Torres recursivas de tipo Artin-Schreier

Horacio Navarro

IMAL-UNL

Primer encuentro argentino de cuerpos finitos
Córdoba, 20 de octubre de 2017

Torres de cuerpos de funciones

Una sucesión de cuerpos de funciones $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ se dice una **torre** si para todo $i \geq 0$ se cumple que:

- ✓ $F_i \subset F_{i+1}$,
- ✓ F_{i+1}/F_i es una extensión finita y separable,
- ✓ $\mathbb{F}_q$ es el cuerpo total de constantes de F_i y,

además,

- ✓ existe $j \geq 0$ tal que el género de F_j cumple que $g(F_j) \geq 2$.

Torres de cuerpos de funciones

Una sucesión de cuerpos de funciones $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ sobre $\mathbb{F}_q$ se dice una **torre** si para todo $i \geq 0$ se cumple que:

- ✓ $F_i \subset F_{i+1}$,
- ✓ F_{i+1}/F_i es una extensión finita y separable,
- ✓ $\mathbb{F}_q$ es el cuerpo total de constantes de F_i y,

además,

- ✓ existe $j \geq 0$ tal que el género de F_j cumple que $g(F_j) \geq 2$.

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una torre sobre $\mathbb{F}_q$ y denotemos por $N(F_i)$ el número de lugares racionales de cuerpo F_i. Definimos:

- ✓ **El límite** de $\mathcal{F}$

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}.$$

- ✓ **La tasa de descomposición** de $\mathcal{F}$ (sobre F_0)

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

- ✓ **El género** de $\mathcal{F}$ (sobre F_0)

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

- ✓ **El límite** de $\mathcal{F}$

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}.$$

- ✓ **La tasa de descomposición** de $\mathcal{F}$ (sobre F_0)

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

- ✓ **El género** de $\mathcal{F}$ (sobre F_0)

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

$$0 \leq \lambda(\mathcal{F}) \leq \sqrt{q} - 1 \quad \text{(Drinfeld-Vladut)}$$

✓ **El límite** de $\mathcal{F}$

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}.$$

✓ **La tasa de descomposición** de $\mathcal{F}$ (sobre F_0)

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

✓ **El género** de $\mathcal{F}$ (sobre F_0)

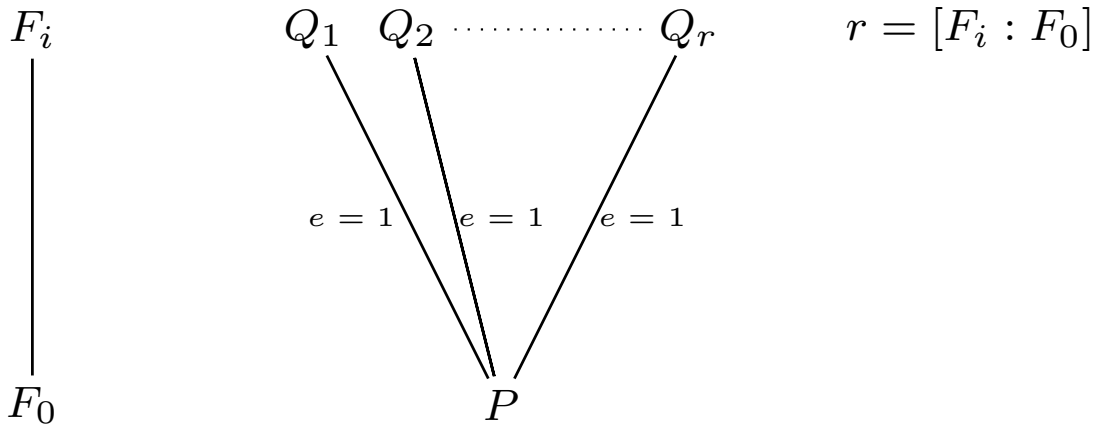
$$\gamma(\mathcal{F}) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}.$$

$$0 \leq \lambda(\mathcal{F}) \leq \sqrt{q} - 1 \quad \text{(Drinfeld-Vladut)}$$

Asintóticamente	**mala**	**buena**	**óptima**
$\lambda(\mathcal{F})$	0	> 0	$\sqrt{q} - 1$

Espacios de descomposición y de ramificación de una torre

Diremos que un lugar P de F_0 se **descompone completamente** en la torre $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ si para cada $i \geq 1$ existen $[F_i : F_0]$ lugares en F_i arriba de P.



Espacios de descomposición y de ramificación de una torre

Espacio de descomposición (sobre F_0)

$$\mathcal{S}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ es racional y se desc. complet. en } \mathcal{F}\}$$

Espacios de descomposición y de ramificación de una torre

Espacio de descomposición (sobre F_0)

$$\mathcal{S}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ es racional y se desc. complet. en } \mathcal{F}\}$$

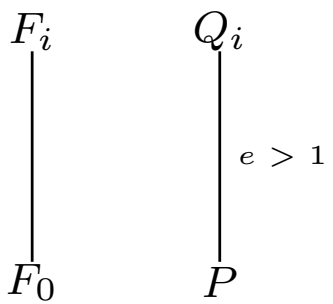
Teorema

Si $\mathcal{F}$ es una torre con espacio de descomposición no vacío, entonces

$$\nu(\mathcal{F}) \geq |\mathcal{S}(\mathcal{F})|.$$

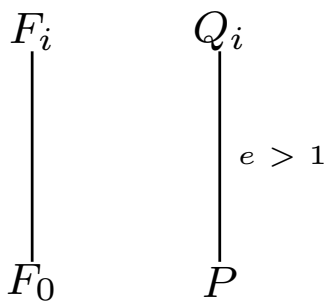
Espacio de ramificación (sobre F_0)

$$\mathcal{R}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ ramifica en } F_n/F_0 \text{ para algún } n \geq 1\}$$



Espacio de ramificación (sobre F_0)

$$\mathcal{R}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ ramifica en } F_n/F_0 \text{ para algún } n \geq 1\}$$



Espacio de ramificación (sobre F_0)

$$\mathcal{R}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ ramifica en } F_n/F_0 \text{ para algún } n \geq 1\}$$

Teorema

Si $\mathcal{F}$ es una torre B-acotada, con espacio de ramificación finito, entonces el género de $\mathcal{F}$ es finito.

$$\mathcal{R}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ ramifica en } F_n/F_0 \text{ para algún } n \geq 1\}$$

$$\mathcal{S}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ es racional y se desc. complet. en } \mathcal{F}\}$$

$$\mathcal{R}(\mathcal{F}) \cap \mathcal{S}(\mathcal{F}) = \emptyset$$

$$\mathcal{R}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ ramifica en } F_n/F_0 \text{ para algún } n \geq 1\}$$

$$\mathcal{S}(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : P \text{ es racional y se desc. complet. en } \mathcal{F}\}$$

$$\mathcal{R}(\mathcal{F}) \cap \mathcal{S}(\mathcal{F}) = \emptyset$$

Teorema

Si $\mathcal{F}$ es una torre B-acotada, con espacio de ramificación finito y espacio de descomposición no vacío, entonces la torre $\mathcal{F}$ es asintóticamente buena.

Una torre $\mathcal{F}$ es **recursiva** si existe una sucesión $\{x_i\}_{i=0}^{\infty}$ de elementos trascendentes sobre $\mathbb{F}_q$ y un polinomio $H(X,Y) \in \mathbb{F}_q[X,Y]$ tales que

- ✓ $F_0 = \mathbb{F}_q(x_0)$ es el cuerpo de la funciones racionales y
- ✓ $F_{i+1} = F_i(x_{i+1})$ donde $H(x_i, x_{i+1}) = 0$ para todo $i \geq 0$.

Una torre recursiva $\mathcal{F}$ es de tipo **Artin-Schreier** si el polinomio $H(X,Y)$ tiene la forma especial

$$H(X,Y) = b_2(X) \cdot a(Y) - b_1(X),$$

donde $b_1(X), b_2(X) \in \mathbb{F}_q[X]$, $p = \mathrm{char}(\mathbb{F}_q)$ y $a(Y)$ es un polinomio **aditivo** y separable, esto es,

$$a(Y) = a_n Y^{p^n} + a_{n-1} Y^{p^{n-1}} + \cdots + a_1 Y^p + a_0 Y \in \mathbb{F}_q[Y],$$

con $a_n \cdot a_0 \neq 0$.

Una torre recursiva $\mathcal{F}$ es de tipo **Artin-Schreier** si el polinomio $H(X,Y)$ tiene la forma especial

$$H(X,Y) = b_2(X) \cdot a(Y) - b_1(X),$$

donde $b_1(X), b_2(X) \in \mathbb{F}_q[X]$, $p = \mathrm{char}(\mathbb{F}_q)$ y $a(Y)$ es un polinomio **aditivo** y separable, esto es,

$$a(Y) = a_n Y^{p^n} + a_{n-1} Y^{p^{n-1}} + \cdots + a_1 Y^p + a_0 Y \in \mathbb{F}_q[Y],$$

con $a_n \cdot a_0 \neq 0$.

Usualmente se dice que la torre $\mathcal{F}$ sobre $\mathbb{F}_q$ está definida por la ecuación

$$a(Y) = b(X) := \frac{b_1(X)}{b_2(X)}.$$

Ecuaciones de tipo AS

$$Y^q + Y = \frac{X^q}{X^{q-1}+1}, \qquad \text{sobre } \mathbb{F}_{q^2}$$

$$Y^2 + Y = \frac{X^2+X+1}{X}, \quad \text{sobre } \mathbb{F}_8$$

$$Y^q - Y = \frac{X^q}{1-X}, \qquad \text{sobre } \mathbb{F}_{q^p}$$

$$Y^q - Y = \frac{X^q + f(X)}{1-X-f(X)}, \text{ sobre } \mathbb{F}_{q^p}$$

con $f = 0$ o $\deg f > 1$ y $(q - \deg f, p) = 1$.

Lema

Sean $a(Y) \in \mathbb{F}_q[Y]$ *aditivo y separable,* $b_1(X), b_2(X) \in \mathbb{F}_q[X]$ *coprimos tales que* $k := \deg(b_1) - \deg(b_2) > 0$ *y . Sea* $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ *sobre* $\mathbb{F}_q$ *la sucesión de cuerpos de funciones definida recursivamente por*

$$a(Y) = b(X) := \frac{b_1(X)}{b_2(X)}.$$

Si existen al menos dos lugares P_1, P_2 *en* F_0 *tales que*

$$\nu_{P_i}(b(x_0)) < 0 \qquad y \qquad (k \cdot \nu_{P_i}(b(x_0)), \deg a) = 1,$$

entonces $\mathcal{F}$ *es una torre. En particular,* P_1, P_2 *son totalmente ramificados en* $\mathcal{F}$*.*

Lema

Sean $a(Y) \in \mathbb{F}_q[Y]$ *aditivo y separable,* $b_1(X), b_2(X) \in \mathbb{F}_q[X]$ *coprimos tales que* $k := \deg(b_1) - \deg(b_2) > 0$ *y . Sea* $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ *sobre* $\mathbb{F}_q$ *la sucesión de cuerpos de funciones definida recursivamente por*

$$a(Y) = b(X) := \frac{b_1(X)}{b_2(X)}.$$

Si existen al menos dos lugares P_1, P_2 *en* F_0 *tales que*

$$\nu_{P_i}(b(x_0)) < 0 \qquad y \qquad (k \cdot \nu_{P_i}(b(x_0)), \deg a) = 1,$$

entonces $\mathcal{F}$ *es una torre. En particular,* P_1, P_2 *son totalmente ramificados en* $\mathcal{F}$*.*

Si, además, existe una función racional $\varphi(T)$ *tal que* $\mathrm{Z}_{\varphi \circ a} \subseteq \mathbb{F}_q \cap \mathrm{Z}_{\varphi \circ b}$ *entonces*

$$S(\mathcal{F}) \supseteq \mathrm{Z}_{\varphi \circ a} \qquad y \qquad \nu(\mathcal{F}) \geq |\, \mathrm{Z}_{\varphi \circ a} \,|.$$

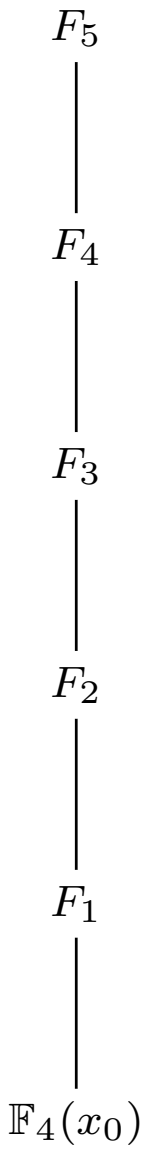
Torres de tipo AS

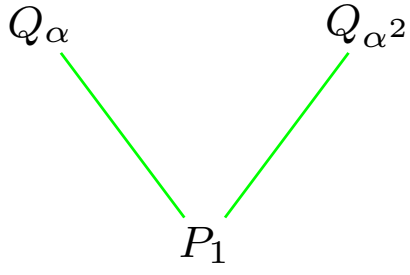
ecuación	Lug .Tot. Ram.	φ	$\lvert Z_{\varphi\circ a}\rvert$	asint.
$Y^q + Y = \dfrac{X^q}{X^{q-1}+1}$	$\{P_\infty\} \cup \{P_\alpha : \alpha^{q-1} = -1\}$	$\dfrac{1-T^{q-1}}{T}$	$q^2 - q$	buena
$Y^2 + Y = \dfrac{X^2+X+1}{X}$	$\{P_0, P_\infty\}$	$T^3 + T + 1$	6	buena
$Y^q - Y = \dfrac{X^q}{1-X}$	$\{P_1, P_\infty\}$	$T + 1$	q	mala
$Y^q - Y = \dfrac{X^q + X^{q-1} + 1}{-X - X^{q-1}}$	$\{P_0, P_\infty\}$	$T + 1$	q	?

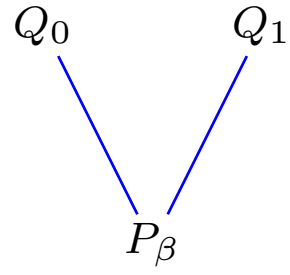
Otras Torres de tipo AS

$$Y^2 + Y = \frac{X}{X^2 + X + 1}, \text{ sobre } \mathbb{F}_4$$

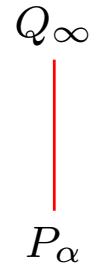
$$Y^p + bY = \frac{1}{X^p + cX}, \text{ sobre } \mathbb{F}_{p^r} \text{ con } b \neq c.$$



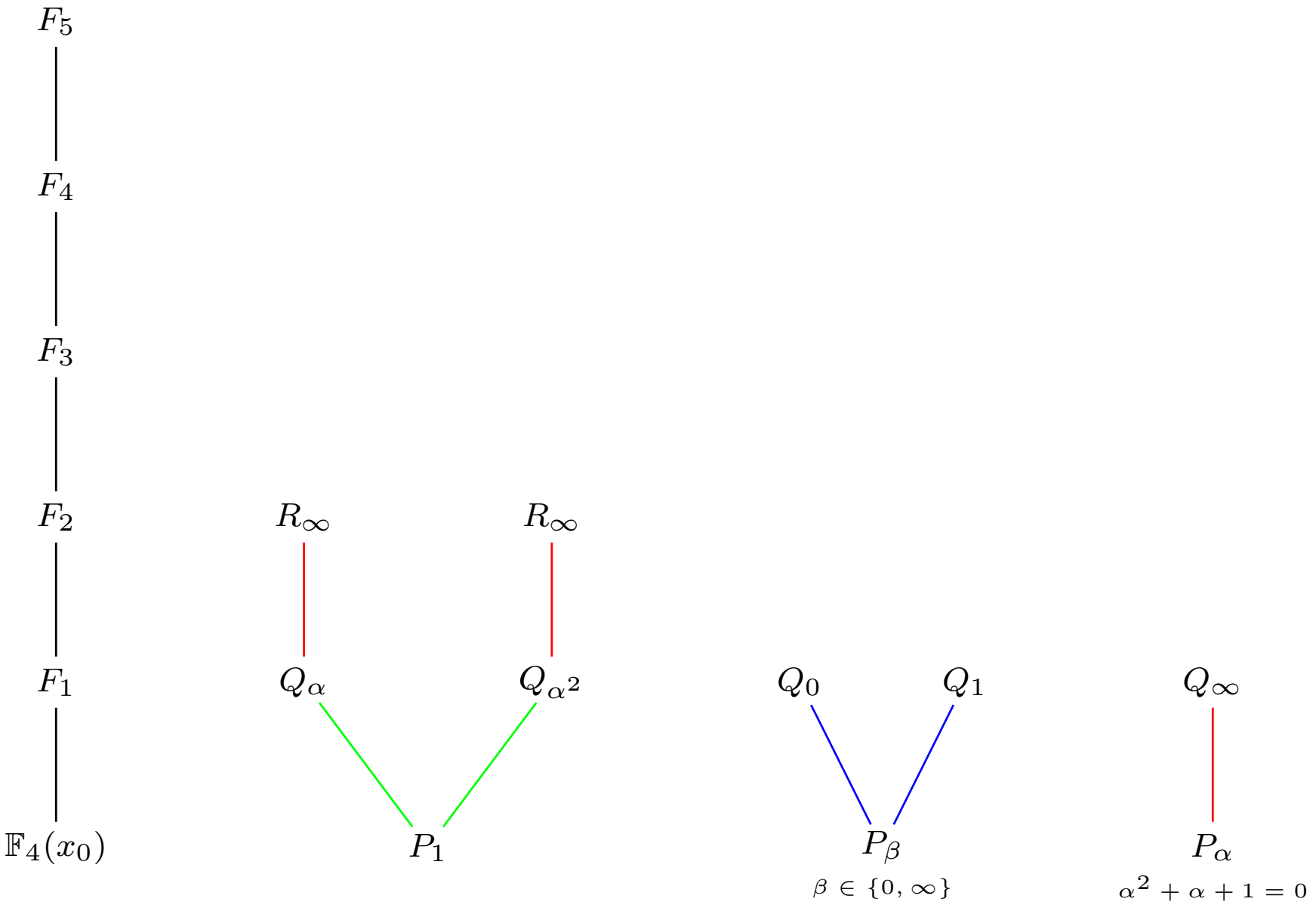


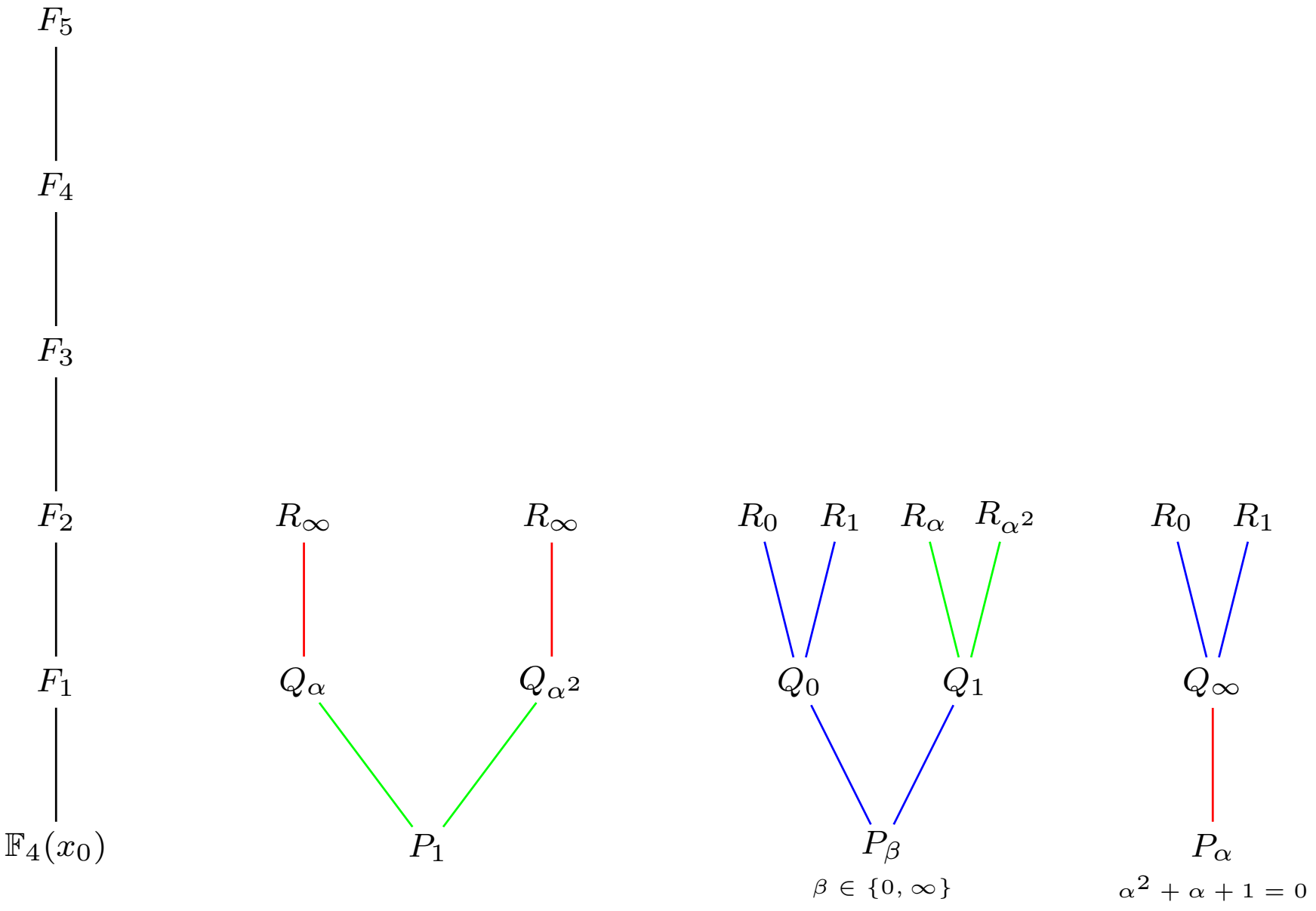


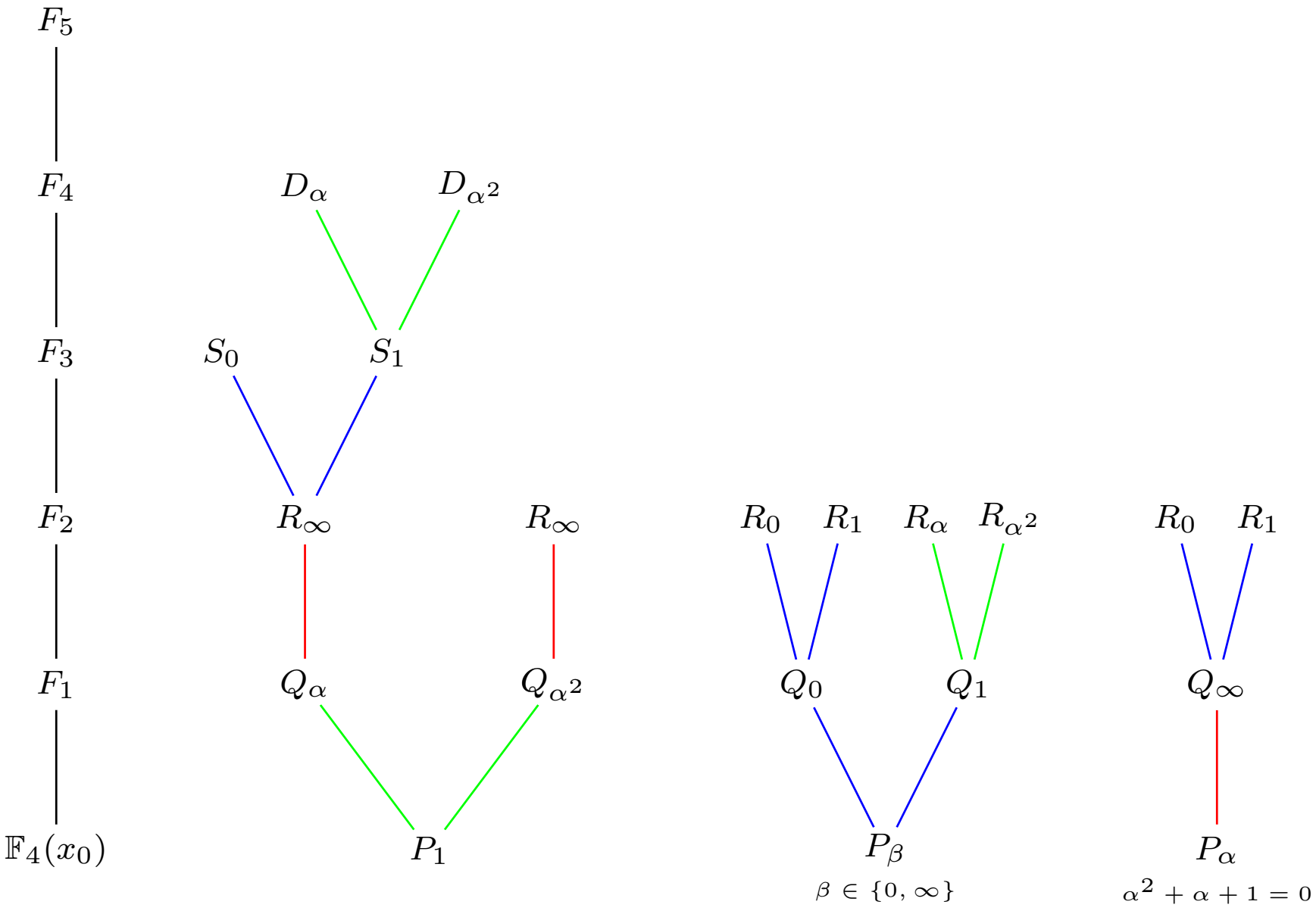
$\beta \in \{0, \infty\}$

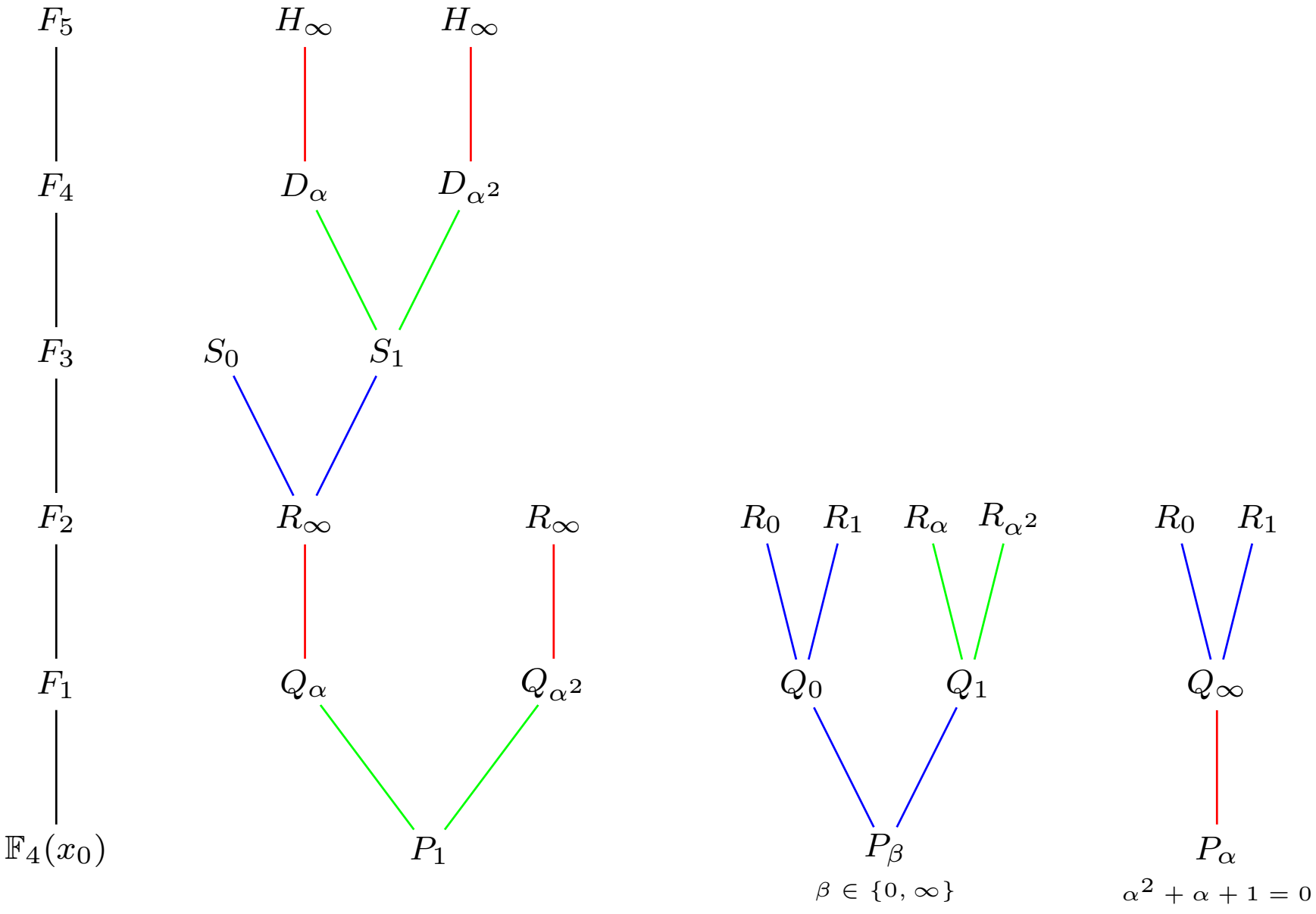


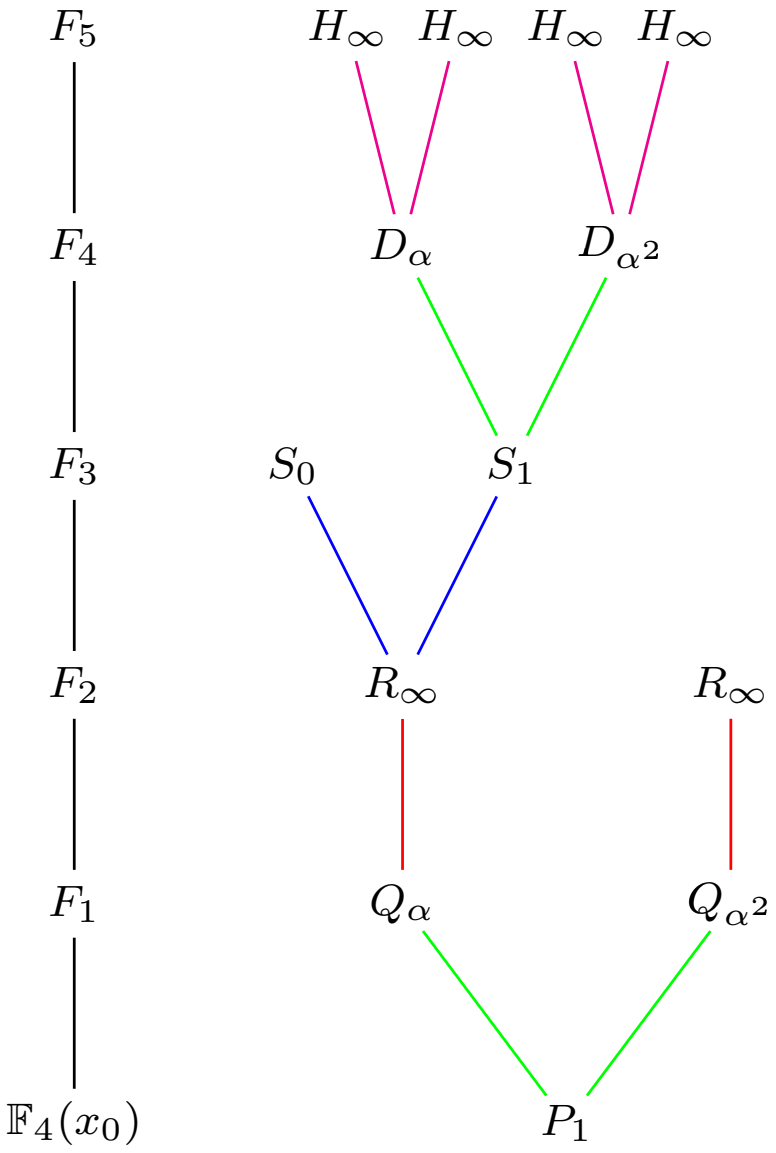
$\alpha^2 + \alpha + 1 = 0$

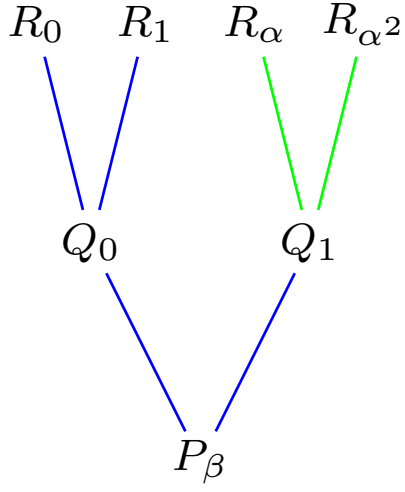

F_5
F_4
F_3
F_2
F_1
$\mathbb{F}_4(x_0)$
R_∞
R_∞
Q_α
Q_{α^2}
P_1
Q_0
Q_1
P_β
$\beta \in \{0, \infty\}$
Q_∞
P_α
$\alpha^2 + \alpha + 1 = 0$


F_5
F_4
F_3
F_2
F_1
$\mathbb{F}_4(x_0)$
R_∞
R_∞
Q_α
Q_{α^2}
P_1
R_0
R_1
R_α
R_{α^2}
Q_0
Q_1
P_β
$\beta \in \{0, \infty\}$
R_0
R_1
Q_∞
P_α
$\alpha^2 + \alpha + 1 = 0$

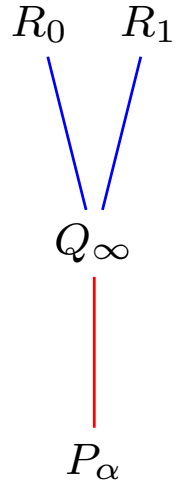

F_5
F_4
F_3
F_2
F_1
$\mathbb{F}_4(x_0)$
D_α
D_{α^2}
S_0
S_1
R_∞
R_∞
Q_α
Q_{α^2}
P_1
R_0
R_1
R_α
R_{α^2}
Q_0
Q_1
P_β
$\beta \in \{0, \infty\}$
R_0
R_1
Q_∞
P_α
$\alpha^2 + \alpha + 1 = 0$


F_5
F_4
F_3
F_2
F_1
$\mathbb{F}_4(x_0)$
H_∞
H_∞
D_α
D_{α^2}
S_0
S_1
R_∞
R_∞
Q_α
Q_{α^2}
P_1
R_0
R_1
R_α
R_{α^2}
Q_0
Q_1
P_β
$\beta \in \{0, \infty\}$
R_0
R_1
Q_∞
P_α
$\alpha^2 + \alpha + 1 = 0$





$\beta \in \{0, \infty\}$



$\alpha^2 + \alpha + 1 = 0$

Otras Torres de tipo AS

$$Y^2 + Y = \frac{X}{X^2 + X + 1}, \text{ sobre } \mathbb{F}_4$$

$$Y^p + bY = \frac{1}{X^p + cX}, \text{ sobre } \mathbb{F}_{p^r}$$

con $b \neq c$ y $bc(b-c)^{2p-2} = 1.$


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.