1. Estructura del grupo abeliano $(\mathbb{Z}_n^\times, .)$

La intención de estas notas es dar una descripción de la estructura del grupo abeliano $(\mathbb{Z}_n^\times, .)$. A lo largo de las mismas notaremos simplemente $\mathbb{Z}_n^\times$ a dicho grupo.

Prosición 1.1. *Sean m, n dos números naturales coprimos entre si entonces $\mathbb{Z}_{nm}^\times \simeq \mathbb{Z}_n^\times \oplus \mathbb{Z}_m^\times$*

Proof. Definimos la función $\psi : \mathbb{Z}_{nm}^\times \to \mathbb{Z}_n^\times \oplus \mathbb{Z}_m^\times$ por $\psi(u \bmod (nm)) = (u \bmod (n), u \bmod (m))$. Es fácil ver que ψ es un morfismo de grupos. Como ambos grupos tienen el mismo cardinal ($\phi(nm) = \phi(n)\phi(m)$ si $(n, m) = 1$) alcanza con ver que ψ es injectiva, pero si $u \equiv 1 \bmod n$ y $u \equiv 1 \bmod m$ como n y m con coprimos, $u \equiv 1 \bmod (nm)$. $\square$

Nota: es fácil ver que ψ es suryectiva usando el teorema chino del resto.

Corolario. *si $n = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$ entonces $\mathbb{Z}_n^\times \simeq \mathbb{Z}_{p_1^{r_1}}^\times \oplus \mathbb{Z}_{p_2^{r_2}}^\times \oplus \cdots \oplus \mathbb{Z}_{p_s^{r_s}}^\times$.*

Prosición 1.2. *Si K es un "cuerpo" y $p(x) \in K[x]$ es un polinomio, entonces $p(x)$ tiene a lo sumo $\deg(p(x))$ raices en K.*

Proof. Usando el algoritmo de división para polinomios (acá se usa que K es un cuerpo, o sea que si $a \in K$ y $a \neq 0$, entonces existe $a^{-1} \in K$ tal que $aa^{-1} = 1$) es claro que si α es raíz de $p(x)$ entonces $p(x) = (x - \alpha)q(x)$ donde $q(x) \in K[x]$ y $\deg(q(x)) = \deg(p(x)) - 1$ $\square$

¿Es cierto esta proposición si K no es un cuerpo? ¿ Cuantas raices tiene $x^2 - 1$ en $\mathbb{Z}_{15}$?

Teorema 1.1. *Si p es primo $\mathbb{Z}_p^\times$ es cíclico de orden $p - 1$.*

Proof. es claro que $\mathbb{Z}_p^\times$ es un grupo de orden $p-1$. Sea $e(\mathbb{Z}_p^\times)$ el exponente de $\mathbb{Z}_p^\times$ (o sea el mínimo n tal que $x^n = 1$ para todo $x \in \mathbb{Z}_p^\times$). Luego si $x \in \mathbb{Z}_p^\times$, $x^e = 1$. Como p es primo, $\mathbb{Z}_p$ es un cuerpo (¿ por que?), entonces el polinomio $p(x) = x^e - 1$ tiene a lo sumo e raices. Como todo elemento de $\mathbb{Z}_p^\times$ es raíz de $p(x)$ $e \geq p - 1$. A la vez como $e(\mathbb{Z}_p^\times)$ divide al orden del grupo se tiene la igualdad $e = p - 1$. $\mathbb{Z}_p^\times$ es abeliano y es facil ver que en todo grupo abeliando G existe un $x \in G$ tal que $\mathrm{ord}(x) = e(G)$. $\square$

Prosición 1.3. *si p es primo, entonces $\mathbb{Z}_{p^2}$ es cíclico.*

Proof. Si $p = 2$ es claro. Si $p \neq 2$, el cardinal de $\mathbb{Z}_{p^2}^\times$ es $p(p-1)$. Sea $\pi : \mathbb{Z}_{p^2}^\times \to \mathbb{Z}_p^\times$ el morfismo de grupos dado por $\pi(u \bmod p^2) = u \bmod p$. Sea $x \in \mathbb{Z}_p^\times$ un generador, e $y \in \mathbb{Z}_{p^2}^\times$ cualquier elemento de $\pi^{-1}(x)$ (π es suryectiva). Como $\mathrm{ord}(\pi(x)) \mid \mathrm{ord}(x)$ tenemos que $\mathrm{ord}(y) = p - 1$ o $\mathrm{ord}(y) = p(p-1)$. Por el Teorema de Cauchy, existe $z \in \mathbb{Z}_{p^2}^\times$ de orden p, entonces (como $p \neq 2$) el elemento yz tiene orden $p(p-1)$. $\square$

Prosición 1.4. *Sea p un primo y k un entero positivo. Definimos la función*

$$F_p : \mathbb{Z}_{p^k}^\times \to \mathbb{Z}_{p^{k+1}}^\times \text{ por } F_p(\overline{x}) = \overline{x^p}$$

F_p es un morfismo de grupos. Además si $p \neq 2$, F_p es inyectiva.

Proof. Primero tenemos que verificar que F_p esta bien definida. Sea x un representante de una clase en $\mathbb{Z}_{p^k}$ (digamos $0 \leq x \leq p^k - 1$) entonces $(x+p^k r)^p = x^p + p^{k+1}s$ entonces $(x + p^k r)^p \equiv x^p \bmod (p^{k+1})$.
Para ver que F_p es injectiva, hacemos inducción en k. Si $k = 1$ es claro porque si $x^p \equiv 1 \bmod (p^2) \Rightarrow x^p \equiv 1 \bmod p$, pero $x^p \equiv x \bmod (p)$.
Supongamos cierto para k, y queremos verlo para $k + 1$. Si $x \in \mathbb{Z}^{\times}_{p^{k+1}}$ (digamos $0 \leq x < p^{k+1}$), entonces $x = y + x_k p^k$ donde $0 \leq y < p^k$. Supongamos que $x^p \equiv 1 \bmod p^{k+2}$, entonces

$$1 \equiv (y + x_k p^k)^p \equiv y^p + p^{k+1}y^{p-1}x_k + p^{k+2}w \equiv y^p + p^{k+1}y^{p-1}x_k \bmod (p^{k+1}) \tag{1}$$

Aca estamos usando que $p \neq 2$ (¿ por que?). Si reducimos (1) módulo p^{k+1} obtenemos:

$$1 \equiv y^p \bmod (p^{k+1}) \tag{2}$$

Luego por hipótesis inductiva $y \equiv 1 \bmod (p^k)$, e $y < p^k$ entonces $y = 1$. Si reemplazamos en (1) obtenemos

$$1 \equiv 1^p + p^{k+1}x_k \equiv 1 + p^{k+1}x_k \bmod (p^{k+2})$$

Entonces $x_k \equiv 0 \bmod p$, y $x = 1 + p^k x_k \equiv 1 \bmod (p^{k+1})$. □

Corolario. *Sea p un primo distinto de 2, y g un generador de $\mathbb{Z}^{\times}_{p^2}$, entonces g es un generador de $\mathbb{Z}^{\times}_{p^k}$ para cualquier $k \geq 2$.*

Proof. Hacemos nuevamente inducción en k. Sea $\pi : \mathbb{Z}^{\times}_{p^{k+1}} \to \mathbb{Z}^{\times}_{p^k}$ reducir módulo p^k. Supongamos que $\langle \overline{g} \rangle = \mathbb{Z}^{\times}_{p^k}$, queremos ver que si $\overline{h} \in \mathbb{Z}_{p^{k+1}}$ es tal que $\pi(\overline{h}) = \overline{g}$ entonces $\langle \overline{h} \rangle = \mathbb{Z}^{\times}_{p^{k+1}}$. Como F_p es inyectiva, $\operatorname{ord}(F_p(g)) = \operatorname{ord}(g) = (p-1)p^{k-1}$. Además como $\pi(\overline{h}) = \overline{g}$, $(\overline{h})^p = (\overline{g})^p \bmod p^{k+1}$ (o sea $\operatorname{ord}((\overline{h})^p) = (p-1)p^{k-1}$), entonces $(p-1)p^{k-1} \mid \operatorname{ord}(\overline{h}) \mid (p-1)p^k$. Por hipótesis $k \geq 2$, si $\operatorname{ord}(\overline{h}) = (p-1)p^{k-1} \Rightarrow \operatorname{ord}((\overline{h})^p) = (p-1)p^{k-2}$ lo que es una contradicción. □

Corolario. *Si $p \neq 2$, $\mathbb{Z}_{p^k}$ es cíclico.*

¿ Que pasa con el primo 2?

Ejercicio: $\mathbb{Z}^{\times}_8 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Prosición 1.5. *sea $n \geq 2$ un entero positivo, entonces* $\operatorname{ord}(5) = 2^{n-2}$ *en* $\mathbb{Z}^{\times}_{2^n}$. *Además* $-1 \notin \langle 5 \rangle$.

Proof. Hacemos inducción en n para demostrar que $5^{2^{n-2}} = 1 + 2^n s$ con s impar.

- Si $n = 3$, $5^2 = 1 + 2^3 3$.
- $(5^{2^{k-2}})^2 = 5^{2^{k+1-2}} = (1 + 2^k s)^2 = 1 + 2^{k+1}s + 2^{2k}s^2 = 1 + 2^{k+1}(s + 2^{k-1}s)$. Como $k \geq 2$, $s + 2^{k-1}s$ es par.

□

Corolario. $\mathbb{Z}^{\times}_{2^n} \simeq \mathbb{Z}_{2^{n-2}} \oplus \mathbb{Z}_2$

Proof. Es fácil chequear que el morfismo $\phi : \mathbb{Z}_{2^{n-2}} \oplus \mathbb{Z}_2 \to \mathbb{Z}^{\times}_{2^n}$ dado por $\phi((a, b)) = 5^a(-1)^b$ es un isomorfismo. □