Clase 7: Grupos abelianos finitamente generados

§14. Teorema chino del resto (continuación):

Ejemplo: Una consecuencia del Teo. chino del resto es que si $n_1, \dots, n_r \in \mathbb{N}^{\geq 2}$ son primos relativos y $a_1, \dots, a_r \in \mathbb{Z}$, entonces

$$\left\{ \begin{array}{l} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{array} \right\}$$

posee solución $x \in \mathbb{Z}$ (única si asumimos $0 \leq x < N$) $\leftarrow$ Pues si $N = n_1 \cdots n_r$ entonces $\mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ es un isomorfismo ($\Rightarrow$ sobreyectivo).

Obs: $N_i := N/n_i$ y $\operatorname{mcd}(N_i, n_i) = 1 \overset{\text{Bézout}}{\Longrightarrow} \exists\, y_i \in \mathbb{Z}$ tq $N_i y_i \equiv 1 \pmod{n_i}$

$\rightsquigarrow x := a_1 N_1 y_1 + \dots + a_r N_r y_r$ funciona!

En la práctica:
$$\left\{ \begin{array}{ll} x \equiv 0 & \pmod 3 \\ x \equiv 3 & \pmod 4 \\ x \equiv 4 & \pmod 5 \end{array} \right\} \rightsquigarrow N = 3 \cdot 4 \cdot 5 = 60. \rightsquigarrow \begin{array}{l} N_1 = 20 \\ N_2 = 15 \\ N_3 = 12 \end{array}$$

$$\left. \begin{array}{l} N_1 = 20 \equiv 2 \pmod 3 \rightsquigarrow y_1 = 2 \ \checkmark \\ N_2 = 15 \equiv 3 \pmod 4 \rightsquigarrow y_2 = 3 \ \checkmark \\ N_3 = 12 \equiv 2 \pmod 5 \rightsquigarrow y_3 = 3 \ \checkmark \end{array} \right\} \begin{array}{l} x = 0 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \\ \quad = 279 \rightsquigarrow x_{min} = 39 \text{ solución minimal en } \{0, 1, \dots, 59\}. \end{array}$$

Recuerdo: Un grupo abeliano $(G,+)$ es FINITAMENTE GENERADO si existen $x_1,\dots,x_r \in G$ tal que el morfismo

$$p : \mathbb{Z}^r \to G, \quad (a_1,\dots,a_r) \mapsto a_1x_1+\dots+a_rx_r$$ sea sobreyectivo.

Proposición 2.4.4. — *Sea G un grupo abeliano finitamente generado y sea $H \leq G$ un sub-grupo. Entonces H es finitamente generado.*

Dem (inducción en nº de generadores r): Si $p : \mathbb{Z}^r \to G$ sobrey. y denotamos

$K := p(\mathbb{Z}^{r-1}\times\{0\}) \leftarrow$ generado por $r-1$ elementos

Sea $\pi : G \to G/K$ proy. canónica y sea

$$\varphi := \pi\circ p : \mathbb{Z}^r \to G \to G/K$$
$$(a_1,\dots,a_r) \mapsto \sum a_ix_i \mapsto \left[\sum a_ix_i\right] = [a_rx_r] \mod K$$

$\Rightarrow \varphi$ se factoriza en

$$\mathbb{Z}^r \to \mathbb{Z}^r/(\mathbb{Z}^{r-1}\times\{0\}) \simeq \mathbb{Z} \xrightarrow{\hat{\varphi}} G/K$$
$$(a_1,\dots,a_r) \mapsto [a_r] \longmapsto [a_rx_r]$$

$\overset{\text{Noether}}{\Rightarrow}$ $G/K \cong \mathbb{Z}/\ker(\hat{\varphi}) \cong \mathbb{Z}/d\mathbb{Z}$ cierto $d\in\mathbb{N}^{\geq 1}$

Dem (continuación):

Usemos esto:

$H \leq G$ y sea $\psi : H \hookrightarrow G \xrightarrow{\pi} G/K \cong \mathbb{Z}/d\mathbb{Z}$ composición

$\Rightarrow \ker(\psi) = H \cap K$ finitamente generado (Hip. de Inducción!)

Por otro lado, $\mathrm{Im}(\psi) \overset{\text{Noether}}{\cong} H/(H \cap K)$ subgrupo de $G/K \cong \mathbb{Z}/d\mathbb{Z}$

$\Rightarrow \mathrm{Im}(\psi) \simeq \mathbb{Z}/e\mathbb{Z}$ cierto $e \mid d$

$\Rightarrow H/(H \cap K)$ generado por 1 elemento & $H \cap K$ fin. gen.

$\Rightarrow H$ fin. generado ∎

§15. Grupos abelianos libres finitamente generados

Terminología: Como antes, sea $(G,+)$ grupo abeliano finitamente generado por $\mathcal{B} = \{x_1, \dots, x_r\} \subseteq G$, i.e.,

$$p : \mathbb{Z}^r \twoheadrightarrow G, \quad (a_1, \dots, a_r) \mapsto a_1 x_1 + \dots + a_r x_r \quad \text{es sobreyectivo.}$$

Decimos que G es LIBRE si $p : \mathbb{Z}^r \xrightarrow{\sim} G$ es un isomorfismo (i.e, $G \cong \mathbb{Z}^r$) y en tal caso decimos que $\mathcal{B} = \{x_1, \dots, x_r\}$ es una BASE de G.

Obs: Más generalmente, decimos que $\{x_1, \dots, x_r\} \subseteq G$ es LINEALMENTE INDEPENDIENTE si el morfismo asociado $p : \mathbb{Z}^r \hookrightarrow G$, $(a_1, \dots, a_r) \mapsto \sum_{i=1}^r a_i x_i$ es inyectivo.

Asumiremos (sin demostración) el siguiente resultado de "álgebra lineal":

Lema útil: Sea $A \in M_{m\times n}(\mathbb{Z})$. Entonces, $\exists P \in GL_m(\mathbb{Z})$ y $\exists Q \in GL_n(\mathbb{Z})$ tales que

$$PAQ = \begin{pmatrix} d_1 & & & & \\ & \ddots & & 0 & \\ & & d_s & & \\ & 0 & & 0 & \\ & & & & \ddots \\ & & & 0 \cdots & 0 \end{pmatrix}$$

con $d_1, \dots, d_s \in \mathbb{N}^{\geq 1}$ cumplen $d_1 \mid d_2 \mid \cdots \mid d_s$.

Los d_i son los FACTORES INVARIANTES de A (únicamente determinados por A!)

Teorema 2.4.7. — *Todas las bases de un grupo abeliano libre finitamente generado G tienen el mismo cardinal, llamado el* **rango** *de G.* $\rightsquigarrow$ $rg(G)$ ó Nº de Betti

<u>Dem</u>: Veamos que si $\{x_1, \dots, x_r\}$ base de G y $\{y_1, \dots, y_n\} \subseteq G$ l.i.

$\Rightarrow n \leq r$.

Escribimos $y_j = \sum_{i=1}^{r} a_{ij} x_i \rightsquigarrow A = (a_{ij}) \in M_{r \times n}(\mathbb{Z})$

matriz asoc. a $\mathbb{Z}^n \to G$, $e_i \mapsto y_i$

Lema útil: $\exists P, Q$ invertibles tq $PAQ = \begin{pmatrix} D & 0 \\ 0 & 0_{(r-s)\times(n-s)} \end{pmatrix}$

Si $\underline{n > r} \Rightarrow PAQe_n = 0 \overset{P \text{ invertible}}{\Rightarrow} A\underbrace{Qe_n}_{(q_1, \dots, q_n) \neq 0 \ (Q \text{ invertible})} = 0$

$\Rightarrow q_1 \underbrace{Ae_1}_{y_1} + \dots + q_n \underbrace{Ae_n}_{y_n} = 0 \Rightarrow \{y_1, \dots, y_n\}$ es l.d. $\lightning$

$\blacksquare$

Teorema 2.4.8 (de la base adaptada). — *Sea G un grupo abeliano libre de rango r y sea $H \leq G$ un sub-grupo. Entonces H es un grupo abeliano libre de rango $s \leq r$. Más aún, existe $\{e_1, \dots, e_r\}$ base de G y $d_1, \dots, d_s \in \mathbb{N}^{\geq 1}$ tales que*

1. $\{d_1 e_1, \dots, d_s e_s\}$ *es una base de H.*
2. $d_1 \mid d_2 \mid \cdots \mid d_s$.

Dem: Sea $\{x_1, \to x_r\}$ base de G y $\Phi : \mathbb{Z}^r \xrightarrow{\sim} G$ isomorfismo asociado.

$H \leq G \overset{\text{Prop}}{\Longrightarrow} H = \langle y_1, \to y_n \rangle$ ciertos $y_i \in H$.

Escribamos $y_j = \sum_{i=1}^{r} a_{ij} x_i \rightsquigarrow A = (a_{ij}) \in M_{r \times n}(\mathbb{Z})$ asociada a $\mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^r$, $\varepsilon_i \longmapsto A\varepsilon_i$

base canónica de $\mathbb{Z}^n$

Por def, $\mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^r \xrightarrow[\Phi]{\sim} G$, $\varepsilon_i \longmapsto f(\varepsilon_i) = y_i \in H \Rightarrow \mathrm{Im}(f) = H$.

Lema útil $\Rightarrow \exists\, P, Q$ cambios de base tq $f \circ Q \overset{\text{def}}{=} \Phi \circ A \circ Q = \Phi \circ P^{-1} \circ \underbrace{(P \circ A \circ Q)}_{\text{"sencilla"}}$

i.e., $\underbrace{\mathbb{Z}^n \xrightarrow[\sim]{Q} \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^r \xrightarrow[\sim]{P} \mathbb{Z}^r}_{\text{"sencillo"}} \underbrace{\xrightarrow[\sim]{P^{-1}} \mathbb{Z}^r \xrightarrow[\sim]{\Phi} G}_{\tilde{\Phi} : \mathbb{Z}^r \xrightarrow{\sim} G} \rightsquigarrow \{e_1, \dots, e_r\}$ base de G !

Dem (continuación):

En esta base, $H = \operatorname{Im}(f) = \operatorname{Im}(f \circ Q) = \langle d_1 e_1, \ldots, d_s e_s \rangle$

l.i.

$\Rightarrow H \cong \mathbb{Z}^s$ y $\{d_1 e_1, \ldots, d_s e_s\}$ "base adaptada" ∎

Teorema 2.4.9 (de estructura de grupos abelianos de tipo finito) ie, fin. gen.

Sea G un grupo abeliano finitamente generado. Entonces existen naturales $r, s \in \mathbb{N}$ y enteros $1 < d_1 \mid \cdots \mid d_s$, únicamente determinados por G, tales que

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

En particular, se tiene que G es finito si y sólo si $r = 0$, y que G es abeliano libre si y sólo si $s = 0$.

★ Ej: $(n=3)$ $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$

$H = 2\mathbb{Z} \times \{0\} \times \{0\}$

$\rightsquigarrow G \cong \mathbb{Z}^3 / H$

$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2$

Dem:

Existencia: G fin. gen. $\overset{\text{dy}}{\Longrightarrow} \exists\, \Phi: \mathbb{Z}^n \twoheadrightarrow G$ sobreyectivo

Base adaptada: $H = \ker(\Phi) \simeq \mathbb{Z}^s$ con $s \le n$ y $\exists \{e_1, \ldots, e_n\}$ base de $\mathbb{Z}^n$ y $d_1 \mid d_2 \mid \cdots \mid d_s$ tq $H = \langle d_1 e_1, \ldots, d_s e_s \rangle$.

ie, $H \cong d_1\mathbb{Z} \times d_2\mathbb{Z} \times \cdots \times d_s\mathbb{Z} \underset{(★)}{\overset{\text{Noether}}{\Longrightarrow}} G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}^{n-s}$

$r = n-s$

Sin pérdida de generalidad, podemos sup. que $d_i > 1 \ \forall i$ ✓

Dem (continuación): Unicidad (de r, s y los d_i):

Consideramos $T(G) := \{ x \in G \text{ tq } \exists\, m \in \mathbb{N}^{\geq 1} \text{ tq } mx = 0 \}$ ← TORSIÓN DE G.

$\Rightarrow T(G) \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$ y $G/T(G) \simeq \mathbb{Z}^r$ ← rango $r = n-s$ único !

Veamos que los d_i son únicos:

Usamos el Teo. chino del resto con cada $\mathbb{Z}/d_i\mathbb{Z}$ y obtenemos

$$T(G) \cong \prod_{j \in J} \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$$ con p_j primos (quizás repetidos)

La idea es recuperar los d_i a partir de los $p_j^{\alpha_j}$ (☆)

(eg. d_s es el mcd de los $p_j^{\alpha_j}$ y luego $d_s = \prod_{j \in J' \subseteq J} p_j^{\alpha_j}$

⇝ d_{s-1} es mcd de $p_j^{\alpha_j}$ con $j \notin J'$, etc.)

⇝ Basta probar que los $p_j^{\alpha_j}$ son únicos:

Dem (continuación):

Sea p primo y consideramos

$$T_p(G) = \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z}$$

p-torsión de G.

$\alpha_1 \leq \cdots \leq \alpha_s$

Notamos finalmente que los subgrupos

$$T_{p^i}(G) := \{x \in G \text{ tq } p^i x = 0\} \leq T_p(G)$$

$\rightsquigarrow$ determinan únicamente cada α_i ✓ ∎

La demostración del teorema anterior provee un algoritmo para calcular los factores invariantes de un grupo abeliano finito G:

Escribir los factores $p_j^{\alpha_j}$ (quizás repetidos) en una tabla con una línea por cada primo, en orden creciente, y alinear cada línea a la última columna.

$\rightsquigarrow$ Los d_i se obtienen al tomar los productos de cada columna.

Ejemplos:

① $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$

$2 \qquad 10 = 2 \cdot 5 \qquad 16 = 2^4$

$$\rightsquigarrow \quad \begin{array}{ccc} 2 & 2 & 2^4 \\ & & 5 \\ \downarrow & \downarrow & \downarrow \\ d_1 = 2 & d_2 = 2 & d_3 = 80 \end{array}$$

$\Rightarrow G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/80\mathbb{Z}$

(i.e. $G \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/80\mathbb{Z}$)

② Todos los grupos abelianos de orden $2020 = 2^2 \cdot 5 \cdot 101$ están determinados por las posibles secuencias $1 < d_1 \mid d_2 \mid \cdots \mid d_s$ tales que $d_1 \cdots d_s = 2020$.

$\rightsquigarrow$ $s = 1$: $d_1 = 2020 \Rightarrow G \cong \mathbb{Z}/2020\mathbb{Z}$

$s = 2$: $(d_1, d_2) \in \{(2, 1010)\} \Rightarrow G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/1010\mathbb{Z}$.

$s \geq 3$: Imposible en este caso.

$\exists$ sólo 2 grupos abelianos de orden 2020!

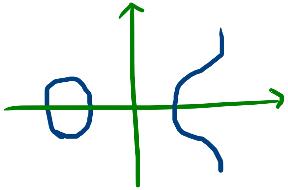
Cultura general

Una CURVA ELÍPTICA sobre un cuerpo k es

$$E(k) := \{[x,y,z] \in \mathbb{P}^2(k) \text{ tq } y^2 z = x^3 + axz^2 + bz^3\} \subseteq \mathbb{P}^2(k)$$

donde $a, b \in k$ cumplen $\Delta := -16(4a^3 + 27b^2) \neq 0$ y donde $E(k) \neq \emptyset$.

<u>Hechos</u>: $E(k)$ puede ser dotada de estructura de GRUPO ABELIANO!



$k = \mathbb{R}$

[Teorema de Mordell-Weil (1922): $E(\mathbb{Q})$ es finitamente generado!

$\rightsquigarrow E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T(E)$, con $T(E)$ abeliano finito.

[Teorema de Mazur (1977): $T(E) \cong \mathbb{Z}/d\mathbb{Z}$ con $d \in \{1, \ldots, 10, 12\}$ ó bien
$T(E) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ con $d \in \{2, 4, 6, 8\}$.

<u>Conjectura</u> (Problema abierto): $\operatorname{rg} E(\mathbb{Q})$ puede ser arbitrariamente grande.

↳ Record a la fecha: $\operatorname{rg} E(\mathbb{Q}) = 28$

$$y^2 + xy + y = x^3 - x^2 - 20\,067\,762\,415\,575\,526\,585\,033\,208\,209\,338\,542\,750\,930\,230\,312\,178\,956\,502x + 34\,481\,611\,795\,030\,556\,467\,032\,985\,690\,390\,720\,374\,855\,944\,359\,319\,180\,361\,266\,008\,296\,291\,939\,448\,732\,243\,429$$

Elkies (2006)

§16. Grupos simples y series de composición

Para reducir el problema de clasificación de grupos finitos necesitaremos estudiar grupos simples:

Recuerdo: Sea G un grupo. Decimos que G es un GRUPO SIMPLE si:
1º) $G \neq \{e\}$
2º) si $H \trianglelefteq G$ entonces $H = \{e\}$ ó $H = G$.

Ejemplos:

1. $\mathbb{Z}/n\mathbb{Z}$ es simple $\Longleftrightarrow n = p$ es primo.
2. si $n \geq 3$, $A_n \trianglelefteq S_n$ y luego S_n NO es simple.
3. A_3 tiene orden $3!/2 = 6/2 = 3$ y luego $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ es simple ✓
4. A_4 NO es simple, pues las dobles transposiciones $(a,b)(c,d)$ en S_4 son todas conjugadas

$\Rightarrow K := \{Id; (1,2)(3,4); (1,3)(2,4); (1,4)(2,3)\} \trianglelefteq A_4$ ← Obs: $K \cong (\mathbb{Z}/2\mathbb{Z})^2$ GRUPO DE KLEIN