Anexo

En este anexo se pueden encontrar diversos resultados enunciados en la sección 1.2., desarrollados con mayor profundidad.

Teorema 1. ***(Algoritmo de la división en*** $K[x]$***)***
Sean K un cuerpo y $0 \neq g \in K[x]$*, entonces, todo polinomio* $f \in K[x]$ *puede escribirse como*

$$f = qg + r,$$

donde $q, r \in K[x]$*, y o bien* $r = 0$*, o* $gr(r) < gr(g)$*. Además, dichos q y r son* ***únicos****, y existe un algoritmo para calcularlos.*

Demostración. El pseudocódigo del algoritmo para dicho cálculo es el siguiente:

Datos: g, f
Resultado: q, r
Inicialización: $q := 0, r := f$
mientras $r \neq 0$ ***y*** $in(g)$ *divida a* $in(r)$ **hacer**
  $q := q + in(r)/in(g)$
  $r := r - (in(r)/in(g))g$
fin

Algoritmo 4: Algoritmo de la división en $K[x]$

Apoyémonos en dicho algoritmo para demostrar el teorema anterior. Para empezar, notemos que $f = qg + r$ es cierto para los valores iniciales del algoritmo. Es más, en todo momento dicha igualdad se mantiene, puesto que

$$f = qg + r = (q + in(r)/in(g))g + (r - (in(r)/in(g))g).$$

Por otro lado, la condición **mientras** ... **hacer** finaliza cuando la condición "$r \neq 0$ y $in(g)$ divida a $in(r)$" es falsa. Esto equivale a decir que el algoritmo acaba cuando $r = 0$ o $gr(r) < gr(g)$, dado que $gr(r) \leq gr(g) \iff in(r)$ divide a $in(g)$.

Debemos demostrar que llega un momento en el que la condición dentro del **mientras** ... **hacer** se convierte en falsa, dado que si no daría lugar a un bucle sin fin. Supongamos que

$$r = a_0x^m + ... + a_m, \text{ con } in(r) = a_0x^m,$$
$$g = b_0x^k + ... + b_k, \text{ con } in(g) = b_0x^k,$$

y supongamos que $m \geq k$. Entonces se tiene que

$$r - (in(r)/in(g))g = (a_0x^m + ... + a_m) - (a_0/b_0)x^{m-k}(b_0x^k + ... + b_k),$$

de modo que el grado de r va decreciendo cada iteración. Como el grado de los polinomios involucrados es finito, se concluye que el algoritmo finaliza en un número finito de pasos.

Por último, falta demostrar la unicidad de q y r. Supongamos que $f = qg + r = q'g + r'$, donde el grado de r y r' es inferior al de g. Si tenemos que $r \neq r'$, entonces, $gr(r - r') < gr(g)$. Por otro lado, se tiene que $(q - q')g = r' - r$, de modo que $q \neq q'$. Entonces

$$gr(r' - r) = gr((q - q')g) = gr(q - q') + gr(g) \geq gr(g).$$

Por consecuente, $r = r'$, y mediante $(q - q')g = r' - r$, concluimos que $q = q'$. □

Durante el primer capítulo se menciona que $K[X]$ es un DIP, resultado que resulta crucial para solventar los problemas de descripción y pertenencia al ideal. A continuación, la demostración de dicho resultado.

Corolario. *Sea K un cuerpo, entonces, $K[x]$ es un dominio de ideales principales (DIP), es decir, todo ideal $I \subset K[x]$ se puede escribir como $I = \langle f \rangle$, para algún $f \in K[x]$. Además, dicho f es único salvo múltiplos constantes no nulos.*

Demostración. Sea $I \subset K[x]$. Si $I = \{0\}$, trivialmente, $I = \langle 0 \rangle$. Supongamos que $I \neq \{0\}$, y sea $g \in I$ un polinomio de grado mínimo en I. Entonces, empleando el algoritmo de la división, es claro que para todo $f \in g$, existen $q, r \in K[x]$ con $r = 0$, o bien $gr(r) < gr(g)$. De este modo, $r = f - qg \in I$, luego forzosamente $r = 0$, ya que el grado de g lo habíamos supuesto mínimo. Por tanto, $\langle g \rangle \subset I$. Trivialmente, $\langle g \rangle = I$, dado que cualquier múltiplo polinómico de g pertenece a I. □

Asimismo, en el primer capítulo se utiliza otro ingrediente algebraico: el máximo común divisor de polinomios en $K[x]$.

Definición. *Denominamos **máximo común divisor** de $f_1, ..., f_s \in K[x]$ a un polinomio h tal que:*
(i) h divide a $f_1, ..., f_s$.
(ii) si p es otro polinomio que divide a $f_1, ..., f_s$, entonces p divide a h.
En tal caso, escribimos que $h = MCD(f_1, ..., f_s)$.

La siguiente proposición se apoya en el uso del máximo común divisor de polinomios para solucionar el primer problema (I), el problema de descripción de un ideal en $K[x]$.

Proposición. *Sean $f_1, ..., f_s \in K[x]$, con $s \geq 2$, entonces:*
(i) $MCD(f_1, ..., f_s)$ es un generador del ideal $\langle f_1, ..., f_s \rangle$.
(ii) Si $s \geq 3$, $MCD(f_1, ..., f_s) = MCD(f_1, MCD(f_2, ..., f_s))$.
(iii) Existe un algoritmo para calcular $MCD(f_1, ..., f_s)$.

Demostración. (i) Sea $h = MCD(f_1, ..., f_s)$. Procedamos por doble contenido. Si $p \in \langle f_1, ..., f_s \rangle$, entonces $p = \sum_{i=1}^{t} p_i f_i$ para ciertos $p_i \in K[x]$. Se tiene que h divide a todo f_i, luego podemos escribir $f_i = g_i h \ \forall f_i$, para ciertos g_i. De este modo, $p = \sum_{i=1}^{t} p_i g_i d$, luego h divide a p, ergo $p \in \langle h \rangle$. Falta ver el otro contenido: sea $p \in \langle h \rangle$. Como h es el máximo común divisor de $f_1, ..., f_s$, se tiene que $h = \sum_{i=1}^{t} q_i f_i$ para ciertos q_i. Además, $p = hq$ para cierto q, por lo tanto, $hq = p = \sum_{i=1}^{t} q q_i f_i$, luego $p \in \langle f_1, ..., f_s \rangle$.

(ii) Sea $h = MCD(f_2, ..., f_s)$, queremos demostrar primero que $\langle f_1, h \rangle = \langle f_1, ..., f_s \rangle$. Por doble contenido: sea $p \in \langle f_1, ..., f_s \rangle$. Entonces, $p = \sum_{i=1}^{t} q_i f_i$ para ciertos q_i. Como h divide

a f_i $\forall i \neq 1$, se tiene que $p = q_1 f_1 + \sum_{i=2}^{t} q_i q_i' h$ para ciertos q_i', luego $p \in \langle f_1, h \rangle$. Para demostrar el otro contenido, notar que como h es el máximo común divisor, existen $q_2, ..., q_s$ tales que $h = \sum_{i=2}^{t} q_i f_i$, luego $p = q_1 f_1 + \sum_{i=2}^{t} q_i f_i = \sum_{i=1}^{t} q_i f_i$. Por último, mediante (i) se tiene que $\langle GCD(f_1, h) \rangle = \langle MCD(f_1, ..., f_s) \rangle$ y, como el máximo común divisor es único salvo multiplicación por constante por ser un generador principal del ideal, concluimos que $MCD(f_1, ..., f_s) = MCD(f_1, MCD(f_2, ..., f_s))$. □

La tercera parte de la proposición anterior quedará demostrada tras el siguiente resultado.

Proposición. ***(Algoritmo de Euclides)***
Sean $f, g \in K[x]$, para calcular el $MCD(f, g)$ basta aplicar el siguiente algoritmo, presentado como pseoudocódigo, donde $resto(h, s)$ representa el resto de efectuar la división de h entre s:

Datos: f, g
Resultado: h
Inicialización: $h := f, s := g$
mientras $s \neq 0$ **hacer**
  $res := resto(h, s)$
  $h := s$
  $s := res$
fin

Demostración. Si efectuamos la división de f entre g, obtendremos que $f = gq + r$ para ciertos q y r satisfaciendo las propiedades del Teorema 1. Necesitamos demostrar que

$$MCD(f, g) = MCD(f - qg, g) = MCD(f)$$

Empleando el apartado (i) de la proposición anterior, basta demostrar que $\langle f, g \rangle$ y $\langle f - gq, g \rangle$ son iguales. Demostrémoslo por doble contenido: sea $p \in \langle f, g \rangle$, entonces $p = q_1 f + q_2 g$ para ciertos q_1 y q_2. Pero $f = gq + r$, ergo $p = q_1(gq + r) + q_2 g = q_1 r + (q_1 q + q_2) g = q_1(f - gq) + (q_1 q + q_2) g \in \langle f - gq, g \rangle$. Análogamente, sea $p \in \langle f - gq, g \rangle$. Entonces, $p = q_1(f - gq) + q_2 g$ para ciertos q_1 y q_2. De modo que $p = q_1(f - gq) + q_2 g = q_1 f + (q_2 - q_1 q) g \in \langle f, g \rangle$.

Una vez demostrado esto, notemos que entonces $MCD(f, g) = MCD(g, r)$. Además, $gr(g) > gr(r)$ o $r = 0$. Si $r = 0$, hemos terminado el proceso de cálculo. Si no, podemos continuar con el proceso dividiendo g entre r. Si $g = q' r + r'$, y así, $MCD(g, r) = MCD(r, r')$. De nuevo, $gr(r) > gr(r')$ o $r' = 0$. Si $r' \neq 0$, proseguimos sucesivamente. Dado que el grado de los polinomios iniciales es finito y que el grado del resto va disminuyendo conforme transcurre el algoritmo, concluimos que el último resto no nulo es nuestro máximo común divisor. □

De este modo, el apartado (iii) de la penúltima proposición queda demostrado: para calcular $MCD(f_1, ..., f_s)$ basta emplear conjuntamente el algoritmo de Euclides y el apartado (ii) de dicha proposición.