Álgebra II
Primer Cuatrimestre — 2007
Primer parcial

1	
2	
3	
4	

Apellido y nombre: ....
Comisión: .... L.U.: .... Páginas: ....

1. *a*) Un grupo de orden 3325 o 6125 es producto directo de sus subgrupos de Sylow.

Solución. En los dos casos es fácil, usando el teorema de Sylow, que para cada primo p que divide al orden, el número de p-subgrupos de Sylow es $n_p = 1$. Esto implica, en particular, que los subgrupos de Sylow son normales. El ejercicio sigue entonces de un resultado visto en la práctica que afirma que un grupo en el que los subgrupos de Sylow son normales es producto directo de ellos.

b) Un grupo de 80 o 520 elementos no es simple.

Solución. Sea G un grupo de orden $80 = 2^4 \cdot 5$. Sean n_2 y n_5 las cantidades de 2- y 5-subgrupos de Sylow. El teorema de Sylow nos dice que $n_5 | 2^4$ y que $n_5 \equiv 1 \pmod{5}$. Calculando, es fácil ver que esto implica que $n_5 \in \{1, 16\}$. Supongamos que $n_5 = 16$. Como dos subgrupos de orden 5 de G se intersecan trivialmente, la union de los 5-subgrupos de Sylow tiene $16 \cdot (5-1) = 64$ elementos. Luego hay a lo sumo $80 - 64 - 1 = 15$ elementos de orden potencia de 2. Como un 2-subgrupo de Sylow tiene 16 elementos, vemos que debe ser $n_2 = 1$. Así, G no es simple.
Sea ahora G un grupo de orden $520 = 2^3 \cdot 5 \cdot 13$. Supongamos que G es simple. El teorema de Sylow implica entonces que $n_{13} = 40$ así que hay en G $40 \cdot (13-1) = 480$ elementos de orden 13. El mismo teorema implica que hay al menos 26 5-subgrupos de Sylow, esto es, al menos $26 \cdot (5-1) = 101$ elementos de orden 5. Como $480 + 101 > 520$, esto es imposible. Luego G no puede ser simple.
(Notemos que hemos probado que o bien tiene un único 5-subgrupo de Sylow P_5 o bien tiene un único 13-subgrupo de Sylow P_{13}. En el primer caso es fácil ver, de la misma forma, que en G/P_5 hay un único 13-subgrupo de Sylow; en el segundo, que en G/P_{13} hay un único 5-subgrupo de Sylow. Vemos así que en cualquier caso G es extensión de p-grupos. Luego G es soluble.)

2. Sea G un grupo finito y H un subgrupo. Supongamos que H es *especial*, esto es, que

> para todo $x \in G \setminus H$ e $y \in G$, existe un único $u \in H$ tal que $y^{-1}xy = u^{-1}xu$.

a) Si $x \in G \setminus H$, entonces $G = \mathsf{C}(x)H$ y $\mathsf{C}(x) \cap H = 1$.

Solución. Sea $y \in G$. Por hipótesis, existe $h \in H$ tal que $y^{-1}xy = u^{-1}xu$, de manera que $xyu^{-1} = yu^{-1}x$, esto es, $yu^{-1} \in \mathsf{C}(x)$. Vemos que entonces $y = (yu^{-1})u \in \mathsf{C}(x)H$.
Si $y \in \mathsf{C}(x) \cap H$, entonces $y^{-1}xy = 1^{-1}x1$ y la hipótesis de unicidad implica inmediatamente que $y = 1$. Esto nos dice que $\mathsf{C}(x) \cap H = 1$. □

b) H es normal.

Solución. Sea $h \in H$ y $y \in G$ y supongamos que, contradiciendo lo que queremos probar, es $x = yhy^{-1} \notin H$. Por hipótesis, entonces, existe $u \in H$ tal que $h = y^{-1}xy = u^{-1}xu$ y, en particular, $x = uhu^{-1} \in H$. Esto es absurdo. □

c) Si $x \in G \setminus H$, entonces el grupo G es isomorfo a un producto semidirecto de $\mathsf{C}(x)$ por H.

Solución. Esto sigue del resultado de la primera parte usando un ejercicio de la práctica. □

d) Si $x \in G \setminus H$, entonces $H = \{u^{-1}xux^{-1} : u \in H\}$. Concluya que Hx es una clase de conjugación de G.

Solución. Consideremos la función $f : u \in H \mapsto u^{-1}xux^{-1} \in H$. Como H es normal, cualquiera sea $u \in H$ es $xux^{-1} \in H$, así que $f(u) = u \cdot xux^{-1} \in H$. Esto nos dice que f está bien definida. Es además inyectiva: si $f(u) = f(v)$, entonces $u^{-1}xu = v^{-1}xv$ y la hipótesis hecha sorbe H implica que $u = v$.
Como H es finito, vemos así que f es biyectiva y, en particular, que $H = \operatorname{im} f$. Esto es precisamente el contenido de la primera afirmación del ejercicio.
Usando esto, es claro que $Hx = \{u^{-1}xu : u \in H\}$, de manera que $Hx \subset \mathsf{cl}(x)$. Si, por otro lado, $y \in \mathsf{cl}(x)$, existe $z \in G$ tal que $y = z^{-1}xz$ y, por hipótesis, existe a su vez $u \in H$ tal que $z^{-1}xz = u^{-1}xu$. Así, $u \in Hx$. Concluímos que $Hx = \mathsf{cl}(x)$, como queríamos. □

e) Muestre que $H = \{[x, y] : x, y \in G\}$.

Solución. Sea $X = \{[x, y] : x, y \in G\}$. En vista del ejercicio anterior, $H \subset X$. Sean $x, y \in H$. Si $x \in H$ o $y \in H$, entonces por esto mismo es $[x, y] \in H$. Si, por el contrario, $x, y \in G \setminus H$, existe $u \in H$ tal que $y^{-1}xy = u^{-1}xu$, así que $[y^{-1}, x] = [u^{-1}, x] \in H$. Así, $X \subset H$. □

f) Si $x \in G \setminus H$, entonces $\mathsf{C}(x)$ es abeliano.

Solución. Sean $x, y \in \mathsf{C}(x)$. Entonces $[x,y] \in H \cap \mathsf{C}(x) = 1$. $\square$

3. Sea A un anillo.

a) Si en el diagrama de A-módulos y morfismos de A-módulos

$$\begin{tikzcd}
& & & & 0 \arrow[d] \\
& & N \arrow[r] \arrow[d] & P \arrow[r] \arrow[d] & Q \arrow[d] \\
& M' \arrow[r] \arrow[d] & N' \arrow[r] \arrow[d] & P' \arrow[r] \arrow[d] & Q' \\
0 \arrow[r] & M'' \arrow[r] \arrow[d] & N'' \arrow[r] \arrow[d] & P'' & \\
& M''' \arrow[r, "f"] \arrow[d] & N''' & & \\
& 0 & & &
\end{tikzcd}$$

las filas y columnas son exactas, entonces el morfismo f es inyectivo.

Solución. Llamemos f a todos los morfismos horizontales del diagrama y g a los verticales, e indiquemos—cuando sea necesario—el dominio con un subíndice. Así, escribimos $f_{M''}$ al morfismo $M'' \to N''$ del diagrama.
Sea $m''' \in M'''$ tal que $f(m''') = 0$. Como $g_{M''}$ es sobreyectivo, existe $m'' \in M''$ tal que $g(m'') = m'''$. Entonces $g(f(m'')) = f(g(m'')) = f(m''') = 0$, así que $f(m'') \in \ker g_{N''} = \operatorname{im} g_{N'}$. Luego existe $n' \in N'$ tal que $g(n') = f(m'')$. Notemos que $g(f(n')) = f(g(n')) = f(f(m'')) = 0$, esto es, que $f(n') \in \ker g_{P'} = \operatorname{im} g_P$, de manera que existe $p \in P$ tal que $g(p) = f(n')$. Es $g(f(p)) = f(g(p)) = f(f(n')) = 0$. Como g_Q es inyectiva, esto nos dice que $f(p) = 0$, esto es, que $p \in \ker f_P = \operatorname{im} f_N$. Si $n \in N$ es tal que $f(n) = p$, entonces $f(g(n) - n') = g(f(n)) - f(n') = g(p) - g(p) = 0$ y vemos que existe $m' \in M'$ tal que $f(m') = g(n) - n'$.
Ahora bien, $f(g(m') - m'') = g(f(m')) - f(m'') = g(g(n) - n') - g(n') = 0$ y, como $f_{M''}$ es inyectiva, concluímos que $g(m') = m''$. Pero entonces $m''' = g(m'') = g(g(m')) = 0$. $\square$

b) Si en el siguiente diagrama conmutativo de A-módulos y morfismos de A-módulos

$$\begin{tikzcd}
0 \arrow[dr] & & & & 0 \\
& M \arrow[dr, "a_1"] & & N \arrow[ur] \arrow[dd, "g"] & \\
& & P \arrow[ur, "b_2"] \arrow[dr, "a_2"'] & & \\
& M' \arrow[uu, "f"] \arrow[ur, "b_1"'] & & N' \arrow[dr] & \\
0 \arrow[ur] & & & & 0
\end{tikzcd}$$

las diagonales son exactas, entonces hay un isomorfismo $\ker g \cong \operatorname{coker} f$.

Solución. Sea $\phi = b_2 a_1 : M \to N$. Es $g\phi = gb_2 a_1 = a_2 a_1 = 0$, así que $\operatorname{im}\phi \subset \ker g$. Recíprocamente, si $n' \in N'$ es tal que $g(n') = 0$, entonces existe $p \in P$ tal que $b_2(p) = n'$ y, como $a_2(p) = g(b_2(p)) = g(n') = 0$, es $p \in \ker a_2 = \operatorname{im} a_1$. Luego existe $m \in M$ tal que $a_1(m) = p$. Pero entonces $\phi(m) = b_1(a_1(m)) = b_1(p) = n$. Concluímos que $\operatorname{im}\phi = \ker g$.
Por otro lado, $\phi f = b_2 a_1 f = b_2 b_1 = 0$, de manera que $\ker f \subset \ker\phi$ y si $m \in \ker\phi$, entonces como $b_2(a_1(m)) = 0$, $a_1(m) \in \ker b_2 = \operatorname{im} b_1$ y existe $m' \in M'$ tal que $b_1(m') = a_1(m)$. Entonces $a_1(f(m') - m) = 0$. Como a_1 es inyectivo, esto nos dice que $m = f(m') \in \operatorname{im} f$. Así, $\ker\phi = \operatorname{im} f$.
El segundo teorema de isomorfismo nos permite concluir entonces que ϕ induce un isomorfismo $\operatorname{coker} f = M/\ker f = M/\ker\phi \to \operatorname{im}\phi = \ker g$. □

4. Sea A un anillo conmutativo nötheriano. Si M es un A-módulo y $\mathfrak{p} \in \operatorname{Spec} A$, decimos que $\mathfrak{p}$ es un *primo asociado a* M si existe $m \in M$ tal que $\operatorname{ann}(m) = \mathfrak{p}$. Escribimos $\operatorname{Ass}_A(M)$ al conjunto de los primos asociados a M.

a) Mostrar que si $\mathfrak{p}$ es un elemento máximal del conjunto de ideales $\{\operatorname{ann}(m) : m \in M \setminus 0\}$, entonces $\mathfrak{p} \in \operatorname{Ass}_A(M)$.

Solución. Sea $\mathfrak{p}$ un elemento maximal de $\{\operatorname{ann}(m) : m \in M \setminus 0\}$. Para ver que $\mathfrak{p} \in \operatorname{Ass}_A(M)$ hay que mostrar que $\mathfrak{p}$ es primo. Supongamos entonces que $a, b \in A$ son tales que $ab \in \mathfrak{p}$. Supongamos que $a \notin \mathfrak{p}$, esto es, que $am \neq 0$. Por contrucción, existe $m \in M \setminus 0$ tal que $\mathfrak{p} = \operatorname{ann}(m)$. Como $\operatorname{ann}(bm) \supset \operatorname{ann}(m)$ y $a \in \operatorname{ann}(bm) \setminus \operatorname{ann}(m)$, la maximalidad de $\mathfrak{p}$ implica que debe ser $bm = 0$, esto es, $b \in \mathfrak{p}$. □

b) $\operatorname{Ass}_A(M) = \emptyset$ sii $M = 0$.

Solución. La suficiencia es evidente. Por otro lado, si $M \neq 0$, entonces el conjunto de ideales $\{\operatorname{ann}(m) : m \in M \setminus 0\}$ es no vacío. Como A es nötheriano, hay elementos maximales y, por la parte anterior, cada uno de ellos es un elemento de $\operatorname{Ass}_A(M)$. Así, $\operatorname{Ass}_A(M) \neq \emptyset$, probando la necesidad de la condición. □

c) $\mathfrak{p} \in \operatorname{Ass}_A(M)$ sii $\mathfrak{p} \in \operatorname{Spec} A$ y M posee un submódulo isomorfo a $A/\mathfrak{p}$.

Solución. Supongamos que $\mathfrak{p} \in \operatorname{Ass}_A(M)$, de manera que existe $m \in M$ tal que $\mathfrak{p} = \operatorname{ann}(m)$. Entonces el núcleo del morfismo $f : a \in A \mapsto am \in M$ es precisamente $\mathfrak{p}$, y el segundo teorema de isomorfismo nos dice que M tiene como súbmódulo a $\operatorname{im} f \cong A/\mathfrak{p}$.
Recíprocamente, supongamos que $\mathfrak{p}$ es primo y que hay un monomorfismo $f : A/\mathfrak{p} \to M$. Sea $\bar{1}$ la clase de 1 en $A/\mathfrak{p}$ y $m = f(\bar{1})$. Entonces como $\mathfrak{p}\bar{1} = 0$, $\mathfrak{p}m = \mathfrak{p}f(\bar{1}) = f(\mathfrak{p}\bar{1}) = 0$ y $\mathfrak{p} \subset \operatorname{ann}(m)$. Si ahora $a \in A$ es tal que $am = 0$, entonces $f(\bar{a}) = f(a\bar{1}) =$

$af(\bar{1}) = am = 0$; como f es inyectivo, $\bar{a} = 0$ en $A/\mathfrak{p}$, esto es, $a \in \mathfrak{p}$. Así, vemos que $\mathfrak{p} = \mathsf{ann}(m) \in \mathsf{Ass}_A(M)$. □

d) Si $\mathfrak{p} \in \mathsf{Spec}\, A$, entonces $\mathsf{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$.

Solución. El ejercicio anterior implica inmediatamente que $\mathfrak{p} \in \mathsf{Ass}_A(A/\mathfrak{p})$.
Sea $a \in A$ con clase $\bar{a} \in A/\mathfrak{p}$ no nula, de forma que $a \notin \mathfrak{p}$. Afirmamos que $\mathfrak{p} = \mathsf{ann}(\bar{a})$. En efecto, es claro que $\mathfrak{p} \subset \mathsf{ann}(\bar{a})$ y si $b \in A$ es tal que $b\bar{a} = \overline{ba} = 0$ en $A/\mathfrak{p}$, entonces $ba \in \mathfrak{p}$. Como $\mathfrak{p}$ es primo y $a \notin \mathfrak{p}$, esto nos dice que $b \in \mathfrak{p}$. Esto prueba nuestra afirmación.
Vemos entonces que $\mathfrak{p}$ es el anulador de todos los elementos no nulos de $A/\mathfrak{p}$. Por supuesto, esto implica que $\mathsf{Ass}_A(A/\mathfrak{p}) \subset \{\mathfrak{p}\}$. □

e) Si $A = \mathbb{Z}$ y $n \in \mathbb{N}$, determine $\mathsf{Ass}_{\mathbb{Z}}(\mathbb{Z}_n)$.

Solución. Mostremos que $\mathsf{Ass}_{\mathbb{Z}}(\mathbb{Z}_n) = \{(p) : p \in \mathbb{N} \text{ es primo y } p \mid n\}$.
Si $p \in \mathbb{N}$ es primo y $p \mid n$, pongamos $m = n/p$ y sea $\bar{m}$ la clase de m en $\mathbb{Z}_n$. Es evidente que $p\bar{m} = 0$; por otro lado, si $a \in \mathbb{Z}$ es tal que $a\bar{m} = 0$, debe ser $pm = n \mid am$ y entonces $p \mid a$. Esto nos dice que $\mathsf{ann}(\bar{m}) = (p)$ y que $(p) \in \mathsf{Ass}_{\mathbb{Z}}(\mathbb{Z}_n)$.
Recíprocamente, si $p \in \mathbb{N}$ es un primo tal que $(p) \in \mathsf{Ass}_{\mathbb{Z}}(\mathbb{Z}_n)$, entonces existe $m \in \mathbb{Z}$ con clase $\bar{m} \in \mathbb{Z}_n \setminus 0$ tal que $\mathsf{ann}(\bar{m}) = (p)$. Esto implica, en particular, que $\overline{pm} = p\bar{m} = 0$ en $\mathbb{Z}_N$, esto es, que $n \mid pm$. Si $(p, n) = 1$ y $\alpha, \beta \in \mathbb{Z}$ son tales que $\alpha p + \beta n = 1$, entonces $n \mid \alpha pm + \beta nm = m$. Esto es imposible, porque supusimos que $\bar{m} \neq 0$ en $\mathbb{Z}_m$. Luego debe ser $(p, n) \neq 1$ y, en consecuencia, $p \mid n$.

f) Sea $S \subset A$ es un subconjunto multiplicativamente cerrado en A. Si $\mathfrak{p} \in \mathsf{Ass}_A(M)$ es tal que $\mathfrak{p} \cap S = \emptyset$, entonces $\mathfrak{p} \in \mathsf{Ass}_A(M_S)$.

Solución. Sea $\mathfrak{p} \in \mathsf{Ass}_A(M)$ tal que $\mathfrak{p} \cap S = \emptyset$. Entonces existe $m \in M$ tal que $\mathfrak{p} = \mathsf{ann}(m)$. Es claro que $\mathfrak{p} \cdot m/1 = 0$; si, por otro lado, $a \in A$ tal que $a \cdot m/1 = 0$, entonces existe $s \in S$ tal que $sam = 0$, esto es, tal que $sa \in \mathfrak{p}$ y, como $s \notin \mathfrak{p}$, vemos que $a \in p$. Luego $\mathfrak{p} = \mathsf{ann}(m/1) \in \mathsf{Ass}_A(M_S)$. □

g) Es $\mathsf{Ass}_A(M_S) = \mathsf{Ass}_A(M) \cap \{\mathfrak{p} \in \mathsf{Spec}\, A : \mathfrak{p} \cap S = \emptyset\}$.

Solución. En vista del ejercicio anterior, solo tenemos que mostrar que el lado izquierdo está contenido en el derecho.
Sea $\mathfrak{p} \in \mathsf{Ass}_A(M_S)$ y sea $m/s \in M_S \setminus 0$ tal que $\mathfrak{p} = \mathsf{ann}(m/s)$.
Supongamos que $\mathfrak{p} \cap S \neq \emptyset$, de manera que existe $u \in S$ tal que $u \cdot m/s = 0$. Entonces existe $v \in S$ tal que $vum = 0$ y, como $vu \in S$, esto implica que $m/s = 0$, contra la hipótesis. Luego $\mathfrak{p} \cap S = \emptyset$.
Como A es nötheriano, existen $p_1, \dots, p_k \in A$ tales que $\mathfrak{p} = (p_1, \dots, p_k)$. Si $1 \leq i \leq k$, $p_i \cdot m/s = 0$, así que existe $t_i \in S$ tal que $t_i p_i m = 0$. Sea $t = t_1 \cdots t_k$. Afirmamos que

$\mathfrak{p} = \mathsf{ann}(tm)$. En efecto, si $1 \leq i \leq k$, es claro que $p_i tm = 0$ porque t_i divide a t; esto dice que $\mathfrak{p} \subset \mathsf{ann}(tm)$. Por otro lado, si $a \in A$ es tal que $atm = 0$, entonces $at \in \mathfrak{p}$ y como $t \notin \mathfrak{p}$, debe ser $a \in \mathfrak{p}$. Esto prueba nuestra afirmación.
Concluímos entonces que $\mathfrak{p} \in \mathsf{Ass}_A(M)$ y $\mathfrak{p} \cap S = \emptyset$, como queríamos. □

h) Usando *c)* muestre que si

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

es una sucesión exacta de A-módulos, entonces

$$\mathsf{Ass}_A(M) \subset \mathsf{Ass}_A(M') \cup \mathsf{Ass}_A(M'').$$

Solución. Sea $\mathfrak{p} \in \mathsf{Ass}_A(M)$. Usando *c)*, vemos que existe un submódulo $N \subset M$ tal que $N \cong A/\mathfrak{p}$; como $A/\mathfrak{p}$ es un dominio, esto implica que $\mathsf{ann}(n) = \mathfrak{p}$ para todo $n \in N$. Si $N \cap f(M') = 0$, entonces $g(N)$ es un submódulo de M'' isomorfo a $A/\mathfrak{p}$, así que en este caso $\mathfrak{p} \in \mathsf{Ass}_A(M'')$. Supongamos entonces que, por el contrario, existe $n' \in M'$ tal que $f(n') \in N$. Si $a \in A$, entonces $a \in \mathsf{ann}(n')$ sii $an' = 0 \iff f(an') = 0$ sii $a \in \mathsf{ann}(f(n'))$ porque f es inyectivo. Como $f(n') \in N$, la observación hecha arriba implica que $\mathsf{ann}(n') = \mathsf{ann}(f(n')) = \mathfrak{p}$. Luego $\mathfrak{p} \in \mathsf{Ass}_A(M')$.

i) Si A es nötheriano y M es un A-módulo finitamente generado no nulo, entonces existe una cadena creciente finita de submódulos

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M$$

e ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathsf{Spec}\, A$ tales que

$$M_i/M_{i-1} \cong A/\mathfrak{p}_i, \qquad \forall i \in \{1, \ldots, n\}.$$

Además, es $\mathsf{Ass}_A(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Solución. Supongamos que $n \geq 0$ y que tenemos una cadena

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n$$

de submódulos de M e ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathsf{Spec}\, A$ tales que $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ si $1 \leq i \leq n$ y $\mathsf{Ass}_A(M_n) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Notemos que cuando $n = 0$ esta hipótesis se satisface trivialmente.
Si $M_n \subsetneq M$, entonces $M/M_n \neq 0$ y existe $\mathfrak{p}_{n+1} \in \mathsf{Ass}_A(M/M_n)$. En particular, existe un submódulo N de M/M_n tal que $N \cong A/\mathfrak{p}_{n+1}$. El tercer teorema de isomorfismo implica entonces que existe un submódulo M_{n+1} de M que contiene a M_n y tal que $M_{n+1}/M_n \cong N$. Además, la sucesión exacta

$$0 \longrightarrow M_n \longrightarrow M_{n+1} \longrightarrow M_{n+1}/M_n \cong A/\mathfrak{p} \longrightarrow 0$$

implica que

$$\mathsf{Ass}_A(M_{n+1}) \subset \mathsf{Ass}_A(M_n) \cup \mathsf{Ass}_A(A/\mathfrak{p}_{n+1}) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \cup \{\mathfrak{p}_{n+1}\}.$$

De esta forma obtenemos, en particular, una cadena creciente $\{M_i\}_{i\geq 0}$ finita o infinita de submódulos de M. Como A es nötheriano y M finitamente generado, esta cadena no puede ser infinita. Esto significa que existe $n \in \mathbb{N}$ tal que $M_n = M$. Es claro que esto prueba el ejercicio. $\square$