y)\left(x^2+1\right)+r(x,y)=q(x,y)\left(x^2+1\right)+q'(x,y)\left(y^2+1\right)+r'(x,y),$$

donde el grado de $r'(x,y)$ en las dos indeterminadas x e y es menor que 2. A saber, existen $a,b,c,d\in\mathbb{R}$ tales que $r(x,y)=(a+bx)+(c+dx)y$. Aplicando ahora φ a la igualdad obtenida, como f es un elemento del núcleo, tenemos que

$$\begin{aligned} 0=\varphi(f)=\varphi(r'(x,y))=r'(i,y)=(a+bi)+(c+di)y \iff \\ \iff a+bi=c+di=0 \iff a=b=c=d=0, \end{aligned}$$

donde las últimas equivalencias son ciertas porque igualamos por coeficientes reales en $\mathbb{C}$. A saber, se ha probado que $r'(x,y)=0$ y, por tanto, se ha demostrado que $f\in\left(x^2+1,y^2+1\right)$. Por el **Primer Teorema de Isomorfía** para el homomorfismo φ construido, es

$$\frac{\mathbb{R}[x,y]}{(x^2+1,y^2+1)}\cong\frac{\mathbb{C}[x]}{(x^2+1)}.$$

Ahora bien, es obvio que $\mathbb{C}[x]$ es un DE (**Ejercicio** 5 **de la Hoja** 3). Luego, dado que x^2+1 es trivialemente reducible en $\mathbb{C}[x]$ por tener (al menos) un raíz compleja, el ideal $\left(x^2+1\right)$ no es primo, y el cociente correspondiente no es DI. Así, por el isomorfismo probado, se tiene que $\left(x^2+1,y^2+1\right)$ no puede ser ideal primo en $\mathbb{R}[x,y]$ tal y como se nos pedía demostrar. Esto prueba que, en general, más de dos polinomios irreducibles pueden generar un ideal no primo.

CONCLUSIONES: Los dos primeros apartados bastante bien en general (salvo típicos líos), pero en el último hay de todo[10] (quien lo deja en blanco, quien da muchas vueltas para dar la resolución, etc). En particular, destacar un grupo de personas porque dicen que $(x^2+1,x^2y)=(\mathrm{mcd}(x^2+1,x^2y))=\mathbb{R}[x,y]$. Esto no es cierto en los DFU que no son DIP en general, dado que nada nos asegura que (x^2+1,x^2y) sea ideal principal. OJO con este tipo de errores. Por último, es necesario justificar todos los isomorfismos que se emplean a lo largo de la resolución, y por muy trivial que sea algo, hay que justificarlo un mínimo.

[10]Obsérvese que se ha incluido un nuevo apartado, porque sino no queda del todo cerrada la pregunta que se está intentando responder, pero la resolución es igual a la otra salvo por los datos.