Álgebra III - 2do C. 2020 - Clase 14 - 16/10/2020

10 Extensiones ciclotómicas

Esta sección no es muy rigurosa, sobre todo trata de dar pautas y herramientas para trabajar. Los resultados se van a desarrollar con más detalle en la práctica.

10.1 Hechos generales

Definición 10.1.1 (Extensión ciclotómica)
Sea K un cuerpo. Se dice que E es una extensión ciclotómica de K *si $E = K(\xi)$ donde $\xi \in \overline{K}$ es una raíz n-ésima de 1 para algún $n \in \mathbb{N}$.*

Ejemplos

- $\mathbb{Q}(\xi_n)/\mathbb{Q}$ donde ξ_n es raíz n-ésima (primitiva o no) de 1.
- $\mathbb{F}_{p^n}/\mathbb{F}_p$ pues $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ donde θ es raíz de $\theta^{p^n-1} = 1$.

Observación 10.1.2 (Puede haber pocas raíces n-ésimas de 1 en $\overline{K}$)
Sea K con $\operatorname{car}(K) = p$ y $n = p^k m$ con $p \nmid m$. Entonces

$$X^n - 1 = X^{p^k m} - 1 = (X^m - 1)^{p^k}.$$

Observar que el polinomio $X^m - 1$ es separable y hay m raíces de 1 en $\overline{K}$.

Proposición 10.1.3 (El grupo multiplicativo de raíces n-ésimas de 1)
Sea K cuerpo y $G := \{\xi \in \overline{K} : \xi^n = 1\} \subset \overline{K}$. Entonces

1. *$(G, \cdot)$ es un grupo cíclico.*
2. *Sea $\xi \in G$, entonces $K(\xi)/K$ es Galois.*

Prueba.–

1. G es obviamente un grupo, y es cíclico al ser un subgrupo multiplicativo finito de un cuerpo. Sus generadores son las raíces primitivas de orden n.

2. Si $\mathrm{car}(K) = p$ y $\xi^n = 1$, entonces ξ es raíz primitiva de algún orden d con $d \,|\, m$ si $n = p^k m$.

   Entonces $K(\xi) = K(X^d - 1)$ es el cuerpo de descomposición de un polinomio separable en $K[X]$.

■

Proposición 10.1.4 $(\mathrm{Gal}(K(\xi_n)/K) < \mathcal{U}(\mathbb{Z}/n\mathbb{Z}))$
Sea $\xi_n \in \overline{K}$ una raíz n-ésima primitiva *de 1. Entonces el morfismo de grupos*

$$\begin{array}{ccc} \mathrm{Gal}(K(\xi_n)/K) & \longrightarrow & \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \\ \sigma & \longmapsto & k \quad si \;\; \sigma(\xi_n) = \xi_n^k \end{array}$$

es

1. *siempre inyectivo,*

   y por lo tanto $\mathrm{Gal}(K(\xi_n)/K) < \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ *y* $|\mathrm{Gal}(K(\xi_n)/K)| \mid \varphi(n)$.

2. *puede no ser sobreyectivo.*

Prueba.–
Observar que $f(\xi_n, K) \,|\, \Phi_n(X)$ en $\mathbb{F}_p[X]$ y por lo tanto $\xi_n \mapsto \xi_n^k$ con $\mathrm{mcd}(k, n) = 1$: el morfismo está bien definido.

1. Es obvio.

2. En $\mathbb{F}_3[X]$,

   $$X^8 - 1 = (X-1)(X+1)(X^2+1)(X^2+X-1)(X^2-X-1).$$

   Cada raíz $\xi \neq \pm 1$ define la extensión $\mathbb{F}_9$ de grado 2 sobre $\mathbb{F}_3$:

   $$|\mathrm{Gal}(\mathbb{F}_3(\xi)/\mathbb{F}_3)| = 2 < 4 = \varphi(8).$$

10.2 Extensiones ciclotómicas sobre $\mathbb{Q}$

- Sea $\xi_n \in \mathbb{C}$ es una raíz n-esima primitiva de la unidad, entonces recordemos:

$$\mathbb{Q}(X^n - 1) = \mathbb{Q}(\xi_n) = \mathbb{Q}(\Phi_n)$$

donde el minimal de ξ_n es

$$\Phi_n \;=\; \prod_{\substack{1\le k<n \\ \mathrm{mcd}(k,n)=1}} \left(X - e^{\frac{2k\pi\, i}{n}}\right)$$

que es un polinomio irreducible en $\mathbb{Q}[X]$ de grado $\varphi(n)$.

O sea $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$.

- $\mathbb{Q}(\xi_n)/\mathbb{Q}$ es una extensión Galois *abeliana* (con grupo de Galois abeliano):

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) & \simeq & \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \\ \sigma & \mapsto & k \quad \text{si} \quad \sigma(\xi_n) = \xi_n^k \end{array}$$

Revisar la estructura como grupo abeliano de $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$:

Observación 10.2.1 (Intersección y compuesto)

1. *Sean* $m, n \in \mathbb{N}$ *con* $\mathrm{mcd}(m,n) = 1$. *Entonces*

$$\mathbb{Q}(\xi_m)\,\mathbb{Q}(\xi_n) \;=\; \mathbb{Q}(\xi_{mn}) \quad y \quad \mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) \;=\; \mathbb{Q}.$$

2. *Generalizar al caso* m, n *arbitrarios:*

Prueba.–

1. Se sabe que $\mathbb{Q}(\xi_m), \mathbb{Q}(\xi_n) \subset \mathbb{Q}(\xi_{mn})$ lo que implica que

$$\mathbb{Q}(\xi_m)\,\mathbb{Q}(\xi_n) \subset \mathbb{Q}(\xi_{mn}).$$

   Pero además si $\mathrm{mcd}(m,n) = 1$,

   $\xi_m\,\xi_n$ es raíz primitiva de orden mn de 1,

   y entonces

$$\mathbb{Q}(\xi_{mn}) \subset \mathbb{Q}(\xi_m)\,\mathbb{Q}(\xi_n).$$

   Para $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n)$, hacer diagrama justificando bien

2.

■

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

Para p primo, $\mathbb{Q}(\xi_p)/\mathbb{Q}$ es extensión Galois *cíclica* (con grupo de Galois cíclico) pues

$$\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \simeq \mathcal{U}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Asi $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) = \langle\sigma\rangle$ con σ de orden $p-1$.
Por lo tanto $\mathbb{Q}(\xi_p)/\mathbb{Q}$ tiene una subextensión F para cada $d' \mid p-1$, con

$$\mathrm{Gal}(\mathbb{Q}(\xi_p)/F) \simeq \mathbb{Z}/d'\mathbb{Z} \quad \text{y} \quad [\mathbb{Q}(\xi_p) : F] = d',$$

y esta es única (pues un grupo cíclico tiene un único subgrupo para cada divisor).
Además esta subextensión F es Galois también (¿por qué?),
de grado $d := \dfrac{p-1}{d'}$, y la llamamos F_d.
Se tiene $F_d = \mathbb{Q}(\xi_p)^H$ donde $H = \langle\sigma^d\rangle$ es el único subgrupo de $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ de orden d', y

$$\mathrm{Gal}(F_d/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\xi_p)/F_d) \simeq \mathbb{Z}/(p-1)\mathbb{Z}\,/\,\mathbb{Z}/d'\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}.$$

Observación 10.2.2

Sean F_d y F_e las subsextensiones de $\mathbb{Q}(\xi_p)/\mathbb{Q}$ de grados d y e resp. Entonces

$$F_d \subset F_e \quad \Longleftrightarrow \quad d \,|\, e.$$

En ese caso, $\mathrm{Gal}(F_e/F_d) \simeq \mathbb{Z}/\frac{e}{d}\mathbb{Z}$.

Prueba.–

Sabemos que $F_d = \mathbb{Q}(\xi_p)^{\langle\sigma^d\rangle}$ y $F_e = \mathbb{Q}(\xi_p)^{\langle\sigma^e\rangle}$ y como la correspondencia revierte inclusiones,

$$F_d \subset F_e \quad \Longleftrightarrow \quad \langle\sigma^d\rangle \supset \langle\sigma^e\rangle \quad \Longleftrightarrow \quad d \,|\, e.$$

Todo es Galois, y

$$\mathrm{Gal}(F_e/F_d) \simeq \mathrm{Gal}(\mathbb{Q}(\xi_p)/F_d)/\,\mathrm{Gal}(\mathbb{Q}(\xi_p)/F_e) \simeq \langle\sigma^d\rangle/\langle\sigma^e\rangle \simeq \mathbb{Z}/\tfrac{e}{d}\mathbb{Z}$$

Ejemplo $(\mathbb{Q}(\xi_5)/\mathbb{Q})$

Por simplicidad para mí, $\xi_5 =: \omega$

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

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

$$\begin{cases} \sigma: & \omega & \mapsto & \omega^2 \\ \sigma^2: & \omega & \mapsto & \omega^4 = \omega^{-1} \\ \sigma^3: & \omega & \mapsto & \omega^3 \\ \sigma^4 & = & \mathrm{id}_{\mathbb{Q}(\omega)} & \end{cases}$$

Los subgrupos de G son

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

¿Quién es la subextensión F_2 tal que $\mathrm{Gal}(\mathbb{Q}(\omega)/F_2) = \langle\sigma^2\rangle$?

$F_2 = \mathbb{Q}(\omega)^{\sigma^2}$ y $[\mathbb{Q}(\omega) : F_2] = 2$.

Se tiene $\sigma^2(\omega + \omega^{-1}) = \omega^{-1} + \omega$.

Esto implica que $\mathbb{Q}(\omega+\omega^{-1}) \subset F_2$ con $[F_2 : \mathbb{Q}] = \frac{4}{2} = 2$ y la inclusión no puede ser estricta, porque sino sería $\mathbb{Q} = \mathbb{Q}(\omega+\omega^{-1})$ pero $\sigma(\omega+\omega^{-1}) = \omega^2+\omega^{-2} \neq \omega+\omega^{-1}$.

Asi, $F_2 = \mathbb{Q}(\omega+\omega^{-1}) = \mathbb{Q}(\cos(2\pi/5)) \subset \mathbb{R}$.

Más aún

$$\begin{aligned} f(\omega+\omega^{-1},\mathbb{Q}) &= \big(X-(\omega+\omega^{-1})\big)\big(X-\sigma(\omega+\omega)\big) \\ &= \big(X-(\omega+\omega^{-1})\big)\big(X-(\omega^2+\omega^{-2})\big) \\ &= X^2+X-1 \;=\; \big(X-\frac{-1+\sqrt{5}}{2}\big)\big(X-\frac{-1-\sqrt{5}}{2}\big) \end{aligned}$$

Esto implica que si $\omega = e^{2\pi\, i/5}$,

entonces $\cos(2\pi/5) = \dfrac{\omega+\omega^{-1}}{2} = \dfrac{-1+\sqrt{5}}{4}$, y en particular

$$F_2 \;=\; \mathbb{Q}(\omega+\omega^{-1}) \;=\; \mathbb{Q}(\cos(2\pi/5)) \;=\; \mathbb{Q}(\sqrt{5}).$$

(La extensión $\mathbb{Q}(\omega)/\mathbb{Q}$ contiene la subextensión real $\mathbb{Q}(\sqrt{5})$.)

Por otro lado como $\mathrm{Gal}(\mathbb{Q}(\omega)/F_2) = \langle\sigma^2\rangle$,

$$\begin{aligned} f(\omega,F_2) &= (X-\omega)(X-\sigma^2(\omega)) = (X-\omega)(X-\omega^{-1}) \\ &= X^2-(\omega+\omega^{-1})X+1 \;=\; X^2-\Big(\frac{-1+\sqrt{5}}{2}\Big)X+1. \end{aligned}$$

De aquí se deduce

$$\omega = \frac{\frac{-1+\sqrt{5}}{2} \pm \sqrt{\frac{-5-\sqrt{5}}{2}}}{2}.$$

En particular ω se puede expresar por radicales...