Apuntes de Teoría de Galois

Lara Olmos Camarena

12 de enero de 2017

Referencias

[1] Apuntes del curso de *Teoría de Galois*, 2016-2017, UAM. Profesor: Margarita Otero.

[2] *Galois Theory*. Joseph Rotman.

¡OJO! Estos apuntes no están libres de errores. Para cualquier corrección contactar: lara.olmos@estudiante.uam.es

Índice

1. Resultados preliminares

1.1. Grupos

Definición 1 (Grupo). Un conjunto G con operación binaria $*$ en él definida se dice **grupo** si se cumplen las siguientes propiedades:

1. La operación $*$ es **cerrada** en G.
2. La operación $*$ es **asociativa**.
3. Existe elemento **neutro**.
4. Existe **inverso**: $x \in G, x^{-1} \in G$.

Definición 2 (Grupo abeliano). Se cumple que $x * y = y * x \ \forall x, y \in G$.

Definición 3 (Subgrupo). Dado G grupo, $H \subseteq G, H \neq \emptyset$, H es subgrupo si cumple:

1. $x, y \in H \Rightarrow xy \in H$
2. $x \in H \Rightarrow x^{-1} \in H$

1.2. Anillos, dominios y cuerpos

Definición 4 (Anillo). Un conjunto A con las operaciones binarias cerradas $+, *$ se dice **anillo** si se cumplen las siguientes propiedades.

1. $(A, +)$ es un **grupo abeliano**. Es decir, la operación + es asociativa y conmutativa, $\exists$ elemento neutro e inverso respecto a +.
2. La operación $*$ es **asociativa**.
3. La operación $*$ cumple la propiedad **distributiva**: $(a + b) * c = a * c + b * c$, $c * (a + b) = c * a + c * b \ \forall a, b, c \in A$.

Definición 5 (Subanillo). Un subconjunto B de un anillo $(A, +, *)$ se dice **subanillo** si cumple que $(B, +)$ es un **subgrupo de (A,+)** y el producto *** es cerrado en B**.

$$\forall b_1, b_2 \in B \ b_1 + b_2 \in B, b_1 * b_2 \in B$$

Definición 6 (Anillo conmutativo y unitario). Un **anillo conmutativo** es un anillo en el que la operación $*$ es conmutativa. Un **anillo unitario** es un anillo en el que existe un elemento 1_A tal que $1_A * a = a * 1_A = a$.
NOTACIÓN: *acu* $\equiv$ anillo conmutativo y unitario.

Definición 7 (Dominio de integridad). Dado un anillo conmutativo y unitario, R es un **dominio** si $\forall a, b \in R$, $ab = 0 \Rightarrow a = 0$ o $b = 0$. El conjunto de **unidades** de R es:

$$U(R) = \{a \in R : \exists b \in R \text{ tal que } ab = 1\}$$

Definición 8 (Cuerpo). Un cuerpo es un **anillo conmutativo unitario** que cumple que $(A^*, *)$ es un grupo (es un anillo con división). Dicho de otra forma, un cuerpo K es un dominio tal que $U(K) = K \setminus \{0\}$.
NOTACIÓN: $A^* \equiv A \setminus \{0\}$.

Definición 9 (Subcuerpo). Un subcuerpo S de K cumple que $(S, +) \subseteq (K, +)$ y $(S^*, *) \subseteq (K^*, *)$ (subgrupos). $(S, +, *)$ es un cuerpo.

Definición 10 (Anillo de polinomios). R[X], donde R es un anillo conmutativo y unitario. Sea $f(X) \in R[X]$, $f(X) = a_n X^n + ... + a_1 X + a_0$ con $a_i \in R (i = 0, ..., n)$ y $a_n \neq 0$.

- El **coeficiente director** de f es $cd(f) = a_n$. f es **mónico** si $a_n = 1$.
- El grado de f es $gr(f(x)) = n$. El polinomio nulo no tiene grado.
- El término constante de f es a_0. f es un polinomio constante si $n = 0$ o f es el polinomio nulo.

Propiedades de anillos. Sea R un anillo conmutativo y unitario.

1. $\forall a \in R, 0a = 0$ 2. $\forall a \in R, -a = (-1)a$ 3. $\forall a \in R, (-1)(-a) = a$
4. R es un dominio $\Leftrightarrow \forall a, b, c \in R$ con $c \neq 0$, $ac = bc \Rightarrow b = c$
5. Si R es un dominio $\Rightarrow$ R[X] es un dominio.
6. Si R es un dominio $\Rightarrow \forall f(X), g(X) \in R[X]$ tal que $cd(g) \in U(R)$ $\exists$ únicos $q(x)$, $r(x) \in R[X]$ (**cociente** y **resto**) tales que:

$$f(X) = q(X)g(X) + r(X) \text{ con } r(X) = 0 \text{ o } gr(r) < gr(g)$$

Demostración: La unicidad se ve como en el caso de que R sea un cuerpo. La existencia, por inducción. Caso base $f = 0$, $gr(f) = 0$, $gr(f) < gr(g)$. Para $gr(f) = n$, definimos $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_n \neq 0$ y $g(x) = \sum_{j=0}^{n} b_j x^j$ con $b_m \neq 0$, $n \geqslant m$, $b_m \in U(R)$. Tenemos que $\exists c \in R$ tal que $bac = 1$ y $gr(f - a_n c x^{n-m} g) \leqslant n - 1$. Por hipótesis de inducción, $f - a_n c x^{n-m} g = q_1 g + r_1$; $f = (a_n c x^{n-m} + q_1)g + r_1$

Definición 11 (Cuerpo de fracciones de un dominio). Dado R dominio, definimos en $R \times (R \setminus \{0\})$ la relación de equivalencia:

$$(a, b) \sim (c, d) \text{ si } ad = bc, \forall (a, b), (c, d) \in R \times (R \setminus \{0\})$$

El conjunto cociente es $\mathbf{cf(R)} = \{\mathbf{a/b : a, b \in R, b \neq 0}\}$ con las operaciones:

- $a/b + c/d = (a * d + b * c)/b * d$
- $a/b * c/d = a * c/b * d$

es el **cuerpo de fracciones** de R. NOTACIÓN: a/b es la clase de equivalencia de (a,b).

1.3. Homomorfismos e ideales

Definición 12 (Homomorfismo de anillos (unitarios))**.** Sean R y S dos *acu*. Sea $\psi : R \to S$ una aplicación. ψ es un **homomorfismo de anillos unitarios** si $\psi(1) = 1$, $\psi(a+b) = \psi(a) + \psi(b)$ y $\psi(ab) = \psi(a)\psi(b)$ $\forall a, b \in R$.
Un homomorfismo ψ es un **isomorfismo** si es biyectiva. Un homomorfismo es **automorfismo** si es un isomorfismo y R = S.
El **núcleo** de ψ es $Ker(\psi) = \{a \in R : \psi(a) = 0\}$.

Propiedades de homomorfismos unitarios. Sea $\psi : R \to S$ un homomorfismo.

1. Si $a \in R$ es una **unidad** de $R \Rightarrow \psi(a)$ es una unidad de S.
2. La aplicación $\psi' : R[X] \to S[X] : \sum_{i=0}^{n} a_i X^i \to \sum_{i=0}^{n} \psi(a_i) X^i$ es un homomorfismo, y es isomorfismo si ψ lo es.
3. $Im(\psi)$ es un subanillo de S. $Ker(\psi)$ es un subanillo de R.
4. ψ es inyectiva $\Leftrightarrow Ker(\psi) = \{0\}$

Definición 13 (Homomorfismo evaluación)**.** Un homomorfismo evaluación en $c \in R$:

$$ev_c : R[X] \to R : f(X) = \sum a_i X^i \to f(c) = \sum a_i c^i$$

$c \in R$ es **raíz** de $f(X) \in R[X]$ si $f(c) = 0$.

Definición 14 (Ideal)**.** Un ideal de un ***acu*** R es un conjunto $I \subseteq R$ tal que $0 \in I$, $\forall a, b \in I$ $a - b \in I$ y $\forall c \in R$ $\forall d \in I$ $cd \in I$.
Si $b \in R$, el **ideal principal generado por b** es $(b) = \{ab : a \in R\}$. Si $b_1, ..., b_m \in R$, el ideal generado por ellos es $(b_1, ..., b_m) = \{a_1 b_1 + ... + a_m b_m : a_i \in R, i = 1, ..., m\}$

Propiedades de ideales 1. Sea R un *acu*.

1. R contiene al menos dos ideales: $\{0\}$ y R.
2. $\psi : R \to S$ es homomorfismo de anillos unitarios $\Rightarrow Ker(\psi)$ es un ideal de R.
3. Si $u \in U(R)$ e I un ideal de R entonces $u \in I \Rightarrow I = R$ y $(ub) = (b)$ $\forall b \in R$.
4. Si R es un dominio y $b_1, b_2 \in R \Rightarrow (b_1) = (b_2) \Leftrightarrow b_1 = ub_2$, para algún $u \in U(R)$.
5. R es un cuerpo $\Leftrightarrow$ sus únicos ideales son $\{0\}$ y R.
   Demostración:
   $(\rightarrow)$ I ideal de R, $I \neq \{0\} \Rightarrow \exists\, a \in I$, $a \neq 0 \Rightarrow a \in U(R) \Rightarrow (a) = (1) = R \Rightarrow I = R$.
   $(\leftarrow)$ Basta demostrar que $U(R) = R \setminus \{0\}$. Así $ab = 0$ y $a \neq 0 \Rightarrow b = 0$.
   $a \in R \setminus \{0\}$, $(a) \neq \{0\}$ por lo tanto $(0) = R \Rightarrow a \in U(R)$.

Definición 15 (Anillo cociente de R módulo I)**.** Dado R *acu* e I ideal de R, definimos la relación de equivalencia $a \sim b \Leftrightarrow a - b \in I$. El **conjunto cociente**

$$R/I = \{a + I : a \in R\}$$

con las operaciones $(a + I) + (b + I) = (a + b) + I$, $(a + I)(b + I) = (ab) + I$ es un *acu* llamado **anillo cociente de R módulo I**.

Propiedades de los anillos cocientes:

1. La **proyección natural** $\pi : R \to R/I : a \to a + I$ es homomorfismo de anillos.
2. $\exists$ una biyección entre el conjunto de ideales intermedios $I \subseteq J \subseteq R$ y el conjunto de ideales de R/I, dada por: $J \to \pi(J) = J/I = \{a + I : a \in J\}$.
   Además si $J \subseteq J'$ son ideales intermedios entonces $\pi(J) \subseteq \pi(J')$.
3. Si S es un anillo unitario y $\psi : R \cong S \Rightarrow R/I \cong S/\psi(I) : a + I \to \psi(a) + \psi(I)$

Primer teorema de isomorfía. Si $\psi : R \to S$ es un homomorfismo de anillos unitarios **sobreyectivo**, entonces existe un isomorfismo de anillos unitarios

$$R/Ker(\psi) \to Im(\psi) : a + Ker(\psi) \to \psi(a)$$

Definición 16 (Dominio de ideales principales)**.** Sea R un *acu*, R es un **dominio de ideales principales si cada ideal de R es principal**. NOTACIÓN: DIP.

Definición 17 (Ideal primo e ideal maximal)**.** Sea I un ideal R (R *acu*).
I es **primo** si $I \neq R$ y $ab \in I \Rightarrow a \in I$ ó $b \in I$.
I es **maximal** si $I \neq R$ y no existe $J \subseteq R$ ideal tal que $I \subset J \subset R$.

Propiedades de ideales 2. Sea R un *acu* e I ideal de R.

1. Si R es un **cuerpo** $\Rightarrow R[X]$ es un **dominio de ideales principales**.
2. I es un **ideal primo** $\Leftrightarrow R/I$ es un **dominio**.
3. I es un **ideal maximal** $\Leftrightarrow R/I$ es un **cuerpo**. **Demostración:**
   ($\to$) Los únicos ideales de R/I son $\{0 + I\}$ y R/I. J ideal de $R/I \Rightarrow J^* = J/I$ para algún ideal $I \subseteq J \subseteq R$. I maximal $\Rightarrow J = I$ o $J = R$.
   ($\leftarrow$) Sea J ideal de R, $I \subset J \subseteq R$. Por la biyección J/I es $\{0\}$ o R/I o $J = I$ o $J = R$.
4. Si I es un ideal **maximal** $\Rightarrow$ I es un ideal **primo**.
5. Si R es un DIP e I es un ideal primo $I \neq \{0\} \Rightarrow$ I es un ideal maximal.

Definición 18 (Divisibilidad)**.** Sea R *acu*. Sean $a, b \in R$. *a* **divide** a *b* si existe $c \in R$ tal que $ac = b \Leftrightarrow (b) \subseteq (a)$. NOTACIÓN: $a|b$.

1.4. Anillos de polinomios sobre un cuerpo

Sea F cuerpo. Los polinomios de esta sección son elementos de F[X].

Definición 19 (Raíz). Sea R un dominio, $f(X) \in R[X]$, $a \in R$. a es **raíz** de $f \Leftrightarrow (x-a)|f(X)$. a es **raíz múltiple** de un polinomio $f(X) \in R[X]$ si $(X-a)^n|f(X)$.

Definición 20 (Máximo común divisor). El máximo común divisor de f(X) y g(X) es un polinomio d(X) tal que:

1. $d(X)|f(X)$ y $d(X)|g(X)$.
2. Si $c(X)|f(X)$ y $c(X)|g(X) \Rightarrow c(X)|d(X)$.
3. d(X) es **mónico**.

f(X) y g(X) son **coprimos** si $d(X) = (f(X), g(X)) = 1$. Notación: $d(X) = (f(X), g(X))$

Propiedades del mcd:

1. **Identidad de Bezout**. Sean $f(X)$ y $g(X) \neq 0 \Rightarrow \exists d(X) = (f(X), g(X))$, y $\exists a(X), b(X)$ tales que $\mathbf{d(X) = a(X)f(X) + b(X)g(X)}$. d(X) se calcula con el **algoritmo de Euclides**.
2. Si $(f(X), g(X)) = 1$ y $f(X)|(g(X)h(X)) \Rightarrow f(X)|h(X)$ en F[X].
3. Si F es un subcuerpo de un cuerpo E $\Rightarrow (f(X), g(X))$ calculado en F[X] es el mismo que el calculado en E[X].

Definición 21 (Irreducible). Sea R **dominio**. Un polinomio no nulo $p(X) \in R[X]$ es **irreducible sobre R** si $p(X) \notin U(R[X])$ y **no** existe una factorización en R[X] $\mathbf{p(X) = f(X)g(X)}$ con $f(X), g(X) \notin U(R[X])$.
Si R es un **cuerpo**, $gr(p(X)) \geqslant 1$ y **no existen** $f(X), g(X) \in R[X]$ con $gr(f(X)) < gr(p(X))$ y $gr(g(X)) < gr(p(X))$ tales que $p(X) = f(X)g(X)$.

Ejemplo 1. Veamos que $2x-4$ es irreducible en $\mathbb{Q}[X]$. Tenemos que $2x-4 \notin U(\mathbb{Q}[X])$. Supongamos que $\exists f(X), g(X) \in \mathbb{Q}[X]$ tales que $2x-4 = f(X)g(X)$. Se cumple que $gr(f(X)g(X)) = gr(f(X)) + gr(g(X)) = 1$. Así, $gr(f(X)) = 0$ y $gr(g(X)) = 1$ (o viceversa). Como por hipótesis $f(X) \neq 0$, $f(X) \in \mathbb{Q}^* \Rightarrow f(X) \in U(\mathbb{Q}[X])$, lo que contradice que exista factorización. Análogo para $g(X)$ en el caso de que $gr(g(X)) = 0$.

Observación: Los anillos $F[X_1, ..., X_n]$ son dominios de factorización única.

Definición 22 (Descomposición). Un polinomio $f(X) \in F[X]$ se **descompone sobre F** si es producto de factores lineales.

Propiedades de polinomios irreducibles 1.

1. Si $gr(p(X))$ es 2 o 3, $p(X)$ es irreducible sobre F $\Leftrightarrow$ p(X) no tiene raíces en F.
2. Si $p(X)$ es irreducible sobre F y $g(X) \in F[X]$ no es constante entonces, o bien $(p(X), g(X)) = 1$ o $p(X)|g(X)$.
3. Si p(X) es irreducible sobre F y $p(X)|q_1(X)...q_s(X) \Rightarrow p|q_j(X)$ para algún j.
4. $\mathbf{p(X)}$ **es irreducible** sobre F $\Leftrightarrow$ $(\mathbf{p(X)})$ es **ideal maximal** de F[X].
5. Si $f(X) \in F[X]$ es no nulo entonces existen $p_1(X), .., p_s(X) \in F[X]$ **mónicos e irreducibles sobre F** (no necesariamente distintos) y $a \in F$ no nulo tales que $\mathbf{f(X) = ap_1(X)...p_s(X)}$ la **factorización es única** salvo el orden.
6. Si $f(X) = ap_1(X)^{k_1}...p_t(X)^{k_t}$ y $g(X) = bp_1(X)^{n_1}...p_t(X)^{n_t}$ donde $k_i \geqslant 0$, $n_i \geqslant 0$, $a, b \in F^*$ y los $p_i(X)$ polinomios irreducibles sobre F mónicos y distintos, entonces $(f(X), g(X)) = p_1(X)^{m_1}...p_t(X)^{m_t}$, donde $m_i = min\{k_i, n_i\}$.

Propiedades de raíces de polinomios. Sea F un cuerpo y $f(X), g(X) \in F[X]$.

1. f(X) se descompone en F $\Leftrightarrow$ tiene todas sus raíces en F.
2. $\forall a \in F$ existe $q(X) \in F[X]$ tal que $f(X) = q(X)(X - a) + f(a)$.
3. Si $gr(f(X)) = n$, $f(X)$ tiene a lo más n raíces en F.
4. Si $f(a) = g(a) \forall a \in F$ y F tiene al menos $max\{gr(f(X)), gr(g(X))\} + 1$ elementos (en particular, si F es infinito) entonces $f(X) = g(X)$.
5. Si $f(X) = \prod_{i=1}^{n}(x - a_i)$, f no tiene raíces múltiples $\Leftrightarrow$ f y f′ no tienen un cero en común $\Leftrightarrow$ $(f(X), f'(X)) = 1$.

1.5. Criterios de irreducibilidad

Propiedades de transferencia de irreducibilidad.

1. Sean R y S dominios y $\phi : R \to S$ un homomorfismo y $\phi' : R[X] \to S[X]$ el homomorfismo inducido por ϕ'.
   a) Si $\phi'(p(X)) \in S[X]$ es irreducible sobre S y $gr(\phi'(p(X))) = gr(p(X)) \Rightarrow$ p(X) no es un producto de dos polinomios de grado menor $gr(p(X))$.
   b) Si ϕ es un isomorfismo $\Rightarrow \phi'$ es un isomorfismo. $\phi'(p(X)) \in S[X]$ es irreducible sobre S $\Leftrightarrow$ p(X) es irreducible sobre R.
2. Sea $\pi : \mathbb{Z} \to \mathbb{F}_p$ la proyección natural. Si $p(X) \in \mathbb{Z}[X]$ es mónico y $\pi(p(X))$ irreducible sobre $\mathbb{F}_p$, entonces p(X) es irreducible sobre $\mathbb{Z}$.
3. Sea R un dominio y $a \in R \Rightarrow$ la aplicación $\phi_a : R[X] \to R[X] : f(X) \to (X + a)$ es un automorfismo del dominio R[X] y por tanto $p(X) \in R[X]$ es irreducible sobre R $\Leftrightarrow$ p(X+a) es irreducible sobre R.

Definición 23 (Polinomio primitivo)**.** Un polinomio $f(X) = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$ es **primitivo** si el mcd de sus coeficientes es 1.

Propiedades de polinomios primitivos.

1. **Lema de Gauss**: El producto de polinomios primitivos es un polinomio primitivo. **Demostración:**

   Sea $f(X) = \sum_{i=0}^{n} a_i X^i$, $g(X) = \sum_{j=0}^{m} b_j X^j$ con $mcd(a_i) = 1, 0 \leqslant i \leqslant n$, $mcd(b_j) = 1$ $0 \leqslant j \leqslant m$. Tenemos que $f(X)g(X) = \sum_{k=0}^{n+m} c_k x^k$ donde $c_k = \sum_{i+j=k}^{n+m} a_i b_j$. Supongamos que existe p primo tal que $p | c_k \forall k = 0, ..., n+m$. Sean i,j mínimos números tal que $p \nmid a_i$, $p \nmid b_j$, entonces
   $a_i b_j = c_{i+j} - (a_0 b_{i+j} + a_i b_{i+j-1} + ... + a_{i-1} b_{j+1} + a_{i+1} b_{j-1} + a_{n_j} b_n)$

   $p | (a_{i+1} b_{j-1} + a_{n_j} b_n)$ y $p | (a_i b_j = c_{i+j} - (a_0 b_{i+j} + a_i b_{i+j-1})$, por lo que $p | a_i b_j$, contradicción.
2. Todo $f(X) \in \mathbb{Q}[X]$ no nulo tiene una única factorización $f(X) = c(f) f^*(X)$ donde **contenido de f**, c(f), es racional y $c(f) > 0$ y $f^*(X) \in \mathbb{Z}[X]$ es primitivo.
3. Si $f(X) \in \mathbb{Z}[X]$, $c(f) \in \mathbb{Z}$ y es el mcd de los coeficientes de f.
4. Si $f(X) \in \mathbb{Q}[X]$ se factoriza como $f(X) = g(X)h(X)$ en $\mathbb{Q}[X]$ entonces $c(f) = c(g)c(h)$ y $f^*(X) = g^*(X)h^*(X)$.
5. Si $f(X) \in \mathbb{Z}[X]$ no es producto de dos polinomios de $\mathbb{Z}[X]$ de grado menor que el de f(X), entonces f(X) es irreducible sobre $\mathbb{Q}(X)$.

Criterio de Eisenstein. Sea $f(X) = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$. Si existe un primo $p \in \mathbb{N}$ tal que:

1. $p | a_i$ para todo $i < n$.
2. $p \nmid a_n$ y $p^2 \nmid a_0$

entonces $f(X)$ es irreducible sobre $\mathbb{Q}$.

Definición 24 (Polinomio ciclotómico). El **p-ésimo polinomio ciclotómico** es

$$\Phi_p(X) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + ... + x + 1$$

Propiedades de polinomios irreducibles 2.

7. Para cada p primo, el p-ésimo polinomio ciclotómico es irreducible sobre $\mathbb{Q}$.
8. $\forall a \in \mathbb{Z}$, $a \neq \pm 1$ y a libre de cuadrados, y para todo $n \geqslant 2$, el polinomio $x^n - a$ es irreducible sobre $\mathbb{Q}$.

1.6. Conceptos de grupos. Grupos finitos

Definición 25 (Subgrupo normal). $N \leqslant G$, $\forall x \in G$ $Nx = xN$. Se denota $N \trianglelefteq G$. Algunos resultados son:

- $N \trianglelefteq G \Leftrightarrow x^{-1}Nx = N$ $\forall x \in G$.
- Si $N \leqslant G$, $[G : N] = 2 \Rightarrow H \trianglelefteq G$.
- Si $(A, *)$ abeliano, $N \leqslant A \Rightarrow N \trianglelefteq A$.
- Sea G grupo y N único subgrupo de G con orden $|N| < \infty \Rightarrow N \trianglelefteq G$.
- Si $\varphi : G \to H$ es un homomorfismo, $Ker(\varphi) = \{g \in G : f(g) = 1\} \trianglelefteq G$.

Definición 26 (Índice de un grupo). $H \leqslant G$, $[G : H] = |\{Hx : x \in G\}| = |\{xH : x \in G\}|$

Teorema I.1. Teorema de Lagrange. Sea H un subgrupo de G grupo, entonces $|G| = [G : H] * |H|$. Si H es un subgrupo normal de G, $|G/H| = |G|/|H|$.

Definición 27 (Centro de un grupo). $Z(G) = \{g \in G : gh = hg \ \forall h \in G\}$. $Z(G) \trianglelefteq G$.

Definición 28 (Grupo simple). Grupo que no tiene subgrupos normales, excepto el trivial y el total.

Teorema I.2. Teorema de Cauchy. Si p es un primo que divide el orden de G, entonces G tiene un elemento de orden p.

Lema. Si G es abeliano y no trivial, entonces contiene un subgrupo de índice primo.

Hoja 1

1. Halla las unidades de los siguientes anillos.

   a) $\mathbb{Z}/9\mathbb{Z}$

   Gracias a la función φ de Euler,

   $$\varphi(n) = |\{n \in \mathbb{N} : n \leqslant m \text{ y } (n, m) = 1\}|$$

   sabemos que hay $\varphi(9) = \varphi(3^2) = 6$ unidades en este anillo. Así,

   $$U(\mathbb{Z}/9\mathbb{Z}) = \{[1], [2], [4], [5], [7], [8]\} = \{[1], [2], [4], [-2], [-4], [-1]\}$$

   b) $\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\}$

   Si $(a + bi) \in \mathbb{Z}$ es unidad, $(a + bi)^{-1} = \frac{a-bi}{a^2+b^2} \in \mathbb{Z}$ también. Los únicos que cumplen esas condiciones son: $U(\mathbb{Z}[i]) = \{-1, -i, 1, i\}$, obtenidos al sustituir por $a = 0$, después $b = 0$ en las expresiones anteriores. Para $a \neq 0$ y $b \neq 0$, $\frac{a}{a^2+b^2} \notin \mathbb{Z}$ y $\frac{b}{a^2+b^2} \notin \mathbb{Z}$.

   c) $\mathbb{R}[X]$

   Supongamos que $\exists f(X) \neq 0$ tal que $f(X)g(X) = 1$ con $g(X) \neq 0 \Rightarrow gr(f(X)g(X)) = gr(f(X)) + gr(g(X)) = 0 \Rightarrow gr(f(X)) = 0$ y $gr(g(X)) = 0$. Por tanto, $f(X) \in U(\mathbb{R}[X])$, $g(X) \in U(\mathbb{R}[X])$.
   Así, $U(\mathbb{R}[X]) = U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.

2. Halla el cociente y el resto de dividir $X^3 + 2iX + 1$ por $iX + 2$ en $\mathbb{Z}[i]$.
   Cociente: $-iX^2 + 2X + 2 + 4i$. Resto: $-3 - 8i$.

3. Demuestra que todo subanillo de un cuerpo es un dominio.
   Sea $A \subset K$, K cuerpo y A subanillo. Sean $a, b \in A \subset K$, $ab \in A$ por ser A subanillo. Si $ab = 0 \in A \Rightarrow a = 0$ o $b = 0$ por cumplirse esta condición en K cuerpo. Por tanto, A es dominio.

4. Demuestra que cualquier intersección no vacía de subcuerpos de un cuerpo es un cuerpo.
   $F := \bigcap_{i \in I} K_i \neq \{\emptyset\}$, $F \subset K$. Observamos que:

   - $\forall a, b \in F$, $a \pm b \in F$. Es cierto porque $\forall a, b \in K_i \ \forall i \in I \ a \pm b \in K_i \ \forall i \in I$ por ser cada K_i un cuerpo $(K_i, +)$ es un grupo. Además la operación $+$ es asociativa y conmutativa en cada K_i por definición de cuerpo, por lo tanto, la **operación + es asociativa y conmutativa en F**.

   - $\forall a, b \in F$, $ab \in F$. Es cierto porque $\forall a, b \in K_i \ \forall i \in I \ ab \in K_i \ \forall i \in I$ por ser cada K_i un cuerpo. Además la operación $*$ es asociativa, conmutativa y cumple la propiedad distributiva en cada K_i por definición de cuer-

po, por lo tanto, la **operación * es asociativa, conmutativa y cumple la propiedad distributiva en F**.

- $0 \in F$, $1 \in F$. Por definición de cuerpo, $0 \in K_i \ \forall i \in I \Rightarrow 0 \in F$. Análogamente, $1 \in K_i \ \forall i \in I \Rightarrow 1 \in F$.
- $\forall a \in F, a \neq 0, a * 1 \in F$. Esta propiedad se cumple en cada K_i por definición de cuerpo, por lo que en F también se cumple. Esto equivale a decir que $U(F) = F^*$.

Por tanto F es un cuerpo.

5. Sea $p \in \mathbb{N}$ primo.

   a) Demuestra que $\mathbb{F}_p[X]$ es un dominio infinito que contiene a $\mathbb{F}_p$ como subanillo. ($\mathbb{F}_p \equiv \mathbb{Z}/p\mathbb{Z}$)

   $\mathbb{F}_p[X] = \{\sum_{i=0}^{n} a_i X^i : a_i \in \mathbb{F}_p, i = 0, ..., n \in \mathbb{Z}\}$.

   $\mathbb{F}_p$ es un cuerpo $\Rightarrow \mathbb{F}_p[X]$ es un dominio.

   $\mathbb{F}_p[X]$ es infinito porque contiene el subconjunto infinito $\{x^m : m \in \mathbb{N}\}$.

   Sea el homomorfismo evaluación $ev_0 : \mathbb{F}_p[X] \to \mathbb{F}_p : p(x) \to p(0) = a_0 \in \mathbb{F}_p$. Por ser ev_0 homomorfismo de anillos $Im(ev_0) = ev_0(\mathbb{F}_p[X]) = \mathbb{F}_p$ es un subanillo de $\mathbb{F}_p[X]$.

   b) Demuestra que existe un cuerpo infinito que contiene a $\mathbb{F}_p$ como subcuerpo.

   El cuerpo de fracciones de $\mathbb{F}_p$ es:
   $\mathbb{F}_p(X) = \{\frac{f(X)}{g(X)} : f(X), g(X) \in \mathbb{F}_p[X], g(X) \neq 0\} \supset \mathbb{F}_p[X]$ basta que $g(X) = 1 \in \mathbb{F}_p$.
   Así, $\mathbb{F}_p(X) \supset \mathbb{F}_p[X] \supset \mathbb{F}_p$, por el apartado anterior.

   c) Halla dos polinomios distintos f(X) y g(X) en $\mathbb{F}_p[X]$ tales que $f(a) = g(a)$ $\forall a \in \mathbb{F}_p$.

   Ejemplo 1: $f(x) = x(x-1)(x-2)...(x-(p-1))$,
   $g(x) = x(x-1)^2(x-2)...(x-(p-1))$

   Ejemplo 2: En $\mathbb{F}_2[X]$ $f(x) = x^3 + 1$, $g(x) = x + 1$.

6. Sea R un dominio. Halla el núcleo del homomorfismo de evaluación $ev_0 : R[X] \to R : f(X) \to f(0)$.

   $Ker(ev_0) = \{p(x) \in R[X] : p(0) = 0\} = \{\sum_{i=0}^{n} a_i x^i \in R[X] : a_0 = 0, n \in \mathbb{N}\} =$
   $R[X] \setminus R \cup \{0\} = (x)$

7. Demuestra que el conjunto $I = \{f(X) \in \mathbb{Z}[X] : 2 \text{ divide a } f(0)\}$ es un ideal de $\mathbb{Z}[X]$ y halla un conjunto (mínimo) de generadores de I.

   Veamos que I cumple las propiedades de ideales:

   - $2|0 \Rightarrow 0 \in I$.
   - Dados $a(x), b(x) \in I$, $a(x) - b(x) \in I$ porque $\exists\ f(x), g(x) \in R[X]$ tales que $a(0) = 2f(0)$, $b(0) = 2g(0) \Rightarrow a(0) - b(0) = 2(f(0) - g(0))$.
   - Dados $a(x), b(x) \in \mathbb{Z}[X]$, $a(x) \in I \Rightarrow 2|a(0) \Rightarrow 2|a(0)b(0) \Rightarrow a(x)b(x) \in I$.

   El conjunto mínimo de generadores es $\{2, x\}$, porque:
   $f(x) = x^n a_n + ... + a_1 x + a_0 = x(a_n x^{n-1} + ... + a_1) + \frac{a_0}{2} * 2$.

   Probemos que es mínimo. Supongamos que $I = (f(x))$ es el ideal mínimo tal que $2 \in I$, $2 = f(x)g(x)$ para $g(x) \in R[X] \Rightarrow f(x) \equiv cte. \Rightarrow f(x) = \pm 2 \Rightarrow (-2) = (2) \Rightarrow x \in (\pm 2)$, lo cual lleva a contradicción.

8. Sea R un dominio. Sea $I = (X)$ en $R[X]$. Demuestra que $R[X]/I \approxeq R$.

   Consideremos el homomorfismo $ev_0 : R[X] \to R$. Por el ejercicio 6, $Ker(ev_0) = (X)$. ev_0 es sobreyectivo, porque $\forall b \in S$, $b = ev_0(b)$. Por el primer teorema de isomorfía se cumple que $R[X]/(X) \approxeq R = Im(ev_0)$.

9.

10.

11.

12.

13.

14.

15.

16.

2. Extensiones de cuerpos

2.1. Propiedades básicas

Definición 29 (Extensión de F)**.** Sean E y F dos cuerpos. E es una **extensión de F** si existe $\psi : F \to E$ homomorfismo de cuerpos, es decir, un homomorfismo entre los anillos conmutativos unitarios de F y E. NOTACIÓN: E/F.

Observación: Sea $\psi : F \to E$ homomorfismo de cuerpos.

1. Todo homomorfismo de cuerpos es inyectivo. **Demostración:** $\mathrm{Ker}(\psi)$ es un ideal de F, por lo tanto $\mathrm{Ker}(\psi) \neq F$ o $\{0\}$. Por lo tanto, $\mathrm{Ker}(\psi) = \{0\}$ y ψ es inyectivo.
2. $\psi(1) = 1 \neq 0$, entonces $F \cong \psi(F)$. E contiene una copia de F que identificaremos con F. Así, dada **E/F, F es un subcuerpo de E**.
3. Dada **E/F** extensión de cuerpos, entonces **E es un F-espacio vectorial** (F-ev).

Ejemplo 1. $E = \mathbb{R}[X]/(x^2+1)$, $\varphi : \mathbb{R} \to \mathbb{R}[X]/(x^2+1)$.

$\mathbb{R}[X]/(x^2+1) = \{f(x) + (x^2+1) : f(x) \in \mathbb{R}[X]\} = \{a + bx + (x^2+1) : a, b \in \mathbb{R}\}$

Ejemplo 2. $\mathbb{Q}[X]/(x^2-2) (\cong \mathbb{Q}(\sqrt{2}))$, $\mathbb{Q} \to \mathbb{Q}[X]/(x^2-2)$: $a \to a + (x^2-2)$

Tenemos que $\mathbb{Q}[X]/(x^2-2)$ es un cuerpo porque x^2-2 irreducible en $\mathbb{Q}[X]$ (no tiene raíces sobre $\mathbb{Q}[X]$ y tiene grado 2), por lo que genera un ideal maximal.

Lema II.1. Sea F un cuerpo y $p(x) \in F[X]$ irreducible. Entonces $E := F[X]/(p(x))$ es una extensión de F y p(x) (su imagen en E[X]) tiene una raíz en E.

Demostración: Dada $\psi : F \to E$: $a \to a + p(x)$, ψ es homomorfismo porque es composición de los homomorfismos $F \to F[X] \to F[X]/(p(x))$. Como p(x) es irreducible, (p(x)) es un ideal maximal y por lo tanto, $E = F[X]/(p(x))$ es un cuerpo.

Sea $p(x) = \sum_{i=0}^{n} a_i x^i$, $I = (p(x))$, $\alpha = x + I$. Veamos que α es raíz de $p(x) \in E[X]$. Entonces $\mathbf{p(\alpha) = \sum (a_i + I)\alpha^i = \sum (a_i + I)(x+I)^i = \sum (a_i + I)(x^i + I) = \sum a_i x^i + I}$ $= p(x) + I = I$. $p(\alpha) \in E[\alpha]$.

Ejemplo 3. $\mathbb{Q}[X]/(x^3-2) \cong \mathbb{Q}(\sqrt[3]{2})$.

Ejemplo 4. $\mathbb{F}_3[X]/(x^2+1)$ extiende porque x^2+1 no tiene raíces en $\mathbb{F}_3$, x^2+1 es irreducible porque tiene grado 2. En $\mathbb{F}_3(\alpha)$, $\alpha^2+1=0 \Rightarrow \alpha^2=2$. $\mathbb{F}_3[X]/(x^2+1)$ es un $\mathbb{F}_3$-ev.

Teorema II.2. (**Teorema de Kronecker**). Sea F un cuerpo y $f(x) \in F[X] \setminus F$. Entonces existe E/F tal que f(x) se **descompone** en E.

Demostración: Si $gr(f(x))=1$, E = F. Si $gr(f(x))>1$ y sea $p(x)$ irreducible, tal que $p(x)|f(x)$. Por el **Lema II.**1 existe F_1/F y $\alpha \in F_1$ tal que $p(\alpha)=0$.

$(x-\alpha)|p(x)$ en F_1/F, $f(x)=(x-\alpha)h(x)$ en F_1, donde $0<gr(h(x))<gr(f(x))$.

Por hipótesis de inducción existe E/F_1 donde h(x) se descompone, por lo tanto f se descompone en E. E/F_1 y $F_1/F \Rightarrow E/F$.

Lema II.3. Sea E/F extensión de cuerpo. Sea $\alpha \in E$, $p(x) \in F[X]$ polinomio mónico e irreducible en F tal que $p(\alpha)=0$ en E. Entonces

1. $\forall f(x) \in F[X]^*$, $f(\alpha)=0 \Rightarrow gr(p(x)) \leqslant gr(f(x))$.
2. p(x) es el único polinomio mónico de grado $gr(p(x))$ tal que $p(\alpha)=0$.

Demostración:

(1) Sea $I=\{g(x) \in F[X] : g(\alpha)=0\}$ ideal de $F[X]$. Sea $p(x) \in F[X]$. Sea $f(x) \in F[X]^*$, $f(\alpha)=0$, $f(x) \in I$. Sea $d(x)=(p(x),f(x))$, $d(x)|p(x) \Rightarrow d(x)=p(x)$ porque d y p son mónicos, por lo tanto $p(x)|f(x)$. En particular, $gr(p(x)) \leqslant gr(f(x))$.

(2) Sea $m=gr(p(x))$. Sea $f(x) \in I$, $gr(f(x))=m$ otro polinomio mónico que cumple $f(\alpha)=0$. Entonces, $p(x)|f(x)$, $gr(p(x))=gr(f(x))$, f y p son mónicos y $f(x)=p(x)$.

Ejemplo 5. $\mathbb{C}/\mathbb{Q}$, $\sqrt{2} \in \mathbb{C}$, x^2-2 es mónico, irreducible y tiene a $\sqrt{2}$ como raíz, es el único polinomio que cumple eso.

Definición 30 (Grado E sobre F. Extensión por adjunción de elementos.)**.** Dada E/F.

1. El **grado de E sobre F** es $[E:F] := \dim_F E$, (dimensión de E como F-ev).
2. Sea $\alpha_1,...,\alpha_n \in E$ el menor subcuerpo de E que contiene a F y a $\alpha_1,...,\alpha_n$ es $F(\alpha_1,...,\alpha_n)$ es **extensión de F** por **adjunción de elementos** $\alpha_1,...,\alpha_n$.

Proposición II.4. Sea F cuerpo, $p(x) \in F[X]$ irreducible con $gr(p)=d$. Entonces $E := F[X]/(p(x))$ es una extensión de F de grado d, es decir, $[E:F]=d$.

Además, sea $\alpha = x+(p(x))$, raíz de p en E. Entonces, la base de E como F-ev es $\{1,\alpha,\alpha^2,...,\alpha^{d-1}\}$.

Demostración: Basta demostrar que $B = \{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$ es una base de E, por tanto, que sus elementos son linealmente independientes: $\sum_{i=0}^{d-1} a_i \alpha^i = 0$, $a_i \in F$.

Sea $f(x) = \sum_{i=0}^{d-1} a_i x^i \in F[X]$ con $f(\alpha) = 0$. Por el Lema II.3, $gr(p) \leqslant gr(f)$ o $f = 0$. Si $f \neq 0$ obtenemos una contradicción, por tanto, tenemos que $a_i = 0\ \forall i = 0, ..., d-1$.

Ahora comprobemos que B genera E. Dado $f(x) \in F[x]$, $f(x) = g(x)p(x) + r(x)$.

- Si $r(x) = 0$, $f \in (p(x))$, $f = 0$ en E.
- Si $r(x) \neq 0$, $gr(r) < a$.
  $f(x) + (p(x)) = r(x) + (p(x))$. $f(x) + (p(x)) = \sum_{i=0}^{d-1} a_i x^i + (p(x)) = \sum_{i=0}^{d-1} (a_i + (p(x)))\alpha^i$

Ejemplo 6. Como dijimos en el ejemplo 4, $\mathbb{F}_3[X]/(x^2+1)$ es un $\mathbb{F}_3$-ev. En $\mathbb{F}_3(\alpha)$, $\alpha^2 + 1 = 0 \Rightarrow \alpha^2 = 2$. $\mathbb{F}_3[X]/(x^2+1) = \{a + bx + I : a, b \in \mathbb{F}_3\}$. La dimensión como $\mathbb{F}_3$-ev es 2, su base $\{1, \alpha\}$.

Definición 31 (Algebraico. Transcendente)**.** Sea F cuerpo y E extensión de F, E/F.

- α es **algebraico** sobre F si $\exists p(x) \in F[X]^*$ tal que $p(\alpha) = 0$.
- α es **transcendente** sobre F si no es algebraico.

La extensión E/F es algebraica si $\forall x \in E$, x es algebraico sobre F.

Ejemplo 7. $\pi \in \mathbb{R}$, π es transcendente sobre $\mathbb{Q}$. $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$, es raíz del polinomio $x^2 - 2$ en $\mathbb{R}$ extensión de $\mathbb{Q}$.

Proposición II.5. E/F extensión de cuerpos. Si E/F es finita $\Rightarrow$ E/F es algebraica.

Demostración: Sea $\alpha \in E$. Sea $n = dim_F E$. Sabemos que $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ son linealmente dependientes por lo que $\exists a_i \in F$ $i = 0, ..., n$ tal que $\sum_{i=0}^{n} a_i \alpha^i = 0$, por lo tanto α es raíz de $p(x) = \sum_{i=0}^{n} a_i x^i$. Luego, α es algebraico en F.

Teorema II.6. Sea F cuerpo y E/F. Sea $\alpha \in E$ algebraico sobre F. Entonces

1. Existe $p(x) \in F[X]$ mónico e irreducible tal que $p(\alpha) = 0$.
2. $F[X]/(p(x)) \cong F(\alpha)$, es decir, existe ϕ isomorfismo tal que $\phi : F[X]/(p(x)) \to F(\alpha) : x + (p(x)) \to \alpha$, $\phi|_F = id_F$.
3. p(x) es el único polinomio mónico de grado mínimo de F[X] que tiene a α como raíz.
4. $[F(\alpha) : F] = gr(p(x))$.

Demostración:

(1) $\psi : F[X] \to E$, $f(x) \to f(\alpha)$, $\psi = ev_x|_{F[X]}$. $Ker(\psi) = \{f(x) \in F[X] : f(\alpha) = 0\} \neq \{0\}$ ya que α es algebraico en F. Por el primer teorema de isomorfía, $F[X]/Ker(\psi) \cong Im(\psi)$.

$Im(\psi)$ es un subanillo de F cuerpo, por lo que $Im(\psi)$ es un dominio $\Rightarrow$ $Ker(\psi)$ es un ideal primo no nulo $\Rightarrow$ $F[X]$ es un dominio de ideales principales, $Ker(\psi) = (p(x))$.

$Ker(\psi)$ es un ideal primo y no nulo $\Rightarrow$ p(x) es irreducible y podemos suponer que mónico. Además, $p(\alpha) = 0$.

(2) ψ induce el isomorfismo $\phi : F[X]/(p(x)) \to Im(\psi) : x + (p(x)) \to \psi(x)$,
$c + (p(x)) \to c$ para cada $c \in F$.

p(x) es irreducible $\Rightarrow$ (p(x)) es un ideal maximal $\Rightarrow$ $F[X]/(p(x))$ es un cuerpo e $Im(\psi)$ es subcuerpo, $Im(\psi) = \{f(\alpha) : f(x) \in F[X]\}$. $Im(\psi)$ es el mínimo cuerpo que contiene a F y a α.

(3) Lema II.3
(4) Proposición II.4

Ejemplo 8. $\sqrt{2} \in \mathbb{R}$ algebraico sobre $\mathbb{Q}$. $x^2 - 2$ es irreducible en $\mathbb{Q}$ porque tiene grado 2 y no tiene raíces en $\mathbb{Q}$. $\mathbb{Q}[X]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Ejemplo 9. $\sqrt[3]{5} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$. Tomamos $w^3 = 1$, w es raíz cúbica primitiva de 1 para resolver $x^3 - 5 = 0$: $\sqrt[3]{5}$, $\sqrt[3]{5}w$, $\sqrt[3]{5}w^2$.
$\mathbb{Q}[X]/(x^3 - 5) = \mathbb{Q}(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2 : a, b, c \in \mathbb{Q}\}$, con base $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$

Ejemplo 10. $\sqrt{5} + 1 \in \mathbb{R}$, $x = \sqrt{5} + 1 \Rightarrow x - 1 = \sqrt{5} \Rightarrow x - 2x - 4$ irreducible.

Ejemplo 11. $e^{2\pi i/7} \in \mathbb{C}$, es la expresión de las raíces séptimas de la unidad, $x^7 - 1$. No es irreducible porque $x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$. El segundo factor es el 7-ésimo polinomio ciclotómico, que es irreducible sobre $\mathbb{Q}$ por ser 7 primo.

Definición 32 (Polinomio irreducible sobre F)**.** Sea E/F cuerpo. Sea $\alpha \in E$ algebraico sobre F. El **polinomio irreducible** o mínimo sobre F es $Irred(\alpha; F)$ es el único polinomio de F[X] mónico e irreducible que tiene a α como raíz (coincide con el poliniomio del Teorema II.6.1). Así

$$F[X]/(p(x)) \cong F(\alpha) = \{a_0 + a_1\alpha + ... + a_{d-1}\alpha^{d-1} : a_i \in F \ \forall i = 0, ..., d\}$$

Definición 33 (Cuerpo primo). Dado F cuerpo el **cuerpo primo** de F es el mínimo subcuerpo de F, es la intersección de todos los subcuerpos de F.

Observación: Todo cuerpo es extensión de su cuerpo primo.

Proposición II.7. Sea F cuerpo, E cuerpo primo de F es isomorfo a $\mathbb{Q}$ o a $\mathbb{F}_p$ para algún primo p.

Demostración: $\psi : \mathbb{Z} \to F, 1 \to 1$. ψ es homomorfismo de acu. Por el primer teorema de isomorfía $\mathbb{Z}/Ker(\psi) \approxeq Im(\psi)$. También, $Im(\psi)$ es un subanillo de F. Como F es cuerpo $\Rightarrow$ $Im(\psi)$ es un dominio $\Rightarrow$ $Ker(\psi)$ es un ideal primo de $\mathbb{Z}$ $\Rightarrow$ $Ker(\psi) = (0)$ o $Ker(\psi) = (p)$ con p primo. Si $Ker(\psi) = (0) \Rightarrow \psi$ es inyectiva. $\mathbb{Z} \approxeq Im(\psi) \subseteq F \Rightarrow \mathbb{Q} = cf(\mathbb{Z}) \approxeq cf(Im(\psi)) \subseteq F$. Por lo tanto, F tiene un subcuerpo isomorfo a $\mathbb{Q}$ y es mínimo. Si $Ker(\psi) = (p) \Rightarrow \mathbb{Z}/(p) \approxeq \mathbb{F}_p \approxeq Im(\psi) \subseteq F$. Por lo tanto, F tiene un subcuerpo isomorfo a $\mathbb{F}_p$ y es mínimo.

Definición 34 (Característica de un cuerpo). Sea F cuerpo.
Si $\mathbb{Q}$ es el cuerpo primo de $F \Rightarrow ch(F) = 0$.
Si $\mathbb{F}_p$ es el cuerpo primo de $F \Rightarrow ch(F) = p$.

Observación: Sea F cuerpo, $ch(F) = p$, $a, b \in F \Rightarrow (a+b)^p = a^p + b^p$.

Demostración: $(a+b)^p = a^p + \sum_{i=1}^{p} \binom{p}{i} a^i b^{p-i} + b^p$ donde $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ para $1 \leqslant i \leqslant p-1$. Por lo tanto, $p|\binom{p}{i}$ $\forall i = 1, ..., p-1$. Como $ch(F) = p \Rightarrow F/\mathbb{F}_p$.
$\sum_{i=1}^{p} \binom{p}{i} a^i b^{p-i} = 0$.

Demostremos por inducción que $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. Para el caso base $n = 1$ es cierto. Supongamos que es cierto para n.
Para $n+1$: $(a+b)^{p^{n+1}} = ((a+b)^{p^n})^p = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}$ es cierto también, por la hipótesis de inducción.

Observación: $ch(\mathbb{F}_p(X)) = p$.

Ejemplo 12. Por el ejemplo 6 sabemos que $x^2 + 1 \in \mathbb{F}_3[X]$, $x^2 + 1 = Irred(\alpha, \mathbb{F}_3)$. Denotamos $\mathbb{F}_3(\alpha) \approxeq \mathbb{F}_3[X]/(x^2+1)$ al cuerpo con $\alpha^2 + 1 = 0$. También sabemos que $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 2$ por lo que $\mathbb{F}_3(\alpha) \approxeq \mathbb{F}_3 \times \mathbb{F}_3$. Como la base de $\mathbb{F}_3(\alpha)$ es $\{1, \alpha\}$, $\mathbb{F}_3(\alpha) = \{a + b\alpha : a, b \in \mathbb{F}_3\}$. Tenemos que $|\mathbb{F}_3(\alpha)| = 9$.

Observación: Todo cuerpo finito tiene p^k elementos para algún primo p y algún $k > 0$.

Demostración: Sea F finito $F/\mathbb{F}_p$ para algún p primo. F es un $\mathbb{F}_p - ev$ de dimensión finita. Sea $n = \dim_{\mathbb{F}_p} F$ por lo tanto $F \approxeq \mathbb{F}_p \times ...^{(n-2)} \times \mathbb{F}_p$. $|F| = |\mathbb{F}_p \times ...^{(n-2)} \times \mathbb{F}_p| = p^n$.

Teorema II.8. Para cada p primo y $n \in \mathbb{N}^*$ existe un cuerpo de p^n elementos.

Demostración: F cuerpo con $|F| = p^n = q$. F^* es grupo multiplicativo, $|F^*| = q-1$. $\forall a \in F^*$, $a^{q-1} = 1$. $\forall a \in F$ a es raíz de $x^q - x \in \mathbb{F}_p[X]$, $x^q - x = x(x^{q-1} - 1)$.

Sea $g(x) = x^q - x \in \mathbb{F}_p[X]$. Por el Teorema de Kronecker existe $E/\mathbb{F}_p$ donde g se descompone.

Sea $F := \{\alpha \in E : g(\alpha) = 0\}$. Veamos si $g(x)$ tiene raíces múltiples.
$g'(x) = qx^{q-1} - 1 = p^n x^{p^n - 1} - 1 = -1$, $mcd(g(x), g'(x)) = 1$. Por la propiedad 5 de raíces de polinomios, g no tiene raíces múltiples. Así, $|F| = q$. Veamos que F es cuerpo. $0, 1 \in F \Rightarrow -\alpha \in F$, $(-\alpha)^q = (-1)^q \alpha$. Si q es impar $(-\alpha)^q = -\alpha$, si q es par $(-\alpha)^q = \alpha = -\alpha \Leftrightarrow p = 2$.

$\alpha, \beta \in F$, entonces $(\alpha+\beta)^q = (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. $(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta$. Si $\alpha \neq 0$, $\alpha^{q-1} \Rightarrow \alpha^{-1} = \alpha^{q-2} \in F$. F es cuerpo y $|F| = q = p^n$.

Ejemplo 13. $|F| = 4 = 2^2$, $x^4 - x \in \mathbb{F}_2[X]$. $\mathbb{F}_2$ es cuerpo primo de F, $\dim_{\mathbb{F}_2} F = 2$, $\{1, \alpha\}$ es base de $F/\mathbb{F}_2$.

$F = \{a + b\alpha : a, b \in \mathbb{F}_2\} = \{0, 1, \alpha, \alpha+1\}$. Así, $\alpha^2 = \alpha + 1$. Tenemos que $1 + \alpha + \alpha^2 = 0$.

Descomponemos $x^4 - x \in \mathbb{F}_2[X]$. $x^4 - x = x(x-1)(x^2+x+1)$. $1 + x + x^2$ es irreducible en $\mathbb{F}_2$. Entonces, $F = \mathbb{F}_2[X]/(x^2+x+1)$ es cuerpo de extensión de $\mathbb{F}_2$. Sea $\alpha = x + (x^2+x+1)$ raíz de $t^2 + t + 1 \in F[T]$. La tabla multiplicativa de los elementos de F es:

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Ejemplo 14. $|F| = 8 = 2^3$, $x^8 - x \in \mathbb{F}_2[X]$. $x^8 - x = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x(x-1)(x^3+x+1)(x^3+x^2+1)$.

$F = \mathbb{F}_2[X]/(x^3+x+1)$, $[F : \mathbb{F}_2] = gr(x^3+x+1) = 3$. $\alpha = x + (x^3+x+1)$. La base de F como $\mathbb{F}_2 - ev$ es $\{1, \alpha, \alpha^2\}$, por lo que $F = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{F}_2\}$. $\alpha^3 = 1 + \alpha$.

Proposición II.9. (Fórmula de los grados) Sea $F \subset B \subseteq E$ extensiones de cuerpos, con $[E : B] = m$ y $[B : F] = n$ finitas. Entonces E/F es finita y $[E : F] = mn$.

$$[E : F] = [E : B][B : F]$$

Demostración: Sea $\{\alpha_1, ..., \alpha_n\}$ base de E como $B-ev$. Sea $\{\beta_1, ..., \beta_n\}$ base de B como $F-ev$. Basta demostrar que $\{\alpha_i\beta_j : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n\}$ es base de E como F-ev.

Veamos que son linealmente independientes:
$0 = \sum_{(i,j)=(1,1)}^{(m,n)} a_{ij}\alpha_i\beta_j = \sum_{i=1}^{m}(\sum_{j=1}^{n} a_{ij}\beta_j)\alpha_i$ donde $\alpha_i \in F$, $\beta_j \in B \Rightarrow \sum_j^n a_{ij}\beta_j \in B$.

Como los α_i son linealmente independientes para todo $i = 1, ..., m$, $\sum_j^n a_{ij}\beta_j = 0$, $a_{ij} \in F$ y los β_j son linealmente independientes para todo $j = 1, ..., n \Rightarrow a_{ij} = 0$.

Veamos que generan los elementos de E. Sea $\gamma \in E$, entonces $\exists a_i \in B$ tal que $\gamma = \sum_{i=1}^{m} b_i\alpha_i$. Para cada $i = 1, ..., m$ $\exists c_{ij} \in E$ tal que $b_i = \sum_{j=1}^{n} c_{ij}\beta_j$. Así, podemos escribir $\gamma = \sum_{i=1}^{m}(\sum_{j=1}^{n} c_{ij})\beta_j\alpha_i = \sum_{(i,j)=(1,1)}^{(m,n)} c_{ij}\alpha_i\beta_j$.

Ejemplo 15. Calculemos $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$. Sabemos que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] =$
$gr(Irred(\mathbb{Q}(\sqrt{2}))) * gr(Irred(\sqrt{3}, \mathbb{Q}(\sqrt{2}))) = 2 * 2 = 4$ porque:

$Irred(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$. Veamos que no tiene raíces en $\mathbb{Q}(\sqrt{2})$.
$a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2} = 3$, $\sqrt{2} = \frac{3-a^2+2b^2}{2ab}$ si $ab \neq 0$ es imposible, $\sqrt{2} \notin \mathbb{Q}$. Si $a = 0$ $2b^2 = 3$, imposible porque $b \in \mathbb{Q}$. Si $b = 0$ $a^2 = 3$, imposible porque $a \in \mathbb{Q}$. Por lo tanto, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

Hoja 2

1. Sean $f(X), g(X) \in F[X]$. Demuestra que $(f(X), g(X)) \neq 1 \Leftrightarrow \exists$ un cuerpo conteniendo a F y a una raíz común de f(X) y g(X).

   ($\rightarrow$) Sean $f(X), g(X) \in F[X]$ tales que $(f(X), g(X)) = d(X) \in F[X] \setminus F \Rightarrow d(X)|f(X)$ y $d(X)|g(X)$. Por el **Teorema de Kronecker**, existe E/F en la cual $d(X)$ se descompone. Así, f(X) y g(X) comparten una raíz en el cuerpo E del polinomio d(X).

   ($\leftarrow$) Sea E/F, $\alpha \in E$, $f(\alpha) = g(\alpha) = 0$. Sea $p(X) = \mathrm{Irred}(\alpha; F) \in F[X]$.
   $gr(p(X)) < gr(f(X))$, entonces podemos escribir $f(X) = q(X)p(X) + r(X)$, donde $gr(r(X)) < gr(p(X))$. f(X) tiene a α como raíz, luego $0 = f(\alpha) = r(\alpha) \Rightarrow r(X) = 0$ por lo tanto $p(X)|f(X)$ en F[X]. Análogamente para $g(X)$, tenemos que $p(X)|g(X)$ en F[X]. Así, $(f(X), g(X)) \neq 1$.

2.

3. Demuestra que un cuerpo de 8 elementos no puede ser extensión de un cuerpo de 4 elementos.

   Sea E cuerpo tal que $|E| = 8 = 2^3$ y F cuerpo tal que $|F| = 4 = 2^2$. E y F tienen como cuerpo primo a $\mathbb{F}_2$. Entonces, $E/\mathbb{F}_2$, $F/\mathbb{F}_2$ porque todo cuerpo es extensión de su cuerpo primo, y además, son extensiones finitas por ser E y F cuerpos finitos. Suponiendo que E/F, entonces, por la fórmula de los grados, tenemos que $[E : \mathbb{F}_2] = [E : F][F : \mathbb{F}_2] \Rightarrow [E : F] = \frac{[E:\mathbb{F}_2]}{[F:\mathbb{F}_2]} = \frac{3}{2} \notin \mathbb{N}$. Por tanto, E no es extensión de F.

   Hay otras formas de justificarlo. No existen homomorfismos de grupos en $|E^*| = 3$, $|K^*| = 7$. También, no existe F $\mathbb{F}_2 - ev$ subespacio del E $\mathbb{F}_2 - ev$.

4. Da las tablas de adición y de multiplicación de un cuerpo con 9 elementos.

   Sea F cuerpo tal que $|F| = 9 = 3^2$. Tenemos que $\mathbb{F}_3$ es el cuerpo primo de F. Busquemos una extensión $F/\mathbb{F}_3$ tal que $[F : \mathbb{F}_3] = 2$ y para formarla, un polinomio irreducible de grado 2 en $\mathbb{F}_3$: $x^2 + 1$.

   $x^2 + 1$ es irreducible porque no tiene raíces en $\mathbb{F}_3$ y es de grado $2 \Rightarrow (x^2 + 1)$ es un ideal maximal $\Rightarrow F := \mathbb{F}_3/(x^2 + 1)$ es un cuerpo y por tanto, una extensión. Sea $\alpha \in \mathbb{F}_3$ raíz de $x^2 + 1 \Rightarrow \alpha^2 + 1 = 0 \Rightarrow \alpha^2 = 2$. La base de F como $\mathbb{F}_3 - ev$ es $\{1, \alpha\}$.

   $F = \{a + b\alpha : a, b \in \mathbb{F}_3\} = \{0, 1, 2, \alpha, 2\alpha, \alpha + 1, \alpha + 2, 2\alpha + 1, 2\alpha + 2\}$. Sabiendo que $\alpha^2 = 2$ y los elementos del cuerpo, ya podemos formar las tablas de adición y multiplicación.

5.

6.

7. Sea E/F y sean $\alpha, \beta \in E$ algebraicos sobre F con $\alpha \neq 0$. Demuestra que $\alpha + \beta$ y α^{-1} son algebraicos sobre F.

   Por la fórmula de los grados, $[F(\alpha\beta) : F] = [F(\alpha\beta) : F(\beta)][F(\beta) : F]$. Como α es algebraico en $F \Rightarrow \alpha$ es algebraico sobre $F(\beta) \Rightarrow [F(\alpha, \beta) : F(\beta)]$ es finito. Así, $[F(\alpha\beta) : F]$ es finito.

   Para el caso $\beta = \alpha^{-1}$ tenemos que $F(\alpha^{-1}) = F(\alpha)$ y $[F(\alpha^{-1}) : F]$ es finito, por lo que α^{-1} es algebraico en F.

   $\alpha + \beta \in F(\alpha, \beta)$ y $[F(\alpha, \beta)]$ es finita. $F \subseteq F(\alpha + \beta) \subseteq F(\alpha, \beta) \Rightarrow [F(\alpha + \beta) : F]$ es finito, $F(\alpha, \beta)$ es un F-ev de dimensión finita sobre F.

8.

9.

10. Sea F un cuerpo finito. Demuestra que F es algebraico sobre su cuerpo primo.

    Un cuerpo primo, P, es el mínimo subcuerpo de F, $P \subset F$. Así, F es extensión de su cuerpo primo. Como F es finito, F/P es una extensión finita, es decir, $[F : P] = \dim_P F = n < \infty$ (dimensión de F como P-ev) $\Rightarrow F/P$ es algebraica, por la proposición II.5.

    $(P \approx \mathbb{Q}$ o $P \approx \mathbb{F}_p)$

11. Sean B y E extensiones de F con $B \subseteq E$ y $[E : F]$ finita. Demuestra que ambas E/B y B/F son finitas y que $[E : F] = [E : B][B : F]$.

    Sea $[E : F] = n < \infty$. Como B es extensión de F y $B \subseteq E$, entonces, B es un F-subespacio de E, (E es un F-ev por ser E/F). Entonces, tenemos que $[B : F] < n$. Por tanto, B/F es finita.

    También, como $[E : F] = n < \infty$, $\exists \{\alpha_1, ..., \alpha_n\}$ base de E sobre $F \Rightarrow \{\alpha_1, ..., \alpha_n\}$ genera E como B-ev. $\dim_B E = [E : B] \leqslant n$.

    Ahora podemos aplicar la fórmula de los grados para obtener la igualdad.

2.2. Cuerpos de descomposición

Definición 35 (Cuerpo de descomposición). Sea F cuerpo y $f(X) \in F[X]$. Un **cuerpo de descomposición** (c. de d.) de f(x) sobre F es una E/F tal que f(X) se descompone en E y no existe otro cuerpo E_1, $F \subseteq E_1 \subseteq E$ tal que f se descompone en E.

Ejemplo 16. $x^2-2 \in \mathbb{Q}[X]$, $\mathbb{Q} \subset \mathbb{C}$. $\mathbb{Q}(\sqrt{2})$ es c. de d. de x^2-2;
$x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.

Ejemplo 17. $x^3-1 \in \mathbb{Q}[X]$, $w = e^{2\pi i/3}$,
$x^3-1 = (x-1)(x^2+x+1) = (x-1)(x-w)(x-\overline{w}) = (x-1)(x-w)(x-w^2)$

Ejemplo 18. $x^n-1 \in \mathbb{Q}[X]$ $x^n-1 = (x-1)(x-w)(x-w^2)(...)(x-w^{n-1})$ donde $w = e^{2\pi i/n}$ es la raíz n-ésima primitiva de 1. $\mathbb{Q}(w)$ es c. de d. de x^n-1.

Ejemplo 19. $x^n-a \in \mathbb{Q}[X]$. $x^n-a = a[(\frac{x}{\sqrt[n]{a}})^n-1] = a(\frac{x^n}{a}-1)$ $\sqrt[n]{a} \in \mathbb{R}$.

$y := \frac{x}{\sqrt[n]{a}}$, $w = e^{2\pi i/n}$ $\quad a(y^n-1) = a(y-1)(y-w)...(y-w^{n-1})$
$x^n-a = a(\frac{x}{\sqrt[n]{a}}-1)(\frac{x}{\sqrt[n]{a}}-w)...(\frac{x}{\sqrt[n]{a}}-w^{n-1}) = (x-\sqrt[n]{a})(x-\sqrt[n]{a}w)...(x-\sqrt[n]{a}w^{n-1})$

$\sqrt[n]{a} \in E$, $\sqrt[n]{a}w \in E \Rightarrow w = \frac{\sqrt[n]{a}w}{\sqrt[n]{a}} \in E$. Así, $\mathbb{Q}(\sqrt[n]{a}, w)$ es c. de d. de x^n-a.

Corolario (al teorema de Kronecker). Todo polinomio sobre un cuerpo tiene un cuerpo de descomposición.

Demostración: Sea F cuerpo y $f(X) \in F[X]$. Por el Teorema de Kronecker existe E/F donde f(X) se descompone. Sean $\alpha_1, ..., \alpha_s \in E$ raíces de f en E. Entonces $F(\alpha_1, ..., \alpha_s)$ es un cuerpo de descomposición de $f(X) \in F[X]$, donde $f(X) = \prod_{j=1}^{s}(x-\alpha_i)^{n_i}$ y f se descompone en $F(\alpha_1, ..., \alpha_s)$.

Si E_1/F y f se descompone en E_1 entonces $\alpha_1, ..., \alpha_s \in E_1$ y como $F(\alpha_1, ..., \alpha_s)$ es el mínimo cuerpo que contiene a F y a las raíces α_i, $F(\alpha_1, ..., \alpha_s) \subseteq E_1$.

Observación: Sea $f(X) \in F[X]$ y sea E un cuerpo de descomposición de f(X) $\Rightarrow [E : F]$ es finita.

Demostración: $E = F(\alpha_1, ..., \alpha_s)$ donde α_i son raíces de f.
$[E : F] = [F(\alpha_1, ..., \alpha_s) : F(\alpha_1, ..., \alpha_{s-1})][F(\alpha_1, ..., \alpha_{s-1}) : F(\alpha_1, ..., \alpha_{s-2})]...[F(\alpha_1) : F]$
Cada α_i es raíz de $f(X) \in F[X]$ por lo que α_i es algebraico sobre F. Luego, α_i es algebraico sobre $F(\alpha_1, ..., \alpha_{i-1})$. Por lo tanto, $[F(\alpha_1, ..., \alpha_i) : F(\alpha_1, ..., \alpha_{i-1})]$ es finita. Así, $[E : F]$ es producto de grados finitos. Luego [E:F] es finito.

Definición 36 (Polinomio separable)**.** Sea F cuerpo.

1. Sea $p(X) \in F[X]$ irreducible. $p(X)$ es **separable** si no tiene raíces múltiples.
2. Sea $f(X) \in F[X]$. $f(X)$ es **separable** si $f(X) \in F$, es decir, es constante, o $\forall p(X) | f(X)$, $p(X)$ es un polinomio irreducible y separable.

Ejemplo 20. $x-2, (x-2)^2 \in \mathbb{Q}[X]$ son separables.

Ejemplo 21. $x^2+1 \in \mathbb{Q}[X]$ es separable porque no tiene raíces múltiples porque $(x^2+1, 2x) = 1$.

Ejemplo 22. $x^2+x+1 \in \mathbb{F}_2[X]$ es irreducible y $(x^2+x+1, 2x+1) = 1$, luego es separable.

Ejemplo 23. $x^p - 1 \in \mathbb{F}_p[X]$ no es separable porque $(x^p - 1, px^{p-1}) \neq 1$.

Observación: Sea F cuerpo con $ch(F) = 0 \Rightarrow$ todo polinomio es separable.

Demostración: Sea $f(X) \in F[X]$. Si f(X) es una constante es separable. Si $f(X) \notin F$, sea $q(X)|f(X)$, con $q(X)$ irreducible. Veamos que q(X) no tiene raíces múltiples, $(q, q') = 1$.

Como la $ch(F) = 0 \Rightarrow q'(X) \neq 0$, por lo tanto, $gr(q') < gr(q) \Rightarrow (q(X), q'(X)) \neq q(X)$. q(X) es irreducible $\Rightarrow (q(X), q'(X)) = 1$.

Observación: Sea F cuerpo con $ch(F) = p$ y $q(X) \in F[X]$ irreducible. q(X) es separable $\Leftrightarrow q'(X) \neq 0$.

Demostración: $(\rightarrow)$ Sea q(X) separable y supongamos que $q'(X) = 0$. Entonces $(q(X), q'(X)) = q(X) \neq 1$ por lo que $q(X)$ tiene raíces múltiples.

$(\leftarrow)$ Si $q'(X) \neq 0 \Rightarrow gr(q'(X)) < gr(q(X))$, $(q, q') = 1$ ya que q es irreducible y q no divide a q'.

Definición 37 (Extensión separable. Cuerpo perfecto)**.** Sea F cuerpo y E/F.

1. $\alpha \in E$ es **separable sobre F** si α es transcendente sobre F o $Irred(\alpha, F)$ es separable.
2. E es una **extensión separable de F** si $\forall \alpha \in E$ α es separable en F.
3. F es **perfecto** si todo $f(X) \in F[X]$ es separable.

Lema II.10. F cuerpo con $ch(F) = p$ primo, $n \in \mathbb{N}^*$, $a \in F$. Entonces $x^{p^n} - a$ es irreducible sobre $F \Leftrightarrow a \notin F^p = \{b^p : b \in F\}$.

Demostración: ($\rightarrow$) Si $a \in F^p \Rightarrow a = b^p$ para algún $b \in F$ por lo tanto $x^{p^n} - a = x^{p^n} - b^p = (x^{p^{n-1}} - b)^p$ por lo tanto, $x^{p^n} - a$ es reducible.

($\leftarrow$) Supongamos $x^{p^n} - a$ reducible. Sea E/F y $\alpha \in E$, α raíz de $x^{p^n} - a \Rightarrow \alpha^{p^n} = a$. $x^{p^n} - a \in E[X]$, $f(x) = (x - \alpha)^{p^n}$. Sea $g(x) \in F[X]$, factor irreducible propio de f(X) en $E[X] \Rightarrow g(x)|(x - \alpha)^{p^n}$.

Como $E[X]$ es un DFU $\Rightarrow g(x) = (x - \alpha)^m$ para algún $1 \leqslant m \leqslant p^n$. $g(0) = -\alpha^m \in F$ $\Rightarrow \alpha^m \in F \Rightarrow g(x) \in F[X]$.

$d = (m, p^n) \Rightarrow d = p^k$ para algún $0 \leqslant k < n$, $p^k = ml + p^n s$, $l, s \in \mathbb{Z}$ por la igualdad de Bezout. $\alpha^{p^k} = (\alpha^{p^m})^l (\alpha^{p^n})^s \in F$, $\alpha^{p^{n-1}} = (\alpha^{p^k})^{p^{n-1-k}} \in F$, $a = \alpha^{p^n} = (\alpha^{p^{n-1}})^p \in F^p$

Observación: $x^p - t \in (\mathbb{F}_p(t))[X]$ es irreducible.

Demostración: $\sqrt[p]{t} \notin \mathbb{F}_p(t)$, $\sqrt[p]{t} \neq \frac{f(t)}{g(t)}$, $f(t), g(t) \in \mathbb{F}_p[t]$ son coprimos por ser $\mathbb{F}_p[t]$ DFU. $t(g(t))^p = (f(t))^p \Rightarrow t|(f(t))^p \Rightarrow t|f(t)$.

Teorema II.11. F es perfecto $\Leftrightarrow$ $ch(F) = 0$ o $ch(F) = p$ y $F = F^p$.

Demostración: ($\rightarrow$) Sea F perfecto. Si $ch(F) = 0$ queda demostrado. Veamos si $ch(F) = p$. Sea $a \in F \setminus F^p$, $q(x) = x^p - a$ es irreducible por el Lema 10. $q'(x) = 0$ por lo tanto q(x) no es separable. Obtenemos una contradicción con la hipótesis de que F es un cuerpo perfecto.

($\leftarrow$) $ch(F) = 0 \Rightarrow$ F es un cuerpo perfecto (por la observación). Supongamos $ch(F) = p$ y $F = F^p$. Sea $q(x) \in F[X]$ podemos suponer que $q(x)$ es irreducible. Veamos que q(x) es separable. $q(x) = \sum_i a_i x^i$, $q'(x) = \sum_i i a_i x^{i-1}$. Supongamos $q'(x) = 0$, $ia_i = 0$, $\forall i \Rightarrow p \nmid i \Rightarrow a_i = 0$.

$q(x) = \sum_j a_{jp} x^{jp} = \sum_j b_{jp}^p x^{jp} = (\sum b_{jp} x^j)^p$ por lo tanto q(x) es reducible.

Corolario: Todo cuerpo finito es perfecto.

Demostración: F finito $\Rightarrow ch(F) = p$ para algún p. Por el automorfismo de Frobenius $\sigma_p : F \to F, a \to a^p$, $F = \sigma_p(F) = F^p \Rightarrow$ F es perfecto (por el teorema).

Lema II.12. Sea $\sigma : F_1 \to F_2$ isomorfismo de cuerpos. Sea $\sigma^* : F_1[X] \cong F_2[X]$ isomorfismo de a.c.u. inducido por σ. Sea $p(x) \in F_1[X]$ irreducible y sea $p^*(x) := \sigma^*(p(x))$ irreducible. Sea α una raíz de $p(x)$ y β raíz de $p^*(x)$. Entonces existe un único isomorfismo $\tilde{\sigma} : F_1 \to F_2(\beta)$ tal que $\tilde{\sigma}|_{F_2} = \sigma$, $\tilde{\sigma}(\alpha) = \beta$.

Demostración: Unicidad: $\tilde{\sigma}$ está determinada conociendo $\tilde{\sigma}|_{F_1}$ y $\tilde{\sigma}(\alpha)$.

Existencia: $F_1(\alpha) \xrightarrow{\psi_1^{-1}} F_1[X]/(p(x)) \xrightarrow{\tilde{\sigma}} F_2[X]/(p^*(x)) \xrightarrow{\psi_2} F_2(\beta)$, donde ψ_i y $\tilde{\sigma}^*$ son isomorfismos por el Teorema II.6 y por propiedades de anillos cocientes respectivamente. $\psi_1^{-1}|_{F_1} = id_{F_1}$, $\tilde{\sigma}^*|_{F_1} = \sigma^*$, $\psi_2^{-1}|_{F_2} = id_{F_2}$. $\alpha \to x + p(x) \to x + (p^*(x)) \to \beta$, $\tilde{\sigma}(\alpha) = \beta$.

Teorema II.13. Sea $\psi : F_1 \to F_2$ isomorfismo de cuerpos. Sea $f(x) \in F_1[X]$ y $f^*(x) := \psi^*(f(x))$ (ψ^* isomorfismo inducido por ψ). Sean E_1/F_1 y E_2/F_2 cuerpos de descomposición de f y f^* respectivamente. Entonces:

1. Existe $\tilde{\psi} : E_1 \to E_2$ isomorfismo tal que $\tilde{\psi} \supseteq \psi$.
2. Si f es separable existe exactamente $[E_1 : F_1]$ isomorfismos de E_1 en E_2 extendiendo ψ.

Demostración: E_1/F_1 es c. de d. por lo que $[E_1 : F_1]$ finita. Por inducción sobre $n = [E_1 : F_1]$:
$n = 1 \Rightarrow E_1 = F_1 \Rightarrow E_2 : F_2 \Rightarrow \psi = \tilde{\psi}$.
$n > 1$. Existe $q(x)|f(x)$ tal que $q(x) \in F_1[X]$ irreducible, $gr(q(x)) \geqslant 2$. Sea $q^* = \psi^*(q(x))$ (irreducible porque $gr(q^*) = d$). Sea α raíz de $q(x)$ en E_1. Para cada β raíz de $q^*(x)$ en E_2 existe, por el lema, un único $\psi_\beta : F_1(\alpha) \xrightarrow{\cong} F_2(\beta)$ que extiende ψ. Sean $f(x) \in F_1(\alpha)[X]$, $f^*(x) \in F_2(\beta)[X]$. $E_1/F_1(\alpha)$ y $E_2/F_2(\beta)$ cuerpos de descomposición de f y f^* respectivamente. Por la fórmula de los grados

$$[E_1 : F_1(\alpha)] = \frac{[E_1:F_1]}{[F_1(\alpha):F_1]} = \frac{n}{d} < n$$

Por hipótesis de inducción, $\exists \tilde{\psi} \supseteq \psi_\beta \supseteq \psi$, $E_1 \xrightarrow{\cong} E_2 \Rightarrow$ queda demostrado (1).

Si f es separable y $f = gq \Rightarrow g$ y q son separables de $F_1[X] \Rightarrow q^*(x)$ es separable. Por lo tanto, q^* tiene d raíces distintas, $\{\beta_1, ..., \beta_d\}$.
Para cada β_i existe un único $\psi_{\beta_i} : F_1(\alpha) \xrightarrow{\cong} F_2(\beta_i)$, $\psi_{\beta_i} \supseteq \psi$ y para cada $\psi_{\beta_i} : F_1(\alpha) \xrightarrow{\cong} F_2(\beta_i)$.

Tenemos $g(x) \in F_1(\alpha)[X]$ y $g^*(x) \in F_2(\beta_i)[X]$, $E_1/F_1(\alpha)$ y $E_2/F_2(\beta_i)$ cuerpos de descomposición de g y g^*, respectivamente.

Además, g es separable y $[E_1 : F_1(\alpha)] = \frac{n}{d} < n$. Por hipótesis de inducción existen exactamente $\frac{n}{d}$ extensiones de ψ_{β_i} (que son isomorfismos entre E_1 y E_2), por lo tanto, en total hay n extensiones de ψ (isomorfismo de $E_1 \cong E_2$).

Corolario 1: Sea F cuerpo y $f(x) \in F[X]$. Entonces existe un único (salvo isomorfismos) cuerpo de descomposición de f.

Demostración: F cuerpo $f(x) \in F[X]$, $id : F \to F$. Sean E_1/F y E_2/F cuerpos de descomposición de f. Por el teorema II.13, la aplicación identidad se extiende a un isomorfismo de $E_1 \cong E_2$.

Corolario 2: Para cada p primo y $n > 0$ existe un único cuerpo (salvo isomorfismo) de p^n elementos.

Demostración: Sea $|F| = p^n$. Sabemos que existe al menos un cuerpo (por el teorema II.8), además, por su demostración sabemos que F es un cuerpo de descomposición de $x^{p^n} - x \in \mathbb{F}_p[X]$. Por el corolario 1, F es único salvo isomorfismos.

3. Teoría de Galois

3.1. Grupo de Galois

Definición 38 (Grupo de Galois)**.** Sea E/F extensión de cuerpo $(F \subseteq E)$.

1. Un **F-automorfismo de E** es un $\sigma \in Aut(E)$ de cuerpos tal que $\sigma|_F = id_F$.
2. El **grupo de Galois** de E/F es: $\mathbf{Gal(E/F)} = \{\boldsymbol{\sigma \in Aut(E) : \sigma|_F = id_F}\}$.
3. Sea $f(x) \in F[X]$ y sea E cuerpo de descomposición de f sobre $F[X]$. El **grupo de Galois de f** (sobre F) es: $Gal(f) := Gal(E/F)$.

Observación:

1. E cuerpo $\Rightarrow Aut(E)$ es un grupo.
2. $Gal(E/F) \leqslant Aut(E)$.
3. $\sigma \in Aut(E)$, E cuerpo $\sigma|_F = id_F$ para F cuerpo primo de E.
   $E/\mathbb{Q} : \sigma(1) = 1 \Rightarrow \sigma|_{\mathbb{Z}} = id_{\mathbb{Z}} \Rightarrow \sigma|_{\mathbb{Q}} = id_{\mathbb{Q}}$.
   $E/\mathbb{F}_p : \sigma(1) = 1 \Rightarrow \sigma|_{\mathbb{F}_p} = id_{\mathbb{F}_p}$.

Ejemplo 24. $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$, porque:
$\alpha = \sqrt[3]{2} \Rightarrow \sigma(\alpha^3) = \sigma(2) = 2 \Rightarrow \sigma(\alpha)^3 = 2 \Rightarrow \sigma(\alpha) = \alpha$

Ejemplo 25. $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \sigma\}$ donde $\sigma(\sqrt{2}) = -\sqrt{2}$, porque:
$\alpha = \sqrt{2} \Rightarrow \alpha^2 = 2 \Rightarrow \sigma(\alpha^2) = 2 \Rightarrow \sigma(\alpha)^2 = 2 \Rightarrow \sigma(\alpha) = \pm 2$

Lema III.1. Sea $f(x) \in F[X]$, E/F extensión, $\alpha \in E$. Sea $\sigma \in Gal(E/F)$, $f(\alpha) = 0 \Rightarrow f(\sigma(\alpha)) = 0$.

Demostración: $f(x) = \sum a_i x^i \in F[X]$, $\sigma \in Aut(E)$, $\sigma|_F = id_F$.
$f(x) = 0 \Rightarrow \sigma(f(\alpha)) = 0 \Rightarrow \sum a_i \sigma(x)^i = 0$ por lo tanto, $\sigma(\alpha)$ es raíz de f en E.

Observación: E/F extensión, $\alpha_1, ..., \alpha_n \in E$. Entonces

1. $\sigma \in Gal(F(\alpha_1, ..., \alpha_n)/F)$ y $\sigma(\alpha_i) = \alpha_i \ \forall i \in 1, ..., n \Rightarrow \sigma = id$.
2. Sean $\sigma, \tau : F(\alpha_1, ..., \alpha_n) \to E$ homomorfismos tales que $\sigma(a) = \tau(a) \ \forall a \in F$, $\sigma(\alpha_i) = \tau(\alpha_i) \ \forall i = 1, ..., n \Rightarrow \sigma = \tau$.

Teorema III.2. Sea F cuerpo, $f(x) \in F[X]$ y E cuerpo de descomposición de E/F. Entonces:

1. Si f tiene n raíces y se descompone en E $\Rightarrow Gal(f) \approxeq H \leqslant S_n$. En particular, $|Gal(f)|$ divide a $n!$.
2. Si f es separable, $|Gal(f)| = [E : F]$.

Demostración: (1) $Gal(f) = Gal(E/F)$. Sea $x = \{\alpha_1, ..., \alpha_n\}$ raíces de f en E, $E = F(\alpha_1, ..., \alpha_n)$. $\sigma \in Gal(E/F) \to \sigma|_\alpha \in BiyX$. $Gal(E/F) \to BiyX, \sigma \to \sigma|_X$. Por la observación, $\sigma \to \sigma|_X$ es inyectiva y homomorfismo. $Gal(E/F) \approxeq H \leqslant BiyX$, $Gal(f) = Gal(E/F) \approxeq H \leqslant S_n$, $|X| = n \to BiyX \approxeq S_n$.

(2) $|Gal(f)| = \{\sigma : E \to E : \sigma$ automorfismo y $\sigma \approxeq id_F\}$. Por el teorema II.13 f es separable, E/F es cuerpo de descomposición de $f|_F \Rightarrow$ existen exactamente $[E : F]$ isomorfismos de $id_F : F \to F$ automorfismos de E, $|Gal(f)| = [E : F]$.

Observación: f separable y E cuerpo de descomposición de $f|_F$. $|Gal(E/F)| = [E : F]$.

Corolario: Sea $p(x) \in F[X]$ irreducible. E/F cuerpo de descomposición de $p(x)|_F$, $d = gr(p(x))$. Entonces

1. $d|[E : F]$
2. p es separable $\Rightarrow d| \, |Gal(f)|$

Demostración: (1)$d = gr(p(x))$, $[F(x) : F] = d$. Sea α raíz de $p(x)$ en E, $F(\alpha) \subseteq E$, $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, $d|[E : F]$.

(2) por la parte (2) del teorema.

Ejemplo 26. (IMPORTANTE) $x^3 - 5 \in \mathbb{Q}[X]$. Hallamos $Gal(x^3 - 5)$. Denotamos w como la raíz cúbica primitiva de F en C, cumple que $w^2 + w + 1 = 0$.
$x^3 - 5 = (x - \sqrt[3]{5})(x - \sqrt[3]{5}w)(x - \sqrt[3]{5}w^2)$. $\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{5}w, \sqrt[3]{5}w^2) = \mathbb{Q}(\sqrt[3]{5}, w)$, porque $w = \frac{\sqrt[3]{5}w}{\sqrt[3]{5}} \in \mathbb{Q}(\sqrt[3]{5},)$. $Gal(x^3 - 5) \leqslant H \leqslant S_3$.
Como $x^3 - 5$ es separable, $|Gal(x^3 - 5)| = [\mathbb{Q}(\sqrt[3]{5}, w) : F] = [\mathbb{Q}(\sqrt[3]{5}, w) : \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$ $= 2 * 3 = 6$, porque $x^2 + x + 1 = Irred(w, \mathbb{Q}(\sqrt[3]{5}))$ ya que no tiene raíces en $\mathbb{Q}(\sqrt[3]{5})$ y sus raíces están en $\mathbb{C} \setminus \mathbb{R}$. Como $|Gal(x^3 - 5)| = 6 \Rightarrow Gal(x^3 - 5) \approxeq S_3$. Los posibles automorfismos del grupo son:

	id	σ_1	σ_2	σ_3	σ_4	σ_5
$\sqrt[3]{5}$	$\sqrt[3]{5}$	$\sqrt[3]{5}w$	$\sqrt[3]{5}w^2$	$\sqrt[3]{5}$	$\sqrt[3]{5}w$	$\sqrt[3]{5}w^2$
w	w	w	w	w^2	w^2	w^2

Tenemos que σ_1 es un elemento de orden 3, σ_3 es un elemento de orden 2.
$Gal(x^3 - 5) =< \sigma_1, \sigma_3 >$

3.2. Raíces de la unidad. Cuerpos de Galois

Teorema III.3. Sea F cuerpo, $G \leqslant F \setminus \{0\}$. Si G es un grupo finito $\Rightarrow$ G es cíclico.

Demostración: Dado F cuerpo, $F \setminus \{0\}$ es un grupo abeliano, por lo tanto, G es un grupo abeliano y finito. Por el teorema de clasificación de los grupos abelianos finitos (todo grupo abeliano finito es isomorfo al producto de grupos cíclicos de órdenes potencias de primos),

$$\exists\, \psi : G \cong \mathbb{Z}/p_1^{m_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{m_1 s_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_n^{m_{n1}}\mathbb{Z} \times ... \times \mathbb{Z}/p_n^{m_n s_n}\mathbb{Z}$$

donde $m_j \leqslant m_{i\,j+1}$.

Sea $g = \psi^{-1}(0, ..., 0, 1, 0, ..., 1, ..., 0, ..., 0, 1)$ (los 1s están en las posiciones S_1, S_i, S_n). $o(g) = p_1^{m_1 s_1}$. Tenemos que $G =< g >$, por lo que $m = mcm\{o(a) : a \in G\}$, $a^m = 1$ $\forall a \in G$, $\forall a \in G$ y a es raíz de $x^m - 1$. Como F es un cuerpo, $x^m - 1$ tiene a lo más m raíces, $|G| \leqslant m$, $m = o(g) = o(< g >) \leqslant |G|$, $|G| = m$.

Definición 39 (Raíz n-ésima de la unidad)**.** Dado F cuerpo, una **raíz n-ésima de la unidad** en F es $a \in F$ tal que $a^n = 1$, es decir, $a \in F \setminus \{0\} : o(a)|n$.

Ejemplo 27. En $\mathbb{Q}$, 1 es la única raíz cúbica de 1.

Ejemplo 28. Busquemos las raíces cúbicas en $\mathbb{F}_5$. $a \in \mathbb{F}_5$, $a^3 = 1 \Rightarrow o(a)|3$ y $a \in \mathbb{F}_5 \setminus \{0\}$ $o(a)|4$, entonces $o(a) = 1$. Por lo tanto, 1 es la única raíz cúbica de la unidad en $\mathbb{F}_5$.

Ejemplo 29. En $\mathbb{C}$, $1, e^{\frac{2\pi}{3}i}, e^{4\pi 3i}$ son las raíces cúbicas de 1, cumplen $w^2 + w + 1 = 0$.

Ejemplo 30. Busquemos las raíces cúbicas en $\mathbb{F}_4$. $\mathbb{F}_4 = \mathbb{F}_2[X]/(x^2 + x + 1) = \mathbb{F}_2(\alpha) =$ $= \{a + b\alpha : a, b \in \mathbb{F}_2\} = \{0, 1, \alpha, 1 + \alpha\}$. $1, \alpha, 1 + \alpha$ son las raíces cúbicas de la unidad.

Corolario 1. Sea F cuerpo, $G = \{a \in F : a^n = 1\}$ es un grupo cíclico, es el grupo de raíces de la unidad de F.

Demostración: G es grupo ya que $G = \{a \in F \setminus \{0\} : o(a)|n\}$, $F \setminus \{0\}$ es abeliano. $\forall a \in G$, a raíz de $x^n - 1$ en F, $|G| \leqslant n$. G es finito. Por el teorema, G es cíclico.

Definición 40 (Raíz n-ésima primitiva de la unidad)**.** Dado F cuerpo, una **raíz n-ésima primitiva de la unidad** en F es un $a \in F \setminus \{0\}$ tal que $o(a) = n$.

Ejemplo 31. En $\mathbb{Q}$ y en F_5 no hay raíces cúbicas primitivas de la unidad.

Ejemplo 32. Sea $C^n = \{a \in \mathbb{C} : a^n = 1\}$, $\zeta = e^{\frac{2\pi}{n}i}$ una raíz n-ésima primitiva de 1 en $\mathbb{C}$, porque $\{\zeta^k : k \text{ coprimo con } n\} = \{\text{raíces n-ésimas primitivas de1 en } \mathbb{C}\}$.

Ejemplo 33. Sea $x^n - 1 \in \mathbb{Q}[X]$, busquemos su cuerpo de descomposición.
$x^n - 1 = (x - \zeta)(x - \zeta^2)...(x - \zeta^{n-1})$, $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^k)$ para cualquier k coprimo con n.
$< \zeta >=< \zeta^k > \leqslant \mathbb{C}^* \ \forall k$ coprimo con n.

Ejemplo 34. En $\mathbb{F}_4$ hay 3 raíces cúbicas de 1, como vimos en el ejemplo 30. Además, son raíces primitivas.

Observación: Para $n > 1$, si un cuerpo contiene una raíz n-ésima primitiva de la unidad, entonces, contiene todas las raíces n-ésimas primitivas.

Demostración: El cuerpo de descomposición de $x^n - 1 \in F[X]$, dado F cuerpo, es $F(\alpha)$ si α es raíz n-ésima primitiva de 1.

Corolario 2. Sea $F = GF(p^n)$, con p primo (GF ≡ cuerpo de Galois de p^n elementos). Entonces $F \setminus \{0\}$ es cíclico y $F = \mathbb{F}_p(\alpha)$, con α raíz de un polinomio de grado n.

Demostración: F es cuerpo de descomposición de $x^{p^n} - x \in \mathbb{F}_p[X]$, $[F : \mathbb{F}_p] = n$. $F \setminus \{0\}$ es un grupo finito, luego es cíclico.

F es el cuerpo de descomposición de $x^{p^n-1} - 1 \in \mathbb{F}_p[X]$, α es raíz $(p^n - 1)$-ésima de la unidad en F. (Si α es generador de $F \setminus \{0\}$, que existe por ser $F \setminus \{0\}$ cíclico. $o(\alpha) = |F \setminus \{0\}| = p^n - 1$, α es una raíz $(p^n - 1)$-ésima de la unidad en F.) Por lo tanto, $F = \mathbb{F}_p(\alpha)$.

$n = [F : \mathbb{F}_p] = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = gr(Irred(\alpha, \mathbb{F}_p))$. Por tanto, α es raíz de $Irred(\alpha, \mathbb{F}_p)$ que tiene grado n.

Observación: $<\alpha> = F \setminus \{0\} \Rightarrow F = \mathbb{F}_p(\alpha)$.

Ejemplo 35. Sea F cuerpo con $|F| = 9 = 3^2$. Sea $x^9 - x \in \mathbb{F}_3[X]$. Su factorización es:
$x^9 - x = x(x^8 - 1) = x(x - 1)(x^7 + x^6 + x^5 + ... + x + 1) = x(x - 1)(x^4 + 1)(x^2 + 1)(x + 1)$
$x^2 + 1 = Irred(\alpha, \mathbb{F}_3)$ y $\alpha^8 - 1 = 0$, α es raíz octava de 1 en $\mathbb{F}_9$. Pero como $\alpha^2 = -1$, el orden de α es 4, α no es raíz primitiva, no genera $F \setminus \{0\}$.

Definición 41 (Elemento primitivo). (De un cuerpo y de una extensión).

1. Un **elemento** $\alpha \in F$ **es primitivo** de un cuerpo finito F con $ch(F) = p$ si $F = \mathbb{F}_p(\alpha)$.
2. Un **elemento** $\alpha \in E$ **es primitivo** para E extensión de F si $E = F(\alpha)$.

RESUMEN. Sea $|F| = p^n$, p primo. $F = \mathbb{F}_p(\alpha)$ con $n = [F : \mathbb{F}_p] = gr(Irred(\alpha, \mathbb{F}_p))$. $F = \{\sum_{i=0}^{n-1} a_i \alpha^i : a_i \in \mathbb{F}_p\}$. F^* es un grupo cíclico de orden $p^n - 1$, generado por α, $F = <\alpha>$. El orden de α, $o(\alpha) = p^n - 1$, es decir, α es raíz $(p^n - 1)$-ésima primitiva de la unidad en F y α es raíz del polinomio $x^{p^n-1} - 1$.

Observación: $\mathbb{C}^2 = \mathbb{C}$, $\forall a, b \in \mathbb{R}$ $a, b \notin \mathbb{R}^2 \Rightarrow ab \in \mathbb{R}^2$.

Corolario 3. Sea F cuerpo finito. $\forall a, b \in F$, $a, b \notin F^2 \Rightarrow ab \in F^2$.

Demostración: Sea $F = \mathbb{F}_p(\alpha)$ para algún p primo. Sea α raíz $(|F| - 1)$-ésima de la unidad en F. $F^* = <\alpha>$, $\beta \in F^* \Rightarrow \beta = \alpha^i$ para algún $0 \leqslant i \leqslant |F|$. $a, b \notin F^2 \Rightarrow a = \alpha^i$, $b = \alpha^j$, con i, j impares. Por lo tanto, $ab = \alpha^{i+j}$, con $i + j$ par, $ab \in F^2$.

Observación: $x^4 - 10x^2 + 1$ es reducible en F, para todo F cuerpo finito.

- Si $ch(F) = 2$, $f(x) = x^4 + 1 = (x^2 + 1)^2$. Si $ch(F) \neq 2$, $x^2 = 5 \pm 2\sqrt{6}$.
- Si $6 \in F^2$, $f(x) = (x^2 - 5 + 2\sqrt{6})(x^2 - 5 - 2\sqrt{6})$, $\sqrt{6} \in F$. Si $6 \notin F^2$, entonces $2 \in F^2$ o $3 \in F^2$.
  - Si $2 \in F^2 \Rightarrow f(x) = (x^2 - 1)^2 - 8x^2 = (x^2 - 1 - 2\sqrt{2}x)(x^2 - 1 + 2\sqrt{2}x)$
  - Si $3 \in F^2 \Rightarrow f(x) = (x^2 + 1)^2 - 12x^2 = (x^2 + 1 - 2\sqrt{3}x)(x^2 + 1 + 2\sqrt{3}x)$

Teorema III.4. $F = GF(p^n)$. Entonces $Gal(F/\mathbb{F}_p) = <\sigma_p>$ es cíclico de orden n, donde $\sigma_p : F \to F; a \to a^p$.

Demostración:

- $\sigma_p \in Gal(F/\mathbb{F}_p)$ ya que $\sigma_p \in Aut(F)$ y $\forall a \in \mathbb{F}_p$, $a^p = a$, por lo tanto, $\sigma_p|_{\mathbb{F}_p} = id_{\mathbb{F}_p}$.
- $F = \mathbb{F}_p(\alpha)$ con α raíz de un polinomio irreducible de grado n. Si $\sigma \in Gal(F/\mathbb{F}_p)$, σ queda determinada mediante $\sigma(\alpha)$ y hay n posibilidades. $|Gal(F/\mathbb{F}_p)| \leqslant n$, por lo que $o(\sigma_p) \leqslant n$.

  Veamos que $o(\sigma_p) = n$. Si $o(\sigma_p) = m < n$, $\sigma_p^m = id_F$, $\forall a \in F$, $\sigma_p^m(a) = a \Leftrightarrow a^{p^m} = a \forall a \in F$. $F \subseteq \{$ raíces de $x^{p^m} - x\} \Rightarrow |F| \leqslant p^m < p^n$. Llegamos a una contradicción.

Teorema III.5. $E = F(\alpha)$ α raíz n-ésima primitiva de la unidad en E. Entonces, $Gal(E/F) \cong H \leqslant U(\mathbb{Z}/n\mathbb{Z})$.

Demostración: $\alpha^n = 1$, $\sigma \in Gal(E/F)$, $\sigma(\alpha) = \sigma$. $\alpha^n = 1 \Rightarrow (\sigma(\alpha))^n = 1 \Rightarrow \sigma(\alpha) \in E$ es raíz n-ésima de 1. El grupo de raíces n-ésimas de 1 en E está generado por α. Por lo tanto, $\sigma(\alpha) = \alpha^i$. $\sigma \in Aut(E) \Rightarrow o(\sigma(\alpha)) = o(\alpha) \Rightarrow$ i es coprimo con n porque: $o(a^m) = \frac{o(a)}{mcd(o(a),m)}$.

NOTACIÓN: $\sigma \in Gal(E/F)$, $\sigma(\alpha) = \alpha^i$, $\sigma_i := \sigma$.

Definimos $\psi : Gal(E/F)U(\mathbb{Z}/n\mathbb{Z})$, $\sigma_i \to i$. Veamos que ψ es un homomorfismo inyectivo:

- $\sigma_i\sigma_j(\alpha) = \sigma_i(\alpha^j) = \alpha^{ij}$. Así, $\psi(\sigma_i\sigma_j = ij = \psi(\sigma_i)\psi(\sigma_j)$. $\psi(\sigma_i) = 1 \Rightarrow i = 1 \Rightarrow \sigma_i = id_E$. Por lo tanto, ψ es homomorfismo.
- ψ es inyectiva, $Ker(\psi) = \emptyset$.

$Gal(E/F) \approx Im(\psi) \leqslant U(\mathbb{Z}/n\mathbb{Z})$.

Ejemplo 36. $F = \mathbb{Q}$, $\zeta = e^{\frac{2\pi}{p}i}$, p primo, ζ raíz p-ésima primitiva de la unidad. $\mathbb{Q}(\zeta)$, $\phi_p(x) = x^{p-1} + ... + x^2 + x + 1$ es $Irred(\zeta, \mathbb{Q})$.

$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \approx H \leqslant U(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$, $|Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = p - 1 \Rightarrow$

$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \approx (\mathbb{Z}/p\mathbb{Z})^*$.

Ejemplo 37. $\mathbb{F}_9/\mathbb{F}_3$, $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$. α es raíz octava primitiva de 1 en $\mathbb{F}_9$. (Ver el ejemplo 35). $Gal(\mathbb{F}_9/\mathbb{F}_3) \approx H \leqslant U(\mathbb{Z}/8\mathbb{Z}) = \{1, 3, -1, -3\}$

$\sigma_3 : \mathbb{F}_9 \to \mathbb{F}_9$, $o(\sigma_3) = 2$, $\sigma_3^2(a) = \sigma_3(a^3) = a^9 = a$. $<\sigma_3> = Gal(\mathbb{F}_9/\mathbb{F}_3) \approx \mathbb{Z}/2\mathbb{Z}$

3.3. Acciones de grupo. Resolubilidad

Definición 42 (Grupo actúa sobre un conjunto)**.** Sea G un grupo, X un conjunto. Decimos que **G actúa sobre X**, $G \curvearrowright X$ si existe una aplicación $G \times X \to X$; $(g, x) \to gx$ tal que $1x = x$, $g(hx) = (gh)x$.

Ejemplo 38. $G \leqslant S_n$, $X = I_n = \{1, ..., n\}$. G actúa sobre X porque $\sigma i := \sigma(i)$.

Ejemplo 39. Sea G grupo, $H \trianglelefteq G$, G actúa sobre H por conjugación, $gh := ghg^{-1}$. $g(lh) = g(lhl^{-1}) = g(lhl^{-1})g^{-1} = (gl)h(gl)^{-1} = (gl)h$

Ejemplo 40. $G = Gal(E/F)$, $f(x) \in F[X]$, $Z = \{\alpha \in E : f(\alpha) = 0\}$. G actúa sobre Z, $\sigma\alpha := \sigma(\alpha) \in Z$.

Definición 43. Sea G grupo, X conjunto. G actúa sobre X. Sea $x \in X$.

- La **órbita de x** en G es $\mathbf{orb}(x) = \{gx : g \in G\} \subseteq X$.
- El **estabilizador de x** en G es $G_x = \{g \in G : gx = x\} \subseteq G$.
- G actúa sobre X **transitivamente** si $\forall x, y \in X$, $\exists g \in G$ tal que $gx = y$.

Ejemplo 41. En S_4, $G = <(123)>$, $X = I_4 = \{1, 2, 3, 4\}$. Calculemos las órbitas de los elementos de X. $orb(1) = \{1, 2, 3\} = orb(2) = orb(3)$. $orb(4) = \{4\}$.
Veamos los estabilizadores: $G_1 = \{id\} = G_2 = G_3$. $G_4 = G$.
Veamos si G actúa transitivamente. Para $1, 4 \in I_4$, no existe $\sigma \in <(123)>$ tal que $\sigma(1) = 4$, por tanto, no es transitiva.

Ejemplo 42. $h \in H \trianglelefteq G$. $orb(h) = \{ghg^{-1} : g \in G\} = cl_G(h)$
$G_h = \{g \in G : ghg^{-1} = h\} = C_G(h)$, centralizador de h en G. Si $H \neq 1$, la acción no es transitiva. Para $h \in H$, $h \neq 1$, entonces $\exists g \in G$, $g1g^{-1} = h$.

Ejemplo 43. $Gal(x^3 - 2) = Gal(Q(\sqrt[3]{2})/Q) = <\sigma, \tau>$, donde $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}w$, $\sigma(w) = w$, $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$,$\tau(w) = w^2$.
$orb(\sqrt[3]{2}) = \{\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2\} = orb(\sqrt[3]{2}w) = orb(\sqrt[3]{2}w^2)$.
$G_{\sqrt[3]{2}} = \{1, \tau\}$, $G_{\sqrt[3]{2}w} = \{1, \sigma^2\tau\}$, $G_{\sqrt[3]{2}w^2} = \{1, \sigma\tau\}$.

Observación: $orb(x) = X \Rightarrow$ G actúa sobre X transitivamente.

Teorema III.6. Sea F cuerpo, $f(x) \in F[X]$ y E/F cuerpo de descomposición de $f(x)$ en F. Sea $X = \{\alpha \in E : f(\alpha) = 0\}$. Entonces:

1. f es irreducible $\Rightarrow Gal(E/F) \curvearrowright X$ es transitiva.
2. Si f no tiene raíces múltiples, entonces $Gal(E/F) \curvearrowright X$ transitiva $\Rightarrow$ f es irreducible.

Demostración: (1) Sabemos que $Gal(E/F) \cap_{\to} X$. Sean $\alpha, \beta \in X$. Como f es irreducible (suponemos mónico), $f = Irred(\alpha; F) = Irred(\beta; F)$. Por el lema II.12 $\exists \psi : F(\alpha) \to F(\beta)$ isomorfismo tal que $\psi|_F = id_F$, $\psi(\alpha) = \beta$.

$x - \alpha | f$ en $F(\alpha)[X]$, $f = f_1(x)(x - \alpha)$
$x - \beta | f$ en $F(\beta)[X]$, $f = f_2(x)(x - \beta)$

Sea $\psi^* : F(\alpha)[X] \to F(\beta)[X]$. $\psi^*(f) = \psi^*(f(x - \alpha)) = \psi^*(f_1)(x - \beta)$, $\psi^*(f) = f_2(x - \beta)$, por lo tanto, $\psi^*(f_1) = f_2$. Tenemos que E es cuerpo de descomposición de $f_1(x)$ en $F(\alpha)$ y que E es cuerpo de descomposición de $f_2(x)$ en $F(\beta)$. Por el resultado II.13 $\exists \psi'$ extensión de ψ tal que $\psi' : E \to E$ isomorfismo. Por lo tanto, $\psi' \in Aut(E)$, $\psi'|_F = \psi|_F = id$ luego $\psi' \in Gal(E/F)$. $\psi'(\alpha) = \psi(\alpha) = \beta$.

(2) Sea f sin raíces múltiples y f reducible. Entonces, $f(x) = f_1(x)f_2(x)$ donde α, β son raíces de f_1, f_2, respectivamente, en E. $\sigma \in Gal(E/F)$, $\sigma(\alpha)$ es raíz de f_1, por lo que $\sigma(\alpha) \neq \beta$. Por tanto, Gal(E/F) no actúa transitivamente.

Corolario 1. Sea F cuerpo, sea $w \in F$, w **raíz n-ésima primitiva de** 1.
Sea $f(x) = x^n - c \in F[X]$. Entonces $\exists \varphi : Gal(f) \to \mathbb{Z}/n\mathbb{Z}$ homomorfismo inyectivo. Además, φ es isomorfismo $\Leftrightarrow$ f es irreducible en F.

Demostración: Sea E/F c. de d. de f(x) en F. Sea $\alpha \in E$, $\alpha^n = c$.
$f(x) = (x - \alpha)(x - \alpha w)(...)(x - \alpha w^{n-1})$. $\forall \sigma \in Gal(f) = Gal(E/F)$ $\exists!$ $i \in \{0, ..., n-1\}$ tal que $\sigma(\alpha) = \alpha w^i$. Sea $\sigma_i \in Gal(f)$, $\sigma_i(\alpha) = \alpha w^i$.

Definimos $\varphi : Gal(f) \to \mathbb{Z}/n\mathbb{Z}$; $\sigma_i \to i$. Veamos que φ es:

- Homomorfismo. $\varphi(\sigma_i \circ \sigma_j) = \varphi(\sigma_i) + \varphi(\sigma_j)$; $(\sigma_i \circ \sigma_j)(\alpha) = \sigma_i(\alpha w^j) = \alpha w^i w^j = \sigma_{i+j}(\alpha)$.
- Inyectiva. $Ker(\varphi) = \{\sigma_0\} = \{id\}$.
- Isomorfismo $\Leftrightarrow$ φ es sobreyectiva $\Leftrightarrow \forall i \in \mathbb{Z}/n\mathbb{Z}$ $\exists \sigma \in Ga(f)$ tal que $\sigma(\alpha) = \alpha w^i$ $\Leftrightarrow^*$ $\forall \gamma, \beta \in \{\alpha, \alpha w, ..., \alpha w^{n-1}\} = X$, $\exists \sigma \in Gal(f)$, $\sigma(\gamma) = \beta$.

  ($\overset{*}{\to}$) En particular, para $\gamma = \alpha$ y $\beta = \alpha w^i$ existe $\sigma \in Gal(f)$ tal que $\sigma(\alpha) = \beta$.

  ($\overset{*}{\leftarrow}$) $\gamma = \alpha w^j$, $i, j \in \{0, ..., n-1\}$ $\exists \sigma$, $\sigma(\alpha) = \alpha w^i$, $\exists \tau$ $\tau(\alpha) = \alpha w^j$, $\tau\sigma^{-1}(\gamma) = \beta$, $\sigma, \tau \in Gal(f)$, $\tau\sigma^{-1} \in Gal(f)$.

Supongamos que f tiene raíces múltiples, $\alpha w^i = \alpha w^j$ para $i > j$, $i, j \in \{0, ..., n-1\}$ $\Rightarrow$ $w^{i-1} = 1$, es imposible, porque w es raíz n-ésima primitiva de la unidad. Por tanto, f no tiene raíces múltiples.

Por último, como $\forall \gamma, \beta$ $\exists \sigma \in Gal(f)$ tal que $\sigma(\gamma) = \beta \Leftrightarrow Gal(f) \cap_{\to} X$ transitivamente $\Rightarrow$ f es irreducible por el teorema III.6.2.

Observación: Sea F cuerpo, $w \in F$, w raíz n-ésima primitiva de 1. $ch(F) = p$ entonces **p no puede dividir a n**.

$x^{pn} - 1 = (x^n - 1)^p$. Como $w^n = 1 \Rightarrow (w^m - 1)^p = 0 \Rightarrow w^n - 1 = 0 \Rightarrow o(w)|n$ y $o(w) < n$. Pero supusimos que w es raíz n-ésima primitiva, es decir, $o(w) = n$.

Corolario 2. Sea p primo, $w \in F$ raíz p-ésima primitiva de 1. Sea $f(x) = x^p - c \in F[X]$. Entonces,

- f se descompone en F y $Gal(f) = \{id\}$.
- f es irreducible en F y $Gal(f) = \mathbb{Z}/p\mathbb{Z}$.

Demostración: Si f se descompone en F, entonces F es igual al cuerpo de descomposición de f en F, por tanto, $Gal(f) = \{id\}$.

Si f no se descompone en F y E c. de d. de f en F entonces $[E : F] > 1$. Dada w raíz p-ésima primitiva de 1, si $\alpha \in E$, $\alpha^p = c \Rightarrow \{\alpha, \alpha w, ..., \alpha w^{p-1}\}$ tiene p elementos y f tiene p raíces distintas en E, por lo tanto, f es separable.

$|Gal(f)| = [E : F] > 1$. Por el Corolario 1, $Gal(f) \cong H \leqslant \mathbb{Z}/p\mathbb{Z} \Rightarrow \varphi$ es isomorfismo, entonces f es irreducible y $Gal(f) \cong \mathbb{Z}/p\mathbb{Z}$.

Corolario 3. Sea F cuerpo y p primo, $f(x) = x^p - c \in F[X]$. f es irreducible en $F \Leftrightarrow c \notin F^p$.

Demostración: Tenemos que para $ch(F) = p$ es cierto por el Lema II.10. Supongamos F cuerpo con $ch(F) \neq p$.

$(\rightarrow)$ Si $c \in F^p$, $a^p = c$ con $a \in F$ (si $c = 0$, $f(x) = x^p$ es reducible y $c \in F^p$),
$x^p - a^p = (x - a)(x^{p-1} + ax^{p-2} + ... + a^{p-2}x + a^{p-1})$ por lo que f es reducible.

$(\leftarrow)$ Supongamos $f(x) = g(x)h(x)$, $f(x) = \prod_{i=0}^{p-1}(x - \alpha w^i)$ donde $\alpha, w \in E$ cuerpo de descomposición de f en F y $\alpha^p = c$. Por lo tanto, para $g(x) = \prod_{j \in J}(x - \alpha w^j)$ donde $J \subset \{0, ..., p-1\}$, $g(0) = \pm\alpha^k w^m$ donde $k = gr(g) < p$, $0 < k < p$.

$g(0)^p = \pm\alpha^{kp} w^{km} = \pm c^k$, k y p coprimos $\Rightarrow \exists n, \nu \in \mathbb{Z}$, $1 = ku + p\nu$.
Por lo que $c = c^{ku+p\nu} = (c^k)^u (c^p)^\nu = \pm(g(0)^u)^p (c^\nu)^p \in F^p$ por lo tanto, $c \in F^p$.

Teorema III.7. Sea G grupo, X conjunto, G actúa sobre X. Entonces $\forall x \in X$, $|orb(x)| = [G : G_x]$. Si además G es finito, $|X| = n$ y G actúa sobre X transitivamente $\Rightarrow n \mid |G|$.

Demostración: $orb(x) = \{gx : g \in G\}$. $G_x = \{g \in G : gx = x\}$. $[G : G_x] = |G/\equiv^i_{G_x}|$;
$orb(x) \rightarrow G/\equiv^i_{G_x}$; $gx \rightarrow gG_x$. $gx = hx \Leftrightarrow h^{-1}gx = x \Rightarrow h^{-1}g \in G_x \Leftrightarrow hG_x = gG_x$ por lo tanto es una aplicación inyectiva sobre gG_x, es imagen de gx.

Definición 44 (Subgrupo transitivo). $G \leqslant S_n$ es transitivo si $G \cap_{\to} I_n$ transitiva.

Ejemplo 44. $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. Buscamos $G \cap_{\to} I_3$, G está generado por $\sigma \in G$, $\sigma \circ i := \sigma(i)$ $i \in I_3 = \{1, 2, 3\}$. $G = <(123)>$.

Ejemplo 45. S_n, $G \leqslant S_n$, $(a_1 ... a_n) \in G$, $(12...n) \in G$ son transitivos.

Teorema III.8. Sea G grupo finito $H \leqslant G$ con $[G : H] = n$. Entonces existe $\varphi : G \to S_n$ homomorfismo $Ker(\varphi) \subset H$.

Demostración: $X = \{gH : g \in G\}$, $|X| = n$ (es el índice del subgrupo H en el grupo G, cardinal del conjunto cociente). Sea $G/\equiv_H^i$ y $Biy(X) \approx S_n$. Basta demostrar que existe $\psi : G \to Biy(X)$ homomorfismo con $Ker(\psi) \subseteq H$. Así, $\varphi : \psi' \circ \psi : G \to S_n$ homomorfismo. $Ker(\varphi) = Ker(\psi' \circ \psi) = Ker(\psi) \subseteq H$.

$\psi(g) : X \to X; g_1H \to gg_1H$. $g_1H = g_2H \Rightarrow g_1^{-1}g_2 \in H$ por lo que $(gg_1)^{-1}gg_2 = g_1^{-1}g_2 \in H$
$gg_1H = gg_2H$. $\psi(g)$ está bien definida, $\psi(g_1g_2)(g_3H) = g_1g_2g_3H$
$\psi(g_1)\psi(g_2)(g_3H) = \psi(g_1)(g_2g_3H) = g_1g_2g_3H$

$g \in Ker(\psi) \Rightarrow \psi(g) = id_x$ $\forall g_1H \in X, \psi(g)(g_1H) = g_1H$, $gg_1H = g_1H$ $\forall g_1 \in G$. En particular $gH = H$ por lo tanto $g \in H \Rightarrow Ker(\psi) \subset H$.

Corolario 1. S_5 no tiene ningún subgrupo de orden 30 o 40.

Demostración: Sea $H \leqslant S_5$, $|H| = 30$, $|S_5| = 120$. $[G : H] = 4$, por lo tanto existe un homomorfismo $\varphi : S_5 \to S_4$, $Ker(\varphi) \subset H$, $Ker(\varphi) \trianglelefteq S_5 \Rightarrow Ker(\varphi) = \{1\}$ o A_5 o S_5. Como $|A_5| = 60$ y $|S_5| = 120$, no puede ser $Ker(\varphi) = A_5$ o $S_5 \subset H$. Entonces, $Ker(\varphi) = \{1\}$, φ es inyectiva, por lo que no existe H de orden 30.

Para $|H| = 40 \Rightarrow [G : H] = 3$. $\exists : S_5 \to S_3$. $Ker(\varphi) \subset H$. Análogamente, $Ker(\varphi) = \{1\}$. φ inyectiva. Entonces, no existe H de orden 40.

Corolario 2. $\forall \sigma$ 5-ciclo y τ trasposición, $\sigma, \tau \in S_5$. Se tiene que $S_5 = <\sigma, \tau>$.

Demostración: Sin pérdida de generlidad, $\sigma = (12345)$ $\tau = (1i)$ $i \neq 1$. $\exists k \sigma^k(i) = 1$ con $0 < k < 5$. $\sigma^k(1i)\sigma^{-k} = (\sigma^k(1), \sigma^k(i)) = (j1)$.

$j \neq i$ ya que si $j = i$ $\sigma^k(1i) = (1i)\sigma^k$ y σ^k y $(1i)$ conmutan, imposible ya que σ^k es 5-ciclo, por ser 5 primo y 5 no divide a k. $(1i)$ es una trasposición y no son disjuntos, por lo que no conmutan.

Sea $H = <\sigma, \tau>$ $\tau \in H \Rightarrow 2| |H|$ $\sigma \in H \Rightarrow 5| |H|$.

$(1ij) = (1j)(1i)$ $(ij) = \sigma^k(1i)\sigma^{-k} \in H$ $(1i) = \tau \in H$ $(1ij) \in H$.

3 divide a $|H|$ por lo que $|H| \neq 30$. 30 divide a $|H|$ por lo que $|H| = 60$, $H = A_5$, imposible porque $(1i) \neq A_5$. Por lo tanto, $H = S_5$.

Ejemplo 46. $f(x) \in \mathbb{Q}[X]$ irreducible de grado 5 tal que f tiene 3 raíces reales distintas y 2 complejas (no reales). Entonces $Gal(f) \approxeq S_3$.

f con 5 raíces distintas $\Rightarrow Gal(f) \approxeq H \leqslant S_5$. f es irreducible y separable por lo que $5 \mid |Gal(f)|$.

Sea $X = \{\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2\}$ raíces de f con $\beta \in \mathbb{C} \setminus \mathbb{R}$. Identificando Gal(f) con H tenemos $Gal(f) \leqslant S_5$.

$\sigma \mid |Gal(f)| \Rightarrow \exists\ \sigma \in Gal(f)$, $o(\sigma) = 5 \Rightarrow \sigma$ es un 5-ciclo. $\exists \tau \in Gal(f)$, $\tau(\beta) = \overline{\beta}$ y $\tau(\alpha_i) = \alpha_i\ i = 1, 2, 3$. $\overline{\tau} \in Aut(\mathbb{C})$, $\overline{\tau}(a + bi) = a - bi$. $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \beta, \overline{\beta})$, entonces $\overline{\tau}|_E : E \to E$ tal que $\overline{\tau}(\beta) = \overline{\beta}$. $\tau = \overline{\tau}|_E \in Gal(f)$, $\tau = (4\ 5)$. Como $S_5 = <\sigma, \tau>$ entonces, por el corolario 2 $Gal(f) \approxeq S_5$.

3.3.1. Resolubilidad

Definición 45 (Serie normal en un grupo)**.** Sea G grupo, una **serie normal** en G es:

$$\{1\} = G_n \leqslant G_{n-1} \leqslant ... \leqslant G_{i+1} \leqslant G_i \leqslant ... \leqslant G_1 \leqslant G_0 = G$$

tal que $G_{i+1} \trianglelefteq G_i$.

Observación: $\trianglelefteq$ no es una relación transitiva. $S = \{\{1\}, (12)(34), (13)(24), (14)(23)\}$, $<(12)(34)> \trianglelefteq S \trianglelefteq S_4$, pero no es cierto que $<(12)(34)> \trianglelefteq S_4$.

Definición 46 (Grupo resoluble)**.** Un grupo G es **resoluble** si tiene una serie normal $\{1\} = G_n \leqslant G_{n-1} \leqslant ... \leqslant G_1 \leqslant G_0 = G$ tal que G_i/G_{i+1} son abelianos. Los grupos G_i/G_{i+1} son los **grupos factores**.

Ejemplo 47. Si G es abeliano, entonces cualquier serie $\{1\} = G_n \leqslant G_{n-1} \leqslant ... \leqslant G_0 = G$ es normal y los grupos factores son abelianos. Por tanto, **abeliano** $\Rightarrow$ **resoluble**.

Ejemplo 48. $\{(1)\} \trianglelefteq <(123)> \trianglelefteq S_3$. $<(123)>/<(1)> \approxeq <(123)>$ orden 3 abeliano, $|S_3/<(123)>| = 2$ es abeliano. Por tanto S_3 es resoluble.

Ejemplo 49. $\{(1\} \leqslant S \leqslant A_4 \leqslant S_4$, $S = <(12)(34), (13)(24)> \Rightarrow S \trianglelefteq A_4$. $A_4 \trianglelefteq S_4$. S abeliano, $|A_4/S| = \frac{12}{4} = 3$ abeliano, $|S_4/A_4| = 2$ abeliano. Por lo tanto, S_4 es resoluble.

Ejemplo 50. $\{(1)\} \trianglelefteq A_5 \trianglelefteq S_5$

Ejemplo 51. $\{(1,1)\} \trianglelefteq \{(1)\} \times S_3 \trianglelefteq S_3 \times S_3$.

Definición 47 (Conmutador)**.** Sea G un grupo. Sean, $x, y \in G$. El **conmutador** de x e y es $[x, y] = xyx^{-1}y^{-1} \in G$. El **subgrupo permutador** o **derivado** de G es

$$G' = [G, G] = <\{[x, y] : x, y \in G\}>$$

Observación: $[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y,x]$

Observación: Sea G un grupo.

1. $G' \trianglelefteq G$ y G/G' es abeliano.
2. $N \trianglelefteq G$ y G/N abeliano $\Rightarrow G' \leqslant N$. Además, G' es el mínimo subgrupo normal de G tal que el cociente es abeliano. **G/G'** es el **abelianizado de G**.

Demostración: (1) $G' \trianglelefteq G$. $[x,y] \in G'$. $g \in G$. $g[x,y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gxg^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}] \in G'$.

G/G' abeliano $\Leftrightarrow \forall x,y \in G\ xyG' = yxG' \Leftrightarrow (yx)^{-1}xy \in G' \Leftrightarrow x^{-1}y^{-1}xy \in G' \Rightarrow [x^{-1}, y^{-1}] \in G'$.

(2) Sea $N \trianglelefteq G$ con G/N abeliano $\Leftrightarrow \forall x,y \in G$, $[x^{-1}, y^{-1}] \in N \Leftrightarrow G' \leqslant N$.

Ejemplo 52. G abeliano $\Rightarrow G' = \{1\}$.

Ejemplo 53. $S_3' = A_3$ porque los subgrupos normales de S_3 son $\{1\}, A_3, S_3$ y S_3/A_3 es abeliano.

Ejemplo 54. $S_n' = A_n$. Sabemos que A_n está generado por los 3-ciclos. S_n/A_n es abeliano $\Rightarrow S_n' \leqslant A_n$. $\sigma = (ijk)$, $\sigma^2 = (ijk) = (ij)(ik)$. $\sigma^4 = [(ij),(ik)] \in S_n'$. Por lo tanto, $A_n \leqslant S_n'$, $S_n' = A_n$.

Ejemplo 55. Suponemos G simple. Si G es abeliano, $G' = \{1\}$. Si G no es abeliano, $G = G'$, es un grupo perfecto.

Ejemplo 56. $G = A_5 \times A_5$, $G = G'$ aunque G no es simple. $\{1\} \times A_5 \trianglelefteq A_5 \times A_5$.

Definición 48 (n-ésimo subgrupo conmutador)**.** El n-ésimo subgrupo conmutador de un grupo G es $G^{(n)}$. Definimos $G^{(0)} = G$, $G^{(n+1)} := (G^{(n)})'$.

Teorema III.9. Sea G un grupo. G es resoluble $\Leftrightarrow \exists\, n \in \mathbb{N}$ tal que $G^{(n)} = \{1\}$.

Demostración: ($\rightarrow$) G es resoluble, por lo tanto existe una serie normal $\{1\} = G_n \leqslant G_{n-1} \leqslant \ldots \leqslant G_1 \leqslant G_0 = G$ con G_i/G_{i+1} abeliano. Veamos que $G^{(i)} \leqslant G_i$. Así, $G^{(n)} = \{1\}$. Por inducción en i, $i = 0$, $G^{(0)=G=G_0}$. Supongamos $G^{(i)} \leqslant G_i \Rightarrow G^{(i+1)} = (G^{(i)})' \leqslant (G_i)'$. Tenemos que G_i/G_{i+1} es abeliano, por lo tanto $(G_i)' \leqslant G_{i+1} \Rightarrow G^{(i+1)} \leqslant G_{i+1}$.

($\leftarrow$) Si $\{1\} = G^{(n)}$ entonces $\{1\} = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \ldots \trianglelefteq G(i+1) \trianglelefteq G^{(i)} \trianglelefteq \ldots \trianglelefteq G^{(0)} \trianglelefteq G$ es una serie normal. $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ abeliano.

Corolario 1. Sea G un grupo resoluble. Entonces:

1. Si $H \leqslant G$ entonces H es resoluble.
2. Si $\varphi : G \to H$ homomorfismo entonces $\varphi(G)$ es resoluble. En particular, si $N \trianglelefteq G$ entonces G/N es resoluble.

Demostración: (1) $H \leqslant G \Rightarrow H^{(i)} \leqslant G^{(i)}$ por inducción en i. G es resoluble entonces, por el Teorema, existe n tal que $G^{(n)} = 1$, por lo que $H^{(n)} = 1$.

(2) $\varphi(G^{(i)}) = (\varphi(G))^{(i)}$. Por inducción en i, $\varphi(G') = \{\varphi(<[x,y] : x,y \in G>)\} =$ $<\{\varphi([x,y]) : x,y \in G\}>$ = $<\{[\varphi(x),\varphi(y)] : x,y \in G\}>$ = $(\varphi(G))'$. Así existe n tal que $G^{(n)} = \{1\}$, por lo que $(\varphi(G))^{(n)} = \{1\}$. $\pi : G \to G/N$ es homomorfismo sobreyectivo.

Corolario 2. Sea G grupo, $N \trianglelefteq G$, N y G/N son resolubles $\Leftrightarrow$ G resoluble.

Demostración: ($\leftarrow$) Por corolario 1.
($\rightarrow$) N es resoluble, luego existe una serie normal $\{1\} = N_n \leqslant N_{n-1} \leqslant ... \leqslant N_1 \leqslant N_0 = N$ con N_i/N_{i+1} abeliano.
Denotamos $G^* := G/N$ resoluble, entonces existe la serie
$\{1\}^* = G_l^* \leqslant G_{l-1}^* \leqslant ... \leqslant G_1^* \leqslant G_0^* = G^*$ con G_i^*/G_{i+1}^* abeliano, $G_i^* = H_i/N$ con $N \leqslant H_j$.
$G_{j+1}^* \trianglelefteq G_j^* \Rightarrow H_{j+1} \trianglelefteq H_j$.
De la cadena normal anterior se induce que $N = H_l \trianglelefteq H_{l-1} \trianglelefteq ... \trianglelefteq H_0 = G$.
$H_j/H_{j+1} \cong (H_j/N)/(H_{j+1}/N) = G_j^*/G_{j+1}^*$ abeliano.
Así, $\{1\} = N_m \trianglelefteq ... \trianglelefteq N_0 = N = H_l \trianglelefteq ... \trianglelefteq G$ es una serie normal de G con grupos factores abelianos.

Corolario 3. S_n es resoluble $\Leftrightarrow n \leqslant 4$.

Demostración: ($\leftarrow$) $S_1 = \{(1)\}$, $S_2 = \{(1),(12)\}$ son abelianos, luego resolubles. Ya vimos en los ejemplos que S_3 y S_4 también son resolubles.

$\rightarrow$ Por corolario 1 $G_1 \cong G_2 \Rightarrow \{G_1$ resoluble $\Leftrightarrow G_2$ resoluble $\}$.

Observación: Para $n \geqslant 5$ basta ver que $S_5 \cong H \leqslant S_n$ y S_5 no es resoluble, por lo que H tampoco. En consencuencia, S_n no es resoluble.

Demostración: $S_5' = A_5$ es simple, no conmutativo, por lo que no tiene subgrupos normales $\Rightarrow A_5' = A_5$. $S_5^{(m)} = A_5$ $\forall m \geqslant 1$. Entonces no existe j tal que $S_5^{(j)} = \{1\}$, por lo que S_5 no es resoluble.

Corolario 4. $H \leqslant S_5$, H resoluble $\Rightarrow |H| \leqslant 24$.

Demostración: $|S_5| = 5! = 2^3 * 3 * 5$. Supongamos que existe $H \leqslant S_5$, $|H| > 24 \Rightarrow |H| = 5!$ o $2^2 * 3 * 5$, $2^3 * 5$, $2 * 3 * 5$. Ya vimos que los dos últimos casos no se pueden dar, por lo que $H = S_5$ ó $H = A_5$, pero no son resolubles.

Observación: De hecho, para $|G| < 60 \Rightarrow G$ es resoluble y en el corolario es $\Leftrightarrow$.

Lema para el Corolario 5. Sea $G \neq \{1\}$ grupo abeliano finito $\Rightarrow$ contiene un subgrupo de índice primo.

Demostración: $G \neq \{1\}$ abeliano y finito, $H \neq \{1\}$. **$|G|$ no es primo, entonces existe $H < G$.** $\exists p$ primo tal que $p| |G|$ y $p \neq |G|$. Por Cauchy existe $H \leqslant G$, $|H| = p$, por lo que $H < G$. Sea $|G| = p_1 ... p_n$ con los p_i primos no necesariamente distintos. Por inducción en n existe un subgrupo de índice primo $m = 1$, $[G : \{1\}] = |G| = p_1$.

Si $m > 1$, sea $\{1\} \neq H < G$ entonces $\{1\} \neq G/H \cong G$. $|G/H| \mid |G|$. Por hipótesis de inducción, existe $K/H < G/H$ de índice primo. Así, $[G : H] = [G/H : K/H]$ primo.

Corolario 5. Sea G un grupo finito resoluble y $G \neq \{1\}$. Entonces G tiene un subgrupo de índice primo.

Demostración: $G' < G$ ya que G es resoluble. G/G' abeliano y distinto de $\{1\}$. Por el lema, $\exists\, H/G' \leqslant G/G'$ de índice primo tal que $[G : H]$ es primo.

3.4. Extensiones radicales

Definición 49 (Extensión pura)**.** Una extensión de cuerpos E/F es una **extensión pura** si $E = F(\alpha)$ para algún α tal que $\alpha^m \in F$ para algún $m > 0$.

Definición 50 (Extensión radical)**.** Una extensión de cuerpos E/F es una **extensión radical** si existe $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_t = E$ extensiones tales que F_{i+1}/F_i es pura $\forall i = 1, ..., t-1$.

Definición 51 (Polinomio resoluble por radicales)**.** Sea $f(x) \in F[x]$, F cuerpo. f(x) es resoluble por radicales si existe una E/F radical tal que f se descompone en E.

Ejemplo 57. $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ es radical. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2+\sqrt{2}})$. $2 = \alpha^2 \in \mathbb{Q}$, $2+\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. $x^2 = 2+\sqrt{2} \Rightarrow x^4 - 4x + 2$ es resoluble por radicales, $\exists\, \mathbb{Q}(\sqrt{2+\sqrt{2}})$ cuerpo de descomposición y extensión radical.

Objetivo*: Queremos ver que, dado $f(x) \in \mathbb{Q}[x]$, f es resoluble por radicales $\Leftrightarrow$ Gal(f) es resoluble.

Observación: $ch(F) = 0$, $gr(f) \leqslant 4$ (no tiene raíces múltiples). $Gal(f) \cong H \leqslant S_4$ y S_4 es resoluble. Por *, todo polinomio de grado menor o igual que 4 sobre F es resoluble por radicales.

Definición 52 (Extensión pura de tipo m)**.** Sea E/F extensión pura. Decimos que es de tipo m si $E = F(\alpha)$ con $\alpha^m \in F$ y m mínimo.

3.4.1. Resolubilidad de las ecuaciones cuadráticas

Sea $X^2 + bX + c \in F_0(b,c)[X]$, $F_0(b,c) = F$, $F_0 = \mathbb{Q}$, $\mathbb{F}_p$, $p \neq 2$ primo.

$X = x - \frac{b}{2}$, $(x - \frac{b}{2})^2 + b(x - \frac{b}{2}) + c = 0$. $x^2 - \frac{b^2}{4} + c = 0$, $x = \pm\sqrt{(\frac{b}{2})^2 - c}$. $x^2 + bx + c = 0$ se resuelve en $F(\sqrt{(\frac{b}{2})^2 - c})$. $F \subseteq F(\sqrt{(\frac{b}{2})^2 - c})$ extensión pura de tipo 2. $(\frac{b}{2})^2 - c \in F$. $x^2 + bx + c$ se descompone en $F(\sqrt{(\frac{b}{2})^2 - c})$. Cualquier polinomio de grado 2 sobre un cuerpo de característica distinta de 2 es resoluble.

Definición 53 (Cuerpo intermedio). Sean $F \subseteq F_1 \subseteq E$ cuerpos. F_1 es el cuerpo intermedio de la extensión E/F.

Teorema III.10. Sean $F_1 \subseteq F_2 \subseteq F_3$ extensiones de cuerpos tales que F_2/F_1 c. de d. de $f(x) \in F_1[x]$, F_3/F_1 c. de d. de $g(x) \in F_1[x]$. Entonces $Gal(F_3/F_2) \trianglelefteq Gal(F_3/F_1)$,

$$Gal(F_3/F_1)/Gal(F_3/F_2) \approxeq Gal(F_2/F_1)$$

Demostración: Basta demostrar que $\psi : Gal(F_3/F_1) \to Gal(F_2/F_1)$ es homomorfismo sobreyectivo y $Ker(\psi) = Gal(F_3/F_2)$. Así, por el primer teorema de isomorfía, $Gal(F_3/F_1)/Gal(F_3/F_2) \approxeq Gal(F_2/F_1)$.

Sea $\sigma \in Gal(F_3/F_1)$, $\psi(\sigma) := \sigma|_{F_2}$. Veamos que $\psi(\sigma) \in Gal(F_2/F_1)$. $\psi(\sigma)|_{F_1} = id|_{F_1}$ basta ver que $\sigma(F_2) = F_2$. $F_2 = F_1(\alpha_1, ..., \alpha_n)$ donde $\{\alpha_1, ..., \alpha_n\}$ = {raíces de f}. $\sigma|_{F_1}$, $\sigma(\{\alpha_1, ..., \alpha_n\}) = \{\alpha_1, ..., \alpha_n\}$, $\sigma(F_2) \subseteq F_2$. Por lo tanto, ψ está bien definida.

Veamos que ψ es homomorfismo. $\psi(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|_{F_2} = \sigma_1|_{F_2}\sigma_2|_{F_2} = \psi(\sigma_1)\psi(\sigma_2)$.

Veamos que $Ker(\psi) = Gal(F_3/F_2)$. Sea $\sigma \in Ker(\psi)$, $\sigma|_{F_2} = id$. $\sigma \in Aut(F_3)$ y $\sigma|_{F_3} = id|_{F_2}$. Sea $\tau \in Gal(F_3/F_2) \Rightarrow \tau \in Gal(F_3/F_1)$ y $\tau|_{F_2} = id|_{F_2}$ por lo tanto, $\tau \in Ker(\psi)$.

Sea $\tau \in Gal(F_2/F_1)$, F_3/F_1 es c. de d. de $g(x) \in F_1[x]$, F_3/F_2 es c. de d. de $g(x) \in F_2[x]$.

$\tau \in Aut(F_2) \Rightarrow \tau$ se extiende $\sigma \in Aut(F_3)$, por el Teorema II.13. $\tau = \sigma|_{F_2}$ como $\tau|_{F_1} = id|_{F_1}$ por lo tanto, $\sigma|_{F_1} = id|_{F_1}$. Por lo que $\sigma \in Gal(F_3/F_1)$, $\psi(\sigma) = \tau$ y ψ es sobreyectiva.

Ejemplo 58. $f(x) = x^4 - 2x^2 + 8x - 3$, raíces $1 \pm \sqrt{2}, 1 \pm \sqrt{2}i$. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i)$.

$$Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})/Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(\sqrt{2}) \approxeq Gal(\mathbb{Q}(\sqrt{2}/\mathbb{Q})$$

Definición 54 (Cuerpo compuesto). Sean $F_1, F_2 \subset E$, los tres cuerpos. El compuesto de F_1, F_2 ($F_1 \vee F_2$) es el mínimo subcuerpo de E que tiene a F_1 y a F_2. De forma similar si $F_1, ..., F_s \subseteq E$, $F_1 \vee ... \vee F_s$ es el mínimo subcuerpo de E que tiene a todos los F_i para $i = 1, ..., s$.

Observación: Si F_1/F extensión finita de cuerpos $\Rightarrow \exists$ E/F_1 tal que E/F es c. de d. algún polinomio sobre F.

Demostración: F_1/F es finita, $F_1 = F(\alpha_1, ..., \alpha_s)$ para algunos $\alpha_i \in F_i$ algebraico sobre F. Sea $p_i = Irred(\alpha_i, F_i)$, E c. de d. de $f = p_1...p_s \in F[x]$. Tal extensión E/F así definida se llama **cierre por descomposición** de F_1/F.

Lema 1. Sea F_1/F extensión finita de cuerpos. Sea E/F **cierre por descomposición** de F_1/F y sea $Gal(E/F) = \{\sigma_1, ..., \sigma_r\}$. Entonces $E = \sigma_1(F_1)...\sigma_r(F_1)$.

Demostración: $F_1 = F(\alpha_1, ..., \alpha_s)$ $p_i = Irred(\alpha_i, F)$, E es c. de d. de $f = p_1...p_s \in F[x]$. Veamos que $E = \sigma_1(F_1)...\sigma_r(F_1)$.

$(\supseteq)$ Sea $\sigma_j \in Gal(E/F)$. $F_1 \subseteq E \Rightarrow \sigma_j(F_1) \subseteq E$, por lo tanto, $\sigma_1(F_1), ..., \sigma_r(F_1) \subseteq E$.

$(\subseteq)$ Basta demostrar que para todo α $f(\alpha) = 0 \Rightarrow \alpha \in \sigma_i(F_1), ..., \sigma_r(F_1)$. Sea α, $f(\alpha) = 0$ $\Rightarrow$ $\exists i = 1, ..., s$ tal que $p_i(\alpha) = 0$, $p_i(x) \in F[x]$ es irreducible y se descompone en E. Entonces, $Gal(E/F) \cap_{\rightarrow}$ {raíces de $p_i(x)$} transitivamente (EJ1 H5). Por lo tanto, $p_i(\alpha) = p_i(\alpha_i) = 0$ y $\exists$ j para el que $\sigma_j \in Gal(E/F)$, $\alpha = \sigma_j(\alpha_i) \in \sigma_j(F_1)$.

Lema 2. Sea $F \subseteq F_t$, F_t/F extensión radical de cuerpos. Sea $E \supseteq F_t$ y $\sigma \in Gal(E/F)$. Entonces $F \subseteq \sigma(F_t)$ es radical.

Demostración: Sea $F \subset F_t$ radical, entonces existe $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_{t-1} \subseteq F_t$ cadena de extensiones puras. Por inducción en t, $\forall E \supseteq F_t$ $\forall \sigma \in Gal(E/F)$, $F \subseteq \sigma(F_t)$ es radical.

Para $t = 1$, $F_1 = F(\alpha)$ con $\alpha^m \in F$ para algún $m > 0$. $F \subseteq F(\alpha)$. Sea $E \supseteq F(\alpha)$ y $\sigma \in Gal(E/F)$, $\sigma(F) \subseteq \sigma(F(\alpha)) = \sigma(F)(\sigma(\alpha))$ por lo tanto, $F \subset F(\sigma(\alpha))$.
$\sigma(\alpha^m) \in F \Rightarrow \sigma(\alpha)^m \in F$ $F \subseteq \sigma(F_1) = F(\sigma(\alpha))$ es pura.

Para $t > 1$. Sea $F = F_0 \subseteq ... \subseteq F \subseteq F_{t-1} \subseteq F_t$ cadena de extensiones puras, $E \supseteq F_t$ y $\sigma \in Gal(E/F)$. Así, $F \subseteq F_1 \subseteq ... \subseteq F_{t-1}$ extensión puras $E \supset F_{t-1}$ $\sigma \in Gal(E/F)$. Por hipótesis de inducción, $F \subset \sigma(F_{t-1})$ es radical. $F_t = F_{t-1}(\alpha)$ con $\alpha^m \in F_{t-1}$ para algún $m > 0$ $\sigma(F_t) = \sigma(F_{t-1})(\sigma(\alpha))$. $\sigma(\alpha)^m = \sigma(\alpha^m) \in \sigma(F_{t-1})$. Así, $F \subseteq \sigma(F_{t-1}) \subseteq \sigma(F_t)$, F radical y $\sigma(F_{t-1})$ pura. Por lo tanto, $F \subseteq \sigma(F_t)$ es radical.

Corolario. Sea $F \subseteq F_t$ extensión radical. Entonces existe $E \subseteq F_t$ tal que E/F es c. de d. y $F \subseteq E$ radical. En particular, dado $f(x) \in F[x]$ f(x) resoluble y E c. de d. de f en F, entonces existe $F \subseteq F_t$ radical y $E \supseteq F_t$ y F_t/F es c. de d. en F.

Demostración: $f(x) \in F[x]$ resoluble por radicales $\Leftrightarrow$ existe $E \supseteq F$ radical tal que E/F es c. de d. y f se descompone en E.

$(\rightarrow)$ Existe $F_t \supseteq F$ radical tal que f se descompone en F_t. Por la primera parte del corolario existe $E \supseteq F_t$ tal que E/F es c. de d. y $F \subseteq E$ es radical. f se descompone en $F_t \subseteq E$ entonces f se descompone en E.

(1^a parte del col.) Sea $F \subseteq F_t$ radical, entonces F_t/F es finita. Sea E/F cierre por descomposición de F_t/F. Por el lema 1, $E = \sigma_1(F_t)...\sigma_s(F_t)$ donde $\{\sigma_1, ..., \sigma_s\} = Gal(E/F)$. Así, E/F es c. de d., $E \supseteq F_t$. Por el lema 2, $F \subseteq F_t$ es radical, entonces $F \subseteq \sigma_i(F_t)$ es radical. Por el ejercicio 7 de la hoja 5, $F \subseteq \sigma_1(F_t)...\sigma_s(F_t)$ es radical, es decir, $F \subseteq E$ radical.

Lema 3. Sea $f(x) \in F[x]$ resoluble por radicales. Sea E c. de d. de f en F con $F \subset E$. Entonces:

1. Existe $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_t$ tal que $E \subseteq F_t$ y las extensiones F_i/F_{i-1} son puras y F_t/F son c. de d. en F de tipo p_i primo para $i = 1, ..., t$.
2. Si F_t/F es un radical como en (1) y si F contiene una raíz p_i-ésima primitiva de 1 para $i = 1, ..., t$ entonces $Gal(E/F)$ es resoluble.

Demostración: (1) Por el corolario del lema 2, existe F_t/F radical tal que $E \subseteq F_t$ y F_t es c. de d. en F. $F \subset F_t$ es radical y propia. Por el ejercicio 6 de la hoja 5, entonces existe una cadena $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_t$ como en 1.

(2) Sea $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_t$ como en 1. $F_i = F_{i-1}(\alpha_i)$, $\alpha_i^{p_i} \in F_{i-1}$ para p_i primo $i = 1, ..., t$. F_i es c. de d. de $f_i(x) = x^{p_i} - \alpha^{p_i} \in F_{i-1}[x]$. $f_i(x) = p_i x^{p_i - 1}$ y $p_i \neq ch(F_{i-1})$ (ya que F, y por lo tanto, F_{i-1} contiene una raíz p_i-ésima primitiva de 1). f_i es separable, por lo tanto $|Gal(F_i/F_{i-1})| = [F_i : F_{i-1}] = p_i$ por lo tanto, $Gal(F_i/F_{i-1})$ es cíclico, por lo tanto abeliano.

Veamos que $Gal(E/F)$ es resoluble. $F \subseteq E \subseteq F_t$. F_t/F es c. de d. en F, E/F es c. de d. en F. Por lo tanto, $Gal(F_t/E) \trianglelefteq Gal(F_t/F)$ y $Gal(F_t/F)/Gal(F_t/E) \approxeq Gal(E/F)$. Basta demostrar que $Gal(F_t/F)$ es resoluble.

$G_i = Gal(F_t/F_i)$, $G_0 = Gal(F_t/F)$, $F_{i-1} \subseteq F_i \subseteq F_t$, F_t/F_{i-1} es c. de d. en F_{i-1}, F_i/F_{i-1} es c. de d. de $f|_{F_{i-1}}$.

Por el Teorema III.10 $G_i) Gal(F_t/F_i) \trianglelefteq Gal(F_t/F_{i-1}) = G_{i-1}$ y
$G_{i-1}/G_i = Gal(F_t/F_{i-1})/Gal(F_t/F_i) \approxeq Gal(F_i/F_{i-1})$ abeliano.
$\{1\} = G_t \trianglelefteq G_{t-1} \trianglelefteq ... \trianglelefteq G_1 \trianglelefteq G_0$ y G_{i-1}/G_i abeliano, por lo tanto, G_0 es resoluble.

Teorema III.11. Sea F cuerpo, $ch(F) = 0$. Sea $f(x) \in F[x]$. f es resoluble por radicales $\Rightarrow$ Gal(f) es resoluble.

Demostración: Sea E/F c. de d. de $f(x)|_F$. Por 1 del Lema 3 existe $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_t$ cuerpos tales que F_t/F c. de d. de $h(x)|_F$ $E \subseteq F_t$. $F_i = F_{i-1}(\alpha_i)$ con $\alpha^{p_i} \in F_{i-1}$ con p_i primo para $i = 1, ..., t$.

Sea $m = mcm\{p_1, ..., p_t\}$, $ch(F) = 0$. Entonces $g(x) = x^m - 1$ tiene m raíces distintas. Sea w una raíz m-ésima primitiva de la unidad en $\tilde{F}/F$ (existe ya que $ch(F) = 0$), $w_i = w^{m/p_i}$ es una raíz p_i-ésima primitiva de 1, que pertenece a $\tilde{F}$.

Sea $E' = F_t(w)$. $F \subseteq E \subseteq E'$, E'/F es c. de d. de $h(x)(x^m - 1) \in F[x]$. E/F es c. de d. de $f(x) \in F[x]$ por lo tanto (y por el teorema III.10) $Gal(E'/F) \trianglelefteq Gal(E'/F)$ y

$$Gal(E'/F)/Gal(E'/E) \approxeq Gal(E/F) = Gal(f)$$

Así, basta demostrar que $Gal(E'/F)$ es resoluble. $F \subseteq F(w) \subseteq E'$, E'/F c. de d., $F(w)/F$ es c. de d. de $x^m - 1 \in F[x]$. Por el Teorema III.10, $Gal(E'/F(w)) \trianglelefteq Gal(E'/F)$ y $Gal(E'/F)/Gal(E'/F(w)) \approxeq Gal(F(w)/F)$. Para demostrar que Gal(E'/F) es resoluble basta demostrar que:

- $Gal(E'/F(w))$ es resoluble
- $Gal(E'/F)/Gal(E'/F(w)) \approxeq Gal(F(w)/F) \approxeq H \leqslant U(\mathbb{Z}/m\mathbb{Z})$, por lo que el cociente es resoluble.

$F(w) = F_0(w) \subseteq F_1(w) \subseteq ... \subseteq F_t(w) = E'$. $F_i(w) = F_{i-1}(\alpha_i)(w) = F_{i-1}(w)(\alpha_i)$ con $\alpha_i^{p_i} \in F_{i-1} \subseteq F_{i-1}(w)$. E'/F c. de d. $\Rightarrow E'/F(w)$ c. de d. en $F(w)$. Así, $E'/F(w)$ es como en 1 del Lema 3.

Como $F(w)$ contiene las $w_i = w^{m/p_i}$ son raíces p-ésimas primitivas de la unidad. Podemos aplicar 2 del Lema 3 y concluir que $Gal(E'/F(w))$ es resoluble.

Corolario. Existe $p(x) \in \mathbb{Z}[x]$ de grado 5 no resoluble por radicales.

Demostración: $p(x) = x^5 - 4x + 2$. $Gal(p) \approxeq S_5$ no es resoluble, por el teorema, p(x) no es resoluble por radicales.

3.5. Extensiones de Galois

Definición 55 (Carácter del grupo). Sea G un grupo. Un **carácter del grupo G** de un cuerpo E es un homomorfismo $\chi : G \to E \setminus \{0\}$.

Ejemplo 59. Si E es un cuerpo y $\sigma \in Aut(E) \Rightarrow \sigma|_{E\setminus\{0\}} : E \setminus \{0\} \to E \setminus \{0\}$ homomorfismo de grupos (multiplicativos) y por tanto un carácter que denotamos por σ.

Definición 56 (Caracteres independientes). Un conjunto de caracteres $\{\sigma_1, ..., \sigma_n\}$ de G en E es **independiente** si $\sum_{i=1}^{n} a_i\sigma_i(x) = 0\ \forall x \in G \Rightarrow a_i = 0\ \forall i = 1, ..., n\ a_i \in E$.

Lema 1. Cualquier conjunto de n caracteres distintos, $n \geqslant 1$, de un grupo G en un cuerpo E es independiente.

Demostración: Por inducción sobre n. Para $n = 1$, $a\sigma(x) = 0\ \forall x \in G \Rightarrow a\sigma(1) = 0 \Rightarrow a * 1 = 0 \Rightarrow a = 0$.

Sea $n > 1$ y $\sum_{i=1}^{n} a_i\sigma_i(x) = 0\ \forall x \in G$. Supongamos que existe $a_i \neq 0$. Por hipótesis de inducción podemos suponer $a_i \neq 0\ \forall i = 1, ..., n$. Dividiendo $\sum_{i=1}^{n} a_i\sigma_i(x) = 0$ por a_n podemos suponer $a_n = 1$, $\sigma_1 \neq \sigma_n \Rightarrow \exists y \in G$, $\sigma_1(y) \neq \sigma_n(y)$. Fijemos tal y, considerando el sumatorio para todo elemento de G: $0 = \sum_{i=1}^{n} a_i\sigma_i(x) = \sum_{i=1}^{n} a_i\sigma_i(x)\sigma_i(y)$.

Dividiendo por $\sigma_n(y)$: $a_1\sigma_1(x)\sigma_n(y)^{-1}\sigma_1(y) + ... + a_{n-1}\sigma_n(x)\sigma_n(y)^{-1}\sigma_{n-1}(y) + \sigma_n(x) = 0$
$a_1\sigma_1(x) + ... + a_{n-1}\sigma_n(x) + \sigma_n(x) = 0$

$a_1\sigma_1(x)(\sigma_n(y)^{-1}\sigma_1(y) - 1) + a_2\sigma_2(x)(\sigma_n(y)^{-1}\sigma_2(y) - 1) + ...$
$+a_{n-1}\sigma_{n-1}(x)(\sigma_n(y)^{-1}\sigma_{n-1}(y) - 1) = 0$

$\forall x \in G$ por hipótesis de inducción $a_1(\sigma_n(y)^{-1}\sigma_1(y) - 1) = 0 \Rightarrow \sigma_n(y) = \sigma_1(y)$. Contradicción.

Corolario. Cualquier conjunto de automorfismos de un cuerpo E es independiente.

Definición 57 (Cuerpo fijo). Sea E cuerpo, $S \subseteq Aut(E)$.

$$E^S = \{\alpha \in E : \sigma(\alpha) = \alpha\ \forall \sigma \in S\}$$

1. Si S = G grupo, E^G es un cuerpo que se llama **cuerpo fijo de G**. $1 \in E^S$, $\alpha, \beta \in E^S \Rightarrow \sigma(\alpha \pm \beta) = \sigma(\alpha) \pm \sigma(\beta) = \alpha \pm \beta$, $\sigma(\alpha * \beta) = \sigma(\alpha) * \sigma(\beta) = \alpha * \beta$ $\forall \sigma \in S$.
2. $S_1 \subseteq S_2 \Rightarrow E^{S_2} \subseteq E^{S_1}$.
3. $G = Gal(E/F)$, $F \subseteq E^G \subseteq E$.

Ejemplo 60. $E = \mathbb{Q}(\sqrt[3]{2})$, $Gal(E/\mathbb{Q}) = \{id\} = G$, $E^G = E$.

Ejemplo 61. $E = \mathbb{F}_p(t)(\alpha)$ t transcendente en $\mathbb{F}_p$ y $\alpha^p = t$. E es c. de d. de $x^p - t = x^p - \alpha^p = (x-\alpha)^p$. $Gal((x-\alpha)^p) = \{id_{\mathbb{F}_p}\}$. $E^G = E$.

Ejemplo 62. $E = F(x_1, ..., x_n)$ x_i variables, E es el cuerpo de funciones racionales en n variables sobre F. $G = Gal(E/F)$, $S_n \cong H \leqslant G$. $\sigma \in S_n$ $\sigma(\frac{f(x_1,...,x_n)}{g(x_1,...,x_n)}) = \frac{f(x_{\sigma(1)},...,x_{\sigma(n)})}{g(x_{\sigma(1)},...,x_{\sigma(n)})}$.

$E^{S_n} = \{\alpha \in E : \sigma(\alpha) = \alpha \ \forall \sigma \in S_n\}$ es el **cuerpo de las funciones simétricas** en n variables. $\prod_{i=1}^n (T - x_i) \in E[T]$.
$\prod_{i=1}^n (T - x_i) = T^n - S_1(x_1, ..., x_n)T^{n-1} + ... + (-1)^{n-1}S_{n-1}(x_1, ..., x_n)T + (-1)^n S_n(x_1, ..., x_n)$

$S_1(x_1, ..., x_n) = x_1 + x_2 + ... + x_n$
$S_2(x_1, ..., x_n) = x_1x_2 + x_2x_3 + x_1x_3 + ... + x_{n-1}x_n = \sum_{i<j}^{x} {}_i x_j$
...
$S_n(x_1, ..., x_n) = x_1...x_n$

$\sigma \in S_n$, $\sigma(S_1(x_1, ..., x_n)) = x_{\sigma(1)} + x_{\sigma(2)} + ... + x_{\sigma(n)} = S_1(x_{\sigma(1)}, ..., x_{\sigma(n)})$
$\sigma(S_2(x_1, ..., x_n)) = \sigma(\sum_{i<j} x_i x_j) = \sum_{i<j} x_{\sigma(i)}x_{\sigma(j)} = S_2(x_{\sigma(1)}, ..., x_{\sigma(n)})$
...
$\sigma(S_n(x_1, ..., x_n)) = S_n(x_{\sigma(1)}, ..., x_{\sigma(n)})$

Lema 2. Sea E cuerpo. Sea $S = \{\sigma_1, ..., \sigma_n\} \subseteq Aut(E)$, $|S| = n$. Entonces $[E : E^S] \geqslant n$.

Demostración: Supongamos que $[E : E^S] = r < n$. $r = dim E$ como $E^S - e.v.$ Sea $\{\alpha_1, ..., \alpha_n\}$ base de E. Consideremos el siguiente sistema:

$$* \begin{cases} \sigma_1(\alpha_1)x_1 + ... + \sigma_n(\alpha_1)x_n = 0 \\ ... \\ \sigma_1(\alpha_r)x_1 + ... + \sigma_n(\alpha_r)x_n = 0 \end{cases}$$

$AX = 0$, $A \in M_{r\times n}(E)$, $rg(A) \leqslant r < n \Rightarrow$ existe solución no trivial de $*$. Sea $(a_1, ..., a_n) \in E^n$ tal que $\sum_{j=1}^n \sigma_j(\alpha_i)a_j = 0 \ \forall i = 1, ..., r$. Sea $\beta \in E$ entonces $\beta = \sum_{i=1}^r b_i\alpha_i$, $b_i \in E^S$.
$\sum_{j=1}^n a_j\sigma_j(\beta) = \sum_{j=1}^n a_j \sum_{i=1}^r b_i\sigma_j(\alpha_i) = \sum_{i=1}^r b_i \sum_{j=1}^n a_j\sigma_j(\alpha_i) = 0 \ \forall i = 1, ..., r$

Como esto ocurre $\forall \beta \in E$ y los $\sigma_1, ..., \sigma_n$ son independientes tenemos que $a_j = 0$ $\forall j = 1, ..., n$. Contradicción con la no trivialidad e la solución $(a_1, ..., a_n)$ de *.

Teorema III.12. Sea E cuerpo. Sea $G \leqslant Aut(E)$, G finito. Entonces $[E : E^G] = |G|$.

Demostración: Por el Lema 2, $[E : E^G] \geqslant |G| = n$. $G = \{\sigma_1, ..., \sigma_n\}$. Supongamos que $[E : E^G] > n$. Sean $\alpha_1, ..., \alpha_{n+1} \in E$ linealmente independientes sobre E^G. Consideremos el siguiente sistema:

$$* \begin{cases} \sigma_1(\alpha_1)x_1 + ... + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ ... \\ \sigma_n(\alpha_1)x_1 + ... + \sigma_n(\alpha_{n+1})x_{n+1} = 0 \end{cases}$$

$AX = 0$, $A \in M_{nx(n+1)}(E)$. $rg(A) \geqslant n < n+1$, por lo tanto el sistema * tiene solución no trivial.

Consideremos una solución de * no trivial con el mínimo número, digamos r, de componentes no nulas. Reordenando los α_i, y por lo tanto los x_i, y dividiendo por la componente r-ésima, podemos suponer que la solución de * es $(a_1, ..., a_{r-1}, 1, 0, ..., 0)$, $a_j \neq 0 \; \forall j = 1, ..., r$. $\sigma_i(\sum_{j=1}^{n+1} a_j\alpha_j) = \sum_{j=1}^{n+1} \sigma_i(a_j)\sigma_i(\alpha_j) = \sum_{j=1}^{n+1} a_j\sigma_j(\alpha_j) = 0 \; \forall i = 1, ..., n$. $\sigma_i \in Aut(E)$, por lo tanto, $\sum_{j=1}^{n+1} a_j\alpha_j = 0$, contradicción con $\alpha_1, ..., \alpha_{n+1}$ linealmente independientes.

$(a_1, ..., a_{r-1}, 1, 0, ..., 0)$ es solución de *, se puede suponer que $a_1 \notin E^G$ (reenumerando los α_j). $a_i \notin E^G \Rightarrow \exists k \in \{1, ..., n\}$ tal que $\sigma_k(a_i) \neq a_i$, $\sigma(\alpha_1)x_1 + ... + \sigma_i(\alpha_{n+1})x_{n+1} = 0$ $i = 1, ..., n$.

$(A)_i$, $a_i\sigma_i(\alpha_1) + ... + a_{r-1}\sigma_i(\alpha_{r-1}) + \sigma_i(\alpha_n) = 0 \; \forall i = 1, ..., n$. Aplicamos σ_k y sea $\sigma_s := \sigma_k\sigma_i$

$(B)_s$, $\sigma_k(a_i)\sigma_s(\alpha_1) + ... + \sigma_k(a_{r-1})\sigma_s(\alpha_{r-1}) + \sigma_s(\alpha_r) = 0$. G es un grupo, por lo tanto, $G = \{\sigma_1, ..., \sigma_n = \{\sigma_k\sigma_1, ..., \sigma_k\sigma_n\}, porlotanto, (B)_s \; \forall s = 1, ..., n$.

$(a_1, ..., a_{r-1}, 1, 0, ..., 0)$ es solución de * con mínimo número de componentes n nulas. $(A)_s ... (B)_s$, $(a_1 - \sigma_k(a_1))\sigma_s(\alpha_1) + ... + (a_{r-1} - \sigma_k(a_{r-1}))\sigma_r(\alpha_{r-1}) = 0 \; \forall s = 1, ..., n$.

Por lo tanto, $(a_1 - \sigma_k(a_1), ..., a_{r-1} - \sigma_k(a_{r-1}), 0, ..., 0)$ es solución de * no trivial $(a_1 \neq \sigma_k(a_i))$ con menos de r componentes no nulas. Contradicción con minimalidad de r.

Corolario 1. Sea E cuerpo. Sea $G \leqslant Aut(E)$, G finito. Entonces $\forall \sigma \in Aut(E)$, si σ deja fijo E^G entonces $\sigma \in G$.

Demostración: Sea $\sigma \in Aut(E)$. Si σ deja fijo E^G, $\sigma(\alpha) = \alpha \quad \forall \alpha \in E^G$, entonces $E^G = E^{G \cup \{\sigma\}}$. $G \subseteq G \cup \{\sigma\} \Rightarrow \tau(\alpha) = \alpha \; \forall \tau \in E^G$ y además, $\sigma(\alpha) = \alpha$, $\alpha \in E^{G \cup \{\sigma\}}$.
$|G| = [E : E^G] = [E : E^{G \cup \{\sigma\}}] \geqslant |G \cup \{\sigma\}| = |G|$, $\sigma \in G$.

Corolario 2. Sea E cuerpo. Sean $H_1, H_2 \leqslant Aut(E)$ finitos $H_1 \neq H_2 \Rightarrow E^{H_1} \neq E^{H_2}$.

Demostración: Si $E^{H_1} = E^{H_2}$, $\sigma \in H_1 \;\; \Leftrightarrow \sigma$ deja fijo $E^{H_1} \Leftrightarrow \sigma$ deja fijo $E^{H_2} \Leftrightarrow \sigma \in H_2$.

Observación: $G \leqslant Aut(E)$ finito, $Gal(E/E^G) = G$. $\sigma \in Gal(E/E^G) \Rightarrow \sigma \in Aut(E)$ y σ deja fijo E^G. Por el corolario 1, entonces $\sigma \in G$, por lo tanto $Gal(E/E^G) \subseteq G$. $\sigma \in G$ $\Rightarrow \sigma \in Aut(E)$ y σ deja fijo E^G, entonces $\sigma \in Gal(E/E^G)$.

Definición 58 (Extensión normal y extensión de Galois)**.** Sea E/F extensión finita de cuerpos.

1. E/F **extensión normal** si $\forall \alpha \in E$, $Irred(\alpha, F)$ se descompone en E (si E contiene una raíz de un polinomio irreducible de F) en E contiene todas las raíces del polinomio.
2. E/F **extensión de Galois** si E es el c. de d. de un polinomio separable de F.

Teorema III.12.2. E/F de Galois $\Rightarrow |Gal(E/F)| = [E : F]$.

Ejemplo 63. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal, $x^3 - 2$ y $\sqrt[3]{2}w \notin \mathbb{Q}(\sqrt[3]{2})$. $\mathbb{Q}(\sqrt[3]{2}, w)/\mathbb{Q}$ es de Galois.

Teorema III.13. (Caracterización de extensiones de Galois). Sea E/F extensión finita de cuerpos. Sea $G = Gal(E/F)$. Entonces las siguientes proposiciones son equivalentes:

1. E/F es extensión de Galois.
2. $E^G = F$.
3. E/F es normal y separable.

En particular, si E/F es de Galois, entonces E contiene todas las raíces de cualquier polinomio irreducible sobre F que tenga una raíz en E.

Demostración:

$(1) \to (2)$ E/F es de Galois. Por el Teorema II.2 $|G| = |Gal(E/F)| = [E : F]$. Por el Teorema III.12 $[E : E^G] = |G|$. $|G| = [E : F] = [E : E^G][E^G : F] = |G|[E^G : F]$ por lo tanto $[E^G : F] = 1$, $E^G = F$.

$(2) \to (3)$ Sea $\alpha \in E$, $p(x) = Irred(\alpha, F)$. Consideramos el conjunto
$\{\sigma(x) : \sigma \in G\} = \{\alpha_1, ..., \alpha_n\}$ $n \geqslant 1$, $\alpha_i \neq \alpha_j$ $\forall i \neq j$.

Sea $g(x) = \prod_{i=1}^{n}(x - \alpha_i) = x^n + s_1(\alpha_1, ..., \alpha_n)x^{n-1} + ... + s_n(\alpha_1, ..., \alpha_n)$, donde $s_i(\alpha_1, ..., \alpha_n)$ son polinomios simétricos elementales en $\alpha_1, ..., \alpha_n$. $\sigma \in G$, σ permuta las α_i, $i = 1, ..., n$ $\sigma(s_i(\alpha_1, ..., \alpha_n)) = s_i(\alpha\delta_{(1)}, ..., \alpha\delta_{(n)})$ donde $\alpha\delta_{(j)} := \sigma(\alpha_j)$.

Como las s_i son simétricas $\sigma(s_i(\alpha_1, ..., \alpha_n)) = s_i(\alpha_1, ..., \alpha_n)$, por lo tanto $\sigma g(x) = g(x)$ y esto ocurre para todo $\sigma \in G$. Así, por (2) $g(x) \in F[X]$.

Como $g(\alpha) = 0$, $p(x)|g(x)$ y $p(x)$ no tiene raíces múltiples y $p(x)$ se descompone en E. E/F es normal y separable. Vemos que es normal porque el $Irred(\alpha, F)$ se descompone, $\alpha \in E$ y todas las raíces de $Irred(\alpha, F)$ están en E.

(3) $\rightarrow$ (1) Supongamos E/F normal y separable. Si $E = F$, $a \in F$, E es c. de d. de $x - a$ en F, por lo que E/F es de Galois.

Si $E \neq F$. Sea $\alpha \in E \setminus F$. Sea $p_1(x) = Irred(\alpha_1, F)$ y sea F_1 c. de d. de p_1 en F. E/F es extensión normal por lo que p_1 se descompone en E, por lo que $F_1 \subseteq E$. E/F es separable, entonces p_1 es separable.

Si $E = F_1$ entonces E/F es de Galois. Si $F_1 \subset E$ entonces $\exists \alpha_2 \in E \setminus F_1$ y sea $p_2 = Irred(\alpha_2, F)$ (p_2 se descompone en E y es separable). Sea F_2 c. de d. de $p_1 p_2 \in F[X]$, $F_2 \subseteq E$ y $p_1 p_2$ es separable.

Si $F_2 = E$ queda demostrado. Si $F_2 \neq E$, repetimos el proceso. $F \subset F_1 \subset ... \subset F_m \subseteq E$ tal que F_m es c. de d. de $p_1 ... p_m \in F[x]$ separable. Como E/F es finita existe $s \in \mathbb{N}$ tal que $F_s = E$. Así E es c. de d. de $p_1 ... p_s \in F[X]$ separable. E/F es de Galois.

Teorema III.14. Teorema fundamental de la teoría de Galois. Sea E/F extensión de Galois (de cuerpos). Sea **G=Gal(E/F)**. Entonces,

1. Existe una biyección γ entre los **subgrupos de G** y los **cuerpos intermedios de E/F**, tal que para $H \leqslant G$, $\gamma(H) := E^H$.
   Su inversa es $F \subseteq F_1 \subseteq E$. $\delta(F_1) := Gal(E/F_1)$.
   En particular, $\delta\gamma(H) = Gal(E/E^H) = H$, $\gamma\delta(F_1) = E^{Gal(E/F_1)} = F_1$.
2. Sean $H_1, H_2 \leqslant G$, $H_1 \leqslant H_2 \Rightarrow E^{H_2} \subseteq E^{H_1}$ y $F_1 \subseteq F_2 \Rightarrow Gal(E/F_2) \leqslant Gal(E/F_1)$.
3. $[G : H] = [E^H : F]$ y $[F_1 : F] = [Gal(E/F) : Gal(E/F_1)]$.
4. F_1/F Galois $\Leftrightarrow Gal(E/F_1) \trianglelefteq G$.

Demostración:

(1) Veamos que γ es una biyección. $H_1 \neq H_2 \Rightarrow E^{H_1} \neq E^{H_2}$, por el Teorema III.12 γ es inyectiva.

F_1 es cuerpo intermedio de E/F, $Gal(E/F_1) \leqslant Gal(E/F)$ por lo tanto δ es aplicación. $\gamma\delta(F_1) = \gamma(Gal(E/F_1)) = E^{Gal(E/F_1)} = F_1$ por el Teorema III.13(2). $\gamma\delta = id$ porque γ es sobreyectiva, entonces γ es biyección y δ su inversa.

$Gal(E/E^H) = \delta(E^H) = \delta(\gamma(H)) = H$
$E^{Gal(E/F_1)} = \gamma(Gal(E/F_1)) = \gamma\delta(F_1) = F_1$.

(2) $H_1 \leqslant H_2, \alpha \in E^{H_2} \Rightarrow \sigma(\alpha) = \alpha \, \forall \sigma \in H_2 \Rightarrow \sigma(\alpha) = \alpha \, \forall \sigma \in H_1 \Rightarrow \alpha \in E^{H_1}$. $\sigma \in Gal(E/F_2)$ $\Rightarrow \sigma \in Aut(E)$ y $\sigma|_{F_2} = id|_{F_2} \Rightarrow \sigma \in Aut(E)$, $\sigma|_{F_1} = id \Rightarrow \sigma \in Gal(E/F_1)$.

(3) $F \subseteq F_1 \subseteq E$, $[F_1 : F] = \frac{[E:F]}{[E:F_1]} = \frac{|G|}{|Gal(E/F_1)|} = [G : Gal(E/F_1)]$
$[E^H : F] = [G : Gal(E/E^H)] = [G : H]$ (porque $F_1 = E^H$).

(4) ($\rightarrow$) Sea F_1/F extensión de Galois $F \subseteq F_1 \subseteq E$. E/F es c. de d. de un polinomio separable en F. Por el Teorema III.10, $Gal(E/F_1) \trianglelefteq Gal(E/F)$.

($\leftarrow$) Supongamos $Gal(E/F_1) \trianglelefteq G$ (obs $H \trianglelefteq G \Rightarrow \sigma E^H = E^{\sigma H \sigma^{-1} = E^H}$).

Sea $H = Gal(E/F_1)$, $H \trianglelefteq G$, $E^H = E^{Gal(E/F_1)=F_1}$. Veamos que E^H/F es de Galois. Por el Teorema III.13(3), basta demostrar que E^H/F es normal y separable.

- E^H/F es separable ya que $E^H \subseteq E$ y E/F es de Galois (por tanto separable).
- Veamos que E^H/F es normal. Sea $\alpha \in E^H$, $p(x) = Irred(\alpha, F)$ separable y se descompone en E ya que E/F es de Galois.

  Por el ejercicio 1 de H5 G actúa transitivamente sobre el conjunto $\{$ raíces de $p(x)\}$. Sea $\beta \in E$ tal que $p(\beta) = 0$, veamos que $\beta \in E^H$. Existe $\sigma \in G$ tal que $\sigma(\alpha) = \beta$. Como $H \trianglelefteq G$, $\sigma(\alpha) \in \sigma(E^H) = E^H$ por lo que $\beta \in E^H$.

Observación: Sea $F \subseteq F_1 \subseteq E$, $\sigma \in Gal(E/F)$, $Gal(E/\sigma F_1) = \sigma Gal(E/F_1)\sigma^{-1}$.

Observación: E cuerpo, $\sigma \in Aut(E)$, $H \leqslant Aut(E)$ finito. Entonces $E^{H^\sigma} = \sigma E^H$.
$\alpha \in E^{H^\sigma} = E^{\sigma H \sigma^{-1}} \Leftrightarrow \forall \tau \in H \; \sigma\tau\sigma^{-1}(\alpha) = \alpha \Leftrightarrow \forall \tau \in H \; \tau\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha) \Leftrightarrow {}^{-1}(\alpha) \in E^H$
$\Leftrightarrow \alpha \in \sigma E^H$.

Definición 59 (Retículo). Un retículo es $(R, \leqslant)$ conjunto parcialmente ordenado tal que $\forall a, b \in R$ existe un $sup\{a, b\} = a \vee b$ e $inf\{a, b\} = a \wedge b$.

Ejemplo 64. $H_1, H_2 \leqslant G$. $H_1 \vee H_2 =< H_1 H_2 >$. $H_1 \wedge H_2 = H_1 \cap H_2$.

Para E/F extensión de cuerpos, dados F_1, F_2 cuerpos intermedios de E/F:
$F_1 \vee F_2 = F_1 F_2$ (compuesto)
$F_1 \wedge F_2 = F_1 \cap F_2$

Observación: Sean $(R_1, \leqslant)$ y $(R_2, \leqslant)$ retículos y $\gamma : R_1 \to R_2$ biyección tal que
$a \leqslant b \Leftrightarrow \gamma(b) \leqslant \gamma(a)$.
Entonces $\gamma(a * b) = \gamma(a) \vee \gamma(b)$, $\gamma(a \vee b) = \gamma(a) \wedge \gamma(b)$.

Corolario al Teorema Fundamental. Sea E/F extensión de Galois.
Sean $H_1, H_2 \leqslant G = Gal(E/F)$. $\gamma : Subgr(G) \to C.Interm(E/F)$ es biyección tal que $H_1 \leqslant H_2 \Leftrightarrow \gamma(H_2) \leqslant \gamma(H_1)$.

Por lo tanto, $E^{H_1 \cap H_2} = E^{H_1} E^{H_2}$, $E^{H_1 \wedge H_2} = E^{H_1} \cap E^{H_2}$. Si F_1, F_2 es cuerpo intermedio de E/F entonces:
$Gal(E/F_1 \cap F_2) = Gal(E/F_1) \vee Gal(E/F_2)$
$Gal(E/F_1 F_2) = Gal(E/F_1) \wedge Gal(E/F_2)$

Demostración: Por el apartado 3 del Teorema Fundamental,
$H_1, H_2 \leqslant G \Rightarrow H_1 \leqslant H_2 \Rightarrow E^{H_2} \subseteq E^{H_1} \Leftrightarrow \gamma(H_2) \leqslant \gamma(H_1)$.
F_1, F_2 son cuerpos intermedios de E/F. $F_1 \subseteq F_2 \Rightarrow Gal(E/F_2) \leqslant Gal(E/F_1)$.
$H_1 \leqslant H_2 \Leftrightarrow \gamma(H_2) \leqslant \gamma(H_1)$. Por la observación queda demostrado.

4. Aplicaciones

Teorema IV.1. Si E/F es extensión de cuerpos finita y **separable** entonces existen solamente un número finito de cuerpos intermedios de E/F.

Demostración: Sea E/F extensión finita y separable. Sea E'/F cierre por descomposición de E/F. Veamos que E'/F es separable.

Si $E = F(\alpha_1, ..., \alpha_n)$ entonces $p_i = Irred(\alpha_i, F)$ es separable. E' es cuerpo de descomposición de $p_1(x)...p_n(x) = p(x)$ es separable. Además E'/F es de Galois.

Sea $G = Gal(E'/F)$. Por el Teorema Fundamental existe una biyección entre los cuerpos intermedios de E'/F y los subgrupos de G. Como $|G| = [E' : F]$ es finita, $|Subgr(G)|$ es finito y $|C.Interm(E'/F)|$ es finito.

Si F_1 es cuerpo intermedio de E/F, como $E \subseteq E'$, F_1 es cuerpo intermedio de E'/F. E/F tiene un número finito de cuerpos intermedios.

Comentario. Sea $\mathbb{F}_p(u, v)$, para u,v transcendentes y algebraicamente independientes (no algebraicos sobre el otro). Es un cuerpo de característica p. $[F(\sqrt[p]{u}, \sqrt[p]{v}) : F] = p^2$ (no es extensión separable). $F \subseteq F(a\sqrt[p]{u} + \sqrt[p]{v}) \subseteq F(\sqrt[p]{u}, \sqrt[p]{v}\ \forall a \in F$. Existen infinitos cuerpos infinitos del tipo $F \subseteq F(a\sqrt[p]{u} + \sqrt[p]{v})$.

Teorema IV.2. (Teorema del elemento primitivo). Sea E/F extensión de cuerpos finita y separable. Entonces existe $\alpha \in E$ tal que $E = F(\alpha)$. (α es un elemento primitivo de E/F).

Demostración: Si F es finito, entonces E es finito, $|E| = p^n$ para algún p primo y $n \geqslant 1$, por el corolario al Teorema III.3. $E = \mathbb{F}_p(\alpha) = F(\alpha)$.

Si F es infinito. Por el Teorema IV.1 la extensión E/F tiene una cantidad finita de cuerpos intermedios. $E = F(\alpha_1, ..., \alpha_n)$. Basta demostrar que $\forall \alpha, \beta \in E$ existe $\gamma \in E$ tal que $F(\alpha, \beta) = F(\gamma)$. Sean $\alpha, \beta \in E$. $F \to C.Interm(E/F)$; $a \to F(\alpha + a\beta)$.

F es infinito y $|C.Interm(E/F)|$ es finito . $\exists a, b \in F$ tal que $a \neq b$, $a, b \neq 0$ tal que $F(\alpha + a\beta) = F(\alpha + b\beta)$. Sea $\gamma = \alpha + a\beta$, $\alpha + a\beta$, $\alpha + b\beta \in F(\gamma)$. $(a - b)\beta \in F(\beta)$. $\beta \in F(\gamma)$. $\alpha \in F(\gamma)$, $F(\alpha, \beta) \subseteq F(\gamma)$. $\gamma \in F(\alpha, \beta)$. $F(\gamma) = F(\alpha, \beta)$.

Teorema IV.3. Sea F cuerpo, $ch(F) = 0$. Sea E/F extensión de Galois, $Gal(E/F)$ es resoluble $\Leftrightarrow \exists E' \supseteq E$ tal que E'/F es radical.

Corolario 1. Sea F cuerpo de $ch(F) = 0$. Sea $f(x) \in F[x]$. $Gal(f)$ resoluble $\Leftrightarrow$ f resoluble por radicales.

Demostración: ($\rightarrow$) Sea E/F c. de d. de $f(x) \in F[x]$. $Gal(f) = Gal(E/F)$ resoluble. Por el Teorema, existe $E' \supseteq E$ tal que E'/F es extensión radical. Como f se descompone en $E \subseteq E'$, por definición, f es resoluble por radicales.

($\leftarrow$) Visto en el Teorema III.2.

Lema 1. Sea E/F extensión de Galois con $[E : F] = p$, p primo. Si existe $\omega \in F$ tal que $\omega^p = 1$, $\omega \neq 1$ (no es raíz p-ésmia primitiva de la unidad), entonces $\exists \beta \in E$ tal que $E = F(\beta)$ y $\beta^p \in F$. ($F \subseteq F(\beta) = E$, es pura de tipo primo).

Demostración: Sea $G = Gal(E/F)$. E/F es de Galois, entonces $|G| = [E : F] = p$, por lo que $|G| = p$, $G \approxeq \mathbb{Z}/p\mathbb{Z}$, por lo tanto, $G =< \sigma >$. $\sigma \neq id$, $\sigma^p = id$. $G = \{1, \sigma, \sigma^2, ..., \sigma^{p-1}\}$ (independientes).

Basta encontrar un $\beta \in E$ tal que $\sigma(\beta) = \omega^{-1}\beta$. $\omega = \frac{\beta}{\sigma(\beta)} \Rightarrow 1 = \omega^p = \frac{\beta^p}{(\sigma(\beta))^p} = \frac{\beta^p}{\sigma(\beta)^p}$.

$\sigma(\beta^p) = \beta^p$ por lo tanto, $a = \beta^p \in F$. $x^p - a \in F[x]$ (Corolario 2 al Teorema III.6). F cuerpo primo $\omega \in F$ (ω raíz p-ésima primitiva de 1). Entonces $x^p - a$ es irreducible en F o se descompone en F, $\sigma(\beta) = \omega^{-1}\beta \Rightarrow \beta \notin F$ por lo que $x^p - a$ no se descompone en F. $x^p - a$ es irreducible, $[F(\beta) : F] = gr(Irred(\beta; F)) = gr(x^p - a) = p$. $F(\beta) \subseteq E$, entonces $E = F(\beta)$.

Veamos que existe $\beta \in E$ tal que $\sigma(\beta) = \omega^{-1}\beta$, por lo tanto $\sigma \in Aut(E) \subseteq End(E)$. Por lo tanto lo que buscamos es un vector propio de $\beta \in E$ asociado a un valor propio ω^{-1}.

Por lo tanto, basta demostrar que ω^{-1} es un autovalor. σ es raíz de $x^p - 1 \in F[x]$. Como $\{1, \sigma, \sigma^2, ..., \sigma^{p-1}\}$ son independientes. σ no es raíz de ningún polinomio de F[x] de grado menor que p, por lo que $x^p - 1$ es el polinomio mínimo de $\sigma \in End(E)$.

$p = gr(x^p - 1)$, $p = dim_F E$ = gr(polinomio característico de σ). $x^p - 1$ es el polinomio característico de σ, $x^p - 1$ es el polinomio característico de σ y $(w^{-1})^p = w^p = 1$. Por lo tanto, w^{-1} es un autovector de σ.

Lema 2. Sea E/F c. de d. de $f(x) \in F[x]$. Sea $G = Gal(E/F)$ si F'/F y E'/F' es c. de d. de $f(x) \in F'[x]$ con $E \subseteq E'$. Entonces $Gal(E'/F') \rightarrow Gal(E/F)$; $\sigma \rightarrow \sigma|_E$ es un homomorfismo inyectivo.

Demostración: $E = F(\alpha_1, ..., \alpha_n)$ $\{\alpha_1, ..., \alpha_n\} = \{$ raíces de f$\}$. $E' = F'(\alpha_1, ..., \alpha_n)$ $\sigma \in Gal(E'/F')$ $\sigma|_F = id_F$, entonces $\sigma|_F = id_F$. σ conmuta las α_i, $i = 1, ..., n$, $\sigma(E) \subseteq E$. Por lo tanto, $\sigma|_E \in Gal(E/F)$, $\sigma \rightarrow \sigma|_E$ es homomorfismo. $\sigma \in Gal(E'/F')$ y $\sigma|_E = id_E \Rightarrow \sigma(\alpha_i) = \alpha_i$ $\forall i = 1, ..., n$. $\sigma = id_{E'}$, el homomorfismo es inyectivo.

Teorema IV.3 Sea F cuerpo, $ch(F) = 0$. Sea E/F extensión de Galois, $Gal(E/F)$ es resoluble $\Leftrightarrow \exists E' \supseteq E$ tal que E'/F es radical.

Demostración: Sea E/F c. de d. de $f(x) \in F[x]$. f(x) separable.

($\leftarrow$) Si existe $E' \supseteq E$ tal que E'/F es radical entonces, como f se descompone en E', f es resoluble por radicales. Por lo tanto, $Gal(f) = Gal(E/F)$ es resoluble (Teorema III.2).

($\rightarrow$) E/F Galois $\Rightarrow$ G = Gal(E/F). $|G| = [E : F]$ por ser c. de d. de un polinomio separable. Por inducción en $|[E : F]|$, $[E : F] = 1$ tomamos $E' = E$. $[E : F] \geqslant 1$, $G = Gal(E/F) \neq \{1\}$, y G es resoluble. Por el Corolario 5 al Teorema III.9 existe $H \trianglelefteq G$ tal que $[G : H] = p$ primo. Sea ω una raíz p-ésima primitiva de 1 (que existe en una extensión de F ya que $ch(F) = 0$).

- Si $\omega \in F$, entonces $F \subseteq E^H \subseteq E$. $G \neq H$, $F = E^G \neq E^H$. $[E : F] = [E : E^H][E^H : F]$ $(E^H : F] \neq 1$, por lo tanto, $[E : E^H] < [E : F]$.

  E/E^H es de Galois. $Gal(E/E^H) = H \geqslant G$ resoluble. Por hipótesis de inducción, existe $E' \supseteq E^H$ tal que E'/E^H es radical. $H \trianglelefteq G$, por el Teorema Fundamental E^H/F es de Galois.

  $[E^H : F] = [G : H] = p$. Por el Lema 1, $\exists \beta \in E^H$ tal que $E^H = F(\beta)$, $\beta^p \in F$. $F \subseteq F(\beta)$ pura de tipo p. $F \subseteq F(\beta) = E^H \subseteq F$ (E^H/F radical), por lo que E/F es radical.

- Si $\omega \notin F$ (caso general). $F' = F(\omega)$ y $E' = E(\omega)$. E' es c. de d. de $f(x) \in F'[x]$. Por el Lema 2, $G = Gal(E'/F')G_2 \leqslant Gal(E/F) = G$, G es resoluble.

  Si $G_2 < G$ (propio), entonces $[E' : F'] < [E : F]$. Por hipótesis de inducción, existe $E'' \supseteq E'$ tal que E''/F' es radical. $F \subseteq F(\omega) = F' \subseteq E''$, $F(w)/F$ extensión pura de tipo p. E''/F es radical y $E'' \supseteq E$.

  Si $G_2 = G$, G_1G entonces existe $H_1 \trianglelefteq G_1$, $[G_1 : H_1] = p$. Como $w \in F'$ podemos obtener como en el caso $\omega \in F$ un E''/F radical con $E' \subseteq E''$. Así, $F \subseteq F(w) = F' \subseteq E''$. Por lo tanto, E''/F es radical.

5. Resumen

Extensiones de cuerpos

- E/F extensión de cuerpos si existe $\psi : F \to E$ homomorfismo de cuerpos. Todo homomorfismo de cuerpos es inyectivo. F es subcuerpo de E. **E es un F-espacio vectorial**. El **grado de E sobre F** es $[E : F] = \dim_F E$.
- Dado F cuerpo y $p(x) \in F[x]$ irreducible, $E := F[x]/(p(x))$ es una extensión de F y p(x) tiene una raíz en E.
- **Teorema de Kronecker**. Sea F cuerpo y $f(x) \in F[x] \setminus F$. Entonces existe E/F tal que f(x) se descompone en E (tiene todas las raíces en E).
- Sea E/F extensión de cuerpo. Sea $\alpha \in E$, $p(x) \in F[X]$ polinomio mónico e irreducible en F tal que $p(\alpha) = 0$ en E. Entonces
  1. $\forall f(x) \in F[X]^*$, $f(\alpha) = 0 \Rightarrow gr(p(x)) \leqslant gr(f(x))$.
  2. p(x) es el único polinomio mónico de grado $gr(p(x))$ tal que $p(\alpha) = 0$.
- Sea $p(x) \in F[x]$ irreducible con $gr(p(x)) = d$. Entonces $\mathbf{E := F[X]/(p(x))}$ $\mathbf{[E : F] = gr(p(x))}$. La base de E como F-ev es $\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$.
  $F[X]/(p(x)) \cong F(\alpha) = \{a_0 + a_1\alpha + ... + a_{d-1}\alpha^{d-1} : a_i \in F \ \forall i = 0, ..., d\}$.
- α es **algebraico** sobre F si $\exists p(x) \in F[x]^*$ tal que $p(\alpha) = 0$. α es **transcendente** sobre F si no es algebraico.
- E/F finita $\Rightarrow$ [E/F algebraica $\Leftrightarrow \forall x \in E$, x es algebraico sobre F].
- Sea F cuerpo, E/F. $\alpha \in E$ algebraico sobre F. $\exists p(x) \in F[x]$ mónico e irreducible tal que $p(\alpha) = 0$. p(x) es el único polinomio de grado mínimo de F[x] que tiene a α como raíz.
- **Cuerpo primo** de F es el mínimo subcuerpo de F, la intersección de todos los subcuerpos de F. Todo cuerpo es extensión de su cuerpo primo.
- Sea F cuerpo, E cuerpo primo de F es isomorfo a $\mathbb{Q}$ o a $\mathbb{F}_p$ para algún primo p. Si $\mathbb{Q}$ es el cuerpo primo de F, $ch(F) = 0$. Si $\mathbb{F}_p$ es el cuerpo primo de F $\Rightarrow$ ch(F) = p. $ch(\mathbb{F}_p(x)) = p$.
- Si $ch(F) = p \Rightarrow \forall a, b \in F \ (a + b)^p = a^p + b^p$ y $\forall n \in \mathbb{N}$, $(a + b)^{p^n} = a^{p^n} + b^{p^n}$.
- Para cada p primo y cada $n \in \mathbb{N}^*$ existe un cuerpo de p^n elementos.
- **Fórmula de los grados**. Sea $F \subset B \subseteq E$ extensiones de cuerpos, con $[E : B] = m$ y $[B : F] = n$ finitas. Entonces E/F es finita y $[E : F] = mn$. $\mathbf{[E : F] = [E : B][B : F]}$.

Cuerpos de descomposición

- Sea F cuerpo y $f(x) \in F[x]$. Un **cuerpo de descomposición** de f(x) sobre F es una E/F tal que f(x) se descompone en E y no existe otro cuerpo E_1 tal que $F \subseteq E_1 \subseteq E$ tal que f se descompone en e.
- **Corolario al Teorema de Kronecker**. Todo polinomio sobre un cuerpo tiene un cuerpo de descomposición. E c. de d. de f(x) $\Rightarrow$ $[E : F]$ es finita.
- **Polinomio separable**. F cuerpo, $p(x) \in F[x]$ irreducible. p(x) es separable si no tiene raíces múltiples. Si $p(x)$ no es irreducible, es separable si f(x) es constante o $p(x)|f(x)$, p(x) irreducible y separable.
- F cuerpo con ch(F)=0 $\Rightarrow$ todo polinomio es separable. Sea F cuerpo con $ch(F) = p$ y $q(x) \in F[x]$ irreducible, $q(x)$ es separable $\Leftrightarrow$ $q'(x) \neq 0$.
- $\alpha \in E$, E/F para F cuerpo. $\boldsymbol{\alpha}$ **es separable** sobre F si es **transcendente sobre F** o $\mathbf{Irred}(\boldsymbol{\alpha}, \mathbf{F})$ es separable.
- E es una **extensión separable** de F si $\forall \alpha \in E$ α es separable en F. F es un **cuerpo perfecto** si todo $f(x) \in F[x]$ es separable. F es perfecto $\Leftrightarrow$ $ch(F) = 0$ o $ch(F) = p$ y $F = F^p$. Todo cuerpo finito es perfecto.
- Sea F finito y $ch(F) = p$, el automorfismo de Frobenius es: $\sigma_p : F \to F : a \to a^p$.
- F cuerpo con $ch(F) = p$ primo, $n \in \mathbb{N}^*$, $a \in F$. Entonces $\boldsymbol{x^{p^n} - a}$ es irreducible sobre F $\Leftrightarrow$ $\boldsymbol{a \notin F^p = \{b^p : b \in F\}}$.
- Sean $\psi : F \to F'$ y $\psi^* : F[x] \to F'[x]$ un isomorfismo de cuerpos y su isomorfismo de acu inducido. Sean $p(x) \in F[x]$ irreducible y $p^*(x) = \psi^*(p(x))$. Si β es una raíz de p(x) en una extensión de F y β' es una raíz de $p^*(x)$ en una extensión de F', entonces existe un único isomorfismo

$$\tilde{\psi} : F(\beta) \to F'(\beta') \text{ que extiende } \psi \text{ y tal que } \psi(\beta) = \beta'$$

- Sea $\psi : F \to F'$ un isomorfismo de cuerpos. Sea $f(x) \in F[x]$ y $f^*(x) = \psi^*(f(x))$. Sean E y E' c. de d. de f(x) sobre F y de $f^*(x)$ sobre F', respectivamente. Entonces:
  1. Existe un isomorfismo $\tilde{\psi} : E \to E'$ que extiende ψ.
  2. Si f(x) es separable $\Rightarrow$ ψ tiene exactamente $[E : F]$ extensiones $\tilde{\psi}$.
- Sea F cuerpo y $f(x) \in F[x]$. Entonces existe un único (salvo isomorfismos) cuerpo de descomposición de f.
- Para cada p primo y $n > 0$ existe un único cuerpo (salvo isomorfismos) de p^n elementos.

Grupo de Galois

- **Grupo de Galois**. Sea E/F extensión de cuerpo.

  $$\mathbf{Gal(E/F) = \{\sigma \in Aut(E) : \sigma|_F = id_F\}}$$

  sus elementos son F-automorfismos de E. Sea $f(x) \in F[x]$ y E c. de d. de f sobre F[x], $Gal(f(x)) := Gal(E/F)$. Si E es un cuerpo, Aut(E) es un grupo. $Gal(E/F) \leqslant Aut(E)$.

- Sea $f(x) \in F[x]$ y E/F, $\alpha \in E$, sea $\sigma \in Gal(E/F)$ con $f(\alpha) = 0 \Rightarrow f(\sigma(\alpha)) = 0$.

- Sea F cuerpo, $f(x) \in F[x]$, E c. de d. sobre F. Entonces,

  1. Si f tiene **n raíces** y se descompone en E $\Rightarrow$ $\mathbf{Gal(f) \approx H \leq S_n}$.
     $|Gal(f)|$ divide a $n!$.
  2. Si **f es separable**, $\mathbf{|Gal(f)| = |Gal(E/F)| = [E : F]}$.

- Sea $p(x) \in F[x]$ irreducible. E/F c. de d. de p(x) sobre F, $d = gr(p(x))$. Entonces $d|[E : F]$. Si f es separable $\Rightarrow$ d divide a $|Gal(f)|$.

Raíces de la unidad y cuerpo de Galois

Sea F cuerpo. $F^* = F \setminus \{0\}$.

- $G \leqslant F^*$. Si G es un grupo finito $\Rightarrow$ G es cíclico.

- **Raíz n-ésima de la unidad** en F es $a \in F^*$ tal que $\mathbf{a^n = 1}$ $\mathbf{o(a)|n}$.
  $G = \{a \in F : a^n = 1\}$ es cíclico (grupo de las raíces de la unidad de F).
  Raíz n-ésima primitiva de la unidad en F es $a \in F^*$ tal que $\mathbf{o(a) = n}$. Para $n > 1$, si un cuerpo contiene una raíz n-ésima primitiva de la unidad entonces contiene todas.

- $F = GF(p^n)$ con p primo el **cuerpo de Galois** con p^n elementos. Entonces F^* es cíclico y $F = \mathbb{F}_p(\alpha)$ con α raíz de un polinomio de grado n. $<\alpha>= F^* \Rightarrow F = \mathbb{F}_p(\alpha)$.

- Sea $\alpha \in F$ es **primitivo de un cuerpo finito** F con $ch(F) = p$ si $F = \mathbb{F}_p(\alpha)$. Sea $\alpha \in E$ es **primitivo para la extensión** E/F si $E = F(\alpha)$.

- $|F| = p^n$ con p primo, $F = \mathbb{F}_p(\alpha)$ con $n = [F : \mathbb{F}_p] = gr(Irred(\alpha, \mathbb{F}_p))$. F^* es un grupo cíclico de orden $p^n - 1$, generado por α, $F = <\alpha>$. $o(\alpha) = p^n - 1$, α es raíz $(p^n - 1)$-ésima primitiva de la unidad en F y α es raíz del polinomio $x^{p^n-1} - 1$.

- Sea F cuerpo finito, $\forall a, b \in F$, $a, b \notin F^2 \Rightarrow ab \in F^2$.

- $F = GF(p^n) \Rightarrow Gal(F/\mathbb{F}_p) = <\sigma_p>$ es cíclico de orden n (σ_p autom. Frob.)

- $E = F(\alpha)$ α **raíz n-ésima primitiva** de la unidad en E $\Rightarrow$ $\mathbf{Gal(E/F) \approx H \leq U(\mathbb{Z}/n\mathbb{Z})}$.
  En particular, $Gal(E/F)$ es abeliano.

Acciones de grupo

- Sea G grupo, X conjunto. **G actúa sobre X** si existe una aplicación $G \times X \to X$; $(g, x) \to gx$ tal que $1x = x$, $g(hx) = (gh)x$.
  $H \trianglelefteq G$, G actúa sobre H por conjugación, $gh := ghg^{-1}$.
  $G = Gal(E/F)$, $f(x) \in F[x]$, $Z = \{\alpha \in E : f(\alpha) = 0\}$, G actúa sobre Z, $\sigma\alpha := \sigma(\alpha) \in Z$.
- X conjunto, $x \in X$, G grupo que actúa sobre X.
  La **órbita de x** es $\mathbf{orb(x) = \{gx : g \in G\} \subseteq X}$.
  El **estabilizador de x** en G es $G_x = \{g \in G : gx = x\} \subseteq G$.
- Sea X conjunto, G grupo que actúa sobre X. **G actúa sobre X transitivamente** si $\forall x, y \in X$, $\exists g \in G$ tal que $gx = y$.
- Si $orb(x) = X \Rightarrow$ G actúa sobre X transitivamente.
- Sea F cuerpo, $f(x) \in F[x]$ y E/F c. de d. de f(x) en F. Sea $X = \{\alpha \in E : f(\alpha) = 0\}$. Entonces:
  1. f es irreducible $\Rightarrow$ Gal(E/F) actúa sobre X transitivamente.
  2. Si f no tiene raíces múltiples y Gal(E/F) actúa sobre X transitivamente $\Rightarrow$ f(x) es irreducible.
- Sea F cuerpo, $w \in F$ raíz n-ésima primitiva de 1. $f(x) = x^n - c \in F[x]$. Entonces $\exists \phi : Gal(f) \to \mathbb{Z}/n\mathbb{Z}$ homomorfismo inyectivo. Además ϕ es isomorfismo $\Leftrightarrow$ f es irreducible en F.
- Sea F cuerpo, $w \in F$ raíz n-ésima primitiva de 1. $ch(F) = p \Rightarrow$ p no divide a n.
- Sea p primo, $w \in F$ raíz p-ésima primitiva de 1. Sea $f(x) = x^p - c \in F[x]$. Entonces f se descompone en E y $Gal(f) = \{id\}$ o f irreducible en F y $Gal(f) = \mathbb{Z}/p\mathbb{Z}$.
- Sea G grupo y X conjunto, G actúa sobre X. Entonces $\forall x \in X$, $\mathbf{|orb(x)| = [G : G_x]}$.
  Si además G es finito, $|X| = n$ y G actúa sobre X transitivamente $\Rightarrow n \mid |G|$.
- **Subgrupo transitivo**. $G \leqslant S_n$ es transitivo si G actúa sobre I_n transitivamente.
- Sea G grupo finito, $H \leqslant G$ con $[G : H] = n \Rightarrow \exists \phi : G \to S_n$ homomorfismo, $Ker(\phi) \subset H$.
  S_5 no tiene ningún subgrupo de orden 30 o 40.
  $\forall \sigma$ 5-ciclo y τ trasposición, $\sigma, \tau \in S_5$, se tiene que $S_5 = <\sigma, \tau>$.

Resolubilidad

- **Serie normal en un grupo**. $\{1\} = G_n \leqslant G_{n-1} \leqslant ... \leqslant G_{i+1} \leqslant G_i \leqslant ... \leqslant G_1 \leqslant G_0 = G$ tal que $G_{i+1} \trianglelefteq G_i$. Los grupos G_i/G_{i+1} son los grupos factores.
- **Grupo resoluble**. G es resoluble si tiene una serie normal tal que G_i/G_{i+1} son abelianos. (G abeliano $\Rightarrow$ G resoluble).
  $H \leqslant G$, H es abeliano si su índice es $|G : H| = 2$.
  $H \leqslant G$, H es abeliano si es el único subgrupo de orden $|H| < \infty$.
- **Conmutador**. Sea G grupo, $x, y \in G$. El conmutador de x e y es $[x, y] = \mathbf{xyx^{-1}y^{-1}} \in \mathbf{G}$.
  El **subgrupo permutador** de G es: $G' = [G, G] = <\{[x, y] : x, y \in G\}>$. $[x, y]^{-1} = [y, x]$.
  $G' \trianglelefteq G$ y G/G' es abeliano.
  $N \trianglelefteq G$ y G/N abeliano $\Rightarrow G' \leqslant N$
  G' es el mínimo subgrupo normal de G tal que el cociente es abeliano, G/G' es el **abelianizado de G**.
- El **n-ésimo subgrupo conmutador** de un grupo G es $G^{(n)}$. $G^{(0)} = G$, $G^{(n+1)} := (G^{(n)})'$.
- G grupo resoluble $\Leftrightarrow \exists n \in \mathbb{N}$ tal que $G^{(n)} = \{1\}$.
- Sea G grupo resoluble, entonces:
  1. $H \leqslant G \Rightarrow$ H resoluble.
  2. $\phi : G \to H$ homomorfismo $\Rightarrow \phi(G)$ es resoluble. Si $N \trianglelefteq G \Rightarrow G/N$ es resoluble.
- G grupo, $N \trianglelefteq G$. Si N y G/N son resolubles $\Rightarrow$ G es resoluble.
- S_n es resoluble $\Leftrightarrow n \leqslant 4$.
  $H \leqslant S_5$, H resoluble $\Rightarrow |H| \leqslant 24$.
- $G \neq \{1\}$ un grupo abeliano finito $\Rightarrow$ contiene un subgrupo de índice primo.
  $G \neq \{1\}$ un grupo finito resoluble $\Rightarrow$ G tiene un subgrupo de índice primo.

Extensiones radicales

- **Extensión pura**. E/F, $E = F(\alpha)$ para algún α tal que $\alpha^m \in F$ para algún $m > 0$.
  Extensión pura de tipo m. E/F pura $E = F(\alpha)$ con $\alpha^m \in F$ y m mínimo.
- **Extensión radical**. E/F es radical si existe $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_t = E$ extensiones tales que F_{i+1}/F_i es pura $\forall i = 1, ..., t-1$.
- **Polinomio resoluble por radicales**. $f(x) \in F[x]$, F cuerpo, $f(x)$ es resoluble por radicales si existe E/F radical tal que f se descompone en E.
- **Cuerpo intermedio**. $F \subseteq F_1 \subseteq E$ cuerpos, F_1 es el cuerpo intermedio de E/F.
- (Teorema III.10) Sean $F_1 \subseteq F_2 \subseteq F_3$ ext. de cuerpos tales que F_2/F_1 es c. de d. de $f(x) \in F_1[x]$ y F_3/F_1 es c. de d. de $g(x) \in F_1[x]$. Entonces $\mathbf{Gal(F_3/F_2) \trianglelefteq Gal(F_3/F_1)}$ y
  $\mathbf{Gal(F_3/F_1)/Gal(F_3/F_2) \approxeq Gal(F_2/F_1)}$
- **Cuerpo compuesto**. Sean $F_1, F_2 \subset E$ cuerpos. $F_1 \vee F_2$ es el mínimo subcuerpo de E que tiene a F_1 y a F_2.
- F_1/F extensión finita de cuerpos, existe E/F_1 tal que E/F es c. de d. de algún polinomio sobre F.
  Si $F_1 = F(\alpha_1, ..., \alpha_s)$ para algunos $\alpha_i \in F_i$ algebraico sobre F. $p_i = Irred(\alpha_i, F_i)$, E c. de d. de $f = p_1...p_s \in F[x]$. E es el **cierre por descomposición** de F_1/F.
- Sea F_1/F finita, E/F cierre por descomposición de F_1/F y sea $Gal(E/F) = \{\sigma_1, ..., \sigma_r\}$. Entonces $E = \sigma_1(F_1)...\sigma_r(F_1)$.
- $F \subseteq F_t$, F_t/F extensión radical de cuerpos. Sea $F_t \subseteq E$ y $\sigma \in Gal(E/F)$. Entonces $F \subseteq \sigma(F_t)$ es radical.
- $F \subseteq F_t$ extensión radical. Entonces existe $E \subseteq F_t$ tal que E/F es c. de d. y $F \subseteq E$, E radical. Dado f(x) $\in F[x]$, f(x) resoluble y E c. de d. de f en F $\Rightarrow \exists F \subseteq F_t$ radical y $F_t \subset E$ y F_t/F es c. de d. en F.
- Sea $f(x) \in F[x]$ resoluble por radicales, E c. de d. en f en F con $F \subset E$. Entonces:
  1. $\exists F = F_0 \subseteq F_1 \subseteq ... \subseteq F_t$ tal que $E \subseteq F_t$ y las extensiones F_i/F_{i-1} son puras y F_t/F son c. de d. en F de tipo p_i primo $(i = 1, ..., t)$.
  2. Si F_t/F es un radical como el anterior y si F contiene una raíz p_i-ésima primitiva de 1 para $i = 1, ..., t \Rightarrow Gal(E/F)$ es resoluble.
- Sea F cuerpo, $ch(F) = 0$. Sea $f(x) \in F[x]$. f es resoluble por radicales $\Rightarrow Gal(f)$ es resoluble.
- Existe $p(x) \in \mathbb{Z}[x]$ de grado 5 no resoluble por radicales.
  (Por ejemplo, $p(x) = x^5 - 4x + 2$, $Gal(p(x)) \approxeq S_5$ no es resoluble por radicales).

Extensiones de Galois

- **Carácter del grupo**. Sea G grupo, un caractér del grupo G de un cuerpo E es un homomorfismo $\chi : G \to E \setminus \{0\}$.
- **Cuerpo fijo**. E cuerpo, $S \subseteq Aut(E)$. $E^S = \{\alpha \in E : \sigma(\alpha) = \alpha \forall \sigma \in S\}$.
  1. $S = G$ grupo, E^G es el cuerpo fijo de G.
  2. $S_1 \subseteq S_2 \Rightarrow E^{S_2} \subseteq E^{S_1}$.
  3. $G = Gal(E/F)$, $F \subseteq E^G \subseteq E$
- E cuerpo, $S = \{\sigma_1, ..., \sigma_n\} \subseteq Aut(E)$, $|S| = n$. Entonces $[E : E^S] \geqslant n$.
- Sea E cuerpo, $G \leqslant Aut(E)$, G finito. Entonces $[E : E^G] = |G|$.
- Sea E cuerpo, $G \leqslant Aut(G)$, G finito. Entonces $\forall \sigma \in Aut(E)$, si σ deja fijo E^G $\Rightarrow \sigma \in G$.
- E cuerpo, $H_1, H_2 \leqslant Aut(E)$ finitos, $H_1 \neq H_2 \Rightarrow E^{H_1} \neq E^{H_2}$.
  $G \leqslant Aut(E)$ finito, $Gal(E/E^G) = G$.
- E/F extensión finita es una **extensión normal** si $\forall \alpha \in E$, $Irred(\alpha, F)$ se descompone en E (si contiene una raíz del pol. irred. contiene todas las raíces del polinomio).
- E/F ext. finita, E/F es una **extensión de Galois** si E es el c. de d. de un polinomio separable de F.
- E/F de Galois $\Rightarrow |Gal(E/F)| = [E : F]$.
- **Caracterización de extensiones de Galois**. E/F finita, $G = Gal(E/F)$. Entonces son equivalentes:
  1. E/F es extensión de Galois; 2. $E^G = F$; 3. E/F es normal y separable.
  En particular, si E/F es de Galois, entonces E contiene todas las raíces de cualquier polinomio irreducible sobre F que tenga una raíz en E.
- **Teorema fundamental de la teoría de Galois**. (Ver junto con dem.)
- **Corolario al Teorema fundamental**.

Índice alfabético