ISSN 1853-709X

Fascículo 39

Cursos y seminarios de matemática

Serie A

J. J. Martínez

Tópicos sobre teoría de cuerpos

Departamento de Matemática

Facultad de Ciencias Exactas y Naturales

Universidad de Buenos Aires

2011

Cursos y Seminarios de Matemática – Serie A

Fascículo 39

ISSN 1853-709X (Versión Electrónica)
ISSN 0524-9643 (Versión Impresa)

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria – Pabellón I
(1428) Ciudad de Buenos Aires
Argentina.
http://www.dm.uba.ar
e-mail. secre@dm.uba.ar
tel/fax: (+54-11)-4576-3335

DEPARTAMENTO DE
MATEMATICA
Cursos y Seminarios
Fascículo 39

Tópicos Sobre Teoría de Cuerpos

Juan José Martínez

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
UNIVERSIDAD DE BUENOS AIRES

Ciudad Universitaria - Pabellón I
1428 Buenos Aires, ARGENTINA

TÓPICOS SOBRE TEORÍA DE CUERPOS

Juan José Martínez

Índice

TÓPICOS SOBRE TEORÍA DE CUERPOS 5

1. Introducción 5

2. Bibliografía 5

3. Grupos de permutaciones 6

4. Grupos resolubles 20

5. p-grupos 27

6. Polinomios Simétricos. 29

6.1. El discriminante. 32

7. Grupo de Galois de un polinomio. 36

7.1. Cápsula normal 42

7.2. Extensiones resolubles 43

7.3. Extensiones resolubles por radicales 45

8. Polinomios generales. 51

9. Polinomios con coeficientes racionales de Grupo de Galois simétrico 54

TÓPICOS SOBRE TEORÍA DE CUERPOS

1. Introducción

El presente volumen contiene las Notas del curso "Tópicos sobre teoría de cuerpos", ofrecido como materia optativa en 1976 por el Dr. Juan José Martínez en la Facultad de Ciencias Exactas y Naturales. Se utilizó como fuente los apuntes de una asistente al curso, de modo que seguramente ésta no es la presentación que el Dr. Martínez hubiera aprobado. Sin embargo, la publicación de estas notas sería de utilidad para el estudiante de matemática con orientación hacia el álgebra o la teoría de números.

El material de estas notas complementa el curso de "Teoría de cuerpos" del Dr. Juan José Martínez, publicado en la Serie C de los Trabajos de Matemática de FaMAF, No. 17/95.

Agradezco a Graciela Fernández, Fernando Cukierman y Carlos Sánchez por su interés en el proyecto de publicar las notas de los cursos del Dr. Martínez; a Luisa Gallardo por su dedicación en el tipeado de un manuscrito de díficil lectura; a Inés Pacharoni por su colaboración en la fatigosa correción final.

Nicolás Andruskiewitsch

2. Bibliografía

Bourbaki, *Algébre.* Chapitres V, VI. Hermann, París, 1968.

Jacobson, *Lectures in Abstract Algebra.* Vol III. Springer Verlag, Nueva York, 1975.

Lang, *Algebra.* Springer Verlag, Nueva York, 1975.

Van der Waerden, *Modern Algebra.* Vol. I.

Martínez, *Teoría de Cuerpos.* Trabajos de Matemática, Fa.M.A.F. Córdoba, 1995.

3. Grupos de permutaciones

Sea C un conjunto. El conjunto de aplicaciones de C en C, provisto de la composición usual de aplicaciones, es un semigrupo, cuyo grupo de inversibles se llama el grupo simétrico de C, y se nota $\mathbf{S}(C)$. Los elementos de $\mathbf{S}(C)$, o sea, las biyeccciones de C en sí mismo, se llaman transformaciones, o permutaciones, de C. (Esta última denominación suele reservarse para el caso en que C es finito). Consistentemente, se llama grupo de transformaciones, o grupo de permutaciones, a todo subgrupo de $\mathbf{S}(C)$.

Dada una biyección de conjuntos $\alpha : C \to D$, la aplicación $\mathbf{S}(\alpha) : \mathbf{S}(C) \to \mathbf{S}(D)$ dada por

$$\pi \quad \mapsto \alpha\pi\alpha^{-1},$$

es un morfismo de grupos. Más aún la validez de las fórmulas

$$\mathbf{S}(\beta \circ \alpha) = \mathbf{S}(\beta) \circ \mathbf{S}(\alpha) \quad \text{y} \quad \mathbf{S}(\mathrm{id}_C) = \mathrm{id}_{\mathbf{S}(C)},$$

garantiza que $\mathbf{S}(\alpha)$ es un isomorfismo, cuyo morfismo inverso es $\mathbf{S}(\alpha^{-1})$. Luego $\mathbf{S}$ puede considerarse como un functor de la categoría de isomorfismos de conjuntos en la categoría de isomorfismos de grupos.

Además, dados conjuntos C y D tales que $C \subseteq D$, $\mathbf{S}(C)$ se sumerge canónicamente en $\mathbf{S}(D)$. En efecto, la aplicación $\pi \mapsto \pi'$ definida por

$$\pi'(x) = \begin{cases} \pi(x) & x \in C \\ x & x \in D - C \end{cases}$$

es un monomorfismo de grupos. De esta manera $\mathbf{S}$ puede también considerarse un functor de la categoría de inclusiones de conjuntos[1] en la categoría de monomorfismos de grupos[2]. Las dos posibles asignaciones de morfismos son compatibles en el siguiente sentido: dado un diagrama conmutativo de conjuntos

$$\begin{array}{ccc} C & \xrightarrow{\alpha} & D \\ \downarrow & & \downarrow \\ E & \xrightarrow{\beta} & F \end{array}$$

donde α, β son biyecciones, y las flechas verticales son inclusiones, el diagrama resultante

$$\begin{array}{ccc} \mathbf{S}(C) & \xrightarrow{\mathbf{S}(\alpha)} & \mathbf{S}(D) \\ \downarrow & & \downarrow \\ \mathbf{S}(E) & \xrightarrow{\mathbf{S}(\beta)} & \mathbf{S}(F) \end{array}$$

---

[1] Esta categoría tiene como objetos las inclusiones y como flechas, los diagramas conmutativos como más abajo.

[2] Ver nota anterior.

es conmutativo.

Dado $n \in \mathbb{N}_0$, $\mathbf{S}(\mathbb{I}_n)$ se llama el grupo simétrico de grado n, y se nota $\mathbb{S}_n$. Aquí, $\mathbb{I}_n$ es el conjunto $\{1, 2, \ldots, n\}$. $\mathbb{S}_n$ es un grupo finito de orden $n!$ y el grupo simétrico de cualquier conjunto con n elementos es isomorfo a $\mathbb{S}_n$.

Dada una permutación π de grado n (o sea, $\pi \in \mathbb{S}_n$) se emplea la notación

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

Ejercicios.

i) Escribir la tabla de multiplicar de $\mathbb{S}_3$.

ii) Probar que $\mathbb{S}_n$ no es conmutativo, si $n \geq 3$.

TEOREMA (CAYLEY). Todo grupo G admite una representación fiel en sí mismo; vale decir, G es isomorfo a un subgrupo de $\mathbf{S}(G)$. En particular, si G tiene orden n, G resulta isomorfo a un subgrupo de $\mathbb{S}_n$.

DEMOSTRACIÓN. Se considera a G actuando en sí mismo según la operación

$$G \times G \to G,$$
$$(s, x) \mapsto s.x$$

La representación correspondiente carece de operadores triviales $\neq 1$, de modo que es un monomorfismo. □

Ejercicios.

1. Sea $n \in \mathbb{N}$. Sea A un anillo conmutativo.

i) El conjunto $\mathbb{P}(n, A)$ de matrices de orden n, con coeficientes en A, tales que en cada fila y en cada columna, tienen un único coeficiente que vale 1 mientras que los restantes son 0 (matrices de permutación) es un subgrupo de $GL(n, A)$, isomorfo a $\mathbb{S}_n$.

ii) Si G es un grupo finito de orden n, G resulta isomorfo a un subgrupo de $GL(n, A)$.

2. Sea G un grupo. Haciendo actuar G en sí mismo por conjugación, o sea

$$(s, x) \quad \mapsto \quad s.x.s^{-1},$$

deducir que $\operatorname{Int} G \simeq G/C(G)$. Aquí, $\operatorname{Int} G$ es el grupo de morfismos interiores y $C(G)$ es el centro de G.

Sean $n, r \in \mathbb{N}$. Una permutación π de grado n se dice un ciclo de longitud r, o un r-ciclo, sii existe una sucesión $(i_j)_{1 \leq j \leq r}$ de r elementos distintos de $\mathbb{I}_n$ tal que

$$\pi(i_j) = i_{j+1}, \quad 1 \leq j < r,$$
$$\pi(i_r) = i_1,$$
$$\pi(k) = k \qquad \forall k \in \mathbb{I}_n - \{i_j, 1 \leq j \leq r\}.$$

En tal caso, π se suele representar con la notación $(i_1 i_2 ... i_r)$. Por ejemplo en $\mathbb{S}_5$,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} = (2\,4\,3)$$

En esta notación, un r-ciclo tiene r representaciones:

$$(i_1 i_2 ... i_r) = (i_2 i_3 ... i_r i_1) = ...$$

La permutación identidad es el único 1-ciclo, y tiene n notaciones: $(1), (2), ..., (n)$.

Propiedades. Sean $n, r \in \mathbb{N}$, con $r \leq n$.

I). *El número de r-ciclos de grado n, es* $\frac{1}{r} \prod_{0 \leq i < r} (n - i)$, *si* $r > 1$.

DEMOSTRACIÓN. Cualquier r-ciclo se obtiene en la forma siguiente: se toma un subconjunto C de r elementos de $\mathbb{I}_n$ (el número de tales subconjuntos es $\binom{n}{r}$), y se considera una numeración de C (de las cuales hay $r!$, pues dada una numeración $\gamma_0 : \mathbb{I}_r \to C$, $(\gamma \circ \pi)$, $\pi \in \mathbb{S}_r$, es la familia de tales numeraciones).

Además, si π y π' son ciclos definidos a partir de conjuntos C y C', $\pi = \pi' \Rightarrow C = C'$. En efecto, suponiendo $C \neq C'$, si, por ejemplo, $C \not\subseteq C'$, sea $i \in C - C'$. Luego $\pi(i) \neq i$ pues $i \in C$ y $r > 1$, mientras que $\pi'(i) = i$ pues $i \notin C'$.

Por otra parte, dada una numeración $(i_j)_{1 \leq j \leq r}$ de un tal conjunto C, hay exactamente r numeraciones de C que definen el mismo ciclo. En definitiva, el número de r-ciclos es $\frac{1}{r}\binom{n}{r} r!$. □

II). *El inverso del ciclo $(i_1 i_2 ... i_r)$ es el ciclo $(i_r i_{r-1} ... i_1)$.*

DEMOSTRACIÓN. Sea $\pi = (i_1 i_2 ... i_r)$; o sea

$$\pi(i_j) = i_{j+1}, \quad 1 \leq j < r, \qquad \pi(i_r) = i_1, \qquad \pi(k) = k, \quad k \neq i_j \quad (1 \leq j \leq r).$$

Luego,

$$\pi^{-1}(i_{j+1}) = i_j, \qquad \pi^{-1}(i_1) = i_r, \qquad \pi^{-1}(k) = k, \quad k \neq i_j \quad (1 \leq j \leq r).$$

Es decir, π^{-1} es el ciclo definido por $(i_{r+1-j})_{1 \leq j \leq r}$. □

III). *Dada una permutación π y un ciclo $(i_1 i_2 ... i_r)$,*

$$\pi \circ (i_1 i_2 ... i_r) \circ \pi^{-1} = (\pi(i_1)\, \pi(i_2) ... \pi(i_r)).$$

DEMOSTRACIÓN. Sea $\rho = (i_1 i_2 ... i_r)$. Se tiene

$$(\pi\rho\pi^{-1})(\pi(i_j)) = \pi\rho(i_j) = \pi(i_{j+1}), \quad 1 \leq j < r,$$
$$\pi\rho\pi^{-1}(\pi(i_r)) = \pi\rho(i_r) = \pi(i_1).$$

Supongamos entonces que $k \neq \pi(i_j)$; queremos calcular $\pi\rho\pi^{-1}(k)$.

Pero $k \neq \pi(i_j)$, $1 \leq j \leq r \Rightarrow \pi^{-1}(k) \neq i_j \Rightarrow \rho\pi^{-1}(k) = \pi^{-1}(k) \Rightarrow \pi\rho\pi^{-1}(k) = \pi\pi^{-1}(k) = k$. □

IV). *Todo r-ciclo tiene orden r.*

DEMOSTRACIÓN. Sea $\pi = (i_1 i_2 ... i_r)$. En primer lugar, $\pi^r = (1)$. En efecto, dado $1 \leq j \leq r$,.

$$\pi^r(i_j) = \pi^{r-1}(i_{j+1}) = \pi^{r-2}(i_{j+2}) = \cdots = \pi^{r-k}(i_{j+k}) = \ldots = \pi^j(i_r)$$
$$= \pi^{j-1}(i_1) = \pi^{j-2}(i_2) = \ldots = \pi(i_{j-1}) = i_j.$$

(Se efectúan $(r-j)+(j-1)+1 = r$ pasos).

Dado $s \in \mathbb{N}$, $s < r, \pi^s \neq 1$. En efecto,

$$\pi^s(i_1) = \pi^{s-1}(i_2) = \pi^{s-2}(i_3) = \ldots = \pi(i_s) = i_{s+1} \neq i_1.$$

□

V). *Sean α y β, r-ciclos. Si existe $p \in \mathbb{I}_n$ tal que α y β mueven a p, y $\alpha^k(p) = \beta^k(p)$, para todo $k \in \mathbb{Z}$ (o si se quiere, para todo k tal que $1 \leq k < r$), entonces $\alpha = \beta$.*

DEMOSTRACIÓN. Sean $\alpha = (i_1 i_2 \ldots i_r), \beta = (j_1 j_2 \ldots j_r)$. Se puede suponer $i_1 = j_1 = p$. Luego

$$i_k = \alpha^{k-1}(i_1) = \beta^{k-1}(i_1) = \beta^{k-1}(j_1) = j_k, 1 \leq k \leq r.$$

□

Ejercicio. Si $n \geq 3$, existen 2-ciclos α y β en $\mathbb{S}_n$ tales que $\alpha\beta$ es un 3-ciclo.

Moraleja: Dados dos elementos de un grupo no conmutativo, nada razonable puede decirse del orden del producto en función del orden de los factores.

DEFINICIÓN. Sean π, ρ permutaciones de grado n. Se dice que π y ρ son *disjuntas* sii

$$\forall\, i \in \mathbb{I}_n : \text{ o bien } \pi(i) = i, \text{ o bien } \rho(i) = i.$$

Dado un conjunto de permutaciones, se dice que está formado por permutaciones disjuntas cuando lo son dos a dos.

Propiedades.

I). *Si π y ρ son permutaciones disjuntas, $\pi\rho = \rho\pi$.*

II). *Dados ciclos $\alpha = (i_1 i_2 \dots i_r)$, $\beta = (j_1 j_2 \dots j_s)$, de longitudes > 1, se verifica que α y β son disjuntas si y sólo si $\{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\} = \emptyset$.*

III). *Dada una permutación π, presentada en la forma $\pi = \prod_{i=1}^{m} \alpha_i$, donde $(\alpha_i)_{i=1}^{m}$ es una sucesión de ciclos disjuntos; si α_i tiene longitud r_i, entonces el orden de π es $[r_1; r_2; \dots; r_m]$, el mínimo común múltiplo de los r_j.*

DEMOSTRACIÓN.

I). Sea $i \in \mathbb{I}_n$. Supongamos que $\pi(i) \neq i$. Luego $\quad \rho(i) = i \Rightarrow \pi\rho(i) = \pi(i)$. Pero

$$\rho\pi(i) = \pi(i) \Leftarrow \pi(\pi(i)) \neq \pi(i) \Leftarrow \pi(i) \neq i.$$

Por otro lado, si $\pi(i) = i$, entonces $\rho\pi(i) = \rho(i)$. Ahora, si $\pi\rho(i) \neq \rho(i) \Rightarrow \rho(\rho(i)) = \rho(i) \Rightarrow \rho(i) = i \Rightarrow \pi\rho(i) = \pi(i) = i = \rho(i)$. Absurdo.

II). Dado $i \in \mathbb{I}_n$, $\alpha(i) = i$ o $\beta(i) = i \Leftrightarrow i \notin \{i_1, \dots, i_r\}$ o $i \notin \{j_1, \dots, j_s\} \Leftrightarrow i \notin \{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\}$.

III). Sea $r = [r_1; r_2; \dots; r_m]$. Ante todo, como $(\alpha_i)_{i=1,\dots,m}$ es una sucesión de permutaciones que conmutan, resulta

$$\pi^k = \prod \alpha_i^k, \ \forall k \in \mathbb{Z}, \text{ con lo cual } \pi^r = (1).$$

Por otra parte, con la notación $M(\pi) = \{i \in I_n : \pi(i) \neq i\}$, valen las fórmulas

$$M(\prod_{i=1}^{n} \pi_i) \subseteq \bigcup_{i=1}^{n} M(\pi_i), \qquad M(\pi^{-1}) = M(\pi).$$

De allí $M(\pi^k) \subseteq M(\pi)$, $\forall k \in \mathbb{Z}$. En nuestro caso, $M(\pi^k) \subseteq \bigcup_{i=1}^{m} M(\alpha_i^k)$ (esta inclusión, para $k = r$, da nuevamente que $\pi^r = (1)$); pero, en realidad, vale la igualdad. En efecto,

$$p \in M(\alpha_i^k) \Rightarrow p \in M(\alpha_i) \overset{\alpha_i \text{ ciclo}}{\Longrightarrow} \alpha_i^k(p) \in M(\alpha_i)$$
$$\Rightarrow \alpha_i^k(p) \notin M(\alpha_j^k), j \neq i, \Rightarrow \pi^k(p) = \prod_{j \neq i} \alpha_j^k(\alpha_i^k(p)) = \alpha_i^k(p) \neq p.$$

Luego, aplicando la igualdad,

$$\pi^k = (1) \Rightarrow \alpha_i^k = (1) \quad \forall i \Rightarrow r_i | k \ \forall i \Rightarrow r | k.$$

□

Ejercicio. Sea π una permutación de grado n. Se dice que π es *regular* sii $\pi = (1)$ o π carece de puntos fijos y π es producto de ciclos disjuntos de la misma longitud. Probar que π es regular si y sólo si π es una potencia de un n-ciclo.

Ejemplo.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 3 & 1 & 2 & 9 & 4 & 6 & 8 \end{pmatrix} = (174)\,(25)\,(3)\,(698).$$

TEOREMA. Toda permutación se escribe como producto de ciclos disjuntos, de longitud > 1, en forma unívoca, salvo el orden de los factores.

DEMOSTRACIÓN. Sea π una permutación de grado n, y sea G el subgrupo generado por π. G actúa en $\mathbb{I}_n$ como subgrupo de $\mathbb{S}_n$, vale decir a partir de la representación definida por la inclusión. Puede considerarse $\mathbb{I}_n/G$.

Dado cualquier $C \in \mathbb{I}_n/G$, existe $i \in \mathbb{I}_n$ tal que

$$C = \{\pi^j(i) : j \in \mathbb{Z}\}.$$

Tomando $m = \text{mín}\,\{j \in \mathbb{N} : \pi^j(i) = i\}$, resulta que $(\pi^j(i))_{0 \le j < m}$ es una numeración de C (notar que $m = \operatorname{card} C$).

Sea $\alpha_C = (i, \pi(i), \ldots, \pi^{m-1}(i))$. Notar la buena definición de α_C : si $i' \in C$, existe un (único) $j \in \mathbb{Z}$, $0 \le j < m : i' = \pi^j(i)$, de donde el ciclo α'_C, definido a partir de i', o sea por $(\pi^k(i'))_{0 \le k < m}$ coincide con α_C. En efecto,

$$\begin{aligned} \alpha'_C &= (\pi^j(i), \pi^{j+1}(i), \ldots, \pi^{j+k-1}(i), \ldots, \pi^{m-1}(i), \ldots, \pi^{m+j-1}(i)) \\ &= (\pi^j(i), \ldots, \pi^{m-1}(i), i, \pi(i), \ldots, \pi^{j-1}(i)) = \alpha_C. \end{aligned}$$

Ahora, (α_C), $C \in \mathbb{I}_n/G$, es una familia de ciclos disjuntos, y además $\pi = \prod_C \alpha_C$, sobre los $C \in \mathbb{I}_n/G$. En efecto, para todo $i \in \mathbb{I}_n$, existe un único $D \in \mathbb{I}_n/G$ tal que $i \in D$. Luego

$$\prod_C \alpha_C(i) = \alpha_D \prod_{C \neq D} \alpha_C(i)) = \alpha_D(i),$$

ya que $C \neq D$ implica $i \notin C$, y por ende $\alpha_C(i) = i$. Pero si $i \in D$, entonces

$$\alpha_D = (i, \pi(i), \ldots, \pi^{m-1}(i)),$$

con $m = \operatorname{card} D$. Luego $\alpha_D(i) = \pi(i)$.

De modo que, si $\mathcal{C} = \{C \in \mathbb{I}_n/G : \operatorname{card} C > 1\}$, $(\alpha_C)_{C \in \mathcal{C}}$ es una flia de ciclos disjuntos, de longitud > 1, tal que $\pi = \prod_{C \in \mathcal{C}} \alpha_C$.

Veamos la unicidad. Sean $(\alpha_i)_{i=1}^r$, $(\beta_j)_{j=1}^s$ sucesiones de ciclos disjuntos, de longitud > 1, tales que $\pi = \prod_{i=1}^{r} \alpha_i = \prod_{j=1}^{s} \beta_j$. Suponiendo $r \leq s$, se procede por inducción en s. El caso $s = 0$ es trivial. Supongamos entonces que $s > 0$. Sea $u \in \mathbb{I}_s$; sea $p \in \mathbb{I}_n$ un punto móvil de β_u. Luego, p es movido por $\prod \beta_j$ (por ser los β_j disjuntos). Como $\prod \beta_j = \prod \alpha_i$, se tiene que p es movido por α_t, para algún $t \in \mathbb{I}_r$. , se tiene que α_t y β_u mueven a p, y $\alpha_t^k(p) = \pi^k(p) = \beta_u^k(p)$, para todo $k \in \mathbb{Z}$. Luego $\alpha_t = \beta_u$. Cancelando,

$$\prod_{\substack{1 \leq i \leq r, \\ i \neq t}} \alpha_i = \prod_{\substack{1 \leq j \leq s, \\ j \neq u}} \beta_j.$$

La unicidad sigue así por recurrencia. □

COROLARIO. Si p es un número primo, los elementos de orden p en $\mathbb{S}_n$ son los productos no vacíos, de p-ciclos disjuntos. En particular, los elementos de orden p en $\mathbb{S}_p$, son los p-ciclos.

DEMOSTRACIÓN. Dada $\pi \in \mathbb{S}_n$, $\pi = \prod_{i=1}^{m} \alpha_i$, donde $(\alpha_i)_{i=1}^m$ es una sucesión de ciclos disjuntos, y α_i tiene longitud $r_i > 1$, $(1 \leq i \leq m)$. Así,

$$\operatorname{ord} \pi = p \Longleftrightarrow [r_1; \ldots; r_m] = p \Longleftrightarrow r_i = p \text{ para todo } i,\ 1 \leq i \leq m.$$

□

OBSERVACIÓN. Existen elementos de orden p en $\mathbb{S}_n \Longleftrightarrow$ existen p-ciclos de grado $n \Longleftrightarrow p \leq n \Longleftrightarrow p | n!$.

Ejercicios.

1. Escribir la siguiente permutación como producto de ciclos disjuntos:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 6 & 1 & 7 & 3 & 4 & 9 & 8 \end{pmatrix}.$$

2. Sea π una permutación de grado n, y sea G el subgrupo generado por π, que actúa en $\mathbb{I}_n$ como subgrupo de $\mathbb{S}_n$. Traducir en $\mathbb{I}_n/G$ las siguientes proposiciones:

i) π es un r-ciclo.

ii) π es regular.

3. Sea G un grupo finito de orden n. Si ρ es una representación de Cayley de G, en $\mathbb{I}_n$ entonces ρ_s es una permutación regular, $\forall s \in G$. (Dada una numeración de G, la representación de Cayley asociada es la representación deducida de $G \to \mathbf{S}(G) \simeq \mathbb{S}_n$).

DEFINICIÓN. Una permutación π de grado n se dice una *transposición* sii es un 2-ciclo. Vale decir, si existen $i, j \in \mathbb{I}_n$, $i \neq j$, tales que

$$\pi(i) = j, \qquad \pi(j) = i, \qquad \pi(k) = k, \quad \text{si } k \notin \{i, j\}.$$

TEOREMA. Toda permutación se escribe como producto de transposiciones.

Equivalentemente, el conjunto de transposiciones de grado n es un sistema de generadores de $\mathbb{S}_n$. Este sistema tiene $\dfrac{n(n-1)}{2}$ elementos.

DEMOSTRACIÓN. Basta verificarlo para un ciclo $(i_1\, i_2, \ldots, i_r)$, lo que haremos por inducción en r. Siendo el caso $r = 1$ trivial, podemos suponer $r > 1$. Pero $(i_1\, i_2, \ldots, i_r) = (i_1\, i_3, \ldots, i_r)(i_1\, i_2)$. □

Explícitamente, un r-ciclo se escribe como producto de $r-1$ transposiciones:

$$(i_1\, i_2, \ldots, i_r) = \prod_{0 \leq j \leq r-2} (i_1\, i_{r-j}) = (i_1\, i_r)(i_1\, i_{r-1}), \ldots (i_1\, i_2)$$

Ejercicio.

Dado un 3-ciclo de grado n, por ejemplo (123), escribirlo como:

i) Producto de 2 transposiciones, en 2 formas distintas. ¿ Conmutan los factores?

ii) Producto de 4 transposiciones sin 2 factores consecutivos iguales, para $n > 3$.

Extraer conclusiones.

PROPOSICIÓN. $\mathbb{S}_n$ admite los siguientes sistemas de generadores:

(i) Las $n-1$ transposiciones (12), (13), ... , $(1n)$.

(ii) las $n-1$ transposiciones (12) (23), ... , $(n-1, n)$.

(iii) los ciclos (12) y $(12\ldots n)$.

DEMOSTRACIÓN. (i). Sea G el subgrupo de $\mathbb{S}_n$ generado por $(1i)$, $2 \leq i \leq n$. Basta verificar, que $\forall i, j, i \neq j$, la transposición $(ij) \in G$. Esto es claro si $i = 1$ o $j = 1$. Suponiendo $i, j > 1$, $(ij) \in G$ pues $(ij) = (1i)\,(1j)\,(1i)$, ya que $\pi(i_n, \ldots, i_1)\pi^{-1} = (\pi(i_1), \ldots, \pi(i_n))$.

(ii). Ahora, sea G el subgrupo de $\mathbb{S}_n$ generado por $(i-1\ i)$, $2 \leq i \leq n$. En virtud de *(i)*, como $(1\,2) \in G$, argumentando por inducción, basta ver que si $(1\ i) \in G$, entonces $(1\, i+1) \in G$, para todo $i < n$.

En efecto,

$$(1\ i+1) = (1i)(i\ i+1)(1i).$$

(iii). Sea G el subgrupo generado por (12) y $(12, \ldots, n)$. Nuevamente, argumentando por inducción, basta verificar, gracias a *(ii)*, que

$$(i-1\ i) \in G \overset{?}{\Rightarrow} (i\ i+1) \in G, \quad \forall i,\ 2 \leq i < n.$$

Pero $(i\ i+1) = (1\,2\,\ldots n)(i-1\ i)(1\,2,\ldots,n)^{-1}$. $\square$

Sea π una permutación de grado n, y sea t

$$t = \prod_{1\le i<j\le n} (j-i).$$

Tomando $t_\pi = \prod_{1\le i<j\le n} (\pi(j)-\pi(i))$, resulta $t_\pi = \chi(\pi).t$, donde $\chi(\pi) = (-1)^{\nu_\pi}$ y

$$\nu_\pi = \text{card}\{(i,j), 1 \le i < j \le n \text{ y } \pi(i) > \pi(j)\}.$$

En efecto,

$$t_\pi = \prod_{\pi(i)<\pi(j)} (\pi(j)-\pi(i)) \prod_{\pi(i)>\pi(j)} (\pi(j)-\pi(i)) = \chi(\pi) \prod_{\pi(i)<\pi(j)} (\pi(j)-\pi(i)) \prod_{\pi(i)>\pi(j)} (\pi(i)-\pi(j)).$$

Sea $C = \{(i,j),\ 1 \le i < j \le n\}$ y sea $\alpha : C \to C$

$$\alpha(i,j) = \begin{cases} (\pi(i),\ \pi(j)) & \text{si } \pi(i) < \pi(j) \\ (\pi(j), \pi(i)) & \text{si } \pi(i) > \pi(j) \end{cases}$$

α es inyectiva. En efecto, si $\alpha(i,j) = \alpha(i',j')$ entonces $(\pi(i),\pi(j)) = (\pi(j'),\pi(i'))$ pues los otros casos son imposibles; luego $i = j'$ y $j = i'$, de donde $j' = i < j = i'$, absurdo.

Luego α es biyectiva, ergo

$$t_\pi = \chi(\pi) \prod_{(i,j)\in C} (\alpha(i,j)_2 - \alpha(i,j)_1) = \chi(\pi) \prod_{(i,j)\in C} ((i,j)_2 - (i,j)_1) = \chi(\pi)t.$$

Notaciones.

ν_π se llama el número de inversiones de π y $\chi(\pi)$ se dice la signatura de π. La permutación π se dice par (resp., impar), sii ν_π es un número par (resp, impar); o sea, $\chi(\pi) = 1$ (resp., -1).

Generalizando la fórmula anterior, si $(x_i)_{1\le i\le n}$ es una sucesión de elementos en un anillo conmutativo A, entonces

$$\prod_{i<j}(x_{\pi(j)} - x_{\pi(i)}) = \chi(\pi) \prod_{i<j}(x_j - x_i).$$

Por ejemplo, si se considera la sucesión $(X_i)_{i=1}$ en $A[X_1,\ldots,X_n]$, $\widehat{\pi}$ es el automorfismo de $A[X_1,\ldots,X_n]$ definido por π y $g = \prod_{i<j}(X_j - X_i)$, entonces

$$\widehat{\pi}(g) = \chi(\pi).g$$

OBSERVACIÓN. Si $\alpha : I \to J$ es cualquier función, denotamos por $\widehat{\alpha} : A[X_i]_{i\in I} \to A[X_j]_{j\in J}$ al único morfismo de álgebras tal que $\widehat{\alpha}(X_i) = X_{\alpha(i)}$.

PROPOSICIÓN. El conjunto $\mathbb{A}_n$ de permutaciones pares de rango n es un subgrupo normal de $\mathbb{S}_n$, llamado el grupo alternado de grado n. Además, si $n > 1$, el índice de A_n es 2, y en consecuencia, el orden de $\mathbb{A}_n$ es $\frac{n!}{2}$.

DEMOSTRACIÓN. Dadas $\pi, \rho \in \mathbb{S}_n$, considerando la sucesión $(\rho_i)_{1\leq i\leq n}$ en el anillo $\mathbb{Z}$ resulta

$$\prod_{i<j}(\rho_{\pi(j)} - \rho_{\pi(i)}) = \chi(\pi).\prod_{i<j}(\rho_j - \rho_i)$$

O sea:

$$t_{\rho\pi} = \chi(\pi).t_\rho = \chi(\pi).\chi(\rho).t$$

Luego $\chi(\rho\pi) = \chi(\rho)\chi(\pi)$.

Ergo $\chi : \mathbb{S}_n \to \mathbb{G}_2 = \{1, -1\}$ es un morfismo de grupos, cuyo núcleo es $\ker \chi = \mathbb{A}_n$. Así, $\mathbb{A}_n$ es normal. Si $n > 1$, χ es un epimorfismo (con lo cual $\mathbb{S}_n/\mathbb{A}_n \simeq \mathbb{G}_2$). Por ejemplo (12) es una permutación impar pues $\nu_{(12)} = 1$. □

Ejercicios.

1. $\mathbb{S}_n$ es isomorfo a un subgrupo de $\mathbb{A}_{n+2}$.

2. Si G es un grupo de permutaciones de grado n, que contiene una permutación impar, entonces el orden de G es par y exactamente la mitad de sus elementos son permutaciones impares.

TEOREMA. Una permutación es par si y sólo si se escribe como producto de un número par de transposiciones.

DEMOSTRACIÓN. Basta verificar que cualquier transposición es impar, pues dada una permutación π presentada como producto de transposiciones $\pi = \prod_{i=1}^{n} \tau_i$, resulta $\chi(\pi) = \prod \chi(\tau_i)$.

Suponiendo que existan i, j, $i \neq j$ tales que $(ij) \in A_n$, si π es una permutación tal que $\pi(i) = 1$, $\pi(j) = 2$, entonces $(12) = \pi(ij)\pi^{-1} \in \mathbb{A}_n$. Absurdo pues (12) es impar. □

COROLARIO. El número de factores en cualquier factorización de una permutación en transposiciones es siempre par, o siempre impar. O sea, si $(\tau_i)_{i=1}^{r}$ y $(\omega_j)_{j=1}^{s}$ son sucesiones de transposiciones tales que

$$\prod \tau_i = \prod \omega_j \Rightarrow r \equiv s \mod 2.$$

COROLARIO. Un r-ciclo es par (resp. impar) si y sólo si r es impar (resp. par).

Ejercicio.

Sea A un anillo conmutativo, de característica $\neq 2$. Si a es la matriz de una permutación π, sobre A, entonces det $a = 1$ (resp det a = - 1) si y sólo si π es par (resp, impar).

Vale decir, se tiene $\mu : \mathbb{S}_n \longrightarrow GL(n, A) \xrightarrow{\det} A$, donde $\mu(\pi)e_i = e_{\pi(i)}$, de modo que $\chi = \det \mu$.

PROPOSICIÓN. Toda permutación par es producto de 3-ciclos. Equivalentemente, el conjunto de 3-ciclos de grado n es un sistema de generadores de $\mathbb{A}_n$. Este sistema tiene $\dfrac{n(n-1)(n-2)}{3}$ elementos.

DEMOSTRACIÓN. Basta verificarlo para un producto de 2 transposiciones. En efecto,

$$(ij)(ij) = 1, \qquad (ij)(jk) = (ijk), \qquad (ij)(kl) = (kil)(ijk).$$

□

PROPOSICIÓN. $(12i)$, $3 \leq i \leq n$ es una familia de generadores de $\mathbb{A}_n$.

DEMOSTRACIÓN. Sea G el subgrupo de $\mathbb{A}_n$ generado por $(12i)$, $3 \leq i \leq n$. Basta ver que G contiene cualquier 3-ciclo γ. Se procede por casos:

i) Si γ mueve a 1 y a 2: Entonces existe $i > 2$ tal que $\gamma = (12i)$ o $\gamma = (1i2)$. Pero $(1i2) = (12i)^2$.

ii) Si γ mueve a 2 y no a 1: Entonces existen $i, j > 2$, $i \neq j$ tales que $\gamma = (2ij)$. Pero

$$(2ij) = (12i)(12j)(12i)^{-1}.$$

iii) Si γ mueve a 1 y no mueve a 2: Entonces existen $i, j > 2$, $i \neq j$ tales que: $\gamma = (1ij) = (ij1) = (12i)(2ji)(12i)^{-1}$. Luego por ii), $\gamma \in G$.

iv) Si γ no mueve a 1 ni a 2: Sean $i, j, k > 2$ $i \neq j \neq k$, tales que $\gamma = (ijk)$; pero entonces $\gamma = (12i)(2jk)(12i)^{-1}$. □

Ejercicio. Si n es impar, $\mathbb{A}_n$ está generado por los ciclos (1 2 3) y $(12\ldots n)$; si n es par, por (1 2 3) y $(23\ldots n)$.

DEFINICIÓN. Se llama *estructura cíclica* de una permutación π de grado n a la sucesión $(c_i)_{i=2}^n$ donde c_i es el número de i-ciclos de la factorización de π (como producto de ciclos disjuntos de longitud > 1).

TEOREMA. Dos permutaciones π y ρ son conjugadas si y sólo si tienen igual estructura cíclica.

DEMOSTRACIÓN. *Necesidad.* Sea σ una permutación tal que

$$\sigma\pi\sigma^{-1} = \rho,$$

y sea $(\gamma_i)_{1\leq i\leq m}$ una sucesión de ciclos disjuntos de longitud > 1, tal que $\pi = \prod_{i=1}^{m}\gamma_i$. Luego

$$\rho = \prod_i \sigma\gamma_i\sigma^{-1}.$$

Pero $(\sigma\gamma_i\sigma^{-1})_i$ es una sucesión de ciclos disjuntos de longitud > 1; más aún, γ_i y $\sigma\gamma_i\sigma^{-1}$ tienen igual longitud.

Notar que si γ es un ciclo definido a partir de un conjunto C, $\sigma\gamma\sigma^{-1}$ es un ciclo definido a partir de $\sigma(C)$, pues

$$\sigma(i_1, i_2, \ldots, i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r)),$$

con lo cual $\operatorname{long}\gamma = \operatorname{long}\sigma\gamma\sigma^{-1}$.

Además, si γ' es un ciclo definido a partir de C', γ y γ' disjuntos $\Longrightarrow$ $\sigma\,\gamma\,\sigma^{-1}$ y $\sigma\gamma'\sigma^{-1}$ son disjuntos.

Suficiencia. Sean $\pi = \prod_{i=1}^{m}\gamma_i$, $\rho = \prod_{i=1}^{m}\gamma_i'$, las descomposiciones cíclicas de π y ρ. Notar que $m = \sum c_i$. Renumerando convenientemente, puede suponerse $\operatorname{long}\gamma_i = \operatorname{long}\gamma_i'$. Sea $\gamma_i = (p_{i_1}\, p_{i_2}\ldots p_{i_{l_i}})$, $\gamma_i' = (p'_{i_1}\, p'_{i_2}\ldots p'_{i_{l_i}})$. Notemos $F(\pi) = \{i \in \mathbb{I}_n : \pi(i) = i\}$; de modo que $\operatorname{card} F(\pi) = \operatorname{card}(\mathbb{I}_n - M(\pi)) = \operatorname{card}(\mathbb{I}_n - \bigcup M(\gamma_i)) = n - \sum_i ic_i$.

Sea β una biyección de $F(\pi)$ en $F(\rho)$ y sea σ la permutación definida por

$$\sigma(p_{i_j}) = p'_{i_j}, \qquad \sigma(q) = \beta(q), \quad q \in F(\pi).$$

Luego $\sigma\gamma_i\,\sigma^{-1} = \gamma_i'$, con lo cual $\sigma\,\pi\,\sigma^{-1} = \rho$. □

PROPOSICIÓN. Sea p un número primo. Si G es un grupo de permutaciones de grado p que contiene una transposición y un p-ciclo, entonces $G = \mathbb{S}_p$.

DEMOSTRACIÓN. Sea $(ij) \in G$. Si $\nu \in G$ es un p-ciclo, entonces ν mueve todos los índices. Luego ν admite una representación $(i_1, i_2, \ldots, i_p)$ tal que $i_1 = i$. Además, si k es el índice tal que $i_k = j$, entonces $\nu^{k-1}(i) = j$. Pero ν^{k-1} es un p-ciclo pues $\nu^{k-1} \neq 1$ (recordar que los p-ciclos de grado p, están caracterizados como los elementos de orden p); que p sea primo es esencial, considerar por ejemplo $(1234)^2 = (13)(24)$.

Por lo tanto no hay inconveniente en suponer que $\nu = (i_1 i_2, \ldots, i_p)$ con $i_1 = i, i_2 = j$. En consecuencia, no sólo (ij) es conjugado con (12) y γ es conjugado con $(12\ldots p)$ sino que existe una misma permutación π que realiza ambas conjugaciones:

$$\pi(ij)\pi^{-1} = (12), \qquad \pi\gamma\pi^{-1} = (12\ldots p).$$

Basta tomar π que satisfaga: $\pi(i_k) = k$, $1 \leq k \leq p$.

Por lo tanto $(12), (12\ldots p) \in \pi G\pi^{-1}$, de donde $\pi G\pi^{-1} = \mathbb{S}_p$, o sea $G = \mathbb{S}_p$. □

LEMA. Sea $n \in \mathbb{N}$. Si G es un subgrupo normal de $\mathbb{A}_n$ que contiene un 3-ciclo, entonces $G = \mathbb{A}_n$.

DEMOSTRACIÓN. Como $\mathbb{A}_n$ es un subgrupo normal de $\mathbb{S}_n$, reemplazando G por un conjugado (en $\mathbb{S}_n$), no hay inconveniente en suponer que $(123) \in G$. En efecto, si $(ijk) \in G$, existe una permutación π tal que $\pi(ijk)\pi^{-1} = (123)$, con lo cual $(123) \in \pi G \pi^{-1} \subseteq \pi \mathbb{A}_n \pi^{-1} = \mathbb{A}_n$.

Ante todo $(213) = (123)^2 \in G$. Para $3 < i \leq n$, $(12i) = \pi(213)\pi^{-1}$, tomando $\pi = (12)(3i) \in \mathbb{A}_n$. Con esto $(12i) \in G$, para todo i. □

Ejercicios.

1. Probar que

(i) El número de permutaciones de grado n con estructura cíclica $(2, 0, \ldots, 0)$ es

$$\frac{n(n-1)(n-2)(n-3)}{8}.$$

(ii) El número de permutaciones de grado n con estructura cíclica $(1, 1, 0, \ldots, 0)$ es

$$\frac{n(n-1)(n-2)(n-3)(n-4)}{6}.$$

2. Clasificar las permutaciones de grado n por su estructura cíclica, indicando número, orden y paridad para $n = 2, 3, 4$, y 5.

3. (i) Escribir explícitamente los elementos de $\mathbb{A}_4$.

(ii) Verificar que $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ es un subgrupo normal de $\mathbb{S}_4$, contenido en $\mathbb{A}_4$. V se llama *Vierergruppe de Klein.*

(iii) $W = \{(1), (12)(34)\}$ es un subgrupo normal de V; pero W no es normal considerado como subgrupo de $\mathbb{A}_4$.

Conclusiones. 1) $\mathbb{A}_4$ no es simple. 2) La normalidad de subgrupos no es transitiva.

TEOREMA. $\mathbb{A}_n$ es un grupo simple si y sólo si $n = 3$ o $n > 4$.

DEMOSTRACIÓN. Lo único no trivial es verificar que $\mathbb{A}_n$ es simple, para $n > 4$. Por el lema, basta verificar que si G es un subgrupo normal no trivial de $\mathbb{A}_n$, entonces G contiene un 3-ciclo.

Sea $\pi \in G, \pi \neq 1$, una permutación tal que su número m de puntos móviles es mínimo. Por supuesto, $m \geq 3$, y veremos que $m \not> 3$. Considerando la descomposición cíclica de π, todos los factores son de longitud 2, o bien existe un factor de longitud > 2. En el primer caso, el número de factores es par, con lo cual la descomposición cíclica de π adopta alguna de las formas siguientes:

1, i) $\pi = (i_1\, i_2)\,(i_3\, i_4)$.

1, ii) $\pi = (i_1\, i_2)\,(i_3\, i_4)\,(i_5\, i_6).\rho,\ \rho \neq 1$.

En el segundo caso, $\pi = (i_1 i_2 \ldots, i_r).\rho$, con $r \geq 3$. Además, suponiendo $m > 3$, para $\rho \neq 1$, resulta $r \geq 5$.

En definitiva, la descomposición cíclica de π adopta una de las formas siguientes:

2, i) $\pi = (i_1\, i_2\, i_3\, i_4\, i_5 \ldots i_r)\tau\ ,\ \ r \geq 5$

2, ii) $\pi = (i_1\, i_2\, i_3\, i_4)\,(i_5 \ldots i_r)\tau\ ,\ \ r > 5$

2, iii) $\pi = (i_1\, i_2\, i_3)\,(i_4\, i_5 \ldots i_r)\tau\ ,\ \ r \geq 5.$

Ahora, sea $\sigma = (i_3 i_4 i_5)$; está bien definido salvo en 1, i). Allí se escoje $i_5 \neq i_j$. $1 \leq j < 5$. Esto puede hacerse pues $n > 4$. Sea $\pi' = \sigma\pi\sigma^{-1}$, $\pi' \in G$ pues G normal en A_n. Explícitamente

1, i)' $\pi' = (i_1\, i_2)\,(i_4\, i_5)$

1, ii)' $\pi' = (i_1\, i_2)\,(i_4\, i_5)(i_3\, i_6).\rho$

2, i)' $\pi' = (i_1\, i_2\, i_4\, i_5\, i_3, \ldots, i_r)\tau$

2, ii)' $\pi' = (i_1\, i_2\, i_4\, i_5)(i_3, \ldots, i_r).\tau$

2, iii)' $\pi' = (i_1\, i_2\, i_4)(i_5 i_3, \ldots, i_r)\tau$

Ante todo $\pi' \neq \pi$ pues

$$\left.\begin{array}{l}1,\text{i)}\\ 1,\text{ ii)}\end{array}\right\}\ \pi(i_4) = i_3, \quad \pi'(i_4) = i_5;$$

$$\left.\begin{array}{l}2,\text{i)}\\ 2,\text{ ii)}\\ 2,\text{ iii)}\end{array}\right\}\ \pi(i_2) = i_3, \quad \pi'(i_2) = i_4.$$

Además $\pi'\pi^{-1} \neq 1$, y $\pi'\pi^{-1} \in G$. La demostración se completa observando que $\pi'\pi^{-1}$ mueve menos de m puntos. En efecto, si un punto es movido por $\pi'\pi^{-1}$, entonces es movido por π^{-1} (o sea por π) o bien por π', esto es por π, excluyendo el caso 1, i). Pero por ejemplo i_2 es movido por π y no es movido por $\pi'\pi^{-1}$. En el caso 1 i), $\pi'\pi^{-1}$ mueve a lo sumo, i_3, i_4, i_5. Pero $m > 3$, y el teorema sigue. □

PROPOSICIÓN. Los únicos subgrupos normales de $\mathbb{S}_n$ son 1, $\mathbb{A}_n$ y $\mathbb{S}_n$, si y sólo si, $n \neq 4$.

DEMOSTRACIÓN. La necesidad es clara: considerar el Vierergruppe. La suficiencia también lo es para $n = 1, 2$; con lo cual puede suponerse $n = 3$ o $n > 4$, o sea que $\mathbb{A}_n$ es simple. Si G es un subgrupo normal de $\mathbb{S}_n$, como $G \cap \mathbb{A}_n$ es un subgrupo normal de $\mathbb{S}_n$, $\mathbb{A}_n \subseteq G$ o bien $G \cap \mathbb{A}_n = 1$. Si $\mathbb{A}_n \subseteq G$, entonces $G = \mathbb{A}_n$ o $G = \mathbb{S}_n$ pues $(\mathbb{S}_n : \mathbb{A}_n) = 2$.

Si $G \cap \mathbb{A}_n = 1$, suponiendo $G \neq 1$, resulta que G tiene orden 2, por la misma razón. Sin embargo, los subgrupos de orden 2 de $\mathbb{S}_n$ no pueden ser normales. Basta ver que si $\pi \in \mathbb{S}_n$ tiene orden 2, o sea π es un producto no vacío de transposiciones disjuntas, entonces π tiene un conjugado π', distinto de π. En efecto:

Si $\pi = (ij)$ tomo $\pi' = (ik)$, con $k \neq i, j$ $(n \geq 3)$.

Si π contiene las transposiciones (ij) y (kl), se define π' reemplazándolas por (ik) y (jl). Notar que π es un conjugado de π por tener la misma estructura cíclica. □

4. Grupos resolubles

DEFINICIÓN. Se llama *serie normal* de un grupo G a toda sucesión finita $(G_i)_{0\leq i\leq n}$ de subgrupos de G, tal que G_{i+1} es normal en G_i, $0 \leq i < n$, $G_0 = G$; $G_n = 1$

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1.$$

Los *factores* de la serie son los grupos G_i/G_{i+1}; $0 \leq i < n$. La *longitud* de la serie es el número de índices i, $0 \leq i \leq n$, tales que $G_i \neq G_{i+1}$. (O sea, el i-ésimo factor G_i/G_{i+1} es no trivial).

DEFINICIÓN. Se llama serie de resolubilidad de un grupo G a toda serie normal de G cuyos factores son grupos abelianos. G se dice *resoluble*, (o metaabeliano) si G tiene alguna serie de resolubilidad. En caso contrario, G se llama irresoluble.

Ejemplos.

i) Todo grupo abeliano es resoluble. Basta tomar $(G; 1)$.

ii) Todo grupo simple no abeliano es irresoluble.

iii) A_n es resoluble $\Leftrightarrow$ $n \leq 4$. En efecto, si $n \leq 3$ entonces $\mathbb{A}_n$ es abeliano, luego es resoluble. Consideremos $\mathbb{A}_4$: una serie de resolubilidad es $(\mathbb{A}_4, V, W, 1)$. Los índices son respectivamente $\frac{4!}{2.4} = 3, \frac{4}{2} = 2, 2$. Si $n > 4$, entonces $\mathbb{A}_n$ es simple y no abeliano.

PROPOSICIÓN. *$\mathbb{S}_n$ es resoluble si y sólo si $n \leq 4$.*

DEMOSTRACIÓN. Si $n \leq 2$, entonces $\mathbb{S}_n$ es abeliano. Si $n = 3$, $(\mathbb{S}_3, \mathbb{A}_3, 1)$ es una serie de resolubilidad de $\mathbb{S}_3$; si $n = 4$, $(\mathbb{S}_4, \mathbb{A}_4, V, W, 1)$ es una serie de resolubilidad de $\mathbb{S}_4$.

Supongamos entonces que $n > 4$. Sea $(G_i)_{0\leq i\leq m}$ una serie normal de $\mathbb{S}_n$. Sea $j = \min\{i : 0 \leq i \leq m, G_i \neq \mathbb{S}_n\}$. Como $G_i = \mathbb{S}_n$, $0 \leq i < j$; G_j es un subgrupo normal de $\mathbb{S}_n$, y como $G_j \neq \mathbb{S}_n$, $G_j = A_n$ o $G_j = 1$.

En el primer caso, sea $k = \min\{i, j \leq i \leq m \text{ y } G_i \neq \mathbb{A}_n\}$; entonces $G_i = 1$ para $k \leq i \leq m$. Luego

$$G_i/G_{i+1} = \begin{cases} 1 & 0 \leq i \leq j-2 \\ \mathbb{S}_n/\mathbb{A}_n & i = j-1 \\ 1 & j \leq i \leq k-2 \\ \mathbb{A}_n & i = k-1 \\ 1 & j \leq i \leq m \end{cases}$$

El segundo caso es claro. □

PROPOSICIÓN. *Dado un morfismo de grupos $\varphi : G \to H$, si $\ker\varphi$ e $\operatorname{Im}\varphi$ son resolubles, entonces G es resoluble.*

DEMOSTRACIÓN. Sea $(H_i)_{i=0}^n$ una serie de resolubilidad de $\operatorname{Im}\varphi$. Tomando $G_i = \varphi^{-1}(H_i)$, $(G_i)_{i=0}^n$ es una sucesión de subgrupos de G que satisface

i) G_{i+1} es normal en G_i, $0 \leq i < n$ (pues H_{i+1} es normal en H_i).

ii) $G_0 = G$.

iii) $G_n = \ker\varphi$.

Además, considerando $\varphi|G_i : G_i \to H$, se tiene $\ker\varphi|G_i = \ker\varphi$, $\operatorname{Im}\varphi|G_i = H_i$, con lo cual $H_i \simeq G_i/\ker\varphi$, coherentemente con i). De donde

$$H_i/H_{i+1} \simeq (G_i/\ker\varphi)/(G_{i+1}/\ker\varphi) \simeq G_i/G_{i+1}.$$

Como $\ker\varphi$ es resoluble, si $(K_j)_{j=0}^m$ es una serie de resolubilidad de $\ker\varphi$, tomando $G_{n+j+1} = K_j$ $0 \leq j \leq m$, resulta que $(G_i)_{i=0}^{n+m+1}$ es una serie de resolubilidad de G. □

COROLARIO. *Sea S un subgrupo normal de un grupo G; si S y G/S son resolubles, entonces G es resoluble.*

DEMOSTRACIÓN. Considerar la proyección $\pi : G \to G/S$. □

OBSERVACIÓN. Como se probará que la resolubilidad es una propiedad homomórfica (en particular, algebraica), el corolario resulta equivalente a la proposición.

COROLARIO. *Sea G un grupo que es producto directo de una sucesión $(S_i)_{1\leq i\leq n}$ de subgrupos. Si S_i es resoluble, $1 \leq i \leq n$, entonces G es resoluble.*

DEMOSTRACIÓN. Para $n = 0$, es trivial. Sea $n > 0$. Se considera el morfismo $\varphi : G \to S_1$ dado por $\varphi(x) = x_1$, si $x = \prod_{i=1}^n x_i$, con $x_i \in S_i$. $\operatorname{Im}\varphi = S_1$ es resoluble; $\ker\varphi$ es producto directo de la sucesión de subgrupos $(S_i)_{i=2}^n$, que argumentando por inducción, se puede suponer que es resoluble. □

PROPOSICIÓN. *Si G es un grupo resoluble, todo subgrupo S de G es resoluble.*

DEMOSTRACIÓN. Si $(G_i)_{i=0}^n$, es una serie normal de G, entonces $(G_i \cap S)_{i=0}^n$ es una serie normal de S. Además, la inclusión de $G_i \cap S$ en G_i define, pasando al cociente, un monomorfismo de $G_i \cap S/G_{i+1} \cap S$ en G_i/G_{i+1}, para $0 \leq i < n$. □

DEFINICIÓN. Dadas series normales $(G_i)_{i=0}^n$, $(G'_j)_{j=0}^m$ de un grupo G, se dice que (G'_j) es un *refinamiento* de (G_i) sii existe una aplicación estrictamente creciente

$$\alpha : \mathbb{I}_{m-1} \to \mathbb{I}_{n-1}$$

tal que $G_i = G'_{\alpha(i)}$, $0 < i < n$. En particular, $n \leq m$.

OBSERVACIÓN. Todo factor de un refinamiento es imagen homomórfica de un subfactor (i.e, subgrupo de un factor) de la serie original.

En efecto, conservando las notaciones de la definición, se extiende α tomando $\alpha(0) = 0$. Dado $j \in \mathbb{Z}, 0 \leq j < m$, queremos determinar G'_j/G'_{j+1}.

Sea $p = \max\{i \in \mathbb{Z}; 0 \leq i < n \text{ y } \alpha(i) \leq j\}$. Entonces

$$\alpha(p) \leq j \Rightarrow G_p = G'_{\alpha(p)} \supseteq G'_j,$$
$$p+1 > p \Rightarrow \alpha(p+1) > j \Rightarrow G_{p+1} = G'_{\alpha(p+1)} \subseteq G'_{j+1}.$$

O sea:

$$G_p \supseteq G'_j \supseteq G'_{j+1} \supseteq G_{p+1}.$$

Ahora, como G_{p+1} es normal en G_p, resulta normal en G'_j, y está definido el grupo G'_j/G_{p+1}. Por pasaje al cociente de la aplicación idéntica de G'_j, se obtiene un epimorfismo de G'_j/G_{p+1} en G'_j/G'_{j+1} y G'_j/G_{p+1} en un subgrupo de G_p/G_{p+1}.

En consecuencia, si los factores de una serie normal gozan de una cierta propiedad hereditaria y homomórfica, también la tienen los factores de cualquier refinamiento. Es así, por ejemplo, que cualquier refinamiento de una serie de resolubilidad es una serie de resolubilidad.

El conjunto de las series normales de un grupo G resulta parcialmente ordenado por refinamiento:

$$(G_i)_{i=0}^n \leq (G'_j)_{j=0}^m \Longleftrightarrow (G'_j) \text{ es un refinamiento de } (G_i).$$

DEFINICIÓN. Dadas series normales $(G_i)_{i=0}^n$ y $(H_j)_{j=0}^m$ de grupos G y H, se dice que las series son *equivalentes* sii existe una biyección

$$\beta : \{0, 1, \ldots, n-1\} \to \{0, 1, \ldots, m-1\}$$

tal que

$$G_i/G_{i+1} \simeq H_{\beta(i)}/H_{\beta(i)+1}, \quad 0 \leq i < n.$$

En particular, $n = m$.

OBSERVACIONES. (i) Si los factores de una serie normal gozan de una cierta propiedad algebraica, también la tienen los factores de cualquier serie equivalente.

(ii) Esta relación es una relación de equivalencia en la clase de *todas* las series normales.

Recordatorio. Sean S y T subgrupos de un grupo G. Sea $S.T = \{x.y,\ x \in S,\ y \in T\}$; sea $S \vee T =< S \cup T >$. Se verifican:

i) Si S o T es normal, entonces $S.T$ es un subgrupo.

ii) Si S y T son normales, $S.T$ es normal.

iii) (Tercer teorema de isomorfismo). Si T es un subgrupo normal de G, entonces $S \cap T$ es un subgrupo normal de S, y $S/S \cap T \simeq S.T/T$.

OBSERVACIÓN. i) Si S es normal entonces

$$\forall x \in G,\ \forall\, y \in S,\ \exists\, y' \in S: \quad xy = y'x.$$

ii) Si $\pi : G \to G/T$ es la proyección, se considera $\pi|S$. Entonces $\ker \pi|S = S \cap T$, $\operatorname{Im} \pi|S = S.T/T$.

LEMA (ZASSENHAUS). *Si H y K son subgrupos de un grupo G, y H' y K' son subgrupos normales de H y K respectivamente, entonces $H'.(H \cap K')$ es un subgrupo normal de $H'.(H \cap K)$; $K'.(K \cap H')$ es un subgrupo normal de $K'.(K \cap H)$, y*

$$H'.(H \cap K)/H'.(H \cap K') \simeq K'.(K \cap H)/K'.(K \cap H').$$

DEMOSTRACIÓN. Trabajando en el grupo H, $H' \cap K = H' \cap (H \cap K)$ es un subgrupo normal de $H \cap K$. Del mismo modo, $K' \cap H$ es un subgrupo normal de $K \cap H$. Por lo tanto, $(H' \cap K).(H \cap K')$ es un subgrupo normal de $H \cap K$. Luego, $H'.(H' \cap K).(H \cap K')$ resulta un subgrupo normal de $H'.(H \cap K)$. Pero $H'.(H' \cap K).(H \cap K') = H'.(H \cap K')$.

A continuación se empleará el tercer teorema de isomorfismo, en la situación:

$$G = H'.(H \cap K), \qquad T = H'.(H \cap K'), \qquad S = H \cap K.$$

Entonces

$$S.T = G$$
$$S \cap T = \underbrace{(H' \cap K).(H \cap K')}_{II}$$

En efecto $S \cap T = \underbrace{(H \cap K) \ \cap \ (H'.(H \cap K'))}_{I}$.

Veamos que $I \subseteq II$. Sea $x \in H'$, $y \in H \cap K' : xy \in H \cap K$.

Hay que ver que $x \in H' \cap K$. Basta ver que $x \in K$; pero $\left.\begin{matrix} xy \in K \\ y \in K' \subset K \end{matrix}\right\} \Longrightarrow x \in K.$

Veamos ahora que $I \supseteq II$. Es obvio que $H' \cap K \subset H \cap K$; como $H' \cap K \subset H' \Longrightarrow H' \cap K \subset H'(H \cap K')$. Como además $H' \cap K' \subset H \cap K$ y $H \cap K' \subset H'(H \cap K')$, la inclusión sigue.

Por el tercer teorema de isomorfismo, resulta así por simetría

$$H \cap K/(H' \cap K).(H \cap K') \simeq H'.(H \cap K)/H'(H \cap K').$$

Por ende $H \cap K/(H' \cap K).(H \cap K') = K \cap H/(H \cap K').(H \cap K) \simeq K'(K \cap H)/K'(K \cap H')$. □

TEOREMA (SCHREIER). Dos series normales de un mismo grupo, tienen refinamientos que son equivalentes.

DEMOSTRACIÓN. Sean $\Sigma_1 = (G_i)_{i=0}^n$, $\Sigma_2 = (H_j)_{j=0}^m$ series normales de un grupo G. Se procederá a construir un refinamiento Σ_1' de Σ_1 intercalando entre G_i y G_{i+1}, $m-1$ subgrupos $(G_{i_j})_{j=1}^{m-1}$ $(0 \leq i < n)$, y un refinamiento Σ_2' de Σ_2, intercalando $n-1$ subgrupos H_{j_i}, $1 \leq i \leq n-1$, entre H_j y H_{j+1}, $0 \leq j < m$. Notar que como Σ_1 tiene $n+1$ términos, y Σ_2 tiene $m+1$ términos, tanto Σ_1' como Σ_2' tienen $nm+1$.

Se definen

$$G_{i_j} = G_{i+1}.(G_i \cap H_j), \quad 0 \leq i < n, \quad 0 \leq j \leq m,$$
$$H_{j_i} = H_{j+1}.(H_j \cap G_i), \quad 0 \leq j < m, \quad 0 \leq i \leq n.$$

Notar que

$$G_{i_0} = G_{i+1}.G_i = G_i, \qquad G_{i_m} = G_{i+1}, \qquad H_{j_0} = H_j, \qquad H_{j_n} = H_{j+1}.$$

Ahora, aplicando el lema de Zassenhaus en la situación

$$\begin{array}{ccc} & G & \\ \nearrow & & \nwarrow \\ G_i & & H_j \\ \uparrow & & \uparrow \\ G_{i+1} & & H_{j+1} \end{array}$$

para $0 \leq i < n$, $0 \leq j < m$, resulta

$$G_{i_j}/G_{i_{j+1}} \simeq H_{j_i}/H_{j_{i+1}}.$$

□

LEMA. *Si G es un grupo resoluble, para todo subgrupo normal K de G existe una serie de resolubilidad de G que tiene a K por uno de sus términos.*

DEMOSTRACIÓN. Sea $\Sigma_1 = (G_i)_{i=0}^n$ una serie de resolubilidad de G. Sea $\Sigma_2 = (G, K, 1)$. Por el teorema anterior, Σ_1 y Σ_2 tienen refinamientos Σ_1', Σ_2' equivalentes.

Como Σ_1 es una serie de resolubilidad, y Σ_1' es un refinamiento de Σ_1, Σ_1' también lo es. Además, como Σ_2' es un refinamiento de Σ_2, Σ_2' tiene a K como uno de sus términos, pero como $\Sigma_1' \sim \Sigma_2'$, resulta Σ_2' una serie de resolubilidad. □

PROPOSICIÓN. *Dado un morfismo de grupos $\varphi : G \to H$ si G es resoluble,* $\operatorname{Im}\varphi$ *es resoluble.*

DEMOSTRACIÓN. Sea $K = \ker\varphi$ y apliquemos el lema. Sea $(G_i)_{i=o}^n$ una serie de resolubilidad de G tal que $G_m = K$ para algún índice m. Tomando $H_j = \varphi(G_j)$, para $0 \leq j \leq m$, resulta

i) H_{j+1} es normal en H_j (pues G_{j+1} lo es en G_j);

ii) $H_0 = \operatorname{Im}\varphi$ (pues $G_0 = G$);

iii) $H_m = 1$ (pues $G_m = K$).

Además $H_j \simeq G_j/K$, con lo cual

$$H_j/H_{j+1} \simeq (G_j/K)/(G_{j+1}/K) \simeq G_j/G_{j+1}, \quad 0 \leq j < m.$$

□

DEFINICIÓN. Una *serie de composición* de un grupo G es una serie normal de G tal que G_i/G_{i+1} es un grupo simple (o sea G_{i+1} como subgrupo normal de G_i es maximal), para $0 \leq i < n$. Se dice que G tiene *longitud finita* si G tiene alguna serie de composición.

Ejemplos.

i) G es trivial si y sólo si, (G) es una serie de composición (en cuyo caso, es la única).

ii) G es simple si y sólo si $(G, 1)$ es una serie de composición de G (en cuyo caso es la única).

iii) $(\mathbb{S}_n, \mathbb{A}_n, 1)$ es una serie de composición de $\mathbb{S}_n$ si y sólo si $n = 3$ o $n > 4$.

iv) $(\mathbb{S}_4, \mathbb{A}_4, V, W, 1)$ es una serie de composición de $\mathbb{S}_4$.

v) Todo grupo finito tiene longitud finita, y si es abeliano, vale la recíproca.

DEMOSTRACIÓN. v). Sea G un grupo finito. Se definen subgrupos G_i de G en la forma siguiente: $G_0 = G$; y, supuesto definido G_i, si $G_i = 1$ se interrumpe el proceso; pero si $G_i \neq 1$ se toma G_{i+1} como un elemento maximal del conjunto de subgrupos normales, propios, de G_i, conjunto que es finito y no vacío. Como G es finito, $\exists n \in \mathbb{N}_0$, $n < (G : 1)$ tal que $G_n = 1$; tomando el mínimo, $(G_i)_{i=0}^n$ es una serie de composición.

Recíprocamente, sea G abeliano, y $(G_i)_{i=0}^n$ una serie de composición de G. G_n es obviamente finito pues $G_n = 1$. Si G_{n-i} es finito, entonces G_{n-i-1} es finito $0 < i \leq n$, pues G_{n-i-1}/G_{n-i} es simple y abeliano, luego finito. Ergo G_0 es finito. □

LEMA. *Una serie normal estrictamente decreciente de un grupo G es una serie de composición de G si y sólo si carece de refinamientos propios estrictamente decrecientes.*

DEMOSTRACIÓN. Sea $\Sigma = (G_i)_{i=0}^n$ una serie normal de G, estrictamente decreciente. Si existe un índice j tal que G_{j+1} como subgrupo normal de G_j no es maximal, se tiene un subgrupo normal H de G_j tal que

$$G_{j+1} \subset H \subset G_j$$

Basta intercalar H entre G_j y G_{j+1}, en Σ, para obtener un refinamiento Σ' de Σ estrictamente decreciente, con $\Sigma' \neq \Sigma$.

Recíprocamente, supongamos que Σ admite un tal refinamiento Σ'. Como $\Sigma' \neq \Sigma$, existe un índice j tal que G_j y G_{j+1} no son términos consecutivos en Σ'. Tomando H como el primer término de

Σ' que figura después de G_j, resulta que $G_j \supset H \supset G_{j+1}$, y H es normal en G_j. Luego G_{j+1} no es maximal en G_j. □

TEOREMA (JORDAN - HÖLDER). Dos series de composición de un mismo grupo son equivalentes (en particular, tienen igual longitud).

DEFINICIÓN. Si G es un grupo de longitud finita, se llama *longitud* de G a la longitud de una serie de composición de G, que notaremos ℓG.

DEMOSTRACIÓN. Sean Σ_1 , Σ_2 series de composición de un grupo G. Como series normales de G, Σ_1 y Σ_2 tienen refinamientos Σ_1' y Σ_2' tales que $\Sigma_1' \sim \Sigma_2'$ (Schreier). No hay inconveniente en suponer que Σ_1' y Σ_2' son estrictamente decrecientes. Luego, por el lema $\Sigma_1' = \Sigma_1$ y $\Sigma_2' = \Sigma_2$ con lo cual $\Sigma_1 \sim \Sigma_2$. □

Ejemplos:

i) Los grupos de longitud 0 son los grupos triviales.

ii) Los grupos de longitud 1 son los grupos simples.

iii) $\ell(\mathbb{S}_n) = 2$ si $n = 3$ o $n > 4$.

iv) $\ell(\mathbb{S}_4) = 4$.

v) Si G es finito, $l(G) \leq \log_2 (G : 1)$.

En efecto si $(G_i)_{i=0}^n$ es una serie normal estrictamente decreciente de G,

$$(G : 1) = (G_0 : G_n) = \prod_{0 \leq i \leq n} (G_i : G_{i+1}) \geq 2^n.$$

ADVERTENCIA. Sean G y G' grupos de longitud finita. Es inmediato que si $G \simeq G'$, entonces G y G' tienen series de composición que son equivalentes; en particular, $\ell(G) = \ell(G')$. Sin embargo, existen grupos abelianos finitos G y G' que tienen series de composición equivalentes, pero no son isomorfos. Basta tomar como G un grupo cíclico de orden 4 (o sea, $G \simeq \mathbb{Z}_4$) y como G' un grupo no cíclico de orden 4 (o sea, $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$).

PROPOSICIÓN. *Si G es un grupo de longitud finita toda serie normal de G estrictamente decreciente entonces tiene un refinamiento que es una serie de composición de G.*

DEMOSTRACIÓN. Sea Σ_0 una serie de composición de G, y sea Σ cualquier serie normal de G, estrictamente decreciente. Por el teorema de Schreier, Σ_0 y Σ tienen refinamientos Σ_0' y Σ' que son equivalentes. Por supresión de términos, podemos suponer que Σ_0' y Σ' son estrictamente decrecientes (por serlo Σ_0 y Σ). Luego $\Sigma_0' = \Sigma_0$, de donde $\Sigma_0 \sim \Sigma'$ y así Σ' es una serie de composición. □

COROLARIO. *Si G es un grupo resoluble de longitud finita, entonces G tiene una serie normal cuyos factores son grupos de orden primo; en particular, G es finito.*

DEMOSTRACIÓN. Aplicar la proposición a una serie de resolubilidad Σ de G, que puede suponerse estrictamente decreciente. Sea Σ' una serie de composición de G, que refina a Σ. Así, Σ' es una serie de resolubilidad, con lo cual los factores de Σ' son abelianos; pero –además– son simples. Luego los factores de Σ' son grupos de orden primo. □

5. p-grupos

DEFINICIÓN. Un *G- conjunto* es un conjunto C provisto de una acción de G en C.

Dados $x, y \in C$, se dice que x es *conjugado* con y si existe un $s \in G$ tal que $s.x = y$.

Dado $x \in C$ se llama *órbita* de x al conjunto $\mathcal{O}_x$ de conjugados de x. Con C/G se nota $\mathcal{O}_x : x \in C\}$.

Se dice que x es *invariante* si y sólo si $\mathcal{O}_x = \{x\}$ (x es el único conjugado), vale decir, para todo $s \in G$, $s.x = x$. El conjunto de elementos invariantes se nota ${}^G C$.

Dado $x \in C$, $G_x = \{s \in G : s.x = x\}$ es un subgrupo de G, llamado el *estabilizador* (o grupo de isotropía) de x.

Dada una extensión E/K, se llama *grupo de Galois* de E/K, notado $\mathbb{G}(E/K)$, al conjunto de automorfismos de E/K provisto de de la composición usual de aplicaciones.

PROPOSICIÓN. *Sea G un grupo; y sea C un G-conjunto. Si R es un sistema de representantes de C/G, entonces*

$$\operatorname{card} C = \operatorname{card} {}^G C + \sum_{X \in R - {}^G C} (G : G_X).$$

DEMOSTRACIÓN. La aplicación de G en C, $s \mapsto s.x$ tiene por imagen a $\mathcal{O}_x$ y además

$$sx = tx \Leftrightarrow (t^{-1}s)x = x \Leftrightarrow t^{-1}s \in G_x.$$

Luego, por pasaje al cociente, se obtiene una biyección de G/G_x en $\mathcal{O}_x$, lo cual prueba que

$$\operatorname{card} \mathcal{O}_x = (G : G_x).$$

Por otra parte,

$$x \in {}^G C \Leftrightarrow \mathcal{O}_x = \{x\} \Leftrightarrow G_x = G.$$

Luego $C = \bigcup_{x \in R} \mathcal{O}_x = {}^G C \cup (\bigcup_{x \in R - {}^G C} \mathcal{O}_x)$, de donde sigue el enunciado. □

TEOREMA (CAUCHY). Si G es un grupo finito, cuyo orden es divisible por un número primo p, entonces G contiene un elemento de orden p.

DEMOSTRACIÓN. En primer término, supóngase G abeliano. Sea $x \in G$, $x \neq 1$, y sea $n = \operatorname{ord} x$. Si $p|n$ entonces $x^{\frac{n}{p}}$ tiene orden p. Si p no divide a n, $p|(G :< x >)$. Luego como $(G :< x >) < (G : 1)$, argumentando inductivamente, existe $y \in G/< x >$ de orden p. Cualquier $z \in y$ es un elemento de G de orden un múltiplo de p, y se está en el caso anterior.

En el caso general, supongamos que existe $x \notin \mathcal{C}(G)$, tal que $p|(\mathcal{C}(x) : 1)$, donde $\mathcal{C}(x) = \{y \in G : xy = yx\}$ es el centralizador de x. Como $(\mathcal{C}(x) : 1) < (G : 1)$, puede argumentarse por inducción.

Luego, puede asumirse que p no divide a $(\mathcal{C}(x) : 1)$, con lo cual $p|(G : \mathcal{C}(x))$, para todo $x \notin \mathcal{C}(G)$. Haciendo actuar G en sí mismo por conjugación, la ecuación de clases correspondiente es:

$$(G : 1) = (\mathcal{C}(G) : 1) + \sum_{x \in R - \mathcal{C}(G)} (G : \mathcal{C}(x)).$$

Luego $p/(\mathcal{C}(G) : 1)$, con lo cual estamos en el caso G abeliano. □

DEFINICIÓN. Si el orden de cualquiera de sus elementos es una potencia de p, G se dice un p-grupo.

COROLARIO. *Un grupo finito G es un p-grupo si y sólo si $(G : 1) = p^n$, para algún $n \in \mathbb{N}_0$.*

DEMOSTRACIÓN. *Suficiencia.* sigue del teorema de Lagrange.
Necesidad. es consecuencia del teorema de Cauchy. □

LEMA. *Si G es un p-grupo finito, y C es un G-conjunto finito, entonces*

$$\operatorname{card}{}^G C \equiv \operatorname{card} C \mod p.$$

DEMOSTRACIÓN. Se sigue de la ecuación de clases, ya que $(G : G_x)|(G : 1) = p^n$. □

TEOREMA. Si G es un p-grupo finito, y $G \neq 1$ entonces $\mathcal{C}(G) \neq 1$.

DEMOSTRACIÓN. Haciendo actuar G en sí mismo por conjugación, el lema dice que

$$(\mathcal{C}(G) : 1) \equiv (G : 1) \equiv 0 \mod p.$$

□

PROPOSICIÓN. *Si G es un p-grupo finito, entonces G es resoluble.*

DEMOSTRACIÓN. Puede suponerse que $G \neq 1$, con lo cual $(G : \mathcal{C}(G)) < (G : 1)$, por el teorema anterior. Luego, argumentando por inducción, puede asumirse que $G/\mathcal{C}(G)$ es resoluble, y como $\mathcal{C}(G)$ es resoluble (por ser abeliano), resulta G resoluble. □

COROLARIO. *Si $(G : 1) = p^n$, entonces G tiene una serie normal de longitud n, cuyos factores son grupos de orden p. En particular, $\ell(G) = n$.*

DEMOSTRACIÓN. Como G es resoluble tiene una serie normal $(G_i)_{i=0}^m$ tal que G_i/G_{i+1} es un grupo de orden primo p_i, $0 \leq i < m$. Pero

$$(G : 1) = \prod (G_i : G_{i+1});$$

así, $p^n = \prod_{0 \leq i < n} p_i$ implica que $p_i = p$ para todo i y que $m = n$. □

6. Polinomios Simétricos.

Sea A un anillo conmutativo, y sea $n \in \mathbb{N}$. Si σ es una permutación de grado n, define un automorfismo $\widehat{\sigma}$ de la estructura de álgebra de $A[X_1, \ldots, X_n]$, a saber

$$\widehat{\sigma}(f) = f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}).$$

La aplicación $\sigma \to \widehat{\sigma}$ es un morfismo (inyectivo) de $\mathbb{S}_n$ en $\mathrm{Aut}_{\mathrm{Alg}}(A[X_1, \ldots, X_n])$. Luego, se tiene la acción

$$\sigma.f = \widehat{\sigma}(f)$$

de $\mathbb{S}_n$ en $A[X_1, \ldots, X_n]$, que es compatible con la estructura de álgebra de $A[X_1, \ldots, X_n]$.

DEFINICIÓN. Un polinomio $f \in A[X_1, \ldots, X_n]$ se dice *simétrico* sii es invariante por la acción de $\mathbb{S}_n$ en $A[X_1, \ldots, X_n]$. El conjunto ${}^{\mathbb{S}_n}A[X_1, \ldots, X_n]$ de polinomios simétricos es una subálgebra de $A[X_1, \ldots, X_n]$.

En $A[X_1, \ldots, X_n][X]$, se considera

$$h = \prod_{i=1}^{n}(X - X_i),$$

que debe interpretarse como el polinomio mónico con coeficientes en A, en una indeterminada, con n raíces genéricas. En efecto, si B es una A-álgebra conmutativa, $(x_i)_{i=1}^n$ es una sucesión de elementos de B, y $f \in B[X]$ es el polinomio $\prod_{i=1}^{n}(X - x_i)$, entonces f se obtiene como $f = h(x_1, x_2, \ldots, x_n, X)$, considerando a h como un polinomio en $A[x_1, \ldots, x_n, X]$.

Vista la definición de h, resulta

$$h = X^n + \sum_{k=1}^{n}(-1)^k s_k X^{n-k},$$

donde

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} \prod_{1 \le j \le k} X_{i_j}.$$

Como $h = \prod_{i=1}^{n}(X - X_{\sigma(i)}) = h(X_{\sigma(1)}, \ldots, X_{\sigma(n)}, X)$, (h considerado en $A[X_1, \ldots, X_n, X]$ es invariante por las permutaciones de grado $n+1$ que dejan fijo a $n+1$) resulta que s_k, que es un polinomio homogéneo de grado k, es simétrico:

$$h = X^n + \sum_{k=1}^{n}(-1)^k \underbrace{s_k(X_{\sigma(1)}, \ldots, X_{\sigma(n)})}_{\sigma.s_k} X^{n-k}$$

$$\Rightarrow (-1)^k(\sigma.s_k) = (-1)^k s_k \Rightarrow \sigma.s_k = s_k.$$

Por esta razón, s_k se llama el *polinomio simétrico elemental de grado* k. Está probado que la subálgebra generada por $(s_k)_{k=1}^n$ está contenida en la subálgebra de polinomios simétricos; en símbolos,

$$A[s_1,\dots,s_n] \subseteq {}^{\mathbb{S}_n}A[X_1,\dots,X_n].$$

DEFINICIÓN. Dado $g \in A[X_1,\dots,X_n]$, $g = \sum_{m\in\mathbb{Z}^n_{\geq 0}} a_m \prod_{i=1}^n X_i^{m_i}$, se llama *peso* de g a

$$\mu(g) = \text{máx}\left\{\sum_{i=1}^n im_i; a_m \neq 0\right\}.$$

(Obsérvese que $\text{gr}\, g = \text{máx}\{\sum m_i\}$).

Como s_k es un polinomio homogéneo de grado k, resulta que $\text{gr}\, g(s_1,\dots,s_n) \leq \mu(g)$. En efecto:

$$\text{gr}(\sum_m a_m \prod_{i=1}^n s_i^{m_i}) \leq \text{máx}_{a_m\neq 0}\ \text{gr}(\prod_{i=1}^n s_i^{m_i}) = \text{máx}(\sum im_i) = \mu(g).$$

TEOREMA. *La familia* (s_k), $k = 1,\dots,n$ *es una familia de generadores algebraicamente independientes de* ${}^{\mathbb{S}_n}A[X_1,\dots,X_n]$.

Además, $\text{gr}\, g(s_1,\dots,s_n) = \mu(g)$, *para todo* $g \in A[X_1,\dots,X_n]$.

DEMOSTRACIÓN. Se comprobará que

(i). Si $f \in A[X_1,\dots,X_n]$ es simétrico, de grado d, existe $g \in A[X_1,\dots X_n]$ tal que $\mu(g) = d$ y $f = g(s_1,\dots,s_n)$.

(ii). $(s_k)_{k=1}^n$ es una familia algebraicamente independiente en $A[X_1,\dots,X_n]$.

OBSERVACIÓN. Dados $f,g,h \in A[X_i]_{i\in I}$, si $f.h = g.h$ y h es un monomio cuyo coeficiente no es un divisor de cero en A, entonces $f = g$.

(i). Se procede por inducción en n. El caso $n = 1$ es inmediato: todo $f \in A[X_1]$ se presenta $f = f(X_1)$; pero $s_1 = X_1$, y $\text{gr}\, f = \mu(f)$.

Sea $n > 1$. Obsérvese que $s'_k = s_k(X_1,\dots,X_{n-1},0)$ es el polinomio simétrico elemental de grado k en $A[X_1,\dots,X_{n-1}]$. En efecto,

$$s'_k = \sum_{\substack{i_1<\cdots<i_k \\ 1\leq i_j\leq n \\ i_k\neq n}} \prod_{j=1}^k X_{i_j} = \sum_{\substack{i_1<\cdots<i_k \\ 1\leq i_j\leq n-1}} \prod_{j=1}^k X_{i_j}.$$

Otra forma de verlo: se tiene la igualdad

$$\left(\prod_{i=1}^{n-1}(X - X_i)\right) X = h(X_1,\dots,X_{n-1},0,X) = X^n + \sum_{1\leq k\leq n}(-1)^k s'_k X^{n-k} =$$

$$(X^{n-1} + \sum_{k=1}^{n-1}(-1)^k s'_k X^{n-1-k})X$$

en $A[X_1,\dots,X_n,X]$, y gracias a la observación anterior, la afirmación sigue.

Como $f \in A[X_1, \ldots, X_n]$ es simétrico, también lo es $f(X_1, \ldots, X_{n-1}, 0) \in A[X_1, \ldots, X_{n-1}]$. En efecto, si σ es una permutación de grado $n-1$, $f(X_{\sigma(1)}, \ldots, X_{\sigma(n-1)}, X_n) = f(X_1, \ldots, X_{n-1}, X_n)$, y basta sustituir X_n por 0.

Luego, por hipótesis inductiva, existe $g' \in A[X_1, \ldots, X_{n-1}]$ tal que

$$f(X_1, \ldots, X_{n-1}, 0) = g'(s'_1, \ldots, s'_{n-1})$$

y $\mu(g') = \operatorname{gr} f(X_1, \ldots, X_{n-1}, 0) \leq \operatorname{gr} f = d$.

Ahora, sea $f' = f - g'(s_1, \ldots, s_{n-1}) \in A[X_1, \ldots, X_n]$; f' es simétrico, y

$$f'(X_1, \ldots, X_{n-1}, 0) = f(X_1, \ldots, X_{n-1}, 0) - g'(s'_1, \ldots, s'_{n-1}) = 0,$$

con lo cual $X_n | f'$. Sea σ la transposición (in), $1 \leq i \leq n-1$. Como f' es simétrico,

$$X_n | f' \Rightarrow X_i = \widehat{\sigma}(X_n) | \widehat{\sigma}(f') = f'.$$

Luego, $s_n = \prod_{i=1}^{n} X_i$ divide a f'. O sea $f' = s_n . f''$, para algún $f'' \in A[X_1, \ldots, X_n]$, y f'' resulta simétrico. En efecto, $f' = \sigma . f' = \sigma . (s_n f'') = (\sigma . s_n)(\sigma . f'') = s_n \sigma . f'' \Rightarrow s_n f'' = s_n \sigma . f'' \Rightarrow f'' = \sigma f''$.

Además, $\operatorname{gr} f'' = \operatorname{gr} f' - \operatorname{gr} s_n = \operatorname{gr} f' - n$, y como $\operatorname{gr} f' \leq \max\{\operatorname{gr} f, \operatorname{gr} g'(s_1, \ldots, s_{n-1})\}$, se sigue que $\operatorname{gr} f'' = \operatorname{gr} f' - n \leq d - n < d$.

Ahora, por inducción global en el grado, $\exists\ g'' \in A[X_1, \ldots, X_n]$ tal que $f'' = g''(s_1, \ldots, s_n)$ y $\mu(g'') = \operatorname{gr} f'' \leq d - n < d$. En definitiva,

$$f = f' + g'(s_1, \ldots, s_{n-1}) = s_n . f'' + g'(s_1, \ldots, s_{n-1}) = s_n . g''(s_1, \ldots, s_n) + g'(s_1, \ldots, s_{n-1}).$$

Luego, tomando $g = g' + X_n g'' \in A[X_1, \ldots, X_n]$, resulta $f = g(s_1, \ldots, s_n)$ y

$$d = \operatorname{gr} f = \operatorname{gr} g(s_1, \ldots, s_n) \leq \mu(g) \leq \max(\mu(g'), n + \mu(g'') \leq \max(d, d - n) = d.$$

O sea

$$\mu(g) = d.$$

(ii). $(s_k)_{1 \leq k \leq n}$ es una familia algebraicamente independiente en $A[X_1, \ldots, X_n]$.

Se procede por inducción en n. El caso $n = 1$ es trivial: $s_1 = X_1$.

Sea $n > 1$. Por el absurdo, supóngase que existe $f \in A[X_1, \ldots, X_n]$, $f \neq 0$ tal que $f(s_1, \ldots, s_n) = 0$, y asúmase que $\operatorname{gr} f = d$ es mínimo.

Sea $f = \sum_{i=0}^{d} f_i . X_n^i$, con $f_i \in A[X_1, \ldots, X_{n-1}]$.

Si $f_0 = 0$, $\Rightarrow \exists\ g$ tal que $f = X_n . g$, $g \in A[X_1, \ldots, X_n]$, $g \neq 0$. Entonces $s_n . g(s_1, \ldots, s_n) = 0 \Rightarrow g(s_1, \ldots, s_n) = 0$ y $g \neq 0$.

Además $\operatorname{gr} g \leq \operatorname{gr} f - \operatorname{gr} X_n = \operatorname{gr} f - 1 < d$. Absurdo. Por lo tanto $f_0 \neq 0$. Sustituyendo X_n por 0 en $\sum_{i=0}^{d} f_i(s_1, \ldots, s_{n-1}).s_n^i = 0$, se tiene

$$\sum_{i=0}^{d} f_i(s'_1, \ldots, s'_{n-1}).{s'_n}^i = 0 :$$

pero como $s'_n = 0$, resulta $f_0(s'_1, \ldots, s'_{n-1}) = 0$, y por hipótesis inductiva, $f_0 = 0$. □

Ejercicio. Sea K un cuerpo. Por analogía a lo expuesto para $A[X_1, \ldots, X_n]$, definir una acción de $\mathbb{S}_n$ en $K(X_1, \ldots, X_n)$ e introducir la noción de fracción racional simétrica. Luego, usando el teorema de Artin para los grupos finitos de automorfismos de un cuerpo, probar las dos proposiciones siguientes:

i) Si $f \in K(X_1, \ldots, X_n)$ es simétrico, existe una única fracción $g \in K(X_1, \ldots, X_n)$:

$$f = g(s_1, \ldots, s_n)$$

Indicación. Sea $h = \prod_{i=1}^{n}(X - X_i)$; considerar su cuerpo de descomposición sobre $K(X_1, \ldots, X_n)$.

ii) Si G es cualquier grupo finito, existe una extensión E/L y un cuerpo intermedio F de E/L tal que E/F es galoisiana y $\mathbb{G}(E/F) \simeq G$.

Indicación. Considerar a G como subgrupo de $\mathbb{S}_n$ para algún n, y usar el teorema de Artin.

TEOREMA (ARTIN). *Si G es un grupo finito de automorfismo de un cuerpo E y $K = {}^G E$, entonces $G = \mathbb{G}(E/K)$ y E/K una extensión galoisiana de grado finito.*

6.1. El discriminante.. En $A[X_1, \ldots, X_n]$ se considera el polinomio

$$g = \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

(En lugar de g, puede emplearse $\prod_{1 \leq i < j \leq n} (X_i - X_j) = (-1)^{\frac{n(n-1)}{2}} g$). Se ve que, dada una permutación π de grado n, $\pi.g = \chi(\pi).g$, donde $\chi(\pi)$ es la signatura de π.

Luego $d = g^2$ es un polinomio simétrico, pues

$$\pi(g^2) = (\pi g)(\pi g) = (\pi g)^2 = \chi(\pi)^2 g^2 = g^2 = d.$$

Explícitamente,

$$d = \prod_{i<j}(X_j - X_i)^2 = \prod_{i<j}(X_i - X_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(X_i - X_j).$$

Por lo tanto, está unívocamente determinado $\delta \in A[X_1, \ldots, X_n]$ por la propiedad

$$d = \delta(s_1, \ldots, s_n).$$

Más aún, si P es el subanillo primo de A, como $d \in P[X_1, \ldots, X_n]$ pues $g \in P[X_1, \ldots, X_n]$, resulta $\delta \in P[X_1, \ldots, X_n]$.

Sea $p_k = \sum_{i=1}^n X_i^k$, $k \in \mathbb{N}_0$. Por ejemplo, $p_0 = n$, $p_1 = s_1$. Como $g = v(X_1, \ldots, X_n) = \det(X_i^{j-1})_{1 \leq i,j \leq n} = \det\ a$, donde

$$a = \begin{pmatrix} 1 & X_1 & X_1^2 & \ldots & X_1^{n-1} \\ 1 & X_2 & X_2^2 & \ldots & X_2^{n-1} \\ 1 & X_n & X_n^2 & \ldots & X_n^{n-1} \end{pmatrix}.$$

(es decir, v es el determinante de van der Monde.)

Resulta que

$$d = det(p_{i+j-2})_{0 \leq i,j \leq n} = \det \begin{pmatrix} p_0 & p_1 & p_2 & \ldots & p_{n-1} \\ p_1 & p_2 & p_3 & \ldots & p_n \\ \vdots & \vdots & \vdots & & \vdots \\ p_{n-1} & p_n & p_{n+1} & \ldots & p_{2n-2} \end{pmatrix}.$$

En efecto, $d = g^2 = (\det\ a)^2 = \det(a^t.a)$, y $(a^t.a)_{ij} = \sum_{k=1}^n a_{ki}.a_{kj} = \sum_{k=1}^n X_k^{i-1} X_k^{j-1} = \sum_{k=1}^n X_k^{i+j-2} = p_{i+j-2}$.

Se tiene en general $\det b = \sum_{\pi \in \mathbb{S}_n} \chi(\pi) \prod_{i=1}^n b_{i\pi(i)}$. De modo que, explícitamente,

$$d = \sum_{\pi \in \mathbb{S}_n} \chi(\pi) \prod_{i=1}^n p_{i+\pi(i)-2}.$$

Ejemplos.

i) Caso $n = 2$. Por un lado,

$$d = \det \begin{pmatrix} 2 & p_1 \\ p_1 & p_2 \end{pmatrix} = 2p_2 - p_1^2,$$

mientras que

$$p_1 = X_1 + X_2 = s_1,$$
$$p_2 = X_1^2 + X_2^2 = (X_1 + X_2)^2 - 2X_1X_2 = s_1^2 - 2s_2.$$

Luego $d = 2(s_1^2 - 2s_2) - s_1^2 = s_1^2 - 4s_2$, y por lo tanto

$$\delta = X_1^2 - 4X_2.$$

ii) Caso $n = 3$.

$$d = \det \begin{pmatrix} 3\,p_1 & p_2 \\ p_1 & p_2 & p_3 \\ p_2 & p_3 & p_4 \end{pmatrix} = 3p_2p_4 + 2p_1p_2p_3 - p_2^3 - p_1^2p_4 - 3p_3^2.$$

Por otra parte

$$\begin{aligned} p_1 &= X_1 + X_2 + X_3 = s_1 \\ p_2 &= X_1^2 + X_2^2 + X_3^2 = (X_1 + X_2 + X_3)^2 - 2(X_1X_2 + X_1X_3 + X_2X_3) \\ &= s_1^2 - 2p_2 \end{aligned}$$

Para calcular p_3 y p_4, se considera

$$h = (X - X_1)(X - X_2)(X - X_3) = X^3 - s_1X^2 + s_2X - s_3.$$

Como $h(X_i) = 0$,

$$X_i^3 = s_1X_i^2 - s_2X_i + s_3$$

y

$$X_i^4 = s_1X_i^3 - s_2X_i^2 + s_3X_i.$$

Luego

$$\begin{aligned} p_3 &= X_1^3 + X_2^3 + X_3^3 \\ &= s_1(X_1^2 + X_2^2 + X_3^2) - s_2(X_1 + X_2 + X_3) + 3s_3 \\ &= s_1(s_1^2 - 2s_2) - s_2s_1 + 3s_3 = \\ &= s_1^3 - 3s_1s_2 + 3s_3; \end{aligned}$$

$$\begin{aligned} p_4 &= X_1^4 + X_2^4 + X_3^4 \\ &= s_1(X_1^3 + X_2^3 + X_3^3) - \\ &\quad - s_2(X_1^2 + X_2^2 + X_3^2) + s_3(X_1 + X_2 + X_3) = \\ &= s_1(s_1^3 - 3s_1s_2 + 3s_3) - s_2(s_1^2 - 2s_2) + s_3s_1 = \\ &= s_1^4 - 3s_1^2s_2 + 3s_1s_3 - s_1^2s_2 + 2s_2^2 + s_1s_3 = \\ &= s_1^4 - 4s_1^2s_2 + 4s_1s_3 + 2s_2^2. \end{aligned}$$

Finalmente,

$$d = 18s_1s_2s_3 + s_1^2\,s_2^2 - 4s_1^3\,s_3 - 4s_2^3 - 27s_3^2.$$

A continuación, el anillo A de coeficientes es un cuerpo K. Dado $f \in K[X]$, no constante y mónico, sea E/K un cuerpo de descomposición de f, y sea $(\rho_i)_{1\leq i\leq n}$ una numeración por multiplicidad de las raíces de f en E. (Esto significa que $\text{mult}(\rho_i, f) = \text{card}\{j : \rho_j = \rho_i\}$, vale decir $f = \prod_{i=1}^{n}(X - \rho_i)$.)

DEFINICIÓN. Se llama *discriminante* de f a $d_f = d(\rho_1, \ldots, \rho_n)$.

Explícitamente, $d_f = \prod_{i<j}(\rho_j - \rho_i)^2 = \prod_{i<j}(\rho_i - \rho_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\rho_i - \rho_j)$.

Disgresión. Consideremos una extensión E/K de grado $[E : K] = n$. Siendo E/K separable, disponemos de la forma traza $(x, y) \mapsto T_{E/K}(x.y)$. Dada una matriz $(a_i)_{i=1}^n$, se define

$$\text{dis}_{E/K}(a_i)_{i=1}^n := \det(T_{E/K}(a_i.a_j))_{1\leq i,j\leq n} = \det(\varphi_i(a_j))^2_{1\leq i,j\leq n},$$

donde $(\varphi_i)_{i=1}^n$ es una numeración de $\text{Hom}(E/K, C/K)$, y C/K es una clausura algebraica de E.

Tomando $E = K(a)$, se tiene $\text{dis}_{E/K}(a^{i-1})_1^n = \prod_{i<j}(a_j - a_i)^2$.

Notar que si f es irreducible y separable, y $a \in E$ es cualquier raíz de f, entonces

$$d_f = \text{dis}_{K(a)/K}\,(a^{i-1})_{1\leq i\leq n}.$$

Propiedades del discriminante.

I). $d_f = 0$ *si y sólo si* f *tiene una raíz múltiple.*

DEMOSTRACIÓN. Trivial, a partir de la expresión explícita de d_f. □

II). *Si* $f = X^n + \sum_{k=1}^n (-1)^k a_k\, X^{n-k}$, *entonces* $d_f = \delta(a_1, \ldots, a_n)$. *Luego* $d_f \in P[a_1, \ldots, a_n] \subseteq K$ *(*P *es el subanillo primo).*

DEMOSTRACIÓN. Se tiene $d_f = \delta(s_1, \ldots, s_n) \Rightarrow d_f = \delta(s_1(\rho_1, \ldots, \rho_n), \ldots, s_n(\rho_1, \ldots, \rho_n))$.

Por otra parte, consideremos $h = \prod_{i=1}^{n}(X - X_i) = X^n + \sum_{k=1}^{n}(-1)^k s_k\, X^{n-k}$. Con lo cual

$$f = \prod(X - \rho_i) \Rightarrow f = h(\rho_1, \ldots, \rho_n, X) = X^n + \sum_{k=1}^{n}(-1)^k s_k(\rho_1, \ldots, \rho_n)X^{n-k}.$$

Por lo tanto, $a_k = s_k(\rho_1, \ldots, \rho_n)$, $1 \leq k \leq n$. □

III). *La definición de* d_f *no depende de la elección de un cuerpo de descomposición* E/K *de* f *ni de la elección de una numeración por multiplicidad* $(\rho_i)_{i=1}^n$ *de las raíces de* f *en* E.

DEMOSTRACIÓN. Basta aplicar ii) pues δ está unívocamente determinado por d, y a su vez d está unívocamente determinado por $n = \operatorname{gr} f$. □

Ejemplos:

i) Grado 2. Si $f = X^2 - a_1X + a_2$, $d_f = a_1^2 - 4a_2$.

ii) Grado 3. Si $f = X^3 - a_1X^2 + a_2X - a_3$, entonces $d_f = 18a_1a_2a_3 + a_1^2a_2^2 - 4a_1^3a_3 - 4a_2^3 - 27a_3^2$.

Ejercicio. Conservando las notaciones anteriores se toma $n = 4$.

Sea $g = (X - \tau_1)(X - \tau_2)(X - \tau_3)$, donde

$$\tau_1 = \rho_1\rho_2 + \rho_3\rho_4,$$

$$\tau_2 = \rho_1\rho_3 + \rho_2\rho_4,$$

$$\tau_3 = \rho_1\rho_4 + \rho_2\rho_3.$$

g se llama el *resolvente cúbico* de f.

i) Probar que $d_f = d_g$.

ii) Verificar que $g = X^3 - b_1\,X^2 + b_2\,X - b_3$, donde

$$b_1 = a_1, \qquad b_2 = a_1a_3 - 4a_4, \qquad b_3 = a_1a_4 - 2a_2a_4 + a_3^2.$$

Luego $g \in P[a_1, a_2, a_3, a_4][X] \subseteq K[X]$.

iii) Expresar d_f en $P[a_1, a_2, a_3, a_4]$.

7. Grupo de Galois de un polinomio.

Sea K un cuerpo. Sea f un polinomio $\in K[X]$, f no constante. Si E/K es un cuerpo de descomposición de f y R es el conjunto de raíces de f en E, cada automorfismo σ de E/K define una permutación σ_R de R pues $\sigma(R) = R$. La aplicación $\sigma \mapsto \sigma_R$ es un morfismo de $\mathbb{G}(E/K)$ en $\mathbb{S}(R)$, que resulta inyectivo, pues R es un sistema de generadores de E/K. Además, si $(\rho_i)_{i=1}^n$ es una numeración de R, se tiene un isomorfismo

$$\mathbb{S}(\rho) : \mathbb{S}_n \to \mathbb{S}(R).$$

En definitiva, empleando ambos morfismos, se obtiene un monomorfismo de $\mathbb{G}(E/K)$ en $\mathbb{S}_n$.

DEFINICIÓN . $\mathbb{G}_f = \operatorname{Im}(\mathbb{G}(E/K) \to \mathbb{S}_n)$ se llama el *grupo de Galois de* f.

En realidad, esta definición depende de la elección de un cuerpo de descomposición E/K de f, y de una numeración $(\rho_i)_{i=1}^n$ del conjunto R de raíces de f en E. Efectuando una nueva elección de tales objetos, se obtiene un grupo de permutaciones de grado n, isomorfo al anterior. Luego, se ha definido una clase de isomorfía de grupos; más precisamente, de grupos de permutaciones de grado n.

La independencia, salvo isomorfismos, de la elección de una numeración $(\rho_i)_{i=1}^n$ del conjunto R de raíces de f en E se verifica en la forma siguiente:

Si $(\rho_i')_{i=1}^n$ es otra numeración de R, existe una (única) permutación π de R tal que $\rho_i' = \pi_{\rho(i)}$, para $1 \leq i \leq n$ (a saber $\pi = \rho'\rho^{-1}$). Luego, es conmutativo el triángulo

$$\begin{array}{ccc} \mathbb{S}(R) & \xrightarrow{\mathbb{S}(\pi)} & \mathbb{S}(R) \\ & \mathbb{S}(\rho)\nwarrow \quad \nearrow \mathbb{S}(\rho') & \\ & \mathbb{S}_n. & \end{array}$$

Por lo tanto, si G es el grupo de permutaciones de R, $\mathbb{S}(\rho)^{-1}(G) \simeq \mathbb{S}(\rho')^{-1}(G)$. En efecto $\rho' = \pi\rho$, implica $\mathbb{S}(\pi)\mathbb{S}(\rho) = \mathbb{S}(\rho')\rho$ y $\mathbb{S}(\pi)\mathbb{S}(\rho) = \mathbb{S}(\rho') \Rightarrow \mathbb{S}(\rho)^{-1}\mathbb{S}(\pi)^{-1} = \mathbb{S}(\rho')^{-1} \Rightarrow \mathbb{S}(\rho')^{-1}(G) = \mathbb{S}(\rho)^{-1}(\mathbb{S}(\pi)^{-1}(G)) \simeq \mathbb{S}(\rho)^{-1}(G)$.

En cuanto a la independencia, salvo isomorfismos, de la elección de un cuerpo de descomposición E/K de f, si E'/K es también un cuerpo de descomposición de f, existe un isomorfismo $\varphi : E/K \to E'/K$, que induce una biyección $\psi : R \to R'$, donde R' es el conjunto de raíces de f en E'. Luego, se tiene el cuadrado conmutativo

$$\begin{array}{ccc} \mathbb{G}(E/K) & \longrightarrow & \mathbb{S}(R) \\ \mathbb{G}(\varphi)\downarrow & & \downarrow \mathbb{S}(\psi) \\ \mathbb{G}(E'/K) & \longrightarrow & \mathbb{S}(R'). \end{array}$$

Por lo tanto, $\operatorname{Im}(\mathbb{G}(E/K) \to \mathbb{S}(R)) \simeq \operatorname{Im}(\mathbb{G}(E'/K) \to \mathbb{S}(R'))$.

Ejemplos (que se obtienen reformulando resultados conocidos).

i) Si K es un cuerpo finito de q elementos, y $f = X^{q^n} - X$ entonces $\mathbb{G}_f$ es un grupo cíclico de orden n.

En efecto, sea E/K un grupo de descomposición de f, de modo que $\mathbb{G}_f \simeq \mathbb{G}(E/K)$.

Como K finito y $[E : K] < \infty$, E/K es cíclica. Esto nos dice que E/K es galoisiana y que $\mathbb{G}(E/K)$ es cíclico. Como $(G(E/K) : 1) = [E : K]$, debe verificarse que $[E : K] = n$.

Sea R el conjunto de raíces de f en E. Sea σ el automorfismo de E dado por $x \mapsto xq^n$. Por un lado $\partial f = -1 \Rightarrow \operatorname{card} R = q^n$. Por otro, ${}^{\sigma}E = R \Rightarrow R$ es un subcuerpo de $E \Rightarrow E = K(R) = R$ $\Rightarrow E$ tiene q^n elementos.

ii) Si K es un cuerpo de característica p y $f = X^n - 1$, donde $p \nmid n$, entonces $\mathbb{G}_f$ es isomorfo a un subgrupo de $\mathbb{U}_n$ con lo cual $\mathbb{G}_f$ es abeliano de orden un divisor de $\varphi(n)$.

Además $\mathbb{G}_f$ tiene orden $\varphi(n)$, vale decir $\mathbb{G}_f \simeq \mathbb{U}_n \Leftrightarrow C_n$ (el polinomio ciclotómico sobre K de índice n) es irreducible en $K[X]$.

iii) Si K es un cuerpo que contiene las raíces n-ésimas de la unidad, y $f = X^n - a$, con $a \in K^\times$, entonces $\mathbb{G}_f$ es un grupo cíclico de orden un divisor d de n. Además $d = \min\{r \in \mathbb{N} : a^r \in (K^\times)^n\}$.

iv) Si K es un cuerpo de característica p, $p \neq 0$, y $f = X^p - X - a$, entonces $\mathbb{G}_f$ es trivial (f tiene una raíz -y en consecuencia todas- en K) o $\mathbb{G}_f$ es un grupo cíclico de orden p (f es irreducible).

Ejercicios.

1) Sea K un cuerpo. Sea p un número primo. Dado $a \in K$, si $X^p - a$ no tiene raíces en K, entonces es irreducible en $K[X]$.

2) Sea K un cuerpo de característica p, y sea $f = X^n - c$, con $c \in K$. Entonces $\mathbb{G}_f$ es isomorfo a un subgrupo del grupo de permutaciones de $\mathbb{Z}_n$ de la forma $x \mapsto ax + b$ con $a \in \mathbb{U}_n$, $b \in \mathbb{Z}_n$, con lo cual $(G_f : 1) | \varphi(n).n$

Además, en el caso $K = \mathbb{Q}$, y f irreducible (por ejemplo, c primo), $(G_f : 1) = \varphi(n).n$, vale decir $\mathbb{G}_f$ es isomorfo al grupo de permutaciones indicado.

Recordemos brevemente que la teoría de Galois determina una correspondencia entre el conjunto de cuerpos intermedios de una extensión galoisiana de grado finito $\mathcal{I}(E/K)$ y el conjunto de subgrupos del grupo de Galois $\mathcal{S}(E/K)$. Esta correspondencia esta dada por $F \mapsto \mathbb{G}(E/F)$, $H \mapsto E^H$

Fijado un cuerpo de descomposición E/K de f y una numeración $(\rho_i)_{i=1}^n$ de las raíces de f en E, vista la definición de $\mathbb{G}_f$, resulta fijado un isomorfismo de $\mathbb{G}(E/K)$ en $\mathbb{G}_f$. Luego se tienen aplicaciones recíprocas entre $\mathcal{S}(E/K)$ y el conjunto $\mathcal{S}_f$ de subgrupos de $\mathbb{G}_f$. Componiendo estas aplicaciones con las aplicaciones de Galois correspondientes a E/K, se obtienen aplicaciones entre $\mathcal{I}(E/K)$ y $\mathcal{S}_f$. Dado un cuerpo intermedio F de E/K, si $G_{f,F}$ nota el grupo de Galois de $f \in F[X]$, definido a partir de E/F y $(\rho_i)_{i=1}^n$, (que resulta un subgrupo de G_f) entonces, $F \to G_{f,F}$ es la aplicación construída de $\mathcal{I}(E/K)$ en $\mathcal{S}_f$.

Llamando $g : \mathcal{I}(E/K) \to \mathcal{S}_f$ y $c : \mathcal{S}_f \to \mathcal{I}(E/K)$ a las aplicaciones construidas, el teorema de Galois se formula como sigue:

TEOREMA (GALOIS). *Se verifican las siguientes proposiciones:*

i) Respecto de la relación de inclusión, $\mathcal{I}(E/K)$ y $\mathcal{S}_f$ son reticulados completos, y c y g son aplicaciones decrecientes.

ii) $g \circ c = \mathrm{id}_{\mathcal{S}_f}$. Además $(H : 1) = [E : c(H)]$ para todo $H \in \mathcal{S}_f$.

iii) Si f es separable, $c \circ g = \mathrm{id}_{\mathcal{I}(E/K)}$. Además

$$[F : K] = (g(K) : g(F)), \quad \forall F \in \mathcal{I}(E/K).$$

Sea K un cuerpo, $f \in K[X]$, f no constante, E/K un cuerpo de descomposición de f, y $(\rho_i)_{i=1}^n$ una numeración de las raíces de f en E. En consecuencia, está fijado un monomorfismo $\mathbb{G}(E/K) \to \mathbb{S}_n$, $\sigma \mapsto \sigma_f$, vale decir

$$\sigma(\rho_i) = \rho_{\sigma_f(i)},$$

para $1 \leq i \leq n$, y por definición

$$\mathbb{G}_f = \{\sigma_f;\ \sigma \in \mathbb{G}(E/K)\}.$$

OBSERVACIÓN. El siguiente diagrama conmuta:

$$\begin{array}{ccccc} & & \mathbb{G}_f & \xrightarrow{\subseteq} & \mathbb{S}_n \\ & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mathbb{G}_f/\mathbb{S}_n \cap \mathbb{A}_n & \longrightarrow & \mathbb{S}_n/\mathbb{A}_n. \end{array}$$

TEOREMA. *Sea* $a = \prod_{i<j}(\rho_j - \rho_i)$. *Si la característica de* K *no es 2, y las raíces de* f *son simples, entonces*

$$\mathbb{G}_{f,K(a)} = \mathbb{G}_f \cap \mathbb{A}_n,$$

vale decir, $K(a)$ *es el cuerpo de invariantes deducido de* $\mathbb{G}_f \cap \mathbb{A}_n$.

DEMOSTRACIÓN.

Si $g = \prod_{i<j}(X_j - X_i)$, entonces, para toda permutación π de grado n, se tiene $\pi.g = \chi(\pi).g$, donde $\chi(\pi)$ es la asignatura de π. Luego, $\sigma_f.g = \chi(\sigma_f)g$, para todo automorfismo σ de E/K. Especializando ambos miembros de esta igualdad en $(\rho_i)_{1\leq i\leq n}$ resulta

$$\sigma(a) = \chi(\sigma_f).a.$$

En efecto

$$\sigma_f(g) = g(X_{\sigma_f(1)}, \ldots, \chi_{\sigma_f(n)}) \Rightarrow$$

$$\sigma_f.g(\rho_i, \ldots, \rho_n) = g(\rho_{\sigma_f(1)}, \ldots, \rho_{\sigma_f(n)}) = g(\sigma(\rho_1), \ldots, \sigma(\rho_n)) = \sigma(g(\rho_1, \ldots, \rho_n)) = \sigma(a),$$

y $[\chi(\sigma_f).g](\rho_1, \ldots, \rho_n) = \chi(\sigma_f)a$. Luego, considerando que $\operatorname{car} K \neq 2$, y $a \neq 0$

$$(*) \qquad \sigma(a) = a \Longleftrightarrow \chi(\sigma_f) = 1.$$

En efecto, $\Leftarrow$ vale siempre, y $\Longrightarrow$ sigue porque $\chi(\sigma_f)(a) = a \Longrightarrow \chi(\sigma_f).1 = 1 \Longrightarrow \chi(\sigma_f) \equiv 1(\operatorname{car} K) \Longrightarrow \chi(\sigma_f) = 1$. De (*), $\mathbb{G}_{f,k(a)} = \mathbb{G}_f \cap \mathbb{A}_n$. El teorema de Galois nos permite ahora concluir. □

COROLARIO. *Las permutaciones de* $\mathbb{G}_f$ *son pares si y sólo si,* $a \in K$. *En particular, en caso de que* f *sea mónico, las permutaciones de* $\mathbb{G}_f$ *son pares, si y sólo si,* d_f *es un cuadrado en* K.

DEMOSTRACIÓN. i) $\mathbb{G}_f \subseteq \mathbb{A}_n \Longleftrightarrow \mathbb{G}_f \cap \mathbb{A}_n = \mathbb{G}_f \Longleftrightarrow \mathbb{G}_{f,K(a)} = \mathbb{G}_f \Longleftrightarrow$ (gracias al teorema de Galois) $K(a) = K \Longleftrightarrow a \in K$. Si f es mónico $d_f = a^2$, y $a \in K \Longleftrightarrow a^2 \in K^2$. □

Ejercicio.

Sea $a = \sum_{\pi\in\mathbb{A}_n} \prod_{1\leq i\leq n} \rho_{\pi(i)}^{i-1}$. Si car $K = 2$, y las raíces de f son simples, entonces $\mathbb{G}_{f,K(a)} = \mathbb{G}_f \cap \mathbb{A}_n$, vale decir $K(a)$ es el cuerpo de invariantes deducido de $\mathbb{G}_f \cup \mathbb{A}_n$.

Indicación. $\supseteq$ es fácil: $\sigma_f \in \mathbb{A}_n \Rightarrow \sigma(a) = a$.

$\subseteq$: Si $\sigma \in E/K$, $\sigma(a) = a$ y $\sigma \notin \mathbb{A}_n$. (Usar el determinante de Van der Monde).

TEOREMA. *Si f es irreducible, entonces $\mathbb{G}_f$ es transitivo. Recíprocamente, si $\mathbb{G}_f$ es transitivo y las raíces de f son simples, entonces f es irreducible.*

DEMOSTRACIÓN. $\Rightarrow$) Suponiendo f irreducible, cualesquiera sean los índices i, j; ρ_i y ρ_j tienen el mismo polinomio minimal. Luego, como E/K es una extensión normal, $\exists\, \sigma \in \mathbb{G}(E/K) : \sigma(\rho_i) = \rho_j$, con lo cual $\sigma_f(i) = j$.

$\Leftarrow$) Recíprocamente, sea g un divisor irreducible de f en $K[X]$, y sea i un índice tal que ρ_i es raíz de g. Como $\mathbb{G}_f$ es transitivo, $\forall j\ \exists \pi \in \mathbb{G}_f : \pi(i) = j$. Luego, si σ es el automorfismo de E/K tal que $\sigma_f = \pi$, $\sigma(\rho_i) = \rho_j$, con lo cual ρ_j es raíz de g. Por lo tanto, suponiendo las raíces de f simples, g es un asociado de f. En particular, f es irreducible. $\square$

Ejercicio.

Si K es un cuerpo finito y $f \in K[X]$ es irreducible y tiene grado $n > 0$, entonces $\mathbb{G}_f$ está generado por un n-ciclo, que puede tomarse como $(12\ldots n)$.

Indicación. Como K es perfecto, f es separable. además E/K es cíclica.

Ejemplos.

i) grado 2. Si f tiene una raíz múltiple, entonces $\mathbb{G}_f = \mathbb{S}_1 = 1$. Si f tiene sus raíces simples, escribiendo

$$f = X^2 - a_1 X + a_2$$

(no hay inconveniente en suponer f mónico), resulta, para $\operatorname{car} K \neq 2$:

$$\mathbb{G}_f = \begin{cases} \mathbb{A}_2 = 1 & \text{si } a_1^2 - 4a_2 \in K^2, \\ \mathbb{S}_2 & \text{si no.} \end{cases}$$

ii) grado 3.

Si f tiene una raíz $c \in K$ de multiplicidad m, y $G \in K[X]$ satisface $f = (x-c)^m g$, entonces $\mathbb{G}_f \simeq \mathbb{G}_g$, suponiendo g no constante. (Pues $E = K(R) = K(R - \{c\})$. Por lo tanto

$$\mathbb{G}_f = \begin{cases} \mathbb{G}_g & \text{ya calculado en i) si } m = 1, \\ \mathbb{S}_1 = 1 & \text{si } m = 2, \\ \mathbb{S}_1 = 1 & \text{si } m = 3. \end{cases}$$

Si f no tiene raíces en K, f resulta irreducible, con lo cual $\mathbb{G}_f$ es $\mathbb{S}_3$ o $\mathbb{A}_3$ (pues es transitivo); si $\operatorname{car} K \neq 2$, más precisamente, escribiendo $f = X^3 - a_1 X^2 + a_2 X - a_3$, se tiene

$$\mathbb{G}_f = \begin{cases} \mathbb{A}_3 & \text{si } 18\, a_1 a_2 a_3 + a_1^2 a_2^2 - 4a_1^3 a_3 - 4a_2^3 - 27 a_3^2 \in K^2 \\ \mathbb{S}_3 & \text{si no.} \end{cases}$$

Ejercicios.

1. Calcular $\mathbb{G}_f$ en los siguientes casos:

i) $f = X^2 - a$.

ii) $f = X^3 + bX + c$.

El interés de esto reside en el siguiente resultado. Sea K un cuerpo de caracaterística p. Sea $f \in K[X]$, $\operatorname{gr} f = n > 0$. Si p no divide a n, f puede transformarse mediante una substitución lineal, en un polinomio $g \in K[X]$, mónico, de grado n, con coeficiente nulo en X^{n-1}, pero $\mathbb{G}_f \simeq \mathbb{G}_g$.

2. Se conservan las notaciones generales fijadas. Además, se supone $\operatorname{car} K \neq 2$; $\operatorname{gr} f = 4$, y que las raíces de f son simples. g es resolvente cúbico de f, con raíces τ_i, $1 \leq i \leq 3$. Probar que $\mathbb{G}_{f,K(\tau_1,\tau_2,\tau_3)} = \mathbb{G}_f \cap V$. ($V$ es el *Vierergruppe de Klein.*)

Sugerencia. $\supseteq$: $\sigma_f \in V \Rightarrow \sigma(\tau_i) = \tau_i$, $1 \leq i \leq 3$.

$\subseteq$: Es fácil ver que $\mathbb{G}_{f,K(\tau_1,\tau_2,\tau_3)} \subseteq \mathbb{G}_{f,K(a)}$. Pero $\mathbb{G}_{f,K(a)} = \mathbb{G}_f \cap \mathbb{A}_4$. Si $\sigma_f \in \mathbb{A}_4 - V \Rightarrow \sigma_f = (ijk)$, absurdo pues $\sigma(\tau_p) \neq \tau_q$.

3. Mostrar que $\mathbb{G}_g \simeq \mathbb{G}_f / \mathbb{G}_f \cap V$. Luego, verificar que, suponiendo f irreducible

i) Si $\mathbb{G}_f = \mathbb{S}_4 \Rightarrow \mathbb{G}_g$ tiene orden 6.

ii) Si $\mathbb{G}_f = \mathbb{A}_4 \Rightarrow \mathbb{G}_g$ tiene orden 3.

iii) Si $\mathbb{G}_f = V \Rightarrow \mathbb{G}_g$ tiene orden 1.

iv) Si $\mathbb{G}_f$ es un conjugado de C, $\mathbb{G}_g$ tiene orden 2.

v) Si $\mathbb{G}_f$ es un conjugado de D, $\mathbb{G}_g$ tiene orden 2.

Luego, el orden de $\mathbb{G}_g$ cuando no es 2, permite calcular $\mathbb{G}_f$.

4. Si f es irreducible y $\mathbb{G}_g$ tiene orden 2, entonces: $\mathbb{G}_f \simeq C$ ó $\mathbb{G}_f \simeq D$ según que f sea o no, respectivamente reducible sobre $K(a)$.

Sugerencia: En cualquiera de estos casos, $\mathbb{G}_f \not\subseteq \mathbb{A}_4$, con lo cual $a \in k$, vale decir $[K(a) : K] = 2$. Entonces calcular $(\mathbb{G}_f : 1)$ usando $\mathbb{G}_{f,K(a)}$.

OBSERVACIÓN. Si $f = f_1 f_2$, $\operatorname{gr} f_i = 2$, se deduce del teorema de Galois que $\mathbb{G}_f / \mathbb{G}_{f_1} \simeq \mathbb{G}_{f_2}$. De modo que se tiene una sucesión exacta

$$1 \to \mathbb{G}_{f_1} \to \mathbb{G}_f \to \mathbb{G}_{f_2} \to 1.$$

5. Calcular el grupo de Galois de $X^4 + 3X^3 - 3X - 2$ sobre $\mathbb{Q}$. Idem con $X^4 - 2$.

6. (Van der Waerden) Calcular los grupos de Galois sobre $\mathbb{Q}$ de los polinomios:

$$X^3 - 2; \quad X^3 + 2X + 1; \quad X^4 - 5X^2 + 6;$$
$$X^4 + X^2 + 1; \quad X^4 + 1; \quad X^4 + X^2 + X + 1$$

7. (Lang) (Cap 8, ejercicio 12 p. 276, Aguilar).

7.1. Cápsula normal.

DEFINICIÓN. Dada una extensión algebraica E/K, se llama *cápsula normal* de E/K a toda extensión normal N/K que tiene a E como cuerpo intermedio tal que si L/K es una subextensión normal de N/K que tiene a E como cuerpo intermedio, entonces $L = N$.

Propiedades. Dada una extensión algebraica E/K, se verifican:

I). *Dado un isomorfismo de extensiones $\varphi : N/K \to N'/K$, si N/K es una cápsula normal de E/K, entonces N'/K es una cápsula normal de $\varphi(E)/K$. (En particular, es una cápsula normal de E/K si $N/E \simeq N'/E$).*

DEMOSTRACIÓN. Como N/K es una extensión normal tal que $E \in \mathcal{I}(N/K)$, resulta N'/K resulta una extensión normal tal que $\varphi(E) \in \mathcal{I}(N'/K)$. Si L'/K es una subextensión normal de N'/K que tiene a $\varphi(E)$ por cuerpo intermedio, entonces empleando el isomorfismo inverso de φ, $\varphi^{-1}(L')/K$ es una subextensión normal de N/K que tiene a $E = \varphi^{-1}\varphi(E)$ por cuerpo intermedio, con lo cual $\varphi^{-1}(L') = N' \Rightarrow L' = \varphi(N) = N'$. □

II). *Si N/K y N'/K son cápsulas normales de E/K, entonces $N/E \simeq N'/E$; más aún, si N/K y N'/K son subextensiones de una misma extensión de K, entonces $N = N'$.*

DEMOSTRACIÓN. En el caso en que N/K y N'/K son subextensiones de una misma extensión de K, resulta $N = N'$ considerando $N \cap N'/K$. En el caso general, sean C/E y C'/E clausuras algebraicas de E que tienen a N y N' por cuerpos intermedios, respectivamente. Dado un isomorfismo $\varphi : C/E \to C'/E$, aplicando I), $\varphi(N)/K$ es una cápsula normal de E/K, y como $\varphi(N)/K$ y N'/K son subextensiones de C'/K, resulta $\varphi(N) = N'$. □

III). *Si L/K es una extensión normal que tiene a E por cuerpo intermedio, existe una (única) cápsula normal N/K de E/K, que es una subextensión de L/K. Explícitamente, si G es el grupo de Galois de L/K y S es un sistema de generadores de E/K, entonces $N = K(\cup_{\sigma\in G}\sigma(S))$.*

DEMOSTRACIÓN. Tomar, para la existencia,

$$N = \bigcap\{F \in \mathcal{I}(L/E) : F/K \text{ es normal}\}.$$

En cuanto a la descripción explícita, no hay inconveniente en suponer que L es algebraicamente cerrado. En efecto, si C/K es una clausura algebraica que tiene a L por cuerpo intermedio y $H = \mathbb{G}(C/K)$, como todo automorfismo de L/K es inducido por un automorfismo de C/K, $\cup_{\sigma\in G}\sigma(S) \subseteq \cup_{\tau\in H}\tau(S)$. La normalidad de L/K da la inclusión recíproca. Luego, es claro que $K(\cup_{\sigma\in G}\sigma(S))/K$ es una extensión normal: $\cup_{\sigma\in G}\sigma(S)$ es el saturado de S para la conjugación de L/K. Además, $E = K(S) \subseteq K(\cup_{\sigma}\sigma(S))$.

Si F/K es una subextensión normal de $K(\cup_\sigma \sigma(S))/K$ que tiene por cuerpo intermedio a E,

$$S \subseteq E \subseteq F \Rightarrow \sigma(S) \subset \sigma(F) \subset F \Rightarrow K(\cup_\sigma \sigma(s)) \subseteq F.$$

□

IV). *Existen cápsulas normales de E/K.*

V). *Si $[E:K] < \infty$, también lo es el grado de cualquier cápsula normal de E/K.*

DEMOSTRACIÓN. Con la notación de iii), $\cup_{\sigma\in G} \sigma(S) = \cup_{x\in s} \mathcal{O}_x$, donde $\mathcal{O}_x = \{\sigma(x) : \sigma \in G\}$.

Alternativamente, si $H = \mathrm{Hom}(E/K, L/K)$, $\cup_{\sigma\in G} \sigma(S) = \cup_{\varphi\in H} \varphi(S)$, pues se tiene una aplicación $G \to H$, $\sigma \mapsto \sigma/E$, que es suryectiva por la normalidad de L/K. En este caso, se escoge S finito, y dada cualquier cápsula normal N/K de E/K se toma L conteniendo a N, por ejemplo $L = N$. □

VI). *Si E/K es separable, entonces toda cápsula normal de E/K es separable, o sea Galoisiana.*

DEMOSTRACIÓN. Se vuelve a usar III) tomando S arbitrariamente, por ejemplo $S = E$. □

7.2. Extensiones resolubles.

PROPOSICIÓN. *Dada una extensión algebraica E/K, son equivalentes las siguientes condiciones:*

i) Existe una cápsula normal N_0/K de E/K tal que $\mathbb{G}(N_0/K)$ es resoluble.

ii) Para toda cápsula normal N/K de E/K, $\mathbb{G}(N/K)$ es resoluble.

iii) Existe una extensión normal L/K, que tiene a E por cuerpo intermedio, tal que $\mathbb{G}(L/K)$ es resoluble.

DEMOSTRACIÓN.

i) $\Rightarrow$ ii). Como $N_0/K \simeq N/K$, $\mathbb{G}(N_0/K) \simeq \mathbb{G}(N/K)$.

ii) $\Rightarrow$ iii) pues existen cápsulas normales de E/K.

iii) $\Rightarrow$ i). Se toma N_0/K como la cápsula normal de E/K en L/K. Como N_0/K es una subextensión normal de L/K, que también es normal, $\mathbb{G}(N_0/K)$ es imagen homomórfica de $\mathbb{G}(L/K)$:

$$\mathbb{G}(L/K) \to \mathbb{G}(N_0/K), \qquad \sigma \mapsto \sigma_{N_0}.$$

□

DEFINICIÓN. Una extensión E/K se dice *resoluble* sii E/K es separable de grado finito y E/K satisface una de las condiciones, y en consecuencia todas, de la proposición.

PROPOSICIÓN. *Una extensión E/K es resoluble si y sólo si existe una extensión L/K Galoisiana de grado finito tal que $E \in \mathcal{I}(L/K)$ y tal que $\mathbb{G}(L/K)$ es resoluble.*

DEMOSTRACIÓN. *Suficiencia.* E/K, como subextensión de L/K, resulta separable de grado finito. Además E/K satisface *iii)* de la definición, por medio de L/K.

Necesidad. E/K satisface *i)* de la definición, y basta tomar $L = N_0$. □

COROLARIO. *Sea E/K una extensión Galoisiana de grado finito. E/K es resoluble si y sólo si $\mathbb{G}(E/K)$ es resoluble.*

DEMOSTRACIÓN.

Suficiencia. Por la suficiencia de la proposición anterior.

Necesidad. E/K satisface *i)*; pero $N_0 = E$ por normalidad. □

LEMA. *Dado un isomorfismo de extensiones algebraicas $\varphi : E/K \to E'/K$, si N/K y N'/K son cápsulas normales de E/K y E'/K, entonces existe un isomorfismo $\psi : N/K \to N'/K$ que induce a φ.*

DEMOSTRACIÓN. Si C/E y C'/E' son clausuras algebraicas de E y E' que tienen a N y N' por cuerpos intermedios, respectivamente, existe un isomorfismo $\omega : C/K \to C'/K$ que induce a φ. Como N/K es una cápsula normal de E/K, $\omega(N)/K$ resulta una cápsula normal de E'/K ,$(\omega(E) = \varphi(E) = E')$. Además como $\omega(N)/K$ y N'/K son subextensiones de C'/K, resulta $\omega(N) = N'$. □

PROPOSICIÓN. *Dado un isomorfismo de extensiones $\varphi : E/K \to E'/K$, si E/K es resoluble, entonces E'/K también es resoluble.*

DEMOSTRACIÓN. Con las notaciones del lema, $\mathbb{G}(N/K) \simeq \mathbb{G}(N'/K)$. □

DEFINICIÓN. Una clase de extensiones C de cuerpos se dice *distinguida* si satisface

i) Dadas extensiones E/F y F/K, " $E/F \in C$ y $F/K \in C$" si y sólo si $E/K \in C$.

ii) Si E/K y F/K son subextensiones de L/K ; $E/K \in C$ implica $F(E)/F \in C$ [3].

TEOREMA. *La clase de extensiones resolubles es distinguida.*

DEMOSTRACIÓN. Sean E/K y F/K subextensiones de una extensión L/K, con E/K resoluble. Sea N/K una extensión resoluble galoisiana que tiene a E por cuerpo intermedio. No hay inconveniente en suponer que N/K es una subextensión de L/K. En efecto, puede asumirse que L es algebraicamente cerrado, pues basta tomar una extensión algebraicamente cerrada de L. Si C es la cerradura algebraica de K en L, C/K es una clausura algebraica de K que tiene a E por cuerpo intermedio, y basta tomar N/K como la cápsula normal de E/K en C/K.

Luego, como N/K es una extensión galoisiana de grado finito que tiene a E por cuerpo intermedio, $F(N)/F$ es una extensión galoisiana de grado finito que tiene a $F(E)$ por cuerpo intermedio. Como

[3] $F(E)$ denota el menor cuerpo que contiene a F y aE

N/K es una subextensión normal de $F(N)/K$, se tiene un morfismo de $\mathbb{G}(F(N)/K)$ en $\mathbb{G}(N/K)$, cuyo núcleo es $\mathbb{G}(F(N)/N)$.

Luego como $\mathbb{G}(F(N)/N) \cap \mathbb{G}(F(N)/F) = 1$, por restricción se obtiene un monomorfismo de $\mathbb{G}(F(N)/F)$ en $\mathbb{G}(N/K)$. Considerando que $\mathbb{G}(N/K)$ es resoluble, también lo es $\mathbb{G}(F(N)/F)$, y está probado que $F(E)/F$ es una extensión resoluble. Es inmediato que subextensiones de extensiones resolubles son resolubles.

Para terminar, sean E/F y F/K extensiones resolubles. Sea C/K una clausura algebaraica de K que tiene a E por cuerpo intermedio. Como F/K es resoluble, existe una extensión resoluble galoisiana L/K que tiene a F por cuerpo intermedio; y no hay inconveniente en suponer que L/K es una subextensión de C/K. Como E/F y L/F son subextensiones de C/F y E/F es resoluble, $L(E)/L$ es resoluble, y en consecuencia, existe una extensión resoluble galoisiana N/L que tiene a $L(E)$ por cuerpo intermedio. Sea M/K la cápsula normal de N/K en C/K. Es claro que M/K es una extensión galoisiana, de grado finito, que tiene a E por cuerpo intermedio.

Falta verificar que $\mathbb{G}(M/K)$ es resoluble. Como L/K es una subextensión normal de M/K que también es normal, se tiene un epimorfismo de $\mathbb{G}(M/K)$ en $\mathbb{G}(L/K)$, que es un grupo resoluble, cuyo núcleo es $\mathbb{G}(M/L)$. Basta comprobar entonces que $\mathbb{G}(M/L)$ es resoluble. Como $M = K(\cup_{\sigma\in G}\sigma(N))$, donde $G = \mathrm{Hom}(N/K, C/K)$, teniendo presente que $\sigma(N)/L$ es galoisiana (pues N/L es galoisiana y $\sigma(L) = L$,) se obtiene un morfismo de $\mathbb{G}(M/L)$ en $\mathbb{G}(\sigma(N)/L)$. Luego se obtiene un morfismo de $\mathbb{G}(M/L) \to \prod_{\sigma\in G} \mathbb{G}(\sigma(N)/L)$, que es inyectivo pues $\cup_\sigma \sigma(N)$ genera M/K. Pero $\mathbb{G}(\sigma(N)/L) \simeq \mathbb{G}(N/L)$ es resoluble. □

7.3. Extensiones resolubles por radicales.

DEFINICIÓN. Sea K un cuerpo de característica p. Una *torre de raíces* de una extensión E/K es una sucesión $(E_i)_{0\le i\le n}$ de cuerpos intermedios de E/K tal que E_{i+1} es una extensión de E_i, $0 \le i \le n$, que se obtiene adjuntando una raíz de un polinomio de la forma $x^n - a$, con $n \in \mathbb{N}$ no divisible por p y $a \in E_i$, o $X^p - X - a$, con $a \in E_i$, si $p \neq 0$, y además $E_0 = K$ y $E_n = E$.

Propiedades.

I). *Si una extensión E/K tiene una torre de raíces $(E_i)_{0\le i\le n}$, entonces E_j/E_i, con $0 \le i \le j \le n$ es una extensión separable de grado finito. En particular, E/K lo es.*

DEMOSTRACIÓN. Si $j = i$ claro. Si $j > i$, se deduce por transitividad del hecho de que E_{i+1}/E_j es una extensión separable de grado finito, pues se obtiene adjuntando a E_i un elemento algebraico separable de E_j. □

II). *Dado un isomorfismo de extensiones $\varphi : E/K \to E'/K$, si E/K tiene una torre de raíces, entonces E'/K también tiene una torre de raíces.*

DEMOSTRACIÓN. Si $(E_i)_{0\leq i\leq n}$ es una torre de raíces de E/K, entonces $(\varphi(E_i))_{0\leq i\leq n}$ es una torre de raíces de E'/K. Tener presente que si $E_{i+1} = E_i(x)$, donde x es raíz de $f \in E_i[X]$, entonces $\varphi(E_{i+1}) = \varphi(E_i)(\varphi(x))$, donde $\varphi(x)$ es raíz de $\overline{\varphi}(f) \in \varphi(E_i)[X]$. □

III). *La clase de extensiones que admiten torres de raíces satisface las condiciones de transitividad y de extensión de escalares.*

DEMOSTRACIÓN. Dadas extensiones E/F y F/K, si $(E_i)_{0\leq i\leq n}$ es una torre de raíces de E/F, y $(F_j)_{0\leq j\leq m}$ es una torre de raíces de F/K, entonces $(L_k)_{0\leq k\leq n+m+1}$ es una torre de raíces de E/K, donde

$$L_k = \begin{cases} F_k & si\ 0 \leq k \leq m \\ E_{k-m+1} & m \leq k \leq n+m+1. \end{cases}$$

Sean E/K y F/K subextensiones de una extensión de K, y sea $(E_i)_{0\leq i\leq n}$ una torre de raíces de E/K. Luego $(F(E_i))_{0\leq i\leq n}$ es una torre de raíces de $F(E)/F$, tener presente que si $E_{i+1} = E_i(x)$, con x raíz de $f \in E_i[X]$, entonces $F(E_{i+1}) = F(E_i)(x)$ y $f \in F(E_i)[X]$. □

DEFINICIÓN. Una extensión E/k se dice *resoluble por radicales* sii existe una extensión L/K que tiene a E por cuerpo intermedio y que admite una torre de raíces.

Propiedades.

I). *Si una extensión E/k es resoluble por radicales, entonces E/k es separable de grado finito.*

DEMOSTRACIÓN. E/K es subextensión de una extensión L/K que es separable de grado finito. □

II). *Dado un isomorfismo de extensiones $\varphi : E/K \to E'/K$, si E/K es resoluble por radicales, entonces E'/K también es resoluble por radicales.*

DEMOSTRACIÓN. Sea L/K una extensión, con una torre de raíces que tiene a E por cuerpo intermedio, y sea C'/K una clausura algebraica de K que tiene a E' por cuerpo intermedio, L/K es algebraica, φ es inducido por un morfismo $\psi : L/K \to C'/K$, pero $\psi(L)/K$ tiene una torre de raíces, pues L/K la tiene, y $\psi(L)$ tiene por cuerpo intermedio a $\psi(E) = \varphi(E) = E'$. □

DEFINICIÓN. Sea K un cuerpo, y sea $f \in K[X]$, no constante. Se dice que la ecuación $f(x) = 0$ (o por abuso, de lenguaje que f es) *resoluble por radicales*, sii existe un cuerpo de descomposición E/K de f que es una extensión resoluble por radicales. Se dice que f es *absolutamente resoluble por radicales* sii f es resoluble por radicales sobre $P(M)$, donde P es el cuerpo primo de K, y M el conjunto de coeficientes de f.

Propiedades .

I). *f es resoluble por radicales si y sólo si todo cuerpo de descomposición de f es resoluble por radicales.*

II). *Si f es resoluble por radicales, entonces f es separable, o sea, los cuerpos de descomposición de f son separables (o sea, galoisianas).*

III). *Dada una exensión F/K, si f es resoluble por radicales sobre K, entonces f es resoluble por radicales sobre F. En particular, si f es absolutamente resoluble por radicales, entonces f es resoluble por radicales.*

DEMOSTRACIÓN. Sea C/F una extensión algebraicamente cerrada. Como $f \in C[X]$, si R es el conjunto de raíces de f en C y $E = K(R)$, entonces E/K es un cuerpo de descomposición de $f \in K[X]$. Luego, E/K es resoluble por radicales, y en consecuencia $F(E)/F$ también es resoluble por radicales. Por otra parte, $F(E) = F(K)(R) = F(R)$, con lo cual $F(E)/F$ es un cuerpo de descomposición de $f \in F[X]$. □

PROPOSICIÓN. *Si una extensión E/K tiene una torre de raíces, existe una extensión galoisiana L/K que tiene a E por cuerpo intermedio y que también tiene una torre de raíces.*

COROLARIO. *Una extensión E/K es resoluble por radicales si y sólo si existe una extensión galoisiana L/K que tiene a E por cuerpo intermedio y que admite una torre de raíces.*

DEMOSTRACIÓN. *Suficiencia.* trivial.

Necesidad. Existe una extensión F/K que tiene a E por cuerpo intermedio y que admite una torre de raíces, por definición. Luego basta aplicar la proposición a F/K. □

DEMOSTRACIÓN DE LA PROPOSICIÓN. Sea $(E_i)_{0\leq i\leq n}$ una torre de raíces de E/K, y sea C/K una clausura algebraica de K que tiene a E por cuerpo intermedio. Se construirá una sucesión $(L_i)_{0\leq i\leq n}$ de cuerpos intermedios de C/K tal que L_i/K es una extensión galoisiana que tiene a E_i por cuerpo intermedio, y que admite una torre de raíces, con lo cual bastará tomar $L = L_n$.

Tomando $L_0 = K$ las condiciones enunciadas se verifican trivialmente. Argumentando por inducción, se supone definido L_i y se toma L_{i+1}/K como la cápsula normal de $L_i.E_{i+1}/K$ en C/K. Como $L_i.E_{i+1}/K$ es separable, pues L_i/K y E_{i+1}/K son separables, entonces L_{i+1}/K es galoisiana, y obviamente tiene a E_{i+1} por cuerpo intermedio. Sean $a_i \in E$, $0 \leq i < n$, tales que

$$E_{i+1} = E_i(a_i),$$

donde $a_i^{n_i} \in E_i$, con $n_i \in \mathbb{N}$ no divisible por p, o $a_i^p - a_i \in E_i$, siendo $p \neq 0$. Como $E_{i+1} = E_i(a_i)$, resulta que $L_i.E_{i+1} = L_i(E_i)(a_i)$, por lo tanto $L_i\, E_{i+1} = L_i(a_i)$, de donde $L_{i+1} = L_i(O_{a_i})$.

En efecto, sea $G = \mathbb{G}(C/K)$; entonces $L_{i+1} = K\left(\cup_{\sigma\in G}\, \sigma(L_i(a_i))\right) = K(\cup_{\sigma\in G} L_i(\sigma(a_i))) = K(L_i \cup O_{a_i}) = L_i(O_{a_i})$.

Como L_i/K tiene una torre de raíces y $L_i.E_{i+1} = L_i(a_i)$, $L_i.E_{i+1}/K$ también tiene una torre de raíces. Luego basta verificar que $L_{i+1}/L_i.E_{i+1}$ tiene una torre de raíces. En efecto: si $(\sigma_j(a_i))_{1\leq j\leq m}$ es una numeración de O_{a_i}, con $\sigma_1(a_i) = a_i$, se tiene

$$L_i.E_{i+1} = L_i(a_i) = L_i(\sigma_1(a_i)) \subseteq L_i(\sigma_1(a_i), \sigma_2(a_i)) \cdots \subseteq L_i(\sigma_1(a_i), \ldots, \sigma_n(a_i)) = L_{i+1},$$

pero

$$L_i(\sigma_1(a_i), \ldots, \sigma_{j+1}(a_i)) = L_i(\sigma_1(a_i), \ldots, \sigma_j(a_i))(\sigma_{j+1}(a_i))$$

y $\sigma_{j+1}(a_i)^{n_i} = \sigma_{j+1}(a_i^{n_i}) \in \sigma_{j+1}(E_i) \subseteq \sigma_{j+1}(L_i) \subseteq L_i$, o bien $\sigma_{j+1}(a_i)^p - \sigma_{j+1}(a_i) \in L_i$, según que $a_i^{n_i} \in E_i$ ó $a_i^p - a_i \in E_i$. □

TEOREMA. *Una extensión E/K es resoluble por radicales si y sólo si, E/K es resoluble.*

DEMOSTRACIÓN. *Suficiencia.* Sea L/K una extensión galoisiana resoluble que tiene a E por cuerpo intermedio. Sea

$$M = \{p \in \mathbb{P} : p|[L : K] \text{ y } p \neq \operatorname{car} K\},$$

donde $\mathbb{P}$ es el conjunto de primos positivos. Sea $m = \prod_{p\in M} p$.

Sea C/K es una clausura algebraica de K tal que $L \in \mathcal{I}(C/K)$. Sea F/K el cuerpo ciclotómico de índice m en C/K. Como L/K es una extensión galoisiana resoluble, $F(L)/F$ también lo es. Basta probar que $F(L)/F$ tiene una torre de raíces. En efecto, como $F = K(w)$, donde $w \in C$ es una raíz m-ésima primitiva, resulta que $F(L)/K$ tiene una torre de raíces; pero $E \in \mathcal{I}(F(L)/K)$, con lo cual E/K es resoluble por radicales.

Sea entonces $(G_i)_{0\leq i\leq n}$ una serie normal de $G = \mathbb{G}(F(L)/F)$ tal que $(G_i : G_{i+1})$ es un primo p_i, $0 \leq i < n$. Tomando $E_i = {}^{G_i}F(L)$, $(E_i)_{0\leq i\leq n}$ es una sucesión de cuerpos intermedios de $F(L)/F$, y se tiene

$$G_0 = G \Rightarrow E_0 = F, \qquad G_n = 1 \Rightarrow E_n = F(L),$$

$$G_i \supseteq G_{i+1} \Rightarrow E_i \subseteq E_{i+1}, \qquad [E_{i+1} : E_i] = (G_i : G_{i+1}) = p_i.$$

Más aún, como G_{i+1} es normal en G_i, E_{i+1}/E_i es normal, o sea, galoisiana y

$$\mathbb{G}(E_{i+1}/E_i) \simeq G_i/G_{i+1}.$$

En definitiva, E_{i+1}/E_i es una extensión galoisiana de grado p_i. Si $p_i = \operatorname{car} K$, E_{i+1}/E_i es un cuerpo de descomposición de un polinomio de la forma $X^{p_i} - X - a$, con $a \in E_i$, y en consecuencia, se obtiene adjuntando una raíz cualquiera de ese polinomio.

Si $p_i \neq \operatorname{car} K$, como $p_i = (G_i : G_{i+1})|(G : 1) = [F(L) : F]|^4[L : K] \Rightarrow p_i|m$, y así, puesto que $F \subseteq E_i$, E_i contiene las raíces p_i-ésimas de la unidad. Luego E_{i+1} E_i es un cuerpo de descomposición de un polinomio de la forma $X^{p_i} - a$, con $a \in E_i$, y en consecuencia, se obtiene adjuntando una raíz cualquiera de ese polinomio.

Luego $(E_i)_{0 \leq i \leq n}$ es una torre de raíces de $F(L)/F$.

Necesidad. Sea L/K una extensión galoisiana que tiene a E por cuerpo intermedio y que admite una torre de raíces, con "exponentes" e_i, $0 \leq i < n$. Sea

$$m = \prod_{\substack{0 \leq i \leq a_i \\ e_i \neq \operatorname{car} K}} e_i.$$

Si C/K es una clausura algebraica de K que tiene a E por cuerpo intermedio, sea F/K el cuerpo ciclotómico de índice m en C/K. Basta probar que $F(L)/F$ es resoluble. En efecto, como F/K es resoluble trivialmente (pues F/K es abeliana de grado finito), resulta que $F(L)/K$ es resoluble, de donde -por ser subextensión- E/K es resoluble. Como L/K tiene una torre de raíces, $F(L)/F$ también la tiene, más aún, con los mismos exponentes e_i, $0 \leq i \leq n$; sea esa torre $(E_i)_{0 \leq i \leq n}$. Tomando $G_i = \mathbb{G}(F(L)/E_i)$, $(G_i)_{0 \leq i \leq n}$ es una sucesión de subgrupos de $G = \mathbb{G}(F(L)/F)$, y se tiene

$$E_0 = F \Rightarrow G_0 = G, \qquad E_n = F(L) \Rightarrow G_n = 1,$$

$$E_i \subseteq E_{i+1} \Rightarrow G_i \supseteq G_{i+1}, \qquad [E_{i+1} : E_i] = (G_i : G_{i+1}) = n_i.$$

Si E_{i+1} se obtiene adjuntando a E_i una raíz de un polinomio de la forma $X^{e_i} - X - a$, con $a \in E_i$, (lo cual significa que $e_i = \operatorname{car} K \neq 0$), entonces E_{i+1}/E_i es un cuerpo de descomposición de ese polinomio, y en consecuencia, E_{i+1}/E_i es una extensión galoisiana, con lo cual G_{i+1} es normal en G_i, de grado 1 o e_i, pero en cualquier caso G_i/G_{i+1} es cíclico. Por otra parte, si E_{i+1} se obtiene adjuntando a E_i una raíz de un polinomio de la forma $X^{e_i} - a$, con $a \in E_i$ (y en consecuencia $\operatorname{car} K \not| e_i$), como $e_i|m$ (y así, E_i contiene las raíces e_i-ésimas de la unidad) resulta que E_{i+1}/E_i es un cuerpo de descomposición del polinomio $X^{e_i} - a$. Luego E_{i+1}/E_i es una extensión cíclica, con lo cual G_{i+1} es normal en G_i, y $G_i/G_{i+1} \simeq \mathbb{G}(E_{i+1}/E_i)$ es cíclico. Luego $(G_i)_{0 \leq i \leq n}$ es una serie de resolubilidad de $\mathbb{G}(F(L)/F)$. □

COROLARIO. *Sea K un cuerpo. Sea $f \in K[X]$ no constante. f es resoluble por radicales si y sólo si f es separable y $\mathbb{G}_f$ es resoluble.*

---

[4]Como L/K es una subextensión normal de $F(L)/K$, se tiene un morfismo de $\mathbb{G}(F/L)/K)$ en $\mathbb{G}(L/K)$, cuyo núcleo es $\mathbb{G}(F(L)/L)$. Luego, por restricción a $G(F(L)/F)$, se obtiene un monomorfismo de $\mathbb{G}(F(L)/F)$ en $\mathbb{G}(L/K)$. En consecuencia, $(\mathbb{G}(F(L)/F) : 1)|(\mathbb{G}(L/K) : 1)$.

DEMOSTRACIÓN. Sea E/K un cuerpo de descomposición de f.

Suficiencia. Como f es separable, E/K es una extensión galoisiana. Por otra parte $\mathbb{G}(E/K) \simeq \mathbb{G}_f$, luego es resoluble. Por ende E/K es resoluble, y por el teorema, E/K resulta resoluble por radicales.

Necesidad. Por el teorema, E/K es resoluble. Además f resulta separable, con lo cual E/K es galoisiana. Por lo tanto $\mathbb{G}_f \simeq \mathbb{G}(E/K)$ es resoluble. □

DEFINICIÓN. Sea K un cuerpo de característica p. Una *torre clásica de raíces* de una extensión E/K es una sucesión $(E_i)_{0\leq i\leq n}$ de cuerpos intermedios de E/K tal que E_{i+1} es una extensión de E_i, para $0 \leq i < n$, que se obtiene adjuntando una raíz de un polinomio de la forma $X^q - a$, con q primo $\neq p$, y $a \in E_i$, que es irreducible en $E_i[X]$, y además $E_0 = K$ y $E_n = E$.

Una extensión E/K se dice *clásicamente resoluble por radicales* sii existe una extensión L/K que tiene a E por cuerpo intermedio, y que admite una torre clásica de raíces.

Se supone ahora $p \neq 0$. Una *p-torre de raíces* de una extensión E/K es una sucesión $(E_i)_{0\leq i\leq n}$ de cuerpos intermedios de E/K tal que E_{i+1} es una extensión de E_i, $0 \leq i < n$, que se obtiene adjuntando una raíz de un polinomio de la forma $X^p - X - a$, con $a \in E_i$, que es irreducible en $E_i[X]$, y además $E_0 = K$ y $E_n = E$.

Una *p-extensión de* K es una extensión galoisiana E/K tal que $\mathbb{G}(E/K)$ es un p-grupo.

Ejercicios.

1. i) Sea E/K un cuerpo ciclotómico de índice n. Si $\operatorname{car} K$ es 0, o bien es mayor que los divisores primos de n, entonces E/K es clásicamente resoluble por radicales.

ii) Exhibir torres clásicas de raíces en los casos $K = \mathbb{Q}$ y $n = 5, 7$.

Idea de la solución de i). Sea $d = [E : K]$. Como $d|\varphi(n)$, resulta $d < n$, descartando el caso trivial $n = 1$, y además todo divisor primo de d es menor o igual que un divisor primo de n, con lo cual las hipótesis sobre K se satisfacen respecto de d (como índice).

Si $n = \prod_{i=1}^{r} p_i^{e_i}$ entonces $\varphi(n) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$, pues $\mathbb{U}_n \simeq \prod_{i=1}^{r} \mathbb{U}_{p_i^{e_i}}$ y $\varphi(p^e) = p^{e-1}(p-1)$.

Sea p primo: si $p|\varphi(n)$, entonces existe j tal que $p = p_j$, ó $p|p_j - 1$; o sea, existe j: $p = p_j$, ó $p \leq p_j - 1 < p_j$.

Luego, si C/K es una clausura algebraica de K que tiene a E por cuerpo intermedio y F/K es el cuerpo ciclotómico de índice d en C/K, argumentando por inducción global en el índice, puede suponerse que F/K es clásicamente resoluble por radicales. Si L/K es una extensión que tiene a F por cuerpo intermedio y que admite una torre clásica de raíces, no hay inconveniente en asumir que L es un subcuerpo de C, pues existen morfismos de L/F en C/F. Ahora, como $L(E)/L$, es una extensión abeliana, $[L(E) : L]|d$ y L contiene las raíces d-ésimas de la unidad (pues $F \subseteq L$), resulta que $L(E)/L$ tiene una torre clásica de raíces.

2. i) Sea E/K una extensión de grado finito tal que $\operatorname{car} K = 0$, ó es mayor que los divisores primos de $[E : K]$ y, en este último caso, E/K es galoisiana. Si E/K es resoluble por radicales, entonces E/K es clásicamente resoluble por radicales.

ii) Si E/K es una extensión tal que $\operatorname{card} K = 2^2$ y $\operatorname{card} E = 2^6$, entonces E/K es clásicamente resoluble por radicales (Pues $\operatorname{car} K = 2 < 3 = [E : K]$).

3. Sea K un cuerpo de característica $p \neq 0$. E/K es una p-extensión de grado finito si y sólo si E/K es una exensión normal con una p-torre de raíces.

8. Polinomios generales.

Sea K un cuerpo, sea $n \in \mathbb{N}$.

DEFINICIÓN. $f = X^n + \sum_{1 \leq i \leq n} (-1)^i X_i X^{n-i} \in K(X_1, \ldots, X_n)[X]$ se llama el *polinomio* (mónico) *general de grado* n, o también el polinomio (mónico) con n coeficientes genéricos sobre K.

OBSERVACIÓN. Dado $g \in K[X]$, mónico, de grado n, si $g = X^n + \sum_{i \leq i \leq n} (-1)^i a_i X^{n-i}$, entonces $g = f(a_1, \ldots, a_n, X)$ considerando f en $K[X_1, \ldots, X_n, X]$.

TEOREMA. *Si f es el polinomio general sobre K de grado n, entonces $\mathbb{G}_f = \mathbb{S}_n$.*

DEMOSTRACIÓN. Sea h el polinomio (mónico) con n raíces genéricas sobre K:

$$h = \prod_{i \leq i \leq n} (X - X_i) = X^n + \sum_{i=1}^{n} (-1)^i s_i X^{n-i} \in K(s_1, \ldots, s_n)[X]$$

Se afirma que $\mathbb{G}_h = \mathbb{S}_n$. Es claro que $K(X_1, \ldots, X_n)/K(s_1, \ldots, s_n)$ es un cuerpo de descomposición de h. Por otra parte, cada permutación π de grado n define un automorfismo $\widehat{\pi}$ de $K(X_1, \ldots, X_n)/K$, dada por la especialización por $(X_{\pi(i)})_{1 \leq i \leq n}$. La aplicación $\pi \mapsto \widehat{\pi}$ es un morfismo (inyectivo) de $\mathbb{S}_n$ en $\mathbb{G}(K(X_1, \ldots, X_n)/K)$. Luego la acción $\pi.f = \widehat{\pi}(f) = f(X_{\pi(1)}, \ldots, X_{\pi(n)})$ de $\mathbb{S}_n$ en $K(X_1, \ldots, X_n)$ es compatible con la estructura de extensiones de $K(X_1, \ldots, X_n)/K$. Las fracciones racionales en ${}^{\mathbb{S}_n}K(X_1, \ldots, X_n)$ se dicen simétricas. Se afirma que $\mathbb{G}(K(X_1, \ldots, X_n)/K(S_1, \ldots, S_n)) = \operatorname{Im}(\mathbb{S}_n \to G(K(X_1, \ldots, X_n)/K))$. Tomando G como la imagen, o sea

$$G = \{\widehat{\pi} : \pi \in \mathbb{S}_n\},$$

como ${}^{G}K(X_1, \ldots, X_n) = {}^{\mathbb{S}_n}K(X_1, \ldots, X_n) \supseteq {}^{\mathbb{S}_n}K[X_1, \ldots, X_n]$, resulta que ${}^{G}K(X_1, \ldots, X_n) \supseteq K(S_1, \ldots, S_n)$. Ahora bien, por un teorema de Artin,

$$[K(X_1, \ldots, X_n) : {}^{G}K(X_1, \ldots, X_n)] = (G : 1) = n!,$$

en tanto que

$$[K(X_1, \ldots, X_n) : K((S_1, \ldots, S_n)] \leq n!,$$

pues $\operatorname{gr} h = n$. Luego ${}^{G}K(X_1, \ldots, X_n) = K(S_1, \ldots, S_n)$, y así

$$\mathbb{G}(K(X_1, \ldots, X_n)/K(S_1, \ldots, S_n)) = G.$$

Definiendo $\mathbb{G}_h$ a partir de $K(X_1, \ldots, X_n)/K(S_1, \ldots, S_n)$, y $(X_i)_{1 \leq i \leq n}$ como $\widehat{\pi}(X_i) = X_{\pi(i)}$ $(1 \leq i \leq n)$, vale decir $\widehat{\pi}_h = \pi$, lo cual prueba que $\mathbb{G}_h = \mathbb{S}_n$. Esto también es claro pues $\mathbb{G}_h \simeq G$ y $(G : 1) = n!$

Pasando a la demostración propiamente dicha, como $(s_i)_{1 \leq i \leq n}$ es una familia algebraicamente independiente en $K(X_1, \ldots, X_n)/K$, la especialización por $(s_i)_{1 \leq i \leq n}$ induce un isomorfismo $\varphi : K(X_1, \ldots, X_n)/K \to K(s_1, \ldots, s_n)/K$, tal que $\overline{\varphi}(f) = h$. Luego, si $E/K(X_1, \ldots, X_n)$ es un cuerpo de descomposición de f, por razones de unicidad de los cuerpos de descomposición, existe un isomorfismo $\psi : E/K \to K(X_1, \ldots, X_n)/K$ que induce a φ.

Luego $\mathbb{G}(E/K(X_1, \ldots, X_n)) \simeq \mathbb{G}(K(X_1, \ldots, X_n)/K(s_1, \ldots, s_n))$ por la aplicación

$$\sigma \mapsto \psi\sigma\psi^{-1};$$

tomando $x_i = \psi^{-1}(X_i)$, resulta $(x_i)_{1 \leq i \leq n}$ una numeración de las raíces de f en E, por resultar estas simples.

Definiendo $\mathbb{G}_f$ a partir de $E/K(X_1, \ldots, X_n)$ y de $(x_i)_{1 \leq i \leq n}$ se obtiene el diagrama:

$$\begin{array}{ccc} \mathbb{G}(E/K(X_1, \ldots, X_n)) & \xrightarrow{\sim} & \mathbb{G}(K(X_1, \ldots, X_n)/K(s_1, \ldots, s_n) \\ \downarrow & & \downarrow \\ \mathbb{S}_n & = & \mathbb{S}_n, \end{array}$$

que es conmutativo. En efecto, dado un automorfismo σ de $E/K(X_1, \ldots, X_n)$, $\sigma(x_i) = x_j \Rightarrow (\sigma\psi^{-1})(X_i) = \psi^{-1}(X_j) \Rightarrow (\psi\sigma\psi^{-1})(X_i) = X_j$. Luego $\sigma_f = (\psi\sigma\psi^{-1})_h$, con lo cual,

$$\mathbb{G}_f = \mathbb{G}_h$$

De todas formas, $\mathbb{G}_f = \mathbb{S}_n$ resulta de

$$\mathbb{G}_f \simeq \mathbb{G}(E/K(X_1, \ldots, X_n)) \simeq \mathbb{G}(K(X_1, \ldots, X_n)/K(S_1, \ldots, S_n)) = G,$$

ya que $(G : 1) = n!$ □

COROLARIO. *f es un polinomio irreducible y sus raíces son simples.*

DEMOSTRACIÓN. Como el grado de las permutaciones de $\mathbb{G}_f$ coincide con $\operatorname{gr} f$, resulta que las raíces de f son simples (por supuesto este hecho está contenido en la demostración del teorema). Luego como $\mathbb{G}_f$ es transitivo, resulta que f es irreducible. □

COROLARIO (TEOREMA DE ABEL-RUFFINI). *f es resoluble por radicales si y sólo si $n \leq 4$.*

DEMOSTRACIÓN. Siendo f un polinomio separable, f es resoluble por radicales si y sólo si $\mathbb{G}_f$ es resoluble. Por otra parte, $\mathbb{S}_n$ es resoluble si y sólo si $n \leq 4$. □

Ejercicio.

Sea $E/K(X_1, \ldots, X_n)$ un cuerpo de descomposición de f, y sea $(x_i)_{1 \leq i \leq n}$ una numeración de las raíces de f en E. Si $(e_i)_{1 \leq i \leq n}$ es una sucesión de elementos de K, entonces $\sum_{1 \leq i \leq n} e_i x_i$ es un elemento primitivo de $E/K(X_1, \ldots, X_n)$.

Indicación. $(x_i)_{1 \leq i \leq n}$ es linealmente independiente en E/K pues es algebraicamente independiente.

PROPOSICIÓN. *Sea $E/K(X_1, \ldots, X_n)$ un cuerpo de descomposición de f, y sea $(x_i)_{1 \leq i \leq n}$ una numeración de las raíces de f en E. Se supone* $\operatorname{car} K \neq 2$. *Sea* $a = \prod_{i<j}(x_j - x_i)$. *Entonces* $\mathbb{G}_{f, K(X_1, \ldots, X_n)(a)} = \mathbb{A}_n$, *o equivalentemente,* $K(X_1, \ldots, X_n)(a)$ *es el cuerpo deducido de* $\mathbb{A}_n$.

OBSERVACIÓN. $d_f \notin K(X_1, \ldots, X_n)^2$, si $n > 1$.

Ejemplos.

1) Grado 2.

$f = X^2 - X_1 X + X_2$ Se supone $\operatorname{car} K \neq 2$. Considerando para $\mathbb{S}_2$ la serie normal trivial $(\mathbb{S}_2, 1)$ resulta que $E/K(X_1, X_2)$ "es" una torre de raíces. Explícitamente, como $\mathbb{A}_2 = 1$, $K(X_1, X_2)(a) = E$, donde $a = x_2 - x_1$. Pero a es una raíz de $X^2 - d_f$ y $d_f \in K(X_1, X_2)$. Además, considerando que $x_1 = S_1(x_1, x_2) = x_1 + x_2$, resulta que $x_2 = \dfrac{X_1 + a}{2}$ y $x_1 = \dfrac{X_1 - a}{2}$.

Luego, como a y $-a$ son las raíces de $X^2 - d_f$, si $\sqrt{d_f}$ representa una cualquiera de ellas, las raíces de f se calculan con la fórmula

$$\frac{X_1 \pm \sqrt{d_f}}{2},$$

o más explícitamente $\dfrac{X_1 \pm \sqrt{X_1^2 - 4X_2}}{2}$.

En consecuencia, dado un polinomio $g \in K[X]$ de grado 2, las raíces de g se determinan con la fórmula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

si $g = aX^2 + bX + c$, pues el monizado de g es $f\left(\dfrac{-b}{a}, \dfrac{c}{a}, X\right)$.

Ejercicio. Se emplean las notaciones generales fijadas para $n = 4$, de modo tal que $f = X^4 - X_1 X^3 + X_2 X^2 - X_3 X + X_4$, con raíces x_i, $1 \leq i \leq 4$. Además, f se reemplaza por $g = f(X + \frac{1}{4}X_1)$, que tiene raíces $y_i = x_i - \frac{1}{4}X_1$, y es de la forma $g = X^4 + pX^2 + qX + r$, con $p, q, r \in K' = K(X_1, X_2, X_3, X_4)$. (Se supone $\operatorname{car} K \neq 2, 3$). Sea h el resolvente cúbico de g, con raíces, z_i, $1 \leq i \leq 3$.

i) Verificar que $h = X^3 - pX^2 - 4rX + (2pr - q^2)$. Además $\mathbb{G}_h = \mathbb{S}_3$, con lo cual h es irreducible.

ii) Sea d el discriminante de h, y sean $t_1 = z_2 + z_3$, $t_2 = z_1 + z_3$, $t_3 = z_1 + z_2$. Existe una sucesión $(E_i)_{0 \le i \le 4}$ de cuerpos intermedios de E/K':

$$E_0 = K', \quad E_1 = K'(\sqrt{d}), \quad E_2 = K'(z_1, z_2, z_3) = E_1(z_1) = E_1(z_2) = E_1(z_3),$$
$$E_3 = E_2(\sqrt{-t_1}), \quad E_4 = E = E_3(\sqrt{-t_2}) = E_3(\sqrt{-t_3}).$$

iii) Con la elección de radicales $\sqrt{-t_1}.\sqrt{-t_2}.\sqrt{-t_3} = -q$, resulta

$$2y_1 = \sqrt{-t_1} + \sqrt{-t_2} + \sqrt{-t_3},$$
$$2y_2 = \sqrt{-t_1} - \sqrt{-t_2} - \sqrt{-t_3},$$
$$2y_3 = -\sqrt{-t_1} + \sqrt{-t_2} - \sqrt{-t_3},$$
$$2y_4 = -\sqrt{-t_1} - \sqrt{-t_2} + \sqrt{-t_3}.$$

Luego, las raíces de g están dadas por las fórmulas

$$\frac{\sqrt{-t_1} + \sqrt{-t_2} + \sqrt{-t_3}}{2},$$

donde los radicales se eligen satisfaciendo que su producto sea $-q$.

9. Polinomios con coeficientes racionales de Grupo de Galois simétrico

PROPOSICIÓN. *Si $f \in \mathbb{Q}[x]$ es irreducible de grado primo p, y exactamente 2 de las raíces de f en $\mathbb{C}$ no son reales, entonces $\mathbb{G}_f = \mathbb{S}_p$.*

DEMOSTRACIÓN. Sea $E/\mathbb{Q}$ el cuerpo de descomposición de f en $\mathbb{C}/\mathbb{Q}$, y sea $G = \mathbb{G}(E/\mathbb{Q})$. Si $z \in \mathbb{C}$ es una raíz de f, el monizado de f es el polinomio minimal de z sobre $\mathbb{Q}$, con lo cual $[\mathbb{Q}(z) : \mathbb{Q}] = p$. Esto prueba que $p|[E : \mathbb{Q}] = (G : 1)$, luego definido $\mathbb{G}_f$ a partir de una numeración ρ_i, $1 \le i \le p$, de las raíces de f en $\mathbb{C}$, resulta que $\mathbb{G}_f$ tiene algún elemento de orden p, o sea, un p-ciclo. Si $\sigma \in G$ es el automorfismo definido por la conjugación de $\mathbb{C}$, y si j y k son los índices tales que ρ_k y $\rho_j \notin \mathbb{R}$, entonces $\sigma(\rho_j) = \rho_k$ pues $\sigma(p_j) = \overline{p_j} \ne p_j$ y $\sigma(p_j) \notin \mathbb{R}$; con lo cual $\sigma(p_j) = p_k$. Por lo tanto $(j\,k) = \sigma \in \mathbb{G}_f$. Luego $\mathbb{G}_f = \mathbb{S}_p$. □

PROPOSICIÓN. *Dado $n \in \mathbb{N}$, si $n = 2$ o n es impar $\ne 1$, existe $f \in \mathbb{Q}[X]$, tal que f es irreducible de grado n, tal que exactamente 2 de las raíces de f en $\mathbb{C}$ no son reales.*

TEOREMA. *Para cada primo p, existe $f \in \mathbb{Q}[X]$ tal que $\mathbb{G}_f = \mathbb{S}_p$.*

DEMOSTRACIÓN (DE LA PROPOSICIÓN). Si $n = 2$, basta tomar $f = X^2 + 1$. Si $n = 3$, basta tomar $f = X^3 - 2$.

Sea entonces $n > 3$. Dada una sucesión creciente $(r_i)_{1 \leq i \leq n-2}$ de números enteros pares, y dado un entero positivo m, se define

$$g = (X^2 + m) \prod_{i=1}^{n-2} (X - r_i) \in \mathbb{Z}[X].$$

Notar que g es un polinomio de la forma $X^n + \sum_{i=1}^{n} a_i X^{n-i}$, donde $2|a_i$, para $1 \leq i \leq n-1$, y $4|a_n$. Luego $f = g - 2 \in \mathbb{Z}[X]$ resulta irreducible en $\mathbb{Q}[X]$ por el criterio de Eisentein para el primo 2. El grado de f es n.

Dado $x \in \mathbb{R}$, se tiene:

$$r_i < x < r_{i+1},\ (1 \leq i \leq n-3), \Rightarrow g(x) \begin{cases} > 0 & si\ i \equiv 1(2), \\ < 0 & si\ i \equiv 0(2). \end{cases}$$

En efecto, $x - r_j > 0$ para $1 \leq j \leq i$ con lo cual $\prod_{j=1}^{i} (x - r_j) > 0$; $x - r_j < 0$ para $i+1 \leq j \leq n-2$; con lo cual $\prod_{j=i+1}^{n-2} (x - r_j)$ se compara con 0 según la paridad del número de factores, que es

$$n - 2 - i \equiv i + 1(2).$$

Se define $x_i \in (r_i, r_{i+1})$ para $1 \leq i \leq n-3$, satisfaciendo $g(x_i) > 2$, si $i \equiv 1(2)$ Esto es posible porque $|g(s)| \geq 6$, si s es un entero impar. En efecto,

$$|g(s)| = |s^2 + m| \prod_{i=1}^{n-2} |s - r_i| \geq 2 \prod_{i=1}^{n-2} |s - r_i|$$

y $|s - r_i| \geq 1$; pero si $|s - r_i| = 1$ para $1 \leq i \leq n-2$, se tendría $n - 2 \leq 2$. Con lo cual existe j tal que $|s - r_j| \geq 2$, y por ende $|s - r_j| > 2$ pues $s - r_j \equiv 1(2)$.

En consecuencia $|g(s)| \geq 2.3 = 6$.

Además, se toma $x_0 = r_1$, y $x_{n-2} > r_{n-2}$ tal que

$$g(x_{n-2}) > 2$$

(es posible pues $\lim_{x \to \infty} g(x) = \infty$.) Luego, si $1 \leq i \leq n-2$,

$$f(x_i) \begin{cases} > 0 & si\ i \equiv 1(2) \\ < 0 & si\ i \equiv 0(2). \end{cases}$$

Así $f(x_{i-1}).f(x_i) < 0$, $1 \leq i \leq n-2$. Luego, aplicando el teorema de Bolzano a f, considerado como función polinómica, se obtienen raíces $\rho_i \in (x_{i-1}, x_i)$, $1 \leq i \leq n-2$.

Sean ρ_{n-1}, $\rho_n \in \mathbb{C}$ tales que $f = \prod_{i=1}^{n} (X - \rho_i)$.

Calculando los coeficientes de X^{n-1} y X^{n-2} en $\prod_{i=1}^{n}(X-\rho_i) = g-2$, se obtiene

$$\sum_{i=1}^{n}\rho_i = \sum_{i=1}^{n} r_i, \qquad \sum_{i\le i<j\le n}\rho_i\rho_j = \sum_{1\le i<j\le n-2} r_i r_j + m,$$

de donde

$$\sum_{i=1}^{n}\rho_i^2 = (\sum_{i=1}^{n}\rho_i)^2 - 2\sum_{1\le i\le j\le n}\rho_i\rho_j = \sum r_i^2 - 2m < 0,$$

si $m > \dfrac{\sum r_i^2}{2}$. □

PROPOSICIÓN. *Sea K un cuerpo, y sea $f \in K[X]$ no constante, mónico, con raíces simples. Dado un cuerpo de descomposición E/K de f y una numeración $(\rho_i)_{i=1}^n$ de las raíces de f en E, sea $g = \prod_{\pi\in\mathbb{S}_n}(X - \sum_{i=1}^{n}\rho_{\pi(i)}X_i) \in E[X_1,\dots,X_n,X]$. Se verifican:*

i) $g \in K[X_1,\dots,X_n,X]$, y su definición es independiente de la elección de E/K y de la numeración (ρ_i) de las raíces de f en E.

ii) Si d es un divisor irreducible mónico de g, en $K(X_1,\dots,X_n)[X]$, y si $\sum_{i=1}^{n}\rho_{\pi(i)}X_i$ es una raíz de d en $E(X_1,\dots X_n)$, entonces

$$d = \prod_{\nu\in\mathbb{G}_f}\left(X - \sum_{i=1}^{n}\rho_{\nu\pi(i)}X_i\right).$$

En particular, $\operatorname{gr} d = (\mathbb{G}_f : 1)$.

iii) En $K[X][X_1,\dots,X_n]$, g es simétrico, y el estabilizador de d es $\pi^{-1}\mathbb{G}_f\pi$.

DEMOSTRACIÓN.

i) Si P es el subanillo primo de K, sea

$$h = \prod_{\pi\in\mathbb{S}_n}\left(X - \sum_{i=1}^{n} Y_{\pi(i)}X_i\right) \in P[X_1,\dots,X_n,X,Y_1,\dots,Y_n]$$

con lo cual

$$g = h(X_1,\dots,X_n,X,\rho_1,\dots,\rho_n).$$

En $P[X_1,\dots,X_n,X][Y_1,\dots,Y_n]$, el polinomio h es simétrico: pues si $\nu\in\mathbb{S}_n$,

$$\nu.h = \prod_{\pi\in\mathbb{S}_n}(X - \sum_{i=1}^{n} Y_{\nu\pi(i)}X_i) = h,$$

cambiando variables según la transformación $\pi \mapsto \nu\pi$ de $\mathbb{S}_n$.

Luego, está unívocamente determinado $k \in P[X_1,\dots,X_n,X][Y_1\dots Y_n]$, respecto de la propiedad

$$h = k(s_1,\dots,s_n)$$

donde s_i es el polinomio simétrico elemental de grado i en $P[X_1,\ldots,X_n,X]$ $[Y_1,\ldots,Y_n]$, para $1 \leq i \leq n$. Por lo tanto,

$$g = k(s_1(\rho_1,\ldots,\rho_n),\ldots,s_n(\rho_1,\ldots,\rho_n)).$$

Ahora bien, escribiendo

$$f = X^n + \sum_{i=1}^{n}(-1)^i a_i X^{n-i},$$

como $f = \prod_{i=1}^{n}(X-\rho_i)$, resulta $s_i(\rho_1,\ldots,\rho_n) = a_i$, $1 \leq i \leq n$, por el caracter "universal" de los polinomios simétricos universales. En consecuencia, $g = k(a_1,\ldots,a_n) \in K[X_1,\ldots,X_n,X]$; y esta igualdad también suministra la buena definición de g, pues k está unívocamente determinado por h, que a su vez está unívocamente determinado por $n = \operatorname{gr} f$.

ii) Dada una permutación π de grado n, sea

$$f_\pi = \sum_{1\leq i\leq n} \rho_{\pi(i)}\, X_i \in E[X_1,\ldots,X_n].$$

Cada automorfismo ν de E/K define un automorfismo $\bar{\nu}$ de $E(X_1,\ldots,X_n)/K(X_1,\ldots,X_n)$ (más aún, la aplicación $\nu \longmapsto \bar{\nu}$ es un monomorfismo de $\mathbb{G}(E/K)$ en $\mathbb{G}(E(X_1,\ldots,X_n)/K(X_1,\ldots,X_n))$.

Ahora bien, siendo $f_\pi \in E(X_1,\ldots,X_n)$ una raíz de $d \in K(X_1,\ldots,X_n)[X]$, $\bar{\nu}(f_\pi) = f_{\nu\pi}$ también es una raíz de d:

$$\bar{\nu}(f_\pi) = \bar{\nu}(\sum_{i=1}^{n}\rho_{\pi(i)}\,X_i) = \sum_{i=1}^{n}\nu(\rho_{\pi(i)})X_i = \sum_{i=1}^{n}\rho_{\nu\pi(i)}X_i = f_{\nu\pi}.$$

Ahora bien, las raíces de g son simples:

$$f_\pi = f_{\pi'} \Rightarrow \rho_{\pi(i)} = \rho_{\pi'(i)} \quad \forall i,\, 1 \leq i \leq n \Rightarrow \pi(i) = \pi'(i), \forall i\, 1 \leq i \leq n \Rightarrow \pi = \pi',$$

y por lo tanto

$$\prod_{\nu\in\mathbb{G}_f}(X - f_{\nu\pi}) | d.$$

Considérese cualquier raíz f_ν de d, $\nu \in \mathbb{S}_n$. $E(X_1,\ldots,X_n)/K(X_1,\ldots,X_n)$ es una extensión algebraica, más aún, de grado finito, pues E/K lo es. Sea $C/K(X_1,\ldots,X_n)$ una clausura algebraica de $K(X_1,\ldots,X_n)$ que tiene a $E(X_1,\ldots,X_n)$ por cuerpo intermedio. Como f_π y f_ν son elementos de C que tienen el mismo polinomio minimal d sobre $K(X_1,\ldots,X_n)$, existe un automorfismo τ de $C/K(X_1,\ldots,X_n)$ tal que $\tau(f_\pi) = f_\nu$, con lo cual $\tau(\rho_{\pi(i)}) = \rho_{\nu(i)}$, $1 \leq i \leq n$. Luego, considerando que $(\rho_i)_{i=1}^n$ es una familia de generadores de E/K, $\tau(E) \subseteq E$, y así, τ induce un automorfismo σ de E/K tal que $\sigma(\rho_{\pi(i)}) = \rho_{\nu(i)}$, para $1 \leq i \leq n$. Ahora, $\rho_{\sigma\pi(i)} = \rho_{\nu(i)} \Rightarrow \sigma_f\pi = \nu$. Por lo tanto $d = \prod_{\nu\in\mathbb{G}_f}(X - f_{\nu\pi})$.

iii) Como $\nu.f_\pi = \sum_{i=1}^{n} \rho_{\pi(i)} X_{\nu(i)} = \sum_{i=1}^{n} \rho_{\pi\nu^{-1}(\nu(i))} X_{\nu(i)} = f_{\pi\nu^{-1}}$, cambiando índices según la transformación $\pi \longmapsto \pi\nu^{-1}$, resulta que $\nu.g = \prod_{\pi\in\mathbb{S}_n} (X - f_{\pi\nu^{-1}}) = g$. Si $\mu \in \mathbb{S}_n$,

$$\mu.d = d \Longleftrightarrow \prod_{\nu\in\mathbb{G}_f} (X - f_{\nu\pi}) = \prod_{\nu\in\mathbb{G}_f} (X - f_{\nu\pi\mu^{-1}})$$

y como el factor correspondiente a $\nu = (1)$ en el miembro derecho de la igualdad debe figurar como factor en el miembro izquierdo, existe $\nu \in \mathbb{G}_f$ tal que

$$\pi\mu^{-1} = \nu\pi \Rightarrow \mu\pi^{-1} = \pi^{-1}\nu^{-1} \Rightarrow \mu = \pi^{-1}\nu^{-1}\pi \Rightarrow \mu \in \pi^{-1}\mathbb{G}_f\pi.$$

Recíprocamente, dado $\mu \in \mathbb{G}_f$, $(\pi^{-1}\mu\pi).d = \prod_{\nu\in\mathbb{G}_f} (X - f_{(\nu\mu^{-1})\pi}) = d$, cambiando índices según la transformación $\nu \longmapsto \nu\mu^{-1}$ de $\mathbb{S}_n$. □

COROLARIO. *$\mathbb{G}_f = \mathbb{S}_n$ si y sólo si g es irreducible en $K(X_1, \ldots, X_n)[X]$.*

DEMOSTRACIÓN. Empleando ii), g es irreducible $\Longleftrightarrow g = d \Longleftrightarrow \operatorname{gr} g = \operatorname{gr} d \Longleftrightarrow n! = (\mathbb{G}_f : 1) \Longleftrightarrow \mathbb{G}_f = \mathbb{S}_n$ □

PROPOSICIÓN. *Sea K el cuerpo de fracciones de un anillo factorial A, sea $f \in A[X]$ y sea P un ideal primo de A tal que, si $f' \in K'[X]$ (donde K' es cuerpo de fracciones de A/P), la reducción de f módulo P, f' tiene sus raíces simples. Entonces se verifica:*

i) $g \in A[X_1, \ldots, X_n, X]$ y g' coincide con la reducción de g módulo P.

ii) Dado un cuerpo de descomposición E'/K' de f', con una adecuada numeración $(\rho_i')_{i=1}^n$ de las raíces de f' en E', $\mathbb{G}_{f'}$ es un subgrupo de $\mathbb{G}_f$.

DEMOSTRACIÓN. i) Empleando las notaciones de la demostración de i) de la proposición anterior, como $a_i \in A$, $1 \leq i \leq n$, y $P \subseteq A$, es claro que $g = k(a_1, \ldots, a_n) \in A[X_1, \ldots, X_n]\,[X]$. Notando con $^-$ la reducción módulo P de polinomios con coeficientes en A, en el número de indeterminadas que sea necesario, también es claro que $\overline{h} = h'$, pues $\operatorname{gr} f' = n$; pero entonces

$$h' = \overline{h} \Rightarrow g' = \overline{k(s_1, \ldots, s_n)} = \overline{k}(\overline{s}_1, \ldots, \overline{s}_n) = \overline{k}(s_1', \ldots, s_n')$$
$$\Rightarrow k' = \overline{k} \Rightarrow g' = k'(a_1', \ldots, a_n') = \overline{k}(\overline{a}_1, \ldots, \overline{a}_n) = \overline{k(a_1, \ldots, a_n)} = \overline{g}.$$

Retomando ii) de la proposición anterior, sea $g = \prod_{i=1}^{r} g_i$, con $g_i \in K(X_1, \ldots, X_n)[X]$ irreducible y mónico. Existe una sucesión $(\pi_i)_{1\leq i\leq r}$ de permutaciones de grado n tal que

$$g_i = \prod_{\nu\in\mathbb{G}_f} (X - f_{\nu\pi_i}),$$

con lo cual los conjuntos $(\mathbb{G}_f \pi_i)_{i=1}^r$ forman una partición de $\mathbb{S}_n$, vale decir $(\pi_i)_{i=1}^r$ es una familia de representantes del conjunto cociente $\mathbb{S}_n/\mathbb{G}_f$ (coclases a *derecha*), y si $\pi_1 \in \mathbb{G}_f$, por ejemplo, no hay inconveniente en escoger $\pi_1 = (1)$. En el caso en cuestión $-f \in A[X]-$, como $g \in A[X_1, \ldots, X_n]\,[X]$ puede tomarse $g_i \in A[X_1, \ldots, X_n]\,[X]$ (también mónicos), $1 \leq i \leq r$, pues A es factorial. Por lo tanto, reduciendo módulo P,

$$g' = \prod_{i=1}^{r} \overline{g}_i.$$

Como $\mathbb{G}_f$ es el estabilizador de g_1, y la acción de $\mathbb{S}_n$ conmuta con la reducción módulo P, $\mathbb{G}_f$ actúa trivialmente sobre $\overline{g}_1$. Además, si $\mu \in \mathbb{S}_n - \mathbb{G}_f$, $\mu.g_1 = g_j$, para algún $j > 1$, con lo cual $\mu\, \overline{g}_1 = \overline{g}_j$, y se tiene: $\overline{g}_1 \neq \overline{g}_j$ por ser las raíces de g' simples. Por lo tanto, $\mathbb{G}_f$ es el estabilizador de $\overline{g}_1$, y probando que $\mathbb{G}'_f$ actúa trivialmente sobre $\overline{g}_1$, resulta que $\mathbb{G}_{f'} \subseteq \mathbb{G}_f$. Se fija la numeración $(\rho'_i)_{1 \leq i \leq n}$ de las raíces de f' en E' exigiendo que $\sum_{i=1}^{n} \rho'_i X_i$ sea una raíz de $\overline{g}_1$ ($\overline{g}_1$ no constante pues g_1 mónico), con lo cual $d' = \prod_{\nu' \in \mathbb{G}'_f} (X - f'_{\nu'})$ es un divisor irreducible de $\overline{g}_1$. Como $\nu' \in \mathbb{G}_{f'}$ deja invariante a d', los divisores irreducibles de $\nu' g_1$ no pueden obtenerse de los divisores irreducibles de $\overline{g}_i$, $1 < i \leq r$, con lo cual $\nu' \overline{g}_1 = \overline{g}_1$. $\square$