Examen final de Estructuras Algebraicas.

8-II-2013

1. Responder a las siguientes cuestiones.

   a) En el grupo $\mathbb{Z}$ de los enteros, todos los subgrupos son de la forma $m\mathbb{Z}$ para cierto número natural m.

   Sea $S \subset \mathbb{Z}$ un subgrupo no nulo de $(\mathbb{Z}, +)$. Para $x \in S$ se tiene que su opuesto $-x \in S$, por tanto $S \cap \mathbb{N} \neq \emptyset$ y por el principio de la buena ordenación de los naturales, $S \cap \mathbb{N}$ tiene un primer elemento m. Por ser S un subgrupo, deben pertencer a S los elementos $m + m$, $m + m + m, \cdots$; es decir los multiplos de m. También deben estar los inversos de m, $2m$, $3m$; es decir $-m$, $-2m$, $\ldots$. Así pues, están todos los términos de la forma km con $k \in \mathbb{Z}$. Luego $m\mathbb{Z} \subset S$. También se da el contenido contrario: en efecto si $s \in S$ es un elemento cualquiera, sabemos que existen $q, r \in \mathbb{Z}$ tales que $s = mq + r$ con $0 \leq r < m$. Ahora $mq, s \in S \Rightarrow r = s - mq \in S$. Cómo m es el primer elemento positivo de S, se tiene que $r = 0$ y por tanto $s = mq \in m\mathbb{Z}$, y así $S = m\mathbb{Z}$.

   b) Si H_1 y H_2 son subgrupos de $\mathbb{Z}$, dar la forma explícita de $H_1 \cap H_2$ y de $H_1 + H_2$ (de acuerdo con el apartado a)).

   Sean $H_1 = n\mathbb{Z}$ y $H_2 = m\mathbb{Z}$ para ciertos $n, m \in \mathbb{N}$.

   Ahora bien, $H_1 \cap H_2$ es el conjunto de múltiplos de n y de m. Es decir, los números que son múltiplos de $mcm(m, n)$. Así, $H_1 \cap H_2 = mcm(m, n)\mathbb{Z}$

   Por otro lado $H_1 + H_2 = \{jm + kn \mid j, k \in \mathbb{Z}\}$. Gracias a la identidad de Bezout, sabemos que el mínimo de esas sumas (sin ser nula) es el máximo común divisor. Por lo tanto, $H_1 + H_2 = mcd(m, n)\mathbb{Z}$

   c) Si se considera $\mathbb{Z}$ como un anillo, hallar todos los ideales de $\mathbb{Z}$ indicando cuáles son ideales primos y cuáles son ideales maximales.

   Sea $I \subset \mathbb{Z}$ un ideal del anillo $(\mathbb{Z}, +, \cdot)$. En particular I tiene que ser un subgrupo de $\mathbb{Z}$. Por tanto (apartado a)), las únicas posibilidades son $I = m\mathbb{Z}$ para cierto natural m. Veamos que en efecto $m\mathbb{Z}$ es un ideal, para todo $m \in \mathbb{N}$. Sean $k \in \mathbb{Z}$ y $j \in m\mathbb{Z}$: podemos escribir $j = z \cdot m$ para cierto $z \in \mathbb{Z}$. Así, $k \cdot j = k \cdot (z \cdot m) = (k \cdot z) \cdot m$. Cómo $k \cdot z \in \mathbb{Z}$, tenemos que para cualquier m el subgrupo $m\mathbb{Z}$ es un ideal.

   Para ver qué ideales son primos, buscaremos alguna condición sobre m. Si m es primo y tenemos que $k \cdot j$ es múltiplo de m, entonces necesariamente, k ó j son múltiplos de m. Así, si m es un número primo, entonces $m\mathbb{Z}$ es un ideal primo. De manera análoga, si $m = k \cdot j$, obviamente $k, j \notin m\mathbb{Z}$ pero $k \cdot j \in m\mathbb{Z}$. Así $m\mathbb{Z}$ no es un ideal primo si m no es primo.

Basta observar que $n \mid m$ implica que $n\mathbb{Z} \supseteq m\mathbb{Z}$ para notar que los ideales maximales de $\mathbb{Z}$ coinciden con los ideales primos.

d) Estudiar para qué valores de $m \in \mathbb{Z}$ es $\mathbb{Z}_m$ un cuerpo.

Cómo $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$, éste será cupo si y sólo si $m\mathbb{Z}$ es un ideal maximal. Es decir, si m es primo.

2. Sean H, L subgrupos normales de un grupo G, tales que $HL = G$ y $H \cap L = \{0\}$. Probar que $H \times L$ es isomorfo a G. ¿ Es cierta la afirmación en el caso en que solamente uno de ellos sea normal?.

3. a) Dadas las matrices $A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $B := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ de $GL(2, \mathbb{Z})$, probar que $A^4 = 1$, $B^3 = 1$ y AB tiene orden infinito.

   Primero observamos que $C := AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Ahora bien, se puede comprobar que $C^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq 1$ si $n > 0$. Por tanto, C tiene orden infinito.

   b) Sea G un grupo cualquiera. Si dos elementos $a, b \in G$ conmutan y $ord(a) = n$ y $ord(b) = m$, probar que $ord(ab) \mid m.c.m.(n, m)$.

   Basta ver que $(ab)^{m.c.m(n,m)} = 1$. Cómo a, b conmutan podemos escribir que $(ab)^{m.c.m(n,m)} = (ab)^{m.c.m(n,m)} = a^{m.c.m(n,m)} b^{m.c.m(n,m)} = a^{k_1 n} b^{k_2 m} = 1 \cdot 1 = 1$.

   Extraer alguna consecuencia de las dos afirmaciones anteriores.

   El resultado del apartado b) no se puede generalizar si los elementos en cuestión no conmutan.

4. Sea G un grupo.

   a) Definir el centro $Z(G)$ de G.

   b) Obtener $Z(G)$ como conjunto de puntos fijos de una acción de G sobre G. (Definir dicha acción)

   c) Supongamos que G verifica la siguiente condición: "existe un número entero $n \geq 2$ y $a \in G$ de modo que a es el único elemento de orden n". Probar que $a \in Z(G)$ y calcular el valor de n.

5. Describir una lista completa de grupos abelianos de orden 360, no isomorfos dos a dos.

   Descomponemos $360 = 2^3 3^2 5$. Tenemos las siguientes combinaciones:

   - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
   - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
   - $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
   - $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
   - $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

- $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

6. Probar que los 3-ciclos generan el grupo alternado $\mathcal{A}_5$. Probar que $\mathcal{A}_5$ es un subgrupo normal de $\mathcal{S}_5$.

   El grupo $\mathcal{A}_5$ está formado por los elementos de $\mathcal{S}_\bigtriangledown$ que es producto de un número par de trasposiciones. Para ello tenemos que escribir el producto de dos trasposicones cómo producto de 3-ciclos. Tenemos dos casos. Caso 1(un elemento en común): $(1\,2)(2\,3) = (1\,2\,3)$. Caso 2 (dos trasposiciones disjuntas): $(1\,2\,3)(2\,3\,4) = (4\,3)(1\,2)$. Así todo producto par de trasposiciones se puede escribir cómo producto de 3-ciclos.

   ¿ Cuántos homomorfismos hay de $\mathbb{Z}_3$ en $\mathcal{A}_5$? ¿Son todos inyectivos?

   Para esta cuestión debemos tener en cuenta que si $\varphi : G \to H$ es un homomorfismo, entonces $ord(\varphi(g)) \mid ord(g)$ para todo $g \in G$. Los elementos, no nulos, de $\mathbb{Z}_3$ tiene orden 3. Por tanto su imagen debe tener orden 1 o 3. El producto de dos trasposiciones disjuntas tiene orden 2. El orden de un 3-ciclo es 3. El orden del neutro es 1. Así para formar un homomorfismo, la imagen del 1, debe ser un 3-ciclo o la identidad. Contamos por tanto, el número de 3-ciclos. Podemos elegir cualquiera de los 5 elementos para la primera posición, cualquiera de los 4 restantes para la segunda y cualquiera de los 3 restantes para la tercera posición. Así tenemos 60 posibilidades. Ahora bien $(1\,2\,3) = (2\,3\,1) = (3\,1\,2)$. Por tanto debemos dividir por 3, obteniendo 20 homomorfismos no triviales. Debemos contar también el homomorfismo trivial, es decir el que cumple $\varphi(1) = 0$.

   Todos los homomorfismos son inyectivos, excepto el último.

7. ¿Cuántos elementos de orden 7 hay en un grupo **simple** de orden 168 ?

   Primero calculamos el número de subgrupos de Sylow de 7 elementos $S_7(G)$. Por un lado, $S_7(G) \mid 24$. Por otro lado, $S_7(G) \equiv 1(mod\ 7)$. Así $S_7(G) = 1$ ó $S_7(G) = 8$. Al ser G un grupo simple, no tiene subgrupos normales, y por tanto $S_7(G) = 8$. En cada uno de estos subgrupos hay 6 elementos de orden 7 (el séptimo elemento es el neutro). Así, hay 48 elementos de orden 7.

8. Definición de ideal, y de ideal principal. Sea K un cuerpo. ¿Puede K contener ideales no triviales? Probar que todos los ideales del anillo $K[x]$ son principales.

9. Sea $h(x)$ un polinomio mónico con coeficientes enteros, y p un número primo. Si $h(x)$ es irreducible en $\mathbb{Z}_p[x]$, ¿ es también irreducible en $\mathbb{Z}[x]$?.

   Procedemos por reducción al absurdo. Suponemos $p(X) = q(X)r(X)$, con $p(X), q(X), r(X) \in \mathbb{Z}[X]$. Consideramos el cociente $\pi : \mathbb{Z} \to \mathbb{Z}/(p\mathbb{Z})$.Tomamos $p' = \pi(p)$, $q' = \pi(q)$ y $r' = \pi(r)$, tenemos que $p' = q'r'$ y por tanto el polinomio es reducible.

   Probar que el polinomio $x^2 + 1$ es reducible en $\mathbb{Z}_{17}[x]$, pero no es reducible en $\mathbb{Z}[x]$.

   Es fácil ver que $x^2+1 = (x+4)(x-4)$ en $\mathbb{Z}_{17}$. Sin embargo, si tuviera raíces enteras, éstas tendrían que ser ± 1. Pero estos valores no son raíces del polinomio.

10. Sea $A \subset \mathbb{Q}^{2\times 2}$ el subanillo de matrices definido por:

$$A := \{\begin{pmatrix} z & a \\ 0 & z \end{pmatrix},\ \text{con } z \in \mathbb{Z} \text{ y } a \in \mathbb{Q}\}$$

a) Probar que todo ideal primo de A contiene a los elementos de la forma $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$ con $a \in \mathbb{Q}$ y que estos elementos constituyen un ideal J de A.

b) Probar que A/J es isomorfo a $\mathbb{Z}$. Calcular los ideales primos de A.

a) Sea I un ideal primo cualquiera. La matriz nula

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$$

Observamos que cualquier elemento de forma $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$ está en A y cumple:

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$$

Por tanto si I es primo, $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \in I, \forall a \in \mathbb{Q}$.

La demostración de que J es ideal en A es directa. Luego tenemos que todo ideal primo contiene a J

b) Establecemos un homomorfismo f de anillos de A en $\mathbb{Z}$, mediante:

$$f(\begin{pmatrix} z & a \\ z & z \end{pmatrix}) = z$$

Se comprueba directamente que $f(M+N) = f(M)+f(N)$ y $f(M.N) = f(M).f(N)$ para $M, N \in A$ cualesquiera y por tanto es homomorfismo. Además f es sobre, y su núcleo es $\ker f = J$. Por el teorema de isomorfía se tiene que f induce un isomorfismo $\overline{f} : A/J \to \mathbb{Z}$.

Para la segunda pregunta basta observar que f transforma ideales en ideales y da lugar a una biyección entre los ideales primos que contienen a J y los ideales primos de $\mathbb{Z}$. Por tanto los ideales primos de A son los de la forma J_m con m primo, definidos por:

$$J_m = \{\begin{pmatrix} z & a \\ 0 & z \end{pmatrix}, \text{ con } z \in m\mathbb{Z} \text{ y } a \in \mathbb{Q}\}.$$

LOS ALUMNOS QUE SE PRESENTAN A TODO EL CURSO DEBEN HACER LOS EJERCICIOS DEL 1 AL 9.

LOS ALUMNOS QUE LIBERARON LA PARTE DE GRUPOS DEBEN REALIZAR LOS APARTADOS $c), d)$ DEL EJERCICIO 1, Y LOS EJERCICIOS 8,9 Y 10 ENTEROS.

DURACIÓN DEL EXAMEN: 3 HORAS.