Álgebra computacional. Examen parcial 1. Soluciones
Universidad de El Salvador, 12/04/2019

Ejercicio 1. Consideremos el ideal

$$I = (xy,\, x^3 - y^2 + x) \subset k[x, y].$$

a) Encuentre la base de Gröbner reducida de I respecto al orden graduado lexicográfico.

b) Encuentre una base monomial de $k[x, y]/I$ como un espacio vectorial sobre k.

Este ejercicio nada más pone a prueba el manejo de los algoritmos básicos, y escogí a propósito polinomios que no requieren muchos cálculos. Denotemos

$$f := xy, \quad g := x^3 - y^2 + x.$$

Calculemos el S-polinomio de f y g. Primero,

$$\operatorname{mcm}(LT(f), LT(g)) = \operatorname{mcm}(xy, x^3) = x^3 y.$$

Ahora

$$S(f, g) = \frac{x^3 y}{xy}\, xy - \frac{x^3 y}{x^3}\, (x^3 - y^2 + x) = y^3 - xy.$$

La división con resto nos da

$$y^3 - xy = (-1) \cdot xy + 0 \cdot (x^3 - y^2 + x) + y^3.$$

Entonces, hay que agregar a nuestra base el polinomio

$$h := y^3.$$

Procedamos calculando

$$\begin{aligned} S(h, f) &= \frac{xy^3}{y^3}\, y^3 - \frac{xy^3}{xy}\, xy = 0, \\ S(h, g) &= \frac{x^3 y^3}{y^3}\, y^3 - \frac{x^3 y^3}{x^3}\, (x^3 - y^2 + x) = y^5 - xy^3 = (y^2 - x) \cdot y^3. \end{aligned}$$

Entonces, el criterio de Buchberger nos dice que los polinomios

$$G = \{xy,\, x^3 - y^2 + x,\, y^3\}$$

forman una base de Gröbner. Notamos que esta ya es reducida.

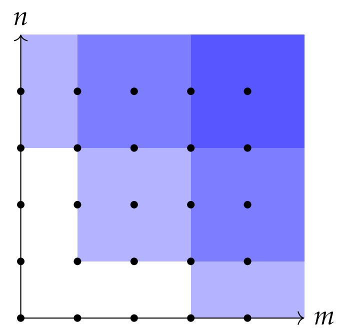
Ahora

$$(LT(G)) = (xy,\, x^3,\, y^3).$$

Los monomios que no están en este ideal son

$$1, y, y^2, x, x^2,$$

y estos forman una base de $k[x,y]/I$ como un espacio vectorial sobre k.



Ejercicio 2. Los polinomios de la forma $x^\alpha - x^\beta \in k[x_1, \dots, x_n]$ se llaman **binomios**. Se dice que un ideal I es **binomial** si I puede ser generado por algunos binomios. En este ejercicio vamos a probar que I es binomial si y solo si su base de Gröbner reducida consiste en binomios.

a) Demuestre que para dos binomios $f_1 = x^{\alpha(1)} - x^{\beta(1)}$ y $f_2 = x^{\alpha(2)} - x^{\beta(2)}$ el polinomio $S(f_1, f_2)$ es también un binomio si $f_1 \neq f_2$.

b) Sean $f = x^\alpha - x^\beta$, $f_1 = x^{\alpha(1)} - x^{\beta(1)}, \dots, f_s = x^{\alpha(s)} - x^{\beta(s)}$ binomios. Demuestre que el algoritmo de división con resto de f por $(f_1, \dots, f_s)$ produce
$$f = q_1 f_1 + \cdots + q_s f_s + r,$$
donde $r = 0$ o r es también un binomio.

c) Demuestre que todo ideal binomial tiene una base de Gröbner que consiste en binomios.

d) Demuestre que la base de Gröbner reducida de un ideal binomial consiste en binomios.

Este ejercicio es más interesante y requiere análisis un poco más creativo del algoritmo de división con resto y el algoritmo de Buchberger.

Primero, por la definición, tenemos para dos binomios
$$\begin{aligned} S(x^{\alpha(1)} - x^{\beta(1)}, x^{\alpha(2)} - x^{\beta(2)}) &= x^{\gamma-\alpha(1)} (x^{\alpha(1)} - x^{\beta(1)}) - x^{\gamma-\alpha(2)} (x^{\alpha(2)} - x^{\beta(2)}) \\ &= x^{\gamma-\alpha(2)+\beta(2)} - x^{\gamma-\alpha(1)+\beta(1)}, \end{aligned}$$
donde $x^\gamma = \operatorname{mcm}(x^{\alpha(1)}, x^{\alpha(2)})$. Entonces, el S-polinomio de dos binomios es también un binomio.

Ahora analicemos el algoritmo de división de $x^\alpha - x^\beta$ por binomios $f_1, \dots, f_s$. Al inicio del algoritmo, se tiene
$$q_1 := \cdots := q_s := 0, \quad r := 0, \quad p := f,$$
y entonces $r + p$ es un binomio. Vamos a probar por inducción que a cada paso se cumple una de las siguientes posibilidades:

- $r = x^\gamma - x^\delta$ es un binomio, $p = 0$ (y en este caso el algoritmo se termina),
- $p = x^\gamma - x^\delta$ es un binomio, $r = 0$,
- $p = x^\gamma$, $r = -x^\delta$,
- $r = x^\gamma$, $p = -x^\delta$.

Durante la ejecución del algoritmo ocurren dos situaciones.

i) Si $LT(f_i) \mid LT(p)$ para algún i, entonces en el algoritmo $r + p$ se remplaza por
$$r + p', \quad \text{donde } p' := p - (LT(p)/LT(f_i))\, f_i.$$
Si $p = x^\gamma - x^\delta$ es un binomio y $r = 0$, entonces
$$p' = x^{\beta(i)+\gamma-\alpha(i)} - x^\delta.$$
Si $p = x^\gamma$ y $r = -x^\delta$, entonces
$$p' = x^{\beta(i)+\gamma-\alpha(i)}.$$
De la misma manera, si $r = x^\gamma$ y $p = -x^\delta$, entonces
$$p' = -x^{\beta(i)+\delta-\alpha(i)}.$$

ii) Si $LT(f_i) \nmid LT(p)$ para ningún i, entonces r y p se remplazan por

$$r' := r + LT(p), \quad p' := p - LT(p).$$

Si $p = x^\gamma - x^\delta$ es un binomio y $r = 0$, entonces

$$r' = x^\gamma, \quad p' = -x^\delta.$$

Si $p = x^\gamma$ y $r = -x^\delta$, entonces

$$r' = x^\gamma - x^\delta, \quad p' = 0.$$

De la misma manera, si $r = x^\gamma$ y $p = -x^\delta$, entonces

$$r' = x^\gamma - x^\delta, \quad p' = 0.$$

Estas consideraciones nos permiten concluir que el algoritmo produce el resto que es también un binomio.

Ahora si I es un ideal binomial, podemos ejecutar el algoritmo de Buchberger sobre los generadores binomiales de I. A cada paso el algoritmo calcula los S-polinomios, y todos estos serán binomios gracias a la parte a). Los polinomios que se añaden a la base son restos de división de S-polinomios, y estos son binomios gracias a b). Podemos concluir que el algoritmo de Buchberger construye una base de Gröbner que consiste en binomios.

Quitando los polinomios innecesarios, se obtiene una base de Gröbner mínima $G = \{g_1, \ldots, g_s\}$ que también consiste en binomios. El algoritmo que construye la base reducida a cada paso remplaza g_i por $\overline{g_i}^{G \setminus \{g_i\}}$, y todos estos son binomios gracias a la parte b).

Ejercicio 3. En este ejercicio vamos a calcular el radical de un ideal monomial.

a) Demuestre que un ideal monomial $I \subset k[x_1, \ldots, x_n]$ es primo si y solo si $I = (x_{i_1}, \ldots, x_{i_s})$ es el ideal generado por algunas variables $\{x_{i_1}, \ldots, x_{i_s}\} \subseteq \{x_1, \ldots, x_n\}$.

b) Demuestre que si A es cualquier anillo conmutativo e $I, J \subseteq A$ son ideales, entonces

$$\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}, \quad \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

c) Para un monomio $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ demuestre que $\sqrt{(x^\alpha)} = (\sqrt{x^\alpha})$, donde

$$\sqrt{x^\alpha} := x_1^{\text{mín}(1,\alpha_1)} \cdots x_n^{\text{mín}(1,\alpha_n)} = \text{producto de las variables que están en } x^\alpha.$$

d) Demuestre que el ideal $(\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}})$ es radical.
Sugerencia: note que si $\sqrt{x^\alpha} = x_{i_1} \cdots x_{i_k}$, entonces $\sqrt{(x^\alpha)} = (x_{i_1}) \cap \cdots \cap (x_{i_k})$. Usando esta observación, exprese $(\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}}) = \bigcap_i \mathfrak{p}_i$, donde $\mathfrak{p}_i$ son algunos ideales monomiales primos.

e) Demuestre que $\sqrt{(x^{\alpha(1)}, \ldots, x^{\alpha(s)})} = \sqrt{(\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}})} = (\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}})$.

Este ejercicio no tiene nada que ver con las bases de Gröbner, sino revisa las propiedades de ideales monomiales que juegan papel importante en el curso. Consideremos entonces un ideal monomial propio

$$I = (x^{\alpha(1)}, \ldots, x^{\alpha(s)}),$$

donde $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ son generadores minimales. Para todo i existe j tal que $x_j \mid x^{\alpha(i)}$. Si $x^{\alpha(i)} \neq x_j$, entonces podemos escribir

$$x^{\alpha(i)} = x_j\, x^{\alpha'(i)},$$

y se ve que $x_j, x^{\alpha'(i)} \notin I$ (por la minimalidad de la base), lo que significa que el ideal no es primo. Entonces, los generadores de un ideal primo son necesariamente variables.

Viceversa, si un ideal I está generado por las variables $x_1, \ldots, x_\ell$, entonces

$$k[x_1, \ldots, x_n]/I \cong k[x_{\ell+1}, \ldots, x_n],$$

así que I es primo. Esto establece la parte a).

La parte b) es una propiedad general de radicales y la vimos en el curso de álgebra conmutativa. Para la suma de dos ideales $I, J \subseteq A$, podemos notar que

$$\sqrt{I+J} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \supseteq I+J}} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \supseteq I \text{ y } \mathfrak{p} \supseteq J}} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \supseteq \sqrt{I} \text{ y } \mathfrak{p} \supseteq \sqrt{J}}} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \supseteq \sqrt{I} + \sqrt{J}}} = \sqrt{\sqrt{I} + \sqrt{J}}.$$

Aquí hemos usado dos propiedades. Primero, cualquier ideal contiene $I + J$ si y solo si este contiene I y contiene J. Segundo, si $\mathfrak{p}$ es un ideal primo, entonces $\mathfrak{p} \supseteq I$ si y solo si $\mathfrak{p} \supseteq \sqrt{I}$ (se sigue de $\sqrt{I} \supseteq I$ y $\sqrt{\mathfrak{p}} = \mathfrak{p}$).

También, como nos propuso Mario, se podía ocupar directamente la definición del radical

$$\sqrt{I} := \{f \in A \mid f^r \in I \text{ para algún } r = 1, 2, 3, \ldots\}.$$

A saber, tenemos $I + J \subseteq \sqrt{I} + \sqrt{J}$, y luego $\sqrt{I+J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$. Esta es la inclusión trivial. Para la otra inclusión, notamos que si $f \in \sqrt{\sqrt{I} + \sqrt{J}}$, esto quiere decir que existen r, s, t tales que

$$f^r = g + h, \quad g^s \in I, \quad h^t \in J.$$

Ahora

$$f^{r\,(s+t)} = (g+h)^{s+t} = \sum_{i+j=s+t} \binom{s+t}{i} g^i\, h^j.$$

Aquí para cada término $g^i\, h^j$ se cumple $i \ge s$ o $j \ge t$, así que $g^i\, h^j \in I$ o $g^i\, h^j \in J$. Esto nos permite concluir que $f \in \sqrt{I+J}$.

Para la intersección de ideales, notamos que $f \in \sqrt{I \cap J}$ si y solo si existe r tal que $f^r \in I$ y $f^r \in J$, y luego $f \in \sqrt{I} \cap \sqrt{J}$. Viceversa, si $f \in \sqrt{I} \cap \sqrt{J}$, entonces existen r, s tales que $f^r \in I$ e $f^s \in J$. Para $t := \max\{r, s\}$ tenemos entonces $f^t \in I \cap J$, así que $f \in \sqrt{I \cap J}$. (Este es el argumento directo propuesto por Mario.)

La parte c) en realidad viene de una propiedad más general: *si A es un dominio de factorización única y $f \in A$ es un elemento que se factoriza como $f \sim f_1^{m_1} \cdots f_s^{m_s}$, donde $f_1, \ldots, f_s$ son elementos irreducibles no asociados entre sí y $m_1, \ldots, m_s \ge 1$, entonces $\sqrt{(f)} = (\sqrt{f})$, donde $\sqrt{f} := f_1 \cdots f_s$.*

En efecto, primero está claro que

$$f \mid (f_1 \cdots f_s)^m, \quad \text{donde } m := \max\{m_1, \ldots, m_s\},$$

y esto nos permite concluir que $(f_1 \cdots f_s) \subseteq \sqrt{(f)}$. Viceversa, asumamos que $g \in \sqrt{(f)}$. Luego, existe r tal que $f \mid g^r$. Factoricemos

$$g \sim g_1 \cdots g_t,$$

donde $g_1, \ldots, g_t$ son irreducibles (no necesariamente distintos). Tenemos entonces

$$(f_1^{m_1} \cdots f_s^{m_s}) \mid g_1^r \cdots g_t^r.$$

Por la irreducibilidad de los f_i y g_j, esto nos permite concluir que cada f_i es asociado con algún g_j, y luego

$$f_1 \cdots f_s \mid g,$$

Lo que establece la otra inclusión $\sqrt{(f)} \subseteq (f_1 \cdots f_s)$. ■

En este ejercicio particular, $f_1, \ldots, f_s$ son algunas variables $x_{i_1}, \ldots, x_{i_s}$. Como vimos arriba, la inclusión $(\sqrt{x^\alpha}) \subseteq \sqrt{(x^\alpha)}$ es fácil. Para la otra inclusión, tenemos que probar que si para un polinomio $g = \sum_\beta c_\beta\, x^\beta \in k[x_1, \ldots, x_n]$ se tiene $x^\alpha \mid g^r$ para algún r, entonces $\sqrt{x^\alpha} \mid g^r$. Uno puede tratar de analizar los términos de

$$g^r = \sum_\gamma \left(\sum_{\beta_1 + \cdots + \beta_r = \gamma} c_{\beta_1} \cdots c_{\beta_r} \right) x^\gamma,$$

pero no es una buena idea... Mejor ocupar las factorizaciones como en el argumento que acabo de dar.

En la parte d), usando

$$\sqrt{x^\alpha} = (x_{i_1}) \cap \cdots \cap (x_{i_t}).$$

podemos expresar

$$(\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}}) = \sum_{1 \le i \le s} (\sqrt{x^{\alpha(i)}})$$

como una suma de intersecciones de la forma $(x_{i_1}) \cap \cdots \cap (x_{i_t})$, y luego usar la distributividad[*] de $\cap$ respecto a la suma $\sum$ para escribir el ideal de arriba como una intersección de sumas

$$(x_{i_1}) + \cdots + (x_{i_t}) = (x_{i_1}, \ldots, x_{i_t}),$$

que son ideales primos gracias a la parte a).

Luego,

$$\sqrt{(\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}})} = \sqrt{\bigcap_i \mathfrak{p}_i} = \bigcap_i \sqrt{\mathfrak{p}_i} = \bigcap_i \mathfrak{p}_i = (\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}}).$$

Ahora combinando las partes b), c), y d), se tiene

$$\sqrt{(x^{\alpha(1)}, \ldots, x^{\alpha(s)})} = \sqrt{(\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}})} = (\sqrt{x^{\alpha(1)}}, \ldots, \sqrt{x^{\alpha(s)}}).$$

[*] En la tarea 1 hemos analizado intersecciones de ideales monomiales, y es fácil observar que $I \cap (J_1 + J_2) = (I \cap J_1) + (I \cap J_2)$ para ideales monomiales $I, J_1, J_2 \subseteq k[x_1, \ldots, x_n]$.