Capítulo 13
Aritmética

La matemática es la reina de las ciencias y la aritmética es la reina de las matemáticas.

Gauss

Una gran parte de la teoría de anillos y en general de las matemáticas importantes del fin del siglo XIX fue desarrollada para generalizar la aritmética de los números enteros a los anillos conmutativos, o estudiar las obstrucciones que aparecen en este intento. Esto se estudia en detalles en la teoría de números algebraica, y en este capítulo vamos a ver algunas nociones básicas. En particular, vamos a definir ciertas clases importantes de anillos:

$$\text{dominios euclidianos} \subsetneq \text{dominios de ideales principales} \subsetneq \text{dominios de factorización única}$$

y terminar por una breve discusión de anillos de números. Este material generaliza los resultados clásicos sobre los números enteros. El lector puede consultar, por ejemplo, el primer capítulo de [IR1990].

En este capítulo R siempre va a denotar un anillo conmutativo sin divisores de cero; es decir, un dominio de integridad.

13.1 Divisibilidad en dominios de integridad

lección 17
25.09.18

13.1.1. Definición. Para elementos $x, y \in R$ se dice que x **divide** a y si $y = zx$ para algún $z \in R$. En este caso también se dice que x es un **divisor** de y y que y es un **múltiplo** de x y se escribe "$x \mid y$".

Se dice que x e y son **asociados** si $x \mid y$ e $y \mid x$. En este caso se escribe "$x \sim y$".

Hagamos primero algunas observaciones triviales.

13.1.2. Observación.

1) $1 \mid x$ *para cualquier* $x \in R$,

2) $x \mid 1$ *si y solamente si* $x \in R^\times$,

3) $x \mid 0$ *para cualquier* $x \in R$,

4) $0 \mid x$ *si y solamente si* $x = 0$.

Demostración. En 1) basta notar que $x = 1 \cdot x$. En 2), si $x \mid 1$, entonces $1 = xy$ para algún $y \in R$ y $y = x^{-1}$. En 3), siempre se cumple $0 = 0 \cdot x$ y en 4), si $x = 0 \cdot y$, entonces $x = 0$. ■

La relación $x \sim y$ significa precisamente que son iguales salvo un múltiplo invertible.

13.1.3. Observación. *En un dominio de integridad se cumple $x \sim y$ si y solamente si $y = ux$ para algún $u \in R^\times$.*

Demostración. Si tenemos $x \sim y$, entonces $x \mid y$ e $y \mid x$; es decir, $x = vy$ e $y = ux$ para algunos $u, v \in R$. Luego, $x = uvx$, así que $x(1 - uv) = 0$. Esto implica que $x = 0$, y en este caso $y = 0$ y se tiene $y = 1 \cdot x$; o $uv = 1$, y en este caso $u \in R^\times$.

Viceversa, si $y = ux$ donde $u \in R^\times$, entonces $x = u^{-1}y$, así que $x \mid y$ e $y \mid x$. ■

13.1.4. Observación. *En un dominio de integridad, si $z \neq 0$, entonces $xz \mid yz$ implica $x \mid y$.*

Demostración. Si $yz = axz$ para algún a, entonces, puesto que $z \neq 0$, podemos cancelarlo y obtener $y = ax$. ■

Notamos que

1) $x \mid 0$ para todo $x \in R$;
2) si $x \mid y$ e $x \mid z$, entonces $x \mid (y + z)$;
3) si $x \mid y$, entonces $x \mid zy$ para todo $z \in R$.

Esto significa que los múltiplos de x forman un ideal. Es precisamente el ideal generado por x:

$$(x) = \{yx \mid y \in R\}.$$

13.1.5. Definición. Un ideal $I \subseteq R$ tal que $I = (x)$ para algún $x \in R$ se llama un **ideal principal**.

La relación de divisibilidad $x \mid y$ puede ser interpretada en términos de ideales (x) e (y).

13.1.6. Observación (Divisibilidad e ideales principales).

1) $x \mid y$ si y solamente si $(x) \supseteq (y)$.

2) $x \sim y$ si y solamente si $(x) = (y)$.

3) $x \in R^\times$ si y solamente si $(x) = R$.

4) si $x \mid y$, pero $y \nmid x$, entonces $(x) \supsetneq (y)$.

Demostración. En la parte 1), si $y = z\,x$, entonces $y \in (x)$, y luego $(y) \subseteq (x)$. Viceversa, si $(y) \subseteq (x)$, entonces $y = z\,x$ para algún $z \in R$. La parte 2) sigue inmediatamente de 1). La parte 3) sigue del hecho de que $x \in R^\times$ si y solamente si $x \sim 1$. ■

Notamos que la relación de divisibilidad es reflexiva y transitiva: para cualesquiera $x, y, z \in R$

$$x \mid x,$$
$$x \mid y,\ y \mid z \Longrightarrow x \mid z.$$

La relación $\sim$ es una relación de equivalencia: para cualesquiera $x, y, z \in R$ se cumple

$$x \sim x,$$
$$x \sim y \Longrightarrow y \sim x,$$
$$x \sim y,\ y \sim z \Longrightarrow x \sim z.$$

La relación de divisibilidad es una relación de **preorden** sobre R. Para que esto sea una relación de **orden**, falta la propiedad de antisimetría: $x \mid y$ e $y \mid x$ no implica $x = y$, sino que $x \sim y$ (por la definición). Esto significa que la divisibilidad es una relación de orden sobre las clases $R/\sim$.

Notamos que todo elemento y es divisible por 1 y por sí mismo, y en consecuencia por todo x tal que $x \sim 1$ (es decir, $x \in R^\times$) o $x \sim y$. Estos divisores de y son triviales. Un elemento que no tiene divisores no triviales se llama **irreducible**.

13.1.7. Definición. Un elemento $p \in R$ es **irreducible** si

1) $p \neq 0$ y $p \notin R^\times$,

2) $x \mid p$ implica que $x \in R^\times$ o $x \sim p$.

Se dice que un elemento $x \in R$ tal que $x \neq 0$ y $x \notin R^\times$ es **reducible** si existe un divisor no trivial $y \mid x$; es decir, $y \notin R^\times$ y $y \not\sim x$. Tenemos entonces cuatro clases disjuntas de elementos:

$$R = R^\times \sqcup \{0\} \sqcup \{\text{irreducibles}\} \sqcup \{\text{reducibles}\}.$$

13.1.8. Observación. *Un elemento $p \neq 0$ es irreducible si y solamente si el ideal (p) es **maximal entre los ideales principales**; es decir,*

1) $(p) \neq R$,

2) si $(p) \subseteq (x) \subseteq R$, entonces $(p) = (x)$ o $(x) = R$.

Demostración. Está claro a partir de 13.1.6. ■

El momento delicado de la teoría general es la distinción entre los elementos primos e irreducibles.

13.1.9. Definición. Un elemento $p \in R$ es **primo** si

1) $p \neq 0$ y $p \notin R^\times$,

2) para cualesquiera $x, y \in R$, si $p \mid xy$, entonces $p \mid x$ o $p \mid y$.

13.1.10. Ejemplo. En el anillo de los números enteros $\mathbb{Z}$ los elementos invertibles son ± 1. Se cumple $x \sim y$ si y solo si $y = \pm x$. Las clases de equivalencia en $\mathbb{Z}$ módulo la relación de equivalencia $\sim$ pueden ser representadas por los números no negativos.

Los elementos irreducibles son $\pm p$ donde $p = 2, 3, 5, 7, 11, \ldots$ es primo. Convenientemente, los elementos primos son los mismos. ▲

13.1.11. Observación. *Un elemento $p \neq 0$ es primo si y solamente si el ideal $(p) \subseteq R$ es primo.*

Demostración. La condición $p \notin R^\times$ es equivalente a $(p) \neq R$. La condición $p \mid xy \Rightarrow p \mid x$ o $p \mid y$ es equivalente a $xy \in (p) \Rightarrow x \in (p)$ o $y \in (p)$. ■

13.1.12. Observación. *Todo elemento primo es irreducible.*

Demostración. Supongamos que $p \in R$ es un elemento que no es irreducible. Esto significa que $p = xy$, donde $x, y \notin R^\times$ y $x \not\sim p$, $y \not\sim p$. Entonces, $p \mid xy$, pero $p \nmid x$ y $p \nmid y$, así que p no es primo. ■

En general, un elemento irreducible no tiene por qué ser primo.

13.1.13. Contraejemplo. En el anillo cociente $k[X, Y, Z]/(Z^2 - XY)$ la clase $\overline{Z}$ es irreducible. Sin embargo, se tiene $\overline{Z} \mid \overline{X}\,\overline{Y}$, aunque $\overline{Z} \nmid \overline{X}$ y $\overline{Z} \nmid \overline{Y}$. Esto significa que $\overline{Z}$ es un elemento irreducible, pero no es primo. ▲

13.1.14. Contraejemplo. Si $n \geq 3$ es un entero libre de cuadrados, entonces en el anillo

$$\mathbb{Z}[\sqrt{-n}] := \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$$

el número 2 es irreducible, pero no es primo. Véase el ejercicio 13.2. ▲

13.1.15. Definición. Para $x_1, \ldots, x_n \in R$ se dice que $d \in R$ es un **máximo común divisor** de $x_1, \ldots, x_n$ si

1) $d \mid x_1, \ldots, d \mid x_n$,

2) si para otro elemento $z \in R$ se cumple $z \mid x_1, \ldots, z \mid x_n$, entonces $z \mid d$.

(¡Note que la definición no afirma que tal d siempre existe!)

13.1.16. Observación. *Si para $x_1, \ldots, x_n \in R$ existe su máximo común divisor, entonces este está definido de modo único salvo $\sim$. En este caso se escribe por abuso de notación $d = \operatorname{mcd}(x_1, \ldots, x_n)$.*

Demostración. Si d e d' son mcd de $x_1, \ldots, x_n$, entonces la definición implica que $d \mid d'$ y $d' \mid d$. ■

Debido a la última observación, todas las identidades con mcd se entienden salvo $\sim$.

13.1.17. Ejemplo. Para los números enteros $\mathbb{Z}$, normalmente como $\operatorname{mcd}(x_1, \ldots, x_n)$ se toma un número positivo. ▲

13.1.18. Ejemplo. Tenemos $\operatorname{mcd}(x, 0) = x$ para cualquier x. En efecto, $x \mid x$ y $x \mid 0$. La segunda condición de la definición de mcd se cumple trivialmente. De la misma manera, se ve que $\operatorname{mcd}(x, x) = x$ para cualquier x. ▲

13.1.19. Observación. *El mcd tiene las siguientes propiedades.*

1) $\operatorname{mcd}(x, y) = x$ *si y solamente si* $x \mid y$*;*

2) si $\operatorname{mcd}(x, y)$ *existe, entonces* $\operatorname{mcd}(y, x)$ *también existe y se tiene* $\operatorname{mcd}(x, y) = \operatorname{mcd}(y, x)$*;*

3) $\operatorname{mcd}(\operatorname{mcd}(x, y), z) = \operatorname{mcd}(x, \operatorname{mcd}(y, z)) = \operatorname{mcd}(x, y, z)$*, en el sentido de que si uno de los tres elementos existe, los otros dos también existen y todos son iguales.*

Demostración. Las primeras dos propiedades son evidentes de la definición. Para la tercera, se puede notar que las propiedades que definen a $\operatorname{mcd}(\operatorname{mcd}(x, y), z)$ y $\operatorname{mcd}(x, \operatorname{mcd}(y, z))$ corresponden a la propiedad que define a $\operatorname{mcd}(x, y, z)$. ■

13.1.20. Lema. *Se cumple* $\operatorname{mcd}(zx, zy) = z \operatorname{mcd}(x, y)$ *(es decir, si uno de estos elementos existe, entonces el otro también existe y son asociados).*

Demostración. Si $z = 0$, esto es obvio, así que podemos asumir que $z \neq 0$.

Sea $d = \operatorname{mcd}(x, y)$. Entonces, $zd \mid zx$ y $zd \mid zy$, así que $zd \mid \operatorname{mcd}(zx, zy)$. Viceversa, puesto que $z \mid zx$ y $z \mid zy$, se tiene $z \mid \operatorname{mcd}(zx, zy)$, tenemos $\operatorname{mcd}(zx, zy) = zc$ para algún $c \in R$. Esto significa que $zc \mid zx$ y $zc \mid zy$. Pero puesto que $z \neq 0$, esto implica que $c \mid x$ y $c \mid y$, así que $c \mid d$, y luego $zc = \operatorname{mcd}(zx, zy) \mid zd$. ■

De la misma manera se define el mínimo común múltiplo $\operatorname{mcm}(x, y)$.

13.1.21. Definición. Para $x_1, \ldots, x_n \in R$ se dice que $m \in R$ es un **mínimo común múltiplo** de $x_1, \ldots, x_n$ si

1) $x_1 \mid m, \ldots, x_n \mid m$,

2) si para otro elemento $z \in R$ se cumple $x_1 \mid z, \ldots, x_n \mid z$, entonces $m \mid z$.

De nuevo, estas condiciones definen a m de modo único salvo la relación $\sim$, y normalmente se escribe $m = \operatorname{mcm}(x_1, \ldots, x_n)$.

13.1.22. Ejemplo. Tenemos $\operatorname{mcm}(x, 0) = 0$ para todo $x \in R$. En efecto, $x \mid 0$ y $0 \mid 0$. Luego, si hay otro elemento z tal que $x \mid z$ y $0 \mid z$, lo último implica que $z = 0$, y de hecho $0 \mid 0$. ▲

El mcm satisface las mismas propiedades que el mcd.

13.1.23. Observación.

1) $\operatorname{mcm}(x, y) = x$ *si y solamente si* $y \mid x$.
   En particular, $\operatorname{mcm}(x, x) = \operatorname{mcd}(x, 1) = x$.
2) *Si* $\operatorname{mcm}(x, y)$ *existe, entonces* $\operatorname{mcm}(y, x)$ *también existe y se tiene* $\operatorname{mcm}(x, y) = \operatorname{mcm}(y, x)$.
3) $\operatorname{mcm}(\operatorname{mcm}(x, y), z) = \operatorname{mcm}(x, \operatorname{mcm}(y, z)) = \operatorname{mcm}(x, y, z)$, *en el sentido de que si uno de los tres elementos existe, los otros dos también existen y todos son iguales.*

13.1.24. Proposición. *Si para* $x, y \in R$ *existe uno de los* $\operatorname{mcd}(x, y)$ *o* $\operatorname{mcm}(x, y)$, *entonces existe el otro y se cumple*

$$\operatorname{mcd}(x, y)\ \operatorname{mcm}(x, y) = xy.$$

Demostración. Supongamos por ejemplo que existe $d = \operatorname{mcd}(x, y)$. El caso de $x = y = 0$ es trivial y podemos descartarlo desde el principio. Entonces, se puede asumir que $d \neq 0$.

En particular, esto significa que $d \mid x$ e $d \mid y$. Escribamos

$$x = d\,x', \quad y = d\,y'$$

para algunos $x', y' \in R$. Definamos

$$m := d\,x'\,y'.$$

Tenemos $dm = xy$ y nos gustaría probar que m satisface la propiedad de $\operatorname{mcm}(x, y)$. Primero,

$$m = x\,y' = x'\,y,$$

así que $x \mid m$ e $y \mid m$. Sea z otro elemento tal que $x \mid z$ e $y \mid z$. Necesitamos deducir que $m \mid z$. Notamos que según 13.1.20

$$d = \operatorname{mcd}(x, y) = \operatorname{mcd}(dx', dy') = d \cdot \operatorname{mcd}(x', y'),$$

y luego

$$\operatorname{mcd}(x', y') = 1.$$

Pero en este caso

$$\operatorname{mcd}(zx', zy') = z\ \operatorname{mcd}(x', y') = z.$$

Luego, $m \mid zx'$ y $m \mid zy'$, y por lo tanto $m \mid z$. ■

13.2 Dominios de ideales principales

lección 18
26.09.18

13.2.1. Definición. Sea R un dominio de integridad. Se dice que R es un **dominio de ideales principales** si R es un dominio de integridad y todo ideal $I \subseteq R$ es principal; es decir $I = (x)$ para algún $x \in R$.

13.2.2. Ejemplo. Todo cuerpo es obviamente un dominio de ideales principales.

El anillo $\mathbb{Z}$ es un dominio de ideales principales. Esto ya no es tan obvio y se demuestra usando la división con resto; véase el apéndice A. Usando las mismas ideas, vamos a ver un poco más adelante que el anillo de polinomios $k[X]$ (donde k es un cuerpo) y el anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ son también dominios de ideales principales.

Los anillos $\mathbb{Z}\left[\frac{1}{n}\right]$ y $\mathbb{Z}_{(p)}$ para p primo son también dominios de ideales principales. Esto sigue de la descripción de los ideales en la localización y el hecho de que $\mathbb{Z}$ es un dominio de ideales principales. ▲

13.2.3. Ejemplo. El anillo de polinomios en dos variables $k[X,Y]$ no es un dominio de ideales principales. Por ejemplo, tenemos el ideal (X,Y) que no puede ser generado por un elemento.

En efecto, asumamos que $(X,Y) = (f)$ para algún polinomio $f \in k[X,Y]$. Entonces, $(X) \subseteq (f)$ y $(Y) \subseteq (f)$, pero esto significa que $f \mid X$ y $f \mid Y$. Sin embargo, los elementos X e Y son irreducibles y esto implica que f es invertible en $k[X,Y]$, de donde $(f) = k[X,Y]$. Contradicción. ▲

13.2.4. Ejemplo. El anillo de polinomios $\mathbb{Z}[X]$ no es un dominio de ideales principales. Por ejemplo, el ideal (p,X) donde p es un número primo no puede ser generado por un elemento. Notamos que este ideal es propio:

$$(p,X) = \{p\,f + X\,g \mid f,g \in \mathbb{Z}[X]\} = \{a_0 + a_1\,X + \cdots + a_d\,X^d \mid a_0,a_1,\ldots,a_d \in \mathbb{Z},\ p \mid a_0\}.$$

En efecto, el ideal (p,X) es maximal. De hecho, consideremos el homomorfismo sobreyectivo de anillos

$$\begin{aligned} \mathbb{Z}[X] &\twoheadrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}, \\ f &\mapsto f(0) \pmod p \end{aligned}$$

—este homomorfismo primero evalúa un polinomio en 0 y luego reduce el resultado módulo p. El núcleo de este homomorfismo viene dado por los polinomios con el término constante divisible por p, pero esto es precisamente (p,X). El primer teorema de isomorfía nos permite concluir que $\mathbb{Z}[X]/(p,X) \cong \mathbb{Z}/p\mathbb{Z}$, lo que es un cuerpo.

Ahora asumamos que $(p,X) = (f)$ para algún polinomio $f \in \mathbb{Z}[X]$. En particular, esto quiere decir que $(p) \subseteq (f)$ y por ende $f \mid p$, así que $f = \pm 1$ o $\pm p$. Si $f = \pm p$, el ideal $(f) = p\,\mathbb{Z}[X]$ no puede contener a X. Si $f = \pm 1$, entonces $(f) = \mathbb{Z}[X]$. Contradicción. ▲

En general, es muy difícil encontrar el número mínimo posible de generadores para un ideal.

13.2.5. Proposición. *Sea R un dominio de ideales principales que no es un cuerpo. Entonces, los ideales maximales en R son precisamente los ideales primos no nulos.*

(Note que la hipótesis de que R no sea un cuerpo es importante: ¡en un cuerpo el ideal nulo es maximal!)

Demostración. Si $(p) \subset R$ un ideal primo no nulo, entonces $p \in R$ es un elemento primo (véase 13.1.11). Si tenemos $(p) \subseteq (x)$ para otro ideal, entonces $x \mid p$, lo que implica $x \in R^\times$ o $x \sim p$; es decir, $(x) = R$ o $(x) = (p)$. ■

13.2.6. Proposición. *En un dominio de ideales principales todo elemento irreducible es primo.*

Demostración. Si $p \in R$ es irreducible, entonces el ideal (p) es maximal entre los ideales principales. Pero por la hipótesis *todos* los ideales son principales, así que (p) es un ideal maximal en R. Todo ideal maximal es primo, lo que significa que p es un elemento primo. ■

13.2.7. Proposición (Relación de Bézout). *En todo dominio de integridad R tenemos*

1) *si $(x_1,\ldots,x_n) = (d)$, entonces $d = \operatorname{mcd}(x_1,\ldots,x_n)$;*

2) si $(x_1) \cap \cdots \cap (x_n) = (m)$, *entonces* $m = \operatorname{mcm}(x_1, \ldots, x_n)$.

Además, si R es un dominio de ideales principales, entonces mcd *y* mcd *siempre existen. En este caso se tiene*

1) $(x_1, \ldots, x_n) = (d)$, *donde* $d = \operatorname{mcd}(x_1, \ldots, x_n)$;

2) $(x_1) \cap \cdots \cap (x_n) = (m)$, *donde* $m = \operatorname{mcm}(x_1, \ldots, x_n)$.

Demostración. Vamos a ver el caso del mcd; el caso del mcm es parecido.

Si $(x_1, \ldots, x_n) = (d)$, entonces $(x_i) \subseteq (d)$ para todo $i = 1, \ldots, n$, lo que significa que $d \mid x_i$. Supongamos que $z \mid x_i$ para todo i. Tenemos entonces

$$c_1 x_1 + \cdots + c_n x_n = d$$

para algunos c_i y luego $z \mid d$.

Ahora si R es un dominio de ideales principales, sea $d = \operatorname{mcd}(x_1, \ldots, x_n)$. Tenemos $d \mid x_i$ para todo i; es decir, $(x_i) \subseteq (d)$. El ideal $(x_1, \ldots, x_n)$ es el ideal mínimo tal que $(x_i) \subseteq (x_1, \ldots, x_n)$ para todo i, así que $(x_1, \ldots, x_n) \subseteq (d)$. Para ver la otra inclusión, notamos que $(x_1, \ldots, x_n) = (z)$ para algún $z \in R$, puesto que R es un dominio de ideales principales. Luego, $z = \operatorname{mcd}(x_1, \ldots, x_n)$ por la primera parte, así que $(z) = (d)$. ■

La igualdad $(x_1, \ldots, x_n) = (d)$ donde $d = \operatorname{mcd}(x_1, \ldots, x_n)$ significa que en un dominio de ideales principales R, el máximo común divisor de los x_i puede ser expresado como una combinación R-lineal de los x_i. Esto se llama la relación de Bézout.

13.2.8. Corolario (Elementos coprimos). *En un dominio de ideales principales,* $\operatorname{mcd}(x, y) = 1$ *si y solamente si* $(x, y) = R$.

13.2.9. Ejemplo. En el anillo $k[X, Y]$ los elementos X e Y son irreducibles y son divisibles solamente por las constantes no nulas, así que $\operatorname{mcd}(X, Y) = 1$. Sin embargo, $(X, Y) \neq k[X, Y]$. Esto demuestra una vez más que el anillo $k[X, Y]$ no es un dominio de ideales principales.

De la misma manera, en $\mathbb{Z}[X]$ se tiene $\operatorname{mcd}(p, X) = 1$, aunque $(p, X) \neq \mathbb{Z}[X]$. ▲

13.3 Dominios de factorización única

13.3.1. Definición. Se dice que un dominio de integridad R es un **dominio de factorización única** si todo elemento no nulo $x \in R$ puede ser descompuesto en factores irreducibles y esta descomposición es única salvo el orden de los múltiplos y la relación de equivalencia $\sim$.

En otras palabras, para dos descomposiciones

$$x = u\, p_1 \cdots p_s = v\, q_1 \cdots q_t$$

donde $u, v \in R^\times$ y p_i, q_j son irreducibles, se tiene necesariamente $s = t$, y después de una permutación de los múltiplos, se cumple $p_i \sim q_i$ para todo $1 \leq i \leq s$.

13.3.2. Comentario. En la factorización $x = u\, p_1 \cdots p_s$ *no* se supone que entre los p_i no hay repeticiones. Diferentes p_i y p_j pueden ser asociados.

13.3.3. Ejemplo. Todo cuerpo es trivialmente un dominio de factorización única: todo elemento no nulo es invertible y la condición de la definición es vacía. ▲

13.3.4. Ejemplo. El anillo de los enteros $\mathbb{Z}$ es un dominio de factorización única. Este resultado se conoce como el **teorema fundamental de aritmética** y fue probado rigurosamente por primera vez por Gauss. De hecho, eventualmente en este capítulo lo vamos a probar otra vez más. ▲

Para probar que algo es un dominio de factorización única, necesitamos ciertas herramientas especiales. Lo que es fácil es probar es que un anillo específico no posea factorizaciones únicas: basta encontrar dos diferentes factorizaciones del mismo elemento.

13.3.5. Ejemplo. En el anillo $\mathbb{Z}[\sqrt{-5}]$ definamos la norma por

$$N(a+b\sqrt{-5}) := (a+b\sqrt{-5})\,(a-b\sqrt{-5}) = a^2+5\,b^2.$$

Esto es una función multiplicativa:

$$N(xy) = N(x)\,N(y) \quad \text{para cualesquiera } x, y \in \mathbb{Z}[\sqrt{-5}].$$

Ahora si $x \mid y$, entonces $y = zx$ y $N(y) = N(z)\,N(x)$, así que $N(x) \mid N(y)$. Se sigue que los elementos invertibles deben tener norma 1, así que $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$. Notamos que si $x \mid y$ donde $N(x) = N(y)$, entonces $y = zx$ donde $N(z) = 1$, así que $x \sim y$; es decir, $x = \pm y$.

Notamos que los números 2 y 3 no pueden ser expresados como $a^2 + 5\,b^2$, así que en $\mathbb{Z}[\sqrt{-5}]$ no hay elementos de esta norma. Esto nos lleva a las siguientes conclusiones.

1) $1 \pm \sqrt{-5}$ es irreducible. En efecto, si $x \mid (1 \pm \sqrt{-5})$, entonces $N(x) \mid 6$ y luego $N(x) = 1$ o $N(x) = 6$. En el primer caso, $x \in \mathbb{Z}[\sqrt{-5}]^\times$; en el segundo caso, $x \sim 1 \pm \sqrt{-5}$.

2) 2 es irreducible: si $x \mid 2$, entonces $N(x) \mid 4$ y $N(x) = 1$ o 4 y tenemos dos casos parecidos.

3) 3 es irreducible. Si $x \mid 3$, entonces $N(x) \mid 9$ y $N(x) = 1$ o 9.

Ahora la identidad

$$6 = 2 \cdot 3 = (1+\sqrt{-5})\,(1-\sqrt{-5})$$

significa que 6 puede ser expresado de dos maneras diferentes como un producto de elementos irreducibles. ▲

lección 19
27.09.18

13.3.6. Ejemplo. Consideremos el anillo $\mathbb{Z}[\sqrt{-3}]$. La norma viene dada por $N(a+b\sqrt{-3}) = a^2+3\,b^2$. Los elementos de norma 1 son ± 1 y enotratonces $\mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}$. Está claro que no existen elementos de norma 2.

Ahora 2 es un elemento irreducible: si $x \mid 2$, entonces $N(x) \mid 4$, lo que implica $N(x) = 1$ o 4. El elemento $1 \pm \sqrt{-3}$ también tiene norma 4 y es irreducible por las mismas razones. La identidad

$$4 = 2 \cdot 2 = (1+\sqrt{-3})\,(1-\sqrt{-3}) \tag{13.1}$$

demuestra que $\mathbb{Z}[\sqrt{-3}]$ no es un dominio de factorización única.

Sin embargo, se puede considerar el anillo más grande

$$\mathbb{Z}[\omega], \quad \omega := \frac{1+\sqrt{-3}}{2}.$$

La norma es

$$N\,(a+b\,\omega) = \left(a+b\,\frac{1+\sqrt{-3}}{2}\right)\left(a+b\,\frac{1-\sqrt{-3}}{2}\right) = a^2+ab+b^2.$$

Ahora hay más elementos de norma 1: son

$$\pm 1, \quad \pm\omega, \quad \pm(1-\omega),$$

y de hecho son precisamente las raíces de la unidad de orden 6:

$$(1-\omega)^2 = -\omega, \quad (1-\omega)^3 = -1.$$

Ahora podemos volver a nuestra factorización de 4 en (13.1). La fórmula se vuelve

$$4 = 2 \cdot 2 = 2\,\omega \cdot 2\,(1-\omega).$$

Pero ω y $1-\omega$ son invertibles, así que esta fórmula ya no es un ejemplo de diferentes factorizaciones. En efecto, el anillo $\mathbb{Z}[\omega]$ es un dominio de factorización única, pero lo vamos a ver un poco más adelante usando otras herramientas. ▲

El descubrimiento de anillos que no son dominios de factorización única fue uno de los sucesos más importantes en la matemática del siglo XIX.

13.3.7. Lema. *En un anillo noetheriano, todo elemento no invertible es divisible por un elemento irreducible.*

Demostración. Sea R un anillo noetheriano y $x \in R$ un elemento tal que $x \neq 0$ y $x \notin R^\times$. Si x es irreducible, no hay nada que probar. Si x es reducible, entonces podemos escribir $x = x_1\,y_1$ donde x_1 es un divisor no trivial: $x_1 \notin R^\times$ y $x_1 \not\sim x$. Si x_1 es irreducible, la prueba está terminada. En el caso contrario, podemos escribir $x_1 = x_2\,y_2$ donde $x_2 \notin R^\times$ y $x_2 \not\sim x_1$. Continuando de esta manera, se obtienen elementos $x_1, x_2, x_3, \ldots$ tales que

$$x_1 \mid x, \quad x_2 \mid x_1, \quad x_3 \mid x_2, \quad x_4 \mid x_3, \quad \ldots,$$

lo que nos da una cadena de ideales

$$(x) \subseteq (x_1) \subseteq (x_2) \subseteq (x_3) \subseteq (x_4) \subseteq \cdots \subset R.$$

Pero R es noetheriano por hipótesis, así que en algún momento la cadena se estabiliza, lo que significa que $(x_n) = (x_{n+1})$ para n suficientemente grande; es decir, $x_n \sim x_{n+1}$. Podemos concluir que el proceso siempre termina y nos da un factor irreducible de x. ■

13.3.8. Lema. *Sea R un anillo noetheriano. Todo elemento $x \neq 0$ posee una **factorización en irreducibles**; es decir, puede ser escrito como*

$$x = u\,p_1 \cdots p_n$$

donde $u \in R^\times$ y $p_1, \ldots, p_n \in R$ son elementos irreducibles.

Demostración. Sea R un anillo noetheriano. Si para $x \neq 0$ se tiene $x \in R^\times$ o x es irreducible, no hay que probar nada. En el caso contrario, por el resultado anterior, podemos escribir $x = p_1\,x_1$ donde p_1 es irreducible. Luego, si $x_1 \in R^\times$ o x_1 es irreducible, la prueba está terminada. En el caso contrario, escribamos $x_1 = p_2\,x_2$, etcétera. Esto nos da una cadena de ideales

$$(x) \subseteq (x_1) \subseteq (x_2) \subseteq (x_3) \subseteq \cdots \subset R.$$

Esta cadena necesariamente se estabiliza, lo que significa que $x_n \sim x_{n+1}$ para n suficientemente grande, así que x_n es irreducible. Tenemos entonces

$$x = p_1 x_1 = p_1 p_2 x_2 = \cdots = p_1 \cdots p_n x_n$$

donde los factores de la última expresión son irreducibles. ■

Para probar que algo es un dominio de factorización única, se puede usar el siguiente criterio.

13.3.9. Teorema. *Sea R un dominio de integridad donde todo elemento admite factorización en elementos irreducibles. Entonces, R es un dominio de factorización única si y solo si todo elemento irreducible es primo.*

Demostración. Supongamos primero que R es un dominio de factorización única. Sea p un elemento irreducible. Hay que probar que p es primo. Si $p \mid xy$, se tiene $xy = pz$ para algún $z \in R$. Factoricemos x, y, z en elementos irreducibles:

$$x = u\,p_1 \cdots p_r, \quad y = v\,p_{r+1} \cdots p_s, \quad z = w\,q_1 \cdots q_t,$$

donde $u, v, w \in R^\times$, $p_1, \ldots, p_s, q_1, \ldots, q_t$ son irreducibles. Tenemos

$$uv\,p_1 \cdots p_s = w\,p\,q_1 \cdots q_t.$$

Por la unicidad de factorizaciones, tenemos $p \sim p_i$ para algún $1 \leq i \leq r$. Esto quiere decir que $p \mid x$ o $p \mid y$.

Ahora supongamos que todo elemento irreducible es primo. En este caso la hipótesis nos dice que todo elemento admite una factorización en elementos primos

$$x = u\,p_1 \cdots p_s.$$

Falta ver que estas factorizaciones son únicas. Sea entonces

$$x = v\,q_1 \cdots q_t$$

otra factorización. Sin pérdida de generalidad, asumamos que $s \leq t$ y procedamos por inducción sobre s.

Si $s = 0$, no hay que probar nada: $u = v\,q_1 \cdots q_t$ para $t > 0$ implica que $q_1 \cdots q_t = uv^{-1}$ es invertible, pero luego todo q_i es invertible, lo que no es el caso, puesto que los q_i son primos. Entonces, $t = 0$.

Asumamos que el resultado es cierto para $s - 1$ factores. Consideremos la igualdad

$$u\,p_1 \cdots p_s = v\,q_1 \cdots q_t.$$

Dado que p_s es primo y $p_s \mid v\,q_1 \cdots q_t$, tenemos $p_s \mid q_i$ para algún $1 \leq i \leq t$ (notamos que p_s, siendo primo, no puede dividir al elemento invertible v). Después de una renumeración de los múltiplos, podemos asumir que $p_s \mid q_t$. Pero q_t es también primo, así que $p_s \sim q_t$; es decir, $p_s = w\,q_t$ para algún $w \in R^\times$. Ahora en la identidad

$$u\,p_1 \cdots p_{s-1}\,(w\,q_t) = v\,q_1 \cdots q_{t-1}\,q_t$$

podemos cancelar q_t y obtener

$$uw\,p_1 \cdots p_{s-1} = v\,q_1 \cdots q_{t-1}.$$

Por la hipótesis de inducción, se tiene $s - 1 = t - 1$ y $p_i \sim q_i$ para todo $1 \leq i \leq s - 1$, después de una permutación de los múltiplos. ■

13.3.10. Corolario. *Todo dominio de ideales principales es un dominio de factorización única.*

Demostración. Siendo un dominio de ideales principales, en particular el anillo es noetheriano y por ende admite factorización en elementos irreducibles según 13.3.8. En 13.2.6 hemos probado en que en un dominio de ideales principales todo elemento irreducible es primo. ■

Hay muchos ejemplos de dominios de factorización única que no son dominios de ideales principales. Por ejemplo, el anillo de polinomios en n variables $k[X_1, \ldots, X_n]$ donde k es un cuerpo es un dominio de factorización única. Lo vamos a probar más adelante. Nuestro próximo objetivo es obtener algún método para ver que ciertos anillos son dominios de ideales principales. Para esto nos va a servir la noción de **dominios euclidianos**.

13.4 Dominios euclidianos

Un dominio euclidiano es un dominio de integridad que admite el algoritmo de división con resto.

13.4.1. Definición. Se dice que un dominio de integridad R es un **dominio euclidiano** si sobre R existe una función $\delta\colon R \setminus \{0\} \to \mathbb{N}$ (llamada **norma euclidiana**) que satisface la siguiente propiedad. Para todo $x, y \in R$, $y \neq 0$ existen $q, r \in R$ tales que $x = qy + r$, donde $r = 0$ o $\delta(r) < \delta(y)$.

13.4.2. Comentario. No se supone que los elementos q, r son únicos.

El ejemplo primordial de dominios euclidianos fue estudiado por Euclides en sus "Elementos".

13.4.3. Ejemplo. El anillo de los enteros $\mathbb{Z}$ es un dominio euclidiano respecto al valor absoluto $\delta(x) := |x|$. En efecto, dados $m, n \in \mathbb{Z}$, $n \neq 0$, podemos considerar el conjunto

$$X := \{m - xn \mid x \in \mathbb{Z}\}.$$

Notamos que este conjunto contiene elementos no negativos. Sea $r = m - qn$ el elemento mínimo no negativo en X. Si tenemos $r \geq |n|$, podemos considerar dos casos:

1) si $n > 0$, entonces $r = m - qn \geq n$, así que

$$0 \leq m - (q+1)\, n < r.$$

2) si $n < 0$, entonces $r = m - qn \geq -n$, así que

$$0 \leq m - (q-1)\, n < r.$$

Pero ambos casos contradicen nuestra elección de r. Entonces, necesariamente $0 \leq r < |n|$. ▲

13.4.4. Ejemplo. Sea k un cuerpo. El anillo de polinomios en una variable $k[X]$ es un dominio euclidiano respecto al grado $\delta(f) := \deg f$. Sean $f, g \in k[X]$ dos polinomios, $g \neq 0$. Nos gustaría probar que existen polinomios $q, r \in k[X]$ tales que

$$f = qg + r, \quad r = 0 \text{ o } \deg r < \deg g.$$

Si $\deg f < \deg g$, podemos tomar $q = 0$ y $r = f$. En el caso contrario, procedamos por inducción sobre $\deg f$. Si tenemos

$$f = a_d\, X^d + a_{d-1}\, X^{d-1} + \cdots + a_1\, X + a_0,$$

donde $a_d \neq 0$ y

$$g = b_n\, X^n + b_{n-1}\, X^{n-1} + \cdots + b_1\, X + b_0,$$

donde $b_n \neq 0$ y $d \geq n$, consideremos

$$f' := f - a_d\, b_n^{-1}\, X^{d-n}\, g.$$

Notamos que $\deg f' < \deg f$. Por inducción, podemos escribir

$$f' = q'g + r, \quad r = 0 \text{ o } \deg r < \deg g.$$

Tenemos

$$f = (q' + a_d\, b_n^{-1}\, X^{d-n})\, g + r.$$

De hecho, lo que acabamos de describir es el algoritmo de división habitual. Notamos que es importante que los coeficientes de los polinomios estén en un cuerpo. En general, este argumento funciona si el coeficiente mayor de g es invertible; por ejemplo si es igual a 1 (en este caso se dice que g es un polinomio **mónico**). ▲

13.4.5. Comentario. El ejemplo del anillo $k[X]$ es la única razón por que en la definición el caso de $r = 0$ se considera por separado. Tenemos $\deg(0) = -\infty$, pero nos gustaría usar el grado como la norma euclidiana.

13.4.6. Ejemplo. El anillo de los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ es un dominio euclidiano respecto a la norma

$$N(a + b\sqrt{-1}) := (a + b\sqrt{-1})\,(a - b\sqrt{-1}).$$

En efecto, dados dos elementos $x, y \in \mathbb{Z}[\sqrt{-1}]$, $y \neq 0$, podemos dividir x por y en el cuerpo de fracciones $\mathbb{Q}(\sqrt{-1})$:

$$\frac{x}{y} = s + t\,\sqrt{-1} \quad \text{para algunos } s, t \in \mathbb{Q}.$$

Ahora podemos escoger $m, n \in \mathbb{Z}$ tales que

$$|s - m| \leq \frac{1}{2}, \quad |t - n| \leq \frac{1}{2}.$$

Pongamos

$$q := m + n\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$$

y

$$r := x - qy = (s + t\,\sqrt{-1})\,y - y\,(m + n\sqrt{-1}) = y\,(s - m + (t - n)\sqrt{-1}).$$

Por la multiplicatividad de la norma,

$$N(r) = N(y)\,N(s - m + (t - n)\,\sqrt{-1}) = N(y)\left((s - m)^2 + (t - n)^2\right) \leq \frac{1}{2}\,N(y).$$

En particular,

$$x = qy + r, \quad 0 \leq N(r) < N(y).$$

▲

La razón de ser de la noción de dominio euclidiano es el siguiente resultado.

13.4.7. Teorema. *Todo dominio euclidiano es un dominio de ideales principales.*

Demostración. Sea R un dominio euclidiano y sea $I \subseteq R$ un ideal. Necesitamos probar que I es un ideal principal. Si $I = (0)$, no hay que probar nada. Si $I \neq (0)$, sea $x \in I$ un elemento con la norma euclidiana $\delta(x)$ mínima posible. Tenemos $(x) \subseteq I$. Supongamos que existe un elemento $y \in I$ tal que $y \notin (x)$. Esto quiere decir que y no puede ser escrito como qx para algún $q \in R$. Podemos dividir y por x con resto: tenemos

$$y = qx + r, \quad r \neq 0,\ \delta(r) < \delta(x)$$

para algunos $q, r \in R$. Sin embargo, $r = y - qx \in I$ y esto contradice nuestra elección de x. Podemos concluir que $I = (x)$. ■

13.4.8. Corolario. *Todo dominio euclidiano es un dominio de factorización única.*

En general, existen dominios de ideales principales que no son dominios euclidianos. Sin embargo, no es fácil encontrar un ejemplo específico: hay que probar que cierto dominio de ideales principales no admite *ninguna* norma euclidiana.

13.4.9. Ejemplo (Para el lector interesado). Sea R un dominio euclidiano que no es un cuerpo. Sea $x \in R$ un elemento no nulo y no invertible con el mínimo posible valor $\delta(x)$. Esto implica que para cualquier elemento $y \in R$ tenemos

$$y = qx + r, \quad \text{donde } r = 0 \text{ o } \delta(r) < \delta(x).$$

Por nuestra elección de x, esto significa que hay dos posibilidades: $x \mid y$ o $r \in R^\times$.

Ahora consideremos el anillo

$$\mathbb{Z}[\omega], \quad \omega := \frac{1+\sqrt{-19}}{2}.$$

Al analizar la norma

$$N(a + b\,\omega) := (a + b\,\omega)\,(a + b\,\overline{\omega}) = a^2 + ab + 5\,b^2$$

se ve que $\mathbb{Z}[\omega]^\times = \{\pm 1\}$ y que en $\mathbb{Z}[\omega]$ no hay elementos de norma 2 o 3. Esto implica que los números 2 y 3 son irreducibles en $\mathbb{Z}[\omega]$.

Ahora si $\mathbb{Z}[\omega]$ fuera un dominio euclidiano, entonces tendríamos algún elemento no nulo y no invertible $x \in \mathbb{Z}[\omega]$ tal que para todo $y \in \mathbb{Z}[\omega]$ se cumple $x \mid y$, o se puede escribir $y = qx + r$ donde $r = \pm 1$. Es decir, x siempre debe dividir a y o $y \pm 1$. Primero tomemos $y = 2$.

1) Si $x \mid 2$, entonces necesariamente $x = \pm 2$ (como notamos, 2 es irreducible y x no es invertible).

2) Si $x \mid (2+1)$, entonces $x = \pm 3$ (de nuevo, 3 es irreducible y x no es invertible).

3) El caso $x \mid (2-1)$ no es posible, puesto que x no es invertible.

Entonces, necesariamente $x = \pm 2$ o ± 3, así que $N(x) = 4$ o 9. Tomemos ahora $y = \omega$. Hay tres casos, pero cada uno de ellos se descarta:

1) $x \nmid \omega$, puesto que $N(\omega) = 5$;

2) $x \nmid (1+\omega)$, puesto que $N(1+\omega) = 7$;

3) $x \nmid (-1+\omega)$, puesto que $N(-1+\omega) = 5$.

Podemos concluir que $\mathbb{Z}[\omega]$ no es un dominio euclidiano. Sin embargo, se puede probar que es un dominio de ideales principales. Para una prueba directa, véase [DF2004, §8.2], pero esto surge de ciertos cálculos en la teoría de números algebraica que vamos a explicar brevemente un poco más adelante.

En efecto, en lugar de $\frac{1+\sqrt{-19}}{2}$ también funcionaría

$$\omega = \frac{1+\sqrt{-43}}{2}, \quad \frac{1+\sqrt{-67}}{2}, \quad \frac{1+\sqrt{-163}}{2}.$$

▲

Los ejemplos como el de arriba nada más demuestran que la noción de dominio euclidiano no tiene ningún sentido profundo; es puramente utilitaria y se ocupa solo para probar que ciertos anillos son dominios de ideales principales. En práctica no es fácil demostrar que algo es un dominio euclidiano (salvo los casos básicos como $\mathbb{Z}$ y $k[X]$), ni que no lo es.

13.5 Valuaciones p-ádicas

lección 20
02.10.18

Sea R un dominio de factorización única. Todo elemento no nulo $x \in R$ está definido, salvo un múltiplo invertible, por sus factores primos. Es conveniente juntar factores repetidos y escribir x como $u\, p_1^{k_1} \cdots p_n^{k_n}$ donde los p_i son primos no asociados entre sí (es decir, $p_i \not\sim p_j$ para $i \neq j$). El exponente k de un factor primo p se llama la **valuación p-ádica** de x.

13.5.1. Definición. Sea $p \in R$ un elemento primo. Para un elemento $x \in R$, $x \neq 0$ definamos

$$v_p(x) := \text{máx}\{k \mid p^k \mid x\}$$

y para el elemento nulo pongamos

$$v_p(0) := \infty.$$

El número $v_p(x)$ se llama la **valuación p-ádica** de x.

En otras palabras, para un elemento no nulo se tiene $v_p(x) = n$ precisamente cuando se puede escribir $x = p^n\, x'$, donde $p \nmid x'$. La factorización única en R significa que para todo $x \neq 0$ se cumple

$$x \sim \prod_p p^{v_p(x)},$$

donde el producto es sobre las clases de equivalencia de los elementos primos módulo la relación $\sim$. Notamos que en realidad este producto es finito, puesto que $v_p(x) = 0$ para todo p, salvo un número finito.

13.5.2. Ejemplo. Tenemos

$$v_2(60) = 2, \quad v_3(60) = 1, \quad v_5(60) = 1$$

y $v_p(60) = 0$ para $p \neq 2, 3, 5$. ▲

13.5.3. Proposición. *La valuación p-ádica satisface las siguientes propiedades.*

V1) $v_p(x) = \infty$ *si y solamente si* $x = 0$.

V2) $v_p(xy) = v_p(x) + v_p(y)$.

V3) $v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

Demostración. La parte V1) hace parte de la definición. Para la parte V2), si $x = 0$ o $y = 0$, la igualdad es evidente. Ahora si x e y no son nulos y $v_p(x) = m$ y $v_p(y) = n$, esto significa que

$$x = p^m\, x', \quad y = p^n\, y',$$

donde $p \nmid x'$ y $p \nmid y'$. Luego,

$$xy = p^{m+n}\, x'y',$$

donde $p \nmid x'y'$, así que $v_p(xy) = m + n$. De la misma manera, la parte V3) es evidente cuando $x = 0$ o $y = 0$. Para x e y no nulos, de nuevo podemos asumir que $v_p(x) = m$ y $v_p(y) = n$, donde sin pérdida de generalidad $m \leq n$. Luego,

$$x + y = p^m\, x' + p^n\, y' = p^m\, (x' + p^{n-m}\, y'),$$

entonces $p^m \mid (x + y)$ y por ende $v_p(x + y) \geq m$. ■

13.5.4. Observación. *Si $u \in R^\times$, entonces $v_p(u) = 0$ y $v_p(ux) = x$ para todo $x \in R$. En particular, $v_p(-x) = v_p(x)$ para todo $x \in R$.*

Demostración. Si $u \in R^\times$, entonces u no es divisible por ningún primo, así que $v_p(u) = 0$ para cualquier p. Luego,

$$v_p(ux) = v_p(u) + v_p(x) = 0 + v_p(x) = v_p(x).$$

■

Nos conviene extender las valuaciones p-ádicas al cuerpo de fracciones de R.

13.5.5. Definición. Sean R un dominio de factorización única, $p \in R$ un elemento primo y K el cuerpo de fracciones de R. Para $\frac{x}{y} \in K$ definamos la valuación p-ádica sobre K mediante

$$v_p\left(\frac{x}{y}\right) := v_p(x) - v_p(y).$$

Hay que verificar que esta definición tiene sentido: si $\frac{x}{y} = \frac{x'}{y'}$, entonces $xy' = x'y$. Luego,

$$v_p(x) + v_p(y') = v_p(x') + v_p(y);$$

es decir,

$$v_p(x) - v_p(y) = v_p(x') - v_p(y').$$

Esto significa que

$$v_p\left(\frac{x}{y}\right) = v_p\left(\frac{x'}{y'}\right).$$

Notamos que para toda fracción no nula se tiene

$$\frac{x}{y} = \prod_p p^{v_p(x/y)},$$

donde el producto se toma sobre todos los primos en R salvo la relación $\sim$, y la igualdad se entiende salvo un múltiplo $u \in R^\times$.

13.5.6. Ejemplo. Para $x = \frac{12}{34} = \frac{2^2 \cdot 3}{2 \cdot 17}$ se tiene

$$v_2(x) = 1, \quad v_3(x) = 1, \quad v_{17}(x) = -1,$$

y $v_p(x) = 0$ para otros p. ▲

13.5.7. Observación. *La valuación p-ádica sobre K satisface las mismas propiedades:*

V1) $v_p\left(\frac{x}{y}\right) = \infty$ *si y solamente si* $\frac{x}{y} = \frac{0}{1}$.

V2) $v_p\left(\frac{x_1}{y_1}\,\frac{x_2}{y_2}\right) = v_p\left(\frac{x_1}{y_1}\right) + v_p\left(\frac{x_2}{y_2}\right)$.

V3) $v_p\left(\frac{x_1}{y_1} + \frac{x_2}{y_2}\right) \geq \min\left\{v_p\left(\frac{x_1}{y_1}\right), v_p\left(\frac{x_2}{y_2}\right)\right\}$.

Demostración. En V1) basta recordar que $\frac{x}{y} = \frac{0}{1}$ si y solo si $x = 0$.

En V2), tenemos

$$v_p\left(\frac{x_1}{y_1}\,\frac{x_2}{y_2}\right) = v_p\left(\frac{x_1 x_2}{y_1 y_2}\right) = v_p(x_1x_2) - v_p(y_1y_2) = v_p(x_1) + v_p(x_2) - v_p(y_1) - v_p(y_2)$$
$$= v_p\left(\frac{x_1}{y_1}\right) + v_p\left(\frac{x_2}{y_2}\right).$$

En fin, en V3)

$$\begin{aligned} v_p\left(\frac{x_1}{y_1}+\frac{x_2}{y_2}\right) = v_p\left(\frac{x_1y_2+x_2y_1}{y_1y_2}\right) &= v_p(x_1y_2+x_2y_1) - v_p(y_1) - v_p(y_2) \\ &\geq \text{mín}\{v_p(x_1)+v_p(y_2), v_p(x_2)+v_p(y_1)\} - v_p(y_1) - v_p(y_2) \\ &= \text{mín}\{v_p(x_1)-v_p(y_1), v_p(x_2)-v_p(y_2)\} = \text{mín}\left\{v_p\left(\frac{x_1}{y_1}\right), v_p\left(\frac{x_2}{y_2}\right)\right\}. \end{aligned}$$

■

La desigualdad $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$ puede ser mejorada de la siguiente manera.

13.5.8. Observación. *Para cualesquiera $x, y \in R$, si $v_p(x) \neq v_p(y)$, entonces*

$$v_p(x+y) = \text{mín}\{v_p(x), v_p(y)\}.$$

De la misma manera, para cualesquiera $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in K$, si $v_p\left(\frac{x_1}{y_1}\right) \neq v_p\left(\frac{x_2}{y_2}\right)$, entonces

$$v_p\left(\frac{x_1}{y_1}+\frac{x_2}{y_2}\right) = \text{mín}\left\{v_p\left(\frac{x_1}{y_1}\right), v_p\left(\frac{x_2}{y_2}\right)\right\}.$$

Demostración. La propiedad en cuestión sigue formalmente de las propiedades V1), V2), V3). Asumamos que se cumple la desigualdad estricta

$$v_p(x+y) > \text{mín}\{v_p(x), v_p(y)\}.$$

Entonces, tenemos

$$v_p(x) = v_p(x+y-y) \geq \text{mín}\{v_p(x+y), v_p(y)\} = v_p(y)$$

y de la misma manera

$$v_p(y) = v_p(x+y-x) \geq \text{mín}\{v_p(x+y), v_p(x)\} = v_p(x).$$

■

13.5.9. Comentario. Por inducción, de la última observación se sigue que si $x = x_1 + \cdots + x_n$ y existe $i = 1, \ldots, n$ tal que $v_p(x_i) < v_p(x_j)$ para $i \neq j$, entonces $v_p(x) = v_p(x_i)$.

13.5.10. Observación. *Se tiene*

$$R = \{x \in K \mid v_p(x) \geq 0 \text{ para todo primo } p\},$$

donde se consideran todos los primos en R salvo la relación $\sim$ y

$$R^\times = \{x \in K \mid v_p(x) = 0 \text{ para todo primo } p\}.$$

Demostración. Tenemos $x = \prod_p p^{v_p(x)}$ salvo un múltiplo $u \in R^\times$, así que si $v_p(x) \geq 0$ para todo p, se tiene $x \in R$. ■

13.6 Lema de Gauss y factorización de polinomios

El objetivo de esta sección es probar el siguiente resultado: si R es un dominio de factorización única, entonces el anillo de polinomios $R[X]$ es también un dominio de factorización única. El argumento que vamos a ver esencialmente pertenece a Gauss (como una gran parte del resto de esta sección).

Primero, nos va a servir la siguiente extensión de las valuaciones p-ádicas al anillo de polinomios $K[X]$.

13.6.1. Definición. Sean R un dominio de factorización única, K su cuerpo de fracciones y $p \in R$ un elemento primo. Para un polinomio $f = \sum_{i\geq 0} a_i X^i \in K[X]$ definamos

$$v_p(f) := \min_i \{v_p(a_i)\}.$$

En particular,

$$v_p(0) = \infty.$$

De la definición debe estar claro que

$$v_p(f+g) \geq \min\{v_p(f), v_p(g)\}.$$

También tenemos la propiedad deseada para los productos.

13.6.2. Lema. *Para cualesquiera $f, g \in K[X]$ se cumple*

$$v_p(fg) = v_p(f) + v_p(g).$$

Demostración. Esto es evidente si $f = 0$ o $g = 0$, así que podemos asumir que $f, g \neq 0$. Tenemos

$$f = \sum_{i\geq 0} a_i X^i, \quad g = \sum_{j\geq 0} b_j X^j, \quad fg = \sum_{k\geq 0} c_k X^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

Ahora

$$v_p(c_k) \geq \min_{i+j=k} \{v_p(a_i) + v_p(b_j)\} \geq v_p(f) + v_p(g),$$

y por ende

$$v_p(fg) \geq v_p(f) + v_p(g).$$

Para concluir que se tiene la igualdad, hay que ver que algún coeficiente c_k tiene valuación $v_p(f) + v_p(g)$. Asumamos que $v_p(f) = v_p(a_m)$, donde el índice m es el mínimo posible:

$$v_p(a_m) < v_p(a_i) \text{ para } 0 \leq i < m, \quad v_p(a_m) \leq v_p(a_i) \text{ para } i \geq m.$$

De la misma manera, supongamos que $v_p(g) = v_p(b_n)$, donde n es el mínimo posible:

$$v_p(b_n) < v_p(b_i), \text{ para } 0 \leq i < n, \quad v_p(b_n) \leq v_p(b_i), \text{ para } i \geq n.$$

Luego,

$$v_p(c_{m+n}) \geq \max_{i+j=m+n} \{v_p(a_i) + v_p(b_j)\}.$$

Dado que $i + j = m + n$, se tiene $i < m$ o $j < n$, salvo el caso $i = m$, $j = n$. Por nuestra elección de m y n, esto significa que $v_p(a_m) + v_p(b_n)$ es estrictamente menor que otros términos, así que gracias a 13.5.9 se puede concluir que

$$v_p(c_{m+n}) = v_p(a_m) + v_p(b_n) = v_p(f) + v_p(g).$$

■

lección 21
03.10.18

13.6.3. Definición. Sean R un dominio de factorización única y K su cuerpo de fracciones. Para un polinomio $f \in K[X]$ su **contenido** está definido por

$$\operatorname{cont}(f) := \prod_p p^{v_p(f)},$$

donde el producto se toma sobre todos los primos en R salvo la relación de equivalencia $\sim$. Esto define a $\operatorname{cont}(f)$ salvo un múltiplo invertible $u \in R^\times$.

He aquí algunas observaciones sobre el contenido que serán útiles más adelante.

1) Para un polinomio constante $f = c$ se tiene $\operatorname{cont}(c) = c$, salvo un múltiplo invertible $u \in R^\times$.

2) Si $f \in R[X]$, entonces $\operatorname{cont}(f) \in R$.

3) Si $\operatorname{cont}(f) = 1$, entonces $v_p(f) = 0$ para todo p; es decir, $f \in R[X]$ (véase 13.5.10) y además para todo p existe i tal que $p \nmid a_i$.

4) Para $f \in K[X]$ se tiene $\frac{1}{\operatorname{cont}(f)} f \in R[X]$.

13.6.4. Observación. *Sea R un dominio de factorización única y K su cuerpo de fracciones. Para cualesquiera $f, g \in K[X]$ se tiene*

$$\operatorname{cont}(fg) = \operatorname{cont}(f) + \operatorname{cont}(g).$$

Demostración. Sigue inmediatamente de 13.6.2. ■

13.6.5. Lema (Gauss). *Sea R un dominio de factorización única y sea K su cuerpo de fracciones. Si $f \in R[X]$ es un polinomio irreducible en $K[X]$ y $\operatorname{cont}(f) = 1$, entonces f es irreducible en $R[X]$.*

Demostración. Supongamos que $f = gh$ para algunos $g, h \in R[X]$. Vamos a probar que $g \in R[X]^\times$ o $h \in R[X]^\times$. Interpretando $f = gh$ como una factorización en $K[X]$, podemos concluir que $g \in K[X]^\times = K^\times$ o $h \in K[X]^\times = K^\times$. Asumamos por ejemplo que $g = c \in K^\times$. Tenemos

$$\operatorname{cont}(c)\ \operatorname{cont}(h) = \operatorname{cont}(f) = 1,$$

lo que significa que $\operatorname{cont}(c) \in R^\times$, así que $c \in R^\times$. Hemos probado entonces que $g = c \in R[X]^\times$. ■

13.6.6. Ejemplo. La condición $\operatorname{cont}(f) = 1$ es necesaria. Por ejemplo, el polinomio $f = 2X^2 + 2X - 2$ tiene $\operatorname{cont}(f) = 2$. Es irreducible en $\mathbb{Q}[X]$, pero en $\mathbb{Z}[X]$ tenemos una factorización no trivial $f = 2(X^2 + X - 1)$. ▲

13.6.7. Teorema. *Si R es un dominio de factorización única, entonces el anillo de polinomios $R[X]$ es también un dominio de factorización única.*

Demostración. Sea K el cuerpo de fracciones de R. El anillo de polinomios $K[X]$ es un dominio euclidiano y en particular un dominio de factorización única.

Sea $f \in R[X]$ un polinomio no nulo. En $K[X]$ tenemos una factorización única

$$f = c\, p_1 \cdots p_s,$$

donde $c \in K^\times$ y $p_1, \ldots, p_s \in K[X]$ son polinomios irreducibles en $K[X]$. Luego,

$$\operatorname{cont}(f) = \operatorname{cont}(c)\ \operatorname{cont}(p_1) \cdots \operatorname{cont}(p_s),$$

así que

$$\frac{1}{\operatorname{cont}(f)}\, f = \frac{1}{\operatorname{cont}(c)}\, c \cdot \frac{1}{\operatorname{cont}(p_1)}\, p_1 \cdots \frac{1}{\operatorname{cont}(p_s)}\, p_s.$$

Notamos que los polinomios $\frac{1}{\operatorname{cont}(f)}\, f$, $\frac{1}{\operatorname{cont}(c)}\, c$, $\frac{1}{\operatorname{cont}(p_i)}\, p_i$ tienen contenido 1 y en particular pertenecen a $R[X]$. Tenemos necesariamente $\frac{1}{\operatorname{cont}(c)}\, c \in R^\times$. Por el lema de Gauss, $\frac{1}{\operatorname{cont}(p_i)}\, p_i$ son polinomios irreducibles en $R[X]$, puesto que son irreducibles en $K[X]$.

Entonces, hemos logrado factorizar el polinomio $\frac{1}{\operatorname{cont}(f)}\, f \in R[X]$ en polinomios irreducibles en $R[X]$. Luego, en R tenemos una factorización única

$$\operatorname{cont}(f) = u\, x_1 \cdots x_t$$

donde $u \in R^\times = R[X]^\times$ y $x_1, \ldots, x_t$ son irreducibles en R, y por ende son irreducibles en $R[X]$ (un polinomio constante puede ser escrito solo como un producto de polinomios constantes).

Entonces,

$$f = \operatorname{cont}(f)\, \frac{1}{\operatorname{cont}(f)}\, f = v\, x_1 \cdots x_t \cdot \frac{1}{\operatorname{cont}(p_1)}\, p_1 \cdots \frac{1}{\operatorname{cont}(p_s)}\, p_s,$$

(donde $v := u\, \frac{1}{\operatorname{cont}(c)}\, c \in R^\times$) es una factorización de f en polinomios irreducibles en $R[X]$. Falta ver que estas factorizaciones son únicas.

Asumamos que hay otra factorización

$$f = w\, y_1 \cdots y_{t'} \cdot q_1 \cdots q_{s'}$$

donde $w \in R^\times = R[X]^\times$, $y_1, \ldots, y_{t'}$ son elementos irreducibles en R y $q_1, \ldots, q_{s'}$ son polinomios no constantes irreducibles en $R[X]$. Esta factorización puede ser considerada como una factorización en $K[X]$ que es un dominio de factorización única. Notamos que $w\, y_1 \cdots y_{t'} \in K^\times$. Los polinomios p_i son irreducibles en $K[X]$, así que para todo i existe j tal que $p_i \mid q_j$:

$$q_j = g_{ij}\, p_i$$

para algún polinomio $g_{ij} \in K[X]$. Luego, tenemos una identidad en $R[X]$

$$\frac{1}{\operatorname{cont}(q_j)}\, q_j = \frac{1}{\operatorname{cont}(q_{ij})}\, g_{ij}\, \frac{1}{\operatorname{cont}(p_i)}\, p_i.$$

Pero q_j es irreducible en $R[X]$ por nuestra hipótesis, y el polinomio p_i no es constante, lo que implica que q_j y $\frac{1}{\operatorname{cont}(p_i)}\, p_i$ son asociados en $R[X]$: existe $u_j \in R^\times = R[X]^\times$ tal que

$$q_j = u_j\, \frac{1}{\operatorname{cont}(p_i)}\, p_i. \tag{13.2}$$

En particular, q_j son irreducibles en $K[X]$, y entonces necesariamente $s = s'$, dado que $K[X]$ es un dominio de factorización única. Podemos comparar las dos factorizaciones:

$$f = v\, x_1 \cdots x_t \cdot \frac{1}{\operatorname{cont}(p_1)}\, p_1 \cdots \frac{1}{\operatorname{cont}(p_s)}\, p_s = w\, y_1 \cdots y_{t'} \cdot q_1 \cdots q_s.$$

Gracias a 13.2, podemos cancelar los términos $\frac{1}{\operatorname{cont}(p_i)}\, p_i$ con correspondientes q_j y nos queda una identidad en R

$$v\, x_1 \cdots x_t = w'\, y_1 \cdots y_{t'}$$

donde $w' := w\, u_1 \cdots u_s \in R^\times$. Pero R es un dominio de factorización única y x_i, y_j son irreducibles, así que $t' = t$ y $y_i \sim x_i$ después de una permutación. ■

13.6.8. Comentario. La prueba de arriba revela que los elementos irreducibles en $R[X]$ son las constantes irreducibles en R y los polinomios no constantes $f \in R[X]$ tales que $\mathrm{cont}(f) = 1$ y f es irreducible en $K[X]$.

13.6.9. Comentario. En particular, si $R = k$ es un cuerpo, es trivialmente un dominio de factorización única y $k[X]$ es un dominio de factorización única. Sin embargo, la prueba de arriba no considera este caso, sino está basada en él.

13.6.10. Ejemplo. El anillo de polinomios $\mathbb{Z}[X]$ es un dominio de factorización única. Los elementos irreducibles (primos) en $\mathbb{Z}[X]$ son los primos $p = \pm 2, \pm 3, \pm 5, \pm 7, \pm 1, \ldots$ y los polinomios $\pi \in \mathbb{Z}[X]$ que son irreducibles en $\mathbb{Q}[X]$, por ejemplo

$$\pi = X, \quad 2\,X + 1, \quad X^2 + 2\,X + 2, \quad X^3 + 2.$$

Como vimos en 13.2.4, $\mathbb{Z}[X]$ no es un dominio de ideales principales: hemos observado que (p, X) es un ideal maximal que no puede ser generado por un elemento. En general, tenemos la siguiente descripción de ideales primos en $\mathbb{Z}[X]$:

0) el ideal nulo (0),

1) los ideales principales (p) para $p = 2, 3, 5, 7, 11, \ldots$,

2) los ideales principales (π) donde $\pi \in \mathbb{Z}[X]$ es un polinomio no constante que es irreducible en $\mathbb{Q}[X]$,

3) los ideales maximales (p, π), donde $p = 2, 3, 5, 7, 11, \ldots$ y $\pi \in \mathbb{Z}[X]$ es un polinomio no constante tal que $\overline{\pi} \in \mathbb{F}_p[X]$ es irreducible.

Primero, notemos que los ideales de la lista son primos. La parte 0) es obvia: $\mathbb{Z}[X]$ es un dominio de integridad. Las partes 1) y 2) siguen de la descripción de los elementos irreducibles (primos) en $\mathbb{Z}[X]$. Para la parte 3), notamos que

$$\mathbb{Z}[X]/(p, \pi) \cong \mathbb{F}_p[X]/(\overline{\pi}),$$

donde $\overline{\pi}$ es la imagen de π respecto al homomorfismo canónico $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ (la reducción de los coeficientes módulo p). El anillo $\mathbb{F}_p[X]$ es un dominio euclidiano y por ende es un dominio de ideales principales. Por nuestra hipótesis, $\overline{\pi}$ es irreducible (primo) en $\mathbb{F}_p[X]$, así que el ideal $(\overline{\pi}) \subset \mathbb{F}_p[X]$ es maximal y $\mathbb{F}_p[X]/(\overline{\pi})$ es un cuerpo. Podemos concluir que el ideal $(p, \pi) \subset \mathbb{Z}[X]$ es también maximal.

Para completar la descripción, hay que probar que todo ideal primo $\mathfrak{p} \subset \mathbb{Z}[X]$ es de la forma 0)–3). Si $\mathfrak{p} = (0)$, estamos en el caso 0), así que asumamos que $\mathfrak{p} \neq (0)$.

La intersección $\mathfrak{p} \cap \mathbb{Z}$ es un ideal primo en $\mathbb{Z}$, siendo la preimagen de $\mathfrak{p}$ respecto al homomorfismo canónico $\mathbb{Z} \hookrightarrow \mathbb{Z}[X]$.

Asumamos primero que $\mathfrak{p} \cap \mathbb{Z} \neq (0)$. En este caso existe un número primo p tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Luego, $p\mathbb{Z}[X] \subseteq \mathfrak{p}$.

Ahora $\overline{\mathfrak{p}} := \mathfrak{p}/(p\mathbb{Z}[X])$ es un ideal primo en el anillo cociente $\mathbb{Z}[X]/(p) \cong \mathbb{F}_p[X]$. Esto implica que $\overline{\mathfrak{p}} = (0)$ o $\overline{\mathfrak{p}} = \overline{\pi}\,\mathbb{F}_p[X]$ donde $\overline{\pi} \in \mathbb{F}_p[X]$ es algún polinomio irreducible. Entonces, hay dos posibilidades:

$$\mathfrak{p} = p\mathbb{Z}[X], \quad \mathfrak{p} = p\mathbb{Z}[X] + \pi\,\mathbb{Z}[X],$$

donde $\overline{pi} = \pi \pmod{p}$. Esto corresponde a los casos 1) y 3) de la lista.

Asumamos que $\mathfrak{p} \cap \mathbb{Z} = (0)$. Sea $f \in \mathfrak{p}$ un polinomio no nulo. Tenemos la factorización única

$$f = \pm \pi_1 \cdots \pi_s,$$

donde $\pi_i \in \mathbb{Z}[X]$ son polinomios irreducibles (primos). Puesto que $\mathfrak{p}$ es un ideal primo, se tiene necesariamente $\pi := \pi_i \in \mathfrak{p}$ para algún $i = 1, \ldots, s$. La hipótesis que $\mathfrak{p} \cap \mathbb{Z} = (0)$ implica que este polinomio π no es constante. Nuestro objetivo es probar que $\mathfrak{p} = \pi\mathbb{Z}[X]$. Sea entonces $g \in \mathfrak{p}$ cualquier polinomio no nulo.

Asumamos que π no divide a g en $\mathbb{Q}[X]$. Dado que π es un polinomio no constante que es irreducible en $\mathbb{Z}[X]$, es también irreducible en $\mathbb{Q}[X]$, y por ende $\mcd(\pi, g) = 1$, lo que significa que

$$h_1\,\pi + h_2\,g = 1$$

para algunos $h_1, h_2 \in \mathbb{Q}[X]$. Tomemos n suficientemente grande tal que los polinomios $n\,h_1\,\pi$ y $n\,h_2\,g$ tienen coeficientes enteros. Luego,

$$n\,h_1\,\pi + n\,h_2\,g = n \in \mathfrak{p},$$

pero esto contradice nuestra hipótesis de que $\mathfrak{p} \cap \mathbb{Z} = (0)$.

Entonces, π tiene que dividir en $\mathbb{Q}[X]$ a cualquier polinomio $g \in \mathfrak{p}$: tenemos

$$g = \pi\,r$$

para algún $r \in \mathbb{Q}[X]$. Sin embargo,

$$\operatorname{cont}(g) = \operatorname{cont}(\pi)\,\operatorname{cont}(r),$$

Donde $\operatorname{cont}(\pi) = 1$, dado que π es un polinomio irreducible en $\mathbb{Z}[X]$. Entonces, $\operatorname{cont}(r) = \operatorname{cont}(g) \in \mathbb{Z}$ y $r \in \mathbb{Z}[X]$. Esto demuestra que $g \in \pi\mathbb{Z}[X]$. ▲

13.6.11. Corolario. *Si R es un dominio de factorización única, entonces el anillo de polinomios en n variables $R[X_1, \ldots, X_n]$ es también un dominio de factorización única.*

Demostración. Inducción sobre n, usando isomorfismos $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$. ■

13.6.12. Comentario. Si R es un dominio de factorización única, el anillo de las series formales $R[\![X_1, \ldots, X_n]\!]$ no tiene por qué ser un dominio de factorización única[*]. Sin embargo, es cierto si $R = k$ es un cuerpo (las palabras claves son "el **teorema de preparación de Weierstrass**").

13.6.13. Comentario. El teorema 13.6.7 puede ser probado sin recurrir a las valuaciones p-ádicas (véase por ejemplo [DF2004, §9.3]); las hemos revisado porque son muy importantes en la teoría de números.

13.7 Criterios de irreducibilidad

lección 22
04.10.18

Ahora ya que sabemos que para un dominio de factorización única R los polinomios $R[X]$ también forman un dominio de factorización única, sería interesante saber cuándo un polinomio $f \in R[X]$ es irreducible. Esto es un problema profundo desde el punto de vista teórico y algorítmico y aquí vamos a ver solo un par de criterios útiles en práctica.

13.7.1. Lema. *Sean R un anillo conmutativo e $I \subseteq R$ un ideal. Entonces, hay un isomorfismo natural*

$$R[X]/IR[X] \cong (R/I)[X],$$

donde $IR[X]$ es el ideal generado por I en $R[X] \supset R$:

$$IR[X] = \left\{ \sum_{i \geq 0} a_i\,X^i \;\middle|\; a_i \in I \right\}.$$

[*] Véase por ejemplo el artículo de Pierre Samuel https://projecteuclid.org/euclid.ijm/1255629643 para un estudio de este problema.

Demostración. Consideremos la aplicación

$$\begin{aligned} R[X] &\to (R/I)[X], \\ \sum_{i\geq 0} a_i\, X^i &\mapsto \sum_{i\geq 0} \overline{a_i}\, X^i \end{aligned}$$

que reduce los coeficientes de un polinomio módulo I. Las fórmulas para la suma y producto de polinomios demuestran que esto es un homomorfismo de anillos. Es visiblemente sobreyectivo, y su núcleo es precisamente $IR[X]$. ■

13.7.2. Proposición. *Sea R un dominio de integridad y sea $f \in R[X]$ un polinomio mónico (con coeficiente mayor igual a 1) no constante. Sea $I \subset R[X]$ un ideal propio tal que la imagen $\overline{f}$ en el cociente $R[X]/IR[X] \cong (R/I)[X]$ no se factoriza como un producto de polinomios de grado $< \deg \overline{f}$. Entonces, f es irreducible en $R[X]$.*

Demostración. Asumamos que f es reducible en $R[X]$; es decir, $f = gh$ donde $g, h \notin R[X]^\times = R^\times$. Si $g = a_m\, X^m + a_{m-1}\, X^{m-1} + \cdots$ y $h = b_n\, X^n + b_{n-1}\, X^{n-1} + \cdots$, entonces el coeficiente mayor de gh es $a_m\, b_n = 1$. Esto implica que $a_m, b_n \in R^\times$, y en particular g y h no son polinomios constantes, y luego $\deg g, \deg h < \deg f$. Gracias a nuestra hipótesis de que $I \neq R$, tenemos $a_m, b_n \notin I$, así que

$$\deg \overline{g} = \deg g, \quad \deg \overline{h} = \deg h.$$

La reducción módulo I nos da entonces una factorización $\overline{f} = \overline{g}\,\overline{h}$, donde $\deg \overline{g}, \deg \overline{h} < \deg \overline{f}$. ■

13.7.3. Ejemplo. Es fácil saber cuándo un polinomio con coeficientes en $\mathbb{F}_p$ es irreducible: hay un número finito de polinomios de grado fijo. Para compilar una lista de polinomios irreducibles en $\mathbb{F}_p[X]$ se puede usar la **criba de Eratóstenes**. Por ejemplo, sea $p = 2$. Los polinomios de grado 1 son siempre irreducibles:

$$X, \quad X + 1.$$

Los polinomios de grado 2 son

$$X^2, \quad X^2 + 1, \quad X^2 + X, \quad X^2 + X + 1.$$

Entre ellos los polinomios reducibles son los productos de polinomios lineales:

$$X^2 = X \cdot X, \quad X^2 + X = X\,(X+1), \quad X^2 + 1 = (X+1)^2.$$

Entonces, $X^2 + X + 1$ es irreducible. Luego, los polinomios cúbicos reducibles son los productos de polinomios de grado 1 y 2:

$$\begin{aligned} X^3 &= X^3, \\ X^3 + X^2 + X + 1 &= (X+1)^3, \\ X^3 + X^2 &= X^2\,(X+1), \\ X^3 + X &= X\,(X+1)^2, \\ X^3 + X^2 + X &= (X^2 + X + 1)\,X, \\ X^3 + 1 &= (X^2 + X + 1)\,(X+1). \end{aligned}$$

Los dos polinomios cúbicos que nos quedan son irreducibles:

$$X^3 + X + 1, \quad X^3 + X^2 + 1.$$

Continuando de la misma manera, se puede ver que los polinomios irreducibles de grado cuatro son

$$X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1.$$

El número de polinomios irreducibles en $\mathbb{F}_p[X]$ de grado n crece rápido con p y n. En el siguiente capítulo vamos a ver cómo contarlos. ▲

13.7.4. Ejemplo. El polinomio $f = X^2 + 1$ es irreducible en $\mathbb{Z}[X]$ y $\overline{f}$ se vuelve reducible en $\mathbb{F}_p[X]$ si y solo si -1 es un cuadrado módulo p. Esto sucede precisamente para $p \equiv 1 \pmod 4$. Por ejemplo, en $\mathbb{Z}/5\mathbb{Z}[X]$ se cumple

$$X^2 + 1 = (X + 2)\,(X + 3).$$

▲

13.7.5. Ejemplo. Consideremos el polinomio

$$f = X^3 + X^2 - 2\,X - 1 \in \mathbb{Z}[X].$$

Al reducirlo módulo 2 nos queda un polinomio irreducible

$$\overline{f} = X^3 + X^2 + 1 \in \mathbb{F}_2[X].$$

Podemos tratar de reducir el mismo polinomio f módulo otros números primos. La tabla de abajo nos da las factorizaciones de $\overline{f} \in \mathbb{F}_p[X]$ en factores irreducibles. He excluido los casos cuando $\overline{f}$ queda irreducible, como para $p = 2$.

$$\begin{array}{rl} p = 7\colon & (X + 5)^3, \\ p = 13\colon & (X + 3)\,(X + 5)\,(X + 6), \\ p = 29\colon & (X + 11)\,(X + 22)\,(X + 26), \\ p = 41\colon & (X + 4)\,(X + 11)\,(X + 27), \\ p = 43\colon & (X + 24)\,(X + 28)\,(X + 35), \\ & \dots \end{array}$$

Un experimento numérico demuestra que $\overline{f}$ queda irreducible para $\frac{2}{3}$ de los números primos, y para $\frac{1}{3}$ de los números primos $\overline{f}$ es un producto de tres diferentes polinomios lineales. El caso $p = 7$ es excepcional: se tiene un cubo del mismo polinomio lineal.

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163
1171	1181	1187	1193	1201	1213	1217	1223	1229	1231	1237	1249
1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321
1327	1361	1367	1373	1381	1399	1409	1423	1427	1429	1433	1439
1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601
1607	1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693
1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783
1787	1789	1801	1811	1823	1831	1847	1861	1867	1871	1873	1877
1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987

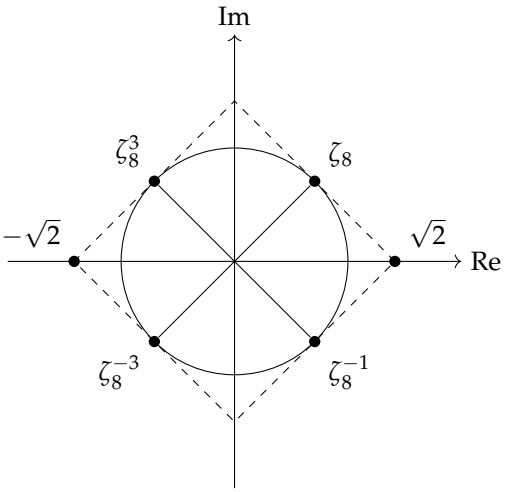
Los primos tales que $X^3 + X^2 - 2\,X - 1$ es irreducible en $\mathbb{F}_p[X]$

▲

Aunque nuestro criterio de irreducibilidad es muy sencillo, existen polinomios irreducibles $f \in \mathbb{Z}[X]$ tales que $\overline{f} \in \mathbb{F}_p[X]$ es reducible para cualquier primo p.

13.7.6. Ejemplo. El polinomio $f = X^4 + 1$ es irreducible en $\mathbb{Z}[X]$. Lo veremos más adelante usando otro método, pero por el momento podemos presentar una explicación directa. Las raíces complejas de f son

$$\zeta_8 := e^{\frac{1}{8}\cdot 2\,\pi\sqrt{-1}}, \quad \zeta_8^{-1} = \overline{\zeta_8}, \quad \zeta_8^3, \quad \zeta_8^{-3} = \overline{\zeta_8^3}.$$



Tenemos entonces una factorización en $\mathbb{C}[X]$

$$f = (X - \zeta_8)\,(X - \overline{\zeta_8})\,(X - \zeta_8^3)\,(X - \overline{\zeta_8^3}).$$

Supongamos que $f = gh$ para algunos $g, h \in \mathbb{Z}[X]$. Dado que f es mónico, el coeficiente mayor de g y h es ± 1. Si $g, h \neq \pm 1$ no son polinomios constantes, entonces $\deg g, \deg h \geq 1$. Es imposible que $\deg g = 1$ o $\deg h = 1$: un polinomio lineal que tiene $\zeta_8^{\pm 1}$ o $\zeta_8^{\pm 3}$ como su raíz no puede tener coeficientes enteros. Entonces, f y g deben ser cuadráticos. Sin embargo, si un polinomio con coeficientes reales (en particular enteros) tiene $z \in \mathbb{C}$ como su raíz, entonces $\overline{z}$ es también una raíz. Pero se tiene

$$\begin{aligned}(X - \zeta_8)\,(X - \overline{\zeta_8}) &= X^2 - (\zeta_8 + \overline{\zeta_8})\,X + \zeta_8\,\overline{\zeta_8} = X^2 - \sqrt{2}\,X + 1,\\ (X - \zeta_8^3)\,(X - \overline{\zeta_8^3}) &= X^2 + \sqrt{2}\,X + 1,\end{aligned}$$

lo que demuestra que un polinomio con raíces $\zeta_8, \overline{\zeta_8}$ o $\zeta_8^3, \overline{\zeta_8^3}$ no puede tener coeficientes enteros.

Ahora se puede probar que el polinomio $X^4 + 1$ se vuelve reducible módulo cualquier primo. Por ejemplo,

$$\begin{aligned}
p = 2\colon&\quad (X+1)^4,\\
p = 3\colon&\quad (X^2 + X + 2)\,(X^2 + 2X + 2),\\
p = 5\colon&\quad (X^2 + 2)\,(X^2 + 3),\\
p = 7\colon&\quad (X^2 + 3X + 1)\,(X^2 + 4X + 1),\\
p = 11\colon&\quad (X^2 + 3X + 10)\,(X^2 + 8X + 10),\\
p = 13\colon&\quad (X^2 + 5)\,(X^2 + 8),\\
p = 17\colon&\quad (X+2)\,(X+8)\,(X+9)\,(X+15),\\
&\quad \cdots
\end{aligned}$$

En efecto, para $p = 2$ se tiene la factorización $X^4 + 1 = (X+1)^4$. Para p impar tenemos necesariamente $p \equiv 1, 3, 5, 7 \pmod 8$.

1) Si $p \equiv 1$ o $5 \pmod 8$, entonces $p \equiv 1 \pmod 4$, y en este caso -1 es un cuadrado módulo p. Tenemos $-1 = a^2$ para algún $a \in \mathbb{F}_p$ y podemos escribir

$$X^4 + 1 = X^4 - a^2 = (X^2 + a)\,(X^2 - a).$$

2) Si $p \equiv 7 \pmod 8$, entonces 2 es un cuadrado módulo p; se tiene $2 = a^2$ para algún $a \in \mathbb{F}_p$, y luego

$$(X^2 + aX + 1)\,(X^2 - aX + 1) = X^4 + (2 - a^2)\,X + 1 = X^4 + 1.$$

3) Si $p \equiv 3 \pmod 8$, entonces $p \equiv 3 \pmod 4$ y ni -1, ni 2 no es un cuadrado módulo p. En este caso -2 es un cuadrado. Si $-2 = a^2$, entonces

$$(X^2 + aX - 1)\,(X^2 - aX - 1) = X^4 - (2 + a^2)\,X + 1 = X^4 + 1.$$

(Esto sigue de las leyes suplementarias de reciprocidad cuadrática; véase 13.7.7.)

Un experimento numérico demuestra que para $\frac{3}{4}$ de los primos p el polinomio $X^4 + 1$ se factoriza en $\mathbb{F}_p[X]$ como un producto de dos polinomios cuadráticos irreducibles, y para $\frac{1}{4}$ de los primos la factorización es un producto de cuatro diferentes polinomios lineales (en efecto, estos son los primos tales que $p \equiv 1 \pmod 8$). El primo $p = 2$ es excepcional.

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163
1171	1181	1187	1193	1201	1213	1217	1223	1229	1231	1237	1249
1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321
1327	1361	1367	1373	1381	1399	1409	1423	1427	1429	1433	1439
1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601
1607	1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693
1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783
1787	1789	1801	1811	1823	1831	1847	1861	1867	1871	1873	1877
1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987

Los primos tales que X^4+1 se factoriza en cuatro polinomios irreducibles en $\mathbb{F}_p[X]$

▲

13.7.7. Comentario. El argumento de arriba usa las **leyes suplementarias de reciprocidad cuadrática**: para p impar se cumple

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases} \tag{13.3}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv 1,7 \pmod 8, \\ -1, & p \equiv 3,5 \pmod 8. \end{cases} \tag{13.4}$$

Ambas leyes pueden ser deducidas del **criterio de Euler**

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

(véase el capítulo 7). Para $a = -1$ se obtiene (13.3). Para $a = 2$, tenemos

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p.$$

Para identificar el número a la derecha, podemos usar las raíces octavas de la unidad que ya han surgido en 13.7.6. Consideremos el anillo

$$\mathbb{Z}[\zeta_8] = \left\{ \sum_{0 \le i \le 7} n_i \zeta_8^i \;\middle|\; n_i \in \mathbb{Z} \right\} \subset \mathbb{C}$$

donde $\zeta_8 := e^{2\pi\sqrt{-1}/8}$. Denotemos

$$\alpha := \zeta_8 + \zeta_8^{-1} = \sqrt{2}.$$

Notamos que en $\mathbb{Z}[\zeta_8]$ se cumple

$$\alpha^p = (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \equiv \begin{cases} \zeta_8 + \zeta_8^{-1} = +\alpha, & p \equiv \pm 1 \pmod 8, \\ \zeta_8^3 + \zeta_8^{-3} = -\alpha, & p \equiv \pm 3 \pmod 8. \end{cases} \pmod p$$

(usando la identidad $(x+y)^p \equiv x^p + y^p \pmod p$). Puesto que $\alpha = \sqrt{2}$, calculamos

$$2^{\frac{p-1}{2}} = \alpha^{p-1} = \alpha^p\, \alpha^{-1} \equiv \begin{cases} +1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases} \pmod p.$$

Esto establece (13.4).

13.7.8. Comentario. En la teoría de números algebraica se estudian los patrones en la factorización de $\overline{f} \in \mathbb{F}_p[X]$ para diferentes p. Los "experimentos numéricos" mencionados en 13.7.5 y 13.7.6 no son coincidencias; estos fenómenos se explican por el famoso **teorema de densidad de Chebotarëv**[*]. Para más detalles, véase el artículo P. Stevenhagen y H. W. Lenstra http://www.math.leidenuniv.nl/~hwl/papers/cheb.pdf

lección 23
11.10.18

He aquí otro criterio de irreducibilidad útil en práctica.

13.7.9. Teorema (Criterio de Eisenstein). *Sean R un dominio de integridad y $\mathfrak{p} \subset R$ un ideal primo, Sea*

$$f = X^n + a_{n-1}\, X^{n-1} + \cdots + a_1\, X + a_0$$

un polinomio mónico con coeficientes en R tal que $a_i \in \mathfrak{p}$ para todo $i = 0, 1, \ldots, n-1$, pero $a_0 \notin \mathfrak{p}^2$. Entonces, f es irreducible.

Demostración. Asumamos que f es reducible y $f = g\,h$ donde $g, h \notin R[X]^\times = R^\times$. Notamos que necesariamente

$$1 \leq \deg g, \deg h < n$$

—si uno de estos polinomios fuera constante, este sería invertible, dado que f es un polinomio mónico. Reduciendo módulo $\mathfrak{p}$, se obtiene una identidad

$$\overline{X^n} = \overline{f} = \overline{g}\,\overline{h} \quad \text{en } (R/\mathfrak{p})[X]$$

por la hipótesis sobre los coeficientes de f. Puesto que $\mathfrak{p}$ es un ideal primo, $R/\mathfrak{p}$ es un dominio de integridad, y podemos encajarlo en su cuerpo de fracciones $K := K(R/\mathfrak{p})$. La identidad de arriba considerada en $K[X]$ implica que

$$\overline{g} = c\,\overline{X^k}, \quad \overline{h} = c^{-1}\,\overline{X^\ell},$$

para algún $c \in K^\times$ y para $k, \ell \geq 0$ tales que $k + \ell = n$. Notamos que $k \leq \deg g$ y $\ell \leq \deg h$, así que $k, \ell < n$, lo que implica que $k, \ell > 0$.

Sin embargo, si ambos g y h se reducen a un polinomio sin término constante, esto significa que los términos constantes de g y h están en $\mathfrak{p}$. Esto implicaría que el término constante de f está en $\mathfrak{p}^2$, pero no es el caso según la hipótesis.

Hemos llegado a una contradicción que significa que f es irreducible. ∎

[*] Nikolaĭ Chebotarëv (1894–1947), un matemático soviético.

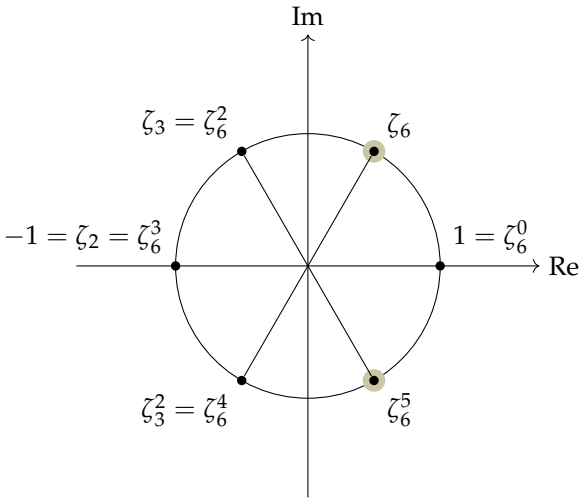
Terminemos por una aplicación importante del criterio de Eisenstein. Recordemos que el grupo de las n-ésimas raíces de la unidad

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1\} = \{\zeta_n^k \mid k = 0, \ldots, n-1\}, \quad \zeta_n := e^{2\pi\sqrt{-1}/n},$$

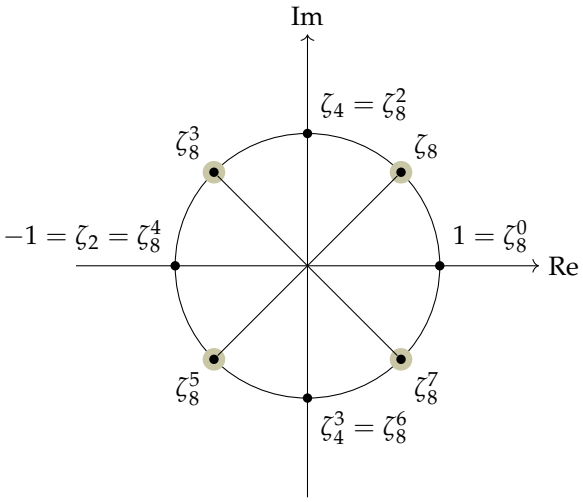
es cíclico de orden n y por ende tiene $\phi(n)$ diferentes generadores. Las raíces n-ésimas que generan a $\mu_n(\mathbb{C})$ se llaman las raíces n-ésimas **primitivas**. Son precisamente ζ_n^k donde k y n son coprimos.

13.7.10. Ejemplo. He aquí una pequeña lista de los grupos $\mu_n(\mathbb{C})$; los elementos subrayados son las raíces primitivas.

$$\begin{aligned}
\mu_1(\mathbb{C}) &= \{1\},\\
\mu_2(\mathbb{C}) &= \{1, \underline{-1}\},\\
\mu_3(\mathbb{C}) &= \{1, \underline{\zeta_3}, \underline{\zeta_3^2}\} = \left\{1, \underline{\tfrac{-1+\sqrt{-3}}{2}}, \underline{\tfrac{-1-\sqrt{-3}}{2}}\right\},\\
\mu_4(\mathbb{C}) &= \{1, \underline{\zeta_4}, \zeta_4^2, \underline{\zeta_4^3}\} = \{1, \underline{\sqrt{-1}}, -1, \underline{-\sqrt{-1}}\},\\
\mu_5(\mathbb{C}) &= \{1, \underline{\zeta_5}, \underline{\zeta_5^2}, \underline{\zeta_5^3}, \underline{\zeta_5^4}\},\\
\mu_6(\mathbb{C}) &= \{1, \underline{\zeta_6}, \zeta_6^2, \zeta_6^3, \zeta_6^4, \underline{\zeta_6^5}\} = \left\{1, \underline{\tfrac{1+\sqrt{-3}}{2}}, \frac{-1+\sqrt{-3}}{2}, -1, \frac{-1-\sqrt{-3}}{2}, \underline{\tfrac{1-\sqrt{-3}}{2}}\right\},\\
\mu_7(\mathbb{C}) &= \{1, \underline{\zeta_7}, \underline{\zeta_7^2}, \underline{\zeta_7^3}, \underline{\zeta_7^4}, \underline{\zeta_7^5}, \underline{\zeta_7^6}\},\\
\mu_8(\mathbb{C}) &= \{1, \underline{\zeta_8}, \zeta_8^2, \underline{\zeta_8^3}, \zeta_8^4, \underline{\zeta_8^5}, \zeta_8^6, \underline{\zeta_8^7}\}\\
&= \left\{1, \underline{\tfrac{\sqrt{2}+\sqrt{-2}}{2}}, \sqrt{-1}, \underline{\tfrac{-\sqrt{2}+\sqrt{-2}}{2}}, -1, \underline{\tfrac{-\sqrt{2}-\sqrt{-2}}{2}}, -\sqrt{-1}, \underline{\tfrac{-\sqrt{2}+\sqrt{-2}}{2}}\right\}.
\end{aligned}$$



El grupo $\mu_6(\mathbb{C})$



El grupo $\mu_8(\mathbb{C})$

▲

13.7.11. Definición. El n-ésimo **polinomio ciclotómico**[*] es el polinomio mónico que tiene como sus raíces las raíces n-ésimas primitivas de la unidad:

$$\Phi_n = \prod_{\substack{1\leq k<n \\ \mathrm{mcd}(k,n)=1}} (X - \zeta_n^k).$$

Este polinomio tiene grado $\phi(n) = \#\{k \mid 1 \leq k < n,\ \mathrm{mcd}(k,n) = 1\}$.

13.7.12. Ejemplo. Los primeros polinomios ciclotómicos son

$$\begin{aligned}
&\Phi_1 = X - 1,\\
&\Phi_2 = X + 1,\\
&\Phi_3 = (X - \zeta_3)\,(X - \zeta_3^2) = X^2 - (\zeta_3 + \zeta_3^2)\,X + \zeta_3^3 = X^2 + X + 1,\\
&\Phi_4 = (X - \sqrt{-1})\,(X + \sqrt{-1}) = X^2 + 1,\\
&\Phi_5 = \cdots = X^4 + X^3 + X^2 + X + 1,\\
&\Phi_6 = (X - \zeta_6)\,(X - \zeta_6^5) = X^2 - (\zeta_6 + \zeta_6^5)\,X + \zeta_6^6 = X^2 - X + 1,\\
&\Phi_7 = \cdots = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,\\
&\Phi_8 = \cdots = X^4 + 1,\\
&\quad \cdots
\end{aligned}$$

▲

13.7.13. Comentario. Aunque revisando los primeros Φ_n uno puede pensar que los coeficientes son ± 1, para $n = 105 = 3 \cdot 5 \cdot 7$ en Φ_n aparecen por primera vez coeficientes diferentes:

[*] La palabra "ciclotomia" significa "división del círculo".

$$\Phi_{105} = X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34} + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} + X^{12} - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1.$$

13.7.14. Proposición.

1) Para todo primo p se tiene

$$\Phi_p = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{p-1}.$$

2) Para todo primo p y $k \geq 1$ se tiene

$$\Phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \Phi_p(X^{p^{k-1}}) = 1 + X^{p^{k-1}} + X^{2p^{k-1}} + \cdots + X^{(p-1)\,p^{k-1}}.$$

3) Para todo n se tiene

$$\prod_{d|n} \Phi_d = X^n - 1.$$

4) Todos los polinomios Φ_n tienen coeficientes enteros.

Demostración. En la parte 1), basta notar que entre las raíces p-ésimas, todas son primitivas, salvo la raíz trivial 1.

De la misma manera, en 2) notamos que un número $1 \leq a < p^k$ tal que $a \mid p^k$ necesariamente divide a p^{k-1}, así que las raíces de orden p^k que no son primitivas son precisamente las raíces de orden p^{k-1}.

En la parte 3), basta notar que todas las n-ésimas raíces de la unidad son las raíces complejas del polinomio $X^n - 1$, y cada una de estas raíces aparece una vez como un factor $(X - z)$ en Φ_d para algún d.

La parte 4) se demuestra fácilmente por inducción. Es cierto, por ejemplo, para $n = 1$. Luego, si $\Phi_m \in \mathbb{Z}[X]$ para todo $m < n$, entonces

$$\prod_{d|n} \Phi_d = \Big(\prod_{\substack{d|n \\ d\neq n}} \Phi_d\Big) \cdot \Phi_n = X^n - 1,$$

así que

$$\Phi_n = \frac{X^n - 1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_d}.$$

A priori, este polimomio tiene coeficientes en $\mathbb{Q}$, pero

$$\operatorname{cont}\Big(\prod_{\substack{d|n \\ d\neq n}} \Phi_d\Big) \cdot \operatorname{cont}(\Phi_n) = \operatorname{cont}(X^n - 1) = 1,$$

así que $\Phi_n \in \mathbb{Z}[X]$. ∎

lección 24
16.10.18

13.7.15. Lema. *Para todo $a \in R$ un polinomio no constante $f \in R[X]$ es irreducible si y solo si $f(X + a)$ es irreducible.*

Demostración. Notamos que $\deg f(X) = \deg f(X+a)$. Una factorización no trivial $f(X+a) = g(X)\,h(X)$ nos daría una factorización $f(X) = g(X-a)\,h(X-a)$. ■

13.7.16. Proposición. *Para todo primo p el polinomio Φ_p es irreducible en $\mathbb{Z}[X]$.*

Demostración. El polinomio

$$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$$

es irreducible si y solo si

$$\begin{aligned}\Phi_p(X+1) &= 1 + (X+1) + (X+1)^2 + \cdots + (X+1)^{p-1} \\ &= \binom{p}{1} + \binom{p}{2} X + \binom{p}{3} X + \cdots + \binom{p}{p-1} X^{p-2} + \binom{p}{p} X^{p-1}\end{aligned}$$

es irreducible. Notamos que

$$\binom{p}{k} \equiv 0 \pmod{k} \text{ para todo } 1 \leq k < p,$$

pero

$$\binom{p}{1} = p \not\equiv 0 \pmod{p^2}.$$

Entonces, se puede aplicar el criterio de Eisenstein respecto al ideal $p\mathbb{Z}$. ■

13.7.17. Proposición. *Para todo primo p y $k \geq 1$ el polinomio Φ_{p^k} es irreducible en $\mathbb{Z}[X]$.*

Demostración. Ya vimos el caso $k = 1$. Podemos asumir entonces que $k \geq 2$. De nuevo, consideremos la sustitución

$$\Phi_{p^k}(X+1) = \frac{(X+1)^{p^k} - 1}{(X+1)^{p^{k-1}} - 1} = \sum_{0 \leq i \leq p-1} (X+1)^{i\,p^{k-1}}.$$

Tenemos para todo $k \geq 2$

$$(X+1)^{p^{k-1}} \equiv X^{p^{k-1}} + 1 \pmod{p},$$

y luego

$$\begin{aligned}\Phi_{p^k}(X+1) \equiv \sum_{0 \leq i \leq p-1} (X^{p^{k-1}} + 1)^i &= \frac{(X^{p^{k-1}} + 1)^p - 1}{(X^{p^{k-1}} + 1) - 1} \\ &= \frac{(X^{p^{k-1}} + 1)^p - 1}{X^{p^{k-1}}} \equiv \frac{X^{p^k}}{X^{p^{k-1}}} = X^{p^{k-1}(p-1)} \pmod{p}.\end{aligned}$$

Todos los coeficientes menores de $\Phi_{p^k}(X+1)$ son divisibles por p. El coeficiente constante es igual a

$$\Phi_{p^k}(1) = \Phi_p(1^{p^{k-1}}) = \Phi_p(1) = p,$$

que no es divisible por p^2. Podemos aplicar el criterio de Eisenstein. ■

13.7.18. Ejemplo. El polinomio $\Phi_8 = X^4 + 1$ es irreducible en $\mathbb{Z}[X]$. Esto sigue del criterio de Eisenstein aplicado a

$$\Phi_8(X+1) = X^4 + 4X^3 + 6X^2 + 4X + 2.$$

▲

En general, Gauss probó que Φ_n es irreducible para cualquier n, pero nos contentamos con el caso de $n = p^k$ como una aplicación del criterio de Eisenstein.

13.7.19. Ejemplo. Probemos que el polinomio $f = X^2 + Y^2 - Z^2$ es irreducible en $\mathbb{C}[X, Y, Z]$.

Usando la identificación $\mathbb{C}[X, Y, Z] \cong \mathbb{C}[Y, Z][X]$, podemos considerar f como un polinomio en X con término constante $Y^2 - Z^2$. Para aplicar el criterio de Eisenstein, necesitamos encontrar un ideal primo $\mathfrak{p} \subset \mathbb{C}[Y, Z]$ tal que $Y^2 - Z^2 \in \mathfrak{p}$, pero $Y^2 - Z^2 \notin \mathfrak{p}^2$. Sería suficiente tomar $\mathfrak{p} = (p)$ donde $p \in \mathbb{C}[Y, Z]$ es algún polinomio irreducible en $\mathbb{C}[Y, Z]$ tal que $p \mid (Y^2 - Z^2)$, pero $p^2 \nmid (Y^2 - Z^2)$. El mismo $Y^2 - Z^2$ es reducible: se tiene

$$Y^2 - Z^2 = (Y + Z)\,(Y - Z).$$

Sin embargo, cada uno de los factores $Y \pm Z$ es irreducible, siendo un polinomio lineal, y su cuadrado no divide a $Y^2 - Z^2$. Podemos generalizar este argumento al caso de

$$f = X^n + Y^n - Z^n \in \mathbb{C}[X, Y, Z].$$

De la misma manera, bastaría ver que el polinomio $Y^n - Z^n$ no tiene cuadrados en su factorización en $\mathbb{C}[Y, Z]$. Notamos que en el cuerpo de fracciones $\mathbb{C}(Y, Z) = \{f/g \mid f, g \in \mathbb{C}[Y, Z],\ g \neq 0\}$ se tiene

$$\left(\frac{Y}{Z}\right)^n - 1 = \prod_{0 \leq k \leq n-1} \left(\frac{Y}{Z} - \zeta_n^k\right),$$

donde $\zeta_n := e^{2\pi\sqrt{-1}/n}$, y luego

$$Y^n - Z^n = \prod_{0 \leq k \leq n-1} (Y - \zeta_n^k\, Z).$$

Las ecuaciones de la forma $X^n + Y^n - Z^n$ se conocen como las **ecuaciones de Fermat**. El **último teorema de Fermat** (demostrado en 1995 por el matemático inglés Andrew Wiles con ayuda de Richard Taylor) afirma que para $n > 2$ sus únicas soluciones racionales son de la forma

$$\begin{cases} \{(x, 0, x), (0, y, y)\}, & n \text{ impar}, \\ \{(\pm x, 0, \pm x), (0, \pm y, \pm y)\}, & n \text{ par}. \end{cases}$$

▲

13.8 Ejercicios

Ejercicio 13.1. *Hemos notado que el anillo $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única. En este ejercicio vamos a probar que en efecto $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de ideales principales. De nuevo, nos va a servir la norma*

$$N(a+b\sqrt{-5}) := (a+b\sqrt{-5})\,(a-b\sqrt{-5}) = a^2+5\,b^2.$$

Consideremos el ideal $I = (3, 2+\sqrt{-5})$. Supongamos que $I = (\alpha)$ para algún $\alpha \in \mathbb{Z}[\sqrt{-5}]$. En particular, existen $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$ tales que

$$3 = \beta\alpha, \quad 2+\sqrt{-5} = \gamma\alpha.$$

Analice las normas y obtenga una contradicción. Concluya que el ideal I no es principal.

Ejercicio 13.2. *Sea $n \geq 3$ un entero libre de cuadrados. En este ejercicio vamos a probar que el anillo $\mathbb{Z}[\sqrt{-n}]$ no es un dominio de factorización única. (Los anillos $\mathbb{Z}[\sqrt{-1}]$ y $\mathbb{Z}[\sqrt{-2}]$ son dominios euclidianos y por ende sí son dominios de factorización única.) Consideremos la norma*

$$N(a+b\sqrt{-n}) := (a+b\sqrt{-n})\,(a-b\sqrt{-n}) = a^2+n\,b^2.$$

1) *Demuestre que 2 es irreducible en $\mathbb{Z}[\sqrt{-n}]$.*

2) *Demuestre que $1 \pm \sqrt{-n}$ es irreducible en $\mathbb{Z}[\sqrt{-n}]$.*
   Indicación: si $1 \pm \sqrt{-n} = xy$ para $x, y \notin \mathbb{Z}[\sqrt{-n}]^\times$, analice las normas.

3) *Si n es par, demuestre que $2 \mid (\sqrt{-n})^2$, pero $2 \nmid \sqrt{-n}$.*

4) *Si n es impar, demuestre que $2 \mid (1+\sqrt{-n})\,(1-\sqrt{-n})$, pero $2 \nmid (1 \pm \sqrt{-n})$.*

Concluya que 2 es un elemento irreducible, pero no es primo, así que $\mathbb{Z}[\sqrt{-n}]$ no puede ser un dominio de factorización única.

Ejercicio 13.3. *Ya sabemos que los enteros de Gauss $\mathbb{Z}[\sqrt{-1}]$ forman un dominio de factorización única. En este ejercicio vamos a describir los elementos primos (irreducibles) en $\mathbb{Z}[\sqrt{-1}]$. Para encontrarlos, hay que factorizar los enteros primos $p = 2, 3, 5, 7, 11, \ldots$ en $\mathbb{Z}[\sqrt{-1}]$.*

1) *Demuestre que si para un elemento $\pi = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ la norma $N(\pi) = a^2+b^2 = p$ es un número entero primo, entonces π es un elemento primo en $\mathbb{Z}[\sqrt{-1}]$.*

2) *Sea π un elemento primo en $\mathbb{Z}[\sqrt{-1}]$. Demuestre que $\pi \mid p$ donde p es un número entero primo. Factorice $2, 3, 5$ en elementos primos en $\mathbb{Z}[\sqrt{-1}]$.*
   Sugerencia: note que $\pi \mid N(\pi)$.

3) *Sea $p \in \mathbb{Z}$ un número entero primo. Demuestre que p es compuesto en $\mathbb{Z}[\sqrt{-1}]$ si y solamente si $p = a^2+b^2$ para algunos $a, b \in \mathbb{Z}$, y en este caso p se descompone en dos factores primos conjugados.*

Comentario. En la teoría de números elemental se demuestra que un primo $p \in \mathbb{Z}$ puede ser escrito como una suma de dos cuadrados a^2+b^2 si y solamente si $p = 2$ o $p \equiv 1 \pmod 4$.

Ejercicio 13.4. *Demuestre que el anillo $\mathbb{Z}[\sqrt{-2}]$ es un dominio euclidiano respecto a la norma habitual*

$$N(a+b\sqrt{-2}) := (a+b\sqrt{-2})\,(a-b\sqrt{-2}) = a^2+2\,b^2.$$

Ejercicio 13.5. *Demuestre que el anillo $\mathbb{Z}[\omega]$ donde $\omega := \frac{1+\sqrt{-3}}{2}$ es un dominio euclidiano respecto a la norma habitual*

$$N(a+b\,\omega) := (a+b\,\omega)\,(a+b\,\overline{\omega}) = a^2+ab+b^2.$$

Ejercicio 13.6. *Sea p un número primo. Para el anillo $\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ p \nmid b \right\}$ definamos*

$$v_p\left(\frac{a}{b}\right) := \max\{k \mid p^k \mid a\}, \quad v_p(0) := +\infty.$$

1) *Demuestre que para cualesquiera $x, y \in \mathbb{Z}_{(p)}$ se cumple*

$$v_p(xy) = v_p(x) + v_p(y).$$

2) *Demuestre que todo elemento no nulo $x \in \mathbb{Z}_{(p)}$ puede ser escrito como up^n donde $u \in \mathbb{Z}_{(p)}^{\times}$ y $n = v_p(x)$.*

3) *Demuestre que todo elemento irreducible en $\mathbb{Z}_{(p)}$ está asociado con p.*

4) *Demuestre que $\mathbb{Z}_{(p)}$ es un dominio euclidiano respecto a v_p.*

Ejercicio 13.7. *Sea k un cuerpo. Consideremos el anillo de las series de potencias $k[\![X]\!]$. Definamos para $f = \sum_{i \geq 0} a_i X^i \in k[\![X]\!]$*

$$v_X(f) := \max\{i \mid a_i = 0\}, \quad v_X(0) := +\infty.$$

1) *Demuestre que para cualesquiera $f, g \in k[\![X]\!]$ se cumple*

$$v_X(fg) = v_X(f) + v_X(g).$$

2) *Demuestre que toda serie no nula $f \in k[\![X]\!]$ puede ser escrita como $g\,X^n$ donde $g \in k[\![X]\!]^{\times}$ y $n = v_X(f)$.*

3) *Demuestre que todo elemento irreducible en $k[\![X]\!]$ está asociado con X.*

4) *Demuestre que $k[\![X]\!]$ es un dominio euclidiano respecto a v_X.*

Comentario. $\mathbb{Z}_{(p)}$ y $k[\![X]\!]$ son ejemplos de **anillos de valuación discreta**.

Ejercicio 13.8. *Sea R un dominio de integridad. Una **norma de Dedekind** es una función $\delta\colon R \setminus \{0\} \to \mathbb{N}$ que satisface la siguiente propiedad: para cualesquiera $x, y \in R \setminus \{0\}$, si $x \nmid y$, entonces existen $a, b \in R$ tales que*

$$ax + by \neq 0, \quad \delta(ax + by) < \delta(x).$$

Demuestre que si sobre R existe una norma de Dedekind, entonces R es un dominio de ideales principales.

Ejercicio 13.9 (H.F. Trotter, The American Mathematical Monthly, Vol. 95, No. 4). *Definamos un **polinomio trigonométrico** como una suma finita*

$$f(x) = a_0 + \sum_{1 \leq k \leq n} (a_k \cos kx + b_k \operatorname{sen} kx),$$

*donde $a_k, b_k \in \mathbb{R}$. Digamos que el **grado** de f es el mayor k tal que $a_k \neq 0$ o $b_k \neq 0$.*

1) *Demuestre que si f y g son polinomios trigonométricos de grado m y n respectivamente, entonces fg es un polinomio trigonométrico de grado $m + n$.*

2) *Demuestre que los polinomios trigonométricos forman un dominio de integridad. Denotémoslo por $Trig_{\mathbb{R}}$.*

3) *Demuestre que los elementos invertibles en $Trig_{\mathbb{R}}$ son los polinomios trigonométricos no nulos de grado 0.*

4) *Demuestre que todo polinomio trigonométrico de grado 1 es irreducible en $Trig_{\mathbb{R}}$.*

5) *Observando la identidad $(\operatorname{sen} x)^2 = (1 + \cos x)(1 - \cos x)$, demuestre que $Trig_{\mathbb{R}}$ no es un dominio de factorización única.*

Valuaciones p-ádicas

Ejercicio 13.10. *Sea $p = 2, 3, 5, 7, \ldots$ un número primo y $k = 1, 2, 3, 4, \ldots$ Calcule que*

$$v_p\left(\binom{p^k}{n}\right) = k - v_p(n) \quad \text{para todo } n = 1, 2, \ldots, p^k.$$

Indicación: calcule las valuaciones p-ádicas de ambos lados de la identidad

$$n!\binom{p^k}{n} = p^k\,(p^k-1)\,(p^k-2)\cdots(p^k-n+1).$$

Note que $v_p(p^k - a) = v_p(a)$ para todo $a = 1, 2, \ldots, p^k - 1$

Ejercicio 13.11 (Fórmula de Legendre). *Demuestre que para todo primo p y todo número natural n se tiene*

$$v_p(n!) = \sum_{i\geq 1} \lfloor n/p^i \rfloor.$$

En particular, calcule $v_2(100!)$.

Ejercicio 13.12 (Normas p-ádicas). *Sea R un dominio de factorización única y $p \in R$ un elemento primo. Fijemos un número real $0 < \rho < 1$ y pongamos para todo $x \in R$*

$$|x|_p := \rho^{v_p(x)}.$$

Demuestre que $|\cdot|_p$ cumple las siguientes propiedades.

N1) $|x|_p = 0$ *si y solo si* $x = 0$.

N2) $|xy|_p = |x|_p \cdot |y|_p$.

N3) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$, *y se cumple la igualdad si* $|x|_p \neq |y|_p$.

Factorizaciones de polinomios

Ejercicio 13.13. *Compile una lista de los polinomios cuadráticos irreducibles en $\mathbb{F}_3[X]$.*

Ejercicio 13.14. *Sean k un cuerpo y $f \in k[X]$ un polinomio de grado 2 o 3. Demuestre que f es irreducible en $k[X]$ si y solo si f no tiene raíces en k.*

Ejercicio 13.15. *Consideremos el polinomio $f := X^3 + 2X + 1 \in \mathbb{Z}[X]$.*

1) *Demuestre que $\overline{f} \in \mathbb{F}_2[X]$ es reducible.*
2) *Demuestre que $\overline{f} \in \mathbb{F}_3[X]$ es irreducible.*
   Indicación: use el ejercicio anterior.
3) *Demuestre que f es irreducible en $\mathbb{Z}[X]$.*

Ejercicio 13.16. *Factorice el polinomio $X^4 + 4$ en polinomios irreducibles en $\mathbb{Z}[X]$.*

Ejercicio 13.17. *Consideremos el polinomio $f = X^3 + 8X^2 + 6 \in \mathbb{Z}[X]$.*

1) *Demuestre que f es irreducible usando el criterio de Eisenstein.*

2) *Factorice este polinomio en* $\mathbb{F}_p[X]$ *para* $p = 2, 3, 5, 7$.

(En efecto, el primer primo p *tal que* $\overline{f}$ *queda irreducible en* $\mathbb{F}_p[X]$ *es* 29.*)*

Ejercicio 13.18. *Factorice el polinomio* $X^n + Y^n$ *en polinomios lineales en* $\mathbb{C}[X, Y]$.

Ejercicio 13.19 (Teorema de las raíces racionales). *Sea*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

un polinomio con coeficientes enteros. Demuestre que si $\frac{a}{b}$ *es una raíz racional de* f*, entonces* $a \mid a_0$ *y* $b \mid a_n$.

Ejercicio 13.20. *Consideremos el polinomio* $f = X^3 - nX + 2 \in \mathbb{Z}[X]$. *Demuestre que es irreducible para todo* $n \neq -1, 3, 5$. *Encuentre sus factorizaciones para* $n = -1, 3, 5$.
Indicación: use el ejercicio anterior.

Ejercicio 13.21. *Encuentre los coeficientes en la expansión de los polinomios ciclotómicos* Φ_{10} *y* Φ_{15}.

Ejercicio 13.22. *Sea* p *un número primo. Factorice el polinomio ciclotómico* Φ_{p^k} *en* $\mathbb{F}_p[X]$.

Bibliografía

[DF2004] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[IR1990] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716
https://doi.org/10.1007/978-1-4757-2103-4