Apuntes de clase

José Antonio de la Rosa Cubero

Teorema 1. *1. Para cada divisor positivo d de n, $\langle x^{n/d} \rangle$ tiene orden d. Por tanto $\langle x^{n/d} \rangle = C_d$.*

2. Sea H un subgrupo propio de C_n. Sea $s = \min\{r \geq 1 : x^r \in H\}$ Entonces $s|n$ y $H = \langle a^s \rangle$.

3. Hay una biyección ($d \mapsto \langle x^{n/d} \rangle$) entre los divisores de n y los subgrupos de C_n.

4. $d_1|d_2$ si y solo si $\langle x^{n/d_1} \rangle \leq \langle x^{n/d_2} \rangle$

Demostración. Puesto que $\mathrm{ord}(x^{n/d}) = \frac{n}{\gcd(n,n/d)} = \frac{n}{n/d} = d$ y se tiene que el grupo es el cíclico de orden d.

En segundo lugar, puesto que $s \in \{r \geq 1 : x^r \in H\}$ tenemos que $x^s \in H$. Entonces tenemos que $\langle x^s \rangle \leq H$. Dividemos m entre s, con lo que $m = sq+t$, $0 \leq t \leq s$. Tenemos que $x^m = x^{sq}x^t$ y que $x \in H$, tenemos que por fuerza $t = 0$. Entonces $m = sq$ con lo que $x^m = x^{sq} \in \langle x^s \rangle$.

Por tanto $\langle x^s \rangle = H$. Puesto que $x^n = 1 \in H$ entonces $s|n$ por el mismo razonamiento anterior.

$\square$

Ejemplo: Describir $\mathrm{Sub}(C_{p^n})$ siendo p un número pimo y mayor o igual que uno.

$$\mathrm{Sub}(C_{p^{n-1}}) = \langle x^{n-k} \rangle$$

Otro ejemplo: Puesto que el orden de S_3 tiene orden 6, sus posibles subgrupos serán de orden $1, 2, 3, 4, 5, 6$. De orden 1 es $\{1\}$ y de orden 6 es $\{S_3\}$. De orden 2 hay tres subgrupos de orden 2 (todos cíclicos por ser 2 primo). Del mismo modo, como todo grupo de orden 3 es cíclico, $\langle (1 \quad 2 \quad 3) \rangle$