EXISTENCIA DE SUBGRUPOS

Queremos ver que el inverso del Teorema de Lagrange se cumple en ciertos casos.

1. Grupos Abelianos

Vamos a comenzar viendo que siempre es cierto para grupos abelianos.

Lema 1.1 (Inverso de Lagrange para abelianos)**.** *Sea $|G| = n$ abeliano. Si $d \mid n$, existe un subgrupo H de G de orden d.*

Demostración. Podemos suponer que G no es cíclico. Vamos a demostrarlo primero para el caso $d = p$ primo, por inducción sobre $n = |G|$. Tomamos un elemento $g \neq e$ de G, y consideramos $N = \langle g \rangle$. Si $p \mid |N|$, por inducción hemos acabado. En otro caso, tenemos que $p \mid |G/N|$, que por inducción da un elemento de orden p en G/N, luego un elemento h de orden pa en G. Pero h^a tiene orden p en G.

El caso general también lo vamos a demostrarlo por inducción en n. Sea $p \mid d$. Tomamos en G un elemento g de orden p. Entonces, consideramos $G/\langle g \rangle$. Como es un grupo de orden n/p, por inducción tiene un subgrupo de orden d/p que levantándolo a G nos da un subgrupo de orden d. □

2. p-grupos

Vamos a ver que para grupos de orden potencia de un primo, los llamados *p-grupos*, también se cumple el inverso del teorema de Lagrange.

Lema 2.1 (Inverso de Lagrange para p-grupos)**.** *Todo p-grupo finito es resoluble y por tanto para cada divisor del orden del grupo existe un subgrupo de ese orden.*

Demostración. Deberíamos encontrar algún subgrupo normal no trivial. Vamos a ver que el centro es no trivial. Si lo fuera, la ecuación de clases de conjugación quedaría

$$p^\alpha = 1 + \text{suma de potencias de } p$$

lo que es imposible porque el lado izquierdo es divisible por p y el derecho no. Así, el centro Z no es trivial. Si $G = Z$ entonces G es abeliano luego soluble. Si $G \neq Z$, entonces por inducción G/Z y Z son resolubles, y por tanto G.

Como G es resoluble, por la parametrización de resolubles tenemos que el subgrupo generado por $a_\alpha, a_{\alpha-1}, \ldots, a_{\alpha-\beta+1}$ tiene orden p^β. □

3. p-SUBGRUPOS DE GRUPOS GENERALES

Vamos a ver que el resultado anterior se extiende a cualquier grupo finito, en el sentido de que para divisores que sean potencias de un primo siempre hay subgrupos de ese orden. Las herramientas para demostrarlo van a ser de nuevo el cociente y la ecuación de clases de conjugación.

Lema 3.1 (Inverso Lagrange para p-subgrupos)**.** *Si G es finito y p^β divide al orden del grupo, entonces existe un subgrupo de G de orden p^β.*

Demostración. Por el resultado anterior, vemos que es suficiente encontrar un p-subgrupo de G maximal, es decir, de orden p^α con $|G| = p^\alpha m$, $p \nmid m$. También podemos suponer que G no es abeliano. Por inducción en $n = |G|$, vamos a ver que podemos encontrar dicho subgrupo maximal

- buscando entre los centralizadores si $p \nmid |Z|$.
- extrayéndolo de un cociente por elementos del centro, cuando $p \mid |Z|$.

Si el centro $p \nmid |Z|$, vamos a ver que uno de los centralizadores $C_G(g), g \in G$ contiene al subgrupo que buscamos. Si existe $C_G(g)$, $g \neq e$, tal que $p^\alpha \mid |C_G(g)|$, como $|C_G(g)| < n$ esto es cierto por inducción. En otro caso tendríamos que $|G/C_G(g)|$ sería múltiplo de p para todo g, luego la ecuación de clases quedaría

$$p^\alpha m = |Z| + \text{múltiplos de } p$$

que no puede ser.

Si $p \mid |Z|$, tomamos un elemento z del centro de orden p, y como $\langle z \rangle \lhd G$ y $|G/\langle z \rangle| < n$, por inducción en $G/\langle z \rangle$ tenemos un p-subgrupo maximal, que levantándolo da un subgrupo maximal de G. □

Este resultado fue demostrado por Sylow en el caso general y por Cauchy en el caso $\alpha = 1$. Por eso, a los p-subgrupos maximales de un grupo G se les llama *p-subgrupos de Sylow*.

4. Ejemplos

Todas las demostraciones que hemos visto pueden usarse como algoritmos para encontrar subgrupos. Por ejemplo, vamos a ver cómo aplicar el último caso al grupo $G = \mathrm{GL}(2, \mathbb{Z}_5)$. Tenemos que $|G| = 4 * (4 * 5 * 6)$. Así, debe tener algún subgrupo de orden $32 = 2^5$. Como

$Z = \{I, 2I, 3I, 4I\}$, tenemos que $P = G/Z$ es un grupo de tamaño $4 * 5 * 6 = 120$, luego debería tener un subgrupo de orden 8. Es sencillo ver que el centro de P es trivial. Así, vamos a mirar entre los centralizadores. Para ello, como $\langle g \rangle \leq C_G(g)$, deberíamos mirar a elementos de orden potencia de dos. Por ejemplo, el elemento

$$h_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

es de orden 2, y vemos que una matriz conmute con h_0 equivale a

$$\begin{pmatrix} a & b \\ -c & -d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} a & -b \\ c & -d \end{pmatrix}.$$

En el cociente, esto nos da

$$C_G(h_0) = \{ \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ x & 0 \end{pmatrix} : x \in \mathbb{Z}_5^\times \}$$

que es de orden 8. Elevándolo a G nos da el subgrupo

$$H = \{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : a, b, c, d \in \mathbb{Z}_5^\times \}.$$

que es de orden 32.