I: GRUPOS

Defin Sea G un conjto y $\circ : G \times G \to G$, $(g, g') \mapsto g \circ g'$ una aplicación a la que llamaremos **operación**.

$$(G, \circ) \text{ grupo} :\iff \begin{cases} i) \circ \text{ asociativa} : (g \circ g') \circ g'' = g \circ (g' \circ g'') \\ ii) \exists \text{ elto neutro} : \exists 1 : g \cdot 1 = 1 \, g = g \\ iii) \text{Todo elto tiene inverso} : \forall g \; \exists g^{-1} : g \, g^{-1} = 1. \end{cases}$$

$(G, \circ)$ se dice **abeliano** o conmutativo si $g \circ g' = g' \circ g \;\; \forall g, g'$.

- Si la operación se denota con "+" se dice que el neutro es el "0" y el inverso con opuesto y se denota con $-g$.

Lema El elto neutro y el inverso de un elto son únicos.

Defin: Sea $H \subseteq (G, \circ)$ grupo. Se dice que H es un subgrupo, $H \leq G$ ó $H < G$, si $(H, \circ|_{H \times H})$ es un grupo, ie,

$$(H, \circ) \text{ subgrupo} \iff \begin{cases} i) \; h, h' \in H \Rightarrow h \circ h' \in H \;\; (\circ \text{ bien def}) \\ ii) \; 1 \in H \\ iii) \; \forall h \; \exists h^{-1} \in H. \end{cases}$$

Teorema (Caracterización de Subgrupo): Sea $H \subseteq G$.

$$H \leq G \iff h \circ h'^{-1} \in H \quad \forall h, h' \in H.$$

• $(\mathbb{Z}, +)$ es un gpo. ¿Cuáles son sus subgpos?

Teorema: Todo subgpo de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$.

Defn: Una función $f: G_1 \longrightarrow G_2$ es un morfismo de gpos si

$$f(a \cdot b) = f(a) \cdot f(b)$$

• f mor de gpos $\Rightarrow f(1_{G_1}) = 1_{G_2}$; y $f(a^{-1}) = f(a)^{-1}$.

Defn: Sea $f: G \to G'$ morfismo de gpos. Se llama

$$\ker f := \{ g \in G : f(g) = 1_{G'} \} \quad (= f^{-1}(1))$$

$$\operatorname{Im} f := \{ f(g) : g \in G \} \subseteq G' \quad (= f(G))$$

Propos: f(subgpo) es un subgpo y f^{-1}(subgpo) también. En particular $\ker f$ y $\operatorname{Im} f$ lo son.

Defn: Sea $H \leq G$. Entonces se define una relación de equivalencia en G:

$$\boxed{a \equiv b \iff a^{-1}b \in H}$$

y se llaman clases de g a $[g] = \overline{g} = \{ g' \in G : g \equiv g' \}$.

• $[1] = H$ y $[a] = aH$.

Propos: Las clases de equivalencia son bien iguales bien disjuntas.

Defin: Un subgpo $H \leq G$ se dice **normal** si $\forall g \in G \quad gHg^{-1} \subseteq H$.

- Todo gpo abeliano es normal.
- G/H es un gpo cuando H es normal vía $\overline{g} \cdot \overline{g'} := \overline{g \cdot g'}$ (bien def).

Defin: Llamamos **orden** de G a $|G| := \text{card } G = \#G$.

Teorema (Lagrange): $|G/H| = \dfrac{|G|}{|H|}$.

Corolario: El orden de un subgpo divide al orden del gpo.

Teorema (Propiedad Universal del Gpo Cociente): Sea $f: G \to G'$ hom gpos y π la proyección canónica al cociente, y $H \leq G$ normal

f factoriza a través de la π ($\text{ie}, \exists\, \varphi: G/H \to G' : f = \varphi \circ \pi$) $\iff H \subseteq \ker f$.

- $f^{-1}(f(g)) = g \cdot \ker f$. Ej: f inyectiva $\iff \ker f = 1$.

Corolario (Teorema de Isomorfía): $G/\ker f \simeq \text{Im } f$.

GRUPOS CÍCLICOS

Definición: Un gpo G se dice **cíclico** si $G = \langle g \rangle = \{g^n\}_{n \in \mathbb{Z}}$ para algún $g \in G$.

Teorema: G cíclico $\iff G \simeq \mathbb{Z}/n\mathbb{Z}$.

- n = menor natural posible tal que $g^n = 1$.

Teorema:

1) $\langle \bar{m} \rangle = \mathbb{Z}/n\mathbb{Z} \iff n$ y m son primos entre sí

2) $n\mathbb{Z} \cap m\mathbb{Z} = c\mathbb{Z} \iff c = mcm(n,m)$

3) $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z} \iff d = mcd(n,m)$.

Propos. Todo subgpo de un gpo cíclico es cíclico.

Propos: $|G| = p \Rightarrow G$ cíclico.

Teorema: Todo gpo abeliano finito generado es isomorfo a producto directo de cíclicos.

$$G \simeq \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{m_r}\mathbb{Z}.$$

- El producto directo de dos gpos, $G_1 \times G_2$, es gpo con la operación

$$(g_1, g_2) * (g_1', g_2') := (g_1 *_1 g_1', g_2 *_2 g_2').$$

Propos: $H, H' \leq G$ normales (en G) tal que $H \cap H' = \{1\}$ $\Rightarrow$ el producto cartesiano de los elts de H y H' y $H \times H' \simeq H \cdot H'$.

Propos: $H, H' \leq G$ con $h'Hh'^{-1} \subseteq H$ (H normal en H') y $H \cap H' = \{1\} \Rightarrow$

$H \times H' \longrightarrow HH'$, $(h,h') \mapsto hh'$ es biyectiva.

- ¡OJO! La aplicación anterior es una biyección, pero no es un isomorfismo de gpos.

Para que la aplicación anterior sea morf de gpos hay que definir en $H \times H'$ otra operación.

Definición: Se llama producto semidirecto de H y H', $H \rtimes H'$, al grupo que como conjunto es $H \times H'$ y en el cual está definida la operación

$$(h_1, h_1') * (h_2, h_2') := (h_1 h_1' h_2 h_1'^{-1}, h_1' h_2')$$

que es la operación con la que $H \rtimes H' \simeq HH'$ es subgrupo (hip implícita) en las hipótesis de la Prop. anterior.

GRUPO SIMÉTRICO

- $S_n := \{$ permutaciones (biyecciones) de un conjunto X de n elementos $\} = B_{1,\dots,n}$ y X.
- $|S_n| = n!$
- $\sigma = (x_1, \dots, x_r)$ es un r-ciclo, $(x_i x_j)$ una trasposición.

Propos: Toda permutación es producto de ciclos disjuntos. Más aún, toda permutación es producto de trasposiciones.

- Si $\sigma = \sigma_1 \cdots \sigma_r$, y $\sigma_i = (x_{i_1}, \dots, x_{i_{d_i}})$, se le llama **forma** de la permutación a $d_1, \dots, d_r$, de menor a mayor.
- Se llama **orden** de $(x_1, \dots, x_r)$ a r.

Lema: $\tau (x_1, \dots, x_r) \tau^{-1} = (\tau(x_1), \dots, \tau(x_r))$.

Propos: Dos permutaciones tienen la misma forma $\iff$ son conjugadas.

- Notar que el producto de ciclos disjuntos **conmuta**!
- Notar que en S_n hay $\binom{n}{r}(r-1)! = \frac{n \cdot (n-1) \cdot \dots \cdot (n-r+1)}{r}$ r-ciclos.

Definición: Tomamos el polinomio $\delta(x_1,\dots,x_n) := \prod_{i<j}(x_i - x_j)$. Se llama signo de una permutación $\sigma \in S_n$ a 1 ó -1 que cumple

$$\delta(x_1,\dots,x_n)^\sigma = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}) = (\pm 1)\prod_{i<j}(x_i - x_j)$$

$$= (\operatorname{sgn}\sigma)\cdot\delta(x_1,\dots,x_n).$$

- $\operatorname{sgn}: (S_n, \circ) \longrightarrow (\{1,-1\}, \cdot)$, $\sigma \longmapsto \operatorname{sgn}\sigma$ es un morfismo de grupos, luego

$$\operatorname{sgn}(\sigma\circ\tau) = (\operatorname{sgn}\sigma)\cdot(\operatorname{sgn}\tau).$$

- $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau\sigma\tau^{-1})$
- $\operatorname{sgn}(12) = -1$, y en general $\operatorname{sgn}(t_{ij}) = -1$.

Proposición: $\operatorname{sgn}(x_1,\dots,x_r) = (-1)^{r-1} = \begin{cases} -1 & \text{si } r \text{ par} \\ 1 & \text{si } r \text{ impar.} \end{cases}$

Defn: Se llama grupo alternado a

$$A_n := \{\sigma \in S_n : \operatorname{sgn}\sigma = +1\} = \ker(\operatorname{sgn}) \leq S_n.$$

- $S_n/A_n \simeq \{\pm 1\}$, luego $|A_n| = \frac{n!}{2}$.
- Resulta que $A_n \cap \langle(12)\rangle = \{Id\}$, y $(12)A_n(12) \subsetneq A_n$, y $A_n \subsetneq A_n\cdot\langle(12)\rangle \subsetneq S_n$ $\Rightarrow A_n\cdot\langle(12)\rangle = S_n$, se tiene

$$A_n \rtimes \langle(12)\rangle \simeq S_n.$$

6

G-conjuntos

Defn Sea $(G, \cdot)$ un grupo y X un conjunto. Se dice que X es un **G-conjunto** si existe alguna aplicación

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g * x \end{aligned}$$

tal que

i) $1 * x = x \quad \forall x$

ii) $g * (g' * x) = (g \cdot g') * x$

y se dice que G **opera en** X.

Defn: Sea $(G, \cdot)$ grupo y X, Y dos G-conjuntos. Se dice que una aplicación $f: X \to Y$ es un **morfismo de G-conjuntos** si $f(g * x) = g * f(x)$.

- G es G-conjunto operando por dch, izda, conjugación. G/H es G-conj.

Defn. Sea $x \in X$. Se llama **órbita de x** a $G * x = \{ g * x \}_{g \in G}$.

Prop: Sean $x, x' \in X$. Dos órbitas $G * x$ y $G * x'$ son bien iguales bien disjuntas.

- Podemos definir una rel. de eq. con $x \equiv x' \Rightarrow G * x = G * x'$. Así se tiene

$$G/X = \{ [x] \}_{x \in Y}.$$

Defn: Se llama grupo de isotropía a $I_x := \{g \in G : g * x = x\}$.

Propos: $G * x \cong G/I_x$ es un isomorfismo de G-conjuntos.

Defn: Sea X un G-conjunto. Se llama invariantes de X por la acción de G a

$$X^G := \{x \in X : G * x = x\}$$

- Notar que $x \in X^G \Leftrightarrow I_x = G \Leftrightarrow G * x = x$

Defn: Se llama centro de G a $Z(G) := \{g \in G : g \text{ conmuta con todo } G\}$.

- Notar que si G es un G-conjunto por conjugación, entonces $G^G = Z(G)$.

* **Teorema** (Fórmula de Clase): Sea $|G| = p^n$, G grupo y X un G-conjunto. Entonces

$$\boxed{|X| \equiv |X^G| \pmod{p}}$$

Corolario: $|G| = p^n \Rightarrow |Z(G)| > 1$. $(Z(G) \neq \{1_G\})$

CLASIFICACIÓN DE GRUPOS

* **Teorema** (Cauchy): $|G| = p \Rightarrow \exists\, H \leq G : |H| = p$.

Defn: Llamamos normalizador de $H \leq G$ a $N_G(H) := \{g \in G : gHg^{-1} = H\}$.

Lema: $(G/H)^H = N_G(H)/H$.

Defn: Sea $|G| = p^n \cdot m$, $n>0$, p primo y $\text{mcd}(p,m) = 1$. Se llaman **p-subgrupos de Sylow** a los subgrupos de orden p^n.

* **Teorema** (Primer Teorema de Sylow): $|G| = p^n \cdot m \Rightarrow \exists H \leq G : |H| = p^n$ (p-subgrupo de Sylow)

* **Teorema** (Segundo Teorema de Sylow): $|G| = p^n \cdot m \Rightarrow$ todos los p-subgrupos de Sylow son conjugados entre sí.

Corolario: H p-subgrupo de Sylow es normal $\iff$ es el único p-subgrupo de Sylow en G.

Teorema (Tercer Teorema de Sylow): $|G| = p^n s m$, y r es el nº de p-subgrupos de Sylow, entonces r divide a m y $r \equiv 1 \pmod p$.

Definición: Se llama **grupo diédrico** D_n a las isometrías del plano que dejan invariante el polígono regular de n lados.

Propos: $D_n = \langle \underset{"g"}{\text{giro de } \tfrac{2\pi}{n}}, \underset{"\tau"}{\text{simetría}} \rangle$.

- $D_n = \langle g \rangle \rtimes \langle \tau \rangle = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. $\Rightarrow |D_n| = 2n$.
- $D_n \hookrightarrow S_n$, $g = (12\ldots n)$; $\tau(i) = n-i$.

GRUPOS RESOLUBLES

Defin: Una **serie normal** de subgrupos de G es una cadena $1 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_r = G$ donde G_i es normal en G_{i+1}. A cada G_{i+1}/G_i se le llama **factor**.

Defn: Un gpo G es resoluble si existe una serie normal de factores de orden primo.

- S_2, S_3 y S_4 son resolubles.

Propos: Sea $f: G \to G'$ un mfmo de gpos, $H \leq G$, $H' \leq G'$ normales. Entonces $f^{-1}(H')$ es un subgpo normal, y si f epiyectiva, $f(H)$ también.

Teorema Sea G gpo y $H \leq G$ normal.

$$G \text{ resoluble} \iff H,\ G/H \text{ resolubles}$$

Corolario: Todo subgpo de un gpo resoluble es resoluble.

Corolario: G_1, G_2 resolubles $\iff G_1 \times G_2$ resoluble. , y en general

$G_1, \dots, G_n$ resolubles $\iff G_1 \times \dots \times G_n$ resolubles.

Propos:

1) G abeliano $\Rightarrow$ G resoluble

2) $|G| = p^n$ $\Rightarrow$ G resoluble

Lema I: $A_n \subset S_n$ está generado por los tres ciclos.

Lema II: Sea A_n un A_n-conjugado por conjugación. Para $n \geq 5$ se tiene

$$A_n \cap (123) = \{\text{tres-ciclos}\}.$$

Lema III: Sea G grupo abeliano, y $f: A_n \to G$ un morfismo de grupos ($n \geq 5$) $\Rightarrow f(\sigma) = 1 \; \forall \sigma$.

Lema IV: No existe ningún subgrupo $H \subseteq A_n$ normal tal que $|A_n/H| = p$ (hip A_n no resoluble)

Teorema: S_n no es resoluble ($n \geq 5$)

Corolario: El único subgrupo normal propio de S_n es A_n, y éste no contiene ningún subgrupo normal propio.

II : PRODUCTO TENSORIAL

REPASO

- $(A, +, \cdot)$ anillo $\Leftrightarrow$ i) $(A,+)$ grupo abeliano; ii) $\cdot$ asociativa; iii) $\cdot$ distributiva respecto de $+$

- En adelante A será un anillo conmutativo con unidad, ie, $a \cdot b = b \cdot a$ y $1 \in A$.
- $a \in A$ divisor de cero si $\exists b \neq 0 : a \cdot b = 0$; y A íntegro o dominio si no tiene divisores de cero $\neq 0$.
- $a \in A$ propio si no es ni nulo ni invertible, y $a \in A$ irreducible si no se puede poner como producto de propios.

- $(M, +, \cdot)$ A-módulo $\Leftrightarrow$ i) $(M,+)$ grupo abeliano; ii) "$+$" y "$\cdot$" son distrib. y asoc. con los elts del anillo A
- $\prod_{i \in I} M_i = M_1 \times M_2 \times \dots$ es el producto directo de A-módulos.
- $\bigoplus_{i \in I} M_i \subseteq \prod_{i \in I} M_i$ es el submódulo de elts con todas las componentes nulas salvo finitas.
- $M_1 \times \dots \times M_r = M_1 \oplus \dots \oplus M_r$ $(r < \infty)$.
- M finito generado si $M = \langle u_1, \dots, u_r \rangle$, y libre cuando admite base. (que sean L.I. y generen, ie, $M = A \oplus \dots \oplus A$). Se llama rango al nº de elts de la base.

PRODUCTO TENSORIAL

• Sean M, N A-módulos y consideremos un nuevo A-módulo $M \square N := \bigoplus^{M\times N} A$, libre.

Existen $\{m_i \square n_j\}_{\substack{m_i \in M \\ n_j \in N}}$ es base, ie, $m_i \square n_j = (0, \dots, 1, \dots 0, \dots)$. Consideremos

$$R := \left\langle \begin{array}{l} (m+m') \square n - m \square n - m' \square n \\ m \square (n+n') - m \square n - m \square n' \\ (am) \square n - a\,(m \square n) \\ m \square (an) - a\,(m \square n \end{array} \right\rangle \quad \begin{array}{l} m, m' \in M \\ n, n' \in M \\ a \in A. \end{array}$$

Definición: Llamaremos **producto tensorial** de M y N sobre el anillo A a

$$M \otimes_A N := M \square N / R$$

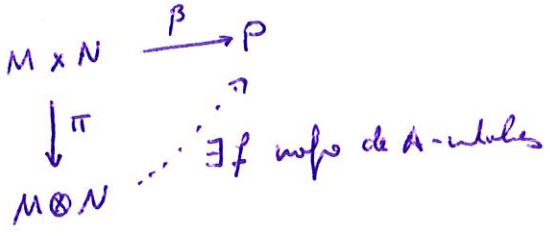
y de forma natural, por definición, se cumple que

$$\begin{cases} (m+m') \otimes n = m \otimes n + m' \otimes n \\ m \otimes (n+n') = m \otimes n + m \otimes n' \\ (am) \otimes n = a\,(m \otimes n) \\ m \otimes an = a\,(m \otimes n) \end{cases}$$

Teorema (Propiedad Universal del Producto Tensorial): Sea $\beta : M \times N \to P$ bilineal.

Entonces existe un único mapa de A-módulos

$f : M \otimes_A N \to P$ tal que $\beta = f \circ \pi$.



En particular se cumple

$$\mathrm{Hom}(M \otimes_A N, P) \xrightarrow{\quad\quad} \mathrm{Bil}_A(M, N; P)$$

• Este teorema dice que para definir un mapa de A-módulos $M \otimes_A N \to P$, basta con que sea **bilineal**!!

Teorema:

1) $A \otimes_A M = M$

2) $(A/I) \otimes_A M = M/IM$ (I ideal, $IM = \{\sum_{\text{finita}} i_j m_j\}$)

3) (DISTRIBUTIVA): $(M_1 \oplus M_2) \otimes_A N = (M_1 \otimes_A N) \oplus_A (M_2 \otimes N)$,

y en general $\left(\bigoplus M_i\right) \otimes_A N = \bigoplus (M_i \otimes_A N)$.

4) (CONMUTATIVA): $M \otimes_A N = N \otimes_A M$

5) (ASOCIATIVA): $(M \otimes_A N) \otimes_A P = M \otimes_A (N \otimes_A P) = M \otimes_A N \otimes_A P$

6) $\dfrac{M/N}{N'} = M/_{N+N'}$

7) $\left(\bigoplus^n A\right) \otimes_A \left(\bigoplus^m A\right) = \bigoplus^{n \cdot m} A$ $\left(A^n \otimes A^m = A^{n \cdot m}\right)$

- Los elementos de $M \otimes_A N$ no son de la forma $m \otimes n$, sino $\sum m_i \otimes n_j$.

Pero si los $\{m_i\}$ generan M, y los $\{n_j\}$ N, entonces $\{m_i \otimes n_j\}$ generan $M \otimes_A N$

y basta ver a donde van los de este tipo.

Proposición: $\mathrm{Hom}_A(M \otimes_A N, P) = \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$

NOTA: Por la bilinealidad de $\otimes$, se tiene que, si $M = \langle m_i \rangle_{i \in I}$, y $N = \langle n_j \rangle_{j \in J}$, entonces $M \otimes_A N = \langle m_i \otimes n_j \rangle_{\substack{i \in I \\ j \in J}}$

ÁLGEBRAS

Definición: Sean A, B dos anillos. Se dice que B es una **A-álgebra** si hay un morfismo de anillos $f: A \to B$, $a \longmapsto f(a) \overset{\text{NOT}}{=} a$.

- $\mathbb{R}$ es una $\mathbb{Q}$-álgebra. Todo anillo es una $\mathbb{Z}$-álgebra, $\mathbb{Q}[x]$ es una $\mathbb{Q}$-álgebra.

Definición: Sean B, C A-álgebras. Se dice que $f: B \to C$ es un **morfismo de A-álgebras** si es un morfismo de anillos y $f(a) = a$.

- Toda A-álgebra es un A-módulo, luego puedes hacer $B \otimes_A C$ (como A-módulos). Pues resulta que el A-módulo $B \otimes_A C$ es una A-álgebra.

Moraleja: El producto tensorial de A-álgebras (como A-mods) es A-álgebras.

Teorema: $\operatorname{Hom}_{A\text{-alg}}(B \otimes_A C, D) = \operatorname{Hom}_{A\text{-alg}}(B, D) \times \operatorname{Hom}_{A\text{-alg}}(C, D)$.

CAMBIO DE ANILLO BASE

- Sea B una A-álgebra y M un A-módulo. Quiero obtener un B-módulo. ¿Cómo?

Definición: Se llama **módulo obtenido por el cambio de anillo base** de A a B al B-módulo $M \otimes_A B$.

- $\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}^n$

Propiedades:

1) $(M \otimes_A N) \otimes_A B \cong (M \otimes_A B) \otimes_B (N \otimes_A B)$.

2) $(M \otimes_A B) \otimes_B C \cong M \otimes_A C$

Propiedad: $\mathrm{Hom}_{A\text{-alg}}(B, C) \cong \mathrm{Hom}_{C\text{-alg}}(B \otimes_A C, C)$

- $\mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[x]$
- $\mathbb{Q}[x]/(p(x)) \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}[x]/(p(x))$.
- $\mathbb{C}[x]/(x-\alpha) \cong \mathbb{C}$.

LOCALIZACIÓN DE ANILLOS

Definición: Sea A un anillo. Se dice que $S \subset A$ es un sistema multiplicativo si

i) $1 \in S$
ii) $s \cdot s' \in S \quad \forall s, s' \in S$.

Definición: Sea A un anillo y S un sistema multiplicativo. Se llama localización de A por S, y se denota como A_S, a

$$A_S := \left\{ \frac{a}{s} : a \in A, s \in S : \frac{a}{s} = \frac{a'}{s'} \iff \exists t, t' \in S : \underbrace{\begin{matrix} at = a't' \\ st = s't' \end{matrix}} \right\}$$

$$\begin{cases} at = a't' \\ st = s't' \end{cases}$$

¡OJO!: $\frac{a}{s}$ es notación. No es as^{-1}.

- Podemos definir la suma $\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'}$ y el producto $\frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$, y está bien definido: no depende de los rep. elegidos.

- Además tiene neutro para la suma: $\frac{0}{1}$, y para el producto: $\frac{1}{1}$.

Lema. $\frac{a}{s} = \frac{0}{1} \iff \exists t \in S : t \cdot a = 0$

$\iff a = 0$.

(A íntegro, $0 \notin S$)

Proposición. $\frac{a}{s} = \frac{a'}{s'} \iff \exists t \in S : t(as' - a's) = 0$

$\iff as' = a's$.

(A íntegro, $0 \notin S$)

- $\frac{a}{s} = \frac{a \cdot t}{s \cdot t}$.

Proposición. $A_S = \{0\} \iff 0 \in S$

- $Q := \mathbb{Z}_{\mathbb{Z} \setminus \{0\}}$; $Q(X) := Q[X]_{Q[X] \setminus \{0\}} = \mathbb{Z}[X]_{\mathbb{Z}[X] \setminus \{0\}}$; $K(X_1, \dots, X_n) := K[X_1 \dots X_n]_{K[X_1 \dots X_n] \setminus \{0\}}$

Definición. Llamo morfismo de localización a $A \longrightarrow A_S$, $a \longmapsto \frac{a}{1}$

Propos. $\mathrm{Hom}(A_S, B) = \{ f \in \mathrm{Hom}(A, B) : f(s) \in B \text{ invertible } \forall s \in S \}$

Proposición: $(A_S)_{S'} = A_{S \cdot S'}$

ESPECTRO PRIMO

Definición: Un ideal es un subconjunto $I \subseteq A$: $a \cdot i \in I \ \forall a \in A, i \in I$.

Definición: Se dice que un ideal $\mathfrak{p} \subsetneq A$ es primo si $a \cdot b \in \mathfrak{p} \Rightarrow a$ ó $b \in \mathfrak{p}$.

Se dice que $\mathfrak{m} \subsetneq A$ es un ideal maximal cuando el único ideal que lo contiene es A.

Se llama espectro de A, $\operatorname{Spec} A = \{$ ideales primos de $A \}$.

Teorema: Sea A anillo y I un ideal

1) I primo $\Leftrightarrow$ A/I íntegro

2) I maximal $\Leftrightarrow$ A/I cuerpo.

Corolario: $\operatorname{Spec}_{max} A \subseteq \operatorname{Spec} A$, ie, maximal $\Rightarrow$ primo.

Definición: Un ideal se dice principal si $I = (a)$; y un anillo se dice que es un dominio de ideales principales (DIP) si todo ideal es principal.

- Se dice que $x \in \operatorname{Spec} A$, es decir, $\mathfrak{p}_x \in \operatorname{Spec}$.

Definición: Sea $I \subseteq A$ ideal. Llamemos ceros de I a

$$(I)_0 := \{ x \in \operatorname{Spec} : I \subset \mathfrak{p}_x \}.$$

- $\operatorname{Spec} K(x) = \{ (0), (p(x)) \}_{p(x) \text{ irreducible en } k(x)}$.
- Todo anillo $\neq 0$ contiene algún ideal maximal
- Todo ideal $\neq A$ está contenido en algún ideal maximal.

Proposición:

1) $(I)_0 = \emptyset \iff I = A$

2) $(I_1 + I_2)_0 = (I_1)_0 \cap (I_2)_0$

3) $(I_1 \cdot I_2)_0 = (I_1)_0 \cup (I_2)_0$

Lema: La antiimagen de un ideal (primo) es un ideal (primo).

- Este lema motiva la siguiente definición:

Definición: Sea $f: A \to B$ un morfismo de anillos. Existe un morfismo de forma natural

$$\begin{array}{ccc} \operatorname{Spec} B & \xrightarrow{f^*} & \operatorname{Spec} A \\ \mathfrak{P} & \longmapsto & f^{-1}(\mathfrak{P}). \end{array}$$

Teorema: Sea $I \subset A$ un ideal (no necesariamente primo) y consideremos el paso al cociente: $\pi: A \to A/I$.

$$\begin{array}{ccc} \operatorname{Spec}(A/I) & \xrightarrow{\pi^*} & (I)_0 \\ \overline{\mathfrak{P}} & \longmapsto & \mathfrak{P} \end{array}$$

Teorema: Sea A anillo y $S \subset A$ un sistema multiplicativo, y consideremos el localizado A_S, y el morfismo de localización $A \xrightarrow{i} A_S$.

$$\operatorname{Spec}(A_S) \xrightarrow{i^*} \{ x \in \operatorname{Spec} A : \mathfrak{P}_x \cap S = \emptyset \}.$$

Definición: Llamamos **radical** de un anillo A a

$$\operatorname{rad} A := \{ a \in A : \exists\, n > 0 : a^n = 0 \}$$

Se dice que esos $a \in A$ son **nilpotentes**.

- $\operatorname{rad} A$ es un ideal

Teorema: $\operatorname{rad} A = \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$.

Definición: Se dice que un anillo A es **reducido** si $\operatorname{rad} A = 0$.

- $(p_1^{n_1}(x) \cdots p_r^{n_r}(x))_0 = \{ (p_1(x)), \ldots (p_r(x)) \}$

- $\operatorname{Spec} \frac{k(x)}{(p_1^{n_1}(x) \cdots p_r^{n_r}(x))} = \{ (\overline{p_1(x)}), \ldots (\overline{p_r(x)}) \}$.

- $\operatorname{rad} \frac{A}{(p_1^{n_1} \cdots p_r^{n_r})} = (p_1 \cdots p_r)$, p_i irreducible (primo en A pol. irred. en $k(x)$)

III: EXTENSIONES FINITAS DE CUERPOS

POLINOMIOS

Definición: Se dice que $\alpha \in K$ es **raíz** de $p(x) \in K[x]$ si $p(\alpha) = 0$.

Lema: α es raíz de $p(x) \iff p(x) = \dot{} \; x - \alpha$

Proposición: Si $\frac{n}{m} \in \mathbb{Q}$ es raíz de $p(x) = a_0 x^n + \dots + a_n$, entonces n divide a a_n y m divide a a_0.

- Este resultado dice que para encontrar las raíces racionales de un polinomio solo hay que buscar entre los de la forma $\frac{n}{m}$ con n en $\mathbb{Z}$.

Lema: n° raíces de $p(x) \in K[x] \leq gr\, p(x)$.

Teorema (Fórmula de interpolación de Lagrange): Dados $a_0, \dots, a_n$ distintos y $b_0, \dots b_n \in K$, $\exists\, p(x)$, $gr\, p(x) \leq n$, tal que $p(a_i) = b_i$, y en particular,

$$p(x) = \sum_{i=0}^{n} b_i \frac{(x-a_0)\cdots\widehat{(x-a_i)}\cdots(x-a_n)}{(a_i-a_0)\cdots\widehat{(a_i-a_i)}\cdots(a_i-a_n)}$$

Definición: Un polinomio $p(x) \in A[x]$ se dice **primitivo** cuando no existe ningún elemento propio que divida a todos sus coeficientes.

Lema (Gauss): Sea $p(x) \in \mathbb{Z}[x]$ primitivo.

$$p(x) \text{ irreducible en } \mathbb{Z}[x] \iff p(x) \text{ irreducible en } \mathbb{Q}[x].$$

Teorema (Criterio de Eisenstein): Sea $p(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$. Si $\exists p$ primo tal que

1) p no divide a a_0
2) p divide a $a_1, \dots, a_n$
3) p^2 no divide a a_n

$\Rightarrow p(x)$ es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$.

Teorema (Criterio de Nietsnerie): Sea $p(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$. Si $\exists p$ primo tal que

1) p no divide a a_n
2) p divide a $a_0, \dots, a_{n-1}$
3) p^2 no divide a a_0

$\Rightarrow p(x)$ es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$.

Definición: Un **dominio de factorización única** (DFU) es un anillo íntegro en el que todo elemento puede escribirse como producto de irreducibles de modo único salvo orden e invertibles.

Proposición: DIP $\Rightarrow$ DFU.

- $\mathbb{Z}$, $K[x]$ son DFU.

Lema (Euclides): Sea A DIP. Entonces son equivalentes:

1) $a \in A$ irreducible
2) (a) ideal primo
3) (a) ideal maximal

es decir, $\operatorname{Spec} A = \operatorname{Spec}_{max} A = \{(a)\}_{a \text{ irreducible}}$.

Corolario: Sea A DFU. Entonces

$$a \in A \text{ irreducible} \iff (a) \text{ ideal primo}$$

es decir, $\operatorname{Spec} A = \{(a)\}_{a \text{ irreducible}}$.

Lema (Gauss DFU): Sea A DFU y $\Sigma := A_{A\setminus\{0\}}$ su cuerpo de fracciones, y sea $p(x) \in A[x]$ primitivo.

$$p(x) \text{ irreducible en } A[x] \iff p(x) \text{ irreducible en } \Sigma[x].$$

Teorema (Criterio de Eisenstein): Igual pero con $p \in A$ irreducible, en A DFU.

Teorema (Gauss): A DFU $\Rightarrow A[x]$ DFU.

Corolario: $\mathbb{Z}[x_1,\dots,x_n]$ y $K[x_1,\dots,x_n]$ son DFU.

EXTENSIONES DE CUERPOS

Definición: Una *extensión de cuerpos* es un morfismo $K \hookrightarrow L$ (necesariamente injectivo). Se dice que L es una *K-extensión de cuerpos*. Se dice que la extensión es *finita* si $\dim_K L < \infty$ (como K-EV), ie, si $L = K \times \dots \times K$. A este número se le llama *grado* de L sobre K, y se denota como $[L:K]$.

* **Proposición**: $\dim_K \dfrac{K[x]}{(p(x))} = \operatorname{gr} p(x)$, como K-álgebra (K-EV). K-ext. de cpo

Definición: Denotemos como $K[\alpha_1,\dots,\alpha_n]$, $\alpha_1,\dots,\alpha_n \in L$, $K \hookrightarrow L$ extensión de cuerpos, al mínimo subanillo de L que contiene a K y a $\alpha_1,\dots,\alpha_n$. Explícitamente,

$$K[\alpha_1,\dots,\alpha_n] = \left\{ p(\alpha_1,\dots,\alpha_n) \;\middle|\; p(x_1,\dots,x_n) \in K[x_1,\dots,x_n] \right\}.$$

Además, denotemos con $k(\alpha_1,\dots,\alpha_n)$ al mínimo subcuerpo de K que contiene a k y a $\alpha_1,\dots,\alpha_n$:

$$k(\alpha_1,\dots,\alpha_n) = \left\{ \frac{p(\alpha_1,\dots,\alpha_n)}{q(\alpha_1,\dots,\alpha_n)} \right\}_{\substack{p(x_1,\dots,x_n),\, q(x_1,\dots,x_n) \in k[x_1,\dots,x_n] \\ q(\alpha_1,\dots,\alpha_n) \neq 0.}}$$

Definición: Sea $k \hookrightarrow K$. Diremos que $\alpha \in K$ es **k-algebraico** si existe $p(x) \in k[x]$ tal que $p(\alpha) = 0$. Si $\alpha \in K$ no es algebraico se dice **transcendente**.

*

Teorema: Sea $k \hookrightarrow K$, y $\alpha \in K$ k-algebraico, y sea $p(x)$ el polinomio mónico mínimo que anula a α. Entonces

$$k(\alpha) = k[\alpha] \cong \frac{k[x]}{(p(x))}.$$

X

Proposición: $k \hookrightarrow k(\alpha)$ es una ext. finita de cps $\iff$ $\alpha \in K$ algebraico sobre k.

*

Proposición: La composición de extensiones finitas de cps es una extensión finita de cps. En partic, si $k \hookrightarrow K$ es de grado n, $K \hookrightarrow \Sigma$ de grado m $\Rightarrow k \hookrightarrow \Sigma$ de grado $n \cdot m$.

Definición: Se dice que una extensión de cps $k \hookrightarrow K$ es **algebraica** si todo elemento de K es k-algebraico.

Proposición: Sea $k \hookrightarrow K$ una extensión de cpos.

1) * finita $\Rightarrow$ algebraica

2) $\alpha_1, \dots \alpha_n \in K$ k-algebraicos, $k \hookrightarrow k(\alpha_1 \dots \alpha_n)$ es finita, hgo algebraica

3) $k \hookrightarrow K$ ext. finita $\iff \exists\, \alpha_1, \dots \alpha_n \in K$ k-algebraicos tal que $K = k(\alpha_1, \dots \alpha_n)$.

Proposición: La composición de extensiones algebraicas es algebraica.

Proposición *: Sean $k \hookrightarrow K$, $k \hookrightarrow K'$ ext. de cpos. Entonces existe una k-extensión de cpos L tal que hay extensiones $K \hookrightarrow L$ y $K' \hookrightarrow L$. En particular, $L = K \otimes_k K' / m$, y si $\dim_k K = n$, $\dim_k K' = m$, n y m primos entre sí, $\Rightarrow K \otimes_k K' = K \otimes_k K' / m$ y es una k-extensión finita.

Teorema (Kronecker): Sea $p(x) \in k[x]$. Existe una extensión finita de cuerpos $k \hookrightarrow K$ en la que $p(x)$ descompone en factores mnls, ie, existen $\alpha_1, \dots \alpha_n \in K$ tal que $p(x) = a_0 (x - \alpha_1) \cdots (x - \alpha_n)$. Si K' es otra k-extensión finita con $p(x) = a_0 (x - \beta_1) \cdots (x - \beta_n)$ entera en toda extensión L que contenga a K y K' se tiene que $\{\alpha_1 \dots \alpha_n\} = \{\beta_1, \dots \beta_n\}$. Se dice que $\alpha_1, \dots \alpha_n$ son las raíces de $p(x)$.

- En otras palabras: dado un polinomio $p(x) \in k[x]$, hay una cuerpo "gordo" que tiene a todas las raíces de $p(x)$.

Definición: Un cuerpo K se dice **algebraicamente cerrado** si todo polinio $p(x) \in K[x]$ tiene todas sus raíces en K. Es decir, si K no admite extensiones finitas de cuerpos.

Teorema: Dado un cuerpo K, existe una única extensión de cuerpos $K \hookrightarrow \bar{K}$ única salvo isomorfismo K-algebraica y algebraicamente cerrado. A dicha extensión $\bar{K}$ se le llama **cierre algebraico** de K.

FUNCIONES SIMÉTRICAS

Teorema (Fórmulas de Cardano): Sea $p(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$, y $\alpha_1, \dots \alpha_n$ sus raíces. Etc.

$$
\left.
\begin{aligned}
a_0 &= c \\
a_1 &= c \cdot (-1) \cdot \sum_{i=1}^{n} \alpha_i \\
a_2 &= c \cdot (-1)^2 \cdot \sum_{i<j} \alpha_i \alpha_j \\
&\vdots \\
a_i &= c\,(-1)^i \sum_{j_1 < \dots < j_i} \alpha_{j_1} \cdots \alpha_{j_i} \\
&\vdots \\
a_n &= c\,(-1)^n\, \alpha_1 \cdots \alpha_n
\end{aligned}
\right\} \text{FÓRMULAS DE CARDANO}
$$

Definición: Dadas $x_1 \dots x_n$ variables, se llaman **funciones simétricas elementales** en las letras $x_1 \dots x_n$ a

$$S_i := \sum_{j_1 < \dots < j_i} x_{j_1} \cdots x_{j_i} .$$

• Estos los fórmulas de Cardano se pueden expresar como

$$a_i = \mathbb{C} \cdot (-1)^i \cdot S_i$$

donde S_i son los f.s.e. expresados en las letras $x_1, \dots, x_n$.

• $k[x_1, \dots, x_n]$ es un S_n-conjunto con la acción $\sigma * p(x_1 \dots x_n) := p(x_{\sigma(1)}, \dots x_{\sigma(n)})$

Definición: Diremos que $p(x_1 \dots x_n) \in k[x_1 \dots x_n]$ es simétrico si $\sigma * p(x_1 \dots x_n) = p(x_1 \dots x_n)$, y denotaremos con $k[x_1 \dots x_n]^{S_n}$ al conjunto de pol. simétricos.

Teorema (de las Funciones Simétricas):

$$k[x_1, \dots, x_n]^{S_n} = k[S_1, \dots, S_n]$$

• Este Th dice que todo pol simétrico puede escribirse en términos de los f.s.e. en las letras $x_1 \dots x_n$.

Teorema (Fundamental del Álgebra): Todo polinomio $p(x) \in \mathbb{C}[x]$ tiene todas sus raíces en $\mathbb{C}$, ie, $\mathbb{C}$ es un cuerpo algebraicamente cerrado

Definición: Llamemos anillo de series formales a

$$k[[x]] := \left\{ \sum_{i=1}^{\infty} a_i x^i : a_i \in k \right\}$$

• $k[[x]]$ es un anillo con la suma y producto usuales de series, y $k((x)) := k[[x]]_{k[[x]] \setminus \{0\}}$.

Teorema: Sea $p(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$, y $p'(x)$ su derivada, y sean $\alpha_1, \dots \alpha_n$ las raíces de $p(x)$ y denotemos $\sigma_i = \alpha_1^i + \dots + \alpha_n^i$. Entonces

1) $$\frac{p(x)}{p'(x)} = \frac{1}{x-\alpha_1} + \dots + \frac{1}{x-\alpha_n}$$

2) **Fórmula de Girard**: $$\frac{p(x)}{p'(x)} = \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \dots + \frac{\sigma_i}{x^{i+1}} + \dots \in k((\tfrac{1}{x})).$$

3) **Fórmulas de Newton**:

$$0 = a_0 \sigma_1 + a_1$$
$$\vdots$$
$$0 = a_0 \sigma_i + \dots + a_{i-1} \sigma_1 + a_i \, i$$
$$\vdots$$
$$0 = a_0 \sigma_{n-1} + \dots + a_{n-2} \sigma_1 + a_{n-1} (n-1)$$

Definición: Sea $p(x) \in k[x] \subset K[x]$, $p(x) = a_0 (x-\alpha_1) \cdots (x-\alpha_n)$. Se llama discriminante de $p(x)$ a

$$\Delta(p(x)) := \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

- Notese que $\Delta(p(x))$ es un pol. simétrico, y que $p(x)$ tiene raíces múltiples $\Leftrightarrow$ $\Leftrightarrow \Delta(p(x)) = 0$.

Teorema: Sea $p(x) = x^n + a_1 x^{n-1} + \dots + a_n$. Entonces

$$\Delta(p(x)) = \begin{vmatrix} \sigma_0 & \sigma_1 & \cdots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & & \vdots \\ \vdots & & & \vdots \\ \sigma_{n-1} & \cdots & \cdots & \sigma_{2n-2} \end{vmatrix}.$$

• Nota que los σ_i se pueden sobre de la fórmula de Girard: como $\frac{P(x)}{P'(x)} = \sum_{i=1}^{\infty} \frac{\sigma_i}{x^{i+1}}$,

estas al hacer $\frac{P(x)}{P'(x)}$ $\Big|\; \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \dots$ salen los σ_i !!

k-ÁLGEBRAS FINITAS

Definición: Sea $k \hookrightarrow A$ una k-álgebra. Se dice que A es una **k-álgebra finita** si $\dim_k A < \infty$.

• Toda k-álg. es un k-módulo $\Rightarrow$ k-EV, por tiene sentido hablar de $\dim_k A$.

• $\frac{k[x]}{(p(x))}$ es una k-álg. finita (de dim grado $p(x)$)

Teorema: Sea $A = A_1 \times \dots \times A_n$ un producto cartesiano de anillos.

1) Los ideales de A son productos cartesianos de ideales de cada factor:

$$\{\text{ideales de } (A_1 \times \dots \times A_n)\} = \{ I_1 \times \dots \times I_n \;/\; I_i \text{ ideal de } A_i \}.$$

2) Los ideales primos de A son productos de los factores, con un ideal primo de un factor anulado:

$$\operatorname{Spec}(A_1 \times \dots \times A_n) = \{ A_1 \times \dots \times \mathfrak{p}_i \times \dots \times A_n \;/\; \mathfrak{p}_i \in \operatorname{Spec} A_i,\ i = 1, \dots, n \}.$$

Lema: A k-álgebra finita íntegra $\Rightarrow$ A cuerpo.

Teorema ✱: En toda k-álgebra finita A se tiene que

1) $\operatorname{Spec} A = \operatorname{Spec}_{\max} A$

2) $\#\operatorname{Spec} A \leq \dim_k A$.

Defn: Un anillo se dice **local** cuando solo tenga un ideal maximal.

Teorema: Todo k-alg. finita decompone en producto cartesiano $A = A_1 \times \dots \times A_n$ de k-alg. finitas locales.

Propos: Sea $p(x) = p_1^{n_1}(x) \cdots p_r^{n_r}(x)$, $p_i(x)$ irreducibles.

$$\frac{k[x]}{(p(x))} \text{ reducida} \iff n_1 = \dots = n_r = 1.$$

$$\text{local} \iff p(x) = p_i(x)^{n_i},\ p_i \text{ irredc.}$$

TEOREMA DE KRONECKER PARA ÁLGEBRAS

Definición: Dada un k-álgebra A, se dice que $x \in \operatorname{Spec} A$ es un punto **racional** si $A/\mathcal{P}_x = k$. Se dice que la k-álgebra A es **racional** cuando todos sus ideales sean racionales.

Propos: $\frac{k[x]}{(p(x))}$ racional $\iff$ $p(x)$ tiene todas sus raíces en k.

Propos: Sea $k \hookrightarrow K$ una extensión de cps

A k-álgebra finita local k-racional $\Longrightarrow A \otimes_k K$ K-álgebra finita local K-racional

Lema: A k-alg. finita k-racional $\Longrightarrow A \otimes_k K$ K-álgebra finita K-racional

Teorema (de Kronecker para k-álgebras finitas): Sea A una k-alg. finita. Existe una extensión finita de cuerpos $k \hookrightarrow K$ tal que $A \otimes_k K$ es una K-álgebra finita K-racional.

IV : TEORÍA DE GALOIS

Definición: Una k-alg. finita A se dice <u>trivial</u> si $A = k \times \dots \times k$.

Proposición: $\frac{k[x]}{(p(x))}$ k-alg. fin. trivial $\iff$ todas las raíces están en k y tiene multp. 1.

Proposición ✱: Sea A una k-álgebra finita.

$$\text{trivial} = \text{reducida} + \text{racional}$$

Teorema: Sea A una k-alg. trivial, $D \subset A$ subálgebra y $I \subset A$ ideal y B una k-álgebra trivial.

1) A/I trivial
2) D trivial
3) $A \otimes_k B$ trivial
4) $A \times B$ trivial

Proposición ✱✱: $\mathrm{Hom}_{k\text{-alg}}(A, k) \longrightarrow \{$ puntos racionales de $A\}$

Corolario ✱✱: A racional $\iff \#\mathrm{Hom}_{k\text{-alg}}(A, k) = \#\operatorname{Spec} A$.

Teorema: Sea A k-alg. finita. $\#$

1) A trivial $\iff \#\,\mathrm{Hom}_{k\text{-alg}}(A,k) = \dim_k A$

2) A trivial $\iff \#\,\mathrm{Spec}\ A = \dim_k A$.

k-ALG FINITAS SEPARABLES

Definición: Una k-álgebra finita A se dice **separable** si existe una ext. de cuerpos $k \hookrightarrow K$ tal que $A \otimes_k K$ sea trivial. Se dice que K **trivializa** a A.

Proposición: $\dfrac{k[x]}{(p(x))}$ k-alg. finita separable $\iff$ todas las raíces son de multiplicidad 1.

Proposición: Sea $k \hookrightarrow K$, y A k-alg. finita. Si K trivializa a A, cualquier extensión de cuerpos más grande también trivializa.

Teorema: Sea A una k-alg finita separable, $\mathbb{D}$ subálgebra, y B otra k-alg separable.

1) $A/\mathbb{D}$ separable

2) $\mathbb{D}$ separable

3) $A \otimes_k B$ separable

4) $A \times B$ separable.

Teorema (Fórmula de los puntos): Sea A k-alg y $k \hookrightarrow K$ ext. de cuerpos.

$$\#\mathrm{Hom}_{k\text{-alg}}(A, K) \leq \dim_k A \ , \ \forall$$

$$\#\mathrm{Hom}_{k\text{-alg}}(A, K) = \dim_k A \iff K \text{ trivializa a } A.$$

Lema: Supongo que K trivializa a A, y sea $\mathrm{Hom}_{k\text{-alg}}(A, K) = \{g_1, \dots, g_n\}$. Esto el isomfismo exacto es

$$A \otimes_k K \xrightarrow{\ =\ } K \times \dots \times K$$

$$a \otimes \lambda \longmapsto (g_1(a)\cdot\lambda, \dots, g_n(a)\cdot\lambda)$$

Proposición: Sea $\#k = \infty$, y A k-alg. finit. A separable $\Rightarrow \exists\, a \in A : A = k[a]$.

Definición: Sea A una k-alg. finita. Se dice que $a \in A$ es separable si $k[a]$ es separable, ie, si el pol. min. anulador de a tiene todas sus raíces de multiplicidad 1.

Teorema: A separable $\iff$ $a \in A$ separable $\forall a \in A$.

Teorema: A separable $\iff$ $A \otimes_k K$ reducida $\forall\, k \hookrightarrow K$ (universalmente reducida)

Teorema: A separable (sobre k) $\iff$ $A \otimes_k K$ separable (sobre K).

Propos: A separable (sobre k) $\iff$ $A \otimes_k K$ separable (sobre K).

Corolario: A separable $\Rightarrow$ A reducida.

Definición: Sea A un anillo. Se llama **característica** de A, $\operatorname{char} A$, al mínimo natural $n>0$ tal que $1+\overset{n}{\dots}+1=0$. Si $1+\overset{(n)}{\dots}+1\neq 0$ $\forall n$, se dice que $\operatorname{char} A=0$.

- Sea $\mathbb{Z}\xrightarrow{\varphi} A$, $1\longmapsto 1$, $1+1\longmapsto 1+1$, $\dots$. Entonces $\ker\varphi=(\operatorname{char} A)$.
- Sea $A=k$, cuerpo. Entonces consideramos $\mathbb{Z}\xrightarrow{\varphi} k\hookleftarrow$, luego $\mathbb{Z}\to \mathbb{Z}/\ker\varphi=\mathbb{Z}/(\operatorname{char} k)$, (con $\operatorname{char} k\neq 0$)

$\mathbb{Z}/n\mathbb{Z}$ $(n=\operatorname{char} k)$ íntegro $\Leftrightarrow n=p$ primo. Luego tenemos $\mathbb{Z}/p\mathbb{Z}\hookrightarrow k$.

Proposición: Sea $\operatorname{char} k=0$, y A k-alg. finita.

$$A \text{ separable} \iff A \text{ reducida}.$$

Corolario: Si $\operatorname{char} k=0$, toda ext. finita de cuerpos es separable

- Trivial $\Rightarrow$ Separable $\Rightarrow$ Reducida

Teorema (Resumen para $k[x]/(p(x))$): Consideramos la k-alg. fin. $k[x]/(p(x))$.

1) $\dim k[x]/(p(x)) = \operatorname{gr} p(x)$, en particular una base es $\{\bar 1, \bar x, \dots, \overline{x^{n-1}}\}$.

2) $\operatorname{Spec}\left(k[x]/(p(x))\right)=\{(\overline{p_1(x)}),\dots,(\overline{p_r(x)})\}$, donde $p(x)=p_1^{n_1}(x)\cdots p_r^{n_r}(x)$.

3) $\operatorname{red}\left(k[x]/(p(x))\right)=(p_1(x)\cdots p_r(x))$, donde $p(x)=p_1^{n_1}(x)\cdots p_r^{n_r}(x)$.

4) $k[x]/(p(x))$ cuerpo $\iff$ $p(x)$ irreducible

5) $k[x]/(p(x))=k(\alpha)=k[\alpha]$ si $p(x)$ es el pol. mín. anulador de α k-algebraico.

6) $\frac{k[x]}{(p(x))}$ local $\iff$ $p(x)$ es una potencia de un irreducible

7) $\frac{k[x]}{(p(x))}$ reducido $\iff$ $p(x)$ es producto de irreducibles no repetidos.

8) $\frac{k[x]}{(p(x))}$ racional $\iff$ $p(x)$ tiene todas las raíces en k

9) $\frac{k[x]}{(p(x))}$ trivial $\iff$ $p(x)$ tiene todas las raíces en k y de multiplicidad 1.

10) $\frac{k[x]}{(p(x))}$ separable $\iff$ $p(x)$ tiene todas sus raíces de multiplicidad 1.

11) La mínima extensión que trivializa a $\frac{k[x]}{(p(x))}$ es $k(\alpha_1,\dots\alpha_n)$, donde α_i son las raíces de $p(x)$. En particular es una extensión de Galois. Si las raíces son distintas entre sí.

12) $\frac{k[x]}{(p(x))}$ Galois $\iff$ todas las raíces de $p(x)$ son de multipl. 1 y están $\frac{k[x]}{(p(x))} = k(\alpha)$, $p(x)$ polinomio de α.

EXTENSIONES DE GALOIS

Definición: Una extensión finita de cuerpos $k \hookrightarrow K$ se dice **de Galois** si se trivializa a sí misma, i.e., si $K \otimes_k K = K \times \dots \times K$. En este caso se define el **grupo de Galois de K** a $G := Aut_{k-alg}(K)$.

- Galois $\Rightarrow$ separable
- $\mathbb{Q}(\sqrt{2})$ es de Galois.

Teorema: Sea $k \hookrightarrow K$ una extensión finita de cuerpos.

K es de Galois $\iff$ $\#Aut_{k-alg}(K) = \dim_k K$.

Definición: Sea $p(x) \in k[x]$, de raíces $\alpha_1, \dots, \alpha_n$. Llamaremos **cuerpo de descomposición** de $p(x)$ a $k(\alpha_1, \dots, \alpha_n)$.

Proposición *: Si las raíces de $p(x)$ $\alpha_1, \dots \alpha_n$ son distintas (ie, $k[x]/(p(x))$ separable), entonces $k(\alpha_1, \dots \alpha_n)$ es clase extensión de Galois y en particular es la mínima extensión que trivializa a $k[x]/(p(x))$.

Definición: En este caso, se llama **grupo de Galois de $p(x)$** a $G := Aut_{k-alg}(k(\alpha_1, \dots \alpha_n))$.

- Notar que $G = Aut(k(\alpha_1, \dots \alpha_n)) \subseteq S_n$, ie, las automorfismos están determinados por cierta permutación de las raíces.

Teorema: Dada A una k-álgebra finita separable, existe la mínima extensión de cuerpo que trivializa a A, y es de Galois, la cual se denomina **envolvente de Galois** de A.

- Si $p(x) \in k[x]$ tiene todas las raíces distintas (de multiplic. 1), entonces la envolvente de Galois de $k[x]/(p(x))$ es $k(\alpha_1, \dots \alpha_n)$ ($\alpha_1, \dots \alpha_n$ raíces de $p(x)$).

Teorema *: Sea $k \hookrightarrow K$ separable. Son equivalentes:

1) $k \hookrightarrow K$ de Galois
2) Todo polinomio $p(x) \in k[x]$ irreducible que tiene una raíz en K tiene todas sus raíces en K.
3) (**Teorema del Agujero Único**): Existe una única inmersión de K en el cierre algebraico de k, salvo automorfismos de K.

Teorema: Sea $k \hookrightarrow K$ separable.

$k \hookrightarrow K$ de Galois $\iff$ K es el cuerpo de descomposición de un polinomio (en $k[x]$).

EXTENSIONES CICLOTÓMICAS

- $\mu_n = \{ e^{\frac{2\pi i}{n} k} \in \mathbb{C} : k = 0, \dots, n-1 \} \equiv$ raíces n-ésimas de la unidad. Los denotaremos como $\mathcal{E}$.

- $(\mu_n, \cdot) \leq (\mathbb{C}^*, \cdot)$, y es cíclico, pues $\mu_n = \langle e^{\frac{2\pi i}{n}} \rangle$. Luego $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Luego $\mu_n = \langle e^{\frac{2\pi i}{n} \cdot k} \rangle \iff k$ primo con n.

Definimos: Llamaremos raíces primitivas n-ésimas de la unidad a las que generan μ_n, y al conjunto de todas ellas lo denotaremos como R_n.

Definición: Llamaremos polinomio ciclotómico n-ésimo al polinomio mónico

$$\Phi_n(x) := \prod_{\mathcal{E} \in R_n} (x - \mathcal{E}) = \prod_{\substack{0 < k < n \\ k \text{ primo con } n}} \left(x - e^{\frac{2\pi i}{n} k} \right)$$

Lema: $\Phi_n(x) = \dfrac{x^n - 1}{\prod\limits_{\substack{d \mid n \\ d \neq n}} \Phi_d(x)}$, ($d \mid n \equiv d$ divide a n.), y

cada $\Phi_n(x) \in \mathbb{Z}[x]$.

V: APLICACIONES DE LA T^a DE GALOIS

RESOLUBILIDAD POR RADICALES

Teorema: Sea $k \hookrightarrow K$ de gr n, y supongas que k contiene las raíces n-ésimas de la unidad (finita).

$$K \text{ es de Galois de grupo cíclico} \iff \exists\, a \in k : K = k(\sqrt[n]{a})$$

- De la dem. se extrae que $a = R^n$ donde R verifica que $\sigma(R) = e^{\frac{2\pi i}{n}} R$ (ie, $\sigma(R^n) = R^n$),

donde $G = \langle \sigma \rangle$.

Teorema (de Independencia de Artin): Sea $k \hookrightarrow K$ de Galois de grupo $G = \{g_1, \dots, g_n\}$.

Entonces $g_1, \dots, g_n$ son K-L.I.

- Surge una pregunta inmediata: si se da el 1er TH, ¿cómo expresar $\alpha \in K$ en términos de k y $\sqrt[n]{a}$?

Definición: Dado $\alpha \in K$, $\varepsilon \in \mu_n$ y $G = \langle \sigma \rangle$, se llama resolvente de Lagrange de α por ε a

$$R(\alpha, \varepsilon) := \sum_{i=0}^{n-1} \sigma^i(\alpha)\, \varepsilon^i$$

- Dado $\alpha \in K$ y $\varepsilon \in \mu_n$ primitiva, se ve que $\sigma(R(\alpha,\varepsilon)) = \varepsilon^{-1} R(\alpha,\varepsilon)$; luego $\sigma(R^n(\alpha,\varepsilon)) = R^n(\alpha,\varepsilon)$, y para todo el grupo $\Rightarrow R^n(\alpha,\varepsilon) \in k$, luego $a = R^n(\alpha,\varepsilon)$.

Proposición: Sea $\alpha \in k$ y $\varepsilon \in$ una primitiva.

$$\alpha = \frac{1}{n} \sum_{j=0}^{n-1} R(\alpha, \varepsilon^j)$$

Definición: Sea $p(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in k(a_1, \dots, a_n)[x]$ ($a_1, \dots, a_n$ VARIABLES).
Se llama polinomio general de grado n a $p(x)$.

Lema: Las raíces del polinomio general de grado n son algebraicamente independientes, ie, no verifican ninguna relación algebraica, ie, $\forall f(x_1 \dots x_n) \neq 0$, $f(\alpha_1, \dots \alpha_n) \neq 0$.

Proposición: Sea la extensión $k(a_1, \dots a_n) \hookrightarrow k(a_1, \dots a_n)(\alpha_1, \dots, \alpha_n) \overset{\text{Cardan}}{=\!=} k(\alpha_1, \dots \alpha_n) \equiv$ cuerpo de descomposición del pol. general $p(x)$. Entonces

$$\underset{k(a_1 \dots a_n)\text{-alg}}{\mathrm{Aut}}\left(k(\alpha_1, \dots \alpha_n)\right) = S_n .$$

- **Resolución de la ec. de 2º grado**: $\mathbb{Q}(a_1, a_2) \hookrightarrow \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(a_1, a_2)(\sqrt{a})$, y si el pol. es $x^2 + a_1 x + a_2$, entonces $\alpha = \dfrac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2}$.

Definición: Una extensión de cuerpos $k \hookrightarrow k(\sqrt[n]{a})$ se dice radical, y se dice que es una extensión por radicales si es una cadena en cuyo eslabón es radical, ie,

$$k \hookrightarrow k(\sqrt[n_1]{a_1}) \hookrightarrow k(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}) \hookrightarrow \dots \hookrightarrow k(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r}),$$

con $a_i \in k(\sqrt[n_1]{a_1}, \dots, \sqrt[n_{i-1}]{a_{i-1}})$.

CONSTRUCCIONES CON REGLA Y COMPÁS

Definición: Una extensión por radicales cuadráticos es una extensión finita de cuerpos que se va obteniendo tomando raíces cuadradas de la extensión anterior:

$$K \hookrightarrow K(\sqrt{a_1}) \hookrightarrow K(\sqrt{a_1}, \sqrt{a_2}) \hookrightarrow \dots \hookrightarrow K(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n})$$

$$a_2 \in K(\sqrt{a_1}) \qquad a_n \in K(\sqrt{a_1}, \dots \sqrt{a_{n-1}})$$

- Si $K \hookrightarrow K(\sqrt{a_1}, \dots \sqrt{a_n}) = L$ ext. por rad. cuadr. $\Longrightarrow \dim_K L = 2^m$. Ly

Propos: $\dim_K L \neq 2^m \Longrightarrow L$ no ext. por rad. cuadr.

Teorema ✱: Sea $K \hookrightarrow L$ de Galois.

L ext. por radicales cuadráticos $\Longleftrightarrow \dim_K L = 2^m$.

Propos: Toda subextensión de una extensión por radicales cuadráticos es una extensión por radicales cuadráticos.

Definición: Se dice que $\alpha \in L$ es un irracional cuadrático de K si existe una extensión por radicales cuadráticos $K \hookrightarrow \Sigma$ tal que $\alpha \in \Sigma$. (ie, α es un falso raíz cuadrado)
ie, $K(\alpha)$ ext. por rad. cuadr.

Teorema: $\alpha \in \mathbb{C}$ irracional cuadrático $\Longleftrightarrow K(\alpha)$ está incluido en una extensión de Galois de orden 2^m.

$$K \hookrightarrow K(\alpha) \hookrightarrow \Sigma \qquad (K \hookrightarrow \Sigma : 2^m)$$

Definición: Sea $\mathbb{P} := \{$ unos cuantos ptos del plano euclídeo $\equiv$ ptos complejos $\}$. Se dice que una recta es <u>construible</u> si pasa por dos ptos de $\mathbb{P}$, y se dice que un punto es construible si se obtiene del corte de dos rectas construibles o del corte de una circunferencia de radio distancia entre dos ptos construibles y centro un pto construible con una recta construible, o de dos circunferencias.

- Son construibles: los ejes $\mathbb{R}$, $\mathbb{R}i$, la perpendicular a un recta, la paralela que una recta que pase por un pto, la circunferencia que pase por 3 ptos, la bisectriz de un ángulo.
- Denotamos $\mathcal{C}(\mathbb{P}) = \{$ ptos construibles a partir de $\mathbb{P}\}$.

Lema: $a+bi \in \mathcal{C}(\mathbb{P}) \iff a, b \in \mathcal{C}(\mathbb{P})$.

Teorema: $\mathcal{C}(\mathbb{P}) \subset \mathbb{C}$ es un subcuerpo estable por raíces cuadradas (ie, contiene a todas las raíces cuadradas de los elementos de $\mathcal{C}(\mathbb{P})$).

- Esto dice que dados dos complejos construibles, podemos sumar, restar, dividir, y tomar raíces con regla y compás!

Teorema: Sea k el mínimo cuerpo (dentro de $\mathbb{C}$) que contiene a $\mathbb{P}$.

$$\alpha \in \mathcal{C}(\mathbb{P}) \iff \alpha \text{ es irracional cuadrático de } k.$$

- Si $\mathbb{P} = \{0, 1\}$, $k = \mathbb{Q}$; si $\mathbb{P} = \{0, 1, \sqrt[3]{2}\}$, $k = \mathbb{Q}(\sqrt[3]{2})$.

Teorema: Dado $P = \{0, 1\}$, el polígono regular de n lados es construible con regla y compás $\iff n = 2^m \cdot p_1 \cdots p_r$ tal que $(p_i - 1) = 2^{k_i}$.

Definición: A los primos que verifican que $p - 1 = 2^u$ se llaman primos de Fermat, ie, $p = 1 + 2^u$ para algún u.

Teorema: p primo de Fermat $\Rightarrow p = 1 + 2^{2^m}$ para cierto m.

- Los únicos primos de Fermat conocidos hasta la fecha son $3, 5, 17, 257, 65\,537$.