# Campos de descomposición

Facultad de Ciencias UNAM

# Introducción

Antes de empezar, un par de recordatorios amistosos: Supongamos que $F$ es un campo y que $p(x) \in F[x]$.

1. Si $\alpha_1, \ldots, \alpha_k \in F$ son raíces de $p(x)$, entonces

$$(x - \alpha_1) \cdots (x - \alpha_k) \text{ divide a } p(x) \text{ en } F[x]$$

   En particular, $p(x)$ tiene a lo mas $\deg p(x)$ raíces.

2. Existe una extensión de campos $K/F$ tal que $p(x)$ tiene una raíz en $K$.

   En lo que sigue, usaremos mucho este resultado, pero casi no usaremos específicamente a $K$. Por esta razón, casi siempre omitimos a $K$ y solo decimos "supongamos que $\alpha$ es una raíz de $f(x)$". De hecho, tomamos mas libertades y nos damos el lujo de considerar a $F(\alpha)$ sin especificar la extensión de campos sobre la cual estamos generando a $F(\alpha)$ (obviamente, esta extensión de campos es $K$).

# $f(x)$ se descompone en $K/F$

## Definición

Supongamos que $K/F$ es una extensión de campos y que $f(x) \in F[x]$. Decimos que $f(x)$ se **descompone en** $K/F$ si existen $c \in F$ y $\alpha_1, \ldots, \alpha_n \in K$ (no necesariamente distintos) tales que

$$f(x) = c \cdot (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Por obvias razones, en este caso también decimos que $K$ *contiene a todas las raíces de* $f(x)$.

# Campos de descomposición

## Definición

Supongamos que $K$ es una extensión de $F$. Decimos que $K$ es un **campo de descomposición de $f(x)$ sobre $F$** si

1. $f(x)$ se descompone en $K/F$ y
2. No existe $L$ campo tal que $F \subset L \subsetneq K$ y $f(x)$ se descompone en $L/F$.

Recordando que $f(x)$ se descompone en $K/F$ si y solo si $K$ contiene a todas las raíces de $f(x)$, obtenemos que $K$ es un campo de descomposición de $f(x)$ sobre $F$ si y solo si

1. $K$ contiene a todas raíces de $f(x)$ y
2. ningún campo (propiamente) intermedio de $K/F$ contiene a todas las raíces de $f(x)$.

Intuitivamente, podemos pensar en un campo de descomposición de $f(x)$ sobre $F$ como la extensión mas chica de $F$ en donde $f(x)$ se descompone. Eventualmente veremos que esta idea es correcta pero con un detalle: si $K$ y $K'$ son campos de descomposición de $f(x)$ sobre $F$, entonces no podremos garantizar que $K = K'$, pero si podremos garantizar que $K \cong K'$ (demostrar este isomorfismo es el objetivo de la siguiente sección).

# La multiplicidad de una raíz

Supongamos que $F$ es un campo, que $f(x) \in F[x]$, y que $n = \deg f(x) \geq 1$. Si $K$ es una extensión de $F$ con $n$ raíces *distintas* de $f(x)$, entonces el recordatorio 1 implica que $f(x)$ se descompone en $K/F$.

Sin embargo, el converso no es cierto. La razón es que en la definición de descomposición en $K$ *no* pedimos que los $\alpha_i$ sean *distintos*. Por eso, introducimos la siguiente definición.

## Definición

Supongamos que $k \in \mathbb{Z}_{\geq 1}$, que $F$ es un campo, y que $f(x) \in F[x]$. Si $\alpha \in F$ es una raíz de $f(x)$, decimos que la **multiplicidad de $\alpha$ es** $k$ si $k$ es el máximo entero $\geq 1$ tal que $(x - \alpha)^k$ divide a $f(x)$ en $F[x]$.

# Para todo polinomio existe una extensión en donde este se puede descomponer

**Proposición 1**

Supongamos que $F$ es un campo. Si $f(x) \in F[x]$ tiene grado $\geq 1$, entonces existe una extensión $E$ de $F$ en donde $f(x)$ se descompone en $E/F$.

*Demostración.* Procedamos por inducción sobre el grado del polinomio.

*Paso base.* Supongamos que $f(x) \in F[x]$ tiene grado 1. Entonces existen $a, b \in F$ tales que

$$f(x) = ax + b = a\left(x + \frac{b}{a}\right).$$

Por lo tanto, $E = F$ cumple lo deseado.

*Paso inductivo.* Sea $n > 1$ y supongamos que

> *Para todo campo y todo polinomio sobre este campo con grado* $\leq n-1$*, existe una extensión del campo en donde el polinomio se puede descomponer.*

Cabe recalcar que esta inducción es un poquito extraña porque no estamos fijando el campo pero también debería de ser claro que esto no tiene nada de malo.

Ahora si, supongamos que $f(x) \in F[x]$ y $n = \deg f(x)$. Como $F[x]$ es un DFU[1] y $f(x)$ no es invertible[2], entonces podemos factorizar a $f(x)$ en irreducibles.

*Caso 1. Todos los factores irreducibles de* $f(x)$ *tienen grado 1.*

Entonces existen $a_1, b_1, \ldots, a_n, b_n \in F$ tales que

$$\begin{aligned} f(x) &= (a_1x + b_1)(a_2x + b_2)\cdots(a_nx + b_n) \\ &= a_1a_2\cdots a_n\left(x + \frac{b_1}{a_1}\right)\left(x + \frac{b_2}{a_2}\right)\cdots\left(x + \frac{b_n}{a_n}\right) \end{aligned}$$

Por lo tanto, $E = F$ cumple lo deseado.

---

[1] Pues $F$ es campo.
[2] Pues $\deg f(x) \geq 1$.

*Caso 2. No todos los factores irreducibles de $f(x)$ tienen grado 1.*

Entonces debe existir un factor irreducible de $f(x)$ con grado $\geq 2$, digamos $p(x)$. Por el recordatorio 2, sabemos que existe una extensión de campos $L/F$ tal que $p(x)$ tiene una raíz en $L$, digamos $\alpha$. Luego, por el recordatorio 1, sabemos que $(x-\alpha)$ divide a $f(x)$ en $L[x]$ o equivalentemente, sabemos que existe $g(x) \in L[x]$ tal que

$$f(x) = (x-\alpha)g(x).$$

Como $\deg f(x) = n$ y $\deg(x-\alpha) = 1$, la ecuación anterior implica que $\deg g(x) = n-1$. Pero entonces, por hipótesis de inducción, existe una extensión $E$ de $L$ en donde $g(x)$ se descompone en $E/F$. Como $\alpha \in L \subset E$, claramente $E$ cumple lo deseado. $\square$

Si todas las raíces de un polinomio viven en una extensión dada, el campo de descomposición de este polinomio es el campo generado por sus raíces

## Proposición 2

Supongamos que $F$ es un campo, que $f(x) \in F[x]$, y que $n = \deg f(x) \geq 1$. Si $E$ es una extensión de $F$ y $f(x)$ se descompone en $E/F$, digamos

$$f(x) = c \cdot (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \text{ con } c \in F \text{ y } \alpha_1, \ldots, \alpha_n \in E,$$

entonces $F(\alpha_1, \ldots, \alpha_n) \subset E$ es un campo de descomposición de $f(x)$ sobre $F$.

En particular, tenemos el siguiente resultado: si $E/F$ es una extensión de campos en donde $f(x)$ se descompone, entonces $E$ contiene a un campo de descomposición de $f(x)$ sobre $F$.

*Demostración.* Claramente, $f(x)$ se descompone en $F(\alpha_1, \ldots, \alpha_n)/F$. Resta ver que $K$ es la extensión de $F$ mas chica en donde $f(x)$ se descompone. Para esto, supongamos que $L$ es un campo tal que $F \subset L \subsetneq F(\alpha_1, \ldots, \alpha_n)$. Veamos por contradicción que $f(x)$ no se descompone en $L/F$, es decir, supongamos que

$$f(x) = d(x - \beta_1)(x - \beta_2) \cdots (x - \beta_m) \text{ con } c \in F \text{ y } \beta_1, \ldots, \beta_m \in L$$

Entonces

$$c \cdot (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = d(x - \beta_1)(x - \beta_2) \cdots (x - \beta_m)$$

pero como $E[x]$ es un DFU y $x - \gamma \in E[x]$ es irreducible, la igualdad anterior implica que $n = m$ y que existe una reordenación de los índices en donde $\alpha_i = \beta_i$ para toda $i \in \{1, \ldots, n\}$. En particular, $\alpha_1, \ldots, \alpha_n \in L$ y por lo tanto, $L = F(\alpha_1, \ldots, \alpha_n)$, contradiciendo $L \subsetneq F(\alpha_1, \ldots, \alpha_n)$. □

# Una demostración alternativa de la proposición anterior

En lo que sigue, presentaremos una demostración de la proposición anterior que ayudara a justificar nuestra intuición de que el campo de descomposición de $f(x)$ sobre $F$ es la extensión mas chica de $F$ en donde $f(x)$ se descompone. El lector familiarizado con conceptos como la cerradura de un subconjunto de un espacio topológico, apreciara esta demostración.

*Demostración alternativa de la proposición anterior.*

Supongamos que $E/F$ es una extensión de campos tal que $f(x)$ se descompone en $E/F$. Entonces

$$\mathcal{F} = \left\{ S/F \mid f(x) \text{ se descompone en } S/F \right\}$$

es no vacío y por eso podemos definir

$$K = \bigcap \mathcal{F}.$$

Es fácil verificar que $K$ es un campo de descomposición de $f(x)$ sobre $F$. $\square$

# Todo polinomio no constante tiene un campo de descomposición

**Teorema 3**

Supongamos que $F$ es un campo. Si $f(x) \in F[x]$ tiene grado $\geq 1$, entonces existe una extensión $K$ de $F$ que es un campo de descomposición de $f(x)$ sobre $F$.

*Demostración.* Es consecuencia inmediata de juntar los dos proposiciones anteriores. En efecto, recordemos que ahí vimos

1. que para todo polinomio existe una extensión en donde este se puede descomponer y
2. que si $E/F$ es una extensión de campos en donde $f(x)$ se descompone, entonces $E$ contiene a un campo de descomposición de $f(x)$ sobre $F$.

□

# Algunas aplicaciones de la proposición anterior

- Cabe recalcar que el concepto de campo de descomposición no solo depende del polinomio, también depende del campo sobre el cual estemos viendo el polinomio. Por ejemplo,
  - Un campo de descomposición de $x^2 - 2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{2})$: las raíces de $x^2 - 2$ son $\pm\sqrt{2}$.
  - En contraste, es fácil verificar que un campo de descomposición de $x^2 - 2$ sobre $\mathbb{R}$ es $\mathbb{R}$.
- Un campo de descomposición de $(x^2 - 2)(x^2 - 3)$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{R}$: las raíces de $(x^2 - 2)(x^2 - 3)$ son $\pm\sqrt{2}, \pm\sqrt{3} \in \mathbb{R}$.

- Un campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \subset \mathbb{C}$:

  Las raíces de $x^3 - 2$ son

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right), \quad \sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right) \in \mathbb{C}.$$

  Finalmente, como

$$\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right), \quad \sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right) \in \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}),$$

  obtenemos lo deseado.

- Un campo de descomposición de $x^4 + 4$ sobre $\mathbb{Q}$ es $\mathbb{Q}(i) \subset \mathbb{C}$:

  Primero notemos que

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2).$$

  Usando la chicharronera, vemos que las raíces de $x^4 + 4$ son

$$1 + i, \quad 1 - i, \quad -1 + i, \quad -1 - i \in \mathbb{C}.$$

  Finalmente, como cada una de estas raíces pertenece a $\mathbb{Q}(i)$, obtenemos lo deseado.

# El campo de descomposición de $x^n - 1$

Antes de empezar, unos recordatorios amistosos:

Recuerda que todo numero complejo $a + bi \in \mathbb{C}$ puede ser escrito de manera única como

$$re^{i\theta} r(\cos\theta + i\sin\theta) \quad r > 0,\ 0 \leq \theta < 2\pi.$$

Si vemos a $a + ib$ como un vector en el plano complejo, entonces en la expresión anterior $r$ es la longitud del vector $(a, b)$ y $\theta$ es el ángulo que $(a, b)$ forma con el real positivo. Usando esto es fácil verificar que las $n$ soluciones en $\mathbb{C}$ a la ecuación $x^n = 1$ son

$$e^{i\frac{2\pi k}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right), \quad k = 1, \ldots, n.$$

En efecto, usando la famosa formula de Euler $e^{i\pi} = 1$ obtenemos que

$$\left(e^{i\frac{2\pi k}{n}}\right)^n = e^{i\left(\frac{2\pi k}{n}\right)\cdot n} = e^{i2\pi k} = \left(e^{i\pi}\right)^{2i} = 1^{2i} = 1.$$

para cada $k = 1, \ldots, n$.

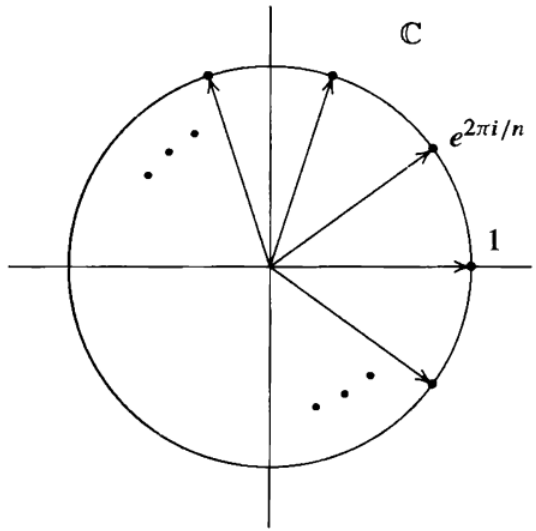
Mas aun, como

$$\left(e^{\frac{i2\pi}{n}}\right)^k = e^{i\frac{2\pi k}{n}} \text{ para toda } k = 1, \ldots, n,$$

entonces un campo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$ es

$$\mathbb{Q}\left(e^{i\frac{2\pi}{n}}\right) \subset \mathbb{C}.$$

Es interesante notar que geométricamente, las raíces de $x^n - 1$ son los vértices de un $n$-polígono regular inscrito en la circunferencia de radio 1 y con centro en el origen.



Una aplicación importante de conocer las $n$ distintas soluciones en $\mathbb{C}$ a la ecuación $x^n = 1$ es la siguiente: Dado un $z \in \mathbb{C}$ y una solución en $\mathbb{C}$ a la ecuación $x^n = z$, obtenemos el resto de las soluciones de $x^n = z$ a través de multiplicarle (a la solución dada) las soluciones de $x^n = 1$. En efecto, si $\zeta^n = 1$ y $\eta^n = z$, entonces $(\zeta\eta)^n = z$.

Otra forma de escribir el resultado anterior es de la siguiente manera: Supongamos que $z \in \mathbb{C}$ y que $n \in \mathbb{Z}_{\geq 1}$. Si $\zeta_1, \ldots, \zeta_n \in \mathbb{C}$ son las $n$ distintas raíces de $x^n - 1$ y $\eta$ es una raíz de $x^n - z$, entonces

$$\zeta_1\eta, \quad \zeta_2\eta, \quad \ldots, \quad \zeta_n\eta$$

son las $n$ distintas raíces de $x^n - z$.

Por otro lado, notemos que si $K/F$ es *cualquier* extensión de campos y $K$ es un campo de descomposición de $x^n - 1$ sobre $F$, entonces el conjunto de las raíces de $x^n - 1$ forma un subgrupo multiplicativo de $K$. En efecto, si $\alpha^n = 1$ y $\beta^n = 1$, entonces $(\alpha\beta)^n = 1$.

Usando el teorema fundamental de grupos abelianos finitamente generados se puede demostrar que cualquier subgrupo finito del grupo multiplicativo de un campo es cíclico. Desafortunadamente, este resultado esta fuera de los objetivos del curso y por eso lo omitimos.

Sin embargo, teniendo esto en mente, podemos reescribir el resultado de la diapositiva anterior de la siguiente manera: Supongamos que $z \in \mathbb{C}$ y que $n \in \mathbb{Z}_{\geq 1}$. Si $\zeta$ es un generador del grupo de las raices de $x^n - 1$ y $\eta$ es una raiz de $x^n - z$, entonces

$$\eta, \quad \zeta\eta, \quad \zeta^2\eta, \quad \ldots, \quad \zeta^{n-1}\eta$$

son las $n$ distintas raíces de $x^n - z$.

Como el conjunto de las raíces de $x^n - 1$ es un subgrupo finito del grupo multiplicativo de un campo, entonces lo anterior implica que también es un grupo cíclico. Por ejemplo, en el caso $F = \mathbb{Q}$ y $K = \mathbb{C}$ ya vimos que un generador de este grupo es $e^{i\frac{2\pi}{n}}$. Para el caso general, introducimos la siguiente definición.

# $n$-esima raíz primitiva y el campo ciclotómico

## Definición

Supongamos que $K/F$ es una extensión de campos. Si $K$ es un campo de descomposición de $x^n - 1$ sobre $F$, entonces

- Decimos que $\alpha \in K$ es una **$n$-esima raíz de la unidad en** $F$ si $\alpha$ es una raíz de $x^n - 1$.
- Decimos que $\zeta_n \in K$ es una **$n$-esima raíz primitiva de la unidad en** $F$ si $\zeta_n$ es un generador del grupo (cíclico) de las $n$-esimas raíces de $F$.

# Observación

Supongamos que $K/F$ es una extensión de campos y que $K$ es un campo de descomposición de $x^n - 1$ sobre $F$. Si $\zeta_n$ es una $n$-esima raíz primitiva de $F$, entonces (por teoría básica de grupos cíclicos) las otras $n$-raíces primitivas de $F$ son

$$(\zeta_n)^k \text{ con } 1 \leq k < n \text{ y } (k, n) = 1.$$

En particular, si $\varphi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ es la función dada por

$$\begin{aligned} \varphi(n) &:= \left|\{k \in \mathbb{Z}_{\geq 1} \mid k < n \text{ y } (k, n) = 1\}\right| \\ &= \text{el numero de enteros positivos} < \text{n que son primos relativos a } n, \end{aligned}$$

entonces (por lo anterior) hay $\varphi(n)$ $n$-raíces primitivas de $F$. Esta función es particularmente importante y se conoce como **la función $\varphi$ de Euler**.

# Campos ciclotómicos

## Definición

Supongamos que $\zeta_n \in \mathbb{C}$ es cualquier $n$-esima raíz primitiva de la unidad en $\mathbb{Q}$. El campo $\mathbb{Q}(\zeta_n)$ es llamado **el campo ciclotómico de las $n$-esimas raíces de la unidad**.

# El grado de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$

## Proposición 4

Supongamos que $p \in \mathbb{Z}_{\geq 1}$ es primo. Si $\zeta_p$ es una $p$-esima raíz primitiva de la unidad en $\mathbb{Q}$, entonces

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

En palabras, el campo ciclotómico de las $p$-esimas raíces de la unidad tiene grado $p - 1$ sobre $\mathbb{Q}$.

*Demostración.* Supongamos que $p \in \mathbb{Z}_{\geq 1}$ es primo y recordemos que el polinomio $p$-ciclotómico es

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots x + 1.$$

En la sección 1.28 demostramos que $\phi_p(x)$ es irreducible en $\mathbb{Q}[x]$.

Ahora bien, notemos que si $\zeta_p$ es una $p$-esima raíz primitiva de la unidad en $\mathbb{Q}$, entonces $\zeta_p \neq 1$ (el grupo multiplicativo generado por 1 es simplemente $\{1\}$). Por lo tanto, $\zeta_p$ es una raíz de $\phi_p(x)$. Entonces $\varphi_p(x) = m_{\zeta_p,\mathbb{Q}}(x)$ y por lo tanto

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg_{\mathbb{Q}} \zeta_p = \deg m_{\zeta_p,\mathbb{Q}}(x) = p - 1.$$

□

En general se puede demostrar que para cualquier entero positivo $n$,

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Desafortunadamente no nos daremos el tiempo de ver este resultado y lo mencionamos simplemente como una curiosidad.

# El campo de descomposición de $x^2 - p$ sobre $\mathbb{Q}$

## Proposición 5

Supongamos que $p \in \mathbb{Z}_{\geq 1}$ es primo. Si $\zeta_p$ es una $p$-esima raíz primitiva de la unidad en $\mathbb{Q}$, entonces un campo de descomposición de $x^p - 2$ sobre $\mathbb{Q}$ es

$$\mathbb{Q}(\sqrt[p]{2}, \zeta_p) \subset \mathbb{C}.$$

Además,

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1).$$

*Demostración.* Supongamos que $p \in \mathbb{Z}_{\geq 1}$ es primo y que $\zeta$ es cualquier $p$-esima raíz primitiva de $\mathbb{Q}$. Como $(\zeta)^p = 1$ y $(\sqrt[p]{2})^p = 2$, entonces $(\zeta\sqrt[p]{2})^p = 1$. Mas aun, como hay exactamente $p$ $p$-esimas raíces primitivas de $\mathbb{Q}$, entonces las raíces de $x^p - 2$ son

$$\zeta\sqrt[p]{2}, \qquad \text{con } \zeta \text{ una } p\text{-esima raíz de la unidad en } \mathbb{Q}.$$

En particular, si $\zeta_p$ es una $p$-esima raíz primitiva de la unidad en $\mathbb{Q}$, entonces las raíces de $x^p - 2$ son

$$\sqrt[p]{2}, \quad \zeta_p\sqrt[p]{2}, \quad (\zeta_p)^2\sqrt[p]{2} \quad , \ldots , \quad (\zeta_p)^{p-1}\sqrt[p]{2}.$$

Usando (i) esto, (ii) la ecuación

$$\zeta_p\sqrt[p]{2} \cdot \frac{1}{\sqrt[p]{2}} = \zeta_p$$

y (iii) la proposición 3, es fácil ver que

$$\mathbb{Q}(\sqrt[p]{2}, \zeta_p) \subset \mathbb{C}.$$

es un campo de descomposición del polinomio $x^p - 2$ sobre $\mathbb{Q}$.

Veamos que

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1).$$

Para esto, consideremos el concepto de producto entre campos[3]. Es fácil verificar que

$$\mathbb{Q}(\sqrt[p]{2}, \zeta_p) = \mathbb{Q}(\sqrt[p]{2})\, \mathbb{Q}(\zeta_p). \tag{1}$$

Por otro lado, como $p$ y $p-1$ son primos relativos, entonces el corolario 2.8.4 implica que

$$[\mathbb{Q}(\sqrt[p]{2})\, \mathbb{Q}(\zeta_p) : \mathbb{Q}] = p(p-1). \tag{2}$$

Juntando (1) y (2) obtenemos lo deseado. □

[3]Recuerda que $K_1K_2$ es el campo mas chico que contiene a $K_1 \cup K_2$.

# $x^p - 2$ es irreducible sobre $\mathbb{Q}(\zeta_p)$

## Corolario 6

Supongamos que $p \in \mathbb{Z}_{\geq 1}$ es primo. Si $\zeta_p$ es una $p$-esima raíz primitiva de la unidad en $\mathbb{Q}$, entonces $x^p - 2$ es irreducible sobre $\mathbb{Q}(\zeta_p)$.

*Demostración.* Supongamos lo contrario. Entonces

$$\deg_{\mathbb{Q}(\zeta_p)} \sqrt[p]{2} = \deg m_{\sqrt[p]{2},\mathbb{Q}(\zeta_p)}(x) < \deg(x^p - 2) = p$$

y por lo tanto

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = \left[\left(\mathbb{Q}(\zeta_p)\right)(\sqrt[p]{2}) : \mathbb{Q}(\zeta_p)\right] \underbrace{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]}_{p-1} < p(p-1).$$

Contradiciendo la proposición anterior. □