Kummer's Theorem

Unit 23

Gil Cohen

May 23, 2022

Overview

1. Kummer's Theorem I
2. Kummer's Theorem II
3. Kummer's Theorem III

Kummer's Theorem

Throughout this unit we consider finite separable extensions F/L of E/K.

The goal in this unit is to find all prime divisors in $\mathbb{P}(F)$ lying over a given $\mathfrak{p} \in \mathbb{P}(E)$.

To this end, we will take $y \in \mathcal{O}'_{\mathfrak{p}}$ s.t. $F = E(y)$.

Recall that the minimal polynomial

$$\varphi(T) = \sum c_i T^i \in E[T]$$

of such y over E is in fact in $\mathcal{O}_{\mathfrak{p}}[T]$.

In what follows, we denote by $\bar{\varphi}(T) \in E_{\mathfrak{p}}[T]$ the projection of $\varphi(T)$ to $E_{\mathfrak{p}}[T]$ (where, recall, $E_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$), namely,

$$\bar{\varphi}(T) = \sum (c_i + \mathfrak{m}_{\mathfrak{p}}) T^i = \sum c_i(\mathfrak{p}) T^i = \sum \bar{c}_i T^i.$$

Kummer's Theorem

Theorem 1 (Kummer's Theorem I)

Let F/L *be a finite separable extension of* E/K*, and let* $y \in \mathsf{F}$ *be s.t.* $\mathsf{F} = \mathsf{E}(y)$*. 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*. Factor*

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i} \in \mathsf{E}_{\mathfrak{p}}[T]$$

where $\gamma_i(T) \in \mathsf{E}_{\mathfrak{p}}[T]$ *are irreducible and distinct (and* $\varepsilon_i \geq 1$*).*

Let $\varphi_i(T) \in \mathcal{O}_{\mathfrak{p}}[T]$ *be s.t.* $\bar{\varphi}_i(T) = \gamma_i(T)$ *and* $\deg \varphi_i = \deg \gamma_i$*.*

Then, $\exists \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(\mathsf{F})$ *lying over* $\mathfrak{p}$ *s.t.*

1. $\forall i \in [r] \quad \varphi_i(y) \in \mathfrak{m}_{\mathfrak{P}_i}$ *(equivalently,* $(\varphi_i(y))(\mathfrak{P}_i) = 0$*).*
2. $f(\mathfrak{P}_i/\mathfrak{p}) \geq \deg \gamma_i(T)$*.*
3. *The prime divisors* $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ *are distinct.*

Kummer's Theorem

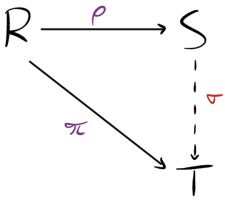
In the proof we make use of the following simple claim.

Claim 2

Let R, S, T rings. In the notation of the diagram below, assuming ρ is onto and that

$$\ker \rho \subseteq \ker \pi \qquad (\iff \quad \rho(r_1) = \rho(r_2) \implies \pi(r_1) = \pi(r_2)).$$

Then, there exists a unique homomorphism $\sigma : S \to T$ s.t the diagram commutes.



Kummer's Theorem

Proof. (Proof of Theorem 1)

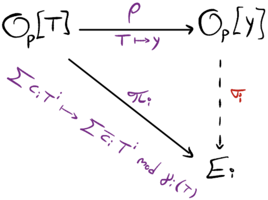
Denote

$$\mathsf{E}_i = \mathsf{E}_{\mathfrak{p}}[T]/\langle \gamma_i(T) \rangle.$$

As $\gamma_i(T)$ is irreducible over $\mathsf{E}_{\mathfrak{p}}$ we have that E_i is a field extension of $\mathsf{E}_{\mathfrak{p}}$ of degree $[\mathsf{E}_i : \mathsf{E}_{\mathfrak{p}}] = \deg \gamma_i$.

Denote $n = [\mathsf{F} : \mathsf{E}] = [\mathsf{E}(y) : \mathsf{E}]$ and consider the ring homomorphisms in the diagram, where

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



Kummer's Theorem

Proof.

Observe that

$$\ker \rho = \varphi(T)\mathcal{O}_{\mathfrak{p}}[T] = \langle \varphi(T) \rangle.$$

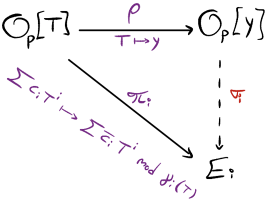
Moreover,

$$\pi_i(\varphi(T)) = \bar{\varphi}(T) \bmod \gamma_i(T) = 0.$$

Thus,

$$\ker \rho \subseteq \ker \pi_i,$$

and so by Claim 2 there exists a unique homomorphism σ_i for which the diagram below commutes.



Kummer's Theorem

Proof.

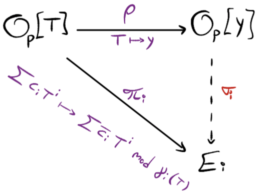
σ_i takes the explicit form

$$\sigma_i\left(\sum_{j=0}^{n-1} c_j y^j\right) = \sum_{j=0}^{n-1} \bar{c}_j T^j \mod \gamma_i(T).$$

π_i is onto and thus so is σ_i. We claim that

$$\ker \sigma_i = \mathfrak{m}_\mathfrak{p}\mathcal{O}_\mathfrak{p}[y] + \varphi_i(y)\mathcal{O}_\mathfrak{p}[y].$$

The inclusion $\supseteq$ is trivial. We turn to show the other direction.



Kummer's Theorem

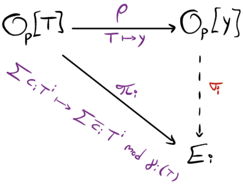
Proof.

Take $\sum_{j=0}^{n-1} c_j y^j \in \ker \sigma_i$. Then, (recall $\gamma_i(T) = \bar{\varphi}_i(T)$)

$$\sum_{j=0}^{n-1} \bar{c}_j T^j = \bar{\varphi}_i(T)\bar{\psi}(T)$$

for some $\psi(T) \in \mathcal{O}_{\mathfrak{p}}[T]$. Thus,

$$\sum_{j=0}^{n-1} c_j T^j - \varphi_i(T)\psi(T) \in \mathfrak{m}_{\mathfrak{p}} \cdot \mathcal{O}_{\mathfrak{p}}[T].$$



Kummer's Theorem

Proof.

Recall

$$\sum_{j=0}^{n-1} c_j T^j - \varphi_i(T)\psi(T) \in \mathfrak{m}_\mathfrak{p} \cdot \mathcal{O}_\mathfrak{p}[T],$$

and so

$$\sum_{j=0}^{n-1} c_j y^j - \varphi_i(y)\psi(y) \in \mathfrak{m}_\mathfrak{p} \cdot \mathcal{O}_\mathfrak{p}[y].$$

Hence,

$$\sum_{j=0}^{n-1} c_j y^j \in \varphi_i(y) \cdot \mathcal{O}_\mathfrak{p}[y] + \mathfrak{m}_\mathfrak{p} \cdot \mathcal{O}_\mathfrak{p}[y],$$

as desired. Namely,

$$\ker \sigma_i = \mathfrak{m}_\mathfrak{p}\mathcal{O}_\mathfrak{p}[y] + \varphi_i(y)\mathcal{O}_\mathfrak{p}[y].$$

Kummer's Theorem

For the proof of Theorem 1, we recall the following lemma.

Lemma 3

Let F/K *be a function field and let* R *be a subring of* F *with* $K \subseteq R \subseteq F$*. Suppose that* $\{0\} \neq I \subsetneq R$ *is a proper ideal of* R*. Then,*

$$\exists \mathfrak{p} \in \mathbb{P}(F) \quad \textit{s.t.} \quad I \subseteq \mathfrak{m}_{\mathfrak{p}} \quad \textit{and} \quad R \subseteq \mathcal{O}_{\mathfrak{p}}.$$

Proof. (Proof of Theorem 1 continued)

Going back to the proof, by Lemma 3,

$$\exists \mathfrak{P}_i \in \mathbb{P}(F) \quad \text{s.t.} \quad \ker \sigma_i \subseteq \mathfrak{m}_{\mathfrak{P}_i} \quad \text{and} \quad \mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathcal{O}_{\mathfrak{P}_i}.$$

Hence, $\mathfrak{P}_i$ lies over $\mathfrak{p}$ and $\varphi_i(y) \in \mathfrak{m}_{\mathfrak{P}_i}$.

This establishes Item 1.

Kummer's Theorem

Proof.

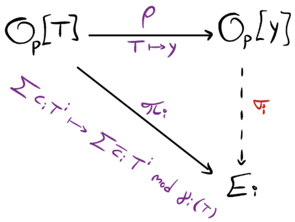
$$\exists \mathfrak{P}_i \in \mathbb{P}(F) \quad \text{s.t.} \quad \ker \sigma_i \subseteq \mathfrak{m}_{\mathfrak{P}_i} \quad \text{and} \quad \mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathcal{O}_{\mathfrak{P}_i}.$$

To prove Item 2, namely, $f(\mathfrak{P}_i/\mathfrak{p}) \geq \deg \gamma_i(T)$, observe that

$$E_i \cong \mathcal{O}_{\mathfrak{p}}[y] \big/ \ker \sigma_i \hookrightarrow \mathcal{O}_{\mathfrak{P}_i} \big/ \mathfrak{m}_{\mathfrak{P}_i} = F_{\mathfrak{P}_i}$$

and so

$$f(\mathfrak{P}_i/\mathfrak{p}) = [F_{\mathfrak{P}_i} : E_{\mathfrak{p}}] \geq [E_i : E_{\mathfrak{p}}] = \deg \gamma_i(T).$$



Kummer's Theorem

Proof.

To conclude the proof, we show that the $\mathfrak{P}_i$-s are distinct.

For $i \neq j$, $\gamma_i(T) = \bar{\varphi}_i(T)$ and $\gamma_j(T) = \bar{\varphi}_j(T)$ are relatively prime in $\mathrm{E}_{\mathfrak{p}}[T]$. Thus, $\exists\, \lambda_i(T), \lambda_j(T) \in \mathcal{O}_{\mathfrak{p}}[T]$ s.t.

$$1 = \bar{\varphi}_i(T)\bar{\lambda}_i(T) + \bar{\varphi}_j(T)\bar{\lambda}_j(T).$$

Thus,

$$\varphi_i(y)\lambda_i(y) + \varphi_j(y)\lambda_j(y) - 1 \in \mathfrak{m}_{\mathfrak{p}} \cdot \mathcal{O}_{\mathfrak{p}}[y].$$

Recall that

$$\ker \sigma_i = \mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y] + \varphi_i(y)\mathcal{O}_{\mathfrak{p}}[y],$$

and so

$$1 \in \ker \sigma_i + \ker \sigma_j \subseteq \mathfrak{m}_{\mathfrak{P}_i} + \mathfrak{m}_{\mathfrak{P}_j},$$

which implies that $\mathfrak{P}_i \neq \mathfrak{P}_j$. □

Overview

1. Kummer's Theorem I
2. Kummer's Theorem II
3. Kummer's Theorem III

Kummer's Theorem II

F/L a finite separable extension of E/K, $\mathrm{F} = \mathrm{E}(y)$, and $\mathfrak{p}$ s.t. $y \in \mathcal{O}'_{\mathfrak{p}}$.

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

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i} \in \mathrm{E}_{\mathfrak{p}}[T]$$

where $\gamma_i(T) \in \mathrm{E}_{\mathfrak{p}}[T]$ are irreducible and distinct (and $\varepsilon_i \geq 1$).

Let $\varphi_i(T) \in \mathcal{O}_{\mathfrak{p}}[T]$ be s.t. $\bar{\varphi}_i(T) = \gamma_i(T)$ and $\deg \varphi_i = \deg \gamma_i$.

Theorem 4 (Kummer's Theorem II)

Under the hypothesis of Theorem 1, if in addition $\varepsilon_1 = \cdots = \varepsilon_r = 1$ then,

1. *The prime divisors $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are all the prime divisors in F lying over $\mathfrak{p}$;*
2. $\forall i \in [r] \quad e(\mathfrak{P}_i/\mathfrak{p}) = 1$; *and*
3. $\forall i \in [r] \quad f(\mathfrak{P}_i/\mathfrak{p}) = \deg \gamma_i(T)$.

Kummer's Theorem II

Proof.

By the additional hypothesis,

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T).$$

Thus,

$$[\mathsf{F} : \mathsf{E}] = \deg \varphi = \sum_{i=1}^{r} \deg \varphi_i .$$

By Item 2 of Theorem 1, $f(\mathfrak{P}_i/\mathfrak{p}) \geq \deg \varphi_i$ and so

$$[\mathsf{F} : \mathsf{E}] \leq \sum_{i=1}^{r} f(\mathfrak{P}_i/\mathfrak{p}) \leq \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) = [\mathsf{F} : \mathsf{E}],$$

where we used the fundamental equality. The proof then follows. □

Overview

1 Kummer's Theorem I

2 Kummer's Theorem II

3 Kummer's Theorem III

Kummer's Theorem III

F/L a finite separable extension of E/K, $F = E(y)$, and $\mathfrak{p}$ s.t. $y \in \mathcal{O}'_{\mathfrak{p}}$.

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

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i} \in E_{\mathfrak{p}}[T]$$

where $\gamma_i(T) \in E_{\mathfrak{p}}[T]$ are irreducible and distinct (and $\varepsilon_i \geq 1$).

Let $\varphi_i(T) \in \mathcal{O}_{\mathfrak{p}}[T]$ be s.t. $\bar{\varphi}_i(T) = \gamma_i(T)$ and $\deg \varphi_i = \deg \gamma_i$.

Theorem 5 (Kummer's Theorem III)

Under the hypothesis of Theorem 1, if in addition $1, y, y^2, \dots, y^{n-1}$ is a local integral basis for $\mathfrak{p}$, where $n = [F : E]$, then

1. *The prime divisors $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ are all prime divisors in F lying over $\mathfrak{p}$;*
2. $\forall i \in [r] \quad e(\mathfrak{P}_i/\mathfrak{p}) = \varepsilon_i$; *and*
3. $\forall i \in [r] \quad f(\mathfrak{P}_i/\mathfrak{p}) = \deg \gamma_i(T)$.

Kummer's Theorem III

Proof.

We start with Item (1). We have that

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \bar{\varphi}_i(T)^{\varepsilon_i} \qquad \text{in } \mathrm{E}_{\mathfrak{p}}[T] = \left(\mathcal{O}_{\mathfrak{p}} \big/ \mathfrak{m}_{\mathfrak{p}}\right)[T].$$

Therefore,

$$\bar{\varphi}(y) = \prod_{i=1}^{r} \bar{\varphi}_i(y)^{\varepsilon_i} \qquad \text{in } \mathrm{E}_{\mathfrak{p}}[y] = \left(\mathcal{O}_{\mathfrak{p}} \big/ \mathfrak{m}_{\mathfrak{p}}\right)[y],$$

and so

$$0 = \varphi(y) = \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \qquad \mod \mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y].$$

Kummer's Theorem III

Proof.

So far

$$0 = \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \qquad \bmod \mathfrak{m}_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}[y].$$

Fix $\mathfrak{P}/\mathfrak{p}$. Since $y \in \mathcal{O}'_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{P}}$, we have that

$$\mathfrak{m}_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathfrak{m}_{\mathfrak{p}} \mathcal{O}_{\mathfrak{P}} \subseteq \mathfrak{m}_{\mathfrak{P}},$$

and so

$$\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \in \mathfrak{m}_{\mathfrak{P}}.$$

$\mathfrak{m}_{\mathfrak{P}}$ is a prime (in fact, maximal) ideal of $\mathcal{O}_{\mathfrak{P}}$ and so $\exists i \in [r]$ s.t. $\varphi_i(y) \in \mathfrak{m}_{\mathfrak{P}}$. Thus,

$$\varphi_i(y) \mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathfrak{m}_{\mathfrak{P}} \cap \mathcal{O}_{\mathfrak{p}}[y].$$

Kummer's Theorem III

Proof.

$$\varphi_i(y)\mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathfrak{m}_{\mathfrak{P}} \cap \mathcal{O}_{\mathfrak{p}}[y].$$

As $y \in \mathcal{O}'_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{P}}$ one also has that

$$\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathfrak{m}_{\mathfrak{p}}\mathcal{O}'_{\mathfrak{p}} \subseteq \mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{P}} \subseteq \mathfrak{m}_{\mathfrak{P}},$$

and so

$$\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathfrak{m}_{\mathfrak{P}} \cap \mathcal{O}_{\mathfrak{p}}[y].$$

To summarize,

$$\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y] + \varphi_i(y)\mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathfrak{m}_{\mathfrak{P}} \cap \mathcal{O}_{\mathfrak{p}}[y].$$

Kummer's Theorem III

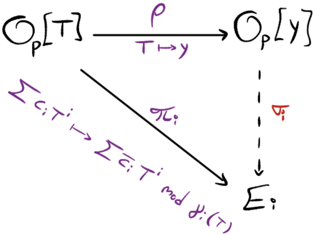
Proof.

$$\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y] + \varphi_i(y)\mathcal{O}_{\mathfrak{p}}[y] \subseteq \mathfrak{m}_{\mathfrak{P}} \cap \mathcal{O}_{\mathfrak{p}}[y].$$

In the proof of Theorem 1 we showed that the LHS is $\ker \sigma_i$ where the image of σ_i is the field E_i. Thus, the LHS is a maximal ideal of $\mathcal{O}_{\mathfrak{p}}[y]$.

The RHS is clearly a non-trivial ideal of $\mathcal{O}_{\mathfrak{p}}[y]$ and so we have

$$\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y] + \varphi_i(y)\mathcal{O}_{\mathfrak{p}}[y] = \mathfrak{m}_{\mathfrak{P}} \cap \mathcal{O}_{\mathfrak{p}}[y]. \tag{1}$$



Kummer's Theorem III

Proof.

$$\mathfrak{m}_\mathfrak{p}\mathcal{O}_\mathfrak{p}[y] + \varphi_i(y)\mathcal{O}_\mathfrak{p}[y] = \mathfrak{m}_\mathfrak{P} \cap \mathcal{O}_\mathfrak{p}[y].$$

However, as $\varphi_i(y) \in \mathfrak{m}_{\mathfrak{P}_i}$ (Theorem 1, Item (1)) we also have, by the same reasoning, that

$$\mathfrak{m}_\mathfrak{p}\mathcal{O}_\mathfrak{p}[y] + \varphi_i(y)\mathcal{O}_\mathfrak{p}[y] = \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}_\mathfrak{p}[y].$$

Thus,

$$\mathfrak{m}_\mathfrak{P} \cap \mathcal{O}_\mathfrak{p}[y] = \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}_\mathfrak{p}[y].$$

Now, per our hypothesis $\mathcal{O}_\mathfrak{p}[y] = \mathcal{O}'_\mathfrak{p}$, we have that

$$\mathfrak{m}_\mathfrak{P} \cap \mathcal{O}'_\mathfrak{p} = \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}'_\mathfrak{p}.$$

As we now explain, unless $\mathfrak{P} = \mathfrak{P}_i$ this contradicts the WAT. This will establish Item 1.

Kummer's Theorem III

Proof.

For $\mathfrak{P} \neq \mathfrak{P}_i$, $\mathfrak{m}_{\mathfrak{P}} \cap \mathcal{O}'_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}'_{\mathfrak{p}}$ contradicts the WAT.

To see this, for simplicity, say $\mathfrak{p}$ has three prime divisors lying above it $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$. Then,

$$\begin{aligned}\mathfrak{m}_{\mathfrak{P}_1} \cap \mathcal{O}'_{\mathfrak{p}} &= \mathfrak{m}_{\mathfrak{P}_1} \cap (\mathcal{O}_{\mathfrak{P}_1} \cap \mathcal{O}_{\mathfrak{P}_2} \cap \mathcal{O}_{\mathfrak{P}_3}) \\ &= (\mathfrak{m}_{\mathfrak{P}_1} \cap \mathcal{O}_{\mathfrak{P}_1}) \cap (\mathcal{O}_{\mathfrak{P}_2} \cap \mathcal{O}_{\mathfrak{P}_3}) \\ &= \mathfrak{m}_{\mathfrak{P}_1} \cap (\mathcal{O}_{\mathfrak{P}_2} \cap \mathcal{O}_{\mathfrak{P}_3}) .\end{aligned}$$

Similarly,

$$\mathfrak{m}_{\mathfrak{P}_2} \cap \mathcal{O}'_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{P}_2} \cap (\mathcal{O}_{\mathfrak{P}_1} \cap \mathcal{O}_{\mathfrak{P}_3}) ,$$

and so

$$\mathfrak{m}_{\mathfrak{P}_1} \cap (\mathcal{O}_{\mathfrak{P}_2} \cap \mathcal{O}_{\mathfrak{P}_3}) = \mathfrak{m}_{\mathfrak{P}_2} \cap (\mathcal{O}_{\mathfrak{P}_1} \cap \mathcal{O}_{\mathfrak{P}_3}) .$$

Kummer's Theorem III

Proof.

$$\mathfrak{m}_{\mathfrak{P}_1} \cap (\mathcal{O}_{\mathfrak{P}_2} \cap \mathcal{O}_{\mathfrak{P}_3}) = \mathfrak{m}_{\mathfrak{P}_2} \cap (\mathcal{O}_{\mathfrak{P}_1} \cap \mathcal{O}_{\mathfrak{P}_3}).$$

In particular, we have that

$$\mathfrak{m}_{\mathfrak{P}_1} \cap (\mathcal{O}_{\mathfrak{P}_2} \cap \mathcal{O}_{\mathfrak{P}_3}) \subseteq \mathfrak{m}_{\mathfrak{P}_2}.$$

Thus,

$$\upsilon_{\mathfrak{P}_1}(x) > 0 \ \ \& \ \ \upsilon_{\mathfrak{P}_2}(x) \geq 0 \ \ \& \ \ \upsilon_{\mathfrak{P}_3}(x) \geq 0 \quad \Longrightarrow \quad \upsilon_{\mathfrak{P}_2}(x) > 0.$$

This contradicts the WAT that guarantees the existence of an element x with

$$\upsilon_{\mathfrak{P}_1}(x) > 0 \ \ \& \ \ \upsilon_{\mathfrak{P}_2}(x) = 0 \ \ \& \ \ \upsilon_{\mathfrak{P}_3}(x) = 0.$$

This proves Item 1.

Kummer's Theorem III

Proof.

We turn to prove Items 2,3, namely,

$$\forall i \in [r] \quad e(\mathfrak{P}_i/\mathfrak{p}) = \varepsilon_i \text{ and } f(\mathfrak{P}_i/\mathfrak{p}) = \deg \gamma_i(T).$$

Item 1, and our hypothesis imply

$$\mathcal{O}_{\mathfrak{p}}[y] = \mathcal{O}'_{\mathfrak{p}} = \bigcap_{i=1}^{r} \mathcal{O}_{\mathfrak{P}_i}.$$

Using the WAT we can find elements $t_1, \ldots, t_r \in \mathrm{F}$ s.t.

$$\upsilon_{\mathfrak{P}_i}(t_j) = \delta_{i,j}.$$

Let $t \in \mathrm{E}$ be s.t. $\upsilon_{\mathfrak{p}}(t) = 1$.

In the proof of Item 1 (Equation (1)) we proved that

$$\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y] + \varphi_i(y)\mathcal{O}_{\mathfrak{p}}[y] = \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}_{\mathfrak{p}}[y].$$

Kummer's Theorem III

Proof.

$$\mathfrak{m}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}[y] + \varphi_i(y)\mathcal{O}_{\mathfrak{p}}[y] = \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}_{\mathfrak{p}}[y].$$

and so, as $\mathfrak{m}_{\mathfrak{p}} = t\mathcal{O}_{\mathfrak{p}}$,

$$t_i \in \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}_{\mathfrak{p}}[y] = t\mathcal{O}_{\mathfrak{p}}[y] + \varphi_i(y)\mathcal{O}_{\mathfrak{p}}[y].$$

Thus, we can write

$$t_i = \varphi_i(y)a_i(y) + tb_i(y) \qquad a_i(y), b_i(y) \in \mathcal{O}_{\mathfrak{p}}[y].$$

Thus,

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = a(y)\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} + t \cdot b(y)$$

for some $a(y), b(y) \in \mathcal{O}_{\mathfrak{p}}[y]$. E.g.,

$$\begin{aligned} t_1 t_2 &= (\varphi_1 a_1 + tb_1)(\varphi_2 a_2 + tb_2) \\ &= a_1 a_2 \cdot \varphi_1\varphi_2 + t \cdot (\varphi_1 a_1 b_2 + b_1\varphi_2 a_2 + tb_1 b_2). \end{aligned}$$

Kummer's Theorem III

Proof.

So far

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = a(y) \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} + t \cdot b(y)$$

for some $a(y), b(y) \in \mathcal{O}_{\mathfrak{p}}[y]$. Now, as $t\mathcal{O}_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}$,

$$\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} = \varphi(y) \mod t \cdot \mathcal{O}_{\mathfrak{p}}[y].$$

Moreover $\varphi(y) = 0$, and so

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = t \cdot c(y)$$

for some $c(y) \in \mathcal{O}_{\mathfrak{p}}[y]$.

Kummer's Theorem III

Proof.

So far,

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = t \cdot c(y) \qquad c(y) \in \mathcal{O}_{\mathfrak{p}}[y].$$

Thus,

$$\varepsilon_i = v_{\mathfrak{P}_i}\left(\prod_{i=1}^{r} t_i^{\varepsilon_i}\right) = v_{\mathfrak{P}_i}(t) + v_{\mathfrak{P}_i}(c(y)) \geq v_{\mathfrak{P}_i}(t),$$

where the last inequality follows as $c(y) \in \mathcal{O}_{\mathfrak{p}}[y] = \mathcal{O}'_{\mathfrak{p}} = \cap_i \mathcal{O}_{\mathfrak{P}_i}$.

But

$$v_{\mathfrak{P}_i}(t) = e(\mathfrak{P}_i/\mathfrak{p}) \cdot v_{\mathfrak{p}}(t) = e(\mathfrak{P}_i/\mathfrak{p}),$$

and so we conclude that

$$\varepsilon_i \geq e(\mathfrak{P}_i/\mathfrak{p}).$$

Kummer's Theorem III

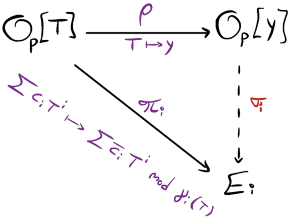
Proof.

Taking a detour, recall that in the proof of Theorem 1, to prove Item 2 we noted that

$$E_{\mathfrak{p}}[T] \Big/ \langle \gamma_i(T) \rangle \triangleq E_i \cong \mathcal{O}_{\mathfrak{p}}[y] \Big/ \ker \sigma_i \hookrightarrow \mathcal{O}_{\mathfrak{P}_i} \Big/ \mathfrak{m}_{\mathfrak{P}_i} = F_{\mathfrak{P}_i},$$

and so

$$f(\mathfrak{P}_i/\mathfrak{p}) = [F_{\mathfrak{P}_i} : E_{\mathfrak{p}}] \geq [E_i : E_{\mathfrak{p}}] = \deg \gamma_i(T).$$



Kummer's Theorem III

Proof.

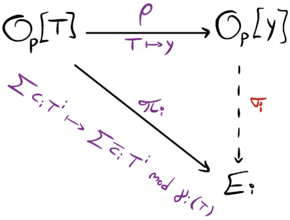
Returning to our proof, to recap, we showed that

$$\ker \sigma_i = \mathfrak{m}_\mathfrak{p} \mathcal{O}_\mathfrak{p}[y] + \varphi_i(y)\mathcal{O}_\mathfrak{p}[y] = \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}_\mathfrak{p}[y],$$

and we claim that this implies

$$f(\mathfrak{P}_i/\mathfrak{p}) = \deg \gamma_i(T)$$

establishing Item 3.



Kummer's Theorem III

Proof.

We have that $\ker \sigma_i = \mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}_{\mathfrak{p}}[y]$, and we wish to prove

$$f(\mathfrak{P}_i/\mathfrak{p}) = \deg \gamma_i(T).$$

Recall the second isomorphism theorem for commutative rings which states that

$$(\mathsf{S} + J)\Big/ J \cong \mathsf{S}\Big/ (\mathsf{S} \cap J)$$

for S a subring of R and J an ideal of R.

In our case ($\mathsf{R} = \mathcal{O}_{\mathfrak{P}_i}$),

$$\begin{aligned}(\mathcal{O}_{\mathfrak{p}}[y] + \mathfrak{m}_{\mathfrak{P}_i})\Big/ \mathfrak{m}_{\mathfrak{P}_i} &\cong \mathcal{O}_{\mathfrak{p}}[y]\Big/ (\mathfrak{m}_{\mathfrak{P}_i} \cap \mathcal{O}_{\mathfrak{p}}[y]) \\ &= \mathcal{O}_{\mathfrak{p}}[y]\Big/ \ker \sigma_i \\ &= \mathsf{E}_i \\ &= \mathsf{E}_{\mathfrak{p}}[T]\Big/ \langle \gamma_i(T) \rangle.\end{aligned}$$

Kummer's Theorem III

Proof.

We wish to prove

$$f(\mathfrak{P}_i/\mathfrak{p}) = \deg \gamma_i(T).$$

So far we proved that

$$(\mathcal{O}_\mathfrak{p}[y] + \mathfrak{m}_{\mathfrak{P}_i}) \Big/ \mathfrak{m}_{\mathfrak{P}_i} \cong \mathsf{E}_\mathfrak{p}[T] \Big/ \langle \gamma_i(T) \rangle.$$

The proof will follow by showing that

$$\mathcal{O}_\mathfrak{p}[y] + \mathfrak{m}_{\mathfrak{P}_i} = \mathcal{O}_{\mathfrak{P}_i}.$$

Indeed, recall that $\mathcal{O}_{\mathfrak{P}_i} \Big/ \mathfrak{m}_{\mathfrak{P}_i} = \mathsf{F}_{\mathfrak{P}_i}$ and that

$$f(\mathfrak{P}_i/\mathfrak{p}) = [\mathsf{F}_{\mathfrak{P}_i} : \mathsf{E}_\mathfrak{p}],$$
$$\deg \gamma_i(T) = [\mathsf{E}_\mathfrak{p}[T]/\langle \gamma_i(T) \rangle : \mathsf{E}_\mathfrak{p}].$$

Kummer's Theorem III

Proof.

We turn to prove that

$$\mathcal{O}_{\mathfrak{p}}[y] + \mathfrak{m}_{\mathfrak{P}_i} = \mathcal{O}_{\mathfrak{P}_i}.$$

The $\subseteq$ direction is trivial, so take $z \in \mathcal{O}_{\mathfrak{P}_i}$. Per our assumption,

$$\mathcal{O}_{\mathfrak{p}}[y] = \mathcal{O}'_{\mathfrak{p}} = \bigcap_{j=1}^{r} \mathcal{O}_{\mathfrak{P}_j}.$$

By the WAT, we can find $y \in$ F s.t.

$$\begin{aligned} &v_{\mathfrak{P}_i}(y - z) > 0, \\ &v_{\mathfrak{P}_j}(y) \geq 0 \qquad \forall j \neq i. \end{aligned}$$

Thus, $z = (z - y) + y$ with $z - y \in \mathfrak{m}_{\mathfrak{P}_i}$ and $y \in \mathcal{O}'_{\mathfrak{p}}$.

This establishes Item 3.

Kummer's Theorem III

Proof.

Going back to Item 2, using the fundamental equality and what we proved, namely,

$$e(\mathfrak{P}_i/\mathfrak{p}) \le \varepsilon_i \qquad \& \qquad f(\mathfrak{P}_i/\mathfrak{p}) = \deg \gamma_i(T)$$

we get that

$$\begin{aligned}[\mathrm{F} : \mathrm{E}] &= \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) \le \sum_{i=1}^{r} \varepsilon_i \deg \gamma_i(T) \\ &= \deg \gamma(T) = [\mathrm{F} : \mathrm{E}].\end{aligned}$$

Thus, $\varepsilon_i = e(\mathfrak{P}_i/\mathfrak{p})$ for all $i \in [r]$, completing the proof. □