ÁLGEBRA II
SEGUNDO CUATRIMESTRE 2023
CICLICIDAD DEL GRUPO DE UNIDADES DE $\mathbb{Z}_p$

El objetivo de estas notas es probar que, si $p \in \mathbb{N}$ es un número primo, entonces el grupo

$$\mathcal{U}_p = \{[k] : k \in \mathbb{Z}, (k : p) = 1\} = \{[1], \dots, [p-1]\}, \qquad [k] \cdot [l] := [kl].$$

es cíclico.

Lema 1. *Sea* G *un grupo abeliano de orden* $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *con* $p_1, \dots, p_k$ *números primos distintos y* $\alpha_1, \dots, \alpha_k \in \mathbb{N}$. *Si notamos* Q_{p_i} *a cada* p_i*-subgrupo de Sylow de* G*, entonces*

$$G \cong Q_{p_1} \times \cdots \times Q_{p_k}.$$

Demostración. Sea $H_1 = Q_{p_1}$ y, para cada $j \in \{2, \dots, k\}$,

$$H_j = H_j \cdot Q_{p_j} = Q_{p_i} \cdot \cdots \cdot Q_{p_j}.$$

Notemos que, como G es abeliano y todo subgrupo resulta normal, cada uno de estos conjuntos son subgrupos de G. Procedemos a probar, por inducción, que $H_j \cong Q_{p_1} \times \cdots \times Q_{p_j}$ para todo j.

El enunciado es cierto para $j = 1$. Supongamos ahora que $H_j \cong Q_{p_1} \times \cdots \times Q_{p_j}$ para cierto $j < k$. En particular $|H_j| = p_1^{\alpha_1} \cdots p_j^{\alpha_j}$ es coprimo con $p_{j+1}^{\alpha_{j+1}}$, así que que

$$H_j \cap Q_{p_{j+1}} = \{1\}.$$

Como tanto H_j como $Q_{p_{j+1}}$ son normales en H_{j+1} pues lo son en G, y $H_{j+1} = H_j \cdot Q_{p_{j+1}}$ por definición, se sigue que

$$H_{j+1} \cong H_j \times Q_{p_{j+1}} \cong Q_{p_1} \times \cdots \times Q_{p_j} \times Q_{p_{j+1}}$$

como buscábamos. □

Teorema 2. *Si* $p \in \mathbb{N}$ *es un número primo, entonces* $\mathcal{U}_p$ *es cíclico.*

Demostración. Como un producto de grupos cíclicos de orden coprimo es cíclico, basta ver que cada q-subgrupo de Sylow de $\mathcal{U}_p$ es cíclico. Sea q un primo que divide a $p-1$ y $n \in \mathbb{N}$ tal que $p - 1 = q \cdot m$, $q \perp m$. Consideremos Q el q-subgrupo de Sylow asociado. Notar que como $\mathbb{Z}_p$ es un cuerpo, el polinomio

$$x^{q^{n-1}} - 1 \in \mathbb{Z}_p[X]$$

tiene a lo sumo q^{n-1} raíces. Como $|Q| > q^{n-1}$, no puede ser que todo elemento de Q tenga orden divisor de q^{n-1}. Debe existir entonces $y \in Q$ tal que $\operatorname{ord}(y) = q^n$; es decir, tal que $Q = \langle y \rangle$. □