

CUERPOS. EXTENSIONES DE UN CUERPO

1.1.	Cuerpos .	1
1.2.	Subcuerpos.	4
1.3.	Característica de un cuerpo. Subcuerpo primo.	6
1.4.	Cuerpos finitos.	9
1.5.	Extensiones de un cuerpo.	14
1.6.	Extensiones trascendentes y extensiones algebraicas.	16
1.7.	Nota Bibliográfica.	19

1.1. CUERPOS:

Vemos en este primer apartado la definición de cuerpo o campo, junto con algunas condiciones básicas de caracterización y de propiedades de homomorfismo.

Def. 1.1:

Se llama, por definición, *cuerpo*, a todo anillo $(K, +, \cdot)$, con elemento unidad e ($1 \neq 0$) tal que $\forall a \in K - \{0\}, \exists a^{-1} \in K / a \cdot a^{-1} = a^{-1} \cdot a = e$.

Def. 1.2:

La ley "+" se llama *ley aditiva del cuerpo* y la ley "." se llama *ley multiplicativa*.

Prop. 1.1:

Para que un anillo $(K, +, \cdot)$ sea un cuerpo es condición necesaria y suficiente que $K - \{0\}$ sea un *grupo multiplicativo*.

En efecto:

Si $K' = K - \{0\}$ es grupo multiplicativo $\Rightarrow \forall a \in K', \exists a^{-1} \in K' / a \cdot a^{-1} = a^{-1} \cdot a = e$
 $\Rightarrow K$ es cuerpo (por Def. 1.1).

Si K es cuerpo $\Rightarrow \forall a \in K', \exists a^{-1} \in K' / a \cdot a^{-1} = a^{-1} \cdot a = e$ $\Rightarrow$ Es ley interna, asociativa, con elemento neutro (el elemento e) y simetrizada $\Rightarrow K' = K - \{0\}$ es grupo multiplicativo.

Prop. 1.2:

1º) En un cuerpo cualquiera K se cumple que $\forall (a, b) \in K' \times K$, las ecuaciones $a \cdot x = b$ y $y \cdot a = b$ tienen, cada una, una y solo una solución, dada por $x = b \cdot a^{-1}$, $y = b \cdot a^{-1}$.

2º) Dado un anillo cualquiera K tal que $K \neq \{0\}$ y tal que $\forall (a, b) \in K' \times K$ cada una de las ecuaciones $a \cdot x = b$, $y \cdot a = b$ tenga al menos una solución, entonces K es un cuerpo.

En efecto:

$$1^\circ) a \cdot x = b \Rightarrow a^{-1} \cdot a \cdot x = a^{-1} \cdot b \Rightarrow (a^{-1} \cdot a) \cdot x = a^{-1} \cdot b \Rightarrow e \cdot x = a^{-1} \cdot b \Rightarrow x = a^{-1} \cdot b.$$

$$y.a = b \quad \text{D} \quad y.a \cdot a^{-1} = b.a^{-1} \quad \text{D} \quad y.(a.a^{-1}) = b.a^{-1} \quad \text{D} \quad y.e = b.a^{-1} \quad \text{D} \quad y = b.a^{-1}.$$

si x' , y' fueran también soluciones respectivas de $a.x = b$ y de $y.a = b$, se tendrá:

$x' = a^{-1}.b$, $x = a^{-1}.b$, por lo que es $x' = x$ y la ecuación $a.x = b$ tiene solución única.

$y' = b.a^{-1}$, $y = b.a^{-1}$, por lo que es $y' = y$ y la ecuación $y.a = b$ tiene solución única.

2º) Sea $a \in K' = K - \{0\}$, entonces existe un e que es solución de la ecuación $a.x = a$ y existe también un e' que es solución de la ecuación $y.a = a$. Esto es, cumplen que $a.e = a$ y $e'.a = a$.

Además, es $e = e'$, elemento unidad de K :

$$\begin{aligned} \forall r \in K, \exists m \in K / m.a = r & \Rightarrow \left\{ \begin{array}{l} m.(a.e) = r \Rightarrow (m.a).e = r \Rightarrow r.e = r \\ (e'.a).m' = r' \Rightarrow e'.(a.m') = r' \Rightarrow e'.r' = r' \end{array} \right. \Rightarrow \\ \forall r' \in K, \exists m' \in K / a.m' = r' & \end{aligned}$$

$\Rightarrow e$ es, por tanto, elemento unidad a la derecha, y e' es elemento unidad a la izquierda, por lo que $e.e' = e'.e = e = e'$.

En cuanto al elemento simétrico, veamos:

$$\begin{aligned} \forall r \in K, \exists m \in K / m.a = r & \Rightarrow \left\{ \begin{array}{l} \exists a' \in K / a'.a = e \\ \exists a'' \in K / a.a'' = e \end{array} \right. \Rightarrow \exists a', a'' \in K / a'.a = a.a'' = e \Rightarrow \\ \forall r' \in K, \exists m' \in K / a.m' = r' & \Rightarrow \left\{ \begin{array}{l} \exists a' \in K / a'.a = e \\ \exists a'' \in K / a.a'' = e \end{array} \right. \\ \Rightarrow a'.(a.a'') = a'.e \Rightarrow (a'.a).a'' = a' \Rightarrow e.a'' = a' \Rightarrow a'' = a' \Rightarrow \forall a \in K - \{0\}, \\ \exists a^{-1} \in K / a.a^{-1} = a^{-1}.a = e & \end{aligned}$$

Por consiguiente, K es grupo multiplicativo D K es cuerpo.

Prop. 1.3:

Todo anillo íntegro, y en particular todo dominio de integridad con un número finito de elementos, es un cuerpo.

En efecto:

De Teoría de Grupos, $A' = A - \{0\}$ es un conjunto finito tal que "." es ley interna, asociativa, con elemento neutro y simplificativa $\Rightarrow (A, .)$ es un grupo multiplicativo $\Rightarrow (A, +, .)$ es cuerpo finito, por Prop. 1.1.

Prop. 1.4:

Para todo dominio de integridad D , existe un cuerpo K y un homomorfismo inyectivo

$$f: D \rightarrow K.$$

En efecto:

De Teoría de Anillos, K sería el cuerpo de fracciones del dominio de integridad D .

Prop. 1.5:

Sea K un cuerpo y A un anillo ($A \neq \{0\}$). Si $f: K \rightarrow A$ es un homomorfismo inyectivo, entonces $f(K) \subseteq A$ es un cuerpo isomorfo a K .

En efecto:

K cuerpo $\Rightarrow K$ anillo $\Rightarrow K$ anillo $\wedge f$ homomorfismo de anillos $\Rightarrow f(K)$ es subanillo de A .

Además:

a) $(f(K), +, \cdot)$ tiene elemento unidad:

Sea e el elemento unidad de $(K, +, \cdot) \Rightarrow \forall x \in K, f(x) = f(x \cdot e) = f(e \cdot x) = f(x) \cdot f(e) = f(e) \cdot f(x) \Rightarrow f(e)$ es elemento unidad de $f(K)$

b) La ley multiplicativa de $f(K)$ está simetrizada:

$f(e) = f(x \cdot x^{-1}) = f(x^{-1} \cdot x) \Rightarrow f(e) = f(x) \cdot f(x^{-1}) = f(x^{-1}) \cdot f(x) \Rightarrow f(x^{-1})$ es el inverso de $f(x) \Rightarrow f(x^{-1}) = [f(x)]^{-1}$.

Luego, $(f(K), +, \cdot)$ es un grupo multiplicativo, y, por Prop. 1.1., es un cuerpo que, por construcción, es isomorfo a K .

1.2. SUBCUERPOS:

Caracterizamos en esta página el concepto de subcuerpo de un cuerpo dado. Pretendemos establecer que el conjunto de los subcuerpos de un cuerpo K es una familia de Moore y retículo completo.

Def. 1.4:

Un subconjunto H de un cuerpo $(K, +, \cdot)$ se dice que es un subcuerpo de K si $(H, +, \cdot)$ es un cuerpo. Si $(H, +, \cdot)$ es un subcuerpo de $(K, +, \cdot)$ se dirá que K es un *supercuerpo* de $(H, +, \cdot)$.

El conjunto $B = \{z \in K / x \cdot z \cdot x^{-1} = z, \forall x \in K - \{0\}\}$, se llama *centro del cuerpo* K .

Prop. 1.6:

La condición necesaria y suficiente para que $H \subseteq K$ sea un subcuerpo de $(K, +, \cdot)$ es que:

$$\forall x, y \in H, y \neq 0 \quad (x - y) \in H, \quad x \cdot y^{-1} \in H$$

En efecto:

$$H \subseteq K \text{ subcuerpo de } K \iff (H - \{0\}) \text{ grupo aditivo y multiplicativo} \iff \\ \iff (\forall x, y \in H, y \neq 0 \quad (x - y) \in H, \quad x \cdot y^{-1} \in H)$$

Prop. 1.7:

El centro de un cuerpo K es un subcuerpo de K .

En efecto:

$$\forall z_1, z_2 \in B \setminus \{0\}, \forall x \in K - \{0\}, \begin{cases} x \cdot (z_1 - z_2) \cdot x^{-1} = x \cdot z_1 \cdot x^{-1} - x \cdot z_2 \cdot x^{-1} = z_1 - z_2 \\ x \cdot z_1 \cdot z_2^{-1} \cdot x^{-1} = x \cdot z_1 \cdot x^{-1} \cdot x \cdot z_2^{-1} \cdot x^{-1} = z_1 \cdot z_2^{-1} \end{cases} \Rightarrow \\ \Rightarrow \begin{cases} z_1 - z_2^{-1} \in B \\ z_1 \cdot z_2^{-1} \in B \end{cases} \Rightarrow (B, +, \cdot) \text{ es, por Prop. 1.6, un subcuerpo de } K.$$

Prop. 1.8:

La familia F_K de todos los subcuerpos de un cuerpo K es una *familia de Moore* y un *retículo completo*.

En efecto:

1º) Se sabe, de Teoría de Conjuntos, que una familia de partes de un conjunto A es una *Familia de Moore* si es cerrada para la intersección y si A es elemento de la familia. En el caso de la familia F_K de los subcuerpos de K :

- $K \in F_K$, pues K es subcuerpo de K .
- $\{H_i\} \in F_K$, colección de subcuerpos de $K \Rightarrow \bigcap_{i \in I} H_i = \bigcap_{i \in I} H_i \in F_K$

2º) Considerando $(F_K, \subseteq)$, toda subfamilia $\{S_i\}_{i \in I}$ de F_K tiene ínfimo y tiene supremo:

$$\inf\{S_i\}_{i \in I} = \bigcap_{i \in I} S_i$$

$$\sup\{S_i\}_{i \in I} = \bigcap\{H / H \in F_K \wedge S_i \subseteq H, \forall i \in I\}$$

Luego, $(F_K, \subseteq)$ es un retículo completo.

NOTA 1.: En realidad, toda familia de Moore es un retículo completo.

NOTA 2.: A toda familia de Moore, de partes definidas de K , le corresponde una *clausura de Moore*, que se define como una aplicación desde el conjunto de partes de K en el conjunto de partes definidas de K (F_K) de modo que a cada parte X de K le corresponde la mínima parte definida X' que contiene a X . En el caso de la familia de Moore de los subcuerpos, F_K , se tiene:

$$X \subseteq K \rightarrow X' = \bigcap\{H \in F_K / X \subseteq H\}$$

1.3. CARACTERÍSTICA DE UN CUERPO. SUBCUERPO PRIMO:

Se trata aquí de precisar el concepto de característica de un cuerpo y el de subcuerpo primo. Es importante tener en cuenta que solo los cuerpos finitos tienen característica no nula, y, como veremos más adelante, esto tiene gran importancia a la hora de resolver la ecuación $x^N - x = 0$, pues la característica del cuerpo de las raíces está relacionada con el grado de esta ecuación.

Def. 1.5:

Se llama característica de $x \in K - \{0\}$, *car* x , al mínimo entero positivo p tal que $p \cdot x = 0$. Será el elemento x de característica nula si solamente es $p \cdot x = 0$ cuando $p = 0$.

Prop. 1.9:

1º) Todos los elementos de un cuerpo K tienen la misma característica, que representará, por tanto, un invariante del cuerpo. Se llama *característica del cuerpo* y se puede simbolizar por *car* K .

2º) La característica de un cuerpo es cero, o bien, es un número primo.

3º) " $x \in K - \{0\}$ se tiene:

- Si *car* $K = 0$, entonces el subgrupo aditivo engendrado por x es monógeno infinito.
- Si *car* $K = p$, entonces el subgrupo aditivo engendrado por x es finito de orden p .

En efecto:

1º) La misma característica:

$$\begin{aligned} \text{car } x = p_x &\Rightarrow \begin{cases} p_x \cdot x = 0 \\ p_y \cdot y = 0 \end{cases} \Rightarrow \begin{cases} (p_x \cdot x) \cdot y = 0 \\ (p_y \cdot y) \cdot x = 0 \end{cases} \Rightarrow \begin{cases} p_x \cdot y = 0 \\ p_y \cdot x = 0 \end{cases} \Rightarrow p_x = p_y \end{aligned}$$

O sea, " $x \in K - \{0\}$, *car* $x = \text{constante} = \text{car } K$.

2º) La característica puede ser nula (si $p \cdot x = 0 \Rightarrow p = 0$), pues siempre es $0 \cdot x = 0$.

La característica no puede ser 1 o -1, pues siempre es $1 \cdot x = x \neq 0$ ó $(-1) \cdot x = -x \neq 0$.

La característica es, por tanto, 0 o bien un número primo $p \in \mathbb{Z} - \{-1, 0, 1\}$ donde p puede ser un número primo o un número compuesto.

Si p es compuesto, o sea si $p = c.h$ ($c, h \in \mathbb{Z} - \{-1, 0, 1\}$), se tendría:

$$\begin{aligned} p = c.h \\ p.e = 0 \end{aligned} \Rightarrow (c.h).e = (c.e).(h.e) = 0 \Rightarrow \begin{cases} c.e = 0 \\ h.e = 0 \end{cases} \Rightarrow$$

$\Rightarrow p$ no sería característica de K . Por tanto, p no puede ser compuesto, sino primo.

3º) Si $\text{car } K = 0$, entonces $G_x = \{mx / m \in \mathbb{Z}\}$ es un grupo monógeno infinito engendrado por

x . Y si $\text{car } K = p$, entonces $G_x = \{0, x, 2x, \dots, (p-1)x\}$ es un grupo monógeno infinito engendrado por p .

NOTA 3: De lo anterior se sabe que $(G_x, +)$, grupo monógeno aditivo engendrado por x , es finito o infinito, según que la característica del cuerpo sea nula o no nula, respectivamente. $(G_x, +)$ es un subgrupo de $(K, +)$, pero $(G_x, +, \cdot)$ no es, en general, subgrupo de $(K, +, \cdot)$, pues, por ejemplo, si es $G_x = \{0, x, 2x, \dots, (p-1)x\}$ se tiene que " $r, s \in [1, (p-1)] \nsubseteq \mathbb{N}$, $rx.sx = rs.x^2 \notin G_x$, pues $x^2 \neq x$, salvo en los casos de idempotencia. Así, pues, los elementos de un cuerpo K engendran subgrupos aditivos de K , pero sólo los elementos idempotentes ($x^2 = x$) engendran subcuerpos de K . Uno de tales elementos es el elemento unidad, e , del cuerpo ($e^2 = e$).

Def. 1.6:

El subcuerpo del cuerpo $(K, +, \cdot)$ engendrado por el elemento unidad, e , recibe el nombre de *subcuerpo primo* de K . Se representará en adelante por la expresión $(\Pi_K, +, \cdot)$.

El subcuerpo primo es así, por construcción, el mínimo subcuerpo de K , contenido en cualquier otro subcuerpo de K . Esto quiere decir que los elementos mínimo y máximo del retículo completo de los subcuerpos de K (familia F_K) son:

$$\begin{aligned} \text{Mín}(F_K) &= P_K \\ \text{Máx}(F_K) &= K \end{aligned}$$

La proposición siguiente establece la expresión del subcuerpo primo.

Prop. 1.10:

El subcuerpo primo de K , P_K , es siempre cuerpo conmutativo y su expresión viene dada por:

$$\text{a) Si } \text{car } K = 0, \quad P_K = \{(me)(ne)^{-1} / m, n \in \mathbb{Z} \setminus \{0\}\}$$

$$\text{b) Si } \text{car } K = p \neq 0, \quad P_K = \{0, e, 2e, \dots, (p-1).e\}$$

En efecto:

La conmutatividad del subcuerpo primo es inmediata, pues $(re).(se) = r.se = s.re = se).(re)$, " $r, s \in \mathbb{Z}^2$ ", y se basa en la conmutatividad del anillo de los números enteros.

a) Si $\text{car } K = 0$, $L_K = \{(me)(ne)^{-1}/m, n \in \mathbb{Z} \setminus \{0\}\}$ cumple que $L_K \subseteq P_K$, y, además, L_K es cerrado para la multiplicación, que es asociativa, distributiva respecto a la adición y simetrizada, luego L_K es cuerpo $\mathcal{P} L_K = P_K$.

b) Si $\text{car } K = p$, $L_K = \{0, e, 2e, \dots, (p-1).e\}$ cumple que $L_K \subseteq P_K$ y tiene las propiedades de ser cerrado para la multiplicación, la cual es asociativa, distributiva a la suma y es simetrizada, luego L_K es un cuerpo $\mathcal{P} L_K = P_K$.

NOTA 4: El subcuerpo primo P_K está incluido en el centro B de K , pues se tiene que " $x \in K$, $x.(ne) = (ne).x$, y también $(ne)^{-1}.x = x.(ne)^{-1}$ ".

NOTA 5: El subcuerpo primo P_K de un cuerpo K de característica p , $P_K = \{0, e, 2e, \dots, (p-1).e\}$ es isomorfo al conjunto $\mathbb{Z}/p\mathbb{Z}$, que es también un cuerpo. Así, pues, se tiene que es:

$$P_K \cong \mathbb{Z}/p\mathbb{Z}, \text{ si } P_K \text{ es finito.}$$

1.4. CUERPOS FINITOS:

En este apartado estudiamos someramente los campos de Galois hasta lograr establecer que todo campo de Galois, K , es el cuerpo de descomposición del polinomio $p(x) = x^N - x$ donde $N = p^r$ es el orden del campo (p es la característica y r es la dimensión del espacio vectorial $(K, +, \cdot, \mathbb{P}_K)$), y, asimismo, que para toda potencia $N = p^r$, con p primo y r natural, existe un campo de Galois que descompone al polinomio $p(x) = x^N - x$. Establecemos, también, que todo campo de Galois es perfecto, esto es, que todo polinomio irreducible de $K[x]$ es separable (no tiene raíces múltiples).

Def. 1.7:

Un cuerpo con un número finito de elementos se llama *cuerpo finito*, o bien, *campo de Galois*. El orden de un campo de Galois, $O(K)$, es el cardinal del cuerpo.

Prop. 1.10:

La característica de un campo de Galois es un número primo.

En efecto:

Si $\text{car } K = 0 \Rightarrow \Pi_K = \{(m)(n)^{-1} \mid m, n \in \mathbb{Z} \times (\mathbb{Z} - \{0\})\}$ es infinito $\wedge \Pi_K \subseteq K \Rightarrow K$ es infinito $\Rightarrow K$ no es campo de Galois. Por tanto:

$$K \text{ campo de Galois} \Rightarrow \text{car } K \neq 0 \Rightarrow \text{car } K = p \Rightarrow p \text{ primo}$$

Prop. 1.11:

El orden de un campo de Galois es una potencia de su característica. O sea:

$$K \text{ campo de Galois} \Rightarrow \exists \hat{N} \mid O(K) = (\text{car } K)^{\hat{r}}$$

En efecto:

Sea el espacio vectorial $(K, +, \cdot, \mathbb{P}_K)$, donde el cuerpo finito K es el grupo abeliano de los vectores del espacio y donde el cuerpo primo de K , $\mathbb{P}_K$, es el cuerpo de los escalares. Sea r la dimensión de este espacio vectorial y sea $\{v_1, v_2, \dots, v_r\}$ una base. En estas condiciones, se tiene:

$$\forall v \in K, v = a_1.v_1 + a_2.v_2 + \dots + a_r.v_r, \quad a_i \in \mathbb{P}_K$$

esto quiere decir que el número total de vectores del espacio (o cardinal de K) coincide con todas las maneras de tomar los p elementos a_i del cuerpo P_k en subconjuntos de r elementos. Son, pues las variaciones con repetición $O(K) = RVp, r = p^r \Rightarrow O(K) = (\text{car } K)^r$.

Prop. 1.12:

Sea K un campo de Galois de $N = p^r$ elementos (p primo). Entonces, K es, salvo isomorfismo, el cuerpo de descomposición del polinomio $x^N - x$. Además, K es isomorfo a todo campo de Galois con el mismo número de elementos.

En efecto:

Sabemos que el cuerpo de descomposición del polinomio $p(x)$ es el cuerpo cuyos elementos son las raíces de la ecuación $p(x) = 0$. En este caso es $p(x) = x^N - x$.

Sea $K' = K - \{0\}$. Si es $O(K) = N \Rightarrow O(K') = N - 1$.

"a $\in K'$, el orden del subgrupo cíclico $\langle a \rangle$ divide a $N - 1 \Rightarrow a^{N-1} = e \Rightarrow a^N = a \Rightarrow a^N - a = 0$. También es $0^N - 0 = 0$.

Entonces, "a $\in K$, $a^N - a = 0$ y todos los elementos de K son las raíces de la ecuación $x^N - x = 0$. O sea: $x^N - x = (x - a_1)(x - a_2) \dots (x - a_n) \Rightarrow K = \{a_1, a_2, \dots, a_N\}$.

El polinomio $x^N - x$ se descompone, pues, en $K[x]$, en factores lineales, sin que esto ocurra para otro cuerpo intermedio H ($H / P_k \subseteq H \subseteq K$), puesto que si $H \neq K$, entonces no contiene todos los ceros de $x^N - x$.

Como el polinomio $x^N - x$ tiene los coeficientes en P_k (o sea, $x^N - x \in P_k[x]$), se tiene que el campo K queda determinado por dos números: por su subcuerpo primo P_k (o bien por su característica p) y por el número r tal que $N = p^r$, ya que su determinación quedaría reducida, entonces, a obtener el cuerpo de descomposición de $x^N - x \in P_k[x]$, cuerpo de descomposición que es único, salvo isomorfismo. De esto se deduce que dos campos de Galois de igual orden son isomorfos.

Prop. 1.13:

Dado p primo y r entero positivo, existe un campo de Galois K , tal que $O(K) = p^r$.

En efecto:

Para todo p primo existe el cuerpo Z / pz de las clases de restos módulo p .

Sea $P_k = \{0, e, 2.e, \dots, (p-1).e\}$ uno de los infinitos cuerpos primos isomorfos a Z / pz , siendo $p = \text{car}(P_k)$.

Sea el polinomio $p(x) = x^N - x \in P_k[x]$, con $N = p^r$, y sea L un supercuerpo de P_k tal que es cuerpo de descomposición de todo polinomio de $P_k[x]$ en factores lineales.

Veamos que los ceros de $p(x) = x^N - x$ son todos distintos:

$p'(x) = N \cdot x^{N-1} - e = 0 - e = -e \neq 0$ (pues $N \cdot x = 0$, " $x \notin L$ "). Entonces al ser $p'(x) \neq 0$, " $x \notin L$ ", $p(x)$ no tiene raíces múltiples.

Veamos que el conjunto $\{a_1, a_2, \dots, a_N\}$ de los ceros de $p(x) = x^N - x$ es un cuerpo:

$$\begin{aligned} \text{a) } \forall a_i, a_j \in K, a_i^N = a_i \wedge a_j^N = a_j &\Rightarrow (a_i - a_j)^N = \sum_{k=0}^N \binom{N}{k} a_i^k (-a_j)^{N-k} = \\ &= a_i^N - a_j^N = a_i - a_j \Rightarrow (a_i - a_j)^N = a_i - a_j \Rightarrow a_i - a_j \in K. \\ \text{b) } \forall a_i, a_j \in K, a_i^N = a_i \wedge a_j^N = a_j &\Rightarrow (a_i \cdot a_j^{-1})^N = a_i^N \cdot (a_j^{-1})^N = a_i \cdot a_j^{-1} \Rightarrow \\ &\Rightarrow a_i \cdot a_j^{-1} \in K \end{aligned}$$

Se acostumbra de denominar a este cuerpo K mediante $\text{CG}(p^r)$, o bien, $\text{CF}(p^r)$.

Prop. 1.14:

1º) El producto de los elementos no nulos de un campo de Galois es igual a $-e$.

2º) Si $K = \mathbb{Z} / p\mathbb{Z}$, entonces " $x \in \mathbb{Z}$, $x^p \equiv x \pmod{p}$ ". (Teorema de Fermat)

3º) Si $K = \mathbb{Z} / p\mathbb{Z}$, entonces $(p-1)! \equiv -1 \pmod{p}$. (Teorema de Wilson)

En efecto:

$$\begin{aligned} 1^\circ) \quad x^N - x &= \prod_{i=1}^N (x - a_i) = (x - 0) \cdot \prod_{i=1}^{N-1} (x - a_i) = x \cdot \prod_{i=1}^{N-1} (x - a_i) \Rightarrow x^{N-1} - e = \\ &= \prod_{i=1}^{N-1} (x - a_i) = \prod_{i=1}^{N-1} x + \prod_{i=1}^{N-1} a_i = x^{N-1} + \prod_{i=1}^{N-1} a_i \Rightarrow -e = \prod_{i=1}^{N-1} a_i \end{aligned}$$

2º) si es $K = \mathbb{Z} / p\mathbb{Z}$, $K = \text{CG}(p) = \mathbb{P}_k \ni x^p \equiv x \pmod{p}$, " $x \in \mathbb{Z}$ "

3º) Si es $K = \mathbb{Z} / p\mathbb{Z}$, $K = \text{CG}(p) = \mathbb{P}_k = \{0, e, 2.e, \dots, (p-1).e\} \cup e = 1 \in \mathbb{P}$
 $\mathbb{P} \setminus \mathbb{P}_k = \{0, 1, 2, \dots, (p-1)\} \ni -1 = 1 \cdot 2 \cdot \dots \cdot (p-1) \in \mathbb{P}$
 $(p-1)! \equiv -1$

Prop. 1.15:

Si K es un campo finito tal que $O(K) = N = p^r$, entonces el grupo multiplicativo $K' = K - \{0\}$ es cíclico.

En efecto:

Sea $K' = K - \{0\}$. El orden de K' es $O(K') = N - 1 = m$. Vamos a comprobar que existe un elemento ξ de K' que genera al grupo multiplicativo $(K', +)$.

Como los elementos de K verifican $x^N - x = 0$, los de K' verifican $x^{N-1} - e = 0$, o bien que $x^m = e$.

Sea la descomposición de m en factores primos la siguiente: $m = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$

$x^{m/p_i} = e$ tiene m/p_i raíces en K' , todas distintas. Eligiendo un u_i distinto de cualquiera de las raíces de la ecuación $x^{m/p_i} = e$. Se tiene:

llamando $u_i^{m/p_i^{a_i}} = e \Rightarrow c_i^{p_i^{a_i}} = \left(u_i^{m/p_i^{a_i}}\right)^{p_i^{a_i}} = u_i^m = e \Rightarrow$ el orden de c_i es divisor de $p_i^{a_i}$. Veamos que el orden de c_i es $p_i^{a_i}$ exactamente:

pues si $c_i^{p_i^{a_i}} = u_i^m \neq e \Rightarrow$ (pues u no es, por construcción, raíz de $x_i^{m/p_i^{a_i}} - e = 0$) entonces el exponente mínimo de c_i con el que se obtiene e es $p_i^{a_i}$. De todo esto, $O(c_i) = p_i^{a_i}$.

Análogamente:

$$O(c_1) = p_1^{a_1}, \quad O(c_2) = p_2^{a_2}, \quad \dots, \quad O(c_k) = p_k^{a_k}$$

Por lo cual, el elemento

$$\xi = c_1 \cdot c_2 \cdot \dots \cdot c_k \Rightarrow O(\xi) = O(c_1) \cdot O(c_2) \cdot \dots \cdot O(c_k) = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k} = m$$

Es decir, en definitiva:

Existe un $\xi \in K'$ tal que su orden es el orden de $K' \Rightarrow K'$ es grupo multiplicativo cíclico.

El elemento generador ξ , que existe siempre en todo campo de Galois, recibe el nombre específico que se concreta en la definición siguiente.

Def. 1.8:

Se llama *raíz primitiva de la unidad*, de orden m , o bien, *raíz m -sima de la unidad*, en el cuerpo K , al elemento ξ generador del grupo cíclico conmutativo de orden m , $K' = K - \{0\}$.

Se puede extraer el siguiente corolario: *Todo cuerpo finito es conmutativo*. Pues todo grupo multiplicativo cíclico es conmutativo.

Prop. 1.16:

Todo campo de Galois es un cuerpo perfecto.

En efecto:

Un cuerpo K se dice *perfecto* si todo polinomio $f(x) \in K[x]$ irreducible es *separable*, es decir, no tiene raíces múltiples. Si un polinomio tuviera raíces múltiples, éstas anularían también al polinomio derivado $f'(x)$. Veamos que esto no ocurre en el anillo $K[x]$, cuando es K un cuerpo finito.

Si $f(x)$ y $f'(x)$ tuvieran una raíz común sería, para tal valor, $f(x) = 0$ y $f'(x) = 0$ y siendo $f(x)$ irreducible, $f'(x) = f(x).p(x)$, pero al ser $\text{grad } f(x) > \text{grad } f'(x) \Rightarrow f'(x) \equiv q(x) \equiv 0$

Para que $f'(x) \equiv 0$ es necesario y suficiente que $f(x)$ sea de la forma:

$$f(x) = c_0 + c_1.x^p + c_2.x^{2p} + \dots + c_s.x^{sp}, \quad c_i \in K$$

Pero en este caso no sería $f(x)$ irreducible, pues:

$$\forall c_i \in K \Rightarrow c_i^N - c_i = 0 \Rightarrow (c_i^p)^{p^{r-1}} - c_i = 0 \Rightarrow (c_i^{p^{r-1}})^p - c_i = 0 \Rightarrow a_i^p - c_i = 0,$$

siendo $a_i = c_i^{p^{r-1}}$. O sea:

$$f(x) = c_0 + c_1.x + \dots + c_s.x^{sp} = (a_0 + a_1.x + \dots + a_s.x^s)^p \Rightarrow f(x) \text{ no es irreducible}$$

Luego, si $f(x)$ es irreducible $\Rightarrow f(x)$ y $f'(x)$ no tienen raíces comunes $\Rightarrow f(x)$ es separable $\Rightarrow K$ es cuerpo perfecto.

1.5. EXTENSION DE UN CUERPO:

Veremos aquí el concepto de extensión de un cuerpo, de extensión por adjunción, de extensión simple, de extensión trascendente y de extensión algebraica, así como el hecho de que toda extensión por adjunción es una clausura de Moore en el retículo de los subcuerpos de un cuerpo dado.

Def. 1.9:

Se llama extensión de un cuerpo K a otro cuerpo L que contiene un subcuerpo isomorfo a K . Es claro que un cuerpo es una extensión de cualquiera de sus subcuerpos.

Def. 1.10:

Si el cuerpo L es extensión del cuerpo K , puede considerarse el espacio vectorial L sobre el cuerpo K . La dimensión de este espacio vectorial se llama grado de la extensión y se simboliza por $[L : K]$ o (L / K) , símbolos utilizados también para indicar que es L extensión sobre K y se lee " L sobre K ".

Def. 1.11:

Si K es un cuerpo, H subcuerpo de K y S una parte cualquiera de K , el mínimo subcuerpo que contiene a H y a S se denomina *extensión de H por adjunción de S* y se simboliza por $H(S)$.

Es claro que $H(S) = (H \cup S)'$, es decir, se trata de la clausura de Moore en la familia de Moore de los subcuerpos de K .

Si S tiene un solo elemento, $S = \{a\}$, $H(S)$ se dirá *extensión simple* del cuerpo H .

Prop. 1.17:

Si H es un subcuerpo de K y S_1, S_2 son dos partes cualesquiera de K , se cumple que:

$$H(S_1 \cup S_2) = H(S_1)(S_2)$$

En efecto:

Por definición es:

$$H(S_1 \cup S_2) = (H \cup (S_1 \cup S_2))' \quad (\text{clausura de Moore})$$

$$H(S_1)(S_2) = (H(S_1)U(S_2))' = ((HUS_1)' U S_2)' \quad (\text{clausura de Moore})$$

$$\text{a) puesto que } H, S_1, S_2 \subseteq H(S_1)(S_2) \Rightarrow H(S_1US_2) \subseteq H(S_1)(S_2)$$

$$\text{b) puesto que } H, S_1 \subseteq H(S_1US_2) \Rightarrow H(S_1) \subseteq H(S_1US_2) \Rightarrow H(S_1) \subseteq H(S_1US_2) \wedge S_2 \subseteq H(S_1US_2) \Rightarrow H(S_1)(S_2) \subseteq H(S_1US_2)$$

$$\text{Por tanto, de a) y de b), es } H(S_1)(S_2) = H(S_1US_2)$$

En particular, $H(a_1, a_2, \dots, a_n) = H(a_1)(a_2)\dots(a_n)$, es decir, se puede reemplazar la adjunción simultanea de n elementos del cuerpo K por n adjunciones sucesivas.

1.6. EXTENSIONES TRASCENDENTES Y ALGEBRAICAS:

Definimos los conceptos de extensión trascendente y de extensión algebraica de un cuerpo, y comprobamos que todo campo de Galois es extensión algebraica simple de su subcuerpo primo.

Prop. 1.18:

Dado un cuerpo conmutativo K , un subcuerpo L , y un homomorfismo $F: K[x] \rightarrow K[a]$, "a" $\in L$, tal que " $f(x) \in K[x]$ ", es $F(f(x)) = f(a)$, se cumple que los anillos $K[x]$ y $K[a]$ son K -isomorfos.

En efecto:

$$\text{Ker } F = \{f(x) \in K[x] / F(f(x)) = f(a) = 0\}$$

Los polinomios de $\text{ker } F$ son, pues, los $t_0 + t_1.x + t_2.x^2 + \dots + t_m.x^m$ tales que se verifica que

$$t_0 + t_1.a + t_2.a^2 + \dots + t_m.a^m = 0$$

Descomponiendo canónicamente el homomorfismo F , se tiene:

$$\begin{array}{ccc} K[x] & \rightarrow & K[a] \\ \downarrow & & \uparrow \\ K[x]/\text{Ker } F & \approx & K[a] \end{array}$$

De lo cual:

$K[x]/\text{Ker } F \cong K[a]$ y es un K -isomorfismo, pues todo elemento de K permanece fijo.

Def. 1.12:

1º) Dado L supercuerpo de K , se dice que $a \in L$ es *trascendente sobre K* si cualquier homomorfismo F de los definidos en Prop. 1.18 es tal que $\text{Ker } F = \{0\}$.

Esto es, si $a \in L$ es trascendente sobre K , entonces ningún polinomio no nulo $t_0 + t_1.x + t_2.x^2 + \dots + t_m.x^m$ se anula para $x = a$.

2º) Dado L supercuerpo de K , se dice que $a \in L$ es *algebraico sobre K* , si, para el homomorfismo F se tiene que $\text{Ker } F \neq \{0\}$.

Esto es, si $a \in L$ es algebraico sobre K , entonces existen polinomios no idénticamente nulos $t_0 + t_1.x + t_2.x^2 + \dots + t_m.x^m$ que se anulan para $x = a$:

$$t_0 + t_1.a + t_2.a^2 + \dots + t_m.a^m = 0$$

Def. 1.13:

1º) Una extensión L de K se dice *trascendente* si $\exists a \in L$ tal que a es transcendente sobre K . $\hat{L} / K \gg K$.

2º) Una extensión L de K se dice *algebraica* si $\forall a \in L$, a es algebraico sobre K . $\hat{L} / K \approx K$.

Prop. 1.19:

Sea $F: K[x] \rightarrow K[a]$ tal que, " $f(x) \in K[x]$, es $F(f(x)) = f(a)$ y sea $a \in L$ algebraico sobre K . $\hat{L}$, es decir, $\text{Ker } F \neq \{0\}$. Entonces se cumple que $\text{Ker } F$ es ideal principal, primo y maximal y se verifica que $K[x] / \text{Ker } F \approx K[a] = K(a)$.

En efecto:

a) $\text{Ker } F$ es principal por ser $K[x]$ anillo principal. Sea $p(x) \in K[x]$ la base de este ideal:

$$\text{Ker } F = (p(x))$$

b) $\text{Ker } F$ es irreducible, pues caso contrario sería $p(x) = p_1(x).p_2(x)$ y $p(a) = p_1(a).p_2(a) = 0 \Rightarrow p_1(a) = 0 \vee p_2(a) = 0$ (pues $K[a]$ es dominio de integridad) $\Rightarrow p_1(x) \in \text{Ker } F \vee p_2(x) \in \text{Ker } F \Rightarrow$ contradictorio con que $p(x)$ es base de $\text{Ker } F$.

Por tanto, $p(x)$ es irreducible y $\text{Ker } F = (p(x))$ es ideal primo.

c) En un anillo principal, sin divisores de cero, todo ideal primo es maximal. Luego $\text{Ker } F$ es, efectivamente, ideal principal, primo y maximal.

Por otra parte:

$$K[x] \text{ maximal} \Rightarrow \begin{cases} K[x] & \text{maximal} \\ K[x] & \text{con elem. unidad} \end{cases} \Rightarrow K[x] / \text{Ker } F \text{ cuerpo} \Rightarrow \begin{cases} K[x] / \text{Ker } F \text{ cuerpo} \\ K[x] / \text{Ker } F \approx K[a] \end{cases} \Rightarrow K[a] \text{ cuerpo}$$

Esto quiere decir que $K[a]$ es cuerpo y $K[a] \in K(a) \subseteq K(a)$ es el mínimo cuerpo que contiene a K y a a . Por tanto, es $K[a] = K(a)$.

Entonces: $K[x] / \text{Ker } F \approx K[a] = K(a)$

Prop. 1.20:

Todo cuerpo finito es extensión algebraica simple de su subcuerpo primo.

En efecto:

Por Prop. 1.15 sabemos que todo elemento de $K' = K - \{0\}$ es de la forma e^N , donde e es la raíz $(N-1)$ -ésima de la unidad:

$$e^N - e = 0$$

es decir, e es elemento de K algebraico sobre Π_k .

Por ser e generador de K' , se tiene que K es el mínimo cuerpo que contiene a Π_k y a e :

$$K = \Pi_k.(e) = \Pi_k.[e]$$

K es, pues, extensión simple de Π_k . y, como $e \in K$ es algebraico sobre Π_k , K es extensión simple de Π_k .

1.7. NOTA BIBLIOGRÁFICA:

1. Artin, E. Galois Theory.
2. Artin, E. Geometric Algebra
3. Birkhoff-Mc Lane. Algebra moderna.
4. Birkhoff, G., Bartee, T.C., Modern Applied Algebra, Mc Graw-Hill, 1970.
5. Bourbaki. Algebre, Ch. II - 3ra. Ed.
6. Bourbaki. Algebre, Ch. VII - 2da. Ed.
7. Bourbaki, N. Algèbre.
8. Burton, D.M., Introduction to Modern Abstract Algebra, Addison-Wesley, 1967.
9. Caton, G. y Grossman, S. J., Linear Algebra.,., Ed. Wordsworth Publ. Co. 1980.
10. Childs, L., A Concrete Introduction to Higher Algebra, Springer-Verlag, 1979.
11. Cignoli, R. O., Apuntes de la materia Lógica (Computadores): Algebras de Boole.
Cálculo proposicional.
12. Fraleigh, J. A First Course in Abstract Algebra.
13. Fraleigh, J.B., A First Course in Abstract Algebra, Addison-Wesley, 1967.
14. Friedberg, S, Insel, A, Spence, L., Linear Algebra, Prentice Hall (1979).
15. Gamtmacher, F. R., The Theory of Mathematics., Vol. I y II., Ed. Chelsea, 1974.
16. Gentile, E., Estructuras algebraicas I. (Public. OEA).
17. Gentile, E., Notas de Algebra (EUDEBA).
18. Gentile, E., Notas de Algebra II, Editorial Docencia.
19. Godement, R., Cours d'algèbre.
20. Herstein, I. N., Algebra Moderna.
21. Herstein, I. N., Topics in Algebra.
22. Hoffman, K y R. Kunze, Algebra lineal, Prentice Hall.
23. Hoffman, K, y R. Kunz, Linear Algebra, Prentice Hall, 1971.
24. Hungerford, T.W., Álgebra.
25. Jacobson, N., Lecture in Abstract Algebra, Princeton, N.J. Van Nostrand, 1951-1964.
26. Jacobson, N. Basic Algebra I.
27. Kaplansky, I. Linear Algebra and Geometry
28. Lang, Serge, Algebra lineal, Addison Wesley.
29. Larotonda, A., Algebra lineal y Geometría. Eudeba.
30. Lipschutz, S., Algebra lineal, Serie Schaum.
31. Rotman, J., The Theory of Groups.
32. Strang G., Algebra Lineal con aplicaciones., Ed. Fondo Educativo Interamericano, 1981.
33. Van der Waerden, B.L. Moderne Algebra.
34. Vargas, J.A. Algebra Abstracta.
35. Zariski, O. y Samuel, P. Commutative Algebra I y II.