Tema 4.-. Grupos resolubles. Aplicaciones. Caracteres de grupos. Teorema de Cauchy.

4.1. Grupos resolubles.

En esta sección se tratarán las bases de una aplicación fundamental de la teoría de grupos a la resolución de ecuaciones algebraicas. Se probará más adelante que una ecuación es resoluble por radicales si y sólo si un grupo asociado a la ecuación es 'resoluble', concepto que definimos ahora.

DEFINICIÓN 4.1.1.– Un grupo G se dice *resoluble* si existe una cadena finita de subgrupos:

$$\{1\} = G_0 \subset G_1 \subset \ldots G_n = G$$

tales que, para cada $i = 0, \ldots, n-1$:

1. $G_i \lhd G_{i+1}$ y
2. G_{i+1}/G_i es abeliano.

A la anterior cadena, cuando exista, la llamaremos *torre abeliana* de G. EJEMPLO 4.1.2.–

1. Todo grupo abeliano es resoluble.
2. S_3 es resoluble. Basta ver que $1 \lhd A_3 \lhd S_3$ es una torre abeliana de S_3.
3. A_4 es resoluble. Basta ver que $1 \lhd V \lhd A_3$ es una torre abeliana de A_4, donde $V = \{1, (12)(34), (13)(24), (14)(23)\}$.
4. S_4 es resoluble. Basta ver que $1 \lhd V \lhd A_3 \lhd S_3$ es una torre abeliana de S_3.
5. El primer ejemplo de grupo no resoluble es A_5, ya que se conoce que A_5 es simple (ver ejercicio de la relación), por lo que la única cadena posible es $1 \lhd A_5$, pero A_5 no es abeliano: $(12)(34)(345) \neq (345)(12)(34)$.

Veamos ahora algunas propiedades elementales de los grupos resolubles. PROPOSICIÓN 4.1.3.–

1. Todo subgrupo H de un grupo resoluble G es resoluble.
2. Todo cociente G/H de un grupo resoluble G por un subgrupo normal H es resoluble.
3. Si H es un subgrupo normal resoluble de G y G/H es resoluble, entonces G es resoluble.

PRUEBA:

1. Basta cortar una torre abeliana de G por H.
2. Basta aplicar la proyección natural $\pi : G \to G/H$ a una torre abeliana de G.
3. Basta 'pegar' una torre abeliana de H con la imagen inversa por π de una torre abeliana de G/H.

$\square$

Del primer apartado y del último ejemplo se deduce que S_5 tampoco es resoluble.

4.2. Caracteres.

DEFINICIÓN 4.2.1.– Sea G un grupo y k un cuerpo. Se llama *carácter* de G sobre k a un homomorfismo σ de grupos $\sigma : G \to k^*$, donde $k^* = k \setminus \{0\}$ es el grupo multiplicativo del cuerpo k.

DEFINICIÓN 4.2.2.– Los caracteres $\{\sigma_1, \ldots, \sigma_n\}$ de un grupo G sobre k se dicen *dependientes*, si existen $a_1, \ldots, a_n \in k$ no todos nulos, tales que

$$a_1\sigma_1(g) + \ldots + a_n\sigma_n(g) = 0$$

para todo $g \in G$. En otro caso se dicen *independientes*.

TEOREMA 4.2.3.– *Teorema de independencia de caracteres.* (Dedekind) Si G es un grupo, k es un cuerpo y $\{\sigma_1, \ldots, \sigma_n\}$ son caracteres distintos de G sobre k, entonces estos caracteres son independientes.

Demostración. Si $n = 1$ entonces $a_1\sigma_1(g) = 0$ para todo $g \in G$, y como $\sigma_1(g) \in k^*$ se sigue que $a_1 = 0$. Supongamos, por inducción, que $n - 1$ caracteres distintos son independientes, y que para todo $g \in G$

$$a_1\sigma_1(g) + \ldots a_n\sigma_n(g) = 0 \tag{1}$$

para ciertos $a_i \in k$, no todos nulos. Es más, por la hipótesis de inducción, podemos suponer todos los $a_i \neq 0$. Como $\sigma_1 \neq \sigma_n$, existe $g' \in G$ tal que $\sigma_1(g') \neq \sigma_n(g')$. La expresión anterior es válida para todo g. Cambiamos g por $g'g$ y nos queda

$$\begin{aligned} &a_1\sigma_1(g'g) + a_2\sigma_2(g'g) + \ldots + a_{n-1}\sigma_{n-1}(g'g) + a_n\sigma_n(g'g) = 0, \\ &a_1\sigma_1(g')\sigma_1(g) + a_2\sigma_2(g')\sigma_2(g) + \ldots + a_{n-1}\sigma_{n-1}(g')\sigma_{n-1}(g) + a_n\sigma_n(g')\sigma_n(g) = 0 \end{aligned} \tag{2}$$

para todo $g \in G$. Multiplicamos la ecuación (1) por $\sigma_n(g')$ y se la restamos a la ecuación (2). Obtenemos

$$\begin{aligned} &(\sigma_n(g') - \sigma_1(g'))a_1\sigma_1(g) + (\sigma_n(g') - \sigma_2(g'))a_2\sigma_2(g) + \ldots + \\ &(\sigma_n(g') - \sigma_{n-1}(g'))a_{n-1}\sigma_{n-1}(g) = 0 \end{aligned}$$

que se verifica para todo $g \in G$. Pero el primer coeficiente es no nulo, lo que da una relación de dependencia no trivial con $n - 1$, o menos, caracteres. $\square$

COROLARIO 4.2.4.– Sea K un cuerpo y $\psi_1, \ldots, \psi_n$ distintos automorfismos de K. Entonces $\psi_1, \ldots, \psi_n$ son caracteres independientes del grupo K^* sobre K, es decir no hay una combinación lineal no trivial con coeficientes en K de los automorfismos dados.

4.3. Teorema de Cauchy.