Ideales, Variedades y Algoritmos: Ch 1, Section 1

Francisco Javier Cruz Ortiz

22 de diciembre de 2022

1. Geometría Algebra y Algoritmos

1.1. Polinomios y espacios afín

Ejercicio 1.1.1. *Sea* $\mathbb{F}_2 = \{0, 1\}$ *con adición y multiplicación definidas por* $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 =$ *y* $1 \cdot 1 = 1$, *explicar porqué* $\mathbb{F}_2$ *es un campo.*

Solución: Note, por como se definen las operaciones en $\mathbb{F}_2$, es claro que $\mathbb{F}_2$ es asociativo con la suma y con el producto, además no es necesario verificar que se cumplen las propiedades distributivas puesto que las operaciones están bien definidas y el resultado de distrubuir el producto sobre la suma con los elementos $0, 1$ da como resultado ya sea 0 o 1, así basta con mostrar quienes son los inversos aditivos y multiplicativos además de las indentidades. En efecto, tenemos que la identidad aditiva en $\mathbb{F}_2$ es 0 puesto que cumple que para $0, 1 \in \mathbb{F}_2$ se cumple que $0 + 1 = 1 = 1 + 0$ y $0 + 0 = 0$. La identidad multiplicativa claramente es 1 puesto que para $0, 1 \in \mathbb{F}_2$ se tiene que $1 \cdot 0 = 0 = 0 \cdot 1$ y $1 \cdot 1 = 1$. Además los inversos aditivos de $0, 1 \in \mathbb{F}_2$ son ellos mismos puesto que $0 + 0 = 0$ y $1 + 1 = 0$ en $\mathbb{F}_2$. Y por ultimo tenemos que el inverso multiplicativo de $1 \in \mathbb{Z}_2$ es el mismo puesto que $1 \cdot 1 = 1$, omitiendo claramente al 0 puesto que 0 no tiene inverso multipliticativo. Concluyendo así que $\mathbb{F}_2$ es campo.

Ejercicio 1.1.2. *Sea* $\mathbb{F}_2$ *el campo del Ejercicio 1.1.1.*

1. *Conside el polinomio* $g(x, y) = x^2y + y^2x \in \mathbb{F}_2[x, y]$. *Demostrar que* $g(x, y) = 0$ *para todo* $(x, y) \in \mathbb{F}_2^2$, *y explicar porque esto no contradice la Proposición 5.*
2. *Encontrar un polinomio no cero en* $\mathbb{F}_2[x, y, z]$ *que se anule en todo punto de* $\mathbb{F}_2^3$.*Intentar encuentrar uno que involucre las tres variables.*
3. *Encontrar un polinomio en* $\mathbb{F}_2[x_1, ..., x_n]$ *que se anule en todo punto de* $\mathbb{F}_2^n$.*¿Es posible encontrar un polinomio en el que aparezcan todas las indeterminadas* $x_1, ..., x_n$*?*

Solución: Sea $\mathbb{F}_2 = \{0, 1\}$.

1. Sea, $\mathbb{F}_2^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$, y $g(x, y) = x^2y + y^2x \in \mathbb{Z}_2[x, y]$, así

$$\begin{aligned} g(0,0) =& (0)^2(0) + (0)^2(0) \\ =& 0, \\ g(0,1) =& (0)^2(1) + (1)^2(0) \\ =& 0 \\ g(1,0) =& (1)^2(0) + (0)^2(1) \\ =& 0 \\ g(1,1) =& (1)^2(1) + (1)^2(1) \\ =& 1 + 1 \\ =& 0 \end{aligned}$$

por lo que g se anula en todo punto de $\mathbb{F}_2^2$ y esto no contradice la proposición 5 puesto que $\mathbb{F}_2$ es un campo finito.

2. Sea $\mathbb{F}_2^3 = \{(0,0,0),(0,0,1),(0,1,0),(1,0,0),(0,1,1),(1,1,0),(1,0,1),(1,1,1)\}$, entonces note que

$$
\begin{aligned}
0 =& (0)(0)(0) + (0)(0)(0)^2 \\
0 =& (0)(0)(1) + (0)(0)(1)^2 \\
0 =& (0)(1)(0) + (0)(1)(0)^2 \\
0 =& (1)(0)(0) + (1)(0)(0)^2 \\
0 =& (0)(1)(1) + (0)(1)(1)^2 \\
0 =& (1)(1)(0) + (1)(1)(0)^2 \\
0 =& (1)(0)(1) + (1)(0)(1) \\
0 =& (1)(1)(1) + (1)(1)(1)^2
\end{aligned}
$$

lo cuál sucede puesto que $0^2 = 0$ y $1^2 = 1$. Además, con esto hay que observar que contruimos 7 "sumas" de dos 0 y una de dos ünos" . pues en el producto xyz si x, y o z es cero, entonces $xyz = 0$ y $xyz^2 = 0$, por lo que $xyz + xyz^2 = 0$ en estos casos. Por otra parte, si $x = y = z = 1$ entonces $xyz = 1$ y $xyz^2 = 1$. Entonces $xyz + xyz^2 = 0$ (pues $1 + 1 = 0$ en $\mathbb{F}_2$). Por lo que $g(x,y,z) = xyz + xyz^2$ es un polinomio en $\mathbb{F}_2[x,y,z]$ que se anula en todo $\mathbb{F}_2^3$.

3. Usando un argumento similar al inciso anterior tenemos que

$$g(x_1, x_2, ..., x_n) = x_1x_2...x_n + x_1x_2...x_n^2$$

es un polinomio en $\mathbb{F}[x_1, ..., x_n]$ que se anula en todo punto de $\mathbb{F}_2^n$.

Ejercicio 1.1.3. *Sea p un número primo. El anillo de enteros módulo p es un campo con p elementos, que denotaremos como $\mathbb{F}_p$.*

1. *Explica porqué $\mathbb{F}_p \setminus \{0\}$ es un grupo bajo el producto.*
2. *Usa el Teorema de Lagrange para mostrar que $a^{p-1} = 1$ para todo $a \in \mathbb{F}_p$.*
3. *Prueba que $a^p = a$ para todo $a \in \mathbb{F}_p$.*
4. *Encuentra un polinomio no cero en $\mathbb{F}_p[x]$ que se anule en todos los puntos de $\mathbb{F}_p$.*

Demostración. Sea $\mathbb{Z}_p = \mathbb{F}_p$. Usaremos $=$ en vez de $\equiv$ en los incisos b,c y d.

1. Es claro que el producto en general para $\mathbb{Z}_n$ está bien definido y en particular para $\mathbb{Z}_p$, además es claro que es asociativo pues si para $a, b, c \in \mathbb{Z}_n$ tales que $(ab)c \equiv d \pmod{n}$ p.a $d \in \mathbb{Z}_n$ entonces $d \equiv a(bc) \pmod{n}$ y por transitividad se tiene lo deseado y en particular sucede en $\mathbb{Z}_p$. Luego, se sabe que la identidad multiplicativa en $\mathbb{Z}_n$ es la clase del 1 y en particular lo és para $\mathbb{Z}_p$. Pero en general no todo elemento de $\mathbb{Z}_n$ tiene inverso multiplicativo puesto que hay elementos no nulos en $\mathbb{Z}_n$ cuyo produto es cero. Tomemos por ejemplo el caso de $\mathbb{Z}_6$ y los elementos 3 y 4 cuyo producto resulta

$$3 \cdot 4 \equiv 0 \pmod{6}$$

así que si se quiere para $a \in \mathbb{Z}_n$ no nulo exista un inverso multiplicativo $b \in \mathbb{Z}_n$ no nulo debe de cumplir que $ab \equiv 1 \pmod{n}$ lo que equivale a que $ab - 1 = nk$ con $k \in \mathbb{Z}$ si y sólo si $ab - nk = 1$ lo que significa en términos más generales que mcd(a,n)=mcd(b,n)= 1, es decir, $a \in \mathbb{Z}_n$ tendra inverso multiplicativo b en $\mathbb{Z}_n$ si y sólo si mcd(a,n)= 1 (de igual forma con b tomando a su inverso como a). Y en particular notemos que para $\mathbb{Z}_p \setminus \{0\} = \{1, 2, ..., p-1\}$ se cumple que mcd(a,p)= 1 para todo $a \in \mathbb{Z}_p \setminus \{0\}$ ya que en caso contrario de que mcd(a,n)= d con $d > 1$ y $a \in \{1, 2, ..., p-1\}$ se tendría que

$$d|p \Leftrightarrow d = p$$

pues $d > 1$ y p es primo. Además se tiene que $d|a$ de dónde $p|a$ y a sería un multiplo de p lo que no es posible puesto que $a < p$ pues $a \in \mathbb{Z}_p \setminus \{0\}$. Por lo que se garantiza que en $\mathbb{Z}_p \setminus \{0\}$ todo elemento tiene un inverso multiplicativo y así $\mathbb{Z}_p \setminus \{0\}$ tiene estructura de grupo.

2. Sea $a \in \mathbb{F}_p \setminus \{0\}$ puesto que $\mathbb{F}_p \setminus \{0\}$ es un grupo finito de orden $p-1$, recordemos que el *Teorema de Lagrange* indica que el orden de todo subgrupo de un grupo G divide al orden de G. Consideremos así al subgrupo $H = \{a^n : a \in \mathbb{F}_p \setminus \{0\}, n \in \mathbb{Z}\}$. Sabemos que H es un subgrupo ciclico de $\mathbb{F}_p \setminus \{0\}$ generado por a dónde $|H| = o(a)$ (pues $\mathbb{F}_p \setminus \{0\}$ es un grupo finito) y así afirmamos que $a^{|\mathbb{F}_p \setminus \{0\}|} = 1$. En efecto, puesto que H es un subgrupo de $\mathbb{F}_p \setminus \{0\}$ entonces por el teorema de Lagrange se tiene que $|H| \mid |\mathbb{F}_p \setminus \{0\}|$ y como $|H| = o(a)$ se tiene que $o(a) \mid |\mathbb{F}_p \setminus \{0\}|$ y como $|\mathbb{F}_p \setminus \{0\}| = p-1$ entonces se tiene que $p - 1 = o(a)k$ para algún $k \in \mathbb{Z}$ y así

$$\begin{aligned} a^{|\mathbb{F}_p \setminus \{0\}|} &= a^{p-1} \\ &= a^{o(a)k} \\ &= (a^{o(a)})^k \\ &= (1)^k \\ &= 1 \end{aligned}$$

es decir, $a^{p-1} = 1$ para todo $a \in \mathbb{F}_p \setminus \{0\}$.

3. Sea $a \in \mathbb{F}_p$, si $a = 0$ entonces es claro que $a^p = 0$ puesto que $0^p \equiv 0 \mod p$. Luego, si $a \neq 0$ entonces $a \in \mathbb{F}_p \setminus \{0\}$ y por el inciso anterior vimos que $a^{p-1} = 1$ para toda $a \in \mathbb{F}_p \setminus \{0\}$ y así

$$\begin{aligned} (a)a^{p-1} &= (a)1 \\ a^p &= a \end{aligned}$$

para todo $a \in \mathbb{F}_p \setminus \{0\}$, y como esto se cumple para toda $a \in \mathbb{F}_p$ podemos concluir que $a^p = a$ para todo $a \in \mathbb{F}_p$.

4. Mostramos anteriormente que para todo $a \in \mathbb{F}_p$ sucede que $a^p = a$ de aquí tenemos que $a^p - a = 0$ para toda $a \in \mathbb{F}_p$ por lo que podemos contruir un polinomio en $\mathbb{F}_p[x]$ dado por

$$x^p - x$$

el cual se anula en todo punto de $\mathbb{F}_p$.

□

Ejercicio 1.1.4. *Sea $\mathbb{F}$ un campo finito con q elementos. Adapta el argumento del Ejercicio 1.1.3 para demostrar que $x^q - x$ es un polinomio no nulo en $\mathbb{F}[x]$ que se anula en todo punto de $\mathbb{F}$.*

Demostración. Sea $\mathbb{F}$ un campo con q elementos, digase $q = p^n$ dónde p es un número primo, tenemos que $\mathbb{F} \setminus \{0\}$ es grupo multiplicativo de orden $q - 1$, por lo que dicho grupo es de orden finito, así, para cada $a \in \mathbb{F} \setminus \{0\}$ consideramos al subgrupo $H = \{a^n : a \in \mathbb{F} \setminus \{0\}, n \in \mathbb{Z}\}$. Sabemos que H es un subgrupo ciclico de $\mathbb{F} \setminus \{0\}$ generado por a dónde $|H| = o(a)$ (pues $\mathbb{F} \setminus \{0\}$ es un grupo finito) y así afirmamos que $a^{|\mathbb{F} \setminus \{0\}|} = 1$. En efecto, puesto que H es un subgrupo de $\mathbb{F}_q \setminus \{0\}$ entonces por el teorema de Lagrange se tiene que $|H| \mid |\mathbb{F} \setminus \{0\}|$ y como $|H| = o(a)$ se tiene que $o(a) \mid |\mathbb{F} \setminus \{0\}|$ y como $|\mathbb{F} \setminus \{0\}| = q - 1$ entonces se tiene que $q - 1 = o(a)k$ para algún $k \in \mathbb{Z}$ y así

$$
\begin{aligned}
a^{|\mathbb{F}\setminus\{0\}|} &= a^{q-1} \\
&= a^{o(a)k} \\
&= (a^{o(a)})^k \\
&= (1)^k \\
&= 1
\end{aligned}
$$

y así se cumple que $a^{q-1} = 1$ de donde $a^q = a$ para todo $a \in \mathbb{F} \setminus \{0\}$. Además es claro que $0^q = 0$ en $\mathbb{F}$ de modo que el polinomio $x^q - x$ se anula en todo $\mathbb{F}$. Más aún, la construcción de este polinomio sobre un campo finito indica que la proposición 1.1 en efecto pude fallar absolutamente sobre todos los campos finitos. $\square$

Ejercicio 1.1.5. *En la demostración de la Proposición 5, tomamos $f \in k[x_1, ..., x_n]$ y lo escribimos como un polinomio en x_n con coeficientes en $k[x_1, ..., x_{n-1}]$. Para ver cómo se ve esto en un caso específico, considere el polinomio*

$$f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3.$$

a) *Escribe a f como un polinomio en $k[y, z]$.*

b) *Escribe a f como un polinomio en $k[x, z]$.*

c) *Escribe a f como un polinomio en $k[x, y]$.*

Solución: Sea $f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3 \in \mathbb{K}[x, y, z]$.

a) Reordenamos a $f(x, y, z)$ por orden los exponentes de la variable x como se sigue:

$$f(x, y, z) = x^5y^2z - x^4y^3 + x^2z + xy + 2x - 5z + y^4 - y^3z + 3$$

y factorizando terminos iguales con diferente coeficiete y asociando constantes independientes obtenemos que

$$f(x, y, z) = x^5y^2z - x^4y^3 + x^2z + (y + 2)x + (y^4 - y^3z + 5z + 3).$$

b) Reordenamos a $f(x, y, z)$ por orden los exponentes de la variable y como se sigue:

$$f(x, y, z) = y^5 - y^3x^4 - y^3z + y^2x^5z + yx + x^2z + 2x - 5z + 3$$

y factorizando terminos iguales con diferente coeficiete y asociando constantes independientes obtenemos que

$$f(x, y, z) = y^5 - y^3(x^4 - z) + y^2(x^5z) + y(x) + (x^2z + 2x - 5z + 3)$$

c) Reordenamos a $f(x, y, z)$ por orden los exponentes de la variable z como se sigue:

$$f(x, y, z) = zx^5y^2 + zx^2 - zy^3 - 5z - x^4y^3 + xy + y^5 - 2x + 3$$

y factorizando terminos iguales con diferente coeficiete y asociando constantes independientes obtenemos que

$$f(x, y, z) = z(x^5y^2 + x^2 - y^3 - 5) - (x^4y^3 - xy - y^5 + 2x - 3).$$

Ejercicio 1.1.6. *Dentro de $\mathbb{C}^n$ tenemos el subconjunto $\mathbb{Z}^n$, que consta de todos los puntos con coordenadas enteras.*

a) *Demostrar que si $f \in \mathbb{C}[x_1, ..., x_n]$ se anula en todo punto de $\mathbb{Z}^n$ entonces, f es el polinomio cero.*

b) *Sean $f \in \mathbb{C}[x_1, ..., x_n]$ y M el máximo de los exponentes de cualquier variable que aparezca en f. Sea $\mathbb{Z}^n_{M+1}$ el conjunto de los puntos en $\mathbb{Z}^n$ para lo que todas sus coordendas están entre 1 y $M+1$, inclusive. Demostrar que si f se anula en todos los puntos de $\mathbb{Z}^n_{M+1}$ entonces, f es el polinomio cero.*

Demostración. a) Sea $f \in \mathbb{C}[x_1, ..., x_n]$ un polinomio no cero que se anula en todo punto de $\mathbb{Z}^n$, por inducción sobre el número de variables y coordenadas en $\mathbb{Z}$. Si $n = 1$ y f es un polinomio en $\mathbb{C}[x_1]$ que se anula en todo punto de $\mathbb{Z}$, con $\deg(f) = m > 0$ (pues un polinomio contante no cero no se anula en ningún punto), f puede tener a lo más m raíces (no necesariamente distintas), en particular si $f \in \mathbb{C}[x_1]$ es tal que $f(a) = 0$ para todo $a \in \mathbb{Z}$, entonces f tendría infinitas raíces ya que $\mathbb{Z}$ es un conjunto infinito lo que contradice que $\deg(f) = m > 0$ por lo que tiene que suceder que f es el polinomio cero.

Ahora supongamos que es cierto para $n-1$, es decir, si $f \in \mathbb{C}[x_1, ..., x_{n-1}]$ es un polinomio que se anula en todo punto de $\mathbb{Z}^{n-1}$ entonces f es el polinomio cero.

Luego, sea $f \in \mathbb{C}[x_1, ..., x_n]$ un polinomio tal que $f(a_1, ..., a_n) = 0$ para todo $(a_1, ..., a_n) \in \mathbb{Z}^n$, dado que $f \in \mathbb{C}[x_1, ..., x_n]$ entonces podemos ver a f como:

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n}$$

con $\alpha = (\alpha_1, ..., \alpha_n)$. Tomando a N como el exponente más grande en la varieble x_n, es decir, el máximo de los α_n tal que $x_n^{\alpha_n}$, podemos reescribir a f como

$$f = \sum_{j=0}^{N} g_j(x_1, ..., x_{n-1}) x_n^j$$

dónde $g_j(x_1, ..., x_{n-1}) \in \mathbb{C}[x_1, ..., x_{n-1}]$. Sea entonces $(b_1, ..., b_{n-1}) \in \mathbb{Z}^{n-1}$ tal que

$$f(b_1, ..., b_{n-1}, x_n) = \sum_{j=0}^{N} g_j(b_1, ..., b_{n-1}) x_n^j$$

con $g_j(b_1, ..., b_{n-1}) x_n^j \in \mathbb{C}[x_n]$ y supongamos que $x_n = b_n$ para algún $b_n \in \mathbb{Z}$, así

$$0 = f(b_1, ..., b_{n-1}, b_n) = \sum_{j=0}^{N} g_j(b_1, ..., b_{n-1}) b_n^j$$

pues f se anula en todo $\mathbb{Z}^n$ por hipotesís. Así f se anula en $\mathbb{Z}$ y por la base inductiva f es el polinomio cero en $\mathbb{C}[x_n]$. Por lo que para toda $j = 0, 1, ..., N$, $g_j \in \mathbb{C}[x_1, ..., x_{n-1}]$ se anula en todo $\mathbb{Z}^{n-1}$ y por la hipótesis de inducción $g_j(x_1, ..., x_{n-1})$ es el polinomio cero en $\mathbb{C}[x_1, ..., x_{n-1}]$ para todo $j = 0, 1, ..., N$ y concluyendo que f es el polinomio cero en $\mathbb{C}[x_1, ..., x_n]$.

b) Sean $f \in \mathbb{C}[x_1, ..., x_n]$ y M el máximo exponente de cualquier variable que aparece en f, si $M = 0$ no hay nada que demostrar. Supongamos entonces que $M > 0$ de dónde $M + 1 > 0$, entonces aplicando inducción sobre el número de variables y número de coordenadas en $\mathbb{Z}$. Cuando $n = 1$ entonces f es un polinomio en $\mathbb{C}[x_1]$ que se anula en todo punto de $\mathbb{Z}_{M+1}$ pero M es el máximo exponente de x_1 en f, es decir, $\deg(f) = M$ por lo que f puede tener a lo más M raíces en $\mathbb{Z}_{M+1}$ (no necesariamente distintas), lo que contradice el hecho de que $\deg(f)$ es M por lo que tiene que suceder que f es el polinomio cero. Ahora supongamos que es cierto para $n-1$, es decir, si $f \in \mathbb{C}[x_1, ..., x_{n-1}]$ es un polinomio que se anula en todo punto de $\mathbb{Z}^{n-1}_{M+1}$ donde M es el exponente que aparece en cualquier indeterminada de f, entonces f es el polinomio cero.

Luego, para el paso inductivo, si $f \in \mathbb{C}[x_1, ..., x_n]$ es un polinomio que se anula en todo punto de $\mathbb{Z}^n_{M+1}$ donde M es el máximo exponente que apaerece en cualquier indeterminada de f, entonces tenemos que $f(a_1, ..., a_n) = 0$ para todo $(a_1, ..., a_n) \in \mathbb{Z}^n_{M+1}$, y dado que $f \in \mathbb{C}[x_1, ..., x_n]$ podemos ver a f en la forma

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n}$$

con $\alpha = (\alpha_1, ..., \alpha_n)$. Por hipótesis tenemos que M es el exponente más grande en la varieble x_n, es decir, podemos reescribir a f como

$$f = \sum_{j=0}^{M} g_j(x_1, ..., x_{n-1}) x_n^j$$

dónde $g_j(x_1, ..., x_{n-1}) \in \mathbb{C}[x_1, ..., x_{n-1}]$. Sea entonces $(b_1, ..., b_{n-1}) \in \mathbb{Z}_{M+1}^{n-1}$ tal que

$$f(b_1, ..., b_{n-1}, x_n) = \sum_{j=0}^{M} g_j(b_1, ..., b_{n-1}) x_n^j$$

con $g_j(b_1, ..., b_{n-1}) x_n^j \in \mathbb{C}[x_n]$ y supongamos que $x_n = b_n$ para algún $b_n \in \mathbb{Z}_{M+1}$, así

$$0 = f(b_1, ..., b_{n-1}, b_n) = \sum_{j=0}^{M} g_j(b_1, ..., b_{n-1}) b_n^j$$

pues f se anula en todo $\mathbb{Z}_{M+1}^n$ por hipotesís. Así f se anula en todo $\mathbb{Z}_{M+1}$ y por la base inductiva f es el polinomio cero en $\mathbb{C}[x_n]$. Por lo que para toda $j = 0, 1, ..., M$, $g_j \in \mathbb{C}[x_1, ..., x_{n-1}]$ se anula en todo punto de $\mathbb{Z}_{M+1}^{n-1}$ y por la hipótesis de inducción $g_j(x_1, ..., x_{n-1})$ es el polinomio cero en $\mathbb{C}[x_1, ..., x_{n-1}]$ para todo $j = 0, 1, ..., M$ y concluyendo que f es el polinomio cero en $\mathbb{C}[x_1, ..., x_n]$.

$\square$