Álgebra III - 2do C. 2020 - Clase 12 - 9/10/2020

Lema de Artin

Vamos a ver ahora un importante resultado debido a Émile Artin, conocido como el *Lema de Artin*, que de alguna manera le saca todo el jugo a las relaciones entre cuerpo fijo y Galois.

Teorema 8.2.13 (Lema de Artin)
Sea E un cuerpo y sea $G < \mathrm{Aut}(E)$ un subgrupo finito *de automorfismos de E. Entonces*

- *E/E^G es Galois finita,*
- $\mathrm{Gal}(E/E^G) = G$.

La correspondencia de Galois para una extensión Galois *finita* E/K es directa a partir del lema de Artin:
Probamos que para $H < \mathrm{Gal}(E/K)$ y F/K subextensión de E/K,

- $H \mapsto E^H \mapsto \mathrm{Gal}(E/E^H) = H$, tomando $G = H$.
- $F \mapsto \mathrm{Gal}(E/F) \mapsto E^{\mathrm{Gal}(E/F)} = F$:

  Sea $G = \mathrm{Gal}(E/F)$.

  Por el lema de Artin, $E/E^{\mathrm{Gal}(E/F)}$ es Galois y $\mathrm{Gal}(E/E^{\mathrm{Gal}(E/F)}) = \mathrm{Gal}(E/F)$.

  Esto implica $[E : E^{\mathrm{Gal}(E/F)}] = [E : F]$.

  Pero claramente $F \subset E^{\mathrm{Gal}(E/F)}$, y por lo tanto $F = E^{\mathrm{Gal}(E/F)}$.

Lema auxiliar para probar el lema de Artin (Interesante en sí)
Sea E/K separable y supongamos que existe una cota superior N tal que

$$[K(\alpha) : K] \leq N, \quad \forall\, \alpha \in E.$$

Entonces existe $\theta \in E$ tal que $E = K(\theta)$ (y por lo tanto E/K es finita).

Prueba.–
Sea $\theta \in E$ con $[K(\theta) : K]$ máximo. Entonces $E = K(\theta)$ pues sino $\exists\, \alpha \in E \setminus K(\theta)$ tq $K(\theta) \subsetneq K(\theta, \alpha)$ que es finita y separable, y por lo tanto simple también:
Existe $\beta \in E$ tal que $K(\theta, \alpha) = K(\beta)$ con $[K(\beta) : K] > [K(\theta) : K]$. ¡Absurdo!

$\blacksquare$

Prueba del lema de Artin.–

Notemos $K := E^G$.

Qpq E es el cuerpo de descomposición $K(f)$ de un polinomio $f \in K[X]$ separable, así E/K Galois finita.

Para ello vamos a probar primero que dado $\alpha \in E$, α es raíz de un polinomio $f_\alpha \in K[X]$ separable.

Como venimos haciendo ultimamente, como G es finito, el conjunto de valores *distintos* tomados por $\{\sigma(\alpha) : \sigma \in G\}$ es finito, y lo denotamos por $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$.

(Ojo que aquí los σ son solo automorfismos de E, así que no sé a priori que α va a parar a raíces de ningún minimal.)

Definimos
$$f_\alpha = \prod_{1 \le i \le n} \big(X - \sigma_i(\alpha)\big) \quad \in \ E[X]$$
pues $\alpha \in E$ y $\sigma_i \in \mathrm{Aut}(E)$ implican $\sigma_i(\alpha) \in G$.

Como venimos observando en otras demostraciones, $f_\alpha \in E^G[X] = K[X]$ pues
$$\sigma(f_\alpha) = \sigma\Big(\prod_{1 \le i \le n} \big(X - \sigma_i(\alpha)\big)\Big) = \prod_{1 \le i \le n} \big(X - \sigma \circ \sigma_i(\alpha)\big) = f_\alpha, \ \ \forall\, \sigma \in E.$$

O sea α es raíz de un polinomio separable $f_\alpha \in K[X]$, pero no solo eso, sino que para todo $\alpha \in E$,
$$[K(\alpha) : K] \ \le \ \mathrm{gr}(f_\alpha) \ \le \ |G|,$$
y por lo tanto por el lema auxiliar anterior, $E = K(\theta)$ donde θ es raíz de un polinomio separable $f := f(\theta, K)$, con $\mathrm{gr}(f) \le |G|$, y todas sus raíces en E:
$$E = K(f) \text{ Galois finita} \quad \text{y} \quad |\mathrm{Gal}(E/K)| = [E : K] \le |G|.$$

Probar ahora que $G = \mathrm{Gal}(E/K)$ es inmediato pues $G \subset \mathrm{Gal}(E/K)$:

por definición,
$$\forall\, \sigma \in G, \forall\, \alpha \in K = E^G, \ \sigma(\alpha) = \alpha,$$
y por lo tanto $G = \mathrm{Gal}(E/K)$.

∎

9 Cuerpos finitos (o cuerpos de Galois)

Recuerdo:

- K cuerpo finito $\Rightarrow$ $\mathrm{car}(K) = p$ para algún primo p.
- $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ con las operaciones suma y producto módulo p es el cuerpo primo de K.
- K es un $\mathbb{F}_p$-e.v. de dimensión finita n para algún $n \in \mathbb{N}$ y por lo tanto $|K| = p^n$.
- Miremos $\mathbb{F}_p$ con otros ojos: por el Pequeño Teorema de Fermat, se tiene

  $$a^p = a, \ \forall\, a \in \mathbb{F}_p.$$

  O sea, dada $\overline{\mathbb{F}_p}$ la clausura algebraica de $\mathbb{F}_p$, se tiene

  $$\mathbb{F}_p = \{a \in \overline{\mathbb{F}_p} : \ a \text{ es raíz de } X^p - X\} \ \subset \ \overline{\mathbb{F}_p},$$

  pues los p elementos de $\mathbb{F}_p$ satisfacen la ecuación, que tiene a lo sumo p raíces.

  (Notar que $X^p - X$ es separable pues $(X^p - X)' = -1$ en $\mathbb{F}_p(X)$.)

  O sea, siendo redundantes, podemos mirar a $\mathbb{F}_p$ como un cuerpo de descomposición:

  $$\mathbb{F}_p \ = \ \mathbb{F}_p(X^p - X) \ \subset \ \overline{\mathbb{F}_p}.$$

9.1 Los cuerpos de Galois

Proposición 9.1.1 (Los cuerpos de Galois)
Sea p primo y $n \in \mathbb{N}$. Entonces, el conjunto

$$E := \{\alpha \in \overline{\mathbb{F}_p} \ : \ \alpha \text{ es raíz de } X^{p^n} - X\} \ \subset \ \overline{\mathbb{F}_p}$$

es un cuerpo que tiene exactamente p^n elementos, y que podemos escribir como

$$E = \mathbb{F}_p(X^{p^n} - X) \ \subset \ \overline{\mathbb{F}_p}.$$

Resultado auxiliar importante en sí (y que ya conocemos, o casi)
Sea K *un cuerpo con* $\operatorname{car}(K) = p$, *entonces, para cualquier* $n \in \mathbb{N}$ *se tiene*

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}.$$

Prueba.– Por inducción en n:

$n = 1$:

$$(\alpha+\beta)^p = \alpha^p+\beta^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k} = \alpha^p+\beta^p \quad \text{pues } p \mid \binom{p}{k} \text{ para } 0 < k < p.$$

$n > 1$:

$$\begin{aligned}(\alpha + \beta)^{p^n} &= \left((\alpha + \beta)^p\right)^{p^{n-1}} \underset{n=1}{=} (\alpha^p + \beta^p)^{p^{n-1}} \\ &\underset{HI}{=} (\alpha^p)^{p^{n-1}} + (\beta^p)^{p^{n-1}} = \alpha^{p^n} + \beta^{p^n}\end{aligned}$$

■

Prueba de la proposición 9.1.1.–

- $K = \{\alpha \in \overline{\mathbb{F}_p} \,:\, \alpha^{p^n} - \alpha = 0\}$ es cuerpo pues
  - $0, 1 \in K$
  - $\alpha, \beta \in K \;\Rightarrow\; \alpha \pm \beta \in K$ pues
  - $\alpha, \beta \in K \;\Rightarrow\; \alpha\beta \in K$ pues
  - $\alpha \in K^\times \;\Rightarrow\; \dfrac{1}{\alpha} \in K$ pues
- $|K| = p^n$ pues $X^{p^n} - X$ es un polinomio separable:
- $K = \mathbb{F}_p(X^{p^n} - X)$ pues $\mathbb{F}_p \subset K$:

  y

$$K = \{\alpha_1, \ldots, \alpha_{p^n}\} = \mathbb{F}_p(\alpha_1, \ldots, \alpha_{p^n}),$$

ya que es el menor cuerpo que contiene a $\mathbb{F}_p$ y a $\{\alpha_1, \ldots, \alpha_{p^n}\}$, las p^n raíces de $X^{p^n} - X$ en $\overline{\mathbb{F}_p}$.

■

¡Vale la recíproca!

Proposición 9.1.2 (Unicidad del cuerpo de p^n elementos)
Sea K un cuerpo con $\operatorname{car}(K) = p$ *y* $|K| = p^n$ *para algún* $n \in \mathbb{N}$. *Entonces*

$$K = \mathbb{F}_p(X^{p^n} - X) \ \subset \overline{\mathbb{F}_p},$$

el *cuerpo de descomposición de* $X^{p^n} - X$ *sobre* $\mathbb{F}_p$.

Prueba.–
Ya sabemos que al ser K cuerpo finito de característica p, $\mathbb{F}_p \subset K \subset \overline{\mathbb{F}_p}$, y como $|K| = p^n$, $K^\times$ es un grupo multiplicativo finito de orden $p^n - 1$.
Así, $\forall\, \alpha \in K^\times$,

$$\alpha^{p^n-1} = 1 \quad \underset{\cdot\alpha}{\Longrightarrow} \alpha^{p^n} = \alpha.$$

Como para $\alpha = 0$ también vale $\alpha^{p^n} = \alpha$, se tiene

$$\forall\, \alpha \in K, \quad \alpha^{p^n} = \alpha \quad \text{i.e.} \quad \alpha \ \text{ es raíz de } \ X^{p^n} - X.$$

Por lo tanto, $K \subset \mathbb{F}_p(X^n - X)$, y, como ya sabemos que $\mathbb{F}_p(X^{p^n} - X)$ es un cuerpo con p^n elementos, se concluye porque tienen igual cardinal.

■

Resumimos todo lo obtenido, y más, en el siguiente teorema con notación.

Teorema 9.1.3 (El cuerpo de Galois $\mathbb{F}_{p^n}$)
Sea p primo. Entonces

- *Dado* $n \in \mathbb{N}$, existe *un* único *cuerpo con* p^n *elementos. Este es*

  $$\mathbb{F}_{p^n} := \mathbb{F}_p(X^{p^n} - X) \quad \subset \ \overline{\mathbb{F}_p}.$$

  En particular $\mathbb{F}_{p^n}$ *es Galois sobre* $\mathbb{F}_p$ *por ser cuerpo de descomposición de un polinomio separable.*

- *Todo cuerpo finito de característica p es* $\mathbb{F}_{p^n}$ *para algún* $n \in \mathbb{N}$, *y en particular es Galois sobre* $\mathbb{F}_p$.

- $$X^{p^n} - X = \prod_{\alpha \in \mathbb{F}_{p^n}} (X - \alpha) \quad \in \ \overline{\mathbb{F}_p}[X].$$

Consecuencia obvia *(por si no lo sabíamos ya)*

$$|\overline{\mathbb{F}_p}| =$$

9.2 Subextensiones de $\mathbb{F}_{p^n}$

Ejemplo

$\mathbb{F}_2 = \{0,1\}$, $\mathbb{F}_4 = \mathbb{F}_2(X^4 - X)$, $\mathbb{F}_8 = \mathbb{F}_2(X^8 - X)$, $\mathbb{F}_{16} = \mathbb{F}_2(X^{16} - X)$.

¿Qué contenciones tenemos?

Proposición 9.2.1 (Intersecciones y subextensiones de cuerpos de Galois)
Sean $m, n \in \mathbb{N}$.

1. $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{\mathrm{mcd}(n,m)}}$.
2. $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \,|\, n$.

Prueba.–

1. En Álgebra I en algun momento se vio que

   $$\mathrm{mcd}(X^N - 1, X^M - 1) = X^{\mathrm{mcd}(M,N)} - 1$$

   pues por el Algoritmo de Euclides para el cálculo del mcd, si $N = q\,M + R$, entonces

   $$X^N - 1 = X^{qM+R} - X^R + X^R - 1 = X^R(X^{qM} - 1) + X^R - 1$$

   y como $X^M - 1 \,|\, X^{qM} - 1$ se tiene que $X^N - 1 = Q(X) \cdot (X^M - 1) + X^R - 1$ y

   $$\mathrm{mcd}(X^N - 1, X^M - 1) = \mathrm{mcd}(X^M - 1, X^R - 1), \quad \text{etc.}$$

   Con el mismo razonamiento,

   $$\mathrm{mcd}(p^n - 1, p^m - 1) = p^{\mathrm{mcd}(n,m)} - 1.$$

   Por lo tanto

   $$\mathrm{mcd}(X^{p^n-1} - 1, X^{p^m-1} - 1) = X^{\mathrm{mcd}(p^n-1, p^m-1)} - 1 = X^{p^{\mathrm{mcd}(n,m)}-1} - 1$$

lo que implica

$$\begin{aligned}\operatorname{mcd}(X^{p^n}-X,X^{p^m}-X) &= X\operatorname{mcd}(X^{p^n-1}-1,X^{p^m-1}-1)\\ &= X\big(X^{p^{\operatorname{mcd}(n,m)}-1}-1\big) \;=\; X^{p^{\operatorname{mcd}(m,n)}}-X.\end{aligned}$$

Así,

$$\begin{aligned}\mathbb{F}_{p^n}\cap\mathbb{F}_{p^m} &= \big\{\alpha\in\overline{\mathbb{F}_p}:\ \alpha \text{ raíz de } \ X^{p^n}-X \ \text{ y de } \ X^{p^m}-X\big\}\\ &= \big\{\alpha\in\overline{\mathbb{F}_p}:\ \alpha \text{ raíz de } \ X^{p^{\operatorname{mcd}(n,m)}}-X\big\} \;=\; \mathbb{F}_{p^{\operatorname{mcd}(m,n)}}.\end{aligned}$$

2.

$$\begin{aligned}\mathbb{F}_{p^m}\subset\mathbb{F}_{p^n} &\iff \mathbb{F}_{p^m}\cap\mathbb{F}_{p^n} \;=\; \mathbb{F}_{p^m}\\ &\iff \mathbb{F}_{p^{\operatorname{mcd}(m,n)}} \;=\; \mathbb{F}_{p^m}\\ &\iff \operatorname{mcd}(m,n) \;=\; m \quad\iff\quad m\,|\,n\end{aligned}$$

■

Ejemplo

Dibujar el árbol de extensiones de $\mathbb{F}_5$: