IV, §6. PRINCIPAL RINGS AND FACTORIAL RINGS

We have seen a systematic analogy between the ring of integers $\mathbf{Z}$ and the ring of polynomials $K[t]$. Both have a Euclidean algorithm; both have unique factorization into certain elements, which are called **primes** in $\mathbf{Z}$ or **irreducible polynomials** in $K[t]$. It turns out actually that the most important property is not the Euclidean algorithm, but another property which we now axiomatize.

Definición (de anillo principal)

Let R be an integral ring. We say that R is a **principal ring** if in addition every ideal of R is principal.

Ejemplos: Ya vimos que $\mathbb{Z}$ y $K[X]$ (K cuerpo) son anillos principales.

También vimos que $\mathbb{Z}[X]$ no lo era.

Practically all the properties which we have proved for $\mathbf{Z}$ or for $K[t]$ are also valid for principal rings. We shall now make a list.

Definición 1 (elementos primos o irreducibles)

Let R be an integral ring. Let $p \in R$ and $p \neq 0$. We define p to be **prime** if p is not a unit, and given a factorization

(o irreducible)

$$p = ab \qquad \text{with} \quad a, b \in R$$

then a or b is a unit.

(p primo si $p=ab \Rightarrow \begin{cases} a \in R^* \\ \text{o} \\ b \in R^* \end{cases}$

- Elementos primos en $\mathbb{Z}$: $\pm p$, p número primo.

- Elementos primos en $k[X]$ (k cuerpo): Polinomios irreducibles $f(X) \in k[X]$.

Ejemplo 1: $p(X) \in K[X]$ de grado ≤ 3 sin raíces.

(pues $p(X) = q(X)(aX+b) \Rightarrow x = -\frac{b}{a}$ es raíz)

$X^2+X+1 \in \mathbb{F}_2[X]$ es irreducible

$X^2+1 \in \mathbb{F}_2[X]$ es reducible (1 es raíz): $X^2+1 = (X+1)^2$

$X^2+1 \in \mathbb{F}_3[X]$ es irreducible.

$X^3+2X+2 \in \mathbb{F}_3[X]$ es irreducible (luego $\frac{\mathbb{F}_3[X]}{(X^3+2X+2)}$ es un cuerpo con 27 elementos)

$X^3+6X^2+X+2 \in \mathbb{Q}[X]$ es irreducible (pues sus únicas posibles raíces serían $\pm 1, \pm 2$).

Ejemplo 2: Criterio de Eisenstein

$2X^7+9X^5+3X^4+6X^3+27X^2+12 \in \mathbb{Q}[X]$ es irreducible

(por el criterio de Eisenstein para $p=3$).

$p/12 \wedge p^2 \nmid 12$
$p/27$
$p/6$
$p/3$ $\Rightarrow$ f irr
$p/9$
$p \nmid 2$

Recordemos este criterio:

Theorem 5.4 (Eisenstein's criterion). *Let*

$$f(t) = a_n t^n + \cdots + a_0$$

be a polynomial of degree $n \geq 1$ with integer coefficients. Let p be a prime, and assume

$$a_n \not\equiv 0 \pmod{p}, \qquad a_i \equiv 0 \pmod{p} \quad \text{for all} \quad i < n,$$

$$a_0 \not\equiv 0 \pmod{p^2}.$$

Then f is irreducible over the rationals.

Ejemplo 3. En $\mathbb{C}[X]$ sólo los polinomios de grado 1 son irreducibles, pues $\forall f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{C}[X]$

$f(X) = a_n (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$, donde $\alpha_i \in \mathbb{C}$ son las raíces de $f(X)$. (Teorema Fundamental del Álgebra)

Ejemplo 4 En $\mathbb{R}[X]$ había polinomios irreducibles de grados 1 y 2, e.g. X^2+1

Ejemplo 6. En $\mathbb{Z}[X]$ la situación era diferente.

El polinomio $2x^3+36X^2+124 = 2(x^3+18x^2+62) = 2\cdot q(x)$ es irreducible en $\mathbb{Q}[X]$ porque $q(x)$ lo es (c. Eisenstein con $p=2$) y 2 es una unidad. Pero es reducible en $\mathbb{Z}[X]$ porque 2 no es unidad en $\mathbb{Z}[X]$.

Y, por el lema de Gauss, eso es todo lo que podía ocurrir:

Proposición:

Sea $f(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$, $\deg(f) \geq 1$. Entonces $f(X)$ es irreducible en $\mathbb{Z}[X] \Leftrightarrow f(X)$ es irreducible en $\mathbb{Q}[X]$ y primitivo (i.e. $\mathrm{mcd}(\text{coef. } f(x)) = \mathrm{mcd}(a_0, a_1, \dots, a_n) = 1$).

- En particular, los irred. de $\mathbb{Z}[X]$ son los primos de $\mathbb{Z}$ y los irred. de $\mathbb{Q}[X]$ primitivos.

$(A[X])^* = A^*$, A íntegro

Recordemos la prueba:

$\Leftarrow$) Supongamos que $f = gh$ con $g, h \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$. Entonces, como f es irred. en $\mathbb{Q}[X]$, g ó h es unidad $\Rightarrow g$ ó $h \in \mathbb{Z} \Rightarrow$

$\Rightarrow f = \underbrace{g}_{\in\mathbb{Z}} \cdot (\underbrace{b_0 + b_1X + \dots + b_rX^r}_{h}) = gb_0 + gb_1X + \dots + gb_nX^n$

con $\mathrm{mcd}(\underbrace{gb_0}_{a_0}, \underbrace{gb_1}_{a_1}, \dots, \underbrace{gb_n}_{a_n}) = 1 \Rightarrow g = \pm 1 \Rightarrow$

$\Rightarrow f$ es irreducible en $\mathbb{Z}[X]$.

$\Rightarrow$) Si f es irreducible en $\mathbb{Z}[X]$ tiene que ser primitivo, pues si $\mathrm{mcd}(a_0, a_1, \dots a_n) = d > 1$ entonces $f = d \cdot \left(\frac{a_0}{d} + \frac{a_1}{d}X + \dots + \frac{a_n}{d}X^n\right)$; $\frac{a_k}{d} \in \mathbb{Z}$ luego f no sería irreducible en $\mathbb{Z}$.

Falta ver que f es irreducible en $\mathbb{Q}[X]$.

Si $f = gh$ con $g, h \in \mathbb{Q}[X]$, ponemos: $g(x) = \frac{a}{b} p(x)$, $h(x) = \frac{c}{d} q(x)$ donde $a, b, c, d \in \mathbb{Z}$ de modo que $p(x), q(x) \in \mathbb{Z}[X]$ y son primitivos.

Entonces $f = \frac{ac}{bd} p(x) q(x) \Rightarrow$

$\Rightarrow bd\, f = ac\, p(x) q(x)$

Ahora por el lema de Gauss

$p(x) q(x)$ es primitivo. Y como f también lo es, tendremos $bd = mcd(\text{coef. } bd\, f) = mcd(\text{coef } ac\, pq) = \pm ac$

$\Rightarrow \frac{ac}{bd} = \pm 1 \Rightarrow f(x) = \pm p(x) q(x) \Rightarrow p(x)(\acute{o}\, q(x))$ (f irr. en $\mathbb{Z}[X]$)

es una unidad en $\mathbb{Z}[X] \Rightarrow g(x)(\acute{o}\, h(x))$ es unidad en $\mathbb{Q}[X]$

$\Rightarrow f$ es irr. en $\mathbb{Q}[X]$ c.q.d.

e.g.:

$\frac{3}{7} X + \frac{6}{5} X^3 = \frac{1}{35}(15X + 42X^3) =$

$= \frac{3}{35}(5X + 14X^3)$

$g(x)$ $p(x)$

↓

Esto es el Lema de Gauss (producto de primitivos es primitivo)

$$\left.\begin{array}{l} g \in \mathbb{Z}[X],\ mcd(\text{coef. } g) = 1 \\ h \in \mathbb{Z}[X],\ mcd(\text{coef. } h) = 1 \end{array}\right\} \Rightarrow mcd(\text{coef. } gh) = 1$$

Demostr. (Red. Abs.) Supongamos que p es un número primo que divide a todos los coeficientes de gh.

Consideramos el homomorfismo $\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$, $f = \sum a_i x^i \mapsto \sum \bar{a}_i x^i = \bar{f}$

Estamos suponiendo que $\bar{g}\bar{h} = \bar{0} \Rightarrow \bar{g}\bar{h} = \bar{0} \Rightarrow \bar{g}(\acute{o}\, \bar{h}) = \bar{0} \Rightarrow$

$\Rightarrow mcd(\text{coef. } \bar{g})(\acute{o}\, mcd(\text{coef. } h))$ es un múltiplo de p. $\Rightarrow g$ no es primit.

Contradicción.

Ejemplos: Criterio de reducción

$X^3+17X+62 \in \mathbb{Q}[X]$ es irreducible (porque lo es en $\mathbb{F}_3[X]$: sobre $\mathbb{F}_3$ este polinomio es $x^3+\bar{2}x+\bar{2}$ que hemos visto que es irreducible)

Recordemos este criterio:

Theorem 5.5 (Reduction criterion). *Let $f(t) \in \mathbf{Z}[t]$ be a ~~primitive~~ polynomial with leading coefficient $a_n \neq 1$ which is not ~~divisible by a prime~~. Let $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} = F_p$ be reduction mod p, and denote the image of f by $\bar{f}$. If $\bar{f}$ is irreducible in $F_p[t]$, then f is irreducible in $\mathbf{Q}[t]$.*

Prueba: Consideramos, de nuevo, el homomorfismo de anillos $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$

$$f(x) = \sum a_i x^i \longmapsto \varphi(f(x)) = \overline{f(x)} = \sum \bar{a}_i x^i$$

Por ser mónico, f es obviamente primitivo, luego por el lema de Gauss basta ver que f es irreducible en $\mathbb{Z}[X]$

Pero si fuese $f = p \cdot q$ con $p, q \in \mathbb{Z}[X]$ entonces $\bar{f} = \bar{p} \cdot \bar{q}$, contradiciendo el hecho de que $\bar{f} \in \mathbb{F}_p[X]$ es irreducible.

Definición 2 (factorización única)

An element $a \in R$, $a \neq 0$ is said to have **unique factorization** into primes if there exists a unit u and there exist prime elements p_i $(i = 1, \ldots, r)$ in R (not necessarily distinct) such that

$$a = up_1 \cdots p_r;$$

{ u = unidad
p_i's = primos

and if given two factorizations into prime elements

$$a = up_1 \cdots p_r = u'q_1 \cdots q_s,$$

(unicidad de la factorización)

then $r = s$ and after a permutation of the indices i, we have $p_i = u_i q_i$, where u_i is a unit $i = 1, \ldots, r$.

Ejemplo 7

1) $R = \mathbb{Z}$, $a = 15 = 3 \cdot 5$ (p_1 p_2)
$= (-1)(-3) \cdot 5$ (u q_1 q_2)

2) $R = \mathbb{Q}[X]$ $a = x^2 - 1 = (x-1)(x+1) =$ (p_1, p_2)
$= 3(x-1) \cdot \frac{1}{3}(x+1)$ (q_1, q_2)

Observación

We note that if p is prime and u is a unit, then up is also prime, so we must allow multiplication by units in the factorization. In the ring of integers $\mathbf{Z}$, the ordering allows us to select a representative prime element, namely a prime number, out of two possible ones differing by a unit, namely $\pm p$, by selecting the positive one. This is, of course, impossible in more general rings. However, in the ring of polynomials over a field, we can select the prime element to be the irreducible polynomial with leading coefficient 1. (polinomio mónico)

$\mathbb{Q}[X]$ $\frac{2}{3} + 5X^2$ no tiene raíces $\Rightarrow$ irr $\Rightarrow$ $a(\frac{2}{3} + 5X^2)$ escrib, $a \neq 0$
$(a = 1/5)$ $\frac{2}{15} + X^2$ es irr y es mónico

Definición 3. (anillos factoriales)

A ring is called **factorial**, or a **unique factorization ring**, if it is integral, and if every element $\neq 0$ has a unique factorization into primes.

Ejemplos. $\mathbb{Z}$ y $K[X]$ (K, un cuerpo) son anillos factoriales (como sabemos del curso de Conjuntos y Números)

Ejemplo 9. $\mathbb{Z}[\sqrt{-5}] := \{a+b\sqrt{5}i \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$ es un subanillo de $\mathbb{C}$ que no es factorial.

- Es un subanillo:

a) $1 = 1 + 0\sqrt{5}i \in \mathbb{Z}[-\sqrt{5}]$

b) $z_1, z_2 \in \mathbb{Z}[-\sqrt{5}] \Rightarrow \begin{cases} z_1 = a_1 + b_1\sqrt{5}i\,;\ a_1, b_1 \in \mathbb{Z} \\ z_2 = a_2 + b_2\sqrt{5}i\,;\ a_2, b_2 \in \mathbb{Z} \end{cases} \Rightarrow$

$\Rightarrow z_1 + z_2 = (a_1+a_2) + (b_1+b_2)\sqrt{5}i \in \mathbb{Z}[\sqrt{-5}]$.

c) $z_1 \cdot z_2 = (a_1 + b_1\sqrt{5}i)(a_2 + b_2\sqrt{5}i) =$

$= (a_1a_2 - b_1b_2 5) + (a_1b_2 + b_1a_2)\sqrt{5}i \in \mathbb{Z}[\sqrt{-5}]$

- Es un anillo integro pues está en $\mathbb{C}$.

• Unidades de $\mathbb{Z}[\sqrt{-5}]$

$u = a+b\sqrt{5}i$ es una unidad si $\exists\, u' = a'+b'\sqrt{5}i$ tal que $1 = uu' \Rightarrow 1 = |uu'|^2 = |u|^2|u'|^2 \Rightarrow$ (norma)

$\Rightarrow 1 = (a^2+5b^2)(a'^2+5b'^2)$, con $a,b,a',b' \in \mathbb{Z}$

$\Rightarrow b = 0, a = \pm 1$, luego las unidades son ± 1

• $w = 3,\ 2+\sqrt{5}i,\ 2-\sqrt{5}i$ son elementos irreducibles

$w = zz' \Rightarrow |w|^2 = |z|^2|z'|^2 \Rightarrow 9 = (a^2+5b^2)(a'^2+5b'^2)$

($|z|^2$, $|z'|^2$)

$$\Rightarrow \begin{cases} a^2+5b^2 = 1 \wedge a'^2+5b^2 = 9 \\ a^2+5b^2 = 3 \wedge a'^2+5b^2 = 3 \\ a^2+5b^2 = 9 \wedge a'^2+5b'^2 = 1 \end{cases} \xRightarrow[(w=zz')]{} \begin{cases} z = \pm 1 \wedge z' = \pm w \\ z' = \pm 1 \wedge z = \pm w \end{cases} \Rightarrow w \text{ es irred.}$$

• Tenemos las dos siguientes factorizaciones de 9

$$9 = 3\cdot 3 = (2+\sqrt{5}i)(2-\sqrt{5}i)$$

$2+\sqrt{5}i \neq \pm 3$

i.e no hay factorización única $\Rightarrow$

$\mathbb{Z}[\sqrt{-5}]$ no es un dominio factorial.

• Ejemplo 10.

¿Y el anillo de los enteros de Gauss:

$$\mathbb{Z}[i] = \{ a+bi / \ a, b \in \mathbb{Z} \}$$?

Claramente $(\mathbb{Z}[i])^* = U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

Consideremos las dos siguientes descomposiciones de 10:

$$10 = 2 \cdot 5 = (3+i)(3-i) \qquad (*)$$

¿Prueba esto que $\mathbb{Z}[i]$ no es factorial?

Pues, en principio, no, porque 5 no es primo:

$5 = (2+i)(2-i)$. → ninguno es unidad.

Y $(3+i)$ y $(3-i)$ tampoco:

$(3+i) = (2-i)(1+i)$

$(3-i) = (2+i)(1-i)$

Sustituyendo estas relaciones en $(*)$ queda:

$$10 = 2(2+i)(2-i) = (2-i)(1+i)(2+i)(1-i) \qquad (**)$$

¿Y ahora tenemos dos factorizaciones distintas?

Pues todavía no, porque 2 tampoco es primo:

$$2 = (1+i)(1-i)$$

Sustituyendo esta relación en $(**)$ queda:

$10 = (1+i)(1-i)(2+i)(2-i) = (2-i)(1+i)(2+i)(1-i)$

que sí que son la misma factorización

(salvo el orden).

Luego $\mathbb{Z}[i]$ todavía puede ser factorial

(y, de hecho, veremos que va a serlo)

En cualquier dominio de integridad tiene sentido el concepto de divisibilidad análogo al que tenemos en los anillos $\mathbb{Z}$ y $K[X]$:

Let R be an integral ring, and $a, b \in R$, $a \neq 0$. We say that a **divides** b and write $a|b$ if there exists $c \in R$ such that $ac = b$. We say that $d \in R$, $d \neq 0$ is a **greatest common divisor** of a and b if $d|a$, $d|b$, and if any element c of R, $c \neq 0$ divides both a and b, then c also divides d. Note that a g.c.d. is determined only up to multiplication by a unit.

m.c.d.

En los anillos factoriales estos conceptos van a tener propiedades análogas a las que conocemos en $\mathbb{Z}$ y $K[X]$.

Nuestro próximo objetivo es probar que los anillos principales son siempre factoriales.

Empezaremos probando el siguiente resultado:

Proposition 6.1. *Let R be a principal ring. Let $a, b \in R$ and $ab \neq 0$. Let $(a, b) = (c)$, that is let c be a generator of the ideal (a, b). Then c is a greatest common divisor of a and b.*

i.e. si R es principal, $(a,b)=(c) \Rightarrow c = \text{m.c.d.}(a,b)$

Proof. Since b lies in the ideal (c), we can write $b = xc$ for some $x \in R$, so that $c|b$. Similarly, $c|a$. Let d divide both a and b, and write $a = dy$, $b = dz$ with $y, z \in R$. Since c lies in (a, b) we can write

$$c = wa + tb$$

with some $w, t \in R$. Then $c = wdy + tdz = d(wy + tz)$, whence $d|c$, and our proposition is proved.

Theorem 6.2. *Let R be a principal ring. Then R is factorial.*

Ejemplo 11. El anillo $\mathbb{Z}[i] = \{a+bi / a,b \in \mathbb{Z}\}$ va a ser factorial (como habíamos anunciado) porque es principal. De hecho, para cualquier ideal $I \subset \mathbb{Z}[i]$ vamos a tener

$$I = (\alpha), \text{ donde } 0 \neq \alpha \in I \text{ con norma } |\alpha| \text{ mínima.}$$

Veamos esto:

Sea $\beta \in I$, deseamos ver que $\beta = \gamma\alpha$, para algún $\gamma \in \mathbb{Z}[i]$. ($\mathbb{Q}(i)$)

Consideremos el cociente $\frac{\beta}{\alpha} = r + si \in \mathbb{Q}(i)$

y sean $m,n \in \mathbb{Z}$ tales que $\begin{cases} |r-m| \leq 1/2 \\ |s-n| \leq 1/2 \end{cases}$

$\beta = (r+si)\alpha$ ✗

Sea $\gamma = m+ni \in \mathbb{Z}[i]$. Afirmo que $\beta = \gamma\alpha$.

$$|\beta - \gamma\alpha|^2 = |\alpha(\tfrac{\beta}{\alpha} - \gamma)|^2 = |\alpha|^2 |(r+si) - (m+ni)|^2 =$$

$$= |\alpha|^2 |(r-m) + (s-n)i|^2 = |\alpha|^2 ((r-m)^2 + (s-n)^2) \leq |\alpha|^2 (\tfrac{1}{4} + \tfrac{1}{4}) \Rightarrow$$

$$\Rightarrow |\underset{\in I}{\beta} - \underset{\in I}{\gamma\alpha}|^2 < |\alpha|^2 \Rightarrow \beta - \gamma\alpha = 0 \Rightarrow \beta = \gamma \cdot \alpha \quad \text{c.q.d.}$$

Observ: $5 = (2+i)(2-i) = (1+2i)(1-2i)$ no son factorizaciones distintas, pues $1+2i = i(2-i)$ y $(1-2i) = (-i)(2+i)$.

DEMOSTRACIÓN DEL TEOREMA: R principal ⇒ R factorial

1er paso) Si a irred $\Rightarrow a = a$ c.q.d. Si no $a = a_1 b_1 \Rightarrow (a) \subsetneq (a_1)$.

2º paso) Si a_1, b_1 irred $\Rightarrow a = a_1 b_1$ ". Si no $a_1 = a_2 b_2 \Rightarrow (a) \subsetneq (a_1) \subsetneq (a_2)$

3er paso) " a_2, b_2 " $\Rightarrow a = a_2 b_2 b_1$ " ... " $a_2 = a_3 b_3 \Rightarrow (a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3)$

4º paso) " a_3, b_3 " $\Rightarrow a = a_3 b_3 b_2 b_1$ " ... " $a_3 = a_4 b_4 \Rightarrow (a) \subsetneq (a_1) \subsetneq (a_3) \subsetneq (a_4)$

Basta ver que en algún momento esta cadena para, i.e. $(a_n) \subsetneq (a_{n+1})$ i.e. que (a_n) es max.

Proof. We first prove that every non-zero element of R has a factorization into irreducible elements. Given $a \in R$, $a \neq 0$. If a is prime, we are done. If not, then $a = a_1 b_1$ where neither a_1 nor b_1 is a unit. Then $(a) \subset (a_1)$. We assert that

$$(a) \neq (a_1).$$

Indeed, if $(a) = (a_1)$ then $a_1 = ax$ for some $x \in R$ and then $a = axb_1$ so $xb_1 = 1$, whence both x, b_1 are units contrary to assumption. If both a_1, b_1 are prime, we are done. Suppose that a_1 is not prime. Then $a_1 = a_2 b_2$ where neither a_2 nor b_2 are units. Then $(a_1) \subset (a_2)$, and by what we have just seen, $(a_1) \neq (a_2)$. Proceeding in this way we obtain a chain of ideals

(Necesitamos ver que después de n pasos este proceso se acaba)

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots \subsetneq (a_n) \subsetneq \ldots.$$

We claim that actually, this chain must stop for some integer n. Let

$0 \in (a_n) \Rightarrow 0 \in J$

$x, y \in J \Rightarrow \begin{cases} x \in (a_n) \\ y \in (a_m) \end{cases} \Rightarrow x, y \in (a_m) \Rightarrow x + y \in J$ (con $m \geq n$)

$a \in R, x \in J \Rightarrow ax \in (a_n) \Rightarrow ax \in J$

$$J = \bigcup_{n=1}^{\infty} (a_n).$$

(En general I_1, I_2 ideales $\not\Rightarrow I_1 \cup I_2$ ideal ejemplo??)

Then J is an ideal. By assumption J is principal, so $J = (c)$ for some element $c \in R$. But c lies in the ideal (a_n) for some n, and so we have the double inclusion

$$(a_n) \subset (c) \subset (a_n),$$

($c \in J$) whence $(c) = (a_n)$. Therefore $(a_n) = (a_{n+1}) = \ldots$, and the chain of ideals could not have proper inclusions at each step. This implies that a can be expressed as a product

$$a = p_1 \cdots p_r \qquad \text{where } p_1, \ldots, p_r \text{ are prime.}$$

(Nos falta probar la unicidad)

Next we prove the uniqueness.

Lemma 6.3. *Let R be a principal ring. Let p be a prime element. Let a, $b \in R$. If $p|ab$ then $p|a$ or $p|b$.*

Proof. If $p \nmid a$ then a g.c.d. of p, a is 1, and (p, a) is the unit ideal. Hence we can write

$$1 = xp + ya$$

with some x, $y \in R$. Then $b = bxp + yab$, and since $p|ab$, we conclude that $p|b$. This proves the lemma.

Ahora ya podemos probar la unicidad.

Suppose finally that a has two factorizations

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

into prime elements. Since p_1 divides the product furthest to the right, it follows by the lemma that p_1 divides one of the factors, which we may assume to be q_1 after renumbering these factors. Then there exists a unit u_1 such that $q_1 = u_1 p_1$. We can now cancel p_1 from both factorizations and get

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

The argument is completed by induction. This concludes the proof of the theorem.

Ejemplo 12: $K[X]$ es un anillo factorial, cualquiera que sea el cuerpo K. (e.g. $\mathbb{F}_p[X]$ es factorial).

($\mathbb{Z}[X]$ no es principal y sí va a ser factorial)

$I = (2, X)$ no es principal.

Proposition 6.4. *Let R be a factorial ring. An element $p \in R$, $p \neq 0$ is prime if and only if the ideal (p) is prime.*

1) (irreducible ⇔) 2) Y si R es principal (p) es maximal.

Demostración:

1) Note that for any integral ring R, we have the implication

$$a \in R,\ a \neq 0 \text{ and } (a) \text{ prime} \quad \Rightarrow \quad a \text{ prime.}$$ (i.e. irreducible)

Indeed, if we write $a = bc$ (⇒ $bc \in (a)$) with $b, c \in R$ then $b \in (a)$ or $c \in (a)$ by definition of a prime ideal. Say we can write $b = ad$ with some $d \in R$. Then $a = acd$. Hence $cd = 1$, whence c, d are units, and therefore a is prime.

In a factorial ring, we also have the converse, because of unique factorization. ~~If a principal ring, the [illegible] Lemma 6.5, which means precisely that (p) is a prime ideal.~~

R factorial, $a \in R$ irreducible $\Rightarrow (a)$ primo.

Veamos esto:

$xy \in (a) \Rightarrow xy = ba$. Descomponiendo en factores primos esta igualdad queda:

$$\underbrace{p_1 p_2 \cdots p_e}_{x} \cdot \underbrace{q_1 \cdots q_s}_{y} = \underbrace{r_1 r_2 \cdots r_d}_{b} \cdot a \Rightarrow \begin{cases} a = u\, p_k, & u \in R^* \\ \text{o} \\ a = v\, q_j, & v \in R^* \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} p_k \in (a) \\ \text{o} \\ q_j \in (a) \end{cases} \Rightarrow \begin{cases} x = p_1 \cdots p_e \in (a) \\ \text{o} \\ y = q_1 \cdots q_s \in (a) \end{cases} \qquad \text{c.q.d.}$$

2) Supongamos $(p) \subseteq I \neq R$. Si R es principal, $I = (c) \Rightarrow (p) \subseteq (c) \Rightarrow$

$\Rightarrow p = xc \Rightarrow$ (p irred) $\begin{cases} c \text{ ~~unidad~~ (no, porque } I = (c) \neq R. \\ x \text{ unidad} \Rightarrow (c) = (x^{-1} \cdot p) = (p). \end{cases}$ c.q.d

$(p) \neq 0$

$\{(ua) = (a)\ ;\ ua \in (a)$, $a \in (ua)$ pues $a = u^{-1} \cdot ua\}$

Pregunta: ¿Si el dominio no es factorial, puede ocurrir que un elemento irreducible a genere un ideal (a) no primo? Pues sí:

Ejemplo 13: Consideremos el anillo $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{5}i \,/\, a,b \in \mathbb{Z}\}$ que vimos que no es factorial.

También habíamos visto el elemento $a=3$ es irreducible. ¿Pero es (3) un ideal primo?

$(2+\sqrt{-5})(2-\sqrt{-5}) = 9 \in (3) \overset{?}{\Rightarrow} 2+\sqrt{-5}$ ó $2-\sqrt{-5} \in (3)$

$2+\sqrt{-5} \in (3) \Leftrightarrow 2+\sqrt{-5} = (a+b\sqrt{-5})3 \Rightarrow |a+b\sqrt{-5}|^2 = 1 \Rightarrow$

($2+\sqrt{-5} = 2+\sqrt{5}i$)

$\Rightarrow a^2+5b^2 = 1 \Rightarrow$

$\Rightarrow \begin{cases} a = \pm 1 \\ b = 0 \end{cases} \Rightarrow$

$\Rightarrow 2+\sqrt{-5} = (a+b\sqrt{-5})3$

es imposible $\Rightarrow$

$\Rightarrow 2+\sqrt{5} \notin (3)$ (y lo mismo para $2-\sqrt{5}$)

Conclusión: Si R no es factorial puede ocurrir que un elemento irreducible no genere un ideal primo.

El siguiente teorema nos va a permitir crear muchos ejemplos de anillos factoriales:

> **A factorial $\Rightarrow A[X]$ factorial**

Ejemplos: $\mathbb{Z}[X]$, $K[X]$, $K[X][Y]$, etc.

Let R be an integral ring, and $a, b \in R$, $a \neq 0$. We say that a **divides** b and write $a|b$ if there exists $c \in R$ such that $ac = b$. We say that $d \in R$, $d \neq 0$ is a **greatest common divisor** of a and b if $d|a$, $d|b$, and if any element c of R, $c \neq 0$ divides both a and b, then c also divides d. Note that a g.c.d. is determined only up to multiplication by a unit.

- Como en el caso de $\mathbb{Z}$, si R es un anillo integro y $f(X) = a_0 + a_1X + \dots + a_nX^n$ es un polinomio en $R[X]$ se dice que f es <u>primitivo</u> si

$$\text{mcd}(\text{coef. } f(X)) = \text{m.c.d}(a_0, a_1, \dots, a_n) = 1$$

- Si R es, además, factorial, sigue siendo válido el lema de Gauss y, por tanto, el resultado siguiente (igual que para $\mathbb{Z}$).

<u>Proposición</u>. Sea K el cuerpo de fracciones de R. Sea $f(X) \in R[X]$ con $\deg(f) \geq 1$. Entonces $f(X) \in R[X]$ es irreducible $\iff$ f es irreducible en $K[X]$ y primitivo

La demostración es la misma. Vale el lema de Gauss. El truco del homomorfismo $R[X] \to (R/(p))[X]$ sigue funcionando porque aunque

$R/(p)$ no sea un cuerpo, si va a ser integro, si $p \in R$ es irreducible, y esto es todo lo que se necesita.

Corolario: Si R es un anillo factorial y K es su cuerpo de cocientes, los elementos primos de $R[X]$ son los irreducibles de R y los polinomios primitivos irreducibles en $K[X]$.

Y, de hecho, $R[X]$ va a ser un anillo factorial.

Theorem 6.9. *Let R be a factorial ring. Then $R[t]$ is factorial. The units of $R[t]$ are the units of R. The prime elements of $R[t]$ are either the primes of R, or the primitive irreducible polynomials in $R[t]$.*

Demostración.

1) La última parte subrayada en verde ya la hemos visto.

2) Veamos que todo polinomio $f(t) \in R[t]$ admite una factorización como producto de primos.

Let $f(t) \in R[t]$. We can write $f = cg$ where c is the g.c.d. of the coefficients of f, and g then has relatively prime coefficients. We know that c has unique factorization in R by hypothesis. Let Luego basta probar

" g " " " " R[X].

(primitivo)

Let $g = q_1 \cdots q_r$

be a factorization of g into irreducible polynomials $q_1, \ldots, q_r$ in $K[t]$. Such a factorization exists since we know that $K[t]$ is factorial. By (e incluso principal) there exist elements $b_1, \ldots, b_r \in K$ such that if we let $p_i = b_i q_i$ then p_i has relatively prime coefficients in R. Let their product be

(i.e. p_i es primitivo)

$$u = b_1 \cdots b_r.$$

Then

$$ug = p_1 \cdots p_r.$$

(e.g. $5X + 14X^3 = \frac{35}{3}\left(\frac{3}{7}X + \frac{6}{5}X^3\right)$, p, b, q)

By the Gauss Lemma (el producto de primitivos es primitivo, por ser R factorial), the right-hand side is a polynomial in $R[t]$ with relatively prime coefficients. Since g is assumed to have relatively prime coefficients in R, it follows that $u \in R$ and u is a unit in R. Then

($u = a/b \Rightarrow ag = bp_1 \cdots p_r \Rightarrow$ $a = \mathrm{mcd}(\text{coef } ag) = \mathrm{mcd}(\text{coef } bp_1 \cdots p_r) = b \Rightarrow$ $\Rightarrow a = vb, v \in R^* \Rightarrow u = a/b = v \in R^*$)

$$f = cu^{-1}p_1 \cdots p_r$$

is a factorization of f in $R[t]$ into prime elements of $R[t]$ and an element of R. Thus a factorization exists.

3) Falta ver que la factorización es única.

There remains to prove uniqueness (up to factors which are units, of course). Suppose that

$$f = cp_1 \cdots p_r = dq_1 \cdots q_s,$$

where $c, d \in R$, and $p_1, \ldots, p_r, q_1, \ldots, q_s$ are irreducible polynomials in $R[t]$ with relatively prime coefficients. If we read this relation in $K[t]$, and use the fact that $K[t]$ is factorial, as well as Theorem 6.7, then we conclude that after a permutation of indices, we have $r = s$ and there are elements $b_i \in K$, $i = 1, \ldots, r$ such that

(unidad en $K[t]$) $\qquad p_i = b_i q_i \qquad$ for $\quad i = 1, \ldots, r.$ (por la unicidad de la fact. en $K[t]$)

Since p_i, q_i have relatively prime coefficients in R, it follows that in fact b_i is a unit in R by Lemma 6.8. This proves the uniqueness.

son primitivos porque son irreducibles en $R[t]$.

Si $b_i = \frac{a_i}{d_i}$; $a_i, d_i \in R$, $\quad p_i = b_i q_i \Rightarrow p_i = \frac{a_i}{d_i} q_i \Rightarrow$

$\Rightarrow d_i p_i = a_i q_i \Rightarrow$ $\underbrace{mcd(\text{coef. } d_i p_i)}_{d_i} = \underbrace{mcd(\text{coef. } a_i q_i)}_{a_i}$

$\Rightarrow b_i = \frac{a_i}{d_i} \in R^*$ c.q.d.

Ejemplos: El anillo $\mathbb{Z}[X]$ es factorial

El anillo de polinomios en varias variables con coeficientes en un cuerpo K arbitrario (o en un anillo factorial)

$K[X][Y]$ es un anillo factorial

(donde $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(i), \mathbb{F}_p = \mathbb{Z}/(p)$, etc).

(también $\mathbb{Z}[X][Y]$)

- Un elemento $f \in \underbrace{K[X]}_{R}[Y]$ es de la forma

$$f = \sum_j a_j(X) Y^j, \quad a_j(X) = \sum_i a_{ij} X^i \quad (a_{ij} \in R)$$

$$\Rightarrow f = \sum_j \left(\sum_i a_{ij} X^i \right) Y^j = \sum_{i,j} a_{ij} X^i Y^j$$

i.e. todo elemento de $K[X][Y]$ se escribe de forma única en la forma

$$f(X,Y) = \sum a_{ij} X^i Y^j$$

y por eso escribimos $K[X][Y] = K[X,Y]$

(anillo de polinomios en dos variables con coeficientes en K)

- Si A es un anillo factorial,

el criterio de irreducibilidad

de Eisenstein sigue siendo válido

(y su demostración es la misma)

Por ejemplo, el polinomio

$$f(X,Y) = 3Y^7 + X^2Y^6 + 5X^3Y^3 + 9X^2Y + 5X$$

es un polinomio irreducible en $K[X,Y]$

porque visto en $K[X][Y]$ podemos

→ cuerpo arbitrario

tomar el elemento irreducible X

que satisface las siguientes propiedades:

Criterio de Eisenstein

$$\begin{cases} X \mid a_0 \text{ pero } X^2 \nmid a_0, & a_0 = 5X \\ X \mid a_1, & a_1 = 9X^2 \\ X \mid a_2, & a_2 = 0 \\ X \mid a_3, & a_3 = 5X^3 \\ X \mid a_4, & a_4 = 0 \\ X \mid a_5, & a_5 = 0 \\ X \mid a_6, & a_6 = X^2 \\ X \nmid a_7, & a_7 = 3 \end{cases}$$

Claramente

$$K[X,Y] = K[X][Y] = K[Y][X] = K[Y,X]$$

Del mismo modo se puede definir el anillo de polinomios en 3 variables:

$$K[X,Y,Z] = K[X,Y][Z].$$ $\sum a_{ijk}X^iY^jZ^k$

Y, en general, en n variables:

$$K[X_1, X_2, \dots X_n]$$

que, por la misma razón, es un anillo factorial.

- El grupo (multiplicativo) de las unidades de $K[X,Y]$ coincide con el de las unidades de $K[X]$, luego es K^*.

• El anillo $K[X,Y]$ no es principal.

Por ejemplo, el ideal $I=(X,Y)$ no es principal. En efecto, si existiera un polinomio $f(X,Y)=\sum a_{ij}X^iY^j$ tal que

$$I=(f=f(X,Y))$$

tendríamos:

• $X\in I \Rightarrow X=pf\in K[X,Y]=K[X][Y] \Rightarrow \deg_Y f=0 \Rightarrow f\in K[X] \Rightarrow$

$\Rightarrow Y\notin(f)$. Contradicción.

Pregunta/Respuesta: (X) no es maximal porque

$(X)\subsetneq(X,Y)$

↓

principal

| $(X-1,Y-1)$ tiene (X,Y) es maximal

• En el anillo $K[X,Y]$ seguimos teniendo los morfismos evaluación. Por ejemplo, si $(\alpha,\beta)\in K$ tenemos el homomorfismo:

$$ev_{(\alpha,\beta)} : K[X,Y] \longrightarrow K$$

$$X \longmapsto \alpha$$
$$Y \longmapsto \beta$$
$$a \longmapsto a, \text{ si } a \in K$$

$$\sum a_{ij} X^i Y^j \longmapsto \sum a_{ij} \alpha^i \beta^j$$

Este homomorfismo puede verse como composición de los dos siguientes homomorfismos:

$$K[X][Y] \xrightarrow{ev_\beta} K[X] \xrightarrow{ev_\alpha} K$$

$$Y \longmapsto \beta \qquad X \longmapsto \alpha$$
$$q(X) \longmapsto q(X) \qquad a \longmapsto a$$

de modo que

$$ev_{(\alpha,\beta)} = ev_\alpha \circ ev_\beta$$

(como siempre, la composición de homom. es un homom.)

$$ev_{(\alpha,\beta)}\left(\sum a_{ij} X^i Y^j\right) = \sum a_{ij} \alpha^i \beta^j$$

$$ev_\alpha \circ ev_\beta\left(\sum a_{ij} X^i Y^j\right) = ev_\alpha\left(\sum a_{ij} \beta^j X^i\right) = \sum a_{ij} \beta^j \alpha^i$$

- $ev_{(0,0)} : K[X,Y] \longrightarrow K$

(α β)

$$\sum a_{ij}x^iy^j \longmapsto a_{00}$$

$(\sum a_{ij}x^iy^j = a_{00} + (a_{01}X + a_{10}Y) + \dots)$

- $\underline{\text{Im } ev_{(0,0)} = K}$

- $\text{Ker } ev_{(0,0)} = \left\{ \sum a_{ij}x^iy^j \;/\; a_{00} = 0 \right\}$

Veamos que $\text{Ker } ev_{(0,0)} = (X,Y)$

Claramente $(X,Y) \subset \text{Ker } ev_{(0,0)}$.

Pero por otra parte:

$f = f(X,Y) \in \text{Ker } ev_{(0,0)} \Rightarrow$

$\Rightarrow f = \cancel{a_{00}} + a_{10}X + a_{01}Y + a_{11}XY + a_{20}X^2 + a_{02}Y^2 + \dots$

$= (a_{10}X + a_{11}XY + a_{20}X^2 + \dots) + (a_{01}Y + a_{02}Y^2 + \dots)$

$= \sum_{i\geq 1, j\geq 0} a_{ij}x^iy^j + \left(\sum_{j\geq 1} a_{0j}Y^j\right) =$

$= X\left(\sum_{i\geq 1} a_{ij}x^{i-1}y^j\right) + Y\left(\sum_{j\geq 1} a_{0j}Y^{j-1}\right)$

$\Rightarrow f \in (X,Y) \Rightarrow \text{Ker } ev_{(0,0)} \subseteq (X,Y)$

Luego, finalmente,

$$\boxed{\text{Ker } ev_{(0,0)} = (X,Y)}$$

Por el teorema de isomorfía:

$ev_{(\alpha,\beta)}: \dfrac{K[X,Y]}{(X,Y)} \cong K$

$\bar{X} \mapsto \alpha$, $\bar{Y} \mapsto \beta$

$\bar{f} = \overline{\sum a_{ij} X^i Y^j} \in \dfrac{K[X,Y]}{(X,Y)}$

$= a_{00}$

(K cuerpo) $\Rightarrow$ (X,Y) es un ideal maximal.

(En $\mathbb{Z}[X,Y]$, (X,Y) no será maximal - ¡Pensadlo!.)

- ¿Qué nos dice el teorema de isomorfía para el homomorfismo $ev_0: K[X,Y] \to K[X]$?

$p(X) \mapsto p(X)$

$Y \mapsto 0$

Claramente, $\operatorname{Im} ev_0 = K[X]$

y $(Y) \subseteq \operatorname{Ker} ev_0$.

$ev_0: K[X,Y] \to K[X]$

$a(X) \to a(X)$

$Y \to 0$

Por otra parte, $F(X,Y) = \sum_{i=0}^{n} a_i(X) Y^i \in \operatorname{Ker} ev_0 \Rightarrow \sum_{i=0}^{n} a_i(X) 0^i = 0$

$a_0(X)$

$\Rightarrow a_0(X) = 0 \Rightarrow F(X,Y) = \left(\sum_{i=1}^{n} a_i(X) Y^{i-1}\right) Y \Rightarrow F(X,Y) \in (Y)$.

Luego $\operatorname{Ker} ev_0 = (Y)$ y el teorema de isomorfía nos dice que $\dfrac{K[X,Y]}{(Y)} \cong K[X]$, que es íntegro pero no un cuerpo $\Rightarrow (X)$ es primo pero no maximal.