Álgebra III - 2do C. 2020 - Clase 15 - 20/10/2020

Ejemplo $(\mathbb{Q}(\xi_7)/\mathbb{Q})$

Por simplicidad para mí, $\xi_7 =: \omega$

$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times = \{1,2,3,4,5,6\} = \langle 3\rangle = \langle 4\rangle$

O sea $G := \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \langle\sigma\rangle$ con por ejemplo $\sigma(\omega) = \omega^3$:

$$\omega \overset{\sigma}{\longmapsto} \omega^3 \overset{\sigma}{\longmapsto} \omega^2 \overset{\sigma}{\longmapsto} \omega^{-1} \overset{\sigma}{\longmapsto} \omega^{-3} \overset{\sigma}{\longmapsto} \omega^{-2} \overset{\sigma}{\longmapsto} \omega.$$

Los subgrupos de G son

$$\{\mathrm{id}_{\mathbb{Q}(\omega)}\} \quad , \quad \langle\sigma^2 : \omega \mapsto \omega^2\rangle \quad , \quad \langle\sigma^3 : \omega \mapsto \omega^{-1}\rangle \quad , \quad G$$

Notar que $H_2 := \langle\sigma^2\rangle$ tiene orden 3 y $H_3 := \langle\sigma^3\rangle$ tiene orden 2.

¿Quienes son las subextensiones

$$F_2 = \mathbb{Q}(\omega)^{H_2} \quad \text{y} \quad F_3 = \mathbb{Q}(\omega)^{H_3} \quad ?$$

Fijarse que como en el caso anterior $F_3 = \mathbb{Q}(\omega)^{\sigma^3}$ y $[\mathbb{Q}(\omega) : F_3] = 2$ implican $F_3 = \mathbb{Q}(\omega + \omega^{-1})$ pues $\sigma^3(\omega + \omega^{-1}) = \omega + \omega^{-1}$ implica que $\mathbb{Q}(\omega + \omega^{-1}) \subset F_3$ pero por otro lado la inclusión no puede ser estricta, pues $\omega + \omega^{-1} \notin \mathbb{Q}$ dado que $\sigma(\omega + \omega^{-1}) = \omega^3 + \omega^{-3} \neq \omega + \omega^{-1}$.

Asi, $F_3 = \mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}(\cos(2\pi/7)) \subset \mathbb{R}$.

Busquemos quién es F_2. Por las dudas que no se nos ocurra podemos hacerlo a mano trabajando con la base de $\mathbb{Q}(\omega)/\mathbb{Q}$:

Necesitamos $\sigma^2(\alpha) = \alpha$ para $\alpha = a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4 + a_5\omega^5 + a_6\omega^6$ escrito en términos de la base $\{\omega, \ldots, \omega^6\}$ de $\mathbb{Q}(\omega)/\mathbb{Q}$.

Pero

$$a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4 + a_5\omega^5 + a_6\omega^6 \overset{\sigma^2}{\longmapsto} a_1\omega^2 + a_2\omega^4 + a_3\omega^6 + a_4\omega + a_5\omega^3 + a_6\omega^5$$

así que tiene que ser

$$a_1 = a_4 \ , \ a_2 = a_1 \ , \ a_3 = a_5 \ , \ a_4 = a_2 \ , \ a_5 = a_6 \ , \ a_6 = a_3,$$

es decir

$$\sigma^2(\alpha) = \alpha \iff \alpha = a_1(\omega + \omega^2 + \omega^4) + a_3(\omega^3 + \omega^5 + \omega^6).$$

O sea

$$F_2 = \mathbb{Q}(\omega + \omega^2 + \omega^4, \omega^3 + \omega^5 + \omega^6) = \mathbb{Q}(\omega + \omega^2 + \omega^4),$$

pues

$[F_2 : \mathbb{Q}] = 2 \quad \text{y} \quad \sigma(\omega+\omega^2+\omega^4) = \omega^3+\omega^6+\omega^5 \neq \omega+\omega^2+\omega^4$

implican $\mathbb{Q} \subsetneq \mathbb{Q}(\omega+\omega^2+\omega^4) = F_2$.
Más aún

$$f(\omega+\omega^2+\omega^4, \mathbb{Q}) = \big(X-(\omega+\omega^2+\omega^4)\big)\big(X-(\omega^3+\omega^5+\omega^6)\big)$$
$$= X^2+X+2 \;=\; \big(X-\frac{-1+\sqrt{-7}}{2}\big)\big(X-\frac{-1-\sqrt{-7}}{2}\big)$$

Esto implica que $F_2 \;=\; \mathbb{Q}(\omega+\omega^2+\omega^4) \;=\; \mathbb{Q}(\sqrt{-7})$.
(La extensión $\mathbb{Q}(\omega)/\mathbb{Q}$ contiene la subextensión no real $\mathbb{Q}(\sqrt{-7})$.)

Miremos ahora como expresar ω:

$$f(\omega+\omega^{-1}, \mathbb{Q}) = \big(X-(\omega+\omega^{-1})\big)\big(X-(\omega^3+\omega^{-3})\big)\big(X-(\omega^2+\omega^{-2})\big)$$
$$= X^3+X^2-2X-1,$$

y podemos expresar $\omega+\omega^{-1}$ (y por lo tanto $\cos(2\pi/7)$) por radicales, y después

$$f(\omega, F_3) = (X-\omega)(X-\omega^{-1}) = X^2-(\omega+\omega^{-1})X+1,$$

y también podemos expresar ω por radicales en función de $\omega+\omega^{-1}$.
En particular ω se puede expresar por radicales...

Esto se dio en la práctica así que lo salteamos.

Subextensiones cuadráticas de $\mathbb{Q}(\xi_p)/\mathbb{Q}$:

La proposición siguiente, que podríamos haber visto antes, puede ser útil independientemente de las extensiones ciclotómicas, y permite reintroducir el *discriminante*.

Proposición 10.2.3 (El discriminante)
Sea $f = (X-\alpha_1)\cdots(X-\alpha_n) \in K[X]$ *un polinomio separable de grado* n, *y sea*

$$\Delta(f) = \prod_{i>j}(\alpha_i-\alpha_j)^2 \;\in\; K(f)^2$$

su discriminante. *Entonces*

1. $\Delta(f) \in K$
2. $\Delta(f) \in K^2 \iff K(\sqrt{\Delta(f)}) = K \iff \mathrm{Gal}(f/K) \subset A_n$.

Prueba.–

1. Sabemos que $\mathrm{Gal}(f/K) \subset S_n$, y para todo $\sigma \in S_n$,

$$\sigma(\Delta(f)) = \prod_{i>j}(\sigma(\alpha_i) - \sigma(\alpha_j))^2 = \Delta(f).$$

   Por lo tanto $\Delta(f) \in K$.

2. Notar que entonces $\sqrt{\Delta(f)} = \prod_{i>j}(\alpha_i - \alpha_j) \in K(f)$ define a lo sumo una subextensión cuadrática de $K(f)/K$:

$$\Delta(f) \in K^2 \iff K(\sqrt{\Delta(f)}) = K.$$

   Además, para todo $\sigma \in S_n$,

$$\sigma(\sqrt{\Delta(f)}) = \prod_{i>j}(\sigma(\alpha_i) - \sigma(\alpha_j)) = \mathrm{sg}(\sigma)\sqrt{\Delta(f)},$$

   donde $\mathrm{sg}(\sigma) = 1 \Leftrightarrow \sigma$ es una permutación par, y $\mathrm{sg}(\sigma) = -1$ si σ es una permutación impar.

   Por lo tanto $\sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)} \Leftrightarrow \sigma \in A_n$. Así,

$$K(\sqrt{\Delta(f)}) \subset K(f)^{\mathrm{Gal}(f/K)} = K \iff \mathrm{Gal}(f/K) \subset A_n.$$

■

Proposición 10.2.4 (Subextensiones cuadráticas de $\mathbb{Q}(\xi_p)/\mathbb{Q}$)
Sea p primo impar, entonces la *subextensión cuadrática de $\mathbb{Q}(\xi_p)/\mathbb{Q}$ es:*

$$\mathbb{Q}(\sqrt{p}) \ \ si \ \ p \equiv 1 \ (4) \qquad y \qquad \mathbb{Q}(\sqrt{-p}) \ \ si \ \ p \equiv 3 \ (4).$$

Prueba.–

Como $p-1$ es par, sabemos que $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ admite un (único) subgrupo de índice 2, y por lo tanto $\mathbb{Q}(\xi_p)/Q$ admite una subextensión de grado 2, que es única.

Como $\mathbb{Q}(\xi_p) = \mathbb{Q}(X^p - 1)$, para $\xi_i := \xi_p^i$, $1 \leq i \leq p$, tenemos

$$\Delta(X^p - 1) \;=\; \prod_{i>j}(\xi_i - \xi_j)^2 \;=\; \Big(\prod_{i>j}(\xi_i - \xi_j)\Big)\Big(\prod_{i>j}(\xi_i - \xi_j)\Big),$$

donde los productos en los dos paréntesis son ... ¡un determinante de Vandermonde! por lo tanto

$$\begin{aligned}
\Delta(X^p - 1) = \;& \det\begin{pmatrix} 1 & \cdots & 1 \\ \xi_1 & \cdots & \xi_p \\ \vdots & & \vdots \\ \xi_1^{p-1} & \cdots & \xi_1^{p-1} \end{pmatrix} \cdot \det\begin{pmatrix} 1 & \xi_1 & \cdots & \xi_1^{p-1} \\ \vdots & \vdots & & \vdots \\ 1 & \xi_p & \cdots & \xi_p^{p-1} \end{pmatrix} \\
= \;& \det\begin{pmatrix} p & 0 & \cdots & 0 \\ 0 & & & p \\ \vdots & & & \\ 0 & p & \cdots & 0 \end{pmatrix} \\
= \;& (-1)^{\binom{p-1}{2}} p^p \;=\; \begin{cases} p^p & \text{si} \quad p \equiv 1\ (4) \\ -p^p & \text{si} \quad p \equiv 3\ (4) \end{cases}
\end{aligned}$$

usando que $\xi_1 + \cdots + \xi_p = 0$ y $\xi_1^k + \cdots + \xi_p^k = 0$ para $1 \leq k \leq p-1$.

En conclusión,

$$\sqrt{\Delta(X^p - 1)} \;=\; \begin{cases} p^{\frac{p-1}{2}}\sqrt{p} & \text{si} \quad p \equiv 1\ (4) \\ p^{\frac{p-1}{2}}\sqrt{-p} & \text{si} \quad p \equiv 3\ (4) \end{cases}$$

O sea $\sqrt{p} \in \mathbb{Q}(\xi_p)$ si $p \equiv 1\ (4)$ y $\sqrt{-p} \in \mathbb{Q}(\xi_p)$ si $p \equiv 3\ (4)$.

■

---

11 Dos aplicaciones de la teoría de Galois

11.1 $\mathbb{C}$ es algebraicamente cerrado

Supongamos que $\mathbb{C}$ no es algebraicamente cerrado.
Entonces existe una extensión $E/\mathbb{C}$ finita con $E/\mathbb{R}$ Galois.
Entonces $|\mathrm{Gal}(E/\mathbb{R})| = 2^k\, m$ con m impar y $k \geq 1$.
Por lo tanto $\exists\, H \subset \mathrm{Gal}(E/\mathbb{R})$ 2-subgrupo de Sylow,
y entonces $[E^H : \mathbb{R}] = m$.
Pero como $\mathbb{R}$ no tiene extensiones de grado impar > 1, $m = 1$.
Así $|\mathrm{Gal}(E/\mathbb{R})| = 2^k$ y como $\mathbb{C} \subset E$ y $E/\mathbb{C}$ Galois, $|\mathrm{Gal}(E/\mathbb{C})| = 2^{k-1}$.
Y si $k \geq 2$, por ser 2-grupo, $\mathrm{Gal}(E/\mathbb{C})$ tiene un subgrupo H' de orden 2^{k-2}, y por lo tanto $[E^{H'} : \mathbb{C}] = 2$.
o sea $\mathbb{C}$ tiene una extensión cuadrática...

Conclusión: esta demo usa las dos mismas herramientas que ya habíamos usado:

- que todo polinomio de grado impar en $\mathbb{R}[X]$ tiene una raíz en $\mathbb{R}$
- que todo polinomio de grado 2 en $\mathbb{C}[X]$ tiene sus raíces en $\mathbb{C}$.

11.2 La ecuación general de grado n

El grupo de Galois de la ecuación general de grado n es S_n:
Sea

$$f = X^n - s_1(X_1, \ldots, X_n)X^{n-1} + \cdots + (-1)^n s_n(X_1, \ldots, X_n),$$

$E := K(s_1(\boldsymbol{X}), \ldots, s_n(\boldsymbol{X}))$ y $E(f) = E(X_1, \ldots, X_n) = K(X_1, \ldots, X_n)$.

S_n es un grupo finito de automorfismos de $K(X_1, \ldots, X_n)$.
Entonces por el lema de Artin, $K(X_1, \ldots, X_n)/K(X_1, \ldots, X_n)^{S_n}$
es Galois finita, y $\mathrm{Gal}(K(X_1, \ldots, X_n)/K(X_1, \ldots, X_n)^{S_n}) = S_n$.
Pero $E = K(s_1(\boldsymbol{X}), \ldots, s_n(\boldsymbol{X})) \subset K(X_1, \ldots, X_n)^{S_n}$
y $\mathrm{Gal}(E(f)/E) \subset S_n$:

Concluimos que $\mathrm{Gal}(K(X_1, \ldots, X_n)/K(s_1(\boldsymbol{X}), \cdots, s_n(\boldsymbol{X})) = S_n$.

12 Extensiones resolubles por radicales

12.1 Independencia lineal de caracteres

Empezamos esta sección con un resultado general y una consecuencia, notorios en sí mismos, que nos van a ser útiles para el desarrollo de la teoría de las extensiones resolubles por radicales.

Nota: Un *caracter* de un grupo G en un cuerpo E es simplemente un morfismo de G en el grupo multiplicativo $E^\times$ (Artin, 1966).

Proposición 12.1.1 (Independencia lineal de caracteres)
Sea E un cuerpo y sean $\sigma_1, \ldots, \sigma_n$ automorfismos distintos *de E.*
Entonces $\sigma_1, \ldots, \sigma_n$ son linealmente independientes sobre *E, es decir,*
dados $a_1, \ldots, a_n \in E$,

$$a_1\,\sigma_1 + \cdots + a_n\,\sigma_n = 0 \quad \Longrightarrow \quad a_1 = \cdots = a_n = 0,$$

donde

$$a_1\,\sigma_1 + \cdots + a_n\,\sigma_n = 0 \quad \Longleftrightarrow \quad (a_1\,\sigma_1 + \cdots + a_n\,\sigma_n)(\alpha) = 0, \quad \forall\,\alpha \in E.$$

Dicho recíprocamente,

$$\begin{aligned}(a_1, \ldots, a_n) \neq (0, \ldots, 0) \ \in E^n \quad &\Longrightarrow \quad a_1\,\sigma_1 + \cdots + a_n\,\sigma_n \neq 0 \\ &\Longrightarrow \quad \exists\,\alpha \in E \ \ tq \ \ (a_1\,\sigma_1 + \cdots + a_n\,\sigma_n)(\alpha) \neq 0\end{aligned}$$

Prueba.–
Hacemos la demostración en la cantidad n de caracteres σ_i.
$\underline{n = 1:}$

$a\,\sigma(\alpha) = 0,\ \forall\,\alpha \in E \ \Rightarrow \ a = 0$ ya que $\sigma \in \mathrm{Aut}(E) \ \Rightarrow \ \exists\,\alpha \in E$ tq $\sigma(\alpha) = 1$.

$\underline{n > 1:}$

Como $\sigma_1 \neq \sigma_2$, existe $\beta \in E$ tq $\sigma_1(\beta) \neq \sigma_2(\beta)$, y además como $\beta \neq 0$, $\sigma_1(\beta) \neq 0$.

Supongamos

$$a_1\,\sigma_1(\alpha) + a_2\,\sigma_2(\alpha) + \cdots + a_n\,\sigma_n(\alpha) = 0, \quad \forall\,\alpha \in E \tag{1}$$

En particular

$$\begin{aligned} & a_1\,\sigma_1(\beta\alpha) + a_2\,\sigma_2(\beta\alpha) + \cdots + a_n\,\sigma_n(\beta\alpha) = 0, \quad \forall\,\alpha \in E \\ & \quad \Longrightarrow a_1\,\sigma_1(\beta)\sigma_1(\alpha) + a_2\,\sigma_2(\beta)\sigma_2(\alpha) + \cdots + a_n\,\sigma_n(\beta)\sigma_n(\alpha) = 0, \quad \forall\,\alpha \in E \\ & \quad \Longrightarrow a_1\,\sigma_1(\alpha) + a_2\big(\frac{\sigma_2(\beta)}{\sigma_1(\beta)}\big)\sigma_2(\alpha) + \cdots + a_n\,\big(\frac{\sigma_n(\beta)}{\sigma_1(\beta)}\big)\sigma_n(\alpha) = 0, \quad \forall\,\alpha \in E, \end{aligned} \tag{2}$$

donde en la última implicación, dividimos por $\sigma_1(\beta) \neq 0$.
Restando (2) de (1) queda

$$a_2\big(1 - \frac{\sigma_2(\beta)}{\sigma_1(\beta)}\big)\sigma_2(\alpha) + \cdots + a_n\big(1 - \frac{\sigma_n(\beta)}{\sigma_1(\beta)}\big)\sigma_n(\alpha) = 0, \quad \forall\,\alpha \in E,$$

y por lo tanto para $a_i' = a_i\big(1 - \frac{\sigma_i(\beta)}{\sigma_1(\beta)}\big)$, $2 \leq i \leq n$, tenemos

$$a_2'\sigma_2(\alpha) + \cdots + a_n'\sigma_n(\alpha) = 0, \quad \forall\,\alpha \in E.$$

Por HI, deducimos que $a_2' = \cdots = a_n' = 0$.
Pero $\sigma_1(\beta) \neq \sigma_2(\beta) \;\Rightarrow\; 1 - \frac{\sigma_2(\beta)}{\sigma_1(\beta)} \neq 0$ en E, y por lo tanto $a_2 = 0$.
O sea, volviendo a (1),

$$a_1\,\sigma_1(\alpha) + a_3\sigma_3(\alpha) + \cdots + a_n\,\sigma_n(\alpha) = 0, \quad \forall\,\alpha \in E$$

y nuevamente por HI, ahora sí, $a_1 = a_3 = \cdots = a_n = 0$.

■

¿Quiénes son los caracteres aquí?