ALGEBRA 3 2017
Clase 5 - 29/8/17 ①

CLAUSURA ALGEBRAICA

Definición - Proposición: Sea E un cuerpo. Son equivalentes

① $\forall f \in E[X]$ con gr $f \geq 1$, $\exists \alpha \in E \,/\, f(\alpha) = 0$

② $f = c(X-\alpha_1)\dots(X-\alpha_n)$ en $E[X]$

③ L/E alg $\Rightarrow L = E$

En cualquier caso se dice que E es algebraicamente cerrado

Demostración

$(1 \Rightarrow 2)$ Por ind en gr f

$(2 \Rightarrow 3)$ Sea $\alpha \in L$ y sea $f = f(\alpha, E)$ (irred).

Pero $f = (X-\alpha_1)\dots(X-\alpha_n)$ con $\alpha_1, \dots, \alpha_n \in E \Rightarrow f = X - \alpha$

$\in E[X] \Rightarrow \alpha \in E$

$(3 \Rightarrow 1)$ Sea $f \in E[X]$ y L cpo de desc de f/E

$\Rightarrow L = E(\alpha_1, \dots, \alpha_n)$ es alg $\Rightarrow L = E \Rightarrow \alpha_1, \dots, \alpha_n \in E$.

Ejemplos

- $\mathbb{C}$ es alg cerrado
- $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \,/\, \alpha$ es alg$/\mathbb{Q}\}$ es cpo alg cerrado pues no tiene extensiones algebraicas

Definición (Clausura algebraica)

E es una <u>clausura algebraica</u> de K si

① E es algebraicamente cerrado

② E/K algebraica

Observación: Sea E/K alg tq $\forall f \in K[X]$ con gr $f \geq 1$, entonces f tiene <u>todas</u> sus raíces en E. Entonces E es alg cerrado

Demostración:

Sea $g \in E[X]$ y sea $\alpha \in$ cpo de desc de g/E $\Rightarrow$
α es alg$/E$ $\Rightarrow$ α es alg$/K$ $\Rightarrow \exists f \in K[X]$ tq α raíz de f
y f tiene todas sus raíces en E.

PROBLEMA (para investigar) Sea E/K algebraica tq $\forall f \in K[X]$
con $\operatorname{gr} f \geq 1$, f tiene al menos una raíz en E. Entonces
E es algebraicamente cerrado.

Teorema (Existencia y unicidad de clausura algebraica)

Existencia: alcanza c/probar que $\exists L/K$ alg cerrado pues
después se considera $E = \{\alpha \in L / \alpha \text{ alg}/K\}$

Demostración (ARTIN - 1898-1962)
$\forall f \in K[X]$ mónico con $\operatorname{gr} f \geq 1$, introduzco una variable X_f
Sea $P = K[X_f,\ f \in K[X],\ \operatorname{gr} f \geq 1,\ f \text{ mónico}]$
anillo de pols en ∞ variables y considero
$\mathfrak{a} := \langle f(X_f),\ \forall f \in K[X],\ \operatorname{gr} f \geq 1,\ f \text{ mónico} \rangle$
ideal de P generado por $\{f(X_f), \dots\}$

Afirmación: $\mathfrak{a} \subsetneq P$
Si $1 \in \mathfrak{a}$, existen $g_1, .., g_s \in P$ / $1 = g_1 f_1(X_{f_1}) + \dots + g_s f_s(X_{f_s})$
Sea E cpo de desc de $f_1, .., f_s / K$ y sean $\alpha_1, .., \alpha_s \in E$ tq
$f_1(\alpha_1) = 0, \dots, f_s(\alpha_s) = 0$. Entonces especializando X_{f_1} en $\alpha_1, \dots$
X_{f_s} en α_s, se tiene $1 = 0$ $\emptyset$
Luego $\exists \mathcal{M}$ ideal mxl de P tq $\mathfrak{a} \subseteq \mathcal{M}$

Y en particular $P/\mathcal{M}$ es cuerpo, $K \subseteq P/\mathcal{M}$

Se tiene además que $\forall f \in K[X]$ de grado ≥ 1 (mónico), f tiene una raíz en $P/\mathcal{M}$ pues $\mathfrak{a} \subseteq \mathcal{M} \Rightarrow$

$$\overline{f(X_f)} = f(\overline{X_f}) = \overline{0}.$$

Pero eso es como en el pb anterior: no garantiza que todas las raíces están en $P/\mathcal{M}$ (y no sabemos si es algebraica tampoco)

Se repite entonces el procedimiento:

Pongo $L_1 := P/\mathcal{M}$

Sea ahora L_2 extensión de L_1 con 1 raíz de cada pol (mónico) en $L_1[X]$

$$L_1 \subseteq L_2 \subseteq \dots \subseteq L_n \subseteq$$

$\forall f \in L_i[X]$ de grado ≥ 1 (mónico), $\exists$ una raíz de f en L_{i+1}

Sea $L = \bigcup_{i \geq 1} L_i$. Entonces L es cuerpo por ser cadena y además $\forall f \in L[X]$, $f \in L_i[X]$ para algún i y por lo tanto f tiene alguna raíz en $L_{i+1} \subseteq L$.

Para la unicidad demostramos el resultado esencial siguiente:

Teorema (Extensión de inmersiones)

Sea $\sigma : K \to L$ con L alg. cerrado y sea E/K ext algebraica de K. Entonces σ se extiende a $\overline{\sigma} : E \to L$

$$\begin{tikzcd} E \arrow[r, dashed, "\overline{\sigma}"] & L \\ K \arrow[u, dash, "alg"] \arrow[ur] & \end{tikzcd} \qquad (\text{i.e. } \overline{\sigma}|_K = \sigma)$$

"las ~~mo~~ inmersiones a un cpo alg cerrado se extienden a cualquier extensión alg"

Demostación

(Para E/K alg. finita, lo hicimos en cpos de desc.)

Para el caso general se usa el Lema de Zorn (Kuratowski)
1935 1922

Sea $S \neq \emptyset$ parcialmente ordenado.

Si toda cadena en S tiene cota superior en S,

entonces S tiene elementos maximales

cadena: subconjunto totalmente ordenado

cota superior: elto mayor o igual que todos los demás

elto maxl: elto que no es menor que ningún otro

Aquí: $S := \{(F, \tau) / K \subseteq F \text{ y } \tau|_K = \sigma\} \neq \emptyset$

pues $(K, \sigma) \in S$

$<$: $(F, \tau) < (F', \tau')$ si F'/F ext $(F \subseteq F')$ y $\tau'|_F = \tau$

orden parcial

Sea (F_i, τ_i) una cadena. Entonces $F = \cup F_i$,

$\tau: F \to L$ definido por $\tau(\alpha) = \tau_i(\alpha)$ si $\alpha \in F_i$ $\in S$

pues F es cuerpo y τ está bien definida.

(F, τ) es cota superior: $(F_i, \tau_i) < (F, \tau)$

Luego S admite un elto maximal (F, τ).

Afirmación: $F = E$. Pues sino sea $\alpha \in E - F$ que es algebraico

τ se extiende a

$$\begin{tikzcd} F(\alpha) \arrow[r, dashed, "\bar{\tau}"] & L \\ F \arrow[u, dash] \arrow[ur, "\tau"'] & \end{tikzcd}$$

Rdo: $F(\alpha) \simeq F[X]/_{f(\alpha, F)}$

$$\begin{tikzcd} F(\alpha) \arrow[r, dashed, "\bar{\tau}"] & L \\ F \arrow[u, dash] \arrow[ur, "\tau"] \arrow[r, "\tau"'] & \tau(F) = F' \arrow[u, dash] \end{tikzcd}$$

Sea $\beta \in L$ raíz de $\sigma(f(\alpha, F))$

$\bar{\sigma}: F \to \sigma(F)$

$\alpha \mapsto \beta$

Por lo tanto $F=E$, y $\tilde{\tau}$ extiende a σ. ⊠

Unicidad (salvo $\simeq$) de la clausura algebraica

Sean E, L dos clausuras algebraicas de K. Ent. $E \simeq_K L$

$$\begin{tikzcd} E \arrow[r, dashed, "\bar\sigma"] & L \\ K \arrow[u, dash] \arrow[ur, "id_K"'] & \end{tikzcd}$$

$\exists\, \bar\sigma : E \to L \,/\, \bar\sigma|_K = id_K$

Se tiene $\underbrace{E}_{\text{alg cerrado}} \simeq \underbrace{\bar\sigma(E)}_{\text{alg cerrado}} \subseteq L$

$\bar\sigma(E)$ es subcuerpo alg cerrado de L y $L/\bar\sigma(E)$ algebraica ⊠

$\Rightarrow$ $L = \bar\sigma(E)$.

$\Rightarrow$ de NOTACIÓN PARA CLAUSURA ALGEBRAICA : $\bar{K}, \bar{E} \ldots$

Lema: Sea E/K ext alg y $\sigma : E \to \bar{E}$ K-morf ($\sigma \in Hom(E/K, \bar{E}/K)$)
si $\sigma(E) \subseteq E$, o sea si $\sigma \in End(E/K)$, entonces σ es
K-automorfismo de E (o sea $\sigma \in Gal(E/K)$)

i.e. E/K alg $\Rightarrow$ $End(E/K) = Gal(E/K)$

Demostración: Ya lo probamos por dimensión para $[E:K] < \infty$

En general, reducirse al caso finito.

Sea $\beta \in E$. qpq $\exists\, \alpha \in E \,/\, \sigma(\alpha) = \beta$

Sea $f = f(\beta, K) = (X-\beta_1) \ldots (X-\beta_n) \in \bar{E}[X]$ con $\beta = \beta_1 \in E$

Sea $\{\beta_1, .., \beta_n\} \cap E = \{\beta_1, .., \beta_k\} \neq \emptyset$ pues $\beta_1 \in E$

y $E' = K[\beta_1, .., \beta_k] \subseteq E$.

Probemos que $\sigma|_{E'} : E' \hookrightarrow \bar{E}$ satisface $\sigma|_{E'}(E') \subseteq E'$.

Luego σ es automorfismo de E' por ser finita $\Rightarrow$ $\exists\, \alpha \in E' \subseteq E \,/\, \sigma(\alpha) = \beta$

Pero $\sigma(E) \subseteq E$ y $\sigma(\beta_i) = \beta_j$ $\Rightarrow$ $\sigma(E') \subseteq E'$.

Observación: Si E/K no es alg, es falso

$\sigma(X) = X^2$ es endo pero no auto

El polinomio ciclotómico:

$$x^n - 1 = \prod_{0 \le k \le n-1} \left(x - \left(\cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n}\right)\right)$$

$$= (x-1)(1+x+\dots+x^{n-1}) \in \mathbb{Z}[X]$$

Para $n=p$: $1+x+\dots+x^{p-1}$ es irreducible en $\mathbb{Q}[X]$ (pues lo es en $\mathbb{Z}[X]$)

Para $n=kl$ compuesto, con $k, l > 1$

$$x^n - 1 = x^{kl} - 1 = (x^k)^l - 1 = (x^k - 1)(1 + x^k + \dots + (x^k)^{l-1})$$

luego $1+x+\dots+x^{n-1}$ ya no es irreducible ...

$$\cancel{1} + \dots + x^{n-1} = (1+\dots+x^{k-1})(1+x^k+\dots+(x^k)^{l-1})$$

Aquí entra la φ de Euler (Leonhard Euler, 1763)

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

Se tiene

$$\varphi(p) = p-1$$
$$\varphi(p^n) = p^n - p^{n-1} = p(p^{n-1} - 1)$$

y si $\text{mcd}(m,n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$

Esto implica que si $n = p_1^{k_1} \cdots p_r^{k_r}$,

entonces $\varphi(n) = p_1(p_1^{k_1-1} - 1)\, p_2(p_2^{k_2-1} - 1) \cdots p_r(p_r^{k_r-1} - 1)$

Sabemos que las raíces primitivas de orden n de 1 son

$$\cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n} \quad \text{con} \quad \text{mcd}(k,n) = 1$$

y por lo tanto hay $\varphi(n)$ de ellas.

Ponemos

$$\phi_n = \prod_{mcd(k,n)=1} \left(x - \left(\cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n}\right)\right) \in \mathbb{C}[X]$$

$\phi_1 = X - 1$ $\qquad \phi_5 = X^4 + X^3 + X^2 + X + 1$

$\phi_2 = X + 1$ $\qquad \phi_6 = X^2 - X + 1$

$\phi_3 = X^2 + X + 1$ $\qquad \phi_7 = X^6 + \dots + 1$

$\phi_4 = X^2 + 1$ $\qquad \phi_8 = X^4 + 1$

En general $\displaystyle\prod_{d|n} \phi_d = X^n - 1 \Rightarrow \boxed{\phi_n = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \phi_d} \in \mathbb{Z}[X]}$ Obs

pues todos los pols son mónicos

Ejemplo: $\displaystyle \phi_{p^2} = \frac{X^{p^2} - 1}{X^p - 1} = 1 + X + \dots + X^{p(p-1)} \in \mathbb{Z}[X]$

Curiosidad: Pareciera que los coefs de ϕ_n son $0, \pm 1$ pero para $n = 105$, aparece un 2, y luego aparecen números c/vez más grandes (Bachman 1993)

Proposición: ϕ_n es irreducible en $\mathbb{Q}[X]$

Usado por Gauss en 1808 - Probado por Kronecker en 1854

Demostración:

Sea $\xi_n = \cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n}$ y $f = f(\xi, \mathbb{Q})$ irreducible mónico. Entonces $f \mid \phi_n$ en $\mathbb{Q}[X] \Rightarrow f \in \mathbb{Z}[X]$ pues ϕ_n mónico en $\mathbb{Z}[X]$, i.e. ϕ_n primitivo en $\mathbb{Z}[X]$

$$\phi_n = f\, g \text{ con } f, g \in \mathbb{Q}[X] \text{ mónicos}$$

$\Rightarrow \exists\, c, d \in \mathbb{Q} \,/\, \phi_n = (cf)(dg)$ con $cf \in \mathbb{Z}[X]$, $dg \in \mathbb{Z}[X]$

$cd = 1$ y $c, d \in \mathbb{Z}$ pues $cf \in \mathbb{Z}[X]$, $dg \in \mathbb{Z}[X]$ y f, g mónicos

$\Rightarrow c = d = \pm 1$.

Probemos que dada $\tilde{\xi}$ raíz de f y p primo con $mcd(p,n)=1$, entonces $f(\tilde{\xi}^p)=0$:

Sup que no: $\exists$ p primo coprimo con $f(\tilde{\xi}^p)\neq 0$

Sea g el polinomio irreducible en $\mathbb{Q}[X]$ que anula a $\tilde{\xi}^p$:

$g=f(\tilde{\xi}^p,\mathbb{Q})$: como $g \mid \Phi_n$, ent. $g\in \mathbb{Z}[X]$ (mónico tb)

Se tiene $mcd(f,g)=1$, pues si no son coprimos son iguales pero $f(\tilde{\xi}^p)\neq 0$

Así $\Phi_n = f\,g\,h$. Pero $f(\tilde{\xi})=0$ y $g(\tilde{\xi}^p)=0$

luego $\tilde{\xi}$ es raíz de $g(X^p) \Rightarrow f \mid g(X^p)$ en $\mathbb{Z}[X]$

Trabajamos en $\mathbb{F}_p[X]$ donde $\overline{g(X^p)}=\overline{g(X)}^p$ (tomando clase de los coeftes mód p)

$\bar{f} \mid \overline{g(X^p)}$ en $\mathbb{F}_p[X]$ y si $\bar{r}\in\mathbb{F}_p[X]$ es divisor irreducible de $\bar{f}$, $\bar{r}\mid\bar{f}$ y $\bar{r}\mid\overline{g(x)}^p \Rightarrow \bar{r}\mid\bar{g}$

Así $\bar{r}^2 \mid \bar{\Phi}_n \mid \overline{1+X+\dots+X^{n-1}} \mid \bar{X}^n-1$ en $\mathbb{F}_p[X]$ pues es coprimo

Pero $\bar{X}^n-1$ no tiene raíces múltiples en $\mathbb{F}_p[X]$ pues es coprimo con su derivada ...

Así dado $\tilde{\xi}$ raíz de f y p primo, coprimo con n, $f(\tilde{\xi}^p)=0$

Luego $f(\xi^k)=0$, $\forall$ k coprimo con n. $\boxtimes$

$\Rightarrow \Phi_n \mid f$ también