$y^2 = x^3 - x$ over $\mathbb{F}_5$ in more depth

Unit 18

Gil Cohen

January 4, 2025

Overview

A second floor

In the previous unit we analyzed $\mathsf{F}_1/\mathsf{F}_0$ where

$$\mathsf{F}_0 = \mathbb{F}_5(x),$$
$$\mathsf{F}_1 = \mathbb{F}_5(x, y) \qquad y^2 = x^3 - x.$$

We now further extend by considering

$$\mathsf{F}_2 = \mathsf{F}_1(z) = \mathbb{F}_5(x, y, z) \qquad z^2 = y^3 - y.$$

A second floor

Note that we could have extended $F_2/\mathbb{F}_5(x)$ directly. Indeed,

$$z^2 = y^3 - y = y(y^2 - 1) = y(x^3 - x - 1),$$

and so

$$z^4 = y^2(x^3 - x - 1)^2 = (x^3 - x)(x^3 - x - 1)^2.$$

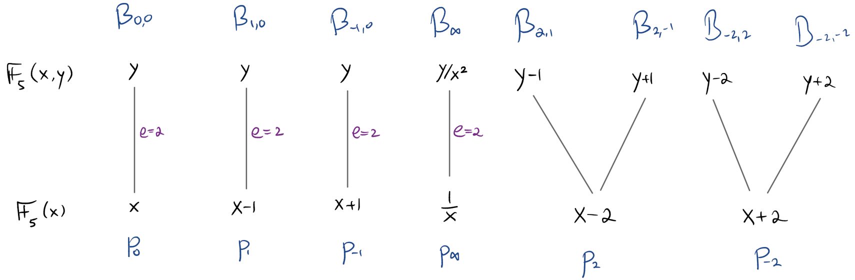
So we could have defined $F_2 = \mathbb{F}_5(x, z)$ with

$$z^4 = (x^3 - x)(x^3 - x - 1)^2.$$

However, it is more convenient to study F_2/F_0 by considering F_1.

More generally, by the primitive element theorem, as $F_2/\mathbb{F}_5(x)$ is finite & separable $\exists w \in F_2$ s.t. $F_2 = \mathbb{F}_5(x, w)$ (in fact all but finitely many w-s would work). So, the geometric interpretation of the primitive element theorem (in our context) is that every function field can be associated with a plane curve!

A second floor - the rational prime divisors



Let's start with $\mathfrak{P}_\infty$. Recall that $v_{\mathfrak{P}_\infty}(y) = -3$. If $\mathfrak{q} \in \mathbb{P}(F_2)$ lies over $\mathfrak{P}_\infty$ then

$$2 \cdot v_{\mathfrak{q}}(z) = v_{\mathfrak{q}}(z^2) = e(\mathfrak{q}/\mathfrak{P}_\infty) \cdot v_{\mathfrak{P}_\infty}(y^3 - y) = e(\mathfrak{q}/\mathfrak{P}_\infty) \cdot \min(-9, -3).$$

Thus, $e(\mathfrak{q}/\mathfrak{P}_\infty) = 2$ and $v_{\mathfrak{q}}(z) = -9$. In particular, $\mathfrak{P}_\infty$ totally ramifies.

A second floor - the rational prime divisors

As

$$(y)_{F_1} = \mathfrak{P}_{0,0} + \mathfrak{P}_{1,0} + \mathfrak{P}_{-1,0} - 3\mathfrak{P}_{\infty},$$

the same holds for $\mathfrak{P}_{0,0}, \mathfrak{P}_{1,0}, \mathfrak{P}_{-1,0}$. E.g., if $\mathfrak{q}/\mathfrak{P}_{0,0}$ then

$$2 \cdot v_{\mathfrak{q}}(z) = v_{\mathfrak{q}}(z^2) = e(\mathfrak{q}/\mathfrak{P}_{0,0}) \cdot v_{\mathfrak{P}_{0,0}}(y^3 - y) = e(\mathfrak{q}/\mathfrak{P}_{0,0}) \cdot \min(3,1),$$

and so $e(\mathfrak{q}/\mathfrak{P}_{0,0}) = 2$ and $v_{\mathfrak{q}}(z) = 1$, namely, z is a local parameter for $\mathfrak{q}$.

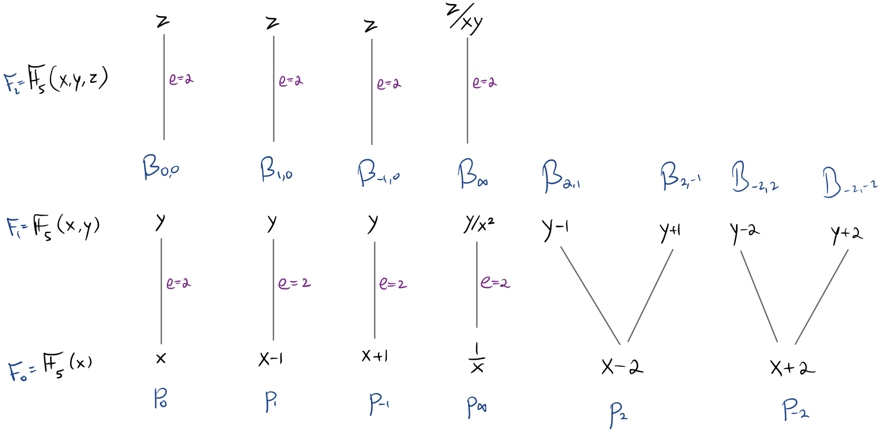
What is a local parameter for the prime divisor $\mathfrak{q}_{\infty}$ lying over $\mathfrak{P}_{\infty}$? We know that

$$\begin{aligned} v_{\mathfrak{q}_\infty}(z) &= -9, \\ v_{\mathfrak{q}_\infty}(y) &= e(\mathfrak{q}_\infty/\mathfrak{P}_\infty) \cdot v_{\mathfrak{P}_\infty}(y) = 2 \cdot (-3) = -6, \\ v_{\mathfrak{q}_\infty}(x) &= e(\mathfrak{q}_\infty/\mathfrak{P}_\infty) \cdot v_{\mathfrak{P}_\infty}(x) = 2 \cdot (-2) = -4, \end{aligned}$$

and so

$$v_{\mathfrak{q}_\infty}\left(\frac{z}{xy}\right) = 1.$$

A second floor - the rational prime divisors



A second floor - the rational prime divisors

Consider now $\mathfrak{P}_{-2,2}$. Since $z^2 = y^3 - y$ and $y^3 - y \in \mathcal{O}_{\mathfrak{P}_{-2,2}}$ we have that $z \in \mathcal{O}'_{\mathfrak{P}_{-2,2}}$. Indeed,

$$\varphi(T) = T^2 - (y^3 - y) \in \mathcal{O}_{\mathfrak{P}_{-2,2}}[T]$$

is a monic polynomial that vanishes at z.

Since $\mathrm{F}_2/\mathrm{F}_1$ is finite and separable, we can apply Kummer's Theorem.

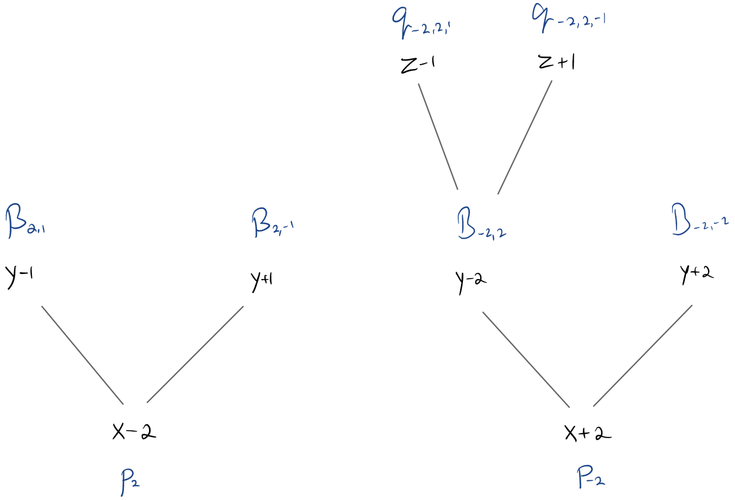
We have the projection

$$\varphi_{-2,2}(T) = T^2 - (2^3 - 2) = T^2 - 1 = (T+1)(T-1).$$

Hence, by Kummer's Theorem, there are two prime divisors lying over $\mathfrak{P}_{-2,2}$. One $\mathfrak{q}_{-2,2,-1}$ for which $z + 1 \in \mathfrak{m}_{\mathfrak{q}_{-2,2,-1}}$, and the other, $\mathfrak{q}_{-2,2,1}$, satisfies $z - 1 \in \mathfrak{m}_{\mathfrak{q}_{-2,2,1}}$.

I leave it for you to verify that these are local parameters.

A second floor - the rational prime divisors



A second floor - the rational prime divisors

Consider now $\mathfrak{P}_{-2,-2}$.

$$\varphi(T) = T^2 - (y^3 - y) \in \mathcal{O}_{\mathfrak{P}_{-2,-2}}[T]$$

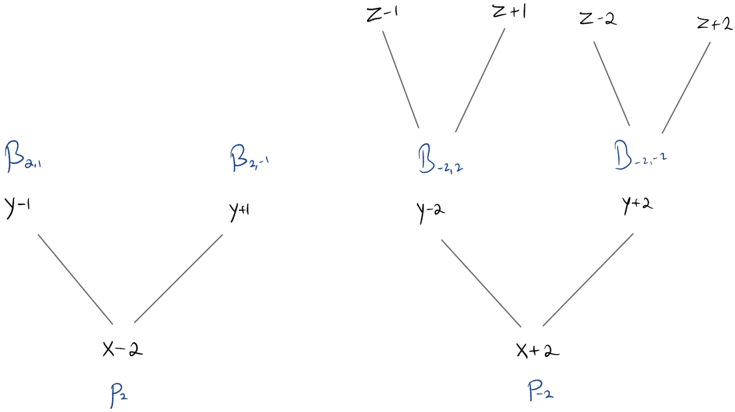
is a monic polynomial that vanishes at z. We have the projection

$$\begin{aligned}\varphi_{-2,-2}(T) &= T^2 - ((-2)^3 - (-2)) \\ &= T^2 + 1 = (T+2)(T-2).\end{aligned}$$

Hence, by Kummer's Theorem, there are two prime divisors lying over $\mathfrak{P}_{-2,-2}$.

I leave it for you to verify that these are local parameters.

A second floor - the rational prime divisors



A second floor - the rational prime divisors

Consider now $\mathfrak{P}_{2,1}$.

$$\varphi(T) = T^2 - (y^3 - y) \in \mathcal{O}_{\mathfrak{P}_{2,1}}[T]$$

is a monic polynomial that vanishes at z. We have the projection

$$\varphi_{2,1}(T) = T^2 - (1^3 - 1) = T^2.$$

Hence, Kummer's Theorem does not apply.

However, we can still prove that $\mathfrak{P}_{2,1}$ totally ramifies using the fundamental equality trick.

A second floor - the rational prime divisors

Let $\mathfrak{q}/\mathfrak{P}_{2,1}$. We have that

$$2 \cdot v_{\mathfrak{q}}(z) = v_{\mathfrak{q}}(z^2) = v_{\mathfrak{q}}(y^3 - y) = e(\mathfrak{q}/\mathfrak{P}_{2,1}) \cdot v_{\mathfrak{P}_{2,1}}(y^3 - y).$$

We want to show that $e(\mathfrak{q}/\mathfrak{P}_{2,1}) = 2$. To this end, it suffices to show that

$$v_{\mathfrak{P}_{2,1}}(y^3 - y) = 1.$$

Now,

$$v_{\mathfrak{P}_{2,1}}(y^3 - y) = v_{\mathfrak{P}_{2,1}}(y^2 - 1) + v_{\mathfrak{P}_{2,1}}(y) = v_{\mathfrak{P}_{2,1}}(y^2 - 1),$$

where the last equality follows as $v_{\mathfrak{P}_{2,1}}(y - 1) > 0$ and so $v_{\mathfrak{P}_{2,1}}(y) > 0$ would imply $v_{\mathfrak{P}_{2,1}}(1) > 0$.

So we need to show that

$$v_{\mathfrak{P}_{2,1}}(y^2 - 1) = 1.$$

A second floor - the rational prime divisors

We need to show that

$$v_{\mathfrak{P}_{2,1}}(y^2 - 1) = 1.$$

Now,

$$y^2 - 1 = x^3 - x - 1 = (x-2)(x^2 + 2x + 3),$$

where, recall $x^2 + 2x + 3$ is irreducible in $\mathbb{F}_5[x]$. Thus,

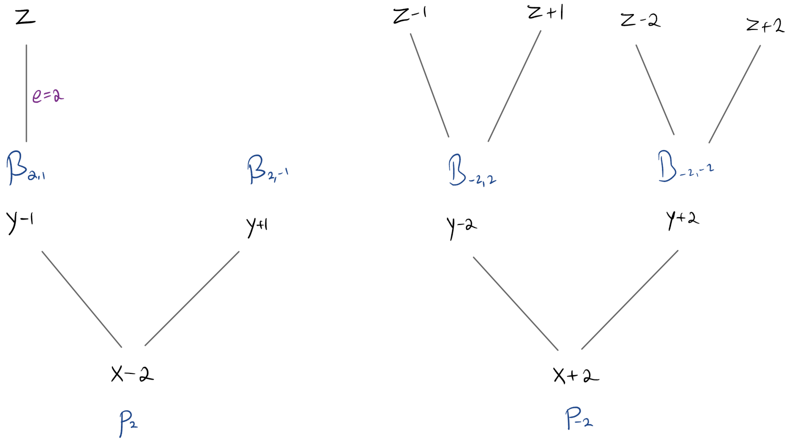
$$\begin{aligned} v_{\mathfrak{P}_{2,1}}(y^2 - 1) &= v_{\mathfrak{P}_{2,1}}((x-2)(x^2 + 2x + 3)) \\ &= e(\mathfrak{P}_{2,1}/\mathfrak{p}_2) \cdot v_{\mathfrak{p}_2}((x-2)(x^2 + 2x + 3)) = 1. \end{aligned}$$

This proves that $e(\mathfrak{q}/\mathfrak{P}_{2,1}) = 2$.

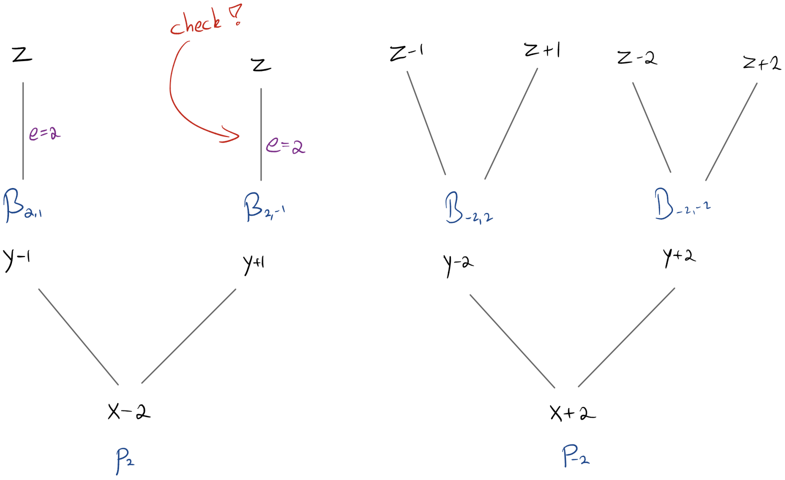
z is a local parameter for $\mathfrak{q}$ since

$$2 \cdot v_{\mathfrak{q}}(z) = v_{\mathfrak{q}}(z^2) = v_{\mathfrak{q}}(y^3 - y) = e(\mathfrak{q}/\mathfrak{P}_{2,1}) \cdot v_{\mathfrak{P}_{2,1}}(y^3 - y) = 2 \cdot 1 = 2.$$

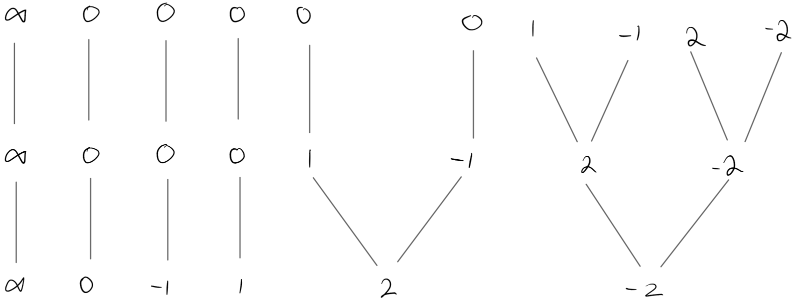
A second floor - the rational prime divisors



A second floor - the rational prime divisors



A second floor - the rational prime divisors



Overview

Hurwitz Genus Formula

Theorem 1 (Hurwitz Genus Formula)

Let F/L *be a finite separable extension of* E/K*. Let* $g_{\mathsf{E}}, g_{\mathsf{F}}$ *be the corresponding genera. Then,*

$$2g_{\mathsf{F}} - 2 = \frac{[\mathsf{F} : \mathsf{E}]}{[\mathsf{L} : \mathsf{K}]} \cdot (2g_{\mathsf{E}} - 2) + \deg \mathrm{Diff}(\mathsf{F}/\mathsf{E}).$$

Diff that appears in Hurwitz Genus Formula is an important divisor called the different of F/E,

$$\mathrm{Diff}(\mathsf{F}/\mathsf{E}) = \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{E})} \sum_{\mathfrak{P}/\mathfrak{p}} d(\mathfrak{P}/\mathfrak{p})\mathfrak{P},$$

where we are not yet in a position to define $d(\mathfrak{P}/\mathfrak{p})$. However, Dedekind's Different Theorem relates $d(\mathfrak{P}/\mathfrak{p})$ with the ramification index $e(\mathfrak{P}/\mathfrak{p})$ in some cases.

Dedekind Different Theorem

Theorem 2 (Dedekind Different Theorem)

Let F/L *be a finite separable extension of* E/K*. Let* $\mathfrak{p} \in \mathbb{P}(\mathrm{E})$ *and* $\mathfrak{P} \in \mathbb{P}(\mathrm{F})$ *lying over* $\mathfrak{p}$*. Then,*

1. $d(\mathfrak{P}/\mathfrak{p}) \geq e(\mathfrak{P}/\mathfrak{p}) - 1$*; and*
2. $d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1 \quad \Longleftrightarrow \quad \mathrm{char}\,\mathrm{K} \nmid e(\mathfrak{P}/\mathfrak{p})$.

Corollary 3

With the above notations,

$$d(\mathfrak{P}/\mathfrak{p}) = 0 \quad \Longleftrightarrow \quad e(\mathfrak{P}/\mathfrak{p}) = 1$$

In particular, for almost all $\mathfrak{p}, \mathfrak{P}/\mathfrak{p}$ *we have that* $e(\mathfrak{P}/\mathfrak{p}) = 1$.

Overview

A second floor - the genus

By Hurwitz Genus Formula, and since $g_1 = 1$,

$$2g_2 - 2 = 2 \cdot (2g_1 - 2) + \deg \mathrm{Diff}(F_2/F_1) \quad \Longrightarrow \quad g_2 = 1 + \frac{1}{2} \cdot \deg \mathrm{Diff}(F_2/F_1).$$

Now,

$$\mathrm{Diff}(F_2/F_1) = \sum_{\mathfrak{P} \in \mathbb{P}(F_1)} \sum_{\mathfrak{q}/\mathfrak{P}} d(\mathfrak{q}/\mathfrak{P})\mathfrak{q}.$$

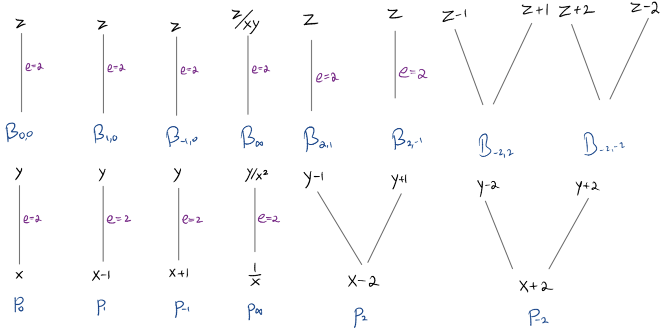
As F_2/F_1 is tame (the characteristic, 5, does not divide the ramification indices $\in \{1, 2\}$), by Dedekind Different Theorem,

$$d(\mathfrak{q}/\mathfrak{P}) = e(\mathfrak{q}/\mathfrak{P}) - 1,$$

and so our task is to find all ramified places in F_2/F_1.

A second floor - the genus

We have already found 6 such places:



are there more? Yes! but let's take a detour, and compute the principal divisors of x, y, z in F_2.

Overview

Some principal divisors

As

$$(x)_{F_1} = 2\mathfrak{P}_{0,0} - 2\mathfrak{P}_{\infty}$$

we have that

$$(x)_{F_2} = 4\mathfrak{q}_{0,0,0} - 4\mathfrak{q}_{\infty}.$$

Similarly, since

$$(y)_{F_1} = \mathfrak{P}_{0,0} + \mathfrak{P}_{1,0} + \mathfrak{P}_{-1,0} - 3\mathfrak{P}_{\infty},$$

we have that

$$(y)_{F_2} = 2\mathfrak{q}_{0,0,0} + 2\mathfrak{q}_{1,0,0} + 2\mathfrak{q}_{-1,0,0} - 6\mathfrak{q}_{\infty}.$$

Let's find $(z)_{F_2}$.

Some principal divisors

First let's find where (at which $\mathfrak{q} \in \mathbb{P}(F_2)$) are the zeros and poles of z.

$$v_{\mathfrak{q}}(z) \neq 0 \iff v_{\mathfrak{q}}(z^2) \neq 0 \iff v_{\mathfrak{P}}(y^3 - y) \neq 0,$$

where $\mathfrak{P} \in \mathbb{P}(F_1)$ lies under $\mathfrak{q}$.

Consider now two cases. First, if $v_{\mathfrak{P}}(y) \neq 0$ then

$$v_{\mathfrak{P}}(y^3) = 3 \cdot v_{\mathfrak{P}}(y) \neq v_{\mathfrak{P}}(y) \implies v_{\mathfrak{P}}(y^3 - y) \neq 0.$$

Thus, z has zeros and poles over those of y.

Recall that

$$(y)_{F_2} = 2\mathfrak{q}_{0,0,0} + 2\mathfrak{q}_{1,0,0} + 2\mathfrak{q}_{-1,0,0} - 6\mathfrak{q}_{\infty}.$$

and so a simple calculation that I will leave to you shows that

$(z)_{F_2} = \mathfrak{q}_{0,0,0} + \mathfrak{q}_{1,0,0} + \mathfrak{q}_{-1,0,0} - 9\mathfrak{q}_{\infty} +$ whatever comes from the other case.

Some principal divisors

$(z)_{F_2} = \mathfrak{q}_{0,0} + \mathfrak{q}_{1,0} + \mathfrak{q}_{-1,0} - 9\mathfrak{q}_\infty +$ whatever comes from the other case.

As a detour recall that

$$\deg(z)_{F_2,\infty} = [F_2 : \mathbb{F}_5(z)].$$

Now,

$$\begin{aligned}[F_2 : \mathbb{F}_5(z)] &= [\mathbb{F}_5(x,y,z) : \mathbb{F}_5(z)] \\ &= [\mathbb{F}_5(x,y,z) : \mathbb{F}_5(y,z)] \cdot [\mathbb{F}_5(y,z) : \mathbb{F}_5(z)].\end{aligned}$$

Recall $z^2 = y^3 - y$, and so $T^3 - T - z^2 \in \mathbb{F}_5(z)[T]$ vanishes at y. It can be shown to be irreducible and so

$$[\mathbb{F}_5(y,z) : \mathbb{F}_5(z)] = 3.$$

Similarly, $[\mathbb{F}_5(x,y,z) : \mathbb{F}_5(y,z)] = 3$ and so

$$\deg(z)_{F_2,\infty} = [F_2 : \mathbb{F}_5(z)] = 3 \cdot 3 = 9.$$

Some principal divisors

$(z)_{F_2} = \mathfrak{q}_{0,0} + \mathfrak{q}_{1,0} + \mathfrak{q}_{-1,0} - 9\mathfrak{q}_\infty +$ whatever comes from the other case.

Moving on to Case 2 - $v_{\mathfrak{P}}(y) = 0$, and so

$$v_{\mathfrak{P}}(y^3 - y) = v_{\mathfrak{P}}(y^2 - 1) + v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(y^2 - 1).$$

Thus, for the prime divisor $\mathfrak{p}$ lying under $\mathfrak{P}$,

$$v_{\mathfrak{p}}(x^3 - x - 1) \neq 0.$$

Recall that $x^3 - x - 1 = (x - 2)(x^2 - 2x + 3)$ and so

$$\mathfrak{p} \in \{\mathfrak{p}_2, \mathfrak{p}_{x^2-2x+3}\}.$$

A calculation I will leave to you shows that the two prime divisors of F_2 lying over $\mathfrak{p}_2$ are simple zeros of z.

Some principal divisors

Denote $\mathfrak{p}' \triangleq \mathfrak{p}_{x^2-2x+3}$.

We have that

$$y^2 - 1 = x^3 - x - 1 = (x-2)(x^2 - 2x + 3)$$

and so

$$\varphi(T) = T^2 - (x-2)(x^2 - 2x + 3) - 1$$

is the minimal polynomial of y over $\mathbb{F}_5(x)$. Thus, $y \in \mathcal{O}'_{\mathfrak{p}'}$ and the projection to $(\mathsf{F}_2)_{\mathfrak{p}'}[T]$ is

$$\bar{\varphi}(T) = T^2 - 1.$$

Thus, by Kummer's Theorem, there are two prime divisors lying over $\mathfrak{p}'$ in F_1 which we denote by

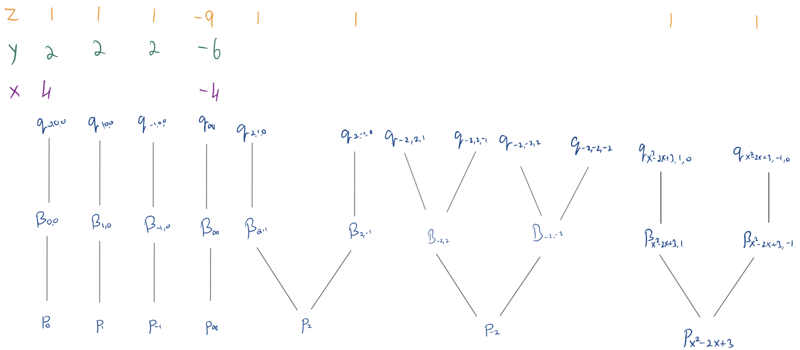
$$\mathfrak{P}_{x^2-2x+3,1}, \mathfrak{P}_{x^2-2x+3,-1}.$$

Some principal divisors

From here it is standard by now to check that each totally ramifies in F_2/F_1.

To summarize, we have that

$$\begin{aligned}(z)_{F_2} = &\mathfrak{q}_{0,0,0} + \mathfrak{q}_{1,0,0} + \mathfrak{q}_{-1,0,0} - 9\mathfrak{q}_{\infty} + \\ &\mathfrak{q}_{2,1,0} + \mathfrak{q}_{2,-1,0} + \mathfrak{q}_{x^2-2x+3,1,0} + \mathfrak{q}_{x^2-2x+3,-1,0}.\end{aligned}$$



A second floor - Weierstrass gaps

Now that we have that

$$(x)_{F_2,\infty} = 4\mathfrak{q}_\infty,$$
$$(y)_{F_2,\infty} = 6\mathfrak{q}_\infty,$$
$$(z)_{F_2,\infty} = 9\mathfrak{q}_\infty,$$

we can look at $\mathcal{L}(r \cdot \mathfrak{q}_\infty)$ for $r = 0, 1, 2, \ldots$

deg	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	1	-	-	-	x	-	y	-	x^2	z	xy	-	y^2	xz	x^2y	yz	xy^2
gil-dim	1	1	1	1	2	2	3	3	4	5	6	6	7	8	9	10	11

Overview

Back to the genus

deg	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	1	-	-	-	x	-	y	-	x^2	z	xy	-	y^2	xz	x^2y	yz	xy^2
gil-dim	1	1	1	1	2	2	3	3	4	5	6	6	7	8	9	10	11

Assuming we can continue on like that, showing that

$$\forall r > 16 \quad \mathcal{L}(r \cdot \mathfrak{q}_\infty) \neq \mathcal{L}((r-1) \cdot \mathfrak{q}_\infty)$$

(and we can), taking into account that the red dashes are me unable to find a function in the corresponding space, we conclude by Riemann-Roch that $g \leq 6$.

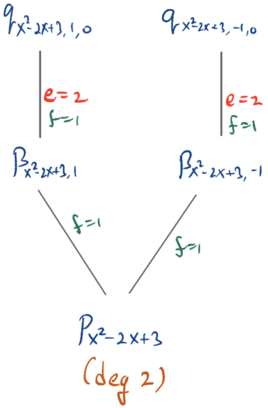
Back to the genus

On the other hand, recall that we have already found 6 ramified places in F_2/F_1, all of degree 1, and so

$$\begin{aligned} g_2 &= 1 + \frac{1}{2} \cdot \deg \operatorname{Diff}(F_2/F_1) \\ &= 1 + \frac{1}{2} \cdot \sum_{\mathfrak{P} \in \mathbb{P}(F_1)} \sum_{\substack{\mathfrak{q}/\mathfrak{P} \\ \text{ramifies}}} \deg \mathfrak{q} \\ &\geq 1 + \frac{1}{2} \cdot 6 = 4. \end{aligned}$$

It turns out that the genus is indeed $g_2 = 6$ - there are two more places in F_2 that ramify, each is of degree 2 over F_1. In fact, both lie over the place $\mathfrak{p}_{x^2-x+3}$ we've encountered before.

Back to the genus

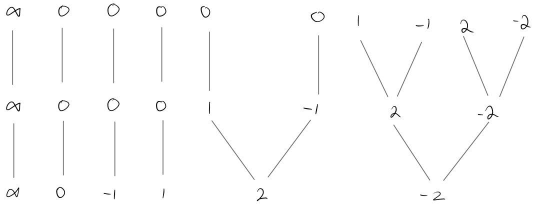


I leave it to you to verify this. In fact, we did almost all the work before, when computing the principal divisors.

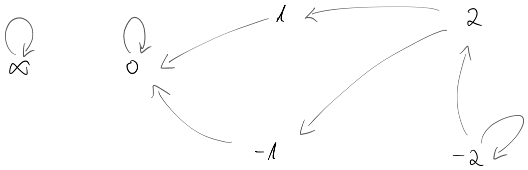
Overview

More floors

For three floors we had

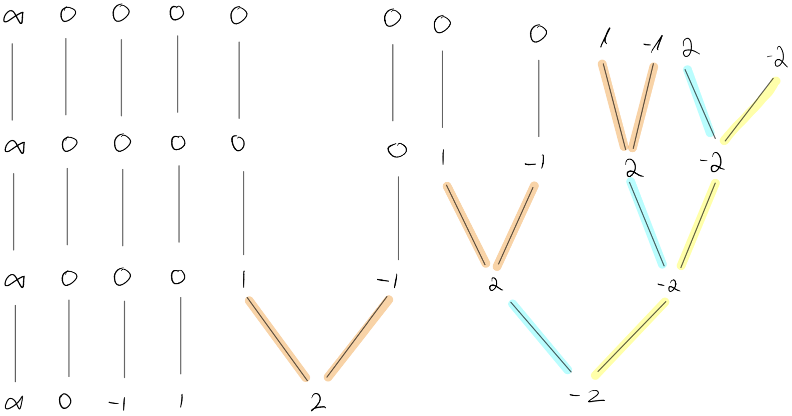


In general, we have the following behavior:



More floors

For four floors we will get



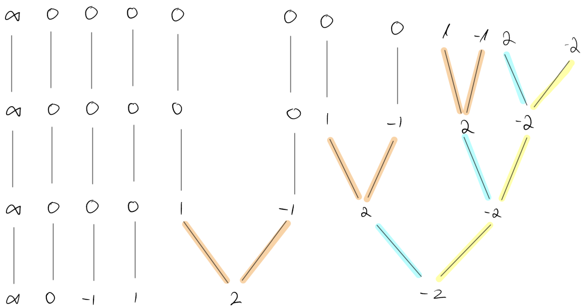
More floors

Denote by $n_i \triangleq \mathrm{N}(\mathrm{F}_i)$ the number of rational prime divisors in $\mathrm{F}_i/\mathbb{F}_5$.

It is easy to see that the following recursive relation holds:

$$n_i = n_{i-1} + 2,$$
$$n_0 = 6,$$

and so $n_i = 6 + 2i$.



More floors

As for the genus $g_i \triangleq g(\mathsf{F}_i)$, by Hurwitz Genus Formula,

$$g_i = 2g_{i-1} - 1 + \frac{1}{2} \deg \operatorname{Diff}(\mathsf{F}_i/\mathsf{F}_{i-1}).$$

Now,

$$\operatorname{Diff}(\mathsf{F}_i/\mathsf{F}_{i-1}) = \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{F}_{i-1})} \sum_{\mathfrak{P}/\mathfrak{p}} d(\mathfrak{P}/\mathfrak{p})\mathfrak{P}.$$

As $\mathsf{F}_i/\mathsf{F}_{i-1}$ is tame, by Dedekind Different Theorem,

$$d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1,$$

and so, even if we only consider the ramification that occurs at rational prime divisors,

$$\deg \operatorname{Diff}(\mathsf{F}_i/\mathsf{F}_{i-1}) \geq \text{ number of } \mathfrak{p} \in \mathbb{P}(\mathsf{F}_{i-1}) \text{ that ramify.}$$

More floors

$$g_i = 2g_{i-1} - 1 + \frac{1}{2}\deg \mathrm{Diff}(\mathsf{F}_i/\mathsf{F}_{i-1}),$$

$$\deg \mathrm{Diff}(\mathsf{F}_i/\mathsf{F}_{i-1}) \geq \text{ number of } \mathfrak{p} \in \mathbb{P}(\mathsf{F}_{i-1}) \text{ that ramify.}$$

It is easy to see that the number of prime divisors in F_i that ramify is $4 + 2i$, and so

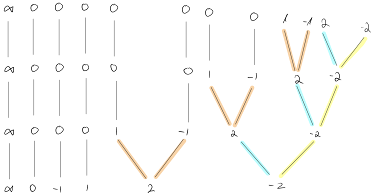
$$\deg \mathrm{Diff}(\mathsf{F}_i/\mathsf{F}_{i-1}) \geq 2 + 2i.$$

Thus,

$$g_i \geq 2g_{i-1} + i.$$

Since $g_0 = 0$ we have

$$g_i \geq 2^{i+1} - i - 2.$$



More floors

To summarize, we have that

$$n_i = 2i + 6,$$
$$g_i \geq 2^{i+1} - i - 2.$$

Recall that Goppa codes satisfy

$$\rho + \delta \geq 1 - \frac{g-1}{n}.$$

Since for $g_i > n_i$ for $i \geq 3$, floors 3 and higher, used in the general construction by Goppa, fail to give meaningful codes.

Overview

A better example

Consider the function field $F = \mathbb{F}_9(x, y)$, where

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

Since this is a degree $n = 2$ extension of $\mathbb{F}_9(x)$ we are in a similar situation as in the previous example. In particular, $\mathbb{F}_9$ is the constant field of F.

Moreover, the ramification indices are either 1 or 2 and anyhow are coprime to the characteristic, 3.

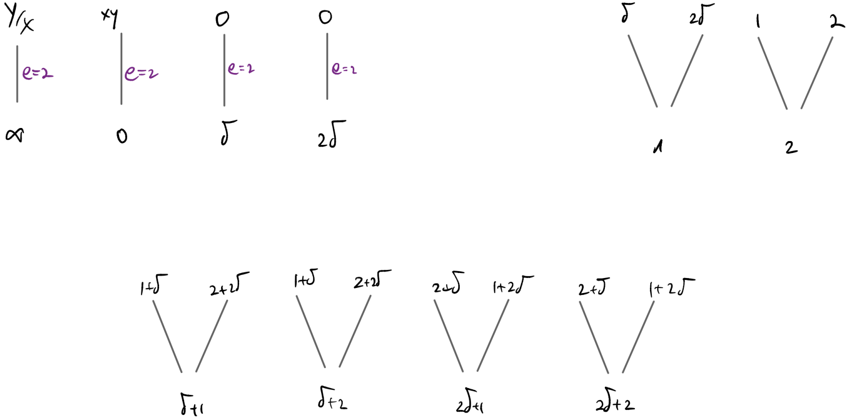
Rational prime divisors

By observing the table, Kummer's Theorem implies that any $\alpha \in \mathbb{F}_9 \setminus \{0, \delta, 2\delta\}$ splits completely in $F/\mathbb{F}_9(x)$.

Using the fundamental equality trick, we can show that $0, \delta, 2\delta$ as well as ∞ totally ramify.

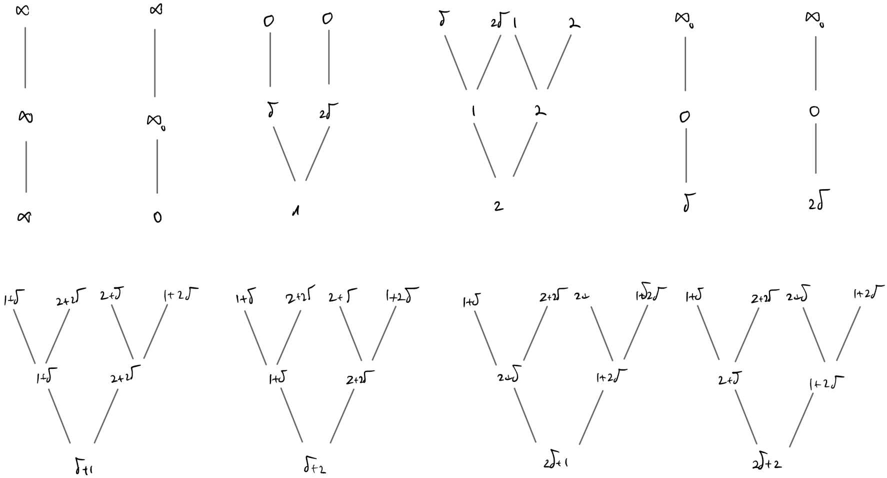
α	α^2	$\frac{1}{\alpha}$	$\alpha + \frac{1}{\alpha}$	$\sqrt{\alpha + \frac{1}{\alpha}}$
0	0	–	–	–
1	1	1	2	$\delta, 2\delta$
2	1	2	1	$1, 2$
δ	2	2δ	0	0
$1+\delta$	2δ	$2+\delta$	2δ	$1+\delta, 2+2\delta$
$2+\delta$	δ	$1+\delta$	2δ	$1+\delta, 2+2\delta$
2δ	2	δ	0	0
$1+2\delta$	δ	$2+2\delta$	δ	$2+\delta, 1+2\delta$
$2+2\delta$	2δ	$1+2\delta$	δ	$2+\delta, 1+2\delta$

Rational prime divisors



I leave it to you to prove that the genus is 1.

Second level



The general tower

It is easy to see that

$$N(F_i) \geq 4 \cdot 2^i.$$

I leave it to you to check that

$$g(F_i) = 2^{i+1} - i + 2.$$

Thus,

$$\frac{g(F_i)}{N(F_i)} \to \frac{1}{2},$$

and so one can get Goppa codes over $\mathbb{F}_9$ of unbounded length with

$$\rho + \delta \geq \frac{1}{2} - o(1).$$

Over $\mathbb{F}_9$, these codes are in fact optimal among Goppa codes. It has to do with the fact that

$$2 = \sqrt{9} - 1.$$