Grupos y Anillos. Grado en Matemáticas. 2012-13. Examen de julio.
Solución de los problemas

1. **Sea A un anillo. Denotamos por $A[[X]]$ al conjunto de las series en una variable con coeficientes en A, es decir fijamos un símbolo X (indeterminada) y los elementos de $A[[X]]$ son expresiones de la forma**

$$\sum_{i\geq 0} a_i X^i = a_0 + a_1 X + a_2 X^2 + \dots$$

con $a_0, a_1, a_2, \dots \in A$. Definimos en $A[[X]]$ la multiplicación imitando las operaciones de polinomios:

$$\begin{aligned} \sum_{i\geq 0} a_i X^i + \sum_{i\geq 0} b_i X^i &= \sum_{i\geq 0} (a_i + b_i) X^i \\ \left(\sum_{i\geq 0} a_i X^i\right)\left(\sum_{i\geq 0} b_i X^i\right) &= \sum_{i\geq 0} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) X^i. \end{aligned}$$

(Piense los elementos de $A[[X]]$ como polinomios que pueden tener infinitos coeficientes no nulos.) Demostrar las siguientes afirmaciones:

a) **$A[[X]]$ es un anillo.**
Sean $a = \sum_{i\geq 0} a_i X^i$ y $b = \sum_{i\geq 0} b_i X^i$ con cada $a_i, b_i \in A$. Entonces $a_i + b_i, \sum_{j=0}^{i} a_j b_{i-j} \in A$ para todo i y por tanto

$$a + b = \sum_{i\geq 0} (a_i + b_i) X^i \in A$$

y

$$ab = \sum_{i\geq 0} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) X^i \in A.$$

Se comprueban de forma rutinaria todas las propiedades de anillo. La más engorrosa es la asociativa del producto:

$$\begin{aligned} (ab)c &= \left(\sum_{n\geq 0} \left(\sum_{m=0}^{i} a_m b_{n-m}\right) X^n\right) c = \sum_{i\geq 0} \left(\sum_{n=0}^{i} \left(\sum_{m=0}^{n} a_m b_{n-m}\right) c_{i-n}\right) X^i \\ &= \sum_{i\geq 0} \left(\sum_{m=0}^{i} a_m \left(\sum_{n=m}^{i} b_{n-m} c_{i-n}\right)\right) X^i = \sum_{i\geq 0} \left(\sum_{m=0}^{i} a_m \left(\sum_{k=0}^{i-m} b_k c_{i-m-k}\right)\right) X^i \\ &= a\left(\sum_{n\geq 0} \left(\sum_{k=0}^{n} b_k c_{n-k}\right) X^n\right) = a(bc). \end{aligned}$$

Está claro que los polinomios 0 y 1 hacen de neutro de la suma y el producto y que $-\sum_{i\geq 0} a_i X^i = \sum_{i\geq 0} (-a_i) X^i$.

b) **Un elemento $a = \sum_{i\geq 0} a_i X^i$ de $A[[X]]$ es invertible en $A[[X]]$ si y sólo si a_0 es invertible en A. Calcula el inverso de $X - 2$ en $\mathbb{Q}[[X]]$.**
Sea $a = \sum_{i\geq 0} a_i X^i$. Si a es invertible y $b = \sum_{i\geq 0} b_i X^i$ es su inverso, entonces $a_0 b_0 = 1$ y por tanto a_0 es invertible. Recíprocamente, supongamos que a_0 es invertible y busquemos un posible inverso $b = \sum_{i\geq 0} b_i X^i$ de a. Entonces se tendrían que verificar

las siguientes igualdades:

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ &\dots \\ a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 &= 0 \end{aligned} \tag{1}$$

Por tanto

$$\begin{aligned} b_0 &= a_0^{-1} \\ b_1 &= -a_0^{-1}a_1b_0 \\ b_2 &= -a_0^{-1}(a_1b_1 + a_2b_0) \\ \dots & \\ b_n &= -a_0^{-1}(a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0). \end{aligned}$$

Esto sólo sirve para hacernos una idea de como podríamos construir el inverso. Más rigurosamente ponemos $b = \sum_{n\geq 0} b_nX^n$ donde definimos los coeficientes con la siguiente regla recursiva:

$$b_0 = a_0^{-1}, \quad b_n = -a_0^{-1}(a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0) \quad (n > 0).$$

Obsérvese que cada b_n con $n > 0$ se define en términos de los anteriores. Ahora comprobamos que $ab = 1$. Eso equivale a comprobar las igualdades de (1) lo cual es fácil pues claramente $a_0b_0 = 1$ y

$$\begin{aligned} a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 &= \\ a_0(-a_0^{-1}(a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0)) + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 &= 0. \end{aligned}$$

c) **Si K es un cuerpo entonces todos los ideales de $K[[X]]$ son principales y los no nulos están generados por una potencia de X.**
Sea I un ideal no nulo de $K[[X]]$ y sea n el menor entero no negativo para el que I contiene un elemento de la forma $a = \sum_{i\geq n} a_iX^i$ con $a_n \neq 0$. Sea $b = \sum_{i\geq n} a_iX^{n-i} = \sum_{i\geq 0} a_{i+n}X^i$. Entonces $a = X^n(\sum_{i\geq n} a_iX^{n-i})$ y, por el apartado b), b es invertible en $K[[X]]$. Por tanto, $X^n \in I$. En particular $(X^n) \subseteq I$. Sea $c = \sum_{i\geq 0} c_iX^i$ un elemento no nulo de I. Por la minimalidad de n tenemos $c_0 = c_1 = \cdots = c_{n-1} = 0$ y por tanto $c = X^n \sum_{i\geq n} c_iX^{n-i} \in (X^n)$. Luego $I = (X^n)$.

d) **Describir los elementos irreducibles y las factorizaciones de $K[[X]]$, para K un cuerpo.**
Es fácil ver que $K[[X]]$ es un dominio. En efecto, sean $a = \sum_{i\geq 0} a_iX^i$ y $b = \sum_{i\geq 0} b_iX^i$ son dos elementos no nulos de $K[[X]]$. Sean n y m los menores enteros tales que $a_n \neq 0$ y $b_m \neq 0$. Entonces el coeficiente de X^{n+m} de ab es $a_nb_m \neq 0$. Luego $ab \neq 0$. Por el apartado c), $K[[X]]$ es un DIP y por tanto los irreducibles son los generadores de ideales maximales. Como $(X) \supseteq (X^2) \supseteq (X^3) \supseteq \dots$ y, por el apartado b), estos son los únicos ideales no nulos, el único ideal maximal es (X). Por tanto los irreducibles son los elementos de la forma Xa con a invertible. Por el apartado b), $a_0 \neq 0$ y por tanto los irreducibles de $K[[X]]$ son los elementos de la forma $\sum_{i\geq 0} a_iX^n$ con $a_0 = 0$ y $a_1 \neq 0$.
Las factorizaciones en $K[[X]]$ serán de la forma aX^n con $a = \sum_{i\geq 0} a_iX^i$ y $a_i \neq 0$.
Observa que este problema se parece mucho al número 2 del examen de junio de 2013.

2. **Sea A_4 el grupo alternado en 4 símbolos y sean $a, b \in A_4 \setminus \{1\}$. Supongamos que a es 3-ciclo y b no.**

a) **Describir el tipo de b.**
Los elementos de A_4 son de tipos $[1]$, $[3]$ y $[2,2]$. Como los dos primeros se han excluido para b, tendremos que b tiene tipo $[2,2]$, es decir es un producto de trasposiciones disjuntas.

b) **Demostrar que $A_4 = \langle a, b\rangle$.**
Reordenando los números $\{1,2,3,4\}$ podemos suponer que $a = (1,2,3)$ y $b = (1,2)(3,4)$. Entonces $aba^{-1} = (2,3)(1,4)$ y $baba^{-1} = (1,3)(2,4)$. Eso implica que $\langle a, b\rangle$ contiene al subgrupo $\langle b, aba^{-1}\rangle = \{1, (1,2)(3,4), (2,3)(1,4), (1,3)(2,4)\}$. Por tanto el orden de $\langle a, b\rangle$ es múltiplo de 3 y de 4 (Teorema de Lagrange). Deducimos que $\langle a, b\rangle$ es múltiplo de 12 y como $|A_4| = 12$ deducimos que $A_4 = \langle a, b\rangle$. Otra alternativa para resolver el problema es ir obteniendo elementos de $\langle a, b\rangle$, a base de multiplicar con a y b, hasta obtener 7 distintos.

c) **Para cada divisor d de 12, calcular el número de subgrupos de A_4 de orden d.**
Todos los subgrupos de orden 1, 2 y 3 han de ser cíclicos. El único de orden 1 es el trivial. Los de orden 2 estarán generados por los productos de dos transposiciones disjuntas y tenemos 3, $\langle(1,2)(3,4)\rangle, \langle(1,3)(2,4)\rangle$ y $\langle(1,4)(2,3)\rangle$. Los de orden 3 estarán generados por 3- ciclos y cada uno de ellos tiene dos generadores, un 3-ciclo y su inverso. Por tanto, el número de subgrupos de orden 3 es la mitad del número de 3-ciclos. Como el número de 3-ciclos es 8, en número de subgrupos de orden 3 es 4. Vamos con los no cíclicos. Obviamente sólo hay un subgrupo de orden 12: A_4. Si H es un grupo de orden 4 no cíclico, estará formado por el 1 y tres elementos de orden 2, pero los únicos elementos de orden 2 son $(1,2)(3,4), (1,3)(2,4)$ y $(1,4)(2,3)$. Como estos cuatro elementos realmente forman un subgrupo, concluimos que hay un único subgrupo de orden 4. El único divisor de 12 que falta considerar es 6. Si H es un subgrupo de orden 6 entonces H tiene un elemento de orden 3, o sea un 3-ciclo, y un elemento de orden 2. Por el apartado b), estos dos elementos generan A_4. Por tanto, A_4 no tiene subgrupos de orden 6. La siguiente tabla resume el número de subgrupos de cada orden

Orden	Nº subgrupos
1	1
2	3
3	4
4	1
6	0
12	1

3. **Demostrar que $\delta(a + b\sqrt{2}) = |a^2 - 2b^2|$ $(a, b \in \mathbb{Z})$ define una función euclídea en $\mathbb{Z}[\sqrt{2}]$. Encontrar infinitos elementos invertibles de $\mathbb{Z}[\sqrt{2}]$. ¿Cómo es posible que se verifique la igualdad $(5+\sqrt{2})(2-\sqrt{2}) = (11-7\sqrt{2})(2+\sqrt{2})$ con los cuatro factores irreducibles?**

En primer lugar observamos que $\delta(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2})$. Además, la aplicación $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ es un automorfismo de de anillos $\mathbb{Q}(\sqrt{2})$ y de $\mathbb{Z}[\sqrt{2}]$. Utilizando esto tenemos que $\delta(xy) = \delta(x)\delta(y)$ y por tanto si $x \mid y$ en $\mathbb{Z}[\sqrt{2}]$ entonces $\delta(x) \mid \delta(y)$ en $\mathbb{Z}$ luego $\delta(x) \leq \delta(y)$.

Sean ahora $a = a_1 + a_2\sqrt{2}, b = b_1 + b_2\sqrt{2}$ con $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ y $b \neq 0$. Entonces $\frac{a}{b} = x + y\sqrt{2}$ con x e y números racionales. Sean q_0 y q_1 los enteros más próximos a x e y respectivamente y pongamos $q = q_0 + q_1\sqrt{2}$ y $r = a - bq$. Entonces $|x - q_0|, |y - q_1| \leq \frac{1}{2}$

y

$$\begin{aligned}\delta(r) &= \delta(b)\delta(\frac{r}{b}) = \delta(b)\delta((x-q_0)+(y-q_1)\sqrt{2}) \\ &= \delta(b)|(x-q_0)^2 - 2(y-q_1)^2| \leq \delta(b)\left(\frac{1}{4}+\frac{1}{2}\right) < \delta(b).\end{aligned}$$

Por tanto, δ es una función euclídea de $\mathbb{Z}[\sqrt{2}]$.

Para obtener infinitos elementos invertibles observamos que $x \in \mathbb{Z}[\sqrt{2}]$ es invertible en $\mathbb{Z}[\sqrt{2}$ si y sólo si $\delta(x) = 1$. Por ejemplo, $\delta(1+\sqrt{2}) = 1$ y por tanto $u = 1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$. Como además $|u| > 1$, todas las potencias u^n son distintas.

La única explicación de la igualdad es que los factores de un lado de la igualdad tienes que ser asociados de los del otro lado. Observa que si a y b son asociados entonces $\delta(a) = \delta(b)$. Como $\delta(5+\sqrt{2}) = \delta(11-7\sqrt{2}) = 23$ y $\delta(2-\sqrt{2}) = \delta(2+\sqrt{2}) = 2$, las asociaciones deberán de ser entre $5+\sqrt{2}$ y $11-7\sqrt{2}$ por un lado, y $2-\sqrt{2}$ y $2+\sqrt{2}$, por otro. En efecto,

$$\frac{5+\sqrt{2}}{11-7\sqrt{2}} = \frac{(5+\sqrt{2})(11+7\sqrt{2})}{23} = 3+2\sqrt{2} = \frac{(2+\sqrt{2})^2}{2} = \frac{2+\sqrt{2}}{2-\sqrt{2}}$$

y $3+2\sqrt{2}$ es unidad pues $\delta(3+2\sqrt{2}) = 1$.

4. **Sea $f : G \to H$ un homomorfismo de grupos y sean G_1 y H_1 dos subgrupos normales de G y H, respectivamente, tales que $f(G_1) \subseteq H_1$. Demostrar que existe un único homomorfismo de grupos $\bar{f} : G/G_1 \to H/H_1$ que hace conmutativo el siguiente diagrama, donde las flechas verticales designan las proyecciones canónicas:**

$$\begin{array}{ccc} G & \stackrel{f}{\to} & H \\ \downarrow & & \downarrow \\ G/G_1 & \stackrel{\bar{f}}{\to} & H/H_1 \end{array}$$

Identificar Ker $(\bar{f})$ **e** Im $(\bar{f})$ **en función de** G_1**,** H_1**,** Ker (f) **e** Im (f)**.**

Vamos a denotar con $\pi_G : G \to G/G_1$ y $\pi_H : H \to H/H_1$ a las dos aplicaciones verticales. En primer lugar supongamos que $\bar{f}$ cumpliera la condición exigida. Entonces tendríamos que para todo $g \in G$ se cumpliría

$$\bar{f}(gG_1) = (\bar{f} \circ \pi_G)(g) = (\pi_H \circ f)(g) = f(g)H_1.$$

Por tanto, la única posibilidad para $\bar{f}$ es la que viene dada por esta fórmula, lo que demostraría la unicidad. Para probar la existencia veamos que la función $\bar{f}$ definida así cumple la condición. Lo primero que tenemos que hacer es asegurarnos de que está bien definida. En efecto, si $x, y \in G$ y $xG_1 = yG_1$, entonces $x^{-1}y \in G_1$ y por tanto $f(x)^{-1}f(y) = f(x^{-1}y) \in f(G_1) \subseteq H_1$. Luego $f(x)H_1 = f(y)H_1$. Ahora comprobar que $\bar{f}$ es homomorfismo y hace conmutativo el diagrama es rutinario:

$$\bar{f}((xG_1)(yG_1)) = \bar{f}((xy)G_1) = f(xy) = f(x)f(y) = \bar{f}(xG_1)\bar{f}(yG_1)$$

y

$$(\bar{f} \circ \pi_G)(g) = \bar{f}(gG_1) = f(g)H_1 = (\pi_H \circ f)(g).$$