Explicit Formulas for the Different

Unit 24

Gil Cohen

January 14, 2025

Recall - local integral bases

Definition 1

Let F/L be an extension of E/K, and let $\mathfrak{p} \in \mathbb{P}(E)$.

A basis $z_1, \ldots, z_n$ of F/E for which

$$\mathcal{O}'_{\mathfrak{p}} = \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} z_i$$

is called an integral basis of $\mathcal{O}'_{\mathfrak{p}}$ over $\mathcal{O}_{\mathfrak{p}}$ (or a local integral basis of F/E for $\mathfrak{p}$).

Note that if $z_1, \ldots, z_n$ is a local integral basis for $\mathfrak{p}$ then $z_1, \ldots, z_n \in \mathcal{O}'_{\mathfrak{p}}$.

But $z_1, \ldots, z_n \in \mathcal{O}'_{\mathfrak{p}}$ only implies

$$\mathcal{O}'_{\mathfrak{p}} \supseteq \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} z_i.$$

Recall - local integral bases and the complementary module

Recall the definition of the complementary module

$$\mathsf{C}_{\mathfrak{p}} = \left\{ z \in \mathsf{F} : \mathrm{Tr}_{\mathsf{F}/\mathsf{E}}(z\mathcal{O}'_{\mathfrak{p}}) \subseteq \mathcal{O}_{\mathfrak{p}} \right\}.$$

Claim 2

Let $z_1, \ldots, z_n$ be a local integral basis of F/E for $\mathfrak{p}$, namely, $z_1, \ldots, z_n$ is a basis of F over E s.t.

$$\mathcal{O}'_{\mathfrak{p}} = \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} z_i$$

(we proved such a basis always exists). Then,

$$\mathsf{C}_{\mathfrak{p}} = \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} z_i^*.$$

Overview

1. A lemma about the dual basis
2. A bound on the different exponent
3. The different exponent and local bases
4. The different exponent and total ramification

A lemma about the dual basis

We have the following lemma about dual bases.

Lemma 3

Let F/L *be a degree* n *separable extension of* E/K *s.t.*

$$\mathsf{F} = \mathsf{E}(y) \qquad y \in \mathsf{F}.$$

Let $\varphi(T) \in \mathsf{E}[T]$ *be the minimal polynomial of* y *over* E*, and write*

$$\varphi(T) = (T - y)(c_0 + c_1 T + c_2 T^2 + \cdots + c_{n-1} T^{n-1}),$$

with $c_i \in \mathsf{F}$*. Then, the dual basis of* $1, y, y^2, \ldots, y^{n-1}$ *is given by*

$$\frac{c_0}{\varphi'(y)}, \ldots, \frac{c_{n-1}}{\varphi'(y)}.$$

Note that $\varphi'(y) \neq 0$ as y is separable over E.

A lemma about the dual basis

Proof.

We need to show that

$$\forall i, \ell \in \{0, 1, \ldots, n-1\} \qquad \mathrm{Tr}_{\mathsf{F}/\mathsf{E}}\left(\frac{c_i}{\varphi'(y)} \cdot y^{\ell}\right) = \delta_{i,\ell}.$$

To this end, consider the n distinct embeddings $\sigma_1, \ldots, \sigma_n$ of F over E into $\bar{\mathsf{F}}$.

Denote $y_j = \sigma_j(y)$. By Galois theory,

$$\varphi(T) = \prod_{j=1}^{n} (T - y_j) \in \bar{\mathsf{F}}[T].$$

Differentiating and substituting $T = y_\nu$ yields

$$\varphi'(y_\nu) = \prod_{i \neq \nu} (y_\nu - y_i).$$

A lemma about the dual basis

Proof.

For $0 \le \ell \le n-1$ consider the polynomial

$$\varphi_\ell(T) = \left(\sum_{j=1}^{n} \frac{\varphi(T)}{T - y_j} \cdot \frac{y_j^\ell}{\varphi'(y_j)} \right) - T^\ell \in \bar{\mathbb{F}}[T].$$

For every $1 \le \nu \le n$,

$$\varphi_\ell(y_\nu) = \left(\prod_{i \ne \nu} (y_\nu - y_i) \right) \cdot \frac{y_\nu^\ell}{\varphi'(y_\nu)} - y_\nu^\ell = 0.$$

Since the y_ν-s are all distinct, and $\deg \varphi_\ell(T) \le n-1$, and , $\varphi_\ell(T)$ is the zero polynomial. That is, for $0 \le \ell \le n-1$,

$$T^\ell = \sum_{j=1}^{n} \frac{\varphi(T)}{T - y_j} \cdot \frac{y_j^\ell}{\varphi'(y_j)}.$$

A lemma about the dual basis

Proof.

$$\forall 0 \leq \ell \leq n-1 \qquad T^\ell = \sum_{j=1}^{n} \frac{\varphi(T)}{T-y_j} \cdot \frac{y_j^\ell}{\varphi'(y_j)}.$$

We extend the embeddings $\sigma_i : \mathsf{F} \to \bar{\mathsf{F}}$ in the natural way to $\mathsf{F}(T) \to \bar{\mathsf{F}}(T)$ by setting $\sigma_i(T) = T$. We get

$$\begin{aligned} T^\ell &= \sum_{j=1}^{n} \sigma_j \left(\frac{\varphi(T)}{T-y} \cdot \frac{y^\ell}{\varphi'(y)} \right) \\ &= \sum_{j=1}^{n} \sigma_j \left(\sum_{i=0}^{n-1} c_i T^i \cdot \frac{y^\ell}{\varphi'(y)} \right) \\ &= \sum_{i=0}^{n-1} \left(\sum_{j=1}^{n} \sigma_j \left(\frac{c_i}{\varphi'(y)} \cdot y^\ell \right) \right) T^i = \sum_{i=0}^{n-1} \mathrm{Tr}_{\mathsf{F}/\mathsf{E}} \left(\frac{c_i}{\varphi'(y)} \cdot y^\ell \right) T^i. \end{aligned}$$

A lemma about the dual basis

Proof.

$$T^\ell = \sum_{i=0}^{n-1} \mathrm{Tr}_{\mathsf{F}/\mathsf{E}} \left(\frac{c_i}{\varphi'(y)} \cdot y^\ell \right) T^i.$$

Comparing coefficients we get that

$$\mathrm{Tr}_{\mathsf{F}/\mathsf{E}} \left(\frac{c_i}{\varphi'(y)} \cdot y^\ell \right) = \delta_{i,\ell}$$

as required. □

Overview

A bound on the different exponent

Theorem 4

Let F/L *be a finite separable extension of* E/K *s.t.*

$$\mathsf{F} = \mathsf{E}(y) \qquad y \in \mathsf{F}.$$

Let $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *be s.t.* $y \in \mathcal{O}'_{\mathfrak{p}}$.

Let $\varphi(T) \in \mathcal{O}_{\mathfrak{p}}[T]$ *be the minimal polynomial of* y *over* E.

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(\mathsf{F})$ *be the prime divisors lying over* $\mathfrak{p}$. *Then,*

$$\forall i \in [r] \quad d(\mathfrak{P}_i/\mathfrak{p}) \leq \upsilon_{\mathfrak{P}_i}(\varphi'(y)).$$

Proof.

Recall that

$$\varphi(T) = (T - y)(c_0 + c_1 T + \cdots + c_{n-2} T^{n-2} + c_{n-1} T^{n-1}) \in \mathcal{O}_{\mathfrak{p}}[T]$$

and $c_i \in \mathrm{F}$. However, we claim that $c_i \in \mathcal{O}_{\mathfrak{p}}[y]$. Indeed, $c_{n-1} = 1$, and looking at the coefficient of T^{n-1} in $\varphi(T)$,

$$c_{n-2} - y c_{n-1} = c_{n-2} - y \in \mathcal{O}_{\mathfrak{p}} \quad \Longrightarrow \quad c_{n-2} \in y + \mathcal{O}_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}[y].$$

Similarly by looking at the coefficient of T^{n-2},

$$c_{n-3} - y c_{n-2} \in \mathcal{O}_{\mathfrak{p}} \quad \Longrightarrow \quad c_{n-3} \in \mathcal{O}_{\mathfrak{p}}[y].$$

The proof follows by a backwards induction using

$$c_{n-i} - y c_{n-i+1} \in \mathcal{O}_{\mathfrak{p}}.$$

A bound on the different exponent

Proof.

So far we showed that

$$c_i \in \mathcal{O}_{\mathfrak{p}}[y] \qquad \forall i = 0, 1, \ldots, n-1.$$

A similar proof can be used to establish that

$$1, y, \ldots, y^{n-1} \in \sum_{j=0}^{n-1} c_j \mathcal{O}_{\mathfrak{p}}.$$

With these observations in mind we go ahead and prove the theorem, namely,

$$\forall i \in [r] \quad d(\mathfrak{P}_i/\mathfrak{p}) \leq \upsilon_{\mathfrak{P}_i}(\varphi'(y)).$$

Equivalently, we need to show that for all $i \in [r]$,

$$\forall z \in \mathrm{C}_{\mathfrak{p}} \quad \upsilon_{\mathfrak{P}_i}(z) \geq -\upsilon_{\mathfrak{P}_i}(\varphi'(y)).$$

A bound on the different exponent

Proof.

We ought to show that for all $i \in [r]$,

$$\forall z \in \mathsf{C}_{\mathfrak{p}} \quad \upsilon_{\mathfrak{P}_i}(z) \geq -\upsilon_{\mathfrak{P}_i}(\varphi'(y)).$$

By Lemma 3, $\{\frac{c_i}{\varphi'(y)} \mid i = 0, 1, \ldots, n-1\}$ is a basis of F/E, and so we can write

$$z = \sum_{i=0}^{n-1} r_i \frac{c_i}{\varphi'(y)} \qquad r_0, \ldots, r_{n-1} \in \mathsf{E}.$$

As $z \in \mathsf{C}_{\mathfrak{p}}$ and $y^{\ell} \in \mathcal{O}'_{\mathfrak{p}}$, we have by Lemma 3,

$$\mathcal{O}_{\mathfrak{p}} \ni \mathrm{Tr}_{\mathsf{F}/\mathsf{E}}(y^{\ell} z) = \sum_{i=0}^{n-1} r_i \mathrm{Tr}_{\mathsf{F}/\mathsf{E}}\left(\frac{c_i}{\varphi'(y)} y^{\ell}\right) = r_{\ell}.$$

A bound on the different exponent

Proof.

So far we wrote

$$z = \sum_{i=0}^{n-1} r_i \frac{c_i}{\varphi'(y)} \qquad r_0, \ldots, r_{n-1} \in \mathcal{O}_{\mathfrak{p}}.$$

By the above observations we have $c_i \in \mathcal{O}_{\mathfrak{p}}[y]$, and so

$$z \in \frac{1}{\varphi'(y)} \mathcal{O}_{\mathfrak{p}}[y] \subseteq \frac{1}{\varphi'(y)} \mathcal{O}'_{\mathfrak{p}}.$$

Hence, for every $\mathfrak{P}_i/\mathfrak{p}$,

$$v_{\mathfrak{P}_i}(z) \geq v_{\mathfrak{P}_i}\left(\frac{1}{\varphi'(y)}\right) = -v_{\mathfrak{P}_i}(\varphi'(y)),$$

as required. □

Overview

The different exponent and local bases

Theorem 5

Let F/L *be a finite separable extension of* E/K *s.t.*

$$\mathsf{F} = \mathsf{E}(y) \qquad y \in \mathsf{F}.$$

Let $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *be s.t.* $y \in \mathcal{O}'_{\mathfrak{p}}$*.*

Let $\varphi(T) \in \mathcal{O}_{\mathfrak{p}}[T]$ *be the minimal polynomial of* y *over* E*.*

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(\mathsf{F})$ *be the prime divisors lying over* $\mathfrak{p}$*. Then,*

$$\mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[y] \quad \Longleftrightarrow \quad \forall i \in [r] \quad d(\mathfrak{P}_i/\mathfrak{p}) = \upsilon_{\mathfrak{P}_i}(\varphi'(y)).$$

Recall that

$$y \in \mathcal{O}'_{\mathfrak{p}} \quad \Longrightarrow \quad \mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathcal{O}'_{\mathfrak{p}}.$$

Moreover, $\mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[y]$ iff $1, y, y^2, \ldots, y^{n-1}$ is a local integral basis for $\mathfrak{p}$.

The different exponent and local bases

Proof. (addendum)

By the observations made in the proof of Theorem 4, we have that

$$\sum_{i=0}^{n-1} \mathcal{O}_{\mathfrak{p}} y^i = \sum_{i=0}^{n-1} \mathcal{O}_{\mathfrak{p}} c_i.$$

For the first direction, assume $\mathcal{O}_{\mathfrak{p}}[y] = \mathcal{O}'_{\mathfrak{p}}$. Then, by Lemma 2 and Lemma 3,

$$\mathrm{C}_{\mathfrak{p}} = \sum_{i=0}^{n-1} \mathcal{O}_{\mathfrak{p}} \frac{c_i}{\varphi'(y)}.$$

Thus,

$$\mathrm{C}_{\mathfrak{p}} = \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_{\mathfrak{p}} c_i = \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_{\mathfrak{p}} y^i$$
$$= \frac{1}{\varphi'(y)} \mathcal{O}_{\mathfrak{p}}[y] = \frac{1}{\varphi'(y)} \mathcal{O}'_{\mathfrak{p}}.$$

The different exponent and local bases

Proof.

So, under the assumption that $\mathcal{O}_\mathfrak{p}[y] = \mathcal{O}'_\mathfrak{p}$ we conclude that

$$\mathrm{C}_\mathfrak{p} = \frac{1}{\varphi'(y)}\mathcal{O}'_\mathfrak{p}.$$

Hence, by the definition of the different exponent,

$$d(\mathfrak{P}_i/\mathfrak{p}) = \upsilon_{\mathfrak{P}_i}(\varphi'(y)).$$

The different exponent and local bases

Proof.

As for the other direction, we need to prove that

$$\forall i \in [r] \quad d(\mathfrak{P}_i/\mathfrak{p}) = \upsilon_{\mathfrak{P}_i}(\varphi'(y)) \quad \Longrightarrow \quad \mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[y].$$

The non-trivial inclusion is $\mathcal{O}'_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}}[y]$.

Take $z \in \mathcal{O}'_{\mathfrak{p}}$ and expand it as

$$z = \sum_{i=0}^{n-1} t_i y^i \qquad t_i \in \mathsf{E}.$$

By the observations we made, $c_j \in \mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathcal{O}'_{\mathfrak{p}}$. Further, per our assumption in this direction,

$$\mathsf{C}_{\mathfrak{p}} = \frac{1}{\varphi'(y)} \mathcal{O}'_{\mathfrak{p}}.$$

The different exponent and local bases

Proof.

Thus,

$$\mathrm{Tr}_{F/E}\left(\frac{1}{\varphi'(y)} \cdot c_j z\right) \in \mathcal{O}_{\mathfrak{p}}.$$

But

$$\begin{aligned}\mathrm{Tr}_{F/E}\left(\frac{1}{\varphi'(y)} c_j \cdot z\right) &= \mathrm{Tr}_{F/E}\left(\sum_{i=0}^{n-1} t_i y^i \frac{c_j}{\varphi'(y)}\right) \\ &= \sum_{i=0}^{n-1} t_i \mathrm{Tr}_{F/E}\left(y^i \frac{c_j}{\varphi'(y)}\right) = t_j\end{aligned}$$

Thus, $t_j \in \mathcal{O}_{\mathfrak{p}}$ and

$$z = \sum_{i=0}^{n-1} t_i y^i \in \mathcal{O}_{\mathfrak{p}}[y].$$

□

A useful corollary

Corollary 6 (addendum)

Let F/L *be a finite separable extension of* E/K *s.t.*

$$\mathsf{F} = \mathsf{E}(y) \qquad y \in \mathsf{F}.$$

Let $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *be s.t.* $y \in \mathcal{O}'_{\mathfrak{p}}$.

Let $\varphi(T) \in \mathcal{O}_{\mathfrak{p}}[T]$ *be the minimal polynomial of* y *over* E.

Assume that

$$\forall \mathfrak{P}/\mathfrak{p} \qquad v_{\mathfrak{P}}(\varphi'(y)) = 0.$$

Then, $\mathfrak{p}$ *is unramified in* F/E *and* $\mathcal{O}_{\mathfrak{p}}[y] = \mathcal{O}'_{\mathfrak{p}}$.

A useful corollary

Proof.

By Theorem 4, and per our assumption, for every $\mathfrak{P}/\mathfrak{p}$,

$$0 \leq d(\mathfrak{P}/\mathfrak{p}) \leq \upsilon_{\mathfrak{P}}(\varphi'(y)) = 0.$$

Thus,

$$\forall \mathfrak{P}/\mathfrak{p} \qquad \upsilon_{\mathfrak{P}}(\varphi'(y)) = d(\mathfrak{P}/\mathfrak{p}) = 0.$$

Therefore, by Theorem 5, $\mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[y]$.

To conclude the proof recall that as $d(\mathfrak{P}/\mathfrak{p}) = 0$, Dedekind's Theorem implies that $e(\mathfrak{P}/\mathfrak{p}) = 1$. □

Overview

The different exponent and total ramification

The following result will be useful when we discuss Artin-Schreier extensions - extensions in which $[\mathrm{F} : \mathrm{E}] = \operatorname{char} \mathrm{K}$.

Proposition 7 (addendum)

Let F/L be a degree n separable extension of E/K. Let $\mathfrak{p} \in \mathbb{P}(\mathrm{E})$ and $\mathfrak{P} \in \mathbb{P}(\mathrm{F})$ lying over $\mathfrak{p}$ s.t. $\mathfrak{P}/\mathfrak{p}$ is totally ramified (namely, $e(\mathfrak{P}/\mathfrak{p}) = n$).

Let $t \in \mathrm{F}$ be a $\mathfrak{P}$-prime element (namely, $v_{\mathfrak{P}}(t) = 1$) and consider the minimal polynomial $\varphi(T) \in \mathrm{E}[T]$ of t over E. Then,

1. $d(\mathfrak{P}/\mathfrak{p}) = v_{\mathfrak{P}}(\varphi'(t))$; and
2. $\mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[t]$.

The different exponent and total ramification

Proof.

We start by showing that $1, t, \ldots, t^{n-1}$ are linearly independent over E. Otherwise,

$$\sum_{i=0}^{n-1} r_i t^i = 0$$

with $r_i \in$ E not all zero.

For every i for which $r_i \neq 0$ we have that

$$\begin{aligned} \upsilon_{\mathfrak{P}}(r_i t^i) &= \upsilon_{\mathfrak{P}}(t^i) + e(\mathfrak{P}/\mathfrak{p}) \cdot \upsilon_{\mathfrak{p}}(r_i) \\ &= i + n \cdot \upsilon_{\mathfrak{p}}(r_i), \end{aligned}$$

and so

$$\upsilon_{\mathfrak{P}}(r_i t^i) \equiv i \mod n.$$

Therefore, $\upsilon_{\mathfrak{P}}(r_i t^i) \neq \upsilon_{\mathfrak{P}}(r_j t^j)$ for $i \neq j$ s.t. $r_i, r_j \neq 0$.

The different exponent and total ramification

Proof.

We start by showing that $1, t, \ldots, t^{n-1}$ are linearly independent over E. Otherwise,

$$\sum_{i=0}^{n-1} r_i t^i = 0.$$

We have shown that $\upsilon_{\mathfrak{P}}(r_i t^i) \neq \upsilon_{\mathfrak{P}}(r_j t^j)$ for $i \neq j$ s.t. $r_i, r_j \neq 0$.

By the strict triangle inequality we conclude that

$$\upsilon_{\mathfrak{P}}\left(\sum_{i=0}^{n-1} r_i t^i\right) = \min\{v_{\mathfrak{P}}(r_i t^i) \mid i \text{ s.t. } r_i \neq 0\}$$

which is finite, contradicting $\upsilon_{\mathfrak{P}}(0) = \infty$.

Thus, $\{1, t, t^2, \ldots, t^{n-1}\}$ is a basis of F over E.

The different exponent and total ramification

Proof.

By the fundamental equality, $\mathfrak{P}$ is the only prime divisor lying over $\mathfrak{p}$. Hence, $\mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{P}}$. Thus, to prove Item 2, we need to show that

$$\mathcal{O}_{\mathfrak{P}} = \sum_{i=0}^{n-1} \mathcal{O}_{\mathfrak{p}} t^i.$$

The only non-trivial inclusion is $\subseteq$. So, take $z \in \mathcal{O}_{\mathfrak{P}}$ and expand

$$z = \sum_{i=0}^{n-1} x_i t^i \qquad x_i \in \mathrm{E}.$$

Now, for $x_i \neq 0$,

$$v_{\mathfrak{P}}(x_i t^i) = v_{\mathfrak{P}}(x_i) + i = n \cdot v_{\mathfrak{p}}(x_i) + i,$$

and so $v_{\mathfrak{P}}(x_i t^i) \neq v_{\mathfrak{P}}(x_j t^j)$ for $i \neq j$ (and $x_i, x_j \neq 0$)

The different exponent and total ramification

Proof.

Recall

$$z = \sum_{i=0}^{n-1} x_i t^i \qquad x_i \in \mathrm{E},$$

and that

$$\upsilon_{\mathfrak{P}}(x_i t^i) = n \cdot \upsilon_{\mathfrak{p}}(x_i) + i.$$

In particular, $\upsilon_{\mathfrak{P}}(x_i t^i) \neq \upsilon_{\mathfrak{P}}(x_j t^j)$ for $i \neq j$ (and $x_i, x_j \neq 0$).

Thus, as $z \in \mathcal{O}_{\mathfrak{P}}$, and using the strict triangle inequality,

$$0 \leq \upsilon_{\mathfrak{P}}(z) = \min\{n \cdot \upsilon_{\mathfrak{p}}(x_i) + i \mid i \text{ s.t. } x_i \neq 0\}.$$

Therefore, $\upsilon_{\mathfrak{p}}(x_i) \geq 0$ for all i and so,

$$z \in \sum_{i=0}^{n-1} \mathcal{O}_{\mathfrak{p}} t^i.$$

Item 1 follows by Theorem 5. □