Ramification Index, Residual Degree and the Fundamental Equality

Ramification Index and Residual Degree

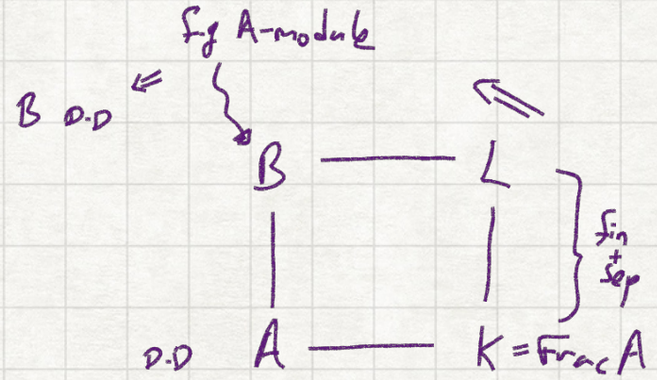
Opening Remarks

We'll consider a D.D A and $K = \mathrm{Frac}\, A$. Let L/K be finite (field) extension.

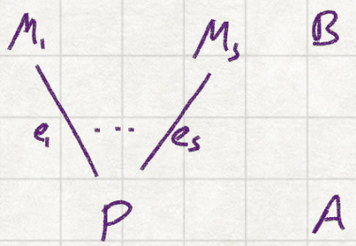
Let B be the integral closure of A in L.

Things are much nicer when B is a f.g A-module.

We proved that in such case B "inherits" A's D.D property. A specific case that is fairly easy to construct / verify which guarantees that B is a f.g. A-module is when L/K is a finite separable extension.



In such case (i.e. B is D.D) consider a prime ideal P of A. The ideal PB (the ideal generated by the elements of P in B) can be factored as $PB = \prod_{i=1}^{s} M_i^{e_i}$ in B (well, assuming $PB \neq B$ which we'll show to always hold).



We'll study this factorization of P in B in this unit (and a lot in the next course).

Lemma

A D.D with $K = \mathrm{Frac}\, A$. B i.c. of A in a finite extension L/K. Then, for every maximal ideal P of A, $PB \neq B$.

Proof

Assume first that $P = pA$ is principal. If $PB = B$ then $\exists b \in B$ s.t. $pb = 1$.

As $P \neq A$, $b \in B \setminus A$. $b \notin A$ is integral over A $\Rightarrow$ $\exists\, f(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_0 \in A[y]$ s.t. $f(b) = 0$ and $n > 1$. Take least such n. But $pb = 1$ yields

$$0 = pf(b) = pb^n + a_{n-1}pb^{n-1} + \cdots + a_0 p$$
$$= b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 + a_0 p$$

in contradiction to the min of n.

For a general prime P in the D.D A, observe that. $PB \neq B \iff (PA_P)B_P \neq B_P$

The fact that A is a D.D yields that A_P is a PID. ∎

Definition

With the notation of the previous lemma, $PB = M_1^{e_1} \cdots M_s^{e_s}$ $M_i \in \operatorname{Max} B$, $e_i \geq 1$.

The integer $e_i \triangleq e_{M_i/P}$ is called the ramification index of M_i over P.

Claim

With the notation above, $\forall i \in [s]$ $A \cap M_i = P$.

Proof

First, since $M_i \neq B$ $1 \notin M_i$ and so $M_i \cap A \neq A$. It is easy to see that $M_i \cap A$ is then a prime ideal of A. Clearly, $P \subseteq M_i \cap A$. As P max we get that $P = M_i \cap A$. ∎

Remark

Since $M_i \cap A = P$ the inclusion $A \subseteq B$ induces an injection

$$A/P \hookrightarrow B/M_i$$
$$a+P \longmapsto a+M_i$$

It is well-defined and indeed injection since $\forall a, a' \in A$

$$a+P = a'+P \iff a-a' \in P \iff a-a' \in M_i \iff a+M_i = a'+M_i$$

Since $P \in \operatorname{Max} A$, $M_i \in \operatorname{Max} B$, A/P and B/M_i are fields and by the above, B/M_i is a field extension of A/P (or of an isomorphic copy of the latter). Since B is a f.g A-module, this field extension is finite.

Definition

The field A/P is called <u>the residue field of A at P</u>. The integer $f_{M_i/P}$ is called <u>the residual degree of M_i over P</u>.

Example

Take $A=\mathbb{Z}$, $B=\mathbb{Z}[i]$ and consider the ideal $P=2\mathbb{Z}$. Observe that in $\mathbb{Z}[i]$, $2=i(i-1)^2$ and i is a unit. Now,

$$\mathbb{Z}[i]/_{\langle i-1\rangle} \cong \left(\mathbb{Z}[y]/_{\langle y^2+1\rangle}\right)/_{\langle y-1\rangle}$$

$$\cong \mathbb{Z}[y]/_{\langle y^2+1,\, y-1\rangle}$$

$$\cong \mathbb{Z}[y]/_{\langle 2,\, y-1\rangle} \qquad (y-1)^2 = y^2+1-2y$$

$$\cong \mathbb{Z}_2[y]/_{\langle y-1\rangle}$$

$$\cong \mathbb{Z}_2.$$

Since $\mathbb{Z}_2$ is a field, $M=(i-1)\mathbb{Z}[i]$ is max. So, $P\mathbb{Z}[i]=M^2$, $e_{M|P}=2$ and $f_{M|P}=1$ since the above computation also shows that the injection $\mathbb{Z}/_{2\mathbb{Z}} \hookrightarrow \mathbb{Z}[i]/_{M}$ is an isomorphism.

We'll now go in the othe direction - start with $M \in \operatorname{Max} B$ and consider $P \triangleq M \cap A$.

Claim

A D.D with $K = \operatorname{Frac} A$. Let L/K be a finite extension. Let B be the i.c. of A in L. Assume B f.g. A-module. Let $M \in \operatorname{Max} B$. Then $P \triangleq M \cap A$ is a max ideal of A.

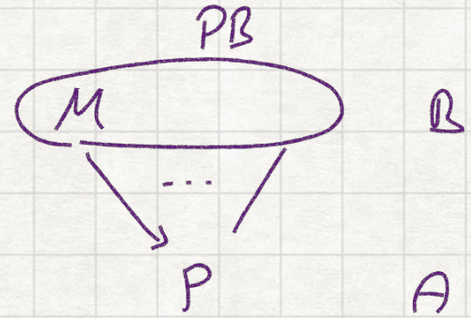
Proof

Clearly $P \neq A$. Further P is a prime ideal (e.g., by noting that $A/P \hookrightarrow B/M$ and B/M is a field and so A/P is a domain). To show $P \in \operatorname{Max} A$ we need to show $P \neq 0$. Take $0 \neq \alpha \in M$. $\exists f(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_0 \in A[y]$ s.t. $f(\alpha) = 0$. We may assume $a_0 \neq 0$ and n is minimal. But then $-a_0 = -\alpha^n - a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha \in M$ as $a_0 \in A$, $0 \neq a_0 \in P \Rightarrow P \neq 0 \Rightarrow P \in \operatorname{Max} A$.

∎

Definition

A D.D with $K = \mathrm{Frac}\, A$. Let L/K be a finite extension. Let B be the i.c. of A in L. Assume B f.g. A-module. Let $M \in \mathrm{Max}\, B$. Then, by the previous claim, $P = A \cap M \in \mathrm{Max}\, A$. We call the integer $\mathrm{ord}_M(PB)$ the ramification index of M over P and denote it by $e_{M/P}$.



The Fundamental Equality

Theorem

A D.D with $K = \mathrm{Frac}\, A$. Let L/K be a finite extension. Let B be the integral closure of A in L. If B is a f.g. A-module then for every $P \in \mathrm{Max}\, A$

$$[L:K] = \sum_{M \mid PB} e_{M/P} f_{M/P}.$$

Proof

B f.g. A-module + A D.D $\Rightarrow$ B D.D $\Rightarrow$ $PB = \prod_{i=1}^{s} M_i^{e_i}$. As $M_i^{e_i}$, $M_j^{e_j}$ coprime for $i \neq j$, CRT implies

$$B/PB \cong \left(B/M_1^{e_1}\right) \times \cdots \times \left(B/M_s^{e_s}\right).$$

Note that each of B/PB, $B/M_i^{e_i}$ is an (A/P)-module and hence (A/P)-vector space. Therefore, to prove the theorem it suffices to prove that:

1) $\dim_{A/P}\left(B/PB\right) = [L:K]$
2) $\dim_{A/P}\left(B/M_i^{e_i}\right) = e_i \dim_{A/P}\left(B/M_i\right)$ as indeed $\dim_{A/P}\left(B/M_i\right) = [B/M_i : A/P] = f_i$.

We first start with the case that both A, B are PID. As B is a domain B is a torsion free f.g. A-module, B is a free A-module.

Claim

B's rank is $n \triangleq [L:K]$.

Proof

Let $b_1, \dots, b_s$ be a basis of B over A. By clearing denominators, any K-linear relation among $b_1, \dots, b_s$ yields an A-linear relation and so rank $\leq [L:K]$.

We proved that every element of L is of the form $\frac{b}{a}$ $b \in B$, $a \in A$. Hence $b_1, \dots, b_s$ generate L as a K-vector space. ∎

Write $P = pA$. Then, $B/PB \cong \overbrace{A \oplus \cdots \oplus A}^{n} / pA \oplus \cdots \oplus pA \cong \overbrace{(A/p) \oplus \cdots \oplus (A/p)}^{n} = (A/p)^n$. Hence, $\dim_{A/P} B/PB = n$, proving (1).

To prove (2) assume $P \subseteq M^e$ so that B/M^e is an (A/P)-vector space. We prove by induction on e that $\dim_{A/P}(B/M^e) = e \cdot \dim_{A/P}(B/M)$.

$e=1$ is trivial. Consider the exact sequence

$$0 \longrightarrow M^{e-1}/M^e \longrightarrow B/M^e \longrightarrow B/M^{e-1} \longrightarrow 0$$

Claim (recall)

Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of A-modules.

Assume M is a f.g. free A-module. Then, $\operatorname{rank} M' + \operatorname{rank} M'' = \operatorname{rank} M$.

Thus, $\dim_{A/P}(B/M^e) = \dim_{A/P}(M^{e-1}/M^e) + \dim_{A/P}(B/M^{e-1})$. Thus, to prove (2) it suffices to show that

$(e-1)\dim_{A/P}(B/M)$

M^{e-1}/M^e is a (B/M)-vector space of dim n and so $\dim_{A/P}(M^{e-1}/M^e) = \dim_{A/P}(B/M)$.

Write $M = mB$. Consider the (B/M)-module hom

$$\psi : B/M \longrightarrow m^{e-1}/m^e$$

which is determined by $1+M \longmapsto m^{e-1}+m^e$. Note that

$$\forall b \in B \qquad \psi(b+M) = \psi((1+M)(b+M))$$

$$= (b+M)(m^{e-1}+m^e)$$

$$= bm^{e-1} + m^e$$

$\Rightarrow \psi$ is surjective (as $M^{e-1} = (mB)^{e-1} = m^{e-1}B$) and $\ker\psi = M$. Thus, $B/M \cong m^{e-1}/m^e$ as B/M-modules, and so since B/M is a field, $\dim_{B/M}(m^{e-1}/m^e) = 1$.

We now do not longer assume that A, B are PID. Write $S = A \setminus P$ and observe that S is a multiplicative subset of both A and B. As A D.D, $S^{-1}A = A_P$ is a PID with $\mathrm{Frac}\, A_P = K$. We further proved that $S^{-1}B$ is the i.c. of A_P in L.

Note that the only max ideals in B that do not intersect S are $M_1, \dots, M_s$. Hence, $S^{-1}B$ is a D.D. with only finitely many maximal ideals. As proven, this implies that $S^{-1}B$ is a PID.

Recall that $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$. As $S^{-1}M_1, \dots, S^{-1}M_s$ are all non-trivial maximal ideals in $S^{-1}B$ we have that

$$(S^{-1}P)(S^{-1}B) = \prod_{i=1}^{s} (S^{-1}M_i)^{e_i}.$$

$S^{-1}B$ being a DD has UFI and so $\uparrow$ is the factorization of $(S^{-1}P)(S^{-1}B)$ in $S^{-1}B$. As $S^{-1}A$, $S^{-1}B$ are PID we conclude that

$$[L:k] = \sum_{i=1}^{s} e_i f_i'$$

where $f_i' = \dim_{S^{-1}A/S^{-1}P} (S^{-1}B/S^{-1}M)$. The proof then follows from the following lemma.

Lemma

A ring. $P \in \mathrm{Max}\, A$. $S \subseteq A \setminus P$ mul. Then, $A/P \cong S^{-1}A/S^{-1}P$ as fields.

Remark

Note that this does indeed proves the theorem since it readily gives $A/P \cong S^{-1}A/S^{-1}P$. Moreover, it implies that $S^{-1}B/S^{-1}M_i \cong B/M_i$ since $S = A \setminus P \subseteq B \setminus M_i$ as indeed $P = M_i \cap A$.

Proof of Lemma

Observe that since $S \subseteq A \setminus P$, $S^{-1}P \in \mathrm{Max}(S^{-1}A)$. Hence, $S^{-1}A/S^{-1}P$ is indeed a field. Consider the composition

$$A \xhookrightarrow{j_S} S^{-1}A \xrightarrow{\pi} S^{-1}A/S^{-1}P$$

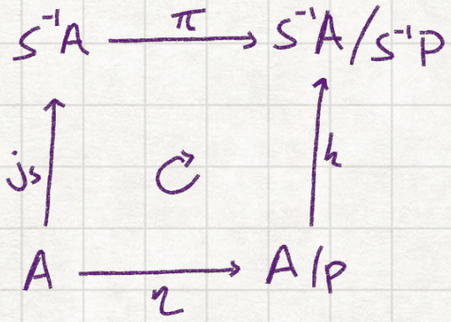
Observe that $(\pi \circ j_S)(P) = 0$ and so $\pi \circ j_S$ "factors through" $\eta : A \to A/P$.

That is, $\exists$ a (unique) ring hom $h: A/P \longrightarrow S^{-1}A/S^{-1}P$

s.t. $\pi \circ j_S = h \circ \eta$. Clearly $h \neq 0$ and so, since

A/P is a field, h is injective. To conclude,

we'll show h is surjective.



Take $\frac{a}{s} + S^{-1}P \in S^{-1}A/S^{-1}P$. Since $s \notin P$, P maximal

$P + sA = A \Rightarrow \exists\, t \in A$ s.t. $ts - 1 \in P$. Thus, $\frac{a(ts-1)}{s} \in S^{-1}P$. However,

$$\frac{a(ts-1)}{s} = \frac{at}{1} - \frac{a}{s} = h(at+P) - \frac{a}{s}.$$

That is, $h(at+P) + S^{-1}P = \frac{a}{s} + S^{-1}P$ and so h is surjective.

∎