Algebra Abstracta II: Tarea #1

Jonathan Andrés Niño Cortés

13 de febrero de 2015

Teorema chino del residuo sobre $\mathbb{Z}$ y el teorema de interpolación de Lagrange

(a) Sean $a, b \in \mathbb{F}$ y $c(x) \in \mathbb{F}[x]$. Muestre que $c(a) = b$ si y solo si $c(x) \equiv \text{mod } (x - a)$.

Demostración. Suponga que $c(x) \equiv b \text{ mod}(x - a)$, entonces existe un polinomio $Q(x)$ tal que $c(x) - b = Q(x)(x - a)$. Es decir que $c(x) = Q(x)(x - a) + b$. Por lo tanto $c(a) = Q(a)(a - a) + b = b$.

Ahora suponga que $c(a) = b$. Tendriamos por lo tanto que el polinomio $f(x) = c(x) - b$ es tal que $f(a) = c(a) - b = b - b = 0$. Por lo tanto $f(x)$ tiene una raiz en a por lo que es divisible por $x - a$. Por lo tanto, $f(x) = c(x) - b \equiv 0 \text{ mod}(x - a)$. De donde se concluye que $c(x) \equiv b \text{ mod}(x - a)$. □

(b) Deduzca el teorema de interpolación de Lagrange del Teorema chino del residuo.

Demostración. El teorema chino del residuo generalizado nos dice que si R es un anillo conmutativo e $I_1 \cdots I_n \subseteq R$ son ideales comaximales dos a dos entonces el homomorfismo $\phi : R \to R/I_1 \times \cdot \times R/I_n$, tal que $\phi(x) \mapsto (x + I_1, \cdots x + I_n)$. Entonces, ϕ es sobreyectiva y $\ker(\phi) = I_1 \cdots I_n$.

Para poder utilizarlo en el teorema de interpolación de Lagrange tenemos que verificar que los supuestos se cumplen. En primer lugar el anillo $\mathbb{F}[x]$ es conmutativo. Los ideales que vamos a tomar son los principales de los polinomios de la forma $x - x_i$. Para demostrar que son comaximales tomese x_i y x_j tales que $i \neq j$. Entonces $1 = \frac{1}{(x_j - x_i)}(x - x_i) - \frac{1}{(x_j - x_i)}(x - x_j)$, por lo que $\langle (x - x_i) \rangle + \langle (x - x_j) \rangle = \langle 1 \rangle$. (Obsérvese que $x_j - x_i \neq 0$ porque alguno de los dos es diferente a 0).

Por lo tanto podemos aplicar el teorema chino del residuo. Como resultado obtenemos que para cualquier $(y_0, \cdots, y_n)$ existe un único polinomio $p(x)$ módulo $\langle (x - x_0) \rangle \cdots \langle (x - x_n) \rangle$ tal que $p(x) \equiv y_i \text{ mod } \langle x - x_i \rangle$ para todo $i \in \{0, \cdots, n\}$. Por el literal anterior, esto equivale a que $p(x_i) = y_i$.

Y que sea único módulo el producto de los ideales implica que únicamente hay un polinomio de grado a lo sumo n que cumple esta propiedad. Que existe un polinomio de grado a lo sumo igual a n es una consecuencia del algóritmo de la división, pues este nos dice que existen unicos polinomios $q(x)$ y $r(x)$ tales que $p(x) = q(x)(x-x_0)\cdots(x-x_n) + r(x)$ con $r(x)$ de grado menor a $n+1$. Por lo tanto tomamos el polinomio $r(x)$, como el polinomio que buscamos en la interpolación de Lagrange.

Por otra parte para demostrar que es único podemos demostrar el siguiente lema.

Lema 1. *Sean $p(x), m(x)$ polinomios tales que deg$(p(x)) <$ deg$(m(x))$.Si $p(x)$ es un polinomio que es congruente a 0 módulo $\langle m(x)\rangle$.*

Demostración. Lo anterior quiere decir que existe un polinomio $q(x)$ tal que $p(x) = q(x)m(x)$. Supongase por contradicción que $p(x) \neq 0$, entonces tenemos que $q(x)$ y $m(x)$ son diferentes de 0 pues $\mathbb{F}[x]$ es un dominio. Entonces, si analizamos los grados tenemos que $\deg(p(x)) = \deg(q(x)m(x)) = \deg(q(x)) + \deg(m(x))$. Pero esto no es posible por nuestra suposición. Por lo tanto, concluimos que $p(x) = 0$. ☐

Por lo tanto, si tomamos $r(x), r'(x)$ tales que cumplen con la interpolación de Lagrange y además que el grado de ambos es a lo sumo n, entonces tenemos que $r(x) \equiv r'(x) \bmod \langle (x-x_0)\cdots(x-x_n)\rangle$. Entonces tenemos que $r(x) - r'(x) \equiv 0 \bmod \langle (x-x_0)\cdots(x-x_n)\rangle$. Y tenemos que $\deg(r(x) - r'(x)) < n < \deg((x-x_0)\cdots(x-x_n))$. Concluimos que $r(x) - r'(x) = 0$ por lo que $r(x) = r'(x)$. ☐

(c) Sean $x_0 \in \mathbb{F}$ y $h(x) \in \mathbb{F}[x]$ tal que $h(x_0) \neq 0$. Encuentre $s_0(x)$ y $t_0(x)$ en $\mathbb{F}[x]$ tales que

$$s_0(x)(x-x_0) + t_0(x)h_0(x) = 1.$$

Demostración. Utilizamos el algoritmo de la división para dividir $h_0(x)$ por $(x-x_0)$ (tal como se haría en el algoritmo de euclides).

Tendriamos que

$$h_0(x) = q(x)(x-x_0) + r(x) \tag{1}$$

Con $q(x)$ y $r(x)$ únicos y $\deg(r(x)) < \deg(x-x_0) = 1$. Por lo tanto $r(x)$ solo puede ser una constante. Además r denotada de esta manera porque es una constante no puede ser igual a la constante 0, pues esto implicaria que $h_0(x)$ sería divisible por $x-x_0$, es decir que al evaluar en x_0, tendriamos que $h_0(x_0) = 0$ que contradice nuestra suposición.

Pero aun más, si reducimos módulo $\langle x-x_0\rangle$ tenemos que $h_0 \equiv r \bmod \langle x-x_0\rangle$. Por el punto tenemoes que esto es equivalente a que $r = h_0(x_0)$.

Finalmente dividimos la ecuación (1) a lado y lado por $h_0(x_0)$ y obtenemos

$$\frac{h_0(x)}{h_0(x_0)} = \frac{q(x)}{h_0(x_0)}(x-x_0) + 1$$

y despejando el 1 obtenemos

$$-\frac{q(x)}{h_0(x_0)}(x-x_0)+\frac{h_0(x)}{h_0(x_0)}=+1$$

Luego $s_0(x)=-q(x)/h_0(x_0)$ y $t_0(x)=1/h_0(x_0)$. □

(d) Encuentre una fórmula explicita para el polinomio $p(x)$ del T.I.L.

Demostración. Siguiendo la misma estrategia descrita para el teorema chino del residuo en los enteros, vamos a buscar polinomios $p_i(x)$ tales que $p_i(x_i)=1$ y $p_i(x_j)=0$ si $i\neq j$. Para encontrarlos buscamos los polinomios $s_i(x)$ y $t_i(x)$ que resuelvan la ecuación

$$s_i(x)(x-x_i)+t_i(x)h_i(x)=1.$$

Donde

$$h_i(x)=\prod_{j=0,j\neq i}^{n}(x-x_j).$$

Entonces, por el punto anterior tenemos que

$$t_i(x)=\frac{1}{h_i(x_i)}=\prod_{j=0,j\neq i}^{n}\frac{1}{x_i-x_j}$$

Luego el polinomio $p_i(x)$que estamos buscando es

$$p_i(x)=t_i(x)h_i(x)=\prod_{j=0,j\neq i}^{n}\frac{x-x_j}{x_i-x_j}$$

Nótese que este polinomio es de grado n porque es la multiplicación de n polinomios de grado 1.

Por ultimo el polinomio $p(x)$ de la interpolación de Lagrange sería

$$p(x)=\sum_{i=0}^{n}y_ip_i(x).$$

Nótese que el grado de este polinomio es a lo sumo n porque es el resultado de la suma de polinomios de grado n. □

Sección 7.5 1. Completa todos los detalles en la prueba del teorema 15.

Demostración. Parte de los detalles que faltan es probar que Q con las operaciones

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \text{ y } \frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}$$

- Las operaciones estan bien definidas: Tengase en cuenta que $\frac{a}{b}=\frac{a'}{b'}$ si y solo si $ab'=ba'$.

  Sean $\frac{a}{b}=\frac{a'}{b'}$ y $\frac{c}{d}=\frac{c'}{d'}$. Por un lado

  $$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \text{ y } \frac{a'}{b'}+\frac{c'}{d'}=\frac{a'd'+b'c'}{b'd'}$$

  Tenemos que $(ad+bc)b'd'=adb'd'+bcb'd'=a'bdd'+c'dbb'=(a'd'+b'c')bd$. Luego la suma esta bien definida

  Similarmente, para la multiplicación tenemos que

  $$\frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd} \text{ y } \frac{a'}{b'}+\frac{c'}{d'}=\frac{a'c'}{b'd'}$$

  Y tenemos que $acb'd'=a'c'bd$, luego la multiplicación esta bien definida

- La suma es asociativa: Sean $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in Q$. Por un lado

  $$\frac{a}{b}+(\frac{c}{d}+\frac{e}{f})=\frac{a}{b}+\frac{cf+de}{df}=\frac{adf+bcf+bde}{bdf}$$

  Por otra parte,

  $$(\frac{a}{b}+\frac{c}{d})+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{adf+bcf+bde}{bdf}$$

  Por lo tanto es asociativa.

- La suma es conmutativa: Sean $\frac{a}{b},\frac{c}{d}\in Q$

  Tenemos que

  $$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}$$

  por lo cual la suma es conmutativa

- $\frac{0}{d}$ es la identidad de la suma:

  En efecto tenemos

  $$\frac{0}{d}+\frac{a}{b}=\frac{0b+da}{db}=\frac{da}{db}=\frac{a}{b}.$$

  La ultima igualdad se da porque $dab=dba$.

- <u>$\frac{-a}{b}$ es el inverso de $\frac{a}{b}$:</u> Tenemos que

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{bb} = \frac{ab - ab}{bb} = \frac{0}{bb}$$

- <u>La multiplicación es asociativa:</u> Sean $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q$. Por un lado

$$\frac{a}{b} \times (\frac{c}{d} \times \frac{e}{f}) = \frac{a}{b} \times \frac{ce}{df} = \frac{ace}{bdf}$$

Por el otro lado

$$(\frac{a}{b} \times \frac{c}{d}) \times \frac{e}{f} = \frac{ac}{bd} \times \frac{ace}{bdf}$$

Por lo que la multiplicación es asociativa.

- <u>La multiplicación es conmutativa:</u> Sean $\frac{a}{b}, \frac{c}{d} \in Q$.

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \times \frac{a}{b}$$

Por lo cual, la multiplicación es conmutativa

- <u>La identidad de Q es $\frac{d}{d}$:</u> En efecto,

$$\frac{d}{d} \times \frac{a}{b} = \frac{da}{db} = \frac{a}{b}$$

La ultima igualdad se da porque $dab = dba$.

- <u>La multiplicación es distributiva:</u> Sea $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q$.

$$\frac{a}{b} \times (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} \times \frac{cf + de}{df} = \frac{acf + ade}{bdf}$$

Por otro lado

$$(\frac{a}{b} \times \frac{c}{d}) + (\frac{a}{b} \times \frac{e}{f}) = \frac{ac}{bd} + \frac{ae}{bf} = \frac{acbf + bdae}{bdbf} = \frac{b}{b} \times \frac{acf + dae}{dbf} = \frac{acf + dae}{dbf}$$

Concluimos que la multiplicación es distributiva.

Por ultimo falta probar que la función $\Phi : Q \mapsto S$ tal que $\Phi(rd^{-1}) = \phi(r)\phi(d)^{-1}$ es un homomorfismo de anillos entre Q y S. Por un lado,

$$\Phi(rd^{-1}se^{-1}) = \Phi(rs(de)^{-1}) = \phi(rs)\phi(de)^{-1} = \phi(r)\phi(s)\phi(d)^{-1}\phi(e)^{-1} = \Phi(rd^{-1})\Phi(se^{-1})$$

Por otro lado,

$$\begin{aligned}
\Phi(rd^{-1}+se^{-1}) &= \Phi((re+ds)(de)^{-1}) \\
&= \phi(re+ds)\phi(de)^{-1} \\
&= (\phi(r)\phi(e)+\phi(d)\phi(s))\phi(d)^{-1}\phi(e)^{-1} \\
&= \phi(r)\phi(e)\phi(d)^{-1}\phi(e)^{-1}+\phi(d)\phi(s)\phi(d)^{-1}\phi(e)^{-1} \\
&= \phi(r)\phi(d)^{-1}+\phi(s)\phi(e)^{-1} \\
&= \Phi(rd^{-1})+\Phi(se^{-1})
\end{aligned}$$

Por lo tanto $\Phi(rd^{-1})$ es un homomorfismo entre anillos. $\square$

Sección 7.5 3. Sea F un campo. Pruebe que F contiene un único subcampo más pequeño F_0 y que F_0 es isomórfico a $\mathbb{Q}$ o $\mathbb{Z}/p\mathbb{Z}$ para un primo p (F_0 se llama el subcampo primo de F).

Demostración. Tomemos el homomorfismo $\phi : \mathbb{Z} \to F$ definido en el ejercicio 26 de la sección 7.3. Por ese punto sabemos que el kernel del homomorfismo debe ser $n\mathbb{Z}$ donde n es la caracteristica del campo. Si n es cero entonces el kernel es $\{0\}$ y por lo tanto el homomorfismo es inyectivo. Es decir que F contiene un subanillo isomorfo a los enteros. Por el Teorema 15 de Dummit hay una única inyección que me da el campo cociente de este subanillo que debe ser isomorfo a $\mathbb{Q}$.

Si n no es cero entonces tenemos que hay un subanillo $\mathbb{Z}/n\mathbb{Z}$ pero al estar contenido en un campo ningún elemento puede ser un divisor de cero. Esta restricción obliga a que n sea igual a p un primo de $\mathbb{Z}$. Pero además como $\mathbb{Z}/p\mathbb{Z}$ es un dominio integro finito, es un campo por un ejercicio demostrado en clase.

Supongamos que F^* sea un subcampo de F. Sea 1_F la identidad de F y $1*$ la identidad de F_*. Si tomamos un elemento cualquiera $a \in F^*$ tenemos que existe $a^{-1} \in F^*$ tal que $aa^{-1} = 1_*$. Sin embargo, los elementos también pertenecen a F por lo que $aa^{-1} = 1_F$. Por lo tanto, $1_* = 1_F$.

Ahora tomemos un campo cualquier F^* sabemos que 1 pertenece a F^*, pero además cualquier elemento de la forma $1+\cdots+1$ debe pertenecer a F^*. Si el campo es de caracteristica p entonces tenemos que hay por lo menos p elementos en F^* pero además estos son los mismos elementos del campo F_0. Por lo tanto $F_0 \subseteq F^*$. Por otro lado si el campo es de caracteristica 0 tenemos que en F^* deben estar contenidos todos los elementos pertenecientes a la imagen del isomorfismo aplicado de $\mathbb{Z}$ a R. Así que el campo generado por estos elementos que es F_0 debe estar incluido en F^*. Así demostramos que F_0 es el más pequeño y es único. $\square$

Sección 8.1 3. Sea R un Dominio Euclideano. Sea m el mínimo entero en el conjunto de normas de elementos diferentes a cero de R. Pruebe que cualquier elemento diferente a cero de R de norma m es una unidad- Deduzca que un elemento no cero de norma cero (si tal elemento existe) es una unidad.

Demostración. Sea $a \in R$ tal que su norma es m. Entonces podemos utilizar el algoritmo de la división para dividir a 1 por r. Entonces tenemos que existen qyr tales que $1 = qa + r$, y que $N(r)$ (N(r) es la norma de r) debe ser menor a $N(a) = m$. Pero como m es la minima norma de un elemento no cero, la única posibilidad es que $r = 0$ por lo cual $1 = qa$ y por lo tanto a es una unidad. Claramente si tengo un elemento no cero con norma 0, esta es la mínima norma que puede tener y por lo demostrado anteriormente sería una unidad. $\square$

Sección 8.1 10. Pruebe que el anillo cociente $\mathbb{Z}[i]/I$ es finito para cualquier ideal no cero I de $\mathbb{Z}[i]$.

Demostración. En el libro mencionan que el anillo $\mathbb{Z}[i]$ tiene una norma tal que $N(a+bi) = a^2 + b^2$, y hay una división euclideana de tal manera que este es un dominio euclideano. Entonces es un dominio de ideales principales por lo que cualquier ideal lo podemos expresar como (α) con $\alpha \in \mathbb{Z}[i]$. Sea $N(\alpha) = n$. Ahora tomemos una clase lateral $\beta + I$. Por el algoritmo de la división tenemos que existen elementos $d, r \in \mathbb{Z}[i]$ tales que $\beta = d\alpha + r$ y $N(r) < n$.

Vemos que $\beta - r = d\alpha$ por lo que $\beta + I = r + I$. Pero por otra parte podemos demostrar que la cantidad de elementos en $\mathbb{Z}[i]$ con norma menor a n son finitos. Esto se puede ver porque el número de elementos tiene una cota superior que son $2n$. Por lo tanto el anillo conciente es finito. $\square$

Sección 8.1 11. Sea R un anillo conmutativo co 1 sea a y b elementos diferentes a cero de R. Un mínimo común múltiplo de a y b es un elemento e de R tal que

(i) $a|e$ y $b|e$, y

(ii) si $a|e'$ y $b|e'$ entonces $e|e'$.

(a) Pruebe que un mínimo común múltiplo de a y b (si existe) es un generador para el único ideal principal más grande contenido en $(a) \cap (b)$.

Demostración. Primero probemos que $m = [a, b]$ es tal que $(m) \in (a) \cap (b)$. Tómese cualquier elemento $x = rm \in (m)$ con $r \in R$. Entonces por las condiciones anteriores sabemos que $m = ka$ por lo que $x = rm = rka$ por lo que pertenece a (a). Igualmente $m = jb$ por lo que $x = rm = rjb$ también pertenece a (b). Luego pertenece a $(a) \cap (b)$. Ahora para probar que es el más grande tómese cualquier otro ideal (m') contenido en $(a) \cap (b)$. Esto quiere decir que $a|m'$ y $b|m'$ porque en particular $m \in (a) \cap (b)$, luego existen $r, r' \in R$ tales que $m' = ra$ y $m' = r'b$. Pero por la segunda propiedad, tenemos que $mk = m'$. Lo que quiere decir que $(m') \subseteq (m)$. Luego vemos que (m) es el más grande además el único ideal principal contenido en $(a) \cap (b)$. □

(b) Deduzca que cualesquiera dos elementos diferentes de cero en un dominio euclideano tiene un mínimo común múltiplo que es único módulo la multiplicación por una unidad.

Demostración. Si tomamos a, b elementos diferentes de 0. Entonces habría que demostrar por una parte que el mínimo común multiplo existe. Este es el caso porque existe $m \in R$ tal que $(m) = (a) \cup (b)$ porque estamos sobre un dominio de ideales principales. Entonces por el punto anterior m es un generador del ideal principal más grande en $(a) \cup (b)$, que es él mismo, luego es un mínimo común múltiplo de a y b.

Además si tomamos m y m' tales que sean mínimos comunes divisores entonces ambos pueden verse como generadores del ideal principal más grande contenido en $(a) \cap (b)$. Por el punto anterior tendriamos que $(m) = (m')$. Por ultimo, por un punto demostrado en la tarea anterior tenemos que $m = um'$ donde u es una unidad del anillo. □

(c) Pruebe que en un dominio euclideano el mínimo común múltiplo de a y b es $\frac{ab}{(a,b)}$, donde (a, b) es el máximo común divisor de a y b.

Demostración. Sabemos que $(a) + (b)$ en un dominio euclideano es igual al ideal generado por (a, b). Además sabemos por el punto anterior que $(a) \cap (b)$ es el ideal generado por $[a, b]$.

Se puede probar que $(a)(b) = (ab)$. Tómese un elemento $rab \in (ab)$, aútomaticamente pertenece a $(a)(b)$ como la suma finita de un solo elemento de la forma rab. Por otro lado tome un elemento $x \in (a)(b)$. Luego $x = \sum_{i=1}^{n} a_i b_i$, con $a_i \in (a)$ y $b_i \in (b)$. Luego $x = \sum_{i=1}^{n} r_i a r'_i b = \sum_{i=1}^{n} r_i r'_i ab = \sum_{i=1}^{n} (r_i r'_i) ab$ y por lo tanto pertenecen a (ab).

Ahora podemos probar que en un dominio euclideano $(ab) = ((a,b)[a,b])$. Tenemos que existen j y k tales que $(a,b)j = a$ y $(a,b)k = b$.

Un elemento d en $((a,b)[a,b])$ es de la forma $r(ax+by)c$ con $r, x, y \in R$ y $c \in (a) \cap (b)$, luego $r(ax+by)c = rxac + rycb$ Vemos que esta es una suma finita de elementos de la forma $a'b'$ con $a' = rxa$ o $a' = ryc$ y $b' = c$ o $b' = b$. Luego $d \in (ab)$.

Por otra parte tómese cualquier elemento $rab \in (ab)$. Por un lado tenemos que $a = k(a,b)$. Y por el otro que $b = j(a,b)$. Luego $rab = rk(a,b)b = raj(a,b)$. Vemos que $kb = ja$, es decir que pertenece a $(a) \cap (b)$. Por lo tanto $rab = rc(a,b)$ donde $c \in (a \cap b)$. Por lo tanto $rab \in ((a,b)[a,b])$. $\square$

Sección 8.1 12. Sea N un entero positivo. Sea M un entero primo relativo a N y sea d un entero primo relativo a $\varphi(N)$, donde φ denota la función φ de Euler. Pruebe que si $M_1 = M^d (\text{mod } N)$entonces $M = M_1^d (\text{mod } N)$ donde d' es el inverso de d mod $\varphi(N) : dd' \equiv 1 \pmod{\varphi(N)}$.

Demostración. Para probar esto utilizamos el teorema de Euler Fermat. Si $(a, m) = 1$ entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Entonces, partiendo de la expresión $M_1 \equiv M^d \pmod{N}$ elevamos a ambos lados por d'. $M_1^{d'} \equiv (M^d)^{d'} \equiv M^{dd'} \pmod{N}$. Pero sabemos que $dd' \equiv 1 \pmod{\varphi(N)}$, por lo que $dd' = k\varphi(N) + 1$. Por lo tanto, $M_1^{d'} \equiv M^{dd'} \equiv M^{k\varphi(N)+1} \equiv (M^{\varphi(N)})^k M \equiv (1)^k M \equiv M (\text{mod } N)$.

$\square$