Some contributions to the representation theory of orders over local factorial Krull domains

Von der Fakultät Mathematik und Physik
der Universität Stuttgart
zur Erlangung der Würde eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
genehmigte Abhandlung

Vorgelegt von
Joachim Ulrich Simon
geboren in Nürtingen

Hauptberichter:	Prof. Dr. K. W. Roggenkamp
Mitberichterin:	Prof. Dr. I. Reiten
Tag der mündlichen Prüfung:	22.09.2003

Institut für Algebra und Zahlentheorie
2003

Contents

Zusammenfassung

Hasse'sche Schiefkörper

Es sei R ein vollständiger diskreter Bewertungsring mit Primzahl π, Quotientenkörper K und einem endlichen Restklassenkörper $\mathfrak{k}$, dessen Mächtigkeit wir mit m bezeichnen. Die diskrete Bewertung auf K heiße ν. In der Arbeit [Has31] aus dem Jahr 1931 hat Helmut Hasse Schiefkörper D mit endlicher K-Dimension untersucht, deren Zentrum der Grundkörper K ist. Es sei $|D : K| = n^2$. Hasse's erste Beobachtung war, daß man die diskrete Bewertung ν eindeutig zu einer "diskreten Bewertung" $\tilde{\nu}$ auf D fortsetzten kann. Für ein beliebiges Element $d \in D$ setzt man $\tilde{\nu}(d) := \frac{1}{|D:K|}\nu(\mathrm{N}_{D/K}(d)) \in \mathbb{Q} \cup \{\infty\}$, wobei $\mathrm{N}_{D/K}$ die Normabbildung von D über K sei. Die Existenz und die Eindeutigkeit von $\tilde{\nu}$ bestimmt in starker Weise die Struktur des Schiefkörpers D. Das erste wichtige Resultat ist, daß die ganzen Elemente in D einen Ring bilden, d.h. daß nur eine eindeutige bestimmte Maximalordnung Δ in D existiert. Mittels $\tilde{\nu}$ kann die Maximalordnung als eine Art nichtkommutativer diskreter Bewertungsring beschrieben werden. Die Bewertungsgruppe von $\tilde{\nu}$ ist $\frac{1}{e}\mathbb{Z}$ für ein $1 \leq e \in \mathbb{N}$. Es ist üblich zur äquivalenten Bewertung $\nu_D := e\tilde{\nu}$ überzugehen. Ein Element $\pi_D \in \Delta$ mit $\nu_D(\pi_D) = 1$ wird eine Primzahl von Δ genannt. Jedes einseitige Ideal J von Δ ist zweiseitig; es existiert ein $k \in \mathbb{N}$ mit $J = {\pi_D}^k\Delta = \Delta{\pi_D}^k$. Somit ist Δ ein lokaler Ring und $\bar{\Delta} := \Delta/\pi_D\Delta$ ein Schiefkörper über $\mathfrak{k}$. Man nennt $f := |\bar{\Delta} : \mathfrak{k}|$ den Trägheitsgrad von Δ über K. In Δ existiert eine Primzahl, die der Bedingung π_D mit ${\pi_D}^n = \pi$ genügt und für die es ein zu n teilerfremdes $r \in \mathbb{N}$ mit $\pi_D\omega{\pi_D}^{-1} = \omega^{m^r}$ gibt. Die Zahl r ist eindeutig bestimmt und der Bruch $\frac{r}{n}$ heißt die Hasse Invariante von D. In D ist eine $(m^f - 1)$-te primitive Einheitswurzel ω enthalten. Den bis auf Konjugation eindeutig bestimmten Körper $W := K(\omega)$ nennt man einen Trägheitskörper von D. $S := \mathrm{alg.int.}_R(W)$ ist ein diskreter Bewertungsring mit Primzahl π. Der Restklassenkörper von S werde mit $\mathfrak{k}'$ bezeichnet. Für jede Hasse Invariante existiert ein zugehöriger Schiefkörper, den man durch eine Matrixdarstellung über seinem Trägheitskörper konstruieren kann. Wir werden dies später in einem allgemeineren Rahmen tun. Es zeigt sich, daß diese Schiefkörper eine vollständige Liste aller Schiefkörper mit Zentrum K und endlicher K-Dimension bilden. Unser erstes Ziel wird es sein, solch einen Schiefkörper zu einem Schiefkörper über dem Polynomring $R[q]$, bzw. über dem Funktionenkörper $K(q)$ zu heben; hierzu wird sich die Sprache der Brauergruppen als nützlich erweisen.

Brauer Gruppen – Verschränkte Produkt Algebren – Zyklische Algebren und Ordnungen

Es seien F ein beliebiger Körper und A und B zwei zentral-einfache F-Algebren. Man nennt A und B ähnlich, falls die Schiefkörperkomponenten von A und B isomorph sind. In diesem Fall schreiben wir $A \sim B$. Die Äquivalenzklasse von A wird mit $[A]$ bezeichnet.

Satz

1. *Es sei* $B(F) := \{[A] \mid A \text{ ist eine zentral-einfache } F\text{-Algebra}\}$. *Die folgende Multiplikation auf* $B(F)$ *ist wohldefiniert und macht* $B(F)$ *zu einer Abelschen Gruppe:*
$$[A][B] := [A \otimes_F B] \quad \text{für alle } [A], [B] \in B(F).$$
$B(F)$ *heißt die Brauer-Gruppe von* F. *Für* $[A] \in B(F)$ *gilt* $[A]^{-1} = [A^{op}]$.

2. *Es sei* L/K *eine Körpererweiterung. Die Abbildung*
$$\Phi_{L/F} : B(F) \ni [A] \longmapsto [L \otimes_F A] \in B(L)$$
ist ein wohldefinierter Gruppenhomomorphismus. Der Kern von $\Phi_{L/F}$ *wird mit* $B(L/F)$ *bezeichnet und heißt die relative Brauer-Gruppe von* L/F.

3. *Mit* $\mathcal{G} := \{L \mid L \text{ ist eine endliche Galois-Erweiterung von } F\}$ *gilt*
$$B(F) = \bigcup_{L \in \mathcal{G}} B(L/F).$$

Es sei L/F eine Galois-Erweiterung mit Gruppe G. Die relative Brauer-Gruppe $B(L/F)$ kann mit Hilfe kohomologischer Methoden beschrieben werden. Die multiplikative Gruppe $L^\times$ ist ein G-Modul. Für $\Psi \in \mathrm{C}^2(G, L^\times)$ wird die zentral-einfache F-Algebra $(L/F, \Psi)$ wie folgt erklärt:

1. Als L-Vektorraum hat $(L/F, \Psi)$ eine Basis der Form $\{u_\sigma \mid \sigma \in G\}$.
2. Die Multiplikation wird durch die folgenden beiden Vorschriften erklärt:
   - $u_\sigma l = \sigma(l) u_\sigma \quad \forall l \in L \, \forall \sigma \in G.$
   - $u_\sigma u_\tau = \Phi(\sigma, \tau) u_{\sigma\tau} \quad \forall \sigma, \tau \in G.$

$(L/F, \Psi)$ heißt verschränkte Produktalgebra.

Satz *Es seien* $\Psi, \Phi \in \mathrm{C}^2(G, L^\times)$. *Die Algebren* $(L/K, \Psi)$ *und* $(L/K, \Phi)$ *sind genau dann isomorph, wenn die Kohomologieklassen* $[\Phi]$ *und* $[\Psi]$ *in* $\mathrm{H}^2(G, L^\times)$ *übereinstimmen. Die folgende Abbildung ist ein Isomorphismus von Abelschen Gruppen:*
$$\begin{aligned} \mathcal{B} : \mathrm{H}^2(G, L^\times) &\longrightarrow B(L/K) \\ [\Psi] &\longmapsto [(L/K, \Psi)]. \end{aligned}$$

Es seien $W = K(\omega)$ ein Trägheitskörper eines Hasse'schen Schiefkörpers D und $\sigma : K(\omega) \ni \omega \longmapsto \omega^m \in K(\omega)$ der Frobenius-Homomorphismus von W/K. Die Galois-Gruppe von W/K ist zyklisch mit Generator σ. Von nun an sei L/F eine *zyklische* Galois-Erweiterung vom Grad n mit Gruppe $G = \langle\tau\rangle$. Für $a \in F^\times$ setzt man $\Phi_a : G \times G \longrightarrow L^\times$ mit $\Phi_a(\tau^i, \tau^j) := \begin{cases} 0 \text{ für } i + j \leq n - 1 \\ a \text{ für } i + j \geq n \end{cases}$.

Definition *Es sei* $a \in K^\times$. *Die verschränkte Produktalgebra* $(L/F, \Phi_a)$ *nennt man eine zyklische Algebra und bezeichnet sie mit* $(L/F, \tau, a)$.

Satz *Für* $\Phi \in \mathrm{C}^2(G, L^\times)$ *existiert ein* $a \in F^\times$ *mit* $(L/F, \Phi) \simeq (L/F, \tau, a)$.

Es sei $A := (L/F, \tau, a)$ eine zyklische Algebra mit Basis $\{\nu_{\tau^i}\}$; $\nu := \nu_\tau$. Dann:

1. $\nu^i = \nu_{\tau^i}$ für $0 \leq i \leq n-1$.
2. Die Beziehungen

$$\nu^n = \nu^{n-1}\nu = \nu_{\tau^{n-1}}\nu_\tau = \Phi_a(\tau^{n-1}, \tau^1)\nu_{\tau^n} \underset{n-1+1=n\geq n-1}{=} a\nu_{\mathrm{id}} = a$$

zeigen, daß es einen Isomorphismus $(L/F, \tau, a) \simeq L[x, \tau]/\langle x^n - a\rangle$ gibt, wobei $L[x, \tau]$ den getwisteten Polynomring bezeichne.

Die zyklische Algebra A hat eine Matrixdarstellung.

Lemma *Für $l \in L$ sei* $\tilde{l} := \begin{pmatrix} l & & \\ & \tau(l) & \\ & & \ddots \\ & & & \tau^{n-1}(l) \end{pmatrix} \in M_n(L)$; $\nu^* := \begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ a & 0 & \dots & 0 \end{pmatrix} \in M_n(L)$.

Die Abbildung

$$\Gamma : (L/F, \sigma, a) \longrightarrow \bigoplus_{i=0}^{n-1} L(\nu^*)^i$$
$$\sum_{i=0}^{n-1} l_i\nu^i \longmapsto \sum_{i=0}^{n-1} \tilde{l}_i(\nu^*)^i$$

ist ein Isomorphismus von F-Algebren.

Es sei weiterhin T ein Integritätsbereich mit Quotientenkörper F und $U := \mathrm{alg.int.}_T(L)$. Für $a \in T \setminus \{0\}$ definiert man die T-Algebra $(U/T, \tau, a)$ analog zur zyklischen Algebra $(L/F, \tau, a)$, d.h.

$$(U/T, \tau, a) := \bigoplus_{i=0}^{n-1} U\lambda^i, \quad \text{mit} \quad (L/F, \tau, a) = \bigoplus_{i=0}^{n-1} L\lambda^i.$$

$(U/T, \tau, a)$ heißt eine zyklische T-Algebra. Durch Einschränken der Matrix Darstellung von $(L/F, \tau, a)$ auf $(U/T, \tau, a)$ erhält man eine Matrix Darstellung von $(U/T, \tau, a)$. Eines von Hasse's Hauptergebnissen läßt sich umformulieren zu

Satz *Es seien φ die Eulersche Phi Funktion und $1 \leq \alpha_1, \dots, \alpha_{\varphi(n)} \leq n$ die $\varphi(n)$ Werte, die relativ prim zu n sind. Die $\varphi(n)$ zyklischen Algebren $(W/K, \rho, \pi^{\alpha_i})$ stellen einen vollständigen Satz paarweiser nicht isomorpher Schiefkörper mit Zentrum K und Index n dar.*

Für unsere Zwecke ist es geschickt zu einer anderen Darstellung der Hasse'schen Schiefkörper überzugehen.

Lemma *Die $\varphi(n)$ zyklischen Algebren $(W/K, \rho^{\alpha_i}, \pi)$ bilden ebenfalls einen vollständigen Satz paarweiser nicht isomorpher Schiefkörper mit Zentrum K und Index n. Wir nennen diese Darstellungen die Standarddarstellungen der Hasse'schen Schiefkörper.*

Lifts

Definition eines Lifts

Nun können wir unsere Definition eines Lifts geben:

Definition *Es sei $0 \neq a \in T$ ein beliebiges Element. Wir setzen $\Lambda := (U/T, \tau, a)$ und $A := (L/F, \tau, a)$. Ein Lift von A ist eine zyklische $L(q)$-Algebra A_f, die den folgenden beiden Bedingungen genügt:*

- *$A_f = L(q)\Lambda_f$ für $\Lambda_f = (U[q]/T[q], \tau, f)$ mit $f \in T[q]$ (somit enthält A_f die zyklische $T[q]$-Ordnung Λ_f).*
- *$\Lambda_f/q\Lambda_f = (U/T, \tau, a)$.*

Für den Spezialfall der Hasse'schen Schiefkörper erhält man

Korollar *Ein Lift der Standarddarstellung eines Hasse'schen Schiefkörpers D ist von der Form $D_h := W(q)\Lambda_h$ mit $\Lambda_h = (S[q]/R[q], \sigma, h)$, wobei $h \in R[q]$ und $h(0) = \varepsilon\pi$ gelten sollen, sodaß ε eine Einheit von R ist. Das Polynom h ist von der Form gf mit f irreduzibel in $S[q]$ und $f(0)$ ist eine Primzahl von R von der wir o.B.d.A. annehmen können daß sie gleich π ist und $g(0)$ ist eine Einheit von R.*

Lifts sind Schiefkörper

Wir betrachten die Standarddarstellung eines Hasse'schen Schiefkörpers D und einen Lift D_f dieser Standarddarstellung. Es ist $D_f = W(q)\Lambda_f$ mit $\Lambda_f = (S[q]/R[q], \sigma, f)$, sodaß $f \in R[q]$ mit $f(0) = \varepsilon\pi$ erfüllt ist, wobei ε eine Einheit von R ist. Wir können jedoch O.B.d.A. annehmen, daß $f(0) = \pi$ gilt.

Satz 3.16 *Die Algebra D_f ist ein Schiefkörper, d.h.* jeder *Lift eines Hasse'schen Schiefkörpers ist wieder ein Schiefkörper.*

Der letzte Satz ist eine direkte Konsequenz aus dem folgenden Lemma, welches natürlich nicht auf den Spezialfall von Hasse'schen Schiefkörpern beschränkt ist.

Lemma 3.20 *Es sei T ein kommutativer Noetherscher Integritätsbereich mit Quotientenkörper F und Λ eine T-Ordnung in einer F-Algebra A. Es sei $q \in T$ eine Nichteinheit. Wenn $\Lambda/q\Lambda$ keine Nullteiler hat, dann ist A ein Schiefkörper.*

Das letzte Lemma konnte zum folgenden Satz verallgemeinert werden.

Satz 3.21 *Es sei T ein Noetherscher kommutativer Integritätsbereich mit Quotientenkörper F. Desweiteren sei Λ eine T-Ordnung in einer F-Algebra A. Es sei $\mathfrak{a} \neq T$ ein invertierbares Ideal. Wenn $\Lambda/\mathfrak{a}\Lambda$ keine Nullteiler hat, dann ist A ein Schiefkörper.*

Lifts der Maximalordnung

Es seien D ein Hasse'scher Schiefkörper und $D_f = W(q)\Lambda_f$ ein Lift. Wir nennen die Ordnung $\Lambda_f = (S[q]/R[q], \sigma, f)$ einen Lift der Maximalordnung. Wir wollen nun entscheiden, wann dieser Lift wieder eine Maximalordnung ist. Um festzustellen, wann Λ_f maximal ist, verwenden wir ein Resultat, welches auf Auslander und Goldmann zurückgeht (siehe [AG60, Theorem 1.17]).

Satz4.3 *Es seien T ein ganz abgeschlossener Noetherscher Integritätsbereich mit Quotientenkörper F und Γ eine T-Ordnung in einer zentral-einfachen F-Algebra B. Die folgenden Aussagen sind äquivalent:*

1. *Γ ist eine maximale T-Ordnung.*
2. *Γ genügt den folgenden zwei Bedingungen:*
   - $\Gamma^{**} = \Gamma$.
   - *Für jedes $\mathfrak{p} \in ht^1(T)$ ist $\Gamma_\mathfrak{p}$ eine maximale $T_\mathfrak{p}$-Ordnung.*

Maximale Lifts der Maximalordnung

Hier betrachten wir Lifts der Form $D_{\tilde{f}} := W(q)(S[q]/R[q], \sigma, \tilde{f})$ mit $\tilde{f} = \left(\prod_{i=1}^{t} g_i\right) f$. Hierbei sei f irreduzibel in $S[q]$ mit $f(0) = \pi$. Die g_i's sind paarweise verschiedene in $S[q]$-irreduzible Polynome mit folgenden Eigenschaften:

- $g_i(0) = \varepsilon_i \in R^\times$ für $1 \leq i \leq t$, somit insbesondere $fR[q] \neq g_i R[q]$ für alle i.
- Die Primideale $g_i R[q]$ sind paarweise verschieden.

In diesem Fall ist $\Lambda_{\tilde{f}} := (S[q]/R[q], \sigma, \tilde{f})$ eine Maximalordnung. Hierfür reicht es zu zeigen, daß $\Lambda_{\tilde{f}}$ die beiden Bedingungen aus Satz 4.3 erfüllt. Der erste Punkt ist automatisch erfüllt, da $\Lambda_{\tilde{f}}$ frei über $R[q]$ ist. Der zweite Punkt beruht wieder auf einem Resultat von Auslander und Goldmann (cf. [AG60, Theorem 2.3]):

Satz 4.4 *Es seien T ein diskreter Bewertungsring mit Quotientenkörper F und Γ eine T-Ordnung in einer zentral-einfachen F-Algebra B. Γ ist genau dann maximal, wenn die folgenden Bedingungen erfüllt sind:*

- *Γ ist erblich.*
- *$rad(\Gamma)$ ist das eindeutig bestimme maximale zweiseitige Ideal von Γ.*

Es sei $\mathfrak{p} \in \mathrm{ht}^1(R)$. Die Ordnung $\Lambda_{\tilde{f},\mathfrak{p}}$ genügt Satz 4.4:

- Wir verwenden nochmals ein Resultat von Auslander und Goldmann (siehe [AG60, Corollary to Theorem 2.2]):

  Lemma 4.5 *Es seien T ein diskreter Bewertungsring und Γ eine T-Algebra, die als T-Modul endlich erzeugt und torsionsfrei ist. Wenn $rad(\Gamma)$ projektiv ist, dann ist Γ ein erblicher Ring.*

  Mit Lemma 4.5 reicht es zu zeigen, daß $\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ projektiv über $\Lambda_{\tilde{f},\mathfrak{p}}$ ist.

- Um nachzuweisen, daß $\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ das eindeutig bestimmte maximale zweiseitige Ideal von $\Lambda_{\tilde{f},\mathfrak{p}}$, zeigen wir, daß die Quotienten $\overline{\Lambda_{\tilde{f},\mathfrak{p}}} := \Lambda_{\tilde{f},\mathfrak{p}}/\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ einfache Algebren sind.

Um die Struktur der Ordnungen $\Lambda_{\tilde{f},\mathfrak{p}}$ zu klären, müssen wir drei Fälle unterscheiden. Zur Vereinfachung dieser Rechnungen können wir o.B.d.A. annehmen, daß $\tilde{f} = f$ ein irreduzibles Polynom in $S[q]$ ist (siehe Beobachtungen 4.82). Da Λ_f eine zyklische Ordnung ist, existiert ein $\lambda \in \Lambda_f$ mit

- $\Lambda = \bigoplus_{i=0}^{n-1} S[q]\lambda^i$,
- $\lambda^n = f$ und $\lambda y = \sigma(y)\lambda$ für alle $y \in S[q]$.

1. Fall: $\mathfrak{p} = fR[q]$

Lemma 4.84 *Es sei $\mathfrak{p} = fR[q]$. Dann ist $rad(\Lambda_{f,\mathfrak{p}}) = \lambda\Lambda_{f,\mathfrak{p}}$ projektiv über Λ und das eindeutig bestimmte maximale zweiseitige Ideal von Λ.*

Zum Beweis von Lemma 4.84 betrachtet man die folgende Situation, die $\Lambda_{f,\mathfrak{p}}$ erfüllt: Es sei T ein beliebiger diskreter Bewertungsring mit Primzahl p und Quotientenkörper F. T braucht *nicht* vollständig zu sein. L/F sei eine zyklische Galois-Erweiterung vom Grad n mit Gruppe $G := \langle\tau\rangle$. Wir setzen $U :=$ alg. $\mathrm{int}._T(L)$ und nehmen an, daß U auch ein diskreter Bewertungsring mit Primzahl p ist. Es sei $\Gamma := (U/T, \tau, p) = \bigoplus_{i=0}^{n-1} U\gamma^i$. Um Determinanten verwenden zu können, geht man zu einer Matrixdarstellung von Γ über und zeigt folgendes Lemma.

Lemma 4.19

1. *Es sei $I \subset \Gamma$ ein Linksideal, dann gibt es ein $k \in \mathbb{N}$ mit $I = \Gamma\gamma^k$.*
2. *Es sei $I \subset \Gamma$ ein Rechtsideal, dann gibt es ein $l \in \mathbb{N}$ mit $I = \gamma^l\Gamma$.*
3. *Für jedes $k \in \mathbb{N}$ gilt $\gamma^k\Gamma = \Gamma\gamma^k$, d.h. jedes einseitige Ideal von Γ ist auch ein zweiseitiges.*
4. *Es gilt $rad(\Gamma) = \gamma\Gamma = \Gamma\gamma$ und Γ ist ein lokaler Ring, also ist $rad(\Gamma)$ insbesondere das eindeutige maximale zweiseitige Ideal von Γ.*

Lemma 4.84 induziert, daß $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ das eindeutige maximale zweiseitige Ideal von $\Lambda_{f,\mathfrak{p}}$ ist. Desweiteren liefert Lemma 4.84 auch, daß $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ ein projektiver $\Lambda_{f,\mathfrak{p}}$-Modul ist und somit ist $\Lambda_{f,\mathfrak{p}}$ erblich.

2. Fall: $\mathfrak{p} = hR[q]$ **mit** $\deg(h) \geq 1$

Es existiert ein Element $\alpha \in \mathbb{N}$ welches n teilt und ein irreduzibles Polynom $g \in S[q]$, so daß $h = g\sigma(g)\cdots\sigma^{\alpha-1}(g)$ erfüllt ist (siehe Kapitel 4.3). Es sei a eine gemeinsame Nullstelle der Polynome h und g in irgendeiner algebraischen Erweiterung von W. Es ist $f + hK[q] \neq 0$ und mittels eines Isomorphismus $K[q]/hK[q] \simeq K(a)$ kann man $f + hK[q]$ mit einem Element $0 \neq b \in K(a)$ identifizieren.

Lemma 4.87

1. *$rad(\Lambda_{f,\mathfrak{p}}) = \mathfrak{p}\Lambda_{f,\mathfrak{p}}$ und*
2. *$\Lambda_{f,\mathfrak{p}}/rad(\Lambda_{f,\mathfrak{p}}) \simeq M_\alpha((W(a)/K(a), \sigma^\alpha, b)$.*

Um Lemma 4.87 zu beweisen, wird eine zweiseitige Pierce-Zerlegung auf den Quotienten $\Lambda_{f,\mathfrak{p}}/\mathfrak{p}\Lambda_{f,\mathfrak{p}}$ angewendet (siehe Abschnitt 4.5). Hier geht ein, wie sich der Galois Automorphismus bei Konjugation mit dem Isomorphismus $S[q]_\mathfrak{p}/\mathfrak{p}S[q]_\mathfrak{p} \simeq \prod_{i=0}^{\alpha-1} S[q]_\mathfrak{p}/\sigma^i(g)S[q]_\mathfrak{p}$, der vom Chinesischen Restsatz herkommt, verhält (siehe Abschnitt 4.4).

Mit Lemma 4.87 erhält man, daß $\mathrm{rad}(\Lambda_{f,\mathfrak{p}}) = g\Lambda_{f,\mathfrak{p}}$ projektiv über $\Lambda_{f,\mathfrak{p}}$ ist und das eindeutige maximal zweiseitige Ideal von $\Lambda_{f,\mathfrak{p}}$ ist, da $M_\alpha((L(a)/K(a), \sigma^\alpha, b)$ einfach ist. Also ist $\Lambda_{f,\mathfrak{p}}$ ist eine maximale $R[q]_\mathfrak{p}$-Ordnung.

3. Fall: $\mathfrak{p} = \pi R[q]$

Lemma 4.89

1. *rad*$(\Lambda_{f,\mathfrak{p}}) = \mathfrak{p}\Lambda_{f,\mathfrak{p}}$
2. $\Lambda_{f,\mathfrak{p}}/rad(\Lambda_{f,\mathfrak{p}}) \simeq (\mathfrak{k}'(q)/\mathfrak{k}(q), \bar{\sigma}, \bar{f})$, *wobei* $\bar{\sigma}$ *der Automorphismus von* $\mathfrak{k}'$ *der von* σ *induziert wird und* $\bar{f} := f + \pi R[q]$. *Da* f *primitiv ist, ist insbesondere* $\bar{f}$ nicht *das Nullelement.*

Der Beweis von Lemma 4.89 basiert hauptsächlich auf

Korollar 4.80 *Die Körpererweiterung* $\mathfrak{k}'(q)/\mathfrak{k}(q)$ *ist Galois vom Grad* n *und es existiert ein Isomorphismus* $Gal(\mathfrak{k}'(q)/\mathfrak{k}(q)) \simeq Gal(L/K)$.

$\mathrm{rad}(\Lambda_{f,\mathfrak{p}}) = \pi\Lambda_{f,\mathfrak{p}}$ ist projektiv über $\Lambda_{f,\mathfrak{p}}$ und somit $\Lambda_{f,\mathfrak{p}}$ erblich. $\Lambda_{f,\mathfrak{p}}/\mathfrak{p}\Lambda_{f,\mathfrak{p}}$ ist eine verschränkte Produktordnung im Bezug auf die Galois-Erweiterung $\mathfrak{k}'(q)/\mathfrak{k}(q)$ ist, d.h. insbesondere eine einfache Algebra. Somit ist $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ das eindeutig bestimmte maximale zweiseitige Ideal von $\Lambda_{f,\mathfrak{p}}$.

Nicht maximale Lifts der Maximalordnung

Nun betrachten wir Lifts eines Hasse'schen Schiefkörpers D, die die Form $D_{hf} := W(q)(S[q]/R[q], \sigma, hf)$ mit $f(0) = \pi$ und $h(0) \in R^\times$ haben. Zumindest eine der folgenden beiden Bedingungen sei erfüllt:

- $h = \tilde{h}g^s$ für ein Polynom $\tilde{h}$ mit $g \notin R^\times = R[q]^\times$ und $s \geq 2$.
- $h = \tilde{h}g$ für ein Polynom $\tilde{h}$ und g ist nicht irreduzibel in $S[q]$.

In diesen Fällen ist $\Lambda_{fh} := (S[q]/R[q], \sigma, hf)$ *keine* Maximalordnung (siehe Satz 5.25).

Der Beweis dieses Satzes beruht auf verschiedenen Beobachtungen, die wir in Kapitel 5 gemacht haben.

Abgeschnittene getwistete Polynomringe und ihre Kohomologieringe

Motivation

Es sei $D_f = W(q)\Lambda_f$ ein Lift eines Hasse'schen Schiefkörpers D, wobei gelten soll: $\Lambda_f = (S[q]/R[q], \sigma, f)$ und $f \in R[q]$ mit $f(0) = \pi$. Wir können Spezialisierungen von Λ_f, d.h. Quotienten der Form $\Lambda_a := \Lambda_f/(q-a)\Lambda_f$ mit $a \in R$ betrachten. Dann gibt es einen Isomorphismus $\Lambda_a \simeq (S/R, \sigma, f(a))$. Es sei a eine Nullstelle von f. In dieser Situation existiert ein Isomorphismus $K\Lambda_a \simeq K[x,\sigma]/(x^n)$, wobei $K[x,\sigma]$ den getwisteten Polynomring bezeichne. Somit ist es natürlich, abgeschnittene getwistete Polynomringe zu betrachten und zu untersuchen, wie weit diese davon entfernt sind, halbeinfach zu sein.

Grundlegendes

Es sei L/F eine beliebige endliche Galois-Erweiterung vom Grad d und $\mathrm{id} \neq \tau$ ein Element der Galois-Gruppe und $2 \leq k \in \mathbb{N}$. Wir bezeichnen mit L_τ den Fixkörper von τ und setzen $A := L[x,\tau]/\langle x^k \rangle$ und $N := x + \langle x^k \rangle \in A$. Es gelten:

1. A ist ein lokaler Ring.
2. Der Modul $S := A/AN$ ist bis auf Isomorphie der einzige einfache A-Modul.
3. Es gibt einen Isomorphismus $S = A/AN \simeq AN^{k-1}$ als A-Moduln.
4. A ist bis auf Isomorphismus der einzige projektiv unzerlegbare A-Modul.
5. Das Zentrum $\mathrm{C}(A)$ von A ist L_τ.

Projektive Auflösungen und Ext-Gruppen

Für $0 \leq i \leq k-1$ wird $\rho_i \in \mathrm{End}_A(S)$ durch

$$\rho_i : A \ni a \longmapsto aN^i \in A$$

definiert. Der Kern von ρ_i ist gleich AN^{k-i}.

Lemma 6.12 *Folgende Sequenz ist eine projektive Auflösung des einfachen A-Moduls S:*

$$\mathcal{P}_0 \cdots\cdots \xrightarrow{\rho_1} A \xrightarrow{\rho_{k-1}} A \xrightarrow{\rho_1} A \xrightarrow{\rho_{k-1}} S \longrightarrow 0,$$

wobei wir S mit AN^{k-1} identifizieren. Für $k = 2$ gilt $k-1 = 2-1 = 1$ und somit $\rho_1 = \rho_{k-1}$. D.h. für $k = 2$ ist die Sequenz periodisch mit Periode 1, in allen anderen Fällen hat sie Periode 2.

Korollar

1. *Es gilt $pdim_A(S) = \infty$ und*
2. *$gl.dim(A) = \infty$.*

Somit ist A in einem gewissen Sinne so weit wie möglich davon entfernt halbeinfacher zu sein. Die Ext-Gruppen $\mathrm{Ext}^i_A(S,S)$ sind Hom's.

Lemma 6.19 *Für $i \in \mathbb{N}$ gilt* $\mathrm{Ext}^i_A(S,S) = \mathrm{Hom}_A(A,S)$.

Kohomologieringe

Wir setzen $\mathrm{ext}_A^*(S,S) := \bigoplus_{i\in\mathbb{N}} \mathrm{ext}_A^i(S,S)$, ein graduierter assoziativer Ring mit komponentenweiser Addition und einer vom Yoneda-Produkt induzierten Multiplikation. Dieser Ring heißt der Kohomologiering von S, er kann kanonisch mit dem Ring $\mathrm{Ext}_A^*(S,S) := \bigoplus_{i\in\mathbb{N}} \mathrm{ext}_A^i(S,S)$ identifiziert werden (siehe Kapitel 7, insbesondere Abschnitt 7.2).

Die Homomorphismen $\varphi_1 \in \mathrm{Hom}_A(A,S) = \mathrm{Ext}_A^i(S,S)$ mit $\varphi_1 : A \ni 1 \longmapsto N \in S$ werden mit f_1^i bezeichnet. Somit erhält man

$$\mathrm{Ext}_A^*(S,S) = \bigoplus_{i\in\mathbb{N}} \mathrm{Ext}_A^i(S,S) = \bigoplus_{i\in\mathbb{N}} L\,\mathrm{f}_1^i\,.$$

Der Fall $k = 2$

In diesem Fall gilt das

Korollar 7.22 *Es gibt einen Isomorphismus* $\mathrm{Ext}_A^*(S,S) \simeq L[y,\tau]$.

Der Fall eines beliebigen $k \geq 3$

Wir setzen $B := \mathrm{Ext}_A^*(S,S) = \bigoplus_{i\in\mathbb{N}} L\,\mathrm{f}_1^i$. Das Ideal $N := \bigoplus_{j \text{ ungerade}} L\,\mathrm{f}_1^j$ ist Abelsch. Mit der Notation $\tilde{\tau} := \tau^k$ erhält man:

Lemma 7.29 $B_0 := \bigoplus_{j\ gerade} L\,\mathrm{f}_1^j = \bigoplus_{t\in\mathbb{N}} L\,\mathrm{f}_1^{2t}$ *ist ein Teilring von* B *und es gibt einen Isomorphismus* $B_0 \simeq L[y,\tilde{\tau}]$.

Lemma 7.31 *Es sei* $V := L^{(\mathbb{N})} = \bigoplus_{i\in\mathbb{N}} Lf_i$. *Für* $i \in \mathbb{N}$ *setzen wir* $e_{2i+1} := f_i$ *und betrachten von nun an die Basis* $\{e_{2i+1} \,|\, i \in \mathbb{N}\}$. *Es seien* $v = \sum_i \alpha_i e_{2i+1} \in V$ *und* $f = \sum_j \beta_j y^j \in L[y,\tilde{\tau}]$ *beliebige Elemente.*

1. *Eine Linksoperation von* $L[y,\tilde{\tau}]$ *auf* V *ist durch die folgende Vorschrift gegeben:*

$$fv := \sum_{i,j} \tilde{\tau}^i(\alpha_j)\beta_i e_{2i+2j+1}.$$

2. *Die Regel*

$$vf := \sum_{i,j} \alpha_i \tilde{\tau}^i(\tilde{\tau}(\beta_j)) e_{2i+2j+1}$$

liefert eine Rechtsoperation von $L[y,\tilde{\tau}]$ *auf* V.

3. *Mit diesen Operationen wird* V *zu einem Bimodul der* F*-Algebra* $L[y,\tilde{\tau}]$.

B kann als ein semidirektes Produkt interpretieren werden.

Satz 7.33 *Mit den Bezeichnungen der Lemmata 7.29 und 7.31 gilt* $V \rtimes B_0 \simeq V \rtimes L[y,\tilde{\tau}] \simeq B$ *als* F*-Algebren.*

Für den Spezialfall $\tau^k = \tilde{\tau} = 1$ gilt darüberhinaus:

1. $B_0 \simeq L[y,\tau^k] = L[y]$ ist kommutativ.

2. Es sei $S : V \ni e_{2i+1} \longmapsto e_{2(i+1)+1} \in V$ der Rechtsshift auf V. Für $f = \sum_i \alpha_i y^i \in L[y]$ setzen wir $f(S) := \sum_i \alpha_i S^i$ und $\tau(f) := \sum_i \tau(\alpha_i) y^i$. Dann schreiben sich Links- und Rechtsoperation von $L[y]$ auf V als:

   - Linksoperation: $fv = (f(S))(v)$.
   - Rechtsperation: $vf = (\tau(f)(S))(v)$.

Die Divisorengruppe einer Maximalordnung

Wenn man die Ergebnisse über die Lifts der Maximalordnung eines Hasse'schen Schiefkörpers untersucht, wird man zu einigen Überlegungen bezüglich divisorieller zweiseitiger Ideale in Maximalordnungen über lokal-faktoriellen Krullbereichen geführt. Von nun an sei R ein *beliebiger* kommutativer lokal-faktorieller Noetherscher Krullbereich mit Quotientenkörper K. A sei eine zentral-einfache K-Algebra und Λ eine Maximalordnung in A.

Notation *Wir setzen* $\tilde{\cdot} := \bigcap_{\mathfrak{p} \in ht^1(R)} (.)_{\mathfrak{p}}$.

Notation *Für* $\mathfrak{p} \in ht^1(R)$ *setzen wir* $\mathfrak{P} := rad(\Lambda_{\mathfrak{p}}) \cap \Lambda$.

Satz 10.41 *Es gibt eine 1-1-Beziehung zwischen der Menge* $P(\Lambda)$ *der maximalen divisoriellen zweiseitigen Ideal von* Λ *und der Menge* $ht^1(R)$*. Diese Bijektion wird durch die folgenden beiden Abbildungen gegeben.*

$$ht^1(R) \ni \mathfrak{p} \longmapsto rad(\Lambda_{\mathfrak{p}}) \cap \Lambda =: \mathfrak{P} \in P(\Lambda)$$
$$P(\Lambda) \ni \mathfrak{P} \longmapsto \mathfrak{P} \cap R =: \mathfrak{p} \in ht^1(R).$$

Jedes zweiseitige divisorielle Ideal von Λ kann mit Hilfe der Ideale $\mathfrak{P} \in \mathrm{P}(\Lambda)$ beschrieben werden.

Lemma 10.42 *Es sei* $J \subset \Lambda$ *ein divisorielles zweiseitiges Ideal. Dann existieren endlich viele* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in ht^1(R)$ *und natürliche Zahlen* $\alpha_1, \ldots, \alpha_n \geq 1$ *mit*

$$J = \bigcap_{i=1}^{n} \left(rad(\Lambda_{\mathfrak{p}_i})^{\alpha_i} \cap \Lambda \right).$$

Umgekehrt ist jedes Ideal dieser Bauart divisoriell.

Wir benötigen eine Äquivalenzrelation auf den zweiseitgen Λ-Idealen in A.

Definition *Es seien J und J' zweiseitige Λ-Ideale in A. Wir sagen, daß J und J' in der gleichen Divisiorenklasse von Λ liegen, falls $\tilde{J} = \tilde{J'}$ gilt, wir schreiben $J \sim J'$.*

Definition *Für ein zweiseitiges Λ-Ideal J in A bezeichnen wir die Äquivalenzklasse von J unter $\sim$ mit $div(J)$. Die Menge der Äquivalenzklassen bezeichnen wir mit $D(\Lambda)$.*

Satz 10.60 *Mit der Verknüpfung $div(I)div(J) := div(IJ)$ ist $D(\Lambda)$ eine freie Abelsche Gruppe mit Basis*

$$\mathcal{B} := \{div(\mathfrak{P}) : \mathfrak{P} \text{ das maximale divisorielle Ideal über } \mathfrak{p} \in ht^1(R)\}.$$

Darüber hinaus gilt:

(a) $div(\Lambda)$ ist das neutrale Element von $D(\Lambda)$.

(b) Für ein zweiseitiges Λ-Ideal in A gilt $div(J)^{-1} = div(J^{-1})$.

(c) Die Abbildung

$$\Phi : D(\Lambda) \longrightarrow \bigoplus_{\mathfrak{p} \in ht^1(R)} \mathbb{Z}$$

$$div\left(\bigcap_{\mathfrak{p} \in ht^1(R)} \left(rad(\Lambda_\mathfrak{p})\right)^{\alpha_\mathfrak{p}} \right) \longmapsto (\alpha_\mathfrak{p})_\mathfrak{p}$$

ist ein Isomorphismus von Abelschen Gruppen.

Lemma 10.61 *Für ein Element $\mathfrak{p} \in ht^1(R)$ existiert ein eindeutiges $1 \leq e \in \mathbb{N}$ mit $div(\mathfrak{p}\Lambda) = div(\mathfrak{P})^e$. Dieses e ist der klassische Verzweigungsindex $\mathfrak{p}R_\mathfrak{p}$ in $\Lambda_\mathfrak{p}$.*

Definition 10.62 *Es $\mathfrak{p} \in ht^1(R)$. Wir bezeichnen die eindeutig bestimmte natürliche Zahl $1 \leq e$ als den Verzweigungsindex von $\mathfrak{p}$ in Λ.*

Die Gruppe der gebrochenen divisoriellen Ideale von R wird mit $\mathrm{D}(R)$ bezeichnet.

Lemma 10.74 *Es gibt eine Injektion von Abelschen Gruppen*

$$\varphi : D(R) \longrightarrow D(\Lambda)$$
$$\mathfrak{a} \longmapsto div(\mathfrak{a}\Lambda),$$

somit können wir $D(R)$ als eine Untergruppe von $D(\Lambda)$ auffassen.

Lemma *Es sei $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = frac(R/\mathfrak{p})$ für jedes $\mathfrak{p} \in ht^1(R)$ ein perfekter Körper. Für ein Primideal $\mathfrak{p} \in ht^1(R)$ bezeichnen $e(\mathfrak{p})$ den Verzweigungsindex von $\mathfrak{p} \in \Lambda$. Dann gelten:*

1. *Es gibt nur endlich viele $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in ht^1(R)$ mit $e(\mathfrak{p}_i) \neq 1$.*
2. *Die Gruppe $D(\Lambda)/D(R) \simeq \prod_{i=1}^n \mathbb{Z}/e(\mathfrak{p}_i)\mathbb{Z}$ ist endlich.*

Lemma *Es sei $J \subset \Lambda$ ein zweiseitiges divisorielles Ideal mit der Eigenschaft $div(J) = \Pi_{i=1}^{k} div(\mathfrak{P}_i)^{\alpha_i}$, wobei $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ maximale divisorielle zweiseitige Ideale von Λ sind. Dann gilt die folgende Gleichheit*

$$J = \bigcap_{i=1}^{k} \widetilde{\mathfrak{P}_i^{\alpha_i}} = \widetilde{\prod_{i=1}^{k} \mathfrak{P}_i^{\alpha_i}}.$$

Satz *Es sei J ein zweiseitiges divisorielles Ideal von Λ mit $\mathfrak{a} := J \cap R$. Äquivalent sind:*

1. *$div(J) \subset \langle div(\mathfrak{P}_1), \ldots, div(\mathfrak{P}_k) \rangle$*
2. *$\mathfrak{a} \in \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_k \rangle$,*

wobei die $\mathfrak{P}_i$'s maximale divisorielle Ideale von Λ mit $\mathfrak{P}_i \cap R = \mathfrak{p}_i \in ht^1(R)$ seien.

Es sei $\mathfrak{p} \in \mathrm{ht}^1(R)$ und $\mathfrak{P}$ das darüberliegende maximale divisorielle Ideal von Λ. Desweiteren seien $1 \leq \alpha \in \mathbb{N}$ und $\mathfrak{a} := \widetilde{\mathfrak{P}^{\alpha}} \cap R$. Es sei e der Verzweigungsindex von $\mathfrak{P}$ über $\mathfrak{p}$. Es existiert ein $1 \leq \beta \in \mathbb{N}$ mit $\mathfrak{a} = \mathfrak{p}^{\beta}$. Wir wollen dieses β bestimmen. Für $\gamma \in \mathbb{R}$ sei $\lceil \gamma \rceil := \min \{a \in \mathbb{Z} \mid a \geq \gamma\}$. Mit dieser Notation gilt

Lemma *Es seien $\mathfrak{p} \in ht^1(R)$ und $\mathfrak{P} \subset \Lambda$ das darüberliegende maximale divisorielle zweiseitige Ideal und $e = e(\mathfrak{P}/\mathfrak{p})$ der zugehörige Verzweigungsindex. Desweiteren sei $n \in \mathbb{N}$, dann existieren eindeutig bestimmte Elemente $k \in \mathbb{N}$ und $m \in \mathbb{N}$ mit $0 \leq m \leq e-1$ so daß $n = ke + m$ und $\widetilde{\mathfrak{P}^n} \cap R = \mathfrak{p}^{\lceil \frac{n}{e} \rceil}$ gelten.*

Eine andere Charakterisierung der Maximalen Divisoriellen Ideale

Wir nehmen nun an, daß die Krull-Dimension von $R \geq 2$ ist.

Lemma *Keines der maximalen divisoriellen zweiseitigen Ideal $\mathfrak{P}$ von Λ ist ein maximales zweiseitiges Ideal des Rings Λ.*

Lemma 11.4 *Die maximalen divisoriellen zweiseitigen Ideale $\mathfrak{P}$ von Λ sind Primideale von Λ.*

Satz *Für ein Primideal P von Λ sind äquivalent:*

1. *$P = \mathfrak{P}$ für ein maximales zweiseitiges divisorielles Ideal $\mathfrak{P}$ von Λ.*
2. *P ist divisoriell.*

Definition *Wir nennen ein Primideal $P \subset \Lambda$ von Höhe 1, falls kein Primideal P_1 mit $0 \subsetneq P_1 \subsetneq P$ existiert.*

Satz 11.10 *Für ein Primideal $P \subset \Lambda$ sind äquivalent:*

1. *P ist von Höhe 1.*
2. *Es existiert ein maximales divisorielles zweiseitiges Ideal $\mathfrak{P}$ mit $P = \mathfrak{P}$.*

Satz 14.19 *R sei lokal mit Radikal $\mathfrak{m}$. Jedes maximale divisorielle zweiseitige Ideal $\mathfrak{P}$ ist im Radikal von Λ enthalten.*

An dieser Stelle möchte ich allen voran Prof. Roggenkamp für die interesannte Themenstellung, viele fruchtbare Diskussionen und seine stetige Unterstützung meinen Dank ausprechen.
Desweiteren möchte ich Frau Prof. Reiten für die Übernahme des Mitberichts danken.

1 Introduction

Hasse Skewfields

Let R be a complete discrete valuation domain with prime π, field of fractions K and a finite residue class field $\mathfrak{k}$ of order m. We denote the discrete valuation on K by ν. In his article [Has31] from 1931 Helmut Hasse has studied skewfields D of finite K-dimension such that the center of D is equal to K. Let $|D:K| = n^2$. Hasse's first observation was that the discrete valuation ν can be uniquely extended to a "discrete valuation" $\tilde{\nu}$ on D. For an arbitrary element $d \in D$ we define $\tilde{\nu}(d) := \frac{1}{|D:K|}\nu(\mathrm{N}_{D/K}(d)) \in \mathbb{Q} \cup \{\infty\}$, where $\mathrm{N}_{D/K}$ is the norm map of D over K. The existence and uniqueness of $\tilde{\nu}$ determine in a strong way the structure of D and the structure of its maximal orders. We call an R-algebra Γ in D an R-order if Γ is finitely generated as an R-module and $K\Gamma = D$ holds (see Definition 2.18). The first important result is that the integral elements of D form a ring, hence there is actually just one *uniquely* determined maximal order in D, say Δ. This maximal order can be described as some kind of a non commutative discrete valuation domain. The valuation group of $\tilde{\nu}$ is $\frac{1}{e}\mathbb{Z}$ for some $1 \leq e \in \mathbb{N}$. It is usual to pass over to the equivalent valuation $\nu_D := e\tilde{\nu}$. We call an element $\pi_D \in \Delta$ a prime of Δ if $\nu_D(\pi_D) = 1$ holds. Every one-sided ideal J of Δ is two-sided; there is some $k \in \mathbb{N}$ with $J = {\pi_D}^k\Delta = \Delta{\pi_D}^k$. So Δ is a local ring and $\bar{\Delta} := \Delta/\pi_D\Delta$ is a skewfield over $\mathfrak{k}$. The degree of $\bar{\Delta}$ over $\mathfrak{k}$ is denoted by f, it is called the inertial degree of Δ over K. In Δ there is a prime element π_D with ${\pi_D}^n = \pi$ such that $\pi_D\omega{\pi_D}^{-1} = \omega^{m^r}$ for some $r \in \mathbb{N}$ which is relative prime to n. The number r is unique, the fraction $\frac{r}{n}$ is called the Hasse invariant of D. The skewfield D contains a $(m^f - 1)$-th primitive root of unity, say ω. We set $W := K(\omega)$, this field is unique up to conjugation; W is called an inertia field of D. $S := \text{alg.int.}_R(W)$ is a discrete valuation domain with prime π. The residue class field of S is denoted by $\mathfrak{k}'$. For every Hasse invariant $\frac{r}{n}$ there exists a corresponding skewfield, which can be constructed via a matrix representation over its inertia field W. We will do this below in a more general context. It turns out that these skewfields form a complete list of all the skewfields which are of finite K-dimension and have center K. Our first purpose is to lift such skewfields to skewfields over the polynomial ring $R[q]$ or over the function field $K(q)$. For this aim the language of Brauer groups will be useful.

Let us give one possible motivation for studying the lifts of the Hasse skewfields. By using the Deformation Theorem of Tits (cf. [CR87, Theorem 68.17] a new proof of the Deformation Theorem can be also found in [Rog01a]) one gets the following result: If W is a Coxeter group $p \in \mathbb{Z}$ a prime and B_0 a block of the p-adic group ring $\tilde{\mathbb{Z}}_pW$, then there is exactly one block B of the completed Iwahori-Hecke order $\widehat{H_W}$ which maps to B under specialization the indeterminate q to 1 (see [Rog00a]). For the basic theory of finite Coxeter groups and their associated Iwahori-Hecke algebras see for example [CR87, Chapter 8]. If the block B_0 has cyclic defect and Brauer tree T (for the theory of blocks of cyclic defect see for example [Rog80], [Rog92], [Rog91] and [Rog99b]) then B has the structure of a Brauer tree order with the same tree T (see again [Rog00a]). The classification of the Hasse skewfields plays an important role in the theory of blocks of cyclic defect and classical Brauer tree orders. So it is an interesting aspect to study the lifts of the Hasse skewfields.

Brauer Groups – Crossed-Product Algebras – Cyclic Algebras and Orders

Let F be an arbitrary field and A and B two central simple F-algebras. We call A and B equivalent (or sometimes similar) if the skewfield parts of A and B are isomorphic. Then we write $A \sim B$ and denote the equivalence class of A by $[A]$.
Theorem

1. *We set*
$$B(F) := \{[A] \mid A \text{ is a central simple } F\text{-algebra}\}.$$
The following product on $B(F)$ is well-defined and turns $B(F)$ into an Abelian group:
$$[A][B] := [A \otimes_F B] \quad \text{for all } [A],[B] \in B(F).$$
$B(F)$ is called the Brauer group of F. For $[A] \in B(F)$ we have $[A]^{-1} = [A^{op}]$.

2. *Let L/K be some field extension. Then there is a well-defined homomorphism of groups:*
$$\Phi_{L/F} : B(F) \ni [A] \longmapsto [L \otimes_F A] \in B(L).$$
The kernel of $\Phi_{L/F}$ is denoted by $B(L/F)$, it is called the relative Brauer group of L/F.

3. *We set $\mathcal{G} := \{L \mid L \text{ is a finite Galois extension of } F\}$ and obtain*
$$B(F) = \bigcup_{L \in \mathcal{G}} B(L/F).$$

Let L/F be a Galois extension with group G. The relative Brauer group $B(L/F)$ can be described with the help of cohomological methods. The multiplicative group $L^\times$ is a G-module. For an element $\Psi \in \mathrm{C}^2(G, L^\times)$ the central simple F-algebra $(L/F, \Psi)$ is defined in the following way:

1. As a vector space over L it has a basis of the form $\{u_\sigma \mid \sigma \in G\}$.
2. The multiplication is given by the following two rules
   - $u_\sigma l = \sigma(l) u_\sigma \quad \forall l \in L \, \forall \sigma \in G.$
   - $u_\sigma u_\tau = \Phi(\sigma, \tau) u_{\sigma\tau} \quad \forall \sigma, \tau \in G.$

$(L/F, \Psi)$ is called a crossed-product algebra.

Theorem *Let Ψ, Φ be in $\mathrm{C}^2(G, L^\times)$. The algebras $(L/K, \Psi)$ and $(L/K, \Phi)$ are isomorphic if and only if the cohomology classes $[\Phi]$ and $[\Psi]$ in $\mathrm{H}^2(G, L^\times)$ coincide. The following map is an isomorphism of Abelian groups:*
$$\begin{aligned} \mathcal{B} : \mathrm{H}^2(G, L^\times) &\longrightarrow B(L/K) \\ [\Psi] &\longmapsto [(L/K, \Psi)]. \end{aligned}$$

Let $W = K(\omega)$ be an inertia field of some Hasse skewfield D and $\sigma : K(\omega) \ni \omega \longmapsto \omega^m \in K(\omega)$ the Frobenius homomorphism of the field extension W/K. The Galois group of W/K is cyclic with generator σ. We assume from

now on that L/F is a *cyclic* Galois extension of degree n with group $G = \langle\tau\rangle$. For $a \in F^\times$ we define $\Phi_a : G \times G \longrightarrow L^\times$ by $\Phi_a(\tau^i, \tau^j) := \begin{cases} 0 \text{ for } i+j \leq n-1 \\ a \text{ for } i+j \geq n \end{cases}$.

Definition *Let $a \in K^\times$. The crossed-product algebra $(L/F, \Phi_a)$ is called a cyclic algebra and it will be denoted by $(L/F, \tau, a)$.*

Theorem *For $\Phi \in \mathrm{C}^2(G, L^\times)$ there is an $a \in F^\times$ with $(L/F, \Phi) \simeq (L/F, \tau, a)$.*

Let $A := (L/F, \tau, a)$ be a cyclic algebra with basis $\{\nu_{\tau^i}\}$. Then:

1. $\nu^i = \nu_{\tau^i}$ for $0 \leq i \leq n-1$.
2. The relations
$$\nu^n = \nu^{n-1}\nu = \nu_{\tau^{n-1}}\nu_\tau = \Phi_a(\tau^{n-1}, \tau^1)\nu_{\tau^n} \underset{n-1+1=n\geq n-1}{=} a\nu_{\mathrm{id}} = a$$
show that there is an isomorphism $L[x,\tau]/\langle x^n - a\rangle$, where $L[x,\tau]$ denotes the twisted polynomial ring.

The cyclic algebra A has a matrix representation.

Lemma *For $l \in L$ let* $\tilde{l} := \begin{pmatrix} l & & \\ & \ddots & \\ & & \tau^{n-1}(l) \end{pmatrix} \in M_n(L)$; $\nu^* := \begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ a & 0 & \dots & 0 \end{pmatrix} \in M_n(L)$.

The map

$$\Gamma : (L/F, \tau, a) \longrightarrow \bigoplus_{i=0}^{n-1} L(\nu^*)^i$$
$$\sum_{i=0}^{n-1} l_i\nu^i \longmapsto \sum_{i=0}^{n-1} \tilde{l}_i(\nu^*)^i$$

is an isomorphism of F-algebras.

Furthermore let T be an integral domain with field of fractions F and set $U := \text{alg.int.}_T(L)$. For an $a \in T \setminus \{0\}$ we define the A-algebra $(U/T, \tau, a)$ analogous to the cyclic algebra $(L/F, \tau, a)$, i.e.,

$$(U/T, \tau, a) := \bigoplus_{i=0}^{n-1} U\lambda^i, \quad \text{with} \quad (L/F, \tau, a) = \bigoplus_{i=0}^{n-1} L\lambda^i.$$

We call $(U/T, \tau, a)$ a cyclic T-algebra. By restricting the matrix representation of $(L/F, \tau, a)$ to $(U/T, \tau, a)$ we obtain a matrix representation of $(U/T, \tau, a)$. One of the most important results of Hasse's can be reformulated as

Theorem *We denote by φ Euler's phi function. Let $1 \leq \alpha_1, \dots, \alpha_{\varphi(n)} \leq n$ be the $\varphi(n)$ values, which are relatively prime to n. The $\varphi(n)$ cyclic algebras $(W/K, \rho, \pi^{\alpha_i})$ give a full set of non isomorphic skewfields with center K and index n.*

For our purpose we prefer another representation of these skewfields, which is given by the following

Lemma *The $\varphi(n)$ cyclic algebras $(W/K, \rho^{\alpha_i}, \pi)$ give also a full set of non isomorphic skewfields with center K and index n. We call these representations the standard representations of the Hasse skewfields.*

Lifts

Definition of a Lift

Now we can state our definition of a lift:

Definition *Let $0 \neq a \in T$ be an arbitrary element. We set $\Lambda := (U/T, \tau, a)$ and $A := (L/F, \tau, a)$. A lift of A is some cyclic $L(q)$-algebra A_f satisfying the following two properties:*

- *$A_f = L(q)\Lambda_f$ for $\Lambda_f = (U[q]/T[q], \tau, f)$ with $f \in T[q]$ (hence A_f contains the cyclic $T[q]$-order Λ_f).*
- *$\Lambda_f/q\Lambda_f = (U/T, \tau, a)$.*

For the special case of a Hasse skewfield we obtain

Corollary *A lift of the standard representation of a Hasse skewfield is of the form $D_h := W(q)\Lambda_h$ with $\Lambda_h = (S[q]/R[q], \sigma, h)$ with $h \in R[q]$ and $h(0) = \varepsilon\pi$ such that ε is a unit of R. The polynomial h is of the form gf with f is irreducible in $S[q]$ and $f(0)$ is a prime of R which we can w.l.o.g. assume to be π and $g(0)$ is a unit of R.*

Lifts are Skewfields

We consider the standard representation of a Hasse skewfield D and a lift D_f of this standard representation. We have $D_f = W(q)\Lambda_f$ with $\Lambda_f = (S[q]/R[q], \sigma, f)$ with $f \in R[q]$ and $f(0) = \varepsilon\pi$ such that ε is a unit of R. However we can w.l.o.g. assume that $f(0) = \pi$ holds.

Theorem 3.16 *The algebra D_f is a skewfield, hence every lift of a Hasse skewfield is again a skewfield.*

This is a direct consequence of the following lemma, which is not restricted to the case of Hasse skewfields.

Lemma 3.20 *Let T be a commutative Noetherian domain with field of fractions F and let Λ be a T-order in an F-algebra A. Let $q \in T$ be an arbitrary non-unit of T. If $\Lambda/q\Lambda$ has no zero divisors then A is a skewfield.*

The last lemma could be generalized to the following theorem.

Theorem 3.21 *Let T be a Noetherian commutative ring with field of fractions F. Let Λ be a T-order in an F-algebra A, and let $\mathfrak{a} \neq T$ be an invertible ideal of T. If $\Lambda/\mathfrak{a}\Lambda$ has no zero divisors then A is a skewfield.*

Lifts of the Maximal Order

Let D be a Hasse skewfield and $D_f = W(q)\Lambda_f$ a lift. We call the order $\Lambda_f = (S[q]/R[q], \sigma, f)$ a lift of the maximal order. Now we will decide when Λ_f is a maximal order. To decide when Λ_f is maximal, we will use a result which is due to Auslander and Goldmann (cf. [AG60, Theorem 1.17]).

Theorem 4.3 *Let T be an integral closed Noetherian domain with field of fractions F. Moreover let Γ be a T-order which is contained in central simple F-algebra B. The following are equivalent:*

1. *Γ is a maximal T-order.*
2. *Γ satisfies the following two properties:*
   - $\Gamma^{**} = \Gamma$.
   - *For every $\mathfrak{p} \in ht^1(T)$ the $T_\mathfrak{p}$-order $\Gamma_\mathfrak{p}$ is maximal.*

Maximal Lifts of the Maximal Order

Here we will consider lifts of the form $D_{\tilde{f}} := W(q)(S[q]/R[q], \sigma, \tilde{f})$ with $\tilde{f} = \left(\prod_{i=1}^{t} g_i\right) f$ such that f is irreducible in $S[q]$ and $f(0) = \pi$. The g_i's are pairwise different polynomials such that they are irreducible in $S[q]$. The following points shall be satisfied:

- $g_i(0) = \varepsilon_i \in R^\times$ for $1 \leq i \leq t$, so in particular $fR[q] \neq g_i R[q]$ for all i's.
- The prime ideals $g_i R[q]$ are pairwise different.

In this case $\Lambda_{\tilde{f}} := (S[q]/R[q], \sigma, \tilde{f})$ is a maximal order. We have to check the two points of Theorem 4.3 for the order $\Lambda_{\tilde{f}}$. In our case the order $\Lambda_{\tilde{f}}$ is free over $R[q]$, so the first point is automatically satisfied. To verify the second point we awake again a Theorem of Auslander and Goldmann (cf. [AG60, Theorem 2.3]):

Theorem 4.4 *Let T be a discrete valuation domain with field of fractions F. A T-order Γ in a central simple F-algebra B is maximal if and only if Γ satisfies the following two properties:*

- *Γ is hereditary.*
- *rad(Γ) is its unique maximal two-sided ideal.*

So we have to check that for every $\mathfrak{p} \in \mathrm{ht}^1(R)$ the order $\Lambda_{\tilde{f},\mathfrak{p}}$ satisfies the two conditions of Theorem 4.4.

- We use the following result which is again due to Auslander and Goldmann (cf. [AG60, Corollary to Theorem 2.2]):

  Lemma 4.5 *Let T be a discrete valuation domain and Γ a T-algebra which is finitely generated and torsionfree as T-module. If rad(Γ) is projective, then Γ is a hereditary ring.*

  With Lemma 4.5 it will be enough to check that $\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ is a projective $\Lambda_{\tilde{f},\mathfrak{p}}$-module.

- To verify that $\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ is the unique maximal two-sided ideal of $\Lambda_{\tilde{f},\mathfrak{p}}$ we will show that the quotients $\overline{\Lambda_{\tilde{f},\mathfrak{p}}} := \Lambda_{\tilde{f},\mathfrak{p}}/\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ are simple algebras.

To determine the structure of the orders $\Lambda_{\tilde{f},\mathfrak{p}}$ we have to distinguish three cases. For simplify the calculations we can *w.l.o.g.* assume that $\tilde{f} = f$ is irreducible in $S[q]$ (see Observations 4.82). Since Λ_f is a cyclic order there is some element $\lambda \in \Lambda_f$ with

- $\Lambda = \bigoplus_{i=0}^{n-1} S[q]\lambda^i$,
- $\lambda^n = f$ and $\lambda y = \sigma(y)\lambda$ for all $y \in S[q]$

Case 1: $\mathfrak{p} = fR[q]$

Lemma 4.84 *Let $\mathfrak{p} = fR[q]$. We have that $rad(\Lambda_{f,\mathfrak{p}}) = \lambda\Lambda_{f,\mathfrak{p}}$ is projective over Λ and it is the unique maximal two-sided ideal of Λ.*

To prove Lemma 4.84 we study the following situation, which is satisfied by $\Lambda_{f,\mathfrak{p}}$: Let T be an arbitrary discrete valuation domain with prime p and field of fractions F. We *do not* assume that T is complete. Furthermore let L/F be a cyclic Galois extension of degree n with group $G := \langle\tau\rangle$. Let $U :=$ alg. $\mathrm{int.}_T(L)$ and assume that U is a discrete valuation domain with prime p. Let $\Gamma := (U/T, \tau, p) = \oplus_{i=0}^{n-1} U\gamma^i$. To use determinants we pass over to the matrix representation of Γ and show the following lemma.

Lemma 4.19

1. *Let $I \subset \Gamma$ be a left ideal then there is some $k \in \mathbb{N}$ with $I = \Gamma\gamma^k$.*
2. *Let $I \subset \Lambda$ a right ideal the there is some $l \in \mathbb{N}$ with $I = \gamma^l\Gamma$.*
3. *For every $k \in \mathbb{N}$ we have moreover $\gamma^k\Gamma = \Gamma\gamma^k$, so every one-sided ideal of Γ is actually a two-sided one.*
4. *We have $rad(\Gamma) = \gamma\Gamma = \Gamma\gamma$, Γ is a local ring and $rad(\Gamma)$ is the unique maximal two-sided ideal of Γ.*

Lemma 4.84 yields that $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ is the unique maximal two-sided ideal of $\Lambda_{f,\mathfrak{p}}$. Lemma 4.84 also yields that $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ is a projective $\Lambda_{f,\mathfrak{p}}$-module and so $\Lambda_{f,\mathfrak{p}}$ is hereditary.

Case 2: $\mathfrak{p} = hR[q]$ **with** $\deg(h) \geq 1$

There is an element $\alpha \in \mathbb{N}$ which divides n and an irreducible polynomial g in $S[q]$ such that $h = g\sigma(g)\cdots\sigma^{\alpha-1}(g)$ holds (see Chapter 4.3). Let a be a common root of the polynomials h and g contained in some algebraic extension of W. We have $f + hK[q] \neq 0$ and by an isomorphism $K[q]/hK[q] \simeq K(a)$ we can identify $f + hK[q]$ with some element $0 \neq b \in K(a)$.

Lemma 4.87

1. $rad(\Lambda_{f,\mathfrak{p}}) = \mathfrak{p}\Lambda_{f,\mathfrak{p}}$ *and*

2. $\Lambda_{f,\mathfrak{p}}/rad(\Lambda_{f,\mathfrak{p}}) = M_\alpha((W(a)/K(a), \sigma^\alpha, b)$.

To prove Lemma 4.87 we apply a two-sided Pierce decomposition to the quotient $\Lambda_{f,\mathfrak{p}}/\mathfrak{p}\Lambda_{f,\mathfrak{p}}$ (see Section 4.5). Here we use how the Galois automorphism transforms by conjugation by applying the isomorphism $S[q]_\mathfrak{p}/\mathfrak{p}S[q]_\mathfrak{p} \simeq \prod_{i=0}^{\alpha-1} S[q]_\mathfrak{p}/\sigma^i(g)S[q]_\mathfrak{p}$ arising from the Chinese Remainder Theorem (this can be found in Chapter 4.4).

With Lemma 4.87 we get $\mathrm{rad}(\Lambda_{f,\mathfrak{p}}) = g\Lambda_{f,\mathfrak{p}}$ is projective over $\Lambda_{f,\mathfrak{p}}$ and it is the uniquely determined maximal two-sided ideal of $\Lambda_{f,\mathfrak{p}}$, hence $\Lambda_{f,\mathfrak{p}}$ is a maximal $R[q]_\mathfrak{p}$-order.

Case 3: $\mathfrak{p} = \pi R[q]$

Lemma 4.89

1. $rad(\Lambda_{f,\mathfrak{p}}) = \mathfrak{p}\Lambda_{f,\mathfrak{p}}$

2. $\Lambda_{f,\mathfrak{p}}/rad(\Lambda_{f,\mathfrak{p}}) \simeq (\mathfrak{k}'(q)/\mathfrak{k}(q), \bar{\sigma}, \bar{f})$, *where* $\bar{\sigma}$ *is the automorphism on* $\mathfrak{k}'$ *which is induced by* σ *and* $\bar{f} := f + \pi R[q]$. *Since* f *is assumed to be primitive we have that* $\bar{f}$ *is* not *zero.*

The proof of Lemma 4.89 is mainly based on the

Corollary 4.80 *The field extension* $\mathfrak{k}'(q)/\mathfrak{k}(q)$ *is Galois of degree* n *and there is an isomorphism* $Gal(\mathfrak{k}'(q)/\mathfrak{k}(q)) \simeq Gal(L/K)$.

Obviously $\mathrm{rad}(\Lambda_{f,\mathfrak{p}}) = \pi\Lambda_{f,\mathfrak{p}}$ is projective over $\Lambda_{f,\mathfrak{p}}$, hence $\Lambda_{f,\mathfrak{p}}$ is hereditary. By Lemma 4.89 $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ is the unique maximal two-sided ideal of $\Lambda_{f,\mathfrak{p}}$.

Non Maximal Lifts of the Maximal Order

Here we will consider lifts of a Hasse skewfield D which are of the form $D_{hf} := W(q)(S[q]/R[q], \sigma, hf)$ with $f(0) = \pi$ and $h(0) \in R^\times$. At least one of the following two possibilities shall be satisfied:

- $h = \tilde{h}g^s$ for some polynomials $\tilde{h}$ and $g \notin R^\times = R[q]^\times$ and $s \geq 2$.
- $h = \tilde{h}g$ for some polynomials $\tilde{h}$ and g in $R[q]$ such that the polynomial g is not irreducible in $S[q]$.

In these cases $\Lambda_{fh} := (S[q]/R[q], \sigma, hf)$ is *not* a maximal order (see Theorem 5.25).

The proof of this Theorem is based on different observations which we did in Chapter 5.

Truncated Twisted Polynomial Rings and their Cohomology Rings

Motivation

We fix a lift $D_f = W(q)\Lambda_f$ of a standard representation of a Hasse skewfield D such that $\Lambda_f = (S[q]/R[q], \sigma, f)$ for $f \in R[q]$ with $f(0) = \pi$. We can consider specializations of Λ_f i.e. quotients $\Lambda_a := \Lambda_f/(q-a)\Lambda_f$ for $a \in R$. There is an isomorphism $\Lambda_a \simeq (S/R, \sigma, f(a))$. Let us assume that a is a zero of f. In this situation there is an isomorphism $K\Lambda_a \simeq K[x,\sigma]/(x^n)$, where $K[x,\sigma]$ denotes the twisted polynomial ring. So it is natural to study these truncated twisted polynomial rings and to see how far they are away from being semisimple.

Generalities

Let us fix the notation. Let L/F be an arbitrary finite Galois extension of degree d, moreover let $\mathrm{id} \neq \tau$ be a Galois automorphism of L. Let $2 \leq k \in \mathbb{N}$. By L_τ we denote the fixed field of τ. Moreover we set $A := L[x,\tau]/\langle x^d \rangle$ and $N := x + \langle x^d \rangle \in A$. We get:

1. A is a local ring.
2. The module $S := A/AN$ is up to isomorphism the only simple A-module.
3. There is an isomorphism of A-modules $S = A/AN \simeq An^{k-1}$.
4. A is up to isomorphism the only projective indecomposable A-module.
5. The center $\mathrm{C}(A)$ of A is L_τ.

Projective Resolutions and Ext-Groups

For $0 \leq i \leq k-1$ we define $\rho_i \in \mathrm{End}_A(S)$ by

$$\rho_i : A \ni a \longmapsto aN^i \in A$$

and observe that the kernel of ρ_i is AN^{k-i}.

Lemma 6.12 *A projective resolution of the simple A-module S is given by the following exact sequence:*

$$\mathcal{P}_0 \cdots\cdots \xrightarrow{\rho_1} A \xrightarrow{\rho_{m-1}} A \xrightarrow{\rho_1} A \xrightarrow{\rho_{m-1}} S \longrightarrow 0,$$

where we identify S with AN^{k-1}. For $k = 2$ we have $k-1 = 2-1 = 1$ and so $\rho_1 = \rho_{k-1}$. Hence in this case the projective resolution of S is periodic with period 1. In the other cases it has period 2.

Corollary

1. $pdim_A(S) = \infty$.
2. $gl.dim(A) = \infty$.

So A is in some sense as far as possible away from being semisimple. The Ext-groups $\mathrm{Ext}^i_A(S,S)$ are Hom's.

Lemma 6.19 *For all $i \in \mathbb{N}$ we have* $\mathrm{Ext}^i_A(S,S) = \mathrm{Hom}_A(A,S)$.

This property will be very helpful for calculating the cohomology ring of A.

Cohomology Rings

We set $\mathrm{ext}^*_A(S,S) := \bigoplus_{i\in\mathbb{N}} \mathrm{ext}^i_A(S,S)$, a graded associative ring with componentwise addition induced from the Baer sum and multiplication induced from the Yoneda splice. This ring is called the cohomology ring of S; this ring can be canonically identified as ring with $\mathrm{Ext}^*_A(S,S) := \bigoplus_{i\in\mathbb{N}} \mathrm{ext}^i_A(S,S)$ (see Chapter 7, especially Section 7.2).

We use the following notation: The homomorphism $\varphi_1 \in \mathrm{Hom}_A(A,S) = \mathrm{Ext}^i_A(S,S)$ with $\varphi_1 : A \ni 1 \longmapsto N \in S$ will be denoted by f^i_1. So we get

$$\mathrm{Ext}^*_A(S,S) = \bigoplus_{i\in\mathbb{N}} \mathrm{Ext}^i_A(S,S) = \bigoplus_{i\in\mathbb{N}} L\,\mathrm{f}^i_1\,.$$

The case $k = 2$

In this case we have the

Corollary 7.22 *There is an isomorphism of rings* $\mathrm{Ext}^*_A(S,S) \simeq L[y,\tau]$.

The case of an arbitrary $m \geq 3$

We set $B := \mathrm{Ext}^*_A(S,S) = \bigoplus_{i\in\mathbb{N}} L\,\mathrm{f}^i_1$ and obtain that $N := \bigoplus_{j \text{ odd}} L\,\mathrm{f}^j_1$ is an Abelian ideal of B. Let $\tilde{\tau} := \tau^k$. With this notation we get

Lemma 7.29 $B_0 := \bigoplus_{j \text{ even}} L\,\mathrm{f}^j_1 = \bigoplus_{t\in\mathbb{N}} L\,\mathrm{f}^{2t}_1$ *is a subring of* B. *Moreover there is an isomorphism* $B_0 \simeq L[y,\tilde{\tau}]$.

Lemma 7.31 *We set* $V := L^{(\mathbb{N})} = \oplus_{i\in\mathbb{N}} L f_i$. *For* $i \in \mathbb{N}$ *we set* $e_{2i+1} := f_i$ *and consider from now on the basis* $\{e_{2i+1} \,|i \in \mathbb{N}\}$. *Let* $v = \sum_i \alpha_i e_{2i+1} \in V$ *and* $f = \sum_j \beta_j y^j \in L[y,\tilde{\tau}]$ *be arbitrary elements.*

1. *A left operation of* $L[y,\tilde{\tau}]$ *on* V *is given by the following definition*

$$fv := \sum_{i,j} \tau^i(\alpha_j)\beta_i e_{2i+2j+1}.$$

2. *The rule*

$$vf := \sum_{i,j} \alpha_i \tau^i(\sigma(\beta_j)) e_{2i+2j+1}$$

   induces a right operation of $L[y,\tilde{\tau}]$ *on* V.

3. *With this operations* V *becomes a bimodule over* $L[y,\tilde{\tau}]$ *as an* F*-algebra.*

Now we can interpret B as a semidirect product by proving the following

Theorem 7.33 *With the notations of the Lemmas 7.29 and 7.31 we get* $V \rtimes B_0 \simeq V \rtimes L[y, \tilde{\tau}] \simeq B$ *as* F*-algebras.*

Let us consider the special case that $\tau^k = \tilde{\tau} = 1$ holds. Then we have:

1. $B_0 \simeq L[y, \tau^k] = L[y]$ is commutative.
2. We set $S : V \ni e_{2i+1} \longmapsto e_{2(i+1)+1} \in V$ to be the right shift on V. For $f = \sum_i \alpha_i y^i \in L[y]$ we set $f(S) := \sum_i \alpha_i S^i$ and $\sigma(f) := \sum_i \sigma(\alpha_i) y^i$. Then we obtain that we can write the left and the right operation of $L[y]$ on V in the following ways:
   - Left Operation: $fv = (f(S))(v)$.
   - Right Operation: $vf = (\sigma(f)(S))(v)$.

The Divisor Group of a Maximal Order

Analyzing our results about the lifts of the maximal order in a Hasse skewfield we were led to some results about divisorial ideals in maximal orders over local factorial Krull domains. From now on let R be a commutative local factorial Noetherian Krull domain with field of fractions K. Let A be a central simple K-algebra and Λ a maximal R-order in A.

Notation *We set* $\tilde{.} := \bigcap_{\mathfrak{p} \in ht^1(R)} (.)_{\mathfrak{p}}$.

Notation *For* $\mathfrak{p} \in ht^1(R)$ *we set* $\mathfrak{P} := rad(\Lambda_{\mathfrak{p}}) \cap \Lambda$.

Theorem 10.41 *There is a one-to-one correspondence between the set* $P(\Lambda)$ *of maximal divisorial two-sided ideals of* Λ *and the set* $ht^1(R)$*. This bijection is given by the following maps:*

$$ht^1(R) \ni \mathfrak{p} \longmapsto rad(\Lambda_{\mathfrak{p}}) \cap \Lambda =: \mathfrak{P} \in P(\Lambda)$$
$$P(\Lambda) \ni \mathfrak{P} \longmapsto \mathfrak{P} \cap R =: \mathfrak{p} \in ht^1(R).$$

Now we will examine an arbitrary two-sided divisorial ideal J of Λ in greater detail, such an ideal can be describe with help of the $\mathfrak{P}$'s.

Lemma 10.42 *Let* $J \subset \Lambda$ *be a divisorial ideal. Then there are finitely many* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in ht^1(R)$ *and natural numbers* $\alpha_1, \ldots, \alpha_n \geq 1$ *with*

$$J = \bigcap_{i=1}^{n} \left(rad(\Lambda_{\mathfrak{p}_i})^{\alpha_i} \cap \Lambda \right).$$

Conversely every ideal of this type is divisorial.

We need an equivalence relation on the two-sided Λ-ideals in A.

Definition *Let* J *and* J' *be two-sided* Λ*-ideals in* A*. We say that* J *and* J' *are in the same divisor class of* Λ *if* $\tilde{J} = \tilde{J'}$ *holds. In this case we will write* $J \sim J'$.

Definition *For an two-sided Λ-ideal J in A we denote the equivalence class of J under $\sim$ by $div(J)$. The set of equivalence classes will be denoted by $D(\Lambda)$.*

Theorem 10.60 *Via the composition rule $div(I)div(J) := div(IJ)$, the set $D(\Lambda)$ is a free Abelian group with basis*

$$\mathcal{B} := \{div(\mathfrak{P}) \ : \ \mathfrak{P} \text{ the maximal divisorial ideal over } \mathfrak{p} \in ht^1(R)\}.$$

Moreover we have

(a) $div(\Lambda)$ is the neutral element of $D(\Lambda)$.

(b) For a two-sided Λ-ideal in A we have $div(J)^{-1} = div(J^{-1})$.

(c) The map $\Phi : D(\Lambda) \longrightarrow \bigoplus_{\mathfrak{p} \in ht^1(R)} \mathbb{Z}$ with

$$div\left(\bigcap_{\mathfrak{p} \in ht^1(R)} \left(rad(\Lambda_\mathfrak{p})\right)^{\alpha_\mathfrak{p}} \right) \longmapsto (\alpha_\mathfrak{p})_\mathfrak{p}$$

is an isomorphism of Abelian groups.

Lemma 10.61 *For an element $\mathfrak{p} \in ht^1(R)$ there is a unique $1 \leq e \in \mathbb{N}$ with $div(\mathfrak{p}\Lambda) = div(\mathfrak{P})^e$. This e is the classical ramification index of $\mathfrak{p}R_\mathfrak{p}$ in the $R_\mathfrak{p}$-order $\Lambda_\mathfrak{p}$.*

Definition 10.62 *Let $\mathfrak{p} \in ht^1(R)$. The unique natural number $1 \leq e$ is called the ramification index of $\mathfrak{p}$ in Λ.*

The group of fractional divisorial R-ideals will be denoted by by $\mathrm{D}(R)$.

Lemma 10.74 *There is an injection of Abelian groups*

$$\begin{aligned} \varphi : D(R) &\longrightarrow D(\Lambda) \\ \mathfrak{a} &\longmapsto div(\mathfrak{a}\Lambda), \end{aligned}$$

so $D(R)$ can be identified with a subgroup of $D(\Lambda)$.

Lemma *Assume that $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = frac(R/\mathfrak{p})$ is a perfect field for every element $\mathfrak{p} \in ht^1(R)$. For a prime ideal $\mathfrak{p} \in ht^1(R)$ we denote the ramification index of $\mathfrak{p} \in \Lambda$ by $e(\mathfrak{p})$. Then*

1. *There are only finitely many elements $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in ht^1(R)$ with $e(\mathfrak{p}_i) \neq 1$.*
2. *We have moreover*

$$D(\Lambda)/D(R) \simeq \prod_{i=1}^{n} \mathbb{Z}/e(\mathfrak{p}_i)\mathbb{Z}$$

is a finite group.

Lemma *Let $J \subset \Lambda$ be a divisorial two-sided ideal, with the property $div(J) = \Pi_{i=1}^k div(\mathfrak{P}_i)^{\alpha_i}$, where $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ denote maximal divisorial two-sided ideals of Λ. Then we have equalities $J = \bigcap_{i=1}^k \widetilde{\mathfrak{P}_i^{\alpha_i}} = \widetilde{\prod_{i=1}^k \mathfrak{P}_i^{\alpha_i}}$.*

Theorem *Let J be divisorial two-sided ideal of Λ with $\mathfrak{a} := J \cap R$. The following are equivalent:*

1. $div(J) \subset \langle div(\mathfrak{P}_1), \ldots, div(\mathfrak{P}_k)\rangle$
2. $\mathfrak{a} \in \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_k\rangle$,

where the $\mathfrak{P}_i$'s are maximal divisorial ideals of Λ with $\mathfrak{P}_i \cap R = \mathfrak{p}_i \in ht^1(R)$.

Let $\mathfrak{p} \in \mathrm{ht}^1(R)$ and $\mathfrak{P}$ the corresponding maximal divisorial two-sided ideal of Λ. Moreover choose some $1 \leq \alpha \in \mathbb{N}$ and set $\mathfrak{a} := \widetilde{\mathfrak{P}^\alpha} \cap R$. Let e be the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. There exists some $1 \leq \beta \in \mathbb{N}$ with $\mathfrak{a} = \mathfrak{p}^\beta$. Let us determine this β. For an element $\gamma \in \mathbb{R}$ we set $\lceil\gamma\rceil := \min\{a \in \mathbb{Z} \mid a \geq \gamma\}$. We obtain

Lemma *Let $\mathfrak{p} \in ht^1(R)$ and $\mathfrak{P} \subset \Lambda$ the corresponding maximal divisorial ideal of Λ. Moreover let $n \in \mathbb{N}$, then we find uniquely determined elements $k \in \mathbb{N}$ and $m \in \mathbb{N}$ with $0 \leq m \leq e-1$ such that $n = ke + m$ holds and get $\widetilde{\mathfrak{P}^n} \cap R = \mathfrak{p}^{\lceil \frac{n}{e} \rceil}$.*

Another Characterization of Maximal Divisorial Ideals

We assume from now on that the Krull-dimension of $R \geq 2$.

Lemma *None of the maximal divisorial two-sided ideals $\mathfrak{P}$ of Λ is a maximal two-sided ideal of the ring Λ.*

Lemma 11.4 *The maximal divisorial two-sided ideals $\mathfrak{P}$ of Λ are prime ideals of Λ.*

Theorem *For a prime ideal P of Λ are equivalent:*

1. *$P = \mathfrak{P}$ for some maximal divisorial two-sided ideal $\mathfrak{P}$ of Λ.*
2. *P is divisorial.*

Lemma 11.6 *Let T be Noetherian integral domain with field of fractions L. Let A be a simple L-algebra and Γ some T-order in A. Then 0 is a prime ideal of Γ.*

Definition *We call a prime ideal $P \subset \Lambda$ a height one prime ideal if there is no prime ideal P_1 with $0 \subsetneq P_1 \subsetneq P$.*

Theorem *For a prime ideal $P \subset \Lambda$ are equivalent:*

1. *P is of height one.*
2. *There is a maximal divisorial two-sided ideal $\mathfrak{P}$ with $P = \mathfrak{P}$.*

Theorem 14.19 *Let R be local with maximal ideal $\mathfrak{m}$. Then every maximal two-sided divisorial ideal $\mathfrak{P}$ is contained in the radical of Λ.*

2 Brauer Groups, Cyclic Algebras and the Theorems of Hasse

2.1 Brauer Groups and Cyclic Algebras

In this section we state the basic facts about Brauer groups and cyclic algebras. Let F be an arbitrary field. For some ring T we denote its opposite ring by T^{op}. We recall that two central simple F-algebras A and B are called equivalent if their skewfield parts are isomorphic. Then we write $A \sim B$. It is easy to see that "$\sim$" is an equivalence relation. The equivalence class of A will be denoted by $[A]$. We set $B(F) := \{[A] \mid A \text{ is a central simple } F\text{-algebra}\}$.

Theorem 2.1 *1. With the following product, $B(F)$ is an Abelian group:*

$$[A][B] := [A \otimes_F B] \quad \textit{for all } [A],[B] \in B(F).$$

The inverse of $[A] \in B(F)$ is $[A^{op}]$; $B(F)$ is called the Brauer group of F.

2. Let L/F be some field extension. The map

$$\Phi_{L/F} : B(F) \ni [A] \longmapsto [L \otimes_F A] \in B(L)$$

is a well-defined homomorphism of groups. The kernel of $\Phi_{L/F}$ is denoted by $B(L/F)$, it is called the relative Brauer group of L/F.

3. We set $\mathcal{G} := \{L \mid L \text{ is a finite Galois extension of } F\}$. Then

$$B(F) = \bigcup_{L \in \mathcal{G}} B(L/F).$$

Proof. Cf. [Pie82, Propositions a. and c. of Section 12.5 and the Corollary of Section 13.5] □

It is enough to understand the groups $B(L/F)$ for finite Galois extensions L/F. We fix a finite Galois extension L/F with group G and consider $L^\times$ as a G-module.

Lemma 2.2 *1. A map $\Phi : G^2 \longrightarrow L^\times$ is called a 2-cocycle with values in $L^\times$ if the relation $g_1\Phi(g_2,g_3) - \Phi(g_1g_2,g_3) + \Phi(g_1,g_2g_3) + \Phi(g_1,g_2) = 0$ holds for all $g_1,g_2,g_3 \in G$. The set of 2-cocycles with values in $L^\times$ is denoted by $\mathrm{C}^2(G,L^\times)$.*

2. A map $\Phi : G^2 \longrightarrow L^\times$ is called a 2-coboundary if there is a map $\varphi : G \longrightarrow L^\times$ with $\Phi(g_1,g_2) = g_1\varphi(g_2) - \varphi(g_1g_2) + \varphi(g_1)$ for all $g_1,g_2 \in G$. We denote the set of 2-coboundaries with values in $L^\times$ by $\mathrm{B}^2(G,L^\times)$.

3. Both $\mathrm{C}^2(G,L^\times)$ and $\mathrm{B}^2(G,L^\times)$ are Abelian groups such that $\mathrm{B}^2(G,L^\times)$ is a subgroup of $\mathrm{C}^2(G,L^\times)$. The quotient $\frac{\mathrm{C}^2(G,L^\times)}{\mathrm{B}^2(G,L^\times)}$ is denoted by $\mathrm{H}^2(G,L^\times)$. For $\Psi \in \mathrm{C}^2(G,L^\times)$ we will denote $\Psi\,\mathrm{B}^2(G,L^\times) \in \mathrm{H}^2(G,L^\times)$ by $[\Psi]$.

Proof. See for example [Bro00, I. 5 and III. 1 Example]. □

Definition 2.3 *Let $\Psi \in \mathrm{C}^2(G, L^\times)$. The F-algebra $(L/F, \Psi)$ is defined in the following way:*

1. *As a vector space over F it has a basis B of the form $\{u_\tau \mid \tau \in G\}$.*
2. *The multiplication is induced from the rules*
   - $u_\tau l = \tau(l) u_\tau$ *for all* $l \in L$ *and for all* $\tau \in G$.
   - $u_\tau u_{\tilde{\tau}} = \Phi(\tau, \tilde{\tau}) u_{\tau\tilde{\tau}}$ *for all* $\tau, \tilde{\tau} \in G$.

The F-algebra $(L/F, \Psi)$ is called a crossed-product algebra.

Lemma 2.4 *For every $\Psi \in \mathrm{C}^2(G, L^\times)$ the F-algebra $(L/F, \Psi)$ is central simple.*

Proof. Cf. [Pie82, 14.1 Proposition]. □

Theorem 2.5 1. *Let Ψ, Φ be in $\mathrm{C}^2(G, L^\times)$. The algebras $(L/K, \Psi)$ and $(L/K, \Phi)$ are isomorphic if and only if $[\Phi]$ and $[\Psi]$ in $\mathrm{H}^2(G, L^\times)$ coincide.*

2. *The following map is an isomorphism of Abelian groups:*

$$\begin{aligned} \mathcal{B} : \mathrm{H}^2(G, L^\times) &\longrightarrow B(L/F) \\ [\Psi] &\longmapsto [(L/F, \Psi)]. \end{aligned}$$

Proof. Cf. [Pie82, 14.2 Lemma and Theorem]. □

From now on assume that L/F is cyclic of degree n with group $G = \langle \tau \mid \tau^n = \mathrm{id} \rangle$.

Notation 2.6 *For an element $a \in F^\times$ we define $\Phi_a : G \times G \longrightarrow L^\times$ by*

$$\Phi_a(\tau^i, \tau^j) := \begin{cases} 1 \text{ for } i + j \leq n - 1 \\ a \text{ for } i + j \geq n \end{cases} .$$

Lemma 2.7 *For every $a \in F^\times$ the map Φ_a is contained in $\mathrm{C}^2(G, L^\times)$.*

Definition 2.8 *Let $a \in F^\times$ be an arbitrary element. Let $\Phi_a \in \mathrm{C}^2(G, L^\times)$ be the cocycle as in Notation 2.6. The crossed product algebra $(L/F, \Phi_a)$ is called a cyclic algebra and will be denoted by $(L/F, \tau, a)$.*

Observations 2.9 *Let us collect the properties of a cyclic algebra. Per. def. there are elements $\nu_{\tau^i} \in (L/F, \tau, a)$ such that the two conditions of Definition 2.3 are satisfied. Let $\nu := \nu_\tau$. We note:*

1. *For $0 \leq i \leq n-1$ we find - using induction and the definition of Φ_a: $\nu^i = \nu_{\tau^i}$. So in particular ν_{id} is the identity element of $(L/F, \tau, a)$.*
2. *Moreover: $\nu^n = \nu^{n-1}\nu = \nu_{\tau^{n-1}}\nu_\tau = \Phi_a(\tau^{n-1}, \tau^1)\nu_{\tau^n} \underset{n-1+1=n\geq n-1}{=} a\nu_{id} = a$.*

Corollary 2.10 *For $a \in F^\times$ there is an isomorphism $(L/F, \tau, a) \simeq L[x, \tau]/\langle x^n - a \rangle$, where $L[x, \tau]$ denotes the twisted polynomial ring as in Definition 6.1.*

Theorem 2.11 *Let $\Phi \in \mathrm{C}^2(G, L^\times)$ be an arbitrary element, then there is an element $a \in F^\times$ such that we have an isomorphism $(L/F, \Phi) \simeq (L/F, \tau, a)$, hence $(L/F, \Phi)$ is a cyclic algebra.*

Proof. Cf. [Rei75, Theorem 30.3]. □

Remark 2.12 *For calculations with cyclic algebras, matrix representation are suitable. Such matrix representations will be given by Lemma 2.14. We need the*

Lemma and Definition 2.13 *For $w \in L$ we set* $\begin{pmatrix} w & & \\ & \tau(w) & \\ & & \ddots \\ & & & \tau^{n-1}(w) \end{pmatrix} \in M_n(L)$. *The map $\tilde{} : L \ni w \longmapsto \tilde{w} \in M_n(L)$ is an embedding of the field L into $M_n(L)$.*

Lemma 2.14 *Let $a \in F^\times$ be an arbitrary element. We set* $\nu^* := \begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ a & 0 & \dots & 0 \end{pmatrix}$ *and $A := {}_L\langle \nu^* \rangle = \bigoplus_{i=0}^{n-1} L(\nu^*)^i$. The map*

$$\Psi : (L/F, \tau, a) \longrightarrow A$$
$$\sum_{i=0}^{n-1} l_i \nu^i \longmapsto \sum_{i=0}^{n-1} \tilde{l}_i (\nu^*)^i$$

is an isomorphism of F-algebras.

It is also possible to read Lemma 2.14 backwards, which gives us immediately the

Corollary 2.15 *Every matrix algebra as in Lemma 2.14 is a cyclic algebra and hence in particular a central simple F-algebra.*

Remark 2.16 *Let $s \in \mathbb{N}$ such that $(s, n) = 1$ holds. Then τ^s is also a generator of the Galois group. Hence for a $b \in F^\times$ we can consider the cyclic algebra $(L/F, \tau^s, b)$.*

Lemma 2.17 *Let $a \in F^\times$ and $s \in \mathbb{N}$ with $(s, n) = 1$. Then the following map is an isomorphism of F-algebras:*

$$\Psi : (L/F, \tau^s, a^s) = \bigoplus_{i=0}^{n-1} L\nu^i \longrightarrow (L/F, \tau, a) = \bigoplus_{i=0}^{n-1} L\mu^i$$
$$\sum_{i=0}^{n-1} l_i \nu^i \longmapsto \sum_{i=0}^{n-1} l_i \mu^{si}.$$

Definition 2.18 *1. Let T be an integral domain with field of fractions F. A T-algebra Γ in an F-algebra A is called a T-order if the following points are satisfied:*

- *Γ is finitely generated as a T-module.*
- *$F\Gamma = A$.*

2. A T-order Γ is called maximal if there is no T-order $\tilde{\Gamma} \subset A$ with $\Gamma \subsetneq \tilde{\Gamma}$.

Remark 2.19 *We have considered cyclic algebras, hence in particular algebras over a* field, *we will also consider a very special kind of orders in these cyclic algebras.*

Notation 2.20 *Let $F = frac(T)$ for an integral domain T with $U := alg.int._T(L)$. For an $a \in T \setminus \{0\}$ we define the T-algebra $(U/T, \tau, a)$ analogous to a cyclic algebra over a field, to be more concrete*

$$(U/T, \tau, a) := \bigoplus_{i=0}^{n-1} U\lambda^i, \quad with \quad (L/F, \tau, a) = \bigoplus_{i=0}^{n-1} L\lambda^i,$$

hence $\lambda l = \tau(l)\lambda$ for all $l \in L$ and $\lambda^n = a$. We call $(U/T, \tau, a)$ a cyclic T-algebra.

Remarks 2.21 *Let all the data be as in Notation 2.20.*

1. *We have* $F(U/T, \tau, a) = (L/F, \tau, a)$.
2. *Let assume that* T *is integral closed. Since* L/F *is in particular a separable extension we know that* U *is finitely generated as a* T*-module and so* $(U/T, \tau, a)$ *is a* T*-order, we will refer to this algebra then also as a cyclic* T*-order.*
3. *We can restrict the matrix representation of* $(L/F, \tau, a)$ *- which was stated in Lemma 2.14 - to* $(U/T, \tau, a)$ *to to obtain a matrix representation of the* T*-order* $(U/T, \tau, a)$.

2.2 The Theorems of Hasse

In this section we will give a brief overview of the classical theory of central skewfields over complete discrete valuation domains as it was developed by Helmut Hasse (see his original article [Has31]). We follow here Hasse's classical approach which does not use the language of Brauer groups. We first need some facts about unramified extensions of complete discrete valuation domains.

Theorem 2.22 *Let* R *be a complete discrete valuation domain with field of fractions* K *and finite residue class field* $\mathfrak{k}$ *of order* m. *For each positive integer* n *there is up to isomorphism a unique unramified extension* W *of* K *with integers* S *that* $|W : K| = |\bar{S} : \bar{R}| = n$. *Namely* $W = K(\omega)$ *for* ω *a primitive* $(m^n - 1)$*-th root of unity. Furthermore,* $S = R[\omega], \quad \bar{S} = \bar{R}(\bar{\omega})$.

Proof. Cf. [Rei75, Theorem 5.10]. □

Theorem 2.23 *Let* R, K, S *etc as in Theorem 2.22. The valuation on* K *is denoted by* ν. *The norm of the field extension* W/K *is denoted by* $N_{W/K}$. *For an element* $\alpha \in K$ *are equivalent:*

1. *The equation* $N_{W/K}x = \alpha$ *is solvable in* L *i.e.,* α *is the norm of some* $x \in L$.
2. n *divides* $\nu(\alpha)$ *in* $\mathbb{Z}$.

Proof. Cf. [Rei75, Theorem 14.1] □

2.2.1 Valuations on a Skewfield

Let R be a complete discrete valuation domain with prime π and field of fractions K. Let ν be the discrete valuation which corresponds to the valuation ring R. The residue class field of R will be denoted by $\mathfrak{k}$. Moreover let D be a skewfield such that K is contained in the center of D and that the rank m of D over K is finite.

Definition 2.24 *For* $d \in D$ *we set* $\tilde{\nu}(d) := \frac{1}{|D:K|}\nu(N_{D/K}(d)) \in \mathbb{Q} \cup \{\infty\}$, *where* $N_{D/K}$ *is the norm map of* D *over* K.

Proposition 2.25 *1. The map* $\tilde{\nu} : D \longrightarrow \mathbb{Q} \cup \{\infty\}$ *has the properties of a discrete valuation i.e.:*

- *For* $d \in D$: $\tilde{\nu}(d) = \infty \Leftrightarrow d = 0$.
- $\tilde{\nu}(d_1 d_2) = \tilde{\nu}(d_1) + \tilde{\nu}(d_2) \forall d_1, d_2 \in D$.
- $\tilde{\nu}(d_1 + d_2) \geq \min\{\tilde{\nu}(d_1), \tilde{\nu}(d_2)\} \forall d_1, d_2 \in D$.

2. *$\tilde{\nu}$ is an extension of ν.*

3. *The value group of $\tilde{\nu}$ is infinite cyclic. There is some $e \in \mathbb{N}$ such that the value group of $\tilde{\nu}$ is $\frac{1}{e}\mathbb{Z}$. We set $\nu_D := e\tilde{\nu}$ and note that ν_D is an equivalent valuation on D with valuation group $\mathbb{Z}$. An element π_D of D with $\nu_D(\pi_D) = 1$ is a called a prime element of D.*

4. *An element $d \in D$ is integral over R if and only if $\omega(d) \geq 0$ holds.*

5. *We set $\Delta := \{d \in D \mid d \text{ is integral over } R\}$. Then Δ is the uniquely determined maximal order in D.*

Proof. Cf. [Rei75, Sections 12 and 13]. □

Lemma 2.26 *Every one-sided ideal of Δ is two sided. If J is an ideal of Δ then there is some $n \in \mathbb{N}$ with $J = {\pi_D}^n\Delta$. In particular Δ is a local ring, hence $\bar{\Delta} := \Delta/\pi_D\Delta$ is a skewfield over $\mathfrak{k}$.*

Lemma and Definition 2.27 1. *There is some $e' \in \mathbb{N}$ with $\pi\Delta = {\pi_D}^{e'}\Delta$. Moreover we have $e = e'$ where the valuation group of the valuation $\tilde{\nu}$ is $\frac{1}{e}\mathbb{Z}$. The natural number e is called the ramification index of D over K.*

2. *The degree $|\bar{\Delta} : \mathfrak{k}|$ is denoted by f; it is called the inertial degree of Δ over K.*

3. *The equality $m = ef$ holds.*

Proof. Cf. [Rei75, Theorem 13.3]. □

2.2.2 The Case of a Finite Residue Class Field

From now on we assume moreover that the residue class field $\mathfrak{k}$ of R is finite of order q and that the center of D is equal to K. Let $m = n^2$. We recall that n is called the index of D over K. The fact that $\mathfrak{k}$ is finite gives additional information about the ramification index e and the inertial degree f, which we state as

Lemma 2.28 *We have $e = n$ and $f = n$.*

An important first step for a description of the skewfield D is the following

Lemma and Definition 2.29 *Let f be the inertial degree of D over K. Then D contains a $q^f - 1$-th primitive root of unity. We set $L := K(\omega)$. The field L is - using Theorem 2.22 combined with the Skolem-Noether-Theorem - unique up to conjugation. We call L an inertia field of D.*

Remark 2.30 *By Lemma 2.27 we have that there is some $e \in \mathbb{N}$ with $\pi\Delta = {\pi_D}^e\Delta$ but it is not clear that we have $\pi = {\pi_D}^e$.*

Theorem 2.31 *There is a prime element $\pi_D \in \Delta$ with the following properties:*

- ${\pi_D}^n = \pi$
- $\pi_D\omega{\pi_D}^{-1} = \omega^{q^r}$ *for some $r \in \mathbb{R}$ which is relative prime to n.*

The number r is unique, we call the fraction $\frac{r}{n}$ the Hasse invariant of D.

Proof. Cf. [Rei75, Theroem 14.5]. □

Remark 2.32 *Theorem 2.31 shows that the skewfield D is a cyclic algebra. This statement is obviously consistent with Theorem 2.11. It is also true that for every r and n as in Theorem 2.31 there is a skewfield with index n and Hasse invariant $\frac{r}{n}$. Theorem 2.31 combined with the matrix representation of a cyclic algebra as stated in Lemma 2.14 gives a clue how to construct such a skewfield in $M_n(L)$.*

Theorem 2.33 *Assume that r and n are relative prime. Let ω be a primitive $q^f - 1$-th root of unity, $L = K(\omega)$ and let σ be the K-automorphism of L which maps ω to ω^{q^r}. We set*

$$\tilde{\cdot} : L \ni w \longmapsto \tilde{w} := \begin{pmatrix} w & & & \\ & \sigma(w) & & \\ & & \ddots & \\ & & & \sigma^{n-1}(w) \end{pmatrix} \in M_n(L).$$

Moreover let $\pi_D := \begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \pi & 0 & \dots & 0 \end{pmatrix}$. *We get*

- $D := K[\tilde{\omega}, \pi_D] = \bigoplus_{i,j=0}^{n-1} K\tilde{\omega}^i {\pi_D}^j = K(\omega)[\pi_D]$ *is a skewfield with center K. The index of D over K is n and its Hasse invariant is $\frac{r}{n}$.*
- $\Delta := R[\tilde{\omega}, \pi_D] = \bigoplus_{i,j=0}^{n-1} R\tilde{\omega}^i {\pi_D}^j = R[\omega][\pi_D]$ *is the uniquely determined maximal R-order in D.*

Proof. Cf. [Rei75, Theorem 14.6], the fact that it is a central simple K-algebra can also be deduced from Corollary 2.15. □

Theorem 2.34 *Let L/K an unramified extension of degree n. Let ρ be the Frobenius automorphism. We denote by φ Euler's phi function. Let $1 \leq \alpha_1, \dots, \alpha_{\varphi(n)} \leq n$ be the $\varphi(n)$ values, which are relatively prime to n. The $\varphi(n)$ cyclic algebras $(L/K, \rho, \pi^{\alpha_i})$ give a full set of non isomorphic skewfields with center K and index n.*

Proof. Cf. [Rei75, Theorem 31.1]. □

Remark 2.35 *For our purpose we prefer another representation of these skewfields, which is given by the following*

Lemma 2.36 *Let the notations be as in Theorem 2.34. The $\varphi(n)$ cyclic algebras $(L/K, \rho^{\alpha_i}, \pi)$ give also a full set of non isomorphic skewfields with center K and index n.*

Proof. Let $1 \leq \alpha \leq n-1$ with $(\alpha, n) = 1$. Then we find $s, t \in \mathbb{N}$ with $s\alpha = 1 + tn$. Assume that there is some prime p with $n = pn'$ and $s = ps'$. Then we get $1 = ps'\alpha - pn't = p(s'\alpha - n't)$, a contradiction. So we get $(s, n) = 1$. Moreover we have $\rho^{s\alpha} = \rho^{1+tn} \underset{\rho^n = \mathrm{id}}{=} \rho$. Hence

$$(L/K, \rho, \pi^\alpha) = (L/K, (\rho^s)^\alpha, \pi^\alpha) \underset{\text{Lemma 2.17}}{\simeq} (L/K, \rho^s, \alpha).$$

So we get obviously the desired bijection and we are done. □

Notation 2.37 *We call the representations in Lemma 2.36 the "standard representations" of the Hasse skewfields.*

3 Lifts and Specializations

3.1 Lifts

3.1.1 The general Definition

Let L/K be a finite cyclic Galois extension of degree n with Galois group $G = \langle\sigma\rangle$. Moreover assume $K = \mathrm{frac}(R)$ for an integral domain R and set $S := \mathrm{alg.int.}_R(L)$. Let q be an indeterminate over K.

Definition 3.1 *Let $0 \neq a \in R$ be an arbitrary element. We set $\Lambda := (S/R, \sigma, a)$ and $A := (L/K, \sigma, a)$. A lift of A is some cyclic $L(q)$-algebra A_q satisfying the following two properties:*

- *$A_q = L(q)\Lambda_f$ for $\Lambda_f = (S[q]/R[q], \sigma, f)$ with $f \in R[q]$ (hence A_q contains a cyclic $R[q]$-order).*
- *$\Lambda_f/q\Lambda_f = (S/R, \sigma, a)$.*

3.1.2 Lifts of the Standard Representation of a Hasse Skewfield

We assume for the rest of the section, that R is a complete discrete valuation ring with prime π, field of fractions K and finite residue class field $\mathfrak{k}$; $m := |\mathfrak{k}|$. We fix some $1 \leq n \in \mathbb{N}$. Theorem 2.22 yields that there is a unique unramified extension of R of degree n. We denote this extension by S and get $S = R[\omega_0]$ for a primitive $(m^n - 1)$-th root of unity ω_0. Moreover let L be the field of fractions of S and σ be a generator of the cyclic Galois group of L/K. We note that $\sigma : \omega_0 \longmapsto \omega_0{}^{q^r}$ holds for some $1 \leq r \leq n-1$ with $(r, n) = 1$. The norm of the field extension L/K will be denoted by N. Let $\nu = \nu_R$ and ν_S the π-adic valuations on R and S respectively.

Lemma 3.2 *Let $\varepsilon \in R^\times$, then there exists a unit $\alpha \in S$ with $N(\alpha) = \varepsilon$.*

Proof. Theorem 2.23 induces that there is some $\alpha \in L^\times$ with $\varepsilon = \mathrm{N}(\alpha)$. Since π is in R we have $\sigma(\pi) = \pi$. Hence we find $0 = \nu(\epsilon) = \nu_S(\mathrm{N}(\alpha)) \underset{|L:K|=n}{=} n\nu_S(\alpha)$, so $\nu_S(\alpha) = 0$ and we get that α is a unit of S. □

Corollary 3.3 *Let $\varepsilon \in R^\times$. We have $(S/R, \sigma, \varepsilon a) = (S/R, \sigma, a)$ for every $0 \neq a \in R$. (We note that we get from Theorem 2.5 just that the two corresponding cyclic K-algebras are isomorphic).*

Proof. Let $(S/R, \sigma, \varepsilon a) = \bigoplus_{i=0}^{n-1} S\lambda$ with $\lambda^n = \varepsilon a$. Lemma 3.2 induces that there is some unit $\alpha \in S$ with $\varepsilon = \prod_{i=0}^{n-1} \sigma^i(\alpha)$. Since α is a unit of S the order $(S/R, \sigma, \varepsilon a)$ contains the element $\lambda_1 := \alpha^{-1}\lambda$. To verify that we have indeed the desired equality it is enough to make the following two observations:

- For $s \in S$ we have $\lambda_1 s = \alpha^{-1}\lambda s \underset{\lambda s = \sigma(s)\lambda}{=} \sigma(s)\alpha^{-1}\lambda = \sigma(s)\lambda_1$.
- We note that an easy induction based on the above calculation yields:

$$\lambda_1{}^n = (\alpha^{-1}\lambda)^n = \mathrm{N}(\alpha^{-1})\lambda^n \underset{\mathrm{N}(\alpha)=\varepsilon, \lambda^n = \varepsilon a}{=} \varepsilon^{-1}\varepsilon a = a.$$

□

Corollary 3.4 *A lift of the standard representation of a Hasse skewfield is of the form $L(q)\Lambda_h$ with $\Lambda_h = (S[q]/R[q], \sigma, h)$ with $h \in R[q]$ and $h(0) = \varepsilon\pi$ such that ε is a unit of R.*

Proof. This follows immediately from Theorem 2.5 and Corollary 3.3. □

Corollary 3.5 *The polynomial h of Corollary 3.4 is of the form gf with f is irreducible in $S[q]$ and $f(0)$ is a prime of R which we can w.l.o.g. assume to be π and $g(0)$ is a unit of R.*

Proof. With π is also $\tilde{\varepsilon}\pi$ a prime for R if $\tilde{\varepsilon}$ is a unit of R. (We also remember Corollary 3.3). □

3.2 Specializations

In this section we will study specializations of lifts of Hasse skewfields. With the help of specializations we obtain in Theorem 3.16 or as a more general statement in Theorem 3.21 that every lift of a Hasse skewfield is a again a skewfield.

3.2.1 Some Generalities

Lemma 3.6 *Let T be an arbitrary commutative ring. Let $a \in T$ some element and q and ξ be two indeterminates over T. The map $\alpha_a : T[\xi] \ni \xi \longmapsto q - a \in T[q]$ is an isomorphism of T-algebras.*

Remark 3.7 *With the isomorphism of Lemma 3.6 we can - when we consider quotients of the form $M/(q-a)M$ - always w.l.o.g. assume that $a = 0$ holds.*

From now on we assume for the rest of this chapter, that R is a complete discrete valuation ring with prime π, field of fractions K and finite residue class field $\mathfrak{k}$. We denote $|\mathfrak{k}|$ by m. We fix some $1 \leq n \in \mathbb{N}$. Theorem 2.22 yields that there is a unique unramified extension of R of degree n. We denote this extension by S, we get $S = R[\omega_0]$ for a primitive $(m^n - 1)$-th root of unity ω_0. Moreover let L be the field of fractions of S and σ be a generator of the cyclic Galois group of L/K. We note that $\sigma : \omega_0 \longmapsto {\omega_0}^{q^r}$ holds for some $1 \leq r \leq n-1$ with $(r, n) = 1$. Moreover let q be an indeterminate over R.

We set Λ_f to be the cyclic $R[q]$-order $(S[q]/R[q], \sigma, f)$ and $D_f := (L(q)/K(q), \sigma, f)$ the corresponding cyclic $K(q)$-algebra. We consider from now on the matrix representations of D_f and Λ_f as they were given in Lemma 2.14 and in Remarks 2.21 respectively.

3.2.2 "Cyclic Algebras" with a Nilpotent Generator

Remarks 3.8 *1. When we have introduced cyclic algebras like $(L/K, \sigma, a)$ or cyclic orders as $(S/R, \sigma, b)$ (see Notation 2.20) we have assumed that the used elements $a \in K$ and $b \in R$ are* different *from 0. For studying all the specializations of a lift of Hasse skewfield we have to get rid of the assumption that $a, b \neq 0$ holds. We could either define these new algebras and orders as quotients of twisted polynomial rings (we will study this point of view in greater detail in Chapter 6) or we can realize them - which is more useful for the specializations - by the use of matrix representations, as we do it in this section.*

2. *According to Lemma 2.14 and Remarks 2.21 respectively we have matrix representations of cyclic algebras and cyclic orders. Now we will slightly modify these matrix representations. Our aim is to introduce new algebras and orders which have a structure analogous to them of cyclic ones but which are generated by a* nilpotent *element.*

Definition 3.9 *Let A be an integral domain with field of fractions F and F' a cyclic Galois extension of F oder order k with group $H = \langle\tau\rangle$. Moreover we set $B := alg.\ int._A(F')$. We identify F' via the map*

$$\tilde{} : F' \ni w \longmapsto \tilde{w} := \begin{pmatrix} w & & & \\ & \sigma(w) & & \\ & & \ddots & \\ & & & \sigma^{k-1}(w) \end{pmatrix} \in M_k(F')$$

with a subfield of $M_k(F')$ (see Lemma and Definition 2.13).

1. *We set* $N := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \ddots & & \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \in M_k(F')$.
2. *Let* $(F'/F, \tau, 0) := \bigoplus_{i=0}^{k-1} F'N^i$ *and*
3. $(B/A, \tau, 0) := \bigoplus_{i=0}^{k-1} BN^i$.

Remark 3.10 *We note that the relation $N^k = 0$ is satisfied.*

Corollary 3.11 *$(F'/F, \tau, 0)$ is an F-algebra and $(B/A, \tau, 0)$ is an A-order and we have identities*

$$(F'/F, \tau, 0) = \left\{ \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_k \\ 0 & \tau(x_1) & \tau(x_2) & \dots & \tau(x_{k-1}) \\ 0 & 0 & \tau^2(x_1) & \dots & \tau^2(x_{k-2}) \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & \tau^{k-1}(x_1) \end{pmatrix} \mid x_1, \dots, x_k \in F' \right\}$$

and

$$(B/A, \tau, 0) = \left\{ \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_k \\ 0 & \tau(x_1) & \tau(x_2) & \dots & \tau(x_{k-1}) \\ 0 & 0 & \tau^2(x_1) & \dots & \tau^2(x_{k-2}) \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & \tau^{k-1}(x_1) \end{pmatrix} \mid x_1, \dots, x_k \in B \right\}.$$

3.2.3 The Specialization Map

Notation 3.12 *We define the map $\Phi_0 : (S[q]/R[q], \sigma, f) \longmapsto (S/R, \sigma, f(0))$ by setting*

$$\Phi_0 : \sum_{i=0}^{n-1} \widetilde{s_i}\lambda^i \longmapsto \sum_{i=0}^{n-1} \widetilde{s_i(0)}\lambda_0,$$

where $\lambda_0 := \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ f(0) & & & 0 \end{pmatrix} \in (S/R, \sigma, f(0))$. *We call Φ_0 the specialization map at 0. We will sometimes denote $\Phi_0(x)$ by $x_{q=0}$ for $x \in (S[q]/R[q], \sigma, f)$.*

Remarks 3.13 *1. We note that $f(0)$ can be equal to 0, so we have to interpret the algebra $(S/R, \sigma, f(0))$ in the sense of Definition 3.9.*

2. The map $\tilde{}: L \longrightarrow M_n(L)$ extends to a map $\tilde{}: L(q) \longrightarrow M_n(L(q))$. For an arbitrary element $h \in S[q]$ we have an equality $\widetilde{h(0)} = \tilde{h}(0)$, where $\tilde{h}(0)$ has to be read as the entry-wise specialization of the matrix $\tilde{h}$.

Lemma 3.14 *The specialization map Φ_0 is a surjective homomorphism of R-algebras with kernel $q\Lambda_f$, so $\Lambda_f/q\Lambda_f \simeq (S/R, \sigma, f(0))$.*

Proof. Straightforward calculation. □

Remark 3.15 *We can use Remark 3.7 and Lemma 3.14 to reduce specializations at elements $0 \neq a \in R$ to the case $a = 0$.*

3.2.4 Lifts are Skewfields - A direct Calculation

Now we assume that we are in the situation of Section 3.1.2 and all notations and assumptions of this section are valid. We consider the standard representation of a Hasse skewfield D and a lift D_f of this standard representation. We have $D_f = L(q)\Lambda_f$ with $\Lambda_f = (S[q]/R[q], \sigma, f)$ with $f \in R[q]$ and $f(0) = \varepsilon\pi$ such that ε is a unit of R. Using Corollaries 3.3 and 3.5 we can w.l.o.g. $f(0) = \pi$ assume.

Theorem 3.16 *The algebra D_f is a skewfield, this means that a lift of a Hasse skewfield is again a skewfield.*

Proof. Let us assume that $x = s_0 + s_1\lambda + s_2\lambda^2 + \cdots + s_{n-1}\lambda^{n-1}$ is a zero divisor of D, hence there has to be some $0 \neq y = t_0 + t_1\lambda + t_2\lambda^2 + \cdots + t_{n-1}\lambda^{n-1} \in D_f$ with $xy = 0$. Since an element $d \in D_f$ is equal to 0 if and only if $sd = 0$ for some $0 \neq s \in L[q]$ we can w.l.o.g. assume that the elements s_i and t_j are in $S[q]$. Hence w.l.o.g. $x, y \in \bigoplus_{i=0}^{n-1} S[q]{\nu_f}^i = (S[q]/R[q], \sigma, f)$. Let us assume that every s_i is divided by q, then $q^{-1}x$ is also a zero divisor. So we can assume w.l.o.g. that neither every s_i is divisible by q nor every t_j is divisible by q. Now we get

$$0 = (xy)_{q=0} \underset{\text{Lemma 3.14}}{=} x_{q=0}y_{q=0} = \Big(\sum_{i=0}^{n-1} {s_i}_{q=0}{\lambda^i}_{q=0}\Big)\Big(\sum_{j=0}^{n-1} {t_j}_{q=0}{\lambda^j}_{q=0}\Big)$$
$$= \Big(\sum_{i=0}^{n-1} {s_i}_{q=0}{\lambda_0}^i\Big)\Big(\sum_{j=0}^{n-1} {t_j}_{q=0}{\lambda_0}^j\Big),$$

both of the last factors are not zero, because we have assumed that not all s_i's and not all t_j's are divisible by q. But we know that $K(S/R, \sigma, f(0))$ is a skewfield by Lemma 2.36. So D_f contains no zero divisors, hence D_f is a skewfield, since D_f is a finite dimensional algebra over a field. □

Remark 3.17 *The proof of Theorem 3.16 was based on a direct matrix calculation in the Hasse skewfield D which we represent as a sub-algebra of $M_n(L)$. In the next section we will give a more formal reason for Theorem 3.16 to hold.*

3.2.5 Lifts are Skewfields - A more formal Proof

We recall Herstein's Lemma, which is deduced from Krull's Intersection Theorem and Nakayama's Lemma.

Lemma 3.18 (Herstein's Lemma) *Let $(T, \mathfrak{m})$ be a local Noetherian commutative ring, let $\mathfrak{a} \subset \mathfrak{m}$ be an ideal of T, and let M be a finitely generated T-module. Then*

$$0 = \tilde{M} := \bigcap_{n \in \mathbb{N}} \mathfrak{a}^n M.$$

A direct consequence is the following corollary which will be needed later on.

Corollary 3.19 *Let T be a commutative Noetherian domain, let $\mathfrak{a} \neq T$ be an ideal of T, and let M be a finitely generated torsion free T-module. Then*

$$0 = \tilde{M} := \bigcap_{n \in \mathbb{N}} \mathfrak{a}^n M.$$

Proof. Choose a maximal ideal $\mathfrak{m}$ of T with $\mathfrak{a} \subset \mathfrak{m}$. The Corollary follows immediately from applying Herstein's Lemma to the local data $\mathfrak{a}_{\mathfrak{m}}$ and $M_{\mathfrak{m}}$. □

Lemma 3.20 *Let R be a commutative Noetherian integral domain with field of fractions K and let Λ be an R-order in a K-algebra A. Let $q \in R$ be an arbitrary non unit of R. If $\Lambda/q\Lambda$ has no zero divisors then A is a skewfield.*

Proof.

1. In a first step we show that there are no zero divisors contained in Λ. Assume $0 \neq \lambda$ is a zero divisor of Λ. So there exists an element $0 \neq \tilde{\lambda}$ with $\lambda\tilde{\lambda} = 0$. An element $\mu \in \Lambda$ with $\mu = q\tilde{\mu}$ for some element $\tilde{\mu}$ is obviously a zero divisor if and only if $\tilde{\mu}$ is a zero divisor (we use that an R-order is torsion free as an R-module). Corollary 3.19 implies $\bigcap_{n \in \mathbb{N}} q^n \Lambda = 0$. So we can w.l.o.g. assume that $\lambda, \tilde{\lambda} \notin q\Lambda$ is satisfied and we have still $\lambda, \tilde{\lambda} \neq 0$. The equation $\lambda\tilde{\lambda} = 0$ carries over to an equation modulo q: $(\lambda + q\Lambda)(\tilde{\lambda} + q\Lambda) = 0$. We have by assumption that no zero divisors contained in $\Lambda/q\Lambda$, so either $\lambda + q\Lambda = 0$ or $\tilde{\lambda} + q\Lambda = 0$. This yields that one of the elements λ and $\tilde{\lambda}$ is contained in $q\Lambda$, a contradiction.

2. Assume that $0 \neq a \in A$ is a zero divisor. Hence there is $0 \neq \tilde{a} \in A$ with $a\tilde{a} = 0$. We find elements $0 \neq s, \tilde{s} \in R$ with $sa, \tilde{s}\tilde{a} \in \Lambda$. Since $(sa)(\tilde{s}\tilde{a}) = 0$ in Λ holds, we get from the first step $sa = 0$ or $\tilde{s}\tilde{a} = 0$ and so $a = 0$ or $\tilde{a} = 0$, a contradiction and so A contains also no zero divisors.

3. Λ is an R-order, hence finitely generated over R, so A has finite dimension as a vector space over K. This implies that A is an Artin algebra. We can apply [Bou58, §3, n° 2, Lemme 3] to deduce that every non zero divisor is invertible. This yields that A is a skewfield and we are done.

□

We can generalize Lemma 3.20 to

Theorem 3.21 *Let R be a Noetherian commutative integral domain with field of fractions K. Let Λ be an R-order in a K-algebra A, and let $\mathfrak{a} \neq R$ be an invertible ideal of R. If $\Lambda/\mathfrak{a}\Lambda$ has no zero divisors then A is a skewfield.*

Proof.

1. Corollary 3.19 yields that there is an $n \in \mathbb{N}$ with $x \in \mathfrak{a}^n\Lambda \setminus \mathfrak{a}^{n+1}\Lambda$.

   Claim. There is an element $\alpha \in \mathfrak{a}^{-1}$ with $\alpha x \in \mathfrak{a}^{n-1}\Lambda \setminus \mathfrak{a}^n\Lambda$. So by induction we find some $k \in K$ with $kx \in \Lambda \setminus \mathfrak{a}\Lambda$.

   Proof of the Claim. We have

   $$\mathfrak{a}^{-1}x \subset \mathfrak{a}^{-1}(\mathfrak{a}^n\Lambda) = (\mathfrak{a}^{-1}\mathfrak{a})\mathfrak{a}^{n-1}\Lambda \underset{\mathfrak{a}^{-1}\mathfrak{a}=R}{=} \mathfrak{a}^{n-1}\Lambda.$$

   Now assume $\mathfrak{a}^{-1}x \subset \mathfrak{a}^n\Lambda$. Then $Rx \underset{\mathfrak{a}^{-1}\mathfrak{a}=R}{=} \mathfrak{a}\mathfrak{a}^{-1}x \subset \mathfrak{a}\mathfrak{a}^n\Lambda = \mathfrak{a}^{n+1}\Lambda$, a contradiction. □

2. So if x, y are two elements of Λ with $x, y \neq 0$ but $xy = 0$ we can w.l.o.g. assume that $x, y \notin \mathfrak{a}\Lambda$ holds.
3. The rest of the proof is analogous to the proof of Lemma 3.20.

□

Corollary 3.22 *Let R be a Noetherian local factorial Krull Domain with field of fractions K. Let Λ be an R-order in a K-algebra A, and let $\mathfrak{a} \neq R$ be a divisorial ideal of R. If $\Lambda/\mathfrak{a}\Lambda$ has no zero divisors then A is a skewfield.*

Proof. Since R is local factorial Noetherian Krull Domain Proposition 10.10 yields that $\mathfrak{a}$ is projective over R, hence $\mathfrak{a}$ is an invertible ideal of R, so we can apply Theorem 3.21. □

Corollary 3.23 *Let R be a local factorial Noetherian Krull Domain with field of fractions K and Λ an R-order in a K-algebra A. For an element $x \in \Lambda$ we have: If there is a divisorial ideal $\neq \mathfrak{a}$ of R such that $x + \mathfrak{a}\Lambda$ is not a zero divisor, then x itself is not a zero divisor.*

Proof. Assume we find an element $y \in \Lambda$ with $y \neq 0$ and $xy = 0$. Then we can by the proof of Lemma 3.22 w.l.o.g. assume that $y \notin \mathfrak{a}\Lambda$ is satisfied, hence a contradiction and so x can not be a zero divisor of Λ. □

Lemma 3.24 *Let R be a local factorial Noetherian Krull Domain with field of fractions K and Λ an R-order in a K-algebra A. For en element $x \in \Lambda$ are equivalent:*

1. *x is not a zero divisor of Λ.*
2. *There is an element $\mathfrak{p} \in ht^1(R)$ with $x + \mathfrak{p}\Lambda$ is not a zero divisor in $\Lambda/\mathfrak{p}\Lambda$.*

Proof. (1) $\Longrightarrow$ (2): If x is not a zero divisor we have an isomorphism of Λ- and so of course of R-modules $\Lambda \simeq \Lambda x$. So Λx is a full R-lattice in A. Since R is a Krull domain, we have $\Lambda_\mathfrak{p} = (\Lambda x)_\mathfrak{p} = \Lambda_\mathfrak{p}\frac{x}{1}$ for almost all elements of $\mathrm{ht}^1(R)$. Now choose an element $\mathfrak{p} \in \mathrm{ht}^1(R)$ with $\Lambda_\mathfrak{p} = \Lambda_\mathfrak{p}\frac{x}{1}$, hence $\frac{x}{1}$ is a unit of $\Lambda_\mathfrak{p}$ (use that $\Lambda_\mathfrak{p}$ is a Noetherian ring). In particular we get by Nakayama's Lemma that $\frac{x}{1}$ is not contained in $\mathfrak{p}\Lambda_\mathfrak{p}$. So $\frac{x}{1} + \mathfrak{p}\Lambda_\mathfrak{p}$ is a unit of $\Lambda_\mathfrak{p}/\mathfrak{p}\Lambda_\mathfrak{p} = R_\mathfrak{p}\Lambda/\mathfrak{p}\Lambda$. But so $x + \mathfrak{p}\Lambda$ can not be a zero divisor.

(2) $\Longrightarrow$ (1): This follows immediately from Corollary 3.23. □

3.2.6 Non Lifts

Remark 3.25 *We have seen that if $\Lambda/\mathfrak{a}\Lambda$ contains no zero divisors for some divisorial ideal $\mathfrak{a}$ then $A = K\Lambda$ is a skewfield. In general it is not true that if A is a skewfield then $\Lambda/\mathfrak{p}\Lambda$ contains no zero divisors. We will now give a counterexample.*

Lemma 3.26 *Let $D := (L(q)/K(q), \sigma, fg)$ where f, g are two polynomials in $R[q]$ such that f is irreducible in $S[q]$ and f divides not g. Then D is a skewfield.*

Proof. We pass - as usual - over to the canonical matrix representation of the cyclic algebra D. Let $x := \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ fg\sigma(x_n) & \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_{n-1}) \\ fg\sigma^2(x_{n-1}) & fg\sigma^2(x_n) & \sigma^2(x_1) & \dots & \sigma^2(x_{n-2}) \\ & & & \ddots & \\ fg\sigma^{n-1}(x_2) & fg\sigma^{n-1}(x_3) & fg\sigma^{n-1}(x_4) & \dots & \sigma^{n-1}(x_1) \end{pmatrix}$ be a zero divisor of D. We can w.l.o.g. assume that all the $x_i's$ are contained in $S[q]$. Furthermore we can assume that f divides not all of them. Since x is a zero divisor of D we get $\det(x) = 0$. We find $\det(x) = N(x_1) + fg \cdot h$ for some element $h \in S[q]$. Since we assume that f is irreducible in $S[q]$ f divides some $\sigma^i(x_1)$, hence f divides x_1 since $f \in R[q]$ holds, so there is some $x_1' \in S[q]$ with $x_1 = fx_1'$. Now we assume by induction that there is some $k \leq n-1$ and elements $x_1', x_2', \dots, x_k'$ with $x_i = fx_i'$ for all $1 \leq i \leq k$. Using again the relation $\det(x) = 0$ and the induction hypotheses we conclude $a^k N(x_{k+1}) = a^{k+1}\tilde{h}$ for some element $\tilde{h} \in S[q]$. Since f divides not g in $S[q]$ and f is irreducible in $S[q]$ we find that f divides some $\sigma^j(x_{k+1})$ and hence f divides x_{k+1}. So by induction f divides all the x_i, a contradiction. This means D contains no zero divisors and so D is a skewfield. □

Example 3.27 *We set $f := \pi q - 1$ and $g := (\pi q^2 - 1)^{n-1}$. For every element $r \in R$ we have $\nu(f(r)g(r))$ congruent 0 mod n. Then $f(r)g(r)$ is a norm of the field extension L/K.*

Proof. For every $a \in R$ we have $(fg)(a) = (\pi a - 1)(\pi a^2 - 1)^{n-1}$ a unit by Nakayama's Lemma. So $(fg)(a)$ is a norm by Theorem 2.23. □

Corollary 3.28 *Let f and g be as in Example 3.27. We consider the cyclic algebra $D := (L(q)/K(q), \sigma, fg)$. We observe that f is of degree 1 and so surely irreducible in $S[q]$, an easy calculation yields that f divides not g in $S[q]$. So we can apply Lemma 3.26 to deduce that D is a skewfield. We set $\lambda := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & 1 \\ fg & 0 & 0 & \dots & 0 \end{pmatrix}$ and $\Lambda := \bigoplus_{i=0}^{n-1} S[q]\lambda^i$. For every $a \in R$ we have that $K(\Lambda/a\Lambda)$ is isomorphic to $M_n(K)$, since $(fg)(a)$ is a norm by Example 3.27. So Λ is not a lift.*

3.2.7 The possible Structures of Specializations

Let us return to the notations and assumptions of Section 3.2.4. Hence we consider the standard representation of a Hasse skewfield D and a lift $D_f = L(q)\Lambda_f$ with $\Lambda_f = (S[q]/R[q], \sigma, f)$ with $f \in R[q]$ and w.l.o.g. $f(0) = \pi$ (remember Corollaries 3.3 and 3.5). In Section 3.2.4 we have considered the natural specialization of D_f at $a = 0$, hence we have passed over to the original Hasse skewfield $D = \Lambda_f/q\Lambda_f$. Now we will study the other possible specializations of D_f or better of Λ_f, i.e. we will consider the quotients $\Lambda_a := \Lambda_f/(q-a)\Lambda_f$ for $a \in R$. Using Remark 3.7 and Lemma 3.14 we know that we have an isomorphism $\Lambda_a \simeq (S/R, \sigma, f(a))$.

We have to distinguish two cases for the element a:

Let us first assume that a is not a zero of the polynomial f, then we find a unit $\varepsilon \in R$ and some $1 \leq s \in \mathbb{N}$ with $f(a) = \varepsilon\pi^s$ and so we get

$$K\Lambda_a = K(S/R, \sigma, \varepsilon\pi^s) \underset{\substack{\text{Theorem 2.5} \\ \text{and Theorem 2.11}}}{\simeq} K(S/R, \sigma, \pi^s).$$

Then [Rei75, Theorem 31.5] yields that there is - depending on (s, n) - some $k \in \mathbb{N}$ and a central skewfield D_1 over K which is contained in $B(K_1/K)$ such that K_1 is an unramified extension of K and that $K(S/R, \sigma, \pi^s) \simeq M_k(D_1)$ holds, hence $K\Lambda_a$ is a central simple K-algebra and so in particular a semi-simple ring.

Now we consider the case that $f(a) = 0$ holds. We can apply Corollary 3.11 to obtain

$$\Lambda_f/a\Lambda_f \simeq (S/R, \sigma, 0) = \left\{ \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_m \\ 0 & \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_{m-1}) \\ 0 & 0 & \sigma^2(x_1) & \dots & \sigma^2(x_{m-2}) \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & \sigma^{m-1}(x_1) \end{pmatrix} \mid x_1, \dots, x_m \in S \right\}.$$

In this situation we are also in the position to apply Corollary 5.6 to conclude that the we have an isomorphism

$$K\Lambda_a \simeq L[x, \sigma]/(x^n),$$

where $L[x, \sigma]$ denotes the twisted polynomial ring. We will study these quotients of twisted polynomial rings in a greater detail in Chapter 6 and there we will see that these algebras are very far away from being semi-simple.

4 The Maximal Lifts of the Maximal Order

We use the notations and preliminaries of Section 3.1.2. We fix a Hasse skewfield D in our standard representation (see Notation 2.37), hence $D = (L/K, \sigma, \pi)$, where σ is some generator of the Galois group $\mathrm{Gal}(L/K)$ (so there is some $1 \leq r \leq n-1$ with $(r,n) = 1$ and $\sigma = \rho^r$, where ρ is the Frobenius homomorphism). D contains the uniquely determined maximal order $\Lambda := (S/R, \sigma, \pi)$.

In this chapter we will consider lifts of the form $A_{\tilde{f}} := L(q)(S[q]/R[q], \sigma, \tilde{f})$ with $\tilde{f} = \left(\prod_{i=1}^{t} g_i\right) f$ such that f is irreducible in $S[q]$ and $f(0) = \pi$ and the g_i's are pairwise different polynomials in $R[q]$ which are irreducible in $S[q]$ such that the following points are satisfied:

- $g_i(0) = \varepsilon_i \in R^\times$ for every $1 \leq i \leq t$, so we have in particular that $fR[q] \neq g_i R[q]$ holds for all the i's.
- The prime ideals $g_i R[q]$ are pairwise different, this means that the g_i are pairwise non adjoint prime elements of $R[q]$.

We note that all the polynomials f and g_i $(1 \leq i \leq t)$ are irreducible in $R[q]$ since they are assumed to be irreducible in $S[q]$. This follows immediately from

Lemma 4.1 *Let B/A an integral extension of factorial domains. If an element $p \in A$ is irreducible in B then we have*

1. *$pB \cap A = pA$ and*
2. *p is irreducible in A.*

Proof. Since p is irreducible in B we have $pB \in \mathrm{ht}^1(B)$. We set $\mathfrak{p} := pB \cap A$ and get $\mathfrak{p} \in \mathrm{Spec}(A)$. A is a factorial ring and so integrally closed, hence we can apply Lemma 4.29 to conclude $\mathfrak{p} \in \mathrm{ht}^1(A)$. Since A is factorial we find a prime element $\tilde{p}$ of A with $\mathfrak{p} = \tilde{p}A$ and get $pB = \tilde{p}B$. Since $pA \subset \tilde{p}A$ holds there is an $a \in A$ with $p = \tilde{p}a$ and so $\tilde{p}aB = \tilde{p}B$, hence a is a unit of B. Lemma 4.33 induces that a is also a unit of A and so p is a prime element of A and we get $pB \cap A = pA$. □

Corollary 4.2 *Let the notations be as in Lemma 4.1. For two prime elements p and q of A, which are also prime in B, are equivalent:*

1. *p and q are not adjoint in A.*
2. *p and q are not adjoint in B.*

Proof. (1) $\Longrightarrow$ (2) : Let p and q be not adjoint in A, but assume that $pB = qB$ holds. Since p and q are prime elements in A and B respectively, we can apply Lemma 4.1 to conclude $pA = A \cap pB = A \cap qB = qA$, a contradiction.

(2) $\Longrightarrow$ (1) : Assume $pA = qA$, then $pB = qB$, a contradiction. □

In the lift $A_{\tilde{f}}$ we will consider the lift $\Lambda_{\tilde{f}} := (S[q]/R[q], \sigma, \tilde{f})$ of the maximal order Λ in D and will show the

Theorem 4.81 *The lift $\Lambda_{\tilde{f}}$ of the maximal order Λ is again a maximal oder.*

In the first section of this chapter we will give a short outline of the proof of Theorem 4.81, which uses the structure of the orders $\Lambda_{\tilde{f},\mathfrak{p}} := \left(\Lambda_{\tilde{f}}\right)_{\mathfrak{p}}$ for $\mathfrak{p} \in \mathrm{ht}^1(R[q]))$. After the outline of the proof of Theorem 4.81 we state in the Sections 4.2 - 4.6 a few results of technical nature which are needed to understand the orders $\Lambda_{\tilde{f},\mathfrak{p}}$.

4.1 An Outline of the Proof of Theorem 4.81

To verify that $\Lambda_{\tilde{f}}$ is a maximal order we will use a well-known criteria which is due to Auslander and Goldmann.

Theorem 4.3 *Let T be an integrally closed Noetherian domain with field of fractions F. Moreover let Γ be a T-order which is contained in central simple F-algebra B. The following are equivalent:*

- *Γ is a maximal T-order.*
- *Γ satisfies the following two properties:*
  1. *$\Gamma^{**} = \Gamma$. (If M is some T-lattice in the F-vector space $V = FM$, we identify M^{**} with a lattice in V, here we use the canonical isomorphisms $F(M^{**}) \simeq \mathrm{Hom}_F(\mathrm{Hom}_F(FM, F), F) \simeq FM$).*
  2. *For every $\mathfrak{p} \in ht^1(T)$ the $T_{\mathfrak{p}}$-order $\Gamma_{\mathfrak{p}}$ is maximal.*

Proof. Cf. [AG60, Theorem 1.17]. □

So we will verify:

1. $\Lambda_{\tilde{f}}$ is reflexive, i.e. $\Lambda_{\tilde{f}} = \left(\Lambda_{\tilde{f}}\right)^{**}$ holds.
2. $\Lambda_{\tilde{f},\mathfrak{p}}$ is a maximal $R[q]_{\mathfrak{p}}$-order for every $\mathfrak{p} \in \mathrm{ht}^1(R[q])$.

Let us sketch how we will prove these points:

Ad (1): In our case the order $\Lambda_{\tilde{f}}$ is free over $R[q]$, so this point is trivial (since every free module is reflexive).

Ad (2): Here we awake again a Theorem of Auslander and Goldman, which gives a criteria when an order over a discrete valuation domain is maximal:

Theorem 4.4 *Let T be a discrete valuation domain with field of fractions F. For a T-order Γ in a central simple F-algebra B are equivalent:*

- *Γ is maximal.*
- *Γ satisfies the following two properties:*
  (a) Γ is hereditary.
  (b) $rad(\Gamma)$ is its unique maximal two-sided ideal.

Proof. Cf. [AG60, Theorem 2.3] □

So we have to check that for every $\mathfrak{p} \in \mathrm{ht}^1(R)$ the order $\Lambda_{\tilde{f},\mathfrak{p}}$ satisfies the two conditions of Theorem 4.4.

Ad (a) We use a result which is again due to Auslander and Goldmann:

Lemma 4.5 *Let T be a discrete valuation domain and Γ a T-algebra which is finitely generated and torsionfree as T-module. If rad(Γ) is projective, then Γ is a hereditary ring.*

Proof. Cf. [AG60, Corollary to Theorem 2.2]. □

With Lemma 4.5 it will be enough to check that $\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ is a projective $\Lambda_{\tilde{f},\mathfrak{p}}$-module.

Ad (b) To verify that $\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ is the unique maximal two-sided ideal of $\Lambda_{\tilde{f},\mathfrak{p}}$ we will calculate the quotients $\overline{\Lambda_{\tilde{f},\mathfrak{p}}} := \Lambda_{\tilde{f},\mathfrak{p}}/\mathrm{rad}(\Lambda_{\tilde{f},\mathfrak{p}})$ and show that they are simple algebras.

4.2 A "non commutative Valuation Domain"

Remark 4.6 *Let T be a complete discrete valuation domain and denote by π some prime number of T, we denote the field of fractions of T by L. Let D be a skewfield of finite rank over L such that L is contained in the center of D. We denote the discrete valuation of the field L belonging to the valuation domain T by ν. Then there is a unique extension of ν to a map $\omega : D \longrightarrow \mathbb{Q}$ which has the properties of a discrete valuation. This map was given by $\omega(d) := \frac{1}{[D:L]}\nu(N_{D/L}(d))$, where $N_{D/L}$ is the norm map of D over L (see for example [Rei75, Sections 12 and 13]). Using the valuation map ω we have obtained that*

- *an element $d \in D$ is integral over T if and only if $\omega(d) \geq 0$ holds and that $\Gamma_D := \{d \in D \mid \omega(d) \geq 0\}$ is the unique maximal T-order in D.*
- *The value group of ω is $\frac{1}{e}\mathbb{Z}$ for some $1 \leq e \in \mathbb{N}$.*

Passing over to the equivalent valuation $\nu_D := e\omega$ these facts have heavy consequences for the ideal structure of the maximal order $\Gamma_D \subset D$ as stated in the Lemma 2.26:

- *Since ν_D is a discrete valuation there is at least one element $\pi_D \in \Gamma_D$ with $\nu_D(\pi_D) = 1$, we have called such elements prime elements of Γ_D or of D.*
- *Every left and right ideal of Γ_D is a two-sided ideal and the ideals ${\pi_D}^n\Gamma_D$ give a complete list of the ideals of Γ_D.*

All in all we can describe the order Γ_D in some sense as a non-commutative discrete valuation domain, this description was obtained by using the discrete valuation ν_D, which existence is based on the completeness of T. A closer examination shows that these properties are indeed properties of the prime π_D.

Lemma 4.7 *Let T be an arbitrary integral domain with field of fractions L and $\Gamma \subset M_n(E)$ is a T-order where E is some field extension of L. If det(γ) is in $T^\times$, then γ is invertible in Γ.*

Proof. Since Γ is a T-order we know that γ is integral over T. An easy application of the Lemma of Gauss yields that the characteristic polynomial χ of γ is contained in $T[q]$. The Theorem of Cayley and Hamilton yields $\chi(\gamma) = 0$, hence there are some elements $a_{n-1}, \ldots, a_1 \in T$ with $\gamma^n + a_{n-1}\gamma^{n-1} + \cdots + a_1\gamma = \det(\gamma)$. Since $\det(\gamma)$ is invertible in T we get $\gamma \cdot \underbrace{\left(\det(\gamma)\left(\gamma^{n-1} + a_{n-1}\gamma^{n-2} + \cdots + a_1\right)\right)}_{\in \sum_{i=0}^{n-1} T\gamma^i \subset \Gamma} = 1$. □

For the rest of this section let R be an arbitrary discrete valuation domain with prime π and maximal ideal $\mathfrak{p} = \pi R$. We *do not* assume that R is complete with respect to the π-adic topology. The field of fractions of R will be denoted by K. Furthermore let W/K be a cyclic Galois extension of K of degree n with group $G := \langle\sigma\rangle$. We set $S :=$ alg. int.$_R(W)$. We assume that S is also a discrete valuation domain and that the extension is unramified, so π is a prime of S. The corresponding discrete valuations will be denoted by ν_R and ν_S. We fix some $\varepsilon \in R^\times$ and set $\Lambda := (S/R, \sigma, \varepsilon\pi)$. We pass over to the matrix representation of Λ which was stated in Remarks 2.21. This means we have $\Lambda = \bigoplus_{i=0}^{n-1} S\lambda^i$ with $\lambda := \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \\ & & & 1 \\ \varepsilon\pi & 0 & \dots & 0 \end{pmatrix}$ and the field W and the ring S respectively will be identified with its image under the following homomorphism:

$$W \ni w \longmapsto \tilde{w} := \begin{pmatrix} w & & & \\ & \sigma(w) & & \\ & & \ddots & \\ & & & \sigma^{n-1}(w) \end{pmatrix} \in M_n(W).$$

Remark 4.8 *If ε is a unit of R then $\varepsilon\pi$ is also a prime element of R and of S respectively, so we can w.l.o.g. assume that from now on $\varepsilon = 1$ holds.*

Observation 4.9 *$\lambda^n = \pi \in S$ and so λ is invertible in $M_n(W)$ with $\lambda^{-1} = \frac{1}{\pi}\lambda^{n-1}$.*

Notation 4.10 *Let $x = \tilde{a_0} + \tilde{a_1}\lambda + \dots + \tilde{a_{n-1}}\lambda^{n-1}$ be an arbitrary element of Λ.*

Observation 4.11 *For the element x are equivalent:*

1. *$x\lambda^{-1}$ is contained in Λ.*
2. *$\tilde{a_0}\lambda^{-1} \in \Lambda$ holds.*

Proof. This is immediately deduced from the following equation:

$$\begin{aligned} x\lambda^{-1} &= \left(\tilde{a_0} + \tilde{a_1}\lambda + \dots + \tilde{a_{n-1}}\lambda^{n-1}\right)\lambda^{-1} = \tilde{a_0}\lambda^{-1} + \tilde{a_1}\lambda\lambda^{-1} + \dots + \tilde{a_{n-1}}\lambda^{n-1}\lambda^{-1} \\ &= \tilde{a_0}\lambda^{-1} + \underbrace{\tilde{a_1} + \tilde{a_2}\lambda + \dots + \tilde{a_{n-1}}\lambda^{n-2}}_{\in\Lambda} \end{aligned}$$

□

Lemma 4.12 *Equivalent are*

(1) $\tilde{a_0}\lambda^{-1} \in \Lambda$.

(2) $\frac{a_0}{\pi} \in S$.

(2′) $\nu_S(a_0) \geq 1$.

Proof. (2) $\Leftrightarrow$ (2′): Obvious.
(1) $\Leftrightarrow$ (2): A straightforward matrix calculation yields:

$$\tilde{a_0}\lambda^{-1} = \begin{pmatrix} 0 & \dots & 0 & \frac{a_0}{\pi} \\ \pi\sigma(\frac{a_0}{\pi}) & & & \\ & \ddots & & \vdots \\ & & \pi\sigma^{n-1}(\frac{a_0}{\pi}) & 0 \end{pmatrix},$$

the last matrix is in Λ if and only if $\frac{a_0}{\pi} \in S$ and we are done. □

Observation 4.13 *We have - dependent on n - $det(\lambda^{-1}) = \frac{1}{\pi}$ or $det(\lambda^{-1}) = -\frac{1}{\pi}$, hence we have $det(\lambda^{-1}) = \varepsilon\frac{1}{\pi}$ for some $\varepsilon \in R^\times$.*

Proof. This done by a straightforward calculation using $\lambda^{-1} = \begin{pmatrix} 0 & \dots & 0 & \frac{1}{\pi} \\ 1 & & & \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix}$. □

Lemma 4.14 *Let $x \in \Lambda$ with $det(x) = a\pi$ for some element $a \in R$, then $x\lambda^{-1} \in \Lambda$ holds and we get a representation $x = (x\lambda^{-1})\lambda$ in Λ and moreover we have $det(x\lambda^{-1}) = a$ or $det(x\lambda^{-1}) = -a$.*

Proof.

- Let $\det(x) = a\pi \in R$. We denote the norm of the field extension W/K by N. We have $x = \begin{pmatrix} a_0 & & \\ \pi * & \ddots & * \\ & & \sigma^{n-1}(a_0) \end{pmatrix} \in M_n(W)$. We obtain $\det(x) = N(a_0) + r\pi$ for some element $r \in R$, hence $N(a_0) + \pi r = \pi a$. This yields immediately that π divides $N(a_0)$. Since S/R is an unramified extension we get that π has also to divide a_0. But this means $\frac{a_0}{\pi} \in S$ and so Lemma 4.12 yields $x\lambda^{-1} \in \Lambda$.
- From Observation 4.13 we get immediately

$$\det(x\lambda^{-1}) = \det(x)\det(\lambda^{-1}) = \pm a\pi\frac{1}{\pi} = \pm a.$$

□

Lemma 4.15 *Every element $x \in \Lambda$ can be written in the form $u\lambda^n$, where u is a unit of Λ and n is some natural number. If we have $det(x) = \varepsilon\pi^{\tilde{n}}$ for $\varepsilon \in R^\times$ and some $\tilde{n} \in \mathbb{N}$, then $n = \tilde{n}$ holds.*

Proof. Λ is an R-order, so every element $x \in \Lambda$ is integral over R, using the Lemma of Gauss and the Theorem of Cayley and Hamilton we get that in particular $\det(x)$ is in R. Since R is a discrete valuation domain with prime π we find a unit $\varepsilon \in R$ and some $n \in \mathbb{N}$ with $\det(x) = \varepsilon\pi^n$. Now we will use induction on n.

- Let us assume that $n = 0$ holds, hence $\det(x) = \varepsilon$ is a unit of R, so we get from Lemma 4.7 that x is a unit of Λ.
- For $n \geq 1$ we are done with Lemma 4.14.

The induction proof shows also that if we have $\det(x) = \varepsilon\pi^n$ then we obtain a representation of x in the form $x = u\lambda^n$ for some unit u. □

Remark 4.16 *Let $x \in \Lambda$ such that $x = u\lambda^n = \tilde{u}\lambda^{\tilde{n}}$ for $u, \tilde{u} \in \Lambda^\times$ and $n, \tilde{n} \in \mathbb{N}$ then we have $n = \tilde{n}$.*

Proof. We know from Lemma 4.15 that the occurring n is the same as in $\det(x) = \varepsilon\pi^n$ and so we are done. □

Observation 4.17 *Using the relation $\tilde{a}\lambda = \lambda\widetilde{\sigma(a)}$ for every $a \in S$ we obtain that for every $x \in \Lambda$ there is some $y \in \Lambda$ with $x\lambda = \lambda y$ and we have of course $det(x) = det(y)$. So we get immediately the*

Corollary 4.18 *For every $x \in \Lambda$ with the representation $x = u\lambda^n$ for a unit u and uniquely determined element $n \in \mathbb{N}$ there is a unit u' in Λ with $x = \lambda^n u'$.*

Lemma 4.19 *1. Let $I \subset \Lambda$ be a left ideal then there is some $n \in \mathbb{N}$ with $I = \Lambda\lambda^n$.*

2. Let $I \subset \Lambda$ a right ideal the there is some $m \in \mathbb{N}$ with $I = \lambda^m\Lambda$.

3. For every $n \in \mathbb{N}$ we have moreover $\lambda^n\Lambda = \Lambda\lambda^n$, so every one-sided ideal of Λ is actually a two-sided one.

4. We have $rad(\Lambda) = \lambda\Lambda = \Lambda\lambda$ and Λ is a local ring and $rad(\Lambda)$ is the unique maximal two sided ideal of Λ.

Proof.

1. Let I be a left ideal of Λ. Every $x \in I$ has representation $x = u\lambda^n$ for some unit u and a uniquely determined $n \in \mathbb{N}$. Now choose a $x \in I$ such that the occurring n is minimal, then we have $\Lambda x = \Lambda u\lambda^n \underset{u \text{ is a unit}}{=} \Lambda\lambda^n \subset I$. On the other side choose some $a \in I$ then $a = u\lambda^m$ with $m \geq n$, hence $a = u\lambda^{m-n}\lambda^n \in \Lambda\lambda^n$. So all in all we have $I = \Lambda\lambda^n$.
2. Analogous to (1).
3. This is a direct consequence of Corollary 4.18.
4. Follows directly from the other parts.

□

4.3 Some Remarks on Cyclic Extensions

4.3.1 Spliting of Polynomials in Cyclic Extensions

We fix some notations for this section. Let L/F be a Galois extension of finite degree n with cyclic Galois group $G = \langle\sigma|\sigma^n = \mathrm{id}\rangle$ and $f \in F[q]$ denotes an irreducible monic polynomial of degree ≥ 1.

Observation 4.20 *The Galois group G operates on $L[q]$ by the following definition:*

$$\sigma : L[q] \longrightarrow L[q]$$
$$\sum_{i=0}^{d} e_i q^i \longmapsto \sum_{i=0}^{d} \sigma(e_i) q^i.$$

Lemma 4.21 *Let L'/F' be an arbitrary Galois extension with group H.*

1. $L'(x)/F'(x)$ is a Galois extension of degree $|L' : F'|$.

2. The map

$$\Phi : Gal(L'/F') \longrightarrow Gal(L'(x)/F'(x))$$
$$\tau \longmapsto \Phi_\tau := \Big[\frac{\sum_i a_i x^i}{\sum_j b_j x^j} \longmapsto \frac{\sum_i \tau(a_i) x^i}{\sum_j \tau(b_j) x^j}\Big]$$

is an isomorphism of groups.

Remark 4.22 *If $g \in L[q]$ is irreducible then $\sigma(g)$ is also irreducible.*

Proof. Assume $\sigma(g) = \tilde{g_1}\tilde{g_2}$ for polynomials $\tilde{g_1}, \tilde{g_2} \in L[q]$ of positive degrees, hence $g = \underbrace{\sigma^{-1}(\tilde{g_1})}_{=:g_1 \in L[q]} \underbrace{\sigma^{-1}(\tilde{g_2})}_{=:g_2 \in L[q]}$. So we obtain a contradiction to the fact that g is irreducible.

□

Notation 4.23 *By $g_1, \ldots, g_\alpha$ we denote irreducible monic polynomials in $L[q]$ such that $f = g_1 \cdots g_\alpha$ holds.*

Observation 4.24 *The polynomials $g_1, \ldots, g_\alpha$ in Notation 4.23 are uniquely determined up to a permutation of the indices.*

Proof. L is a field, so $L[q]$ is a UFD. Assume there is another decomposition of f into monic irreducible factors $f = h_1 \cdots h_\beta$ say. Then we get $\alpha = \beta$ and there exist units $\varepsilon_1, \ldots, \varepsilon_\alpha \in L^\times$ and a new enumeration of the polynomials h_i that we can w.l.o.g. assume $g_i = \varepsilon_i h_i$. But all polynomials g_i and h_i have been assumed to be monic, so we must have $g_i = h_i$ and we are done. □

Lemma 4.25 *Consider again $f = g_1 \cdots g_\alpha$. Then the Galois group operates transitively on the polynomials $g_1, \ldots, g_\alpha$.*

Proof.

1. We know from Remark 4.22 that the polynomials $\sigma(g_1), \ldots, \sigma(g_\alpha)$ are irreducible, they are surely monic. So we have two decompositions of our polynomial $f = g_1 \cdots g_\alpha = \sigma(g_1) \cdots \sigma(g_\alpha)$ of f as a product of monic irreducible polynomials, an application of Observation 4.24 yields that there is a permutation π of the indices $1, \ldots, a$ such that we have $\sigma(g_i) = g_{\pi(i)}$. We conclude that G operates on the set $g_1, \ldots, g_\alpha$.

2. Now assume that this operation is not transitive. So we have at least two orbits of this operation. Take an arbitrary polynomial h of $L[q]$ and consider its orbit $\{\sigma^i(h) \mid 1 \leq i \leq n\}$ under the operation of G. We denote the distinguish elements of this orbit by $h_1, \ldots, h_\beta$ for some $\beta \in \mathbb{N}$. Then we set $h_0 := \prod_{i=1}^{\beta} h_i$. Such a polynomial h_0 is contained in $F[q]$, since $\sigma(h_0) = h_0$ holds. This last observation shows that we get a factorization $f = h_0\tilde{h_0}$ in $F[q]$, a contradiction to the fact that f is irreducible. So the operation of G has to be transitive.

□

Remark 4.26 *We consider again our cyclic extension L/F with group G of order n with generator σ. For $\alpha | n$ we set $G_\alpha := \langle \sigma^\alpha \rangle$ and $L_\alpha := Fix(G_\alpha)$. Since G is an Abelian group we know that G_α is a normal subgroup of G and so L_α/F is a Galois extension with group $Gal(L_\alpha/F) \simeq G/\langle \sigma^\alpha \rangle$ (cf. [Lan93, VI, Theorem 1.10]).*

Corollary 4.27 *We find an $1 \leq \alpha \in \mathbb{N}$ an an irreducible monic polynomial $g \in L[q]$ (we have moreover $g \in L_\alpha[q]$ and g is irreducible in $L_\alpha[q]$) with*

$$f = Nr_{L_\alpha(q)/F(q)}(g) = \prod_{i=1}^{\alpha} \tau^i(g) \quad \text{with } \tau = \sigma\langle\sigma^\alpha\rangle.$$

Proof. We set $f = g_1 \cdots g_\alpha$ as usual, an application of Lemma 4.25 yields that the cyclic group G operates transitively on the polynomials $g_1, \ldots, g_\alpha$. So α has to be a divisor of n and G/G_α operates transitively and faithfully on the g_i's (see for example [Suz82, Theorem 7.9 and (7.16)]) and so we are done by Remark 4.26. □

4.3.2 Integral Considerations

We assume that we are in the same situation as in Section 4.3.1. We first state some lemmas on prime ideals which we need later on.

Some Facts on Prime Ideals in Integral Extensions

Lemma 4.28 *Let B/A an integral extension of integral domains and $\mathfrak{p} \in Spec(A)$ an arbitrary element. Then we get*

$$Spec(B_\mathfrak{p}) = \{\mathfrak{Q}_\mathfrak{p} \mid \exists \mathfrak{P} \in Spec(B) \text{ with } \mathfrak{Q} \subset \mathfrak{P} \text{ and } \mathfrak{P} \cap A = \mathfrak{p}\}.$$

Proof. We know $\mathrm{Spec}(B_\mathfrak{p}) = \{\mathfrak{Q}_\mathfrak{p} \mid \mathfrak{Q} \in \mathrm{Spec}(B) \text{ and } \mathfrak{Q} \cap (A \setminus \mathfrak{p}) = \varnothing\}$. We note that $\mathfrak{Q} \cap (A \setminus \mathfrak{p}) = \varnothing$ holds if and only if $\mathfrak{q} := \mathfrak{Q} \cap A \subset \mathfrak{p}$ is satisfied. So we are done by using "going up" (see for example [Ser00, Chapter III, Corollary to Proposition 2]). □

Lemma 4.29 *Let B/A an integral extension of integral domains such that A is integrally closed. Let $\mathfrak{p} \in Spec(A)$ and $\mathfrak{P} \in Spec(B)$ such that $\mathfrak{P} \cap A = \mathfrak{p}$ holds. Then we have $ht(\mathfrak{p}) = ht(\mathfrak{P})$.*

Proof. Cf. [Ser00, Chapter III, Corollary to Proposition 5]. □

Corollary 4.30 *Let B/A an integral extension of integral domains and $\mathfrak{p} \in ht^1(A)$ an arbitrary element. Then we get*

1. *$Max(B_\mathfrak{p}) = \{\mathfrak{P}_\mathfrak{p} \mid \mathfrak{P} \in ht^1(B) \text{ and } \mathfrak{P} \cap A = \mathfrak{p}\}$.*
2. *$Spec(B) = Max(B) \cup \{0\}$.*

Proof. This is immediately deduced from Lemma 4.29. □

Lemma 4.31 *Let B/A an integral extension of integral domains and $\mathfrak{p} \in Spec(R)$ an arbitrary element. Moreover let $\{\mathfrak{P}_i \mid i \in I\} \subset Spec(B)$ consists of these elements $\mathfrak{P} \in Spec(B)$ with $\mathfrak{P} \cap A = \mathfrak{p}$. We set $S := A \setminus \mathfrak{p}$ and $S' := \bigcap_{i \in I}(B \setminus \mathfrak{P}_i)$. Then we have an equality $S^{-1}B = \left(S'\right)^{-1}B$.*

Proof. Cf. [Bou89c, Paragraph 2.1, Proposition 2] □

Splitting of Integral Polynomials

In Corollary 4.27 we have obtained a result about the factorization of a *monic* polynomial in the extension $L[q]/F[q]$. Let us consider the

Examples 4.32 *Let $F = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. The extension L/F is cyclic of degree 2 and the corresponding Galois group is generated by the complex conjugation, we denote this automorphism by $\bar{\cdot}$. We note that F is the field of fractions of $R := \mathbb{Z}$ and set $S := alg.\ int._R(L) = \mathbb{Z}[i]$.*

1. *We set* $f := 2(q^2+1)$, *this polynomial is contained in* $\mathbb{Z}[q]$ *and obtain a factorization* $f = g \cdot \bar{g}$ *with* $g = (1+i)(q+i)$. *We note that the polynomial* g *is contained in* $S[q]$.

2. *Now let* $f = 3(q^2+1)$. *If there would be a polynomial* $\alpha q + \beta \in L[q]$ *with* $f = g \cdot \bar{g}$ *we would obtain that* 3 *is a norm of the field extension* L/F. *We note that* $\mathbb{Z}[i]$ *is a principal ideal domain. So assume that there are elements* $a, b \in \mathbb{Z}[i]$ *with* $3 = \frac{a}{b} \cdot \frac{\bar{a}}{\bar{b}}$ *and* $(a,b) = 1$ *in* $\mathbb{Z}[i]$. *A straightforward calculation - based on the fact that* 3 *is a prime element of* $\mathbb{Z}[i]$ *- yields that* 3 *has to divide both* a *and* b, *a contradiction and so there is no factorization* $f = g \cdot \bar{g}$.

So a non monic polynomial f need not have a factorization in the form of Corollary 4.27, even if we assume in addition that the polynomial f is integral.

Hence we have to make some additional assumptions on our field extension L/F. We assume now that F is the field of fractions of a *complete* discrete valuation ring R with prime π and finite residue class field $\mathfrak{k}$ with $|\mathfrak{k}| = m$. We assume that L is up to isomorphism the unique unramified extension of F of degree n (see Theorem 2.22). We set $S :=$ alg. int.$_R(L)$ and get $S = R[\omega_0]$ for a primitive (m^n-1)-th root of unity ω_0. The norm of the field extension N/F will be denoted by N. Let $\nu = \nu_R$ and ν_S the π-adic valuations on R and S respectively. We first need a lemma on units in integral extensions.

Lemma 4.33 *Let* B/A *be an integral extension of commutative rings. If* $\varepsilon \in B$ *is a unit such that* ε *is already contained in* A *then* ε *is also invertible in* A. *So we have* $B^\times \cap A = A^\times$.

Proof. That $A^\times \subset B^\times \cap A$ holds is of course trivial. Now choose some $\varepsilon \in B^\times \cap A$, if ε is not a unit in A we find a prime ideal $\mathfrak{p} \subset A$ with $\varepsilon \in \mathfrak{p}$. We get from [Eis99, Prop. 4.15] that there is a prime ideal $\mathfrak{P}$ of B with $\mathfrak{P} \cap A = \mathfrak{p}$ and can conclude $\varepsilon \in \mathfrak{p} \subset \mathfrak{P}$, so ε is contained in a prime ideal of B and can't be invertible, a contradiction. □

Remark 4.34 *If* B/A *is not an integral extension the statement of Lemma 4.33 is in general not true. We give a counterexample: Let* $A = \mathbb{Z}$ *and* $B = \mathbb{Z}[\frac{1}{2}]$. *We have* $2 \in B^\times \cap A$; *but of course* 2 *is not invertible in* $\mathbb{Z}$.

Lemma 4.35 *For* $\tilde{f} \in R[q]$ *are equivalent:*

1. $\tilde{f}$ *is irreducible in* $S[q]$.

2. $\tilde{f}$ *is irreducible in* $L[q]$.

Proof. (2) $\Longrightarrow$ (1): Assume that $\tilde{f}$ is not irreducible in $S[q]$. Since $\tilde{f}$ is irreducible in $R[q]$ we know that $\tilde{f}$ is primitive in $R[q]$. Since S/R is unramified we conclude that $\tilde{f}$ is also primitive in $S[q]$. Hence $\tilde{f}$ has to decompose in polynomials of degree ≥ 1 and so $\tilde{f}$ can't be irreducible in $L[q]$.

(1) $\Longrightarrow$ (2): If $\tilde{f}$ is not irreducible in $L[q]$ then the Lemma of Gauss implies that $\tilde{f}$ is also not irreducible in $S[q]$. □

From now on let us assume that f has degree ≥ 1 and f is contained in $R[q]$ such that f is irreducible in $R[q]$ but not irreducible in $S[q]$. Let $r \in R$ be the leading coefficient of f. Lemma 4.35 yields that f is not irreducible in $L[q]$. Corollary 4.27 yields the existence of an $\alpha \in \mathbb{N}$ which divides n and the existence of some $g \in L_\alpha[q]$

with $r\frac{f}{r} = rg\sigma(g)\dots\sigma^{\alpha-1}(g)$. We set $S_\alpha := \text{alg. int.}_R(L_\alpha) = S \cap L_\alpha$. We find some $b \in R$ with $\sigma^i(b)\sigma^i(g) \in S_\alpha[q]$ and $\nu(b)$ is minimal, this just means that all the polynomials $\sigma^i(b)\sigma^i(g)$ are primitive. We note that $b \in S_\alpha$ holds.

We introduce two polynomials

- $h := f = rg\sigma(g)\dots\sigma^{\alpha-1}(g)$ and
- $h' := bg \cdot \sigma(b)\sigma(g)\cdots\sigma^{\alpha-1}(b)\sigma^{\alpha-1}(g) = (bg)\cdot\sigma(bg)\cdots\sigma^{\alpha-1}(bg)$,

both of these polynomials are contained in $S_\alpha[q]$ and we have $hL_\alpha[q] = h'L_\alpha[q]$.

Lemma 4.36 *There is some $\varepsilon \in R^\times$ with $h = \varepsilon h'$.*

Proof. Since b is contained in R we get immediately $h' \in R[q]$ and $h = f \in R[q]$ is automatically satisfied. So we have $hL[q] = h'L[q]$. This yields that there is a unit of $L[q]$ i.e., some $0 \neq \varepsilon \in L$ with $h = \varepsilon h'$. Hence we have by the Lemma of Gauss

$$0 \underset{h=f \text{ is primitive}}{=} \nu(h) = \nu(\varepsilon h') = \nu(\varepsilon)\nu(h') \underset{h' \text{ is primitive}}{=} \nu\varepsilon,$$

so $\varepsilon \in R^\times = \{k \in F \mid \nu(k) = 0\}$. □

Theorem 2.23 ensures that the unit ε is the norm of some element $c \in S_\alpha$ i.e., $\varepsilon = c\sigma(c)\cdots\sigma^{\alpha-1}(c)$. And so we get finally

$$f = \varepsilon h' = (cbg)\cdot\sigma(cbg)\cdots\sigma^{\alpha-1}(cbd).$$

For further use let us restate the last result as

Corollary 4.37 *Let $f \in R[q]$ be an irreducible polynomial then there is an $\alpha \in \mathbb{N}$ which divides n and an irreducible polynomial g in $S_\alpha[q]$ with $f = g\sigma(g)\cdots\sigma^{\alpha-1}(g)$.*

4.3.3 Adjoining Primitive Elements to Cyclic Extension

Definition 4.38 *1. For a polynomial $\sum_{i=0}^n a_i q^i$ we set*

$$\nu_\mathfrak{p}(f) := \min\{\nu_\mathfrak{p}(a_i) \mid 0 \leq i \leq n\}$$

and call $\nu_\mathfrak{p}(f)$ the $\mathfrak{p}$-content of f.

2. Let $f \in T[q]$ be a polynomial of positive ≥ 1. We call f

a) $\mathfrak{p}$-primitive if $\nu_\mathfrak{p}(f) = 0$ holds.

b) primitive, if f is $\mathfrak{p}$-primitive for all $\mathfrak{p} \in ht^1(T)$.

Applying the well known Lemma of Gauss for factorial ground rings to $T_\mathfrak{p}[q]$ we obtain immediately the following generalization

Lemma 4.39 *$\nu_\mathfrak{p}(fg) = \nu_\mathfrak{p}(f) + \nu_\mathfrak{p}(g)$ holds for all $f, g \in T[q]$.*

From now on we just assume that $f \in K[q]$ is irreducible and has a decomposition $f = g_1\cdots g_\alpha$ with $\alpha | n$. Let a be a zero of f in some splitting field of f.

Lemma 4.40 *We have isomorphisms*

$$frac\Big(R[q]/fR[q]\Big) \simeq F[q]/fF[q] \simeq F(a).$$

Proof.

- Let $0 \neq h + fR[q] \in R[q]/fR[q]$ and assume that $0 = h + fF[q]$ holds. Then we find a polynomial $\tilde{h} \in F[q]$ with $h = f\tilde{h}$. Let $\mathfrak{p} \in \mathrm{ht}^1(R)$ an arbitrary element. By $\nu_{\mathfrak{p}}(b)$ we denote - as usual - the $\mathfrak{p}$-content of a polynomial b (see Definition 4.38). We get from Lemma 4.39:

$$\underbrace{\nu_{\mathfrak{p}}(h)}_{\geq 0 \text{ since } h \in R[q]} = \nu_{\mathfrak{p}}(f\tilde{h}) = \underbrace{\nu_{\mathfrak{p}}(f)}_{=0, \text{ since } f \text{ is primitive}} + \nu_{\mathfrak{p}}(\tilde{h}),$$

  hence $\nu_{\mathfrak{p}}(\tilde{h}) \geq 0$ and so we get $\tilde{h} \in R[q]$ a contradiction. So the universal property of a localization yields immediately that

$$\Phi : \mathrm{frac}\Big(R[q]/fR[q]\Big) \longrightarrow F[q]/fF[q]$$
$$\frac{h_1 + fR[q]}{h_2 + fR[q]} \longmapsto \frac{h_1 + fF[q]}{h_2 + fF[q]}$$

  is a well defined homomorphism. Φ is injective since $\mathrm{frac}\Big(R[q]/fR[q]\Big)$ is a field. Let $h \in F[q]$ be an arbitrary element, we find some $0 \neq s \in R$ with $sh \in R[q]$. So $\Phi(\frac{sh+fR[q]}{s+fR[q]}) = h + fF[q]$ and so Φ is also surjective.

- That $F[q]/fF[q] \simeq F(a)$ holds is obvious (this isomorphism is in fact one possible definition for $F(a)$).

□

Lemma 4.41 *Moreover we have isomorphisms*

$$frac\Big(S[q]/gS[q]\Big) \simeq L[q]/gL[q] \simeq L(a).$$

Proof. We have some decomposition $f = g\sigma(g)\cdots\sigma^{\alpha-1}(g)$. So we can conclude: $0 = f(a) = g(a)\sigma(g)(a)\cdots\sigma^{\alpha-1}(g)(a)$. Hence there is an $0 \leq i \leq \alpha - 1$ with $\sigma^i(g)(a) = 0$. We know that $\sigma^i(g)$ is a irreducible polynomial in $L[q]$ an so the normed representative is the minimal polynomial of a over L. Hence we have an isomorphism $L(a) \simeq L[q]/\sigma^i(g)L[q]$. We can apply Lemma 4.44 to conclude $L(a) \simeq L[q]/\sigma^i(g)L[q] \simeq L[q]/gL[q]$ and we are done. The second isomorphism is again trivial. □

Lemma 4.42 *The degree $|L(a) : F(a)|$ of the field extension $L(a)/F(a)$ is $\frac{n}{\alpha}$.*

Proof.

- We have $f = g\sigma(g)\cdots\sigma^{\alpha-1}(g)$ and so $\deg(f) = \alpha\deg(g)$.
- Lemma 4.41 yields $|L(a) : L| = \deg(g)$, in the same way Lemma 4.40 gives $|F(a) : F| = \deg(f)|$.
- From [Lan93, Chapter V, Proposition 1.2] we get $|L(a) : F| = |L(a) : F(a)| \cdot |F(a) : F|$. So we can conclude (using again [Lan93, Chapter V, Prop. 1.2] during the calculation):

$$|L(a) : F(a)| = \frac{|L(a) : F|}{|F(a) : F|} = \frac{|L(a) : L| \cdot |L : F|}{|F(a) : F|}$$
$$= \frac{\deg(g) \cdot n}{\deg(f)} = \frac{\deg(g) \cdot n}{\deg(g) \cdot \alpha} = \frac{n}{\alpha}.$$

□

Lemma 4.43 *The field extension $L(a)/F(a)$ is Galois, the corresponding Galois group is isomorphic to $\langle\sigma^\alpha\rangle$.*

Proof. By Lemma 4.41 we have an isomorphism $L(a) \simeq L[q]/gL[q]$ so we can w.l.o.g. assume that g is the minimal polynomial of a over the field L. We set

$$\Phi : \langle\sigma^\alpha\rangle \longrightarrow \mathrm{Gal}(L(a)/F(a))$$
$$\sigma \longmapsto [\tau := L(a) \ni \sum_{i=0}^{n/\alpha} l_i a^i \longmapsto \sum_{i=0}^{n/\alpha} \sigma^i(l_i)a^i \in L(a)].$$

Let us first show that τ is well defined.

- We use the isomorphism $L(a) \simeq L[q]/gL[q]$ as it is stated in Lemma 4.41, then Lemma 4.44 ensures that τ is a well defined isomorphism.
- We note that

  $$\iota : F[q]/fF[q] \longrightarrow L[q]/gL[q]$$
  $$h + fF[q] \longmapsto h + gL[q]$$

  is an embedding of fields, which identifies $F(a)$ with a subfield of $L[q]/gL[q]$. Since $\sigma^\alpha(h) = h$ holds for every polynomial $h \in F[q]$, the isomorphism τ restricts on $F[q]/fF[q]$ to the identical mapping and so τ is indeed an element of the Galois group of $L(a)/F(a)$.

That Φ is a well defined group homomorphism is clear. Assume that $\Phi(\sigma^{\alpha i}) = \mathrm{id}$ for some $1 \leq i \leq \frac{n}{\alpha}$. Then we have $\sigma^{\alpha i}(l) = l$ for every element $l \in L \subset L(a)$. And so $\sigma^{\alpha i} = \mathrm{id}$. Since L/F is Galois we get $i = \frac{n}{\alpha}$. So Φ is injective. From [Bou50, §7, no°5, Proposition 8] we get

$$|\mathrm{Gal}(L(a)/F(a))| \leq |L(a) : F(a)| \underset{\text{Lemma 4.42}}{=} \frac{n}{\alpha}$$

and so - using that Φ is injective we can conclude $\mathrm{Gal}(L(a)/F(a)) = |L(a) : F(a)|$. So we can apply the Main Theorem of Galois Theory to conclude that $L(a)/F(a)$ is a Galois extension and so Φ is indeed an isomorphism. □

4.4 A Conjugation Lemma

Lemma 4.44 *Let U be an arbitrary commutative ring and $\mathfrak{a}$ some ideal of U. Moreover let $\tau : U \longrightarrow U$ be an automorphism. Then τ induces an isomorphism*

$$\varphi : U/\mathfrak{a} \longmapsto U/\tau(\mathfrak{a})$$
$$u + \mathfrak{a} \longmapsto \tau(u) + \tau(\mathfrak{a}).$$

Proof. This is verified by a straightforward calculation. □

We will now take a closer look on the Chinese Remainder Theorem, because we need the isomorphism which is given in the Theorem and its inverse map for further calculations in a very explicit way.

Let us fix some notation. Let T be some commutative ring and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of T such that for every pair $i \neq j \in \{1, \ldots, n\}$ the ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are relative prime i.e., $\mathfrak{a}_i + \mathfrak{a}_j = T$. Sometimes we will also use the expression coprime for relative prime.

Lemma 4.45 *There are elements $\alpha_i \in \mathfrak{a}_1 \cdots \mathfrak{a}_{i-1}\mathfrak{a}_{i+1} \cdots \mathfrak{a}_n$ with $\sum_{i=1}^n \alpha_i = 1$.*

Proof. This is done by an induction proof, which is mainly based on the observation that $\langle \mathfrak{a}_1, \mathfrak{a}_2 \cdots \mathfrak{a}_n \rangle = T$ holds. □

Now we can state the

Lemma 4.46 (Chinese Remainder Theorem) *The map*

$$\Phi : T/\mathfrak{a}_1 \cdots \mathfrak{a}_n \longmapsto T/\mathfrak{a}_1 \times \cdots \times T/\mathfrak{a}_n$$
$$r + \mathfrak{a}_1 \cdots \mathfrak{a}_n \longmapsto (r + \mathfrak{a}_1, \ldots, r + \mathfrak{a}_n)$$

is an isomorphism of rings.

For concrete calculations later on we need the inverse map of Φ. For a proof of the Chinese Remainder Theorem see [Lan93, Chapter II, Theorem 2.1].

Lemma 4.47 *Let the map $\Phi : T/\mathfrak{a}_1 \ldots \mathfrak{a}_n \longmapsto T/\mathfrak{a}_1 \times \cdots \times T/\mathfrak{a}_n$ as in the Chinese Remainder Theorem. By Lemma 4.45) there are elements $a_i \in \mathfrak{a}_1 \ldots \mathfrak{a}_{i-1}\mathfrak{a}_{i+1} \ldots \mathfrak{a}_n$ with $\sum_{i=1}^n a_i = 1$. Then the inverse map of Φ is given by the following homomorphism*

$$\Psi : T/\mathfrak{a}_1 \times \cdots \times T/\mathfrak{a}_n \longrightarrow T/\mathfrak{a}_1 \cdots \mathfrak{a}_n$$
$$(r_1 + \mathfrak{a}_1, \ldots, r_n + \mathfrak{a}_n) \longmapsto \Big(\sum_{i=1}^n r_i a_i\Big) + \mathfrak{a}_1 \cdots \mathfrak{a}_n.$$

Lemma 4.48 *Let U be an arbitrary commutative ring, $S \subset U$ a multiplicative set and $\tau : U \longrightarrow U$ an automorphism of U such that $\tau(S) = S$ holds. Then $S^{-1}\tau : S^{-1}U \longrightarrow S^{-1}U$ is also an automorphism.*

Proof. Straightforward. □

Now we have to make some assumptions on the ring T. Let T be a factorial ring with field of fractions F. We assume that L/F is a cyclic Galois extension of degree n with group $G = \langle \tau \rangle$. Moreover we set $U :=$ alg. $\text{int.}_R(L)$. Let f be an irreducible polynomial in $T[q]$ such that there is a factorization $f = g\tau(g) \cdots \tau^{\alpha-1}(g)$ in $S[q]$ with $\alpha | n$ and g is an irreducible polynomial in $U[q]$. We set moreover $\tilde{T} := T[q]$, $\tilde{U} := U[q]$ and $\mathfrak{p} := fT[q]$ an element of $\text{ht}^1(\tilde{T})$. For convenience we introduce the

Notation 4.49 *We set $\widehat{g_i} := g \cdots \tau^{i-1}(g)\tau^{i+1}(g) \cdots \tau^{\alpha-1}(g)$.*

Observation 4.50 *We have $\tau(\widehat{g_i}) = \widehat{g_{i+1}}$, where we regard the indices modulo α, this just means that we use the convention $\widehat{g_\alpha} = \widehat{g_0}$.*

Proof. We have

$$\tau(\widehat{g_i}) = \tau(g\tau(g) \ldots \tau^{i-1}(g)\tau^{i+1}(g) \ldots \tau^{\alpha-1}(g))$$
$$\underset{\substack{\tau \text{ is a} \\ \text{homomorphism}}}{=} \tau(g)\tau(\tau(g)) \ldots \tau(\tau^{i-1}(g))\tau(\tau^{i+1}(g)) \ldots \tau(\tau^{\alpha-1}(g))$$
$$\underset{\tau^\alpha(g)=g}{=} \tau(g)\tau^2(g) \ldots \tau^i(g)\tau^{i+1}(g) \ldots g = \widehat{g_{i+1}}.$$

□

Now we pass over to the localizations $\left(\tilde{T}\right)_{\mathfrak{p}}$ and $\left(\tilde{U}\right)_{\mathfrak{p}}$ and for our convenience we change the notation by referring to $\tau_{\mathfrak{p}}$ just as τ.

Remark 4.51 *Lemma 4.45 ensures that there are elements $a_0, \ldots, a_{\alpha-1} \in \tilde{U}_{\mathfrak{p}}$ with $\sum_{i=0}^{\alpha_1} \widehat{g_i} = 1$. We fix these elements a_i.*

Notations 4.52 *1. We define two maps which are mutually inverse*

$$\Phi : \tilde{U}_{\mathfrak{p}}/f\tilde{U}_{\mathfrak{p}} \longrightarrow \left(\tilde{U}_{\mathfrak{p}}/g\tilde{U}_{\mathfrak{p}}\right) \times \ldots \left(\tilde{U}_{\mathfrak{p}}/\tau^{\alpha-1}(g)\tilde{U}_{\mathfrak{p}}\right)$$
$$u + f\tilde{U}_{\mathfrak{p}} \longmapsto (u + g\tilde{U}_{\mathfrak{p}}, \ldots, u + \tau^{\alpha-1}(g)\tilde{U}_{\mathfrak{p}})$$

and

$$\Psi : \left(\tilde{U}_{\mathfrak{p}}/g\tilde{U}_{\mathfrak{p}}\right) \times \ldots \left(\tilde{U}_{\mathfrak{p}}/\tau^{\alpha-1}(g)\tilde{U}_{\mathfrak{p}}\right) \longrightarrow \tilde{U}_{\mathfrak{p}}/f\tilde{U}_{\mathfrak{p}}$$
$$(u_0 + g\tilde{U}_{\mathfrak{p}}, \ldots, u_{\alpha-1} + \tau^{\alpha-1}(g)\tilde{U}_{\mathfrak{p}}) \longmapsto \Big(\sum_{i=0}^{\alpha-1} a_i \widehat{g_i} u_i\Big) + f\tilde{U}_{\mathfrak{p}}.$$

2. We set

$$\bar{\tau} : \tilde{U}_{\mathfrak{p}}/f\tilde{U}_{\mathfrak{p}} \ni u + f\tilde{U}_{\mathfrak{p}} \longmapsto \tau(u) + f\tilde{U}_{\mathfrak{p}}.$$

Definition 4.53 *The homomorphism $\bar{\tau}'$ is defined via the following commutative diagram:*

$$\begin{array}{ccc} \tilde{U}_{\mathfrak{p}}/f\tilde{U}_{\mathfrak{p}} & \xrightarrow{\Phi} & \left(\tilde{U}_{\mathfrak{p}}/g\tilde{U}_{\mathfrak{p}}\right) \times \cdots \times \left(\tilde{U}_{\mathfrak{p}}/\tau^{\alpha-1}(g)\tilde{U}_{\mathfrak{p}}\right) \\ \Big\downarrow \bar{\tau} & & \Big\downarrow \bar{\tau}' := \Psi\bar{\tau}\Phi \\ \tilde{U}_{\mathfrak{p}}/f\tilde{U}_{\mathfrak{p}} & \xrightarrow{\Phi} & \left(\tilde{U}_{\mathfrak{p}}/g\tilde{U}_{\mathfrak{p}}\right) \times \cdots \times \left(\tilde{U}_{\mathfrak{p}}/\tau^{\alpha-1}(g)\tilde{U}_{\mathfrak{p}}\right). \end{array}$$

We want to determine the homomorphism $\bar{\tau}'$ explicitly and make the

Observations 4.54 *Let $u_0, \ldots, u_{\alpha-1} \in \tilde{S}_{\mathfrak{p}}$.*

1. We find:

$$\bar{\tau}'\left((u_0 + g\tilde{U}_{\mathfrak{p}}, \ldots, u_{\alpha-1} + \tau^{\alpha-1}(g)\tilde{U}_{\mathfrak{p}})\right) = \Phi\Big(\bar{\tau}\Big(\big(\sum_{i=0}^{\alpha-1} a_i \widehat{g_i} u_i\big) + f\tilde{U}_{\mathfrak{p}}\Big)\Big)$$
$$\underset{per.\ def.\ of\ \bar{\tau}}{=} \Phi\Big(\big(\sum_{i=0}^{\alpha-1} \tau(a_i)\tau(\widehat{g_i})\tau(u_i)\big) + f\tilde{U}_{\mathfrak{p}}\Big)$$
$$\underset{\substack{Observation\ 4.50\\ and\ we\ use\ the\\ convention\ \widehat{g_0}=\widehat{g_\alpha}}}{=} \Phi\Big(\big(\sum_{i=0}^{\alpha-1} \tau(a_i)\widehat{g_{i+1}}\tau(u_i)\big) + f\tilde{U}_{\mathfrak{p}}\Big)$$
$$= \Big(\big(\sum_{i=0}^{\alpha-1} \tau(a_i)\widehat{g_{i+1}}\tau(u_i)\big) + g\tilde{U}_{\mathfrak{p}}, \ldots, \Big(\sum_{i=0}^{\alpha-1} \tau(a_i)\widehat{g_{i+1}}\tau(u_i)\Big) + \tau^{\alpha-1}(g)\tilde{U}_{\mathfrak{p}}\Big).$$

2. For an index $0 \leq i \leq \alpha - 1$ we find:

$$\big(\sum_{k=0}^{\alpha-1} \tau(a_k)\hat{g_{k+1}}\tau(u_k)\big) + \tau^i(g)\tilde{U}_{\mathfrak{p}} \underset{\tau^i(g)|\hat{g_j} \Leftrightarrow i \neq j}{=} \tau(a_{i-1}\hat{g_i}\tau(u_{i-1}) + \tau^i(g)\tilde{U}_{\mathfrak{p}}$$

3. Moreover we have

$$\begin{aligned}
&\tau(a_{i-1})\hat{g}_i - 1 \underset{\tau(1)=1}{=} \tau(a_{i-1})\hat{g}_i - \tau(1) \\
&\underset{\sum_{k=0}^{\alpha-1} a_k \hat{g_k}=1}{=} \tau(a_{i-1})\hat{g}_i - \tau\Big(\sum_{k=0}^{\alpha-1} a_k \hat{g_k}\Big) \\
&\underset{\tau \text{ is a homomorphism}}{=} \tau(a_{i-1})\hat{g_{i-1}} - \sum_{k=0}^{\alpha-1} \tau(a_k)\hat{g_{k+1}} \\
&= -\tau(a_0)\underbrace{\hat{g_1}}_{\tau^i(g)\tilde{U}_\mathfrak{p}} - \cdots - \tau(a_{i-2})\underbrace{\hat{g_{i-1}}}_{\tau^i(g)\tilde{U}_\mathfrak{p}} \\
&-\tau(a_i)\underbrace{\hat{g_{i+1}}}_{\tau^i(g)\tilde{U}_\mathfrak{p}} - \cdots - \tau(a_{\alpha-1})\underbrace{\hat{g_0}}_{\tau^i(g)\tilde{U}_\mathfrak{p}} \in \tau^i(g)\tilde{U}_\mathfrak{p}.
\end{aligned}$$

So we all in all we have shown

Lemma 4.55 *For elements $u_0, \ldots, u_{\alpha-1} \in \tilde{U}_\mathfrak{p}$ we find*

$$\begin{aligned}
&\bar{\tau}'\Big(u_0 + g\tilde{U}_\mathfrak{p}, \ldots, u_{\alpha-1} + \tau^{\alpha-1}(g)\tilde{U}_\mathfrak{p}\Big) \\
&= \Big(\tau(u_{\alpha-1}) + g\tilde{U}_\mathfrak{p}, \tau(u_0) + \tau(g)\tilde{U}_\mathfrak{p}, \ldots, \tau(u_{\alpha-2}) + \tau^{\alpha-1}(g)\tilde{U}_\mathfrak{p}\Big).
\end{aligned}$$

4.5 A kind of a Cyclic Algebra

In the following we will use the notations of the Sections 2.2.2 and 3.1.2. We fix some polynomial $h \in R[q]$ with $h := g\sigma(g)\cdots\sigma^{\alpha-1}(g)$ for some irreducible polynomial $g \in S[q]$ and some $\alpha \in \mathbb{N}$ which divides n. Moreover we set $F_i := L[q]/\sigma^i(g)L[q]$ for $i = 0, \ldots, \alpha-1$ and $K_0 := K[q]/fK[q]$. We choose b to be a common root of the polynomials h and g in some algebraic extension of K. We recall some important facts from Section 4.3.3:

- The field K_0 is isomorphic to $K(b)$ (see Lemma 4.40).
- Every field F_i is isomorphic to $L(b)$ (see Lemmas 4.41 and 4.44).
- The field extension $L(b)/K(b)$ is Galois and the corresponding Galois group is isomorphic to $G_\alpha := \langle\sigma^\alpha\rangle \subset \mathrm{Gal}(L/K)$ (this is the content of Lemma 4.43). The rank of this field extension is $s := \frac{n}{\alpha}$.

Notation 4.56 *We set $A := \prod_{i=0}^{\alpha-1} F_i$ and define $\tau : A \longrightarrow A$ to be the homomorphism with*

$$\begin{aligned}
&\tau(a_0 + gL[q], a_1 + \sigma(g)L[q], \ldots, a_{\alpha-1} + \sigma^{\alpha-1}(g)L[q]) \\
&:= (\sigma(a_{\alpha-1}) + L[q], \sigma(a_0) + gL[q], \sigma(a_1) + \sigma(g)L[q], \ldots, \sigma(a_{\alpha-2}) + \sigma^{\alpha-1}(g)L[q])
\end{aligned}$$

Observation 4.57 *By considering the diagonal embedding*

$$K_0 \ni a + fK[q] \longmapsto (a + gL[q], a + \sigma(g)L[q], \ldots, a + \sigma^{\alpha-1}(g)L[q]) \in A$$

of K_0 into A we can identify K_0 with a subfield of A.

Theorem 4.58 (Additive Version of Hilbert's Theorem 90) *Let F'/F be a finite cyclic Galois extension of degree k with $Gal(F'/F) = \langle\nu\rangle$. For an element $x \in F'$ are equivalent:*

1. *There is an element* $x_0 \in F^{'}$ *with* $x = x_0 - \nu(x_0)$.
2. $Tr_{F^{'}/F}(x) = \sum_{i=0}^{k-1} \nu^i(x) = 0$.

Proof. Cf. [Lan93, Chapter VI, §6, Theorem 6.3]. □

Corollary 4.59 *Let* $F^{'}/F$ *the cyclic Galois extension of Theorem 4.58. Let* $h \in F^{'}[x]$ *some element with* $Tr_{F^{'}(x)/F(x)}(h) = 0$ *then there is an element* $\tilde{h} \in F^{'}[q]$ *with* $h = \tilde{h} - \sigma(\tilde{h})$.

Proof. Let $h = \sum_{i=0}^{n} h_i x^i$, then we have

$$\mathrm{Tr}_{F^{'}(x)/F(x)}(h) = \mathrm{Tr}_{F^{'}(x)/F(x)}(\sum_{i=0}^{n} h_i x^i) = \sum_{j=0}^{k} \sigma^j \big(\sum_{i=0}^{n} h_i x^i\big)$$

$$\underset{\text{Lemma 4.21}}{=} \sum_{i=0}^{n} \big(\sum_{j=0}^{k} \sigma^j(h_i)\big) x^i = \sum_{i=0}^{n} \mathrm{Tr}_{F^{'}/F}(h_i) x^i = 0,$$

hence we get $\mathrm{Tr}_{F^{'}/F}(h_i) = 0$ for all $0 \leq i \leq n$. Theorem 4.58 yields the existence of elements $y_i \in F^{'}$ with $h_i = y_i - \sigma(y_i)$. We conclude:

$$h = \sum_{i=0}^{n} h_i x^i = \sum_{i=0}^{n} \big(y_i - \sigma(y_i)\big) x^i = \sum_{i=0}^{n} y_i x^i - \sum_{i=0}^{n} \sigma(y_i) x^i$$

$$\underset{\text{Lemma 4.21}}{=} \underbrace{\sum_{i=0}^{n} y_i x^i}_{=:\tilde{h}} - \underbrace{\sigma\big(\sum_{i=0}^{n} y_i x^i\big)}_{=\sigma(\tilde{h})}$$

and so we are done. □

Lemma 4.60 *For an element* $x \in A$ *are equivalent:*

1. $\tau(x) = a$.
2. $x \in K_0$ *(see Observation 4.57).*

Proof. (1) $\Longrightarrow$ (2): The Chinese Remainder Theorem yields that the homomorphism

$$\Phi : L[q]/fL[q] \ni a + fL[q] \longmapsto (a + gL[q], a + \sigma(g)L[q], \ldots, \sigma^{\alpha-1}(g)L[q]) \in A$$

is an isomorphism. So we find an $a \in L[q]$ with $x = (a + gL[q], \ldots, a + \sigma^{\alpha-1}(g)L[q])$. Hence there is some $h \in L[q]$ with $a - \sigma(a) = fh$. $\tau(x) = x$ means

$$(a + gL[q], a + \sigma(g)L[q], \ldots, a + \sigma^{\alpha-1}(g)L[q])$$
$$= (\sigma(a) + gL[q], \sigma(a) + \sigma(a)L[q], \ldots, \sigma(a) + \sigma^{\alpha-1}(g)L[q]),$$

so we must have $a + \sigma^i(g)L[q] = \sigma(a) + \sigma^i(g)L[q]$ for all $0 \leq i \leq \alpha - 1$, and so $a + fL[q] = \sigma(a) + fL[q]$. Since f is contained in $K[q]$ and so $\sigma(f) = f$ holds we conclude - using Theorem 4.58 - that $\mathrm{Tr}_{L(q)/K(q)}(h) = 0$ holds. By Corollary 4.59 we find a polynomial $\tilde{h} \in L[q]$ with $h = \tilde{h} - \sigma(\tilde{h})$. So we have $a - \sigma(a) = f(\tilde{h} - \sigma(\tilde{h}))$, this yields $a - f\tilde{h} = \sigma(a - f\tilde{h})$ and so we get $a - f\tilde{h} \in K[q]$. And so we have $a + fL[q] = p + fL[q]$ with $p \in K[q]$ and this means now that $(a + gL[q], a + \sigma(g)L[q], \ldots, a + \sigma^{\alpha-1}(g)L[q]) \in K_0$ holds and we are done. □

Remark 4.61 *In the definition of a cyclic algebra as we have stated it (see Definition 2.8) we have assumed that we consider an extension of fields. The definition of a cyclic order (see Notation 2.20) has involved an integral extension of integral domains. In Notations 4.62 we introduce now an algebra which is in some kind also a cyclic algebra, but in whose definition a more general ring extension is involved.*

Notation 4.62 *We denote by $A_\tau[x]$ the twisted polynomial ring over A with indeterminate x (see Definition 6.1). The algebra $\Gamma := (A/K_0, \tau, a)$ is defined as the quotient $(A/K_0, \tau, a) := A_\tau[x]/(x^n - a)$ for some element $a \in A$ with $\tau(a) = a$ (this means - by the virtue of Lemma 4.60 - just that a is contained in K_0). Hence we can interpret Γ as a kind of a cyclic algebra, this means*

- *There is an element $\lambda \in \Gamma$ (the residue class of $x \in A_\tau[x]$), such that the elements $1, \lambda, \ldots, \lambda^{n-1}$ form an A-basis of Γ, i.e. we have as an A-module $\Gamma = A \oplus A\lambda \oplus \cdots \oplus A\lambda^{n-1}$.*
- *Moreover we have $\lambda^n = a \in A$ with $\tau(a) = a$ and $\lambda y = \tau(y)\lambda$ for all $y \in A$.*

Observations 4.63

1. *We know that $L(b)/K(b)$ is a Galois extension which group is isomorphic to the subgroup $G_\alpha := \langle \sigma^\alpha \rangle$ of $Gal(L/K)$ (see Lemma 4.43).*
2. *The element a which was used for the definition of Γ was contained in K_0 and the field K_0 is isomorphic to $K(b)$.*
3. *The last two points yield that we can define the usual cyclic algebra $B := (L(b)/K(b), \sigma^\alpha, a)$. Let $u \in B$ such that*
   - *$B = \bigoplus_{i=0}^{s-1} L(b)u^i$,*
   - *$u^s = a \in L(b)$ and $uy = \sigma^\alpha(y)u$ for all $y \in L(b)$.*
4. *We have*
$$|\Gamma : K_0| = n|A : K_0| = n\alpha|L(b) : K(b)| \underset{|L(b):K(b)|=\frac{n}{\alpha}}{=} n\frac{n}{\alpha}\alpha = n^2.$$
5. *Moreover we get*
$$|M_\alpha(B) : K(b)| = \alpha^2|B : K(b)| = \alpha^2\left(\frac{n}{\alpha}\right)^2 = n^2.$$
6. *So we get all in all $|M_\alpha(B) : K(b)| = |\Gamma : K(b)|$, hence it could be possible - at least from the point of dimensions - that we have an isomorphism $\Gamma \simeq M_\alpha(B)$.*

Notation 4.64 *We set $e_i := (0, \ldots, 0, \underbrace{1}_{\substack{at\ the\ i\text{-}th \\ position}}, 0, \ldots, 0) \in A \subset \Gamma$.*

Remark 4.65 *The elements $e_1, \ldots, e_\alpha$ form a complete set of pairwise orthogonal idempotents.*

Lemma 4.66 (The two sided Pierce Decomposition) *Let T be an arbitrary ring and $e_1, \ldots, e_s \in T$ be pairwise orthogonal idempotents, with $\sum_{i=1}^s e_i = 1$. There is an isomorphism of rings*
$$\Phi : T \longmapsto \begin{pmatrix} e_1Te_1 & \ldots & e_1Te_s \\ e_2Te_1 & \ldots & e_2Te_s \\ & \vdots & \\ e_sTe_1 & \ldots & e_sTe_s \end{pmatrix}$$
$$t \longmapsto (e_ite_j)_{ij}.$$

Corollary 4.67 *An application of the two-sided Pierce Decomposition (see Lemma 4.66) yields that we have an isomorphism*

$$\Gamma \simeq \begin{pmatrix} e_1\Gamma e_1 & \dots & e_1\Gamma e_\alpha \\ \vdots & & \vdots \\ e_\alpha\Gamma e_1 & \dots & e_\alpha\Gamma e_\alpha \end{pmatrix}.$$

Notations 4.68 *1. We represent an arbitrary element x contained in Γ as $x = \sum_{l=0}^{n-1}({a_k}^l)\lambda_{\sigma^l}$ whereby we set $({a_k}^l) := ({a_0}^l, \dots, {a_{\alpha-1}}^l)$.*

2. Moreover let $\lambda_k(h) := (0, \dots, 0, \underbrace{h + \sigma^{k-1}(g)L[q]}_{(k+1)\text{-th position}}, 0, \dots, 0)$ for $0 \le k \le \alpha - 1$ and a polynomial $h \in L[q]$.

Observations 4.69 *We determine the structure of the $e_i\Gamma e_j$'s, whereby we remember that $s = \frac{n}{\alpha}$ holds:*

1. Calculation of $e_i x$ for an arbitrary i:

$$\begin{aligned} e_i x = d_i(1)x = d_i(1)\Big(\sum_{l=0}^{n-1}({a_k}^l)\lambda^l\Big) = \sum_{i=0}^{n-1} d_i(1)({a_k}^l)\lambda^l = \sum_{l=0}^{n-1} d_i({a_i}^l)\lambda^l \\ = (0, \dots, 0, {a_i}^0, 0 \dots, 0) + (0, \dots, 0, {a_i}^1, 0, \dots, 0)\lambda \\ + \dots + (0, \dots, 0, {a_i}^{n-1}, 0, \dots, 0)\lambda^{n-1}. \end{aligned}$$

2. Now we note that there is a uniquely determined element $0 \le l_0 \lneq \alpha$ with $l \equiv l_0 \mod \alpha$. Since $\sigma(1) = 1$ we get $\tau^l(d_j(1)) = \tau^{l_0}(d_j(1)) = d_{j+l_0}(1)$, where the index of d has to be taken modulo α. Using this information we conclude:

$$\begin{aligned} e_i x e_j = \sum_{l=0}^{n-1} d_i({a_i}^l)\lambda^l d_j(1) \underset{\substack{\text{using the} \\ \text{relations in } \Gamma}}{=} \sum_{l=0}^{n-1} d_i({a_i}^l)\tau^l(d_j(1))\lambda^l \\ \underset{\text{let } n=\alpha\cdot s}{=} \sum_{k=0}^{s-1}\sum_{d=0}^{\alpha-1} d_i({a_i}^{k\alpha+d})\tau^{k\alpha+d}(d_j(1))\lambda^{k\alpha+d} \\ = \sum_{k=0}^{s-1}\sum_{d=0}^{\alpha-1} d_i({a_i}^{k\alpha+d})d_{j+d}(a)\lambda^{k\alpha+d} \\ \underset{\text{per. def. of the } d_*()}{=} \sum_{k=0}^{s-1}\sum_{d=0}^{\alpha-1} \underbrace{\delta_{i,j+d}}_{\substack{\text{this Kronecker-}\delta \\ \text{has to be taken} \\ \text{modulo } \alpha \text{ in} \\ \text{both indices}}} d_i({a_i}^{k\alpha+d})\lambda^{k\alpha+d} =: x_0. \end{aligned}$$

We stop our calculation to note that $\delta_{i,j+d} \neq 0$ holds if and only if $i \equiv j + d \mod \alpha$ is satisfied and this is equivalent to $d \equiv i - j \mod \alpha$. Now let $0 \le \gamma_{i,j} \le \alpha - 1$ the representative of the residue class of $i - j$ modulo α. With this notation we can resume our interrupted calculation to obtain:

$$x_0 = \sum_{k=0}^{s-1} d_i({a_i}^{k\alpha+\gamma_{i,j}})\lambda^{k\alpha+\gamma_{i,j}}.$$

3. *Hence an arbitrary element of* $e_i\Gamma e_j$ *has the form*

$$\begin{aligned}&(0,\dots,0,\underbrace{a_0}_{ith\ position},0,\dots,0)\lambda^{\gamma_{i,j}}\\ &+(0,\dots,0,\underbrace{a_1}_{ith\ position},0,\dots,0)\lambda^{\alpha+\gamma_{i,j}}+\dots\\ &+(0,\dots,0,\underbrace{a_{s-1}}_{ith\ position},0,\dots,0)\lambda^{(s-1)\alpha+\gamma_{i,j}}.\end{aligned}$$

Lemma 4.70 *There is an isomorphism of* $K(b)$*-algebras:*

$$\Phi : M_\alpha(B) \longrightarrow \begin{pmatrix} e_1\Gamma e_1 & \dots & e_1\Gamma e_n \\ \vdots & & \vdots \\ e_n\Gamma e_1 & \dots & e_n\Gamma e_n \end{pmatrix}.$$

Proof. We first verify the following

Claim. For every pair i,j and every $0 \leq k \leq s-1$ we have that the element $d_i(1)\lambda^{k\alpha+i-j}$ is contained in $e_i\Gamma e_j$.

Proof of the Claim. We distinguish two cases:

- Let us assume that $i \geq j$ holds, then $i-j \geq 0$ holds and we have of course $\gamma_{i,j} = i-j$ and so we are done by Observations 4.69.
- Now let us assume that $i < j$ is satisfied and so we have $i-j < 0$. But this implies now $\alpha + i - j = \gamma_{i,j}$ and so we are also done by the virtue of Observations 4.69.

□

For every pair i,j we set

$$\begin{aligned}\varphi_{ij} : B &\longmapsto e_i\Gamma e_j\\ u^k &\longmapsto d_i(1)\lambda^{k\alpha+i-j}.\end{aligned}$$

Now we define

$$\begin{aligned}\Phi : M_\alpha(K_0)\otimes_{K_0} B &\longrightarrow (e_i\Gamma e_j)_{ij}\\ (a_{ij})_{ij}\otimes b &\longmapsto (a_{ij}\varphi_{ij}(b))_{ij}.\end{aligned}$$

1. The universal property of the tensor product yields immediately that Φ is a well defined homomorphism of K_0-vector spaces.
2. We find

$$\begin{aligned}&\Phi\Big(\big(e_{ij}\otimes b_k u^k\big)\big(e_{i'j'}\otimes b_{k'}u^{k'}\big)\Big)\\ &\underset{\substack{\text{per. def. of the}\\ \text{mult. in } M_\alpha(K)\times_{K_0} B}}{=} \Phi\Big(e_{ij}e_{i'j'}\otimes b_k u^k b_{k'}u^{k'}\Big)\\ &\underset{\substack{\text{per. def. of the}\\ \text{mult. in } B}}{=} \Phi\Big(e_{ij}e_{i'j'}\otimes b_k\sigma^{k\alpha}(b_{k'})u^{k+k'}\Big)\\ &\underset{\text{obvious}}{=} \Phi\Big(\delta_{ji'}e_{ij'}\otimes b_k\sigma^{k\alpha}(b_{k'})u^{k+k'}\Big)\\ &\underset{\substack{\text{per. def. of }\Phi\\ \text{and the maps } \varphi_{ij}}}{=} \delta_{ji'}e_{ij'}d_i(b_k\sigma^{k\alpha}(b_{k'}))u^{(k+k')\alpha+i-j'}.\end{aligned}$$

3. On the other side we have

$$\begin{aligned}
&\Phi\Big(e_{ij}\otimes b_k u^k\Big)\cdot\Phi\Big(e_{i'j'}\otimes b_{k'}u^{k'}\Big)\\
&\underset{\substack{\text{per. def. of }\Phi\\ \text{and the maps }\varphi_{ij}}}{=} e_{ij}d_i(b_k)u^{k\alpha+i-j}\cdot e_{i'j'}d_{i'}(b_{k'})u^{k'\alpha+i'-j'}\\
&\underset{\substack{\text{we can w.l.o.g.}\\ \text{assume } j=i'}}{=} \delta_{ji'}e_{ij'}d_i(b_k)u^{k\alpha+i-i'}d_{i'}(b_{k'})u^{k'\alpha+i'-j'}\\
&= \delta_{ji'}e_{ij'}d_i(b_k)\tau^{k\alpha+i-i'}(d_i(b_{k'})u^{k\alpha+i-i'+k'\alpha+i'-j'}\\
&\underset{\text{per. def. of }\tau}{=} \delta_{ji'}e_{ij'}d_i(b_k)d_{i'+i-i'}(\sigma^{k\alpha}(b_{k'}))u^{(k+k')\alpha+i-j'}\\
&= \delta_{ji'}e_{ij'}d_i(b_k\sigma^{k\alpha}(b_{k'}))u^{(k+k')\alpha+i-j'}.
\end{aligned}$$

4. The points 2 and 3 yield that Φ is a homomorphism of K_0-algebras.

5. $M_\alpha(K_0)\otimes_{K_0}B$ is a simple K_0-algebra (see for example [Rei75, Theorem 7.6]) and so Φ is - as a homomorphism of algebras - injective. Moreover we get from Observations 4.63 that the K_0-dimensions of $M_\alpha(B)$ and Γ coincide and so we get immediately that Φ is an isomorphism.

□

4.6 Extensions of the residue class field

4.6.1 The Arbitrary Case of a Perfect Residue Class Field

Let $(A,\mathfrak{m})$ be an arbitrary commutative Noetherian local ring with a perfect residue class field $\mathfrak{f} := A/\mathfrak{m}$ and field of fractions F. Moreover let F'/F be a finite separable unramified extension. We set $B :=$ alg. int.$_A(F')$.

Lemma 4.71 *There is an element $\omega\in B$ with $B=A[\omega]$ and $\bar{\omega}\in B/\mathfrak{m}B =: \mathfrak{f}'$ is a primitive element for the field extension $\mathfrak{f}'/\mathfrak{f}$.*

Proof.

- We know that $\mathfrak{f}'/\mathfrak{f}$ is a finite field extension and that $\mathfrak{f}$ is - by our assumption - a perfect field. So $\mathfrak{f}'$ is a finite separable extension of $\mathfrak{f}$. We can apply the Primitive Element Theorem to deduce that there is some element $\alpha\in\mathfrak{f}'$ with $\mathfrak{f}'=\mathfrak{f}(\alpha)=\mathfrak{f}[\alpha]$.

- Choose an element $\omega\in B$ with $\omega+\mathfrak{m}B=\bar{\omega}=\alpha$. For an arbitrary element $b\in B$ we find elements $a_i\in A$ with $\bar{b}=\sum_i\bar{a}_i\alpha^i=\overline{\sum_i a_i\omega^i}$. Hence we have $B=B[\omega]+\mathfrak{m}B$ and Nakayama's Lemma yields $B=B[\omega]$.

□

Remarks 4.72 *1. In the situation of Lemma 4.71 we have - using the same notations as in the Lemma - that $F'=F(\omega)$ holds, hence ω is a primitive element for the field extension F'/F.*

2. *Assume that $\varphi \in A[q]$ is a normed polynomial such that $\bar{\varphi}$ is the minimum polynomial of $\alpha \in \mathfrak{f}'$ where we can w.l.o.g. assume that the degrees of the polynomials φ and $\bar{\varphi}$ coincide.*

   Claim. $\varphi \in F[q]$ is the minimum polynomial of $\omega \in F'$ (so we have in particular $|F' : F| = |\mathfrak{f}' : \mathfrak{f}|$).

   Proof of the Claim. We can w.l.o.g. assume that φ is a normed polynomial. The reduction $\bar{\varphi}$ of φ modulo π is irreducible, so φ itself has to be an irreducible polynomial. Moreover φ has ω as a root, so φ is the minimum polynomial of ω. □

Corollary 4.73 *Let the notations be as in Lemma 4.71 and in its proof. Assume that the field extension F'/F is Galois, then the natural map*

$$\Phi : Gal(F'/F) \longrightarrow Gal(\mathfrak{f}'/\mathfrak{f})$$
$$\sigma \longmapsto [\bar{\sigma} : B/\mathfrak{m}B \ni b + \mathfrak{m}B \longmapsto \sigma(b) + \mathfrak{m}B \in B/\mathfrak{m}B]$$

is an isomorphism of groups, in particular the field extension $\mathfrak{f}'/\mathfrak{f}$ is Galois and we have an equality $|F' : F| = |\mathfrak{f}' : \mathfrak{f}|$.

Proof. We can lift the minimum polynomial of α (a primitive element for the field extension $\mathfrak{f}'/\mathfrak{f}$) to the minimum polynomial of ω (a primitive element of the field extension F'/F). The polynomial $\varphi \in A[q]$ is normed, so all its root are contained in B (where we use that the extension F'/F is Galois and so in particular normal). The roots of φ will be denoted by $\omega_1, \ldots, \omega_n$. So we get $\varphi = \prod_{i=1}^{n}(q - \omega_i) \in B[q]$. Hence $\bar{\varphi} = \prod_{i=1}^{n}(q - \overline{\omega_i}) \in B/\mathfrak{m}B[q] = \mathfrak{f}'[q]$. We have assumed that the field $\mathfrak{k}$ is perfect, so the extension $\mathfrak{f}'/\mathfrak{f}$ is separable and so also its primitive element α has to be separable. So the minimum polynomial $\bar{\varphi}$ has no repeated roots, so all the elements $\overline{\omega_i}$ are pairwise disjoint and they are contained in $\mathfrak{f}'$. So $\mathfrak{f}'/\mathfrak{f}$ is a normal extension and so we have verified that $\mathfrak{f}'/\mathfrak{f}$ is a Galois extension. Since the extension $\mathfrak{f}'/\mathfrak{f}$ is Galois the elements of the Galois group are exactly the maps which send α to some of the $\overline{\omega_i}$, an analogous description for $\mathrm{Gal}(F'/F)$ holds and so Φ is bijective and so in particular an isomorphism of groups. □

4.6.2 An Application for Polynomial Rings

Let T be an arbitrary commutative Noetherian ring and q an indeterminate over T. By $T[q]$ we denote as usual the polynomial ring over T. We describe the spectrum of the ring $T[q]$. In this section we follow [Eis99, Excercise 10.2] to prove

Lemma 4.74 *Let $\mathfrak{P}$ be a prime ideal of $T[q]$ and $\mathfrak{p} := T \cap \mathfrak{P} \in Spec(T)$. Then either*

1. *$\mathfrak{P} = \mathfrak{p}T[q]$ and $ht(\mathfrak{P}) = ht(\mathfrak{p})$ or*
2. *there is a polynomial $f = \sum_{j=0}^{m} r_j q^j \in T[q]$ such that the leading coefficient r_m is not contained in $\mathfrak{p}$ and*

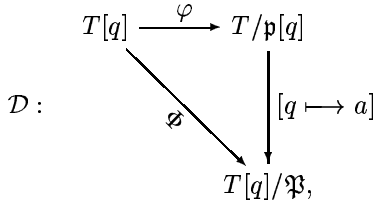
$$\mathfrak{P} = \{g \in T[q] \mid \exists a \in T \setminus \mathfrak{p} \,:\, ag \in \langle \mathfrak{p}, f \rangle\}.$$

   Here we have $ht(\mathfrak{P}) = ht(\mathfrak{p}) + 1$.

Proof.

1. If $\mathfrak{P} = \mathfrak{p}T[q]$ holds, we are done. So we can w.l.o.g. assume that $\mathfrak{P} \supsetneq \mathfrak{p}T[q]$ is satisfied. Let $\Phi : T[q] \longrightarrow T[q]/\mathfrak{P}$ be the reduction modulo $\mathfrak{P}$. The field of fractions of the integral domain $T/\mathfrak{p}$ will be denoted by F.

   Using the universal property of a polynomial ring, we find a field extension L of F and an element $a \in L$ with $a = \Phi(q)$ and $U := T[q]/\mathfrak{P} = \big(T/\mathfrak{p}\big)[a] \subset L$ such that the following diagram is commutative:



   where φ denotes the reduction modulo $\mathfrak{p}T[q]$.

   Using the factorization given by $\mathcal{D}$ we can w.l.o.g. assume that T is an integral domain and $0 = \mathfrak{p} = \mathfrak{P} \cap T$ holds; so $\Phi : q \longmapsto a \in T[a] = T[q]/\mathfrak{P}$. The element a has a minimal polynomial over F, we denote this polynomial by μ. There is some $0 \neq r \in T$ with $f := r\mu \in T[q]$.

   Claim. We have $\mathfrak{P} = \{g \in T[q] \mid \exists 0 \neq s \in T \,:\, sg \in \langle f \rangle\} =: \mathfrak{a}$.

   Proof of the Claim. Let $g \in \mathfrak{a}$, hence we find some $0 \neq s \in T$ with $sg \in \langle f \rangle$ and so $(sg)(a) = s \cdot g(a) = 0$. We get $g(a) = 0$ and this means $g \in \ker \Phi = \mathfrak{P}$.

   Now chose some $g \in \mathfrak{P}$, then $g(a) = 0$, hence f divides g in $K[q]$ and so we find some $0 \neq a \in T$ with $ag \in \langle f \rangle$ as claimed. □

2. Assume that $\mathfrak{P} \neq 0$ holds. The first point yields, that there is a $0 \neq f \in T[q]$ with $\mathfrak{P} = \{g \in T[q] | \exists 0 \neq a \in T : ag \in \langle f \rangle\}$. Assume there is a $\mathfrak{Q} \in \mathrm{Spec}(T[q])$ with $0 \subsetneq \mathfrak{Q} \subset \mathfrak{P}$. So $\mathfrak{Q} \cap T = 0$ and there is some $0 \neq f^{'} \in T[q]$ with $\mathfrak{Q} = \{g \in T[q] \mid \exists 0 \neq a \in T \,:\, ag \in \langle f^{'} \rangle\}$. We know moreover $\langle f \rangle = \langle \mu \rangle$ and $\langle f^{'} \rangle = \langle \mu^{'} \rangle$ in $L[q]$ for some irreducible polynomials μ and $\mu^{'}$ with $\langle \mu^{'} \rangle \subset \langle \mu \rangle$; but both $\langle \mu^{'} \rangle$ and $\langle \mu \rangle$ are maximal ideals of the ring $L[q]$ and so we get $\mathfrak{P} = \mathfrak{Q}$. This observation ensures that there will be no prime ideals between the two types of prime ideals lying over $\mathfrak{p} \in \mathrm{Spec}(T)$. We are done when we can show that $\mathrm{ht}_{T[q]}(\mathfrak{p}T[q]) = \mathrm{ht}_T(\mathfrak{p})$ holds for every $\mathfrak{p} \in \mathrm{Spec}(T)$. For this fact see [Eis99, Corollary 10.13 c].

   □

Let R be a discrete valuation domain with prime π, perfect residue class field $\mathfrak{k}$ and field of fractions K. Let L/K be a finite separable and unramified extension of K. We set $S :=$ alg. $\mathrm{int.}_R(L)$. Moreover let $\mathfrak{k} := R/\pi$ and $\mathfrak{k}^{'} := S/\pi S$.

Remark 4.75 *Since S/R is an unramified extension, S is a discrete valuation domain and π is a prime element of S.*

Proposition 4.76 *Assume that B/A is an extension of integral domains and let $A^{'}$ be the integral closure of A in B. Moreover let q be an indeterminate over A and B respectively. Then we get*

$$\textit{alg. int.}_{A[q]}(B_{[}q]) = A^{'}[q].$$

Proof. Cf. [Bas68, Proposition 5.12]. □

Notations 4.77 *1. For a commutative ring T we denote by $\tilde{T}$ the polynomial ring $T[q]$ over T.*

2. We denote by $\tilde{S}_{(\pi)}$ the localization of the ring $\tilde{S}$ at the multiplicative set $\tilde{R} \setminus \pi\tilde{R} \subset \tilde{S}$.

Lemma 4.78 *1. $\pi S[q]$ is the only prime ideal of $S[q]$ which is over $\pi R[q]$.*

2. We have in particular $Spec(\tilde{S}_{(\pi)}) = \{0, \pi\tilde{S}_{(\pi)}\}$ and so $\tilde{S}_{(\pi)}$ is a discrete valuation domain with radical $\pi\tilde{S}_{(\pi)}$.

Proof.

1. We note first that Proposition 4.76 implies that $\tilde{R}$ is integral closed and $\tilde{S}/\tilde{R}$ is an integral extension, so we are in the situation to apply Lemma 4.29 to deduce that for a $\mathfrak{P} \in \mathrm{Spec}(S[q])$ with $\mathfrak{P} \cap R[q] = \pi R[q]$ follows $\mathrm{ht}(\mathfrak{P}) = 1$. Now assume $\mathfrak{P} \cap R[q] = \mathfrak{p}$ and $\mathfrak{P} \neq \pi S[q]$. Since πS is the only element of $\mathrm{ht}^1(S)$ we get from Lemma 4.74 that $\mathfrak{P} \cap S = 0$ holds. Moreover we have

$$\pi R = R \cap \pi R[q] \underset{\mathfrak{P}\cap R[q]=\pi R[q]}{=} R \cap R[q] \cap \mathfrak{P}$$
$$\underset{R=R\cap S}{=} R \cap S \cap R[q] \cap \mathfrak{P} \subset S \cap \mathfrak{P} = 0,$$

   a contradiction.

2. An application of Corollary 4.30 implies immediately that $\tilde{S}_{(\pi)}$ is a discrete valuation domain with prime π.

□

Observations 4.79 *1. Let us recall a well-know fact. Let T be commutative ring and and assume that $\mathfrak{p}$ is some prime ideal of T. Then there is an isomorphism $T_{\mathfrak{p}}/\mathfrak{p}T_{\mathfrak{p}} \simeq frac(T/\mathfrak{p})$.*

2. We note that $\pi\tilde{R}_{(\pi)}$ is the radical of $\tilde{R}_{(\pi)}$. Using point 1.) we get moreover:

$$\tilde{R}_{(\pi)}/\pi\tilde{R}_{(\pi)} \simeq frac\Big(\tilde{R}/\pi\tilde{R}\Big)$$
$$\underset{per.\ def.\ of\ \tilde{R}}{=} frac\Big(R[q]/\pi R[q]\Big) \underset{R[q]/\pi R[q]\simeq(R/\pi)[q]}{=} frac\Big((R/\pi)[q]\Big)$$
$$= frac(\mathfrak{k}[q]) = \mathfrak{k}(q).$$

3. We get from Lemma 4.78 that $\pi\tilde{S}$ is the only prime ideal which is over $\pi\tilde{R}$, so we can apply Lemma 4.31 to conclude: $\tilde{S}_{(\pi)} = \tilde{S}_{\pi\tilde{S}}$.

4. With the previous point we conclude:

$$\tilde{S}_{(\pi)}/\pi\tilde{S}_{(\pi)} = \tilde{S}_{\pi\tilde{S}}/\pi\tilde{S}_{\pi\tilde{S}} \simeq frac\Big(\tilde{S}/\pi\tilde{S}\Big)$$
$$\underset{per.\ def.\ of\ \tilde{S}}{=} frac\Big(S[q]/\pi S[q]\Big) \underset{S[q]/\pi S[q]\simeq(S/\pi)[q]}{=} frac\Big((R/\pi)[q]\Big)$$
$$= frac(\mathfrak{k}'[q]) = \mathfrak{k}'(q).$$

Corollary 4.80 *The field extension $\mathfrak{k}'(q)/\mathfrak{k}(q)$ is Galois of degree n and there is an isomorphism $Gal(\mathfrak{k}'(q)/\mathfrak{k}(q)) \simeq Gal(L/K)$.*

Proof. We use Corollary 4.73 to deduce that $\mathfrak{k}'/\mathfrak{k}$ is a Galois extension which group is in a natural way isomorphic to $\mathrm{Gal}(L/K)$. Now we are done by using Lemma 4.21. □

4.7 The Theorem and its Proof

For the convenience of the reader we recall the assumptions which we have already stated at the begin of Chapter 4.

- We consider a Hasse skewfield D given in its standard representation, i.e. $D = (L/K, \sigma, \pi)$, where σ is a generator of the Galois group $\mathrm{Gal}(L/K)$. The uniquely determined maximal order in D is $\Lambda = (S/R, \sigma, \pi)$.
- We have fixed a lift $A_{\tilde{f}}$ of D with $A_{\tilde{f}} := L(q)(S[q]/R[q], \sigma, \tilde{f})$ where $\tilde{f} = \left(\prod_{i=1}^{t} g_i\right) f$ such that f is irreducible in $S[q]$, $f(0) = \pi$ holds and the g_i's are irreducible elements in $S[q]$ such that
  - $g_i(0) = \varepsilon_i \in R^\times$ for every $1 \leq i \leq t$, so we have in particular that $fR[q] \neq g_i R[q]$ holds for all the i's.
  - The prime ideals $g_i R[q]$ are pairwise different, this means that the g_i are pairwise non adjoint prime elements of $R[q]$.

  By Lemma 4.1 f and the g_i's are irreducible in $R[q]$. In the lift $A_{\tilde{f}}$ we consider the $R[q]$-order $\Lambda_{\tilde{f}} := (S[q]/R[q], \sigma, \tilde{f})$ which is a lift of the maximal order Λ in D and now can state and afterwards prove

Theorem 4.81 *The lift $\Lambda_{\tilde{f}}$ of the maximal order Λ is again a maximal oder.*

To prove Theorem 4.81 we will verify - using the results of Sections 4.2 - 4.6 - some Lemmas concerning the structure of the localizations $\Lambda_{\tilde{f},\mathfrak{p}} = \left(\Lambda_{\tilde{f}}\right)_{\mathfrak{p}}$ with $\mathfrak{p} \in \mathrm{ht}^1(R[q])$. We have to distinguish three cases for the prime ideal $\mathfrak{p}$. For simplify the arguments we use in the proof we need a reduction, here for we make the

Observations 4.82 *1. Let B/A be an integral extension of factorial domains. We consider an element $a = \prod_{i=1}^{m} p_i \in A$ such that all the factors p_i are irreducible in B, so - using Lemma 4.1 - these elements are also irreducible in A. We assume moreover that the p_i's are pairwise non adjoint in A. We note that by Corollary 4.2 the elements p_i are also not adjoint in B. Now let $\mathfrak{p} \in ht^1(A)$ be an arbitrary element. Since A is a factorial ring, the prime ideal $\mathfrak{p}$ is principal, say $\mathfrak{p} = qA$ for a suitable prime element $q \in A$. We distinguish two cases for the element q:*

- *Let us first assume that q is adjoint to some of the p_i's, i.e. we have $qA = p_i A$ for some $1 \leq i \leq m$. Then $aA_{\mathfrak{p}} = p_i A_{\mathfrak{p}}$, so after localization we can not distinguish the ideals $(aA)_{\mathfrak{p}}$ and $(p_i A)_{\mathfrak{p}}$ and we do can not determine anymore if we have originally considered the ideal aA or $p_i A$.*
- *Now consider the case, that $qA \neq p_i A$ holds for all $1 \leq i \leq m$. Then a is not contained in the prime ideal $\mathfrak{p}$ and so $\frac{a}{1}$ is a unit in $A_{\mathfrak{p}}$ and in $B_{\mathfrak{p}}$ respectively.*

2. *Using the first point we see that the structure of the localized algebras $\Lambda_{\tilde{f},\mathfrak{p}}$ for $\mathfrak{p} \in ht^1(R[q])$ just depends on at most one of the polynomials f and $g_1, \ldots, g_t$. Since we are - according to the sketch of the proof of Theorem 4.81 (see Section 4.81) - just interested in the localizations of $\Lambda_{\tilde{f}}$ at the prime ideals $\mathfrak{p}$ of $ht^1(R[q])$, we can therefor w.l.o.g. assume that $\tilde{f} = f$ holds for some polynomial f which is irreducible in $S[q]$ and so also in $R[q]$ by the virtue of Lemma 4.1. The new polynomial f is either the original polynomial f - the last factor in the representation $\tilde{f} = \left(\prod_{i=1}^{t} g_i\right) f$ - or one of the other factors g_i.*

For concrete calculations we introduce the

Notation 4.83 *Let the element $\lambda \in \Lambda_f$ be, such that*

- $\Lambda = \bigoplus_{i=0}^{n-1} S[q]\lambda^i$,
- $\lambda^n = f$ *and* $\lambda y = \sigma(y)\lambda$ *for all* $x \in S[q]$

hold.

Case 1: $\mathfrak{p} = fR[q]$

Lemma 4.84 *Let $\mathfrak{p} = fR[q]$. We have that $rad(\Lambda_{f,\mathfrak{p}}) = \lambda\Lambda_{f,\mathfrak{p}}$ is projective over Λ and it is the unique maximal two-sided ideal of Λ.*

Proof. We have $\Lambda_{f,\mathfrak{p}} = \bigoplus_{i=0}^{n-1} R[q]_{\mathfrak{p}}\lambda^i$, and so we are in the case, that we can apply Lemma 4.19 to conclude that $\mathrm{rad}(\Lambda_{f,\mathfrak{p}}) = \lambda\Lambda_{f,\mathfrak{p}}$ is the unique maximal two-sided ideal of $\Lambda_{f,\mathfrak{p}}$. Since Λ_f is contained in the skewfield $L(q)\Lambda_f$, it is immediately clear that $\lambda\Lambda_{f,\mathfrak{p}} \underset{\text{Lemma 4.19}}{=} \Lambda_{f,\mathfrak{p}}\lambda$ is a projective $\Lambda_{f,\mathfrak{p}}$-module. □

Case 2: $\mathfrak{p} = hR[q]$ **with** $\deg(h) \geq 1$

For the second case we need first the (see also the Sections 4.3.1 and 4.3.2)

Notation 4.85 *For an $\alpha \in \mathbb{N}$ which divides n we set $G_\alpha := \langle\sigma^\alpha\rangle \subset Gal(L/K)$, $E_\alpha := Fix(G_\alpha)$ and moreover $S_\alpha := alg.\ int._R(E_\alpha) = S \cap E_\alpha$.*

Now we make the

Observations 4.86 *Let $h \in R[q]$ be an irreducible polynomial with $deg(h) \geq 1$.*

1. *By Corollary 4.37 there is an element $\alpha \in \mathbb{N}$ which divides n and a polynomial g in $S_\alpha[q] \subset S[q]$ which is irreducible in $S_\alpha[q]$ and in $S[q]$ respectively such that $h = g\sigma(g)\cdots\sigma^{\alpha-1}(g)$ holds.*
2. *Since S/R is unramified and h is primitive we get immediately that all the polynomials $\sigma^i(g)$ are primitive (in $S[q]$).*
3. *So we can set $\mathfrak{P}_i := \sigma^i S[q]$ and get $\mathfrak{P}_i \in ht^1(S[q])$ for all $0 \leq i \leq \alpha - 1$.*
4. *Let a be a common root of the polynomials h and g contained in some algebraic extension of L. According to the Lemmas 4.40 and 4.41 we have isomorphisms $K[q]/hK[q] \simeq K(a)$ and $L[q]/\sigma^i(g)L[q] \simeq L(a)$ for all $0 \leq i \leq \alpha - 1$.*
5. *Both polynomials f and h are assumed to be irreducible, so they are in particular primitive, hence we have that $fK[q] \neq hK[q]$ holds and we can conclude that $f + hK[q] \neq 0$ is satisfied. Using the isomorphism $K[q]/hK[q] \simeq K(a)$ we will identify the residue class $f + hK[q]$ with some element $0 \neq b \in K(a)$.*

Lemma 4.87 *We use the notations which we have introduced in Notation 4.85 and Observations 4.86. Moreover we assume that* $\mathfrak{p} = hR[q] \neq fR[q]$ *is satisfied. We obtain*

1. $rad(\Lambda_{f,\mathfrak{p}}) = \mathfrak{p}\Lambda_{f,\mathfrak{p}}$ *and*
2. $\Lambda_{f,\mathfrak{p}}/rad(\Lambda_{f,\mathfrak{p}}) = M_\alpha((L(a)/K(a), \sigma^\alpha, b)$.

Proof. The prime ideals $\mathfrak{P}_i$ are exactly the elements of $\mathrm{ht}^1(S[q])$ which are over $hR[q]$, using Lemma 4.29 in combination with Proposition 4.76 we get moreover that these are all the prime ideals of $S[q]$ which lie over $\mathfrak{p}$. Using Lemma 4.30 we obtain that the ideals $\sigma^i(g)S[q]_\mathfrak{p}$ are exactly the maximal ideals of $S[q]_\mathfrak{p}$. We make some observations

- First we examine the quotient $S[q]_\mathfrak{p}/\mathfrak{p}S[q]_\mathfrak{p}$, here for we need the

  Lemma 4.88 *Let* B/A *be an integral extension of integral domains and* $\mathfrak{p} \in Spec(A)$ *an arbitrary element. Moreover let* $\mathfrak{P} \in Spec(B)$ *be such that* $\mathfrak{P} \cap A = \mathfrak{p}$ *holds. There is an isomorphism* $B_\mathfrak{p}/\mathfrak{P}B_\mathfrak{p} \simeq frac(B/\mathfrak{P})$.

  Proof. Cf. [Bou89b, Paragraph 2, no. 5; Proposition 11]. □

  We note again, that the $\mathfrak{P}_i$'s are pairwise disjoint maximal ideals of $S[q]_\mathfrak{p}$, so we can apply the Chinese Remainder Theorem in the following calculation:

$$\begin{aligned} S[q]_\mathfrak{p}/\mathfrak{p}S[q]_\mathfrak{p} &= S[q]_\mathfrak{p}/\prod_{i=0}^{\alpha-1}\sigma^i(g)S[q]_\mathfrak{p} \\ &\underset{\text{Chinese Remainder Theorem}}{=} \prod_{i=0}^{\alpha-1} S[q]_\mathfrak{p}/\sigma^i(g)S[q]_\mathfrak{p} \\ &\underset{\text{Lemma 4.88}}{=} \prod_{i=0}^{\alpha-1} \mathrm{frac}\big(S[q]/\sigma^i(g)S[q]\big) \\ &\underset{\text{Lemma 4.41}}{\simeq} \prod_{i=0}^{\alpha-1} L[q]/\sigma^i(g)L[q] \end{aligned}$$

- We will use the notations of Section 4.4. We know that the generator σ of the Galois Group induces the automorphism

$$\bar{\sigma} : S[q]_\mathfrak{p}/\mathfrak{p}S[q]_\mathfrak{p} \ni s + \mathfrak{p}S[q]_\mathfrak{p} \longmapsto \sigma_\mathfrak{p}(s) + \mathfrak{p}S[q]_\mathfrak{p}.$$

- Applying Lemma 4.55 we obtain that we get the automorphism $\bar{\sigma}'$ when we conjugate $\bar{\sigma}$ with the isomorphism of the Chinese Remainder Theorem:

$$\begin{aligned} &\bar{\sigma}'\left(a_0 + g\tilde{S}_\mathfrak{p}, \ldots, a_{\alpha-1} + \sigma^{\alpha-1}(g)\tilde{S}_\mathfrak{p}\right) \\ &= \left(\sigma(a_{\alpha-1}) + g\tilde{S}_\mathfrak{p}, \sigma(a_0) + \sigma(g)\tilde{S}_\mathfrak{p}, \ldots, \sigma(a_{\alpha-2}) + \sigma^{\alpha-1}(g)\tilde{S}_\mathfrak{p}\right). \end{aligned}$$

  So we are in the situation to apply Lemma 4.70 to conclude that we have an isomorphism $\Lambda_{f,\mathfrak{p}}/\mathfrak{p}\Lambda_{f,\mathfrak{p}} \simeq M_\alpha((L(a)/K(a), \sigma^\alpha, b)$ which is a central simple $K(a)$-algebra, so in particular a simple ring.

With these Observations we are done. □

Case 3: $\mathfrak{p} = \pi R[q]$

Lemma 4.89 *Let $\mathfrak{p} = \pi R[q]$. In this case we obtain*

1. *$rad(\Lambda_{f,\mathfrak{p}}) = \mathfrak{p}\Lambda_{f,\mathfrak{p}}$*
2. *$\Lambda_{f,\mathfrak{p}}/rad(\Lambda_{f,\mathfrak{p}}) \simeq (\mathfrak{k}'(q)/\mathfrak{k}(q), \bar{\sigma}, \bar{f})$, where $\bar{\sigma}$ is the automorphism on $\mathfrak{k}'$ which is induced by σ and $\bar{f} := f + \pi R[q]$. since f is assumed to be primitive we have that $\bar{f}$ is* not *zero.*

Proof. We have

$$\Lambda_{f,\mathfrak{p}} = \Big(\bigoplus_{i=0}^{n-1} S[q]\lambda^i\Big)_{\mathfrak{p}} = R[q]_{\mathfrak{p}} \otimes_{R[q]} \Big(\bigoplus_{i=0}^{n-1} S[q]\lambda^i\Big) = \bigoplus_{i=0}^{n-1} (R[q]_{\mathfrak{p}} \otimes_{R[q]} S[q])\lambda^i.$$

We make some observations:

1. The Lemmas 4.31 and 4.78 yield $R[q]_{\mathfrak{p}} \otimes_{R[q]} = S[q]_{\mathfrak{P}}$ with $\mathfrak{P} = \pi S[q]$.
2. We get

$$\Lambda_{f,\mathfrak{p}}/\mathfrak{p}\Lambda_{f,\mathfrak{p}} = \Big(\bigoplus_{i=0}^{n-1} S[q]_{\mathfrak{P}}\lambda^i\Big) \Big/ \Big(\bigoplus_{i=0}^{n-1} \pi S[q]_{\mathfrak{P}}\lambda^i\Big)$$
$$= \bigoplus_{i=0}^{n-1} (S[q]_{\mathfrak{P}}/\pi S[q]_{\mathfrak{P}})\mu^i \underset{\text{Observations 4.79}}{=} \bigoplus_{i=0}^{n-1} \mathfrak{k}'(q)\mu^i,$$

   where μ is a representative of the residue class of λ. Using Corollary 4.80 we obtain immediately that $\Lambda_{f,\mathfrak{p}}/\mathfrak{p}\Lambda_{f,\mathfrak{p}}$ is a crossed product algebra for the Galois extension $\mathfrak{k}'(q)/\mathfrak{k}(q)$, so in particular a simple algebra.
3. Since $R[q]_{\mathfrak{p}}$ is a local ring and $\Lambda_{f,\mathfrak{p}}$ is finitely generated over $R[q]_{\mathfrak{p}}$ we get $\mathfrak{p}\Lambda_{f,\mathfrak{p}} \subset \mathrm{rad}(\Lambda_{f,\mathfrak{p}})$. Since the quotient $\Lambda_{f,\mathfrak{p}}/\mathfrak{p}\Lambda_{f,\mathfrak{p}}$ is simple we get $\mathrm{rad}(\Lambda_{f,\mathfrak{p}}) = \mathfrak{p}\Lambda_{f,\mathfrak{p}}$ is the unique maximal two sided ideal of $\Lambda_{f,\mathfrak{p}}$.

□

Now we are ready to state the

Proof of Theorem 4.81. We will use Theorem 4.3 to verify that Λ_f is a maximal order. So we have to check the two conditions which were stated in this theorem.

1. Λ_f is surely free over $S[q]$, so it is also free over $R[q]$, since $S[q]$ is free over $R[q]$, using that S is free over R. Since every free lattice is in particular divisorial, we obtain immediately $\bigcap_{\mathfrak{p}\in \mathrm{ht}^1(R[q])} \Lambda_{f,\mathfrak{p}} = \Lambda_f$ and so the first condition of the Theorem is checked.
2. We have to show that for every $\mathfrak{p} \in \mathrm{ht}^1(R[q])$ the $R[q]_{\mathfrak{p}}$-order $\Lambda_{f,\mathfrak{p}}$ is maximal. We use Theorem 4.4 to verify that the orders $\Lambda_{f,\mathfrak{p}}$ are maximal, i.e. we show that $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ is the unique maximal two sided ideal and that $\Lambda_{f,\mathfrak{p}}$ is a hereditary order. To verify that $\Lambda_{f,\mathfrak{p}}$ is hereditary it is, by Lemma 4.5, enough that $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ is projective over Λ. We have to distinguish again the three cases for the prime ideal $\mathfrak{p}$:

   a) Let $\mathfrak{p} = fR[q]$. Lemma 4.84 yields that $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ is the unique maximal two-sided ideal of $\Lambda_{f,\mathfrak{p}}$. Lemma 4.84 also yields that $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ is a projective $\Lambda_{f,\mathfrak{p}}$-module and so $\Lambda_{f,\mathfrak{p}}$ is hereditary.

b) Assume $\mathfrak{p} = gR[q]$ for $gR[q] \neq fR[q]$ and $\deg(g) \geq 1$. With Lemma 4.87 we get $\mathrm{rad}(\Lambda_{f,\mathfrak{p}}) = g\Lambda_{f,\mathfrak{p}}$ is projective over $\Lambda_{f,\mathfrak{p}}$ and it is the uniquely determined maximal two-sided ideal of $\Lambda_{f,\mathfrak{p}}$, hence $\Lambda_{f,\mathfrak{p}}$ is a maximal $R[q]_{\mathfrak{p}}$-order.

c) Let us assume that $\mathfrak{p} = \pi R[q]$ holds. Then obviously $\mathrm{rad}(\Lambda_{f,\mathfrak{p}}) = \pi\Lambda_{f,\mathfrak{p}}$ is projective over $\Lambda_{f,\mathfrak{p}}$, hence $\Lambda_{f,\mathfrak{p}}$ is hereditary. By Lemma 4.89 $\mathrm{rad}(\Lambda_{f,\mathfrak{p}})$ is the unique maximal two-sided ideal of $\Lambda_{f,\mathfrak{p}}$.

□

5 The non Maximal Lifts

Again - as in Chapter 4 - we use the notations and preliminaries of Section 3.1.2. We fix again a Hasse skewfield D in our standard representation (see Notation 2.37), hence $D = (L/K, \sigma, \pi)$, we remember that σ is assumed to be some generator of the Galois group $\mathrm{Gal}(L/K)$ (i.e. $\sigma = \rho^r$, where $1 \leq r \leq n-1$ with $(r,n) = 1$ holds and ρ is the Frobenius homomorphism). In D we consider as always the maximal order $\Lambda := (S/R, \sigma, \pi)$.

In this Chapter now we will consider lifts of $(L/K, \sigma, \pi)$ which are of the form $A_{hf} := L(q)(S[q]/R[q], \sigma, hf)$ such that $f(0) = \pi$ and $h(0) \in R^\times$ hold and at least one of the following two possibilities is satisfied:

- $h = \tilde{h}g^s$ for some polynomials $\tilde{h}$ and $g \notin R^\times = R[q]^\times$ and $s \geq 2$.
- $h = \tilde{h}g$ for some polynomials $\tilde{h}$ and g in $R[q]$ such that the polynomial g is not irreducible in $S[q]$.

Remark 5.1 *We can w.l.o.g. assume that the polynomial f is irreducible. If there are $f_1, f_2 \in R[q]$ with $f = f_1 f_2$, we get immediately $\pi = f(0) = f_1(0)f_2(0)$. Since π is prime in R we w.l.o.g. assume that there is a unit $\varepsilon \in R$ with $f_1(0) = \varepsilon\pi$. Hence $fh = f_1 f_2 h = f_1\varepsilon^{-1}\varepsilon h$. So we can w.l.o.g. assume $f = f_1\varepsilon^{-1}$ and $h = \varepsilon f_2 h$.*

In Theorem 5.25 we will show that with these assumptions the lift $\Lambda_{hf} := (S[q]/R[q], \sigma, hf)$ of Λ is *not* a maximal order. To do this we verify in the Sections 5.1 - 5.3 some lemmas of a more technical nature.

5.1 An Over Order Construction

We fix the notations for this section. Let R be a discrete valuation domain with prime π and set $K := \mathrm{frac}(R)$. Moreover assume that L/K is a finite cyclic Galois extension of degree n with group $G = \langle\sigma\rangle$. We set $S := \mathrm{alg.int.}_R(L)$ and assume that S is a discrete valuation domain and that we have an unramified extension, i.e. π is also a prime number of S. In this section let $\Lambda := (S/R, \sigma, \pi^s b)$ for some $b \in R$ and some element $s \in \mathbb{N}$ such that s divides n.

Lemma 5.2 *We set*

$$\Gamma := \bigoplus_{i=0}^{\frac{n}{s}-1} \bigoplus_{j=0}^{s-1} S\frac{1}{\pi^j}\lambda^{j\frac{n}{s}+i}$$

and get that Γ is an order, which contains Λ strictly as a sub order and so Λ is not a maximal order.

Proof.

1. Surely Γ is a finitely generated R-module and Λ is strictly contained in Γ.
2. It remains to show that Γ is a ring, here for it is enough to verify that Γ is closed under multiplication. We choose arbitrary elements $0 \leq i, j \leq \frac{n}{s}-1$ and

$0 \leq k, l \leq s-1$. We have to prove that $x := \frac{1}{\pi^k}\lambda^{k\frac{n}{s}+i}\frac{1}{\pi^l}\lambda^{l\frac{n}{s}+j}$ is contained in Γ. We note that $\sigma(\pi) = \pi$ holds and so we get

$$\frac{1}{\pi^k}\lambda^{k\frac{n}{s}+i}\frac{1}{\pi^l}\lambda^{l\frac{n}{s}+j} = \frac{1}{\pi^{k+l}}\lambda^{(k+l)\frac{n}{s}+(i+j)}.$$

Let us first assume that $k+l \leq s-1$ holds. We have to distinguish a few cases:

- Let us $i+j \leq \frac{n}{s}-1$ assume. Then we have of course $(i+j)+(k+l)\frac{n}{s} \leq n-1$ and so we get directly from the definition of Γ that $x \in \Gamma$ is satisfied.
- Now consider the case that $i+j \geq \frac{n}{s}$ holds. Here we find a $0 \leq \tilde{i} \leq \frac{n}{s}-1$ with $i+j = \frac{n}{s}+\tilde{i}$ and have to go into the following two sub cases:
  - Let us first assume that we have $k+l \leq s-2$, here we can conclude

$$x = \frac{1}{\pi^{k+l}}\lambda^{\tilde{i}+(k+l+1)\frac{n}{s}} = \pi\frac{1}{\pi^{k+l+1}}\lambda^{\tilde{i}+(k+l+1)\frac{n}{s}} \in \Gamma.$$

  - Now we consider the case that $k+l = s-1$ holds and find

$$x = \frac{1}{\pi^{k+l}}\lambda^{\tilde{i}+(s-1+1)\frac{n}{s}} \underset{k+l=s-1}{=} \frac{1}{\pi^{s-1}}\lambda^{\tilde{i}+n} = \frac{1}{\pi^{s-1}}\lambda^n\lambda^{\tilde{i}}$$
$$\underset{\lambda^n=\pi^s b}{=} b\pi^s\frac{1}{\pi^{s-1}}\lambda^{\tilde{i}} = b\pi\lambda^{\tilde{i}} \in \Gamma.$$

Now assume that we have $k+l \geq s$. Then we find some $0 \leq \tilde{k} \leq s-1$ with $k+l = \tilde{k}+s$ and get

$$x = \frac{1}{\pi^{\tilde{k}+s}}\lambda^{(i+j)+(\tilde{k}+s)\frac{n}{s}} = \frac{1}{\pi^{\tilde{k}+s}}\lambda^{(i+j)+\tilde{k}\frac{n}{s}+n} = \frac{1}{\pi^{\tilde{k}+s}}\lambda^n\lambda^{(i+j)+\tilde{k}\frac{n}{s}}$$
$$\underset{\lambda^n=b\pi^s}{=} b\pi^s\frac{1}{\tilde{k}+s}\lambda^{(i+j)+\tilde{k}\frac{n}{s}} = \frac{1}{\pi^{\tilde{k}}}\lambda^{(i+j)+\tilde{k}\frac{n}{s}} \in \Gamma.$$

We note that in this last case the conclusion that x is contained in Γ did not depend on $i+j \leq s$.

□

5.2 Maximal Ideals of some Orders

For this section let R be a discrete valuation domain with prime π and field of fractions K. Moreover let L/K be a cyclic Galois extension of degree n with group $G = \langle\sigma\rangle$. We set $S := \text{alg. int}_R(L)$. Let us assume that there is some $1 \leq \alpha \leq n$ such that α divides n and that there is some prime element $p \in S$ with $\pi = p\sigma(p)\cdots\sigma^{\alpha-1}(p)$. We need some more

Notations 5.3 *1. Let γ be the automorphism which is induced by σ on the quotient $S/\pi S$ and set $\left(S/\pi S\right)_\gamma[x]$ to be a twisted polynomial ring (see Definition 6.1). Moreover we set $A := \left(S/\pi S\right)_\gamma[x]/(x^n)$.*

2. We set $\Lambda := (S/R, \sigma, \pi^s b)$ for some $b \in R$ and an arbitrary $1 \leq s \in \mathbb{N}$.

Lemma 5.4 *We have an isomorphism* $\Lambda/\pi\Lambda \simeq A$.

Proof. We have

$$\Lambda = \bigoplus_{i=0}^{n-1} S\lambda^i \quad \text{and} \quad \pi\Lambda = \bigoplus_{i=0}^{n-1} \pi S\lambda^i.$$

So we get

$$\Lambda/\pi\Lambda = \Big(\bigoplus_{i=0}^{n-1} S\lambda^i\Big)\Big/\Big(\bigoplus_{i=0}^{n-1} \pi S\lambda^i\Big) \simeq \bigoplus_{i=0}^{n-1} S/\pi S\bar{\lambda}^i,$$

with $\bar{\lambda} := \lambda + \pi\Lambda$.

We make some observations:

- For $a \in S/\pi S$ we find $\bar{\lambda}a = \gamma(a)\bar{\lambda}$.
- $\bar{\lambda}^n \underset{\lambda^n = \pi^s b}{=} \pi^s b + \pi\Lambda = 0$.

From these observations we get can immediately deduce, that we have indeed an isomorphism $\Lambda/\pi\Lambda \simeq A$. □

Remark 5.5 *The proof of Lemma 5.4 does not depend on the fact that we have* $\pi = p\sigma(p)\ldots\sigma^{\alpha-1}(p)$ *in* S. *A close examination of the proof of Lemma 5.4 yields that it is also true for a more general case and we obtain the*

Corollary 5.6 *Let* A *be an integral domain with field of fractions* F, *moreover let* F'/F *be a cyclic Galois extension with group* $H = \langle\tau\rangle$. *Now we set* $B :=$ *alg. int.*$_A(F')$ *and* $\Delta := (B/A, \tau, a)$ *for some* $a \in A$. *Let* $\mathfrak{a} \subset R$ *be some ideal with* $a \in \mathfrak{a}$. *By Lemma 4.44 the isomorphism* τ *induces an isomorphism* $\bar{\tau}$ *on the quotient* $B/\mathfrak{a}B$. *In this situation we have an isomorphism* $\Delta/\mathfrak{a}\Delta \simeq \big(B/\mathfrak{a}B\big)_{\bar{\tau}}[x]/(x^n)$.

Observation 5.7 *The algebra* A *is Artin.*

Proof. By the Chinese Remainder Theorem we have $S/\pi S \simeq \prod_{i=0}^{\alpha-1} S/\sigma^i(p)S$ which is a direct product of fields. Moreover A is finitely generated over $S/\pi S$. Combining these results we can immediately conclude that A is an Artin algebra. □

Notation 5.8 *Let* $y := x + (x^n) \in A$.

Lemma 5.9 *We set* $J := yA \subset A$. *Then* J *is the radical of* A *and we have moreover* $A/J \simeq \prod_{i=0}^{\alpha-1} S/\sigma^i(p)S$.

Proof.

- We have $y^n = 0$ and for every $a \in S/\pi S$ the equation $xa = \gamma(a)x$ holds, hence $J = (y)$ is a nilpotent two-sided ideal of the Artin algebra A (see Observation 5.7), so $J \subset \mathrm{rad}(A)$.
- Moreover we have

$$A/J = \big(S/\pi S\big)_\gamma[x]/(x^n)\Big/(x)/(x^n) \simeq \big(S/\pi S\big)_\gamma[x]/(x)$$

$$\simeq S/\pi S \underset{\text{Chinese Remainder Theorem}}{\simeq} \prod_{i=0}^{\alpha-1} \underbrace{S/\sigma^i(p)S}_{\text{a simple } A\text{module}} \quad ;$$

we note, that an easy calculation shows that the isomorphism which comes from the Chinese Remainder Theorem is a homomorphism of A-modules. So A/J is a semi simple A-module and we can conclude $\mathrm{rad}(A) \subset J$.

□

Observation 5.10 *A contains exactly α maximal two sided ideals which are the inverse images of the ideals $\mathfrak{m}_i := 0 \times \cdots \times S/\sigma^i(p) \times \cdots \times 0 \subset A/J$.*

Corollary 5.11 *The maximal two-sided ideals of A are given by $M_i := \langle \sigma^i(p), y \rangle$.*

Proof.

1. That all the M_i's are indeed two-sided ideals is verified by a straightforward calculation.
2. Now we show that M_i is maximal. We have
$$A/M_i = \left(S/\pi S\right)_\gamma[x]/(x^n)\Big/\langle \sigma^i(p), x\rangle/(x^n) \simeq \left(S/\pi S\right)_\gamma[x]/\langle \sigma^i(p), x\rangle$$
$$\simeq S/\pi S\Big/\sigma^i(p)/\pi S \simeq S/\sigma^i(p)S,$$
a field and so A/M_i is a in particular a simple ring and hence M_i is maximal.
3. Since the ideals $\sigma^i(p)S$ are pairwise different ideals of S and the elements $1, y, \ldots, y^{n-1} \in A$ are linear independent over $S/\pi S$ we get immediately that the M_i's are pairwise different.
4. By Observation 5.10 we know that A contains exactly α different maximal two-sided ideals, hence we are done.

□

Lemma 5.12 *We have*
$$rad(\Lambda) = \langle \pi, \lambda \rangle = \pi S \oplus \bigoplus_{i=1}^{n-1} S\lambda^i.$$

Proof.

1. We first show that the equality $\langle \pi, \lambda \rangle = \pi S \oplus \bigoplus_{i=1}^{n-1} S\lambda^i$ holds.
   - Let $x = \mu_1\pi + \mu_2\lambda \in \langle \pi, \lambda \rangle$ with $\mu_1 = \sum_i s_i\lambda^i$ and $\mu_2 = \sum_i \tilde{s}_i\lambda^i$. Then we have
$$x = \sum_i \pi s_i\lambda^i + \sum_i \tilde{s}_i\lambda^{i+1} \underset{\lambda^n = \pi^s b}{=} \pi s_0 + \pi^s b\tilde{s}_0 + \sum_{i=1}^{n-1}(\pi s_i + \tilde{s}_{i-1})\lambda^i$$
$$= \pi(s_0 + \pi^{s-1}b\tilde{s}_0) + \sum_{i=1}^{n-1}(\pi s_i + \tilde{s}_{i-1})\lambda^i \in \pi S \oplus \bigoplus_{i=1}^{n-1} S\lambda^i.$$
   - The other inclusion is obvious.
2. Since R is a local ring with radical πR and Λ is finitely generated over R we have of course that $\pi\Lambda \subset \mathrm{rad}(\Lambda)$ holds. By Lemma 5.4 we have an isomorphism $\Lambda/\pi\Lambda \simeq A$ which maps $\bar{\lambda}$ to the generator of the radical of A (see Lemma 5.9) and so we obtain $\mathrm{rad}(\Lambda) = \langle \pi, \lambda \rangle$.

□

Corollary 5.13 *The maximal two-sided ideals of* Λ *are exactly the ideals* $\mathcal{M}_i := \langle \sigma^i(p), \lambda \rangle = \sigma^i(p)S \oplus \bigoplus_{i=1}^{n-1} S\lambda^i$.

Proof.

1. The equality $\langle \sigma^i(p), \lambda \rangle = \sigma^i(p)S \oplus \bigoplus_{i=1}^{n-1} S\lambda^i$ is shown with a calculation analogous to the one we did in the proof of Lemma 5.12 (we regard that $\sigma^i(p)$ divides π for every i).

2. We have

$$\Lambda/\mathrm{rad}(\Lambda) \underset{\text{Lemma 5.12}}{=} \Lambda/\langle \pi, \lambda \rangle \underset{\text{by the proof of Lemma 5.12}}{\simeq} A/J,$$

where we use the notations of Lemma 5.9. By observing that the radical is contained in every maximal two-sided ideal we obtain that the maximal two-sided ideals of Λ are exactly the inverse images of the maximal two-sided ideals of A. From Corollary 5.11 we know that the maximal two-sided ideals of A are the ideals $\langle \sigma^i(p), y \rangle$ and so we are done.

□

Corollary 5.14 *For* $\alpha \geq 2$ *the order* Λ *is not maximal.*

Proof. If Λ would be a maximal order, then by the virtue of Theorem 4.4 $\mathrm{rad}(\Lambda)$ would be the unique maximal two-sided ideal of Λ; but for $\alpha \geq 2$ we know from Corollary 5.13 that there are more than one maximal two-sided ideals in the order Λ.
□

5.3 A non projective Radical

For this section let R be a discrete valuation domain with prime π and field of fractions $K := \mathrm{frac}(R)$. We consider a cyclic Galois extension L/K degree n with group $G = \langle \sigma \rangle$ and set $S := \mathrm{alg.int.}_R(L)$. We assume that S is a discrete valuation domain and that the extension L/K is unramified so that π is a prime number of S.

The isomorphism in $S/\pi S$ which is induced from σ will be denoted by γ. We set as in Section 5.1 $A := (S/\pi S)_\gamma[x]/(x^n)$. Moreover let $\Lambda := (S/R, \sigma, \pi^s\varepsilon)$ for some $n \in \mathbb{N}$ with $2 \leq s \leq n$ and some unit $\varepsilon \in R^\times$.

Lemma 5.15 *There is an isomorphism* $\Lambda/\pi\Lambda \simeq A$.

Proof. This immediately deduced from Corollary 5.6. □

Corollary 5.16 *We have* $rad(\Lambda) = \langle \pi, \lambda \rangle = \pi S \oplus \bigoplus_{i=1}^{n-1} S\lambda^i$.

Proof. This follows analogous to the proof of Lemma 5.12 by using Lemmas 5.9 and 5.15. □

Corollary 5.17 *Λ is a local ring.*

Proof. We have

$$\Lambda/\mathrm{rad}(\Lambda) \underset{\text{Corollary 5.16}}{=} \Lambda/\langle\pi,\lambda\rangle \underset{\text{by the proof of Lemma 5.4}}{\simeq} \big(S/\pi S\big)_\gamma[x]/(x^n)\Big/(x)/(x^n)$$
$$\simeq \big(S/\pi S\big)_\gamma[x]/(x) \simeq S/\pi S,$$

which is a field, since π is a prime element of S and so Λ is indeed a local ring. □

We make the short

Observation 5.18 *Let B/A a finite unramified extension of discrete valuation domains with prime p. Let $\hat{A}$ be the p-adic completion of A and $\hat{B}$ the p-adic completion of B. We have an isomorphism $\hat{A}\otimes_A B \simeq \hat{B}$. Both $\hat{A}$ and $\hat{B}$ are discrete valuation domains and $\hat{B}/\hat{A}$ is still a finite and unramified extension.*

Proof.

- For every $i\in\mathbb{N}$ we have $(p^iA)\cdot B = p^iB$, hence the p-adic topology on the A-module B is the same as the p-adic topology of the ring B. So it is clear that we have an isomorphism $\hat{A}\otimes_A B\simeq\hat{B}$.
- Since B/A is a finite extension of discrete valuation domains, we have that B is - as an A-lattice - free over A of finite rank, so $\hat{B}/\hat{A}$ is also a finite extension.
- The completion of any discrete valuation domain T with prime $\tilde{\pi}$ is again a discrete valuation domain and $\tilde{\pi}$ is a prime of $\hat{T}$. Hence $\hat{B}/\hat{A}$ is an unramified extension of discrete valuation domains.

□

Remark 5.19 *We have not assumed that R is complete with respect to the π-adic topology, so we can a priori not assume that a Krull-Schmidt-Theorem holds for Λ. In this section we want to show that Λ is for $s\geq 2$ not hereditary. To ensure that neither the global dimension of the order Λ nor the structure of Λ as a cyclic order is affected by passing over to the π-adic completion $\hat{R}$ of R me make the following*

Observations 5.20 *1. We note that for an arbitrary R-order Γ there is an equality of global dimensions $gl.dim(\Gamma) = gl.dim(\hat{R}\otimes_R\Gamma)$, where $\hat{R}$ denotes the π-adic completion of R (cf. [Rei75, Theorem 3.30]).*

2. We have $\Lambda = \bigoplus_{i=0}^{n-1} S\lambda^i$, hence

$$\hat{R}\otimes_R\Lambda = \hat{R}\otimes_R\Big(\bigoplus_{i=0}^{n-1} S\lambda^i\Big) \simeq \bigoplus_{i=0}^{n-1}(\hat{R}\otimes_R S)\lambda^i$$
$$\underset{Observation\ 5.18}{\simeq} \hat{S}\lambda^i \underset{obvious}{\simeq} (\hat{S}/\hat{R},\hat{\sigma},\pi^s\varepsilon).$$

So we can w.l.o.g. assume that R is complete with respect to the π-adic topology. And so we can now assume that we have a Krull-Schmidt-Theorem for Λ.

Lemma 5.21 *An ideal $I\subset\Lambda$ is projective if and only if there is a non zero divisor $x\in\Lambda$ with $I=\Lambda x$, i.e. I is a free Λ-module of rank 1.*

Proof. Λ is a local ring, hence ${}_\Lambda\Lambda$ is projective indecomposable. By Observations 5.20 we can assume that a Krull-Schmidt-Theorem for Λ holds, so we get that ${}_\Lambda\Lambda$ is up to isomorphism the only projective indecomposable Λ-module. Since Λ is an R-order we argue with the rank over R to see that a projective ideal has to be Λx for some (non zero divisor) $x\in\Lambda$. □

Lemma 5.22 *For $s \geq 2$ the radical of Λ is not projective as Λ-module.*

Proof. By Lemma 5.21 the radical is projective if and only if we find some element $x \in \mathrm{rad}(\Lambda)$ with $\mathrm{rad}(\Lambda) = \Lambda x$. So let us assume that there is such an element $x \in \Lambda$. We know from Corollary 5.16 that there is an equality $\mathrm{rad}(\Lambda) = \pi S \oplus \bigoplus_{i=1}^{n-1} S\lambda^i$. So an arbitrary element x of $\mathrm{rad}(\Lambda)$ is of the form $x = \pi s_0 + s_1\lambda + \cdots + s_{n-1}\lambda^{n-1}$ with $s_i \in S$ for all i. Let us first assume that $s_0 = 0$ holds, so we have $x \in \Lambda\lambda$, hence $\mathrm{rad}(\Lambda) \subset \Lambda\lambda$. Let $\mu = \sum_{i=0}^{n-1} t_i\lambda^i$ be an arbitrary element of Λ, we find $x\mu = \left(\sum_{i=1}^{n-1} s_i\lambda^i\right)\left(\sum_{j=0}^{n-1} t_j\lambda^j\right) = s_1t_{n-1}\lambda^n + y$ with $y \in \Lambda\lambda \setminus S$. Hence $x = s_1t_{n-1}\varepsilon\pi^s + y$. Since we assume that $s \geq 2$ is satisfied, we have that $s_1t_{n-1}\varepsilon\pi^s + y = \pi$ can't be satisfied, so $\pi \notin \Lambda x = \mathrm{rad}(\Lambda)$, a contradiction. So we can from now on assume that $s_0 \neq 0$ holds. Now we show that s_0 is a unit of S. Assume π divides s_0, then w.l.o.g. (we change our notation) $x = s_0\pi^2 + s_1\lambda + \cdots + s_{n-1}\lambda^{n-1}$. But we must find some $\mu \in \Lambda$ with $\mu x = \pi$. On the other side we find - using again that $s \geq 2$ holds - $\mu x = \pi^2\tilde{s_0} + y$ for some $\tilde{s_0} \in S$ and some $y \in \Lambda\lambda \setminus S$, which is again a contradiction, so s_0 has to be a unit of S. We pass over to the matrix representation of Λ (according to Remarks 2.21) to obtain the possibility to take determinants of elements of Λ. Since we have assumed that $s \leq n$ holds we get that the determinant of x is of the form $\det(x) = \pi^s\tilde{s}$ for some $\tilde{s} \in S$. Since $\lambda \in \mathrm{rad}(\Lambda) = \Lambda x$ holds we find some $\mu \in \Lambda$ with $\lambda = \mu x$, we conclude

$$\pm\pi^s\varepsilon \underset{\substack{\text{from the matrix}\\ \text{representation}}}{=} \det(\lambda) = \det(\mu x) = \det(\mu)\det(x) = \det(\mu)\pi^s\tilde{s},$$

since Λ is an R-order we know that determinants of elements of Λ have to be contained R, so the above equation is only possible if $\det(\mu)$ is a unit of R. So we can apply Lemma 4.7 to conclude that μ is a unit of Λ. We find some $\delta \in \Lambda$ with $x = \pi s_0 + \delta\lambda$. Hence we get

$$\lambda = \mu x = \mu(\pi s_0 + \delta\lambda) = \pi\mu s_0 + \mu\delta\lambda,$$

using that s_0 is a unit of S (and so in particular a unit of Λ) and μ is a unit of Λ, we can conclude $\pi = {s_0}^{-1}\mu^{-1}(1 - \mu\delta)\lambda \in \Lambda\lambda$, we have already seen that this is a contradiction and so we are done. □

Corollary 5.23 *For $s \geq 2$ the order Λ is not hereditary.*

Proof. An R-order Γ is hereditary if and only if every Λ-lattice is projective (cf. [Rei75, Corollary 10.7]). By Lemma 5.22 we have that (the Λ-lattice) $\mathrm{rad}(\Lambda)$ is not projective. □

Corollary 5.24 *For $s \geq 2$ the order Λ is not maximal.*

Proof. This follows immediately from Theorem 4.4. □

5.4 Applications to Lifts

Theorem 5.25 *Let $L(q)(S[q]/R[q], \sigma, hf)$ be a lift of $(L/K, \sigma, \pi)$ with $f(0) = \pi$ and $h(0) \in R^\times$, such that at at least one of the following two possibilities hold:*

- *$h = \tilde{h}g^s$ for some polynomials $\tilde{h}$ and $g \notin R^\times = R[q]^\times$ and $s \geq 2$.*
- *$h = \tilde{h}g$ for some polynomials $\tilde{h}$ and g in $R[q]$ such that the polynomial g is not irreducible in $S[q]$.*

Then $\Lambda_{fh} := (S[q]/R[q], \sigma, hf)$ is not *a maximal order.*

Proof. According to Theorem 4.3 it will be enough to find a $\mathfrak{p} \in \mathrm{ht}^1(R[q])$ such that $\Lambda_{fh,\mathfrak{p}} := (\Lambda_{fh})_{\mathfrak{p}}$ is not a maximal order over $R_{\mathfrak{p}}$.

1. Let us first assume that the polynomial g is not irreducible in $S[q]$. After localization at $\mathfrak{p} = gR[q]$ we are in the situation of Section 5.2 and Corollary 5.14 yields that $\Lambda_{fh,\mathfrak{p}}$ is not maximal.
2. Now let us assume that h is divided by g^s with $s \geq 2$. We distinguish two cases:
   a) $s \geq n$. Then we can write $s = n + y$ for $y = s - n \in \mathbb{N}$. After localizing at $\mathfrak{p} = gR[q]$ we consider a cyclic order of the form $(B/A, \tau, p^n b)$ for some prime p of the discrete valuation domain A. Then we can apply the results of Section 5.1 to construct an explicit over order of $\Lambda_{fh,\mathfrak{p}}$ and so $\Lambda_{fh,\mathfrak{p}}$ is not a maximal order.
   b) $s \leq n - 1$. Then after localizing at $\mathfrak{p} = gR[q]$ we are in the situation of Section 5.3 and can apply Corollary 5.24 to conclude that $\Lambda_{fh,\mathfrak{p}}$ is not a maximal order.

□

6 Some Truncated Twisted Polynomial Rings

Let $D_f = W(q)\Lambda_f$ be a lift of a standard representation of a Hasse skewfield D such that $\Lambda_f = (S[q]/R[q], \sigma, f)$ for $f \in R[q]$ with $f(0) = \pi$. We can consider specializations of Λ_f i.e. quotients $\Lambda_a := \Lambda_f/(q-a)\Lambda_f$ for $a \in R$. There is an isomorphism $\Lambda_a \simeq (S/R, \sigma, f(a))$. Let us assume that a is a zero of f. In this situation there is an isomorphism $K\Lambda_a \simeq W[x,\sigma]/(x^n)$, where $W[x,\sigma]$ denotes the twisted polynomial ring (see Section 3.2.7). So it is natural to study these rings and to see how far they are away from being semisimple.

6.1 Generalities

Let us fix the notation. Let L/F be an arbitrary finite Galois extension of degree d, moreover let $\mathrm{id} \neq \tau$ be a Galois automorphism of L. Let $2 \leq k \in \mathbb{N}$. By L_τ we denote the fixed field of τ.

Definition 6.1 *Let x be an indeterminate over L, the twisted polynomial ring $L[x,\tau]$ is given in the following way:*

- *As vector space over L, $L[x,\tau]$ is equal to the polynomial ring $L[x]$.*
- *The multiplication on $L[x,\tau]$ is induced from the rule*

$$xl = \tau(l)x \quad \forall l \in L.$$

*This rule is the reason for the terminology "*twisted *polynomial ring"*

Notation 6.2 *1. For an arbitrary polynomial $\sum_i \alpha_i x^i \in L[x,\tau]$ we set $\tau(f) := \sum_i \tau(\alpha_i)x^i$.*

2. We set $A := L[x,\tau]/\langle x^k\rangle$ and $N := x + \langle x^k\rangle \in A$.

Remark 6.3 *For an arbitrary polynomial $f \in L[x,\tau]$ we find $xf = \tau(f)x$.*

Observations 6.4 *1. The L-dimension of A is equal to k and the F-dimension of A is equal to dk.*

2. The radical of A is AN.

Proof.

- *We have an isomorphism $A/AN \simeq L$ and so A/AN is a simple A-module, hence we get $rad(A) \subset AN$.*
- *From Remark 6.3 we get immediately that AN is a nilpotent ideal, hence it is contained in the radical.*

□

Corollary 6.5 *1.* $A/rad(A) \simeq L$.

2. A *is a local ring.*

3. The module $S := A/AN$ *is up to isomorphism the only simple* A*-module.*

4. The algebra A *has only the two trivial idempotents* 1 *and* 0.

5. A *is up to isomorphism the only projective indecomposable* A*-module.*

Lemma 6.6 *The center* $C(A)$ *of* A *is* L_τ.

Proof. That $L_\tau \subset \mathrm{C}(A)$ holds is trivial deduced from Remark 6.3. Let $f = \sum_i \alpha_{i=0}^{k-1} N^i$ be an element of $\mathrm{C}(A)$. Then $\tau(f)N = fN = Nf$, hence we get that α_0 is an element of $L_\tau \subset \mathrm{C}(A)$. So the element $f - \alpha_0$ is also central, we can therefore w.l.o.g. assume that $\alpha_0 = 0$ holds. Choose an arbitrary element $l \in L$, we get

$$\sum_{i=1}^{k-1} \alpha_i N^i l = \sum_{i=1}^{k-1} \tau(l)\alpha_i N^i = fl = lf = l\sum_{i=1}^{k-1} \alpha_i N^i = \sum_{i=1}^{k-1} l\alpha_i N^i.$$

We conclude $(\tau(l) - l)\alpha_i = 0$ for all i. By assumption we have $\mathrm{id} \neq \tau$, so the Main Theorem of Galois Theory yields that there is some $l \in L$ with $\tau(l) \neq l$, hence $\alpha_i = 0$ for all i. □

Notation 6.7 *For* $0 \leq i \leq k-1$ *we define* $\rho_i \in \mathrm{End}_A(A)$ *by*

$$\rho_i : A \ni a \longmapsto aN^i \in A.$$

Lemma 6.8 *The kernel of* ρ_i *is* AN^{k-i}.

Proof. In the case $0 = i$ we have that ρ_0 is the identity map on A, hence $\ker \rho_0 = 0 = N^{k-0}$. So we can w.l.o.g. assume that $1 \leq i$ holds.

- Using $N^k = 0$ and Remark 6.3 we get immediately $AN^{k-i} \subset \mathrm{Ker}(\rho_i)$.
- Let $f = \sum_{i=0}^{k-1} \alpha_i N^i$ be an arbitrary element of $\mathrm{Ker}(\rho_i)$, then

  $$0 = fN^i \underset{N^k=0}{=} \alpha_0 N^i + \alpha_i N^{i+1} + \cdots + \alpha_{k-i-1} N^{k-1},$$

  hence $\alpha_0 = \alpha_1 = \cdots = \alpha_{k-i-1} = 0$, this implies $f \in AN^{k-i}$ and we are done.

□

Lemma 6.9 *There is an isomorphism of* A*-modules* $S = A/AN \simeq AN^{k-1}$.

Proof. We set

$$\Phi : A/AN \ni a + AN \longmapsto aN^{k-1} \in AN^{k-1}.$$

- Assume $aN = 0$, so $a = \tilde{a}N^{k-1}$ for some $\tilde{a} \in A$ by Lemma 6.8, hence $aN^{k-1} = \tilde{a}N^{k-1}N^{k-1} = 0$ (using $k \geq 2$).
- Φ is a surjective homomorphism of A-modules.
- Assume $a + AN \in \mathrm{Ker}(\Phi)$, then $aN^{k-1} = 0$. Again by Lemma 6.8 we find some $\tilde{a} \in A$ with $a = \tilde{a}N \in AN$. So $\mathrm{Ker}(\Phi) = 0$ and Φ is injective.

□

Remark 6.10 *We have*

$$\mathrm{Hom}_A(A,S) = \mathrm{Hom}_A(A, AN^{k-1}) = \{\varphi_l : A \ni 1 \longmapsto lN^{k-1} \mid l \in L\}.$$

Proof. Let $f = \sum_{i=0}^{k-1} \alpha_i N^i$ be an arbitrary element of A. Since $N^k = 0$ holds we find $fN = \alpha_0 N^{k-1}$. So we get $S = AN^{k-1} = LN^{k-1}$. □

Lemma 6.11 *We have*

$$\mathrm{End}_A(S) = \{\mu_l : AN^{k-1} \ni aN^{k-1} \longmapsto alN^{k-1} \in AN^{k-1} \mid l \in L\} \simeq L,$$

where S is identified with AN^{k-1}.

Proof. Just use

$$\begin{aligned}\mathrm{End}_A(S) &\underset{A/\mathrm{rad}(A)\simeq S}{\simeq} \mathrm{End}_A(A/\mathrm{rad}(A))\\ \simeq \mathrm{End}_{A/\mathrm{rad}(A)}(A/\mathrm{rad}(A)) &\underset{A/\mathrm{rad}(A)\simeq L}{\simeq} \mathrm{End}_L(L) \simeq L,\end{aligned}$$

the rest is straightforward. □

6.2 Projective Resolutions and Ext-Groups

Lemma 6.12 *A projective resolution of the simple A-module S is given by the following exact sequence:*

$$\mathcal{P}_0 \cdots\cdots \xrightarrow{\rho_1} A \xrightarrow{\rho_{k-1}} A \xrightarrow{\rho_1} A \xrightarrow{\rho_{k-1}} S \longrightarrow 0,$$

where we identify S with AN^{k-1} (cf. Lemma 6.9).

Proof. We can apply inductively Lemma 6.8 to construct a projective resolution of S, this construction yields the sequence $\mathcal{P}_0$. □

Remark 6.13 *For $k = 2$ we have $\rho_1 = \rho_{k-1}$. In this case $\mathcal{P}_0$ has period 1.*

Lemma 6.14 *Let B be an arbitrary (not necessarily commutative) local ring and P a finitely generated projective B-module, then P is free over A.*

Proof. Cf. [CR81, Paragraph 6]. □

Corollary 6.15 *We have $pdim_A(S) = \infty$.*

Proof. Using the Lemmas 6.8 and 6.12 we get that none of the syzygies of S is a free module over A. Since A is a local ring by Corollary 6.5, we can apply Lemma 6.14 to conclude, that none of the syzygies is projective. □

Lemma 6.16 *Let B be an Artin ring, with simple modules $S_1, \ldots, S_h$. Then the following numbers coincide:*

1. *gl.dim(A).*
2. $\max\{pdim_A(S_i) \mid 1 \leq i \leq h\}$.
3. *pdim$_A$(rad(A))* $+ 1$.

Proof. Cf. [ARS97, Proposition 5.1]. □

Corollary 6.17 *We have gl.dim$(A) = \infty$.*

Proof. This follows immediately from Corollary 6.15 and Lemma 6.16. □

Remark 6.18 *So A is in some sense as far as possible away from being semi-simple.*

Lemma 6.19 *For all $i \in \mathbb{N}$ we have* $\mathrm{Ext}_i^A(S,S) = \mathrm{Hom}_A(A,S)$.

Proof. To calculate the Ext-groups we have to consider the truncated projective resolution of S i.e., the following complex

$$\mathcal{P}: \cdots\cdots A \xrightarrow{\rho_1} A \xrightarrow{\rho_{k-1}} A \xrightarrow{\rho_1} A \longrightarrow 0.$$

The considered Ext-groups are the homology groups of the new complex $\mathrm{Hom}_A(\mathcal{P}, S)$.

Claim. Im$({\rho_1}^*)$=0, Im$({\rho_{k-1}}^*)$=0.

Proof of the Claim.

- Choose some $\gamma \in \mathrm{Im}({\rho_1}^*) \subset \mathrm{Hom}_A(A,S)$. Then there is some element $\varphi_l \in \mathrm{Hom}_A(A,S)$ with $\gamma = \varphi_l {\rho_1}^* = \rho_1 \varphi_l$, so we get
$$1\gamma = 1\rho_1\varphi_l = N\varphi_l = NlN^{k-1} = \tau(l)N^k = 0$$
and we are done.
- Use $\rho_{k-1} = {\rho_1}^{k-1}$ and the first part, to show that $\mathrm{Im}({\rho_{k-1}}^*) = 0$ holds.

□

Claim. Ker$({\rho_1}^*)$=Hom$_A(A,S)$, Ker$({\rho_{k-1}}^*)$=Hom$_A(A,S)$.

Proof of the Claim. Choose an arbitrary element $l \in L$. We have

- $1(\varphi_l {\rho_1}^*) = 1\rho_1\varphi_l = N\varphi_l = NlN^{k-1} = \tau(l)N^k = 0$. And so we get $\mathrm{Hom}_A(A,S) \subset \mathrm{Ker}({\rho_1}^*)$.
- $1(\varphi_l {\rho_{k-1}}^*) = 1\rho_{k-1}\varphi_l = N^{k-1}\varphi_l = N^{k-1}lN^{k-1} = \tau^{k-1}(l)N^{2(k-1)} = 0$, hence $\mathrm{Hom}_A(A,S) \subset \mathrm{Ker}({\rho_{k-1}}^*)$.

□

Putting these claims together we obtain $\mathrm{Ext}_A^i(S,S) = \mathrm{Hom}_A(A,S)$ for all $i \in \mathbb{N}$.

□

7 Cohomology Rings

Let A be an arbitrary ring. In Section 7.1 we introduce the Yoneda Ext-groups $\mathrm{ext}_A^k(M,N)$ which contain some equivalence classes of exact sequences of A-modules. The Yoneda Ext-groups have the structure of Abelian groups, the composition is given by the Baer sum. The Yoneda splice as a composition of exact sequences will be introduced. We will see that the Yoneda Ext-groups can be identified with the Ext-groups which arise as derive functors of Hom-functors. For a fixed A-module M the Yoneda splice induces a multiplication on the graded Abelian group $\bigoplus_{i\in\mathbb{N}}\mathrm{ext}_A^i(M,M)$, it becomes a ring - the so called cohomology ring of M (see Section 7.2). Finally we calculate in Section 7.3 the cohomology ring of the uniquely simple module S for the truncated twisted polynomial ring $L[x,\tau]/\langle x^k\rangle$ which arise as some specializations of lifts of Hasse skewfields. We have studied these truncated twisted polynomial rings in Chapter 6.

7.1 Yoneda Ext-Groups and Resolutions

In this section let A be some ring and denote by $M, \tilde{M}, N$ and $\tilde{N}$ some A-modules. We give here a a very short introduction to the theory of Yoneda Ext-groups as we need it for the calculation of cohomology rings in Sections 7.2 and 7.3. The Yoneda Ext-groups are a generalization of $\mathrm{ext}_A^1(M,N)$. We assume that the reader is familiar with the theory of $\mathrm{ext}_A^1(M,N)$ (see [Rot79, Chapter 7]), we will use it without mention it. Here we will follow [Lan91, Chapter III].

Definition 7.1 *Let $k \geq 1$. A k-fold exact sequence starting in N and ending in M is an exact sequence of the form*

$$0 \longrightarrow N \longrightarrow B_{k-1} \longrightarrow B_{k-2} \longrightarrow \cdots\cdots\cdots \longrightarrow B_0 \longrightarrow M \longrightarrow 0.$$

Lemma and Definition 7.2 *Let $r, s \geq 1$ and*

$$S := 0 \longrightarrow N \longrightarrow B_{r-1} \longrightarrow B_{r-2} \longrightarrow \cdots\cdots\cdots \longrightarrow B_0 \xrightarrow{\alpha} M \longrightarrow 0$$

be an r-fold exact sequence ending in M and

$$T := 0 \longrightarrow M \xrightarrow{\beta} C_{s-1} \longrightarrow C_{s-2} \longrightarrow \cdots\cdots\cdots \longrightarrow C_0 \longrightarrow X \longrightarrow 0$$

be an s-fold exact sequence starting with M. The following sequence is exact

$$0 \longrightarrow N \longrightarrow B_{r-1} \cdots\cdots B_0 \xrightarrow{\alpha\beta} C_{s-1} \cdots\cdots C_0 \longrightarrow X \longrightarrow 0,$$

it is denoted by $S \circ T$ and is called the Yoneda splice of S and T.

Observation 7.3 *Every k-fold exact sequence S can be represented as a k-fold Yoneda composite of short exact sequences $S = E_k \circ \cdots \circ E_1$.*

Definition 7.4 *Let $S = E_k \circ \cdots \circ E_1$ be a k-fold exact sequence. Let us assume that S starts in N and ends in M. For $\varphi \in \mathrm{Hom}_A(N,\tilde{N})$ and $\psi \in \mathrm{Hom}_A(\tilde{M},M)$ we define $\varphi S := (\varphi E_k) \circ \cdots \circ E_1$ and $S\psi := E_k \circ \cdots \circ (E_1\psi)$.*

Lemma and Definition 7.5 *Let $S = E_k \circ \cdots \circ E_1$ be a k-fold exact sequence, it is said to be congruent to $\tilde{S}$ if $\tilde{S}$ can be obtained from S by applying finitely many of the following operations:*

1. *Some E_i is replaced by a congruent short exact sequence $\tilde{E}_i$.*
2. *Replace $E_i \circ \beta E_{i-1}$ by $E_i\beta \circ E_{i-1}$.*
3. *Replace $E_i\beta \circ E_{i-1}$ by $E_i \circ \beta E_{i-1}$.*

We write $S \equiv \tilde{S}$ if S and $\tilde{S}$ are congruent. "$\equiv$" is an equivalence relation on the set of k-fold exact sequences starting N and ending in M. Let $[S]$ be the congruence class of S and $\operatorname{ext}_A^k(M,N)$ the set of all congruence classes. Moreover $\operatorname{ext}_A^0(M,N) := \operatorname{Hom}_A(M,N)$.

Lemma and Definition 7.6 *Let $1 \leq r,s$, $[S],[\tilde{S}] \in \operatorname{ext}_A^r(M,N)$ and $[T],[\tilde{T}] \in \operatorname{ext}_A^s(X,M)$ with $[S] = [\tilde{S}]$ and $[T] = [\tilde{T}]$. Then $[S \circ T] = [\tilde{S} \circ \tilde{T}]$. We set $[S][T] := [S \circ T]$. Let $[\alpha] \in \operatorname{ext}_A^0(X,M)$ and $[\beta] \in \operatorname{ext}_0^A(N,Y)$; we set moreover $[S][\alpha] = [S\alpha]$ and $[\beta][S] = [\beta S]$. For $[\alpha] \in \operatorname{ext}_A^0(M,N)$ and $[\beta] \in \operatorname{ext}_A^0(X,M)$ we set $[\alpha][\beta] := [\alpha\beta]$.*

Definition 7.7 *Let*

$$S := 0 \longrightarrow N \longrightarrow B_{k-1} \longrightarrow B_{k-2} \longrightarrow \cdots\cdots\cdots \longrightarrow B_0 \longrightarrow M \longrightarrow 0$$

and

$$\tilde{S} := 0 \longrightarrow \tilde{N} \longrightarrow \widetilde{B_{k-1}} \longrightarrow \widetilde{B_{k-2}} \longrightarrow \cdots\cdots\cdots \longrightarrow \widetilde{B_0} \longrightarrow \tilde{M} \longrightarrow 0.$$

A homomorphism $\Gamma : S \longrightarrow \tilde{S}$ is a $(k+2)$-tuple $\Gamma = (\alpha, \beta_{k-1}, \ldots, \beta_0, \gamma)$ with $\alpha \in \operatorname{Hom}_A(N,\tilde{N}), \beta_i \in \operatorname{Hom}_A(B_i,\tilde{B}_i)$ and $\gamma \in \operatorname{Hom}_A(M,\tilde{M})$ such that the diagram

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & N & \longrightarrow & B_{k-1} & \longrightarrow & B_{k-2} & \longrightarrow & \cdots\cdots\cdots & \longrightarrow & B_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \alpha\downarrow & & \beta_{k-1}\downarrow & & \beta_{k-2}\downarrow & & & & \beta_0\downarrow & & \gamma\downarrow & & \\
0 & \longrightarrow & \tilde{N} & \longrightarrow & \tilde{B}_{k-1} & \longrightarrow & \tilde{B}_{k-2} & \longrightarrow & \cdots\cdots\cdots & \longrightarrow & \tilde{B}_0 & \longrightarrow & \tilde{M} & \longrightarrow & 0
\end{array}$$

is commutative. We say Γ starts with α and ends with γ.

Observation 7.8 *Let S be a k-fold exact sequence, which starts in N and ends in M, moreover choose $\alpha \in \operatorname{Hom}_A(N,\tilde{N})$ and $\beta \in \operatorname{Hom}_A(\tilde{M},M)$. Then α induces a homomorphism $\Gamma_\alpha : S \longrightarrow \alpha S$ and β induces a homomorphism $\Gamma_\beta : S\beta \longrightarrow S$.*

Proof. Cf. [Lan91, Chapter III, Section 5]. □

Lemma 7.9 *Each homomorphism $\Gamma : S \longrightarrow \tilde{S}$ starting with α and ending with γ induces a congruence $\alpha S \equiv \tilde{S}\gamma$.*

Proof. Cf. [Lan91, Chapter III, Proposition 5.1]. □

Definition 7.10 *Choose two k-fold exact sequences S and $\tilde{S}$ starting in N and ending in M. Let $S \oplus \tilde{S}$ be the direct sum of the sequences S and $\tilde{S}$, $\bigtriangledown$ the codiagonal of N and Δ the diagonal of M. We set $S + \tilde{S} := \bigtriangledown(S \oplus \tilde{S})\Delta$ and call it the Baer sum of S and $\tilde{S}$.*

Theorem 7.11 *1. For every $k \in \mathbb{N}$ the Baer sum induces a well defined composition $[S]+[T] := [S+T]$ which makes $\mathrm{ext}^k_A(M,N)$ an Abelian group.*

2. For $[S_1],[S_2] \in \mathrm{ext}^k_A(M,N)$, $[T] \in \mathrm{ext}^r_A(X,M)$ and $[\tilde{T}] \in \mathrm{ext}^s_A(N,Y)$ we have

- $([S_1]+[S_2])[T] = [S_1][T]+[S_2][T]$,
- $[\tilde{T}]([S_1]+[S_2]) = [\tilde{T}][S_1]+[\tilde{T}][S_2]$;

here we use Definition 7.6.

3. For $[S_1] \in \mathrm{ext}^{k_1}_A(M_1,M_2), [S_2] \in \mathrm{ext}^{k_2}_A(M_3,M_1)$ and $[S_3] \in \mathrm{ext}^{k_3}_A(M_4,M_3)$ we have the associative law $([S_1][S_2])[S_3] = [S_1]([S_2][S_3])$.

4. $\mathrm{ext}^k_A(M,N)$ is an $\mathrm{End}_A(M)$-$\mathrm{End}_A(N)$-bimodule.

Proof. Cf. [Lan91, Chapter III, Theorem 5.3]. □

Observations 7.12 *1. Let $S \in [S] \in \mathrm{ext}^k_A(M,N)$ with*

$$S = 0 \longrightarrow N \longrightarrow B_{k-1} \longrightarrow B_{k-2} \longrightarrow \cdots\cdots \longrightarrow B_0 \longrightarrow M \longrightarrow 0,$$

hence we can interpret S as a resolution of M.

2. Let

$$\mathcal{P} := \cdots\cdots P_k \xrightarrow{\alpha_k} P_{k-1} \cdots\cdots \xrightarrow{\alpha_0} P_0 \xrightarrow{\alpha_0} M \longrightarrow 0$$

be a projective resolution of M. By the Comparison Theorem we can lift the identical map $id_M : M \longrightarrow M$ to a chain homomorphism $f : \mathcal{P} \longrightarrow S$, so we obtain a commutative diagram

$$\begin{array}{ccccccccccccc}
\cdots\cdots & P_{k+1} & \xrightarrow{\alpha_{k+1}} & P_n & \xrightarrow{\alpha_k} & P_{k-1} & \cdots\cdots & \xrightarrow{\alpha_0} & P_0 & \xrightarrow{\alpha_0} & M & \longrightarrow & 0 \\
 & 0\downarrow & & f_k\downarrow & & f_{k-1}\downarrow & & & f_0\downarrow & & id_M\| & & \\
 & 0 & \longrightarrow & N & \xrightarrow{\beta_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\beta_1} & B_0 & \xrightarrow{\beta_0} & M & \longrightarrow & 0.
\end{array}$$

We can "interpret" S as this chain homomorphism (see Theorem 7.13). We note: $\alpha_{k+1}f_k = 0$, hence $f_k \in Ker({\alpha_{k+1}}^*)$, so $f_k + Im({\alpha_k}^*) \in \mathrm{Ext}^k_A(M,N)$.

Theorem 7.13 *Let the notations be as in Observations 7.12. For arbitrary A-modules M and N and a projective resolution $\mathcal{P}$ of M, there is a well-defined isomorphism of Abelian groups:*

$$\xi : \mathrm{ext}^k_A(M,N) \ni [S] \longmapsto f_k + Im({\alpha_k}^*) \in \mathrm{Ext}^k_A(M,N).$$

Proof.

- We just state the inverse η of ξ which will be needed later on for concrete calculations (for a detailed proof see [Lan91, Chapter III, Theorem 6.4]). Choose any resolution

$$\mathcal{X} := \cdots\cdots X_k \xrightarrow{\delta_k} X_{k-1} \cdots\cdots \xrightarrow{\delta_1} X_0 \xrightarrow{\delta_0} M \longrightarrow 0$$

of M. Next we factor δ_k over its image

$$\begin{array}{ccc}
X_k & & \\
\downarrow{\scriptstyle \delta_k'} & \searrow{\scriptstyle \delta_k} & \\
\delta_k X_k & \xrightarrow{\kappa} & X_{k-1}.
\end{array}$$

Now let $\tilde{h} : X_k \longrightarrow N$ be some k-cocycle, then $\tilde{h}$ can be written as ${\delta_k}' h$ for a uniquely determined map $h : \delta_k : X_k \longrightarrow N$. We set

$$S_k(M, \mathcal{X}) := 0 \longrightarrow \delta_k X_k \xrightarrow{\kappa} X_{k-1} \cdots\cdots \longrightarrow X_0 \longrightarrow M \longrightarrow 0$$

We define $\eta : \mathrm{Ext}^k_A(M, N) \longrightarrow \mathrm{ext}^k_A(M, N)$ by $\eta(\tilde{h} + \mathrm{Im}({\delta_k}^*)) := [hS_k(M, \mathcal{X})$.

□

7.2 Definition of and Basic Facts about Cohomology Rings

In this section A denotes an arbitrary ring and $M, \tilde{M}, N$ and $\tilde{N}$ are some A-modules.

Definition 7.14 *We set* $\mathrm{ext}^*_A(M, M) := \bigoplus_{k\in\mathbb{N}} \mathrm{ext}^k_A(M, M)$. *Theorem 7.11 yields that* $\mathrm{ext}^*_A(M, M)$ *is a graded associative ring. The addition is the componentwise addition induced from the Baer sum and the multiplication is induced from the Yoneda splice. This ring is called the cohomology ring of* M.

Remark 7.15 *Moreover we set* $\mathrm{Ext}^*_A(M, M) := \bigoplus_{k\in\mathbb{N}} \mathrm{Ext}^k_A(M, M)$. *An application of Theorem 7.13 yields that there is an isomorphism of graded Abelian groups*

$$\mathrm{ext}^*_A(M, M) \simeq \mathrm{Ext}^*_A(M, M).$$

This isomorphism induces a ring structure on $\mathrm{Ext}^*_A(M, M)$, *so we will also refer to* $\mathrm{Ext}^*_A(M, M)$ *as the cohomology ring of* M. *The multiplication in* $\mathrm{Ext}^*_A(M, M)$ *is not so natural as the Yoneda splice; but* $\mathrm{Ext}^*_A(M, M)$ *has the advantage that its elements - as residue classes of homomorphisms - are better to handle than congruence classes of exact sequence, so we will restrict ourself on* $\mathrm{Ext}^*_A(M, M)$.

The next results show how the multiplication in $\mathrm{ext}^*_A(M, M)$ via the Yoneda splices carries over to the corresponding multiplication in $\mathrm{Ext}^*_A(M, M)$.

Lemma 7.16 *Let* $\alpha \in \mathrm{Hom}_A(N, \tilde{N})$, $\gamma \in \mathrm{Hom}_A(\tilde{M}, M)$, $1 \leq k$ *and* $[S] \in \mathrm{ext}^k_A(M, N)$ *with*

$$S = 0 \longrightarrow N \xrightarrow{\alpha_k} B_{k-1} \xrightarrow{\alpha_{k-1}} B_{k-2} \cdots\cdots \xrightarrow{\alpha_1} B_0 \xrightarrow{\alpha_0} M \longrightarrow 0.$$

Furthermore let

$$\cdots\cdots \longrightarrow X_r \xrightarrow{\delta_r} \cdots\cdots\cdots\cdots \xrightarrow{\delta_2} X_1 \xrightarrow{\delta_1} X_0 \xrightarrow{\delta_0} M \longrightarrow 0$$

and

$$\cdots\cdots \longrightarrow Y_s \xrightarrow{\epsilon_s} \cdots\cdots\cdots\cdots \xrightarrow{\epsilon_2} Y_1 \xrightarrow{\epsilon_1} Y_0 \xrightarrow{\epsilon_0} \tilde{M} \longrightarrow 0$$

be projective resolutions of M *and* $\tilde{M}$ *respectively. We have a commutative diagram*

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \longrightarrow & X_k & \xrightarrow{\delta_k} & X_{k-1} & \cdots\cdots & \xrightarrow{\delta_2} & X_1 & \xrightarrow{\delta_1} & X_0 & \xrightarrow{\delta_0} & M & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \varphi_k} & & \downarrow{\scriptstyle \varphi_{k-1}} & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \| {\scriptstyle id_M} & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow 0,
\end{array}$$

where φ_k *is a cocycle.*

1. *The homomorphism $\varphi_k\alpha$ is a cocycle and corresponds to the exact sequence αS.*

2. *By the Comparison Theorem we can lift γ to a chain homomorphism*

$$\begin{array}{ccccccccccccccc}
\cdots\cdots & \longrightarrow & Y_k & \xrightarrow{\epsilon_k} & Y_{k-1} & \cdots\cdots & \xrightarrow{\epsilon_2} & Y_1 & \xrightarrow{\epsilon_1} & Y_0 & \xrightarrow{\epsilon_0} & \tilde{M} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_k} & & \downarrow{\scriptstyle \psi_{k-1}} & & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow & 0,
\end{array}$$

Then ψ_k is a cocycle and it corresponds to the exact sequence $S\gamma$.

Proof.

1. Let αS be the exact sequence

$$0 \longrightarrow \tilde{N} \xrightarrow{\beta_k} C_{k-1} \xrightarrow{\beta_{k-1}} C_{k-2} \longrightarrow \cdots\cdots \xrightarrow{\beta_1} C_0 \xrightarrow{\beta_0} M \longrightarrow 0.$$

   By Observation 7.8 α induces a homomorphism $\Sigma : S \longrightarrow \alpha S$. So we obtain the following commutative diagram:

$$\begin{array}{ccccccccccccccc}
X_{k+1} & \xrightarrow{\delta_{k+1}} & X_k & \xrightarrow{\delta_k} & X_{k-1} & \cdots\cdots & \xrightarrow{\delta_2} & X_1 & \xrightarrow{\delta_1} & X_0 & \xrightarrow{\delta_0} & M & \longrightarrow & 0 \\
\downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle \varphi_k} & & \downarrow{\scriptstyle \varphi_{k-1}} & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \|{\scriptstyle \mathrm{id}_M} & & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow & 0 \\
\downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \sigma_{k-1}} & & & \downarrow{\scriptstyle \sigma_1} & & \downarrow{\scriptstyle \sigma_0} & & \|{\scriptstyle \mathrm{id}_M} & & \\
0 & \longrightarrow & \tilde{N} & \xrightarrow{\beta_k} & C_{k-1} & \cdots\cdots & \xrightarrow{\beta_2} & C_1 & \xrightarrow{\beta_1} & C_0 & \xrightarrow{\beta_0} & M & \longrightarrow & 0
\end{array}$$

   for some morphisms σ_i, hence $\varphi_k\alpha$ is a cocycle and it corresponds to the sequence αS (here we use Theorem 7.13).

2. Let

$$0 \longrightarrow N \xrightarrow{\tau_k} D_{k-1} \xrightarrow{\tau_{k-1}} D_{k-2} \longrightarrow \cdots\cdots \xrightarrow{\tau_1} D_0 \xrightarrow{\tau_0} \tilde{M} \longrightarrow 0.$$

   be the sequence $S\gamma$. By Observation 7.8 γ induces a homomorphism $\Gamma : S\gamma \longrightarrow S$. The Comparison Theorem yields that we can lift $\mathrm{id}_{\tilde{M}}$ to a chain homomorphism from the projective resolution of $\tilde{M}$ to $S\gamma$, so all in all we have a commutative diagram:

$$\begin{array}{ccccccccccccccc}
Y_{k+1} & \xrightarrow{\epsilon_{k+1}} & Y_k & \xrightarrow{\epsilon_k} & Y_{k-1} & \cdots\cdots & \xrightarrow{\epsilon_2} & Y_1 & \xrightarrow{\epsilon_1} & Y_0 & \xrightarrow{\epsilon_0} & \tilde{M} & \longrightarrow & 0 \\
\downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle \eta_k} & & \downarrow{\scriptstyle \eta_{k-1}} & & & \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_0} & & \|{\scriptstyle \mathrm{id}_{\tilde{M}}} & & \\
0 & \longrightarrow & N & \xrightarrow{\tau_k} & D_{k-1} & \cdots\cdots & \xrightarrow{\tau_2} & D_1 & \xrightarrow{\tau_1} & D_0 & \xrightarrow{\tau_0} & \tilde{M} & \longrightarrow & 0 \\
\downarrow{\scriptstyle 0} & & \|{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle \gamma_{k-1}} & & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_0} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow & 0.
\end{array}$$

   We know that $\eta_k \in \mathrm{Ker}({\epsilon_{k+1}}^*)$ corresponds to the sequence $S\gamma$. The last diagram shows that we get the chain homomorphism

$$\begin{array}{ccccccccccccccc}
Y_{k+1} & \xrightarrow{\epsilon_{k+1}} & Y_k & \xrightarrow{\epsilon_k} & Y_{k-1} & \cdots\cdots & \xrightarrow{\epsilon_2} & Y_1 & \xrightarrow{\epsilon_1} & Y_0 & \xrightarrow{\epsilon_0} & \tilde{M} & \longrightarrow & 0 \\
\downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle \eta_k} & & \downarrow{\scriptstyle \eta_{k-1}\gamma_{k-1}} & & & \downarrow{\scriptstyle \eta_1\gamma_1} & & \downarrow{\scriptstyle \eta_0\gamma_0} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow & 0,
\end{array}$$

which lifts γ. On the other side the following chain homomorphism also lifts γ:

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \longrightarrow & Y_k & \xrightarrow{\epsilon_k} & Y_{k-1} & \cdots\cdots & \xrightarrow{\epsilon_2} & Y_1 & \xrightarrow{\epsilon_1} & Y_0 & \xrightarrow{\epsilon_0} & \tilde{M} & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \psi_k} & & \downarrow{\scriptstyle \psi_{k-1}} & & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \gamma} & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow 0.
\end{array}$$

The Comparison Theorem yields that there is a homomorphism $s : Y_{k-1} \longrightarrow N$ such that $\eta_k - \psi_k = \epsilon_k s$, hence the images of η_k and ψ_k in $\mathrm{Ext}^k_A(M,N)$ are the same and we are done.

□

Corollary 7.17 *Let $\gamma \in \mathrm{Hom}_A(\tilde{M}, M)$, $1 \leq k$ and $[S] \in \mathrm{ext}^k_A(M,N)$ with*

$$S : 0 \longrightarrow N \xrightarrow{\alpha_k} B_{k-1} \xrightarrow{\alpha_{k-1}} B_{k-2} \cdots\cdots \xrightarrow{\alpha_1} B_0 \xrightarrow{\alpha_0} M \longrightarrow 0.$$

Furthermore let

$$\cdots\cdots \longrightarrow X_r \xrightarrow{\delta_r} \cdots\cdots\cdots \xrightarrow{\delta_2} X_1 \xrightarrow{\delta_1} X_0 \xrightarrow{\delta_0} M \longrightarrow 0$$

and

$$\cdots\cdots \longrightarrow Y_s \xrightarrow{\epsilon_s} \cdots\cdots\cdots \xrightarrow{\epsilon_2} Y_1 \xrightarrow{\epsilon_1} Y_0 \xrightarrow{\epsilon_0} \tilde{M} \longrightarrow 0$$

be projective resolutions of M and $\tilde{M}$ respectively. We have a commutative diagram

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \longrightarrow & X_k & \xrightarrow{\delta_k} & X_{k-1} & \cdots\cdots & \xrightarrow{\delta_2} & X_1 & \xrightarrow{\delta_1} & X_0 & \xrightarrow{\delta_0} & M & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \varphi_k} & & \downarrow{\scriptstyle \varphi_{k-1}} & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \| {\scriptstyle id_M} & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow 0,
\end{array}$$

where φ_n is a cocycle. By the Comparison Theorem we can lift $\gamma : \tilde{M} \longrightarrow M$ to a chain homomorphism

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \longrightarrow & Y_k & \xrightarrow{\epsilon_k} & Y_{k-1} & \cdots\cdots & \xrightarrow{\epsilon_2} & Y_1 & \xrightarrow{\epsilon_1} & Y_0 & \xrightarrow{\epsilon_0} & \tilde{M} & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \gamma_k} & & \downarrow{\scriptstyle \gamma_{k-1}} & & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_0} & & \downarrow{\scriptstyle \gamma} & \\
\cdots\cdots & \longrightarrow & X_k & \xrightarrow{\delta_k} & X_{k-1} & \cdots\cdots & \xrightarrow{\delta_2} & X_1 & \xrightarrow{\delta_1} & X_0 & \xrightarrow{\delta_0} & M & \longrightarrow 0.
\end{array}$$

Then $\gamma_k \varphi_k$ is a cocycle which corresponds to the exact sequence $S\gamma$.

Proof. All in all we have the following commutative diagram:

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \longrightarrow & Y_k & \xrightarrow{\epsilon_k} & Y_{k-1} & \cdots\cdots & \xrightarrow{\epsilon_2} & Y_1 & \xrightarrow{\epsilon_1} & Y_0 & \xrightarrow{\epsilon_0} & \tilde{M} & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \gamma_k} & & \downarrow{\scriptstyle \gamma_{k-1}} & & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_0} & & \downarrow{\scriptstyle \gamma} & \\
\cdots\cdots & \longrightarrow & X_k & \xrightarrow{\delta_k} & X_{k-1} & \cdots\cdots & \xrightarrow{\delta_2} & X_1 & \xrightarrow{\delta_1} & X_0 & \xrightarrow{\delta_0} & M & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \varphi_k} & & \downarrow{\scriptstyle \varphi_{k-1}} & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \| {\scriptstyle \mathrm{id}_M} & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_k} & B_{k-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow 0.
\end{array}$$

Hence $(0, \gamma_k\varphi_k, \gamma_{k-1}\varphi_{k-1}, \ldots, \gamma_0\varphi_0, \gamma)$ is a chain homomorphism which lifts γ, so we can apply Lemma 7.16 (2). □

Lemma 7.18 *Let $1 \leq n, m \in \mathbb{N}$ and $[E] \in \operatorname{ext}_A^n(M,N)$ and $[F] \in \operatorname{ext}_A^m(N,\tilde{M})$. Then the representatives E and F are some exact sequences, say*

$$E = 0 \longrightarrow N \xrightarrow{\alpha_n} B_{n-1} \xrightarrow{\alpha_{n-1}} \cdots\cdots \xrightarrow{\alpha_1} B_0 \xrightarrow{\alpha_0} M \longrightarrow 0$$

and

$$F = 0 \longrightarrow \tilde{M} \xrightarrow{\beta_m} M_{m-1} \xrightarrow{\beta_{m-1}} \cdots\cdots \xrightarrow{\beta_1} M_0 \xrightarrow{\beta_0} N \longrightarrow 0.$$

Furthermore let

$$\cdots\cdots \longrightarrow X_k \xrightarrow{\delta_k} \cdots\cdots \xrightarrow{\delta_2} X_1 \xrightarrow{\delta_1} X_0 \xrightarrow{\delta_0} M \longrightarrow 0$$

and

$$\cdots\cdots \longrightarrow Y_s \xrightarrow{\epsilon_s} \cdots\cdots \xrightarrow{\epsilon_2} Y_1 \xrightarrow{\epsilon_1} Y_0 \xrightarrow{\epsilon_0} N \longrightarrow 0$$

be projective resolutions of M and N respectively. We have a commutative diagram

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \longrightarrow & X_n & \xrightarrow{\delta_n} & X_{n-1} & \cdots\cdots & \xrightarrow{\delta_2} & X_1 & \xrightarrow{\delta_1} & X_0 & \xrightarrow{\delta_0} & M & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n-1}} & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \| {\scriptstyle id_M} & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_n} & B_{n-1} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} & M & \longrightarrow 0,
\end{array}$$

where φ_n is a cocycle, hence we can find a homomorphism $g : \delta_n X_n \longrightarrow N$ such that the following diagram commutes (where $\kappa : \delta_n X_n \longrightarrow X_{n-1}$ denotes the canonical embedding):

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & \delta_n X_n & \xrightarrow{\kappa} & X_{n-1} & \xrightarrow{\alpha_{n-1}} & \cdots\cdots & \xrightarrow{\delta_2} & X_1 & \xrightarrow{\delta_1} & X_0 & \xrightarrow{\delta_0} M & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \varphi_{n-1}} & & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & \| {\scriptstyle id_M} & \\
0 & \longrightarrow & N & \xrightarrow{\alpha_n} & B_{n-1} & \xrightarrow{\alpha_{n-1}} & \cdots\cdots & \xrightarrow{\alpha_2} & B_1 & \xrightarrow{\alpha_1} & B_0 & \xrightarrow{\alpha_0} M & \longrightarrow 0.
\end{array}$$

By the Comparison Theorem we can lift g to a chain homomorphism (we set $\delta_n{}' : X_n \longrightarrow \delta_n X_n$ to be the corestriction of the map δ_n to its image):

$$\begin{array}{ccccccccccccc}
\cdots\cdots & X_{n+m} & \xrightarrow{\delta_{n+m}} & X_{n+m-1} & \cdots\cdots & \xrightarrow{\delta_{n+2}} & X_{n+1} & \xrightarrow{\delta_{n+1}} & X_n & \xrightarrow{\delta_n{}'} & \delta_n X_n & \longrightarrow 0 \\
 & \downarrow{\scriptstyle g_m} & & \downarrow{\scriptstyle g_{m-1}} & & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_0} & & \downarrow{\scriptstyle g} & \\
\cdots\cdots & Y_m & \xrightarrow{\epsilon_m} & Y_{m-1} & \cdots\cdots & \xrightarrow{\epsilon_2} & Y_1 & \xrightarrow{\epsilon_1} & Y_0 & \xrightarrow{\epsilon_0} & N & \longrightarrow 0.
\end{array}$$

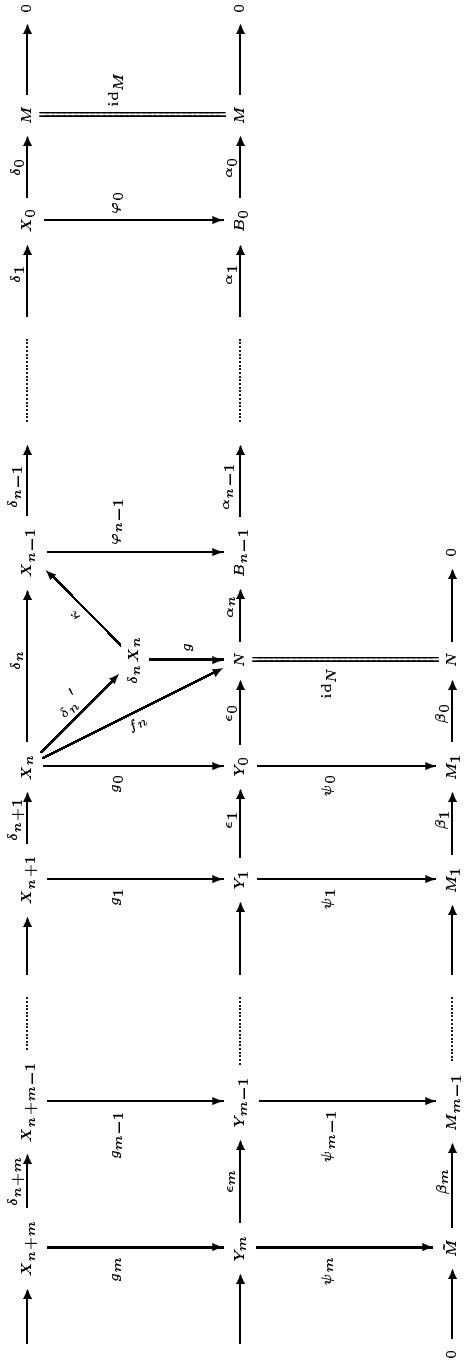
The following chain homomorphism corresponds to F:

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \longrightarrow & Y_m & \xrightarrow{\epsilon_m} & Y_{m-1} & \cdots\cdots & \xrightarrow{\epsilon_2} & X_1 & \xrightarrow{\epsilon_1} & X_0 & \xrightarrow{\epsilon_0} & N & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \psi_m} & & \downarrow{\scriptstyle \psi_{n-1}} & & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \| {\scriptstyle id_N} & \\
0 & \longrightarrow & \tilde{M} & \xrightarrow{\beta_m} & M_{m-1} & \cdots\cdots & \xrightarrow{\beta_2} & M_1 & \xrightarrow{\beta_1} & M_0 & \xrightarrow{\beta_0} & N & \longrightarrow 0.
\end{array}$$

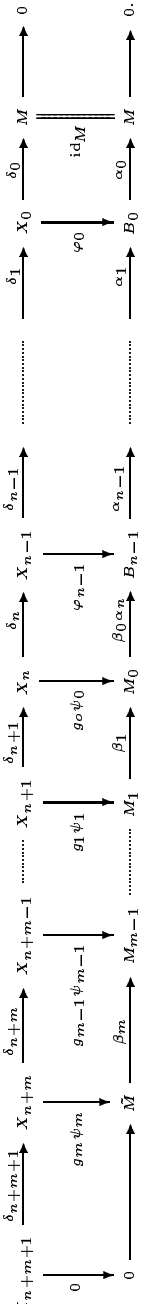
Then the homomorphism $g_m \psi_m$ corresponds to the Yoneda splice $F \circ E$.

Proof.

1. For the convenience of the reader we collect all data which we have stated in the formulation of the lemma in one big commutative diagram:



2. *Claim.* The following diagram is commutative:



This yields in particular that $g_m \psi_m$ is a cocycle.

Proof of the Claim.

a) $g_0\psi_0\beta_0\alpha_n = \delta_n\varphi_{n-1}$ holds by the following calculation:

$$g_0\psi_0\beta_0\alpha_n \underset{\psi_0\beta_0=\epsilon_0\mathrm{id}_N}{=} g_0\epsilon_0\alpha_n \underset{g_0\epsilon_0={\delta_n}'g}{=} {\delta_n}'g\alpha_n$$
$$\underset{g\alpha_n=\kappa\varphi_{n-1}}{=} {\delta_n}'\kappa\varphi_{n-1} \underset{{\delta_n}'\kappa=\delta_n}{=} \delta_n\varphi_{n-1}.$$

b) For $i \geq 1$ holds: $g_i\psi_i \underset{\psi_i\beta_i=\epsilon_i\psi_{i-1}}{=} g_i\epsilon_i\psi_{i-1} \underset{\psi_i\epsilon_i=\delta_{n+i}\psi_{i-1}}{=} \delta_{n+i}g_{i-1}\psi_{i-1}$.

c) $\delta_{n+m+1}g_m\psi_m \underset{\delta_{n+m+1}g_m=g_{m+1}\epsilon_{m+1}}{=} g_{m+1}\epsilon_{m+1}\psi_m \underset{\epsilon_{m+1}\psi_m=0}{=} g_{m+1}0 = 0.$

□

□

7.3 For truncated Twisted Polynomial Rings

We use the notations of Chapter 6 and without mention the isomorphisms of Theorem 7.13. For $1 \leq i$ we have

$$\mathrm{Ext}^i_A(S,S) = \mathrm{Hom}_A(A,S) = \{\varphi_l : A \ni 1 \longmapsto lN \in S \ : \ l \in L\}$$

by Remark 6.10 and Lemma 6.19. We use the following notation: The homomorphism $\varphi_1 \in \mathrm{Hom}_A(A,S) = \mathrm{Ext}^i_A(S,S)$ will be denoted by f^i_1. So we get

$$\mathrm{Ext}^*_A(S,S) = \bigoplus_{i\in\mathbb{N}} \mathrm{Ext}^i_A(S,S) = \bigoplus_{i\in\mathbb{N}} L\,\mathrm{f}^i_1\,.$$

7.3.1 The case $k = 2$

A projective resolution of the simple A-module S is given by

$$\cdots\cdots \xrightarrow{\varphi} A \xrightarrow{\varphi} A \xrightarrow{\varphi} A \xrightarrow{\varphi} S \longrightarrow 0,$$

with $\varphi := \rho_1 : A \ni a \longmapsto aN \in A$ and S is identified wit AN (see Lemma 6.9).

For $1 \leq r, s$ let $[E] \in \mathrm{ext}^r_A(S,S)$ and $[F] \in \mathrm{ext}^s_A(S,S)$. The representatives E and F are some exact sequences, say

$$E : 0 \longrightarrow S \longrightarrow B_{r-1} \longrightarrow \cdots\cdots\cdots\cdots \longrightarrow B_0 \longrightarrow S \longrightarrow 0$$

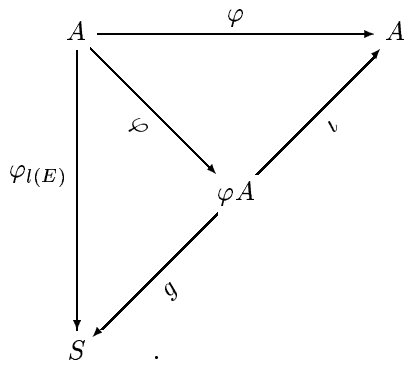
and

$$F : 0 \longrightarrow S \longrightarrow C_{s-1} \longrightarrow \cdots\cdots\cdots\cdots \longrightarrow C_0 \longrightarrow S \longrightarrow 0.$$

To $[E]$ and $[F]$ correspond $\varphi_{l(E)} \in \mathrm{Hom}_A(A,S)$ and $\varphi_{l(F)} \in \mathrm{Hom}_A(A,S)$ respectively. $\varphi_{l(E)}$ is the last part of the following chain homomorphism

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \longrightarrow & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & \cdots\cdots\cdots\cdots & \longrightarrow & A & \xrightarrow{\varphi} & S & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_{l(E)}} & & \downarrow & & & & \downarrow & & \| & & \\
0 & \longrightarrow & S & \longrightarrow & B_{r-1} & \longrightarrow & \cdots\cdots\cdots\cdots & \longrightarrow & B_0 & \longrightarrow & S & \longrightarrow & 0.
\end{array}$$

In the first step to determine the homomorphism $\varphi_{l(F\circ E)} \in \mathrm{Hom}_A(A,S)$ which corresponds to $[F\circ E]$ we have to factor φ over its image and have to determine the unique element $g \in \mathrm{End}_A(S)$ making the following diagram commutative:



An easy calculation shows $g = \mu_{l(E)} \in \mathrm{Hom}_A(S,S)$ (see Lemma 6.11). We have to lift the homomorphism $\mu_{l(E)}$ to a chain homomorphism

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & \varphi A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \gamma_4} & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \mu_{l(E)}} & & \\
\cdots\cdots & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & S & \longrightarrow & 0.
\end{array}$$

Notation 7.19 *For $a \in A$ we define $\nu_a \in \mathrm{End}_A(A)$ by $\nu_a : A \ni \tilde{a} \longmapsto \tilde{a}a \in A$.*

Lemma 7.20 *For all $1 \leq i \in \mathbb{N}$ we can choose $\gamma_i = \nu_{\tau^{i-1}(l(E))}$.*

Proof. We use induction on i:

- Let $i = 1$. There is some $a \in A$ with $\gamma_1 = \nu_a$. Then we must have

$$l(E)N = N\mu_{l(E)} = 1\varphi\mu_{l(E)} = 1\nu_a\varphi = a\varphi = aN,$$

  so we can choose $a = l(E)$ and hence $\gamma_1 = \nu_{l(E)}$.

- Now assume $i \gneq 1$: Let $\gamma_i = \nu_a$ for some $a \in A$. By induction we get $\gamma_{i-1} = \nu_{\tau^{i-2}(l(E))}$. We must have $\gamma_i\varphi = \varphi\nu_{\tau^{i-2}(l(E))}$, hence

$$\begin{aligned} aN = a\varphi = 1\nu_a\varphi = 1\gamma_i\varphi = 1\varphi\gamma_{i-1} = 1\varphi\nu_{\tau^{i-2}(l(E))} \\ = N\nu_{\tau^{i-2}(l(E))} = N\tau^{i-2}(l(E)) = \tau^{i-1}(l(E))N. \end{aligned}$$

□

An easy application of Lemma 7.18 yields that the homomorphism which corresponds to $F\circ E$ is given by $\varphi_{l(F\circ E)} = \nu_{\tau^s(l(E))}\varphi_{l(F)} = \varphi_{\tau^s(l(E))l(F)}$.

Now we have to consider the case that one of the elements r or s is equal to 0. As above we choose $[E] \in \mathrm{Ext}^r_A(S,S)$ and $[F] \in \mathrm{Ext}^s_A(S,S)$. Lemma 6.11 yields

$$\mathrm{End}_A(S) = \{\mu_l : An^{k-1} \ni aN^{k-1} \longmapsto alN^{k-1} \in AN^{k-1} \mid l \in L\} \simeq L.$$

Hence if $r = s = 0$ holds we get $[E] = \mu_{l(E)}$ and $[F] = \mu_{l(F)}$ for some elements $l(E), l(F) \in L$, so to the Yoneda splice $F\circ E$ corresponds the homomorphism $\mu_{l(F)}\mu_{l(E)} = \mu_{l(F)l(E)} \in \mathrm{End}_A(S)$.

Now assume $s = 0$ and $r \geq 1$. This yields $[F] = \mu_{l(F)} \in \mathrm{End}_A(S)$ and $E \in [E] \in \mathrm{Ext}^r_A(S,S)$ with

$$E = 0 \longrightarrow S \longrightarrow B_{r-1} \longrightarrow \cdots\cdots \longrightarrow B_0 \longrightarrow S \longrightarrow 0.$$

To E corresponds $\varphi_{l(E)}$ which is the last part of a chain homomorphism:

$$\begin{array}{ccccccccccc}
\cdots\cdots & \longrightarrow & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & \cdots\cdots & \longrightarrow & A & \xrightarrow{\varphi} & S \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \varphi_{l(E)}} & & \downarrow & & & & \downarrow & & \| \\
0 & \longrightarrow & S & \longrightarrow & B_{k-1} & \longrightarrow & \cdots\cdots & \longrightarrow & B_0 & \longrightarrow & S \longrightarrow 0.
\end{array}$$

An application of Lemma 7.16 (1) yields that to $[F][E] = [\mu_{l(F)}E]$ corresponds the homomorphism $\varphi_{l(E)}\mu_{l(F)} = \varphi_{l(E)l(F)}$.

Now let us assume that $r = 0$ and $s \geq 1$ holds. So we have that $[E] = \mu_{l(E)} \in \mathrm{End}_A(S)$ and $F \in [F] \in \mathrm{Ext}^s_A(S,S)$ is satisfied with

$$F = 0 \longrightarrow S \longrightarrow C_{s-1} \longrightarrow \cdots\cdots \longrightarrow C_0 \longrightarrow S \longrightarrow 0.$$

According to Corollary 7.17 we have to lift $\mu_{l(E)}$ to a chain homomorphism (the existence of this chain homomorphism is guaranteed by the Comparison Theorem):

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & \varphi A \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \gamma_4} & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \mu_{l(E)}} \\
\cdots\cdots & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & S \longrightarrow 0.
\end{array}$$

Lemma 7.20 tells us that we can choose $\gamma_i = \nu_{\tau^{i-1}(l(E))}$ (we use Notation 7.19). Following furthermore Corollary 7.17 we obtain that the homomorphism

$$\gamma_{s+1}\varphi_{l(F)} = \nu_{\tau^s(l(E))}\varphi_{l(F)} = \varphi_{\tau^s(l(E))l(F)} \in \mathrm{Hom}_A(A,S)$$

corresponds to $[F][E] = [F\mu_{l(E)}]$.

If we put together all the facts we have collected in the above discussion we obtain

Lemma 7.21 *For arbitrary $r, s \in \mathbb{N}$ and $l_1, l_2 \in L$ we get:*

$$l_1\,\mathrm{f}_1^r \cdot l_2\,\mathrm{f}_1^s = l_1\tau^r(l_2)\,\mathrm{f}_1^{r+s}.$$

Corollary 7.22 *There is an isomorphism of rings*

$$\mathrm{Ext}^*_A(S,S) \simeq L[y,\tau].$$

Proof. The map Φ which is induced by $\mathrm{Ext}^r_A(S,S) \ni l\,\mathrm{f}_1^r \longmapsto ly^r \in L[y,\tau]$ is surely an isomorphism of L-vector spaces. For $l_1, l_2 \in L$ and $r, s \in \mathbb{N}$ we have

$$\Phi(l_1\,\mathrm{f}_1^r\,l_2\,\mathrm{f}_1^s) = \Phi(l_1\tau^r(l_2)\,\mathrm{f}_1^{r+s}) = l_1\tau^r(l_2)y^{r+s} = l_1y^rl_2y^s = \Phi(l_1\,\mathrm{f}_1^r)\Phi(l_2\,\mathrm{f}_1^s),$$

and we are done. □

7.3.2 The case of an arbitrary $k \geq 3$

Again we consider a projective resolution of the simple module S which will always be identified with AN^{k-1} (see Lemma 6.9):

$$\cdots\cdots \xrightarrow{\rho_1} A \xrightarrow{\rho_{k-1}} A \xrightarrow{\rho_1} A \xrightarrow{\rho_{k-1}} S \longrightarrow 0.$$

First let us assume that we have $1 \leq r, s$; we choose $[E] \in \mathrm{ext}_A^r(S,S)$ and $[F] \in \mathrm{ext}_A^s(S,S)$. The representatives E and F are some exact sequences, say

$$E = 0 \longrightarrow S \longrightarrow B_{s-1} \longrightarrow \cdots\cdots\cdots \longrightarrow B_0 \longrightarrow S \longrightarrow 0$$

and

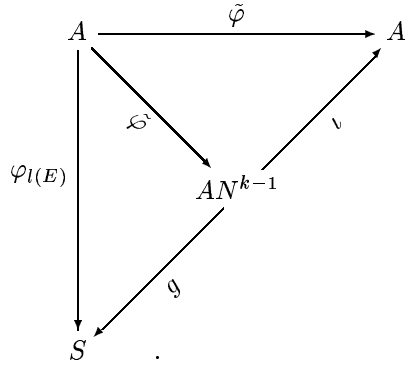
$$F = 0 \longrightarrow S \longrightarrow C_{s-1} \longrightarrow \cdots\cdots\cdots \longrightarrow C_0 \longrightarrow S \longrightarrow 0.$$

To $[E]$ and $[F]$ correspond two homomorphisms $\varphi_{l(E)} \in \mathrm{Hom}_A(A,S)$ and $\varphi_{l(F)} \in \mathrm{Hom}_A(A,S)$. The homomorphism $\varphi_{l(E)}$ is the last part of the following chain homomorphism

$$\begin{array}{ccccccccccc}
\cdots\cdots & \longrightarrow & A & \xrightarrow{\partial} & A & \longrightarrow & \cdots\cdots\cdots & \longrightarrow & A & \longrightarrow & S & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_{l(E)}} & & \downarrow & & & & \downarrow & & \| & & \\
0 & \longrightarrow & S & \longrightarrow & B_{r-1} & \longrightarrow & \cdots\cdots\cdots & \longrightarrow & B_0 & \longrightarrow & S & \longrightarrow & 0.
\end{array}$$

But now we are not in the "lucky" case that the period of the used projective resolution of A is 1, there are indeed - depending on r - two possibilities for the homomorphism ∂. Let us set $\varphi := \rho_1$ and $\tilde{\varphi} := \rho_{k-1}$. There are two cases:

Case 1: r is even. Here the homomorphism ∂ is $\tilde{\varphi}$. We must factor $\tilde{\varphi}$ over its image and obtain a homomorphism $g : AN^{k-1} \longrightarrow S$ which makes the following diagram commutative:



An easy calculation - using Lemma 6.11 - yields that we have $g = \mu_{l(E)}$. As usual we have to lift $\mu_{l(E)}$ to a chain homomorphism:

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \xrightarrow{\tilde{\varphi}} & A & \xrightarrow{\varphi} & A & \xrightarrow{\tilde{\varphi}} & A & \xrightarrow{\varphi} & A & \xrightarrow{\tilde{\varphi}} & \tilde{\varphi}A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_0} & & \downarrow{\scriptstyle \mu_{l(E)}} & & \\
\cdots\cdots & \xrightarrow{\tilde{\varphi}} & A & \xrightarrow{\varphi} & A & \xrightarrow{\tilde{\varphi}} & A & \xrightarrow{\varphi} & A & \xrightarrow{\tilde{\varphi}} & S & \longrightarrow & 0.
\end{array}$$

Lemma 7.23 *We have* $\gamma_i = \begin{cases} \nu_{\tau^{\tilde{i}k}(l(E))} & \text{for } i = 2\tilde{i} \text{ (i even)} \\ \nu_{\tau^{\tilde{i}k+1}(l(E))} & \text{for } i = 2\tilde{i}+1 \text{ (i odd)} \end{cases}$.

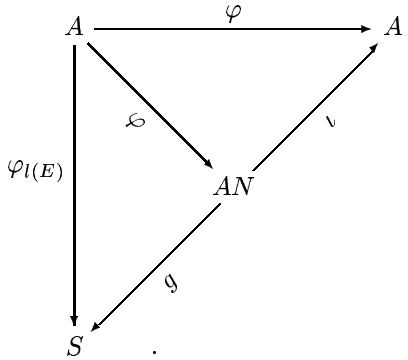
Proof. We use induction on i.

- Let $i = 0$: $\gamma_0 = \nu_a$ has to obey the condition $\tilde{\varphi}\mu_{l(E)} = \nu_a\tilde{\varphi}$, hence
$$l(E)N^{k-1} = N^{k-1}\mu_{l(E)} = 1\tilde{\varphi}\mu_{l(E)} = 1\nu_a\tilde{\varphi} = a\tilde{\varphi} = aN^{k-1},$$
so we can set $\gamma_0 = \nu_l(E)$.
- Now assume $i \gneq 0$. We have to distinguish two cases. First we assume that i is even. So $i = 2\tilde{i}$ for some $\tilde{i} \in \mathbb{N}$, we have $i-1 = 2\tilde{i}-1 = 2(\tilde{i}-1)+1$ is odd. By induction we get $\gamma_{i-1} = \nu_{\tau^{(\tilde{i}-1)k+1}(l(E))}$. Let $\gamma_i = \nu_a$ for some $a \in A$. The homomorphism γ_i must satisfy $\gamma_i\tilde{\varphi} = \tilde{\varphi}\gamma_{i-1}$, so
$$aN^{k-1} = a\tilde{\varphi} = 1\nu_a\tilde{\varphi} = 1\gamma_i\tilde{\varphi} = 1\tilde{\varphi}\gamma_{i-1} = N^{k-1}\nu_{\tau^{(\tilde{i}-1)k+1}(l(E))}$$
$$= N^{k-1}\tau^{(\tilde{i}-1)k+1}(l(E)) = \tau^{(\tilde{i}-1)k+k-1+1}(l(E))N^{k-1} = \tau^{\tilde{i}k}(l(E))N^{k-1},$$
hence $\gamma_i = \nu_{\tau^{\tilde{i}k}(l(E))}$.

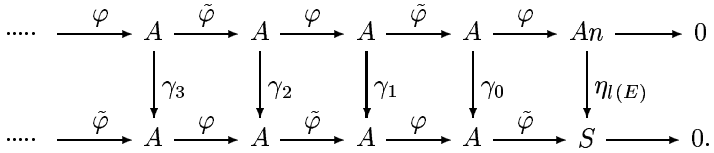
  Now we consider the case that i is odd. There is some $\tilde{i} \in \mathbb{N}$ with $i = 2\tilde{i}+1$, then $i-1 = 2\tilde{i}$ is even, this means (by induction) $\gamma_{i-1} = \nu_{\tau^{\tilde{i}k}(l(E))}$. We set $\gamma_i = \nu_a$ such that $\gamma_i\varphi = \varphi\gamma_{i-1}$ holds. The following equations has to be satisfied
$$aN = a\varphi = 1\nu_a\varphi = 1\gamma_i\varphi = 1\varphi\gamma_{i-1} = N\nu_{\tau^{\tilde{i}k}(l(E))}$$
$$= N\tau^{\tilde{i}k}(l(E)) = \tau^{\tilde{i}k+1}(l(E))N$$
and so we get $\gamma_i = \nu_{\tau^{\tilde{i}k+1}(l(E))}$.

□

Case 2: r is odd. Then we get that the homomorphism ∂ is equal to φ. We factor φ over its image. We obtain again a unique homomorphism g which makes the following diagram commutative:



A straightforward calculation shows that g is the following homomorphism
$$\eta_{l(E)} : AN \ni \tilde{a}N \longmapsto \tilde{a}l(E)N^{k-1} \in AN^{k-1},$$
which has to be lifted to a chain homomorphism



Lemma 7.24 *We find* $\gamma_i = \begin{cases} \nu_{\tau^{(\tilde{i}+1)k-1}(l(E))N^{k-2}} & \text{for } i = 2\tilde{i}+1 \ (i \text{ odd}) \\ \nu_{\tau^{\tilde{i}k}(l(E))} & \text{for } i = 2\tilde{i} \ (i \text{ even}) \end{cases}$.

Proof. We do an induction over i.

- Let $i = 0$. Then for $\gamma_0 = \nu_a$ for some $a \in A$; we must have
$$l(E)N^{k-1} = N\eta_{l(E)} = 1\varphi\eta_{l(E)} = 1\nu_{l(E)}\tilde{\varphi} = a\tilde{\varphi} = aN^{k-1}$$
and so it is possible to set $\gamma_0 = \nu_{l(E)}$.
- Now let us $i \gtrsim 0$ assume. We have to distinguish two cases. If i is odd we have $i = 2\tilde{i}+1$ for some $\tilde{i} \in \mathbb{N}$. We set $\gamma_i = \nu_a$. By induction we know - using that $i-1 = 2\tilde{i}$ is even - that $\gamma_{i-1} = \nu_{\tau^{\tilde{i}k}(l(E))}$ holds. The following equation has to be satisfied:
$$aN = a\varphi = 1\nu_a\varphi = 1\tilde{\varphi}\gamma_{i-1} = 1\tilde{\varphi}\nu_{\tau^{(\tilde{i}k}(l(E))} = N^{k-1}\nu_{\tau^{\tilde{i}k}(l(E))}$$
$$= N^{k-1}\tau^{\tilde{i}k}(l(E)) = \tau^{\tilde{i}k+k-1}(l(E))N^{k-1} = \tau^{(\tilde{i}+1)k-1}(l(E))N^{k-1},$$
hence we set $\gamma_i = \nu_{\tau^{(\tilde{i}+1)k-1}(l(E))N^{k-2}}$.

  Now assume that $i = 2\tilde{i}$ is even, hence $i-1 = 2\tilde{i}-1 = 2(\tilde{i}-1)+1$ is odd. Let $\gamma_i = \nu_a$ for some $a \in A$. Using induction we get $\gamma_{i-1} = \nu_{\tau^{\tilde{i}k-1}(l(E))N^{k-2}}$. We must have:
$$aN^{k-1} = a\tilde{\varphi} = 1\nu_a\tilde{\varphi} = 1\varphi\gamma_{i-1} = 1\varphi\nu_{\tau^{\tilde{i}k-1}(l(E))N^{k-2}}$$
$$= N\nu_{\tau^{\tilde{i}k-1}(l(E))N^{k-2}} = N\tau^{\tilde{i}k-1}(l(E))N^{k-2} = \tau^{\tilde{i}k}(l(E))N^{k-1}.$$
  So we get $\gamma_i = \nu_{\tau^{\tilde{i}k}(l(E))}$.

□

Now we use the Lemmas 7.23 and 7.24 to calculate $\varphi_{l(F\circ E)}$. We have to distinguish four cases.

Case 1): $r, s \equiv 0(2)$. So $\varphi_{l(F\circ E)} = \nu_{\tau^{\frac{s}{2}k}(l(E))}\varphi_{l(F)} = \varphi_{\tau^{\frac{s}{2}k}(l(E))\cdot l(F)}$.

Case 2): $r \equiv 0(2), s \equiv 1(2)$. Then $\varphi_{l(F\circ E)} = \nu_{\tau^{\frac{s-1}{2}k+1}(l(E))}\varphi_{l(F)} = \varphi_{\tau^{\frac{s-1}{2}k+1}(l(E))\cdot l(F)}$.

Case 3): $r \equiv 1(2), s \equiv 0(2)$. Hence $\varphi_{l(F\circ E)} = \nu_{\tau^{\frac{s}{2}k}(l(E))}\varphi_{l(F)} = \varphi_{\tau^{\frac{s}{2}k}(l(E))\cdot l(F)}$.

Case 4): $k, l \equiv 1(2)$. Here we get
$$\varphi_{l(F\circ E)} = \nu_{\tau^{(\frac{s-1}{2}+1)k-1}(l(E))N^{k-2}}\varphi_{l(F)}$$
$$= \varphi_{\tau^{(\frac{s-1}{2}+1)k-1}(l(E))N^{2k-3}} \underset{N^k=0 \text{ and } k\geq 3}{=} 0.$$

Now assume $r = 0, s = 0$. Here $[E] = \mu_{l(E)} \in \mathrm{Ext}^0_A(S,S) \simeq \mathrm{End}_A(S)$ and $[F] = \mu_{l(F)} \in \mathrm{Ext}^0_A(S,S) \simeq \mathrm{End}_A(S)$, hence we get that $F \circ E$ corresponds to the homomorphism $\mu_{l(F)}\mu_{l(E)} = \mu_{l(F)l(E)} = \mu_{l(E)l(F)}$.

Now we consider the case $r = 0$ and $s \geq 1$. So for some $l(E) \in L$ we have $[E] = \mu_{l(E)} \in \mathrm{Ext}^0_A(S,S) \simeq \mathrm{End}_A(S)$ and we get $[F][E] = [F\mu_{l(E)}]$. By Corollary 7.17 we have to lift $\mu_{l(E)}$ to a chain homomorphism

$$\begin{array}{ccccccccccccc}
\cdots\cdots & \xrightarrow{\tilde{\varphi}} & A & \xrightarrow{\varphi} & A & \xrightarrow{\tilde{\varphi}} & A & \xrightarrow{\varphi} & A & \xrightarrow{\tilde{\varphi}} & \tilde{\varphi}A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_0} & & \downarrow{\scriptstyle \mu_{l(E)}} & & \\
\cdots\cdots & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & A & \xrightarrow{\varphi} & S & \longrightarrow & 0.
\end{array}$$

$[F][E]$ corresponds to $\gamma_s \varphi_{l(F)}$ with $\gamma_i = \begin{cases} \nu_{\tau^{\tilde{i}k}(l(E))} & \text{for } i = 2\tilde{i} \ (i \text{ even}) \\ \nu_{\tau^{\tilde{i}k+1}(l(E))} & \text{for } i = 2\tilde{i}+1 \ (i \text{ odd}) \end{cases}$ by Lemma 7.23. So we have to distinguish if s is even or s is odd. If s is even $[F][E]$ corresponds to the homomorphism

$$\nu_{\tau^{\frac{s}{2}k}(l(E))} \varphi_{l(F)} = \varphi_{\tau^{\frac{s}{2}k}(l(E)) \cdot l(F)}.$$

For s odd $[F][E]$ corresponds to

$$\nu_{\tau^{\frac{s-1}{2}k+1}(l(E))} \varphi_{l(F)} = \varphi_{\tau^{\frac{s-1}{2}k+1}(l(E)) l(F)}.$$

We have to consider a last case: $r \geq 1$ and $s = 0$, so there is some element $l(F) \in L$ with $[F] = \mu_{l(F)} \in \mathrm{Ext}^0_A(S,S) \simeq \mathrm{End}_A(S)$ and $[E]$ corresponds in the usual way to a homomorphism $\varphi_{l(E)} : A \longrightarrow S$. According to Lemma 7.16 (1) the homomorphism $\varphi_{l(E)} \mu_{l(F)} = \varphi_{l(E) l(F)}$ belongs to $[F][E] = [\mu_{l(F)} E]$.

Corollary 7.25 *The multiplication in* $\mathrm{Ext}^*_A(S,S)$ *is induced from the following rules:*

$$l_2 \mathrm{f}_1^s \cdot l_1 \mathrm{f}_1^r = \begin{cases} \tau^{\frac{s}{2}k}(l_1) \cdot l_2 \mathrm{f}_1^{r+l} & \textit{for } r, s \equiv 0(2) \\ \tau^{\frac{s-1}{2}k+1}(l_1) \cdot l_2 \mathrm{f}_1^{r+s} & \textit{for } r \equiv 0(2), s \equiv 1(2) \\ \tau^{\frac{s}{2}k}(l_1) \cdot l_2 \mathrm{f}_1^{r+s} & \textit{for } r \equiv 1(2), s \equiv 0(2) \\ 0 & \textit{for } r, s \equiv 1(2) \end{cases}.$$

Notation 7.26 *We set* $B := \mathrm{Ext}^*_A(S,S) = \bigoplus_{i \in \mathbb{N}} L \mathrm{f}_1^i$.

Lemma 7.27 $I := \bigoplus_{j \ odd} L \mathrm{f}_1^j$ *is an Abelian ideal of* B *(i.e.* $J^2 = 0$*).*

Proof. This follows directly from Corollary 7.25. □

Notation 7.28 *We set* $\tilde{\tau} := \tau^k$.

Lemma 7.29 $B_0 := \bigoplus_{i \ even} L \mathrm{f}_1^i = \bigoplus_{t \in \mathbb{N}} L \mathrm{f}_1^{2t}$ *is a subring of* B *and* $B_0 \simeq L[y, \tilde{\tau}]$.

Proof.

1. That B_0 is a subring of B is immediately deduced from Corollary 7.25.
2. With $\Phi : L[y,\tilde{\tau}] \longrightarrow B_0;\ \sum_t \alpha_t y^t \longmapsto \sum_t \alpha_t \mathrm{f}_1^{2t}$ we get
   - Φ maps a basis to a basis, so it is an isomorphism of vector spaces.
   - Let $\sum_i \alpha_i y^i, \sum_j \beta_j y^j$ be arbitrary elements of $L[y,\tilde{\tau}]$. Then we have

$$\Phi\Big((\sum_i \alpha_i y^i)(\sum_j \beta_j y^j)\Big) = \Phi\Big(\sum_{i,j} \alpha_i y^i \beta_j y^j\Big)$$
$$\underset{\text{multiplication in } L[y,\tilde{\tau}]}{=} \Phi\Big(\sum_{i,j} \alpha_i \tilde{\tau}^i(\beta_j) y^{i+j}\Big) \underset{\text{per. def. of } \Phi}{=} \sum_{i,j} \alpha_i \tilde{\tau}^i(\beta_j) \mathrm{f}_1^{2(i+j)}$$
$$\underset{\text{Corollary 7.25}}{=} (\sum_i \alpha_i \mathrm{f}_1^{2i})(\sum_j \beta_j \mathrm{f}_j^{2j}) = \Phi\Big(\sum_i \alpha_i y^i\Big)\Phi\Big(\sum_j \beta_j y^j\Big).$$

So all in all Φ is an isomorphism of rings and we are done.

□

Corollary 7.30 *There are isomorphisms of rings* $B/I \simeq B_0 \simeq L[y,\tilde{\tau}]$.

Lemma 7.31 *We set* $V := L^{(\mathbb{N})} = \bigoplus_{j\in\mathbb{N}} Lf_j$. *We set for* $i \in \mathbb{N}$: $e_{2i+1} := f_i$ *and consider from now on the basis* $\{e_{2i+1} \,|\, i \in \mathbb{N}\}$. *Let* $v = \sum_i \alpha_i e_{2i+1} \in V$ *and* $f = \sum_j \beta_j y^j \in L[y,\tilde{\tau}]$ *be arbitrary elements.*

1. $L[y,\tilde{\tau}]$ *operates from the left on* V *by* $fv := \sum_{i,j} \tilde{\tau}^i(\alpha_j)\beta_i e_{2i+2j+1}$.
2. *The rule* $vf := \sum_{i,j} \alpha_i \tilde{\tau}^i(\tau(\beta_j)) e_{2i+2j+1}$ *induces a right operation.*
3. *With this operations* V *becomes a bimodule over* $L[y,\tilde{\tau}]$ *as an* F*-algebra (this means that the left and the right multiplication of* F *on* V *coincide).*

Proof. Let $g = \sum_k \tilde{\beta}_k y^k$ be another element of $L[y,\tilde{\tau}]$.

1.
   - We find
   $$(fg)v = \Big(\Big(\sum_i \beta_i y^i\Big)\Big(\sum_j \tilde{\beta}_j y^j\Big)\Big)\Big(\sum_k \alpha_k e_{2k+1}\Big)$$
   $$= \Big(\sum_{i,j} \beta_i \tilde{\tau}^i(\tilde{\beta}_j) y^{i+j}\Big)\Big(\sum_k \alpha_k e_{2k+1}\Big) = \sum_{i,j,k} \tilde{\tau}^{i+j}(\alpha_k)\beta_i \tilde{\tau}^i(\tilde{\beta}_j) e_{2(i+j+k)+1}.$$
   - On the other side we have
   $$f(gv) = \Big(\sum_i \beta_i y^i\Big)\Big(\Big(\sum_j \tilde{\beta}_j y^j\Big)\Big(\sum_k \alpha_k e_{2k+1}\Big)\Big)$$
   $$= \Big(\sum_i \beta_i y^i\Big)\Big(\sum_{j,k} \tilde{\tau}^j(\alpha_k)\tilde{\beta}_j e_{2k+2j+1}\Big) = \sum_{i,j,k} \underbrace{\tilde{\tau}^i(\tilde{\tau}^j(\alpha_k)\tilde{\beta}_j)\beta_i}_{=\tilde{\tau}^{i+j}(\alpha_k)\tilde{\tau}^i(\tilde{\beta}_j)\beta_i} e_{2(i+j+k)+1}.$$
2.
   - First we get
   $$v(fg) = \Big(\sum_i \alpha_i e_{2i+1}\Big)\Big(\Big(\sum_k \beta_k y^k\Big)\Big(\sum_l \tilde{\beta}_l y^l\Big)\Big)$$
   $$= \Big(\sum_i \alpha_i e_{2i+1}\Big)\Big(\sum_{k,l} \beta_k \tilde{\tau}^k(\tilde{\beta}_l) y^{k+l}\Big) = \sum_{i,k,l} \alpha_i \tilde{\tau}^i(\tau(\beta_k \tilde{\tau}^k(\tilde{\beta}_l))) e_{2(i+k+l)+1}.$$
   - Moreover we have
   $$(vf)g = \Big(\Big(\sum_i \alpha_i e_{2i+1}\Big)\Big(\sum_k \beta_k y^k\Big)\Big)\Big(\sum_l \tilde{\beta}_l y^l\Big)$$
   $$= \Big(\sum_{i,k} \alpha_i \tilde{\tau}^i(\tau(\beta_k)) e_{2(i+k)+1}\Big)\Big(\sum_l \tilde{\beta}_l y^l\Big)$$
   $$= \sum_{i,k,l} \underbrace{\alpha_i \tilde{\tau}^i(\tau(\beta_k))\tilde{\tau}^{i+k}(\tau(\tilde{\beta}_l))}_{\substack{= \\ \tau \text{ and } \tilde{\tau} \\ \text{commute}} \alpha_i \tilde{\tau}^i(\tau(\beta_k \tilde{\tau}^k(\tilde{\beta}_l)))} e_{2(i+k+l)+1}.$$
3. First we have to verify the "associative law"
   $$f(vg) = (fv)g \;\; \forall f, g \in L[y,\tilde{\tau}] \; \forall v \in V.$$
   - We find
   $$(fv)g = \Big(\big(\sum_i \beta_i y^i\big)\big(\sum_j \alpha_j e_{2j+1}\big)\Big)\Big(\sum_k \tilde{\beta}_k y^k\Big)$$
   $$= \Big(\sum_{i,j} \tilde{\tau}^i(\alpha_j)\beta_i e_{2(i+j)+1}\Big)\Big(\sum_k \tilde{\beta}_k y^k\Big)$$
   $$= \sum_{i,j,k} \tilde{\tau}^i(\alpha_j)\beta_i \tilde{\tau}^{i+j}(\tau(\tilde{\beta}_k)) e_{2(i+j+k)+1}$$

- and

$$\begin{aligned} f(vg) &= \Big(\sum_i \beta_i y^i\Big)\Big((\sum_j \alpha_j e_{2j+1})(\sum_k \tilde{\beta}_k y^k)\Big) \\ &= \Big(\sum_i \beta_i e_{2i+1}\Big)\Big(\sum_{j,k} \alpha_j \tilde{\tau}^j(\tau(\tilde{\beta}_k)) e_{2(j+k)+1}\Big) \\ &= \sum_{i,j,k} \underbrace{\tilde{\tau}^i(\alpha_j \tilde{\tau}^j(\tau(\tilde{\beta}_k)))\beta_i}_{=\tilde{\tau}^i(\alpha_j)\tilde{\tau}^{i+j}(\tau(\tilde{\beta}_k))\beta_i} e_{2(i+j+k)+1}. \end{aligned}$$

A straightforward calculation yields moreover that F operates central on V.

□

Lemma and Definition 7.32 *Let $\tilde{F}$ be a field and T be some $\tilde{F}$-algebra and W a T-bimodule. The semi-direct product $W \rtimes T$ is defined in the following way:*

1. *As an $\tilde{F}$-vector space $W \rtimes T = W \times T$.*
2. *The multiplication is given by:*

$$(w_1, t_1) \cdot (w_2, t_2) := (t_1 w_2 + w_1 t_2, t_1 t_2) \quad \forall (w_1, t_1), (w_2, t_2) \in W \rtimes T.$$

$W \rtimes T$ is an $\tilde{F}$-algebra, which contains the Abelian ideal $J := \{(w, 0) \mid w \in W\}$.

Proof. Cf. [Rog94, Section 4.1]. □

Theorem 7.33 *With the notations of the Lemmas 7.29 and 7.31 we get $V \rtimes B_0 \simeq V \rtimes L[y, \tilde{\tau}] \simeq B$ as F-algebras.*

Proof. We define Φ as a homomorphism of L-vector spaces in the following way on the basis of $V \rtimes L[y, \tilde{\tau}]$:

$$\begin{aligned} \Phi : (e_{2i+1}, 0) &\longmapsto \mathrm{f}_1^{2i+1} \\ \Phi : (0, y^j) &\longmapsto \mathrm{f}_1^{2j}. \end{aligned}$$

1. Since $\{(e_{2i+1}, 0), (0, y^j) \mid i, j \in \mathbb{N}\}$ and $\{\mathrm{f}_1^i \mid i \in \mathbb{N}\}$ form L-bases of $V \rtimes L[y, \tilde{\tau}]$ and B respectively and Φ provides a bijection between these bases, Φ is a well-defined isomorphism of L-vector spaces.
2. Choose $v := \sum_i v_i e_{2i+1}, w := \sum_j w_j e_{2j+1} \in V$ and $f := \sum_{\tilde{i}} \alpha_{\tilde{i}} y^{\tilde{i}}$, $g := \sum_{\tilde{j}} \beta_{\tilde{j}} y^{\tilde{j}} \in L[y, \tilde{\tau}]$.
   a) First we note

$$\begin{aligned} (v, f)(w, g) &\underset{\text{see Def. 7.32}}{=} (vg + fw, fg) \\ &= \Big(\sum_{i,\tilde{j}} \tilde{\tau}^i(\tau(\beta_{\tilde{j}})) v_i e_{2(i+\tilde{j})+1} + \sum_{j,\tilde{i}} \alpha_j \tilde{\tau}^j(w_{\tilde{i}}) e_{2(j+\tilde{i})+1}, \sum_{\tilde{i},\tilde{j}} \alpha_{\tilde{i}} \tilde{\tau}^{\tilde{i}}(\beta_{\tilde{j}}) y^{\tilde{i}+\tilde{j}}\Big) \\ &= \Big(\sum_{i,j} \big(\tilde{\tau}^i(\tau(\beta_j)) v_i + \alpha_i \tilde{\tau}^i(w_j)\big) e_{2(i+j)+1}, \sum_{\tilde{i},\tilde{j}} \alpha_{\tilde{i}} \tilde{\tau}^{\tilde{i}}(\beta_{\tilde{j}}) y^{\tilde{i}+\tilde{j}}\Big). \end{aligned}$$

b) Hence we get (per. def. of Φ):

$$\Phi((v,f)(w,g)) = \sum_{i,j}(\alpha_i\tilde{\tau}^i(w_j) + \tilde{\tau}^i(\tau(\beta_j))v_i)\,\mathrm{f}_1^{2(i+j)+1} + \sum_{\tilde{i},\tilde{j}}\alpha_{\tilde{i}}\tilde{\tau}^{\tilde{j}}(\beta_{\tilde{j}})\,\mathrm{f}_1^{2(\tilde{i}+\tilde{j})}.$$

c) On the other side we have:

$$\begin{aligned}
&\Phi((v,f))\Phi((w,g)) \\
&= \Big(\sum_i v_i\,\mathrm{f}_1^{2i+1} + \sum_{\tilde{i}}\alpha_{\tilde{i}}\,\mathrm{f}_1^{2\tilde{i}}\Big)\Big(\sum_j w_j\,\mathrm{f}_1^{2j+1} + \sum_{\tilde{j}}\beta_{\tilde{j}}\,\mathrm{f}_1^{2\tilde{j}}\Big) \\
&\underset{\text{we use } J^2=0}{=} \Big(\sum_i v_i\,\mathrm{f}_i^{2i+1}\Big)\Big(\sum_{\tilde{j}}\beta_{\tilde{j}}\,\mathrm{f}_1^{2\tilde{j}}\Big) + \Big(\sum_{\tilde{i}}\alpha_{\tilde{i}}\,\mathrm{f}_1^{2\tilde{i}}\Big)\Big(\sum_j w_j\,\mathrm{f}_1^{2j+1}\Big) \\
&\quad + \Big(\sum_{\tilde{i}}\alpha_{\tilde{i}}\,\mathrm{f}_1^{2\tilde{i}}\Big)\Big(\sum_{\tilde{j}}\beta_{\tilde{j}}\,\mathrm{f}_1^{2\tilde{j}}\Big) \\
&\underset{\text{Corollary 7.25}}{=} \sum_{i,j}\tilde{\tau}^i(\tau(\beta_{\tilde{j}}))v_i\,\mathrm{f}_1^{2(i+\tilde{j})+1} + \sum_{\tilde{i},j}\tilde{\tau}^{\tilde{i}}(w_j)\alpha_{\tilde{i}}\,\mathrm{f}_1^{2(\tilde{i}+j)+1} \\
&\quad + \sum_{\tilde{i},\tilde{j}}\tilde{\tau}^{\tilde{i}}(\beta_{\tilde{j}})\alpha_{\tilde{i}}\,\mathrm{f}_1^{2(\tilde{i}+\tilde{j})} \\
&\underset{\text{changing the indices}}{=} \sum_{i,j}\big(\tilde{\tau}^i(\tau(\beta_j))v_i + \alpha_i\tilde{\tau}^i(w_j)\big)\,\mathrm{f}_1^{2(i+j)+1} \\
&\quad + \sum_{\tilde{i},\tilde{j}}\alpha_{\tilde{i}}\tilde{\tau}^{\tilde{i}}(\beta_{\tilde{j}})\,\mathrm{f}_1^{2(\tilde{i}+\tilde{j})}.
\end{aligned}$$

□

Corollary 7.34 *The ring B is Noetherian.*

Proof. For $k = 2$ we have $B \simeq L[y,\tau]$ by Corollary 7.22. This ring is Noetherian, which is shown analogous to the proof of Hilbert's Theorem, (for this proof see [Lan93, Theorem 4.1].) So we $k \geq 3$ assume, hence $B \simeq V \rtimes L[y,\tilde{\tau}]$ by Theorem 7.33 (here we use the notations of Theorem 7.33). In particular B is a left module over the Noetherian ring $L[y,\tilde{\tau}]$. It is enough to show that B is finitely generated over $L[y,\tilde{\tau}]$. We set $b_1 := (e_1, 0)$ and $b_2 := (0,1)$. Let's fix some $\alpha \in L$. Now we find (using Corollary 7.25 and Theorem 7.33): $(0,\alpha y^{i-1})(e_1,0) = (\alpha e_{2i+1}, 0)$ for every $i \geq 1$ and $(0,\alpha y^i)(0,1) = (0,\alpha y^i)$ for every i. So B is generated by the elements b_1 and b_2 as a left-module over $L[y,\tilde{\tau}]$. □

Remark 7.35 *Let us consider the special case that $\tau^k = \tilde{\tau} = 1$ holds, we have:*

1. *$B_0 \simeq L[y,\tau^k] = L[y]$ is a commutative ring.*
2. *Let $S : V \ni e_{2i+1} \longmapsto e_{2(i+1)+1} \in V$ be the right shift on V. For $f = \sum_i \alpha_i y^i \in L[y]$ we set $f(S) := \sum_i \alpha_i S^i$ and $\tau(f) := \sum_i \tau(\alpha_i)y^i$. Then we can write the left and the right operation of $L[y]$ on V in the following ways:*
   - *Left Operation: $fv = (f(S))(v)$.*
   - *Right Operation: $vf = (\tau(f)(S))(v)$.*

7.4 Some Exact Sequences

Up to now we have thought about the cohomology ring in terms of $\mathrm{Ext}_A^i(S,S)$, in this section we want to give the counterparts of the f_i^j's in terms of exact sequences.

7.4.1 For $k = 2$

Lemma 7.36 *f_1^1 corresponds to the exact sequence*

$$\mathcal{E} := 0 \longrightarrow S \xrightarrow{\iota} A \xrightarrow{\cdot N} AN \longrightarrow 0,$$

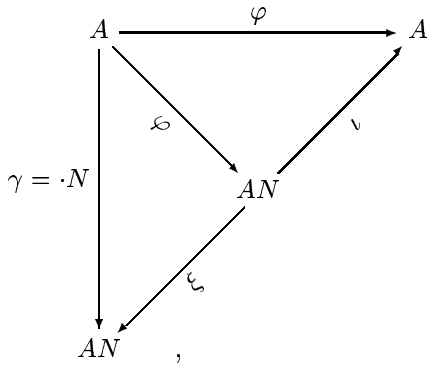
where $\iota : S \to A$ denotes the canonical embedding.

Proof. Let $\varphi : A \ni 1 \longmapsto N \in A$.

- First we note that a projective resolution of the simple module S is given by

$$\cdots\cdots \longrightarrow A \xrightarrow{\varphi} A \xrightarrow{\varphi} A \xrightarrow{\varphi} S \longrightarrow 0.$$

- We have to consider the following commutative diagram, using the proof of Theorem 7.13:



with $\xi = \mathrm{id}_{AN}$, so the correct sequence is indeed $\mathcal{E}$.

□

Then f_1^i corresponds to the sequence $\mathcal{E}^i = \underbrace{\mathcal{E} \circ \cdots \circ \mathcal{E}}_{i \text{ copies}}$ which is given by

$$0 \longrightarrow S \xrightarrow{\iota} A \xrightarrow{\cdot N} A \xrightarrow{\cdot N} A \cdots\cdots A \xrightarrow{\cdot N} S \longrightarrow 0.$$

7.4.2 For $k \geq 3$

First we set - for simplifying the notations - $S_i := A(N, -N^i)$.

Lemma 7.37 *For $1 \leq i \leq k$ there is an isomorphism of A-modules*

$$\Phi : (A \oplus AN^i)/A(N, -N^i) \longrightarrow AN^{i-1}.$$

Proof.

1. We make the following observation: For arbitrary elements $a, b \in A$ we have

$$(a, bN^i) + S_i = (a, bN^i) + b(N, -N^i) + S_i = (a + bN, 0) + S_i.$$

2. By (1) we can represent every element of $(A \oplus AN^i)/S_i$ in the form $(x,0)+S_i$ for some $x \in A$. So we set

$$\Phi : (A \oplus AN^i)/S_i \ni (x,0) + A(N,-N^i) \longmapsto xN^{i-1} \in AN^{i-1}.$$

3. Assume $(x,0)+S_i = 0$, so we find some $a \in A$ with $x = aN$ and $aN^i = 0$. By Lemma 6.8 $aN^i = 0$ if and only if $a \in AN^{k-i}$. So there is an $\tilde{a} \in A$ with $a = \tilde{a}N^{k-i}$ and $x = \tilde{a}N^{k-i}N$. We get

$$\Phi((x,0)+S_i) = xN^{i-1} = \tilde{a}N^{k-i}NN^{i-1} = \tilde{a}N^{k-i+i-1+1} = \tilde{a}N^k \underset{N^k=0}{=} 0,$$

and Φ is well-defined.

4. That Φ is a homomorphism of A-modules, is of course trivial.

5. The homomorphism Φ is obviously surjective.

6. Assume $(x,0)+S_i \in \mathrm{Ker}(\Phi)$, then $xN^{i-1} = 0$, by Lemma 6.8 $x \in AN^{k-(i-1)}$ and we find some $a \in A$ with

$$(x,0)+S_i = (aN^{k-i+1},0)+S_i \underset{aN^{k-i}N^i = aN^k = 0}{=} aN^{k-i}(N,-N^i)+S_i = 0,$$

hence $\mathrm{Ker}(\Phi) = 0$ and so Φ is injective.

□

Corollary 7.38 *For an $(a,bN^i)+A(N,-N^i) \in (A \oplus AN^i)/A(N,-N^i)$ we find some $x \in A$ with $(a,bN^{i-1})+A(N,-N^i) = (x,0)+A(N,-N^i)$.*

Proof. See the proof of Lemma 7.37. □

Lemma and Definition 7.39 *The following sequence is exact:*

$$\mathcal{E}_1 := 0 \longrightarrow AN^{k-1} \xrightarrow{\alpha} AN^{k-2} \xrightarrow{\beta} AN^{k-1} \longrightarrow 0,$$

whereby α denotes the canonical embedding and β the right multiplication with N.

Proof.

1. For $a \in A$ holds: $(aN^{k-1})\alpha\beta = aN^{k-1}\beta = aN^k = 0$, so $\mathrm{Im}(\alpha) \subset \mathrm{Ker}(\beta)$.

2. Let $aN^{k-2} \in Ker\beta$, then $aN^{k-1} = 0$; by Lemma 6.8 there is an $\tilde{a} \in A$ with $a = \tilde{a}N$, so $aN^{k-2} = \tilde{a}N^{k-1} \in \mathrm{Im}(\alpha)$ and we are done.

□

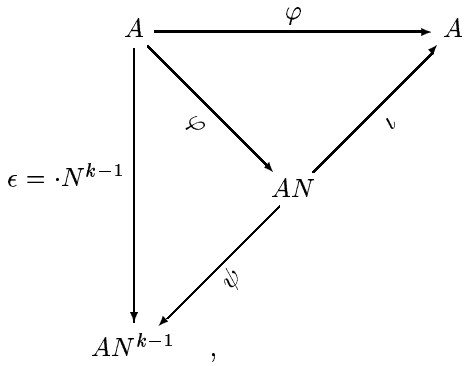
Lemma 7.40 *The homomorphism f_1^1 corresponds to the exact sequence $\mathcal{E}_1$.*

Proof.

1. We set $\varphi : A \ni a \longmapsto aN \in A$ and $\tilde{\varphi} : A \ni a \longmapsto aN^{k-1} \in A$. We know that a projective resolution of S is given by the following exact sequence:

$$\cdots\cdots \longrightarrow A \xrightarrow{\varphi} A \xrightarrow{\tilde{\varphi}} A \xrightarrow{\varphi} A \xrightarrow{\tilde{\varphi}} S \longrightarrow 0.$$

2. The proof of Theorem 7.13 tells us, how $\mathcal{E}_1$ is constructed. First we have to consider the following commutative diagram



with $\psi : AN \ni N \longmapsto N^{k-1} \in AN^{k-1}$.

3. A representative $\tilde{\mathcal{E}}$ of $[\mathcal{E}_1]$ is given through the following pushout diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & AN & \xrightarrow{\iota} & A & \xrightarrow{\tilde{\varphi}} & AN^{k-1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \tilde{\psi}} & & \| & & \\ \tilde{\mathcal{E}} = 0 & \longrightarrow & AN^{k-1} & \xrightarrow{\xi_1} & X & \xrightarrow{\xi_2} & AN^{k-1} & \longrightarrow & 0. \end{array}$$

The A-module X is the pushout of the homomorphisms ψ and ι, hence

$$X = (A \oplus AN^{k-1})/S_{k-1} \underset{\text{Lemma 7.37}}{\overset{\Phi}{\simeq}} AN^{k-2},$$

with $\Phi : (x,0) + S_{k-1} \longmapsto xN^{k-2}$ (see Corollary 7.38).

4. Now let us determine the maps ξ_1 and ξ_2. We set

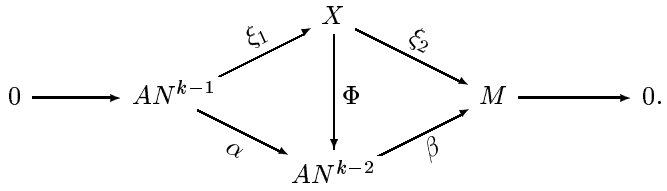
$$\xi_1 : AN^{k-1} \ni x \longmapsto (0,x) + S_{k-1} \in (A \oplus AN^{k-1})/S_{k-1}.$$

We note that ξ_1 is the canonical map into the pushout, so in particular $\psi\xi_1 = \iota\tilde{\psi}$ ($\tilde{\psi}$ is the other canonical map into the pushout). We set

$$\begin{aligned} \xi_2 : (A \oplus AN^{k-1})/S_{k-1} &\longrightarrow AN^{k-1} \\ (x,0) + S_{k-1} &\longmapsto xN^{k-1}. \end{aligned}$$

That ξ_2 is well-defined and ξ_2 and ξ_1 make the diagram commutative such that the bottom row is exact can be found in [Wei97, Proof of Theorem 3.4.3].

5. When we can show that the following diagram is commutative, we are done:



- For $a \in A$ we have

$$\begin{aligned} (aN^{k-1}\xi_1)\Phi = \big((0,aN^{k-1}) + S_{k-1}\big)\Phi &\underset{\text{obvious}}{=} \big((aN,0) + S_{k-1}\big)\Phi \\ = aNN^{k-2} = aN^{k-1} &\underset{\alpha \text{ is the can. embedding}}{=} (aN^{k-1})\alpha. \end{aligned}$$

- Furthermore we have

$$\big((x,0)+S_{k-1}\big)\Phi\beta = xN^{k-2}\beta = xN^{k-1} = \big((x,0)+S_{k-1}\big)\xi_2.$$

□

Lemma 7.41 *An exact sequence which corresponds to* f_1^2 *is given by*

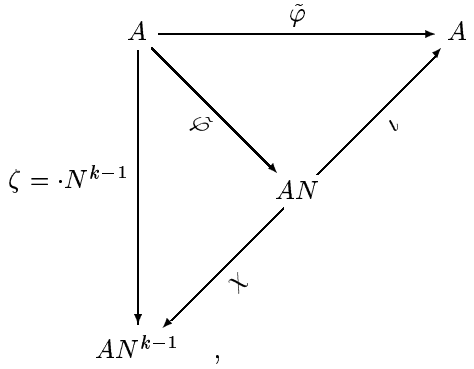
$$\mathcal{E}_2 := 0 \longrightarrow AN^{k-1} \xrightarrow{\iota} A \xrightarrow{\varphi} A \xrightarrow{\tilde{\varphi}} AN^{k-1} \longrightarrow 0,$$

with the same notation as above (and ι *denotes the canonical embedding).*

Proof. We use again the explicit rule given in the proof of Theorem 7.13 to construct the exact sequence $\mathcal{E}_2$. We consider again the sequence

$$\cdots\cdots \longrightarrow A \xrightarrow{\varphi} A \xrightarrow{\tilde{\varphi}} A \xrightarrow{\varphi} A \xrightarrow{\tilde{\varphi}} S \longrightarrow 0,$$

which is a projective resolution of S. We note that the following diagram is commutative:



with $\chi = \mathrm{id}_{AN^{k-1}}$, so we don't have to construct some pushout diagram and get immediately that the sequence $\mathcal{E}_2$ is the correct one. □

Now let us determine the remaining sequences associated to the f_1^j's for $j \geq 3$. We have to distinguish two cases:

Case 1): j is even: Then $j = 2\tilde{j}$ for some $\tilde{j} \in \mathbb{N}$, hence $\mathrm{f}_1^j = \mathrm{f}_1^{2\tilde{j}} = \big(\mathrm{f}_1^2\big)^{\tilde{j}}$. So if $\mathcal{E}_2$ corresponds to f_1^2, the sequence $\underbrace{\mathcal{E}_2 \circ \cdots \circ \mathcal{E}_2}_{\tilde{j}\text{ copies}}$ corresponds to f_1^j. Using the Yoneda splice we conclude that our sequence is:

$$0 \longrightarrow S \xrightarrow{\iota} A \xrightarrow{\varphi} A \xrightarrow{\tilde{\varphi}} A \cdots\cdots A \xrightarrow{\varphi} A \xrightarrow{\tilde{\varphi}} S \longrightarrow 0.$$

Case 2): j is odd: Then $j = 2\tilde{j}+1$ for some $\tilde{j} \in \mathbb{N}$, hence $\mathrm{f}_1^j = \mathrm{f}_1^1 \cdot \big(\mathrm{f}_1^2\big)^{\tilde{j}}$, so the corresponding sequence is $\mathcal{E}_1 \circ \underbrace{\mathcal{E}_2 \circ \cdots \circ \mathcal{E}_2}_{\tilde{j}\text{ copies}}$. Using the Yoneda splice and case 1) we obtain the following exact sequence:

$$0 \longrightarrow S \xrightarrow{\iota} AN^{k-2} \xrightarrow{\cdot N} A \xrightarrow{\varphi} A \xrightarrow{\tilde{\varphi}} A \cdots\cdots S \longrightarrow 0.$$

8 Separable Algebras and Orders

Throughout this chapter let R – if not otherwise stated – be an arbitrary commutative Noetherian ring and Γ an R-algebra.

8.1 The Classical Definition and the Enveloping Algebra

There is a well known definition for algebras over fields (Cf. [Rei75, Paragraph 7c]):

Definition 8.1 *Let K be an arbitrary field and A a K-algebra which is finite dimensional as a vector space over K. We call A separable over K, if A satisfies the following conditions:*

1. *A is semi simple over K, this yields - with Wedderburn's Structure Theorem - that we have*
$$A \simeq M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k),$$
for some natural numbers $n_1, \ldots, n_k \in \mathbb{N}$ and skewfields $D_1, \ldots, D_k$.

2. *The center L_i of D_i is a separable field extension of K for every $1 \leq i \leq k$.*

There is a homological characterization of separable algebras. We need some definitions.

Definition 8.2 1. *The enveloping algebra Γ^e of Γ is defined to be $\Gamma \otimes_R \Gamma^{op}$.*

2. *We will - unless otherwise stated - view Γ as a Γ^e-module in the following way $(\gamma_1 \otimes \gamma_2)\gamma_3 := \gamma_1\gamma_3\gamma_2$ for $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$.*

3. *The map*
$$\begin{aligned} \varepsilon : \Gamma \otimes_R \Gamma^{op} &\longrightarrow \Gamma \\ \sum_{i=1}^{n} \gamma_i \otimes \tilde{\gamma}_i &\longmapsto \sum_{i=1}^{n} \gamma_i\tilde{\gamma}_i \end{aligned}$$
is called the augmentation map of Γ.

4. *The kernel of ε is denoted by $I_R(\Gamma)$ and is called the augmentation ideal of Γ. The exact sequence of Γ-modules*
$$\mathcal{A}(\Gamma) := 0 \longrightarrow I_R(\Gamma) \longrightarrow \Gamma^e \xrightarrow{\varepsilon} \Gamma \longrightarrow 0$$
is called the augmentation sequence of Γ.

5. *We call Γ separable over R if the sequence $\mathcal{A}(\Gamma)$ is split as a sequence of Γ^e-modules.*

Remark 8.3 *The Augmentation Sequence of Γ is a projective presentation of Γ as a module over Γ^e.*

Corollary 8.4 *Equivalent are:*

1. Γ *is separable over* R.
2. Γ *is projective as a* Γ^e*-module.*

Proof. Immediately from Remark 8.3. □

If R is a field we have

Lemma 8.5 *Let* K *be a field and* A *a* K*-algebra which is finite dimensional as a vector space over* K*. Equivalent are:*

1. *The algebra* A *is separable in the sense of Definition 8.1.*
2. *The augmentation sequence of* A *is split as a sequence of* A^e*-modules, i.e.* A *is separable in the sense of Definition 8.2.*

Proof. Cf. [Rei75, Theorem 7.20] □

Lemma 8.6 *Let* Γ *be separable over* R *and* $\varphi : R \longrightarrow S$ *be some ring homomorphism. Then* $S \otimes_R \Gamma$ *is a separable* S*-algebra.*

Proof. Cf. [DI71, Proposition 1.6]. □

Lemma 8.7 *For the* R*-algebra* Γ *are equivalent:*

1. Γ *is separable over* R.
2. $\Gamma_{\mathfrak{m}}$ *is separable over* $R_{\mathfrak{m}}$ *for every maximal ideal* $\mathfrak{m}$ *of* R.
3. $\Gamma/\mathfrak{m}\Gamma$ *is separable over* $R/\mathfrak{m}$ *for every maximal ideal* $\mathfrak{m}$ *of* R.

Proof. Cf. [DI71, Theorem 7.1]. □

Lemma 8.8 *Assume that* R *is a local ring with maximal ideal* $\mathfrak{m}$ *and a perfect residue class field* $k = R/\mathfrak{m}$*; moreover assume that* Γ *is finitely generated as an* R*-module. The following are equivalent:*

1. Γ *is separable over* R.
2. Γ *is unramified over* R*, i.e.* $rad(\Gamma) = \mathfrak{m}\Gamma$.

Proof. (1) $\Longrightarrow$ (2) : Since R is a local ring we have - using Nakayama's Lemma - $\mathfrak{m}\Gamma \subset \mathrm{rad}(\Gamma)$. Lemma 8.7 yields that $\Gamma/\mathfrak{m}\Gamma$ is separable over the field k, hence $\Gamma/\mathfrak{m}\Gamma$ is in particular a semi-simple algebra by Lemma 8.5 and so we conclude $\mathrm{rad}(\Gamma) \subset \mathfrak{m}\Gamma$. So we get $\mathrm{rad}(\Gamma) = \mathfrak{m}\Gamma$ and Γ is unramified over R.

(2) $\Longrightarrow$ (1) : We have $\mathrm{rad}(\Gamma) = \mathfrak{m}\Gamma$. We have assumed that Γ is finitely generated as an R-module, so $\Gamma/\mathfrak{m}\Gamma$ is finitely generated over the field k. We have $\mathrm{rad}(\Gamma/\mathfrak{m}A\Gamma) = \mathrm{rad}(\Gamma/\mathrm{rad}(\Gamma)) = 0$, so $\Gamma/\mathfrak{m}\Gamma$ is an Artin algebra with vanishing radical over a field, hence semi-simple. By Wedderburn's Structure Theorem we find skewfields $D_1, \ldots, D_k$ and $n_1, \ldots, n_k \in \mathbb{N}$ with

$$\Gamma/\mathfrak{m}\Gamma \simeq M_{n_1}(D_1) \times M_{n_k}(D_k).$$

By assumption k is a perfect field, so the centers of the D_i's are separable extensions of K, Lemma 8.5 yields, that $\Gamma/\mathfrak{m}\Gamma$ is separable over $R/\mathfrak{m}$. Since R is local, we conclude with Lemma 8.7, that Γ is separable over R. □

8.2 Hochschild Cohomology

Definition 8.9 *Let M be a Γ^e-module. We set $\mathrm{H}^n_{\Gamma^e}(\Gamma, M) := \mathrm{Ext}^n_{\Gamma^e}(\Gamma, M)$ and call it the n-th Hochschild cohomology group of Γ with values in M.*

Remark 8.10 *For our purpose the first Hochschild Cohomology group will be enough.*

There is another characterization of the first Hochschild cohomology group. First we need a remark and a afterwards a definition.

Remarks 8.11 *1. Let M be some Γ^e-module. Then M becomes a bimodule for the R-algebra Γ via the following definitions:*

- $\gamma m := (\gamma \otimes 1)m \quad \forall \gamma \in \Gamma \, \forall m \in M.$
- $m\gamma := (1 \otimes \gamma)m \quad \forall \gamma \in \Gamma \, \forall m \in M.$

We note that for $r \in R$ and $m \in M$ holds: $rm = mr$.

2. Let N be some bimodule for the R-algebra Γ (this means in particular that every $r \in R$ operates central on N). Then N becomes a Γ^e-module by setting:

$$(\gamma \otimes \tilde{\gamma})n := \gamma n \tilde{\gamma} \quad \forall \gamma, \tilde{\gamma} \in \Gamma \, \forall n \in N.$$

3. With the last two points we can conclude that there is a natural equivalence between the category of Γ^e-modules and the category of Γ-bimodules.

Definition 8.12 *Let M be an arbitrary Γ^e-module and $\varphi \in \mathrm{Hom}_R(\Gamma, M)$.*

1. φ is called a 1-cocycle or a derivation if we have

$$\varphi(\gamma\tilde{\gamma}) = \gamma\varphi(\tilde{\gamma}) + \varphi(\gamma)\tilde{\gamma} \quad \forall \gamma, \tilde{\gamma} \in \Gamma.$$

The R-module of derivations will be denoted by $\mathrm{C}^1_{\Gamma^e}(M)$.

2. φ is called a 1-coboundary or a inner derivation if there is an element $m \in M$ with

$$\varphi(\gamma) = \gamma m - m\gamma \quad \forall \gamma \in \Gamma.$$

The R-module of inner derivations will be denoted by $\mathrm{B}^1_{\Gamma^e}(M)$.

Remark 8.13 *We have obviously $\mathrm{B}^1_{\Gamma^e}(M) \subset \mathrm{C}^1_{\Gamma^e}(M)$.*

Theorem 8.14 *There is an isomorphism of R-modules*

$$\Phi : \mathrm{H}^1_{\Gamma^e}(\Gamma, M) \longrightarrow \mathrm{C}^1_{\Gamma^e}(M) / \mathrm{B}^1_{\Gamma^e}(M).$$

Proof. Cf. [Rog94, 4, Proposition 2]. □

Observation 8.15 *Let M and N be Γ-modules. The Abelian group $\mathrm{Hom}_R(M, N)$ becomes a Γ-bimodule by:*

- $(\gamma\varphi)(m) := \gamma\varphi(m) \quad \forall \varphi \in \mathrm{Hom}_R(M, N) \, \forall \gamma \in \Gamma \, \forall m \in M.$
- $(\varphi\gamma)(m) := \varphi(\gamma m) \quad \forall \varphi \in \mathrm{Hom}_R(M, N) \, \forall \gamma \in \Gamma \, \forall m \in M.$

Proof. A straightforward calculation. □

Theorem 8.16 *Let M and N be Γ-modules such that M is projective over R. There is an isomorphism*

$$\Phi : \mathrm{Ext}^1_\Gamma(M,N) \longrightarrow \mathrm{H}^1_{\Gamma^e}(\Gamma, \mathrm{Hom}_R(M,N)).$$

Proof. Cf. [Rog94, 6, Theorem 2]. □

Theorem 8.17 *Let Γ a separable R-algebra and M a Γ-module which is projective over R. Then M is also projective as a Γ-module.*

Proof. Assume that M is a Γ-module which is projective over R. Let N be an arbitrary Γ-module. We can apply Theorem 8.16 to conclude that there is an isomorphism $\mathrm{Ext}^1_\Gamma(M,N) \simeq \mathrm{H}^1_{\Gamma^e}(\Gamma, \mathrm{Hom}_R(M,N))$. Since Γ is separable over R we get $\mathrm{H}^1_{\Gamma^e}(\Gamma, \mathrm{Hom}_R(M,N)) = 0$ and so $\mathrm{Ext}^1_\Gamma(M,N) = 0$ what implies that M is projective over Γ, since N was arbitrary. □

We can give another nice homological characterization of separable algebras which is closer to a classical theorem we will state first:

Theorem 8.18 *Let F be a field and A an F-algebra which is finite dimensional over F. Equivalent are:*

1. *A is separable over F.*
2. *There is a finite separable extension E of F, such that $E \otimes_F A$ is isomorphic to a finite product of matrix rings over E.*
3. *$E \otimes_F A$ is semi-simple for every field extension E of F.*

Proof. Cf. [Rei75, Theorem 7.18]. □

Definition 8.19 *Let S be some commutative ring and B an S-algebra. We call B S-hereditary, if B satisfies the following property: Every B-module M which is projective over S is also projective over B.*

Remark 8.20 *For an algebra A over some field F are equivalent:*

1. *A is semi-simple.*
2. *A is F-hereditary.*

Theorem 8.21 *For an R-algebra Γ which is finitely generated as an R-module are equivalent:*

1. *Γ is separable over R.*
2. *For every ring homomorphism $\varphi : R \longrightarrow S$ the S-algebra $S \otimes_R \Gamma$ is S-hereditary.*

Proof. (1) $\Longrightarrow$ (2) : Let Γ be separable over R and $\varphi : R \longrightarrow S$ be some ring homomorphism. By 8.6 the S-algebra $S \otimes_R \Gamma$ is separable over S, hence it is S-hereditary by Theorem 8.17.

(2) $\Longrightarrow$ (1) : We fix an arbitrary maximal ideal $\mathfrak{m}$ of R and set $\mathfrak{k} := R/\mathfrak{m}$. Then by assumption $\Gamma/\mathfrak{m}\Gamma$ is $\mathfrak{k}$-hereditary, hence semi-simple by Remark 8.20. Since Γ is finitely generated over R we get that $\Gamma/\mathfrak{m}\Gamma$ is finite dimensional as vector space over $\mathfrak{k}$. Now let $\mathfrak{l}/\mathfrak{k}$ be an arbitrary field extension, in particular there exists a ring homomorphism $\varphi : R \longrightarrow \mathfrak{l}$. By assumption on Γ we can conclude that

$\mathfrak{l} \otimes_{\mathfrak{k}} \Gamma/\mathfrak{m}\Gamma = \mathfrak{l} \otimes_R \Gamma$ is $\mathfrak{l}$-hereditary, hence semi-simple by Remark 8.20. So an application of Theorem 8.18 yields that $\Gamma/\mathfrak{m}\Gamma$ is separable $\mathfrak{k}$. Since $\mathfrak{m}$ was arbitrary we get - using Lemma 8.7 - that Γ is separable over R. □

Theorem 8.22 *Let R be a local factorial Krull-Domain and Λ some R-order. Let $\mathfrak{p} \in ht^1(R)$. If $\Lambda_{\mathfrak{p}}$ is separable, $\Lambda_{\mathfrak{p}}$ is hereditary.*

Proof. By Serre's characterization of integral closed Noetherian rings we know that $R_{\mathfrak{p}}$ is a discrete valuation domain. Let M be an arbitrary $\Lambda_{\mathfrak{p}}$-lattice. Then M is a torsion free $R_{\mathfrak{p}}$-module, hence projective over the discrete valuation domain $R_{\mathfrak{p}}$. Since $\Lambda_{\mathfrak{p}}$ is a separable $R_{\mathfrak{p}}$-algebra we can use Theorem 8.17 to deduce that M is also projective as $\Lambda_{\mathfrak{p}}$-module. Then we are done by using [Rei75, Corollary 10.7].
□

8.3 The Higman Ideal

There is an ideal of R - the so called Higman ideal - which measures how far away the R-algebra Γ is from being separable over R. Before we can define this ideal we need some lemmas.

Lemma 8.23 *Let S be an arbitrary commutative ring and B some S-algebra. Choose two B-modules M and N. Moreover let*

$$\mathcal{P} = 0 \longrightarrow \Omega \longrightarrow P \longrightarrow M \longrightarrow 0$$

be a projective presentation of M as a B-module. Then we have an inclusion

$$Ann_S(\mathrm{Ext}^1_B(M, \Omega)) \subset Ann_S(\mathrm{Ext}^1_B(M, N)).$$

Proof.

- We choose an arbitrary element $[\mathcal{E}] \in \mathrm{Ext}^1_B(M, N)$. By Theorem [Rot79, Theorem 7.19] there is some $\varphi \in \mathrm{Hom}_B(\Omega, N)$ with $[\mathcal{E}] = [\mathcal{P}\varphi]$.
- Now choose some $s \in \mathrm{Ann}_S(\mathrm{Ext}^1_B(M, \Omega))$, so in particular $x[\mathcal{P}] = 0$, hence $x[\mathcal{E}] = x[\mathcal{P}\varphi] = 0$ and we are done.

□

Lemma 8.24 *The following ideals of R coincide:*

1. $\bigcap_{M\ \Gamma^e-module} Ann_R(\mathrm{H}^1_{\Gamma^e}(\Gamma, M))$
2. $Ann_R(\mathrm{H}^1_{\Gamma^e}(\Gamma, I(\Gamma)))$

Proof.

- Since $I(\Gamma)$ is a module for the enveloping algebra Γ^e we have of course the inclusion:

$$\bigcap_{M\ \Gamma^e-\mathrm{module}} \mathrm{Ann}_R(\mathrm{H}^1_{\Gamma^e}(\Gamma, M)) \subset \mathrm{Ann}_R(\mathrm{H}^1_{\Gamma^e}(\Gamma, I(\Gamma))).$$

- The other inclusion is a trivial consequence of Lemma 8.23.

□

Definition 8.25 *The ideal of Lemma 8.24 is called the Higman ideal of* Γ *and we denote it by* $\mathcal{H}_R(\Gamma)$.

Lemma 8.26 *The following are equivalent:*

1. Γ *is separable over* R.
2. $\mathcal{H}_R(\Gamma) = R$ *holds.*

Proof. By Corollary 8.4 Γ is separable over R if and only if Γ is a projective module over Γ^e. But obviously Γ is projective over Γ^e if and only if the augmentation sequence of Γ is split as a sequence of Γ^e-modules; this equivalent to the fact that $1 \in \mathrm{Ann}_R(\mathrm{Ext}^1_{\Gamma^e}(\Gamma, I(\Gamma)))$ holds and so we are done. □

Proposition 8.27 *Let* M *be a finitely generated* R*-module. For every multiplicative set* $S \subset R$ *we have an equality* $S^{-1}Ann_R(M) = Ann_{S^{-1}R}(S^{-1}M)$.

Proof.

- Obviously we have $S^{-1}\mathrm{Ann}_R(M) \subset \mathrm{Ann}_{S^{-1}R}(S^{-1}M)$.
- Now choose $\{m_1, \ldots, m_n\}$ to be some generating system of M as an R-module. Surely $S^{-1}M$ is generated as $S^{-1}R$-module by the elements $\frac{m_1}{1}, \ldots, \frac{m_n}{1}$. Assume that $\frac{r}{s} \in \mathrm{Ann}_{S^{-1}R}(S^{-1}M)$ holds. So for every $1 \leq i \leq n$ we have $\frac{r}{s}\frac{m_i}{1} = 0$, hence for every i we find some element $s_i \in S$ with $s_i r m_i = 0$. We set $\tilde{s} := \Pi_{i=1}^n s_i$ and find $\tilde{s}rm_i = 0$ for every i, so $\tilde{s}r \in \mathrm{Ann}_S(M)$ and we are done.

□

Lemma 8.28 *Let us assume that* Γ *is finitely generated as an* R*-module and let* $S \subset R$ *be a multiplicative set. Then we have an equality* $S^{-1}\mathcal{H}_R(\Gamma) = \mathcal{H}_{S^{-1}R}(S^{-1}\Gamma)$.

Proof. This is an easy consequence from Lemma 8.24 and Proposition 8.27.

□

Corollary 8.29 *If* Γ *is finitely generated as* R*-module and* R *is in addition an integral domain with field of fractions* K *such that* $A := K\Gamma$ *is separable over* K *then* $\mathcal{H}_R(\Gamma) \neq 0$ *holds.*

Proof. By Lemma 8.29 we have $K\mathcal{H}_R(\Gamma) = \mathcal{H}_K(A)$. Since A is separable over K an application of Lemma 8.26 yields $\mathcal{H}_K(A) = K$ and so $\mathcal{H}_R(\Gamma) \neq 0$. □

Lemma 8.30 *Let* R *be a Krull Domain with field of fractions* K. *Moreover let* Λ *be an* R*-order in a separable* K*-algebra* A. *Then* $\Lambda_\mathfrak{p}$ *is not separable over* $R_\mathfrak{p}$ *for only finitely many prime ideals* $\mathfrak{p}$ *in* $ht^1(R)$.

Proof. Since Λ is an R-order in a separable K-algebra an application of Lemma 8.29 yields that $\mathcal{H}_R(\Lambda) \neq 0$ holds. So we can choose some element $0 \neq a \in \mathcal{H}_R(\Gamma)$. By assumption R is a Krull domain, so a is contained in at most finitely many elements $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in \mathrm{ht}^1(R)$. Choose an arbitrary element $\mathfrak{p} \in \mathrm{ht}^1(R) \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. So we find that is a not an element of $\mathfrak{p}$, hence $\frac{a}{1}$ is a unit in $R_\mathfrak{p}$. By Lemma 8.28 we have $\frac{a}{1} \in \left(\mathcal{H}_R(\Lambda)\right)_\mathfrak{p} = \mathcal{H}_{R_\mathfrak{p}}(\Lambda_\mathfrak{p})$, so $\mathcal{H}_{R_\mathfrak{p}}(\Lambda_\mathfrak{p}) = R_\mathfrak{p}$ holds, which yields – by Lemma 8.26 – that $\Lambda_\mathfrak{p}$ *is separable* over $R_\mathfrak{p}$. □

9 The classical one-dimensional case

We recall here first some results about the set of two-sided ideals in maximal orders over discrete valuation Domains. These results will allow us to deduce some information about the two-sided ideals in a maximal order over a ground ring of arbitrary dimension by passing over to localizations at prime ideals of height one. Then we will state the most important results about ideals in maximal orders over Dedekind domains, which are generalized by our results. We will follow [Rei75, Chapters 17-20]. For the Sections 9.1 and 9.2 let us assume that R is a discrete valuation domain (for short a dvd) with maximal ideal $\mathfrak{p} = \pi R$, where π is some prime element of R.

9.1 The complete case

In this section we assume that R is complete with respect to the π-adic topology. Let us fix some more notations: By K we denote the field of fractions of R. We assume that D is a skewfield with center K and that D is of finite K-dimension. Let Δ be the unique maximal R-order in D, we set π_D to be a prime element of Δ. For the notation we refer to Chapter 2.2. Moreover let $1 \leq r$ be in $\mathbb{N}$.

Theorem 9.1 *We set $\Lambda := M_r(\Delta)$ and $A := M_r(D)$.*

1. *Λ is a maximal R-order in A and all two-sided ideals of Λ are given by the ideals ${\pi_D}^n\Lambda = (\pi_D\Lambda)^n$. In particular Λ has a unique maximal two-sided ideal $I := \pi_D\Lambda$ and all two-sided ideals of Λ are powers of I.*
2. *The maximal R-orders in A are exactly the orders $u\Lambda u^{-1}$, where u runs through the units of A.*
3. *The maximal R-orders in A are left and right hereditary rings and all one-sided ideals of these rings are principal.*

Proof. The proof uses heavily the structure theory of Δ as we outlined it in Chapter 2.2 and the Morita Theorems for passing over from Δ to Λ. We note that the fact that R is complete is crucial for using the results of chapter 2.2. For details we refer to [Rei75, Theorem 17.3]. □

The last Theorem contained statements about maximal two-sided ideals, the next Theorem states results about one-sided maximal ideals.

Theorem 9.2 *Let Λ as in Theorem 9.1. We set $\bar{\Lambda} := \Lambda/rad(\Lambda) \simeq M_r(\bar{\Delta})$.*

1. *The rule $J \longmapsto \bar{J} = \frac{J+rad(\Lambda)}{rad(\Lambda)}$ induces a one-to-one correspondence between the maximal right ideals of Λ and the maximal right ideals of $\bar{\Lambda}$. For a maximal right ideal J of Λ we have an isomorphism $\Lambda/J \simeq \bar{\Lambda}/\bar{J}$.*
2. *We set $x_1 := \begin{pmatrix} \pi_D & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$. Then $x_1\Lambda$ is a maximal right ideal of Λ and the ideals $\{ux_1\Lambda u^{-1} \mid u \text{ a unit of } \Lambda\}$ are all maximal right ideals of Λ.*

3. *For $x \in \Lambda$ are equivalent:*
   a) *$x\Lambda$ is a maximal right ideal of Λ.*
   b) *Λx is a maximal left ideal of Λ.*

Proof. The main idea of the proof is that we think about Δ as a non-commutative discrete valuation domain and that we can imitate the elementary divisor algorithm which is well-known for the commutative case. For more details the reader should consult [Rei75, Theorem 17.8]. □

9.2 The local case

Now we will drop the assumption that R is complete with respect to the π-adic topology. The results of the last subsections are now used to deduce some informations about maximal orders over arbitrary discrete valuation domains. By K we denote once again the field of fractions of R. Moreover let B be a central simple K-algebra. We use $\hat{\cdot}$ to denote π-adic completions.

By using that Ext-Groups are well-behaved under completions we get the

Theorem 9.3 *Every maximal R-order in B is left and right hereditary.*

There is another useful tool to gain informations in the non complete case

Theorem 9.4 *Let Λ be some R-algebra which is assumed to be finitely generated as R-module. We set $\bar{\Lambda} := \Lambda/\pi\Lambda$.*

1. *We have for every $s \in \mathbb{N}$ an isomorphism $\Lambda/\pi^s\Lambda \simeq \hat{\Lambda}/\pi^s\hat{\Lambda}$.*
2. *There are isomorphisms of rings $\Lambda/rad(\Lambda) \simeq \bar{\Lambda}/rad(\bar{\Lambda}) \simeq \hat{\Lambda}/rad(\hat{\Lambda})$.*
3. *Let M and N be two finitely generated Λ-modules. Equivalent are:*
   a) *$M \simeq N$ as Λ-modules.*
   b) *There is an isomorphism of $\hat{\Lambda}$-modules $\hat{M} \simeq \hat{N}$.*

Proof. Cf. [Rei75, Theorem 18.2]. □

For our purpose the most important result in the local case is the following theorem.

Theorem 9.5 *Let Λ be a maximal R-order in B. Then Λ has a unique maximal two sided ideal $\mathfrak{P}$, which is given by $\mathfrak{P} = rad(\hat{\Lambda}) \cap \Lambda$. Moreover we get*

1. *$\mathfrak{P} = rad(\Lambda)$, so in particular $rad(\Lambda)$ is a maximal two-sided ideal of Λ.*
2. *Every two-sided ideal of Λ is a power of $\mathfrak{P}$.*
3. *$rad(\hat{\Lambda}) = \hat{\mathfrak{P}}$.*

Proof. The proof is an application of Theorem 9.4. The details can be found in [Rei75, Theorem 18.3]. □

Definition 9.6 *A two-sided Λ-ideal in B is a two-sided Λ-module which is contained in B and which is finitely generated as an R-module.*

Definition 9.7 *Let M and N be two-sided Λ-ideals in B.*

1. $M \cdot N := MN = {}_R\langle mn \mid m \in M, n \in N\rangle$.
2. $M^{-1} := \{x \in B \mid Mx \subset \Lambda\}$.

Theorem 9.8 *The set of two-sided Λ-ideals in B is an infinite cyclic group with generator $\mathfrak{P}$ in particular is every two sided Λ-ideal in B of the form $\mathfrak{P}^z$ for some integer $z \in \mathbb{Z}$.*

Proof. Cf. [Rei75, Theorem 19.3]. □

Remarks 9.9
1. *There is a unique $e \in \mathbb{N}$ with the property that $\mathfrak{P}^e = \mathfrak{p}\Lambda$ holds, where $\mathfrak{p} := \pi R$. This e is called the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$.*
2. *The inverse of $\mathfrak{P}$ is given by $\mathfrak{P}^{-1} = \pi^{-1}\mathfrak{P}^{e-1}$. This could also been used as a definition for $\mathfrak{P}^{-1}$ without Definition 9.7, but we need this definition later on in a more general framework.*

9.3 Prime Ideals of Orders

From now on we assume that R is a Dedekind Domain with field of fractions K, we do not assume longer that R is local. Moreover let B be a central simple K-algebra.

Definition 9.10 *Let Γ be an arbitrary ring. A proper two-sided ideal $\mathfrak{P}$ of Γ is called a prime ideal, if for every pair I and J of two-sided ideals of Γ we have:*

$$IJ \subset \mathfrak{P} \implies I \subset \mathfrak{P} \text{ or } J \subset \mathfrak{P}.$$

Remarks 9.11
1. *Prime ideals in the sense of Definition 9.10 play an important role in the theory of noncommutative Noetherian rings (see for example [MR87]).*
2. *Definition 9.10 is too general for orders, so for orders there will be a slightly different Definition for prime ideals.*
3. *If Γ is a commutative ring Definition 9.12 is the standard definition of a prime ideal.*

Definition 9.12 *Let Γ be an R-order in B. A two sided ideal $\mathfrak{P}$ of Γ will be a called a prime ideal if it is a prime ideal in the sense of Definition 9.10 and it is a full R-lattice, i.e. $K\mathfrak{P} = B$ holds.*

Observation 9.13 *If $\mathfrak{P}$ is a prime ideal of some R-order Γ the ideal $\mathfrak{p} := \mathfrak{P} \cap R$ of R is a non-zero prime ideal of the commutative ring R.*

The next Lemma is just correct for Dedekind Domains, to stress this fact, we will give the proof for this Lemma. In Chapter 11 we will see what the correct formulation in higher dimensions is.

Lemma 9.14 *Let Λ be a maximal R-order in B. For a proper two-sided ideal $\mathfrak{P}$ of Λ are equivalent:*

1. *$\mathfrak{P}$ is a prime ideal of Λ.*
2. *$\mathfrak{P}$ is a maximal two-sided ideal of Λ.*

Proof. (1) $\Longrightarrow$ (2): We set $\mathfrak{p} := \mathfrak{P} \cap R$. By Observation 9.13 $\mathfrak{p}$ is a non-zero prime ideal of the Dedekind Domain R, hence a maximal ideal. So $\mathfrak{k} := R/\mathfrak{p}$ is a field and $\bar{\Lambda} := \Lambda/\mathfrak{P}$ is a $\mathfrak{k}$-algebra of finite $\mathfrak{k}$-dimension. So $\bar{\Lambda}$ is an Artin algebra. The fact that $\mathfrak{P}$ is a prime ideal implies that $\mathrm{rad}(\bar{\Lambda}) = 0$ holds. Using again that $\mathfrak{P}$ is prime in combination with Wedderburn's Structure Theorem we deduce that $\bar{\Lambda}$ is a skewfield and so $\mathfrak{P}$ is a maximal two-sided ideal of Λ.

(2) $\Longrightarrow$ (1): Now let us assume that $\mathfrak{P}$ is a maximal two-sided ideal of Λ. Moreover let us assume that there is a pair of two-sided ideals S and T of Λ with $ST \subset \mathfrak{P}$ both neither $S \subset \mathfrak{P}$ nor $T \subset \mathfrak{P}$ is satisfied. We get - using that $\mathfrak{P}$ is a maximal two-sided ideal - $S + \mathfrak{P} = \Lambda$ and $T + \mathfrak{P} = \Lambda$. An easy calculation - based on $ST \subset \mathfrak{P}$ yields $\mathfrak{P} = \Lambda$, a contradiction. □

Remark 9.15 *The proof of Lemma 9.14 shows that a proper maximal two-sided ideal is always a prime ideal. For the other direction we have use that $\Lambda/\mathfrak{P}$ is of finite length over $R/\mathfrak{p}$, which is based on the fact that R is a Dedekind domain.*

Lemma 9.16 *There is a one-to-one correspondence between the prime ideals $\mathfrak{p}$ of R and the prime ideals $\mathfrak{P}$ of Λ, which is given by $\mathfrak{p} := \mathfrak{P} \cap R$. For a prime ideal $\mathfrak{P}$ of Λ we have $\mathfrak{P} = rad(\Lambda_{\mathfrak{p}}) \cap \Lambda$.*

Proof. Cf. [Rei75, Theorem 22.4]. □

Definition 9.17 *If $\mathfrak{p} = \mathfrak{P} \cap R$ holds, we say that $\mathfrak{P}$ lies over $\mathfrak{p}$.*

Theorem 9.18 *Let Λ be a maximal R-order in the central simple K-algebra B. The Λ-ideals in B form a free Abelian group with basis $\{\mathfrak{P} \mid \mathfrak{P}$ is prime$\}$.*

Proof. Cf. [Rei75, 22.10]. □

10 The Divisor Group of a Maximal Order

10.1 Somme Commutative Facts

All rings occurring in this section are assumed to be commutative, the set of prime ideals of height one of an ring R will be denoted by $\mathrm{ht}^1(R)$.

10.1.1 Local Factorial Krull Rings

Definition 10.1 *A ring R is called local factorial if $R_{\mathfrak{m}}$ is factorial for every maximal ideal $\mathfrak{m}$ of R.*

Remark 10.2 *We note that a ring R is local factorial if and only if $R_{\mathfrak{p}}$ is factorial for every prime ideal $\mathfrak{p}$ of R.*

It turns out that the property to be local factorial is very good understood for the class of Krull-rings. We recall

Definition 10.3 *An integral domain R is called a Krull-ring, if it satisfies the following properties:*

1. *For every $\mathfrak{p} \in ht^1(R)$, the ring $R_{\mathfrak{p}}$ is a discrete valuation domain.*
2. *Every $0 \neq a \notin R^\times$ is contained in only finitely many elements $\mathfrak{p}$ of $ht^1(R)$.*
3. *$R = \cap_{\mathfrak{p} \in ht^1(R)} R_{\mathfrak{p}}$ holds.*

Remark 10.4 *A Krull-ring is not assumed to be Noetherian, but we will restrict ourself soon to Noetherian Krull-rings.*

Lemma 10.5 *If R is a regular Noetherian domain, then R is a local factorial Krull domain.*

Proof. See [Eis99, Theorem 19.19] for the fact that a regular ring is local factorial. □

Corollary 10.6 *R a regular domain, then the polynomial ring $R[q]$ over R is a local factorial Krull domain.*

Sketch of the proof. We need two Theorems.

Theorem 10.7 (Serre) *For a Noetherian ring R are equivalent:*

1. *R is regular.*
2. *$gl.dim(R)$ is finite.*

Then we have that the Krull dimension of R is equal to the global dimension of R.

Proof. Cf. [Mat86, Theorem 19.2]. □

Theorem 10.8 *Let T be an arbitrary commutative ring and q an indeterminate over T. The following equality holds:*

$$gl.dim(T[q]) = gl.dim(T) + 1.$$

Proof. Cf. [Rot79, Theorem 9.34]. □

Applying theses two theorems we conclude (also using Hilbert's Basissatz) that the polynomial ring over a regular ring is again a regular ring, now we can apply Lemma 10.5.

□

We have to recall some facts about a special class of ideals, the so called divisorial ideals.

Definition 10.9 *A (fractional) ideal $\mathfrak{a}$ of (an integral domain) R is called divisorial if $\cap_{\mathfrak{p}\in ht^1(R)}\mathfrak{a}_\mathfrak{p} = \mathfrak{a}$ is satisfied.*

Proposition 10.10 *Let R be a Krull-ring. If every divisorial ideal of R is invertible, then for every maximal ideal $\mathfrak{m}$ of R, $R_\mathfrak{m}$ is a factorial ring. If we assume moreover that R is Noetherian then the converse is also true, i.e. if R is a local factorial Noetherian Krull-ring then every divisorial ideal of R is invertible.*

Proof. Cf. [Bou89d, 3.2 Proposition 1]. □

Corollary 10.11 *If R is a regular domain, then every divisorial ideal is invertible.*

Proof. We note that every regular domain is local factorial (see Lemma 10.5). □

Definition 10.12 *Let R be a Noetherian ring. We say that an ideal J of R has pure codimension 1 if either $J = R$ or $Ass_R(R/J) \subset ht^1(R)$ holds.*

Theorem 10.13 *Let R be a Noetherian local factorial domain and K its field of fractions.*

1. *For an ideal $J \subset R$ are equivalent:*
   a) *J is an invertible ideal.*
   b) *J has pure codimension 1.*
2. *If $J \subset K$ is an invertible fractional ideal, then J is uniquely expressible as $I = \prod_{\mathfrak{p}\in ht^1(R)} \mathfrak{p}^{z(\mathfrak{p})}$ with $z(\mathfrak{p}) \in \mathbb{Z}$ for all $\mathfrak{p}$ and almost all of the $z(\mathfrak{p})$'s are 0.*

Proof. Cf. [Eis99, Theorem 11.8]. □

Corollary 10.14 *If R is a regular domain, then every divisorial fractional ideal is invertible and a product of powers of prime ideals of height one.*

Remark 10.15 *There is a well known fact: Let S be an arbitrary commutative ring and $\mathfrak{a}, \mathfrak{b} \subset S$ two ideals, which are coprime i.e., $\mathfrak{a} + \mathfrak{b} = S$, then we have $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. Let us state the proof, to see where we need the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.*

Proof.

- We have of course $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$.
- Since $\mathfrak{a} + \mathfrak{b} = S$ holds we find elements $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ with $a + b = 1$. Now choose an arbitrary element $x \in \mathfrak{a} \cap \mathfrak{b}$. Then we get:

$$x = 1 \cdot x = (a+b)x = \underbrace{ax}_{\substack{\in \mathfrak{ab}, \text{ since} \\ x \in \mathfrak{b}, a \in \mathfrak{a}}} + \underbrace{bx}_{\substack{\in \mathfrak{ab}, \text{ since} \\ x \in \mathfrak{a}, b \in \mathfrak{b}}} \in \mathfrak{ab},$$

  and so $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$.

□

Example 10.16 *The equality $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ is in general not true, not even for prime ideals. We give a counterexample:*

Let L be an arbitrary field and x, y and z three pairwise commuting indeterminates over L. We consider the polynomial ring $L[x,y,z]$. We set $\mathfrak{p} := \langle x, y \rangle$ and $\mathfrak{q} := \langle x, z \rangle$. The ideals $\mathfrak{p}$ and $\mathfrak{q}$ are obviously prime and not coprime.

- *We have $\mathfrak{p} \cap \mathfrak{q} = \langle x, yz \rangle$, so in particular $x \in \mathfrak{p} \cap \mathfrak{q}$.*

  Proof. We have of course $\langle x, yz \rangle \subset \mathfrak{p} \cap \mathfrak{q}$. Now choose some element $f \in \mathfrak{p} \cap \mathfrak{q}$. Then there are $\alpha, \tilde{\alpha}, \beta, \tilde{\beta} \in L[x,y,z]$ with $f = \alpha x + \beta y = \tilde{\alpha} x + \tilde{\beta} y$, so $(\alpha - \tilde{\alpha})x \in \langle y, z \rangle$, this implies $\alpha = \tilde{\alpha}$. We get $\beta y = \tilde{\beta} z$. Since $L[x,y,z]$ is a factorial ring by the Gauss Lemma, we conclude $\beta = \gamma z$ and $\tilde{\beta} = \tilde{\gamma} z$ for some $\gamma, \tilde{\gamma} \in L[x,y,z]$. Now $f = \alpha x + \gamma yz \in \langle x, yz \rangle$ and we are done. □

- $\mathfrak{pq} = \langle x^2, xy, xz, yz \rangle$
- *To verify that $\mathfrak{pq} \neq \mathfrak{p} \cap \mathfrak{q}$ holds, it is enough to show $x \notin \mathfrak{pq}$.*

  Proof. Let $\alpha, \beta, \gamma, \delta \in L[x,y,z]$ with $x = \alpha x^2 + \beta xy + \gamma xz + \delta yz$, then x divides δyz. Since $L[x,y,z]$ is a factorial ring we find an element $\tilde{\delta}$ with $\delta = \tilde{\delta} x$. Hence

$$x = \alpha x^2 + \beta xy + \gamma xz + \tilde{\delta} xyz \implies 1 = \alpha x + \beta y + \gamma z + \tilde{\delta} yz,$$

  so $1 \in \langle x, y, z \rangle$ an obvious contradiction. □

Remark 10.17 *If R is a local factorial Krull domain then two elements $\mathfrak{p}$ and $\mathfrak{q}$ of $ht^1(R)$ are in general not coprime. For example set $R = \mathbb{Z}[x]$ and take $\mathfrak{p} = \langle x \rangle$ and $\mathfrak{q} = \langle 2 \rangle$. Then we have $\mathfrak{p} + \mathfrak{q} = \langle 2, x \rangle$ a maximal ideal of R. But we have the*

Lemma 10.18 *Let R be a local factorial Krull domain. For different elements $\mathfrak{p}, \mathfrak{q} \in ht^1(R)$ we have $\mathfrak{pq} = \mathfrak{p} \cap \mathfrak{q}$.*

Proof.

- $\mathfrak{p}$ and $\mathfrak{q}$ are divisorial ideals of R, hence invertible by Theorem 10.13. So $\mathfrak{p}\mathfrak{p}^{-1} = R$ and $\mathfrak{q}\mathfrak{q}^{-1} = R$. We get $\mathfrak{pq}\mathfrak{p}^{-1}\mathfrak{q}^{-1} = \mathfrak{p}\mathfrak{p}^{-1}\mathfrak{q}\mathfrak{q}^{-1} = R$ and since $\mathfrak{p}^{-1}\mathfrak{q}^{-1} \subset (\mathfrak{pq})^{-1}$ holds, we conclude that $\mathfrak{pq}$ is invertible, hence also a divisorial ideal of R.

- Proposition 10.25 of the next section yields that $\mathfrak{p} \cap \mathfrak{q}$ is also a divisorial ideal of R and obviously $\mathfrak{pq} \subset \mathfrak{p} \cap \mathfrak{q}$.
- Let $\tilde{\mathfrak{p}}$ be an arbitrary element of $\mathrm{ht}^1(R)$. We have to distinguish two cases:
  - $\tilde{\mathfrak{p}} \neq \mathfrak{p}, \mathfrak{q}$: Here we have $\mathfrak{p}_{\tilde{\mathfrak{p}}} = R_{\tilde{\mathfrak{p}}}$ and $\mathfrak{q}_{\tilde{\mathfrak{p}}} = R_{\tilde{\mathfrak{p}}}$. As in Lemma 10.58 we get $(\mathfrak{pq})_{\tilde{\mathfrak{p}}} = \mathfrak{p}_{\tilde{\mathfrak{p}}}\mathfrak{q}_{\tilde{\mathfrak{p}}}$. Hence
$$R_{\tilde{\mathfrak{p}}} = R_{\tilde{\mathfrak{p}}}R_{\tilde{\mathfrak{p}}} = \mathfrak{p}_{\tilde{\mathfrak{p}}}\mathfrak{q}_{\tilde{\mathfrak{p}}} = (\mathfrak{pq})_{\tilde{\mathfrak{p}}} \underset{\mathfrak{pq}\subset\mathfrak{p}\cap\mathfrak{q}}{\subset} (\mathfrak{p}\cap\mathfrak{q})_{\tilde{\mathfrak{p}}} \underset{\text{obvious}}{\subset} R_{\tilde{\mathfrak{p}}}.$$
    So we have $(\mathfrak{pq})_{\tilde{\mathfrak{p}}} = (\mathfrak{p}\cap\mathfrak{q})_{\tilde{\mathfrak{p}}}$.
  - $\tilde{\mathfrak{p}} = \mathfrak{p}$ ($\tilde{\mathfrak{p}} = \mathfrak{q}$ is clear from symmetry): We use again Lemma 10.58 to conclude
$$(\mathfrak{pq})_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}\mathfrak{q}_{\mathfrak{p}} \underset{\mathfrak{p}\neq\mathfrak{q}}{=} \mathfrak{p}R_{\mathfrak{p}} \underset{\mathfrak{pq}\subset\mathfrak{p}\cap\mathfrak{q}}{\subset} (\mathfrak{p}\cap\mathfrak{q})_{\mathfrak{p}} \underset{\mathfrak{p}\cap\mathfrak{q}\subset\mathfrak{p}}{\subset} \mathfrak{p}R_{\mathfrak{p}},$$
    and so $(\mathfrak{pq})_{\mathfrak{p}} = (\mathfrak{p}\cap\mathfrak{q})_{\mathfrak{p}}$.

  So we have that $(\mathfrak{pq})_{\tilde{\mathfrak{p}}} = (\mathfrak{p}\cap\mathfrak{q})_{\tilde{\mathfrak{p}}}$ holds for every element $\tilde{\mathfrak{p}} \in \mathrm{ht}^1(R)$. Since $\mathfrak{pq}$ and $\mathfrak{p}\cap\mathfrak{q}$ are both divisorial ideals of R, we have $\mathfrak{pq} = \mathfrak{p}\cap\mathfrak{q}$.

□

We can generalize Lemma 10.18. First we need

Definition 10.19 *Let $\mathfrak{a}$ and $\mathfrak{b}$ two divisorial ideals of R, s.t. $\mathfrak{a} = \Pi_{\mathfrak{p}\in ht^1(R)}\mathfrak{p}^{\alpha_\mathfrak{p}}$ and $\mathfrak{b} = \Pi_{\mathfrak{q}\in ht^1(R)}\mathfrak{q}^{\beta_\mathfrak{q}}$. We call $\mathfrak{a}$ and $\mathfrak{b}$ disjoint if $\alpha_\mathfrak{p}\beta_\mathfrak{p} = 0$ for all $\mathfrak{p} \in ht^1(R)$.*

Lemma 10.20 *If $\mathfrak{a}$ and $\mathfrak{b}$ are two disjoint divisorial ideals of R we have $\mathfrak{ab} = \mathfrak{a}\cap\mathfrak{b}$.*

Proof.

- We know that both ideals $\mathfrak{ab}$ and $\mathfrak{a}\cap\mathfrak{b}$ are divisorial ideals of R.
- By the last point it is enough to verify that for every $\mathfrak{p} \in \mathrm{ht}^1(R)$ $(\mathfrak{ab})_\mathfrak{p} = (\mathfrak{a}\cap\mathfrak{b})_\mathfrak{p}$ holds. This is done by a calculation which is analogous to the one we did in the proof of Lemma 10.18.

□

10.1.2 Divisorial lattices

We assume from now on that R is a Noetherian integrally closed domain with field of fractions K.

We can generalize Definition 10.9 to

Definition 10.21 *An R-lattice M is called divisorial if $M = \bigcap_{\mathfrak{p}\in ht^1(R)} M_\mathfrak{p}$ is satisfied.*

First there is a very important characterization of divisorial lattices in terms of the bidual of a lattice. Let us recall a definition

Definition 10.22 *Let S be an arbitrary commutative ring and M an S-module. We set $M^* := \mathrm{Hom}_S(M,S)$ and $M^{**} := (M^*)^*$. We call M^{**} the bidual of M. There is a canonical map of S-modules*

$$\tau_M : M \longrightarrow M^{**}$$
$$m \longmapsto [\tau_m : M^* \ni \varphi \longmapsto \varphi(m) \in S].$$

We call M reflexive if τ_M is an isomorphism of S-modules.

Remarks 10.23 *1. Let L be an arbitrary field and W be a vector space over L. The map τ_W is always injective. Equivalent are:*

a) W is reflexive.

b) The L-dimension of W is finite.

2. Let M be an R-lattice in a finite dimensional K-vector space V. By (1) the map $\tau_V : V \longrightarrow V^{**}$ is an isomorphism. Denote by $\iota : M \longrightarrow V$ the canonical embedding of M into V. There is obviously a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\tau_M} & M^{**} \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota^{**}} \\ V & \xrightarrow[\tau_V]{} & V^{**}. \end{array}$$

We may identify V with V^{**} and so we can interpret M^{**} as an R-lattice in V.

Theorem 10.24 *Let V be a finite dimensional vector space over K. For an R-lattice M in V are equivalent:*

1. *M is a divisorial lattice, i.e. $M = \bigcap_{\mathfrak{p} \in ht^1(R)} M_{\mathfrak{p}}$.*
2. *M is reflexive.*
3. *$Ass_R(V/M) \subset ht^1(R)$.*

Proof. Cf. [Bou89d, 4.2 Theorem 2]. □

Proposition 10.25 *Let V be a finite dimensional vector space over K.*

1. *If M_1 and M_2 are divisorial lattices in V then $M_1 \cap M_2$ is also a divisorial lattice.*
2. *If $W \leq V$ is a sub vector space and M is a divisorial lattice in V then $W \cap M$ is a divisorial lattice in W.*
3. *Let W be another finite dimensional vector space over K and M, N be arbitrary lattices in V and W respectively. If N is divisorial then $N : M := \{f \in \mathrm{Hom}_K(V,W) | f(M) \subset N\}$ is a divisorial lattice in $\mathrm{Hom}_K(V,W)$.*

Proof. Cf. [Bou89d, 4.2 Proposition 6]. □

Divisorial lattices can be constructed with the help of "height one data".

Theorem 10.26 *Let V be a finite dimensional vector space over K and $M \subset V$ an R-lattice in V.*

1. *Let N be an R-lattice in V, then for every $\mathfrak{p} \in ht^1(R)$, $N_\mathfrak{p}$ is an $R_\mathfrak{p}$-lattice in V and for almost all $\mathfrak{p} \in ht^1(R)$ we have an equality $M_\mathfrak{p} = N_\mathfrak{p}$.*
2. *Conversely, suppose given for all $\mathfrak{p} \in ht^1(R)$ a lattice $N(\mathfrak{p})$ with respect to $R_\mathfrak{p}$, such that $N(\mathfrak{p}) = M_\mathfrak{p}$ for almost all $\mathfrak{p} \in ht^1(R)$. Then $N := \cap_{\mathfrak{p} \in ht^1(R)} N(\mathfrak{p})$ is a divisorial lattice of V with respect to R. Moreover N is the only divisorial lattice N' of V with respect to R s.t. $N'_\mathfrak{p} = N(\mathfrak{p})$ for all $\mathfrak{p} \in ht^1(R)$.*

Proof. Cf. [Bou89d, 4.3 Theorem 3]. □

There is a useful proposition about the quotients of divisorial lattices.

Proposition 10.27 *Let*

$$0 \longrightarrow M \longrightarrow N \longrightarrow Q \longrightarrow 0$$

be an exact sequence of R-modules s.t. N is an R-lattice.

1. *If M is a divisorial lattice then $Ass_R(Q) \subset ht^1(R) \cup \{0\}$.*
2. *Conversely if N is divisorial and $Ass_R(Q) \subset ht^1(R) \cup \{0\}$ holds, then M is also divisorial.*

Proof. Cf. [Bou89d, 4. 2 Proposition 7] □

10.2 Two-sided Divisorial Ideals of Maximal Orders

Let us fix the notations for this section. Let R be a commutative local factorial Noetherian Krull-Domain (we note that every regular domain has these properties). The field of fractions of R is denoted by K and A is a central simple K-algebra. Moreover let Λ be an R-order in A which is divisorial as R-lattice. We note that every maximal order is divisorial over R (cf. [Rei75, Theorem 11.4]).

Definition 10.28 *A Λ-ideal J of A is a two-sided Λ-lattice in A. If $J \subset \Lambda$ holds we just call J an ideal of Λ.*

Lemma 10.29 *Let $J \subset \Lambda$ be an ideal such that J is a divisorial lattice, then $J \cap R = J \cap K$ is a divisorial ideal of R and so $J \cap R$ is invertible and a product of height one prime ideals of R.*

Proof.

1. We have surely $J \cap R \subset J \cap K$ and $J \cap R$ is an ideal of R. Since a Krull-domain is integrally closed and every element of the R-order Λ is integral over R, we have of course also $J \cap K \subset J \cap R$.
2. Proposition 10.25 (ii) yields that $J \cap R$ is a divisorial ideal of R, so invertible by Proposition 10.10. An application of Theorem 10.13 yields that $J \cap R$ is a product of elements of $\mathrm{ht}^1(R)$.

□

Remark 10.30 *The proof of Lemma 10.29 yields immediately that for an arbitrary divisorial Λ-ideal J in A, $J \cap K$ is an invertible fractional R-ideal of K an it is a product of powers of elements of $ht^1(R)$.*

Observation 10.31 *For an ideal of Λ we have $Ann_R(\Lambda/J) = J \cap K$.*

Proof. We set $\mathfrak{b} := \mathrm{Ann}_R(\Lambda/J)$ and $\mathfrak{a} := J \cap K$. Then

- $\mathfrak{b}(\Lambda/J) = 0$, so $\mathfrak{b} \subset \mathfrak{b}\Lambda \subset J$, hence $\beta \subset J \cap R = \mathfrak{a}$.
- $\mathfrak{a} = R \cap J \Longrightarrow \mathfrak{a} \subset J \underset{\substack{J \text{ is an} \\ \text{ideal of } \Lambda}}{\Longrightarrow} \mathfrak{a}\Lambda \subset J \Longrightarrow \mathfrak{a} \subset \mathrm{Ann}_R(\Lambda/J) = \mathfrak{b}$.

□

Notation 10.32 *For $\mathfrak{p} \in ht^1(R)$ we set $\mathfrak{P} := rad(\Lambda_\mathfrak{p}) \cap \Lambda$.*

Lemma 10.33 *$\mathfrak{P}$ is a divisorial ideal of Λ.*

Proof. We have

$$\mathfrak{P} = \Lambda \cap \mathrm{rad}(\Lambda_\mathfrak{p}) \underset{\substack{\Lambda \text{ is a divisorial} \\ \text{lattice}}}{=} \mathrm{rad}(\Lambda_\mathfrak{p}) \cap \bigcap_{\mathfrak{q} \in \mathrm{ht}^1(R)} \Lambda_\mathfrak{q}$$

$$= \bigcap_{\mathfrak{p} \neq \mathfrak{q} \in \mathrm{ht}^1(R)} \Lambda_\mathfrak{q} \cap \Lambda_\mathfrak{p} \cap \mathrm{rad}(\Lambda_\mathfrak{p}) = \bigcap_{\mathfrak{p} \neq \mathfrak{q} \in \mathrm{ht}^1(R)} \Lambda_\mathfrak{q} \cap \mathrm{rad}(\Lambda_\mathfrak{p}) = \bigcap_{\mathfrak{q} \in \mathrm{ht}^1(R)} N(\mathfrak{q}),$$

with

$$N(\mathfrak{q}) = \begin{cases} \mathrm{rad}(\Lambda_\mathfrak{p}) \text{ for } \mathfrak{q} = \mathfrak{p} \\ \Lambda_\mathfrak{q} \text{ otherwise} \end{cases}.$$

So $N(\mathfrak{q}) = \Lambda_\mathfrak{q}$ for almost all elements $\mathfrak{q} \in \mathrm{ht}^1(R)$. So we can apply Theorem 10.26 to deduce that $\mathfrak{P}$ is a divisorial ideal of Λ (that $\mathfrak{P}$ is really a two-sided ideal of Λ is trivial). □

Remark 10.34 *$\mathfrak{P}$ is the only divisorial two-sided ideal J of Λ with the property: $J_\mathfrak{q} = \begin{cases} rad(\Lambda_\mathfrak{p}) \text{ for } \mathfrak{q} = \mathfrak{p} \\ \Lambda_\mathfrak{q} \text{ otherwise} \end{cases}$. Moreover $\mathfrak{P}$ is the only divisorial R-lattice in A with this property (see Theorem 10.26).*

From now on we assume that Λ is a *maximal* order.

Lemma 10.35 *$\mathfrak{P}$ is a maximal two-sided divisorial ideal of Λ, i.e. there is no two-sided divisorial ideal J of Λ with $\mathfrak{P} \subsetneq J \subsetneq \Lambda$.*

Proof. Assume $\mathfrak{P} \subset J \subset \Lambda$, where J is a two-sided divisorial ideal of Λ. For every $\mathfrak{p} \in \mathrm{ht}^1(R)$ we have $\mathfrak{P}_\mathfrak{p} \subset J_\mathfrak{p} \subset \Lambda_\mathfrak{p}$. We have to distinguish the following two cases:

- Case 1: $\mathfrak{q} \neq \mathfrak{p}$. Here we have $\Lambda_\mathfrak{q} = \mathfrak{P}_\mathfrak{q} \subset J_\mathfrak{q} \subset \Lambda_\mathfrak{q}$, hence $J_\mathfrak{q} = \Lambda_\mathfrak{q}$ holds.
- Case 2: $\mathfrak{q} = \mathfrak{p}$. We find: $\mathfrak{P}_\mathfrak{p} = \mathrm{rad}(\Lambda_\mathfrak{p}) \subset J_\mathfrak{p} \subset \Lambda_\mathfrak{p}$ and $J_\mathfrak{p}$ is a two-sided ideal of the $R_\mathfrak{p}$-order $\Lambda_\mathfrak{p}$. R is a Krull-domain and $\mathfrak{p}$ an element of $\mathrm{ht}^1(R)$, so it follows that $R_\mathfrak{p}$ is a discrete valuation domain. By assumption Λ is a maximal order over R, so $\Lambda_\mathfrak{p}$ is maximal over $R_\mathfrak{p}$ (cf. [Rei75, Theorem 11.1].) This means that $\Lambda_\mathfrak{p}$ is a maximal order over a discrete valuation domain, hence every two-sided ideal of $\Lambda_\mathfrak{p}$ is a power of $\mathrm{rad}(\Lambda_\mathfrak{p})$ (see Theorem 9.8).

So we have two possibilities:

1. $J_\mathfrak{p} = \mathrm{rad}(\Lambda_\mathfrak{p}) \Longrightarrow J_\mathfrak{q} = \mathfrak{P}_\mathfrak{q}$ for every $\mathfrak{q} \in \mathrm{ht}^1(R)$. So the uniqueness property of Theorem 10.26 yields that $J = \mathfrak{P}$ holds.
2. $J_\mathfrak{p} = \Lambda_\mathfrak{p} \Longrightarrow J \underset{J \text{ is divisorial}}{=} \cap_{\mathfrak{q} \in \mathrm{ht}^1(R)} J_\mathfrak{q} = \cap_{\mathfrak{q} \in \mathrm{ht}^1(R)} \Lambda_\mathfrak{q} \underset{\Lambda \text{ is divisorial}}{=} \Lambda$, a contradiction.

□

Lemma 10.36 *We have* $\mathfrak{P} \cap R = \mathfrak{p}$.

Proof. We reduce the proof to the level of maximal orders over discrete valuation domains. For (*) we refer to [Rei75, Theorems 18.3 and 22.4]:

$$\mathfrak{P} \cap R \underset{\text{per. def. of } \mathfrak{P}}{=} \mathrm{rad}(\Lambda_\mathfrak{p}) \cap \Lambda \cap R \underset{R \cap \Lambda = R}{=} \mathrm{rad}(\Lambda_\mathfrak{p}) \cap R$$
$$\underset{R \subset R_\mathfrak{p}}{=} \big(\mathrm{rad}(\Lambda_\mathfrak{p}) \cap R_\mathfrak{p}\big) \cap R \underset{(*)}{=} \mathrm{rad}(R_\mathfrak{p}) \cap R = \mathfrak{p}R_\mathfrak{p} \cap R \underset{\substack{\mathfrak{p} \text{ is a prime} \\ \text{ideal of } R}}{=} \mathfrak{p}$$

and so we are done. □

Observation 10.37 *We have* $\mathfrak{P} \cdot \Lambda_\mathfrak{p} = rad(\Lambda_\mathfrak{p})$.

Proof. $\mathfrak{P} \cdot \Lambda_\mathfrak{p}$ is a two-sided ideal of $\Lambda_\mathfrak{p}$ which surely contains $\mathfrak{P}_\mathfrak{p} = \mathrm{rad}(\Lambda_\mathfrak{p})$. On the other side we have $\mathfrak{P} \subset \mathrm{rad}(\Lambda_\mathfrak{p}) \Longrightarrow \mathfrak{P} \cdot \Lambda_\mathfrak{p} \subset \mathrm{rad}(\Lambda_\mathfrak{p})$ and we are done. □

By assumption R is a Krull-domain. We recall a lemma which holds for Krull-domains:

Lemma 10.38 *Let M and N be two R-lattices in the K-vector space V. Then for almost all $\mathfrak{p} \in ht^1(R)$ we have $M_\mathfrak{p} = N_\mathfrak{p}$.*

Proof. Both M and N are full R-lattices in V, so there exists an element $0 \neq a \in R$ with $aM \subset N$. The element a is contained in at least finitely many elements $\mathfrak{p}$ of $\mathrm{ht}^1(R)$. For $a \notin \mathfrak{q} \in \mathrm{ht}^1(R)$ we have of course that $\frac{a}{1}$ is a unit of $R_\mathfrak{q}$ and so $(aM)_\mathfrak{q} = M_\mathfrak{q} = N_\mathfrak{q}$ and we are done. □

Observation 10.39 *Let J be a divisorial ideal of Λ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ the elements $\mathfrak{p} \in ht^1(R)$ with $J_\mathfrak{p} \neq \Lambda_\mathfrak{p}$ then we have*

$$J = \bigcap_{i=1}^{n} \big(J_{\mathfrak{p}_i} \cap \Lambda\big).$$

Proof. We have

$$J \underset{J \text{ is divisorial}}{=} \bigcap_{\mathfrak{p} \in \mathrm{ht}^1(R)} J_\mathfrak{p} = \bigcap_{i=1}^{n} J_{\mathfrak{p}_i} \bigcap \bigcap_{\mathfrak{p}_i \neq \mathfrak{q} \in \mathrm{ht}^1(R)} J_\mathfrak{q}$$
$$\underset{J_\mathfrak{q} = \Lambda_\mathfrak{q} \text{ for } \mathfrak{q} \neq \mathfrak{p}_i}{=} \bigcap_{i=1}^{n} J_{\mathfrak{p}_i} \bigcap \bigcap_{\mathfrak{q} \neq \mathfrak{p}_i} \Lambda_\mathfrak{q} \underset{J_{\mathfrak{p}_i} = J_{\mathfrak{p}_i} \cap \Lambda_{\mathfrak{p}_i}}{=} \bigcap_{i=1}^{n} J_{\mathfrak{p}_i} \bigcap \bigcap_{i=1}^{n} \Lambda_{\mathfrak{p}_i} \bigcap \bigcap_{\mathfrak{q} \neq \mathfrak{p}_i} \Lambda_\mathfrak{q}$$
$$= \bigcap_{i=1}^{n} J_{\mathfrak{p}_i} \bigcap \bigcap_{\mathfrak{q} \in \mathrm{ht}^1(R)} \Lambda_\mathfrak{q} \underset{\Lambda \text{ is divisorial}}{=} \bigcap_{i=1}^{n} \big(J_{\mathfrak{p}_i} \cap \Lambda\big).$$

□

Up to now we have managed to show that the $\mathfrak{P}$'s are maximal two-sided divisorial ideals of Λ. Now we want to show that every maximal two-sided divisorial ideal of Λ is one of the $\mathfrak{P}$'s.

Lemma 10.40 *Let J be an arbitrary two-sided divisorial ideal of Λ. There is a unique $\mathfrak{p} \in ht^1(R)$ with $J = \mathfrak{P} = rad(\Lambda_\mathfrak{p}) \cap \Lambda$.*

Proof. We denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ the prime ideals of height one of R for which $\Lambda_{\mathfrak{p}_i} \neq J_{\mathfrak{p}_i}$ holds. For every i we have so $J_{\mathfrak{p}_i} \subsetneq \Lambda_{\mathfrak{p}_i}$. $J_{\mathfrak{p}_i}$ is obviously a proper two-sided ideal of $\Lambda_{\mathfrak{p}_i}$, hence a power of the radical of $\Lambda_{\mathfrak{p}_i}$. So we find natural numbers $\alpha_i \geq 1$ with $J_{\mathfrak{p}_i} = \mathrm{rad}(\Lambda_{\mathfrak{p}_i})^{\alpha_i}$. Now we set $N(\mathfrak{q}) := \begin{cases} \mathrm{rad}(\Lambda_\mathfrak{q}) \text{ for } \mathfrak{q} = \mathfrak{p}_1 \\ \Lambda_\mathfrak{q} \text{ otherwise} \end{cases}$. By Theorem 10.26 $N := \bigcap_{\mathfrak{q} \in \mathrm{ht}^1(R)} N(\mathfrak{q})$ is a divisorial lattice, with $N_\mathfrak{q} = N(\mathfrak{q})$ for all $\mathfrak{q} \in \mathrm{ht}^1(R)$. Obviously we have $N = \mathrm{rad}(\Lambda_{\mathfrak{p}_1}) \cap \Lambda$ and $J_\mathfrak{q} \subset N_\mathfrak{q}$ for all $\mathfrak{q} \in \mathrm{ht}^1(R)$. Both J and N are divisorial, so we get

$$J = \bigcap_{\mathfrak{q} \in \mathrm{ht}^1(R)} J_\mathfrak{q} \subset \bigcap \mathfrak{q} \in \mathrm{ht}^1(R) N_\mathfrak{q} = N.$$

But for some $\mathfrak{p} \in \mathrm{ht}^1(R)$ we have $J_\mathfrak{p} \subsetneq N_\mathfrak{p}$, unless $\alpha_1 = 1$ and $n = 1$ is satisfied. This would imply $J \subsetneq N \subsetneq \Lambda$ and J is not maximal, a contradiction. That there is just one prime ideal $\mathfrak{p} \in \mathrm{ht}^1(R)$ with $J \cap R$ is trivial. □

So we have shown the

Theorem 10.41 *There is a one-to-one correspondence between the set of maximal divisorial two-sided ideals of Λ – we denote this set by $P(\Lambda)$ – and the set $ht^1(R)$ of prime ideals of height one of R. This bijection is given by the following maps:*

$$ht^1(R) \ni \mathfrak{p} \longmapsto rad(\Lambda_\mathfrak{p}) \cap \Lambda =: \mathfrak{P} \in P(\Lambda)$$
$$P(\Lambda) \ni \mathfrak{P} \longmapsto \mathfrak{P} \cap R =: \mathfrak{p} \in ht^1(R).$$

Now we will examine an arbitrary two-sided divisorial ideal J of Λ in a greater detail.

Lemma 10.42 *Let $J \subset \Lambda$ be a divisorial ideal. Then there are finitely many $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in ht^1(R)$ and natural numbers $\alpha_1, \ldots, \alpha_n \geq 1$ with*

$$J = \bigcap_{i=1}^{n} \left(rad(\Lambda_{\mathfrak{p}_i})^{\alpha_i} \cap \Lambda \right).$$

Conversely every ideal of this type is divisorial.

Proof. For the first statement just use Observation 10.39. For the second one we refer to Theorem 10.26. □

Remark 10.43 *J is uniquely determined by the $\mathfrak{p}_i$'s and the α_i's.*

Proof. Use the uniqueness statement of Theorem 10.26. □

Definition 10.44 *Let $J \subset A$ a Λ-ideal. We set $J^{-1} := \{x \in A : Jx \subset \Lambda\}$.*

Observation 10.45 *We have:*

1. J^{-1} *is a* Λ*-ideal in* A.
2. *There is an isomorphism* $J^{-1} \simeq \mathrm{Hom}_\Lambda(J, \Lambda)$.

Proof.

1. Once (2) is shown, it is immediately clear, that J^{-1} is a full R-lattice in $K\,\mathrm{Hom}_\Lambda(J,\Lambda) = \mathrm{Hom}_{K\Lambda}(KJ, K\Lambda) = \mathrm{Hom}_A(A,A) = A$. That J^{-1} is a two-sided Λ-module is obtained from standard calculations.
2. We set

$$\begin{aligned} \Phi : J^{-1} &\longrightarrow \mathrm{Hom}_\Lambda(J,\Lambda) \\ x &\longmapsto [\Phi_x : J \ni j \longmapsto jx \in \Lambda]. \end{aligned}$$

   - An easy calculation shows that Φ is a well defined homomorphism of two-sided Λ-modules.
   - Let us assume $\Phi_x = 0$ for some $x \in J^{-1}$. We get $Jx = 0$, hence $Ax = KJx = 0$, this implies $x = 0$. So Φ is injective.
   - Choose an arbitrary element $\varphi \in \mathrm{Hom}_\Lambda(J,\Lambda)$. The element $K\varphi \in K\,\mathrm{Hom}_\Lambda(J,\Lambda) = \mathrm{Hom}_A(A,A)$ is given by a right multiplication with some element $x \in A$. Then it is easy to see, that $\varphi = \Phi_{\tilde{x}}$ for some $\tilde{x} \in A$. Hence Φ is surjective.

□

Notation 10.46 *We set* $\tilde{\cdot} := \bigcap_{\mathfrak{p} \in ht^1(R)} (\cdot)_\mathfrak{p}$.

Lemma 10.47 *Let* Γ *be an* R*-order and* M *an arbitrary* Γ*-lattice. Then* $\tilde{M}$ *is a* $\tilde{\Gamma}$*-lattice.*

Proof. We just have to show that $\tilde{M}$ is a $\tilde{\Gamma}$-module. So choose elements $x \in \tilde{M}$ and $y \in \tilde{\Gamma}$. For every $\mathfrak{p} \in \mathrm{ht}^1(R)$ we find elements $m \in M, \gamma \in \Gamma$ and $s, t \notin \mathfrak{p}$ with $x = \frac{m}{s}$ and $y = \frac{\gamma}{t}$. Hence we get $yx = \frac{\gamma}{t}\frac{m}{s} = \frac{\gamma m}{st} \underset{\gamma m \in M, st \notin \mathfrak{p}}{\in} M_\mathfrak{p}$, this implies $yx \in \bigcap_{\mathfrak{p} \in \mathrm{ht}^1(R)} M_\mathfrak{p} = \tilde{M}$ and we are done. □

Observation 10.48 *For an* R*-lattice* M *and a* $\mathfrak{p} \in ht^1(R)$ *we have* $M_\mathfrak{p} = \tilde{M}_\mathfrak{p}$.

Proof.

- $M \subset \tilde{M} \Longrightarrow M_\mathfrak{p} \subset \tilde{M}_\mathfrak{p}$.
- $x \in \tilde{M}_\mathfrak{p} \Longrightarrow \exists y \in \tilde{M}$ and $s \notin \mathfrak{p}$ with $x = \frac{y}{s}$, but $y \in \tilde{M}$, so we have $y \in M_\mathfrak{p}$, hence $\frac{y}{s} \in M_\mathfrak{p} \Longrightarrow \tilde{M}_\mathfrak{p} \subset M_\mathfrak{p}$.

□

Lemma 10.49 *For an* R*-order* Γ *and two* Γ*-lattices* M *and* N *we have*

$$\big(\mathrm{Hom}_\Gamma(M,N)\big)^{\tilde{}} = \mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M}, \tilde{N}).$$

Proof.

- For an arbitrary $\mathfrak{p} \in \mathrm{ht}^1(R)$ we have

$$\mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M},\tilde{N}) \subset \big(\mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M},\tilde{N})\big)_{\mathfrak{p}} = \mathrm{Hom}_{\tilde{\Gamma}_{\mathfrak{p}}}(\tilde{M}_{\mathfrak{p}},\tilde{N}_{\mathfrak{p}})$$
$$\underset{\text{Observation 10.48}}{=} \mathrm{Hom}_{\Gamma_{\mathfrak{p}}}(M_{\mathfrak{p}},N_{\mathfrak{p}}).$$

  We conclude

$$\mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M},\tilde{N}) \subset \big(\mathrm{Hom}_{\Gamma}(M,N)\big)\tilde{}.$$

- On the other side we have

$$\big(\mathrm{Hom}_{\Gamma}(M,N)\big)\tilde{} = \bigcap_{\mathfrak{p}\in\mathrm{ht}^1(R)} \big(\mathrm{Hom}_{\Gamma}(M,N)\big)_{\mathfrak{p}} = \bigcap_{\mathfrak{p}\in\mathrm{ht}^1(R)} \mathrm{Hom}_{\Gamma_{\mathfrak{p}}}(M_{\mathfrak{p}},N_{\mathfrak{p}}) \ni f,$$

  for an arbitrary element $x \in \tilde{M} = \bigcap_{\mathfrak{p}\in\mathrm{ht}^1(R)} M_{\mathfrak{p}}$ we have obviously $xf \in N_{\mathfrak{p}}$ since $x \in M_{\mathfrak{p}}$ and $f \in \mathrm{Hom}_{\Gamma_{\mathfrak{p}}}(M_{\mathfrak{p}},N_{\mathfrak{p}})$. So we get $f \in \mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M},\tilde{N})$ (we here fore that f is $\Gamma_{\mathfrak{p}}$-linear, so it is also $\tilde{\Gamma}$-linear).

□

Corollary 10.50 *Let Γ be an arbitrary R-order, M an arbitrary Γ-lattice and N a Γ-lattice, which is divisorial over R. Then we have*

$$\mathrm{Hom}_{\Gamma}(M,N) = \mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M},N).$$

Proof.

- We have

$$\mathrm{Hom}_{\Gamma}(M,N) \subset \big(\mathrm{Hom}_{\Gamma}(M,N)\big)\tilde{}$$
$$\underset{\text{Lemma 10.49}}{=} \mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M},\tilde{N}) \underset{N \text{ is divisorial}}{=} \mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M},N).$$

- The other inclusion is trivial.

□

Corollary 10.51 *If J is a divisorial Λ-ideal in A, then J^{-1} is also divisorial.*

Proof. We have

$$\widetilde{J^{-1}} = \big(\mathrm{Hom}_{\Lambda}(J,\Lambda)\big)\tilde{} \underset{\text{Lemma 10.49}}{=} \mathrm{Hom}_{\tilde{\Lambda}}(\tilde{J},\tilde{\Lambda}) \underset{\Lambda \text{ and } J \text{ are divisorial}}{=} \mathrm{Hom}_{\Lambda}(J,\Lambda) = J^{-1}$$

and we are done. □

Corollary 10.52 *Let Γ be a divisorial R-order, M an arbitrary Γ-lattice and N a Γ-lattice, which is divisorial over R. Then $\mathrm{Hom}_{\Gamma}(M,N)$ is a divisorial R-lattice.*

Proof. Note

$$\big(\mathrm{Hom}_{\Gamma}(M,N)\big)\tilde{} \underset{\text{Lemma 10.49}}{=} \mathrm{Hom}_{\tilde{\Gamma}}(\tilde{M},\tilde{N})$$
$$\underset{\Gamma \text{ and } N \text{ are divisorial}}{=} \mathrm{Hom}_{\Gamma}(\tilde{M},N) \subset \mathrm{Hom}_{\Gamma}(M,N).$$

The other inclusion is trivial, so we get $\big(\mathrm{Hom}_{\Gamma}(M,N)\big)\tilde{} = \mathrm{Hom}_{\Gamma}(M,N)$ and we are done. □

We know that if J is a divisorial Λ-ideal in A, then J^{-1} as well. So let us determine the structure of J^{-1}.

Lemma 10.53 *Let $\mathfrak{P}$ be the maximal divisorial ideal of Λ which is lying over $\mathfrak{p} \in ht^1(R)$. Then we have*

$$\mathfrak{P}^{-1} = (rad(\Lambda_\mathfrak{p}))^{-1} \bigcap \Big(\bigcap_{\mathfrak{p} \neq \mathfrak{q} \in ht^1(R)} \Lambda_\mathfrak{q} \Big).$$

Proof. The ideal $\mathfrak{P}$ is divisorial, so $\mathfrak{P}^{-1}$ is divisorial by Corollary 10.51. So it is enough to determine the lattices $(\mathfrak{P}^{-1})_\mathfrak{q}$ for $\mathfrak{q} \in \mathrm{ht}^1(R)$. We have for a $\mathfrak{q} \in \mathrm{ht}^1(R)$:

$$\big(\mathfrak{P}^{-1}\big)_\mathfrak{q} = \big(\mathrm{Hom}_\Lambda(\mathfrak{P}, \Lambda)\big)_\mathfrak{q} = \mathrm{Hom}_{\Lambda_\mathfrak{q}}(\mathfrak{P}_\mathfrak{q}, \Lambda_\mathfrak{q}) = \big(\mathfrak{P}_\mathfrak{q}\big)^{-1},$$

where we regard $\mathfrak{P}_\mathfrak{q}$ as an $R_\mathfrak{q}$-lattice. Moreover we have

$$\big(\mathfrak{P}_\mathfrak{q}\big)^{-1} = \begin{cases} \big(\Lambda_\mathfrak{q}\big)^{-1} = \Lambda_\mathfrak{q} \text{ for } \mathfrak{q} \neq \mathfrak{p} \\ \big(\mathrm{rad}(\Lambda_\mathfrak{p})\big)^{-1} \text{ for } \mathfrak{q} = \mathfrak{p} \end{cases}.$$

But this yields the desired result. □

More general we have

Lemma 10.54 *Let J be a two-sided Λ-ideal in A with $J = \bigcap_{\mathfrak{p} \in ht^1(R)} \big(rad(\Lambda_\mathfrak{p})\big)^{\alpha_\mathfrak{p}}$ such that $(\alpha_\mathfrak{p})_\mathfrak{p} \in \oplus_{\mathfrak{p} \in ht^1(R)} \mathbb{Z}$. Then we have*

$$J^{-1} = \bigcap_{\mathfrak{p} \in ht^1(R)} \big(rad(\Lambda_\mathfrak{p})\big)^{-\alpha_\mathfrak{p}}.$$

Proof. As in the proof of Lemma 10.53 we find for an arbitrary $\mathfrak{p} \in \mathrm{ht}^1(R)$, $\big(J^{-1}\big)_\mathfrak{p} = \big(J_\mathfrak{p}\big)^{-1}$. But $\big(J_\mathfrak{p}\big)^{-1} = \big(\mathrm{rad}(\Lambda_\mathfrak{p})^{\alpha_\mathfrak{p}}\big)^{-1} = \big(\mathrm{rad}(\Lambda_\mathfrak{p})\big)^{-\alpha_\mathfrak{p}}$ and we are done. □

Definition 10.55 *Let J and J' be two-sided Λ-ideals in A. We say that J and J' are in the same divisor class of Λ if $\tilde{J} = \tilde{J'}$ holds. In this case we will write $J \sim J'$.*

Observation 10.56 *The relation $\sim$ is an equivalence relation on the set of two-sided Λ-ideals in A.*

Proof. Obvious. □

Definition 10.57 *For an two-sided Λ-ideal J in A we denote the equivalence class of J under $\sim$ by $div(J)$. The set of equivalence classes will be denoted by $D(\Lambda)$.*

Lemma 10.58 *Let M and N be two arbitrary R-lattices in A and $S \subset R$ a multiplicative subset. We have $S^{-1}(MN) = (S^{-1}M)(S^{-1}N)$.*

Proof.

- Choose elements $m \in M, n \in N$ and $s, t \in S$, we get $\frac{m}{s}\frac{n}{t} = \frac{mn}{st} \in S^{-1}(MN)$, so we conclude $(S^{-1}M)(S^{-1}N) \subset S^{-1}(MN)$.
- Let $x \in S^{-1}(MN)$. Then we find $m_1, \ldots, m_k \in M$, $n_1, \ldots, n_k \in N$ and an $s \in S$ with $x = \frac{\sum_{i=1}^k m_i n_i}{s} = \sum_{i=1}^k \frac{m_i}{s}\frac{n_i}{1} \in (S^{-1}M)(S^{-1}N)$. This shows $S^{-1}(MN) \subset (S^{-1}M)(S^{-1}N)$.

□

Lemma 10.59 *Let I, J and X be two-sided Λ-ideals in A. If $div(I) = div(J)$ holds, we have $div(IX) = div(JX)$.*

Proof. Choose an arbitrary element $\mathfrak{p} \in \mathrm{ht}^1(R)$. We have

$$(IX)_{\mathfrak{p}} \underset{\text{Lemma 10.58}}{=} I_{\mathfrak{p}} X_{\mathfrak{p}} \underset{\mathrm{div}(I)=\mathrm{div}(J)}{=} J_{\mathfrak{p}} X_{\mathfrak{p}} \underset{\text{Lemma 10.58}}{=} (JX)_{\mathfrak{p}}.$$

Since $\mathfrak{p}$ was arbitrary we get $\mathrm{div}(IX) = \mathrm{div}(JX)$ and we are done. □

Theorem 10.60 *Via the composition rule $div(I)div(J) := div(IJ)$, the set $D(\Lambda)$ is a free Abelian group with basis*

$$\mathcal{B} := \{div(\mathfrak{P}) \ : \ \mathfrak{P} \text{ the maximal divisorial ideal over } \mathfrak{p} \in ht^1(R)\}.$$

Moreover we have

(a) $div(\Lambda)$ is the neutral element of $D(\Lambda)$.

(b) For a two-sided Λ-ideal in A we have $div(J)^{-1} = div(J^{-1})$.

(c) The map

$$\Phi : D(\Lambda) \longrightarrow \bigoplus_{\mathfrak{p} \in ht^1(R)} \mathbb{Z}$$

$$div\left(\bigcap_{\mathfrak{p} \in ht^1(R)} \left(rad(\Lambda_{\mathfrak{p}})\right)^{\alpha_{\mathfrak{p}}} \right) \longmapsto (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$$

is an isomorphism of Abelian groups.

Proof.

1. Lemma 10.59 yields that our composition on $\mathrm{D}(\Lambda)$ is well-defined.
2. Choose an arbitrary class $\mathrm{div}(J)$ where we can w.l.o.g. assume that J is a divisorial Λ-ideal in A. We make some observations:
   a) We find $(\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p} \in \mathrm{ht}^1(R)} \mathbb{Z}$ with $J = \bigcap_{\mathfrak{p} \in \mathrm{ht}^1(R)} \left(\mathrm{rad}(\Lambda_{\mathfrak{p}})\right)^{\alpha_{\mathfrak{p}}}$.
   b) We have $\alpha_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p} \in \mathrm{ht}^1(R)$. Denote the $\mathfrak{p} \in \mathrm{ht}^1(R)$ with $\alpha_{\mathfrak{p}} \neq 0$ by $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Let $\mathfrak{P}_i$ be the maximal divisorial ideal over $\mathfrak{p}_i$. Now it is enough to verify that

$$\left(\left(\mathfrak{P}_1\right)^{\alpha_1} \cdots \left(\mathfrak{P}_n\right)^{\alpha_n} \right)^{\sim} = J$$

   is satisfied. But we have for an arbitrary $\mathfrak{q} \in \mathrm{ht}^1(R)$:

$$\left(\left(\mathfrak{P}_1\right)^{\alpha_1} \cdots \left(\mathfrak{P}_n\right)^{\alpha_n} \right)_{\mathfrak{q}} \underset{\text{Lemma 10.58}}{=} \left((\mathfrak{P}_1)_{\mathfrak{q}}\right)^{\alpha_1} \cdots \left((\mathfrak{P}_n)_{\mathfrak{q}}\right)^{\alpha_n}$$

$$= \begin{cases} \left(\mathrm{rad}(\Lambda_{\mathfrak{p}_i})\right)^{\alpha_i} \text{ for } \mathfrak{q} = \mathfrak{p}_i \text{ for some } 1 \leq i \leq n \\ \Lambda_{\mathfrak{q}} \text{ otherwise} \end{cases} .$$

   So $\mathrm{D}(\Lambda)$ is generated as a group by the elements of $\mathcal{B}$.

3. The elements of $\mathcal{B}$ commute when we localize at an element $\mathfrak{p} \in \mathrm{ht}^1(R)$, so $\mathrm{D}(\Lambda)$ is Abelian.

4. That there are no nontrivial relations among the elements of $\mathcal{B}$ follows immediately from the uniqueness statement of Theorem 10.26.

5. Now choose a maximal divisorial ideal $\mathfrak{P}$ of Λ. For an arbitrary element $\mathfrak{q} \in \mathrm{ht}^1(R)$ we find:

$$\begin{aligned}\left(\mathfrak{P}\mathfrak{P}^{-1}\right)_{\mathfrak{q}} &\underset{\text{Lemma 10.58}}{=} \mathfrak{P}_{\mathfrak{q}}\left(\mathfrak{P}^{-1}\right)_{\mathfrak{q}} = \mathfrak{P}_q\left(\mathfrak{P}_{\mathfrak{q}}\right)^{-1} \\ &= \begin{cases} \mathrm{rad}(\Lambda_{\mathfrak{p}})\left(\mathrm{rad}(\Lambda_{\mathfrak{p}})\right)^{-1} = \Lambda_{\mathfrak{p}} \text{ for } \mathfrak{q} = \mathfrak{p} \\ \Lambda_q\Lambda_{\mathfrak{q}} = \Lambda_{\mathfrak{q}} \text{ otherwise} \end{cases},\end{aligned}$$

   and so we are done.

6. Let us now verify the points (a) - (c):

Ad (a) For an arbitrary two-sided Λ-ideal J in A we have $J\Lambda = \Lambda J = J$.

Ad (b) Clear from the calculation we did for a maximal divisorial ideal $\mathfrak{P}$.

Ad (c) This point is obviously a corollary from our previous results.

□

Lemma 10.61 *For an element $\mathfrak{p} \in ht^1(R)$ there is a unique $1 \leq e \in \mathbb{N}$ with $div(\mathfrak{p}\Lambda) = div(\mathfrak{P})^e$. This e is the classical ramification index of $\mathfrak{p}R_{\mathfrak{p}}$ in the $R_{\mathfrak{p}}$-order $\Lambda_{\mathfrak{p}}$.*

Proof. Let $\mathfrak{q} \in \mathrm{ht}^1(R)$. First we note $(\mathfrak{q})_{\mathfrak{p}} = \begin{cases} \mathfrak{p}R_{\mathfrak{p}} \text{ for } \mathfrak{q} = \mathfrak{p} \\ R_{\mathfrak{p}} \text{ for } \mathfrak{q} \neq \mathfrak{p} \end{cases}$. So we can conclude:

$$\left(\mathfrak{p}\Lambda\right)_{\mathfrak{q}} = \begin{cases} \left(\mathrm{rad}(\Lambda_{\mathfrak{p}})\right)^e \text{ for } \mathfrak{q} = \mathfrak{p} \\ \mathfrak{p}_{\mathfrak{q}}\Lambda_{\mathfrak{q}} = \Lambda_{\mathfrak{q}} \text{ otherwise} \end{cases},$$

where e is the classical ramification index of $\mathfrak{p}R_{\mathfrak{p}}$ in the $R_{\mathfrak{p}}$-order $\Lambda_{\mathfrak{p}}$ (cf. [Rei75]). So we are done. □

Definition 10.62 *Let $\mathfrak{p} \in ht^1(R)$. The unique natural number $1 \leq e$ is called the ramification index of $\mathfrak{p}$ in Λ.*

Let us recall a well-know characterization of projective modules.

Lemma 10.63 (Dual Basis Lemma) *Let T be an arbitrary ring. For a R-module P are equivalent:*

1. *P is projective over T.*
2. *There exist an index set I and elements $p_i \in P$ $(i \in I)$ and homomorphisms $\varphi_i \in P^* = \mathrm{Hom}_T(P,T)$ $(i \in I)$ such that the following conditions are satisfied:*
   - *For every $p \in P$ we have that $\varphi_i(p) = 0$ for almost all $i \in I$.*
   - *For an element $p \in P$ holds: $p = \sum_{i \in I} \varphi_i(p)p_i$.*

Proof. Cf. [CR81, Lemma 3.46]. □

Observation 10.64 *Let $\mathfrak{a}$ be an arbitrary fractional ideal of R, then we have $\mathfrak{a}^{-1}\Lambda \subset \big(\mathfrak{a}\Lambda\big)^{-1}$.*

Proof. We just have to note

$$\mathfrak{a}\Lambda\mathfrak{a}^{-1}\Lambda \underset{K \text{ is in the center of } A}{=} \mathfrak{a}\mathfrak{a}^{-1}\Lambda\Lambda \subset R\Lambda = \Lambda.$$

□

Lemma 10.65 *Let $\mathfrak{a}$ be a divisorial ideal of R. Then $\mathfrak{a}\Lambda$ is a projective Λ-module.*

Proof. Proposition 10.10 implies that $\mathfrak{a}$ is an invertible ideal over R. We note that R is a Noetherian ring, so there are finitely many elements $a_1, \ldots, a_n \in \mathfrak{a}$ and $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}^{-1}$ with $1 = \sum_{i=1}^{n} a_i\alpha_i$. We set

$$\begin{aligned} \varphi_i : \mathfrak{a}\Lambda &\longrightarrow \Lambda \\ x &\longmapsto \alpha_i x. \end{aligned}$$

Since $\alpha_i \in \mathfrak{a}^{-1}$ holds we get immediately that $\varphi_i \in \big(\mathfrak{a}\Lambda\big)^{-1} \underset{\text{Obs. 10.45}}{=} \mathrm{Hom}_\Lambda(\mathfrak{a}\Lambda, \Lambda)$ is satisfied. For an arbitrary element $x = \sum_{j=1}^{m} \underbrace{x_j}_{\in\mathfrak{a}} \underbrace{\lambda_j}_{\in\Lambda} \in \mathfrak{a}\Lambda$ we have

$$\sum_{i=1}^{n} \varphi_i(x)a_i = \sum_{i=1}^{n} \varphi_i\big(\sum_{j=1}^{m} x_j\lambda_j\big)a_i = \sum_{i=1}^{n}\sum_{j=1}^{m} \varphi_i(x_j\lambda_j)a_i$$

$$\underset{\text{per. def. of } \varphi_i}{=} \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_i x_j \lambda_j a_i = \sum_{j=1}^{m} \underbrace{\big(\sum_{i=1}^{n} \alpha_i x_j a_i\big)}_{=x_j} \lambda_j = \sum_{j=1}^{m} x_j\lambda_j = x.$$

Hence an application of Lemma 10.63 yields that $\mathfrak{a}\Lambda$ is indeed projective over Λ.

□

There is a more general version of Lemma 10.65:

Lemma 10.66 *Let P be a projective Λ-module and $\mathfrak{a}$ a divisorial ideal of R then $\mathfrak{a}P$ is projective over Λ.*

To prove Lemma 10.66 we reformulate the Dual Basis Lemma as:

Observation 10.67 *Let S be an arbitrary ring. For an S-module P are equivalent:*

1. *P is projective over S.*
2. *The map*

$$\begin{aligned} \Psi_P : \mathrm{Hom}_S(P, S) \otimes_S M &\longrightarrow \mathrm{End}_S(P) \\ \varphi \otimes p &\longmapsto \varphi \circ p := [P \ni \tilde{p} \longmapsto \varphi(\tilde{p})p] \end{aligned}$$

is an isomorphism. Here we have to note that $\mathrm{Hom}_S(P, S) = M^*$ becomes a right S-module by setting

$$(\varphi s)(p) := \varphi(sp) \quad \textit{for all } s \in S, \varphi \in P^*, p \in P.$$

3. *The map Ψ_P is surjective.*

Proof. Straightforward with the Dual Basis Lemma, we leave the details to the reader. □

Proof of Lemma 10.66. Proposition 10.10 yields that $\mathfrak{a}$ is an invertible ideal of R. We make the following observations

1. We have $\mathfrak{a}^{-1}\operatorname{Hom}_\Lambda(P,\Lambda) \subset \operatorname{Hom}_\Lambda(\mathfrak{a}P,\Lambda)$ (just use that the relation $\mathfrak{a}\mathfrak{a}^{-1} = R$ holds.
2. Since P is projective over Λ, P is flat over Λ, so we can now identify $\mathfrak{a}^{-1}\operatorname{Hom}_\Lambda(P,\Lambda) \otimes_\Lambda \mathfrak{a}P$ with a submodule of $\operatorname{Hom}_\Lambda(\mathfrak{a}P,\Lambda) \otimes_\Lambda \mathfrak{a}P$.
3. If we can show that the restriction of $\Psi_{\mathfrak{a}P}$ to $\mathfrak{a}^{-1}\operatorname{Hom}_\Lambda(P,\Lambda)\otimes_\Lambda P$ is surjective we are done by Observation 10.67. We have of course

$$\Psi_{\mathfrak{a}P}(\mathfrak{a}^{-1}\operatorname{Hom}_\Lambda(P,\Lambda) \otimes_\Lambda \mathfrak{a}P) = \mathfrak{a}^{-1}\mathfrak{a}\Psi_P(\operatorname{Hom}_\Lambda(P,\Lambda) \otimes_\Lambda P)$$
$$\underset{\mathfrak{a}\text{ is invertible}}{=} R\Psi_P(\operatorname{Hom}_\Lambda(P,\Lambda) \otimes_\Lambda P) \underset{P\text{ projective and Observation 10.67}}{=} \Lambda,$$

so we are done.

□

Lemma 10.68 *Direct summands of reflexive modules are reflexive.*

Proof. Let M and N be two S-modules, where S denotes an arbitrary commutative ring. We assume that $M \oplus N$ is reflexive. Let $\tau : M \oplus N \longrightarrow (M \oplus N)^{**}$ be the canonical map, which is – by our assumption – an isomorphism. We know that we have a canonical isomorphism $(M \oplus N)^{**} \simeq M^{**} \oplus N^{**}$. So it is enough to show that $\tau = \tau_M \oplus \tau_N$ holds. Choose $\alpha \in (M \oplus N)^* \simeq M^* \oplus N^*$, so we can write $\alpha = \alpha_M + \alpha_N$. Then for an element $(m,n) \in M \oplus N$ we find $\tau_{(m,n)}(\alpha) = \tau_{(m,n)}(\alpha_M + \alpha_N) = \alpha_M(m) + \alpha_N(n) = (\tau_M)_m(\alpha_M) + (\tau_N)_n(\alpha_N)$ and we are done. □

Corollary 10.69 *Let $\mathfrak{a}$ be a divisorial ideal of R, then $\mathfrak{a}\Lambda$ is a divisorial two-sided ideal of Λ.*

Proof. Lemma 10.65 implies that $\mathfrak{a}\Lambda$ is projective as Λ-module. Λ is divisorial as an R-lattice, hence reflexive by Theorem 10.24. So $\mathfrak{a}\Lambda$ is a direct summand of a reflexive R-module, an application of Lemma 10.68 yields therefor that $\mathfrak{a}\Lambda$ is a reflexive R-module. Now we can again use Theorem 10.24 to conclude that $\mathfrak{a}\Lambda$ is divisorial over R. □

Notation 10.70 *Let us denote the group of fractional divisorial R-ideals by $D(R)$.*

Observation 10.71 *Let $\mathfrak{a} \subset R$ be an arbitrary divisorial ideal of R. We have $(\mathfrak{a}\Lambda)^{-1} = \mathfrak{a}^{-1}\Lambda$.*

Proof. We know from Observation 10.64 that the relation $\mathfrak{a}^{-1}\Lambda \subset (\mathfrak{a}\Lambda)^{-1}$ holds. Now Corollary 10.69 induces that $\mathfrak{a}\Lambda$ is a divisorial ideal of Λ, so $(\mathfrak{a}\Lambda)^{-1}$ is also divisorial by Corollary 10.51. This yields – with the help of Proposition 10.25 – that $\mathfrak{b} := (\mathfrak{a}\Lambda)^{-1} \cap K$ is divisorial, hence projective (by Proposition 10.10). We have

obviously $\mathfrak{a}^{-1} \subset \mathfrak{b}$. If $\mathfrak{a}^{-1} \subsetneq \mathfrak{b}$ holds we get immediately that there is a non integral element x in $\mathfrak{ab}$, this element x lies of course also in $\mathfrak{a}\Lambda\left(\mathfrak{a}\Lambda\right)^{-1} \subset \Lambda$, a contradiction. □

Proposition 10.72 *Let S be a commutative ring. Let E be a flat S-module, F an arbitrary S-module, with two submodules F_1 and F_2. We have*

$$E \otimes_S (F_1 \cap F_2) = (E \otimes_S F_1) \cap (E \otimes_S F_2).$$

Proof. Cf. [Bou89a, 1.6 Proposition 6 and the following Remark 1]. □

Lemma 10.73 *Let $\mathfrak{a}$ be a divisorial ideal of R, then we have $\mathfrak{a}\Lambda \cap R = \mathfrak{a}$.*

Proof. We know by Corollary 10.69 that $\mathfrak{a}\Lambda$ is a divisorial ideal of Λ. So $\mathfrak{b} := \mathfrak{a}\Lambda \cap R$ is a divisorial ideal of R (just use Lemma 10.29). We have surely $\mathfrak{a} \subset \mathfrak{b}$. Choose an arbitrary element $\mathfrak{p} \in \mathrm{ht}^1(R)$. We get

$$\mathfrak{a}_\mathfrak{p} \subset \mathfrak{b}_\mathfrak{p} = (\mathfrak{a}\Lambda \cap R)_\mathfrak{p} \underset{\text{Lemma 10.72}}{=} (\mathfrak{a}\Lambda)_\mathfrak{p} \cap R_\mathfrak{p}.$$

By Theorem 10.13 we get a unique decomposition $\mathfrak{a} = \mathfrak{p}^\alpha \mathfrak{q}$ with $\alpha \in \mathbb{N}$ and $\mathfrak{q}$ is a product of elements from $\mathrm{ht}^1(R)$ which are all distinct from $\mathfrak{p}$. We conclude

$$(\mathfrak{a}\Lambda)_\mathfrak{p} \cap R_\mathfrak{p} = \mathfrak{p}^n \Lambda_\mathfrak{p} \cap R_\mathfrak{p} = \left(\mathfrak{p}R_\mathfrak{p}\right)^n.$$

Hence for every element $\mathfrak{p} \in \mathrm{ht}^1(R)$ we have $\mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$, this implies $\mathfrak{a} = \mathfrak{b}$ since $\mathfrak{a}$ and $\mathfrak{b}$ are divisorial ideals of R and we are done. □

Lemma 10.74 *There is an injection of Abelian groups*

$$\begin{aligned} \varphi : D(R) &\longrightarrow D(\Lambda) \\ \mathfrak{a} &\longmapsto \mathit{div}(\mathfrak{a}\Lambda), \end{aligned}$$

so $D(R)$ can be identified with a subgroup of $D(\Lambda)$.

Proof. We know that $\mathrm{D}(R)$ is free on the elements of $\mathrm{ht}^1(R)$, so a well-defined homomorphism of Abelian groups $\alpha : \mathrm{D}(R) \longrightarrow \mathrm{D}(\Lambda)$ is induced by the rule $\mathrm{ht}^1(R) \ni \mathfrak{p} \longmapsto \mathrm{div}(\mathfrak{p}\Lambda) \in \mathrm{D}(\Lambda)$. For an arbitrary $\mathfrak{p} \in \mathrm{ht}^1(R)$ we have $\varphi(\mathfrak{p}) = \alpha(\mathfrak{p})$, this observation yields that $\varphi = \alpha$ is satisfied. So φ is indeed a well-defined homomorphism of Abelian groups. Now assume that a fractional divisorial ideal $\mathfrak{a}$ of K is in the kernel of φ. We find a decomposition $\mathfrak{a} = \mathfrak{a}_1(\mathfrak{a}_2)^{-1}$ for uniquely determined ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of R. Then

$$\varphi(\mathfrak{a}) = \varphi(\mathfrak{a}_1)(\varphi(\mathfrak{a}_2))^{-1} = \mathrm{div}(\mathfrak{a}_1\Lambda)\mathrm{div}(\mathfrak{a}_2\Lambda)^{-1} = \mathrm{div}(\Lambda).$$

Since $\mathrm{D}(\Lambda)$ is a group we get $\mathrm{div}(\mathfrak{a}_1\Lambda) = \mathrm{div}(\mathfrak{a}_2\Lambda)$. Corollary 10.69 implies that both $\mathfrak{a}_1\Lambda$ and $\mathfrak{a}_2\Lambda$ are divisorial ideals of Λ. Hence we get $\mathfrak{a}_1\Lambda = \mathfrak{a}_2\Lambda$. Then Lemma 10.73 implies immediately $\mathfrak{a}_1 = \mathfrak{a}_2$, so $\mathfrak{a} = \mathfrak{a}_1(\mathfrak{a}_2)^{-1} = R$. So φ is an injection – as claimed. □

Lemma 10.75 *Assume that $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \mathit{frac}(R/\mathfrak{p})$ is a perfect field for every element $\mathfrak{p} \in \mathit{ht}^1(R)$. For a prime ideal $\mathfrak{p} \in \mathit{ht}^1(R)$ we denote the ramification index of $\mathfrak{p}$ in Λ by $e(\mathfrak{p})$. Then*

1. *There are only finitely many elements* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in ht^1(R)$ *with* $e(\mathfrak{p}_i) \neq 1$.
2. *We have moreover*
$$D(\Lambda)/D(R) \simeq \prod_{i=1}^{n} \mathbb{Z}/e(\mathfrak{p}_i)\mathbb{Z}$$
is a finite group.

Proof. We denote the maximal divisorial ideal of Λ which is over $\mathfrak{p} \in \mathrm{ht}^1(R)$ by $\mathfrak{P}(\mathfrak{p})$. An application of Lemma 8.30 yields that there are only finitely many elements $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathrm{ht}^1(R)$ such that $\Lambda_\mathfrak{p}$ is not separable over $R_\mathfrak{p}$. Now choose an arbitrary element $\mathfrak{p} \in \mathrm{ht}^1(R)$. We have to distinguish two cases:

1. $\mathfrak{p} \neq \mathfrak{p}_i$ for all $1 \leq i \leq n$: Here we have that $\Lambda_\mathfrak{p}$ is a separable $R_\mathfrak{p}$-order. We know that $R_\mathfrak{p}$ has a perfect residue class field, so an application of Lemma 8.8 yields that $\mathrm{rad}(\Lambda_\mathfrak{p}) = (\mathfrak{p}R_\mathfrak{p})\Lambda_\mathfrak{p}$ holds. Therefore we get $\mathrm{div}(\mathfrak{p}\Lambda) = \mathrm{div}(\mathfrak{P}(\mathfrak{p}))$, so $\mathrm{div}(\mathfrak{P})$ is the image of $\mathfrak{p}$ under the embedding of $\mathrm{D}(R)$ into $\mathrm{D}(\Lambda)$.
2. Assume now that we have $\mathfrak{p} = \mathfrak{p}_i$ for some i. We set $\mathfrak{P}_i = \mathfrak{P}(\mathfrak{p})$. An application of Lemma 10.61 yields that we have $\mathrm{div}(\mathfrak{P}_i)^{e(\mathfrak{p}_i)} = \mathrm{div}(\mathfrak{p}\Lambda)$.

Putting this data together we have after identifying $\mathrm{D}(R)$ with the image in $\mathrm{D}(\Lambda)$ and applying the isomorphism stated in Theorem 10.60 (c):
$$\mathrm{D}(R) = \left(\bigoplus_{\mathfrak{p}_i \neq \mathfrak{p} \in \mathrm{ht}^1(R)} \mathbb{Z} \right) \bigoplus \left(\bigoplus_{i=1}^{n} e(\mathfrak{p}_i)\mathbb{Z} \right) \quad \text{and}$$
$$\mathrm{D}(\Lambda) = \left(\bigoplus_{\mathfrak{p}_i \neq \mathfrak{p} \in \mathrm{ht}^1(R)} \mathbb{Z} \right) \bigoplus \left(\bigoplus_{i=1}^{n} \mathbb{Z} \right),$$
this yields immediately that we get
$$\mathrm{D}(\Lambda)/\mathrm{D}(R) \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/e(\mathfrak{p}_i)\mathbb{Z}.$$
That the last group is finite is obvious and so we are done. □

Lemma 10.76 *Let* J *be an ideal of* Λ. *The ideal* $\mathfrak{a} := R \cap J$ *is the unique ideal* $\mathfrak{b}$ *of* R *such that* $\mathfrak{b}$ *is maximal with the property* $\mathfrak{b}\Lambda \subset J$.

Proof.

- Let $\mathfrak{b}$ be an arbitrary ideal of R such that $\mathfrak{b}\Lambda \subset J$. Then we get of course $\mathfrak{b}(\Lambda/J) = 0$, hence
$$\mathfrak{b} \subset \mathrm{Ann}_R(\Lambda/J) \underset{\text{Observation 10.31}}{=} J \cap R.$$
So we have for every ideal $\mathfrak{b}$ of R: $\mathfrak{b}\Lambda \subset J \Longrightarrow \mathfrak{b} \subset J \cap R$.
- Now assume that $\mathfrak{b}$ and $\tilde{\mathfrak{b}}$ are both maximal with the mentioned property. Then we get $(\mathfrak{b} + \tilde{\mathfrak{b}})\Lambda \subset J$ and so we must have $\mathfrak{b} = \tilde{\mathfrak{b}}$. So there can be only one maximal $\mathfrak{b}$.
- Finally we have $\mathfrak{a}\Lambda \subset J$, since $\mathfrak{a} = \mathrm{Ann}_R(\Lambda/J)$ holds. So $\mathfrak{a}$ has to be contained in the unique ideal $\mathfrak{b}$ of R with the property $\mathfrak{b}\Lambda \subset J$. Now we can conclude that $\mathfrak{a}$ is this unique ideal.

□

Example 10.77 *Let S be a Dedekind domain with field of fractions L and Γ a maximal S-order in some central simple L-algebra. Let $\mathfrak{P}$ and $\mathfrak{Q}$ be different prime ideals of Γ corresponding to prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of S. Then we have $Ann_S(\Lambda/\mathfrak{P}\mathfrak{Q}) = \mathfrak{p}\mathfrak{q}$.*

Proof.

- Observation 10.76 yields that $\mathrm{Ann}_S(\Lambda/\mathfrak{P}\mathfrak{Q})$ is the unique ideal $\mathfrak{a}$ of S maximal with the property that $\mathfrak{a}\Lambda \subset \mathfrak{P}\mathfrak{Q}$ is satisfied. By the one-to-one correspondence between the maximal ideals of S and the prime ideals of Γ we get $\mathfrak{p} \subset \mathfrak{P}$ and $\mathfrak{q} \subset \mathfrak{Q}$. Hence $\mathfrak{p}\mathfrak{q} \subset \mathfrak{P}\mathfrak{Q}$ and so $\mathfrak{p}\mathfrak{q} \subset \mathfrak{a} \neq S$.
- Since S is a Dedekind domain, the ideal $R \neq \mathfrak{a} \supset \mathfrak{p}\mathfrak{q}$ can only be contained in $\mathfrak{p}$ or in $\mathfrak{q}$. So assume for example $\mathfrak{a} = \mathfrak{p}$.Then we have $\mathfrak{p}\Lambda \subset \mathfrak{P}\mathfrak{Q}$. We localize at the prime ideal $\mathfrak{q}$ and get (where we observe [Rei75, Theorem 22.4]):

$$R_{\mathfrak{q}} \underset{\mathfrak{p}\neq\mathfrak{q}}{=} \mathfrak{p}_{\mathfrak{q}} \subset (\mathfrak{P}\mathfrak{Q})_{\mathfrak{q}} = \mathfrak{P}_{\mathfrak{q}}\mathfrak{Q}_{\mathfrak{q}} = \mathrm{rad}(\Lambda_{\mathfrak{q}})\Lambda_{\mathfrak{q}} = \mathrm{rad}(\Lambda_{\mathfrak{q}}),$$

  hence $1 \in \mathrm{rad}(\Lambda_{\mathfrak{q}})$ an obvious contradiction.

□

In the proof of Example 10.77 we have used that $\mathfrak{p}$ and $\mathfrak{q}$ are both maximal ideals. This example is just a special case of a more general result, which can be proved by just using that $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p}\mathfrak{q}$ holds:

Lemma 10.78 *Let $\mathfrak{P}$ and $\mathfrak{Q}$ be different maximal divisorial two-sided ideals of Λ, corresponding to $\mathfrak{p}$ and $\mathfrak{q}$ in $ht^1(R)$. Then we have*

$$(\mathfrak{P} \cap \mathfrak{Q}) \cap R = (\mathfrak{P}\mathfrak{Q}) \cap R = \mathfrak{p}\mathfrak{q}.$$

Proof. We make some observations:

- $\mathfrak{p} \subset \mathfrak{P}, \mathfrak{q} \subset \mathfrak{Q} \implies \mathfrak{p}\mathfrak{q} \subset \mathfrak{P}\mathfrak{Q}$.
- $\mathfrak{P} \cap R = \mathfrak{p}$, $\mathfrak{Q} \cap R = \mathfrak{q}$.
- $\mathfrak{P}\mathfrak{Q} \subset \mathfrak{P} \cap \mathfrak{Q}$.

So we can conclude:

$$\mathfrak{p}\mathfrak{q} \subset (\mathfrak{P}\mathfrak{Q}) \cap R \subset (\mathfrak{P} \cap \mathfrak{Q}) \cap R = (\mathfrak{P} \cap R) \cap (\mathfrak{Q} \cap R) = \mathfrak{p} \cap \mathfrak{q} \underset{\text{Lemma 10.18}}{=} \mathfrak{p}\mathfrak{q},$$

and we are done. □

Observation 10.79 *Let V be a finite dimensional vector space over K and M, N two torsionfree R-modules in V (we don't assume M and N to be full R-lattices in V). Then we have $\widetilde{(M \cap N)} = \tilde{M} \cap \tilde{N}$.*

Proof. We have

$$\tilde{M} \cap \tilde{N} = \left(\bigcap_{\mathfrak{p}\in \mathrm{ht}^1(R)} M_{\mathfrak{p}}\right) \bigcap \left(\bigcap_{\mathfrak{p}\in \mathrm{ht}^1(R)} N_{\mathfrak{p}}\right) = \bigcap_{\mathfrak{p}\in \mathrm{ht}^1(R)} \left(M_{\mathfrak{p}} \cap N_{\mathfrak{p}}\right)$$
$$\underset{\text{Lemma 10.72}}{=} \bigcap_{\mathfrak{p}\in \mathrm{ht}^1(R)} \left(M \cap N\right)_{\mathfrak{p}} = \widetilde{M \cap N}.$$

□

Corollary 10.80 *Let J be an ideal of Λ. We have $\widetilde{J \cap R} = \tilde{J} \cap R$.*

Proof. $\tilde{J} \cap R \underset{R \text{ is divisorial}}{=} \tilde{J} \cap \tilde{R} \underset{\text{Observation 10.79}}{=} \widetilde{J \cap R}$. □

Lemma 10.81 *Let $\mathfrak{P}_i$ - as usual - the maximal divisorial two-sided ideal over $\mathfrak{p}_i \in ht^1(R)$. For $\alpha_i \in \mathbb{N}$ (with $1 \leq i \leq k$) we have*

$$\left(\mathfrak{P}_1{}^{\alpha_1} \cdots \mathfrak{P}_k{}^{\alpha_k}\right)^{\sim} = \left(\cap_{i=1}^{k} \mathfrak{P}_i{}^{\alpha_i}\right)^{\sim}.$$

Proof. Let $\mathfrak{p} \in \mathrm{ht}^1(R)$ be an arbitrary element.

- $\left(\mathfrak{P}_1{}^{\alpha_1} \cdots \mathfrak{P}_k{}^{\alpha_k}\right)_{\mathfrak{p}} \underset{\text{Proposition 10.72}}{=} \Pi_{i=1}^{k} \left((\mathfrak{P}_i)_{\mathfrak{p}}\right)^{\alpha_i} = \begin{cases} \Lambda_{\mathfrak{p}} \text{ for } \mathfrak{p} \neq \mathfrak{p}_i \; \forall i \\ (\mathrm{rad}(\Lambda_{\mathfrak{p}}) \text{ for } \mathfrak{p} = \mathfrak{p}_i \end{cases}$
- Moreover we get

$$\left(\bigcap_{i=1}^{k} \mathfrak{P}_i{}^{\alpha_i}\right)_{\mathfrak{p}} \underset{\text{Proposition 10.72}}{=} \bigcap_{i=1}^{k} \left(\mathfrak{P}_i{}^{\alpha_i}\right)_{\mathfrak{p}} = \bigcap_{i=1}^{k} \left(\mathfrak{P}_{i\mathfrak{p}}\right)^{\alpha_i} \underset{\text{Proposition 10.72}}{=} \begin{cases} \Lambda_{\mathfrak{p}} \text{ for } \mathfrak{p} \neq \mathfrak{p}_i \; \forall i \\ (\mathrm{rad}(\Lambda_{\mathfrak{p}}) \text{ for } \mathfrak{p} = \mathfrak{p}_i \end{cases}.$$

□

Lemma 10.82 *Let $J \subset \Lambda$ be a divisorial two-sided ideal, with the property $div(J) = \Pi_{i=1}^{k} div(\mathfrak{P}_i)^{\alpha_i}$, where $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ denote maximal divisorial two-sided ideals of Λ. Then we have equalities*

$$J = \bigcap_{i=1}^{k} \widetilde{\mathfrak{P}_i{}^{\alpha_i}} = \widetilde{\prod_{i=1}^{k} \mathfrak{P}_i{}^{\alpha_i}}.$$

Proof.

1. The second equality is immediately deduced from Observation 10.79 and Lemma 10.81.
2. We set $J' := \bigcap_{i=1}^{k} \widetilde{\mathfrak{P}_i{}^{\alpha_i}}$. By Observation 10.79 we can conclude

$$\tilde{J'} = \bigcap_{i=1}^{k} \widetilde{\widetilde{\mathfrak{P}_i{}^{\alpha_i}}} \underset{\widetilde{\mathfrak{P}_i{}^{\alpha_i}} \text{ is divisorial}}{=} \bigcap_{i=1}^{k} \widetilde{\mathfrak{P}_i{}^{\alpha_i}} = J',$$

   hence J' is a divisorial ideal of Λ.
3. By (1) is is enough to verify that for an arbitrary $\mathfrak{p} \in \mathrm{ht}^1(R)$ holds $J_{\mathfrak{p}} = J'_{\mathfrak{p}}$. So let us fix some $\mathfrak{p} \in \mathrm{ht}^1(R)$, we have
   - $J_{\mathfrak{p}} \underset{\substack{\text{we know the structure} \\ \text{of } \mathrm{div}(J) \in \mathrm{D}\Lambda}}{=} \begin{cases} \mathrm{rad}(\Lambda_{\mathfrak{p}})^{\alpha_i} \text{ if } \mathfrak{p} = \mathfrak{p}_i \text{ for some } i \\ \Lambda_{\mathfrak{p}} \text{ otherwise} \end{cases}.$

- Moreover

$$(J')_{\mathfrak{p}} = \Big(\bigcap_{i=1}^{k} \widetilde{\mathfrak{P}^{\alpha_i}}\Big)_{\mathfrak{p}} \underset{\text{Proposition 10.79}}{=} \bigcap_{i=1}^{k} \Big(\widetilde{\mathfrak{P}_i{}^{\alpha_i}}\Big)_{\mathfrak{p}}$$

$$\underset{\text{Observation 10.48}}{=} \bigcap_{i=1}^{k} \Big(\mathfrak{P}_i{}^{\alpha_i}\Big)_{\mathfrak{p}} \underset{\text{Proposition 10.79}}{=} \bigcap_{i=1}^{k} \Big(\mathfrak{P}_{i\mathfrak{p}}\Big)^{\alpha_i}$$

$$= \begin{cases} \mathrm{rad}(\Lambda_{\mathfrak{p}_i})^{\alpha_i} & \mathfrak{p} = \mathfrak{p}_i \text{ for some } i \\ \Lambda_{\mathfrak{p}} & \text{otherwise} \end{cases}$$

□

Definition 10.83 *Let J and J' be two divisorial two-sided ideals of Λ such that $div(J) = \Pi_{i=1}^{k} div(\mathfrak{P}_i)^{\alpha_i}$ and $div(J') = \Pi_{j=1}^{l} div(\mathfrak{Q}_j)^{\beta_j}$, where the $\mathfrak{P}_i$'s and the $\mathfrak{Q}_j$'s are maximal divisorial two-sided ideals of Λ. We call J and J' disjoint if $\mathfrak{P}_i \neq \mathfrak{Q}_j$ holds for all i and j.*

Observations 10.84 *Let J be any divisorial two-sided ideal of Λ such that $J \neq \Lambda$ holds. We set $J \cap R =: \mathfrak{a}$. By Lemma 10.29 we know that $\mathfrak{a}$ is a divisorial ideal of R, hence contained in some $\mathfrak{p}$ from $ht^1(R)$.*

1. $(J \cap R)_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} \underset{\substack{\text{Localizations} \\ \text{preserve inclusions}}}{\subset} \mathfrak{p}R_{\mathfrak{p}}$.

2. *$J_{\mathfrak{p}}$ is a two-sided ideal of $\Lambda_{\mathfrak{p}}$. Since $R_{\mathfrak{p}}$ is a discrete valuation domain and $\Lambda_{\mathfrak{p}}$ is a maximal $R_{\mathfrak{p}}$-order we get from Theorem 9.5 that $J_{\mathfrak{p}}$ is a power of $rad(\Lambda_{\mathfrak{p}})$. If $J_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$ holds, we get $1 \in J_{\mathfrak{p}} \cap R_{\mathfrak{p}} \subset \mathfrak{p}R_{\mathfrak{p}}$, an obvious contradiction.*

3. *By (2) we get $J_{\mathfrak{p}} \subset rad(\Lambda_{\mathfrak{p}})$. Let $\mathfrak{P}$ be the maximal divisorial ideal of Λ which is over $\mathfrak{p}$. We get now $div(J) = div(\mathfrak{P})^{\alpha} div(Q)$ for some divisorial ideal Q of Λ and some $\alpha \geq 1$.*

Corollary 10.85 *Let J and J' two disjoint two-sided divisorial ideals of Λ and set $\mathfrak{a} := J \cap R$, $\mathfrak{a} := J' \cap R$. Then $\mathfrak{a}$ and $\mathfrak{b}$ are disjoint.*

Proof. Assume the contrary. Then we get $\mathfrak{a} \subset \mathfrak{p}$ and $\mathfrak{b} \subset \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{ht}^1(R)$. But Observations 10.84 yields now that $J \subset \mathfrak{P}$ and $J' \subset \mathfrak{P}$ holds for $\mathfrak{P}$ over $\mathfrak{p}$, but we have assumed that J and J' are disjoint. □

Lemma 10.86 *Let J and J' be disjoint divisorial two-sided ideals of Λ with $\mathfrak{a} = J \cap R$ and $\mathfrak{b} = J' \cap R$. Then we have*

$$JJ' \cap R = (J \cap J') \cap R = \mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}.$$

Proof. Corollary 10.85 yields that the two divisorial ideals $\mathfrak{a}$ and $\mathfrak{b}$ are disjoint, hence an application of Lemma 10.20 gives $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. We make a trivial observation: Let J_0 be some divisorial two-sided ideal of Λ with $\mathfrak{c} := J_0 \cap R$, then $\mathfrak{c} \subset J_0$, hence $\mathfrak{c}\Lambda \subset J_0$. By this observation we get $\mathfrak{a} \subset J$, $\mathfrak{b} \subset J^{'}$, hence

$$\mathfrak{ab} \subset JJ^{'} \underset{J,J^{'} \text{ are two sided ideals}}{\subset} J \cap J^{'}.$$

We conclude

$$\mathfrak{ab} \subset JJ^{'} \cap R \subset (J \cap J^{'}) \cap R = (J \cap R) \cap (J^{'} \cap R) = \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}.$$

□

Corollary 10.87 *Let J be a divisorial two-sided ideal of Λ with $J = \bigcap_{i=1}^{k} \widetilde{\mathfrak{P}_i^{\alpha_i}}$ (where $\mathfrak{P}_i$ is the maximal divisorial two-sided ideal over $\mathfrak{p}_i \in ht^1(R)$). Moreover we set $\mathfrak{a}_i := \widetilde{\mathfrak{P}_i^{\alpha_i}}$ and get $J \cap R = \Pi_{i=1}^{k} \mathfrak{a}_i = \bigcap_{i=1}^{k} \mathfrak{a}_i$.*

Proof. This is immediately deduced from Lemma 10.86. □

Lemma 10.88 *Let $\mathfrak{p} \in ht^1(R)$ and $\mathfrak{P}$ the corresponding maximal divisorial two-sided ideal of Λ. For every $1 \leq \alpha \in \mathbb{N}$ we have that $\mathfrak{a} := \widetilde{\mathfrak{P}^{\alpha}} \cap R$ is a power of $\mathfrak{p}$.*

Proof.

- Since $\widetilde{\mathfrak{P}^{\alpha}}$ is a divisorial ideal of Λ, we get from Lemma 10.29 that $\mathfrak{a}$ is a divisorial ideal of R.
- Assume that $\mathfrak{a}$ is contained in some $\mathfrak{q} \neq \mathfrak{p}$. Then Observations 10.84 yields $\mathrm{div}(\widetilde{\mathfrak{P}^{\alpha}}) = \mathrm{div}(\mathfrak{Q})\mathrm{div}(J^{'})$ with $\mathfrak{Q}$ over $\mathfrak{q}$ and $J^{'}$ some divisorial ideal of Λ, a contradiction.
- Since $\alpha \geq 1$ holds we get immediately that $\mathfrak{a} \neq R$ is satisfied and so $\mathfrak{a}$ has to be contained in at least one element of $\mathrm{ht}^1(R)$.
- All in all we can conclude that $\mathfrak{a}$ is a power of $\mathfrak{p}$.

□

Theorem 10.89 *Let J be divisorial two-sided ideal of Λ with $\mathfrak{a} := J \cap R$. The following are equivalent:*

1. *$div(J) \in \langle div(\mathfrak{P}_1), \ldots, div(\mathfrak{P}_k) \rangle$*
2. *$\mathfrak{a} \in \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_k \rangle$,*

where the $\mathfrak{P}_i$'s are maximal divisorial ideals of Λ with $\mathfrak{P}_i \cap R = \mathfrak{p}_i \in ht^1(R)$.

Proof. (1) $\Longrightarrow$ (2) : By assumption on J we have $J = \bigcap_{i=1}^{k} \widetilde{\mathfrak{P}_i^{\beta_i}}$ for some maximal divisorial two-sided ideals $\mathfrak{P}_i$. By Corollary 10.87 we have $\mathfrak{a} = J \cap R = \Pi_{i=1}^{k} \mathfrak{a}_i$, with $\mathfrak{a}_i = \widetilde{\mathfrak{P}_i^{\beta_i}}$. With Lemma 10.88 we can conclude that $\mathfrak{a}_i$ is a power of $\mathfrak{p}_i$ and so we get immediately $\mathfrak{a} \in \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_k \rangle$.

(2) $\Longrightarrow$ (1) : Assume $\mathfrak{a} = \mathfrak{q}\mathfrak{a}'$ for some $\mathfrak{q} \in \mathrm{ht}^1(R)$ with $\mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. Then Observations 10.84 yields $\mathrm{div}(J) = \mathrm{div}(\mathfrak{Q})\mathrm{div}(J')$ for $\mathfrak{Q}$ the maximal divisorial two-sided ideal over $\mathfrak{q}$ and J' some divisorial two-sided ideal of Λ, hence a contradiction to our assumption and we are done. □

Let us fix some notations. Let $\mathfrak{p} \in \mathrm{ht}^1(R)$ and $\mathfrak{P}$ the corresponding maximal divisorial two-sided ideal of Λ. Moreover choose some $1 \leq \alpha \in \mathbb{N}$ and set $\mathfrak{a} := \widetilde{\mathfrak{P}^\alpha} \cap R$. Let e be the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ (i.e., $\mathrm{div}(\mathfrak{p}\Lambda) = \mathrm{div}(\mathfrak{P}^e)$). By Lemma 10.88 we get $\mathfrak{a} = \mathfrak{p}^\beta$ for some $1 \leq \beta \in \mathbb{N}$. Let us determine this β.

Observation 10.90 *Let $1 \leq \alpha \leq e$, then we have $\widetilde{\mathfrak{P}^\alpha} \cap R = \mathfrak{p}$ and so $\beta = 1$.*

Proof. Assume $\mathfrak{a} = \mathfrak{p}^k$ for some $k \geq 2$. Then we get:

$$\widetilde{\mathfrak{P}^\alpha} \cap R = \mathfrak{p}^k \underset{\text{Lemma 10.72}}{\Longrightarrow} \left(\widetilde{\mathfrak{P}^\alpha}\right)_{\mathfrak{p}} \cap R_{\mathfrak{p}} = \mathfrak{p}^k R_{\mathfrak{p}} \Longrightarrow \left(\mathfrak{P}^\alpha\right)_{\mathfrak{p}} \cap R_{\mathfrak{p}} = \mathfrak{p}^k R_{\mathfrak{p}}$$
$$\Longrightarrow \left(\mathfrak{P}_{\mathfrak{p}}\right)^\alpha \cap R_{\mathfrak{p}} = \mathfrak{p}^k R_{\mathfrak{p}} \underset{\mathfrak{P}_{\mathfrak{p}} = \mathrm{rad}(\Lambda_{\mathfrak{p}})}{\Longrightarrow} \left(\mathrm{rad}(\Lambda_{\mathfrak{p}})\right)^\alpha \cap R_{\mathfrak{p}} = \mathfrak{p}^k R_{\mathfrak{p}}.$$

Since $\alpha \leq e$ holds we can conclude furthermore:

$$\underbrace{\mathfrak{p}\Lambda_{\mathfrak{p}} \cap R_{\mathfrak{p}}}_{\underset{\text{Lemma 10.73}}{=} \mathfrak{p}R_{\mathfrak{p}}} \underset{\text{per. def. of } e}{=} \left(\mathrm{rad}(\Lambda_{\mathfrak{p}})\right)^e \cap R_{\mathfrak{p}} \underset{\alpha \leq e}{\subset} \left(\mathrm{rad}(\Lambda_{\mathfrak{p}})\right)^\alpha \cap R_{\mathfrak{p}} = \mathfrak{p}^k R_{\mathfrak{p}},$$

a contradiction to Nakayama's Lemma. □

Observation 10.91 *For all $1 \leq k \in \mathbb{N}$ we have*

$$\widetilde{\mathfrak{P}^{ke}} \cap R = \mathfrak{p}^k.$$

Proof. We find

$$\left(\widetilde{\mathfrak{P}^{ke}}\right)_{\mathfrak{p}} \cap R_{\mathfrak{p}} = \left(\mathfrak{P}^{ke}\right)_{\mathfrak{p}} \cap R_{\mathfrak{p}} = \left(\mathfrak{P}_{\mathfrak{p}}\right)^{ke} \cap R_{\mathfrak{p}} = \left(\mathrm{rad}(\Lambda_{\mathfrak{p}})\right)^{ke} \cap R_{\mathfrak{p}}$$
$$= \left(\mathfrak{p}\Lambda_{\mathfrak{p}}\right)^k \cap R_{\mathfrak{p}} = \mathfrak{p}^k \Lambda_{\mathfrak{p}} \cap R_{\mathfrak{p}} \underset{\text{Lemma 10.73}}{=} \mathfrak{p}^k R_{\mathfrak{p}}$$

and so we are done. □

Notation 10.92 *For an element $\gamma \in \mathbb{R}$ we set*

$$\lceil \gamma \rceil := \min \{a \in \mathbb{Z} \mid a \geq \gamma\}.$$

Lemma 10.93 *Let $\mathfrak{p} \in ht^1(R)$ and $\mathfrak{P} \subset \Lambda$ the corresponding maximal divisorial ideal of Λ. Let $e = e(\mathfrak{P}/\mathfrak{p})$ be the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. Moreover let $n \in \mathbb{N}$, then we find uniquely determined elements $k \in \mathbb{N}$ and $m \in \mathbb{N}$ with $0 \leq m \leq e-1$ such that $n = ke + m$ holds and get*

$$\widetilde{\mathfrak{P}^n} \cap R = \mathfrak{p}^{\lceil \frac{n}{e} \rceil}.$$

Proof. Analogous arguments to the proofs of Observations 10.90 and 10.91. □

Remark 10.94 *The well-defined map*

$$\Phi : D(\Lambda) \longrightarrow D(R)$$
$$div(J) \longmapsto \tilde{J} \cap R$$

is in general not *a group homomorphism.*

Counterexample. Choose a pair $\mathfrak{p}$ and $\mathfrak{P}$ with $e = e(\mathfrak{P}/\mathfrak{p}) \geq 2$, for simplicity assume $e = 2$. Then we get

$$\Phi(\mathrm{div}(\mathfrak{P}))\Phi(\mathrm{div}(\mathfrak{P})) = \mathfrak{p}\mathfrak{p} = \mathfrak{p}^2$$

and on the other side

$$\mathfrak{p} = \Phi(\mathrm{div}(\mathfrak{p}\Lambda)) \underset{e=2}{=} \Phi(\mathrm{div}(\mathfrak{P})\mathrm{div}(\mathfrak{P})) = \Phi(\mathrm{div}(\mathfrak{P}^2)).$$

□

11 Another Characterization of Maximal Divisorial Ideals

We assume in this section that R is a local Krull-Domain with maximal ideal $\mathfrak{m}$, moreover we assume that R is a factorial ring with Krull-dimension ≥ 2. The field of fractions of R is denoted by K and Λ is - as in the last chapter - assumed to be a maximal R-order in a central simple K-algebra B.

Lemma 11.1 *We have $\tilde{\mathfrak{m}} = R$ and so in particular $\widetilde{\mathfrak{m}\Lambda} = \Lambda$.*

Proof.

- R is a local ring and $\mathfrak{m}$ is its radical. Since the Krull-dimension of R is ≥ 2 the radical $\mathfrak{m}$ contains every $\mathfrak{p} \in \mathrm{ht}^1(R)$ properly. So we get for an arbitrary $\mathfrak{p} \in \mathrm{ht}^1(R)$ that $\mathfrak{m}_\mathfrak{p} = R_\mathfrak{p}$ holds and so we get immediately $\tilde{\mathfrak{m}} = R$.
- Let $\mathfrak{p} \in \mathrm{ht}^1(R)$ be an arbitrary element. We have by Proposition 10.72: $(\mathfrak{m}\Lambda)_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}\Lambda_\mathfrak{p} = \Lambda_\mathfrak{p}$.

□

Remark 11.2 *We note that the proof of Lemma 11.1 depends heavily on our assumption that R is a local ring with Krull-dimension ≥ 2.*

Lemma 11.3 *None of the maximal divisorial two-sided ideals $\mathfrak{P}$ of Λ is a maximal two-sided ideal of the ring Λ.*

Proof. Let $\mathfrak{P}$ be a maximal divisorial two-sided ideal of Λ and let $\mathfrak{p} := \mathfrak{P} \cap R$ the corresponding element of $\mathrm{ht}^1(R)$. We set $I_\mathfrak{P} := \mathfrak{P} + \mathfrak{m}\Lambda$. Since Λ is finitely generated as an R-module, we can apply Nakayama's Lemma to deduce that $I_\mathfrak{P} \neq \Lambda$ holds. $I_\mathfrak{P}$ is surely a two-sided ideal of Λ, such that $\mathfrak{P} \subset I_\mathfrak{P}$ holds.

Claim. We have $\mathfrak{P} \neq I_\mathfrak{P}$ and so $\mathfrak{P}$ is not a maximal two-sided ideal of Λ.

Proof of the Claim. Assume that we have the equality $\mathfrak{P} = I_\mathfrak{P}$. We have of course $\mathfrak{m}\Lambda \subset I_\mathfrak{P}$, hence $\Lambda \underset{\text{Lemma 11.1}}{=} \widetilde{\mathfrak{m}\Lambda} \subset \tilde{\mathfrak{P}} = \mathfrak{P}$, a contradiction. □

□

Lemma 11.4 *The maximal divisorial two-sided ideals $\mathfrak{P}$ of Λ are prime ideals of Λ.*

Proof. Let us fix a maximal divisorial two-sided ideal $\mathfrak{P}$. Assume that there are two-sided ideals I and J of Λ such that $IJ \subset \mathfrak{P}$ holds. We can w.l.o.g. assume that both I and J are non-zero. We note that $K\Lambda = A$ is a simple algebra, so I and J are full R-lattices in Λ. We get

$$IJ \subset \widetilde{IJ} \subset \tilde{\mathfrak{P}} \underset{\mathfrak{P} \text{ is divisorial}}{=} \mathfrak{P}.$$

Hence we have in $\mathrm{D}(\Lambda)$ the following equality

$$\mathrm{div}(IJ) = \mathrm{div}(I)\mathrm{div}(J) = \mathrm{div}(\tilde{I})\mathrm{div}(\tilde{J}) = \mathrm{div}(P)\mathrm{div}(Q)$$

for some divisorial ideal Q of Λ. Since $\mathrm{D}(\Lambda)$ is a free Abelian group with the $\mathfrak{P}$'s as a basis, we conclude that either $\mathrm{div}(I) = \mathrm{div}(\mathfrak{P})\mathrm{div}(Q_1)$ or $\mathrm{div}(J) = \mathrm{div}(\mathfrak{P})\mathrm{div}(Q_2)$ for some ideal Q_1 or Q_2 of Λ. So either $I \subset \tilde{I} \subset \mathfrak{P}$ or $J \subset \tilde{J} \subset \mathfrak{P}$ and we are done. □

Theorem 11.5 *For a prime ideal P of Λ are equivalent:*

1. *$P = \mathfrak{P}$ for some maximal divisorial two-sided ideal $\mathfrak{P}$ of Λ.*
2. *P is divisorial.*

Proof. (1) $\Longrightarrow$ (2): The ideals $\mathfrak{P}$ are maximal divisorial by Lemma 10.35 and they are prime ideals by Lemma 11.4.

(2) $\Longrightarrow$ (1): Now assume that P is a divisorial prime ideal of Λ. Since A is simple we know that P is a full R-lattice. So we find maximal divisorial two-sided ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ of Λ and $1 \leq \alpha_1, \ldots, \alpha_k \in \mathbb{N}$ with

$$P = \widetilde{\mathfrak{P}_1{}^{\alpha_1}} \cap \cdots \cap \widetilde{\mathfrak{P}_k{}^{\alpha_k}}.$$

Let us assume that P is not maximal. We have to distinguish two cases:

- Assume first $P = \widetilde{\mathfrak{P}^{\alpha}}$ for some maximal divisorial ideal $\mathfrak{P}$ and some $2 \leq \alpha \in \mathbb{N}$. We set $m := \begin{cases} \frac{\alpha}{2} \text{ for } \alpha \equiv 0(2) \\ \frac{\alpha+1}{2} \text{ for } \alpha \equiv 1(2) \end{cases}$. We have of course $m \lneq \alpha$ and so $\mathfrak{P}^m \not\subseteq P$. Moreover we have $\mathfrak{P}^m \cdot \mathfrak{P}^m \subset P$ and so P is not a prime ideal, a contradiction.
- Now assume $P = \widetilde{\mathfrak{P}_1{}^{\alpha_1}} \cap \cdots \cap \widetilde{\mathfrak{P}_k{}^{\alpha_k}}$ for $k \geq 2$. Let $\mathfrak{p}_i := \mathfrak{P}_i \cap R$. Moreover we set $I := \mathfrak{P}_1{}^{\alpha_1}$ and $J := \mathfrak{P}_2{}^{\alpha_2} \cap \mathfrak{P}_k{}^{\alpha_k}$.

  Claim. $I \not\subseteq P$ and $J \not\subseteq P$.

  Proof of the Claim. Assume first $I \subset P$, then $\mathfrak{P}_1{}^{\alpha_1} \subset \mathfrak{P}_2{}^{\alpha_2}$, hence

  $$\Lambda_{\mathfrak{p}_2} = \left(\mathfrak{P}_1{}^{\alpha_1}\right)_{\mathfrak{p}_2} \subset \left(\mathfrak{P}_2{}^{\alpha_2}\right)_{\mathfrak{p}_2} \subset \mathrm{rad}(\Lambda_{\mathfrak{p}_2}),$$

  a contradiction.

  Now we assume $J \subset P$. So we get $\mathfrak{P}_2{}^{\alpha_2} \cap \mathfrak{P}_k{}^{\alpha_k} \subset \mathfrak{P}_1{}^{\alpha_1}$, hence

  $$\Lambda_{\mathfrak{p}_1} = \left(\mathfrak{P}_2{}^{\alpha_2}\right)_{\mathfrak{p}_1} \cap \cdots \cap \left(\mathfrak{P}_k{}^{\alpha_k}\right)_{\mathfrak{p}_1} = \left(\mathfrak{P}_2{}^{\alpha_2} \cap \mathfrak{P}_k{}^{\alpha_k}\right)_{\mathfrak{p}_1} \subset \left(\mathfrak{P}_1{}^{\alpha_1}\right)_{\mathfrak{p}_1} \subset \mathrm{rad}(\Lambda_{\mathfrak{p}_1}),$$

  also a contradiction. □

  Claim. $IJ \subset P$.

  Proof of the Claim. We have

  $$\begin{aligned} IJ = \left(\mathfrak{P}_1{}^{\alpha_1}\right)\left(\mathfrak{P}_2{}^{\alpha_2} \cap \cdots \cap \mathfrak{P}_k{}^{\alpha_k}\right) &\subset \mathfrak{P}_1{}^{\alpha_1} \cap \mathfrak{P}_2{}^{\alpha_2} \cap \cdots \cap \mathfrak{P}_k{}^{\alpha_k} \\ &\subset \widetilde{\left(\mathfrak{P}_1{}^{\alpha_1} \cap \mathfrak{P}_2{}^{\alpha_2} \cap \cdots \cap \mathfrak{P}_k{}^{\alpha_k}\right)} = P, \end{aligned}$$

  again a contradiction to the fact that P is a prime ideal. □

□

Lemma 11.6 *Let T be some Noetherian integral domain with field of fractions L. Moreover let A be a simple L-algebra and Γ some T-order in A. Then 0 is a prime ideal of Γ.*

Proof. Assume that we find two nonzero ideals I and J of Γ such that $IJ \subset 0$ holds. Since R is Noetherian and so I and J are finitely generated over R the proof of Lemma 10.58 yields immediately that we have $L(IJ) = (LI)(LJ) = 0$. Since A is simple we get $LI = LJ = A$, hence $A^2 = 0$ an obvious contradiction. □

Definition 11.7 *We call a prime ideal $P \subset \Lambda$ a height one prime ideal if there is no prime ideal P_1 with $0 \subsetneq P_1 \subsetneq P$.*

Observation 11.8 *Let J be a prime ideal of Λ then $\mathfrak{a} := J \cap R$ is a prime ideal of R.*

Proof. Assume that there are two elements $a, b \in R$ with $ab \in \mathfrak{a}$, hence $(a\Lambda)(b\Lambda) = ab\Lambda \subset J$. Since J is a prime ideal of Λ we have either $a\Lambda \subset J$ or $b\Lambda \subset J$ and so $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$ and we are done. □

Lemma 11.9 *Let T be an arbitrary commutative Noetherian ring and $\mathfrak{q}$ some prime ideal of R. Then $\mathfrak{q}$ is of finite height and so in particular $\mathfrak{q}$ contains some $\mathfrak{p} \in ht^1(R)$.*

Proof. Cf. [Eis99, Corollary 10.3]. □

Theorem 11.10 *For a prime ideal $P \subset \Lambda$ are equivalent:*

1. *P is of height one.*
2. *There is a maximal divisorial two-sided ideal $\mathfrak{P}$ with $P = \mathfrak{P}$.*

Proof. (1) $\Longrightarrow$ (2): Let $P \subset \Lambda$ be a prime ideal of height one. Observation 11.8 yields that $0 \neq \mathfrak{a} := P \cap R$ is a prime ideal of R. Lemma 11.9 ensures that there is some $\mathfrak{p} \in \mathrm{ht}^1(R)$ with $\mathfrak{p} \subset \mathfrak{a}$ and so $\mathfrak{p}\Lambda \subset P$. Let $\mathfrak{P}$ the maximal divisorial ideal over $\mathfrak{p}$ and denote by e the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. Hence we have

$$\mathfrak{P}^e \subset \widetilde{\mathfrak{P}^e} = \mathfrak{p}\Lambda \subset \mathfrak{a}\Lambda \subset P.$$

Using that P is a prime ideal we can conclude $0 \neq \mathfrak{P} \subset P$ and so $\mathfrak{P} = P$ since P is of height one.

(2) $\Longrightarrow$ (1): Let $\mathfrak{P}$ be a maximal divisorial two-sided ideal of Λ and assume that there is some prime ideal $0 \neq J$ of Λ with $J \subset \mathfrak{P}$. We set $\mathfrak{p} := \mathfrak{P} \cap R \in \mathrm{ht}^1(R)$. By Observation 11.8 the ideal $0 \neq \mathfrak{a} := J \cap R$ is a prime ideal of R. Moreover $0 \neq \mathfrak{a} \subset \mathfrak{p} \in \mathrm{ht}^1(R)$ and so $\mathfrak{a} = \mathfrak{p}$. We get $\mathfrak{p}\Lambda \subset J$. Let e be the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. Then $\mathfrak{P}^e \subset \widetilde{\mathfrak{P}^e} = \mathfrak{p}\Lambda \subset J$. Using that J is a prime ideal we get $\mathfrak{P} \subset J$ and so $\mathfrak{P} = J$. □

12 Divisorial Left Ideals

In this section let R be a local factorial Noetherian Krull-Domain (we note that every regular domain has these properties). The field of fractions of R is denoted by K and A is assumed to be a central simple K-algebra. Moreover let Λ be a maximal R-order in A.

Lemma 12.1 *For a divisorial left ideal M of Λ are equivalent:*

1. *M is a maximal one.*
2. *There is $\mathfrak{p} \in ht^1(R)$ and a maximal left ideal $N(\mathfrak{p})$ of $\Lambda_\mathfrak{p}$ such that $M = N(\mathfrak{p}) \cap \Lambda$ holds.*

Proof. (1) $\Longrightarrow$ (2): Let M be a maximal divisorial left ideal of Λ. Since M is divisorial, it is uniquely determined by the local data $\{M_\mathfrak{p} \mid \mathfrak{p} \in \mathrm{ht}^1(R)\}$ (use Theorem 10.26). Assume that there are two different elements $\mathfrak{p}$ and $\mathfrak{p}'$ in $\mathrm{ht}^1(R)$ with $M_\mathfrak{p} \neq \Lambda_\mathfrak{p}$ and $M_{\mathfrak{p}'} \neq \Lambda_{\mathfrak{p}'}$. Then we set

$$M' := M_\mathfrak{p} \cap \Lambda_{\mathfrak{p}'} \cap \bigcap \mathfrak{p}, \mathfrak{p}' \neq \mathfrak{q} \in \mathrm{ht}^1(R)\Lambda_\mathfrak{q},$$

which is a divisorial ideal of Λ. Of course we have $M \subsetneq M' \subsetneq \Lambda$, a contradiction. So there can be at least one element $\mathfrak{p} \in \mathrm{ht}^1(R)$ with $M_\mathfrak{p} \neq \Lambda_\mathfrak{p}$. If $M_\mathfrak{p}$ is not maximal we can analogous construct M' with $M \subsetneq M' \subsetneq \Lambda$ and so $N(\mathfrak{p}) = M_\mathfrak{p}$ is the correct maximal ideal of $\Lambda_\mathfrak{p}$.

(2) $\Longrightarrow$ (1): First we find

$$M = N(\mathfrak{p}) \cap \Lambda \underset{\substack{\Lambda \text{ maximal,} \\ \text{hence divisorial}}}{=} N(\mathfrak{p}) \cap \left(\bigcap_{\mathfrak{q} \in \mathrm{ht}^1(R)} \Lambda_\mathfrak{q} \right)$$

$$= N(\mathfrak{p}) \cap \Lambda_\mathfrak{p} \cap \left(\bigcap_{\mathfrak{p} \neq \mathfrak{q} \in \mathrm{ht}^1(R)} \Lambda_\mathfrak{q} \right) = N(\mathfrak{p}) \cap \left(\bigcap \mathfrak{p} \neq \mathfrak{q} \Lambda_\mathfrak{q} \right).$$

Then Theorem 10.26 yields

$$M_\mathfrak{q} = \begin{cases} \Lambda_\mathfrak{q} \text{ for } \mathfrak{q} \neq \mathfrak{p} \\ N(\mathfrak{p}) \subset \Lambda_\mathfrak{p} \text{ for } \mathfrak{q} = \mathfrak{p} \end{cases}.$$

Now let us assume that there is a divisorial left ideal $M_0 \subsetneq \Lambda$ with $M \subset M_0$. So for every $\mathfrak{q} \in \mathrm{ht}^1(R)$ we find $M_\mathfrak{q} \subset (M_0)_\mathfrak{q}$. We distinguish two cases.

- Case 1: $\mathfrak{p} \neq \mathfrak{q}$, then $M_\mathfrak{q} = \Lambda_\mathfrak{q}$ and so $(M_0)_\mathfrak{q} = \Lambda_\mathfrak{q}$.
- Case 2: $\mathfrak{p} = \mathfrak{q}$ then we get $M_\mathfrak{p} = N(\mathfrak{p})$ is maximal. So $N(\mathfrak{p}) \subset (M_0)_\mathfrak{p}$, so either $(M_0)_\mathfrak{p} = \Lambda_\mathfrak{p}$ - which would induce $M_0 = \Lambda$ - or $(M_0)_\mathfrak{p} = N(\mathfrak{p})$.

So $M_\mathfrak{q} = (M_0)_\mathfrak{q}$ for all $\mathfrak{q} \in \mathrm{ht}^1(R)$, hence another application of Theorem 10.26 yields $M = M_0$ and we are done. □

Observation 12.2 *Let M be an arbitrary left ideal of Λ, then $J := Ann_\Lambda(\Lambda/M)$ is a two-sided ideal of Λ*

Proof. Obvious. □

Lemma 12.3 *Let $S \subset R$ be an arbitrary multiplicative subset. For a Λ-module M, which is finitely generated as R-module we have $S^{-1}Ann_\Lambda(M) = Ann_{S^{-1}\Lambda}(S^{-1}M)$.*

Proof.

- We choose arbitrary elements $x \in \mathrm{Ann}_\Lambda(M), s \in S$ and $\frac{m}{t} \in S^{-1}M$ and get $\frac{x}{s}\frac{m}{t} = \frac{xm}{st} \underset{xm=0}{=} 0$. Hence $S^{-1}\mathrm{Ann}_\Lambda(M) \subset \mathrm{Ann}_{S^{-1}M}(S^{-1}M)$.
- M is finitely generated as R-module, so M is also finitely generated as a Λ-module. Let $\{m_1, \ldots, m_l\}$ be a system of generators, so $S^{-1}M$ is generated by the elements $\frac{m_1}{1}, \ldots, \frac{m_l}{1}$. Let $\frac{x}{s} \in \mathrm{Ann}_{S^{-1}\Lambda}(S^{-1}M)$, then for every $1 \leq i \leq l$ we get $\frac{x}{s}\frac{m_i}{1} = 0$. So for every $1 \leq i \leq l$ we find an element $s_i \in S$ with $s_i x m_i = 0$. We set $s_0 := \prod_{i=1}^{l} s_i$ and obviously $s_0 x m_i = 0$ for all i and so $s_0 x \in J$ and we are done.

□

Proposition 12.4 *Let $N \subset M$ be two Λ-lattices. We set $J := Ann_\Lambda(M/N)$ and $J' := Ann_{\tilde{\Lambda}}(\tilde{M}/\tilde{N})$. There is an equality $\tilde{J} = J'$.*

Proof.

- Let $x \in \tilde{J}$ and $v \in \tilde{M}$. We fix some $\mathfrak{p} \in \mathrm{ht}^1(R)$. We find $j \in J, m \in M$ and $s, t \notin \mathfrak{p}$ with $x = \frac{j}{s}$ and $v = \frac{m}{t}$. So $xv = \frac{jm}{st}$. Using $JM \subset N$ we conclude $jm \in N$, hence $xv \in N_\mathfrak{p}$. The prime $\mathfrak{p}$ was arbitrary, so $xv \in \tilde{N}$. We get $\tilde{J} \subset J'$.
- Now let $x \in J'$. By Lemma 12.3 it is enough to verify that $x \in \mathrm{Ann}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}/N_\mathfrak{p})$ holds for every $\mathfrak{p} \in \mathrm{ht}^1(R)$. So fix a $\mathfrak{p} \in \mathrm{ht}^1(R)$ and choose an arbitrary element $v \in M_\mathfrak{p}$. Since $M_\mathfrak{p} = (\tilde{M})_\mathfrak{p}$ holds we can write $v = \frac{\tilde{m}}{s}$ with $\tilde{m} \in \tilde{M}$ and $s \notin \mathfrak{p}$. Moreover we nota that $x \in \tilde{\Lambda} \subset \Lambda_\mathfrak{p}$ holds. We get $xv = \frac{\overbrace{x\tilde{m}}^{\in \tilde{N}}}{s}$ and so $x \in \mathrm{Ann}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}/N_\mathfrak{p})$. We have $J' \subset J$.

□

Corollary 12.5 *Let M be a divisorial left ideal of Λ. Then $J := Ann_\Lambda(\Lambda/M)$ is a divisorial two-sided ideal of Λ.*

Proof. We have

$$\tilde{J} = \widetilde{\mathrm{Ann}_\Lambda(\Lambda/M)} \underset{\text{Proposition 12.4}}{=} \mathrm{Ann}_{\tilde{\Lambda}}(\tilde{\Lambda}/\tilde{M}) \underset{\Lambda, M \text{ are div.}}{=} = \mathrm{Ann}_\Lambda(\Lambda/M) = J$$

and so we are done. □

Lemma 12.6 *Let M be a divisorial left ideal of Λ and set $J := Ann_\Lambda(\Lambda/M)$. Moreover let $\mathfrak{p} \in ht^1(R)$ and $\mathfrak{P}$ the corresponding maximal divisorial two-sided ideal of Λ. Equivalent are*

1. *$J \subset \mathfrak{P}$.*
2. *$M_\mathfrak{p} \neq \Lambda_\mathfrak{p}$.*

Proof. (1) $\Longrightarrow$ (2): Let $J \subset \mathfrak{P}$, then $J_\mathfrak{p} \subset \mathfrak{P}_\mathfrak{p} = \mathrm{rad}(\Lambda_\mathfrak{p})$. Assume $M_\mathfrak{p} = \Lambda_\mathfrak{p}$, then

$$J_\mathfrak{p} = \big(\mathrm{Ann}_\Lambda(\Lambda/M)\big)_\mathfrak{p} \underset{\text{Lemma 12.3}}{=} \mathrm{Ann}_{\Lambda_\mathfrak{p}}(\Lambda_\mathfrak{p}/M_\mathfrak{p}) = \mathrm{Ann}_{\Lambda_\mathfrak{p}}(0) = \Lambda_\mathfrak{p},$$

a contradiction.

(2) $\Longrightarrow$ (1): Now assume $M_\mathfrak{p} = \Lambda_\mathfrak{p}$. So

$$J_\mathfrak{p} = \big(\mathrm{Ann}_\Lambda(\Lambda/M)\big)_\mathfrak{p} \underset{\text{Lemma 12.3}}{=} \mathrm{Ann}_{\Lambda_\mathfrak{p}}(\Lambda_\mathfrak{p}/M_\mathfrak{p}) \neq \Lambda_\mathfrak{p},$$

hence $J_\mathfrak{p}$ has to be contained in the radical of $\Lambda_\mathfrak{p}$ by Theorem 9.5. But this implies of course that the divisorial ideal J is contained in $\mathfrak{P}$. □

Theorem 12.7 *Let M be a maximal divisorial left ideal of Λ then $J := Ann_\Lambda(\Lambda/M)$ is a maximal divisorial two-sided ideal of Λ.*

Proof. By Lemma 12.1 we find a $\mathfrak{p} \in \mathrm{ht}^1(R)$ and a maximal ideal $N(\mathfrak{p})$ of $\Lambda_\mathfrak{p}$ with $M = N(\mathfrak{p}) \cap \Lambda$. For $\mathfrak{p} \neq \mathfrak{q} \in \mathrm{ht}^1(R)$ we find $M_\mathfrak{q} = \Lambda_\mathfrak{q}$ On the other side we have - by Lemma 12.6 - $M_\mathfrak{q} = \Lambda_\mathfrak{q}$ if and only if $J \nsubseteq \mathfrak{Q}$, where $\mathfrak{Q}$ denotes the maximal divisorial two-sided ideal over $\mathfrak{q}$. So J is only contained in one maximal divisorial two-ideal ideal which is $\mathfrak{P}$. From $J_\mathfrak{p} = \mathrm{Ann}_{\Lambda_\mathfrak{p}}(\Lambda_\mathfrak{p}/M_\mathfrak{p}) = \mathrm{Ann}_\Lambda(\Lambda_\mathfrak{p}/\underbrace{N(\mathfrak{p})}_{\text{maximal}})$ we get - using [Rei75, Theorem 22.15] - $J_\mathfrak{p} = \mathrm{rad}(\Lambda_\mathfrak{p})$ and so $J = \mathfrak{P}$. □

Observation 12.8 *Let $\mathfrak{P} \subset \Lambda$ be a maximal divisorial two-sided ideal of Λ. Then there is a maximal divisorial left ideal M with $\mathfrak{P} \subset M$. In particular we have $\mathfrak{P} = Ann_\Lambda(\Lambda/M)$.*

Proof.

- Since $\mathfrak{P}$ is divisorial the existence of M follows from the fact that Λ is a Noetherian ring.
- The rest is immediately deduced from Theorem 12.7.

□

Definition 12.9 *Let M be a maximal divisorial left ideal of Λ. We say that M belongs to the maximal divisorial two-sided ideal $\mathfrak{P}$ if Λ of $Ann_\Lambda(\Lambda/M) = \mathfrak{P}$ holds.*

Lemma 12.10 *Let $\mathfrak{P}$ be a maximal divisorial two-sided ideal of Λ and denote the maximal divisorial left-ideals which belong to $\mathfrak{P}$ by $\{M_i | i \in I\}$ for some index set I. Then we have the equality*

$$\mathfrak{P} = \bigcap_{i \in I} M_i.$$

Proof.

- Surely we have $\mathfrak{P} \subset M_i$ for all $i \in I$, hence $\mathfrak{P} \subset \bigcap_{i \in I} M_i$.
- Let $\mathfrak{p} = \mathfrak{P} \cap R$. By Lemma 12.1 we know that for every $i \in I$ exists some maximal ideal $M_i(\mathfrak{p})$ of $\Lambda_\mathfrak{p}$ with $M_i = M_i(\mathfrak{p}) \cap \Lambda$ and every maximal ideal of $\Lambda_\mathfrak{p}$ induces a maximal ideal over $\mathfrak{P}$ in this way. So we get immediately

$$\begin{aligned}\bigcap_{i \in I} M_i &= \bigcap_{\substack{M(\mathfrak{p}) \text{ a maximal} \\ \text{left ideal of } \Lambda_\mathfrak{p}}} \Big(M(\mathfrak{p}) \cap \Lambda \Big) \\ &= \Big(\bigcap_{\substack{M(\mathfrak{p}) \text{ a maximal} \\ \text{left ideal of } \Lambda_\mathfrak{p}}} M(\mathfrak{p}) \Big) \cap \Lambda \\ &\underset{\text{Observation 14.13}}{=} \operatorname{rad}(\Lambda_\mathfrak{p}) \cap \Lambda \underset{\text{Theorem 10.41}}{=} \mathfrak{P}.\end{aligned}$$

□

13 The Norm Map

For this chapter we assume that R is a local factorial Krull-domain with field of fractions K. Moreover let Λ be a maximal R-order in a central simple K-algebra A.

Let us recall a well-know definition for Dedekind domains, first we need a lemma about the structure of finitely generated torsion modules over Dedekind domains. Let B be an arbitrary Dedekind domain.

Lemma 13.1 *Let M be a finitely generated torsion module over B. Then we find maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of B with $M = \bigoplus_{i=1}^{n} N_i$ where every N_i is of the form $N_i = \bigoplus_{j=1}^{n_i} B/{\mathfrak{p}_i}^{\alpha_{i,j}}$ for suitable $1 \leq \alpha_{i,j} \in \mathbb{N}$. The summands $B/{\mathfrak{p}_i}^{\alpha_{i,j}}$ are unique up to permutation.*

Definition 13.2 *The ideal $ord_B(M) := \prod_{i=1}^{n} \prod_{j=1}^{n_i} {\mathfrak{p}_i}^{\alpha_{i,j}}$ is called the order ideal of M.*

Remark 13.3 *For $B = \mathbb{Z}$ a finitely generated torsion module M is finite and $ord_R(M) = |M| \cdot \mathbb{Z}$. So the order ideal of a finitely generated torsion module over a Dedekind domain is a generalization of the order $|M|$ of a finite Abelian group M.*

Notation 13.4 *Let S be an arbitrary commutative ring and M an S-module. For an element $\mathfrak{p} \in Spec(S)$ we set $l_{\mathfrak{p}}(M)$ to be the length of $M_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$.*

Observation 13.5 *We have $ord_B(M) = \prod_{\mathfrak{p} \in ht^1(B)} \mathfrak{p}^{l_{\mathfrak{p}}(M)}$*

Proof. This is immediately deduced from Lemma 13.1. □

The formula for the order ideal of M which was given in Observation 13.5 can be generalized to the following

Definition 13.6 *For a finitely generated torsion module M over R we define $ord_R(M) := \prod_{\mathfrak{p} \in ht^1(R)} \mathfrak{p}^{l_{\mathfrak{p}}(M)}$, this divisorial ideal is called the order ideal of M.*

But with respect to the divisor group of R there is a better definition, which is closely related to the definition of the order ideal (see Observation 13.9).

Definition 13.7 *M a finitely generated torsion module over R, then we set $\chi_R(M) := \sum_{\mathfrak{p} \in ht^1(R)} l_{\mathfrak{p}}(M)\mathfrak{p} \in D(R)$ and call it the content of M.*

Remark 13.8 *The order ideal and the content of M are well-defined expressions since $Ann_R(M)$ is not zero and so we find some $0 \neq a \in Ann_R(M)$ and a is just contained in finitely many elements of $ht^1(R)$.*

Observation 13.9 *For a finitely generated torsion module M we have the equality $div(ord_R(M)) = \chi M$.*

Proof. This is just obvious from the definitions. □

Definition 13.10 *For a divisorial ideal J of Λ we set*

$$N(J) := \chi(\Lambda/J) = div(ord_R(\Lambda/J)),$$

this divisor is called the norm of J.

Remarks 13.11 *Let $J \neq \Lambda$ be an arbitrary two-sided ideal of Λ.*

1. *Since J is a full R-lattice in $K\Lambda$, we know that Λ/J is a torsion module over R, so the expression $\chi(\Lambda/J)$ is well defined; we note that the fact that J is divisorial is not really needed in Definition 13.10.*
2. *Claim. We have $N(J) = N(\tilde{J})$, so there is no less of generality in assuming that J is divisorial, when we define the norm of J.*

   Proof of the Claim. *We have $div(J) = div(J')$ if and only if $J_\mathfrak{p} = J'_\mathfrak{p}$ for all $\mathfrak{p} \in ht^1(R)$, so in particular the quotients $\Lambda_\mathfrak{p}/J_\mathfrak{p}$ and $\Lambda_\mathfrak{p}/J'_\mathfrak{p}$ coincide for $div(J) = div(J')$ and we are done.* □

Lemma 13.12 *Let $\mathfrak{P}$ a maximal divisorial two-sided ideal of Λ, then there is some $f \in \mathbb{N}$ with $N(\mathfrak{P}) = f\mathfrak{p}$, where $\mathfrak{p} = \mathfrak{P} \cap R$ is the corresponding height one prime ideal of R.*

Proof. Fix some maximal two-sided divisorial of Λ, say $\mathfrak{P}$ and set $\mathfrak{p} = \mathfrak{P} \cap R$. We have

$$\mathrm{N}(\mathfrak{P}) = \chi(\Lambda/\mathfrak{P}) = \sum_{\mathfrak{q} \in \mathrm{ht}^1(R)} \mathrm{l}_\mathfrak{q}(\Lambda/\mathfrak{P}) =$$

$$\sum_{\mathfrak{q} \in \mathrm{ht}^1(R)} \mathrm{l}_\mathfrak{q}(\Lambda_\mathfrak{q}/\mathfrak{P}_\mathfrak{q})\mathfrak{q} \underset{\Lambda_\mathfrak{q} = \mathfrak{P}_\mathfrak{q} \text{ for } \mathfrak{q} \neq \mathfrak{p}}{=} \mathrm{l}_\mathfrak{p}(\Lambda_\mathfrak{p}/\mathfrak{P}_\mathfrak{p})\mathfrak{p}.$$

□

Definition 13.13 *For $\mathfrak{P}$ over $\mathfrak{p}$ we call $f(\mathfrak{P}/\mathfrak{p}) := f = l_\mathfrak{p}(\Lambda_\mathfrak{p}/\mathfrak{P}_\mathfrak{p})$ the residue class degree of $\mathfrak{P}$ over $\mathfrak{p}$.*

Lemma 13.14 *Let B/A be an integral extension of Noetherian Krull domains. Then for $\mathfrak{P} \in ht^1(R)$ there is the classical definition $\tilde{N}(\mathfrak{P})$ of the norm of $\mathfrak{P}$ with $\tilde{N}(\mathfrak{P}) := f\mathfrak{p}$, where f is the classical residue class degree of $\mathfrak{P}$ over $\mathfrak{p}$ (hence $f = |frac(B/\mathfrak{P}) : frac(A/\mathfrak{p})|$). The two definitions of the norm coincide.*

Proof. Form Lemma 13.12 we know $\mathrm{N}(\mathfrak{P}) = \mathrm{l}_\mathfrak{p}(B/\mathfrak{P})\mathfrak{p}$. So it is enough to show that we have $|\mathrm{frac}(B/\mathfrak{P}) : \mathrm{frac}(A/\mathfrak{p})| = \mathrm{l}_\mathfrak{p}(B/\mathfrak{P})$. We have an isomorphism $\mathrm{frac}(B/\mathfrak{P}) \simeq \left(B/\mathfrak{P}\right)_\mathfrak{p}$. Moreover we know that $\left(B/\mathfrak{P}\right)_\mathfrak{p}$ is an $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$-module and so the last statement is obvious. □

Observation 13.15 *The norm induces a well-defined map*

$$N : D(\Lambda) \longmapsto D(R)$$
$$div(J) \longmapsto N(\tilde{J}).$$

To this map we will from now on refer as norm.

Proof. Obvious per. def. of the class $\mathrm{div}(J)$. We also refer to Remarks 13.11. □

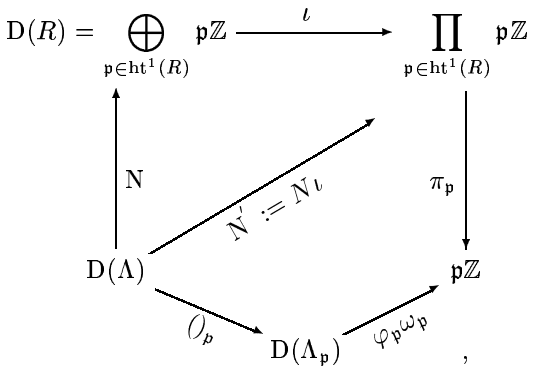
Theorem 13.16 *The map*

$$N\colon D(\Lambda) \longrightarrow D(R)$$

is a group homomorphism.

Proof.

1. We fix some element $\mathfrak{p} \in \mathrm{ht}^1(R)$ and consider the following diagram $\mathcal{D}$ of Abelian groups:



   where shall hold:

   - $\pi_{\mathfrak{p}}$ shall be the canonical projection on $\mathfrak{p}\mathbb{Z}$.
   - $()_{\mathfrak{p}} : \mathrm{D}(\Lambda) \ni \mathrm{div}(J) \longmapsto \mathrm{div}(J_{\mathfrak{p}}) \in \mathrm{D}(\Lambda_{\mathfrak{p}})$. This is a group homomorphism, since localization commutes with taking products of lattices.
   - $\varphi_{\mathfrak{p}} : \mathrm{D}(\Lambda_{\mathfrak{p}}) \ni \mathrm{div}(I) \longmapsto \mathrm{l}_{R_{\mathfrak{p}}}(\Lambda_{\mathfrak{p}}/I)\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{D}(R_{\mathfrak{p}})$ is the classical norm map for an ideal of the $R_{\mathfrak{p}}$-order $\Lambda_{\mathfrak{p}}$.
   - $\omega_{\mathfrak{p}} : \mathrm{D}(R_{\mathfrak{p}}) \ni \alpha\mathfrak{p}R_{\mathfrak{p}} \longmapsto \alpha\mathfrak{p} \in \mathfrak{p}\mathbb{Z}$ is obviously an isomorphism of Abelian groups.

2. We show the following

   Claim. The diagram $\mathcal{D}$ is commutative and $\varphi_{\mathfrak{p}}$ is a group homomorphism.

   Proof of the Claim.

   - Let $\mathfrak{p} \in \mathrm{ht}^1(R)$ be an arbitrary element and $\mathfrak{P}$ the corresponding maximal divisorial ideal of Λ. We fix some divisorial two-sided ideal of Λ, such that $J = \widetilde{\mathfrak{P}^n\mathfrak{Q}}$ holds, where $\mathfrak{P}$ and $\mathfrak{Q}$ are assumed to be disjoint divisorial ideals. Then we have

$$\begin{aligned}
\mathrm{div}(J_{\mathfrak{p}})\varphi_{\mathfrak{p}}\omega_{\mathfrak{p}} &\underset{J=\mathfrak{P}^n\mathfrak{Q}}{=} \Big(\mathrm{rad}(\Lambda_{\mathfrak{p}})^n\Big)\varphi_{\mathfrak{p}}\omega_{\mathfrak{p}} \\
&\underset{\text{per. def. of } \varphi_{\mathfrak{p}}}{=} \Big(\mathrm{l}_{R_{\mathfrak{p}}}(\Lambda_{\mathfrak{p}}/\mathrm{rad}(\Lambda_{\mathfrak{p}})^n)\mathfrak{p}R_{\mathfrak{p}}\Big)\omega_{\mathfrak{p}} \\
&\underset{\text{per. def. of } \omega_{\mathfrak{p}}}{=} \mathrm{l}_{R_{\mathfrak{p}}}(\Lambda_{\mathfrak{p}}/\mathrm{rad}(\Lambda_{\mathfrak{p}})^n)\mathfrak{p}.
\end{aligned}$$

On the other side we have

$$\big(\mathrm{div}(J)\mathrm{N}\big)\pi_{\mathfrak{p}} = \Big(\sum_{\mathfrak{q}\in \mathrm{ht}^1(R)} \mathrm{l}_{\mathfrak{q}}((\Lambda/J)_{\mathfrak{q}})\mathfrak{q}\Big)\pi_{\mathfrak{p}} \underset{\text{per. def. of } \pi_{\mathfrak{p}}}{=} \mathrm{l}_{\mathfrak{p}}((\Lambda/J))\mathfrak{p}$$
$$\underset{J_{\mathfrak{p}}=\mathrm{rad}(\Lambda_{\mathfrak{p}})^n}{=} \mathrm{l}_{R_{\mathfrak{p}}}(\Lambda_{\mathfrak{p}}/\mathrm{rad}(\Lambda_{\mathfrak{p}})^n)\mathfrak{p}.$$

The rest is obvious and so $\mathcal{D}$ is commutative.

- Since Λ is a maximal R-order, the order $\Lambda_{\mathfrak{p}}$ is maximal over $R_{\mathfrak{p}}$, the fact that $\varphi_{\mathfrak{p}}$ is a group homomorphism follows from [Rei75, Theorem 24.4].

□

3. The universal property of the product yields now immediately that N is a group homomorphism.

□

14 The Divisorial Radical of an Order

Let us fix the notation: In this chapter R denotes a Noetherian Krull Domain, the set of height one prime ideals of R is denotes as usual by $\mathrm{ht}^1(R)$. The field of fractions of R is denoted by K. Moreover let Λ be a maximal R-order in a separable K-algebra A. For an arbitrary algebra Γ over a commutative ring S, we denote the Higman ideal of Γ (with respect to S) by $\mathcal{H}_S(\Gamma)$.

Definition 14.1 *We set $\mathcal{P}(\Lambda) := \{\mathfrak{p} \in ht^1(R) \mid \Lambda_\mathfrak{p}$ is not separable over $R_\mathfrak{p}\}$. We call this set the non separability locus of Λ.*

Lemma 14.2 *The set $\mathcal{P}(\Lambda)$ is finite.*

Proof. This is just another formulation of Lemma 8.30. □

There is a stricter formulation, when we assume that $\mathrm{frac}(R/\mathfrak{p})$ is a perfect field for every $\mathfrak{p} \in \mathrm{ht}^1(R)$.

Lemma 14.3 *For a maximal divisorial tow-sided ideal $\mathfrak{P}$ of Λ with $\mathfrak{p} = \mathfrak{P} \cap R$ are equivalent:*

(a) $\mathfrak{P} = \mathfrak{p}\Lambda$.

(a') $e(\mathfrak{P}/\mathfrak{p}) = 1$.

(b) $\Lambda_\mathfrak{p}$ *is a separable* $R_\mathfrak{p}$*-order.*

Proof. (a) $\Leftrightarrow$ (a'): We know from Lemma 10.65 that $\mathfrak{p}\Lambda$ is a divisorial ideal of Λ. Now $e(\mathfrak{P}/\mathfrak{P}) = 1$ if and only if $\tilde{\mathfrak{P}} = \mathfrak{p}\tilde{\Lambda}$, but we have $\tilde{\mathfrak{P}} = \mathfrak{P}$ and $\mathfrak{p}\tilde{\Lambda} = \mathfrak{p}\Lambda$ and so we have proved the first equivalence.

(a) $\Longrightarrow$ (b): Let $\mathfrak{P} = \mathfrak{p}\Lambda$, then we have $\mathrm{rad}(\Lambda_\mathfrak{p}) = \mathfrak{p}\Lambda_\mathfrak{p}$, hence - using Lemma 8.8 - we get that $\Lambda_\mathfrak{p}$ is separable over $R_\mathfrak{p}$.

(b) $\Longrightarrow$ (a'): Assume that $\Lambda_\mathfrak{p}$ is separable over $R_\mathfrak{p}$, then we know - again by Lemma 8.8 - that $\Lambda_\mathfrak{p}$ is unramified over $R_\mathfrak{p}$ i.e., $\mathrm{rad}(\Lambda_\mathfrak{p}) = \mathfrak{p}\Lambda_\mathfrak{p}$ and so we get $\mathfrak{P} = \mathrm{rad}(\Lambda_\mathfrak{p}) \cap \Lambda = \mathfrak{p}\Lambda_\mathfrak{p} \cap \Lambda = \mathfrak{p}\Lambda$. □

Observation 14.4 *Let $\mathfrak{a}$, $\mathfrak{b}$ two ideals of R, then we have $(\mathfrak{a}\Lambda)(\mathfrak{b}\Lambda) = (\mathfrak{a}\mathfrak{b})\Lambda$.*

Proof.

- Let $\sum_i a_i\lambda_i \in \mathfrak{a}\Lambda, \sum_j b_j\lambda'_j \in \mathfrak{b}\Lambda$. Then we have

$$\Big(\sum_i a_i\lambda_i\Big) \cdot \Big(\sum_j b_j\lambda'_j\Big) = \sum_{i,j} \mathfrak{a}_i\lambda_i b_j\lambda'_j \underset{b_j \text{ central in } \Lambda}{=} \sum_{i,j} a_i b_j \lambda_i\lambda'_j \in (\mathfrak{a}\mathfrak{b})\Lambda.$$

- Now let $\sum_i \big(\sum_{j_i} a_{j_i} b_{j_i}\big)\lambda_i \in (\mathfrak{a}\mathfrak{b})\Lambda$. Then we have

$$\sum_i \Big(\sum_{j_i} a_{j_i} b_{j_i}\Big)\lambda_i = \sum_{i,j_i} a_i \cdot 1 \cdot b_j\lambda_i \in (\mathfrak{a}\lambda)(\mathfrak{b}\lambda).$$ □

Lemma 14.5 *Let T be an arbitrary commutative Noetherian ring such that $dim(R) \geq 2$ holds. Then $ht^1(T)$ contains infinitely many elements.*

Proof. By localization and after that passing over to a quotient we can assume that T is a local domain of dimension 2, the radical of T will be denoted by $\mathfrak{m}$. Let $a \in T$ an arbitrary non unit and let $\mathfrak{p}$ be a minimal prime over ideal of a. By Krull's Principal Ideal Theorem (see for example [Eis99, Theorem 10.1]) we get that $\mathfrak{p}$ is of height one. So we can conclude $\bigcup_{\mathfrak{p} \in \mathrm{ht}^1(R)} \mathfrak{p} = \mathfrak{m}$. Now let us assume that $\mathrm{ht}^1(R)$ is a finite set. The prime avoidance (c.f. [Eis99, Lemma 3.3]) yields that $\mathfrak{m} = \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{ht}^1(R)$ a contradiction. □

Lemma 14.6 *Let $\mathfrak{a}, \mathfrak{b} \subset R$ two disjoint divisorial ideals, then we get $\mathfrak{a}\Lambda \cap \mathfrak{b}\Lambda = (\mathfrak{a}\Lambda)(\mathfrak{b}\Lambda)$.*

Proof.

- First we have
$$(\mathfrak{a}\Lambda)(\mathfrak{b}\Lambda) \underset{\text{Observation 14.4}}{=} (\mathfrak{a}\mathfrak{b})\Lambda \underset{\text{Lemma 10.20}}{=} (\mathfrak{a} \cap \mathfrak{b})\Lambda.$$
- So it is enough to show, that $(\mathfrak{a} \cap \mathfrak{b})\Lambda = \mathfrak{a}\Lambda \cap \mathfrak{b}\Lambda$ holds. Proposition 10.25 yields that $\mathfrak{a} \cap \mathfrak{b}$ is a divisorial ideal of R, so an application of Lemma 10.65 induces that $(\mathfrak{a} \cap \mathfrak{b})\Lambda$ is a divisorial ideal of Λ. Again using both Proposition 10.25 and Lemma 10.65 we conclude that $\mathfrak{a}\Lambda \cap \mathfrak{b}\Lambda$ is also a divisorial ideal of Λ. Hence we are done, when we manage to show that for every $\mathfrak{p} \in \mathrm{ht}^1(R)$ the equality $\left(\mathfrak{a}\Lambda \cap \mathfrak{b}\Lambda\right)_{\mathfrak{p}} = \left((\mathfrak{a} \cap \mathfrak{b})\Lambda\right)_{\mathfrak{p}}$ holds. Let us fix some $\mathfrak{p} \in \mathrm{ht}^1(R)$. We know that $R_{\mathfrak{p}}$ is a discrete valuation domain with some prime element, say π. Therefore exist $\alpha, \beta \in \mathbb{N}$ with $\mathfrak{a}R_{\mathfrak{p}} = \pi^{\alpha}R_{\mathfrak{p}}$ and $\mathfrak{b}R_{\mathfrak{p}} = \pi^{\beta}R_{\mathfrak{p}}$. Let us w.l.o.g. $\alpha \leq \beta$ assume. So we get:
  - $\left((\mathfrak{a} \cap \mathfrak{b})\Lambda\right)_{\mathfrak{p}} = (\mathfrak{a} \cap \mathfrak{b})_{\mathfrak{p}}\Lambda_{\mathfrak{p}} = (\mathfrak{a}_{\mathfrak{p}} \cap \mathfrak{b}_{\mathfrak{p}})\Lambda_{\mathfrak{p}} = (\pi^{\alpha}R_{\mathfrak{p}} \cap \pi^{\beta}R_{\mathfrak{p}})\Lambda_{\mathfrak{p}} \underset{\alpha \leq \beta}{=} \pi^{\beta}\Lambda_{\mathfrak{p}}.$
  - $\left(\mathfrak{a}\Lambda \cap \mathfrak{b}\Lambda\right)_{\mathfrak{p}} = (\mathfrak{a}\Lambda)_{\mathfrak{p}} \cap (\mathfrak{b}\Lambda)_{\mathfrak{p}} = \pi^{\alpha}\Lambda_{\mathfrak{p}} \cap \pi^{\beta}\Lambda_{\mathfrak{p}} \underset{\alpha \leq \beta}{=} \pi^{\beta}\Lambda_{\mathfrak{p}}.$

□

Theorem 14.7 *Let R be local with radical $\mathfrak{m}$ and assume moreover that $dim(R) \geq 2$ holds. Then we have*
$$J_0 := \bigcap_{\substack{\mathfrak{P} \text{ maximal divisorial} \\ \text{two-sided ideal of } \Lambda}} \mathfrak{P} = \bigcap_{\substack{M \text{ maximal divisorial} \\ \text{left ideal of } \Lambda}} M = 0.$$

Proof.

- The equality
$$\bigcap_{\substack{\mathfrak{P} \text{ maximal divisorial} \\ \text{two-sided ideal of } \Lambda}} \mathfrak{P} = \bigcap_{\substack{M \text{ maximal divisorial} \\ \text{left ideal of } \Lambda}} M$$
is a direct consequence of Lemma 12.10.

- We know from Lemma 14.2 that there are only finitely many maximal divisorial two-sided ideals $\mathfrak{P}$ with $e(\mathfrak{P}/\mathfrak{p}) \geq 2$, we denote them by $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$. Lemma 14.3 yields that for $\mathfrak{P} \notin \{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$ holds $\mathfrak{P} = \mathfrak{p}\Lambda$. So we get

$$J_0 = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_k \cap \bigcap_{\mathfrak{P} \,:\, e(\mathfrak{P}/\mathfrak{p})=1} \mathfrak{p}\Lambda.$$

  By Lemma 14.5 there are infinitely many elements in $\mathrm{ht}^1(R)$, so there are still infinitely many $\mathfrak{p} \in \mathrm{ht}^1(R)$ such that $e(\mathfrak{P}/\mathfrak{p}) = 1$ holds. We will now reduce our problem to Herstein's Lemma:

- Here for we make some observations:

  1. Let $\mathfrak{p} \neq \mathfrak{q} \in \mathrm{ht}^1(R)$ then $\mathfrak{p}\Lambda$ and $\mathfrak{q}\Lambda$ are disjoint divisorial ideals of Λ. So we can apply Lemma 14.6 and Lemma 10.20 to conclude that $\mathfrak{p}\Lambda \cap \mathfrak{q}\Lambda = \mathfrak{p}\mathfrak{q}\Lambda \underset{\mathfrak{p},\mathfrak{q} \subset \mathfrak{m}}{\subset} \mathfrak{m}\Lambda$ holds.
  2. So an easy induction argument yields now $\bigcap_{i=1}^n \mathfrak{p}_i\Lambda \subset \mathfrak{m}^n\Lambda$. Now Herstein's Lemma yield immediately that we have $J_0 = 0$.

□

Definition 14.8 *1. For a $\mathfrak{p} \in ht^1(R)$ we set $J_{\mathfrak{p}}(\Lambda) := rad(\Lambda_{\mathfrak{p}}) \cap \Lambda$*

2. We set

$$\mathcal{C}(\Lambda) := \bigcap_{\mathfrak{p} \in \mathcal{P}(\Lambda)} J_{\mathfrak{p}}(\Lambda)$$

and call this ideal of Λ the divisorial radical of Λ.

Lemma 14.9 *1. The ideals $J_{\mathfrak{p}}(\Lambda)$ are exactly the maximal divisorial ideals of Λ.*

2. $\mathcal{C}(\Lambda)$ is a divisorial ideal of Λ.

Proof.

1. Just use Lemma 10.33.
2. For this point we refer to Lemma 10.42.

□

Notation 14.10 *We denote the unramified elements of $ht^1(R)$ by $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and set $S := R \setminus \cup_{i=1}^k \mathfrak{p}_i = \cap_{i=1}^n (R \setminus \mathfrak{p}_i)$. Moreover we set $T := S^{-1}R$.*

Observation 14.11 *We have Spec$(T) = \{\mathfrak{p}_i T \mid i = 1, \ldots, k\} \cup \{0\}$. The maximal ideals of T are exactly the $\mathfrak{p}_i T$ (for $i = 1, \ldots, k$).*

Proof.

- We have surely $0 \cap S = \varnothing$ and $\mathfrak{p}_i \cap S = \varnothing$ for all i.
- Now let $\mathfrak{q} \in \mathrm{Spec}(R)$ with $\mathfrak{q} \cap S = \varnothing$, hence $\mathfrak{q} \subset \cup_{i=1}^k \mathfrak{p}_i$. By prime avoidance (see [Eis99, Lemma 3.3]) we deduce that there is some i_0 with $\mathfrak{q} \subset \mathfrak{p}_{i_0}$, hence - since $\mathfrak{p}_{i_0}$ is of height one - we get either $\mathfrak{q} = 0$ of $\mathfrak{q} = \mathfrak{p}_{i_0}$ and so we are done.

□

Lemma 14.12 *T is a Dedekind domain with only finitely many maximal ideals, so in particular a principal ideal domain.*

Proof. For every i we have $T_{\mathfrak{p}_i T} \simeq R_{\mathfrak{p}_i}$ since localization is a transitive process. The rings $R_{\mathfrak{p}_i}$ are discrete valuation domains With Observation 14.12 we get so immediately that $T_{\mathfrak{m}}$ is a discrete valuation domain for every maximal ideal $\mathfrak{m}$ of T. With [Bou89d, Theorem 1 of Paragraoh 2.2] we conclude now that T is a Dedekind domain. The number of maximal ideals of T is finite, so T is a principal ideal domain by [FT91, Corollary 1 to Theorem 4]. □

Observation 14.13 *Let B be an arbitrary commutative ring and Γ a B-algebra which is finitely generated as B-module.*

1. *For a maximal left ideal $M \subset \Gamma$ we have $rad(B)\Gamma \subset M$.*
2. *$rad(B)\Gamma \subset rad(\Gamma)$.*

Proof.

1. Let M be a maximal left ideal of Γ and assume that $\mathrm{rad}(B)\Gamma$ is not contained in M. Then we get $\mathrm{rad}(B)\Gamma + M = \Gamma$. Since Γ is finitely generated as a module over B, we can apply Nakayama's Lemma to deduce that $M = \Gamma$ holds, a contradiction.
2. Immediately clear from the first part.

□

Corollary 14.14 *Let B an arbitrary commutative domain, such that $rad(B) \neq 0$ holds. The field of fractions of B is denoted by K. Moreover let Γ be a maximal order in a central simple K-algebra. Then every maximal ideal of the ring Γ, is a full B-lattice in $K\Gamma$, hence in particular a Γ-ideal.*

Proof. This is immediately deduced from Observation 14.13. □

Theorem 14.15 *We have $S^{-1}\mathcal{C}(\Lambda) = rad(S^{-1}\Lambda)$.*

Proof.

1. $\mathcal{C}(\Lambda)$ is a finite intersection, $\mathcal{C}(\Lambda) = \bigcap_{i=1}^{k} \mathfrak{P}_i$, where $\mathfrak{P}_i$ is the maximal divisorial two-sided ideal over $\mathfrak{p}_i$. Hence we get

$$S^{-1}\mathcal{C}(\Lambda) = S^{-1}\Big(\bigcap_{i=1}^{k} \mathfrak{P}_i\Big) = \bigcap_{i=1}^{k} S^{-1}\mathfrak{P}_i.$$

2. We show the following

   Claim. The maximal ideal of $S^{-1}\Lambda$ which is over the prime ideal $\mathfrak{p}_i A$ is given by $S^{-1}\mathfrak{P}_i$.

Proof of the Claim.

- We know that the maximal ideal $\mathfrak{P}_i^{'}$ over $\mathfrak{p}_i A$ is given by the following expression
$$\mathfrak{P}_i^{'} = \mathrm{rad}(\left(S^{-1}\Lambda\right)_{pri_i A}) \cap S^{-1}\Lambda.$$
Since localization is transitive we get $\mathfrak{P}_i^{'} = \mathrm{rad}(\Lambda_{\mathfrak{p}_i}) \cap S^{-1}\Lambda$.
- On the other side we have
$$\begin{aligned} S^{-1}\mathfrak{P}_i &\underset{\mathfrak{P}_i \text{ is over } \mathfrak{p}_i}{=} S^{-1}\left(\mathrm{rad}(\Lambda_{\mathfrak{p}_i}) \cap \Lambda\right) \\ &\underset{\substack{\text{Localization commutes with} \\ \text{finite intersections}}}{=} S^{-1}\mathrm{rad}(\Lambda_{\mathfrak{p}_i}) \cap S^{-1}\Lambda \\ &\underset{S \subset R \setminus \mathfrak{p}_i}{=} \mathrm{rad}(\Lambda_{\mathfrak{p}_i}) \cap S^{-1}\Lambda \end{aligned}$$
and so the claim is shown.

□

3. By Lemma 14.12 we get that $S^{-1}A$ is a principal ideal domain with only finitely many maximal ideals, so in particular $\mathrm{rad}(S^{-1}A) \neq 0$. So we can apply Corollary 14.14 to deduce that the ideals $S^{-1}\mathfrak{P}_1, \ldots, S^{-1}\mathfrak{P}_k$ are exactly the maximal two-sided ideals of the ring $S^{-1}\Lambda$. An easy application of Nakayama's Lemma - analogous to the proof of Observation 14.13 - yield that the radical of a ring is contained in each of its maximal two sided ideals, hence we get $\mathrm{rad}(S^{-1}\Lambda) \subset S^{-1}\mathcal{C}(\Lambda)$.
4. Now let M be a maximal left ideal of the ring $S^{-1}\Lambda$. By Corollary 14.14 it is a maximal $S^{-1}\Lambda$ ideal and so it belongs to some $S^{-1}\mathfrak{P}_i$ i.e. $S^{-1}\mathfrak{P}_i \subset M$ for some i. And so we get immediately $S{-}1\mathcal{C}(\Lambda) \subset \mathrm{rad}(S^{-1}\Lambda)$.

□

Definition 14.16 *Let T be an arbitrary Noetherian ring (not necessarily commutative). An ideal $J \subset T$ is called semi-prime if for every ideal $I \subset T$ holds:*
$$I^2 \subset J \Longrightarrow I \subset J.$$

Observation 14.17 *Let T be a Noetherian ring. For an ideal J of T are equivalent:*

1. *J is semi-prime.*
2. *$I^n \subset J \Longrightarrow I \subset J$ for every ideal $I \subset T$ and every $1 \leq n \in \mathbb{N}$.*

Proof.

- (1) $\Longrightarrow$ (2): We argue by induction on $1 \leq n$. The case $n = 1$ is of course trivial, so assume $n \geq 2$. If n is even we get $I^{\frac{n}{2}} \subset J$, otherwise we have at least $I^{\frac{n+1}{2}} \subset J$. In both cases we find some $1 \leq m \lneq n$ with $I^m \subset J$, so induction yields $I \subset J$ and we are done.
- (2) $\Longrightarrow$ (1): Trivial by setting $n = 2$.

□

Lemma 14.18 *Let $(T, \mathfrak{m})$ be an arbitrary Noetherian commutative local ring and Γ a T-algebra such that Γ is finitely generated as a T-module. Then $J := rad(\Gamma)$ is a semi-prime ideal of Γ.*

Proof. We have of course $\mathrm{rad}(\Lambda/J) = 0$. Moreover $\mathfrak{k} := R/\mathfrak{m}$ is a field (since R is a local ring) and Λ/J is a $\mathfrak{k}$-algebra, which is finitely generated as a vector space over $\mathfrak{k}$. So Λ/J is an Artin ring. From [ARS97, Proof of Proposition 3.3] we know that the radical of an Artin algebra is the biggest nilpotent ideal of such an algebra. Hence the zero-ideal is the only nilpotent ideal of Λ/J. Now assume that there is an ideal I of Λ such that $I^n \subset J$ holds for some $1 \leq n \in \mathbb{N}$. Then $\frac{I+J}{J}$ is a nilpotent ideal of Λ/J and so we get immediately $I \subset J$ and we are done. □

Theorem 14.19 *Let R local with maximal ideal $\mathfrak{m}$ and assume moreover that the Krull-Dimension of R is ≥ 2. Then every maximal two-sided divisorial ideal $\mathfrak{P}$ is contained in the radical of Λ.*

Proof.

1. Λ is finitely generated as an R-module, so Observation 14.13 yields $\mathfrak{m}\Lambda \subset \mathrm{rad}(\Lambda)$. Let $\mathfrak{p} \in \mathrm{ht}^1(R)$, using that R is local, we get $\mathfrak{p}\Lambda \subset \mathfrak{m}\Lambda \subset \mathrm{rad}(\Lambda)$.
2. Now fix a maximal divisorial two-sided ideal $\mathfrak{P}$ of Λ and let $\mathfrak{p} = \mathfrak{P} \cap R$. We distinguish two cases:
   - $\mathfrak{P}$ is unramified over $\mathfrak{p}$, hence $e(\mathfrak{P}/\mathfrak{p}) = 1$. An application of Lemma 14.3 yields $\mathfrak{P} = \mathfrak{p}\Lambda$ and so $\mathfrak{P} \subset \mathrm{rad}(\Lambda)$ by the previous consideration.
   - Now assume that $e := e(\mathfrak{P}/\mathfrak{p} \geq 2$ holds. So we get $\mathrm{div}(\mathfrak{P}^e) = \mathrm{div}(\mathfrak{p}\Lambda)$, hence $\mathfrak{P}^e \subset \widetilde{\mathfrak{P}^e} = \mathfrak{p}\Lambda$. An application of Lemma 14.18 yields now that we must have $\mathfrak{P} \subset \mathrm{rad}(\Lambda)$.

□

Corollary 14.20 *In the situation of Theorem 14.19 we have an inclusion $\mathcal{C}(\Lambda) \subset rad(\Lambda)$.*

Proof. This follows immediately from the definition of $\mathcal{C}(\Lambda)$ and Theorem 14.19.
□

Bibliography

[AG60] Maurice Auslander and Oscar Goldmann, *Maximal Orders*, Trans. Amer. Math Soc. **97** (1960), 1–24.

[ARS97] Maurice Auslander, Idun Reiten, and Sverre O. Smalø, *Representation Theory of Artin Algebras*, Cambridge University Press, Cambridge, 1997.

[Bas68] Hyman Bass, *Algebraic K-Theory*, W. A. Benjamin, Inc., New York - Amsterdam, 1968.

[Bou50] Nicolas Bourbaki, *Éléments de Mathématique, Livre II, Algèbre, Capitre V, Corps Commutative*, Hermann, Paris, 1950.

[Bou58] ———, *Éléments de Mathématique, Livre II, Algèbre, Capitre VIII, Modules et Anneaux Semi-simples*, Hermann, Paris, 1958.

[Bou89a] ———, *Commutative Algebra, Chapter 1, Flat Modules*, Springer Verlag, Berlin - Heidelberg - New York - London - Paris - Tokyo, 1989.

[Bou89b] ———, *Commutative Algebra, Chapter 2, Localizations*, Springer Verlag, Berlin - Heidelberg - New York - London - Paris - Tokyo, 1989.

[Bou89c] ———, *Commutative Algebra, Chapter 5, Iintegers*, Springer Verlag, Berlin - Heidelberg - New York - London - Paris - Tokyo, 1989.

[Bou89d] ———, *Commutative Algebra, Chapter 7, Divisors*, Springer Verlag, Berlin - Heidelberg - New York - London - Paris - Tokyo, 1989.

[Bro00] Kenneth S. Brown, *Cohomology of Groups*, Springer Verlag, New York - Berlin - Heidelberg - London - Paris - Tokyo - Hong Kong - Barcelona - Budapest, 2000.

[CR81] Charles W. Curtis and Irving Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders, Volume I*, John Wiley and Sons, New York - Chichester - Brisbane - Toronto - Singapore, 1981.

[CR87] ———, *Methods of Representation Theory with Applications to Finite Groups and Orders, Volume II*, John Wiley and Sons, New York - Chichester - Brisbane - Toronto - Singapore, 1987.

[DI71] Frank DeMeyer and Edward Ingraham, *Separable Aalgebras Over Commutative Rings*, Springer Verlag, Berlin - Heidelberg - New York, 1971.

[DR94] Yu. A. Drozd and Klaus W. Roggenkamp, *Cohen Macaulay rings of global dimension two and Krull dimension two*, Comm. Alg. **22** (1994), 3297–3329.

[DR97] ———, *On the global structure of regular orders of dimension two*, Comm. Alg. **25** (1997), 1–9.

[Eis99] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer Verlag, New York - Berlin - Heidelberg - Barcelona - Hong Kong - London - Milan - Paris - Singapore - Tokyo, 1999.

[FT91] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1991.

[Has31] Helmut Hasse, *Über p-adische Sschiefkörper und ihre Bedeutung für die Arithmetik hypercomplexer Zahlsysteme*, Math. Ann. **104** (1931), 495–534.

[Lan91] Saunders Mac Lane, *Homology, Reprint of the 1975 Edition*, Springer Verlag, Berlin - Heidelberg - New York, 1991.

[Lan93] Serge Lang, *Algbera, Third Edition*, Addison-Wesley Publishing Company, Reading - Massachusetts - Menlo Park, California - New York - Don Mills, Ontario - Wokingham, England - Amsterdam - Bonn - Sydney - Singapore - Tokyo - Madrid - San Juan - Milan - Paris, 1993.

[Mat86] Hideyuki Matsumura, *Commutative ring theory*, Cambridge University Press, 1986.

[MR87] J. C. McConnel and J. C. Robson, *Noncommutative Noetherian Rings*, John Wiley & Sons, Chichester - New York - Brisbane - Toronto - Singapore, 1987.

[Pie82] Richard S. Pierce, *Associtive Algebras*, Springer Verlag, New York - Heidelberg - Berlin, 1982.

[RdB80] I. Reiten and M. Van den Bergh, *Two-dimensional tame and maximal orders of finite representation type. Memoirs of the American Mathematical Society,80*, 1980.

[Rei75] Irving Reiner, *Maximal Orders*, Academic Press, London - New York - San Francisco, 1975.

[Rog80] Klaus W. Roggenkamp, *Integral Representations and Structure of Finite Group Rings*, Les Presse de L'Université de Montréal, Montréal, 1980.

[Rog91] ———, *The Structure of the Principal p-Block with Cyclic Normal Defect Group*, Representations of finite-dimensional algebras. Proceedings of the Fifth International Conference on Representation Theory. Canadian Mathematical Society Conference Proceedings, Volume 11 (H. Tachikawa and V. Dlab, eds.), AMS Providence, 1991, pp. 279–286.

[Rog92] ———, *Blocks of Cyclic Defect and Green-Orders*, Comm. Alg. **20(6)** (1992), 1715–1734.

[Rog94] ———, *Cohomology of Lie-Algebras, Groups and Algebras, Seminar Series in Mathematics, Algebra:1*, Ovidius University, Constanţa, Romania, 1994.

[Rog99a] ———, *Cohen-Macaulay modules over two-dimensional graph orders*, Coll. Math. **82** (1999), 25–48.

[Rog99b] ———, *The Structure of Some Group Rings*, Algebra. Some Recent Advance (I. B. S. Passi, ed.), Birkhäuser Basel, 1999, pp. 183–206.

[Rog00a] ———, *Blocks with cyclic defect of Hecke orders of Coxeter groups*, Arch. Math. **74** (2000), 173–182.

[Rog00b] ———, *The Structure over $\mathbb{Z}[q, q^{-1}]$ of Hecke orders of Dihedral Groups*, J. Algebra **224** (2000), 356–396.

[Rog01a] ———, *2-dimensional orders and integral Hecke orders*, Algebra – Representation Theory (Klaus W. Roggenkamp and Mirela Ştefănescu, eds.), Kluwer Academic Publishers, 2001, pp. 301–349.

[Rog01b] ———, *The Cell Structure, the Brauer Tree Structure and Extensions of Cell Modules for Hecke Orders of Dihedral Groups*, J. Algebra **239** (2001), 460–476.

[Rot79] Jospeh J. Rotman, *An Introduction to Homological Algebra*, Academic Press, New York - San Francisco - London, 1979.

[Ser00] Jean Pierre Serre, *Local Alegbra*, Springer Verlag, New York - Berlin - Heidelberg - Barcelona - Hong Kong - London - Milan - Paris - Singapore - Tokyo, 2000.

[Suz82] Michio Suzuki, *Group Theory I*, Springer Verlag, Berlin - Heidelberg - New York, 1982.

[Wei97] Charles A. Weibel, *An introduction to homological algebra*, Cambridge University Press, Cambridge, 1997.

Lebenslauf

Joachim Simon

geboren	am 23. Mai 1976 in Nürtingen.
Eltern	Karl Simon und Christine Simon, geborene Baumann.
Schulbildung	Grundschule Neckartailfingen von 1982 bis 1986. Gymnasium Neckartenzlingen von 1986 bis 1995.
Reifeprüfung	im Juni 1995.
Studium	Mathematik mit Nebenfach Physik an der Universität Stuttgart. Beginn im Wintersemester 1995/96. Vordiplom im Sommersemester 1996.
Diplomprüfung	am 15. September 2000 an der Universität Stuttgart.
Berufstätigkeit	Seit Oktober 2000 Mitarbeiter an der Universität Stuttgart.