Álgebra III - 2do C. 2020 - Clase 6 - 18/9/2020

4 El polinomio ciclotómico

4.1 Generalidades

$$\begin{aligned} X^n - 1 &= (X-1)(1 + X + \cdots + X^{n-1}) \quad \in \mathbb{Z}[X] \\ &= \prod_{0 \le k \le n-1} (X - e^{2k\pi\, i/n}) \quad \in \mathbb{C}[X] \end{aligned}$$

- Para p primo, $1 + \cdots + X^{p-1}$ es irreducible en $\mathbb{Z}[X]$, luego en $\mathbb{Q}[X]$.
- Para mn compuesto con $m, n > 1$, $1 + \cdots + X^{mn-1}$ ya no es irreducible. ¿Por qué?

La φ de Euler (Leonhard Euler, 1763)
Sea $n \in \mathbb{N}$. Entonces,

$$\varphi(n) := |\{1 \le k \le n : \mathrm{mcd}(k, n) = 1\}|.$$

Se tiene

- $\varphi(p) = p - 1$ para p primo
- $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$ para p primo
- $\varphi(mn) = \varphi(m)\varphi(n)$ para m, n coprimos, por lo tanto si $n = p_1^{k_1} \cdots p_r^{k_r}$, entonces
$$\varphi(n) = p_1(p_1^{k_1 - 1} - 1) \cdots p_r(p_r^{k_r - 1} - 1).$$
- Las raíces primitivas de orden n de 1 son $e^{2k\pi\, i/n}$ con $\mathrm{mcd}(k, n) = 1$ y por lo tanto hay $\varphi(n)$ de ellas.

4.2 Irreducibilidad del polinomio ciclotómico

Definimos el *polinomio ciclotómico* de orden n:

$$\Phi_n = \prod_{\substack{1\le k<n \\ \mathrm{mcd}(k,n)=1}} (X - e^{2k\pi\, i/n}) \quad \in \mathbb{C}[X].$$

Ejemplos

$\Phi_1 = X - 1$	$\Phi_4 = X^2 + 1$	$\Phi_7 = X^6 + \cdots + 1$
$\Phi_2 = X + 1$	$\Phi_5 = X^4 + X^3 + X^2 + X + 1$	$\Phi_8 =$
$\Phi_3 = X^2 + X + 1$	$\Phi_6 =$	$\Phi_9 =$

¡Todos parecen estar en $\mathbb{Z}[X]$, y de hecho lo están! Pues

$$X^n - 1 = \prod_{d|n} \Phi_d \quad \Rightarrow \quad \Phi_n = \frac{X^n - 1}{\prod_{d|n, d<n} \Phi_d} \quad \in \mathbb{Z}[X]$$

¿Y eso?

Ejemplo

$$\Phi_{p^2} = \frac{X^{p^2} - 1}{X^p - 1} = 1 + X^p + \cdots + X^{p(p-1)}$$

Curiosidad Pareciera que los coeficientes de Φ_n siempre son 0 o ± 1. Pero no es cierto: para $n = 105$ aparece un coeficiente igual a 2, y luego van apareciendo números cada vez más grandes (Bochman 1993).

Proposición 4.2.1 (Usado por Gauss en 1808, probado por Kronecker en 1854.)

$$\Phi_n \text{ es irreducible en } \mathbb{Q}[X].$$

Prueba.–

Sea $\omega = e^{2\pi i/n}$ y $f := f(\omega, \mathbb{Q}) \in \mathbb{Q}[X]$ irreducible.

Entonces $f \mid \Phi_n$ en $\mathbb{Q}[X]$ pues $\Phi_n(\omega) = 0$.

Alcanza con probar entonces que $\Phi_n \mid f$ en $\mathbb{Q}[X]$ pues son ambos mónicos. Para ello vamos a probar que $f(\omega^k) = 0$, para todo k coprimo con n.

El hecho que $f \mid \Phi_n$ en $\mathbb{Q}[X]$ con $\Phi_n \in \mathbb{Z}[X]$ mónico implica en particular que $f \in \mathbb{Z}[X]$. ¿Por?

Afirmación: Dada cualquier raíz ξ de f y p primo coprimo con n, $f(\xi^p) = 0$:

Sup. que no: sean ξ raíz de f y p primo coprimo con n tal que $f(\xi^p) \neq 0$.

Sea $g := f(\xi^p, \mathbb{Q})$.

Se tiene $g \mid \Phi_n$ pues $\Phi_n(\xi^p) = 0$ dado que $f(\xi) = 0$ implica $\Phi_n(\xi) = 0$ implica $\Phi_n(\xi^p) = 0$ por ser p coprimo con n. Así, $g \in \mathbb{Z}[X]$ también.

Además $g(\xi^p) = 0$ implica $f \mid g(X^p) \in \mathbb{Z}[X]$. ¿Se ve?

Pero $\operatorname{mcd}(f, g) = 1$ pues si no son coprimos son iguales, y $f(\xi^p) \neq 0$.

Esto implica $fg \mid \Phi_n$ en $\mathbb{Z}[X]$.

Consideremos esta divisibilidad en el cuerpo $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ con las operaciones $\bmod p$, donde $\overline{g(X^p)} = \overline{g}(X)^p$, pues si $g = a_d X^d + \cdots + a_1 X + a_0$, entonces

$$\begin{aligned}\overline{g(X^p)} &= \overline{a}_d X^{dp} + \cdots + \overline{a}_1 X^p + \overline{a}_0 \\ &= \overline{a}_d^p X^{dp} + \cdots + \overline{a}_1^p X^p + \overline{a}_0^p \\ &= \left(\overline{a}_d X^d + \cdots + \overline{a}_1 X + \overline{a}_0\right)^p \;=\; \overline{g}(X)^p\end{aligned}$$

ya que

$$(a+b)^p = a^p + \sum_{0<k<p} \binom{p}{k} a^{p-k} b^k + b^p = a^p + b^p \quad \text{en } \mathbb{F}_p, \text{ pues } p \mid \binom{p}{k} \text{ para } 0 < k < p.$$

Por lo tanto, $f \mid g(X^p)$ en $\mathbb{Z}[X]$ implica $\overline{f} \mid \overline{g(X^p)} = \overline{g}^p$ en $\mathbb{F}_p[X]$,

y si $\overline{r}$ es un factor irreducible de $\overline{f}$ en $\mathbb{F}_p[X]$, $\overline{r} \mid \overline{g}^p \;\Rightarrow\; \overline{r} \mid \overline{g}$.

Así,

$$\overline{r} \mid \overline{f} \;\text{ y }\; \overline{r} \mid \overline{g} \quad\Longrightarrow\quad \overline{r}^2 \mid \overline{f}\,\overline{g} \mid \overline{\Phi_n} \mid X^n - 1 \quad \text{en} \quad \mathbb{F}_p[X].$$

¡Pero *si p es coprimo con n*, $X^n - 1$ no tiene raíces múltiples ni aquí ni en la China! Absurdo...

Concluimos que dado ξ cualquiera raíz de f y p coprimo con n, ξ^p es raíz de f. Esto vale para ω...

Por lo tanto, ω^p es raíz de f para todo primo p coprimo con n, y tomando $\xi = \omega^p$ en la afirmación, ω^{p^2} y ω^{pq} son raíces de f para todos los primos p, q coprimos con n. ¿Se ve como sigue?

Dada ω^k una raíz cualquiera de Φ_n, con k coprimo con n, descomponemos k como producto de primos coprimos con n e iteramos lo que hicimos arriba. ¿Qué se concluye?

$$\Phi_n \mid f \quad !$$

■

5 Extensiones normales

5.1 Cuerpos de descomposición

Como consecuencia de la extensión de inmersiones en extensiones algebraicas obtenemos inmediatamente lo siguiente.

Observación 5.1.1
Sean E/K *algebraica y* $\alpha \in E$.
Sea $\beta \in \overline{K}$ *raíz de* $f(\alpha, K)$. *Entonces,*
el K*-isomorfismo* $K(\alpha) \underset{K}{\simeq} K(\beta)$, $\alpha \mapsto \beta$,
se extiende a $\sigma : E \underset{K}{\hookrightarrow} \overline{K}$.

También vimos que si E/K es algebraica, entonces todo K-endomorfismo de E es en realidad un K-automorfismo de E. (Con nuestra notación, en ese caso $\mathrm{End}(E/K) = \mathrm{Gal}(E/K)$.) Para cuerpos de descomposición $K(f)$, pasa algo aún más fuerte: toda K-inmersión de $K(f)$ en $\overline{K}$ es en realidad un K-automorfismo de $K(f)$, o sea en ese caso $\mathrm{Hom}(K(f)/K, \overline{K}/K) = \mathrm{Gal}(K(f)/K)$.

Proposición 5.1.2 (Inmersiones de cuerpos de descomposición)
Sea $K(f)$ *cuerpo de descomposición de* $f \in K[X]$ *sobre* K, *y sea* $\sigma : K(f) \underset{K}{\hookrightarrow} \overline{K}$ *una* K*-inmersión. Entonces* $\sigma(K(f)) \subset K(f)$ *y por lo tanto* σ *es un* K*-automorfismo de* $K(f)$.

Prueba.–
Sabemos que $K(f) = K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$, donde $\alpha_1, \ldots, \alpha_n \in \overline{K}$ son las raíces de f y que $\sigma \in \mathrm{Hom}(K(f)/K, \overline{K}/K)$ permuta las raíces de f. ¿Recuerdan? Por lo tanto $\sigma(\alpha_i) = \alpha_j \in K(f)$ y esto implica que para todo $g(\alpha_1, \ldots, \alpha_n) \in K(f)$ se tiene que $\sigma(g(\alpha_1, \ldots, \alpha_n)) \in K(f)$. O sea $\sigma(K(f)) \subset K(f)$.

■

Pero el cuerpo de descomposición de f tiene una propiedad aún más fuerte con respecto a cualquier polinomio irreducible:

Proposición 5.1.3 (Cuerpos de descomposición y polinomios irreducibles)
Sea $K(f)$ *cuerpo de descomposición de* $f \in K[X]$ *sobre* K, *y sea* $h \in K[X]$ *un polinomio* irreducible. *Si* h *tiene una raíz en* $K(f)$, *entonces* h *tiene todas sus raíces en* $K(f)$ *(o sea* h *se descompone linealmente en* $K(f)[X]$*).*

Prueba.–
Sea $\alpha \in K(f)$ raíz de h, y sea $\beta \in \overline{K}$ otra raíz de h.
Entonces por la observación 5.1.1, existe $\sigma : K(f) \underset{K}{\hookrightarrow} \overline{K}$ tal que $\alpha \mapsto \beta$.
Además por la proposición 5.1.2, σ es un K-auto de $K(f)$: así $\beta \in K(f)$.

■

5.2 Extensiones normales

Esta propiedad de los cuerpos de descomposición motiva la definición de *extensión normal*.

Definición 5.2.1 (Extensión normal)
Sea E/K una extensión de cuerpos. Se dice que E es una extensión normal de K *si E/K es algebraica y para todo $h \in K[X]$* irreducible*, si h tiene una raíz en E, entonces tiene todas sus raíces en E.*

Ejemplos

- $\overline{K}/K$ es
- $K(\sqrt{d})/K$ para $d \in K$ es
- $K(f)/K$ cuerpo de descomposición de $f \in K[X]$ sobre K es
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ es

En el caso finito conocemos bien las extensiones normales.

Proposición 5.2.2 (Extensión normal finita = cuerpo de descomposición)
Sea E/K finita. Entonces E/K es normal si yo solo si existe $f \in K[X]$ tal que $E = K(f)$.

Prueba.–

($\Rightarrow$) Si $E = K(\alpha_1, \ldots, \alpha_n)$ por ser finita, con $\alpha_1, \ldots, \alpha_n$ algebraicos sobre K, ¿quién es $f \in K[X]$ tal que $E = K(f)$?

($\Leftarrow$) OK por la proposición 5.1.3.

Teorema 5.2.3 (Caracterización de extensiones normales)
Sea E/K algebraica. Son equivalentes

1. *E/K normal*
2. *Toda K-inmersión de E en $\overline{K}$ es un K-automorfismo de E*
3. *E es el cuerpo de descomposición de una familia $\{f_i\}_{i\in I}$ de polinomios en $K[X]$ sobre K.*

Prueba.–

($1 \Rightarrow 2$) Sea $\sigma : E \underset{K}{\hookrightarrow} \overline{K}$ y $\alpha \in E$. Qpq $\sigma(\alpha) \in E$, porque así σ endo va a ser auto por ser la extensión algebraica (Prop. 3.4.6).

Tomemos entonces $h := f(\alpha, K)$, que es irreducible. Sabemos que $\sigma(\alpha) = \beta$, alguna raíz de h, y todas las raíces de h pertenecen a E por estar $\alpha \in E$ y ser la extensión normal.

($2 \Rightarrow 1$) Sea $\alpha \in E$ raíz de $h \in K[X]$ irreducible, y sea $\beta \in \overline{K}$ otra raíz de h. Sea $\sigma : E \underset{K}{\hookrightarrow} \overline{K}$ tal que $\alpha \mapsto \beta$ la K-inmersión que existe por la observación 5.1.1. Entonces σ es un K-auto de E y por lo tanto $\beta \in E$.

($2 \Rightarrow 3$) E es el cuerpo de descomposición de $\{f(\alpha, K) : \alpha \in E\}$:

($3 \Rightarrow 2$) Alcanza con probar que si $\sigma : E \underset{K}{\hookrightarrow} \overline{K}$, entonces $\sigma(E) \subset E$.

Pero E es la extensión generada por las raíces de los $f_i, i \in I$. Alcanza entonces con probar que si $\alpha \in E$ es raíz de algún f_i, entonces $\sigma(\alpha) \in E$, y esto es cierto porque $\sigma(\alpha)$ es alguna raíz de f_i que también pertenece a E.

■

5.3 Normalidad vs. torres y compuestos

1. Torres: Sea $E/F/K$ torre.

   - E/K normal $\Rightarrow$ E/F normal:

   - ¿E/K normal $\Rightarrow$ F/K normal?

   - ¿E/F y F/K normales $\Rightarrow$ E/K normal?

2. Compuestos e intersecciones: Sean $K \subset F, L \subset E$.

   - ¿F, L normales sobre K $\Rightarrow$ FL/K normal?

   - ¿F, L normales sobre K $\Rightarrow$ $F \cap L/K$ normal?

5.4 Clausura normal

Va a ser muy útil en lo que sigue trabajar con clausuras normales, que son las menores extensiones normales que contienen un cuerpo dado, ya que ahí sabemos que se cumplen muchas cosas (como que las K-inmersiones son K-autos y ese tipo de cosas).

Definición 5.4.1 (Clausura normal)
Sea E/K algebraica. La clausura normal *N de E/K es la menor extensión normal de K en $\overline{K}$ que contiene a E, i.e.*

$$N = \bigcap \{L : E \subset L \subset \overline{K} \text{ y } L/K \text{ normal}\}$$
$$= K(f(\alpha, K) : \alpha \in E).$$

La clausura normal es también única salvo isomorfismos.

Ejemplo

- La clausura normal de $\mathbb{Q}(\sqrt[3]{2})$ es

Observación 5.4.2 (Extensión finita $\Rightarrow$ Clausura normal finita)
Sea E/K finita y N su clausura normal, entonces N/K es finita también.