UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

DEPARTAMENTO
DE MATEMÁTICA

Profesor: Pedro Montero
Ayudante: Sebastián Fuentes

Pauta Ayudantía 5 Estructuras Algebraicas

21 de abril de 2023

Durante todo el curso A denotará un anillo conmutativo con unidad.

Problema 1. Sea G un grupo finito y $H \trianglelefteq G$ un subgrupo normal. Probar que G admite una serie de composición

$$G =: G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = \{e\}$$

tal que $H = G_i$ para cierto $i \in \{0, \ldots, r\}$.
Indicación: Probar que si $K \trianglelefteq L \trianglelefteq G/H$, entonces $\pi^{-1}(L)/\pi^{-1}(K) \cong L/K$, donde $\pi : G \to G/H$ es la proyección al cociente. Para esto último, determinar el kernel de la composición $\pi^{-1}(L) \to L \to L/K$.

Demostración. Sean $K \trianglelefteq L \trianglelefteq G/H$ y consideremos las proyecciones canónicas $\pi : \pi^{-1}(L) \twoheadrightarrow L, \widetilde{\pi} : L \twoheadrightarrow L/K$. Calculamos el kernel de esta composición como sigue:

$$\begin{aligned}
\ker(\widetilde{\pi} \circ \pi) &= \{x \in \pi^{-1}(L) | \widetilde{\pi}(\pi(x)) = K\} \\
&= \{x \in \pi^{-1}(L) | \pi(x)K = K\} \\
&= \{x \in \pi^{-1}(L) | \pi(x) \in K\} \\
&= \pi^{-1}(K)
\end{aligned}$$

El teorema del isomorfismo de Noether nos entrega entonces un isomorfismo $\pi^{-1}(L)/\pi^{-1}(K) \cong L/K$.
Consideremos ahora G grupo finito y $H \trianglelefteq G$ subgrupo normal. El teorema de Jordan Hölder asegura entonces la existencia de series de composición para H y para G/H pues ambos son grupos finitos. Denotaremos estas series de la siguiente manera:

$$\{e\} \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_m \trianglelefteq H, \qquad \{e\} \trianglelefteq L_1 \trianglelefteq \ldots \trianglelefteq L_n \trianglelefteq G/H$$

Tomando preimagen mediante la proyección canónica $\pi : G \twoheadrightarrow G/H$ de la serie de composición de G/H obtenemos una serie de subgrupos normales en G que contienen a H (imagen inversa de subgrupos normales es normal):

$$H \trianglelefteq \pi^{-1}(L_1) \trianglelefteq \ldots \trianglelefteq \pi^{-1}(L_n) \trianglelefteq G$$

Podemos entonces conectar las dos series para obtener:

$$\{e\} \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_m \trianglelefteq H \trianglelefteq \pi^{-1}(L_1) \trianglelefteq \ldots \trianglelefteq \pi^{-1}(L_n) \trianglelefteq G$$

y únicamente restará verificar que los cocientes sucesivos son grupos simples. Para los factores H_i sabemos que esto es cierto pues son una serie de composición de H. Ahora, para $1 \leq i \leq n$ tenemos $\pi^{-1}(L_{i+1})/\pi^{-1}(L_i) \cong L_{i+1}/L_i$ y los cocientes de la derecha son simples pues corresponden a los términos de una serie de composición de G/H. $\square$

Problema 2. Sea A dominio de integridad, $\mathrm{Fr}(A)$ su cuerpo de fracciones y $\iota_A : A \hookrightarrow \mathrm{Fr}(A), a \mapsto \frac{a}{1}$ el morfismo de inclusión asociado. Demuestre que $\mathrm{Fr}(A)$ satisface la siguiente propiedad universal: *Para todo cuerpo K y todo morfismo de anillos $\varphi : A \hookrightarrow K$ inyectivo existe un único morfismo de anillos $\varphi : \mathrm{Fr}(A) \to K$ tal que el siguiente diagrama es conmutativo:*

$$\begin{tikzcd}
A \arrow[rr, hook, "\varphi"] \arrow[dr, hook, "\iota"'] & & K \\
& \mathrm{Fr}(A) \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}$$

Demostración. Suponer que existe el morfismo $\overline{\varphi}$ con la propiedad del enunciado y sea $\frac{a}{b} \in \mathrm{Fr}(A)$. Tenemos entonces que $\overline{\varphi}(\frac{a}{1}) = \overline{\varphi}(\iota_A(a)) = \varphi(a)$, y similar $\overline{\varphi}(\frac{b}{1}) = \varphi(b)$. Entonces tendríamos que:

$$\varphi(a) = \overline{\varphi}\left(\frac{a}{1}\right) = \overline{\varphi}\left(\frac{a}{b}\right)\overline{\varphi}\left(\frac{b}{1}\right) = \overline{\varphi}\left(\frac{a}{b}\right)\varphi(b)$$

Por tanto, la única manera de definir $\overline{\varphi}$ sería mediante:

$$\overline{\varphi}\left(\frac{a}{b}\right) = \varphi(a)\varphi(b)^{-1} \qquad \forall a, b \in A, b \neq 0$$

Notar en primer lugar que la definición anterior tiene sentido pues si $b \neq 0$, como φ es inyectivo entonces $\varphi(b) \in K \setminus \{0\}$ y dado que K es cuerpo este elemento posee inverso. Restaría ver simplemente si la definición de φ es independiente de la fracción equivalente escogida, y que $\overline{\varphi}$ es morfismo de anillos. Para ello vemos que si $\frac{a}{b} = \frac{a'}{b'}$, es decir, $ab' = a'b$, entonces tenemos:

$$\begin{aligned}
\overline{\varphi}\left(\frac{a}{b}\right) &= \varphi(a)\varphi(a'b)\varphi(ab')^{-1}\varphi(b)^{-1} \\
&= \varphi(a)\varphi(a')\varphi(b)\varphi(a)^{-1}\varphi(b')^{-1}\varphi(b)^{-1} \\
&= [\varphi(a)\varphi(a)^{-1}]\varphi(a')[\varphi(b)\varphi(b)^{-1}]\varphi(b')^{-1} \\
&= \varphi(a')\varphi(b')^{-1} = \overline{\varphi}\left(\frac{a'}{b'}\right)
\end{aligned}$$

Para probar que $\overline{\varphi}$ consideremos $\frac{a}{b}, \frac{c}{d} \in \mathrm{Fr}(A)$. Vemos entonces que:

$$\begin{aligned}
\overline{\varphi}\left(\frac{a}{b} + \frac{c}{d}\right) &= \overline{\varphi}\left(\frac{ad + bc}{bd}\right) \\
&= \varphi(ad + bc)\varphi(bd)^{-1} \\
&= \varphi(ad)\varphi(bd)^{-1} + \varphi(bc)\varphi(bd)^{-1} \\
&= \overline{\varphi}\left(\frac{ad}{bd}\right) + \overline{\varphi}\left(\frac{bc}{bd}\right) \\
&= \overline{\varphi}\left(\frac{a}{b}\right) + \overline{\varphi}\left(\frac{c}{d}\right)
\end{aligned}$$

Para el producto la demostración es similar (ejercicio). $\square$

Problema 3. Sea A anillo. Demuestre el Teorema del binomio:

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad \forall a, b \in A, \forall n \in \mathbb{N}$$

Indicación: Muestre primero la relación $\binom{n}{k+1} + \binom{n}{k} = \binom{n+1}{k+1}$

Demostración. Note en primer lugar que

$$\begin{aligned}
\binom{n}{k+1} + \binom{n}{k} &= \frac{n!}{(k+1)!(n-(k+1))!} + \frac{n!}{k!(n-k)!} \\
&= \frac{n!(n-k)}{(k+1)!(n-k)!} + \frac{n!(k+1)}{(k+1)!(n-k)!} \\
&= \frac{(n+1)!}{(k+1)!((n+1)-(k+1))!} \\
&= \binom{n+1}{k+1}
\end{aligned}$$

Demostramos ahora el resultado. Sean $a, b \in A$. Para $n = 0$ es trivial que $(a+b)^0 = 1$. Por inducción suponemos verdadero para n y calculamos como sigue:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\left[\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}\right] \\
&= \left[\sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k}\right] + \left[\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k+1}\right] \\
&= a^{n+1} + \left[\sum_{k=0}^{n-1}\binom{n}{k}a^{k+1}b^{n-k}\right] + b^{n+1} + \left[\sum_{k=1}^{n}\binom{n}{k}a^k b^{n-k+1}\right] \\
&= a^{n+1} + \left[\sum_{k=1}^{n}\left(\binom{n}{k-1} + \binom{n}{k}\right)a^k b^{(n+1)-k}\right] + b^{n+1} \\
&= \binom{n+1}{n+1}a^{n+1}b^{(n+1)-(n+1)} + \left[\sum_{k=1}^{n}\binom{n+1}{k}a^k b^{(n+1)-k}\right] + \binom{n+1}{0}a^0 b^{(n+1)-0} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{(n+1)-k}
\end{aligned}$$

□

Problema 4. Sea A un anillo y $A[X]$ su anillo de polinomios. Sea $P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in A[X]$

1. Muestre que P es nilpotente $\Leftrightarrow a_0, a_1, \ldots, a_n$ son nilpotentes.
2. Pruebe que P es una unidad en $A[X] \Leftrightarrow a_0$ es una unidad en A y $a_1, \ldots, a_n$ son nilpotentes.
   Indicación: Demuestre en primer lugar que si $x \in A$ es nilpotente entonces $1 + x \in A^\times$.
3. Demuestre que P es un divisor de cero $\Leftrightarrow$ existe $a \neq 0$ en A tal que $aP = 0$.

Demostración.

1. ($\Leftarrow$) Notar que si $a \in A$ es nilpotente, entonces aX^n es nilpotente en $A[X]$. Además, el Teorema del binomio nos permite probar de manera directa que la suma de elementos nilpotentes es nilpotente, por lo que si $P \in A[X]$ posee coeficientes nilpotentes entonces será nilpotente en $A[X]$.
   ($\Rightarrow$) Sea $P \in A[X]$ nilpotente. Sea $n = \deg(P)$ y probemos por inducción. El caso $n = 0$ es trivial. Suponemos entonces que el resultado es cierto para polinomios de grado menor a n. Si $P(X)^k = 0$ entonces es claro que $a_n^k = 0$, ie, el coeficiente principal es nilpotente. Ahora, el polinomio $P(X) - a_nX^n$ es de grado menor a n y la hipótesis de inducción permite concluir.

2. Mostremos primero la indicación. Si $x^n = 0$ entonces vemos que

   $$(1+x)(1 - x + x^2 - \ldots + (-1)^{n-1}x^{n-1}) = 1$$

   así que $1 + x \in A^\times$. Ahora, si $a \in A^\times$ y x nilpotente entonces $a^{-1}x$ es nilpotente, de manera que $1 + a^{-1}x$ es una unidad de A y luego $a + x$ también.
   ($\Rightarrow$) Si P es una unidad entonces existe $Q \in A[X]$ tal que $PQ = 1$. Escribiendo $Q(X) = b_mX^m + b_{m-1}X^{m-1} + \ldots + b_1X + b_0$ vemos entonces que $PQ = a_0b_0 = 1$, es decir, $a_0 \in A^\times$. Para demostrar que los otros coeficientes son nilpotentes usaremos inducción en el grado de P. Suponer entonces que esto es cierto para polinomios de grado menor a n. Notemos entonces que la multiplicación de polinomios resulta en

   $$P(X)Q(X) = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_ib_j\right)X^k = 1$$

Probaremos por inducción también que

$$a_n^{t+1} b_{m-t} = 0 \qquad \forall 0 \le t \le m$$

Si $t = 0$ entonces simplemente tenemos la relación $a_n b_m = 0$. Ahora, suponer que para cierto t tenemos que si $0 \le s < t \le m$ entonces se cumple $a_n^{s+1} b_{m-s} = 0$. Multiplicando el coeficiente de X^{n+m-t} por a_n^t tenemos:

$$\sum_{i+j=n+m-t} a_i a_n^t b_j = 0$$

Si $j > m - t$ entonces por hipótesis de inducción $a_n^t b_j = 0$. Por otro lado, si $j < m - t$ entonces $i > n$, lo cual no tiene sentido en este caso. Únicamente nos queda entonces el coeficiente $a_n^{t+1} b_{m-t} = 0$ lo que prueba la primera parte. Teniendo esto entonces resta notar que tomando $t = m$ tenemos $a_n^{m+1} b_0 = 0$, pero $b_0 \in A^\times$ así que $a_n^{m+1} = 0$, ie, a_n es nilpotente. Considerando ahora el polinomio $P(X) - a_n X^n$, como este tiene grado $n - 1$, la hipótesis de inducción concluye la demostración.
($\Leftarrow$) Suponer que a_0 es una unidad y que $a_1, \ldots, a_n$ son nilpotentes. Gracias al punto anterior, P es la suma de una unidad y de un polinomio nilpotente, y por lo tanto es una unidad en $A[X]$.

3. Si P es divisor de cero, sea $Q \in A[X]$ de grado minimal tal que $PQ = 0$. Si Q no es de grado 0, el producto de los coeficientes principales es 0 y por lo tanto $a_n Q$ es un polinomio de grado estrictamente menor al de Q y $a_n PQ = 0$, lo que contradice la minimalidad. Necesariamente entonces $\deg(Q) = 0$. El recíproco es evidente.

□

Problema 5. Un anillo A (no necesariamente conmutativo) es Booleano si $x^2 = x$ para todo $x \in A$. En un anillo Booleano A, demuestre que

1. Muestre que todo anillo Booleano es conmutativo.
2. $2x = 0$ para todo $x \in A$.
3. Todo ideal primo $\mathfrak{p}$ es maximal, y $A/\mathfrak{p}$ es un cuerpo con dos elementos.
4. Todo ideal finitamente generado en A es principal.

Demostración.

1. Notar primero que

$$-x = (-x)^2 = x^2 = x$$

Entonces para $x, y \in A$ tendremos

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y \quad \Rightarrow \quad xy = -yx$$

y juntando lo anterior $xy = -yx = yx$.

2. Basta con calcular que:

$$x + x = (x + x)^2 = x^2 + 2x^2 + x^2 = x + x + 2x \quad \Rightarrow \quad 2x = 0$$

3. Sea $\mathfrak{p} \subseteq A$ ideal primo. Entonces $A/\mathfrak{p}$ es un dominio, y dado $x + \mathfrak{p} \in A/\mathfrak{p}$ tendremos que $[x]^2 = [x]$ así que $[x]([x] - [1]) = 0$ y por lo tanto tendremos $[x] = 0$ o bien $[x] = [1]$. De esta manera vemos que $A/\mathfrak{p}$ tiene dos elementos y el elemento no nulo es invertible, es decir, $A/\mathfrak{p}$ es cuerpo y en consecuencia $\mathfrak{p}$ es maximal.

4. Para esta propiedad procedemos por inducción en el número de generadores, y entonces basta probar para $n = 2$. Si $x, y \in A$ probemos que $\langle x, y\rangle = \langle x + y + xy\rangle$. En efecto, es directo que $\langle x, y\rangle \supseteq \langle x + y + xy\rangle$, y por otro lado

$$x(x + y + xy) = x^2 + xy + x^2y = x + 2xy = x, \quad (x + y + xy)y = xy + y^2 + xy^2 = y + 2xy = y$$

de donde se obtiene la conclusión.

□

Problema 6. Sea A un dominio entero. Decimos que A es un dominio euclideano [2] si existe una función (euclideana) $\varphi : A\backslash\{0\} \to \mathbb{N}$ tal que para todos $a, b \in A$ con $b \neq 0$ existe una escritura (no necesariamente única)

$$a = bq + r \text{ donde } r = 0, \text{ o bien } r \neq 0 \text{ y } \varphi(r) < \varphi(b).$$

Probar que un dominio euclideano es un dominio de ideales principales.

Demostración. Sea $I \subseteq A$ un ideal de A. Dado que $\mathbb{N}$ es un conjunto bien ordenado, $\varphi(I)$ posee un mínimo. Sea $\varphi(x)$ dicho mínimo. Tomemos $a \in I$. Dado que A es un dominio euclídeo, existen $q, r \in A$ de tal suerte que $a = xq + r$ con $r = 0$ o bien $r \neq 0$ y $\varphi(r) < \varphi(x)$. Notemos que como I es ideal, entonces $xq \in I$ y $a \in I$, y luego $r = a - xq \in I$ ya que los ideales son cerrados bajo la suma. No obstante, como $\varphi(x)$ es minimal en $\varphi(I)$, no puede ocurrir que $\varphi(r) < \varphi(x)$ y $r \neq 0$, por lo cual $r = 0$ y por lo tanto $a = xq$. Se sigue que $I = \langle x\rangle$. □