Álgebra Moderna Tarea 5.1

Tomás Ricardo Basile Álvarez
316617194

9 de diciembre de 2020

a) **Haz una lista con todos los grupos abelianos con 360 elementos.**

Sea G un grupo abeliano de orden 360. Primero notamos que $360 = 2^3 \cdot 3^2 \cdot 5$. Esto implica que el 2-subgrupo de Sylow de G, denotado por P_2 es de orden 8. El 3-subgrupo, denotado por P_3 es de orden 9 y el 5-subgrupo de Sylow, denotado por P_5 es de orden 5.
Sabemos que cada uno de estos son el único subgrupo de Sylow de su respectivo orden por 32.3.
Además, por 32.2 sabemos que $G \simeq P_2 \times P_3 \times P_5$
Ahora hay que encontrar las posibilidades para los grupos P_2, P_3, P_5.
Para ello, usamos la proposición 32.4

- P_2 : Como es de orden 2^3, la proposición 32.4 nos dice que hay que encontrar todos los posibles naturales $a_1, \cdots, a_r \in \mathbb{N}$ tales que $a_1 \geq a_2 \geq \cdots \geq a_r \geq 1$ y que $3 = a_1 + a_2 + \cdots + a_r$. Y entonces tendremos que $G \simeq C_{2^{a_1}} \times \cdots \times C_{2^{a_r}}$
  En este caso, las únicas posibilidades para sumar hasta 3 son $1+1+1, 2+1, 3$. Y por tanto, los grupos posibles son $C_2 \times C_2 \times C_2$, $C_4 \times C_2$, C_8

- P_3 : Hacemos lo mismo que en el anterior. Como es de orden 3^2, la proposición 32.4 nos dice que hay que encontrar todas las posibles sucesiones de naturales mayores que 1 que suman hasta 2. las únicas posibilidades son $1+1, 2$. Y por tanto, los grupos posibles son $C_3 \times C_3$, C_9
- P_5 : Hacemos lo mismo que en el anterior. Como es de orden 5^1, la proposición 32.4 nos dice que la única posibilidad es C_5.

Entonces, las posibilidades para $G \simeq P_2 \times P_3 \times P_5$ son (Juntaremos los productos de grupos cíclicos de órdenes coprimos como en la clase 33 y usamos $C_m \times C_n \simeq C_{mn}$):

- $C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5 \simeq (C_2 \times C_3 \times C_5) \times (C_2 \times C_3) \times C_2 \simeq C_{30} \times C_6 \times C_2$
- $C_2 \times C_2 \times C_2 \times C_9 \times C_5 \simeq (C_2 \times C_5 \times C_9) \times C_2 \times C_2 \simeq C_{90} \times C_2 \times C_2$
- $C_2 \times C_4 \times C_3 \times C_3 \times C_5 \simeq (C_3 \times C_4 \times C_5) \times (C_2 \times C_3) \simeq C_{60} \times C_6$
- $C_2 \times C_4 \times C_9 \times C_5 \simeq (C_4 \times C_5 \times C_9) \times C_2 \simeq C_{180} \times C_2$

- $C_8 \times C_3 \times C_3 \times C_5 \simeq (C_8 \times C_5 \times C_3) \times C_3 \simeq C_{120} \times C_3$
- $C_8 \times C_9 \times C_5 \simeq C_{360}$

.

b) **Sea G un grupo y sea $G_{p^r} = \{g \in G \ : \ |g||p^r\}$. Prueba que si G es p-grupo Abeliano finito entonces G_{p^r} es un subgrupo de G. Da un ejemplo de un p-grupo finito en el que G_{p^r} no forma un subgrupo.**

Inmediatamente se tiene que $G_{p^r} \subset G$ con G finito. Entonces, como G_{p^r} es no vacío (contiene al menos a la identidad porque $|e| = 1|p^r$) para probar que es un subgrupo, basta probar que es cerrado (proposición 8.3 b).

Sea $a, b \in G_{p^r}$. Por lo que $|a| \mid p^r, \ |b| \mid p^r$.
Entonces, vemos que $ab \in G$ (por ser G un grupo) y vemos cuánto vale $(ab)^{p^r}$

$$\begin{aligned}
(ab)^{p^r} &= (ab)(ab)\cdots(ab) \quad \text{(el producto es } p^r \text{ veces)} \\
&= (a \cdot a \cdots a)(b \cdot b \cdots b) \quad \text{(cada producto es } p^r \text{ veces)} \\
&= a^{p^r} b^{p^r} \\
&= e \cdot e \quad \text{porque a,b } \in G_{p^r} \text{ y por tanto, el orden de a y el de b dividen a } p^r \\
&\qquad\qquad\qquad\qquad \text{por lo que } a^{p^r} = b^{p^r} = e \\
&= e
\end{aligned}$$

Entonces, $(ab)^{p^r} = e$. Lo que implica que el orden de ab divide a p^r. Por tanto $ab \in G_{p^r}$. Por lo que la operación es cerrada y sí es un subgrupo de G.

Contraejemplo no abeliano: Consideramos el grupo $G = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$ el grupo diédrico de orden 8.
Entonces, como es de orden $8 = 2^3$, el lema 24.4 nos asegura que G es un 2-grupo.
Ahora consideramos el subconjunto G_{2^1} de todos los elementos de G con orden que dividen a $2^1 = 2$.
Es decir, todos los elementos de G con orden 1 o 2.
Por lo que hemos estudiado de grupos diédricos, dichos elementos son $G_{2^1} = \{1, s, r^2, sr, sr^2, sr^3\}$.
Este conjunto tiene 6 elementos y como 6 no divide a 8, el teorema de Lagrange nos asegura que es imposible que G_{2^1} sea subgrupo de G.

c) **Prueba que si d es un divisor del orden de un grupo abeliano G, entonces G tiene un subgrupo de orden d**

Lo probaremos por inducción sobre el orden de G.
En el caso base, si $|G| = 1$, entonces $G = \{e\}$ y el único divisor del orden es 1. Por

tanto, tiene un subgrupo para cada uno de los divisores.

Ahora suponemos que $|G| = n$ y que el teorema se cumple para todo grupo de orden menor a n.
Sea $d \in \mathbb{N}$ un divisor de n y queremos encontrar un subgrupo de G de orden d.
Podemos escribir d como $d = mp$ donde p es un primo cualquiera y p puede o no dividir a m.

Por el teorema de Cauchy, como p divide a n, G tiene un subgrupo de orden p. Llamemos $H \leq G$ a este subgrupo de orden p.
Además, como G es abeliano, todo subgrupo es normal, por lo que $H \trianglelefteq G$. Esto implica que existe el grupo cociente G/H.

Además, este grupo tiene $|G/H| = |G|/|H| = n/p < n$ elementos. Por hipótesis de inducción eso implica que G/H tiene subgrupos de todos los órdenes que dividan a n/p.
En particular como $mp = d$ divide a n, entonces m divide a n/p. Por lo que G/H tiene un subgrupo de orden m.

Sea $\mathcal{M} \leq G/H$ dicho subgrupo de orden m. Por el teorema de correspondencia, a este $\mathcal{M}$ subgrupo de G/H le corresponde un subgrupo M de G tal que $H \leq M \leq G$.
No sólo eso, sino que el teorema de correspondencia nos asegura que $\mathcal{M} \leq G/H$ tiene la forma M/H para esta $M \leq G$

Entonces, tenemos un grupo $M \leq G$ tal que M/H tiene m elementos.
Luego, $|M/H| = m \;\; \Rightarrow \;\; |M|/|H| = m \; \Rightarrow \; |M| = m|H| = mp = d$.

Por tanto, encontramos un subgrupo de G de d elementos.

Esto prueba el enunciado para el caso $|G| = n$. Y por inducción se sigue que el toerema es válido para todo grupo finito.

d) Determina cuántos subgrupos de orden p^2 hay en $\mathbb{Z}_p \times Z_{p^2}$

Primero que nada, notamos que $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ tiene al elemento $(1, 0)$ de orden p y a $(0, 1)$ de orden p^2 que entre ambos generan a todo $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ y además conmutan. Entonces, podemos ver a este grupo $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ como:

$$\langle a, b \;\mid\; a^p = b^{p^2} = e \;\;, ab = ba \rangle$$

Y lo estudiaremos de esa forma. Todos los elementos de este grupo son de la forma $a^l b^m$ para $0 \leq l < p \ \ , 0 \leq m < p^2$ (por ser abeliano todos los generados de a, b son de estas formas).

Ahora bien, los subgrupos de orden p^2 de este grupo deben de ser también abelianos. Y por lo que hemos visto, estos subgrupos tienen que ser de la forma C_{p^2} o $C_p \times C_p$. Entonces buscamos todos los subgrupos de estas formas.

- **Subgrupos de forma C_{p^2}:**
  Estos grupos tienen que ser cíclicos generados por un elemento de orden p^2. Entonces veamos qué elementos de orden p^2 hay en el grupo. Como dijimos, todos los elementos son de la forma $a^l b^m$ con $0 \leq l < p \ , \ 0 \leq m < p^2$.
  Estos elementos tienen que ser de orden $1, p$ o de orden p^2 (por el teorema de Lagrange y no pueden ser de orden p^3 porque el grupo original no es cíclico).

  Entonces los elementos de orden p^2 son los $a^l b^m$ tales que no son de orden p ni de orden 1. Entonces consideramos $(a^l b^m)^p = (a^l)^p (b^m)^p$ (por ser abeliano) $= a^{lp} b^{mp} = (a^p)^l b^{mp} = e b^{mp} = b^{mp}$.
  Queremos que esto no se anule para que $a^l b^m$ no sea de orden p u orden 1. Entonces, como el orden de b es p^2, necesitamos que mp no sea múltiplo de p^2.
  Por lo que de entre las posibilidades de m, recordando que p es primo, m no puede ser 0 ni p ni $2p$ ni $3p$ $, \cdots ,$ ni $(p-1)p$. Lo que elimina p de las p^2 opciones para m.
  Por lo que tenemos $p^2 - p$ opciones para m tales que $a^l b^m$ es de orden p^2. Mientras que l puede tomar cualquiera de sus p opciones.

  Por tanto, tenemos $(p^2 - p)p$ opciones de elementos de orden p^2.
  El generado de cada uno de estos elementos es un subgrupo de orden p^2 isomorfo a C_{p^2}. Sin embargo, no hay tantos grupos distintos de esta forma ya que muchos tienen generadores repetidos.
  Por ejemplo, sea c uno de los $(p^2 - p)p$ elementos de orden p^2 y consideramos el subgrupo $\{e, c, c^2, \cdots, c^{p^2-1}\}$.Por lo que hemos estudiado de grupos cíclicos, en este subgrupo cíclico hay tantos generadores de todo el subgrupo como elementos de la forma c^i tales que i es coprimo con p^2. Esto es lo mismo que la función phi de Euler evaluada en p^2, que por propiedades de esta función, tiene por resultado $p^2 - p$.

  Entonces, para cada uno de los $(p^2 - p)p$ elementos de orden p^2, el grupo cíclico generado en realidad contiene $p^2 - p$ otros elementos que generan al mismo grupo. Por lo que en realidad, la cantidad de subgrupos de orden p^2 isomorfos a C_{p^2} es $\dfrac{(p^2 - p)p}{p^2 - p} = p$

  Por tanto, tenemos p subgrupos de orden p^2 isomorfos a C_{p^2}.

- **Subrupos de la forma $C_p \times C_p$**
  Estos subgrupos son generados por dos elementos cada uno de orden p tales que conmutan entre sí. Todos los elementos del grupo conmutan con el que empezamos conmutan. Así que necesitamos contar la cantidad de elementos de orden p en el grupo.

  Ya vimos que hay $(p^2 - p)p$ elementos de orden p^2 y hay un elemento de orden 1 (el elemento e). Entonces, el resto de los p^3 elementos del grupo son los de orden p (recordar que no hay ningún elemento de orden p^3 porque el grupo original no es cíclico).
  Para un total de $p^3 - (p^2 - p)p - 1 = p^3 - p^3 + p^2 - 1 = p^2 - 1$ elementos de orden p.

  Ahora bien, un subgrupo isomorfo a $C_p \times C_p$ tiene que estar generado por dos de estos elementos de orden p. Y además, todos los elementos de este subgrupo isomorfo a $C_p \times C_p$ tienen orden p (excepto e que tiene orden 1), esto porque ninguno puede tener orden p^2 ya que eso haría al grupo $C_p \times C_p$ cíclico pero no lo es.
  Entonces, el subgrupo isomorfo a $C_p \times C_p$ debe de contener $|C_p \times C_p| - 1 = p^2 - 1$ elementos de orden p. Pero vimos que el grupo que estamos estudiando tiene exactamente $p^2 - 1$ elementos de orden p. Por lo que el <u>único</u> subgrupo isomorfo a $C_p \times C_p$ es aquél que tiene a todos los $p^2 - 1$ elementos de orden p.
  Sabemos que este conjunto de todos elementos de orden p (y e) es efectivamente un subgrupo por el inciso b) y es único por lo mencionado antes.
  Por lo que hay sólo un subgrupo del grupo original que es isomorfo a $C_p \times C_p$.

Entonces en total, la cantidad de subgrupos de orden p^2 es $p^2 + 1$.

e) **Sea G un grupo Abeliano de tipo $(n_1, n_2, \cdots, n_t)$. Prueba que G contiene un elemento de orden m si y sólo si $m|n_1$**

Ida: Como G es de tipo $(n_1, n_2, \cdots, n_t)$, tenemos que $G \simeq C_{n_1} \times \cdots \times C_{n_t}$.
Donde n_i divide a n_j para todo $i > j$. Sea x_i el generador del grupo C_{n_i}. Entonces todo elemento se ve de la forma $(x_1^{k_1}, x_2^{k_2}, \cdots, x_t^{k_t})$ para naturales k_i con $0 \leq k_i < n_i$.

Vemos que todo los elementos del grupo, que son de la forma $(x_1^{k_1}, x_2^{k_2}, \cdots, x_t^{k_t})$ se anulan al elevarlos a la n_1.
Esto se ve porque $(x_1^{k_1}, x_2^{k_2}, \cdots, x_t^{k_t})^{n_1} = (x_1^{k_1 n_1}, x_2^{k_2 n_1}, \cdots, x_t^{k_t n_1})$
Pero cada uno de estos $x_i^{k_i n_1}$ son el neutro de C_{n_i}. Esto porque n_1 es un múltiplo de n_i para todo i por como se ordenan los n. Y por tanto $k_i n_1$ es un múltiplo de n_i para todo n_i. Como n_i es el orden de x_i, esto implica que x_i se anula al elevarlo a la $k_i n_1$.
Por lo que $(x_1^{k_1}, x_2^{k_2}, \cdots, x_t^{k_t})^{n_1}$ es el neutro de $C_{n_1} \times \cdots \times C_{n_t}$.

Probamos que todo elemento de $C_{n_1} \times \cdots \times C_{n_t}$ se anula al elevarlo a la n_i. Para probar ahora sí el ejercicio, suponemos que existe un elemento $\mathbf{x} \in C_{n_1} \times \cdots \times C_{n_t}$ de orden m. Por el párrafo anterior sabemos que $\mathbf{x}^{n_1}$ es la identidad.
Pero como los únicos exponentes de $\mathbf{x}$ que dan la identidad deben de ser múltiplos del orden m, eso implica que n_1 es múltiplo de m. Y ya se probó lo que buscábamos.

Regreso: Sea m tal que $m|n_1$. Y denotamos $k = \dfrac{n_1}{m}$ que es un entero. Ahora consideramos el elemento $(x_1^k, e_2, e_3, \cdots, e_t) \in C_{n_1} \times \cdots \times C_{n_t}$. Donde x_1 es el generador de C_{n_1} y e_i es el neutro de C_{n_i}.
Entonces, se puede ver que este elemento es de orden m porque:

$$\begin{aligned}(x_1^k, e_2, e_3, \cdots, e_t)^m &= (x_1^{km}, e_2, e_3, \cdots, e_t)\\ &= (x_1^{n_1}, e_2, e_3, \cdots, e_t)\\ &= (e_1, e_2, \cdots, e_t) \qquad \text{porque } x_1 \text{ tiene orden } n_1\end{aligned}$$

Y esto último es el neutro de $C_{n_1} \times \cdots \times C_{n_t}$.
Además, no hay ninguna potencia más pequeña que anule a $(x_1^k, e_2, e_3, \cdots, e_t)$. Porque $km = n_1$ es el primer múltiplo de k que es múltiplo de n_1, el orden de x_1.