Cuerpos de funciones y torres de cuerpos de funciones sobre cuerpos finitos

Horacio Navarro

IMAL-FIQ

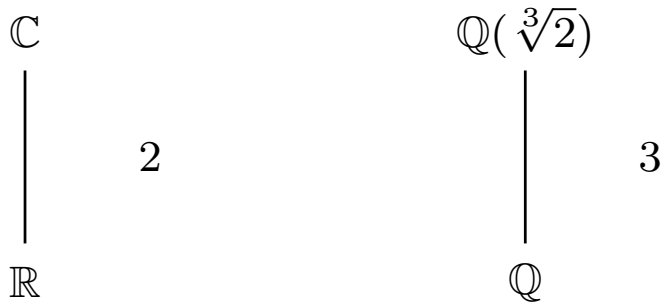
Seminario del IMAL
Santa Fe, 20 de mayo de 2016

Extensiones de cuerpos

Sean K, F cuerpos. Si K es un subcuerpo de F decimos que F/K **es una extensión de cuerpos**. En este caso se considera a F como un K espacio vectorial y la dimensión de F/K se denota por $[F : K]$.

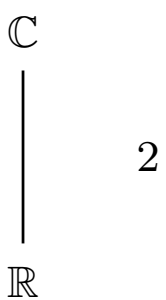
Extensiones de cuerpos

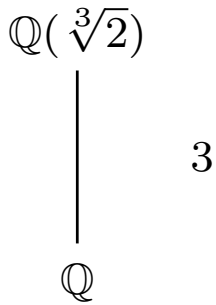
Sean K, F cuerpos. Si K es un subcuerpo de F decimos que F/K **es una extensión de cuerpos**. En este caso se considera a F como un K espacio vectorial y la dimensión de F/K se denota por $[F : K]$.



Extensiones de cuerpos

Sean K, F cuerpos. Si K es un subcuerpo de F decimos que F/K **es una extensión de cuerpos**. En este caso se considera a F como un K espacio vectorial y la dimensión de F/K se denota por $[F : K]$.

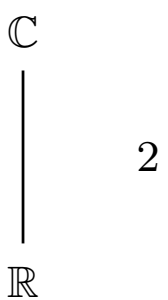


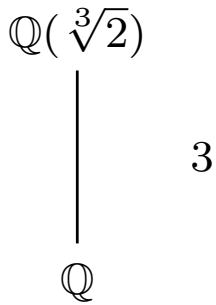


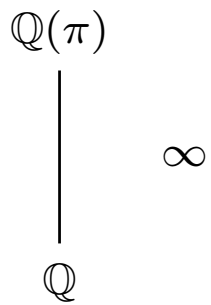
$p(T) = T^2 + 1$ $\qquad$ $p(T) = T^3 - 2$

Extensiones de cuerpos

Sean K, F cuerpos. Si K es un subcuerpo de F decimos que F/K **es una extensión de cuerpos**. En este caso se considera a F como un K espacio vectorial y la dimensión de F/K se denota por $[F : K]$.



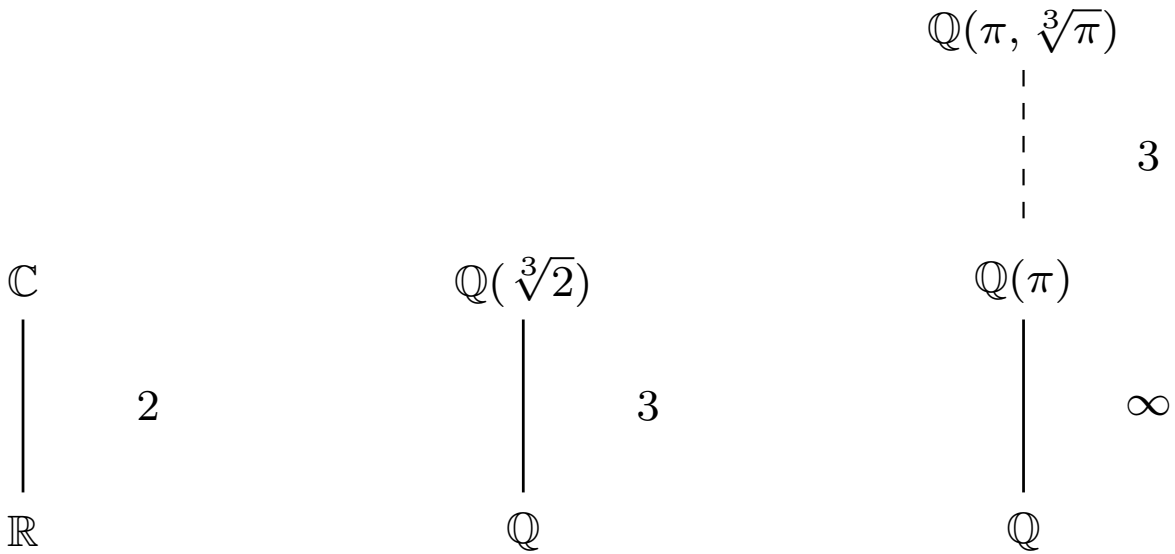




$p(T) = T^2 + 1$ $\qquad$ $p(T) = T^3 - 2$

Extensiones de cuerpos

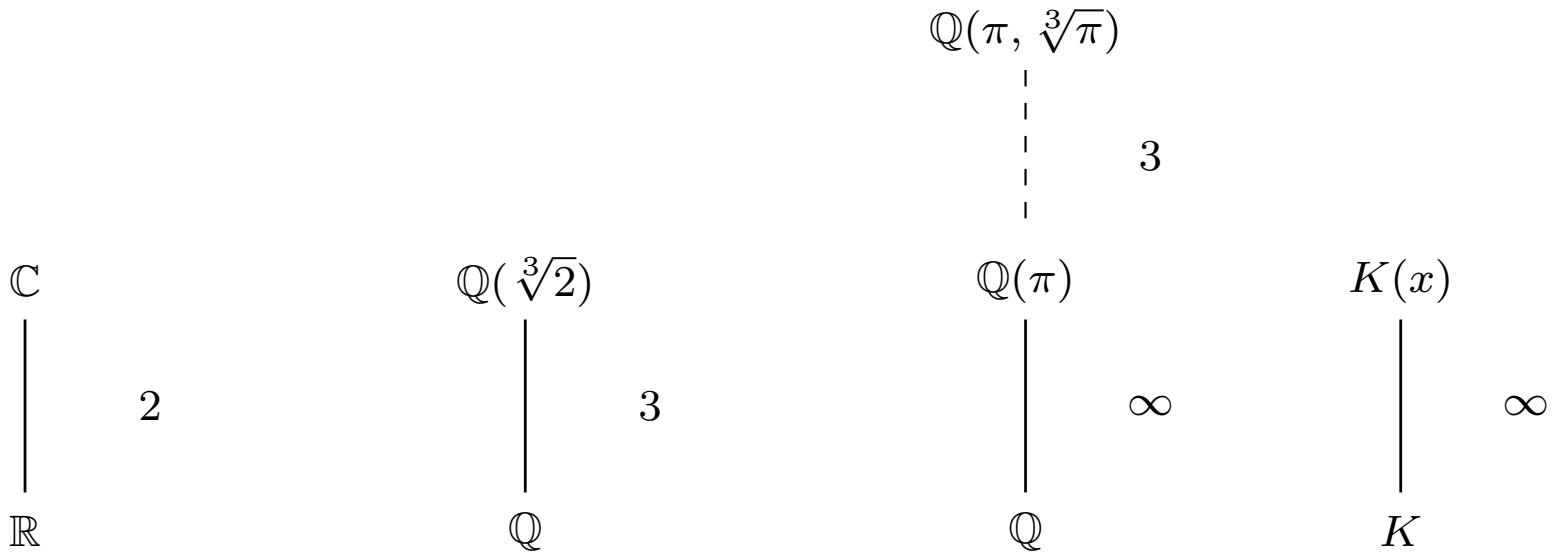
Sean K, F cuerpos. Si K es un subcuerpo de F decimos que F/K **es una extensión de cuerpos**. En este caso se considera a F como un K espacio vectorial y la dimensión de F/K se denota por $[F : K]$.



$p(T) = T^2 + 1$ $\quad$ $p(T) = T^3 - 2$ $\quad$ $p(T) = T^3 - \pi$

Extensiones de cuerpos

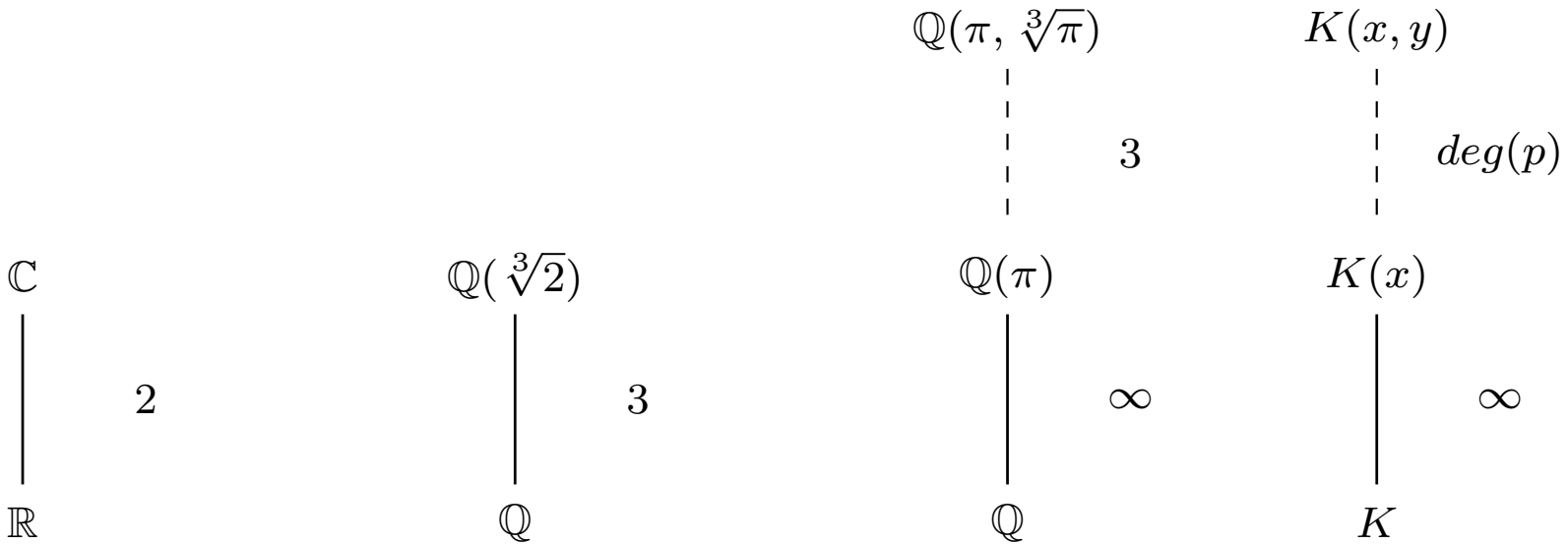
Sean K, F cuerpos. Si K es un subcuerpo de F decimos que F/K **es una extensión de cuerpos**. En este caso se considera a F como un K espacio vectorial y la dimensión de F/K se denota por $[F : K]$.



$p(T) = T^2 + 1$ $p(T) = T^3 - 2$ $p(T) = T^3 - \pi$

Extensiones de cuerpos

Sean K, F cuerpos. Si K es un subcuerpo de F decimos que F/K **es una extensión de cuerpos**. En este caso se considera a F como un K espacio vectorial y la dimensión de F/K se denota por $[F : K]$.



$p(T) = T^2 + 1$ $p(T) = T^3 - 2$ $p(T) = T^3 - \pi$ $p(T) \in K(x)[T]$

Cuerpos finitos

Sean a, b, n enteros con $n > 0$.

$a \sim b$ si $n \mid a - b$

Cuerpos finitos

Sean a, b, n enteros con $n > 0$.

$a \sim b$ si $n \mid a - b \implies \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$

Cuerpos finitos

Sean a, b, n enteros con $n > 0$.

$a \sim b$ si $n \mid a - b \implies \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$

$\mathbb{Z}/p\mathbb{Z}$ es un cuerpo si y sólo si p es primo.

Cuerpos finitos

Sean a, b, n enteros con $n > 0$.

$a \sim b$ si $n \mid a - b \implies \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$

$\mathbb{Z}/p\mathbb{Z}$ es un cuerpo si y sólo si p es primo.

Si F es un cuerpo finito entonces $|F| = p^n$ para algún p primo y $n \in \mathbb{N}$.

Cuerpos finitos

Sean a, b, n enteros con $n > 0$.

$a \sim b$ si $n \mid a - b \implies \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$

$\mathbb{Z}/p\mathbb{Z}$ es un cuerpo si y sólo si p es primo.

Si F es un cuerpo finito entonces $|F| = p^n$ para algún p primo y $n \in \mathbb{N}$.

$$\begin{array}{c} \mathbb{F}_p(\alpha) \\ \Big| \quad \deg(h) \\ \mathbb{F}_p \end{array}$$

$h(T) \in \mathbb{F}_p[T]$

Cuerpos finitos

Sean a, b, n enteros con $n > 0$.

$a \sim b$ si $n \mid a - b \implies \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$

$\mathbb{Z}/p\mathbb{Z}$ es un cuerpo si y sólo si p es primo.

Si F es un cuerpo finito entonces $|F| = p^n$ para algún p primo y $n \in \mathbb{N}$.

$$\begin{array}{c} \mathbb{F}_p(\alpha) \\ | \\ \deg(h) \\ | \\ \mathbb{F}_p \end{array} \qquad \begin{array}{c} \mathbb{F}_2(\alpha) \\ | \\ 2 \\ | \\ \mathbb{F}_2 \end{array}$$

$h(T) \in \mathbb{F}_p[T]$ $\qquad$ $p(T) = T^2 + T + 1$

Cuerpos finitos

Sean a, b, n enteros con $n > 0$.

$a \sim b$ si $n \mid a - b \implies \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$

$\mathbb{Z}/p\mathbb{Z}$ es un cuerpo si y sólo si p es primo.

Si F es un cuerpo finito entonces $|F| = p^n$ para algún p primo y $n \in \mathbb{N}$.

$$\begin{array}{ccc} \mathbb{F}_p(\alpha) & & \mathbb{F}_2(\alpha) \\ | & \deg(h) & | \quad 2 \\ \mathbb{F}_p & & \mathbb{F}_2 \end{array}$$

$h(T) \in \mathbb{F}_p[T]$ $\qquad$ $p(T) = T^2 + T + 1$

$\mathbb{F}_4 := \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$ donde $\alpha^2 + \alpha + 1 = 0$.

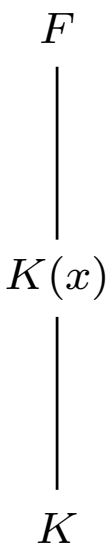
Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.

Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.

Cuerpo de funciones

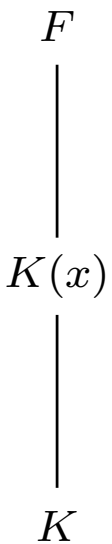


Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.

Sucesión

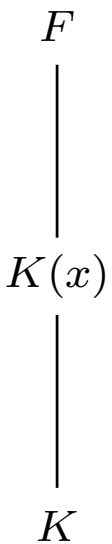
Cuerpo de funciones



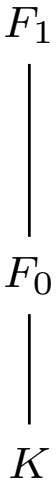
Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.

Cuerpo de funciones



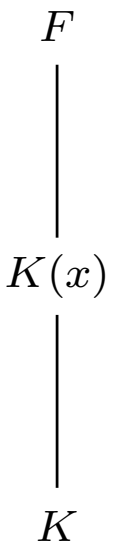
Sucesión



Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.

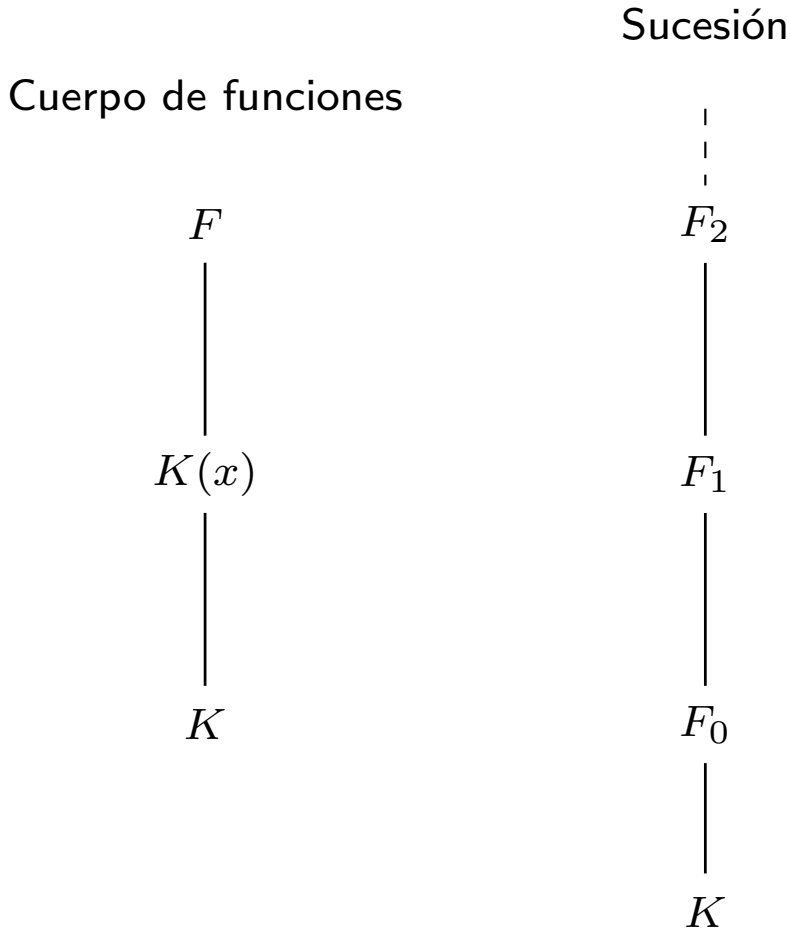
Cuerpo de funciones



Sucesión

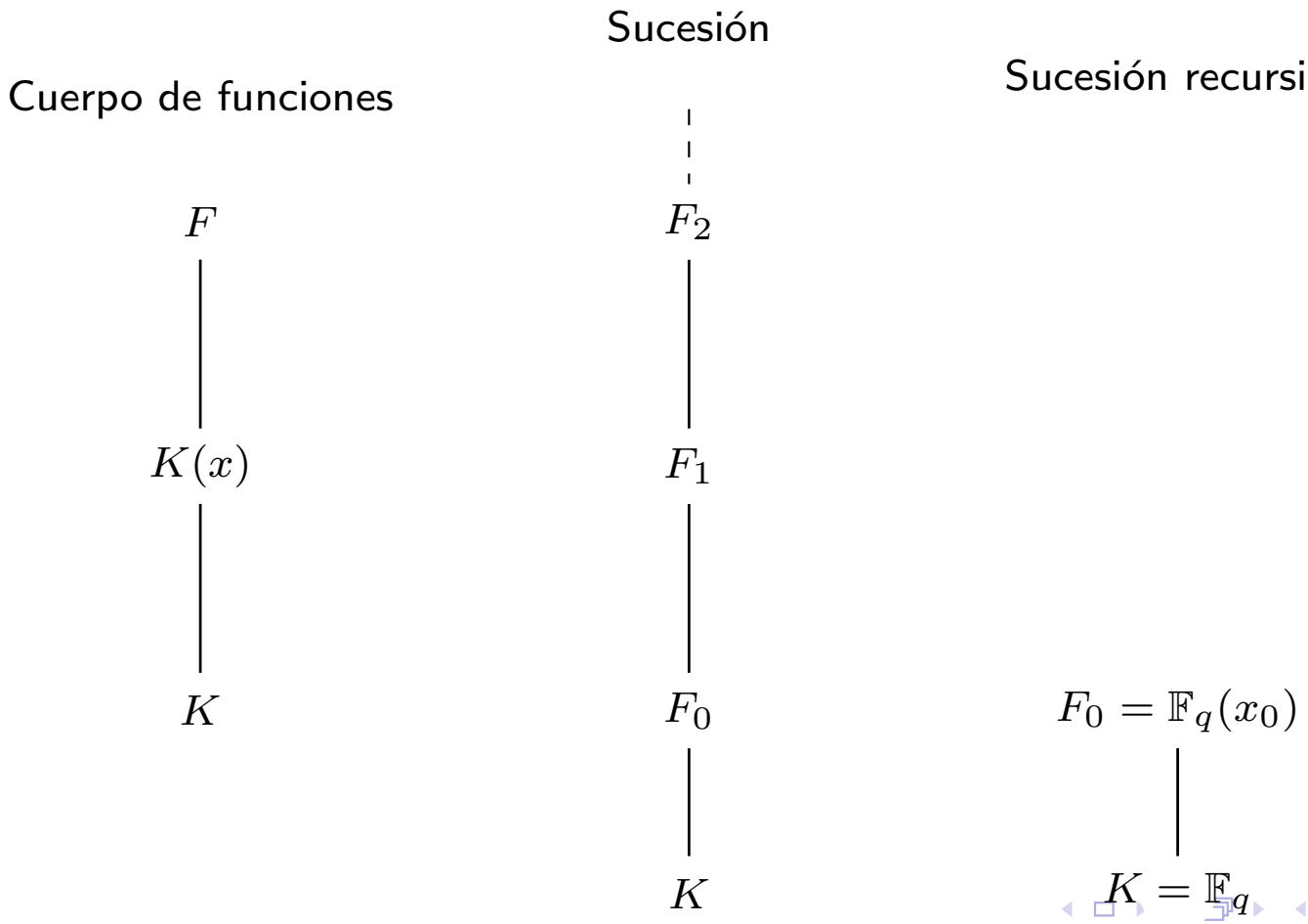
Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.



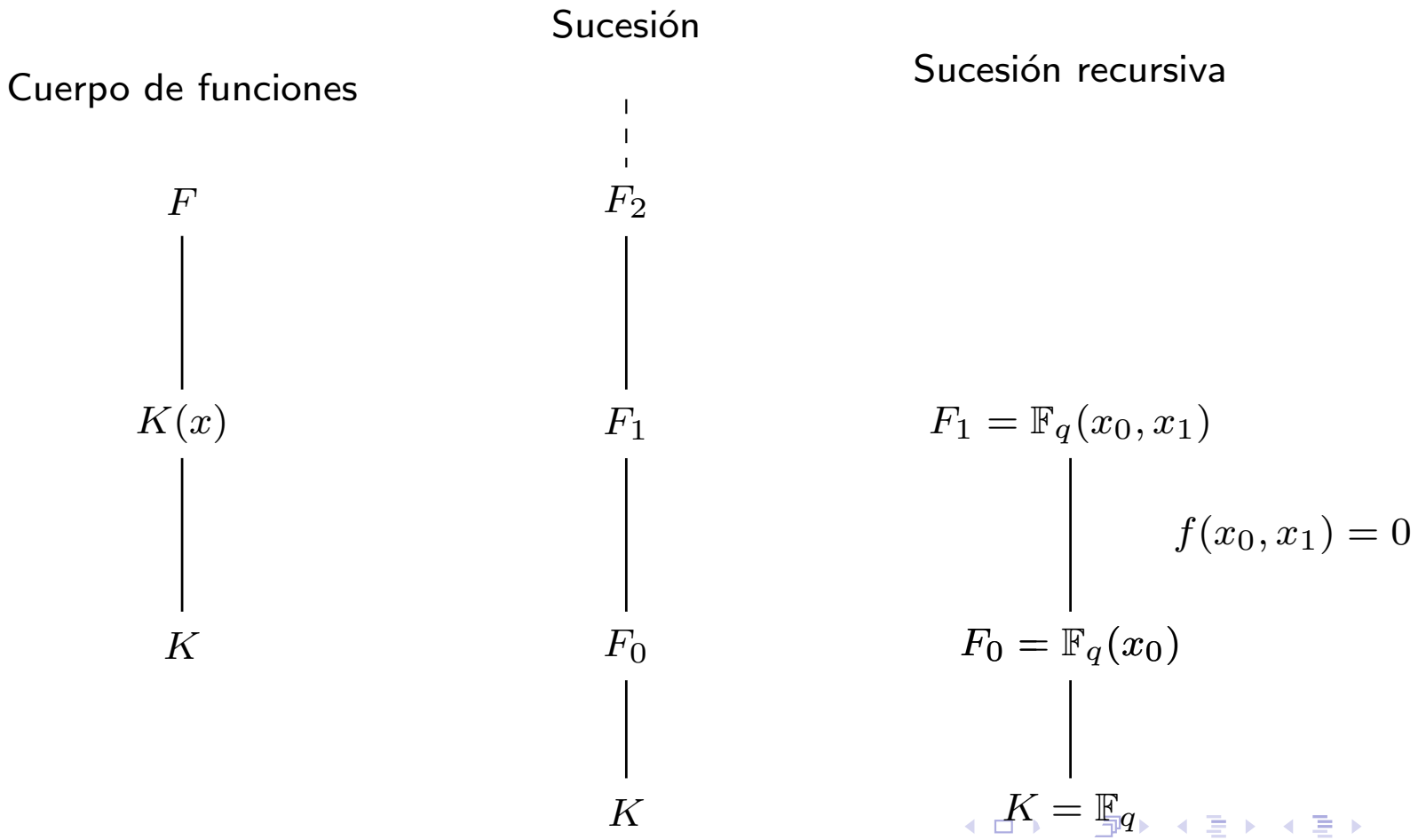
Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.



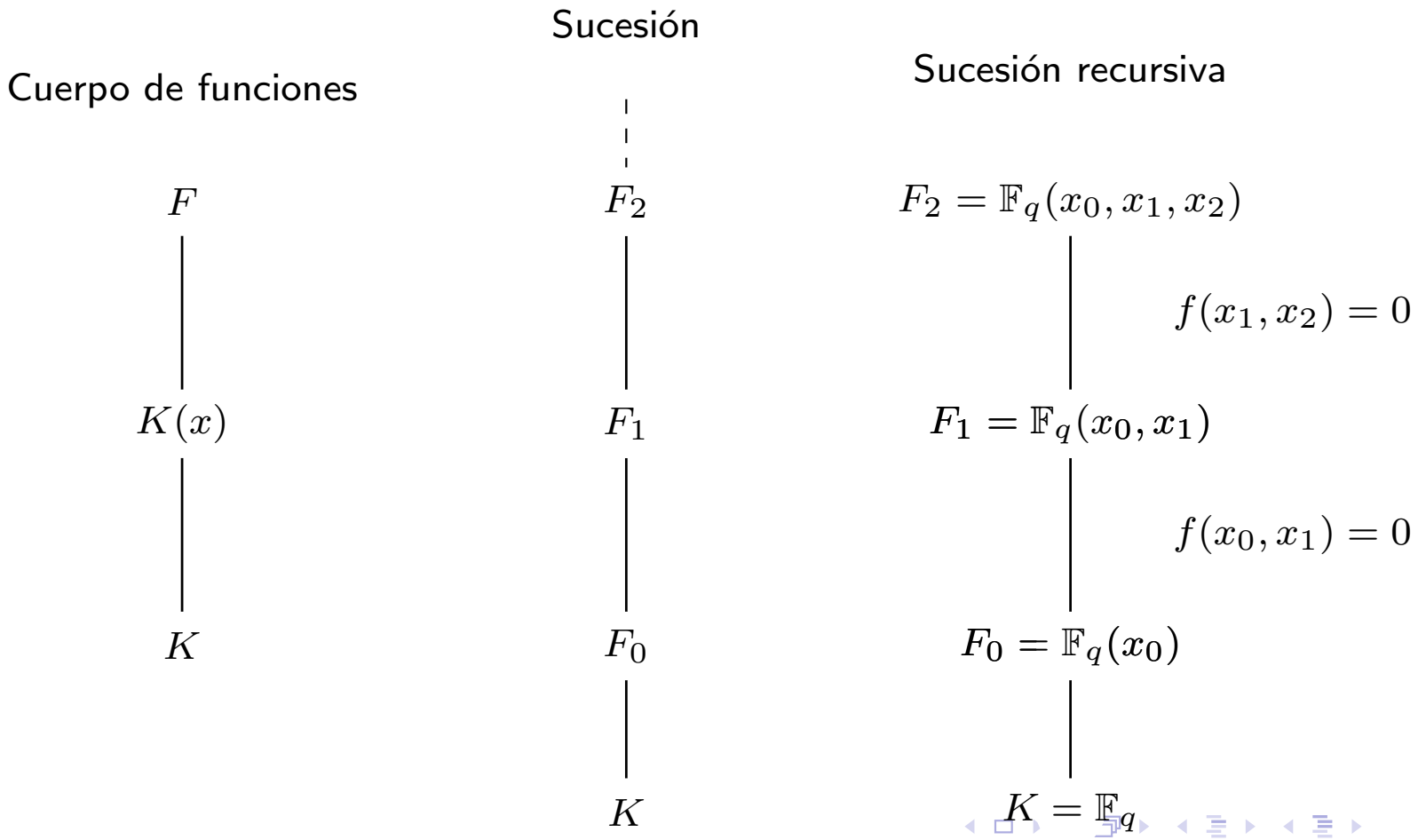
Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.



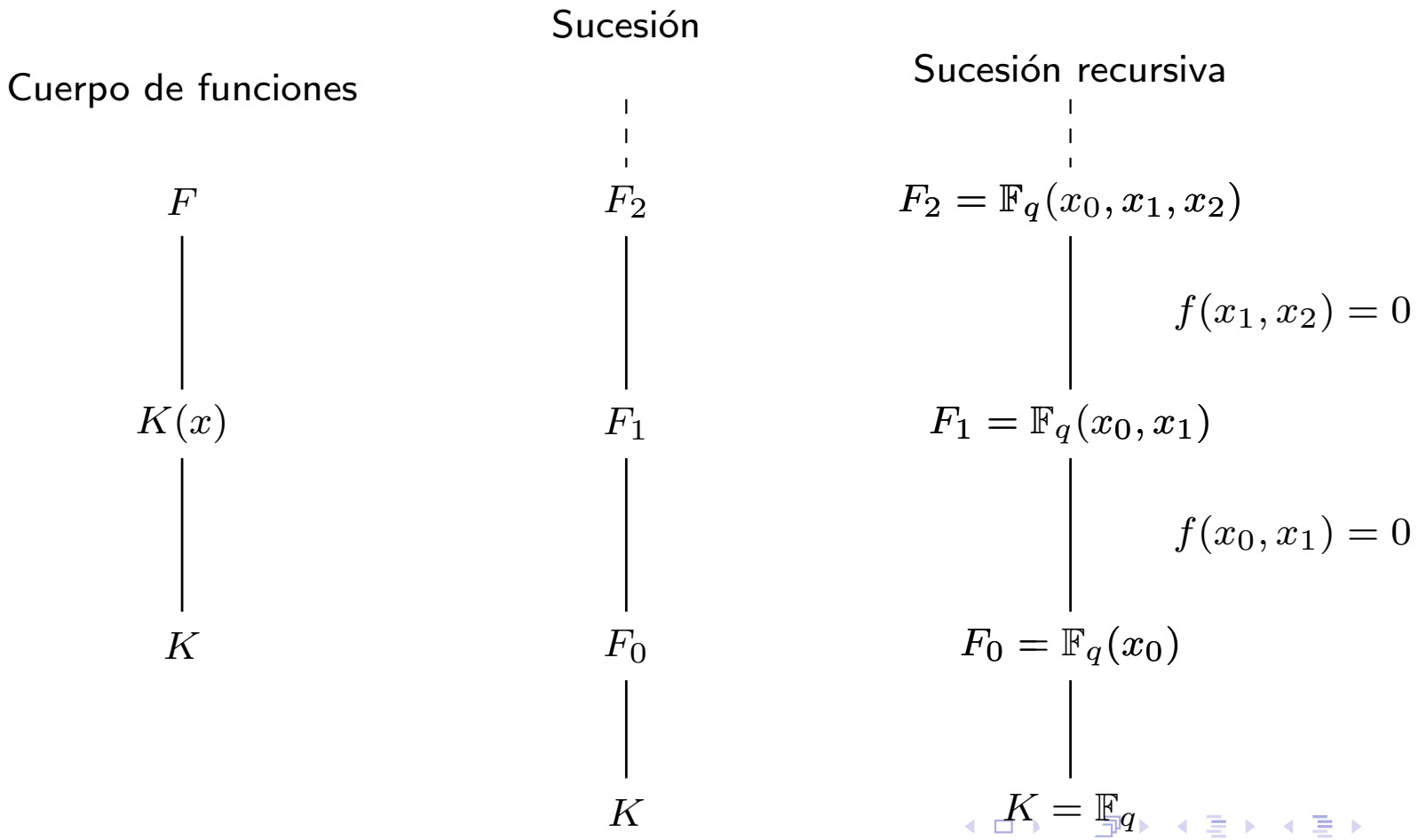
Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.



Torres de cuerpos de funciones

Una extensión de cuerpos F/K se dice **un cuerpo de funciones algebraicas** si existe un elemento $x \in F$ trascendente sobre K tal que la extensión F/K es finita.



Una sucesión de cuerpos de funciones $\mathcal{F} = (F_0, F_1, \dots)$ sobre $\mathbb{F}_q$ se dice una **torre** si:

$i)$ Para todo $i \geq 0$ la extensión F_{i+1}/F_i es finita y separable.

$ii)$ El cuerpo total de constantes de F_i, para todo $i \geq 0$, es $\mathbb{F}_q$.

$iii)$ Existe un cuerpo de funciones F_j con género mayor a uno.

Una sucesión de cuerpos de funciones $\mathcal{F} = (F_0, F_1, \dots)$ sobre $\mathbb{F}_q$ se dice una **torre** si:

$i)$ Para todo $i \geq 0$ la extensión F_{i+1}/F_i es finita y separable.

$ii)$ El cuerpo total de constantes de F_i, para todo $i \geq 0$, es $\mathbb{F}_q$.

$iii)$ Existe un cuerpo de funciones F_j con género mayor a uno.

El género de $\mathcal{F}$ se define como

$$\gamma(\mathcal{F}) := \lim_{i \to \infty} g(F_i)/[F_i : F_0],$$

donde $g(F_i)$ es el género de F_i.

Una sucesión de cuerpos de funciones $\mathcal{F} = (F_0, F_1, \dots)$ sobre $\mathbb{F}_q$ se dice una **torre** si:

$i)$ Para todo $i \geq 0$ la extensión F_{i+1}/F_i es finita y separable.

$ii)$ El cuerpo total de constantes de F_i, para todo $i \geq 0$, es $\mathbb{F}_q$.

$iii)$ Existe un cuerpo de funciones F_j con género mayor a uno.

El género de $\mathcal{F}$ se define como

$$\gamma(\mathcal{F}) := \lim_{i \to \infty} g(F_i)/[F_i : F_0],$$

donde $g(F_i)$ es el género de F_i.

La tasa de descomposición de $\mathcal{F}$ se define por

$$\nu(\mathcal{F}) := \lim_{i \to \infty} N(F_i)/[F_i : F_0],$$

donde $N(F_i)$ el número de lugares racionales de F_i.

Una sucesión de cuerpos de funciones $\mathcal{F} = (F_0, F_1, \dots)$ sobre $\mathbb{F}_q$ se dice una **torre** si:

$i)$ Para todo $i \geq 0$ la extensión F_{i+1}/F_i es finita y separable.

$ii)$ El cuerpo total de constantes de F_i, para todo $i \geq 0$, es $\mathbb{F}_q$.

$iii)$ Existe un cuerpo de funciones F_j con género mayor a uno.

El género de $\mathcal{F}$ se define como

$$\gamma(\mathcal{F}) := \lim_{i \to \infty} g(F_i)/[F_i : F_0],$$

donde $g(F_i)$ es el género de F_i.

La tasa de descomposición de $\mathcal{F}$ se define por

$$\nu(\mathcal{F}) := \lim_{i \to \infty} N(F_i)/[F_i : F_0],$$

donde $N(F_i)$ el número de lugares racionales de F_i.

Se dice que $\mathcal{F}$ es **asint. buena** si $\gamma(\mathcal{F}) < \infty$ y $\nu(\mathcal{F}) > 0$.

Clasificación de Torres recursivas sobre $\mathbb{F}_2$

Sean $F/\mathbb{F}_q$ un cuerpo de funciones, con $p = char(\mathbb{F}_q)$, y $w \in F$ tal que

$$p(T) = T^{p^n} + a_{n-1}T^{p^{n-1}} + \cdots + a_0 T - w$$

es irreducible en $F[T]$ y $a_0 \neq 0$. La extensión $F(y)/F$ con $p(y) = 0$ se dice **de tipo Artin-Schreier**.

Clasificación de Torres recursivas sobre $\mathbb{F}_2$

Sean $F/\mathbb{F}_q$ un cuerpo de funciones, con $p = char(\mathbb{F}_q)$, y $w \in F$ tal que

$$p(T) = T^{p^n} + a_{n-1}T^{p^{n-1}} + \cdots + a_0 T - w$$

es irreducible en $F[T]$ y $a_0 \neq 0$. La extensión $F(y)/F$ con $p(y) = 0$ se dice **de tipo Artin-Schreier**.

Teorema (Beleen-García-Stichtenoth)**.**

Sean $g(T), f(T) \in \mathbb{F}_2(T)$ con $\deg f = \deg g = 2$ y $\mathcal{F}$ una torre recursiva sobre $\mathbb{F}_2$ definida por

$$g(y) = f(x)$$

Entonces $\mathcal{F}$ está descrita por

$$y^2 + y = \frac{1}{(1/x)^2 + (1/x) + b} + c$$

b	c	ecuación	comp. asintótico
0	1	$y^2+y=\dfrac{x^2+x+1}{x}$	buena
1	0	$y^2+y=\dfrac{x^2}{x^2+x+1}$	buena
0	0	$y^2+y=\dfrac{x^2}{x+1}$	buena
1	1	$y^2+y=\dfrac{x}{x^2+x+1}$	?

Teorema.

La torre definida recursivamente sobre $\overline{\mathbb{F}}_2$ por la ecuación

$$y^2 + y = \frac{x}{x^2 + x + 1} \tag{1}$$

tiene espacio de ramificación finito, más específicamente,

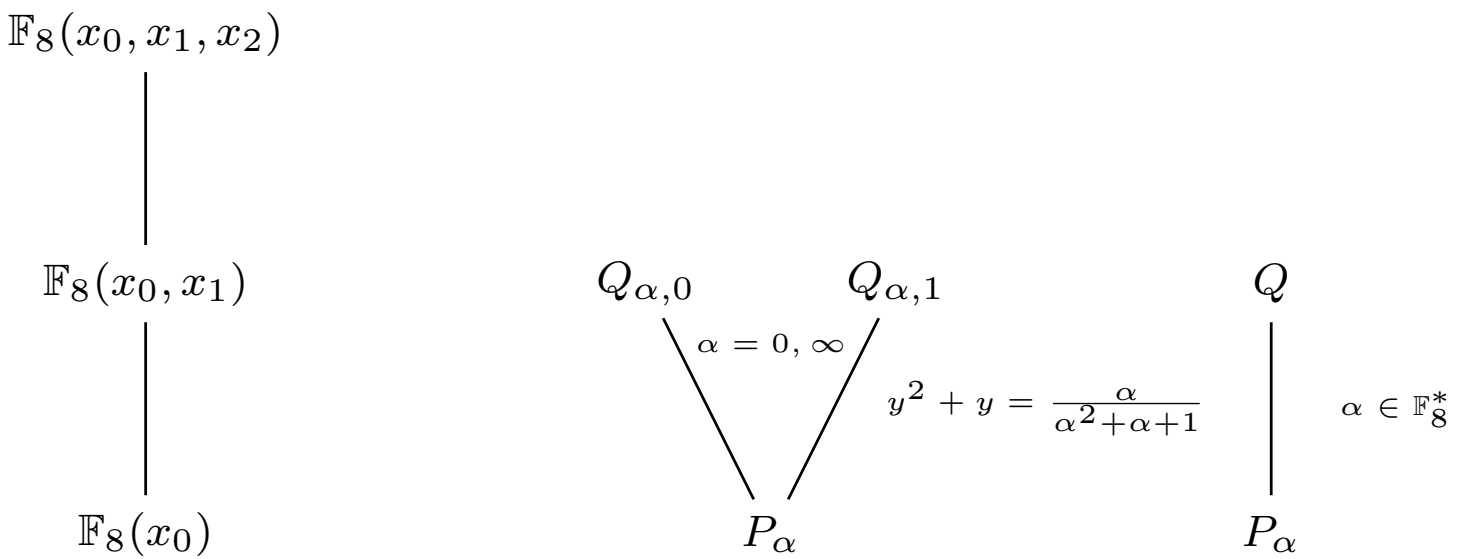
$$Ram(\mathcal{F}) \subseteq \{P_\beta : \beta = 0, 1, \alpha_1, \alpha_2 \text{ o } \infty\}$$

con $\alpha_i \in \overline{\mathbb{F}}_2$ y $\alpha_i^2 + \alpha_i + 1 = 0$.

La tasa de descomposición de la torre

Teorema.

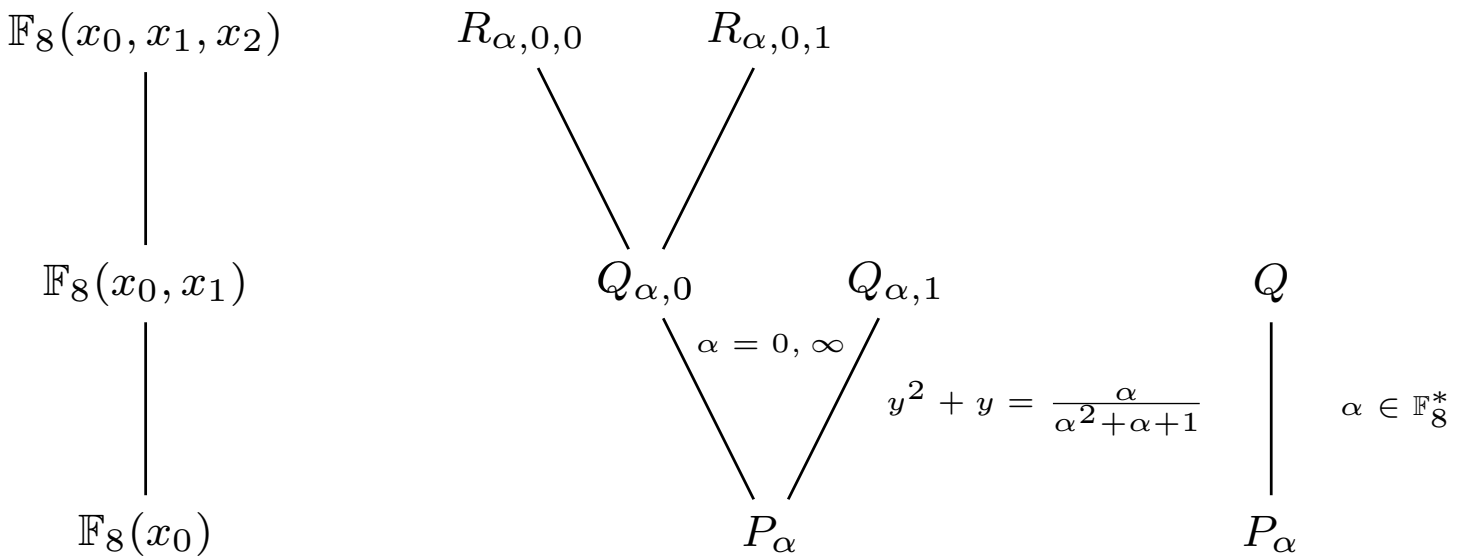
Consideremos la torre de cuerpos de funciones $\mathcal{F}$ sobre $\mathbb{F}_{2^s}$, con s impar, definida recursivamente por la ecuación (1), entonces el número de lugares de racionales de F_i, para todo $i \geq 1$, es constante.



La tasa de descomposición de la torre

Teorema.

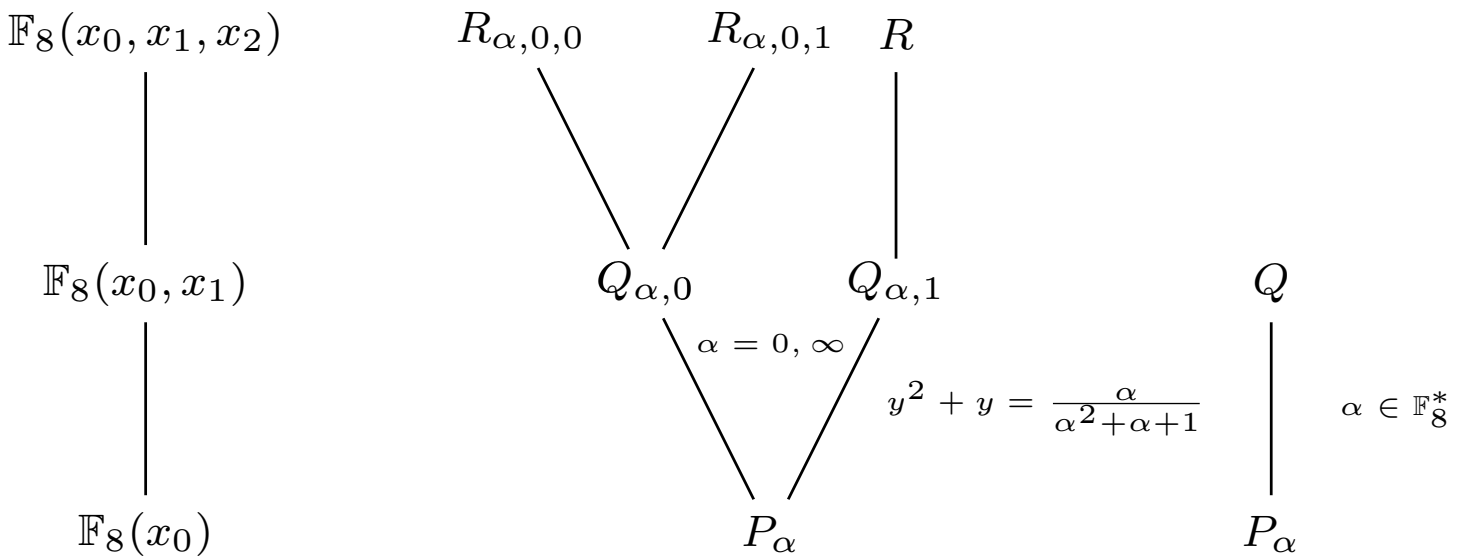
Consideremos la torre de cuerpos de funciones $\mathcal{F}$ sobre $\mathbb{F}_{2^s}$, con s impar, definida recursivamente por la ecuación (1), entonces el número de lugares de racionales de F_i, para todo $i \geq 1$, es constante.



La tasa de descomposición de la torre

Teorema.

Consideremos la torre de cuerpos de funciones $\mathcal{F}$ sobre $\mathbb{F}_{2^s}$, con s impar, definida recursivamente por la ecuación (1), entonces el número de lugares de racionales de F_i, para todo $i \geq 1$, es constante.



La traza de $\mathbb{F}_q$ a $\mathbb{F}_q$ se define como $\mathrm{Tr}(x) = x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x$.

La traza de $\mathbb{F}_q$ a $\mathbb{F}_q$ se define como $\mathrm{Tr}(x) = x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x$.

El polinomio $T^p - T - a$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $\mathrm{Tr}(a) \neq 0$.

La traza de $\mathbb{F}_q$ a $\mathbb{F}_q$ se define como $\mathrm{Tr}(x) = x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x$.

El polinomio $T^p - T - a$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $\mathrm{Tr}(a) \neq 0$.

Para todo $a \in \mathbb{F}_q$ se cumple que $\mathrm{Tr}(a^p) = \mathrm{Tr}(a)$.

La traza de $\mathbb{F}_q$ a $\mathbb{F}_q$ se define como $\mathrm{Tr}(x) = x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x$.

El polinomio $T^p - T - a$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $\mathrm{Tr}(a) \neq 0$.

Para todo $a \in \mathbb{F}_q$ se cumple que $\mathrm{Tr}(a^p) = \mathrm{Tr}(a)$.

La traza es una transformación lineal.

La traza de $\mathbb{F}_q$ a $\mathbb{F}_q$ se define como $\mathrm{Tr}(x) = x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x$.

El polinomio $T^p - T - a$ es irreducible sobre $\mathbb{F}_q$ si y sólo si $\mathrm{Tr}(a) \neq 0$.

Para todo $a \in \mathbb{F}_q$ se cumple que $\mathrm{Tr}(a^p) = \mathrm{Tr}(a)$.

La traza es una transformación lineal.

Lema.

Sean $\theta, \beta \in \mathbb{F}_{2^s}$, con s impar, tales que $\theta^2 + \theta = \frac{\beta}{\beta^2+\beta+1}$. Entonces

$$\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) \neq \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right).$$

Demostración.

Supongamos que $\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) = \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right)$ entonces

$$\mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = 0.$$

Demostración.

Supongamos que $\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) = \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right)$ entonces

$$\mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = 0.$$

Por otra parte, por hipótesis sabemos que $\theta^2+\theta = \frac{\beta}{\beta^2+\beta+1}$ luego

$$\frac{1}{\theta^2+\theta+1} = \frac{\beta^2+\beta+1}{\beta^2+1} = 1 + \frac{\beta}{\beta+1} + \left(\frac{\beta}{\beta+1}\right)^2.$$

Demostración.

Supongamos que $\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) = \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right)$ entonces

$$\mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = 0.$$

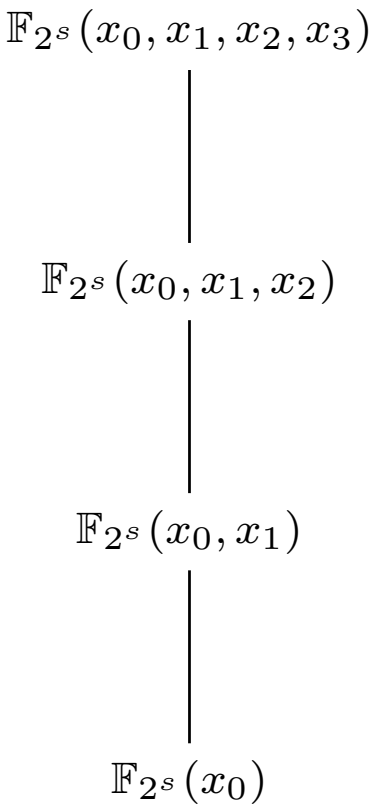
Por otra parte, por hipótesis sabemos que $\theta^2+\theta = \frac{\beta}{\beta^2+\beta+1}$ luego

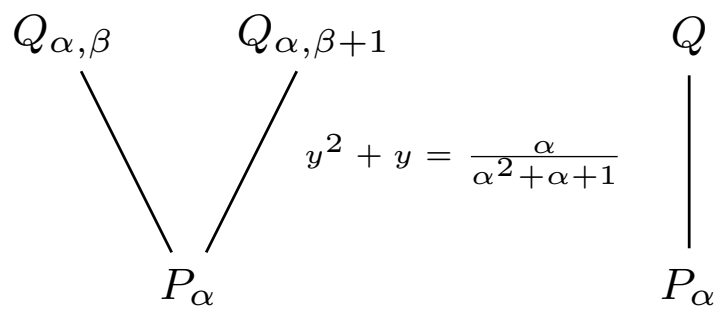
$$\frac{1}{\theta^2+\theta+1} = \frac{\beta^2+\beta+1}{\beta^2+1} = 1 + \frac{\beta}{\beta+1} + \left(\frac{\beta}{\beta+1}\right)^2.$$

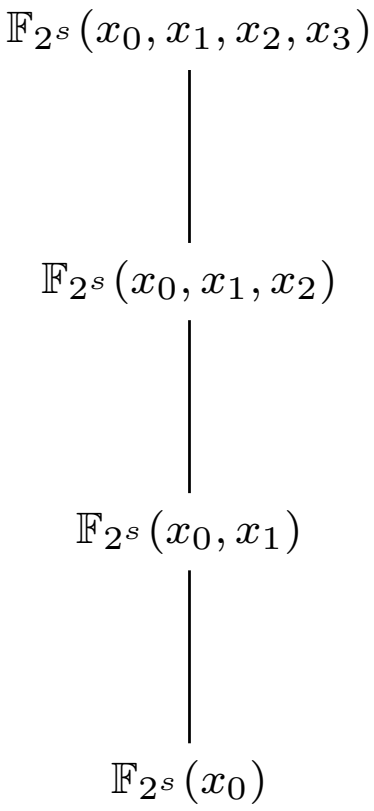
Por último, como $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2)$ para todo $\alpha \in \mathbb{F}_{2^s}$ y $\mathrm{Tr}(1) = 1$ entonces

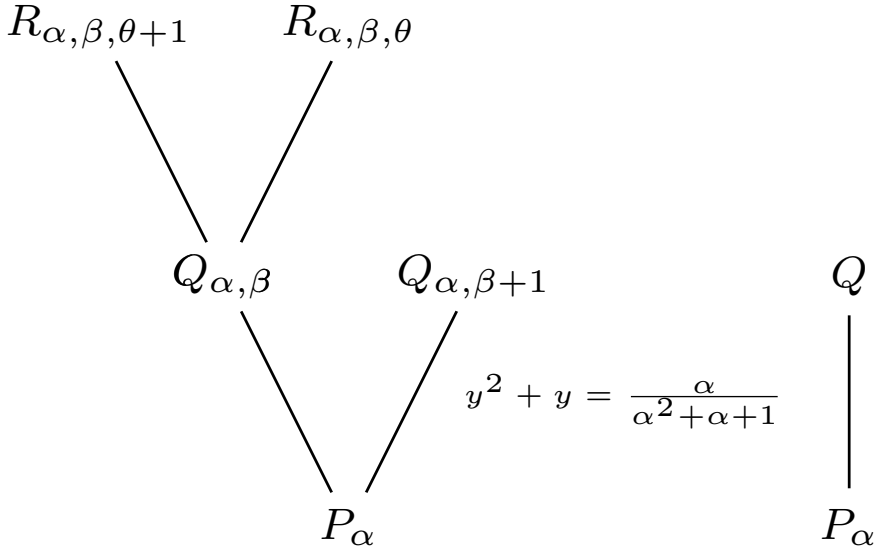
$$\mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = \mathrm{Tr}(1) + \mathrm{Tr}\left(\frac{\beta}{\beta+1}\right) + \mathrm{Tr}\left(\left(\frac{\beta}{\beta+1}\right)^2\right) = 1.$$

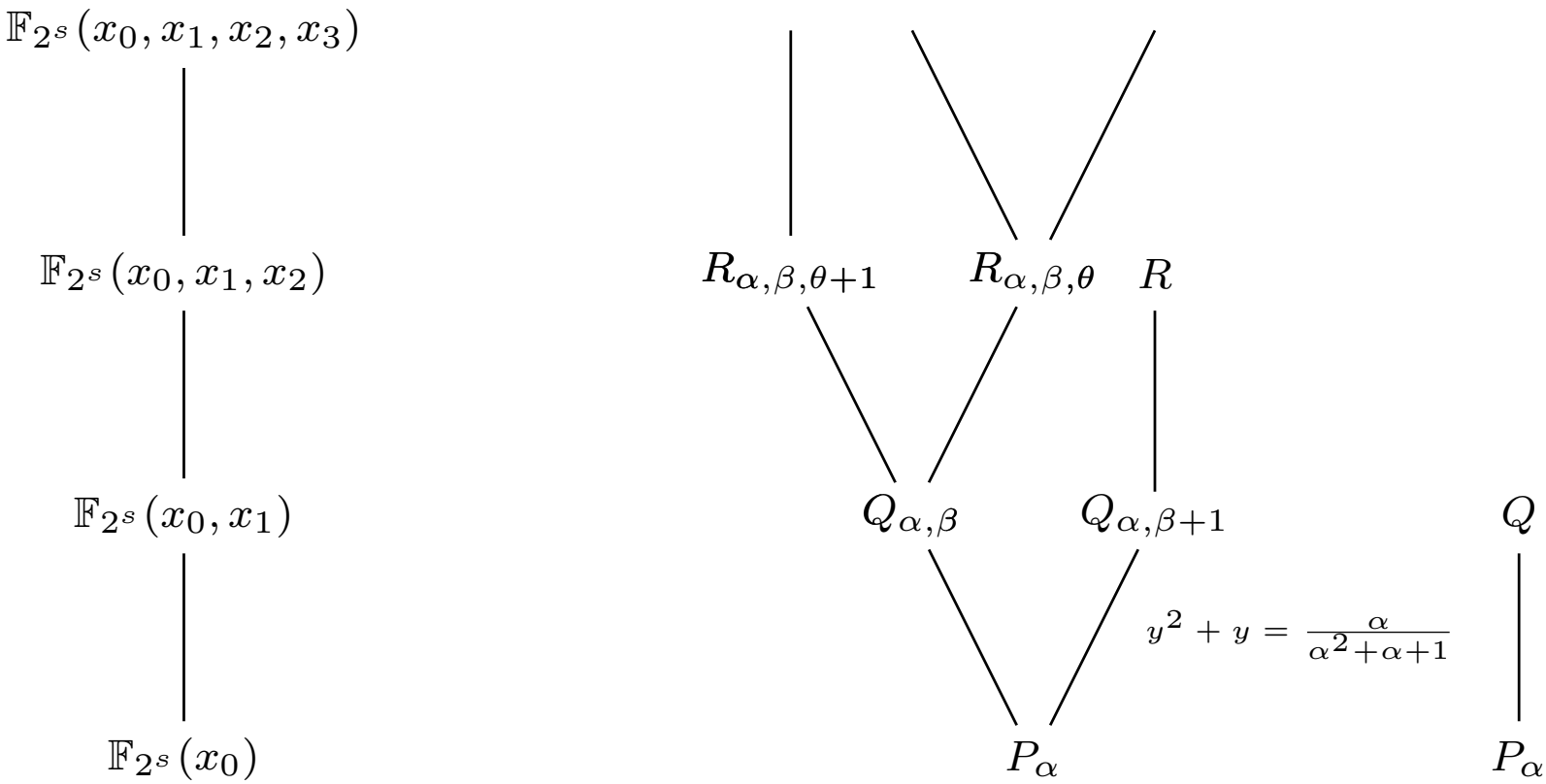
. □


$\mathbb{F}_{2^s}(x_0, x_1, x_2, x_3)$
$\mathbb{F}_{2^s}(x_0, x_1, x_2)$
$\mathbb{F}_{2^s}(x_0, x_1)$
$\mathbb{F}_{2^s}(x_0)$


$Q_{\alpha,\beta}$
$Q_{\alpha,\beta+1}$
$y^2 + y = \frac{\alpha}{\alpha^2+\alpha+1}$
Q
P_α
P_α


$\mathbb{F}_{2^s}(x_0, x_1, x_2, x_3)$
$\mathbb{F}_{2^s}(x_0, x_1, x_2)$
$\mathbb{F}_{2^s}(x_0, x_1)$
$\mathbb{F}_{2^s}(x_0)$


$R_{\alpha,\beta,\theta+1}$
$R_{\alpha,\beta,\theta}$
$Q_{\alpha,\beta}$
$Q_{\alpha,\beta+1}$
P_α
$y^2 + y = \frac{\alpha}{\alpha^2+\alpha+1}$
Q
P_α


$\mathbb{F}_{2^s}(x_0, x_1, x_2, x_3)$
$\mathbb{F}_{2^s}(x_0, x_1, x_2)$
$\mathbb{F}_{2^s}(x_0, x_1)$
$\mathbb{F}_{2^s}(x_0)$
$R_{\alpha,\beta,\theta+1}$
$R_{\alpha,\beta,\theta}$
R
$Q_{\alpha,\beta}$
$Q_{\alpha,\beta+1}$
Q
$y^2 + y = \frac{\alpha}{\alpha^2+\alpha+1}$
P_α
P_α


P. Beelen, A. Garcia and H. Stichtenoth.
Towards a classification of recursive towers of function fields over finite fields.
Finite Fields Appl, 12(1):56–77, 2006.


P. Beelen, A. Garcia and H. Stichtenoth.
On towers of function fields of Artin-Schreier type.
Bull. Braz. Math. Soc., 35(2):151–164, 2004.


H. Stichtenoth.
Algebraic function fields and codes, volume 254 of *Graduate Texts in Mathematics*.
Springer-Verlag, Berlin, second edition, 2009.


G. van der Geer and M. van der Vlugt.
An asymptotically good tower of curves over the field with eight elements.
Bull. London Math. Soc., 34(3):291–300, 2002.