

More On The Different

Unit 24

Gil Cohen

May 10, 2022

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 1

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

$$F = E(y) \quad y \in F.$$

Let $\varphi(T) \in E[T]$ 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 $c_i \in F$. Then, the dual basis of $1, y, y^2, \dots, y^{n-1}$ is given by

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

A lemma about the dual basis

Proof.

We need to show that

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

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

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

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

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 $0 \leq \ell \leq n - 1$ 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 $1 \leq \nu \leq n$,

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

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

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

A lemma about the dual basis

Proof.

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

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

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

A lemma about the dual basis

Proof.

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

Comparing coefficients we get that

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

as required. □

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 bound on the different exponent

Theorem 2

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

$$F = E(y) \quad y \in F.$$

Let $\mathfrak{p} \in \mathbb{P}(E)$ be s.t. y is integral over $\mathcal{O}_{\mathfrak{p}}$.

Recall that the minimal polynomial of y over E , $\varphi(T) \in E[T]$, is in fact in $\mathcal{O}_{\mathfrak{p}}[T]$.

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

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

A bound on the different exponent

Proof.

Recall that

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

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

$$c_{n-2} - y c_{n-1} = c_{n-2} - y \in \mathcal{O}_p \quad \implies \quad c_{n-2} \in y + \mathcal{O}_p \in \mathcal{O}_p[y].$$

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

$$c_{n-3} - y c_{n-2} \in \mathcal{O}_p \quad \implies \quad c_{n-3} \in \mathcal{O}_p[y].$$

The proof follows by a backwards induction using

$$c_{n-i} - y c_{n-i+1} \in \mathcal{O}_p.$$

A bound on the different exponent

Proof.

So far we showed that

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

A similar proof can be used to establish that

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

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

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

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

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

A bound on the different exponent

Proof.

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

$$\forall z \in C_p \quad v_{\mathfrak{p}_i}(z) \geq -v_{\mathfrak{p}_i}(\varphi'(y)).$$

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

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

As $z \in C_p$ and $y^\ell \in \mathcal{O}'_p$, we have by Lemma 1,

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

A bound on the different exponent

Proof.

So far we wrote

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

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

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

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

- 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

Theorem 3

Under the same conditions as Theorem 2 ($F = E(y)$, $y \in \mathcal{O}'_{\mathfrak{p}}$),

$$\begin{aligned}\forall i \in [r] \quad d(\mathfrak{P}_i/\mathfrak{p}) &= v_{\mathfrak{P}_i}(\varphi'(y)) \\ &\Downarrow \\ \mathcal{O}'_{\mathfrak{p}} &= \mathcal{O}_{\mathfrak{p}}[y].\end{aligned}$$

(namely, $\{1, y, \dots, y^{n-1}\}$ is a local integral basis for \mathfrak{p}).

The different exponent and local bases

Proof.

By the observations made in the proof of Theorem 2, we have that

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

For the first direction, assume $\mathcal{O}_p[y] = \mathcal{O}'_p$. Then, by a theorem we proved on complementary modules and dual bases, and using Lemma 1,

$$C_p = \sum_{i=0}^{n-1} \mathcal{O}_p \frac{c_i}{\varphi'(y)}.$$

Thus,

$$\begin{aligned} C_p &= \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_p c_i = \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_p y^i \\ &= \frac{1}{\varphi'(y)} \mathcal{O}_p[y] = \frac{1}{\varphi'(y)} \mathcal{O}'_p. \end{aligned}$$



The different exponent and local bases

Proof.

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

$$C_p = \frac{1}{\varphi'(y)} \mathcal{O}'_p.$$

This, by definition, yields that

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

Indeed, recall that

$$z \in C_p \iff \forall \mathfrak{P}/\mathfrak{p} \quad v_{\mathfrak{P}}(z) \geq -d(\mathfrak{P}/\mathfrak{p}),$$

and

$$z \in \frac{1}{\varphi'(y)} \mathcal{O}'_p \iff \forall \mathfrak{P}/\mathfrak{p} \quad v_{\mathfrak{P}}(z) \geq -v_{\mathfrak{P}}(\varphi'(y)).$$

The different exponent and local bases

Proof.

As for the other direction, we need to prove that the condition

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

implies $\mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[y]$. The only non-trivial direction that needs to be proven is $\mathcal{O}'_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}}[y]$.

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

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

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

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

The different exponent and local bases

Proof.

Thus,

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

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 4

Under the same conditions as Theorem 2 ($F = E(y)$, $y \in \mathcal{O}'_{\mathfrak{p}}$), assume that

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

Then, \mathfrak{p} is unramified in F/E and $\{1, y, \dots, y^{n-1}\}$ is a local integral basis for \mathfrak{p} .

Proof.

By Theorem 2, and per our assumption,

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

In particular, $v_{\mathfrak{P}}(\varphi'(y)) = d(\mathfrak{P}/\mathfrak{p}) = 0$ for every $\mathfrak{P}/\mathfrak{p}$ and so, by Theorem 3, $\mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[y]$.

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

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**

The different exponent and total ramification

Proposition 5

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

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

- 1 $d(\mathfrak{P}/\mathfrak{p}) = v_{\mathfrak{P}}(\varphi'(t))$; and
- 2 $\{1, t, t^2, \dots, t^{n-1}\}$ is a local integral basis for \mathfrak{p} .

The different exponent and total ramification

Proof.

We start by showing that $1, t, \dots, t^{n-1}$ 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

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

and so

$$v_{\mathfrak{P}}(r_i t^i) \equiv i \pmod{n}.$$

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

The different exponent and total ramification

Proof.

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

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

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

By the strict triangle inequality we conclude that

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

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

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

The different exponent and total ramification

Proof.

By the fundamental equality it follows that \mathfrak{P} is the only place lying over \mathfrak{p} . Hence, $\mathcal{O}'_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{P}}$. Thus, 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

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

Now, for $x_i \neq 0$,

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

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

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

and that

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

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

Thus, as $z \in \mathcal{O}_{\mathfrak{P}}$,

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

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

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

