Integrality and the Complementary Module

Unit 20

Gil Cohen

January 15, 2025

Overview

Modules

Definition 1 (Modules)

Let R be a (commutative unital) ring. An abelian group $(M, +)$ is said to be an *R-module* w.r.t an operation $\cdot : R \times M \to M$ such that

1. $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$
2. $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$
3. $(r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$
4. $1 \cdot m = m$

Remarks.

- When R is a field, an R-module is simply an R-vector space.
- Any ideal M of R is an R-module.
- Any R-module that is contained in R is an ideal of R.
- $\mathbb{Z}$-modules are precisely abelian groups.

Modules

Definition 2

An R-module M is finitely generated if $\exists m_1, \ldots, m_n \in \mathrm{M}$ s.t.

$$\mathrm{M} = \mathrm{R}m_1 + \cdots + \mathrm{R}m_n.$$

Remark When R is a field, hence M an R-vector space, this means M is finite dimensional over R. A generating set is a spanning set (but not necessarily a basis).

Separable extensions

Throughout this unit, we let F/L be a finite extension of E/K. Recall that this means that F/E is finite, and we proved that this is equivalent to L/K being finite.

We will further assume that F/E is separable. As we prove below, this implies that L/K is separable.

Lemma 3

Let F/L be a finite extension of E/K. If F/E is separable then L/K is separable.

Proof.

Take $\alpha \in$ L and $f(T) \in$ K$[T]$ its minimal polynomial over K. Since K is algebraically closed in E, as we proved, $f(T)$ is also irreducible over E.

As $\alpha \in$ F and F/E is separable we have that $f(T)$ is separable. □

Integral elements

Definition 4 (Integral elements)

Let R be a domain with field of fractions K. Let L/K be a field extension. We say that $x \in$ L is integral over R if x is the root of a monic polynomial $f(T) \in \mathrm{R}[T]$.

Note that

$$x \text{ is integral over R} \quad \Longleftrightarrow \quad \mathrm{R}[x] \text{ is a finitely generated R-module.}$$

Indeed, if $\deg f = d$ then

$$\mathrm{R}[x] = \mathrm{R} + x\mathrm{R} + \cdots + x^{d-1}\mathrm{R}. \tag{1}$$

On the other hand, if

$$\mathrm{R}[x] = f_1(x)\mathrm{R} + \cdots + f_e(x)\mathrm{R} \qquad f_i(x) \in \mathrm{R}[x]$$

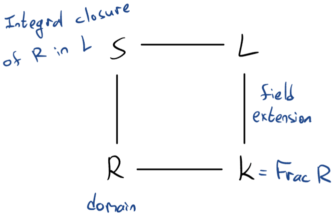
then we get an equation as in (1) and so x^d can be expressed as an R-linear relation between $1, x, \ldots, x^{d-1}$.

It is a (not so trivial) fact that x is integral over R iff R[x] is contained in a ring C that is finitely generated R-module.

Integral closure

Definition 5

Let R be a domain with field of fractions K. Let L/K be a field extension. The integral closure of R in L is the set of elements in L that are integral over R.



Claim 6

The integral closure of R in L is a subring of L.

The proof readily follows by the nontrivial fact mentioned above.

Integral elements

Definition 7

A domain R is said to be integrally closed if the integral closure of R in its field of fractions K is equal to R.

Lemma 8

Let R *be an integrally closed domain with field of fractions* K*. Let* L/K *be an algebraic field extension. Take* $x \in \mathrm{L}$ *integral over R, and let* $f(T) \in \mathrm{K}[T]$ *be its (monic) minimal polynomial over* K*. Then,*

$$f(T) \in \mathrm{R}[T].$$

Integral ring extensions

Proof.

Note that all K-conjugates of x are also integral over R.

Recall that the coefficients of $f(T)$ are elementary symmetric polynomials applied to the roots and, in particular, are all integral over R.

However, the coefficients are also in K and thus, as R is integrally closed, all coefficients are in R. □

We leave the following lemma as an exercise (we actually proved this in a specific setting).

Lemma 9

Let K *be the field of fractions of a domain* R*. Let x be an algebraic element over* K*. Then, $\exists 0 \neq a \in$ R s.t. ax is integral over* R.

Overview

Valuation rings are integrally closed

Lemma 10

Every valuation ring R *is integrally closed.*

Proof.

Let $\mathrm{K} = \operatorname{Frac}\mathrm{R}$ and let $0 \neq x \in \mathrm{K}$ integral over R. We wish to prove that $x \in \mathrm{R}$.

There are $a_0, \ldots, a_{n-1} \in \mathrm{R}$ s.t.

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Dividing by x^{n-1} and rearranging, we get

$$x = -a_{n-1} - a_{n-2}(x^{-1}) - \cdots - a_0(x^{-1})^{n-1}.$$

If $x \in \mathrm{R}$ we are done. Otherwise, $x^{-1} \in \mathrm{R}$ and by the above equation also is x. □

Valuation rings and integral closures

Theorem 11

Let R be a subdomain of a field L. Then, the integral closure of R in L is the intersection of all valuation rings of L that contain R.

Proof. (addendum)

In one direction, take $x \in \mathrm{L}$ that is integral over R. Let $\mathcal{O} \subseteq \mathrm{L}$ be a valuation ring of L that contains R.

Since x is integral over R we have that x is integral over $\mathcal{O}$. But recall that

$$\operatorname{Frac} \mathcal{O} = \mathrm{L}.$$

As we proved in Lemma 10, $\mathcal{O}$ is integrally closed, and so $x \in \mathcal{O}$.

Valuation rings and integral closures

Proof.

As for the other direction, take $x \in \mathrm{L}$ that is not integral over R. We will "cook up" a valuation ring $\mathcal{O}$ of L that contains R yet does not contain x.

Let $\mathrm{S} = \mathrm{R}[x^{-1}]$. Note that $x \notin \mathrm{S}$. Indeed, otherwise

$$x = a_0 + a_1(x^{-1}) + \cdots + a_n(x^{-1})^n,$$

where $a_0, \ldots, a_n \in \mathrm{R}$ and so

$$x^{n+1} - a_0 x^n - \cdots - a_n = 0,$$

implying that x is integral over R.

Valuation rings and integral closures

Proof.

Since $x \notin \mathrm{S} = \mathrm{R}[x^{-1}]$ we have that x^{-1} is not a unit of S and so there exists a maximal ideal $\mathfrak{m}$ of S that contains x^{-1}.

Consider the field $\mathrm{K} = \mathrm{S}/\mathfrak{m}$. As we saw in the recitation, the projection $\mathrm{S} \to \mathrm{K}$ can be extended to a place φ of L. Now,

$$x^{-1} \in \mathfrak{m} \implies \varphi(x^{-1}) = 0 \implies \varphi(x) = \infty.$$

Thus, the valuation ring $\mathcal{O}$ that corresponds to φ does not contain x.

To conclude the proof note that $\mathrm{R} \subseteq \mathcal{O}$ (since $\mathrm{S} = \mathrm{R}[x^{-1}] \subseteq \mathcal{O}$). □

Overview

The trace function

Let L/K be a finite field extension. Given $a \in \mathrm{L}$ note that the map

$$\begin{aligned} m_a : \mathrm{L} &\to \mathrm{L} \\ x &\mapsto ax \end{aligned}$$

is K-linear. Indeed, for $x, y \in \mathrm{L}$

$$m_a(x+y) = a(x+y) = ax + ay = m_a(x) + m_a(y).$$

Moreover, for $k \in \mathrm{K}$,

$$m_a(kx) = a(kx) = k(ax) = km_a(x).$$

Let M_a denote the matrix corresponding to m_a with respect to a fixed, arbitrary, basis of L as a K-vector space. We define the trace map

$$\begin{aligned} \mathrm{Tr}_{\mathrm{L}/\mathrm{K}} : \mathrm{L} &\to \mathrm{K} \\ a &\mapsto \mathrm{trace}(\mathrm{M}_a). \end{aligned}$$

The trace function

Fix $a \in \mathrm{L}$ and denote the minimal polynomial of a over K by

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in \mathrm{K}[x].$$

Then, choosing the basis $1, a, a^2, \ldots, a^{n-1}$ of $\mathrm{K}(a)$ over K, we get

$$M_a = \begin{pmatrix} 0 & 0 & & 0 & -c_0 \\ 1 & 0 & & 0 & -c_1 \\ 0 & 1 & \cdots & \vdots & \vdots \\ \vdots & 0 & & 0 & \\ 0 & \vdots\ 0 & & 1 & -c_{n-1} \end{pmatrix}$$

and so

$$\mathrm{Tr}_{\mathrm{K}(a)/\mathrm{K}}(a) = -c_{n-1}.$$

The trace function

Fix $a \in L$. If we construct the basis for L over K by first constructing a basis for K(a) over K and then picking a basis of L over K(a) then M_a takes the form of a block matrix

$$M_a = \begin{pmatrix} \begin{matrix} 0 & 0 & -c_0 \\ 1 \ddots & \vdots & \vdots \\ 0 & 1 & -c_{n-1} \end{matrix} & 0 & 0 \\ 0 & \begin{matrix} 0 & 0 & -c_0 \\ 1 \ddots & \vdots & \vdots \\ 0 & 1 & -c_{n-1} \end{matrix} & 0 \\ & & \ddots \\ 0 & 0 & \begin{matrix} 0 & 0 & -c_0 \\ 1 \ddots & \vdots & \vdots \\ 0 & 1 & -c_{n-1} \end{matrix} \end{pmatrix}$$

From this we see that

$$\mathrm{Tr}_{L/K}(a) = [L : K(a)] \cdot \mathrm{Tr}_{K(a)/K}(a). \tag{2}$$

The trace function

$$\mathrm{Tr}_{L/K}(a) = [L : K(a)] \cdot \mathrm{Tr}_{K(a)/K}(a).$$

Corollary 12

$$L/K \text{ not separable} \implies \mathrm{Tr}_{L/K} = 0.$$

Proof.

Fix $a \in L$. At least one of $L/K(a)$, $K(a)/K$ is not separable.

In the first case, for some $e \geq 1$ we have that

$$p^e = [L : K(a)]_i \mid [L : K(a)].$$

Assume then that $K(a)/K$ is not separable. Then, the minimal polynomial $f(x)$ of a over K is of degree p^m for some $m \geq 1$, and has the form $h(x^p)$, and so the coefficient of x^{p^m-1} is 0. Thus,

$$\mathrm{Tr}_{K(a)/K}(a) = 0.$$

The trace function

Theorem 13

Let L/K *be a finite separable extension. Let* $\widehat{\mathrm{L}}$ *be the normal closure of* L/K*. Let* S *be the set of* K*-embeddings of* L *into* $\widehat{\mathrm{L}}$*. Then,*

$$\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(a) = \sum_{\sigma \in \mathrm{S}} \sigma(a).$$

Proof.

Let

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in \mathrm{K}[x]$$

be the minimal polynomial of a over K. One can show that

$$f(x) = \chi_x(\mathrm{M}_a) \triangleq \det(xI - \mathrm{M}_a),$$

where M_a is the matrix corresponding to multiplication by a in $\mathrm{K}(a)$.

The trace function

Proof.

Denote the distinct K-conjugates of a by $a = a_1, \ldots, a_m \in \widehat{\mathrm{L}}$. Then, since a is separable over K,

$$\prod_{i=1}^{m}(x - a_i) = f(x) = \det(xI - \mathrm{M}_a).$$

By definition,

$$\mathrm{Tr}_{\mathrm{K}(a)/\mathrm{K}}(a) = \mathrm{trace}(\mathrm{M}_a).$$

In general, $-\mathrm{trace}(\mathrm{M}_a)$ is the coefficient of x^{n-1} in $\det(xI - \mathrm{M}_a)$. So,

$$\mathrm{Tr}_{\mathrm{K}(a)/\mathrm{K}}(a) = \sum_{i=1}^{m} a_i.$$

Equation (2) then implies that

$$\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(a) = [\mathrm{L} : \mathrm{K}(a)] \cdot \sum_{i=1}^{m} a_i. \tag{3}$$

The trace function

Proof.

Recall that

$$S = \left\{ \sigma : \mathsf{L} \hookrightarrow \widehat{\mathsf{L}} \,:\, \sigma|_{\mathsf{K}} = \mathrm{id}_{\mathsf{K}} \right\}.$$

Note that $\sigma(a) = a_i$ for some $i = i(\sigma) \in [m]$. Let

$$S_i = \{ \sigma \in S \,:\, \sigma(a) = a_i \}.$$

It is known from Galois Theory that $|S_i| = |S_j|$ for all i, j. Thus,

$$|S_i| = \frac{|S|}{m} = \frac{[\mathsf{L}:\mathsf{K}]_s}{[\mathsf{K}(a):\mathsf{K}]} = \frac{[\mathsf{L}:\mathsf{K}]}{[\mathsf{K}(a):\mathsf{K}]} = [\mathsf{L}:\mathsf{K}(a)].$$

Therefore,

$$\sum_{\sigma \in S} \sigma(a) = \sum_{i=1}^{m} \sum_{\sigma \in S_i} \sigma(a) = [\mathsf{L}:\mathsf{K}(a)] \cdot \sum_{i=1}^{m} a_i.$$

The proof then follows by Equation (3).

The trace function

The proof of the following result is left as an exception.

Lemma 14

Let $L'/L/K$ *be a tower of finite field extensions. Then,*

$$\mathrm{Tr}_{L'/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{L'/L}$$

We turn to prove

Theorem 15

Let L/K *be a finite separable extension. Then,* $\mathrm{Tr}_{L/K} \neq 0$.

Proof.

First note we may assume that L/K is Galois. Indeed, consider the Galois closure $\widehat{L}$ of L over K. By Lemma 14,

$$\mathrm{Tr}_{\widehat{L}/K} \neq 0 \quad \Longrightarrow \quad \mathrm{Tr}_{L/K} \neq 0.$$

The trace function

Proof.

Write $\mathsf{L} = \mathsf{K}(\alpha)$ and let $f(x) \in \mathsf{K}[x]$ be the minimal polynomial of α over K. Consider the basis $1, \alpha, \ldots, \alpha^{n-1}$ of L over K.

Define the K-bilinear map

$$(x, y) \mapsto \mathrm{Tr}_{\mathsf{L}/\mathsf{K}}(xy),$$

and let M be the $n \times n$ matrix over L s.t.

$$\mathsf{M}_{i,j} = \mathrm{Tr}_{\mathsf{L}/\mathsf{K}}(\alpha^{i+j}).$$

We will show that $\det \mathsf{M} \neq 0$ which would imply that $\mathrm{Tr}_{\mathsf{L}/\mathsf{K}} \neq 0$.

To this end, denote $G = \mathrm{Gal}(\mathsf{L}/\mathsf{K})$. By Theorem 13,

$$\mathrm{Tr}_{\mathsf{L}/\mathsf{K}}(\alpha^{i+j}) = \sum_{\sigma \in G} \sigma(\alpha^{i+j}) = \sum_{\sigma \in G} \sigma(\alpha)^{i+j}.$$

The trace function

Proof.

So,

$$\mathrm{M}_{i,j} = \sum_{\sigma \in G} \sigma(\alpha)^{i+j}.$$

Define the $n \times n$ matrix N over L by

$$\mathrm{N}_{i,\sigma} = \sigma(\alpha^i).$$

Indeed, $[\mathrm{L} : \mathrm{K}] = |\mathrm{Gal}(\mathrm{L}/\mathrm{K})| = |G|$. Then,

$$(\mathrm{N}\mathrm{N}^{\mathrm{T}})_{i,j} = \sum_{\sigma \in G} \mathrm{N}_{i,\sigma}\mathrm{N}_{j,\sigma} = \sum_{\sigma \in G} \sigma(\alpha^i)\sigma(\alpha^j) = \sum_{\sigma \in G} \sigma(\alpha)^{i+j},$$

and so $\mathrm{M} = \mathrm{N}\mathrm{N}^{\mathrm{T}}$. Thus,

$$\det \mathrm{M} = (\det \mathrm{N})^2.$$

The trace function

Proof.

We defined

$$N_{i,\sigma} = \sigma(\alpha^i).$$

and proved that

$$\det M = (\det N)^2.$$

We wish to show $\det M \neq 0$ and it is therefore suffices to show that $\det N \neq 0$. But N is a Vandermonde matrix and so (under some arbitrary order on G),

$$\det N = \prod_{\sigma < \tau} (\sigma(\alpha) - \tau(\alpha)).$$

Since $L = K(\alpha)$, for $\sigma \neq \tau$ we have that $\sigma(\alpha) \neq \tau(\alpha)$. Therefore, $\det N \neq 0$. □

Overview

Dual bases

Let L/K be finite and separable. When considering L as a K-vector space we may consider the dual space of L over K that is given by

$$L^* = \hom_K(L, K)$$

that consists of all K-linear maps from L to K.

Every $x \in L$ induces an element $\varphi_x \in L^*$ that is given by

$$\varphi_x(y) = \mathrm{Tr}_{L/K}(xy).$$

This map is indeed a K-linear functional as it is composition of multiplication by x and the trace function.

For different x, x' we get distinct maps $\varphi_x, \varphi_{x'}$ for if $\varphi_x = \varphi_{x'}$ then

$$\forall y \in L \quad \mathrm{Tr}_{L/K}(xy) = \mathrm{Tr}_{L/K}(x'y) \quad \Longrightarrow \quad \forall y \in L \quad \mathrm{Tr}_{L/K}((x-x')y) = 0.$$

Theorem 15 then implies $x = x'$.

Dual bases

Recall

$$\varphi_x(y) = \mathrm{Tr}_{L/K}(xy).$$

Consider the map

$$\psi : L \to L^*$$
$$x \mapsto \varphi_x$$

This is a K-vector space monomorphism since, e.g.,

$$\mathrm{Tr}_{L/K}((x + x')y) = \mathrm{Tr}_{L/K}(xy) + \mathrm{Tr}_{L/K}(x'y).$$

Recall from linear algebra that

$$\dim_K L = \dim_K L^* < \infty,$$

and so, as ψ is one to one, we have that ψ is a K-vector space isomorphism from L to L^*.

Moreover, for every basis $z_1, \ldots, z_n$ of L over K there is a dual basis $z_1^*, \ldots, z_n^*$ of L^* over K that is characterized by

$$\mathrm{Tr}_{L/K}(z_i^* z_j) = \delta_{i,j}.$$

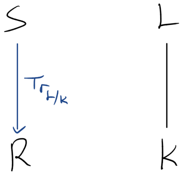
Overview

Trace and integral elements

Claim 16

Let R be a subdomain of L with field of fractions $K \subseteq L$. Assume that R is integrally closed. Then, $\forall x \in L$ that is integral over R, we have that

$$\mathrm{Tr}_{L/K}(x) \in R.$$



Proof.

$\sigma(x)$ is integral over R for every embedding $\sigma : L \hookrightarrow \widehat{L}$ over K. Thus, by Theorem 13, $\mathrm{Tr}_{L/K}(x)$ is also integral over R. The proof follows since R is integrally closed and $\mathrm{Tr}_{L/K}(x) \in K$. □

Integral closure of a valuation ring

Definition 17

Let F/L is a finite separable extension of E/K, and let $\mathfrak{p}$ be a prime divisor of E/K. We denote by $\mathcal{O}'_{\mathfrak{p}}$ the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in F.

Recall

Theorem (Theorem 11)

Let R ($\mathcal{O}_{\mathfrak{p}}$) be a subdomain of a field L (F). Then, the integral closure of R in L ($\mathcal{O}'_{\mathfrak{p}}$) is the intersection of all valuation rings of L (F) that contain R ($\mathcal{O}_{\mathfrak{p}}$).

By red-Theorem 11, $\mathcal{O}'_{\mathfrak{p}}$ is precisely the intersection of all valuation rings of F that contain $\mathcal{O}_{\mathfrak{p}}$. Thus,

$$\mathcal{O}'_{\mathfrak{p}} = \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_{\mathfrak{P}}.$$

Valuation rings and their integral closures are PID

Theorem 18

With the notation above, $\mathcal{O}_{\mathfrak{p}}$ and $\mathcal{O}'_{\mathfrak{p}}$ are both PID.

Proof. (addendum)

We start by considering $\mathcal{O}'_{\mathfrak{p}}$ which recall is equal to $\cap_{\mathfrak{P}/\mathfrak{p}}\mathcal{O}_{\mathfrak{P}}$. Take $0 \neq J$ an ideal of $\mathcal{O}'_{\mathfrak{p}}$. For every $\mathfrak{P}/\mathfrak{p}$ let $x_{\mathfrak{P}} \in J$ be an element with "least" valuation

$$k_{\mathfrak{P}} \triangleq v_{\mathfrak{P}}(x_{\mathfrak{P}}) = \min\{v_{\mathfrak{P}}(x) : x \in J\}.$$

Since $J \subseteq \mathcal{O}_{\mathfrak{P}}$ we have that $v_{\mathfrak{P}}(x) \geq 0$ for all $x \in J$ and so the minimum is well-defined.

Note that

$$\forall \mathfrak{P}'/\mathfrak{p} \quad v_{\mathfrak{P}'}(x_{\mathfrak{P}}) \geq 0$$

as $x_{\mathfrak{P}} \in J \subseteq \mathcal{O}'_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{P}'}$.

Valuation rings and their integral closures are PID

Proof.

Fix $\mathfrak{P}/\mathfrak{p}$. By the WAT $\exists z_{\mathfrak{P}} \in F$ s.t.

$$\begin{aligned} &\upsilon_{\mathfrak{P}}(z_{\mathfrak{P}}) = 0, \\ &\upsilon_{\mathfrak{P}'}(z_{\mathfrak{P}}) > k_{\mathfrak{P}'} \geq 0 \qquad \forall \mathfrak{P}' \neq \mathfrak{P}. \end{aligned}$$

Thus, $z_{\mathfrak{P}} \in \mathcal{O}'_{\mathfrak{p}}$ for all $\mathfrak{P}/\mathfrak{p}$. As $x_{\mathfrak{P}} \in J$ we get that

$$x \triangleq \sum_{\mathfrak{P}/\mathfrak{p}} x_{\mathfrak{P}} z_{\mathfrak{P}} \in J.$$

Clearly, $x\mathcal{O}'_{\mathfrak{p}} \subseteq J$. We turn to prove the converse.

Valuation rings and their integral closures are PID

Proof.

First note that $\upsilon_{\mathfrak{P}'}(x) = k_{\mathfrak{P}'}$ for all $\mathfrak{P}'/\mathfrak{p}$. Indeed,

$$\begin{aligned}
\upsilon_{\mathfrak{P}'}(x_{\mathfrak{P}'} z_{\mathfrak{P}'}) &= \upsilon_{\mathfrak{P}'}(x_{\mathfrak{P}'}) + \upsilon_{\mathfrak{P}'}(z_{\mathfrak{P}'}) = k_{\mathfrak{P}'} + 0 = k_{\mathfrak{P}'}, \\
\upsilon_{\mathfrak{P}'}(x_{\mathfrak{P}} z_{\mathfrak{P}}) &= \upsilon_{\mathfrak{P}'}(x_{\mathfrak{P}}) + \upsilon_{\mathfrak{P}'}(z_{\mathfrak{P}}) \geq \upsilon_{\mathfrak{P}'}(z_{\mathfrak{P}}) > k_{\mathfrak{P}'} \qquad \forall \mathfrak{P}' \neq \mathfrak{P}.
\end{aligned}$$

Thus,

$$\upsilon_{\mathfrak{P}'}(x) = \upsilon_{\mathfrak{P}'}\left(\sum_{\mathfrak{P}/\mathfrak{p}} x_{\mathfrak{P}} z_{\mathfrak{P}}\right) = k_{\mathfrak{P}'}.$$

Valuation rings and their integral closures are PID

Proof.

Take $z \in J$. We wish to prove that $z \in x\mathcal{O}_{\mathfrak{p}'}$, namely, that

$$\frac{z}{x} \in \mathcal{O}_{\mathfrak{p}'}.$$

To this end we will show that

$$\forall \mathfrak{P}/\mathfrak{p} \qquad \frac{z}{x} \in \mathcal{O}_{\mathfrak{P}}.$$

But,

$$v_{\mathfrak{P}}\left(\frac{z}{x}\right) = v_{\mathfrak{P}}(z) - v_{\mathfrak{P}}(x) = v_{\mathfrak{P}}(z) - k_{\mathfrak{P}} \geq 0,$$

and the proof follows.

The same proof with $\mathrm{F} = \mathrm{E}$ shows that $\mathcal{O}_{\mathfrak{p}}$ is a PID. Indeed, in this case the integral closure $\mathcal{O}_{\mathfrak{p}'}$ of $\mathcal{O}_{\mathfrak{p}}$ in $\mathrm{F} = \mathrm{E}$ is simply $\mathcal{O}_{\mathfrak{p}}$. □

Ideals of valuation rings

Definition 19

Let $\mathfrak{p}$ be a prime divisor. An element $t \in \mathcal{O}_\mathfrak{p}$ is called a local parameter for $\mathfrak{p}$ if $v_\mathfrak{p}(t) = 1$.

Note that $\mathfrak{m}_\mathfrak{p} = t\mathcal{O}_\mathfrak{p}$. Indeed,

$$\forall x \in \mathcal{O}_\mathfrak{p} \quad v_\mathfrak{p}(tx) = v_\mathfrak{p}(t) + v_\mathfrak{p}(x) > 0 \quad \Longrightarrow \quad tx \in \mathfrak{m}_\mathfrak{p}.$$

On the other hand,

$$x \in \mathfrak{m}_\mathfrak{p} \quad \Longrightarrow \quad v_\mathfrak{p}(x) \geq 1 \quad \Longrightarrow \quad v_\mathfrak{p}(x/t) \geq 0 \quad \Longrightarrow \quad x \in t\mathcal{O}_\mathfrak{p}.$$

The following claim says that the ideals of $\mathcal{O}_\mathfrak{p}$ form a chain.

Claim 20

Let $\mathcal{O}_\mathfrak{p}$ be a valuation ring with local parameter t. Let $0 \neq J \subseteq \mathcal{O}_\mathfrak{p}$ be an ideal. Then,

$$\exists k \in \mathbb{N} \quad J = t^k \mathcal{O}_\mathfrak{p}.$$

Ideals of valuation rings

Proof. (addendum)

Let
$$k = \min\{v_{\mathfrak{p}}(x) \mid x \in J\}$$
and let $y \in J$ s.t. $v_{\mathfrak{p}}(y) = k$. We will show that $J = t^k \mathcal{O}_{\mathfrak{p}}$.
$$x \in J \implies v_{\mathfrak{p}}(x) \geq k \implies v_{\mathfrak{p}}(x/t^k) \geq 0 \implies x \in t^k \mathcal{O}_{\mathfrak{p}}.$$
On the other hand
$$x \in t^k \mathcal{O}_{\mathfrak{p}} \implies \frac{xy}{t^k} \in J \implies x \in \frac{t^k}{y} J.$$
But $v_{\mathfrak{p}}(t^k/y) = 0$ and so $t^k/y \in \mathcal{O}_{\mathfrak{p}}$. Thus, $x \in J$.

Modules over valuation rings

Claim 21 (addendum)

Let E/K be a function field and $\mathfrak{p}$ a prime divisor. Let $0 \neq J \subseteq E$ be an $\mathcal{O}_\mathfrak{p}$-module. Assume that

$$\min\{v_\mathfrak{p}(x) \mid x \in J\} = k > -\infty.$$

Then, $J = t^m \mathcal{O}_\mathfrak{p}$ for some $m \in \mathbb{Z}$.

Proof.

Let t be a local parameter for $\mathfrak{p}$. Per our assumption,

$$t^{-k} J \subseteq \mathcal{O}_\mathfrak{p}.$$

Thus $t^{-k} J$ is an $\mathcal{O}_\mathfrak{p}$-module that is contained in $\mathcal{O}_\mathfrak{p}$, namely, $t^{-k} J$ is an ideal of $\mathcal{O}_\mathfrak{p}$. By Claim 20,

$$\exists \ell \geq 0 \quad t^{-k} J = t^{\ell} \mathcal{O}_\mathfrak{p}$$

and so $J = t^{k+\ell} \mathcal{O}_\mathfrak{p}$.

Overview

Valuation rings and their integral closures are PID

Definition 22

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

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

Valuation rings and their integral closures are PID

For every $\mathfrak{p}$ there is a local integral basis. As a first step for proving that, we prove the following.

Claim 23 (addendum)

Let $z_1, \ldots, z_n \in \mathcal{O}'_{\mathfrak{p}}$ be a basis of F/E, namely,

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

Then,

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

Valuation rings and their integral closures are PID

Proof.

Given $z \in \mathcal{O}'_{\mathfrak{p}}$ (even in F) we can write

$$z = \sum_{i=1}^{n} a_i z_i^* \qquad a_1, \ldots, a_n \in \mathrm{E}.$$

Now, $z, z_j \in \mathcal{O}'_{\mathfrak{p}}$ and so $zz_j \in \mathcal{O}'_{\mathfrak{p}}$. As $\mathcal{O}_{\mathfrak{p}}$ is integrally closed (Lemma 10), Claim 16 implies that

$$\mathrm{Tr}_{\mathrm{F}/\mathrm{E}}(zz_j) \in \mathcal{O}_{\mathfrak{p}}.$$

But

$$\mathrm{Tr}_{\mathrm{F}/\mathrm{E}}(zz_j) = \mathrm{Tr}_{\mathrm{F}/\mathrm{E}}\left(\sum_{i=1}^{n} a_i z_i^* z_j\right) = \sum_{i=1}^{n} a_i \mathrm{Tr}_{\mathrm{F}/\mathrm{E}}(z_i^* z_j) = a_j.$$

Thus, $a_1, \ldots, a_n \in \mathcal{O}_{\mathfrak{p}}$, proving the claim. □

Valuation rings and their integral closures are PID

Theorem 24 (addendum)

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. By repeatedly applying Lemma 9, 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. $\sum_{j=1}^{n} \mathcal{O}_\mathfrak{p} z_j \subseteq \mathcal{O}'_\mathfrak{p}$.

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 Claim 23, $\mathcal{O}'_\mathfrak{p} \subseteq \sum_{i=1}^{n} \mathcal{O}_\mathfrak{p} z_i^*$. 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).

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.

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

By Theorem 18, $\mathcal{O}_\mathfrak{p}$ is a PID and so

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

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

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

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

$$z - cu_k = (b_1 - ca_1) z_1^* + \cdots + (b_{k-1} - ca_{k-1}) z_{k-1}^*$$
$$\in \mathcal{O}'_{\mathfrak{p}} \cap \sum_{i=1}^{k-1} \mathcal{O}_{\mathfrak{p}} z_i^* = \sum_{i=1}^{k-1} \mathcal{O}_{\mathfrak{p}} u_i.$$

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 $z \in \mathrm{F}$. As z is algebraic over E, Lemma 9 implies that

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

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 $\frac{c_i}{b} \in \mathrm{E}$, and so $\mathrm{F} = \sum_{i=1}^{n} \mathrm{E} u_i$.

This shows that $u_1, \ldots, u_n$ spans F over E. The proof follows as $[\mathrm{E} : \mathrm{F}] = n$. □

Overview

The complementary module

As usual, let F/L be an extension of E/K s.t. F/E is finite and separable.

Let $\mathfrak{p}$ be a prime divisor of E/K with a corresponding valuation ring $\mathcal{O}_\mathfrak{p}$. Let $\mathcal{O}'_\mathfrak{p}$ be the integral closure of $\mathcal{O}_\mathfrak{p}$ in F.

Definition 25

The complementary module over $\mathcal{O}_\mathfrak{p}$ is defined to be

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

Recall that every valuation ring is integrally closed (Lemma 10). Claim 16 then implies that $\mathcal{O}'_\mathfrak{p} \subseteq \mathsf{C}_\mathfrak{p}$.

Note that $\mathsf{C}_\mathfrak{p}$ is closed under addition and that $\mathcal{O}'_\mathfrak{p}\mathsf{C}_\mathfrak{p} \subseteq \mathsf{C}_\mathfrak{p}$. Thus, $\mathsf{C}_\mathfrak{p}$, as its name suggests, is an $\mathcal{O}'_\mathfrak{p}$-module and, in particular, it is also an $\mathcal{O}_\mathfrak{p}$ module.

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 26

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.

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

(as we know exists by Theorem 24). Then,

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

The complementary module

Proof.

Take $z \in \mathsf{C}_{\mathfrak{p}}$. Recall that $z_1^*, \ldots, z_n^*$ is a basis of F over E. Write z as

$$z = \sum_{i=1}^{n} x_i z_i^* \quad \text{where} \quad x_1, \ldots, x_n \in \mathsf{E}.$$

To prove that $\mathsf{C}_{\mathfrak{p}} \subseteq \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} z_i^*$ it suffices to prove that $x_1, \ldots, x_n \in \mathcal{O}_{\mathfrak{p}}$.

Fix $j \in [n]$. As $z_j \in \mathcal{O}'_{\mathfrak{p}}$ we have that

$$z \in \mathsf{C}_{\mathfrak{p}} \quad \Longrightarrow \quad \mathrm{Tr}_{\mathsf{F}/\mathsf{E}}(z z_j) \in \mathcal{O}_{\mathfrak{p}}.$$

But

$$\mathrm{Tr}_{\mathsf{F}/\mathsf{E}}(z z_j) = \mathrm{Tr}_{\mathsf{F}/\mathsf{E}}\left(\sum_{i=1}^{n} x_i z_i^* z_j\right) = \sum_{i=1}^{n} x_i \mathrm{Tr}_{\mathsf{F}/\mathsf{E}}(z_i^* z_j) = x_j,$$

and so $z \in \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} z_i^*$.

The complementary module

Proof.

We turn to prove that $\mathrm{C}_{\mathfrak{p}} \supseteq \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} z_i^*$. To this end we need to take $z \in \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} z_i^*$, $z' \in \mathcal{O}'_{\mathfrak{p}}$ and show that $\mathrm{Tr}_{\mathrm{F}/\mathrm{E}}(zz') \in \mathcal{O}_{\mathfrak{p}}$.

Write

$$z = \sum_{i=1}^{n} x_i z_i^* \qquad z' = \sum_{j=1}^{n} y_j z_j,$$

where $x_i, y_j \in \mathcal{O}_{\mathfrak{p}}$. Now,

$$\begin{aligned}\mathrm{Tr}_{\mathrm{F}/\mathrm{E}}(zz') &= \mathrm{Tr}_{\mathrm{F}/\mathrm{E}}\left(\sum_{i,j} x_i y_j z_i^* z_j\right) = \sum_{i,j} x_i y_j \mathrm{Tr}_{\mathrm{F}/\mathrm{E}}(z_i^* z_j) \\ &= \sum_i x_i y_i \in \mathcal{O}_{\mathfrak{p}},\end{aligned}$$

and the proof follows.

The complementary module

Claim 27

For every $\mathfrak{p}$ there exists $t_{\mathfrak{p}} \in \mathsf{F}$ s.t. $\mathsf{C}_{\mathfrak{p}} = t_{\mathfrak{p}} \mathcal{O}'_{\mathfrak{p}}$.

Proof.

Theorem 24 guarantees the existence of a basis $z_1, \ldots, z_n$ of F/E s.t.

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

Claim 26 then implies that

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

By the WAT we can find $x \in \mathsf{E}$ s.t.

$$\upsilon_{\mathfrak{p}}(x) \geq -\upsilon_{\mathfrak{P}}(z_i^*) \qquad \forall \mathfrak{P}/\mathfrak{p}, \;\; i \in [n].$$

The complementary module

Proof.

$$\upsilon_{\mathfrak{p}}(x) \geq -\upsilon_{\mathfrak{P}}(z_i^*) \qquad \forall \mathfrak{P}/\mathfrak{p}, \;\; i \in [n].$$

Thus, for all $\mathfrak{P}/\mathfrak{p}$ and $i \in [n]$,

$$\upsilon_{\mathfrak{P}}(xz_i^*) = e(\mathfrak{P}/\mathfrak{p})\upsilon_{\mathfrak{p}}(x) + \upsilon_{\mathfrak{P}}(z_i^*) \geq 0.$$

Therefore, for every $i \in [n]$,

$$xz_i^* \in \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_{\mathfrak{P}} = \mathcal{O}'_{\mathfrak{p}}.$$

Recall that

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

Thus,

$$x\mathsf{C}_{\mathfrak{p}} = \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{p}} xz_i^* \subseteq \mathcal{O}'_{\mathfrak{p}}.$$

The complementary module

Proof.

So far we proved that

$$\exists x \in \mathrm{E} \quad \text{s.t.} \quad x\mathrm{C}_{\mathfrak{p}} \subseteq \mathcal{O}'_{\mathfrak{p}}.$$

Recall that $\mathrm{C}_{\mathfrak{p}}$ is an $\mathcal{O}'_{\mathfrak{p}}$-module. It is easy to see that $x\mathrm{C}_{\mathfrak{p}}$ is also an $\mathcal{O}'_{\mathfrak{p}}$-module. But $x\mathrm{C}_{\mathfrak{p}} \subseteq \mathcal{O}'_{\mathfrak{p}}$ and so $x\mathrm{C}_{\mathfrak{p}}$ is an ideal of $\mathcal{O}'_{\mathfrak{p}}$.

Since $\mathcal{O}'_{\mathfrak{p}}$ is a PID (Theorem 18), we have that

$$x\mathrm{C}_{\mathfrak{p}} = y\mathcal{O}'_{\mathfrak{p}}$$

for some $y \in \mathcal{O}'_{\mathfrak{p}}$ and so

$$\mathrm{C}_{\mathfrak{p}} = \frac{y}{x}\mathcal{O}'_{\mathfrak{p}},$$

which concludes the proof. □

The complementary module

Claim 28

Let $t \in \mathsf{F}$ be s.t. $\mathsf{C}_{\mathfrak{p}} = t\mathcal{O}'_{\mathfrak{p}}$. Then,

$$\forall \mathfrak{P}/\mathfrak{p} \qquad v_{\mathfrak{P}}(t) \leq 0.$$

Proof.

Recall that $\mathcal{O}'_{\mathfrak{p}} \subseteq \mathsf{C}_{\mathfrak{p}}$ and so $\mathcal{O}'_{\mathfrak{p}} \subseteq t\mathcal{O}'_{\mathfrak{p}}$, namely,

$$\frac{1}{t}\mathcal{O}'_{\mathfrak{p}} \subseteq \mathcal{O}'_{\mathfrak{p}}.$$

Since $1 \in \mathcal{O}'_{\mathfrak{p}}$, we have that

$$\frac{1}{t} \in \mathcal{O}'_{\mathfrak{p}} = \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_{\mathfrak{P}}.$$

Thus, $\forall \mathfrak{P}/\mathfrak{p}$ we have that $v_{\mathfrak{P}}(\frac{1}{t}) \geq 0$ and so $v_{\mathfrak{P}}(t) \leq 0$, as required. □

The complementary module

Claim 29

Let $t \in \mathrm{F}$ be s.t. $\mathrm{C}_{\mathfrak{p}} = t\mathcal{O}'_{\mathfrak{p}}$. Then, for every $t' \in \mathrm{F}$,

$$\mathrm{C}_{\mathfrak{p}} = t'\mathcal{O}'_{\mathfrak{p}} \iff \forall \mathfrak{P}/\mathfrak{p} \;\; \upsilon_{\mathfrak{P}}(t') = \upsilon_{\mathfrak{P}}(t).$$

Proof.

In general, we have that

$$\begin{aligned} \forall \mathfrak{P}/\mathfrak{p} \;\; \upsilon_{\mathfrak{P}}\left(\frac{t}{t'}\right) \geq 0 \quad &\iff \quad \frac{t}{t'} \in \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_{\mathfrak{P}} = \mathcal{O}'_{\mathfrak{p}} \\ &\iff \quad t\mathcal{O}'_{\mathfrak{p}} \subseteq t'\mathcal{O}'_{\mathfrak{p}}. \end{aligned}$$

The complementary module

Proof.

So far, we showed that

$$\forall \mathfrak{P}/\mathfrak{p} \;\; v_{\mathfrak{P}}\left(\frac{t}{t'}\right) \geq 0 \quad \Longleftrightarrow \quad t\mathcal{O}'_{\mathfrak{p}} \subseteq t'\mathcal{O}'_{\mathfrak{p}}.$$

So,

$$\begin{aligned} \forall \mathfrak{P}/\mathfrak{p} \;\; v_{\mathfrak{P}}(t') = v_{\mathfrak{P}}(t) \quad & \Longleftrightarrow \quad \forall \mathfrak{P}/\mathfrak{p} \;\; v_{\mathfrak{P}}\left(\frac{t}{t'}\right) = 0 \\ & \Longleftrightarrow \quad t'\mathcal{O}'_{\mathfrak{p}} = t\mathcal{O}'_{\mathfrak{p}} = \mathsf{C}_{\mathfrak{p}}, \end{aligned}$$

which concludes the proof. □

Claim 30

For all but finitely many $\mathfrak{p}$, $\mathrm{C}_{\mathfrak{p}} = \mathcal{O}'_{\mathfrak{p}}$.

Proof. (addendum)

Let $z_1, \ldots, z_n$ be some basis of F/E with dual basis $z_1^*, \ldots, z_n^*$. Denote by $p_i(x) \in \mathrm{E}[x]$ the minimal polynomial of z_i over E. Similarly define $p_i^*(x) \in \mathrm{E}[x]$ to be the minimal polynomial of z_i^* over E.

Fix $i \in [n]$. Each coefficient of $p_i(x)$ is in E and so it has a finite number of poles. Let S_i be the union of poles taken over all coefficients of $p_i(x)$. Note that S_i is also finite.

Define S_i^* similarly and let

$$S = \bigcup_{i=1}^{n} (S_i \cup S_i^*).$$

The complementary module

Proof.

Take any prime divisor $\mathfrak{p} \notin S$. Then, each of z_i, z_i^* are integral over $\mathcal{O}_\mathfrak{p}$, namely, in $\mathcal{O}'_\mathfrak{p}$. Thus,

$$\sum_i \mathcal{O}_\mathfrak{p} z_i \subseteq \mathcal{O}'_\mathfrak{p}, \qquad \sum_i \mathcal{O}_\mathfrak{p} z_i^* \subseteq \mathcal{O}'_\mathfrak{p}.$$

By Claim 23 and since the dual of the dual basis is the original basis,

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

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

The complementary module

Proof.

Overall, we have that

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

and so all inclusions are equalities.

By Claim 26,

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

However, by the above equation,

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

and so $\mathsf{C}_\mathfrak{p} = \mathcal{O}'_\mathfrak{p}$, as required. □