Grupos y Anillos. Grado en Matemáticas. 2011-12.
Examen de julio. Soluciones de los problemas

1. **Decir cuáles de los siguientes números se pueden escribir como suma de dos cuadrados enteros y para los que la respuesta sea positiva encontrar una expresión en suma de dos cuadrados: 2015 y 9594.**

   Factorizamos ambos números y obtenemos

   $$2015 = 5 \cdot 13 \cdot 31, \quad 9594 = 2 \cdot 3^2 \cdot 13 \cdot 41.$$

   Como $31 \equiv 3 \mod 4$ deducimos que 2015 no es suma de dos cuadrados. Sin embargo $13 \equiv 41 \equiv 1 \mod 4$ y por tanto 9594 sí que es suma de dos cuadrados. Para escribirlo como suma de dos cuadrados primero escribimos los factores primos con exponente impar como suma de dos cuadrados, o sea como norma de elementos de $\mathbb{Z}[i]$:

   $$2 = 1^2 + 1^2 = N(1+i), \quad 13 = 4 + 9 = N(2+3i), \quad 41 = 16 + 25 = (4+5i).$$

   Por tanto

   $$9595 = N(1+i)N(3)N(2+3i)N(4+5i) = N(3(1+i)(2+3i)(4+5i)) = N(-87+45i) = 87^2+45^2.$$

2. **Demostrar que si p es número primo entonces $\mathbb{Z}/p^n\mathbb{Z}$ y $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\}$ son DIPs con un único ideal maximal.**

   En realidad $\mathbb{Z}/p^n\mathbb{Z}$ no es un dominio si $n > 1$, sin embargo sí que es un anillo de ideales principales pues, por el Teorema de la Correspondencia y el hecho de que $\mathbb{Z}$ es un DIP, todos los ideales de $\mathbb{Z}/p^n\mathbb{Z}$ son de la forma $p^i\mathbb{Z}/p^n\mathbb{Z}$ con $i = 0, 1, \ldots, n$. Como estos ideales forman una cadena:

   $$0 = p^n\mathbb{Z}/p^n\mathbb{Z} \subset p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \subset p^{n-2}\mathbb{Z}/p^n\mathbb{Z} \subset \cdots \subset p^2\mathbb{Z}/p^n\mathbb{Z} \subset p\mathbb{Z}/p^n\mathbb{Z} \subset \mathbb{Z}/p^n\mathbb{Z}.$$

   deducimos que $p\mathbb{Z}/p^n\mathbb{Z}$ es el único ideal maximal de $\mathbb{Z}/p\mathbb{Z}$.

   Pongamos $A = \mathbb{Z}_{(p)}$. Este anillo sí que es un dominio pues es un subanillo del cuerpo de los número racionales. Vamos a ver que todos los ideales son de la forma p^nA para algún entero positivo n. Eso demostrará lo que queremos pues todos son principales y como estos ideales forman una cadena

   $$\cdots \subset p^{n+1}A \subset p^nA \subset p^{n-1}A \subset \cdots \subset p^2A \subset pA \subset A.$$

   deducimos que pA es el único ideal maximal.

   En efecto, sea I un ideal propio no nulo de A. Cada elemento no nulo de A lo podemos escribir de forma única como $x = p^n\frac{a}{b}$ con $n \geq 0$ y $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$. En tal caso escribimos $v(x) = n$. Obsérvese que si $v(x) = 0$ entonces $x^{-1} \in A$ y por tanto x es invertible en A. Por tanto $v(x) > 0$ para todo $x \in I \setminus \{0\}$. Sea $x \in I \setminus \{0\}$ tal que $v(x)$ es mínimo. Entonces $x = p^n y$ con y invertible en A. Eso implica que $p^n \in I$ y por tanto podemos suponer que $x = p^n$. Sea y un elemento no nulo arbitrario de I. Entonces $m := v(y) \geq n$ y por tanto $y = p^m z \in p^n\mathbb{Z}$ para algún $z \in A$. Por tanto $I = p^n\mathbb{Z}$, como queríamos.

3. **Sea G un grupo finito y sea H un subgrupo de G. Se llama exponente de G, denotado $\mathbf{Exp}(G)$, al menor entero positivo n tal que $g^n = 1$ para todo $g \in G$. Demostrar**

   ***a*) $\mathbf{Exp}(G)$ es el mínimo común múltiplo de los órdenes de los elementos de G.**

   ***b*) $\mathbf{Exp}(H)$ divide a $\mathbf{Exp}(G)$.**

   ***c*) Si H es normal en G entonces $\mathbf{Exp}(G/H)$ divide a $\mathbf{Exp}(G)$.**

   ***d*) Para todo entero $n \geq 2$,**

   $$\mathbf{Exp}(S_n) = \begin{cases} \mathbf{Exp}(S_{n-1}), & \text{si } n \text{ no es potencia de un primo;} \\ p\mathbf{Exp}(S_{n-1}), & \text{si } n \text{ es potencia de un primo } p. \end{cases}$$

Sea $e = \text{Exp}(G)$.

a) Sea m el mínimo común múltiplo de los órdenes de los elementos de G. Si $g \in G$ entonces $1 = g^e$ y por tanto e es múltiplo del orden de g. Luego e es múltiplo de m. Por otro lado, $g^m = 1$ para todo $g \in G$, con lo que $e \leq m$. De $e \leq m$ y $m|e$ deducimos que $e = m$.

b) De (a) deducimos que $\text{Exp}(H)$ (= mínimo común múltiplo de los órdenes de los elementos de H) divide al mínimo común múltiplo de los órdenes de los elementos de G y éste es $\text{Exp}(G)$.

c) Si $g \in G$ entonces $g^e = 1$ y por tanto $(gH)^e = g^e H = 1$. Luego e es múltiplo de los órdenes de los elementos de G/H, con lo que del apartado (a) deducimos que $\text{Exp}(G/H)$ divide a e.

d) Vamos a ver primero que $\text{Exp}(S_n) = \text{mcm}\{k : k \leq n\}$. En efecto, para cada $k \leq n$, S_n tiene un k-ciclo. Como cada k-ciclo tiene orden k, deducimos que k divide a $\text{Exp}(S_n)$ para todo $k \leq n$ y por tanto $m := \text{mcm}\{k : k \leq n\}$ divide a $\text{Exp}(S_n)$. Por otro lado, el orden de un elemento g de S_n es el mínimo común múltiplo de las componentes de su tipo. Como estas componentes son menores o iguales que n deducimos que $g^m = 1$. En conclusión $m = \text{Exp}(S_n)$.

Por tanto $\text{Exp}(S_n) = \text{mcm}(n, \text{Exp}(S_{n-1}))$. Si n no es potencia de primo entonces $n = n_1 n_2$ con n_1 coprimos y menores que n. Luego $n = \text{mcm}(n_1, n_2)$ divide a $\text{Exp}(S_{n-1})$ y por tanto $\text{Exp}(S_n) = \text{Exp}(S_{n-1})$. Si $n = p^m$ con p primo entonces p^{m-1} divide a $\text{Exp}(S_{n-1})$ pero p^m no divide a ningún $k < n$. Eso implica que $\text{Exp}(S_n) = \text{mcm}(p^m, \text{Exp}(S_{n-1})) = p\text{Exp}(S_{n-1})$.

4. **Sea G un grupo y N un subgrupo normal de G. Decimos que N es normal maximal si $N \neq G$ y los únicos subgrupos normales de G que contienen a N son G y N.**
   - ***a*) Demostrar que N es normal maximal si y sólo si G/N es simple.**
   - ***b*) Dar un ejemplo de un subgrupo normal maximal que no sea subgrupo maximal.**
   - ***c*) Demostrar que si H es un subgrupo de G y N es normal maximal en G que no contiene a H entonces $N \cap H$ es un subgrupo normal maximal de H.**

   a) Que G/N sea simple significa que el conjunto A de los subgrupos normales de G/N tiene exactamente dos elementos (0 y G/N) y que N sea ideal normal maximal de G significa que el conjunto B de los subgrupos normales de G que contienen a N tiene exactamente dos elementos (N y G). Por el Teorema de la Correspondencia para grupos existe una biyección entre A y B y por tanto A y B tienen el mismo cardinal. Por tanto N es normal maximal si y sólo si $|B| = 2$ si y sólo si $|A| = 2$ si y sólo si G/N es simple.

   b) El subgrupo trivial de A_5 es normal maximal, pues A_5 es simple, pero no es subgrupo maximal de A_5.

   c) Como H no está contenido en N, $N \neq NH$. Como N es normal maximal en G también es normal maximal en HN por tanto HN/N es simple. Por el Tercer Teorema de Isomorfía $HN/N \cong H/H \cap N$, con lo cual también $H/H \cap N$ es simple. Deducimos pues que $H \cap N$ es normal maximal en H.

5. **Dar la lista completa de los grupos abelianos de orden 36 salvo isomorfismos.**

   Por el Teorema de Clasificación de los grupos abelianos finitamente generado cada grupo de orden 36 es isomorfo a $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_1} \times \ldots \mathbb{Z}_{d_k}$ con $1 < d_1 | d_2 | \ldots d_k$ y $d_1 d_2 \cdots d_k = 36$. Las únicas listas $(d_1, \ldots, d_k)$ de números con estas propiedades son $(6, 6)$, $(3, 12)$ $(2, 18)$ y (36). Por tanto todo grupo abeliano de orden 36 es isomorfo a uno de los siguientes:

$$\mathbb{Z}_6 \times \mathbb{Z}_6, \quad \mathbb{Z}_3 \times \mathbb{Z}_{12}, \quad \mathbb{Z}_2 \times \mathbb{Z}_{18}, \quad \mathbb{Z}_{36}.$$

   De la parte de unicidad del Teorema se deduce que estos cuatro grupos son no isomorfos dos a dos.