# Algebraic Geometric Codes

Recitation 12

Shir Peleg

Tel Aviv University

May 24, 2022

# Technical lemma

**Lemma 1**

*Assume $F/E$ is separable. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of $F$ lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.*

# Technical lemma

**Lemma 1**

*Assume $F/E$ is separable. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of $F$ lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.*
*Let $F_{\mathfrak{P},s}$ be the separable closure of $E_{\mathfrak{p}}$ in $F_{\mathfrak{P}}$.*

# Technical lemma

**Lemma 1**

*Assume $F/E$ is separable. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of $F$ lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.*
*Let $F_{\mathfrak{P},s}$ be the separable closure of $E_{\mathfrak{p}}$ in $F_{\mathfrak{P}}$.*
*Let $y \in \mathcal{O}'_{\mathfrak{p}}$ be s.t.*

1. $v_{\mathfrak{P}_j}(y) > 0$ *for* $j = 2, \ldots, r$; *and*
2. $\pi(y) \in F_{\mathfrak{P},s}$.

# Technical lemma

## Lemma 1

*Assume $F/E$ is separable. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of $F$ lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.*
*Let $F_{\mathfrak{P},s}$ be the separable closure of $E_{\mathfrak{p}}$ in $F_{\mathfrak{P}}$.*
*Let $y \in \mathcal{O}'_{\mathfrak{p}}$ be s.t.*

1. $v_{\mathfrak{P}_j}(y) > 0$ *for* $j = 2, \ldots, r$; *and*
2. $\pi(y) \in F_{\mathfrak{P},s}$.

*Then,*

$$\pi\left(Tr_{F/E}(y)\right) = e(\mathfrak{P}/\mathfrak{p}) \cdot Tr_{F_{\mathfrak{P},s}/E_{\mathfrak{p}}}(\pi(y)).$$

# Technical lemma

**Lemma 2**

*Assume $F/E$ is Galois. Function field over a perfect field.*

# Technical lemma

**Lemma 2**

*Assume $F/E$ is Galois. Function field over a perfect field. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of $F$ lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$.*

# Technical lemma

**Lemma 2**

*Assume $F/E$ is Galois. Function field over a perfect field. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of $F$ lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$. Let $y \in \mathcal{O}'_{\mathfrak{p}}$ be s.t.*

1. $v_{\mathfrak{P}_j}(y) > 0$ *for* $j = 2, \ldots, r$; *and*

# Technical lemma

**Lemma 2**

*Assume $F/E$ is Galois. Function field over a perfect field. Let $\mathfrak{p} \in \mathbb{P}(E)$ and $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ be the prime divisors of $F$ lying over $\mathfrak{p}$. Let $\pi : \mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ be the corresponding projective map (that can be extended to a place) which extends the projection map $\pi : \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$. Let $y \in \mathcal{O}'_{\mathfrak{p}}$ be s.t.*

1. $v_{\mathfrak{P}_j}(y) > 0$ *for* $j = 2, \ldots, r$; *and*

*Then,*

$$\pi\left(Tr_{F/E}(y)\right) = e(\mathfrak{P}/\mathfrak{p}) \cdot Tr_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(\pi(y)).$$

# Proof of Lemma 2

**Proof**

Proof Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.

# Proof of Lemma 2

## Proof

Proof Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.
Let $\sigma \in Gal(F/E)$ s.t $\sigma\mathfrak{P} \neq \mathfrak{P}$ or, equivalently, $\mathfrak{P}' := \sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$.

# Proof of Lemma 2

### Proof

Proof Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.
Let $\sigma \in Gal(F/E)$ s.t $\sigma\mathfrak{P} \neq \mathfrak{P}$ or, equivalently, $\mathfrak{P}' := \sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$.
Since $\mathfrak{P}' \neq \mathfrak{P}$ we have, per our assumption, that

# Proof of Lemma 2

## Proof

Proof Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.
Let $\sigma \in Gal(F/E)$ s.t $\sigma\mathfrak{P} \neq \mathfrak{P}$ or, equivalently, $\mathfrak{P}' := \sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$.
Since $\mathfrak{P}' \neq \mathfrak{P}$ we have, per our assumption, that $v_{\mathfrak{P}'}(y) > 0$ and so $v_{\sigma_i^{-1}\mathfrak{P}}(y) > 0$, and so

$$v_{\mathfrak{P}}(\sigma y) = v_{\sigma^{-1}\mathfrak{P}}(y) > 0 \quad \Longrightarrow \quad \sigma y \in \mathcal{O}_{\mathfrak{P}} \text{ and } \pi(\sigma y) = 0.$$

# Proof of Lemma 2

## Proof

Proof Recall then $Tr_{F/E}(y) = \sum_{\sigma \in G} \sigma(y)$.
Let $\sigma \in Gal(F/E)$ s.t $\sigma\mathfrak{P} \neq \mathfrak{P}$ or, equivalently, $\mathfrak{P}' := \sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$.
Since $\mathfrak{P}' \neq \mathfrak{P}$ we have, per our assumption, that
$v_{\mathfrak{P}'}(y) > 0$ and so $v_{\sigma_i^{-1}\mathfrak{P}}(y) > 0$, and so

$$v_{\mathfrak{P}}(\sigma y) = v_{\sigma^{-1}\mathfrak{P}}(y) > 0 \quad \Longrightarrow \quad \sigma y \in \mathcal{O}_{\mathfrak{P}} \text{ and } \pi(\sigma y) = 0.$$

$$\begin{aligned}\pi(Tr_{F/E}(y)) &= \sum_{i=1}^{n} \pi(\sigma_i(y)) = \sum_{\sigma_i \in \mathcal{D}} \pi(\sigma_i(y)) \\ &= \sum_{\alpha \in Aut(F_{\mathfrak{P}}/E_p)} |\{i \mid \sigma_i \in \mathcal{D}, \sigma_i = \alpha\}| \cdot \alpha(\pi(y)).\end{aligned}$$

# Proof of Lemma 2

## Proof

Proof Recall

$$|\{i \mid \sigma_i \in \mathcal{D}, \sigma_i = \alpha\}| = I(\mathfrak{P}/\mathfrak{p}).$$

And

$$e(\mathfrak{P}/p) = \frac{[F:E]_i}{[F_{\mathfrak{P}}:E_{\mathfrak{p}}]_i} I(\mathfrak{P}/\mathfrak{p}).$$

# Proof of Lemma 2

## Proof

Proof Recall

$$|\{i \mid \sigma_i \in \mathcal{D}, \sigma_i = \alpha\}| = I(\mathfrak{P}/\mathfrak{p}).$$

And

$$e(\mathfrak{P}/p) = \frac{[F:E]_i}{[F_{\mathfrak{P}}:E_{\mathfrak{p}}]_i} I(\mathfrak{P}/\mathfrak{p}).$$

Which implies

$$\pi(Tr_{F/E}(y)) = e(\mathfrak{P}/\mathfrak{p}) \sum_{\alpha \in Aut(F_{\mathfrak{P}}/E_p)} \alpha(\pi(y)) = e(\mathfrak{P}/\mathfrak{p})\, Tr_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(\pi(y))$$

# Proof of Lemma 1 - Key Ideas

[

Proof sketch]
Consider $\hat{F}$ the Galois closure of $F$.

# Proof of Lemma 1 - Key Ideas

[

Proof sketch]
Consider $\hat{F}$ the Galois closure of $F$.

- $$Tr_{F/E}(y) = \sum_{E-embeddings} \sigma(y) = \sum_{\hat{\sigma} \in Gal(\hat{F}/E) | \text{diffrent on } F} \hat{\sigma}(y).$$

# Proof of Lemma 1 - Key Ideas

[

Proof sketch]
Consider $\hat{F}$ the Galois closure of $F$.

- $$Tr_{F/E}(y) = \sum_{E-embeddings} \sigma(y) = \sum_{\hat{\sigma} \in Gal(\hat{F}/E) | \text{diffrent on } F} \hat{\sigma}(y).$$
- We want to be smart when we choose $\hat{\sigma}$. We set some $\hat{\mathfrak{P}}/\mathfrak{P}$ and if possible we take $\hat{\sigma} \in D(\hat{\mathfrak{P}}/\mathfrak{p})$.

# Proof of Lemma 1 - Key Ideas

[

Proof sketch]
Consider $\hat{F}$ the Galois closure of $F$.

- $$Tr_{F/E}(y) = \sum_{E-embeddings} \sigma(y) = \sum_{\hat{\sigma}\in Gal(\hat{F}/E)|\text{diffrent on } F} \hat{\sigma}(y).$$
- We want to be smart when we choose $\hat{\sigma}$. We set some $\hat{\mathfrak{P}}/\mathfrak{P}$ and if possible we take $\hat{\sigma} \in D(\hat{\mathfrak{P}}/\mathfrak{p})$. Then we note that $\pi(\hat{\sigma}(y)) = \alpha(\pi(y))$ for some $\alpha \in E_{\mathfrak{p}}$ embedding of $F_{\mathfrak{P},s}$.

# Proof of Lemma 1 - Key Ideas

[

Proof sketch]
Consider $\hat{F}$ the Galois closure of $F$.

- $$Tr_{F/E}(y) = \sum_{E-embeddings} \sigma(y) = \sum_{\hat{\sigma} \in Gal(\hat{F}/E) | \text{diffrent on } F} \hat{\sigma}(y).$$
- We want to be smart when we choose $\hat{\sigma}$. We set some $\hat{\mathfrak{P}}/\mathfrak{P}$ and if possible we take $\hat{\sigma} \in D(\hat{\mathfrak{P}}/\mathfrak{p})$. Then we note that $\pi(\hat{\sigma}(y)) = \alpha(\pi(y))$ for some $\alpha \in E_{\mathfrak{p}}$ embedding of $F_{\mathfrak{P},s}$.
- We then argue that we can obtain any $\alpha$ in such manner, i.e. $\exists \hat{\sigma}$ s.t. $\pi(\hat{\sigma}(y)) = \alpha(\pi(y))$.

# Proof of Lemma 1 - Key Ideas

[

Proof sketch]
Consider $\hat{F}$ the Galois closure of $F$.

- $$Tr_{F/E}(y) = \sum_{E-embeddings} \sigma(y) = \sum_{\hat{\sigma}\in Gal(\hat{F}/E)|\text{diffrent on } F} \hat{\sigma}(y).$$
- We want to be smart when we choose $\hat{\sigma}$. We set some $\hat{\mathfrak{P}}/\mathfrak{P}$ and if possible we take $\hat{\sigma} \in D(\hat{\mathfrak{P}}/\mathfrak{p})$. Then we note that $\pi(\hat{\sigma}(y)) = \alpha(\pi(y))$ for some $\alpha \in E_{\mathfrak{p}}$ embedding of $F_{\mathfrak{P},s}$.
- We then argue that we can obtain any $\alpha$ in such manner, i.e. $\exists\hat{\sigma}$ s.t. $\pi(\hat{\sigma}(y)) = \alpha(\pi(y))$.
- We prove that for every $\alpha$,

$$|\{\hat{\sigma} \in \mathcal{D}(\hat{\mathfrak{P}}/\mathfrak{p}|\pi(\hat{\sigma}(y)) = \alpha(\pi(y))\}| = e(\mathfrak{P}/\mathfrak{p}).$$

# Valuation rings and their integral closures are PID

## Theorem 3

*For every $\mathfrak{p}$ there exists a local integral basis for $\mathfrak{p}$, namely, a basis $z_1, \ldots, z_n$ of $F/E$ s.t.*

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

## Proof

Let $z_1, \ldots, z_n$ be any basis for $F/E$. As we saw in class that we can find $a_i$ s.t. $a_i z_i$ is integral over $O_{\mathfrak{p}}$, we may assume that

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

or equivalently,

$$\sum_{j=1}^{n} \mathcal{O}_{\mathfrak{p}} z_j \subseteq \mathcal{O}'_{\mathfrak{p}}.$$

# Valuation rings and their integral closures are PID

**Proof**

$z_1, \ldots, z_n$ is a basis for $F/E$ s.t. $\sum_{j=1}^{n} \mathcal{O}_{\mathfrak{p}} z_j \subseteq \mathcal{O}'_{\mathfrak{p}}$.

# Valuation rings and their integral closures are PID

## Proof

$z_1, \dots, z_n$ is a basis for $F/E$ s.t. $\sum_{j=1}^{n} \mathcal{O}_\mathfrak{p} z_j \subseteq \mathcal{O}'_\mathfrak{p}$.
The key step of the proof is proving, by induction on $k$, that
$\exists u_1, \dots, u_n \in \mathcal{O}'_\mathfrak{p}$ s.t.

$$\mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^{k} \mathcal{O}_\mathfrak{p} z_i^* = \sum_{i=1}^{k} \mathcal{O}_\mathfrak{p} u_i.$$

# Valuation rings and their integral closures are PID

## Proof

$z_1, \ldots, z_n$ is a basis for $F/E$ s.t. $\sum_{j=1}^{n} \mathcal{O}_{\mathfrak{p}} z_j \subseteq \mathcal{O}'_{\mathfrak{p}}$.
The key step of the proof is proving, by induction on $k$, that $\exists u_1, \ldots, u_n \in \mathcal{O}'_{\mathfrak{p}}$ s.t.

$$\mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} z_i^* = \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} u_i.$$

By a Claim from class, if $\sum_{j=1}^{n} \mathcal{O}_{\mathfrak{p}} z_j \subseteq \mathcal{O}'_{\mathfrak{p}}$, then $\sum_{j=1}^{n} \mathcal{O}_{\mathfrak{p}} z_j^* \supseteq \mathcal{O}'_{\mathfrak{p}}$.

# Valuation rings and their integral closures are PID

## Proof

$z_1, \ldots, z_n$ is a basis for $F/E$ s.t. $\sum_{j=1}^{n} \mathcal{O}_{\mathfrak{p}} z_j \subseteq \mathcal{O}'_{\mathfrak{p}}$.
The key step of the proof is proving, by induction on $k$, that $\exists u_1, \ldots, u_n \in \mathcal{O}'_{\mathfrak{p}}$ s.t.

$$\mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} z_i^* = \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} u_i.$$

By a Claim from class, if $\sum_{j=1}^{n} \mathcal{O}_{\mathfrak{p}} z_j \subseteq \mathcal{O}'_{\mathfrak{p}}$, then $\sum_{j=1}^{n} \mathcal{O}_{\mathfrak{p}} z_j^* \supseteq \mathcal{O}'_{\mathfrak{p}}$.
Thus, if we will prove the above, by setting $k = n$, we can conclude that

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

which will almost prove the lemma (we still have to show that $u_1, \ldots, u_n$ is a basis of $F/E$).

# Valuation rings and their integral closures are PID

**Proof**

So, we wish to prove by induction on $k$, that $\exists u_1, \ldots, u_n \in \mathcal{O}'_{\mathfrak{p}}$ s.t

$$\mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} z_i^* = \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} u_i.$$

The base case $k = 0$ is trivial (empty sum is 0).

# Valuation rings and their integral closures are PID

## Proof

So, we wish to prove by induction on $k$, that $\exists u_1, \ldots, u_n \in \mathcal{O}'_{\mathfrak{p}}$ s.t

$$\mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} z_i^* = \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} u_i.$$

The base case $k = 0$ is trivial (empty sum is 0).
Say that $u_1, \ldots, u_{k-1} \in \mathcal{O}'_{\mathfrak{p}}$ satisfy that

$$\mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k-1} \mathcal{O}_{\mathfrak{p}} z_i^* = \sum_{i=1}^{k-1} \mathcal{O}_{\mathfrak{p}} u_i.$$

# Valuation rings and their integral closures are PID

## Proof

So, we wish to prove by induction on $k$, that $\exists u_1, \ldots, u_n \in \mathcal{O}'_\mathfrak{p}$ s.t

$$\mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^{k} \mathcal{O}_\mathfrak{p} z_i^* = \sum_{i=1}^{k} \mathcal{O}_\mathfrak{p} u_i.$$

The base case $k = 0$ is trivial (empty sum is 0).
Say that $u_1, \ldots, u_{k-1} \in \mathcal{O}'_\mathfrak{p}$ satisfy that

$$\mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^{k-1} \mathcal{O}_\mathfrak{p} z_i^* = \sum_{i=1}^{k-1} \mathcal{O}_\mathfrak{p} u_i.$$

Define

$$J = \{a_k \in \mathcal{O}_\mathfrak{p} \mid \exists a_1, \ldots, a_{k-1} \in \mathcal{O}_\mathfrak{p} \text{ s.t. } a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_\mathfrak{p}\}.$$

Observe that $J$ is an ideal of $\mathcal{O}_\mathfrak{p}$.

# Valuation rings and their integral closures are PID

## Proof

$$J = \{a_k \in \mathcal{O}_{\mathfrak{p}} \mid \exists a_1, \ldots, a_{k-1} \in \mathcal{O}_{\mathfrak{p}} \text{ s.t. } a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_{\mathfrak{p}}\}.$$

# Valuation rings and their integral closures are PID

## Proof

$$J = \{a_k \in \mathcal{O}_\mathfrak{p} \mid \exists a_1, \dots, a_{k-1} \in \mathcal{O}_\mathfrak{p} \ \text{ s.t. } \ a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_\mathfrak{p}\}.$$

As, $\mathcal{O}_\mathfrak{p}$ is a PID, we can write

$$\exists a_k \in J \quad J = a_k \mathcal{O}_\mathfrak{p}.$$

# Valuation rings and their integral closures are PID

## Proof

$$J = \{a_k \in \mathcal{O}_{\mathfrak{p}} \mid \exists a_1, \ldots, a_{k-1} \in \mathcal{O}_{\mathfrak{p}} \text{ s.t. } a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_{\mathfrak{p}}\}.$$

As, $\mathcal{O}_{\mathfrak{p}}$ is a PID, we can write

$$\exists a_k \in J \quad J = a_k \mathcal{O}_{\mathfrak{p}}.$$

Let $a_1, \ldots, a_{k-1} \in \mathcal{O}_{\mathfrak{p}}$ s.t.

$$u_k = a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_{\mathfrak{p}}.$$

# Valuation rings and their integral closures are PID

## Proof

$$J = \{a_k \in \mathcal{O}_\mathfrak{p} \mid \exists a_1, \ldots, a_{k-1} \in \mathcal{O}_\mathfrak{p} \ \text{ s.t. } \ a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_\mathfrak{p}\}.$$

As, $\mathcal{O}_\mathfrak{p}$ is a PID, we can write

$$\exists a_k \in J \quad J = a_k \mathcal{O}_\mathfrak{p}.$$

Let $a_1, \ldots, a_{k-1} \in \mathcal{O}_\mathfrak{p}$ s.t.

$$u_k = a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_\mathfrak{p}.$$

By the choice of $u_k$ and by the induction hypothesis, we get that

$$\mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^{k} \mathcal{O}_\mathfrak{p} z_i^* \supseteq \sum_{i=1}^{k} \mathcal{O}_\mathfrak{p} u_i.$$

# Valuation rings and their integral closures are PID

## Proof

On the other direction, take

$$z \in \mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} z_i^*.$$

Write

$$z = b_1 z_1^* + \cdots + b_k z_k^* \quad \text{with} \quad b_1, \ldots, b_k \in \mathcal{O}_{\mathfrak{p}}.$$

### Proof

On the other direction, take

$$z \in \mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} z_i^*.$$

Write

$$z = b_1 z_1^* + \cdots + b_k z_k^* \quad \text{with} \quad b_1, \ldots, b_k \in \mathcal{O}_{\mathfrak{p}}.$$

Thus, $b_k \in J = a_k \mathcal{O}_{\mathfrak{p}}$ and so $\exists c \in \mathcal{O}_{\mathfrak{p}}$ s.t. $b_k = c a_k$. Recall that

$$u_k = a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_{\mathfrak{p}}.$$

# Valuation rings and their integral closures are PID

## Proof

On the other direction, take

$$z \in \mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} z_i^*.$$

Write

$$z = b_1 z_1^* + \cdots + b_k z_k^* \quad \text{with} \quad b_1, \ldots, b_k \in \mathcal{O}_{\mathfrak{p}}.$$

Thus, $b_k \in J = a_k \mathcal{O}_{\mathfrak{p}}$ and so $\exists c \in \mathcal{O}_{\mathfrak{p}}$ s.t. $b_k = c a_k$. Recall that

$$u_k = a_1 z_1^* + \cdots + a_k z_k^* \in \mathcal{O}'_{\mathfrak{p}}.$$

As $z, u_k \in \mathcal{O}'_{\mathfrak{p}}$ we have that

$$\begin{aligned} z - c u_k &= (b_1 - c a_1) z_1^* + \cdots + (b_{k-1} - c a_{k-1}) z_{k-1}^* \\ &\in \mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k-1} \mathcal{O}_{\mathfrak{p}} z_i^* = \sum_{i=1}^{k-1} \mathcal{O}_{\mathfrak{p}} u_i. \end{aligned}$$

## Valuation rings and their integral closures are PID

### Proof

We conclude that

$$z \in \sum_{i=1}^{k} \mathcal{O}_{\mathfrak{p}} u_i$$

which proves the claim. Namely, $\exists u_1, \ldots, u_n \in \mathcal{O}'_{\mathfrak{p}}$ s.t.

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

and so

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

It remains to show that $u_1, \ldots, u_n$ is a basis of $F/E$.

# Valuation rings and their integral closures are PID

**Proof.**

Take $z \in F$. As $z$ is algebraic over $E$, as before,

$$\exists b \in \mathcal{O}_{\mathfrak{p}} \quad \text{s.t.} \quad bz \in \mathcal{O}'_{\mathfrak{p}}.$$

# Valuation rings and their integral closures are PID

**Proof.**

Take $z \in F$. As $z$ is algebraic over $E$, as before,

$$\exists b \in \mathcal{O}_{\mathfrak{p}} \quad \text{s.t.} \quad bz \in \mathcal{O}'_{\mathfrak{p}}.$$

That is, every element $z$ of $F$ is of the form $\frac{a}{b}$ for $a \in \mathcal{O}'_{\mathfrak{p}}$, $0 \neq b \in \mathcal{O}_{\mathfrak{p}}$. Now,

$$a = \sum_{i=1}^{n} c_i u_i$$

for some $c_1, \dots, c_n \in \mathcal{O}_{\mathfrak{p}}$ and so

$$z = \frac{a}{b} = \sum_{i=1}^{n} \frac{c_i}{b} u_i.$$

# Valuation rings and their integral closures are PID

**Proof.**

Take $z \in F$. As $z$ is algebraic over $E$, as before,

$$\exists b \in \mathcal{O}_{\mathfrak{p}} \quad \text{s.t.} \quad bz \in \mathcal{O}'_{\mathfrak{p}}.$$

That is, every element $z$ of $F$ is of the form $\frac{a}{b}$ for $a \in \mathcal{O}'_{\mathfrak{p}}$, $0 \neq b \in \mathcal{O}_{\mathfrak{p}}$. Now,

$$a = \sum_{i=1}^{n} c_i u_i$$

for some $c_1, \ldots, c_n \in \mathcal{O}_{\mathfrak{p}}$ and so

$$z = \frac{a}{b} = \sum_{i=1}^{n} \frac{c_i}{b} u_i.$$

Since $c_i, b \in \mathcal{O}_{\mathfrak{p}}$ we have that $\frac{c_i}{b} \in E$, and so $F = \sum_{i=1}^{n} E u_i$.

# Valuation rings and their integral closures are PID

**Proof.**

Take $z \in F$. As $z$ is algebraic over $E$, as before,

$$\exists b \in \mathcal{O}_{\mathfrak{p}} \quad \text{s.t.} \quad bz \in \mathcal{O}'_{\mathfrak{p}}.$$

That is, every element $z$ of $F$ is of the form $\frac{a}{b}$ for $a \in \mathcal{O}'_{\mathfrak{p}}$, $0 \neq b \in \mathcal{O}_{\mathfrak{p}}$. Now,

$$a = \sum_{i=1}^{n} c_i u_i$$

for some $c_1, \dots, c_n \in \mathcal{O}_{\mathfrak{p}}$ and so

$$z = \frac{a}{b} = \sum_{i=1}^{n} \frac{c_i}{b} u_i.$$

Since $c_i, b \in \mathcal{O}_{\mathfrak{p}}$ we have that $\frac{c_i}{b} \in E$, and so $F = \sum_{i=1}^{n} E u_i$. This shows that $u_1, \dots, u_n$ spans $F$ over $E$. The proof follows as $[E : F] = n$. □