Capítulo 1

Teoría de anillos

1.1. Definición de anillo

Un anillo intuitivamente no es más que un conjunto en el que podemos sumar, restar y multiplicar con las propiedades habituales excepto que la multiplicación no tiene por qué ser conmutativa, aunque esta salvedad no se considerará en este curso.

Definición: Un *anillo*, A, es un conjunto dotado con dos operaciones cerradas, $\oplus$ y $\otimes$ (suma y multiplicación), de modo que se verifican las siguientes propiedades:

i) A es un grupo abeliano con respecto a $\oplus$.

ii) $\otimes$ es una operación asociativa en A.

iii) Se cumplen las leyes distributivas $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ y $c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$.

Si además $\otimes$ es una operación conmutativa se dice que A es un *anillo conmutativo*, y si $\otimes$ tiene elemento neutro, se dice que A es un *anillo con unidad*.

Observación: Que las operaciones sean *cerradas* simplemente quiere decir que al efectuarlas siempre el resultado estará en A. Con la notación habitual, que seguiremos en lo posible aquí, se escribe 0 para indicar el elemento neutro de $\oplus$ y 1 para indicar el de $\otimes$. Además se suelen utilizar las notaciones de la suma y producto habituales: $+$ y $\cdot$ (muchas veces omitida). Se dice que 1 es la *unidad* del anillo, y en general con la terminología al uso se llama *unidades* (o *elementos invertibles*) a todos los los elementos con inverso respecto de $\otimes$.

Como se ve, incluso para leer la primera definición es necesario saber qué es un grupo. Y, en general, es un requisito indispensable para este curso cierto conocimiento de la teoría de grupos. Como una concesión de primera página, recordaremos al menos la definición.

Definición: Un *grupo*, G, es un conjunto dotado con una operación cerrada, $*$, tal que se verifican las siguientes propiedades:

i) $*$ es asociativa: $g * (h * f) = (g * h) * f$.

ii) Existe el elemento neutro: $\exists e \in G \ : \ e * g = g * e = g \ \forall g \in G$.

iii) Existe el elemento inverso: $\forall g \in G \ \exists h \in G \ : \ h * g = g * h = e$.

Ya hemos insinuado que en este curso sólo aparecerán anillos conmutativos. Ésta es una excusa como cualquier otra para introducir una nueva definición que especifica más el concepto de anillo.

Definición: Se dice que un anillo conmutativo con unidad es un *dominio de integridad* si $a \cdot b = 0 \Rightarrow a = 0$ ó $b = 0$ para cualquier par de elementos a, b.

Observación: Cuando un anillo no es un dominio de integridad, a los elementos no nulos a y b con $a \cdot b = 0$, se les llama *divisores de cero*. Éstos constituyen el obstáculo para poder simplificar en una igualdad (propiedad de cancelación). Concretamente, sólo podemos deducir $x = y$ a partir de $ax = ay$ si a no es un divisor de cero.

Siempre que se estudian estructuras algebraicas abstractas surge en nuestra mente el lejano soniquete de nuestra infancia: "¿y por qué?", "¿y para qué?". Una posible primera respuesta es la economía de medios. Por ejemplo, la teoría de grupos da un marco general que permite hallar los grupos cristalográficos, resolver el cubo de Rubik, dar una demostración rápida del pequeño teorema de Fermat, clasificar partículas en física cuántica o adivinar la última carta de nuestro adversario jugando a la escoba. El concepto de grupo abstrae cierta noción genérica de simetría que podemos aplicar en diferentes problemas. Aunque la unificación de la esencia de varios ejemplos importantes es históricamente responsable de la creación de la mayoría de las estructuras algebraicas, no se agotan ahí las razones para su estudio. La mayoría de los matemáticos situarían a la estética como guía directora. A pesar de que no tenga una "utilidad" clara disponer de una lista de todos los grupos simples, es algo natural, como en otro ámbito lo es colocar los libros en una estantería.

Después de esta inyección de fe ciega, veamos unos cuantos ejemplos.

Ejemplo. $\mathbb{Z}$ es un anillo conmutativo con unidad, de hecho un dominio de integridad.

Ejemplo. $\{a + b\sqrt{2} \ : \ a, b \in \mathbb{Z}\}$ es un dominio de integridad.

Ejemplo. Los enteros pares (divisibles por dos, negativos incluidos) conforman un anillo conmutativo pero no un anillo con unidad.

Ejemplo. $\{z \in \mathbb{C} \ : \ \frac{1}{2}\Re z, \frac{1}{2}\Im z \in \mathbb{Z}\}$ es un anillo conmutativo pero no un anillo con unidad. (Aquí y en lo sucesivo los símbolos $\Im$ y $\Re$ se emplearán para indicar las partes imaginaria y real, respectivamente).

Ejemplo. $\mathbb{Z}_6$, esto es, las clases de restos módulo 6 es un anillo conmutativo con unidad pero no un dominio de integridad porque $\overline{2} \cdot \overline{3} = \overline{0}$.

Ejemplo. Los matrices reales 2×2 forman un anillo, pero no un anillo conmutativo.

En estos ejemplos lo más que hay que comprobar es que las operaciones son cerradas, ya que las tres propiedades de la definición de anillo vienen heredadas por las correspondientes en $\mathbb{C}$, que se dan por supuestas.

Los ejemplo más importantes de anillo en este curso son los anillos de polinomios.

Dado un anillo conmutativo A, se denota con $A[x]$ al *anillo de polinomios sobre* A con la indeterminada x. Es decir al conjunto de expresiones formales del tipo $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ con $a_j \in A$ y las operaciones suma y producto habituales. Abreviaremos la notación $\big(A[x_1]\big)[x_2]$, $\big(\big(A[x_1]\big)[x_2]\big)[x_3]$, etc. escribiendo simplemente $A[x_1, x_2]$, $A[x_1, x_2, x_3]$, etc. Obsérvese que estos anillos corresponden a los polinomios de varias variables.

Ciertamente se podría dar una definición más rigurosa de polinomio (véase [Cl] p. 203) pero el concepto es tan bien conocido de cursos pasados que sólo lograría darnos dolor de cabeza.

Puestos en faena, veamos la definición de grado y una proposición tonta para romper el hielo.

Definición: Si $P \in A[x]$ es de la forma $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ con $a_n \neq 0$ diremos que P tiene *grado* n y escribiremos $\partial P = n$ o también $\operatorname{gr} P = n$. Si $P = 0$ escribiremos formalmente $\partial P = -\infty$ o $\operatorname{gr} P = -\infty$.

Proposición 1.1.1 *Sea A un dominio de integridad. Entonces $A[x]$ también lo es y además para $P, Q \in A[x]$ se cumple:*

1) $\partial(P+Q) \leq \operatorname{máx}(\partial P, \partial Q)$ 2) $\partial(PQ) = \partial P + \partial Q$.

Demostración: Las propiedades 1) y 2) se siguen fácilmente de la definición de grado. Por otra parte si $A[x]$ no fuera un dominio de integridad, entonces existirían P y $Q \in A[x] - \{0\}$ tales que $PQ = 0$ y esto contradice 2). □

Recuérdese que se dice que un polinomio de grado $n \geq 1$, $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$, es *mónico* si $a_n = 1$. Esta definición tiene sentido para cualquier anillo con unidad.

Los polinomios mónicos más sencillos son de la forma $x+\alpha$. Si multiplicamos n de ellos obtendremos un polinomio de grado n:

$$(x+\alpha_1)(x+\alpha_2)\ldots(x+\alpha_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

y se tiene la fórmula $a_{n-k} = \sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ donde σ_k es un polinomio en $\alpha_1, \alpha_2, \ldots, \alpha_n$ igual a la suma de todos los posibles productos de k de estas variables. Por ejemplo

$$\sigma_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_n, \quad \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n, \quad \ldots \quad \sigma_n = \alpha_1\alpha_2\ldots\alpha_n$$

Notación: A $\sigma_k(x_1, x_2, \ldots, x_n)$ se le suele llamar *polinomio simétrico elemental* de grado k y n variables.

En general se dice que un polinomio en varias variables es *simétrico* si queda invariante bajo cualquier permutación de sus variables.

El siguiente resultado justifica por qué a los σ_k se les llama elementales

Teorema 1.1.2 *Cualquier polinomio simétrico sobre un dominio de integridad se puede expresar como un polinomio sobre dicho dominio cuyas variables son los polinomios simétricos elementales.*

Nota: Aunque no lo haremos aquí, es posible probar la unicidad de esta expresión.

Demostración: Sea $P \in A[x_1, x_2, \ldots, x_n]$ simétrico. Apliquemos el siguiente algoritmo:
1) Seleccionar el monomio $kx_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ (algunos α_i pueden ser nulos) que tiene mayor grado en x_1, si todavía hubiera varios escójase entre ellos el de mayor grado en x_2 y si hubiera varios el de mayor grado en x_3, etc. Por la simetría de P se tiene $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$.
2) Sea $Q = P - k\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_n^{\alpha_n}$. Entonces $P = k\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_n^{\alpha_n} + Q$ y ahora se repite todo el proceso con Q hasta llegar a $Q = 0$.
Obsérvese que el monomio selecionado en 1) no aparece en Q y que el algoritmo siempre termina porque al aplicarlo sucesivas veces o bien el grado en x_1 se ha reducido o ha quedado igual, y en este último caso el grado en x_2 se habrá reducido o habrá quedado igual, etc. □

El teorema anterior tiene gran importancia histórica en el desarrollo de la teoría de Galois y la teoría de grupos en general. Para ilustrar su interés demostraremos el siguiente resultado

Corolario 1.1.3 *Sean $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$. Si $P = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ pertenece a $\mathbb{Q}[x]$, entonces para cualquier $Q \in \mathbb{Q}[x]$ el polinomio $P_Q = (x-Q(\alpha_1))(x-Q(\alpha_2))\ldots(x-Q(\alpha_n))$ también pertenece a $\mathbb{Q}[x]$.*

Demostración: Los coeficientes de P_Q son $a_{n-k} = (-1)^k\sigma_k\big(Q(\alpha_1), Q(\alpha_2), \ldots, Q(\alpha_n)\big)$. Considerando los α_i como variables, a_{n-k} define un polinomio simétrico de $\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_n]$, que por el teorema anterior se puede escribir como un polinomio con coeficientes racionales evaluado en $\sigma_1(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\sigma_2(\alpha_1, \alpha_2, \ldots, \alpha_n)$,... etc, y estas últimas cantidades son racionales porque coinciden, salvo un signo, con los coeficientes de P. □

Por ejemplo, de este resultado se deduce que como $\sqrt[3]{2}$ es raíz de $P = x^3 - 2$, entonces para cada $a, b, c \in \mathbb{Z}$, $a\sqrt[3]{2^2} + b\sqrt[3]{2} + c$ también es raíz de un polinomio de grado 3 en $\mathbb{Z}[x]$. Una demostración directa (hallando el polinomio), sería muy farragosa.

Una vez que tenemos anillos podemos considerar aplicaciones entre ellos que respeten las operaciones. La notación rococó es la misma que en teoría de grupos, y ya debería ser conocida.

Definición: Sean A y B anillos con unidad. Un *homomorfismo* de anillos es una función $\phi : A \longrightarrow B$ que respeta la suma, la multiplicación y el elemento unidad, esto es,

$$i)\ \phi(a_1 + a_2) = \phi(a_1) + \phi(a_2) \quad ii)\ \phi(a_1a_2) = \phi(a_1)\phi(a_2) \quad iii)\ \phi(1_A) = 1_B.$$

Nota: Para anillos sin unidad, y a veces en general, la condición *iii*) se suprime.

Definición: i) Si ϕ es inyectiva se dice que es un *monomorfismo.*
ii) Si ϕ es sobreyectiva se dice que es un *epimorfismo.*
iii) Si ϕ es biyectiva se dice que es un *isomorfismo.*
iv) Si ϕ es biyectiva y $A = B$ se dice que es un *automorfismo.*

Si $f : A \longrightarrow B$ es un homomorfismo de anillos, su núcleo y su imagen se definen como en teoría de grupos o álgebra lineal:

$$\text{Ker } f = \{a \in A \ :\ f(a) = 0\}, \qquad \text{Im } f = \{b \in B \ :\ f^{-1}(b) \neq \emptyset\},$$

y es muy fácil comprobar que ambos son anillos (con las operaciones heredadas de A y B respectivamente).

Ejemplo. $f : \mathbb{Z} \longrightarrow \mathbb{C}$, con f la inclusión, es un monomorfismo.

Ejemplo. Sea M el subconjunto de $\mathcal{M}_{2\times 2}(\mathbb{R})$ (el anillo de matrices reales 2×2) definido como $M = \{(a_{ij})_{i,j=1}^2 \ : \ a_{11} = a_{22},\ a_{12} = -a_{21}\}$. Entonces la aplicación $f : \mathbb{C} \longrightarrow M$ dada por

$$f(z) = \begin{pmatrix} \Re z & \Im z \\ -\Im z & \Re z \end{pmatrix}$$

es un isomorfismo.

La biyectividad es obvia, y las propiedades de homomorfismo sencillas de comprobar. Nótese que está garantizado que M es un anillo por ser la imagen de la aplicación f extendida a $\mathbb{C} \longrightarrow \mathcal{M}_{2\times 2}(\mathbb{R})$.

Ejemplo. $f : \mathbb{Z} \longrightarrow \mathbb{Z}_6$ con $f(x) = \overline{x}$, la clase de x módulo 6, es un epimorfismo.

Ejemplo. La conjugación $\mathbb{C} \longrightarrow \mathbb{C}$ es un automorfismo.

Ejemplo. Si $A \subset B$ con A y B anillos conmutativos con unidad. Para cada $b \in B$ la función $f_b : A[x] \longrightarrow B$ dada por $f_b(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = a_n b^n + a_{n-1}b^{n-1} + \cdots + a_0$ es un homomorfismo.

A la imagen de este homomorfismo de evaluación se le denota escribiendo $A[b]$. (Nótese el leve abuso de notación debido a que $A[b]$ no es un anillo de polinomios). Y copiando la notación del análisis se escribe $P(b)$ en lugar de $f_b(P)$. Este tipo de anillos con $A = \mathbb{Z}$ o $\mathbb{Q}$ y b ciertos números complejos, tienen gran importancia en problemas aritméticos e históricamente están en el origen del propio concepto de anillo.

Ejemplo. $\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\}$.

Ejemplo. $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Q}\}$.

Es cierto que todos los ejemplos de anillos y aplicaciones entre ellos incluidos en esta sección, se reducen a una comprobación directa de la definición. Son todos demasiado sencillos. En unos momentos complicaremos las cosas introduciendo anillos cociente. Mientras tanto, el que quiera quejarse por el tiempo perdido, que se dirija a R. Descartes que consideró como una de sus *reglas para la dirección de la mente*: "Hay que dirigir toda la penetración de nuestro espíritu o mente a lo que es menos importante y más fácil. Y es conveniente que nos detengamos en ello durante bastante tiempo, hasta que hayamos adquirido el hábito de ver la verdad por intuición de una manera distinta y clara".

1.2. Ideales y cocientes

Un ideal es un subanillo que es absorbente con respecto al producto. Esto puede que sea verdad, pero como no hay quien lo entienda, demos una definición menos sintética y más comprensible.

Definición: Sea A un anillo. Se dice que $I \subset A$ es un ideal si:

$$i) \quad (I,+) \text{ es un subgrupo}, \qquad ii) \quad a \in A,\ b \in I \ \Rightarrow\ ab, ba \in I.$$

Nótese que estas propiedades aseguran que $+$ y $\cdot$ son cerradas en I, y por tanto I hereda la estructura de anillo de A. Además $ii)$ indica que I es invariante por multiplicaciones. Éste es el significado de la definición sintética.

Notación: Dados $a_1, a_2, \ldots, a_n \in A$, se suele denotar mediante $\langle a_1, a_2, \ldots, a_n \rangle$ o $(a_1, a_2, \ldots, a_n)$ (preferimos la segunda notación por razones tipográficas) al menor ideal, en el sentido de la inclusión, que contiene a $\{a_1, a_2, \ldots, a_n\}$. Se dice que los a_j son *generadores* del ideal. Es fácil ver que la intersección de ideales es un ideal, lo que asegura la existencia del susodicho "menor ideal", basta hacer la intersección de todos los que contienen a $\{a_1, a_2, \ldots, a_n\}$. Si A es un anillo conmutativo con unidad, es un sencillo ejercicio comprobar que

$$\langle a_1, a_2, \ldots, a_n \rangle = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \ :\ \lambda_j \in A\}.$$

Ejemplo. $I = \{\text{números pares}\}$ es un ideal de $\mathbb{Z}$.

Ejemplo. $I = \langle d \rangle = \{\text{múltiplos de } d\}$ es un ideal de $\mathbb{Z}$.

Ejemplo. En $\mathbb{R}[x, y]$, el ideal $\langle x, y \rangle$ es el formado por los polinomios de dos variables cuyo término independiente se anula.

Ejemplo. Los ideales de $\mathbb{Z}_4$ son $I_1 = \{\overline{0}\}$, $I_2 = \{\overline{0}, \overline{2}\}$, $I_3 = \mathbb{Z}_4$.

Ejemplo. En $\mathbb{Z}$, $\langle 2, 5 \rangle = \langle 1 \rangle = \mathbb{Z}$, ya que $3 \cdot 2 + (-1) \cdot 5 = 1$.

Distinguiremos dos tipos de ideales que aparecerán en la próxima sección.

Definición: Se dice que un ideal $I \subset A$ es *principal* si puede generarse con un único elemento. Esto es, si $I = \langle a \rangle$ para cierto $a \in A$.

Definición: Se dice que un ideal $I \subset A$ es *maximal* si es propio ($I \neq \{0\}, A$) y no existe otro ideal J tal que $I \subsetneqq J \subsetneqq A$.

Ejemplo. El ideal $I = \langle 6, 10 \rangle \subset \mathbb{Z}$ es principal, ya que no es difícil probar que $I = \langle 2 \rangle$.

Ejemplo. El ideal del ejemplo anterior es maximal porque si intentamos "añadir" un número impar, $2n + 1$, a I entonces también debería estar $(2n + 1) + (-n) \cdot 2 = 1$ y por tanto todo $\mathbb{Z}$.

Ejemplo. El ideal $I = \langle 9 \rangle \subset \mathbb{Z}$ no es maximal porque $\langle 9 \rangle \subsetneqq \langle 3 \rangle \subsetneqq \mathbb{Z}$

Ejemplo. Por la regla de Ruffini, en $\mathbb{R}[x]$ el ideal $I = \{P \in \mathbb{R}[x] \ :\ P(-1) = 0\}$ es $I = \langle x + 1 \rangle$ y por tanto principal.

Ejemplo. En $\mathbb{R}[x,y]$ el ideal $I=\langle x,y\rangle$ no es principal, ya que $I=\langle P\rangle$ implicaría $P|x$ y $P|y$. Por otra parte, I sí es maximal porque $I\subsetneq J$ sólo es posible si existe $Q\in J$ con término independiente $a_0\neq 0$, y $a_0-Q\in I$ implica $a_0\in J$, y por tanto $1=a_0^{-1}a_0\in J$.

En $\mathbb{Z}$, en realidad los ideales "tienen truco". Como veremos, y no es difícil adivinar, todos los ideales de $\mathbb{Z}$ son principales y los maximales son (p) con p primo. Además se cumple el siguiente resultado que permite simplificar generadores.

Proposición 1.2.1 *En $\mathbb{Z}$, si a y b no son simultáneamente nulos se cumple la igualdad entre ideales*

$$\langle a,b\rangle=\langle \mathrm{mcd}(a,b)\rangle$$

donde $\mathrm{mcd}(a,b)$ *es el máximo común divisor de a y b.*

Demostración: Sean $I=\langle a,b\rangle$ y $J=\langle \mathrm{mcd}(a,b)\rangle$. Evidentemente $I\subset J$ (porque $a,b\in J$). Por otra parte, por la identidad de Bezout existen λ_1,λ_2 tales que $\mathrm{mcd}(a,b)=\lambda_1 a+\lambda_2 b\in I$, y se sigue que $J\subset I$. □

Vayamos ahora a unos cuantos ejemplos más difíciles.

Ejemplo. El ideal $I=\langle 2,1+\sqrt{-5}\rangle$ es maximal en $A=\mathbb{Z}[\sqrt{-5}]$.

Sea $\alpha=a+b\sqrt{-5}\notin I$. Necesariamente $a-b$ es impar porque en otro caso $\alpha=2(a-b)/2+b(1+\sqrt{-5})\in I$. Pero si $a-b$ es impar, $1=2(a-b+1)/2+b(1+\sqrt{-5})+(-1)\alpha$. Por tanto $\langle 2,1+\sqrt{-5},\alpha\rangle=\langle 1\rangle=A$. Es decir, el ideal I no se puede ampliar con ningún elemento.

Ejemplo. El ideal $I=\langle 2,1+\sqrt{-5}\rangle$ no es principal en $A=\mathbb{Z}[\sqrt{-5}]$.

Si $I=\langle\alpha\rangle$ con $\alpha=a+b\sqrt{-5}$, entonces $2=\alpha\beta$ y $1+\sqrt{-5}=\alpha\gamma$ para ciertos $\beta,\gamma\in A$. Multiplicando estas igualdades por sus conjugadas se tiene que a^2+5b^2 debe dividir a 4 y a 6. Esto sólo deja las posibilidades $a=\pm 2,\ b=0$ y $a=\pm 1,\ b=0$. El primer caso es imposible porque $1+\sqrt{-5}$ no es un múltiplo de 2. El segundo caso sólo se daría si $I=A$, y esto no es cierto porque no es difícil ver que si $x+y\sqrt{-5}\in A$ es múltiplo de 2 o de $1+\sqrt{-5}$ entonces x e y tienen la misma paridad.

Ejemplo. El ideal $I=\langle 11+7\sqrt{2},8+11\sqrt{2}\rangle$ es principal en $A=\mathbb{Z}[\sqrt{2}]$.

Tratamos de pasar a números enteros multiplicando por el conjugado, concretamente $23=(11+7\sqrt{2})(11-7\sqrt{2})$ y $-178=(8+11\sqrt{2})(8-11\sqrt{2})$ están en I. Utilizando el algoritmo de Euclides se obtiene $1=31\cdot 23+4\cdot(-178)$. Por tanto,

$$1=\big[31(11-7\sqrt{2})\big](11+7\sqrt{2})+\big[4(8-11\sqrt{2})\big](8+11\sqrt{2}),$$

y el ideal no sólo es principal sino que $I=\langle 1\rangle=A$.

Ejemplo. Estudiar si el ideal $I=\langle 1+4\sqrt{-2},-9+6\sqrt{-2}\rangle$ es principal en $A=\mathbb{Z}[\sqrt{-2}]$.

Como antes, $33=(1+4\sqrt{-2})(1-4\sqrt{-2})\in I$ y $153=(-9+6\sqrt{-2})(-9-6\sqrt{-2})\in I$. El máximo común divisor en $\mathbb{Z}$ de estos números es 3, de forma que si $I=\langle\alpha\rangle$ con $\alpha=a+b\sqrt{-2}$, entonces $3=(a+b\sqrt{-2})\beta$ con $\beta\in A$. Al multiplicar por el conjugado

las posibilidades son $\alpha = \pm 1, \pm 1 \pm \sqrt{-2}, \pm 1 \pm 2\sqrt{-2}$. De estos valores, $1+\sqrt{-2}$ divide a los generadores de I, concretamente $I = \langle (1+\sqrt{-2})(3+\sqrt{-2}), (1+\sqrt{-2})(1+5\sqrt{-2})\rangle$. Ahora con $3+\sqrt{-2}$ y $1+5\sqrt{-2}$ podemos dar lugar a enteros coprimos. Por ejemplo, $5(3+\sqrt{-2}) - (1+5\sqrt{-2}) = 14$ y $\sqrt{-2}(3+\sqrt{-2}) - 3(3+\sqrt{-2}) = -11$. Como $14x + (-11)y = 1$ tiene solución, existen $\gamma, \delta \in A$ tales que $(3+\sqrt{-2})\gamma + (1+5\sqrt{-2})\delta = 1$ y se concluye $I = \langle 1+\sqrt{-2}\rangle$.

Seguramente muchos de los lectores ya habrán perdido la paciencia. Como sucede a menudo en matemáticas, y en particular en álgebra abstracta, las definiciones parecen gratuitas, desmotivadas, y la teoría aislada e inasequible. Podemos tener fe en que hay muchos anillos interesantes y que conviene estudiarlos en general, pero ¿y los ideales? ¿cómo a alguien en su sano juicio se le pudo ocurrir introducirlos? ¿para qué los ideales principales y maximales? Si estos conceptos son triviales en $\mathbb{Z}$, ¿en qué anillos resultó interesante crear esta parte de la teoría? Puede que el lector se sienta engañado al saber que respetando el orden histórico las secciones de este capítulo debieran estar escritas en orden inverso: los problemas de factorización llevaron al concepto de ideal y después se desarrolló la teoría de anillos. Sin embargo desde el punto de vista actual y con la preponderancia de lo deductivo frente a lo inductivo en las matemáticas modernas, es más natural no comenzar la casa por el tejado. De todas maneras, al margen de las buenas palabras, disculpas y excusas, ¿es posible explicar las razones que llevaron a la teoría de ideales? Lo que sigue es un intento un poco burdo desde el punto de vista histórico (para una descripción fiel véase [Ri] y [Sm]) pero que puede arrojar alguna luz.

Los ideales los introdujo E. Kummer tratando de probar el último teorema de Fermat y se revelarían como un instrumento muy adecuado permitiendo demostrarlo para muchos exponentes especiales. La ecuación de Fermat $x^n + y^n = z^n$ se puede factorizar como

$$(x-\zeta y)(x-\zeta^2 y)\cdots(x-\zeta^n y) = z \cdot z^{\overset{n \text{ veces}}{\cdots\cdots}} z \tag{1.1}$$

con $\zeta = e^{\pi i/n}$. Esto conduce a estudiar cuándo dos productos coinciden en el anillo $\mathbb{Z}[\zeta]$. En $\mathbb{Z}$ es evidente que si tenemos unos cuantos números que son coprimos dos a dos con otros, el producto de los primeros no puede coincidir con el de los segundos. Esto es, productos iguales implica divisores comunes de los factores. Sin embargo en otros anillos no ocurre así. Por ejemplo, en $\mathbb{Z}[\sqrt{-5}]$ se cumple

$$3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$$

y sin embargo 3 y $1 \pm 2\sqrt{-5}$ no tienen divisores comunes no triviales en $\mathbb{Z}[\sqrt{-5}]$, ni 7 y $1 \pm 2\sqrt{-5}$. Si no ocurrieran casos patológicos como éste en $\mathbb{Z}[\zeta]$, Kummer disponía de técnicas para probar que (1.1) es imposible con n =primo y $x, y \in \mathbb{Z}^+$ coprimos, de donde se deduciría el último teorema de Fermat. Desafortunadamente estos casos patológicos son habituales en $\mathbb{Z}[\zeta]$, pero la buena noticia es que la teoría de ideales permite tratarlos creando un sustituto de los divisores comunes ausentes. Por ejemplo, partiendo de $3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$, nos gustaría que existiesen los divisores comunes antes indicados, digamos $\alpha_\pm = \mathrm{mcd}(3, 1 \pm 2\sqrt{-5})$, $\beta_\pm = \mathrm{mcd}(7, 1 \pm 2\sqrt{-5})$, de forma que

$$3 = \alpha_+ \cdot \alpha_-, \qquad 7 = \beta_+ \cdot \beta_-, \qquad 1+2\sqrt{-5} = \alpha_+ \cdot \beta_+, \qquad 1-2\sqrt{-5} = \alpha_- \cdot \beta_-. \tag{1.2}$$

Como hemos mencionado, tales $\alpha_\pm, \beta_\pm$ no existen. Pero según la Proposición 1.2.1, al menos en $\mathbb{Z}$, un ideal con dos generadores es un sustituto para el máximo común divisor. Y así resulta que (1.2) pasa a ser cierto reemplazando 3, 7 y $1 \pm 2\sqrt{-5}$ por los ideales que generan, $\alpha_\pm$ por $\langle 3, 1 \pm 2\sqrt{-5}\rangle$ y $\beta_\pm$ por $\langle 7, 1 \pm 2\sqrt{-5}\rangle$ (el producto de ideales se define como el menor ideal que contiene a los productos de sus elementos).

Las cantidades $\alpha_\pm$, $\beta_\pm$ son literalmente "ideales" en (1.2), no existen, y en general sólo corresponderían a cantidades "reales" cuando los ideales fueran principales (esta cantidad real sería el generador). Además, la maximalidad de los ideales indicaría que es imposible seguir descomponiendo en más factores. El obstáculo para probar el último teorema de Fermat con este método, por lo que Kummer sólo tuvo éxito parcial, es que es difícil saber en general si los ideales que aparecen en ciertas factorizaciones son principales, y por tanto si posibles soluciones "ideales" de la ecuación de Fermat son "irreales".

Un ideal I en un anillo A permite establecer una relación de equivalencia dada por

$$a \sim b \;\Leftrightarrow\; a - b \in I.$$

Cuando hay una relación de equivalencia, hay un conjunto cociente A/I (el conjunto de las clases de equivalencia) y es fácil ver, si uno entiende los conceptos básicos, que hereda la estructura de anillo.

Proposición 1.2.2 *Si $I \subset A$ es un ideal, entonces A/I es un anillo con las operaciones heredadas de A (es decir, se definen $\overline{a} + \overline{b} := \overline{a+b}$ y $\overline{a} \cdot \overline{b} := \overline{ab}$).*

Demostración: Las propiedades de las operaciones se siguen de las de A. Sólo hay que comprobar que están bien definidas, no dependiendo del representante elegido. Esto es, si $\overline{a_1} = \overline{b_1}$ y $\overline{a_2} = \overline{b_2}$ donde $\overline{a_j}$ y $\overline{b_j}$ son las clases de equivalencia de a_j y b_j, hay que probar $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ y $\overline{a_1 a_2} = \overline{b_1 b_2}$. Para el producto:

$$x - a_1 a_2 \in I \Leftrightarrow x - a_1 a_2 + a_1(a_2 - b_2) + (a_1 - b_1)b_2 \in I \Leftrightarrow x - b_1 b_2 \in I.$$

Donde se ha usado que $a_2 - b_2, a_1 - b_1 \in I$. Para la suma es aún más sencillo. □

Si pidiéramos a I sólo que fuera un subanillo pero no un ideal, entonces A/I no heredaría la estructura de anillo. Por ejemplo, en $\mathbb{Z} \times \mathbb{Z}$, $I = \{(a, b) \;:\; 2|a - b\}$ es un subanillo pero la operación producto no pasa bien al cociente, por ejemplo $\overline{(0,1)} = \overline{(1,0)}$ pero $\overline{(1,0)} \cdot \overline{(1,0)} = \overline{(1,0)} \neq \overline{(0,1)} \cdot \overline{(1,0)}$.

Es muy fácil comprobar que el núcleo de un homomorfismo es un ideal. El primer teorema de isomorfía para grupos se extiende a este contexto afirmando que para cualquier homomorfismo de anillos $f : A \longrightarrow B$, se tiene que $A/\mathrm{Ker}\, f$ es isomorfo a $\mathrm{Im} f$.

Los cocientes por ideales maximales tienen una insospechada e importante particularidad.

Proposición 1.2.3 *Sea A un anillo conmutativo con unidad. Un ideal $I \subset A$ es maximal si y sólo si todos los elementos de A/I diferentes de $\overline{0}$ son unidades.*

Demostración: Cualquier ideal que contenga a I y a algún $a \in A - I$, obviamente debe contener al ideal $J = \{x \in A \;:\; x - \lambda a \in I \text{ con } \lambda \in A\}$. Evidentemente $J = A$ si y sólo si $1 \in J$, esto es, si y sólo si $1 - \lambda_0 a \in I$ para algún λ_0, o equivalentemente $\overline{1} = \overline{\lambda_0}\overline{a}$. □

Observación: Nótese que A/I no sería un dominio de integridad si algún elemento $x \in I$ se pudiera factorizar como $x = ab$ con $a, b \notin I$. Por ello se llaman *ideales primos* a los que cumplen que A/I es un dominio de integridad. En particular, según el resultado anterior, todo ideal maximal es primo. Surge la pregunta natural de si ambos conceptos son equivalentes. Como el estudio de los ideales primos excede los contenidos de este curso, aquí solamente avanzaremos que en los anillos de polinomios estudiados en Álgebra III los ideales primos y maximales son bien distintos (por ejemplo $\langle x + y^2 \rangle$ es primo no maximal en $\mathbb{R}[x, y]$), mientras que en los anillos de números complejos que se manipulan en Teoría de Números (por ejemplo en todos los $\mathbb{Z}[\sqrt{d}]$) no hay diferencia entre primos y maximales.

En esta sección hemos dado por supuesto que el lector domina perfectamente el concepto de conjunto cociente, y más adelante haremos lo propio con el de grupo cociente. Si esta suposición fuera gratuita, es el momento de repasar cursos anteriores. De todos modos se añaden a continuación unas pocas líneas de nivel ínfimo, para desperezarse.

Cuando tenemos una forma de relacionar los elementos de un conjunto, el conjunto cociente no es más que el conjunto de las colecciones de elementos del mismo tipo. Esta clasificación en diferentes clases no es totalmente ajena al significado del cociente usual de números naturales. Por ejemplo $40 \div 4 = 10$ significa que si repartimos 40 caramelos entre 4 niños, tocan a 10 cada uno. Supongamos que los caramelos estuvieran numerados del 1 al 40 y que cada niño pusiera su nombre a los que recibiera. Si los repartimos de uno en uno ordenadamente, los caramelos 1, 5, 9, 13,... 37 tendrían el nombre del primer niño, los caramelos 2, 6, 10,... 38, el del segundo, etc. Con la relación $a \sim b \Leftrightarrow 4|a - b$, los caramelos relacionados entre sí son los que pertenecen al mismo niño. El conjunto cociente sería $\{N_1, N_2, N_3, N_4\}$ donde N_j es el conjunto de caramelos del niño j-ésimo (la clase de equivalencia de j), como las cuatro clases tienen el mismo tamaño, cada una tiene $40/4 = 10$ elementos. Al principio es un poco lioso que el conjunto cociente sea un conjunto de conjuntos, pero no lo es tanto pensando que por ejemplo un conjunto de libros es un conjunto de conjuntos de páginas.

En grupos (o anillos) hay relaciones de equivalencia (formas de repartir caramelos) naturales asociadas a ciertos subgrupos (o subanillos). Por ejemplo si H es un subgrupo de G uno puede inventarse $g_1 \sim g_2 \Leftrightarrow g_1 \cdot g_2^{-1} \in H$ que expresa algo así como que al repartir los caramelos de G "coherentemente" entre los elementos de H, g_1 y g_2 corresponden al mismo niño (elemento) de H. El conjunto cociente correspondiente se suele denotar como G/H. Una cuestión técnica muy importante es que la operación de grupo de G puede no estar bien definida en G/H. Sólo lo está cuando H es un subgrupo normal. De forma que si queremos descomponer un grupo en grupitos, clasificando sus elementos, no podemos tomar cociente entre un subgrupo cualquiera. Con los anillos ocurre algo similar y debemos limitarnos a las relaciones de equivalencia que vengan de ideales, no de subanillos cualesquiera.

1.3. Factorización

Como ya hemos mencionado, la teoría de ideales surgió en relación con ciertos problemas de factorización en anillos. A título meramente ilustrativo, nótese que por ejemplo hallar las soluciones enteras de $xy = 10^{20}$ requiere factorizar 10^{20} en $\mathbb{Z}$, y hallar las de $x^2 + y^2 = 10^{20}$, debido a la fórmula $x^2 + y^2 = (x - iy)(x + iy)$, requeriría factorizar 10^{20} en $\mathbb{Z}[i]$.

Sabemos que en $\mathbb{N}$ todo número mayor que uno se escribe como producto de primos de forma única salvo el orden de los factores. Éste es el llamado *teorema fundamental de la aritmética*. En $\mathbb{Z}$ la unicidad se complica por culpa de los signos. Por ejemplo

$$30 = 2 \cdot 3 \cdot 5 = (-2) \cdot 3 \cdot (-5) = 2 \cdot (-3) \cdot (-5) = (-2) \cdot (-3) \cdot 5.$$

La culpa la tiene el elemento -1, que al poseer inverso multiplicativo (él mismo), puede introducirse y compensarse a voluntad. En otros anillos puede haber más elementos invertibles que causen problemas similares. La definición de unicidad de la factorización en un anillo tendrá esta particularidad en cuenta. Antes introduciremos una notación *chic* que llama irreducibles a los primos en un anillo (algunos autores los siguen llamando primos).

Definición: Sea A un anillo. Se dice que dos elementos $a, b \in A$ están *asociados* si $a = ub$ con u una unidad.

Definición: Sea A un dominio de integridad. Se dice que un elemento $p \in A - \{0\}$ es *irreducible* si no es una unidad y $p = ab$ implica que p está asociado con a o con b.

Definición: Se dice que un dominio de integridad A es un *dominio de factorización única* si todo elemento de $A - \{0\}$ que no sea una unidad se puede expresar como un producto de factores irreducibles de forma única salvo el orden de los factores y el empleo de irreducibles asociados.

Ejemplo. $\mathbb{Z}$ es un dominio de factorización única.

Ejemplo. $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única, ya que por ejemplo $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Comprobar que los factores de esta doble factorización son realmente irreducibles conlleva algunos cálculos. Si fuera $2 = (x + y\sqrt{-5})(u + v\sqrt{-5})$, multiplicando por el conjugado se tendría $4 = (x^2 + 5y^2)(u^2 + 5v^2)$, y evidentemente esto sólo es posible si $y = v = 0$, y se tiene $x + y\sqrt{-5} = \pm 1$ o $u + v\sqrt{-5} = \pm 1$. La misma demostración sirve para 3. Análogamente $1 \pm \sqrt{-5} = (x + y\sqrt{-5})(u + v\sqrt{-5})$ implica $6 = (x^2 + 5y^2)(u^2 + 5v^2)$, y la única posibilidad, salvo intercambiar x e y por u y v, es $x = \pm 1$, $y = \pm 1$, $u = \pm 1$, $v = 0$.

Los dominios de factorización única se muestran más sencillos en algunos problemas que los anillos que no lo son, y nos gustaría saber detectarlos.

Una vez que sabemos qué queremos hacer, vamos a abstraer las propiedades necesarias para llevarlo a cabo. Si repasamos el teorema fundamental de la aritmética, veremos que la prueba se basa en la existencia del máximo común divisor. A su vez, ésta dependía de la existencia del algoritmo de Euclides. Uniendo estos cabos buscamos un teorema que diga algo así como que los dominios de integridad en los que existe un algoritmo de Euclides son los de factorización única. Pero ¿qué es un algoritmo de Euclides en general? En $\mathbb{N}$ era un procedimiento que simplemente requería la existencia de una división inexacta: dados a y b se calculaba un cociente c y un resto $r < b$ tales que $a = bc + r$. Todo esto lo podemos copiar en anillos arbitrarios salvo el signo "$<$" ya que en general no hay relaciones de orden en un anillo. Por tanto para salvar la idea del algoritmo de Euclides requerimos que exista una función que permita medir lo grandes que son sus elementos traspasando el problema a $\mathbb{N}$. Habida cuenta de todo esto, la siguiente definición concretará la idea buscada de dominio con algoritmo de Euclides.

Definición: Se dice que un dominio de integridad A es un *dominio euclídeo* si existe una función $N : A - \{0\} \longrightarrow \mathbb{N}$ tal que:
i) $\forall a, b \in A - \{0\}$ se cumple $N(a) \leq N(ab)$.
ii) $\forall a, b \in A - \{0\}$ existen $c, r \in A$ tales que $a = bc + r$ con $r = 0$ o $N(r) < N(b)$.

Observación: Algunos autores piden que N sea una función multiplicativa, esto es, $N(ab) = N(a)N(b)$, lo cual es más fuerte que $i)$.

Ejemplo. $\mathbb{Z}$ es un dominio euclídeo con $N(a) = |a|$.

Ejemplo. $\mathbb{Q}[x]$ es un dominio euclídeo con $N(P) = \partial P$.

Veamos qué consecuencias tiene la existencia del máximo común divisor en relación con los ideales. Es interesante comparar el siguiente resultado con la Proposición 1.2.1.

Teorema 1.3.1 *Si A es un dominio euclídeo entonces todos los ideales de A son principales.*

Notación: Para abreviar se suele hablar de *dominio de ideales principales* para indicar un dominio de integridad con todos sus ideales principales.

Demostración: Sea $I \neq \langle 0 \rangle$ un ideal de A y sea b el elemento de I para el que $N(b)$ es mínimo. Dado $a \in I$, por ser A dominio euclídeo $a = bc + r$ con $r = 0$ (ya que $N(r) < N(b)$ es imposible porque $r = a - bc \in I$). Por tanto $a = bc \in \langle b \rangle$ y como esto se cumple para todo $a \in I$, se deduce $I = \langle b \rangle$. □

El próximo resultado simplemente ilustra que en algunas situaciones los ideales maximales son más tangibles que lo que su definición indica.

Proposición 1.3.2 *Sea A un dominio de ideales principales. Un ideal $I \subsetneqq A$ es maximal si y sólo si $I = \langle p \rangle$ con p irreducible.*

Demostración: $\Rightarrow$) Si $I = \langle a \rangle$ con $a = bc$, b y c no invertibles, se tendría $I \subsetneqq \langle b \rangle \subsetneqq A$.
$\Leftarrow$) Si $I = \langle p \rangle \subset J = \langle b \rangle \subset A$ entonces $p \in \langle b \rangle$ implica $p = bc$. Por la irreducibilidad, b o c son invertibles y por consiguiente o bien $J = A$ o bien $J = I$. □

Aparentemente nos hemos desviado en nuestro estudio de la factorización. El siguiente resultado mostrará que estábamos a mitad de camino.

Teorema 1.3.3 *Si A es un dominio de ideales principales entonces A es un dominio de factorización única.*

Demostración: Sea $a \in A - \{0\}$ no invertible. Veamos primero que a se puede escribir como producto de un número finito de irreducibles. Si no fuera así, tendríamos una sucesión infinita de igualdades

$$a = p_1 a_1 = p_1 p_2 a_2 = p_1 p_2 p_3 a_3 = p_1 p_2 p_3 p_4 a_4 = \dots$$

con p_j irreducibles y $a_j = p_{j+1}a_{j+1}$. Sea el ideal $I = \bigcup_{j=1}^{\infty}\langle a_j\rangle$. Por estar en un dominio de ideales principales $I = \langle b\rangle$, con $b \in \langle a_k\rangle$ para cierto k, y esto implica $I = \langle a_k\rangle$ porque $b \in \langle a_k\rangle \supset I = \langle b\rangle$. Lo cual lleva a la contradicción $\langle a_{k+1}\rangle = \langle a_k/p_{k+1}\rangle \notin I$.

Una vez que hemos visto que hay una factorización, debemos probar que es única. Supongamos que hubiera dos factorizaciones en irreducibles que coinciden

$$p_1 \cdot p_2 \cdots p_l = q_1 \cdot q_2 \cdots q_m. \tag{1.3}$$

Queremos probar que ambas son iguales salvo en el orden de los factores y multiplicación por elementos invertibles.

Procedemos por inducción en $n = \min(l, m)$. Evidentemente $l = 1 \Leftrightarrow m = 1$ (por la irreducibilidad) y el caso $n = 1$ es trivial. Sea por tanto $n > 1$. El ideal $I = \langle p_l, q_m\rangle$ debe ser principal, digamos $I = \langle b\rangle$. Por tanto $p_l = rb$, $q_m = sb$, y como p_l y q_m son irreducibles, o bien r y s son invertibles o bien b es invertible. En el primer caso p_l y q_m son asociados porque $p_l = r^{-1}sq_m$, y simplicando en (1.3), el resultado se sigue por la hipótesis de inducción. Si b es invertible $I = A$, en particular

$$1 \in \langle p_l, q_m\rangle \;\Rightarrow\; \lambda p_l + \mu q_m = 1 \;\Rightarrow\; \lambda p_l q_1 q_2 \ldots q_{m-1} + \mu p_1 p_2 \ldots p_l = q_1 q_2 \ldots q_{m-1}.$$

De forma que $cp_l = q_1 q_2 \ldots q_{m-1}$ para cierto $c \in A$ y por la hipótesis de inducción se sigue que p_l es asociado de alguno de los q_j. Simplificando como antes p_l y q_j en (1.3) se concluye la prueba empleando la hipótesis de inducción. □

En resumen, lo que hemos demostrado es:

Dom. euclídeo ⇒ Dom. de ideales principales ⇒ Dom. de factorización única.

Es posible dar contraejemplos a los recíprocos. Por ejemplo, se puede probar (pero no es nada fácil) que $\mathbb{Z}[(1+\sqrt{-19})/2]$ es un dominio de ideales principales pero no un dominio euclídeo (véase en [Cam] una demostración abreviada). También se puede probar que $\mathbb{Z}[x]$ es un dominio de factorización única (se sigue de que $\mathbb{Q}[x]$ lo es) pero no un dominio de ideales principales, ya que $I = \langle 3, x^2\rangle$ no es principal.

A continuación mostramos algunos ejemplos desarrollados que no debieran hacernos demasiado optimistas, porque incluso en anillos sencillos hay todavía problemas abiertos respecto a la factorización única.

Ejemplo. El anillo $\mathbb{Z}[i] = \{a + bi \;:\; a, b \in \mathbb{Z}\}$ es un dominio de factorización única. De hecho es un dominio euclídeo con $N(z) = |z|^2$ donde $|\cdot|$ indica la norma usual en $\mathbb{C}$.

Como $N(z_1z_2) = N(z_1)N(z_2)$, la primera propiedad de los dominios euclídeos está asegurada. Los círculos unitarios $\{z \in \mathbb{C} \;:\; N(z-w) < 1\}$ recubren todo $\mathbb{C}$ cuando w recorre $\mathbb{Z}[i]$; por tanto dados $z_1, z_2 \in \mathbb{Z}[i] - \{0\}$ siempre existe $w \in \mathbb{Z}[i]$ tal que $N(z_1/z_2 - w) < 1$, o lo que es lo mismo $N(z_1 - z_2w) < N(z_2)$. Esto prueba la segunda propiedad con $r = z_1 - z_2w$. Como $N(0) = 0$, el caso $r = 0$ está incluido en $N(r) < N(z_2)$.

Ejemplo. El anillo $\mathbb{Z}[\sqrt{-3}]$ no es de factorización única y por tanto no es de ideales principales ni euclídeo.

Un ejemplo de factorización no única es $2\cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. Para comprobar que cada factor es irreducible se puede usar el mismo argumento empleado para $\mathbb{Z}[\sqrt{-5}]$. De esta doble factorización se deduce que el ideal $I = \langle 2, 1+\sqrt{-3}\rangle$ no es principal. No es muy difícil comprobar que I es maximal.

Ejemplo. El anillo $\mathbb{Z}[(1+\sqrt{-3})/2]$ es de factorización única. De hecho es un dominio euclídeo con $N(z) = |z|^2$.

Observando que $((1+\sqrt{-3})/2)^2 = (-1+\sqrt{-3})/2$, se deduce que

$$\mathbb{Z}[(1+\sqrt{-3})/2] = \{a + b(1+\sqrt{-3})/2 \ : \ a, b \in \mathbb{Z}\}.$$

Como en el caso de $\mathbb{Z}[i]$, los círculos de radio 1 centrados en los puntos de $\mathbb{Z}[(1+\sqrt{-3})/2]$ cubren todo $\mathbb{C}$ y la demostración es similar.

Nota: Los anillos de la forma $\mathbb{Z}[\sqrt{d}]$ son más difíciles de estudiar en el caso $d > 0$. Si queremos probar que son de factorización única, la función N "natural" a considerar es $N(z) = |z \cdot \overline{z}|$ donde $\overline{z}$ es el conjugado real (esto es, $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$) y $|\cdot|$ es el valor absoluto. Parte de la complicación proviene de que ahora hay que considerar recubrimientos por regiones hiperbólicas no acotadas, en vez de por círculos.

Para cerrar el bucle, volvamos al problema del principio de la sección: supongamos que queremos hallar las soluciones de

$$x^2 + y^2 = 10^{20}.$$

En $\mathbb{Z}[i]$ se tiene la factorización $2 = (1+i)(1-i)$ con $1+i$ y $1-i$ irreducibles asociados porque $1+i = i(1-i)$; y $5 = (2+i)(2-i)$. De modo que la ecuación anterior se puede escribir como

$$(x+iy)(x-iy) = (1-i)^{40}(2+i)^{20}(2-i)^{20},$$

lo que implica que existen enteros $0 \le \alpha \le 40$ y $0 \le \beta, \gamma \le 20$ tales que

$$x + iy = u(1-i)^{\alpha}(2+i)^{\beta}(2-i)^{\gamma} \quad \text{y} \quad x - iy = u^{-1}(1-i)^{40-\alpha}(2+i)^{20-\beta}(2-i)^{20-\gamma}$$

con u algún elemento invertible. Conjugando la segunda ecuación y usando que que la factorización es única (recuérdese que $1+i$ y $1-i$ están asociados) se sigue $\alpha = 40-\alpha$, $\beta = 20-\gamma$ y $\gamma = 20-\beta$. Por tanto las soluciones enteras x, y de la ecuación original vienen dadas por

$$x + iy = u(1-i)^{20}(2+i)^{\beta}(2-i)^{20-\beta}.$$

Como hay 21 posibles valores de $0 \le \beta \le 20$ y 4 posibles valores de u (en $\mathbb{Z}[i]$ los elementos invertibles son $1, -1, i, -i$), tenemos 84 soluciones.

Para terminar descansadamente, recordemos los buenos y tiernos tiempos de Conjuntos y Números a través de los inofensivos anillos de polinomios $\mathbb{C}[x]$, $\mathbb{R}[x]$ y $\mathbb{Q}[x]$. Todos ellos son dominios de factorización única por ser dominios euclídeos (basta elegir como función N el grado).

Nos han dicho muchas veces que todo polinomio no constante tiene una raíz compleja, lo que por el teorema del resto se traduce en:

Teorema 1.3.4 (Teorema fundamental del Álgebra) *Sea $P \in \mathbb{C}[x]$ no constante, P es irreducible en $\mathbb{C}[x]$ si y sólo si* $\operatorname{gr} P = 1$.

Seguramente el lector ya habrá visto dos demostraciones de este teorema, una en Topología y otra en Variable Compleja I. No es posible dar una prueba totalmente algebraica porque la propia definición de $\mathbb{C}$ depende de la de $\mathbb{R}$, que está en la base del análisis. De todas formas, si alguien quiere opinar lo contrario puede, cuando termine el curso, leer [St] §18 y hacer caso omiso de las excusas.

En $\mathbb{R}[x]$ las cosas no son muy diferentes:

Teorema 1.3.5 *Si $P \in \mathbb{R}[x]$ es irreducible en $\mathbb{R}[x]$ entonces* $\operatorname{gr} P \leq 2$.

Demostración: Por el teorema anterior, si $\partial P > 1$, existe $z \in \mathbb{C}$ y $Q \in \mathbb{C}[x]$ tal que $P = (x - z)Q$. Si $z \in \mathbb{R}$, entonces $x - z$ es un factor de grado 1 de P en $\mathbb{R}[x]$. En otro caso, conjugando $P = (x - \overline{z})\overline{Q}$. Como $x - z$ y $x - \overline{z}$ son irreducibles no asociados en $\mathbb{C}[x]$, se deduce $R|P$ con $R = (x - z)(x - \overline{z})$, y es evidente que $R \in \mathbb{R}[x]$ con $\partial R = 2$. □

En $\mathbb{Q}[x]$ las cosas son más complicadas. Parece muy fácil probar que quitando denominadores podemos pasar el problema a $\mathbb{Z}[x]$, pero la demostración tiene intríngulis suficiente como para que invoquemos el nombre del *princeps mathematicorum*.

Lema 1.3.6 (Lema de Gauss) *Si $P \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}[x]$ también lo es en $\mathbb{Q}[x]$.*

Demostración: Si $P = P_1P_2$ con $P_1, P_2 \in \mathbb{Q}[x]$ multiplicando por cierto número natural, n, que cancele todos los denominadores tenemos que

$$nP = (b_l x^l + b_{l-1}x^{l-1} + \cdots + b_0)(c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0) \qquad \text{con } b_i, c_i \in \mathbb{Z}. \tag{1.4}$$

Supongamos que n es el menor número tal que nP se descompone en $\mathbb{Z}[x]$. Si $n = 1$ el lema está probado. Supongamos que $n > 1$, sea p un divisor primo de n, entonces no todos los b_i ni todos los c_i pueden ser divisibles por p (ya que en ese caso podríamos simplificar por p en (1.4) reduciendo n a n/p). Sean b_i y c_j tales que $p \not| b_i$, $p \not| c_j$ pero $p|b_r$, $p|c_s$ si $r < i$, $s < j$ (podría ocurrir que $i, j = 0$), entonces igualando en (1.4) los coeficientes de grado $i + j$ se tiene

$$na_{i+j} = b_{i+j}c_0 + b_{i+j-1}c_1 + \cdots + b_i c_j + \cdots + b_0 c_{i+j}$$

y de aquí se deduce que $p|b_i c_j$ en contra de nuestra hipótesis $p \not| b_i$, $p \not| c_j$. □

Decidir si un polinomio es irreducible en $\mathbb{Z}[x]$ o $\mathbb{Q}[x]$ puede ser muy laborioso. Un criterio que es de utilidad en algunos casos es el siguiente.

Proposición 1.3.7 (Criterio de Eisenstein) *Si $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ es un polinomio con coeficientes enteros y p es un primo tal que $p \not| a_n$, $p|a_i$ si $0 \leq i < n$ y $p^2 \not| a_0$ entonces P es irreducible en $\mathbb{Q}[x]$.*

Demostración: Por el Lema de Gauss, si P no es irreducible se puede escribir como $P = (b_l x^l + b_{l-1}x^{l-1} + \cdots + b_0)(c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0)$ con $l + m = n$ y $b_i, c_i \in \mathbb{Z}$. Igualando los coeficientes de los términos del mismo grado, se tiene

$$a_0 = b_0c_0, \quad a_1 = b_1c_0 + b_0c_1, \quad a_2 = b_2c_0 + b_1c_1 + b_0c_2, \quad \ldots$$

Por hipótesis $p|a_0$ pero $p^2 \not| a_0$, así pues p divide a b_0 o a c_0 pero no a ambos simultáneamente. Supongamos por ejemplo que p divide a b_0, entonces por la segunda igualdad, $p|b_1$ y por la tercera $p|b_2$ y en general $p|b_i$ $0 \leq i \leq l$, lo que implica que p divide a todos los a_i lo que contradice nuestra hipótesis $p \not| a_n$. □

Ejemplo. Los polinomios $P = x^5 - 2x + 6$ y $Q = x^7 - 12$ son irreducibles en $\mathbb{Q}[x]$. (Tómese $p = 2$ y $p = 3$ en el criterio de Eisenstein).

Una aplicación indirecta de este criterio prueba que el polinomio llamado *ciclotómico*

$$P = x^{p-1} + x^{p-2} + \cdots + x + 1$$

es irreducible en $\mathbb{Q}[x]$ si p es primo. Para ello nótese que P es irreducible si y sólo si $Q = (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1$ también lo es (ejercicio) y como

$$Q = \frac{(x+1)^p - 1}{x + 1 - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1},$$

el criterio de Eisenstein es aplicable a Q (ejercicio). Además se puede probar que P no es irreducible si p no es primo, aunque no lo haremos aquí.

Recordemos también otro criterio sencillo de Conjuntos y Números. La demostración es muy sencilla y se deja al lector.

Proposición 1.3.8 *Dado $P \in \mathbb{Z}[x]$ sea $\overline{P} \in \mathbb{Z}_p[x]$ el polinomio que resulta al reducir los coeficientes módulo p (primo). Suponiendo que $\partial P = \partial \overline{P}$, si $\overline{P}$ es irreducible en $\mathbb{Z}_p[x]$ entonces P es irreducible en $\mathbb{Q}[x]$.*

Ejemplo. El polinomio $x^3 - 17x^2 + 10x + 105$ es irreducible en $\mathbb{Q}[x]$, porque al tomar módulo 2 obtenemos $x^3 + x^2 + 1$ y si este polinomio se pudiera descomponer en $\mathbb{Z}_2[x]$ se podría escribir como $(x^2 + ax + b)(x - c)$, lo cual es imposible porque ni x ni $x - 1$ dividen a $x^3 + x^2 + 1$.

Ejercicios del Capítulo 1

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 1.1

1. Demostrar que:
i) $\{n + m\sqrt{3} \ : \ n, m \in \mathbb{Z}\}$ es un anillo.
ii) $\{a + b\sqrt{3} \ : \ a, b \in \mathbb{Q}\}$ es un anillo tal que todos sus elementos no nulos son unidades.
iii) $\{a + b\sqrt[4]{3} \ : \ a, b \in \mathbb{Q}\}$ no es un anillo.
♢iv) $\{a + b\sqrt[3]{3} + c\sqrt[3]{9} \ : \ a, b, c \in \mathbb{Q}\}$ es un anillo tal que todos sus elementos no nulos son unidades.

♡**2.** Sean $R_1, \ldots, R_n$ anillos. Demostrar que $R_1 \oplus \ldots \oplus R_n$ es un anillo con las operaciones de suma y producto obvias (las dadas por las de cada R_i coordenada a coordenada).

♡**3.** Escribir la tabla de multiplicación del anillo $\mathbb{Z}_3[i] = \{a + bi : a, b \in \mathbb{Z}_3\}$.

4. El conjunto $\{0, 2, 4, 6, 8\}$ es un anillo conmutativo con unidad, con la suma y el producto módulo 10. ¿Cuál es la unidad multiplicativa? ¿Y los elementos invertibles?

5. Probar que los elementos neutros de las operaciones de un anillo con unidad son únicos.

6. Comprobar que las unidades de $\mathbb{Z}_{17}$ forman un grupo cíclico.

7. ¿Cuántas unidades hay en $\mathbb{Z}_{10^6}$?

8. Hallar todas las unidades en $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[(1 + \sqrt{-3})/2]$ y en el anillo de matrices enteras 2×2.

9. Probar que $2x + 1$ tiene inverso multiplicativo en $\mathbb{Z}_4[x]$.

10. Hallar las unidades del anillo de matrices 2×2 con elementos en $\mathbb{Z}_4$.

11. Hallar el inverso multiplicativo de 5 en $\mathbb{Z}_{21}$ usando el algoritmo de Euclides.

12. Probar que en el anillo de matrices reales $n \times n$, para todo elemento, m, que no es una unidad, existe $m' \neq 0$ tal que $m'm = 0$.

13. Encontrar un anillo R en el que no se verifiquen ninguna de las siguientes propiedades:
i) Si $a^2 = a$, entonces $a = 1$ ó $a = 0$.
ii) Si $ab = ac$ para $a \neq 0$ entonces $b = c$.

14. Si R no es un dominio de integridad la intuición que tenemos sobre ecuaciones algebraicas puede ser completamente errónea. Meditemos sobre este hecho:
i) Buscar un anillo R en el que la ecuación $ax = b$ con $a, b \in R$ tenga más de una solución.

ii) Encontrar todas las soluciones de la ecuación $x^2 - 5x + 6 = 0$ en $\mathbb{Z}_{12}$.

♡**15.** Sea $f : R \to S$ un homomorfismo de anillos. Demostrar que:
i) Para todo $r \in R$, y para todo entero positivo n, se tiene que $f(r^n) = f(r)^n$.
ii) La imagen de R por f, $\{s \in S : s = f(r), \text{ para algún } r \in R\}$, es un subanillo de S.

♡**16.** Sea $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ dada por $\phi(P) = 2^{\partial P}$. Estudiar si es un homomorfismo.

17. Probar que el anillo $\mathbb{Z}_6$ es isomorfo al anillo $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

18. Demostrar que los anillos $\mathbb{Z}[\sqrt{7}] = \{a + b\sqrt{7} : a, b \in \mathbb{Z}\}$ y

$$R = \left\{ \begin{pmatrix} c & 7d \\ d & c \end{pmatrix} : c, d \in \mathbb{Z} \right\}$$

son isomorfos.

19. Demostrar que la aplicación $f : \mathbb{Z}_n \to \mathbb{Z}_n$ dada por $f(x) = x^n$ es un homomorfismo de anillos si n es primo. ¿Es el resultado cierto si n no es primo?

∘**20.** Escribir $x_1^2 + x_2^2 + x_3^2$ y $x_1^3 + x_2^3 + x_3^3$ en términos de los polinomios simétricos elementales.

∘**21.** Sea $s_k = x_1^k + x_2^k + \cdots + x_n^k$ para $0 < k$ y $s_0 = k$. Demostrar las "identidades de Newton"

$$\begin{aligned} (-1)^{k+1} s_k &= \sum_{i=0}^{k-1} (-1)^i s_i \sigma_{k-i} \qquad \text{para } 0 < k \leq n \\ (-1)^{k+1} s_k &= \sum_{i=k-n}^{k-1} (-1)^i s_i \sigma_{k-i} \qquad \text{para } k > n \end{aligned}$$

donde σ_i son los polinomios simétricos elementales. *Indicación*: Defínase $\sigma_i = 0$ para $i > n$ y aplíquese inducción para demostrar simultáneamente ambas identidades.

Sección 1.2

♡**22.** Probar que a y b están asociados si y sólo si $\langle a \rangle = \langle b \rangle$.

23. ¿Cuándo tiene sentido $n\mathbb{Z}/m\mathbb{Z}$?

24. Hallar el generador mónico del ideal $I = \langle x^3 + 1, x^2 + 1 \rangle$ en $\mathbb{Z}_2[x]$.

♡**25.** Demostrar que $\mathbb{Q}[x]/\langle x^2 - 5x + 6 \rangle$ no es un dominio de integridad.

26. En $\mathbb{Z}[x]$ sea I el subconjunto formado por los polinomios tales que la suma de sus coeficientes es cero. Probar que I es un ideal y que $\mathbb{Z}[x]/I$ es isomorfo a $\mathbb{Z}$.

27. Hallar un subanillo de $A = \mathbb{Z}[\sqrt{2}]$ que no sea ideal.

28. Probar que todos los subanillos de $\mathbb{Z}$ son ideales. Dar un contraejemplo si $\mathbb{Z}$ se reemplaza por $\mathbb{Z} \oplus \mathbb{Z}$.

29. Demostrar que el grupo multiplicativo de $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ es cíclico y dar un generador.

30. Hallar los ideales de $\mathbb{Z}_{24}$.

31. Sea $f : R \to S$ un homomorfismo de anillos. Demostrar que:
i) Si $J \subset S$ es un ideal, entonces $f^{-1}(J) = \{r \in R : f(r) \in J\}$ es un ideal en R.
ii) El núcleo de f es un ideal.
iii) Un homomorfismo de anillos es inyectivo si y sólo si su núcleo es $\{0\}$.

32. Dado un anillo R y un ideal $I \subset R$, demostrar que hay una correspondencia biyectiva entre los ideales de R/I y los ideales de R que contienen a I. *Indicación*: usar el homomorfismo natural $\pi : R \to R/I$, que a cada elemento $a \in R$ le asocia su clase módulo I, y observar que la imagen inversa de un ideal por un homomorfismo de anillos es también un ideal.

33. Sea $A = \mathbb{Z}[\sqrt{2}]$. Hallar todos los ideales del anillo $A/2A$.

34. Hallar los ideales de $\mathbb{Q}[x]/\langle x^3-1\rangle$.

35. Decidir si el ideal $\langle 29, 13+\sqrt{-5}\rangle$ es principal en $\mathbb{Z}[\sqrt{-5}]$

36. Probar que el anillo de matrices cuadradas reales $n \times n$ no tiene ideales no triviales.

37. Encontrar todos los ideales maximales de los anillos $\mathbb{Z}_8$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$ y $\mathbb{Z}_n$.

38. Probar que $I = \{(3n, m) : n, m \in \mathbb{Z}\}$ es un ideal maximal en $\mathbb{Z} \oplus \mathbb{Z}$.

39. Sea $I \subset \mathbb{Z}[\sqrt{-5}]$ dado por $I = \{a + b\sqrt{-5} \ : \ a+b \text{ es par}\}$. Demostrar que es un ideal maximal de $\mathbb{Z}[\sqrt{-5}]$.

♢**40.** Sean I y J, con $J \subset I$, ideales de un anillos A. Probar que A/I es isomorfo a $(A/J)/(I/J)$. (Esto requiere en particular probar que este último cociente tiene sentido).

♢**41.** Sea p primo y sea $A \subset \mathbb{Q}$ el anillo formado por todas las fracciones cuya forma irreducible tiene denominador no divisible por p. Hallar un anillo sencillo que sea isomorfo a $A/\langle p\rangle$.

Sección 1.3

42. Sea el conjunto $H = \{1, 5, 9, 13, 17, 21, 25 \dots\}$. Decimos que $p \in H$ es un H-primo si $p \neq 1$ y no es divisible por ningún elemento de H salvo por sí mismo y por uno. Por ejemplo, 5 y 9 son H-primos, pero $25 = 5 \cdot 5$ no. Comprobar que 693 tiene varias posibles descomposiciones en factores H-primos. (Nota: Hilbert (1862-1943) propuso H como un conjunto sencillo en el que no se cumple el análogo del teorema fundamental de la aritmética).

43. Hallar todos los polinomios irreducibles en $\mathbb{Z}_2[x]$ de grados 2, 3 y 4.

44. Decir si son irreducibles en $\mathbb{Q}[x]$ los polinomios $3x^2 - 7x - 5$, $6x^3 - 3x - 18$ y $x^3 - 7x + 1$.

45. Demostrar que $x^3 - x + 1$ es irreducible en $\mathbb{Z}_3[x]$.

46. Demostrar que $x^5 - x^2 + 1$ es irreducible en $\mathbb{Z}_2[x]$.

47. Probar la irreducibilidad en $\mathbb{Q}[x]$ de los polinomios: $x^5 - 3x + 3$, $x^6 - 6x + 2$, $x^2 + 1$, $x^4 + 1$ y $x^6 + x^3 + 1$.

48. Probar que $P \in \mathbb{Q}[x]$ es irreducible si y sólo si Q dado por $Q(x) = P(x + 1)$, lo es.

49. Probar que el criterio de Eisenstein es aplicable al polinomio

$$x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}.$$

50. Decidir si los siguientes polinomios son irreducible en $\mathbb{Q}[x]$: $x^4 + 3x + 6$, $x^3 + 11^{11}x + 13^{13}$, $\frac{1}{3}x^5 + \frac{5}{2}x^4 + \frac{3}{2}x^3 + \frac{1}{2}$, $x^5 - 9x^2 + 1$ y $x^4 - x^3 - x - 1$.

51. Probar que $x^2 + bx + c$ es irreducible en $\mathbb{Z}_7[x]$ si y sólo si $b^2 - 4c = 3, 5, 6$.

52. Estudiar la irreducibilidad de $P = x^2 + 1$ en $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_7[x]$, $\mathbb{Z}_{11}[x]$, $\mathbb{Z}_{13}[x]$ y $\mathbb{Z}_{17}[x]$.

∘**53.** Intentar inducir (sin demostración) una regla general sencilla que permita decidir la irreducibilidad de $P = x^2 + 1$ en $\mathbb{Z}_p[x]$ sin calcular sus raíces.

54. Hallar un contraejemplo a la Proposición 1.3.8 si se omite la condición $\partial P = \partial \overline{P}$.

55. Estudiar si $\mathbb{Z}[\sqrt{-2}]$ es un dominio de factorización única.

56. Demostrar que $\mathbb{Z}[\sqrt{2}]$ es un dominio de factorización única y encontrar la factorización de 20. *Indicación*: La ecuación en enteros $a^2 - 2b^2 = 5$ no tiene solución (lleva a contradicción módulo 5).

57. Estudiar si $\mathbb{Z}[\sqrt{-6}]$ es un dominio de factorización única.

♢**58.** Estudiar si $\mathbb{Z}[\sqrt{6}]$ es un dominio de factorización única.

♢**59.** Demostrar que un polinomio de la forma $P = x^n + px + p^2$ es irreducible en $\mathbb{Z}[x]$.

♢**60.** Sea $p > 2$ primo. Demostrar que existen $n, m \in \mathbb{Z}$ tales que $p = n^2 + mn + m^2$ si y sólo si $P = x^2 + x + 1$ factoriza en $\mathbb{Z}_p[x]$.

Apéndice del Capítulo 1

Conoce a tus héroes

(Más información en: `http://turnbull.mcs.st-and.ac.uk/history/`)

E. Kummer no sólo fue un gran matemático sino también un magnífico profesor con gran predicamento entre los alumnos. Su trabajo relativo al último teorema de Fermat fue verdaderamente revolucionario, tanto es así, que la Academia de Ciencias de París le concedió en 1857 el premio destinado al que probase este resultado, a pesar de que los razonamientos de Kummer no se podían aplicar a todos los exponentes, constituyendo una solución parcial.

Apellido: Kummer
Nombre: (Ernst) Eduard
Nacimiento: 1810 Sorau
Defunción: 1893 Berlín

Bla, bla, bla

- *La introducción de tales números complejos ideales tiene el mismo motivo simple y básico que lleva a introducir fórmulas imaginarias en álgebra y análisis; concretamente, la descomposición de funciones racionales en sus factores más simples, los lineales.* E. Kummer 1847.

- *. . . la fuente de todas las Matemáticas grandiosas es el caso particular, el ejemplo concreto. Es frecuente en Matemáticas que toda aparición de un concepto de aparente gran generalidad sea en esencia la misma que la de un concreto y pequeño caso particular.* P. Halmos.

- [Acerca del título del libro de Al-Khwārizmī, *Hisab al-jabr w'al-muqābala*, que dio origen a la palabra "álgebra"] Jabr *es la colocación de un hueso, de aquí reducción o restauración;* muqābala *es confrotación, oposición, enfrentamiento.* Citado en [Ca], p. 203.

- *En esto fueron razonando los dos, hasta que llegaron a un pueblo donde fue ventura hallar un algebrista, con quien se curó el Sansón desgraciado.* "El ingenioso hidalgo don Quijote de la Mancha"(2ª parte). Capítulo XV.

¿Qué hay que saberse?

Todo lo que no esté en letra pequeña. En particular, hay que saber: manejar el concepto de anillo (y aplicaciones entre ellos) y de ideal (principal, maximal); manipular

cocientes con soltura; comprender el problema de factorización y su relación con los ideales, siendo capaz de estudiar si hay factorización única en ejemplos fáciles; saber decidir la irreducibilidad en $\mathbb{Q}[x]$ y $\mathbb{Z}[x]$ de polinomios sencillos.

(PQR) Preguntón, quejoso y respondón

P- ¿Hay un algoritmo para factorizar en $\mathbb{Q}[x]$?

R- Por el lema de Gauss, basta considerar el problema en $\mathbb{Z}[x]$. Si $R = PQ$ entonces los términos independientes de P y Q son divisores del de R, lo cual da un número finito de posibilidades para ellos, lo mismo se puede hacer inductivamente para el resto de los coeficientes. El problema es que este algoritmo es tan poco eficiente que muy pocas veces lo podríamos llevar a cabo "a mano", de ahí el interés de los trucos como el criterio de Eisenstein.

Q- Si no hay métodos sistemáticos para humanos sin ordenador, ¿cómo quieren que factoricemos en $\mathbb{Q}[x]$ en este curso?

R- Evidentemente los ejemplos están preparados y se trata de atajar los cálculos con ingenio.

Q- Eso de los ideales es una cosa muy rara.

R- Sí que lo es, pero se muestra fundamental al estudiar la factorización.

P- No entiendo por qué para factorizar en $\mathbb{Z}[\sqrt{-5}]$ hay que introducir esos extraños números ideales. Por ejemplo, para hacer un polinomio de $\mathbb{R}[x]$ factorice del todo sólo hay que permitir usar números complejos, que pueden ser raros, pero son números al fin y al cabo.

R- Sí, en principio se podría resolver el problema de factorización en subanillos de $\mathbb{C}$ ampliándolos con nuevos números complejos. Lo malo es que los nuevos números añadidos pueden tener a su vez problemas de factorización entre ellos y necesitar de otra ampliación. La llamada teoría de cuerpos de clases nos dice que el proceso podría no terminar nunca.

P- Entonces los ideales sólo sirven para factorizar.

R- Se inventaron para ello, pero los ideales tienen un alcance mucho más amplio porque son lo único con lo que se pueden hacer cocientes de anillos, es decir, reducirlos. Si tomamos cociente entre los ideales más grandes, los maximales, nos quedaremos con los trozos de anillo más pequeños. Por ejemplo, en geometría algebraica se arreglan las cosas para que una curva algebraica sea un anillo, y en esta correspondencia los puntos son los ideales maximales. En general se puede asignar un anillo a una variedad algebraica (curvas, superficies, etc. definidas por polinomios) y sus ideales primos corresponden a las subvariedades algebraicas.

Q- Eso parece más raro todavía.

P- ¿Dónde se pueden aprender esas cosas?

R- En Álgebra III.