Álgebra II Práctica (clase 21)

Guido Arnone

Universidad de Buenos Aires

7 de Julio de 2020

Prerrequisitos

Para leer estas diapositivas se recomienda haber leído el apunte teórico hasta el Teorema 4.13.

Elementos primos e irreducibles

Sea A un anillo conmutativo. Decimos que $x \in A$ es:

Elementos primos e irreducibles

Sea A un anillo conmutativo. Decimos que $x \in A$ es:

- primo si (x) es un ideal primo. Es decir, si $x \mid ab$ implica $x \mid a$ ó $x \mid b$, para todo $a, b \in A$.

Elementos primos e irreducibles

Sea A un anillo conmutativo. Decimos que $x \in A$ es:

- primo si (x) es un ideal primo. Es decir, si $x \mid ab$ implica $x \mid a$ ó $x \mid b$, para todo $a, b \in A$.
- irreducible si no es una unidad y $x = ab$ implica $a \in A^\times$ ó $b \in A^\times$. Dicho de otra forma, un elemento es irreducible si sólo es divisible por unidades o asociados.

Elementos primos e irreducibles

Sea A un anillo conmutativo. Decimos que $x \in A$ es:

- primo si (x) es un ideal primo. Es decir, si $x \mid ab$ implica $x \mid a$ ó $x \mid b$, para todo $a, b \in A$.
- irreducible si no es una unidad y $x = ab$ implica $a \in A^\times$ ó $b \in A^\times$. Dicho de otra forma, un elemento es irreducible si sólo es divisible por unidades o asociados.

En un DFU, ambos conceptos coinciden.

Elementos primos e irreducibles

Sea A un anillo conmutativo. Decimos que $x \in A$ es:

- primo si (x) es un ideal primo. Es decir, si $x \mid ab$ implica $x \mid a$ ó $x \mid b$, para todo $a, b \in A$.
- irreducible si no es una unidad y $x = ab$ implica $a \in A^\times$ ó $b \in A^\times$. Dicho de otra forma, un elemento es irreducible si sólo es divisible por unidades o asociados.

En un DFU, ambos conceptos coinciden. Un DIP es un DFU: todo elemento se puede escribir de forma única (salvo unidades y asociados) como producto de irreducibles.

Elementos primos e irreducibles

Sea A un anillo conmutativo. Decimos que $x \in A$ es:

- primo si (x) es un ideal primo. Es decir, si $x \mid ab$ implica $x \mid a$ ó $x \mid b$, para todo $a, b \in A$.
- irreducible si no es una unidad y $x = ab$ implica $a \in A^\times$ ó $b \in A^\times$. Dicho de otra forma, un elemento es irreducible si sólo es divisible por unidades o asociados.

En un DFU, ambos conceptos coinciden. Un DIP es un DFU: todo elemento se puede escribir de forma única (salvo unidades y asociados) como producto de irreducibles.

Recordemos también que si $a, b \in A$, entonces $a \mid b$ si y sólo si $(b) \subset (a)$.

Máximo Común Divisor

Definición

Sea A un anillo y $x, y \in A$. Decimos que $z \in A$ es un máximo común divisor de x e y si divide a ambos y todo divisor común de x e y divide a z.

Máximo Común Divisor

Definición

Sea A un anillo y $x, y \in A$. Decimos que $z \in A$ es un máximo común divisor de x e y si divide a ambos y todo divisor común de x e y divide a z.

Esto coincide con la definición usual para $A = \mathbb{Z}$. Se tiene unicidad salvo asociados: dos máximos comunes divisores se dividen entre sí, así que deben diferir en una unidad.

Máximo Común Divisor

Definición

Sea A un anillo y $x, y \in A$. Decimos que $z \in A$ es un máximo común divisor de x e y si divide a ambos y todo divisor común de x e y divide a z.

Esto coincide con la definición usual para $A = \mathbb{Z}$. Se tiene unicidad salvo asociados: dos máximos comunes divisores se dividen entre sí, así que deben diferir en una unidad.

Proposición

Si A es un DIP y $x, y \in A$, existe un máximo común divisor de x e y.

Máximo Común Divisor

Definición

Sea A un anillo y $x, y \in A$. Decimos que $z \in A$ es un máximo común divisor de x e y si divide a ambos y todo divisor común de x e y divide a z.

Esto coincide con la definición usual para $A = \mathbb{Z}$. Se tiene unicidad salvo asociados: dos máximos comunes divisores se dividen entre sí, así que deben diferir en una unidad.

Proposición

Si A es un DIP y $x, y \in A$, existe un máximo común divisor de x e y.

Demostración.

Consideramos $z \in A$ tal que $(z) = (x) + (y)$. Como contiene a (x) e (y), sabemos que $z \mid x, y$. Además, si $a \in A$ divide a x e y entonces $(a) \supset (x), (y)$ y por lo tanto $(a) \supset (x) + (y) = (z)$, de forma que $a \mid z$. □

Máximo Común Divisor (cont.)

De la demostración anterior se deduce que si A es DIP y z es máximo común divisor de elementos $x, y \in A$, existen $a, b \in A$ tales que $ax + by = z$, y además divide a toda tal combinación A-lineal entre a y b.

También vemos que si A es DIP entonces $x, y \in A$ son coprimos (es decir, solo tienen a las unidades como divisores comunes) si y sólo si existen $a, b \in A$ tales que $ax + by = 1$.

Podemos definir similarmente el máximo común divisor de elementos $x_1, \ldots, x_n \in A$ y probar su existencia en un DIP (más todavía, en un DFU).

Morfismos entre anillos de polinomios

Recordemos que un morfismo de anillos $f\colon R \to S$ induce un morfismo $\overline{f}\colon R[X] \to S[X]$ definido por

$$\overline{f}\left(\sum_{i=0}^{n} r_i X^i\right) := \sum_{i=0}^{n} f(r_i) X^i.$$

Morfismos entre anillos de polinomios

Recordemos que un morfismo de anillos $f\colon R \to S$ induce un morfismo $\overline{f}\colon R[X] \to S[X]$ definido por

$$\overline{f}\left(\sum_{i=0}^{n} r_i X^i\right) := \sum_{i=0}^{n} f(r_i) X^i.$$

Observación

Si un polinomio $p \in R[X]$ tiene por coeficiente principal a una unidad (por ejemplo, si es mónico) entonces $\deg p = \deg \overline{f}(p)$.

Morfismos entre anillos de polinomios (cont.)

La observación anterior nos permite probar lo siguiente:

Proposición

Sea $f : R \to S$ un morfismo de anillos con S un dominio y $p \in R[X]$ un polinomio mónico. Si $\overline{f}(p)$ es irreducible en $S[X]$, entonces p es irreducible en $R[X]$.

Morfismos entre anillos de polinomios (cont.)

La observación anterior nos permite probar lo siguiente:

Proposición

Sea $f : R \to S$ un morfismo de anillos con S un dominio y $p \in R[X]$ un polinomio mónico. Si $\overline{f}(p)$ es irreducible en $S[X]$, entonces p es irreducible en $R[X]$.

Demostración.

Si p fuera reducible, existirían $q, h \in R[X]$ no unidades tales que $p = qh$. En particular los coeficientes principales de q y h son unidades.

Morfismos entre anillos de polinomios (cont.)

La observación anterior nos permite probar lo siguiente:

Proposición

Sea $f : R \to S$ un morfismo de anillos con S un dominio y $p \in R[X]$ un polinomio mónico. Si $\overline{f}(p)$ es irreducible en $S[X]$, entonces p es irreducible en $R[X]$.

Demostración.

Si p fuera reducible, existirían $q, h \in R[X]$ no unidades tales que $p = qh$. En particular los coeficientes principales de q y h son unidades. Aplicando $\overline{f}$ es $\overline{f}(p) = \overline{f}(q)\overline{f}(h)$ y entonces sin pérdida de generalidad $\overline{f}(q)$ debe ser constante.

Morfismos entre anillos de polinomios (cont.)

La observación anterior nos permite probar lo siguiente:

Proposición

Sea $f : R \to S$ un morfismo de anillos con S un dominio y $p \in R[X]$ un polinomio mónico. Si $\overline{f}(p)$ es irreducible en $S[X]$, entonces p es irreducible en $R[X]$.

Demostración.

Si p fuera reducible, existirían $q, h \in R[X]$ no unidades tales que $p = qh$. En particular los coeficientes principales de q y h son unidades. Aplicando $\overline{f}$ es $\overline{f}(p) = \overline{f}(q)\overline{f}(h)$ y entonces sin pérdida de generalidad $\overline{f}(q)$ debe ser constante. Por la observación de antes necesariamente q es de grado cero y por lo tanto una unidad. □

¿Reducible o no?

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible.

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$ es reducible

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$ es reducible , pues $q = \prod_{\alpha \in \mathbb{Z}_7, \alpha \neq 0} X - \alpha$.

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$ es reducible , pues $q = \prod_{\alpha \in \mathbb{Z}_7, \alpha \neq 0} X - \alpha$.
- $r = X^4 + X + 1 \in \mathbb{Z}[X]$

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$ es reducible , pues $q = \prod_{\alpha \in \mathbb{Z}_7, \alpha \neq 0} X - \alpha$.
- $r = X^4 + X + 1 \in \mathbb{Z}[X]$ es irreducible.

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$ es reducible , pues $q = \prod_{\alpha \in \mathbb{Z}_7, \alpha \neq 0} X - \alpha$.
- $r = X^4 + X + 1 \in \mathbb{Z}[X]$ es irreducible. Basta ver que lo es en $\mathbb{Z}_2[X]$, aplicando el resultado anterior a la proyección $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$ es reducible , pues $q = \prod_{\alpha \in \mathbb{Z}_7, \alpha \neq 0} X - \alpha$.
- $r = X^4 + X + 1 \in \mathbb{Z}[X]$ es irreducible. Basta ver que lo es en $\mathbb{Z}_2[X]$, aplicando el resultado anterior a la proyección $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

  Como no tiene raíces en $\mathbb{Z}_2$, de ser reducible es producto de dos poliomios de grado dos, y ambos irreducibles.

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$ es reducible , pues $q = \prod_{\alpha \in \mathbb{Z}_7, \alpha \neq 0} X - \alpha$.
- $r = X^4 + X + 1 \in \mathbb{Z}[X]$ es irreducible. Basta ver que lo es en $\mathbb{Z}_2[X]$, aplicando el resultado anterior a la proyección $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

  Como no tiene raíces en $\mathbb{Z}_2$, de ser reducible es producto de dos poliomios de grado dos, y ambos irreducibles. Hay un único tal en $\mathbb{Z}_2$ y es $X^2 + X + 1$.

¿Reducible o no?

- $p = X^2 + Y^2 - 3 \in \mathbb{R}[X, Y]$ es irreducible. Podemos aplicar el resultado anterior al morfismo $\mathrm{ev}_2 : \mathbb{R}[X] \to \mathbb{R}$. Como $Y^2 + 1$ es irreducible en $\mathbb{R}[Y]$, así lo es p en $\mathbb{R}[X, Y] \simeq \mathbb{R}[X][Y]$.
- $q = X^6 - 1 \in \mathbb{Z}_7[X]$ es reducible , pues $q = \prod_{\alpha \in \mathbb{Z}_7, \alpha \neq 0} X - \alpha$.
- $r = X^4 + X + 1 \in \mathbb{Z}[X]$ es irreducible. Basta ver que lo es en $\mathbb{Z}_2[X]$, aplicando el resultado anterior a la proyección $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

  Como no tiene raíces en $\mathbb{Z}_2$, de ser reducible es producto de dos poliomios de grado dos, y ambos irreducibles. Hay un único tal en $\mathbb{Z}_2$ y es $X^2 + X + 1$. Sin embargo,

$$(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq X^4 + X + 1$$

  así que r es irreducible.

Polinomios y Contenido

Proposición

Sea A un DFU. Un polinomio $p = aX - b \in A[X]$ de grado 1 es irreducible si y sólo si a y b son coprimos.

Polinomios y Contenido

Proposición

Sea A un DFU. Un polinomio $p = aX - b \in A[X]$ de grado 1 es irreducible si y sólo si a y b son coprimos.

Demostración.

Si a y b tienen un divisor común $c \in A \setminus A^\times$, entonces existen $a', b' \in A$ tales que $a = a'c, b = b'c$. Por lo tanto $p = aX + b = c(a'X + b')$ es reducible.

Polinomios y Contenido

Proposición

Sea A un DFU. Un polinomio $p = aX - b \in A[X]$ de grado 1 es irreducible si y sólo si a y b son coprimos.

Demostración.

Si a y b tienen un divisor común $c \in A \setminus A^\times$, entonces existen $a', b' \in A$ tales que $a = a'c, b = b'c$. Por lo tanto $p = aX + b = c(a'X + b')$ es reducible. Recíprocamente, si p es reducible debe escribise como $p = c(a'X + b')$ para ciertos $a', b' \in A$ y $c \in A \setminus A^\times$. En particular $c \mid a, b$ es un divisor común de a y b. □

Polinomios y Contenido (cont.)

Esto nos dice por ejemplo que $p = 3X - 2 \in \mathbb{Z}[X]$ es irreducible pero $4X + 2 = 2(2X + 1) \in \mathbb{Z}[X]$ no.

Polinomios y Contenido (cont.)

Esto nos dice por ejemplo que $p = 3X - 2 \in \mathbb{Z}[X]$ es irreducible pero $4X + 2 = 2(2X + 1) \in \mathbb{Z}[X]$ no.

Un ejemplo más interesante es

$$q = XZ + XY + 1 \in \mathbb{Q}[X, Y, Z].$$

Polinomios y Contenido (cont.)

Esto nos dice por ejemplo que $p = 3X - 2 \in \mathbb{Z}[X]$ es irreducible pero $4X + 2 = 2(2X + 1) \in \mathbb{Z}[X]$ no.

Un ejemplo más interesante es

$$q = XZ + XY + 1 \in \mathbb{Q}[X, Y, Z].$$

Como $q = XZ + (XY + 1) \in (\mathbb{Q}[X, Y])[Z]$ y $X, XY + 1 \in \mathbb{Q}[X, Y]$ son coprimos ya que

$$1 = (-Y) \cdot X + 1 \cdot (XY + 1),$$

tenemos que q es irreducible en $\mathbb{Q}[X, Y, Z]$.

Polinomios y Contenido (cont.)

Si A es un DFU y $p = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, definimos el contenido de p como el máximo común divisor de $a_0, \ldots, a_n$.

Polinomios y Contenido (cont.)

Si A es un DFU y $p = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, definimos el contenido de p como el máximo común divisor de $a_0, \ldots, a_n$. Como antes, la unicidad es salvo unidades.

Polinomios y Contenido (cont.)

Si A es un DFU y $p = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, definimos el contenido de p como el máximo común divisor de $a_0, \ldots, a_n$. Como antes, la unicidad es salvo unidades. Decimos que un polinomio es primitivo si su contenido es una unidad.

Polinomios y Contenido (cont.)

Si A es un DFU y $p = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, definimos el contenido de p como el máximo común divisor de $a_0, \ldots, a_n$. Como antes, la unicidad es salvo unidades. Decimos que un polinomio es primitivo si su contenido es una unidad.

Objetivo: probar que si A es DFU, entonces $A[X]$ es DFU. Para esto, primero:

Polinomios y Contenido (cont.)

Si A es un DFU y $p = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, definimos el contenido de p como el máximo común divisor de $a_0, \ldots, a_n$. Como antes, la unicidad es salvo unidades. Decimos que un polinomio es primitivo si su contenido es una unidad.

Objetivo: probar que si A es DFU, entonces $A[X]$ es DFU. Para esto, primero:

- Probaremos un lema de Gauß sobre polinomios primitivos.

Polinomios y Contenido (cont.)

Si A es un DFU y $p = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, definimos el contenido de p como el máximo común divisor de $a_0, \ldots, a_n$. Como antes, la unicidad es salvo unidades. Decimos que un polinomio es primitivo si su contenido es una unidad.

Objetivo: probar que si A es DFU, entonces $A[X]$ es DFU. Para esto, primero:

- Probaremos un lema de Gauß sobre polinomios primitivos.
- Definiremos el cuerpo de fracciones de un dominio íntegro para hacer uso de que $k[X]$ es un dominio euclídeo (en particular, DIP y por lo tanto DFU) cuando k es un cuerpo.

Un lema de Gauß

Lema (Gauß)

Sea A un DFU. Si $f, g \in A[X]$ son dos polinomios primitivos, entonces $fg \in A[X]$ es primitivo.

Un lema de Gauß

Lema (Gauß)

Sea A un DFU. Si $f, g \in A[X]$ son dos polinomios primitivos, entonces $fg \in A[X]$ es primitivo.

Demostración.

Supongamos que fg no es primitivo y sea $p \in A$ un primo que divide a todos los coeficientes de fg.

Un lema de Gauß

Lema (Gauß)

Sea A un DFU. Si $f, g \in A[X]$ son dos polinomios primitivos, entonces $fg \in A[X]$ es primitivo.

Demostración.

Supongamos que fg no es primitivo y sea $p \in A$ un primo que divide a todos los coeficientes de fg. En particular, al considerar el morfismo $\pi : A[X] \to A/(p)[X]$ inducido por la proyección $A \to A/(p)$ debe ser

$$0 = \pi(fg) = \pi(f)\pi(g).$$

Un lema de Gauß

Lema (Gauß)

Sea A un DFU. Si $f, g \in A[X]$ son dos polinomios primitivos, entonces $fg \in A[X]$ es primitivo.

Demostración.

Supongamos que fg no es primitivo y sea $p \in A$ un primo que divide a todos los coeficientes de fg. En particular, al considerar el morfismo $\pi : A[X] \to A/(p)[X]$ inducido por la proyección $A \to A/(p)$ debe ser

$$0 = \pi(fg) = \pi(f)\pi(g).$$

Como $A/(p)$ es un dominio, así lo es $A/(p)[X]$, y por lo tanto o bien $\pi(f) = 0$ o bien $\pi(g) = 0$. Esto es absurdo, pues tanto f como g son primitivos así que p no puede dividir a todos sus coeficientes. □

Un lema de Gauß

Corolario

Sea A un DFU. Si $f, g \in A[X]$ entonces a menos de unidades, el contenido de fg es el producto de los contenidos de f y g.

La demostración queda de ejercicio. Las siguientes observaciones pueden ser de ayuda:

Un lema de Gauß

Corolario

Sea A un DFU. Si $f, g \in A[X]$ entonces a menos de unidades, el contenido de fg es el producto de los contenidos de f y g.

La demostración queda de ejercicio. Las siguientes observaciones pueden ser de ayuda:

- Si $d \in A$ es m.c.d. de $x_1, \cdots, x_n \in A$, entonces $ad \in A$ es m.c.d. de $ax_1, \cdots, ax_n \in A$ para cada $a \in A \setminus \{0\}$.

Un lema de Gauß

Corolario

Sea A un DFU. Si $f, g \in A[X]$ entonces a menos de unidades, el contenido de fg es el producto de los contenidos de f y g.

La demostración queda de ejercicio. Las siguientes observaciones pueden ser de ayuda:

- Si $d \in A$ es m.c.d. de $x_1, \cdots, x_n \in A$, entonces $ad \in A$ es m.c.d. de $ax_1, \cdots, ax_n \in A$ para cada $a \in A \setminus \{0\}$.
- Si $p \in A[X]$ y $c \in A$ es su contenido, entonces existe $q \in A[X]$ primitivo tal que $p = c \cdot q$.

Un lema de Gauß

Corolario

Sea A un DFU. Si $f, g \in A[X]$ entonces a menos de unidades, el contenido de fg es el producto de los contenidos de f y g.

La demostración queda de ejercicio. Las siguientes observaciones pueden ser de ayuda:

- Si $d \in A$ es m.c.d. de $x_1, \cdots, x_n \in A$, entonces $ad \in A$ es m.c.d. de $ax_1, \cdots, ax_n \in A$ para cada $a \in A \setminus \{0\}$.
- Si $p \in A[X]$ y $c \in A$ es su contenido, entonces existe $q \in A[X]$ primitivo tal que $p = c \cdot q$.
- Recíprocamente, si $p = c \cdot q$ y q es primitivo, entonces el contenido de p es c.

Cuerpo de Fracciones

Ejercicio (práctica 7, ej. 10)

Sea A un dominio íntegro. En $A \times (A \setminus \{0\})$ consideramos la relación $(a, b) \sim (c, d) \iff ad = bc$.

a) *Probar que $\sim$ es de equivalencia.*

b) *Sea $K := A \times (A \setminus \{0\}) / \sim$ el conjunto de clases de equivalencia. Notamos $\frac{a}{b}$ a la clase de un elemento (a, b). Probar que las operaciones*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

están bien definidas.

c) *Probar que K es un cuerpo y que $i : a \in A \to \frac{a}{1} \in K$ es un monomorfismo de anillos.*

d) *Probar que dado un cuerpo K' y un monomorfismo de anillos $j : A \to K'$, existe un único morfismo de anillos $\bar{j} : K \to K'$ tal que $\bar{j} \circ i = j$.*

Cuerpo de Fracciones (cont.)

El cuerpo de fracciones de un dominio A es el cuerpo "más pequeño" que contiene a A. Lo solemos notar $\mathrm{Frac}(A)$ o $K(A)$.

A través del morfismo i pensamos que $A \subset \mathrm{Frac}(A)$ identificando $a \in A$ con $\frac{a}{1}$.

Cuerpo de Fracciones (cont.)

El cuerpo de fracciones de un dominio A es el cuerpo "más pequeño" que contiene a A. Lo solemos notar $\mathrm{Frac}(A)$ o $K(A)$.

A través del morfismo i pensamos que $A \subset \mathrm{Frac}(A)$ identificando $a \in A$ con $\frac{a}{1}$. Esto induce a su vez un monomorfismo $A[X] \to \mathrm{Frac}(A)[X]$ que también pensamos como una inclusión.

Cuerpo de Fracciones (cont.)

El cuerpo de fracciones de un dominio A es el cuerpo "más pequeño" que contiene a A. Lo solemos notar $\mathrm{Frac}(A)$ o $K(A)$.

A través del morfismo i pensamos que $A \subset \mathrm{Frac}(A)$ identificando $a \in A$ con $\frac{a}{1}$. Esto induce a su vez un monomorfismo $A[X] \to \mathrm{Frac}(A)[X]$ que también pensamos como una inclusión.

Algunos ejemplos:

Cuerpo de Fracciones (cont.)

El cuerpo de fracciones de un dominio A es el cuerpo "más pequeño" que contiene a A. Lo solemos notar $\mathrm{Frac}(A)$ o $K(A)$.

A través del morfismo i pensamos que $A \subset \mathrm{Frac}(A)$ identificando $a \in A$ con $\frac{a}{1}$. Esto induce a su vez un monomorfismo $A[X] \to \mathrm{Frac}(A)[X]$ que también pensamos como una inclusión.

Algunos ejemplos:

- El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.

Cuerpo de Fracciones (cont.)

El cuerpo de fracciones de un dominio A es el cuerpo "más pequeño" que contiene a A. Lo solemos notar $\mathrm{Frac}(A)$ o $K(A)$.

A través del morfismo i pensamos que $A \subset \mathrm{Frac}(A)$ identificando $a \in A$ con $\frac{a}{1}$. Esto induce a su vez un monomorfismo $A[X] \to \mathrm{Frac}(A)[X]$ que también pensamos como una inclusión.

Algunos ejemplos:

- El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.
- El cuerpo de fracciones de $k[X]$ son las funciones racionales $k(X) = \{\frac{f}{g} : f, g \in k[X], g \neq 0\}$

Cuerpo de Fracciones (cont.)

El cuerpo de fracciones de un dominio A es el cuerpo "más pequeño" que contiene a A. Lo solemos notar $\mathrm{Frac}(A)$ o $K(A)$.

A través del morfismo i pensamos que $A \subset \mathrm{Frac}(A)$ identificando $a \in A$ con $\frac{a}{1}$. Esto induce a su vez un monomorfismo $A[X] \to \mathrm{Frac}(A)[X]$ que también pensamos como una inclusión.

Algunos ejemplos:

- El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.
- El cuerpo de fracciones de $k[X]$ son las funciones racionales $k(X) = \{\frac{f}{g} : f, g \in k[X], g \neq 0\}$
- Si $U \subset \mathbb{C}$ es un abierto conexo, entonces las funciones holomorfas $\mathcal{H}(U)$ en U son un dominio y las meromorfas $\mathcal{M}(U)$ su cuerpo de fracciones.

Polinomios en el cuerpo de fracciones

Fijemos A un DFU y $k = \text{Frac}(A)$. Algunas observaciones sobre la relación entre un polinomio p visto en $A[X]$ y en $k[X]$.

Polinomios en el cuerpo de fracciones

Fijemos A un DFU y $k = \text{Frac}(A)$. Algunas observaciones sobre la relación entre un polinomio p visto en $A[X]$ y en $k[X]$.

- Si $p \in A[X]$ es irreducible en $k[X]$, puede no serlo en $A[X]$. Por ejemplo $2X^2 + 2$ es irreducible en $\mathbb{Q}[X]$ pero no en $\mathbb{Z}[X]$.

Polinomios en el cuerpo de fracciones

Fijemos A un DFU y $k = \mathrm{Frac}(A)$. Algunas observaciones sobre la relación entre un polinomio p visto en $A[X]$ y en $k[X]$.

- Si $p \in A[X]$ es irreducible en $k[X]$, puede no serlo en $A[X]$. Por ejemplo $2X^2 + 2$ es irreducible en $\mathbb{Q}[X]$ pero no en $\mathbb{Z}[X]$. De ser reducible en $A[X]$, tiene que ser $p = a \cdot g$ con $a \in A \setminus A^\times$ y $g \in A[X]$.

Polinomios en el cuerpo de fracciones

Fijemos A un DFU y $k = \mathrm{Frac}(A)$. Algunas observaciones sobre la relación entre un polinomio p visto en $A[X]$ y en $k[X]$.

- Si $p \in A[X]$ es irreducible en $k[X]$, puede no serlo en $A[X]$. Por ejemplo $2X^2 + 2$ es irreducible en $\mathbb{Q}[X]$ pero no en $\mathbb{Z}[X]$. De ser reducible en $A[X]$, tiene que ser $p = a \cdot g$ con $a \in A \setminus A^\times$ y $g \in A[X]$.
- Si $p = \frac{a_n}{b_n} X^n + \cdots + \frac{a_1}{b_1} X + \frac{a_0}{b_0} \in K[X]$, existe $b \in A$ tal que $b \cdot p \in A[X]$.

Polinomios en el cuerpo de fracciones

Fijemos A un DFU y $k = \text{Frac}(A)$. Algunas observaciones sobre la relación entre un polinomio p visto en $A[X]$ y en $k[X]$.

- Si $p \in A[X]$ es irreducible en $k[X]$, puede no serlo en $A[X]$. Por ejemplo $2X^2 + 2$ es irreducible en $\mathbb{Q}[X]$ pero no en $\mathbb{Z}[X]$. De ser reducible en $A[X]$, tiene que ser $p = a \cdot g$ con $a \in A \setminus A^\times$ y $g \in A[X]$.
- Si $p = \frac{a_n}{b_n} X^n + \cdots + \frac{a_1}{b_1} X + \frac{a_0}{b_0} \in K[X]$, existe $b \in A$ tal que $b \cdot p \in A[X]$. Más todavía, existe $a \in A$ tal que $bp = aq$ con q primitivo. Por lo tanto, todo polinomio en $k[X]$ se puede escribir como $\frac{a}{b} q$ con $q \in A[X]$ primitivo.

Polinomios en el cuerpo de fracciones

Fijemos A un DFU y $k = \text{Frac}(A)$. Algunas observaciones sobre la relación entre un polinomio p visto en $A[X]$ y en $k[X]$.

- Si $p \in A[X]$ es irreducible en $k[X]$, puede no serlo en $A[X]$. Por ejemplo $2X^2 + 2$ es irreducible en $\mathbb{Q}[X]$ pero no en $\mathbb{Z}[X]$. De ser reducible en $A[X]$, tiene que ser $p = a \cdot g$ con $a \in A \setminus A^\times$ y $g \in A[X]$.
- Si $p = \frac{a_n}{b_n}X^n + \cdots + \frac{a_1}{b_1}X + \frac{a_0}{b_0} \in K[X]$, existe $b \in A$ tal que $b \cdot p \in A[X]$. Más todavía, existe $a \in A$ tal que $bp = aq$ con q primitivo. Por lo tanto, todo polinomio en $k[X]$ se puede escribir como $\frac{a}{b}q$ con $q \in A[X]$ primitivo. Por ejemplo,

$$\frac{2}{3}X^2 + \frac{4}{5}X = \frac{1}{15}(10X^2 + 12X) = \frac{2}{15}(5X^2 + 6X) \in \mathbb{Q}[X].$$

Polinomios en el cuerpo de fracciones (cont.)

Proposición

Sea A un DFU y K su cuerpo de fracciones. Un polinomio $p \in A[X]$ es irreducible si y sólo si es primitivo e irreducible en $K[X]$.

Polinomios en el cuerpo de fracciones (cont.)

Proposición

Sea A un DFU y K su cuerpo de fracciones. Un polinomio $p \in A[X]$ es irreducible si y sólo si es primitivo e irreducible en $K[X]$.

Demostración.

Supongamos que p es primitivo e irreducible en $K[X]$. De ser reducible en $A[X]$ tendría que ser de la forma $p = ag$ con $a \in A \setminus A^{\times}$, pero no sería entonces primitivo.

Polinomios en el cuerpo de fracciones (cont.)

Proposición

Sea A un DFU y K su cuerpo de fracciones. Un polinomio $p \in A[X]$ es irreducible si y sólo si es primitivo e irreducible en $K[X]$.

Demostración.

Supongamos que p es primitivo e irreducible en $K[X]$. De ser reducible en $A[X]$ tendría que ser de la forma $p = ag$ con $a \in A \setminus A^\times$, pero no sería entonces primitivo.

Supongamos ahora que $p \in A[X]$ es irreducible. Como es divisible por su contenido, es primitivo. Tomemos $a, b, c, d \in A$ y $q, r \in A[X]$ primitivos tales que $p = \frac{a}{b}\frac{c}{d}qr$ y entonces $bd \cdot p = ac \cdot qr$.

Polinomios en el cuerpo de fracciones (cont.)

Proposición

Sea A un DFU y K su cuerpo de fracciones. Un polinomio $p \in A[X]$ es irreducible si y sólo si es primitivo e irreducible en $K[X]$.

Demostración.

Supongamos que p es primitivo e irreducible en $K[X]$. De ser reducible en $A[X]$ tendría que ser de la forma $p = ag$ con $a \in A \setminus A^\times$, pero no sería entonces primitivo.

Supongamos ahora que $p \in A[X]$ es irreducible. Como es divisible por su contenido, es primitivo. Tomemos $a, b, c, d \in A$ y $q, r \in A[X]$ primitivos tales que $p = \frac{a}{b}\frac{c}{d}qr$ y entonces $bd \cdot p = ac \cdot qr$. Por el lema de Gauß qr es primitivo, así que tomando contenidos es $ac = u \cdot bd$ con $u \in A^\times$. Por lo tanto $p = uqr$ y o bien q o bien r debe ser una unidad en $A[X]$, en particular en $K[X]$. □

Polinomios en el cuerpo de fracciones (cont.)

Corolario

Sea A un DFU y K su cuerpo de fracciones. Si $h \in K[X]$ es irreducible, es asociado en $K[X]$ a $\widetilde{h} \in A[X]$ irreducible.

Polinomios en el cuerpo de fracciones (cont.)

Corolario

Sea A un DFU y K su cuerpo de fracciones. Si $h \in K[X]$ es irreducible, es asociado en $K[X]$ a $\widetilde{h} \in A[X]$ irreducible.

Demostración.

Escribimos $h = \frac{a}{b} \cdot \widetilde{h}$ con $\widetilde{h} \in A[X]$ primitivo. Como en $K[X]$ es asociado a h, es irreducible allí, así que es irreducible en $A[X]$. □

Polinomios en el cuerpo de fracciones (cont.)

Corolario

Sea A un DFU y K su cuerpo de fracciones. Si $h \in K[X]$ es irreducible, es asociado en $K[X]$ a $\widetilde{h} \in A[X]$ irreducible.

Demostración.

Escribimos $h = \frac{a}{b} \cdot \widetilde{h}$ con $\widetilde{h} \in A[X]$ primitivo. Como en $K[X]$ es asociado a h, es irreducible allí, así que es irreducible en $A[X]$. □

Ahora sí, tenemos todas las herramientas para probar el teorema.

Polinomios sobre un DFU

Teorema

Si A es un DFU, entonces $A[X]$ es un DFU.

Polinomios sobre un DFU

Teorema

Si A es un DFU, entonces $A[X]$ es un DFU.

Demostración.

Sea K el cuerpo de fracciones de A y $p \in A[X]$ y consideremos $p = c \cdot q$ con $q \in A[X]$ primitivo.

Polinomios sobre un DFU

Teorema

Si A es un DFU, entonces $A[X]$ es un DFU.

Demostración.

Sea K el cuerpo de fracciones de A y $p \in A[X]$ y consideremos $p = c \cdot q$ con $q \in A[X]$ primitivo. Como $K[X]$ es DFU, tenemos una descomposición $q = u \cdot h_1 \cdots h_r$ con $u = \frac{a}{b} \in K$ y cada h_i irreducible. Por los resultados anteriores podemos suponer además $h_i \in A[X]$ irreducibles en $A[X]$.

Polinomios sobre un DFU

Teorema

Si A es un DFU, entonces $A[X]$ es un DFU.

Demostración.

Sea K el cuerpo de fracciones de A y $p \in A[X]$ y consideremos $p = c \cdot q$ con $q \in A[X]$ primitivo. Como $K[X]$ es DFU, tenemos una descomposición $q = u \cdot h_1 \cdots h_r$ con $u = \frac{a}{b} \in K$ y cada h_i irreducible. Por los resultados anteriores podemos suponer además $h_i \in A[X]$ irreducibles en $A[X]$.

Por el lema de Gauß, sabemos que $h_1 \cdots h_r$ es primitivo, así que tomando contenido en la ecuación $bq = ah_1 \cdots h_r$ debe existir $\nu \in A^\times$ tal que $a = b\nu$. En consecuencia $q = \nu h_1 \cdots h_r$ se escribe como producto de irreducibles en $A[X]$.

Polinomios sobre un DFU

Teorema

Si A es un DFU, entonces $A[X]$ es un DFU.

Demostración.

Sea K el cuerpo de fracciones de A y $p \in A[X]$ y consideremos $p = c \cdot q$ con $q \in A[X]$ primitivo. Como $K[X]$ es DFU, tenemos una descomposición $q = u \cdot h_1 \cdots h_r$ con $u = \frac{a}{b} \in K$ y cada h_i irreducible. Por los resultados anteriores podemos suponer además $h_i \in A[X]$ irreducibles en $A[X]$.

Por el lema de Gauß, sabemos que $h_1 \cdots h_r$ es primitivo, así que tomando contenido en la ecuación $bq = ah_1 \cdots h_r$ debe existir $\nu \in A^\times$ tal que $a = b\nu$. En consecuencia $q = \nu h_1 \cdots h_r$ se escribe como producto de irreducibles en $A[X]$.

Si ahora descomponemos a c en irreducibles en A, tenemos una descomposición de $p = cq$ como producto de irreducibles. La unicidad se desprende de la unicidad en de la factorización en A y $K[X]$. □

Polinomios sobre un DFU (cont.)

Corolario

Si A es un DFU, entonces $A[X_1, \cdots, X_n]$ es un DFU.

En particular $\mathbb{Z}[X_1, \cdots, X_n]$ y $k[X_1, \cdots, X_n]$ para k un cuerpo son DFU.

Vemos así que en estos anillos siempre existe un máximo común divisor de finitos elementos, y que un elemento es primo si y sólo si es irreducible, entre otras consecuencias.