

---

# Group rings and twisted group rings for a series of $p$ -groups

---

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

Vorgelegt von  
**Harald Weber**  
geboren in Radolfzell

Hauptberichter: Prof. Dr. K. W. Roggenkamp  
Mitberichter: Prof. Dr. J. Ritter  
Tag der mündlichen Prüfung: 23.07.2003

---

Fachbereich Mathematik der Universität Stuttgart  
2003

---



## CONTENTS

Zusammenfassung	i
	1
0. Introduction	1
1. The Pascal matrix	8
1.1. Preliminaries	8
1.2. Integral group rings and the Pascal matrix	10
1.3. Pascal matrix and Bernoulli numbers	13
1.4. The $q$ -Pascal matrix and Gaussian polynomials	14
1.5. Conjugation with the Pascal matrix	17
2. Recursively defined triangular matrices	20
2.1. Definitions and examples	20
2.2. Calculations	22
2.3. Applications to number theory	27
3. Integral group rings and twisted group rings	31
3.1. The Abelian case	31
3.2. The general case	31
3.3. A twisted group ring as a factor ring of an integral group ring	36
4. Automorphisms and units	49
4.1. Automorphisms of integral group rings	49
4.2. Automorphisms of twisted group rings	51
4.3. Units in integral and in twisted group rings	52
4.4. Explicit calculations	54
5. The twisted group ring $\Lambda$ and a bilinear form	58
6. Over orders of $\Lambda$	60
6.1. The radical idealisator process	60
6.2. Embedding of twisted group rings in hereditary orders	64
6.3. Ideals in hereditary orders	68
6.4. Graphical description of intermediate orders	80
7. Cohomology of twisted group rings	89
7.1. Projective and injective resolutions, Ext-groups	89
7.2. Products in Cohomology	93
8. The representation type of some twisted group rings	105
References	110
Lebenslauf	113



## ZUSAMMENFASSUNG

In dieser Arbeit beschäftigen wir uns mit ganzzahligen Gruppenringen  $\mathbb{Z}G$  für eine Serie von  $p$ -Gruppen  $G$ . Hierfür werden wir den ganzzahligen Gruppenring  $\mathbb{Z}G$  als Pullback betrachten, was uns dann ermöglicht, eine ‘komplizierte Struktur’, den ganzzahligen Gruppenring, durch zwei ‘einfachere Strukturen’, welche durch Kongruenzen verbunden sind, zu verstehen.

Das einfachste Beispiel einer solchen Beschreibung<sup>1</sup> liefert der ganzzahlige Gruppenring einer zyklischen Gruppe  $C_p = \langle c \rangle$  der Primzahlordnung  $p$ :

$$\begin{array}{ccc} \mathbb{Z}C_p & \xrightarrow{\alpha} & \mathbb{Z} \\ \beta \downarrow & & \downarrow \gamma \\ \mathbb{Z}[\zeta] & \xrightarrow{\delta} & \mathbb{F}_p, \end{array}$$

mit einer primitiven  $p$ -ten Einheitswurzel  $\zeta$ ,  $\alpha(c) = 1, \beta(c) = \zeta$  und mit den durch die Ideale  $(p)$  und  $(1 - \zeta)$  bestimmten Quotientenabbildungen  $\gamma$  und  $\delta$ . Somit haben wir einen Isomorphismus von Ringen

$$\mathbb{Z}C_p \simeq \{(a, b) \mid (a, b) \in \mathbb{Z} \times \mathbb{Z}[\zeta], \gamma(a) = \delta(b)\} \subset \mathbb{Z} \times \mathbb{Z}[\zeta].$$

Ähnlich erhält man für den ganzzahligen Gruppenring  $\mathbb{Z}C_{p^{n+1}}$  einer zyklischen Gruppe der Primzahlordnung  $p^{n+1}$  mit einer primitiven  $p^{n+1}$ -ten Einheitswurzel  $\zeta_{p^{n+1}}$  die rekursive Beschreibung:

$$\begin{array}{ccc} \mathbb{Z}C_{p^{n+1}} & \longrightarrow & \mathbb{Z}C_{p^n} \\ \downarrow & & \downarrow \\ \mathbb{Z}[\zeta_{p^{n+1}}] & \longrightarrow & \mathbb{F}_p C_{p^n}. \end{array}$$

Für eine nicht zyklische abelsche  $p$ -Gruppe  $A$  ist eine sukzessive Zerlegung des ganzzahligen Gruppenringes  $\mathbb{Z}A$  durch Pullbackdiagramme zwar prinzipiell möglich, liefert aber aufgrund der komplizierten Kongruenzen keine befriedigende Darstellung. So erhält man schon für die Kleinsche Vierergruppe  $V_4$  den Isomorphismus von Ringen

$$\mathbb{Z}V_4 \simeq \{(a, b, c, d) \mid (a, b, c, d) \in \mathbb{Z}^4, a \equiv b \equiv c \equiv d \pmod{2}, a + b + c + d \equiv 0 \pmod{4}\},$$

eine Darstellung, die für explizite Rechnungen wenig geeignet ist.

Beschreibungen ganzzahliger Gruppenringe für bestimmte nicht abelsche Gruppen als Teilringe von Produkten über Matrixringen wurden durch Roggenkamp

<sup>1</sup>Rim ([Rim]) benutzte diese Beschreibung um mit einer Mayer-Vietoris Sequenz die Klassengruppe des ganzzahligen Gruppenringes zu berechnen. Dabei gilt  $\text{Cl}(\mathbb{Z}C_p) \simeq \text{Cl}(\mathbb{Z}[\zeta])$ .

(siehe [Ro2]) und Künzer (siehe [Kü]) gegeben.

Analog zum abelschen Fall sind die ganzzahligen Gruppenringe von  $p$ -Gruppen mit einer zyklischen maximalen Untergruppe für ein Studium durch entsprechende Pullbacks am geeignetsten. Dieses Gruppen sind (siehe [Rob] Theorem 5.3.4 ):

- (i) eine Diedergruppe  $D_{2^n}$ ,
- (ii) eine Semidiedergruppe  $\langle x, a \mid x^2 = a^{2^{n+1}} = 1, a^x = a^{2^n-1} \rangle$ ,  $n \geq 1$ ,
- (iii) eine Gruppe der Form  $G := \langle a, b \mid a^{p^{n+1}} = 1, b^p = 1, a^b = a^{p^{n+1}} \rangle$ ,  $n \geq 1$ ,
- (iv) eine verallgemeinerte Quaternionengruppe  $Q_{2^n}$ .

Zimmermann untersuchte in [Zi] ganzzahlige Gruppenringe von Diedergruppen  $D_{2^n}$ . Wir werden in dieser Arbeit eine Methode angeben (in Kapitel 3.2), welche die Behandlung der Fälle (i) bis (iii) ermöglicht und dies dann speziell auf den Fall (iii) anwenden, da dieser Fall auch ungerades  $p$  beinhaltet.

Es sei nun  $G$  wie in (iii) definiert. Dann erhält man, analog zu  $\mathbb{Z}C_{p^{n+1}}$ , eine Beschreibung von  $\mathbb{Z}G$  als Pullback:

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}C_{p^n} \times C_p \\ \downarrow & & \downarrow \\ \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p & \xrightarrow{\delta} & \mathbb{F}_p C_{p^n} \times C_p. \end{array}$$

Nun ist man interessiert an einer Beschreibung

- des getwisteten Gruppenringes  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  als Teilring eines Matrixringes,
- der auftretenden Kongruenzen.

Eine Beschreibung von  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  durch Matrizen wurde von Ritter und Sehgal [RiSe] gegeben. Wir werden eine dazu konjugierte Darstellung angeben, welche die  $p$ -adische Struktur berücksichtigt. Dabei gehen wir wie folgt vor:

(Um einige Fallunterscheidungen zu vermeiden, betrachten wir hier den wesentlich aufwändigeren Fall  $p$  ungerade. Selbstverständlich wird in der Arbeit auch der Fall  $p = 2$  behandelt.)

Wir betrachten  $\mathbb{Z}[\zeta_{p^{n+1}}]$  als Modul über  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$ , wobei der Koeffizientenbereich multiplikativ und die Gruppe  $C_p := \langle b \rangle$  durch den Galoisautomorphismus

$$\begin{array}{ccc} b : \mathbb{Z}[\zeta_{p^{n+1}}] & \rightarrow & \mathbb{Z}[\zeta_{p^{n+1}}] \\ \zeta_{p^{n+1}} & \mapsto & \zeta_{p^{n+1}}^{p^n+1} = \zeta \cdot \zeta_{p^{n+1}} \end{array}$$

operiert. Dann ist  $R := \mathbb{Z}[\zeta_{p^n}]$  der Fixring von  $\mathbb{Z}[\zeta_{p^{n+1}}]$  unter dieser Galoisoperation und  $\mathfrak{B}' := \{1, \zeta_{p^{n+1}}, \dots, \zeta_{p^{n+1}}^{p-1}\}$  eine  $R$ -Basis von  $\mathbb{Z}[\zeta_{p^{n+1}}]$ . Indem wir die Basiselemente als Zeilenvektoren interpretieren, erhalten wir die von Ritter und

Sehgal gegebenen Darstellungen der  $R$ -Ordnung  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$

$$A' = \begin{pmatrix} 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ \zeta_{p^n} & & & & 0 \end{pmatrix}, \quad B' = \begin{pmatrix} 1 & & & & \\ & \zeta & & & \\ & & \zeta^2 & & \\ & & & \ddots & \\ & & & & \zeta^{p-1} \\ & & & & & 0 \end{pmatrix}.$$

Nun fragen wir nach diesen Darstellungen bezüglich der  $p$ -adisch geordneten  $R$ -Basis  $\mathfrak{B} := \{1, 1 - \zeta_{p^{n+1}}, \dots, (1 - \zeta_{p^{n+1}})^{p-1}\}$ , wobei der dazugehörige Basiswechsel durch die, durch Binomialkoeffizienten gegebene, Pascalmatrix

$$(\widehat{P})_p = \begin{pmatrix} 1 & 0 & & & 0 \\ 1 & -1 & & & \\ 1 & -2 & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ 1 & -(p-1) & \dots & -(p-1) & 1 \end{pmatrix}$$

gegeben wird. Konjugation von  $A'$  und  $B'$  mit  $(\widehat{P})_p$  liefert die Darstellungen  $A$  und  $B$  (siehe Lemma 3.11), deren Erzeugnis eine  $R$ -Ordnung  $\Lambda$  definiert. Wir erhalten somit  $\Lambda$  als Bild einer Einbettung des getwisteten Gruppenringes  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  in die minimale erbliche Überordnung

$$\Gamma := \begin{pmatrix} R & \dots & R \\ (\pi) & R & \vdots \\ \vdots & \ddots & \ddots \\ (\pi) & \dots & (\pi) & R \end{pmatrix},$$

wobei  $\pi := 1 - \zeta_{p^n} \in R$  prim ist. Insbesondere sind wir somit im zahlentheoretisch interessantesten, vollständig verzweigten Fall.

Wir haben somit den getwisteten Gruppenring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  in eine uns vertraute  $R$ -Ordnung eingebettet, allerdings Darstellungen  $A$  und  $B$  erhalten, die aufgrund ihrer komplizierten Form, insbesondere im Vergleich zu den Darstellungen  $A'$  und  $B'$ , kaum für explizite Rechnungen geeignet sind. Erstaunlicherweise gibt es jedoch Erzeuger  $N$  und  $W$  von  $\Lambda$ ,

$$N := \begin{pmatrix} 0 & & & & \\ 1-\zeta & & & & \\ & \ddots & & & \\ & & & 1-\zeta^{p-1} & 0 \end{pmatrix}, \quad W := \begin{pmatrix} 0 & 1 & & & \\ & & \ddots & & \\ & & & & 1 \\ \pi & & & & 0 \end{pmatrix},$$

welche auch für explizite Rechnungen geeignet sind:

**Satz. 1** [Theorem 3.20 (i)] Sei  $\zeta := \zeta_{p^{n+1}}$ . Dann wird die zum getwisteten Gruppenring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  isomorphe  $R$ -Ordnung  $\Lambda$  erzeugt von  $N$  und  $W$  und den Relationen

$$N^p = 0, \quad W^p = \pi, \quad WN = \zeta \cdot NW + (1 - \zeta).$$

Anschliessend wird gezeigt, dass  $N$  und  $W$  ein maximales Ideal in  $\Lambda$  erzeugen, welches nach Lokalisation an  $p$  mit dem Radikal übereinstimmt.

Wir werden in den Kapiteln 4 bis 8 diesen, für unsere Arbeit zentralen Satz benutzen um uns klassischen Problemen wie der Bestimmung von Überordnungen, der Kohomologie und des Darstellungstyps des getwisteten Gruppenringes  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  zuzuwenden. Darüber hinaus behandeln wir Fragestellungen zu Einheiten und Automorphismen sowohl im getwisteten als auch im ganzzahligen Gruppenring.

Zum Beweis dieses Satzes bedurfte es einer neuen Technik, die der rekursiv definierten Dreiecksmatrizen, welche wir in Kapitel 2 einführen werden. Um deren Notwendigkeit zu demonstrieren, soll der Beweis des obigen Satzes nun skizziert werden:

Wir müssen zeigen, dass die von  $A$  und  $B$  erzeugte  $R$ -Ordnung  $\Lambda$  mit der von  $N$  und  $W$  erzeugten übereinstimmt. Wir haben also zu zeigen, dass

$$(I) : A, B \in {}_R\langle N, W \rangle \text{ und } (II) : N, W \in {}_R\langle A, B \rangle .$$

Nun sind  $N$  und  $W$  von so einfacher Gestalt, dass wir die Matrixprodukte  $N^i W^j$ , mit  $0 \leq i, j < p$ , explizit bilden können. Aus diesen erzeugen wir dann  $A$  und  $B$   $R$ -linear. Somit gilt (I).

Da die durch  $A^i B^j$  gegebenen Matrizen von komplizierter Gestalt sind, überprüfen wir die Bedingung (II) nach Konjugation mit  $(\hat{P})_p$ .

Dabei liefert der von der  $\mathbb{Z}$ -linearen Abbildung

$$\psi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[X] \\ X^i \mapsto (1 - X)^i ,$$

induzierte Basiswechsel die (unendliche) Pascalmatrix

$$\hat{P} := \begin{pmatrix} 1 & 0 & & & 0 \\ 1 & -1 & & & \\ 1 & -2 & 1 & & \\ 1 & -3 & 3 & -1 & \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} .$$

Man rechnet jetzt nach, dass  $\psi$  eine Involution ist, somit gilt dies auch für  $\hat{P}$  und für die durch *Restriktion* erhaltene Matrix  $(\hat{P})_p$ <sup>2</sup>.

Mit  $N' := (\hat{P})_p N (\hat{P})_p$  und  $W' := (\hat{P})_p W (\hat{P})_p$  haben wir zu zeigen, dass

$$N', W' \in {}_R\langle A', B' \rangle .$$

---

<sup>2</sup>Dies war bereits Ende des neunzehnten Jahrhunderts bekannt und findet sich in dem Standardwerk Lehrbuch der Algebra von Heinrich Weber, erstaunlicherweise jedoch nicht in der Literatur der modernen linearen Algebra (siehe Lemma 1.2 und Remark 1.5).

Es besteht nun das Problem  $N'$  und  $W'$  konkret anzugeben. Wir werden dabei dieselben Methoden anwenden, mit denen wir auch  $A$  und  $B$  bestimmt haben. Diese sollen nun am aufwändigsten Teil, der Bestimmung von  $N'$ , veranschaulicht werden:

Es sei  $S := \mathbb{Z}[q]$  der Polynomring,  $\phi_p(q) := q^{p-1} + \dots + q + 1$  das Kreisteilungspolynom einer  $p$ -ten Einheitswurzel  $\zeta$  und  $I_p := \langle \phi_p(q), X^p \rangle$  ein Ideal im Polynomring  $S[X]$ . Dann ist  $S[X]/I_p$  frei als  $S/\langle \phi_p(q) \rangle$ -Modul mit einer Basis  $\{X^i \mid 0 \leq i < p\}$ . Indem wir wieder die Basiselemente als Zeilenvektoren betrachten, erhalten wir die zur Matrix  $N$  gehörende  $S/\langle \phi_p(q) \rangle$ -lineare Abbildung

$$\begin{aligned} \Phi_p : S[X]/I_p &\rightarrow S[X]/I_p \\ X^i &\mapsto (1 - q^i)X^{i-1}. \end{aligned}$$

Die Matrix  $N'$  wird dann durch die Abbildung  $\Phi_p$  bezüglich der  $S/\langle \phi_p(q) \rangle$ -Basis  $\{(1 - X)^i \mid 0 \leq i < p\}$  gegeben.

Die explizite Gestalt von  $N'$  werden wir per Induktion nach  $i$ , also einer Induktion nach den Zeilen der Matrix, verifizieren. Probleme die deshalb auftauchen, weil wir diese Rechnungen für beliebiges  $p$  durchzuführen haben, umgehen wir indem wir die unendlich dimensionale  $S$ -lineare Abbildung

$$\begin{aligned} \Phi : S[X] &\rightarrow S[X] \\ X^i &\mapsto (1 - q^i)X^{i-1} \end{aligned}$$

betrachten, das heißt wir bestimmen  $\Phi$  bezüglich der Basis  $\{(1 - X)^i \mid i \in \mathbb{N}\}$  und erhalten die unendlich dimensionale Matrix  $Id - \widehat{H}$  (siehe Proposition 1.24 (iii)) mit

$$\widehat{H} = \begin{pmatrix} 1 & & & & & \\ 1-q & 1 & & & & \\ (1-q)^2 & (1-q)(1+q) & 1 & & & \\ (1-q)^3 & (1-q)^2(1+2q) & (1-q)(1+q+q^2) & 1 & & \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots \end{pmatrix}.$$

Dabei ist die untere Dreiecksmatrix  $\widehat{H}$  mit Einträgen aus  $S$  rekursiv definiert durch die Anfangsbedingung

$$\mathcal{SC} : (\widehat{H})_{i,i} := 1$$

und der Konstruktionsregel

$$\mathcal{CR} : (\widehat{H})_{i,j} := (1-q)(\widehat{H})_{i-1,j} + q(\widehat{H})_{i-1,j-1} \text{ für } i > j.$$

Jetzt erhalten wir  $N'$  aus der Matrix  $Id - \widehat{H}$  nach *Restriktion* auf die Größe  $p$ , das heißt wir betrachten nur die obersten  $p \times p$  Einträge, und nach *Auswertung* an  $q := \zeta$ .

Um zu zeigen, dass  $N' \in {}_R\langle A', B' \rangle$  ist, rechnen wir wieder mit der allgemeinen Matrix  $\widehat{H}$ . Nach einer geeigneten technischen Modifikation erhalten wir dann die Matrix  $\widehat{H}^\tau$  (siehe Definition 2.4), welche wir dann in ein Produkt zerlegen:

$$\widehat{H}^\tau = \widehat{K} \cdot X.$$

Dabei werden die Spalten des ersten Faktors  $\widehat{K}$  aus geeigneten Elementen von  ${}_R\langle A', B' \rangle$  konstruiert. Der zweite Faktor gibt an, wie diese Spalten  $S$ -linear zu kombinieren sind um  $\widehat{H}^r$  zu erhalten. Um diese Gleichung nach  $X$  aufzulösen betrachten wir die Gleichung

$$\widehat{K} = G \cdot F \cdot D_{1-q},$$

eine Zerlegung von  $\widehat{K}$  in die  $q$ -Pascalmatrix  $G$  und die Diagonalmatrizen  $F$  und  $D_{1-q}$ . Dabei sind die Einträge der  $q$ -Pascalmatrix  $G$  durch die Gausspolynome<sup>3</sup>  $\begin{bmatrix} i \\ j \end{bmatrix}$  gegeben. Durch Bestimmung der inversen  $q$ -Pascalmatrix  $G^{-1}$  (Proposition 1.21) und des Produkts  $G^{-1} \cdot \widehat{H}^r$  (Proposition 2.20) können wir dann die obige Gleichung, durch Rechnungen mit rekursiv definierten Matrizen lösen. Nach *Restriktion* der Lösung  $X$  auf die Größe  $p$  und *Auswertung* an der  $p$ -ten Einheitswurzel  $q := \zeta$  erhalten wir nun  $N' \in {}_R\langle A', B' \rangle$ . Zusätzlich bestimmen diese Einträge auch das Bild  $\delta(N)$  in unserer Pullbackbeschreibung des ganzzahligen Gruppenringes  $\mathbb{Z}G$ .

Mit Hilfe von **Satz 1**, einer Beschreibung der  $R$ -Ordnung  $\Lambda$  durch Erzeugende und Relationen, werden wir noch weitere interessante Charakterisierungen von  $\Lambda$  herleiten.

**Satz. 2** [Theorem 3.22] Die  $R$ -Ordnung  $\Lambda$  hat die folgenden  $R$ -Basen:

- (i)  $\mathfrak{B}_\Lambda = \{N^i W^j \mid 0 \leq i, j \leq p-1\}$ ,
- (ii)  $\mathfrak{B}'_\Lambda = \{W^i N^j \mid 0 \leq i, j \leq p-1\}$ .

Daneben beschreibt **Satz 3** [Theorem 3.30] die  $R$ -Ordnung  $\Lambda$  durch Kongruenzen und liefert ein Kriterium, ob ein Element aus der erblichen Überordnung  $\Gamma$ , welche sehr einfach zu verstehen ist, schon in  $\Lambda$  liegt. Da dieser Satz einer technischen Terminologie bedarf, soll hier nur seine Idee erläutert werden:

Wir notieren mit  $\Lambda_i$  die  $i$ -te Diagonale von  $\Lambda$ , wobei die 0-te Diagonale durch die Hauptdiagonale gegeben ist. Die erste Diagonale ist dann durch die Einträge genau einer Reihe darüber plus dem Eintrag in der letzten Zeile und ersten Spalte gegeben. Die erste Diagonale liegt somit direkt über der 0-ten. Analog definiert man die zweite Diagonale als diejenige direkt über der ersten und so weiter (siehe Definition 3.15). So ist zum Beispiel  $W$  durch seine erste und  $N$  durch seine  $(p-1)$ -te Diagonale bestimmt.

Da die Multiplikation von Matrizen mit dem Konzept der Diagonalen verträglich

---

<sup>3</sup>Die Gausspolynome besitzen, neben ihrer Bedeutung für die Kombinatorik (siehe [An]), die folgenden Anwendungen für die Darstellungstheorie:

Auswertung des Gausspolynoms  $\begin{bmatrix} i \\ j \end{bmatrix}$  an der Primzahlpotenz  $q := p^n$  liefert die Anzahl der  $j$ -dimensionalen Unterräume in  $\mathbb{F}_q^i$ . Damit können in der Darstellungstheorie der symmetrischen Gruppen die Dimensionen von Spechtmoduln bestimmt werden.

ist, folgt mit **Satz 2**, dass es zwischen zwei verschiedenen Diagonalen keine Kongruenzen gibt. Somit liegt  $\gamma \in \Gamma$  genau dann in  $\Lambda$ , wenn für alle  $0 \leq i < p$  die Projektion von  $\gamma$  auf die  $i$ -te Diagonale,  $\gamma_i$ , gilt:  $\gamma_i \in \Lambda_i$ . Nachdem wir aus  $\gamma_i$  einen Spaltenvektor  $\tilde{\gamma}_i$  gebildet haben, können wir anhand des Matrixproduktes

$$(\widehat{P})_p \cdot \tilde{\gamma}_i$$

ablesen, ob  $\gamma_i \in \Lambda_i$  für alle  $i$  und damit  $\gamma \in \Lambda$  gilt.

Insbesondere benutzen wir, um die  $R$ -Ordnung  $\Lambda$  zu beschreiben, die Pascalmatrix  $(\widehat{P})_p$  an zwei wesentlichen Stellen:

- Konjugation mit  $(\widehat{P})_p$  liefert eine Einbettung des getwisteten Gruppenringes  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  in eine minimale erbliche Überordnung  $\Gamma$ .

Allgemein gilt: Sei  $H$  eine Untergruppe von  $\text{Aut}(C_p^{n+1})$  und  $R$  wiederum der Fixring von  $\mathbb{Z}[\zeta_{p^{n+1}}]$  unter der durch  $H$  gegebenen Galoisgruppe. Dann folgt mit Lemma 3.2, dass  $R$  ein Dedekindring mit Primelement  $\pi$  ist. Dabei ist  $p$  über  $\pi$  vollständig verzweigt. Dann erhält man mit den selben Methoden wie oben, also Konjugation mit  $(\widehat{P})_p$ , den konstruktiven

**Satz** (Theorem 3.6). Es gibt eine volle Einbettung des getwisteten Gruppenringes  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$  in die erbliche  $R$ -Ordnung

$$\tilde{\Gamma} := \begin{pmatrix} R & \dots & R \\ (\pi) & R & \vdots \\ \vdots & \ddots & \ddots \\ (\pi) & \dots & (\pi) & R \end{pmatrix}_{|H| \times |H|}.$$

Nun liefert der von Auslander und Rim bewiesene Satz 3.5, dass der getwistete Gruppenring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$  genau dann zur erblichen  $R$ -Ordnung  $\tilde{\Gamma}$  isomorph ist, wenn  $p$  nicht die Ordnung von  $H$  teilt.

- Daneben erhalten wir mit  $(\widehat{P})_p$  ein Kriterium, um zu entscheiden, ob ein Element aus der erbliche Überordnung  $\Gamma$  auch in  $\Lambda$  liegt.

In den restlichen Kapiteln benutzen wir nun die Sätze 1, 2 und 3 für explizite Anwendungen:

In Kapitel 4 betrachten wir Automorphismen und Einheiten sowohl im ganzzahligen als auch im getwisteten Gruppenring:

Die Beschreibung von  $\mathbb{Z}G$  als Pullback

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}C_{p^n} \times C_p \\ \downarrow & & \downarrow \\ \Lambda & \xrightarrow{\delta} & \mathbb{F}_p C_{p^n} \times C_p. \end{array}$$

ermöglicht uns, einen äußeren Automorphismus zu konstruieren. Hierzu nehmen wir eine kanonische Einheit (siehe Remark 3.21 (i))

$$T = \begin{pmatrix} 1 & & & \\ & \zeta & & \\ & & \ddots & \\ & & & \zeta^{p-1} \end{pmatrix} \in \Lambda^\times,$$

welche sich für  $p \in \{2, 3\}$  nicht zu einer Einheit im Gruppenring heben läßt, das heißt, dass im Urbild von  $\delta(\lambda)$  in  $\mathbb{Z}C_{p^n} \times C_p$  keine Einheit liegt. Damit zeigen wir, dass die Konjugation mit  $T$  auf  $\Lambda$ , verknüpft mit der Identität auf  $\mathbb{Z}C_{p^n} \times C_p$ , einen äußeren Automorphismus von  $\mathbb{Z}G$  liefert.

Für das Element  $W \in \Lambda$  gilt mit Satz 1, dass  $W^p = \pi$ . Somit ist  $W$  keine Einheit in  $\Lambda$ , aber rational eine Einheit. Dann können wir den folgenden Satz zeigen, welchen wir dann im Kapitel 7 anwenden, um projektive Auflösungen von geeigneten  $\Lambda$ -Gittern zu konstruieren:

**Satz** (Theorem 4.5). Die Konjugation mit  $W$  liefert einen Automorphismus der  $R$ -Ordnung  $\Lambda$ .

Es sei  $D_4$  die Diedergruppe mit 8 Elementen. Dann bestimmen wir in  $\mathbb{Z}D_4$  die Gruppen der Einheiten mit Augmentation 1 als Untergruppe vom Index 2 in der Einheitengruppe des getwisteten Gruppenringes  $\mathbb{Z}[i] \rtimes C_2$ , wobei  $C_2$  durch komplexe Konjugation operiert. Beide Einheitengruppen beschreiben wir durch Erzeugende und Relationen (siehe Theorem 4.10 und Theorem 4.12).

In Kapitel 6 werden wir uns mit zwischen  $\Lambda$  und  $\Gamma$  gelegenen  $R$ -Ordnungen beschäftigen.

Dabei zeigen wir:

**Satz** (Theorem 6.10).

- (i) Die  $R$ -Ordnung  $\Gamma$  hat eine  $R$ -Basis  $\{b_{i,j}\}$  für  $0 \leq i, j < p$  und

$$b_{i,j} := \frac{N^i W^j}{\pi^{\nu(i,j)}}, \text{ mit } \nu(i,j) = \begin{cases} i \cdot p^{n-1} & \text{falls } i \leq j, \\ i \cdot p^{n-1} - 1 & \text{falls } i > j. \end{cases}$$

- (ii) Der Index der  $R$ -Ordnung  $\Lambda$  in der erblichen  $R$ -Ordnung  $\Gamma$  ist gegeben durch

$$|\Gamma/\Lambda| = p^{(p^n-1)\binom{p}{2}}.$$

Im Falle  $p = 2$  liefert der Radikalidealisorprozeß eine Beschreibung sämtlicher Zwischenordnungen:

**Satz** (Theorem 6.8). Sei  $\Lambda \simeq \mathbb{Z}[\zeta_{2^{n+1}}] \rtimes C_2$ . Dann liefert der Radikalidealisorprozeß folgende Kette von  $R$ -Ordnungen:

$$\Lambda = \Lambda_0 \subsetneq \dots \subsetneq \Lambda_{2^n-1} = \Gamma.$$

Dabei besitzt die Ordnung  $\Lambda_i$  eine  $R$ -Basis

$$\begin{aligned}\mathfrak{B}_{2k} &:= \{1, W, \pi^{-k}N, \pi^{-k}NW\}, & \text{falls } i = 2k, \\ \mathfrak{B}_{2k+1} &:= \{1, W, \pi^{-k}N, \pi^{-(k+1)}NW\}, & \text{falls } i = 2k + 1.\end{aligned}$$

Jede Zwischenordnung  $\tilde{\Lambda}$  ist ein Element dieser Kette.

Für ungerades  $p$  bedarf es jedoch anderer Methoden:

Ein Vergleich von Satz 2 (i) mit dem obigem Satz [Theorem 6.10 (i)] zeigt, dass sich die jeweiligen  $R$ -Basen von  $\Lambda$  und  $\Gamma$  nur durch bestimmte Potenzen von  $\pi$  unterscheiden. Diese Teilbarkeitsbedingungen bezüglich  $\pi$  werden wir benutzen, um bestimmte, zwischen  $\Lambda$  und  $\Gamma$  liegende  $R$ -Gitter grafisch zu beschreiben.

Aufgrund der multiplikativen Abgeschlossenheit liefert nun nicht jedes dieser Gitter auch eine Zwischenordnung. Ob dies der Fall ist, lässt sich zwar im Einzelfall, also für konkrete Zwischenordnungen, anhand der eingeführten grafischen Methoden verifizieren, ist aber für einen allgemeinen Ansatz ungeeignet. Wir gehen deshalb wie folgt, wieder unter Benutzung der grafischen Methoden, vor:

Zunächst zeigen wir, dass bestimmte  $R$ -Gitter  $\Gamma$ -Hauptideale sind. Aus diesen konstruieren wir eine Kette echt aufsteigender  $\Gamma$ -Ideale  $\mathfrak{J}_i$  von maximaler Länge, welche dann zu einer Kette maximaler Länge aufsteigender Zwischenordnungen  $\Lambda[\mathfrak{J}_i]$  führt.

In Kapitel 7 werden wir Ext-Gruppen gewisser  $\Lambda$ -Gitter berechnen. Mit den Spaltenvektoren

$$e_{p-1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_{p-2} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, \dots, e_0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

erhalten wir die folgenden Isomorphismen von  $\Lambda$ -Moduln

$$\Lambda \cdot e_{p-1} \simeq \begin{pmatrix} R \\ \pi \\ \vdots \\ \pi \end{pmatrix}, \dots, \Lambda \cdot e_1 \simeq \begin{pmatrix} R \\ \vdots \\ R \\ \pi \end{pmatrix}, \Lambda \cdot e_0 \simeq \begin{pmatrix} R \\ R \\ \vdots \\ R \end{pmatrix}$$

und diese implizieren

$$\Gamma \simeq \bigoplus_{i=0}^{p-1} \Lambda \cdot e_i.$$

Für diese Summanden wir können wir projektive Auflösungen konstruieren. Dabei wird die projektive Auflösung im Fall  $i = 0$  durch den nilpotenten Erzeuger  $N$  gegeben:

$$\dots \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot N^{p-1}} \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot e_0} \Lambda \cdot e_0 \longrightarrow 0.$$

Die Konjugation mit  $W^i$  liefert nach obigem **Satz** [Theorem 4.5] einem Automorphismus von  $\Lambda$ . Somit erhält man im Falle  $i > 0$  mit  $N_i := W^i N$  die projektiven Auflösungen

$$\dots \Lambda \xrightarrow{\cdot N_i} \Lambda \xrightarrow{\cdot N_i^{p-1}} \Lambda \xrightarrow{\cdot N_i} \Lambda \xrightarrow{\cdot e_i} \Lambda \cdot e_i \longrightarrow 0.$$

Da  $\Lambda$  eine Gorensteinordnung ist (siehe Kapitel 5), können wir in der Kategorie der  $\Lambda$ -Gitter analog injektive Auflösungen der  $\Lambda \cdot e_i$  angeben (siehe Proposition 7.2). Diese wird im Fall  $i = 0$  wie folgt gegeben:

$$0 \longrightarrow \Lambda \cdot e_0 \xrightarrow{\cdot p \cdot e_{p-1}^T} \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot N^{p-1}} \Lambda \xrightarrow{\cdot N} \Lambda \dots$$

Wir verknüpfen nun die projektive mit der injektiven Auflösung und erhalten eine Sequenz, zyklisch vom Grad 2, die wir benutzen, um in Lemma 7.4 die Tatekohomologie  $\widehat{\text{Ext}}_{\Lambda}^n(\Lambda \cdot e_i, \Lambda \cdot e_j)$  zu berechnen.

Weiterhin beschreiben wir dann den Kohomologiering  $H_{\Lambda}^*(\Gamma)$  durch Komposition von Kettenkomplexen. Als Faktorringer erhalten wir dann die Kohomologieringe  $H_{\Lambda}^*(\Lambda \cdot e_i)$ , für die wir eine Obstruktion zur Kommutativität geben können.

In Kapitel 8 bestimmen wir mit Hilfe eines Resultates von Drozd and Kiričenko den Darstellungstyp des gewisteten Gruppenringes  $\Lambda$ :

**Satz** (Theorem 8.7). Sei  $p$  prim und  $n \geq 1$ . Dann ist der Darstellungstyp des gewisteten Gruppenringes  $\Lambda \simeq \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  genau dann endlich, wenn  $p = 2$  ist.

Insbesondere erhält man Beispiele nicht kommutativer, vollständig verzweigter  $R$ -Ordnungen mit endlichem Darstellungstyp.

---

An dieser Stelle möchte ich allen voran Prof. Roggenkamp nicht nur für die interessante Themenstellung, sondern auch für seine Unterstützung in jeder Hinsicht meinen Dank aussprechen.

Für anregende und fruchtbare Diskussionen möchte ich mich besonders bei Martin Hertweck und Matthias Künzer bedanken.

## 0. INTRODUCTION

In this work we will regard integral group rings  $\mathbb{Z}G$  for a series of  $p$ -groups  $G$ . For that reason we consider the integral group ring  $\mathbb{Z}G$  as a pullback diagram. This enables us to understand a ‘complicate structure’, the integral group ring, by means of two ‘easier structures’ which are connected by congruences. The most easiest example of such a description <sup>4</sup> is given by the integral group ring of a cyclic group of prime order  $p$ :

$$\begin{array}{ccc} \mathbb{Z}C_p & \xrightarrow{\alpha} & \mathbb{Z} \\ \beta \downarrow & & \downarrow \gamma \\ \mathbb{Z}[\zeta] & \xrightarrow{\delta} & \mathbb{F}_p, \end{array}$$

where  $\zeta$  is a primitive  $p$ -th root of unity,  $\alpha(c) = 1$ ,  $\beta(c) = \zeta$  and the maps  $\gamma$  and  $\delta$  are given by the kernels  $(p)$  and  $(1 - \zeta)$ .

Hence we get the following isomorphism of rings

$$\mathbb{Z}C_p \simeq \{(a, b) \mid (a, b) \in \mathbb{Z} \times \mathbb{Z}[\zeta], \gamma(a) = \delta(b)\} \subset \mathbb{Z} \times \mathbb{Z}[\zeta].$$

Similary we get a recursive description of the integral group ring  $\mathbb{Z}C_{p^{n+1}}$  of a cyclic group of order  $p^{n+1}$ :

$$\begin{array}{ccc} \mathbb{Z}C_{p^{n+1}} & \longrightarrow & \mathbb{Z}C_{p^n} \\ \downarrow & & \downarrow \\ \mathbb{Z}[\zeta_{p^{n+1}}] & \longrightarrow & \mathbb{F}_p C_{p^n} \end{array}$$

where  $\zeta_{p^{n+1}}$  is a primitive  $p^{n+1}$ -root of unity.

For a non-cyclic abelian  $p$ -group  $A$  we can also decompose the integral group ring  $\mathbb{Z}A$  by pullback diagrams, but we will get complicate congruences which are not suitable for explicit calculations. Even for Klein’s four group  $V_4$  we get the following isomorphism of rings

$$\mathbb{Z}V_4 \simeq \{(a, b, c, d) \mid (a, b, c, d) \in \mathbb{Z}^4, a \equiv b \equiv c \equiv d \pmod{2}, a + b + c + d \equiv 0 \pmod{4}\},$$

which is not suitable for explicit calculations.

Descriptions of integral group rings of some non-abelian groups were given by Roggenkamp (see [Ro2]) and Künzer (see [Kü]).

---

<sup>4</sup>Rim ([Rim]) used this description and the Mayer-Victoris sequence to determine the class group of the integral group ring  $\mathbb{Z}G$ :  $\text{Cl}(\mathbb{Z}C_p) \simeq \text{Cl}(\mathbb{Z}[\zeta])$ .

As in the abelian case integral group rings of  $p$ -groups with cyclic maximal subgroups are most suitable for a description by pullback diagrams. These groups are (see [Rob] Theorem 5.3.2):

- (i) a dihedral group  $D_{2^n}$ ,
- (ii) a semidihedral group  $\langle x, a \mid x^2 = a^{2^{n+1}} = 1, a^x = a^{2^n-1} \rangle$ ,  $n \geq 1$ ,
- (iii) a group of the form  $G := \langle a, b \mid a^{p^{n+1}} = 1, b^p = 1, a^b = a^{p^n+1} \rangle$ ,  $n \geq 1$ ,
- (iv) a generalized quaternion group  $Q_{2^n}$ .

Zimmermann investigated in [Zi] integral group rings of dihedral groups  $D_{2^n}$ . In this work we will introduce a method which enables us to treat the cases (i) - (iii). Then we will apply this method to the case (iii), because this case also includes odd primes.

Now let  $G$  be defined as in (iii). Then we get, as in the case of  $\mathbb{Z}C_{p^{n+1}}$ , a description of  $\mathbb{Z}G$  as pullback:

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}C_{p^n} \times C_p \\ \downarrow & & \downarrow \\ \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p & \xrightarrow{\delta} & \mathbb{F}_p C_{p^n} \times C_p. \end{array}$$

Now one is interested in a description

- of the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  as subring of a matrix ring,
- the congruences.

A description of  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  by matrices is given by Ritter and Sehgal [RiSe]. We will give a conjugate representation which respects the  $p$ -adic structure. Explicitly:

(To avoid some distinction of cases we will now just consider the case  $p$  odd. It's understood that the easier case  $p = 2$  is done in this work as well.)

We consider  $\mathbb{Z}[\zeta_{p^{n+1}}]$  as module over  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$ , where the coefficients act by multiplication and the group  $C_p := \langle b \rangle$  act via the Galois-automorphism

$$\begin{array}{ccc} b : \mathbb{Z}[\zeta_{p^{n+1}}] & \rightarrow & \mathbb{Z}[\zeta_{p^{n+1}}] \\ \zeta_{p^{n+1}} & \mapsto & \zeta_{p^{n+1}}^{p^n+1} = \zeta \cdot \zeta_{p^{n+1}} \end{array} \quad .$$

Now  $R := \mathbb{Z}[\zeta_{p^n}]$  is the fixed ring of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  under this Galois-operation and  $\mathfrak{B}' := \{1, \zeta_{p^{n+1}}, \dots, \zeta_{p^{n+1}}^{p-1}\}$  is an  $R$ -basis of  $\mathbb{Z}[\zeta_{p^{n+1}}]$ . We now consider the elements of the basis as column vectors to get the representation of the  $R$ -order  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$

given by Ritter and Sehgal:

$$A' = \begin{pmatrix} 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ \zeta_{p^n} & & & & 0 \end{pmatrix}, \quad B' = \begin{pmatrix} 1 & & & & \\ & \zeta & & & \\ & & \zeta^2 & & \\ & & & \ddots & \\ & & & & \zeta^{p-1} \\ & & & & & 0 \end{pmatrix}.$$

We are interested in the representations with respect to the  $p$ -adically ordered  $R$ -basis  $\mathfrak{B} := \{1, 1 - \zeta_{p^{n+1}}, \dots, (1 - \zeta_{p^{n+1}})^{p-1}\}$ . The transformation of the  $R$ -bases is given by the Pascal matrix, which is defined using the binomial coefficients

$$(\widehat{P})_p = \begin{pmatrix} 1 & 0 & & & 0 \\ 1 & -1 & & & \\ 1 & -2 & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ 1 & -(p-1) & \dots & -(p-1) & 1 \end{pmatrix}.$$

We conjugate  $A'$  and  $B'$  by  $(\widehat{P})_p$  to get representations  $A$  and  $B$  (see Lemma 3.11), which generate an  $R$ -order  $\Lambda$ . Then we get  $\Lambda$  as image of an embedding of the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  into the minimal hereditary over order

$$\Gamma := \begin{pmatrix} R & \dots & R \\ (\pi) & R & \vdots \\ \vdots & \ddots & \ddots \\ (\pi) & \dots & (\pi) & R \end{pmatrix},$$

with  $\pi := 1 - \zeta_{p^n}$  being prime in  $R$ . Especially we are in the totally ramification case which is of interest in algebraic number theory.

So far we have an embedding of the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  into an order with which we are familiar, but we have got representations  $A$  and  $B$  which are not suitable for explicit calculations, especially if we compare these matrices with  $A'$  and  $B'$ . Surprisingly there are generators  $N$  and  $W$  of the  $R$ -order  $\Lambda$ ,

$$N := \begin{pmatrix} 0 & & & & \\ 1-\zeta & & & & \\ & \ddots & & & \\ & & & 1-\zeta^{p-1} & 0 \end{pmatrix}, \quad W := \begin{pmatrix} 0 & 1 & & & \\ & & \ddots & & \\ & & & & 1 \\ \pi & & & & 0 \end{pmatrix},$$

which are suitable for explicit calculations:

**Theorem. 1** [Theorem 3.20 (i)] Let  $\zeta := \zeta_{p^n}^{p-1}$ . Then the  $R$ -order  $\Lambda$ , which is isomorphic to the twisted group ring  $Z[\zeta_{p^{n+1}}] \rtimes C_p$ , is generated by  $N$  and  $W$  with the relations

$$N^p = 0, \quad W^p = \pi, \quad WN = \zeta \cdot NW + (1 - \zeta).$$

We will show that  $N$  and  $W$  generate a maximal ideal in  $\Lambda$ , which coincides after localization at  $p$  with the radical.

To prove this theorem we will introduce in Chapter 2 the technique of recursively defined matrices. This leads to calculations involving lower triangular matrices of infinite size, for example we have to invert the  $q$ -Pascal matrix  $G$ , where the entries are given by the Gauss polynomials<sup>5</sup>.

We will use **Theorem 1** to characterize the  $R$ -order  $\Lambda$  as follows:

**Theorem. 2** [Theorem 3.22] The  $R$ -order  $\Lambda$  has the following  $R$ -bases:

- (i)  $\mathfrak{B}_\Lambda = \{N^i W^j \mid 0 \leq i, j \leq p-1\}$ ,
- (ii)  $\mathfrak{B}'_\Lambda = \{W^i N^j \mid 0 \leq i, j \leq p-1\}$ .

Then **Theorem 3**[Theorem 3.30] describes the  $R$ -order  $\Lambda$  by congruences and provides a criterion to decide, whether an element of the hereditary over order  $\Gamma$  is even an element of  $\Lambda$ . This criterion involves multiplication with the Pascal matrix  $\widehat{P}$ . Hence there are two important points where the Pascal matrix<sup>6</sup>  $\widehat{P}$  is used to describe the  $R$ -order  $\Lambda$ :

- Conjugation with  $(\widehat{P})_p$  provides an embedding of the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  into the minimal hereditary over order  $\Gamma$ . More general the following holds: Let  $H$  be a subgroup of  $\text{Aut}(C_p^{n+1})$ . Again we denote by  $R$  the fixed ring of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  under the Galois operation given by  $H$ . Lemma 3.2 shows that  $R$  is a Dedekind ring with prime  $\pi$ , where  $p$  is totally ramified over  $\pi$ . Then conjugation with  $(\widehat{P})_p$  yields the constructive

---

<sup>5</sup>The Gauss polynomials have, besides their importance in combinatorics (see [An]), the following application in representation theory:

Evaluation of the Gauss polynomials  $\begin{bmatrix} i \\ j \end{bmatrix}$  at the prime power  $q := p^n$  provides the number of the  $j$ -dimensional subspaces in  $\mathbb{F}_q^i$ . This used to determine the dimensions of the Specht modules in the representation theory of the symmetric groups.

<sup>6</sup>We will show that  $\widehat{P}$  is an involution. This was already known at the end of the nineteenth century and can be found in the standard work *Lehrbuch der Algebra* by Heinrich Weber but surprisingly not in the literature of modern linear algebra (see Lemma 1.2 and Remark 1.5).

**Theorem** (Theorem 3.6). There is a full embedding of the  $R$ -order  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$  into the minimal hereditary  $R$ -order

$$\tilde{\Gamma} = \begin{pmatrix} R & \dots & R \\ (\pi) & R & \vdots \\ \vdots & \ddots & \ddots \\ (\pi) & \dots & (\pi) & R \end{pmatrix}_{|H| \times |H|}.$$

Now a Theorem of Auslander and Rim (see Theorem 3.5) shows that the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$  is isomorphic to  $\tilde{\Gamma}$  if and only if  $p$  does not divide the order of  $H$ .

- Further  $(\hat{P})_p$  can be used to obtain a criterion, to decide, whether an element of the hereditary overorder  $\Gamma$  is even an element of  $\Lambda$ .

In the following chapters we will use the Theorems 1, 2 and 3 for explicit applications:

In Chapter 4 we consider automorphisms and units of the integral and also of the twisted group ring:

The description of  $\mathbb{Z}G$  as pullback

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}C_{p^n} \times C_p \\ \downarrow & & \downarrow \\ \Lambda & \xrightarrow{\delta} & \mathbb{F}_p C_{p^n} \times C_p \end{array}$$

allows us to construct an outer automorphism of the integral group ring  $\mathbb{Z}G$  in the case  $p \in \{2, 3\}$ , which is given by conjugation with the canonical unit (see Remark 3.21 (i))

$$T = \begin{pmatrix} 1 & & & \\ & \zeta & & \\ & & \ddots & \\ & & & \zeta^{p-1} \end{pmatrix} \in \Lambda^\times$$

on  $\Lambda$  and the identity on  $\mathbb{Z}C_{p^n} \times C_p$ .

From Theorem 1 we get that  $W^p = \pi$ , hence  $W$  is no unit in  $\Lambda$  but it is rational unit. It turns out that

**Theorem** (Theorem 4.5). Conjugation with  $W$  provides an automorphism of the  $R$ -order  $\Lambda$ .

We will use this theorem in Chapter 7 to construct projective resolutions of some  $\Lambda$ -lattices we are interested in. Explicitly we get with the column vectors

$$e_{p-1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_{p-2} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, \dots, e_0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

the following isomorphisms of  $\Lambda$ -modules

$$\Lambda \cdot e_{p-1} \simeq \begin{pmatrix} R \\ \pi \\ \vdots \\ \pi \end{pmatrix}, \dots, \Lambda \cdot e_1 \simeq \begin{pmatrix} R \\ \vdots \\ R \\ \pi \end{pmatrix}, \Lambda \cdot e_0 \simeq \begin{pmatrix} R \\ R \\ \vdots \\ R \end{pmatrix}$$

and also

$$\Gamma \simeq \bigoplus_{i=0}^{p-1} \Lambda \cdot e_i.$$

The nilpotent element  $N$  yields the projective resolution

$$\dots \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot N^{p-1}} \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot e_0} \Lambda \cdot e_0 \longrightarrow 0.$$

Then conjugation with  $W^i$  provides projective resolutions for arbitrary  $\Lambda \cdot e_i$ . Since  $\Lambda$  is Gorenstein we also get injective resolutions in the category of  $\Lambda$ -lattices:

$$0 \longrightarrow \Lambda \cdot e_0 \xrightarrow{\cdot p \cdot e_{p-1}^T} \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot N^{p-1}} \Lambda \xrightarrow{\cdot N} \Lambda \dots$$

Hence by splicing together the projective and injective resolution of  $\Lambda \cdot e_0$  (and similar for  $\Lambda \cdot e_i$ ) one gets the following exact sequence, cyclic of degree 2

$$\dots \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot N^{p-1}} \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot N^{p-1}} \Lambda \dots,$$

which we will use to calculate the Tate cohomology. Then we describe products in cohomology by composition of chain maps.

In Chapter 6 we consider orders which lie between  $\Lambda$  and  $\Gamma$ . We will show:

**Theorem** (Theorem 6.10 ).

(i) The  $R$ -order  $\Gamma$  has the  $R$ -basis  $\{b_{i,j}\}$  for  $0 \leq i, j < p$  and

$$b_{i,j} := \frac{N^i W^j}{\pi^{\nu(i,j)}}, \text{ with } \nu(i,j) = \begin{cases} i \cdot p^{n-1} & \text{if } i \leq j, \\ i \cdot p^{n-1} - 1 & \text{if } i > j. \end{cases}$$

(ii) The index of the  $R$ -order  $\Lambda$  in the hereditary  $R$ -order  $\Gamma$  is given by

$$|\Gamma/\Lambda| = p^{(p^n-1)\binom{p}{2}}.$$

In the case  $p = 2$  the radical idealisator process provides all intermediate orders:

**Theorem** (Theorem 6.8 ). Let  $\Lambda \simeq \mathbb{Z}[\zeta_{2^{n+1}}] \rtimes C_2$ .

(i) The radical idealisator process provides a chain of orders

$$\Lambda = \Lambda_0 \subsetneq \dots \subsetneq \Lambda_{2^n-1} = \Gamma.$$

An  $R$ -basis of order  $\Lambda_i$  is given by

$$\begin{aligned} \mathfrak{B}_{2k} &:= \{1, W, \pi^{-k}N, \pi^{-k}NW\} && \text{if } i=2k \text{ is even,} \\ \mathfrak{B}_{2k+1} &:= \{1, W, \pi^{-k}N, \pi^{-(k+1)}NW\} && \text{if } i=2k+1 \text{ is odd.} \end{aligned}$$

(ii) The chain of intermediate orders in (i) is of maximal length. Every intermediate order  $\tilde{\Lambda}$  is an element of this chain.

For odd  $p$  we need other methods: The theorem above [Theorem 6.10 (i)] shows that there are  $R$ -bases of  $\Lambda$  and  $\Gamma$  which are just differing by  $\pi^{-\nu(i,j)}$ . We will introduce a graphical description, which respects this divisibility by  $\pi$ , to get a chain of intermediate orders of maximal length.

In Chapter 8 we prove the following theorem

**Theorem** (Theorem 8.7). Let  $p$  be prime and  $n \geq 1$ . Then the representation type of the twisted group ring  $\Lambda \simeq \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  is finite if and only if  $p = 2$ .

In particular, we get examples of non commutative, totally ramified  $R$ -orders of finite representation type.

## 1. THE PASCAL MATRIX

## 1.1. Preliminaries.

The following matrices will be important for us

**Definition 1.1.** (i) Let  $q$  an indeterminate and  $M_q$  be an infinite matrix with entries

$$(M_q)_{i,j} \in \mathbb{Z}[q], i, j \geq 1.$$

Then we have the following operations on  $M_q$  :

- *evaluation*: Let  $\mu$  be an algebraic number. Then  $M_\mu$  means the evaluation of  $M_q$  at  $\mu$ .
- *restriction*: Let  $n \in \mathbb{N}$ . Then  $(M_q)_n$  is the  $n \times n$  matrix with entries

$$(M_q)_{i,j} \text{ for } 1 \leq i, j \leq n.$$

(ii) The diagonal matrix  $D_q$  is defined by

$$(D_q)_{i+1,j+1} := \delta_{i,j} q^i, \text{ for } i, j \geq 0.$$

(with the Kronecker symbol  $\delta_{i,j}$ .)

(iii) The Pascal matrix  $P$  is defined by the binomial coefficients

$$(P)_{i+1,j+1} := \binom{i}{j}, \text{ with } i, j \geq 1 \text{ and } \binom{i}{j} := 0 \text{ for } j > i.$$

(iv)  $\widehat{P} := PD_{-1}$ .

**Lemma 1.2.** (i)  $P^{-1} = D_{-1}PD_{-1}$ , this means  $(P^{-1})_{i+1,j+1} = (-1)^{i+j} \binom{i}{j}$ .

(ii)  $\widehat{P}$  is an involution. (Also:  $D_{-1}P$  is an involution.)

(iii) Let  $n \in \mathbb{N}$ ,  $n > 1$  and  $\zeta$  a  $n$ -th root of unity. Then  $PD_\zeta$  is of order  $n$ .

*Proof:* (i) and (ii) are equivalent, and (ii) follows from (iii). Thus we only have to show (iii).

(iii): Let  $R$  be a commutative ring with  $\zeta \in R$  and  $R[X]$  the polynomial ring. By considering row vectors,  $PD_\zeta$  transforms the basis  $B := \{1, X, X^2, \dots\}$  to  $B' := \{1, 1+\zeta X, (1+\zeta X)^2, \dots\}$ . Applying  $PD_\zeta$   $n$  times on  $B$  one gets the identity because  $(1+\zeta(1+\dots+\zeta(1+\zeta X)\dots))^i = (1+\zeta+\dots+\zeta^{n-1}+\zeta^n X)^i = X^i$ .  $\square$

**Remark 1.3.** (i) Multiplication of these matrices causes no problems because in every row there are only finitely many nonzero entrances.

(ii) Because of the triangular shape of the matrices, the statements remain true, when we *restrict* each matrix  $M$  to  $(M)_n$ ,  $n \in \mathbb{N}$ .

(iii) Let  $q$  be invertible. Then we have  $D_q^{-1} = D_{q^{-1}}$ .

**Example 1.4.**

$$\hat{P} = \begin{pmatrix} 1 & 0 & & 0 \\ 1 & -1 & 0 & & \\ 1 & -2 & 1 & 0 & \\ 1 & -3 & 3 & -1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \quad (P^{-1})_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 \\ -1 & 3 & -3 & 1 & 0 \\ 1 & -4 & 6 & -4 & 1 \end{pmatrix}.$$

**Remark 1.5.** (i) The idea for the proof of Lemma 1.2 is taken from Heinrich Weber's *Lehrbuch der Algebra* [We], just by replacing  $-1$  by an arbitrary root of unity therefore getting part (iii) of the Lemma 1.2.

(ii) The Pascal matrix appears in Weber's book when the following problem of interpolation is solved:

For a given field  $K$  of characteristic 0 and elements  $p_i \in K$ ,  $0 \leq i \leq n$  one wants to determine the polynomial  $p(X)$  of degree  $n$  with evaluations  $p(i) = p_i$  for  $0 \leq i \leq n$ .

Any polynomial of degree  $n$  can be written in the form

$$c_0 b_0(X) + c_1 b_1(X) + \dots + c_n b_n(X)$$

where  $c_i \in K$  and

$$b_\nu(X) := \frac{X(X-1)\dots(X-\nu+1)}{\nu!}$$

is the binomial polynomial of degree  $\nu$ . This leads, with the vectors  $v := (p_0, \dots, p_n)^t$  and  $c := (c_0, \dots, c_n)^t$ , to the linear system  $(P)_{n+1}c = v$ , which is solved by Lemma 1.2.

(iii) Let  $\lambda$  be a unit of the commutative ring  $R$ . Then the  $R[X]$ -module  $R[X]/(X-\lambda)^n$  is free as  $R$ -module with bases

$$\mathfrak{B} := \{1, X, \dots, X^{n-1}\} \text{ and } \mathfrak{B}' := \{1, X-\lambda, \dots, (X-\lambda)^{n-1}\}.$$

By considering row vectors the basis transformation from  $\mathfrak{B}$  to  $\mathfrak{B}'$  is given by the  $n \times n$  matrix

$$\begin{pmatrix} 1 & & & \\ -\lambda & 1 & & \\ \lambda^2 & -2\lambda & 1 & \\ \vdots & \ddots & \ddots & \ddots \end{pmatrix}_n = (D_{-\lambda})_n (P)_n (D_{-\lambda}^{-1})_n = (D_\lambda)_n (P^{-1})_n (D_\lambda^{-1})_n$$

and hence from  $\mathfrak{B}'$  to  $\mathfrak{B}$  by  $(D_\lambda)_n (P)_n (D_\lambda^{-1})_n$ .

So the Pascal matrix  $P$  and the diagonal matrix  $D_\lambda$  provide a basis transformation between the Jordan and the rational canonical form. (The

Jordan and the rational canonical form coincide for  $\lambda = 0$ , so we handled all cases of classical linear algebra.)

### 1.2. Integral group rings and the Pascal matrix.

Let  $\zeta$  be a  $p$ -th root of unity and  $C_p$  the cyclic group of order  $p$ , generated by  $c$ . Then we consider the integral group ring  $\mathbb{Z}[\zeta]C_p$  as subring of  $\prod_{0 \leq i \leq p-1} \mathbb{Z}[\zeta]$  via the Wedderburn embedding:

$$\begin{array}{ccc} \omega_p : \mathbb{Z}[\zeta]C_p & \xrightarrow{\omega_p} & \prod_{0 \leq i \leq p-1} \mathbb{Z}[\zeta] \\ c & \longmapsto & \zeta^i \end{array}$$

which is obviously an embedding of  $\mathbb{Z}[\zeta]$ -orders, with the following properties:

**Theorem 1.6.** (i) A  $\mathbb{Z}[\zeta]$ -basis of the image  $\text{Im}(\omega_p)$  is given by the columns of  $(\widehat{P})_p \cdot (D_{1-\zeta})_p$ .  
(ii) Let  $v := (v_1, \dots, v_p)^t$  with  $v_i \in \mathbb{Z}[\zeta]$ . Then

$$v \in \text{Im}(\omega_p) \iff (D_{1-\zeta})_p^{-1} (\widehat{P})_p \cdot v \in \mathbb{Z}[\zeta]^p.$$

*Proof.* (i) and (ii) are equivalent, since  $(\widehat{P})_p$  is an involution ( Lemma 1.2 (ii)). (ii) is shown by Kleinert in [Kl]. A proof for both parts in a more general case is given by Künzer and Weber [KüWe].  $\square$

**Remark 1.7.** (i) For Theorem 1.6 one just needs that the coefficients contain a primitive  $p$ -th root of unity. Then the Pascal matrix  $P$  appears twice : In (i) it provides a basis of the group ring and in (ii) one gets a test whether  $v \in \mathbb{Z}[\zeta]^p$  is in the image of the Wedderburn embedding  $\omega_p$ .  
(ii) Later on we will consider the twisted group ring  $\mathbb{Z}[\zeta_{p^n}] \rtimes C_p$ , where  $C_p$  acts via the Galois automorphism  $\sigma \in \text{Gal}(\mathbb{Q}[\zeta_{p^n}], \mathbb{Q})$  with  $\sigma(\zeta_{p^n}) := \zeta_{p^n}^{p^{n-1}+1}$ . After embedding  $\mathbb{Z}[\zeta_{p^n}] \rtimes C_p$  into a matrix ring, we will use the matrix  $(\widehat{P})_p$  to test, whether an element of the matrix ring is in the image of the twisted group ring.  
(iii) The description of the group ring  $\mathbb{Z}[\zeta_{p^n}]C_p$ , via the Wedderburn embedding is very useful for explicit calculations, as one sees when considering the rational idempotents, (i.e. the idempotents in the group ring  $\mathbb{Q}[\zeta_{p^n}]C_p$ ). We illustrate this by giving an elementary proof of a lemma, which is crucial for the generalization of the 'Rigidity of  $\pi$ -adic  $p$ -torsion' from Weiss [Wei], given by Roggenkamp [Ro].

Let us fix the notation:

- $R$  is a  $p$ -adic ring, i.e., the integral closure of the  $p$ -adic integers  $\hat{\mathbb{Z}}_p$  in a finite extension of the  $p$ -adic field  $\hat{\mathbb{Q}}_p$ .
- $G$  is a finite  $p$ -group with normal subgroup  $N \triangleleft G$  and  $I_R(N)$  denotes the augmentation ideal, induced by the exact sequence

$$0 \longrightarrow I_R(N) \longrightarrow RG \longrightarrow RG/N \longrightarrow 0.$$

- An  $RG$ -permutation lattice has a finite  $R$  basis, which is permuted by the  $G$  operation.

Then Weiss proved the following theorem for  $R = \hat{\mathbb{Z}}_p$ .

**Theorem 1.8.** Let  $M$  be an  $RG$ -lattice and  $N \triangleleft G$ , such that

- (i)  $M|_N$  is free as  $RN$  module,
- (ii)  $M/I_R(N)M$  is a permutation lattice for  $G/N$ ,

Then  $M$  is an  $RG$ -permutation lattice.

Roggenkamp generalized this result to  $p$ -adic coefficient rings  $R$ . In [Ro] p.432, (or [RoTa] p.39) he explained :

'Let me briefly point out, where the difficulty with ramification lies: Let  $C_p$  be a cyclic group of order  $p$ . If  $R$  is an unramified extension of  $\hat{\mathbb{Z}}_p$ , let  $\zeta$  be a primitive  $p$ -th root of unity. Then the group ring  $RC_p$  is the pullback

$$\begin{array}{ccc} RC_p & \longrightarrow & R \\ \downarrow & & \downarrow \\ \Lambda & \longrightarrow & R/(p), \end{array}$$

where  $\Lambda = R[\zeta]$  is a finite extension of  $R$ ; moreover the only indecomposable  $RC_p$ -lattices are  $R, \Lambda, RC$ . So one can prove statements about lattices by inspections, as Weiss has done.

If  $R$  now has ramification  $RC_p$  is still a pullback as above, however,  $\Lambda$  is not an order in a field anymore: it is a rather complicated order, and in general, there are infinitely many indecomposable  $RC_p$  lattices,  $RC_p$  is wild in most of the cases.'

Now Roggenkamp has described  $\Lambda_{p-1} := RC_p$  by considering a series of pullbacks:

$$\begin{array}{ccc} \Lambda_i & \longrightarrow & R \\ \downarrow & & \downarrow \\ \Lambda_{i-1} & \longrightarrow & \overline{R}, \end{array}$$

using the following well known Lemma.

**Lemma 1.9.** Let  $S$  be a Dedekind ring with field of quotients  $K$ ,  $\Gamma$  an  $S$ -order in a  $K$ -algebra  $A$  and  $e \in A$  a central idempotent. Then one has the following pullback of  $S$ -orders:

$$\begin{array}{ccc} \Gamma & \xrightarrow{\cdot e} & \Gamma e \\ \cdot(1-e) \downarrow & & \downarrow \\ \Gamma(1-e) & \longrightarrow & \bar{\Gamma}, \end{array}$$

with  $\bar{\Gamma} := \Gamma e / (\Gamma \cap \Gamma e) \simeq \Gamma(1-e) / (\Gamma \cap \Gamma(1-e))$ . The units  $\Gamma^\times$  are given by  $\Gamma^\times \simeq ((\Gamma e)^\times \times (\Gamma(1-e))^\times) \cap \Gamma$ .

Now we use the same decomposition in pullbacks by considering  $RC_p$  via the Wedderburn embedding  $\omega_p$ :

We set  $\Lambda := \omega_p(RC_p)$  and denote for  $0 \leq i < p$  the primitive idempotents by

$$e_i \in R^p, \text{ with } (e_i)_j := \delta_{i,j}, \quad \eta_i := \sum_{j=0}^i e_j \text{ and } \Lambda_i := \Lambda \eta_i.$$

(Hence  $\Lambda_{p-1} \simeq RC_p$  and  $\Lambda_0 \simeq R$ .)

Theorem 1.6 provides an  $R$ -basis of  $\Lambda_i \subseteq R^{i+1}$  by the columns of  $(\hat{P})_{i+1} \cdot (D_\pi)_{i+1}$ , with  $\pi := 1 - \zeta$ , where  $p$  is totally ramified over  $\pi$ . We denote this  $R$ -basis by  $B_i := \{b_{i,0}, \dots, b_{i,i}\}$ , with column vectors  $b_{i,k} := (-\pi)^k \cdot \left( \binom{0}{k}, \dots, \binom{i}{k} \right)^t$ . Then Lemma 1.9 applied to the  $\Lambda_i$  provides Lemma 1 of [Ro] (also Lemma 3.3. of [RoTa]):

**Lemma 1.10.** Let  $0 < i < p$ . Then we have a pullback

$$\begin{array}{ccc} \Lambda_i & \xrightarrow{\cdot \eta_{i-1}} & \Lambda_{i-1} \\ \cdot e_i \downarrow & & \downarrow \phi \\ R & \xrightarrow{\text{mod } \pi^i} & R/(\pi^i), \end{array}$$

where, with respect to the  $R$ -bases  $B_i$  and  $B_{i-1}$ , the maps correspond to the following matrices:

$$\cdot \eta_{i-1} \sim \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \end{pmatrix}, \quad \cdot e_i \sim \begin{pmatrix} 1 \\ -\pi \binom{i}{1} \\ \vdots \\ (-\pi)^i \binom{i}{i} \end{pmatrix}, \quad \phi \sim \begin{pmatrix} 1 \\ -\pi \binom{i}{1} \\ \vdots \\ (-\pi)^{i-1} \binom{i}{i-1} \end{pmatrix} \cdot \text{mod } \pi^i.$$

The kernels are given by the following  $R$ -bases:

$$\begin{aligned} \text{Ker}(\cdot\eta_{i-1}) &: \{b_{i,i}\}, \\ \text{Ker}(\cdot e_i) &: \{b_{i,1} + \pi \binom{i}{1} b_{i,0}, \dots, (-1)^{i-2} b_{i,i-1} + \pi^{i-1} \binom{i}{i-1} b_{i,0}, (-1)^{i-1} b_{i,i} + \pi^i \binom{i}{i} b_{i,0}\}, \\ \text{Ker}(\phi) &: \{b_{i-1,1} + \pi \binom{i}{1} b_{i-1,0}, \dots, (-1)^{i-2} b_{i-1,i-1} + \pi^{i-1} \binom{i}{i-1} b_{i-1,0}, \pi^i \binom{i}{i} b_{i-1,0}\}. \end{aligned}$$

*Proof.* The matrices corresponding to  $\cdot\eta_i$  and  $\cdot e_i$  are given by Theorem 1.6 and the chosen bases. With these matrices we easily get the kernels  $\text{Ker}(\cdot\eta_{i-1})$  and  $\text{Ker}(\cdot e_i)$ .

Since  $(\text{Ker}(\cdot\eta_{i-1})) \cdot e_i \simeq (\pi^i)$ ,  $\phi$  is the uniquely determined map, which makes the diagram commute. The isomorphism given by the multiplication of  $\text{Ker}(\cdot e_i)$  with  $\cdot\eta_{i-1}$  yields to  $\text{Ker}(\phi)$ .  $\square$

### 1.3. Pascal matrix and Bernoulli numbers.

Now we prove Lemma 1.2 using complex analysis:

An analytic function in 0 is uniquely determined by a power series

$$f(X) = \sum_{\nu \geq 0} a_\nu \frac{X^\nu}{\nu!}.$$

By identifying  $f$  with  $a := (a_0, a_1, \dots)^t$  the substitution  $X \rightarrow qX$  corresponds to the multiplication with  $D_q$ , the multiplication with  $e^X$  corresponds to the multiplication with  $P$ . By *specializing*  $q := \zeta$ , a  $n$ -th root of unity, one gets

$$\begin{aligned} PD_\zeta \cdot f(X) &= f(\zeta X) e^X, \\ (PD_\zeta)^2 \cdot f(X) &= f(\zeta^2 X) e^{(\zeta+1)X}, \\ &\dots \\ (PD_\zeta)^n \cdot f(X) &= f(\zeta^n X) e^{(\zeta^{n-1} + \dots + \zeta + 1)X} = f(X). \end{aligned}$$

Since  $f(X)$  is arbitrary,  $PD_\zeta$  is of order  $n$ .

**Remark 1.11.** (i) Now we consider the function

$$f(X) := \frac{X e^{-X/2}}{e^{X/2} - e^{-X/2}} = \sum_{\nu \geq 0} b_\nu \frac{X^\nu}{\nu!},$$

where the coefficients in  $f(X)$  are defining the Bernoulli numbers. Since

$$f(X) = f(-X) \cdot e^X,$$

we consider the Bernoulli numbers as 'eigenvector' to the 'eigenvalue' 1 of the involution  $D_{-1}P$ , (see Lemma 1.2).

(Sometimes the Bernoulli numbers are defined by  $g(X) := \frac{X e^{X/2}}{e^{X/2} - e^{-X/2}}$ , see [Neu], just differing from the first one by  $b_1 = 1/2$  instead of  $b_1 = -1/2$ . Then  $g(X)$  is fixed by the involution  $PD_{-1}$ .)

- (ii) One easily sees that there are no eigenvectors for the Pascal matrix  $P$  and that the space of eigenvectors to the 'eigenvalue' 1 of  $D_{-1}P$  is of infinite dimension. The Bernoulli numbers are the unique eigenvector to the 'eigenvalue' 1 of the modified Pascal matrix, which differs from  $P$ , just by multiplication of the second row with  $-1$ .  
(If we use the function  $g(x)$  for the definition of the Bernoulli numbers, one gets uniqueness by multiplying the second column with  $-1$ .)
- (iii) For any  $n$ -th root of unity  $\zeta$ , one can easily construct an analogous function to  $f$ , which is fixed by  $D_\zeta P$ , but we don't have an application for these coefficients, especially they don't agree with the 'generalized Bernoulli numbers', which appear in the theory of 'Dirichlets  $L$ -functions'.

#### 1.4. The $q$ -Pascal matrix and Gaussian polynomials.

For the rest of this chapter we denote by  $q$  be an indeterminate and we set  $R := \mathbb{Z}[q]$ . Then consider the ring  $A$  generated by  $X$  and  $Y$  with the single relation  $YX = qXY$ , hence  $A$  is free as an  $R$ -module with basis  $\{X^i Y^j\}$ .

**Definition 1.12.** Let  $i, j \in \mathbb{N}$ .

- (i) The Gaussian polynomials  $\begin{bmatrix} i \\ j \end{bmatrix}$  are the following coefficients in  $R$ :

$$(X + Y)^i = \sum_{0 \leq j \leq i} \begin{bmatrix} i \\ j \end{bmatrix} X^j Y^{i-j} \text{ and } \begin{bmatrix} i \\ j \end{bmatrix} = 0 \text{ for } i < j.$$

- (ii)  $\begin{bmatrix} i \\ j \end{bmatrix}_s$  denotes the evaluation of  $\begin{bmatrix} i \\ j \end{bmatrix}$  at  $s$ .

This definition can be found in [PaWa], where is also a proof for the coincidence with the classical definition, which we give in the next lemma. Especially the Gaussian polynomials can be defined analogous to the binomial coefficients by

**Lemma 1.13.** For  $j \leq i \in \mathbb{N}$  let  $[i] := (q^i - 1)/(q - 1)$ , and  $[i]! := \prod_{1 \leq j \leq i} [j]$ . Then the following equation holds:

$$\begin{bmatrix} i \\ j \end{bmatrix} = \frac{[i]!}{[j]![i-j]!}.$$

Now we state some well known results on Gaussian polynomials ([Ja],[PaWa]).

**Proposition 1.14.** Let  $i < j$ . The Gaussian polynomial  $\begin{bmatrix} i \\ j \end{bmatrix}$  is of degree  $j(i-j)$  and satisfies the following relations:

$$(i) \begin{bmatrix} i \\ 0 \end{bmatrix} = 1, \quad (ii) \begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} i-j \\ i-j \end{bmatrix}, \quad (iii) \begin{bmatrix} i \\ j \end{bmatrix}_1 = \binom{i}{j},$$

$$(iv) \begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} i-1 \\ j-1 \end{bmatrix} + q^j \begin{bmatrix} i-1 \\ j \end{bmatrix}, \quad (v) \begin{bmatrix} i \\ j \end{bmatrix} = q^{i-j} \begin{bmatrix} i-1 \\ j-1 \end{bmatrix} + \begin{bmatrix} i-1 \\ j \end{bmatrix}.$$

Applying these results and using induction on  $i$  one proves the following [KüWe]:

**Lemma 1.15.**

$$\begin{bmatrix} i \\ j \end{bmatrix}_{q^{-1}} = q^{-j(i-j)} \begin{bmatrix} i \\ j \end{bmatrix}.$$

*Proof:*  $\begin{bmatrix} i \\ j \end{bmatrix}_{q^{-1}} = \begin{bmatrix} i-1 \\ j-1 \end{bmatrix}_{q^{-1}} + q^{-j} \begin{bmatrix} i-1 \\ j \end{bmatrix}_{q^{-1}} = q^{-j(i-j)} (q^{i-j} \begin{bmatrix} i-1 \\ j-1 \end{bmatrix} + \begin{bmatrix} i-1 \\ j \end{bmatrix}) = q^{-j(i-j)} \begin{bmatrix} i \\ j \end{bmatrix}.$  □

To give a  $q$ -analogous of the binomial theorem, where a slightly different version can be found in [Ja],[KüWe], we need:

**Definition 1.16.** Let  $a$  be an element from the  $R$ -order  $A$ , which is defined above. Then for  $i \in \mathbb{N}$  we set

$$(a; q)_0 := 1 \text{ and } (a; q)_i := (a; q)_{i-1} \cdot (a - q^{i-1}).$$

**Theorem 1.17.** The following equation holds:

$$(X; q)_i = \sum_{0 \leq j \leq i} (-1)^{i-j} q^{\binom{i-j}{2}} \begin{bmatrix} i \\ j \end{bmatrix} X^j.$$

*Proof:* The proof is done by induction, where the case  $i = 0$  is trivial.

Then one multiplies the equation given by  $(X; q)_{i-1}$  with  $(X - q^{i-1})$  and get

$$\begin{aligned} & (-1)^{i-j} q^{\binom{i-j}{2}} \begin{bmatrix} i-1 \\ j-1 \end{bmatrix} - q^{i-1} (-1)^{i-1-j} q^{\binom{i-1-j}{2}} \begin{bmatrix} i-1 \\ j \end{bmatrix} = \\ & (-1)^{i-j} q^{\binom{i-j}{2}} \left( \begin{bmatrix} i-1 \\ j-1 \end{bmatrix} + q^j \begin{bmatrix} i-1 \\ j \end{bmatrix} \right). \end{aligned}$$

Now we are done with Proposition 1.14 (iv). □

**Definition 1.18.** The  $q$ -Pascal matrix  $G$  is defined via the Gaussian polynomials

$$(G)_{i+1, j+1} := \begin{bmatrix} i \\ j \end{bmatrix}.$$

**Example 1.19.**

$$(G)_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1+q & 1 & 0 & 0 \\ 1 & 1+q+q^2 & 1+q+q^2 & 1 & 0 \\ 1 & 1+q+q^2+q^3 & 1+q+2q^2+q^3+q^4 & 1+q+q^2+q^3 & 1 \end{pmatrix}.$$

**Remark 1.20.** The  $q$ -Pascal matrix  $G$  specialize to the Pascal matrix  $P$  by the evaluation at  $q = 1$ :

$$G_1 = P.$$

The inverse of  $G$  is given in [KüWe]. We give a different proof, which can be considered as generalisation of Heinrich Weber's proof of the Lemma 1.2.

**Proposition 1.21.**

$$(G^{-1})_{i+1,j+1} = (-1)^{i-j} q^{\binom{i-j}{2}} \begin{bmatrix} i \\ j \end{bmatrix}.$$

*Proof:* Consider the following sequence of  $R$ -linear maps:

$$\begin{array}{ccccccc} R[X] & \xrightarrow{\alpha} & A & \xrightarrow{\beta} & A & \xrightarrow{\gamma} & R[X] \\ X^i & \longmapsto & X^i & & & & \\ & & X^i Y^j & \longmapsto & (X+Y)^i Y^j & & \\ & & & & X^i Y^j & \longmapsto & X^i. \end{array}$$

By Definitions 1.12 and 1.18 the linear map  $\phi := \alpha \cdot \beta \cdot \gamma$  corresponds with respect to the basis  $\{X^i | i \geq 0\}$  to the  $q$ -Pascal matrix  $G$ . Using Theorem 1.17 it remains to show that  $\phi$  is inverse to

$$\psi : \begin{array}{ccc} R[X] & \longrightarrow & R[X] \\ X^i & \longrightarrow & (X; q)_i \end{array}.$$

Obviously one has  $(X^i)\psi \cdot \alpha \cdot \beta = (X+Y; q)_i$ , so we are done with part (I) of the following statements:

$$\forall i \in \mathbb{N} : \quad (I) : ((X+Y; q)_i)\gamma = X^i, \quad (II) : ((X+qY; q)_i)\gamma = X^i + (q^i - 1)X^{i-1},$$

which we show by a parallel induction:

The statements (I) and (II) are trivial for  $i = 0$ .

(I) :

$$\begin{aligned} ((X+Y; q)_{i+1})\gamma &= ((X+Y; q)_i \cdot (X+Y-q^i))\gamma \\ &= ((X+Y; q)_i \cdot X)\gamma + ((X+Y; q)_i \cdot (Y-q^i))\gamma \\ &= (X \cdot (X+qY; q)_i)\gamma + ((X+Y; q)_i \cdot (Y-q^i))\gamma \\ (II), (I) &= X \cdot (X^i + (q^i - 1)X^{i-1}) + X^i \cdot (1 - q^i) \\ &= X^{i+1}. \end{aligned}$$

(II) :

$$\begin{aligned} ((X+qY; q)_{i+1})\gamma &= ((X+qY-1) \cdot (X+qY-q) \cdots (X+qY-q^i))\gamma \\ &= ((X+qY-1) \cdot q^i \cdot (X/q+Y; q)_i)\gamma \\ &= (q^i \cdot (X-1) \cdot (X/q+Y; q)_i)\gamma + (q^i \cdot qY \cdot (X/q+Y; q)_i)\gamma \\ &= (q^i \cdot (X-1) \cdot (X/q+Y; q)_i)\gamma + (q^{i+1} \cdot (X+Y; q)_i \cdot Y)\gamma \\ (*), (I) &= q^i \cdot (X-1) \cdot (X/q)^i + q^{i+1} \cdot X^i \\ &= X^{i+1} - X^i + q^{i+1} X^i. \end{aligned}$$

ad (\*): This follows also by (I) and the  $R$ -linear substitution  $X \rightarrow X/q$ .  $\square$

### 1.5. Conjugation with the Pascal matrix.

Recall Definition 1.1 for  $P$  and  $D_q$ . We introduce further:

- Definition 1.22.** (i)  $(D_q^-)_{i+1,j+1} := \delta_{i,j+1}q^i$ .  
(ii)  $(D_q^+)_{i+1,j+1} := \delta_{i+1,j}q^i$ .  
(iii) With the convention that  $(\widehat{H})_{i,0} := 0$  we define recursively

$$(\widehat{H})_{i,j} := \begin{cases} \delta_{i,j} & \text{for } i \leq j, \\ (1-q)(\widehat{H})_{i-1,j} + q(\widehat{H})_{i-1,j-1} & \text{for } i > j. \end{cases}$$

**Example 1.23.**

$$D_1^+ = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ \vdots & \ddots & \ddots & \ddots & \ddots \end{pmatrix}, \quad D_1^- - D_q^- = \begin{pmatrix} 0 & 0 & 0 & \cdots \\ 1-q & 0 & 0 & \cdots \\ 0 & 1-q^2 & 0 & \cdots \\ \vdots & \ddots & \ddots & \ddots \end{pmatrix},$$

$$(\widehat{H})_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1-q & 1 & 0 & 0 \\ (1-q)^2 & 1-q^2 & 1 & 0 \\ (1-q)^3 & (1-q)^2(1+2q) & 1-q^3 & 1 \end{pmatrix}.$$

Then by conjugation with the involution  $\widehat{P}$ , see Lemma 1.2, we get

- Proposition 1.24.** (i)  $(\widehat{P}D_q\widehat{P})_{i+1,j+1} = \binom{i}{j}q^j(1-q)^{i-j}$ .  
(ii)  $\widehat{P}D_1^+\widehat{P} = Id - D_1^+$ .  
(iii)  $\widehat{P}(D_1^- - D_q^-)\widehat{P} = Id - \widehat{H}$ .  
(iv)  $\widehat{P}(Id + D_q^- - D_1^-)\widehat{P} = \widehat{H}$ .

*Proof:* We are working with the polynomial ring  $R[X]$ . As in Lemma 1.2  $\widehat{P}$  describes the basis transformation from  $\{X^i \mid i \geq 0\}$  to  $\{(1-X)^i \mid i \geq 0\}$ .

(i) Since  $D_q$  corresponds to the substitution

$$\phi_q : X^i \xrightarrow{D_q} q^i X^i,$$

we have

$$X^i \xrightarrow{\widehat{P}} (1-X)^i \xrightarrow{D_q} (1-qX)^i \xrightarrow{\widehat{P}} (1-q(1-X))^i = ((1-q)+qX)^i$$

and  $(\widehat{P}D_q\widehat{P})_{i+1,j+1}$  is the coefficient of  $X^j$  in  $((1-q)+qX)^i$ .

(ii)  $D_1^+$  corresponds to multiplication by  $X$ , so this statement follows from

$$X^i \xrightarrow{\widehat{P}} (1-X)^i \xrightarrow{D_1^+} X(1-X)^i \xrightarrow{\widehat{P}} (1-X)X^i.$$

(iii) and (iv) are equivalent, thus we only have to show (iv).

With respect to the basis  $\{X^i \mid i \geq 0\}$  the matrix  $Id + D_q^- - D_1^-$  corresponds to

linear map defined by

$$\psi_q : X^i \longrightarrow X^i + (q^i - 1)X^{i-1}.$$

Now we have to show, that for  $i \geq 0$

$$\psi_q((1-X)^i) = \sum_{0 \leq j \leq i} (\widehat{H})_{i+1, j+1} (1-X)^j.$$

By the recursive definition of  $\widehat{H}$  one has to show that:

$$(*) \psi_q((1-X)^i) = (1-q)\psi_q((1-X)^{i-1}) + q\psi_q((1-X)^{i-1})(1-X) + (1-q)(1-X)^i,$$

where the last summand appears since we have to correct the coefficient of  $(1-X)^i$ , because we get by definition

$$(\widehat{H})_{i+1, i+1} = 1 \text{ and not } q \cdot (\widehat{H})_{i, i} = q.$$

The formula (\*) is proved by induction. It is obviously true for  $i = 0$ . Because of

$$(1-X)^i = (1-q)(1-X)^{i-1} + q(1-X)^{i-1} - X(1-X)^{i-1},$$

and the  $R$ -linearity of  $\psi_q$  we get

$$\psi_q((1-X)^i) = (1-q)\psi_q((1-X)^{i-1}) + q\psi_q((1-X)^{i-1}) - \psi_q(X(1-X)^{i-1}).$$

Hence to prove (\*) it remains to show that

$$\Sigma_i := \psi_q(X(1-X)^{i-1}) - qX\psi_q((1-X)^{i-1}) = (q-1)(1-X)^i.$$

By using the definition of  $\psi_q$  one calculates

$$\begin{aligned} \psi_q(X(1-X)^{i-1}) &= \sum_{0 \leq j < i} (-1)^j \binom{i-1}{j} (X^{j+1} + (q^{j+1} - 1)X^j) \\ &= X(1-X)^{i-1} + (q^{j+1} - 1)(1-X)^{i-1}, \\ qX\psi_q((1-X)^{i-1}) &= q \sum_{0 \leq j < i} (-1)^j \binom{i-1}{j} (X^{j+1} + (q^j - 1)X^j) \\ &= qX(1-X)^{i-1} + (q^{j+1} - q)(1-X)^{i-1} \end{aligned}$$

and gets

$$\Sigma_i = (1-q)X(1-X)^{i-1} + (q-1)(1-X)^{i-1} = (q-1)(1-X)^i.$$

□

**Remark 1.25.** We have the coincidence

$$\psi_q(X^i) = ((X+qY; q)_i)\gamma,$$

where  $\psi_q$  is defined in (iv) of the last proof and  $((X+qY; q)_i)\gamma$  is given as statement (II) in the proof Proposition 1.21.

## 2. RECURSIVELY DEFINED TRIANGULAR MATRICES

Again we set  $R := \mathbb{Z}[q]$ .

## 2.1. Definitions and examples.

**Definition 2.1.** A recursively defined matrix  $M$  is a lower triangular matrix over  $R$ , which is determined by:

- (i) The starting condition  $\mathcal{SC}$ : Some entries  $(M)_{i,j}$  are chosen.
- (ii) The construction rule  $\mathcal{CR}$ :  $(M)_{i+1,j+1}$  is recursively defined as  $R$ -linear combination of  $(M)_{i,j}$  and  $(M)_{i,j+1}$ , with the convention  $(M)_{i,0} = 0$  for  $i \in \mathbb{N}$ .

**Remark 2.2.** This definition is compatible with the operations *evaluation* and *restriction* given in Definition 1.1.

Some of the matrices given in the last section can be defined recursively:

**Example 2.3.** (i) The Pascal matrix  $P$  is recursively defined by:

$$\begin{aligned}\mathcal{SC} : (P)_{1,1} &:= 1 \\ \mathcal{CR} : (P)_{i,j} &:= (P)_{i-1,j-1} + (P)_{i-1,j}.\end{aligned}$$

- (ii) From Proposition 1.14 one gets a recursive definition of the  $q$ -Pascal matrix  $G$ , using the relations (i) and (iv):

$$\begin{aligned}\mathcal{SC} : (G)_{1,1} &:= 1 \\ \mathcal{CR} : (G)_{i+1,j+1} &:= (G)_{i,j} + q^j (G)_{i,j+1},\end{aligned}$$

or also, using the relations (i) and (v):

$$\begin{aligned}\mathcal{SC} : (G)_{1,1} &:= 1 \\ \mathcal{CR} : (G)_{i+1,j+1} &:= q^{i-j} (G)_{i,j} + (G)_{i,j+1}.\end{aligned}$$

- (iii) One gets a recursive definition of the inverse  $q$ -Pascal matrix  $G^{-1}$  by:

$$\begin{aligned}\mathcal{SC} : (G^{-1})_{1,1} &:= 1, \\ \mathcal{CR} : (G^{-1})_{i+1,j+1} &:= (G^{-1})_{i,j} - q^{i-1} (G^{-1})_{i,j+1}.\end{aligned}$$

*Proof.* By Proposition 1.21, one has to involve the factor  $(-1)^{i-j} q^{\binom{i-j}{2}}$  into the  $q$ -Pascal matrix  $G$ , which we just have recursively defined in (ii): Using induction on  $i$  we can assume that

$$(G^{-1})_{i,j} = (-1)^{i-j} q^{\binom{i-j}{2}} \begin{bmatrix} i-1 \\ j-1 \end{bmatrix}$$

and

$$(G^{-1})_{i,j+1} = (-1)^{i-j-1} q^{\binom{i-j-1}{2}} \begin{bmatrix} i-1 \\ j \end{bmatrix}.$$

Then we get with

$$\begin{aligned} -q^{i-1}(G^{-1})_{i,j+1} &= (-1)^{i-j} q^{\binom{i-j-1}{2}} \cdot q^{i-j-1} q^j \begin{bmatrix} i-1 \\ j \end{bmatrix} \\ &= (-1)^{i-j} \cdot q^{\binom{i-j}{2}} \cdot q^j \begin{bmatrix} i-1 \\ j \end{bmatrix} \end{aligned}$$

and Proposition 1.14 (iv) that

$$\begin{aligned} (G^{-1})_{i,j} - q^{i-1}(G^{-1})_{i,j+1} &= (-1)^{i-j} q^{\binom{i-j}{2}} \left( \begin{bmatrix} i-1 \\ j-1 \end{bmatrix} + q^j \begin{bmatrix} i-1 \\ j \end{bmatrix} \right) \\ &= (-1)^{i-j} q^{\binom{i-j}{2}} \begin{bmatrix} i \\ j \end{bmatrix} \\ &= (G^{-1})_{i+1,j+1}. \end{aligned}$$

□

(iv) The matrix  $\widehat{H}$  given in the Definition 1.22 has been defined recursively.

**Definition 2.4.** Let  $\mathcal{R}$  be the ring of lower triangular matrices over  $R$  for a fixed size  $n$ ,  $n \in \mathbb{N} \cup \{\infty\}$ , and let  $M \in \mathcal{R}$ . Then  $\tau : \mathcal{R} \longrightarrow \mathcal{R}$  permutes the entries as follows:

$$\begin{array}{ccc} \tau : \mathcal{R} & \longrightarrow & \mathcal{R} \\ M & \longmapsto & M^\tau \end{array}$$

with  $(M^\tau)_{i,j} := (M)_{i,1+i-j}$  for  $i \geq j$ .

**Example 2.5.**

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 4 & 5 & 6 \end{pmatrix}^\tau = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 2 & 0 \\ 6 & 5 & 4 \end{pmatrix}.$$

**Remark 2.6.** (i) The definition of  $\tau$  may look somehow artificial, but it turns out, that  $\tau$  is useful for explicit calculations with recursively defined matrices.

(ii)  $\tau$  is an involution, because  $1-i-(1-i-j) = j$  and obviously an additive homomorphism on  $\mathcal{R}$ .

(iii) The symmetry of the Pascal triangle or more general of the Gaussian polynomials  $\begin{bmatrix} i \\ j \end{bmatrix}$ , see Proposition 1.14 (ii) shows that  $P$  and  $G$  are fixed by  $\tau$ . Since  $G^\tau = G$ ,  $\tau$  interchanges the two different recursive definitions for  $G$  given in Example 2.3.

## 2.2. Calculations.

**Definition 2.7.** Let  $H$  be the recursively defined matrix:

$$\begin{aligned} \mathcal{SC} : (H)_{i,i} &:= 1 \quad \forall i \in \mathbb{N}, \\ \mathcal{CR} : (H)_{i+1,j+1} &:= (H)_{i,j+1} + q(H)_{i,j} \quad \text{for } i > j. \end{aligned}$$

Then one easily proves:

**Proposition 2.8.** (i)  $\widehat{H} = D_{1-q} \cdot H \cdot D_{1-q}^{-1}$ .

(ii)  $\widehat{H}^\tau = H^\tau \cdot D_{1-q}$ .

(iii)  $H^\tau$  is recursively defined by:

$$\begin{aligned} \mathcal{SC} : (H^\tau)_{i,1} &:= 1 \quad \forall i \in \mathbb{N}, \\ \mathcal{CR} : (H^\tau)_{i+1,j+1} &:= q(H^\tau)_{i,j+1} + (H)_{i,j} \quad \text{for } i \geq j \geq 1. \end{aligned}$$

**Example 2.9.**

$$(H^\tau)_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1+q & 1 & 0 & 0 & 0 \\ 1 & 1+q+q^2 & 1+2q & 1 & 0 & 0 \\ 1 & 1+q+q^2+q^3 & 1+2q+3q^2 & 1+3q & 1 & 0 \\ 1 & 1+q+q^2+q^3+q^4 & 1+2q+3q^2+4q^3 & 1+3q+6q^2 & 1+4q & 1 \end{pmatrix}.$$

**Remark 2.10.** One easily sees, that the  $j+1$ -th column of  $H^\tau$  is given by the binomial coefficients  $\binom{i}{j}$ , but we don't need this further on.

**Definition 2.11.** (i) Let  $\pi_i := 1 - q^i$  and  $\widehat{K}$  be recursively defined by:

$$\begin{aligned} \mathcal{SC} : (\widehat{K})_{i,1} &:= 1 \quad \forall i \in \mathbb{N}, \\ \mathcal{CR} : (\widehat{K})_{i+1,j+1} &:= \pi_i (\widehat{K})_{i,j} \quad \text{for } i \geq j \geq 1. \end{aligned}$$

(ii) Let  $K$  be recursively defined by:

$$\begin{aligned} \mathcal{SC} : (K)_{i,1} &:= 1 \quad \forall i \in \mathbb{N}, \\ \mathcal{CR} : (K)_{i+1,j+1} &:= [i](K)_{i,j} \quad \text{for } i \geq j \geq 1, \end{aligned}$$

where  $[i]$  is defined in Lemma 1.13.

(iii) The factorial matrix  $F$  is defined as

$$(F)_{i+1,j+1} := \delta_{i,j} [i]!.$$

(We use the convention  $[0]! := 1$ .)

**Example 2.12.**

$$(\widehat{K})_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & \pi_1 & 0 & 0 & 0 \\ 1 & \pi_2 & \pi_1\pi_2 & 0 & 0 \\ 1 & \pi_3 & \pi_2\pi_3 & \pi_1\pi_2\pi_3 & 0 \\ 1 & \pi_4 & \pi_3\pi_4 & \pi_2\pi_3\pi_4 & \pi_1\pi_2\pi_3\pi_4 \end{pmatrix}.$$

**Remark 2.13.** Later on we need the solutions of the equations

$$\widehat{H}^\tau = \widehat{K} \cdot X \text{ and } PD_{1-q} = \widehat{K} \cdot Y.$$

In the rest of this chapter we will solve these equations. Therefore we give for  $\widehat{K}$  another recursive definition, which provides a decomposition as a product of certain diagonal matrices (which are 'easy to understand', especially it is no problem to invert these matrices), and the  $q$ -Pascal matrix  $G$ , for which the inverse  $G^{-1}$  is given as a recursively defined matrix in example 2.3.

It turns out that the matrices, which solve these two different equations have essentially the same shape.

**Proposition 2.14.** (i)  $\widehat{K}$  is recursively defined by:

$$\mathcal{SC} : (\widehat{K})_{1,1} := 1,$$

$$\mathcal{CR} : (\widehat{K})_{i+1,j+1} := q^j (\widehat{K})_{i,j+1} + \pi_j (\widehat{K})_{i,j} \quad \text{for } i \geq j \geq 0.$$

(ii)  $\widehat{K} = K \cdot D_{1-q}$ .

(iii)  $K$  is recursively defined by:

$$\mathcal{SC} : (K)_{1,1} := 1,$$

$$\mathcal{CR} : (K)_{i+1,j+1} := q^j (K)_{i,j+1} + [j](K)_{i,j} \quad \text{for } i \geq j \geq 0.$$

(iv)  $K = G \cdot F$ .

*Proof:* (i) The construction rule for  $j = 0$  clearly gives the desired result, we just have to consider the case  $j > 0$ .

Therefore we use induction on  $i$ :

The statement is trivial for the first row ( $i = 0$ ).

So assume that it is true for the first  $i$  rows, especially

$$(\widehat{K})_{i,j} = \pi_{i-j+1}\pi_{i-j+2}\dots\pi_{i-1} \text{ and } (\widehat{K})_{i,j+1} = \pi_{i-j}\pi_{i-j+1}\dots\pi_{i-1}.$$

Since  $(\widehat{K})_{i,j+1} = \pi_{i-j}(\widehat{K})_{i,j}$  and  $\pi_j + q^j\pi_{i-j} = \pi_i$  one gets

$$\pi_j(\widehat{K})_{i,j} + q^j(\widehat{K})_{i,j+1} = \pi_i \cdot \pi_{i-j+1}\dots\pi_{i-1} = (\widehat{K})_{i+1,j+1},$$

which is the statement for the  $i + 1$  row.

(ii) is obvious, since  $\pi_i = [i](1 - q)$ .

(iii) follows from (i) and (ii).

(iv) follows by comparing the recursive definition of  $K$  given in (iii) with the recursive definition of  $G$  given in Example 2.3 (ii).  $\square$

**Definition 2.15.** Let  $M$  be a matrix.

- (i) Then  $(M)_{i,*}$  denotes the  $i$ -th row and  $(M)_{*,j}$  denotes the  $j$ -th column of  $M$ .
- (ii)  $(M)_{*+1,*}$  is the matrix  $M$  with an additional row, consisting of zeros, on the top.  $(M)_{*,*+1}$  is the matrix  $M$  with an additional first column, consisting of zeros.
- (iii)  $(M)_{*+1,*+1}$  is the combination of the last two operations.
- (iv)  $(M)_{i,*+1}$  is the  $i$ -th row of  $(M)_{*,*+1}$  and  $(M)_{*+1,j}$  the  $j$ -th column of  $(M)_{*+1,*}$ .

**Remark 2.16.** For smoothness we set moreover  $M_{*,*} := M$ .

**Example 2.17.** There is the following equation for the Pascal matrix  $P$ , which follows from their recursive definition:

$$(P)_{*,*} = (\delta_{1,1})_{*,*} + (P)_{*+1,*} + (P)_{*+1,*+1}.$$

For example:

$$\begin{pmatrix} 1 & & & \\ 1 & 1 & & \\ 1 & 2 & 1 & \\ 1 & 3 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & & & \\ 0 & 0 & & \\ & & & \\ & & & \end{pmatrix} + \begin{pmatrix} 0 & & & \\ 1 & & & \\ 1 & 1 & & \\ 1 & 2 & 1 & \end{pmatrix} + \begin{pmatrix} 0 & & & \\ \vdots & 1 & & \\ & 1 & 1 & \\ & 1 & 2 & 1 \end{pmatrix}.$$

**Proposition 2.18.** (i) The equation  $PD_{1-q} = \hat{K} \cdot Y$  is solved by  $F^{-1}\bar{L}$ , with  $\bar{L}$  recursively defined by:

$$\mathcal{SC} : (\bar{L})_{1,1} := 1,$$

$$\mathcal{CR} : (\bar{L})_{i+1,j+1} := [i - 1](\bar{L})_{i,j+1} + (\bar{L})_{i,j} \quad \text{for } i \geq j, i \geq 1, j \geq 0.$$

(ii)  $G^{-1}P = \hat{L}$ , with  $\hat{L}$  recursively defined by:

$$\mathcal{SC} : (\hat{L})_{1,1} := 1,$$

$$\mathcal{CR} : (\hat{L})_{i+1,j+1} := (1 - q^{i-1})(\hat{L})_{i,j+1} + (\hat{L})_{i,j} \quad \text{for } i \geq j \geq 0.$$

*Proof.* (i) From Proposition 2.14 (ii) and (iv) we get  $\widehat{K} = GFD_{1-q}$  and hence

$$Y = D_{1-q}^{-1}F^{-1}G^{-1}PD_{1-q}.$$

Since the diagonal matrices  $D_{1-q}^{-1}$  and  $F^{-1}$  commute, we are done with  $G^{-1}P = \widehat{L}$ , which we will show in (ii), and with

$$(1 - q^{i-1}) = (1 - q)[i-1],$$

which shows that

$$D_{1-q}^{-1}\widehat{L}D_{1-q} = \bar{L}.$$

(ii) The proof is done by induction on the row index, the starting condition  $\mathcal{SC}$  being satisfied. From Example 2.3 (iii) one gets:

$$(G^{-1})_{i+1,*} = -q^{i-1}(G^{-1})_{i,*} + (G^{-1})_{i,*+1}.$$

Inductively we can assume that:

$$-q^{i-1}(G^{-1})_{i,*}P_{*,*} = -q^{i-1}(\bar{L})_{i,*}.$$

Using Example 2.17, we obtain

$$\begin{aligned} (G^{-1})_{i,*+1}P_{*,*} &= (G^{-1})_{i,*+1}(P)_{*,*+1,*} + (G^{-1})_{i,*+1}(P)_{*,*+1,*+1} \\ &= (G^{-1})_{i,*}P_{*,*} + (G^{-1})_{i,*}(P)_{*,*+1} \\ &= (\widehat{L})_{i,*} + (\widehat{L})_{i,*+1}, \end{aligned}$$

and we conclude that

$$(G^{-1})_{i+1,*}P_{*,*} = -q^{i-1}(\bar{L})_{i,*} + (\widehat{L})_{i,*} + (\widehat{L})_{i,*+1} = (\widehat{L})_{i+1,*}.$$

□

**Remark 2.19.** The matrix  $\bar{L}$  is invertible since it is of triangular shape with entries 1 on the diagonal. Hence Proposition 2.18 (i) shows that

$$PD_{1-q}\bar{L}^{-1}F = \widehat{K}.$$

**Proposition 2.20.** (i)  $G^{-1}H^\tau = \widetilde{L}$  with

$$\widetilde{L} := \begin{pmatrix} 1 & 0 & \dots \\ 0 & \widetilde{L} & \\ \vdots & & \end{pmatrix},$$

where  $\widetilde{L}$  is recursively defined by:

$$\mathcal{SC} : (\widetilde{L})_{1,1} := 1,$$

$$\mathcal{CR} : (\widetilde{L})_{i+1,j+1} := (q - q^i)(\widetilde{L})_{i,j+1} + (\widetilde{L})_{i,j} \quad \text{for } i \geq j \geq 0, i \geq 1.$$

(ii)  $\tilde{L} = D_q D_{1-q} \bar{L} D_{1-q}^{-1} D_q^{-1}$  where  $\bar{L}$  is recursively defined in Proposition 2.18.

(iii) Let

$$\bar{L} := \begin{pmatrix} 1 & 0 & \dots \\ 0 & \bar{L} & \\ \vdots & & \end{pmatrix}.$$

$$\text{Then } \tilde{L} = D_q D_{1-q} \bar{L} D_{1-q}^{-1} D_q^{-1}.$$

*Proof.* (i) With Definition 1.18, Proposition 1.14 and Proposition 2.8 (iii) we get for  $i \in \mathbb{N}$ :

$$(G)_{i+1,1} = \begin{bmatrix} i \\ 0 \end{bmatrix} = 1 = (H^\tau)_{i+1,0},$$

$$(G)_{i+1,2} = \begin{bmatrix} i \\ 1 \end{bmatrix} = [i] = (H^\tau)_{i+1,2},$$

where the last equation follows from  $1 + q[i-1] = [i]$  and the construction rule  $\mathcal{CR}$  in the definition of  $H^\tau$ .

Hence the first two columns of  $H^\tau$  and  $G$  coincide and we verify the statement for the first column of the matrices by showing that

$$(\tilde{L})_{i,1} = \delta_{i,1}.$$

The construction rule  $\mathcal{CR}$  for  $\tilde{L}$  shows, that  $(\tilde{L})_{1,1} = \delta_{1,1}$  and

$$(\tilde{L})_{i+1,1} = (q - q^i)(\tilde{L})_{i,1}.$$

Hence we have  $(\tilde{L})_{2,1} = 0$ , which yields to  $(\tilde{L})_{i,1} = 0$  for  $i > 1$ .

So it remains to prove the construction rule  $\mathcal{CR}$  of  $\tilde{L}$  at the position  $(\tilde{L})_{i+1,j+1}$  for  $j \geq 1$ .

By the recursive definitions of  $G^{-1}$  and  $H^\tau$  given in Example 2.3 (iii) and in Proposition 2.8 one gets for  $j \geq 1$ :

$$(G^{-1})_{i+1,*} = (G^{-1})_{i,*+1} - q^{i-1} \cdot (G^{-1})_{i,*}$$

$$(H^\tau)_{*,j+1} = (H^\tau)_{*+1,j} + q \cdot (H^\tau)_{*+1,j+1}.$$

Writing

$$(I) : (G^{-1} H^\tau)_{i+1,j+1} = (G^{-1})_{i,*+1} (H^\tau)_{*+1,j}$$

$$(II) : \quad \quad \quad + q (G^{-1})_{i,*+1} (H^\tau)_{*+1,j+1}$$

$$(III) : \quad \quad \quad - q^{i-1} (G^{-1})_{i,*} (H^\tau)_{*,j+1},$$

the proof is finished inductively by noting:

$$\begin{aligned}
(I) : & \quad (G^{-1})_{i,*+1}(H^\tau)_{*+1,j} = (G^{-1})_{i,*}(H^\tau)_{*,j} = (\tilde{L})_{i-1,j-1} \\
(II) : & \quad q(G^{-1})_{i,*+1}(H^\tau)_{*+1,j+1} = q(G^{-1})_{i,*}(H^\tau)_{*,j+1} = q(\tilde{L})_{i-1,j} \\
(III) : & \quad -q^{i-1}(G^{-1})_{i,*}(H^\tau)_{*,j+1} = -q^{i-1}(\tilde{L})_{i-1,j},
\end{aligned}$$

which verifies the construction rule  $\mathcal{CR}$ .

(ii) follows from  $q - q^i = q(1 - q)[i - 1]$ .

(iii) follows from (ii).  $\square$

**Example 2.21.**

$$(\bar{L})_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1+q & 2+q & 1 & 0 \\ 0 & 1+2q+2q^2+q^3 & 3+4q+3q^2+q^3 & 3+2q+q^2 & 1 \end{pmatrix}.$$

By the recursive definition of  $\tilde{L}$  one easily sees, that the  $i+1$ -th row of  $L$  is given by the coefficients of  $\prod_{j=0}^i (X + [j])$ .

**Proposition 2.22.** The equation  $\hat{H}^\tau = \hat{K} \cdot X$  is solved by

$$X = F^{-1} D_q \bar{L} D_q^{-1}.$$

*Proof.* This follows from the equations  $\hat{H}^\tau = H^\tau D_{1-q}$  and  $\hat{K} = G F D_{1-q}$  of the Propositions 2.8 and 2.14 and Proposition 2.20.  $\square$

### 2.3. Applications to number theory.

The technique of recursively defined matrices was introduced to get matrices, which enable us to describe the integral group rings for some  $p$ -groups. One can also use this technique to obtain results in number theory:

Some simple linear algebra applied to the matrix  $(\hat{K}_\zeta)_n$  (see Definition 1.1, Proposition 2.11 and Example 2.12) leads to a generalization of a well known number theoretical result.

**Lemma 2.23.** Let  $n \in \mathbb{N}$  and  $\zeta$  a primitive  $n$ -th root of unity. Then the vector  $v := (1, \dots, 1)$  is an eigenvector corresponding to the eigenvalue  $n$  for the matrix  $(\hat{K}_\zeta)_n$ .

*Proof.* We prove this by induction on the columns of  $(\hat{K}_\zeta)_n$ , using the notation

$$\Sigma_i := (1 - \zeta) \cdots (1 - \zeta^i) + (1 - \zeta^2) \cdots (1 - \zeta^{i+1}) + \dots + (1 - \zeta^{n-i}) \cdots (1 - \zeta^{n-1})$$

for the sum of the entries of the  $(i+1)$ -th column of  $(\hat{K}_\zeta)_n$ . Obviously  $\Sigma_0 = n$ . Let  $i \geq 1$  and assume  $\Sigma_{i-1} = n$ . The recursive definition of  $\hat{K}$  in Proposition 2.14

(i) provides the equation

$$\begin{aligned}\Sigma_i &= (1 - \zeta^i)(\Sigma_{i-1} - (1 - \zeta^{n-i+1})\dots(1 - \zeta^{n-1})) \\ &\quad + \zeta^i(\Sigma_i - (1 - \zeta^{n-i})\dots(1 - \zeta^{n-1})).\end{aligned}$$

Setting  $\Delta_i := (1 - \zeta^{n-i+1})\dots(1 - \zeta^{n-1})$  one gets

$$(1 - \zeta^i)\Sigma_i = (1 - \zeta^i)\Sigma_{i-1} - (1 - \zeta^i)\Delta_i - \zeta^i(1 - \zeta^{n-i})\Delta_i.$$

Then  $(1 - \zeta^i) = -\zeta^i(1 - \zeta^{n-i})$  implies  $\Sigma_i = \Sigma_{i-1} = n$ .  $\square$

We reformulate this lemma as

**Corollary 2.24.** Let  $n \in \mathbb{N}$  and  $\zeta$  a primitive  $n$ -th root of unity. Then for  $1 \leq i \leq n - 1$  the equation

$$\sum_{k=0}^{n-i-1} (1 - \zeta^{1+k})\dots(1 - \zeta^{i+k}) = n$$

holds.

**Remark 2.25.** If  $n = p$  is a prime, then the equations for  $i = 1$  and  $i = p - 1$  show that the trace and the norm of  $1 - \zeta$  is equal to  $p$ . One easily sees that for  $k \notin \{1, p - 1\}$  the summands in the above sum are not permuted under Galois-automorphisms, as it happens in the well known cases of the trace and of the norm. Hence we are getting new equations. We illustrate this with the following example:

Let  $\zeta$  be a 5-th root of unity. Then we get from the third column of  $(\widehat{K}_\zeta)_5$  that

$$(1 - \zeta)(1 - \zeta^2) + (1 - \zeta^2)(1 - \zeta^3) + (1 - \zeta^3)(1 - \zeta^4) = 5.$$

Now applying the Galois-automorphism  $\zeta \mapsto \zeta^2$  provides the new equation

$$(1 - \zeta^2)(1 - \zeta^4) + (1 - \zeta^4)(1 - \zeta) + (1 - \zeta)(1 - \zeta^3) = 5.$$

As a second application we will show, that the matrix  $L$  given in Proposition 2.20, yields a criteria to decide whether a prime is regular or irregular.

First we state some well known facts about regularity of primes and Bernoulli numbers. As reference for the rest of this section we refer to [IrRo] Chapter 15.

- Jakob Bernoulli introduced the numbers  $B_n$ , now called Bernoulli numbers (see Remark 1.11), to solve the following problem:

The sum  $S_m(n) := 1^m + \dots + (n - 1)^m$  can be expressed in the following way:

$$(m + 1)S_m(n) = \sum_{i=0}^m \binom{m+1}{i} B_i n^{m+1-i}.$$

Since the Bernoulli polynomials  $B_m(x) := \sum_{i=0}^m \binom{m}{i} B_i x^{m-i}$  fulfill the equation  $\frac{d}{dx} B_m(x) = m B_{m-1}(x)$  one can reformulate Bernoulli's result as

$$S_m(n) = \int_0^n B_m(x) dx = \frac{1}{m+1} (B_{m+1}(n) - B_{m+1}).$$

- Since the Bernoulli numbers are the coefficients of  $\frac{t}{e^t-1}$  developed in a power series at the origin, one easily concludes that  $B_{2n+1} = 0$  for  $n > 0$ .
- By definition a prime  $p$  is regular, if and only if the class number  $h_p$  is not divisible by  $p$ . Kummer proved, that  $p$  is regular if and only if  $p$  does not divide any of the numerators of the Bernoulli numbers  $B_2, B_4, \dots, B_{p-3}$ .

By Example 2.21 the coefficients  $a_i$  of the factorial polynomial

$$F_m(X) := \prod_{i=0}^{m-1} (X+i) = \sum_{i=0}^m a_i X^i$$

are given by the entries of the  $(m+1)$ -th row of  $L_1$ . Especially one has

$$a_0 = 0, a_1 = (m-1)!, a_{m-1} = \binom{m}{2}, a_m = 1.$$

**Theorem 2.26.** Let  $p$  be an odd prime. Then the coefficients  $a_i$  of the factorial polynomial  $F_p(X)$  satisfy:

$$a_2 \equiv a_4 \equiv \dots \equiv a_{p-3} \equiv 0 \pmod{p^2}, \quad a_3 \equiv a_5 \equiv \dots \equiv a_{p-2} \equiv 0 \pmod{p}.$$

The prime  $p$  is irregular if and only if there is an  $i \in \{3, 5, \dots, p-2\}$  with

$$a_i \equiv 0 \pmod{p^2}.$$

*Proof.* We consider the evaluation of  $F_p(X) \pmod{p^2}$ .

Since  $1 \leq n \leq p^2$  is uniquely determined by  $n = n' + n'' \cdot p$  with  $n' \in \{1, \dots, p\}$  and  $n'' \in \{0, \dots, p-1\}$ , we can show that:

- (i)  $F_p(n) \equiv -p \cdot (n'' + 1) \pmod{p^2}$ ,
- (ii)  $pS_{p-1}(n) \equiv p \cdot (n' - 1 - n'') \pmod{p^2}$ .

(i) follows since  $p \cdot (n'' + 1)$  is the only factor of  $n \cdot \dots \cdot (n + p - 1)$  divisible by  $p$  and since the rest is congruent  $-1 \pmod{p}$ , by Wilson's theorem.

(ii) follows since we get with  $z^{p-1} \equiv 1 \pmod{p}$  for  $(p, z) = 1$  that

$$pS_{p-1}(n) \equiv p \cdot (n' - 1 + (p-1)n'') \equiv p \cdot (n' - 1 - n'') \pmod{p^2}.$$

The discussion above shows that  $pS_{p-1}(n) = B_p(n)$  for  $n \in \mathbb{N}$ . So we get for  $1 \leq n \leq p^2$  that  $F_p(n) + p \cdot n \equiv B_p(n)$  and hence

$$F_p(X) \equiv B_p(X) - pX \pmod{p^2}.$$

and comparing coefficients gives for  $2 < i \leq p$ :

$$a_{p-i} \equiv \binom{p}{i} B_i \pmod{p^2}.$$

Then the result follows from the theorem of Kummer.  $\square$

**Remark 2.27.** So one can use the matrix  $L_q$ , to decide whether the prime  $p$  divides the class group of  $\mathbb{Z}[\zeta_p]$ , by evaluating the matrix  $L_q$  at  $q = 1$  and considering the entries in the  $(p+1)$ -th row  $p$ -adically.

Now one can ask if it is possible to get informations on the regularity of a prime  $p$  by evaluating the matrix  $L_q$  at  $q = \zeta_p$ . It turns out, that the  $p$ -adic structure of the coefficients is independent of the regularity of  $p$ . Using the notation  $[j]_\zeta$  for the evaluation of  $[j]$  at  $q = \zeta_p$  and  $u$  for the product of cyclotomic units  $u := \prod_{j=1}^{p-1} [j]_\zeta$  one gets:

$$\prod_{j=0}^{p-1} (X + [j]_\zeta) = X^p + u \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} \frac{1}{1-\zeta} ((1-\zeta)X)^i.$$

(This is proved by setting  $X = -[j]_\zeta$  and inspection of the minimal polynomial of  $\zeta^j - 1$ .)

### 3. INTEGRAL GROUP RINGS AND TWISTED GROUP RINGS

#### 3.1. The Abelian case.

The integral group rings  $\mathbb{Z}C_{p^n}$  of cyclic groups prime power order  $p^n$  are important in integral representation theory. For example there is an analogue of the main theorem on finitely generated Abelian groups. Especially if

$$G \simeq C_{p_1^{n_1}} \times \dots \times C_{p_i^{n_i}}$$

then one has the isomorphism of rings

$$\mathbb{Z}G \simeq \mathbb{Z}C_{p_1^{n_1}} \otimes_{\mathbb{Z}} \dots \otimes_{\mathbb{Z}} \mathbb{Z}C_{p_i^{n_i}}.$$

**Remark 3.1.** (i) There is the well known inductive description of these integral group rings by pullbacks:

$$(*) \quad \begin{array}{ccc} \mathbb{Z}C_{p^{n+1}} & \xrightarrow{\alpha'} & \mathbb{Z}C_{p^n} \\ \beta' \downarrow & & \downarrow \gamma' \\ \mathbb{Z}[\zeta_{p^{n+1}}] & \xrightarrow{\delta'} & \mathbb{F}_p C_{p^n}, \end{array}$$

with  $C_{p^{n+1}} := \langle a \rangle$ ,  $C_{p^n} := \langle \bar{a} \rangle$ ,  $\alpha'(a) = \bar{a}$ ,  $\beta'(a) = \zeta_{p^{n+1}}$ ,  $\gamma'$  and  $\delta'$  are the factor maps mod  $1 - \zeta_p$  and mod  $p$ .

This description follows from Lemma 1.9 with the rational idempotent

$$e := (1 + a^{p^n} + a^{2p^n} + \dots + a^{(p-1)p^n})/p.$$

(ii) Of course one cannot expect to understand  $\mathbb{Z}C_{p^n}$  ‘better’ than the projections  $\mathbb{Z}[\zeta_{p^i}]$ . Specifically since there is no canonical description of the unit group of  $\mathbb{Z}[\zeta_{p^n}]$  one cannot expect to get a canonical description of the unit groups of these integral group rings.

#### 3.2. The general case.

Let  $C_{p^{n+1}} = \langle a \rangle$ ,  $H$  a subgroup of the automorphism group  $\text{Aut}(C_{p^{n+1}})$  and  $G$  be the corresponding semi direct product:  $G \simeq C_{p^{n+1}} \rtimes H$ . Since the subgroups of  $C_{p^{n+1}}$  are characteristic, the pullback above induces a description of  $\mathbb{Z}G$  as pullback. We set  $\bar{G} := G/\langle a^{p^n} \rangle$ .

$$\begin{array}{ccc} \mathbb{Z}G & \xrightarrow{\alpha} & \mathbb{Z}\bar{G} \\ \beta \downarrow & & \downarrow \gamma \\ \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H & \xrightarrow{\delta} & \mathbb{F}_p \bar{G}. \end{array}$$

Since  $\text{Aut}(C_{p^{n+1}}) \simeq \text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}}), \mathbb{Q}) \simeq (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$  one can consider  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$  as  $R$ -order, when  $R := \mathbb{Z}[\zeta_{p^{n+1}}]^H$ , the fixed ring of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  under  $H$ .

**Lemma 3.2.** Using the notation from above, one gets:

- (i)  $R$  is a Dedekind ring with prime element  $\pi \in R$ , where  $p$  is totally ramified over  $\pi$ .
- (ii) An  $R$ -basis of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  is given by  $\mathfrak{B} := \{1, 1 - \zeta_{p^{n+1}}, \dots, (1 - \zeta_{p^{n+1}})^{|H|-1}\}$ .
- (iii)  $R = \mathbb{Z}[\pi]$ .

*Proof.* First we state some well known facts (see [Wa]):

- $\mathbb{Z}[\zeta_{p^{n+1}}]$  is the integral closure of  $\mathbb{Z}$  in  $\mathbb{Q}(\zeta_{p^{n+1}})$ .
- A  $\mathbb{Z}$ -basis of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  is given by  $\mathfrak{B}' := \{1, \zeta_{p^{n+1}}, \dots, \zeta_{p^{n+1}}^{\phi(p^{n+1})-1}\}$ , where  $\phi$  is the Euler  $\phi$ -function.

(i) Let  $S$  be the integral closure of  $\mathbb{Z}$  in  $K := \mathbb{Q}(\zeta_{p^{n+1}})^H$ .

Obviously  $R \subseteq S$ . Conversely  $S \subseteq \mathbb{Z}[\zeta_{p^{n+1}}] \cap K = R$  so  $S = R$ .

We denote by  $\mathfrak{P} := (1 - \zeta_{p^{n+1}})$  the unique prime ideal of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  over  $p$ , with corresponding valuation  $\nu_{\mathfrak{P}}$ , and set  $\pi := Nr_{\mathbb{Q}(\zeta_{p^{n+1}}), K}(1 - \zeta_{p^{n+1}}) \in R$ . Then  $\nu_{\mathfrak{P}}(\pi) = |H|$  implies that  $\pi$  is prime.

(ii), (iii) Obviously  $\mathbb{Z}[\pi]$  is a subring of  $R$  and  $\langle \mathfrak{B} \rangle_{\mathbb{Z}[\pi]}$ , the  $\mathbb{Z}[\pi]$ -module generated by  $\mathfrak{B}$ , is a sublattice of  $\mathbb{Z}[\zeta_{p^{n+1}}]$ .

Now the Pascal matrix  $(\widehat{P})_{\phi(p^{n+1})}$  transforms the  $\mathbb{Z}$ -basis  $\mathfrak{B}'$  of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  to the  $\mathbb{Z}$ -basis

$$\widehat{\mathfrak{B}} = \{1, 1 - \zeta_{p^{n+1}}, \dots, (1 - \zeta_{p^{n+1}})^{\phi(p^{n+1})-1}\}.$$

Let  $0 \leq i < \phi(p^{n+1})$  and  $j, k$  be determined by  $i = |H| \cdot j + k$ ,  $0 \leq k < |H|$ . Then  $(1 - \zeta_{p^{n+1}})^{|H|}/\pi$  is a unit in  $\mathbb{Z}[\zeta_{p^{n+1}}]$ , hence  $(1 - \zeta_{p^{n+1}})^i$  and  $\pi^j(1 - \zeta_{p^{n+1}})^k$  are just differing by a unit. Therefore we get  $\langle \widehat{\mathfrak{B}} \rangle_{\mathbb{Z}[\pi]} = \mathbb{Z}[\zeta_{p^{n+1}}]$ , which implies (ii) and (iii).  $\square$

**Remark 3.3.** Now we state the main results in the theory of twisted group rings, where we fix for the moment the following notation: Let  $R$  be a Dedekind domain with quotient field  $K$ , and let  $S$  be the integral closure in a finite Galois extension  $L$  of  $K$ , with Galois group  $H$ .

Auslander and Goldmann (see [AuGo] or [CuRe], P.591) showed:

**Theorem 3.4.** The twisted group ring  $S \rtimes H$  is a maximal  $R$ -order in  $L \rtimes H$  if and only if the discriminant ideal  $d(S/R)$  coincides with  $R$ .

This is exactly the case, if  $S$  is unramified over  $R$ , so it does not happen for the twisted group  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$ , where we have totally ramification.

The next result is given by Auslander and Rim (see [AuRim] or [CuRe], P.593):

**Theorem 3.5.** The twisted group ring  $S \rtimes H$  is a hereditary  $R$ -order in  $L \rtimes H$  if and only if the Trace ideal  $\text{Tr}_{L/K}(S)$  coincides with  $R$ .

Hence Lemma 3.2 (ii) shows that  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$  is a hereditary  $R$ -order if and only if  $p$  does not divide the order of  $H$ .

We can prove, using the number theoretical Lemma 3.2, the following theorem.

**Theorem 3.6.** Let  $R := \mathbb{Z}[\zeta_{p^{n+1}}]^H$ , the fixed ring of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  under  $H$ . Then there is a full embedding of the  $R$ -order  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$  in the minimal hereditary  $R$ -order

$$\tilde{\Gamma} = \begin{pmatrix} R & \dots & R \\ (\pi) & R & \vdots \\ \vdots & \ddots & \ddots \\ (\pi) & \dots & (\pi) & R \end{pmatrix}_{|H| \times |H|}.$$

*Proof.* We have to show, that we can represent both  $\zeta_{p^{n+1}}$  and  $H$  in  $\Gamma$ .

Therefore we examine the operations of  $\zeta_{p^{n+1}}$  and  $H$  on the  $R$ -module  $\mathbb{Z}[\zeta_{p^{n+1}}]$  with respect to the basis  $\mathfrak{B}$  of Lemma 3.2 (ii), where  $(1 - \zeta_{p^{n+1}})^i$  corresponds to the  $i + 1$ -th row. Now we get the following representations of dimension  $|H|$ :

For  $\zeta_{p^{n+1}}$  the representation is given by the matrix  $(r_{i,j})$ , with

$$\zeta_{p^{n+1}} \cdot (1 - \zeta_{p^{n+1}})^i = \sum_{j=0}^{|H|-1} r_{i+1,j+1} (1 - \zeta_{p^{n+1}})^j,$$

where  $\nu_{\mathfrak{p}}(\zeta \cdot (1 - \zeta_{p^{n+1}})^i) = i$  implies that  $\pi \mid r_{i+1,j+1}$  for  $j < i$ .

The automorphism  $\sigma \in H$  provides the representation  $(s_{i,j})$  given by

$$\sigma((1 - \zeta_{p^{n+1}})^i) = \sum_{j=0}^{|H|-1} s_{i+1,j+1} (1 - \zeta_{p^{n+1}})^j,$$

where  $\nu_{\mathfrak{p}}(\zeta \cdot (1 - \zeta_{p^{n+1}})^i) = i$  implies that  $\pi \mid s_{i+1,j+1}$  for  $j < i$ . □

**Definition 3.7.** Let  $R$  be an integral domain,  $\text{frac}(R) = K$ ,  $\mathfrak{D}$  an  $R$ -order in the finite dimensional  $K$ -algebra  $A$ . With a decomposition into central orthogonal idempotents  $e_1 + \dots + e_n = 1$  the quasi blocks  $B_i$  are defined as  $B_i := \mathfrak{D} \cdot e_i$ .

- Remark 3.8.** (i) With the central primitive idempotent of Remark 3.1  $e := (1 + a^{p^n} + a^{2p^n} + \dots + a^{(p-1)p^n})/p$  the quasi block of  $\mathbb{Z}C_{p^{n+1}} \rtimes H$  corresponding to  $(1 - e)$  is isomorphic to the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes H$ .
- (ii) Note that the method given in the proof of Theorem 3.6 is constructive. As application we give in the next subsection an explicit description of the integral group rings  $\mathbb{Z}G$  for  $G \simeq C_{p^{n+1}} \rtimes C_p$  with  $n \geq 1$ .
- (iii) Theorem 3.6 provides an explicit description of all quasi blocks:  
 Since  $(\mathbb{Z}/2^{n+1}\mathbb{Z})^\times \simeq C_2 \times C_{2^{n-1}}$  and  $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \simeq C_{p-1} \times C_{p^n}$  for  $p$  odd one has to distinguish these two cases:

**Case  $p$  odd:**

One has  $\overline{G} \simeq C_{p^n} \rtimes H$  and  $H \simeq C_q \times C_{p^i}$  with  $q \mid p-1$  and  $i \leq n$ . Let  $b$  and  $c$  be generators of  $C_{p^i}$  and  $C_q$  respectively.

In case of  $i < n$ , the operation of  $H$  on  $C_{p^n}$  is faithfully, hence we are done by induction.

In case of  $i = n$ ,  $\langle b^{p^{i-1}} \rangle$  is the kernel of the operation of  $H$  on  $C_{p^n}$ , hence normal in  $G$ . Then the idempotent  $f := (1 + b^{p^{i-1}} + b^{2p^{i-1}} + \dots + b^{(p-1)p^i})/p$  provides the pullback (Lemma 1.9):

$$\begin{array}{ccc} \mathbb{Z}C_{p^n} \rtimes (C_q \times C_{p^i}) & \xrightarrow{\cdot f} & \mathbb{Z}C_{p^n} \rtimes (C_q \times C_{p^{i-1}}) \\ \cdot (1-f) \downarrow & & \downarrow \\ \mathbb{Z}C_{p^n} \rtimes (C_q \times \langle \xi_{p^i} \rangle) & \longrightarrow & \mathbb{F}_p C_{p^n} \rtimes (C_q \times C_{p^{i-1}}) \end{array}$$

Since  $C_q \times C_{p^{i-1}}$  acts faithfully on  $C_{p^n}$  one can calculate the representations  $\rho(\overline{a})$ ,  $\rho(c)$  and  $\rho(b)$  of  $\mathbb{Z}C_{p^n} \rtimes (C_q \times C_{p^{i-1}})$  inductively.

So it remains to determine the representations of  $\mathbb{Z}C_{p^n} \rtimes (C_q \times \langle \xi_{p^i} \rangle)$ :

Since the operation of  $H$  on  $C_{p^n}$  is not faithfully, one gets  $a^{\xi_{p^i}} = a^b$ . Also  $\xi_{p^i}$  is a root of the minimal polynomial of a primitive  $p^i$ -th root of unity. Hence one gets the representations  $\tau(\overline{a})$ ,  $\tau(c)$  and  $\tau(\xi_{p^i})$ :

$$\tau(\overline{a}) = \rho(\overline{a}), \tau(c) = \rho(c) \text{ and } \tau(\xi_{p^i}) = \zeta_{p^i}^j \cdot \rho(b) \text{ for } 1 \leq j \leq p-1.$$

We have found all representations by a dimension argument.

**Case  $p = 2$ :**

This case is handled analogously. Example 3.9 below serves as illustration.

- (iv) Some special cases of this Theorem were calculated by Roggenkamp.

**Example 3.9.** Let  $G := \langle a, b \mid a^{16} = b^4 = 1, a^b = a^3 \rangle$ , hence  $G \simeq C_{16} \rtimes C_4$ . Then the group ring  $\mathbb{Z}G$  can be written as pullback

$$\begin{array}{ccc} \mathbb{Z}G & \xrightarrow{\alpha} & \mathbb{Z}C_8 \rtimes C_4 \\ \beta \downarrow & & \downarrow \gamma \\ \mathbb{Z}[\zeta_{16}] \rtimes C_4 & \xrightarrow{\delta} & \mathbb{F}_p C_8 \rtimes C_4, \end{array}$$

**Description of the quasiblock  $\mathbb{Z}[\zeta_{16}] \rtimes C_4$  as  $R$ -order:**

One has  $R := \mathbb{Z}[\zeta_{16}]^{C_4} = \mathbb{Z}[\zeta_8 + \zeta_8^3]$ :

$R$  is obviously fixed by the corresponding Galois automorphism  $\sigma : \zeta_{16} \mapsto \zeta_{16}^3$ . We are done since  $R$  is integrally closed and  $\text{rank}_{\mathbb{Z}}(R) = 2 = \phi(16)/4$ . Note that  $\pi := \zeta_8 + \zeta_8^3 = \sqrt{-2}$ .

Lemma 3.2 provides the  $R$ -basis of  $\mathbb{Z}[\zeta_{16}]$ :  $\mathfrak{B} := \{1, 1 - \zeta_{16}, (1 - \zeta_{16})^2, (1 - \zeta_{16})^3\}$  and the Pascal conjugate basis  $\mathfrak{B}' := \{1, \zeta_{16}, \zeta_{16}^2, \zeta_{16}^3\}$ . Then  $\cdot \zeta_{16}$  and  $\sigma$  provides the representations:

$$A' = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & \pi & 0 \end{pmatrix}, \quad B' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ \pi & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}.$$

By conjugation with the Pascal matrix  $(\widehat{P})_4$  we get:

$$A = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 2 - \pi & 2\pi - 4 & 6 - \pi & -3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & -3 & 1 \\ \pi - 2 & 8 & -7 & 0 \\ 3\pi - 4 & 14 & -12 & 3 \end{pmatrix}.$$

Especially the matrices  $A^i B^j$  for  $0 \leq i < 8, 0 \leq j < 4$  give the embedding of  $\mathbb{Z}[\zeta_{16}] \rtimes C_4$  in the hereditary order  $\Gamma$  of Theorem 3.6.

**Description of  $\mathbb{Z}C_8 \rtimes C_4$ :**

Since  $\text{Aut}(C_8) \simeq C_2 \times C_2$  we do not have a faithful operation on  $C_8$ . Therefore we decompose  $\mathbb{Z}C_8 \rtimes C_4$  in quasi blocks via the pullback

$$\begin{array}{ccc} \mathbb{Z}C_8 \rtimes C_4 & \xrightarrow{\alpha} & \mathbb{Z}C_8 \rtimes C_2 \\ \beta \downarrow & & \downarrow \gamma \\ \mathbb{Z}C_8 \rtimes \langle \xi_4 \rangle & \xrightarrow{\delta} & \mathbb{F}_p C_8 \rtimes C_2 \end{array}$$

where the order  $\mathbb{Z}C_8 \rtimes \langle \xi_4 \rangle$  has relations  $a^{\xi_4} = a^3$  and  $\xi_4^2 = -1$ .

Now we have an faithful operation in the induced group ring  $\mathbb{Z}C_8 \rtimes C_2$  and calculate the representations of the quasi block  $\mathbb{Z}[\zeta_8] \rtimes C_2$ , again an  $R$ -order with  $R = \mathbb{Z}[\zeta_8 + \zeta_8^3]$ , as before:

$$A = \begin{pmatrix} 1 & -1 \\ 2 - \pi & \pi - 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 2 - \pi & -1 \end{pmatrix}.$$

The representations of the order  $\mathbb{Z}C_8 \rtimes \langle \xi_4 \rangle$  are given by the matrix  $A$  and by the matrix  $B$  multiplied with the fourth root of unity  $i$ . Note that  $i \notin R$ , therefore  $\mathbb{Z}C_8 \rtimes \langle \xi_4 \rangle$  is no  $R$ -order anymore. Nevertheless we have an embedding of  $\mathbb{Z}C_8 \rtimes \langle \xi_4 \rangle$  in the hereditary order

$$\begin{pmatrix} \mathbb{Z}[\zeta_8] & \mathbb{Z}[\zeta_8] \\ (1 - \zeta_8) & \mathbb{Z}[\zeta_8] \end{pmatrix}.$$

Analogously one can calculate the remaining representations.

### 3.3. A twisted group ring as a factor ring of an integral group ring.

Now we give a description of the integral group rings  $\mathbb{Z}G$ , where  $G \simeq C_{p^{n+1}} \rtimes C_p$ ,  $1 \leq n$ , precisely

$$G := \langle a, b \mid a^{p^{n+1}} = 1, b^p = 1, b^{-1}ab = a^{p^n} \rangle,$$

using the pullback

$$\begin{array}{ccc} \mathbb{Z}G & \xrightarrow{\alpha} & \mathbb{Z}H \\ \beta \downarrow & & \downarrow \gamma \\ \Lambda & \xrightarrow{\delta} & \mathbb{F}_p H, \end{array}$$

where  $H := C_{p^n} \times C_p$ ,  $\Lambda := \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  the twisted group ring ( $\zeta_{p^{n+1}}$  is a primitive  $p^{n+1}$ -th root of unity),  $\beta(a) = \zeta_{p^{n+1}}$  and  $\alpha(a) = \bar{a}$ .

We will give

- a matrix representation of the  $\mathbb{Z}[\zeta_{p^n}]$ -order  $\Lambda$ , which respects the  $p$ -local radical structure.
- an explicit description of the amalgamation  $\delta$ .

For the rest of this chapter we describe the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$ . Therefore we just consider matrices of the size  $p \times p$ , especially we submit  $(\ )_p$  to restrict a matrix of infinite size to a  $p \times p$ -matrix.

**Remark 3.10.** (i) Since the operation of  $b$  on the quotient  $\mathbb{Z}[\zeta_{p^{n+1}}]$  is Galois, with fixed ring  $R := \mathbb{Z}[\zeta_{p^n}]$ , we consider  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  as an  $R$ -order.

(ii) We get from Theorem 3.6 that  $\beta(a)$  and  $\beta(b)$  correspond to the multiplication  $\cdot \zeta_{p^{n+1}}$  and the above Galois operation.

The  $R$ -basis  $\mathfrak{B}' := \{1, \zeta_{p^{n+1}}, \dots, \zeta_{p^{n+1}}^{p-1}\}$  of  $\mathbb{Z}[\zeta_{p^{n+1}}]$  provides the following representation, also given by Ritter and Sehgal [RiSe]:

$$A' = \begin{pmatrix} 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ \zeta_{p^n} & & & & 0 \end{pmatrix}, \quad B' = \begin{pmatrix} 1 & & & & \\ & \zeta & & & \\ & & \zeta^2 & & \\ & & & \ddots & \\ & & & & \zeta^{p-1} \end{pmatrix}.$$

To examine the  $p$ -local structure of  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  we use the  $R$ -basis

$$\mathfrak{B} := \{1, 1 - \zeta_{p^{n+1}}, \dots, (1 - \zeta_{p^{n+1}})^{p-1}\}$$

of  $\mathbb{Z}[\zeta_{p^{n+1}}]$ , given in Lemma 3.2, to prove

**Lemma 3.11.** With respect to the basis  $\mathfrak{B}$ , the representation  $\beta$  is given by the matrices:

$$A = \begin{pmatrix} 1 & -1 & 0 & \dots & 0 \\ 0 & 1 & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 & -1 \\ * & * & * & * & * \end{pmatrix}, \quad B = \begin{pmatrix} 1 & & & & \\ (1-\zeta) & \zeta & & & \\ (1-\zeta)^2 & 2\zeta(1-\zeta) & \zeta^2 & & \\ \vdots & \vdots & \ddots & \ddots & \\ (1-\zeta)^{p-1} & \dots & & & \zeta^{p-1} \end{pmatrix},$$

where the last row of  $A$  is

$$\left( (-1)^p(1 - \zeta_{p^n}), (-1)^{p-1} \binom{p}{p-1}, \dots, (-1)^2 \binom{p}{2}, 1 - \binom{p}{1} \right).$$

*Proof.* Since the basis transformation from  $\mathfrak{B}$  to  $\mathfrak{B}'$  is given by  $\widehat{P}$  one has to conjugate the matrices  $A'$  and  $B'$  with  $\widehat{P}$ :

With the notation given in the Definition 1.22 one decomposes

$$A' = D_1^+ + \zeta_{p^n}(\delta_{p,1}).$$

We easily calculate

$$\widehat{P}(\delta_{p,1})\widehat{P} = (-1)^{p-1}(\delta_{p,1}).$$

Then we have to show, with  $\widetilde{A} := A + (-1)^p \zeta_{p^n}(\delta_{p,1})$  and  $\widetilde{A}' := A' - \zeta_{p^n}(\delta_{p,1})$ , that

$$\widetilde{A}^{\widehat{P}} = \widetilde{A}' \text{ or equivalently } (Id - \widetilde{A})^{\widehat{P}} = Id - \widetilde{A}'.$$

Now we consider the multiplication  $X \cdot$  on the  $\mathbb{Q}[X]$ -module  $\mathbb{Q}[X]/(X-1)^p$ :

With respect to the  $\mathbb{Q}$ -basis  $\{1, X, \dots, X^{p-1}\}$  we get the rational normal form,

exactly the matrix  $Id - \tilde{A}$ . Then the Pascal matrix  $\hat{P}$  transforms this basis to  $\{1, (1 - X), \dots, (1 - X)^{p-1}\}$ , and the equation

$$X \cdot (1 - X)^i = (1 - X)^i - (1 - X)^{i+1}$$

yields to the matrix  $Id - \tilde{A}'$ .

We get the matrix  $B$  with Proposition 1.24 (i) by *evaluation* at  $q := \zeta$  and the *restriction* to size  $p$ .  $\square$

**Definition 3.12.** We fix the following notation:

- (i)  $R := \mathbb{Z}[\zeta_{p^n}]$ ,  $\pi := 1 - \zeta_{p^n}$  and  $\zeta := \zeta_p$ .
- (ii) Let  $\Lambda'$  be the  $R$ -order generated by  $A'$  and  $B'$ .
- (iii) Let  $\Lambda$  be the conjugate  $R$ -order generated by  $A$  and  $B$ .

**Remark 3.13.** We have  $\Lambda' \subseteq (R)_{p \times p}$  and a concrete embedding (Theorem 3.6):

$$\Lambda \subseteq \begin{pmatrix} R & \dots & R \\ (\pi) & R & \vdots \\ \vdots & \ddots & \ddots \\ (\pi) & \dots & (\pi) & R \end{pmatrix}.$$

The  $R$ -order  $\Lambda$  has the advantage, that some of the congruences are put into the  $\pi$ 's, but the generating matrices  $A$  and  $B$  are 'hard to handle', especially by comparing them with  $A'$  and  $B'$ . Surprisingly it turns out, that one can solve this problem, by giving some 'easy to handle' matrices, which also generate the  $R$ -order  $\Lambda$ .

**Definition 3.14.** of the  $p \times p$ -matrices

$$W := \begin{pmatrix} 0 & 1 & & \\ & & \ddots & \\ & & & 1 \\ \pi & & & 0 \end{pmatrix}, T := \begin{pmatrix} 1 & & & \\ & \zeta & & \\ & & \ddots & \\ & & & \zeta^{p-1} \end{pmatrix}, N := \begin{pmatrix} 0 & & & \\ 1-\zeta & & & \\ & 1-\zeta^2 & & \\ & & \ddots & \\ & & & 1-\zeta^{p-1} & 0 \end{pmatrix}.$$

Ritter and Sehgal defined in [RiSe] the  $i$ -th diagonal of a matrix, to describe the twisted group ring  $\Lambda'$ . We are using the following different definition:

**Definition 3.15.** Let  $M$  be a  $p \times p$ -matrix.

- (i) Let  $z \in \mathbb{Z}$ . Then  $\bar{z}, [z]$  are given by:  
 $0 \leq \bar{z} < p$ ,  $0 < [z] \leq p$  and  $z \equiv \bar{z} \equiv [z] \pmod{p}$ .
- (ii) The  $i$ -th diagonal of  $M$ , for  $0 \leq i < p$ , is given by the  $p \times p$ -matrix

$$(\text{diag}_i(M))_{j,k} := \delta_{\overline{k-j}, i} (M)_{j,k}.$$

(iii) The  $p \times p$ -matrix  $M$  lies on the  $i$ -th diagonal if  $M = \text{diag}_i(M)$ .

**Remark 3.16.** (i) Hence the  $i$ -th diagonal is defined via an embedding in a matrix, while Ritter and Sehgal used in [RiSe] a vector for their description.

(ii) Note that if  $M$  lies on the  $i$ -th diagonal and  $M'$  on the  $j$ -th diagonal, then  $MM'$  lies on the  $\overline{i+j}$ -th diagonal.

(iii) The 0-th diagonal is just the diagonal. So  $B' \in \Lambda'$  lies on the diagonal.  $A' \in \Lambda'$  and  $W \in \Lambda$  lie on the first and  $N \in \Lambda$  on the  $(p-1)$ -th diagonal.

(iv) The set  $\{A^i B'^j \mid \leq i, j \leq p-1\}$  is an  $R$ -basis of  $\Lambda'$ , where the elements are lying on diagonals. It will turn out that  $\{N^i W^j \mid \leq i, j \leq p-1\}$  plays the same role for the  $R$ -order  $\Lambda$ .

Therefore it is crucial to understand the diagonals of  $\Lambda$ . For explicit calculations, it is useful to consider the diagonals as vectors. This leads to

**Definition 3.17.** Let  $(m_{i,j})$  be a  $p \times p$  matrix in the matrix ring  $\mathcal{M}$ . Then  $\tau$  is defined by:

$$\begin{aligned} \tau : \mathcal{M} &\rightarrow \mathcal{M} \\ m_{i,j} &\mapsto m_{i,1+i-j} \end{aligned} .$$

**Example 3.18.**

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}^\tau = \begin{pmatrix} 1 & 3 & 2 \\ 5 & 4 & 6 \\ 9 & 8 & 7 \end{pmatrix} .$$

**Remark 3.19.** (i)  $\tau$  permutes the  $i$ -th diagonals with the  $[1-i]$ -th columns.

(ii) For lower triangular matrices of finite size this definition of  $\tau$  (given for matrices of finite size) coincides with Definition 2.4 which is given for lower triangular matrices.

(iii) The entries of  $N^i$  are all zero, except in the  $\overline{p-i}$ -th diagonal, with the entries occurring in the equation given in Corollary 2.24. Note that this entries are just the summands

$$i < k \leq p : \quad (N^i)_{k,k-i} = (1 - \zeta^{k-i}) \dots (1 - \zeta^{k-1}).$$

The main result of this chapter is the following theorem, which is used to given an explicit description of the additive structure (see Theorem 3.22) and the multiplicative structure (see Theorem 3.23) of  $\Lambda$ . Also a complete description of the congruences of the  $R$ -order  $\Lambda$  is given (see Theorem 3.30).

**Theorem 3.20.** (i) Set  $\zeta := \zeta_p^{p^{n-1}}$ . The  $R$ -order  $\Lambda$  is generated as ring by  $W$  and  $N$  and the relations

$$N^p = 0, \quad W^p = \pi, \quad WN = \zeta \cdot NW + (1 - \zeta).$$

(ii) The amalgamation  $\delta$  is determined by:

$$\begin{aligned} p \text{ odd} : \delta(W) &= 1 - \bar{a} + \bar{a}^{-(p-1)}(1 + \bar{b} + \dots + \bar{b}^{p-1}) \sum_{i=1}^{p-1} \frac{\bar{a}^i}{i}, \\ p = 2 : \delta(W) &= (1 + \bar{a})\bar{b}. \end{aligned}$$

Let  $L$  be the as follows recursive defined  $p-1 \times p-1$ -matrix over  $\mathbb{F}_p$ :

$$\mathcal{SC} : (L)_{1,1} := 1,$$

$$\mathcal{CR} : (L)_{i+1,j+1} := (i-1)(L)_{i,j+1} + (L)_{i,j} \quad \text{for } i \geq j \geq 0.$$

$$\text{Then:} \quad \delta(N) = - \sum_{0 < i, j < p} (L)_{i,j} \frac{1}{i!} (1 - \bar{b})^i \bar{a}^{-j}.$$

*Proof.* All matrices in this proof are of size  $p \times p$ , unless the  $p-1 \times p-1$  matrices  $(\bar{L})_{p-1}$  and  $L$ . Therefore, as above, we suppress the index  $(\ )_p$  for *restriction*.

(i) Note that  $W^p = \pi$  and  $R = \mathbb{Z}[\pi]$ , so  $\langle W, N \rangle$  is an  $R$ -module.

We show that  $\Lambda \subseteq \langle W, N \rangle$ . Since  $A$  and  $B$  generate  $\Lambda$ , it is enough to show that  $A, B \in \langle W, N \rangle$ .

( $\alpha$ )  $A \in \langle W, N \rangle$ :

It is enough to show that  $S := A - Id + W \in \langle W, N \rangle$ . The entries of  $S$  are zero except in the last row, where they are all divisible by  $p$ .

Since  $N^{p-1} = p(\delta_{p,1})$  one gets  $N^{p-1}W^i = p(\delta_{p,1+i})$  and

$$S = \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} N^{p-1}W^i \in \langle W, N \rangle.$$

( $\beta$ )  $B \in \langle W, N \rangle$ :

Since the unit  $T = Id - NW$  lies in  $\langle W, N \rangle$ , we have to show that

$$BT^{-1} = D_{1-\zeta} P D_{1-\zeta}^{-1} \in \langle W, N \rangle.$$

Therefore it suffices to show that for

$$0 \leq j < p : \quad \text{diag}_j(D_{1-\zeta} P D_{1-\zeta}^{-1}) = \sum_{i=j}^{p-1} N^i W^{i-j} r_{i,j} \quad \text{with } r_{i,j} \in R.$$

We apply  $\tau$  to this equation and have, since  $P^\tau = P$ , to solve the following equations for

$$0 \leq j < p : \quad (PD_{1-\zeta})_{*,j+1} = \sum_{i=j}^{p-1} (N^i W^{i-j})^\tau r_{i,j} \quad \text{with } r_{i,j} \in R.$$

For  $j \leq i < p$  the  $j+1$ -th column of the matrix  $(N^i W^{i-j})^\tau$  coincides with the  $i+1$ -th column of the matrix  $\widehat{K}_\zeta$  (see Definition 2.11), and the other columns are zero. (So in Example 2.12 one has  $\pi_i := 1 - \zeta^i$ .)

Hence one has to solve the system of linear equations:

$$PD_{1-\zeta} = \widehat{K}_\zeta \cdot (r_{i,j}), \quad \text{with } (r_{i,j}) \in (R)_{p \times p}.$$

Proposition 2.18 (i) gives:

$$(r_{i,j}) = \widehat{K}_\zeta^{-1} PD_{1-\zeta} = F_\zeta^{-1} \bar{L}_\zeta.$$

By construction  $\bar{L}_\zeta \in (R)_{p \times p}$ , moreover it is even a unit, because it is a lower triangular matrix with entries 1 on the diagonal. The matrix of factorials  $F_\zeta$  is also invertible in  $(R)_{p \times p}$ , because it is of diagonal shape, with products of cyclotomic units as entries.

Hence we have shown that  $\Lambda \subseteq \langle W, N \rangle$ .

Next we prove that  $\langle W, N \rangle \subseteq \Lambda$ .

The necessary calculations are performed in a conjugate representation of  $\Lambda$ , namely in  $\Lambda'$ . Exactly, by denoting  $W' := \widehat{P}W\widehat{P}$  and  $N' := \widehat{P}N\widehat{P}$ , it remains to show, that  $W', N' \in \Lambda'$ .

( $\gamma$ )  $W' \in \Lambda'$ :

The matrix  $W'$  is given by:

$$W' = \begin{pmatrix} 1 & -1 & 0 & & \\ & 1 & -1 & & \\ & & \ddots & \ddots & \\ & & & 1 & -1 \\ * & * & * & * & * \end{pmatrix},$$

where the last row of  $W'$  is

$$\left( (-1)^p \zeta_{p^n}, (-1)^{p-1} \binom{p}{p-1}, \dots, (-1)^2 \binom{p}{2}, 1 - \binom{p}{1} \right).$$

The proof is the same as for Lemma 3.11 one just has to replace  $\zeta_{p^n}$  by  $\pi$ .

An easy calculation for  $S' := (Id - B')A'^{-1}$  gives:

$$A'^{-1} = \begin{pmatrix} 0 & & & \zeta_{p^n}^{-1} \\ 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 & 0 \end{pmatrix}, \quad S' := \begin{pmatrix} 0 & & & & \\ 1-\zeta & & & & \\ & 1-\zeta^2 & & & \\ & & \ddots & & \\ & & & 1-\zeta^{p-1} & 0 \end{pmatrix}.$$

Hence  $S'$  is the same matrix as  $N$  and we get for

$$0 \leq i < p : \quad S'^{p-1}A'^i = (p\delta_{p,1+i})_p.$$

This implies for  $p$  odd the equation

$$(*_p) \quad W' = Id - A' - S'^{p-1} \sum_{i=1}^{p-1} (-1)^i \frac{\binom{p}{i}}{p} A'^i \in \Lambda'.$$

Now we handle the special case  $p=2$ :

By conjugation with the Pascal matrix  $\widehat{P}$  we get:

$$\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1-q & -1 \end{pmatrix}.$$

*Evaluation* at  $q := \zeta_{2^n}$  gives the transformation from  $A'$  to  $A$ . So the first diagonal is given by  $-W + (1 - \zeta_{2^n})N$  (instead of  $-W$  in the case  $p$  odd).

*Evaluation* at  $q := 1 - \zeta_{2^n}$  gives the transformation from  $W$  to  $W'$ . So the first diagonal is given by  $-A' + \zeta_{2^n}S'$  (instead of  $-A'$  in the case  $p$  odd), hence we get the equation

$$(*_2) \quad W' = B' - A' + \zeta_{2^n}S' \in \Lambda', \text{ (with } \zeta_{2^n} = A^2).$$

(One easily sees, that it is not possible to change the definition of  $W$  for the case  $p = 2$  by multiplying the first column of  $W$  by  $-1$  in order to unify the proof.)

( $\partial$ )  $N' \in \Lambda'$ :

From Proposition 1.24 (iii) it follows that

$$(**) \quad N' = Id - \widehat{H}_\zeta.$$

So it suffices to show that

$$\text{diag}_j(\widehat{H}_\zeta) = \sum_{i=j}^{p-1} S^i A'^{i-j} r_{i,j} \quad \text{with } r_{i,j} \in R.$$

Now we apply  $\tau$  to this equation. Since for  $0 \leq j \leq i < p$  the matrices  $S^i A'^{i-j} \in \Lambda'$  and  $N^i W^{i-j} \in \Lambda$  coincide one can use the same arguments as in ( $\beta$ ) to reduce

the problem to the system of linear equations

$$\widehat{H}_\zeta^\tau = \widehat{K}_\zeta \cdot (r_{i,j}),$$

where the solution is given by Proposition 2.22 (i):

$$(***) \quad (r_{i,j}) = F_\zeta^{-1} D_\zeta \bar{L}_\zeta D_\zeta^{-1} \in (R)_{p \times p}.$$

Evaluating the equation

$$B'^{-1} A' B' = A^{p^n+1}$$

shows that  $\zeta = \zeta_p^{p^n-1}$ . The relations for  $N$  and  $W$  are following from some easy calculations. Theorem 3.22 will show that there are no other relations.

(ii) Obviously  $\delta(A) = \bar{a}$  and  $\delta(B) = \bar{b}$ . An easy calculation in  $\mathbb{F}_p$  shows that for

$$1 \leq i < p: \quad (-1)^{i-1} \frac{\binom{p}{i}}{p} \equiv \frac{1}{i} \pmod{p}.$$

Since  $\delta(W)$  is determined - up to transformation- by the formulas  $(*_p)$  we obtain the representation for  $\delta(W)$ .

Using  $(**)$ , we determine  $\delta(N)$ :

The  $\overline{-j}$ -th diagonal of  $\widehat{H}_\zeta$  coincides with the  $j+1$ -th column of  $\widehat{H}_\zeta^\tau$  and the  $j+1$ -th column of  $(S^i A^{i-j})^\tau$  coincides with the  $i+1$ -th column of  $\widehat{K}_\zeta$  for  $0 \leq j \leq i < p$ .

So  $(***)$  describes the amalgamation. Obviously

$$\delta(S^i A^{i-j}) = ((1-\bar{b})\bar{a}^{-1})^i \cdot \bar{a}^{i-j} = (1-\bar{b})^i \bar{a}^{-j}.$$

Since  $\widehat{H}_\zeta$  has the same diagonal as the identity  $Id$ , one just has to examine the  $j$ -th diagonals for  $j \geq 1$ . Therefore one only has to consider the submatrix  $\bar{L}_\zeta$ , given in Proposition 2.20 (ii), of the  $p \times p$ -matrix  $\bar{L}_\zeta$ . Obviously  $\bar{L}_\zeta$  coincides modulo  $(1-\zeta)$  with the modular matrix  $(L)_{p-1}$  ( $\delta$  allows to consider the entries modulo  $(1-\zeta)$ ). For the same reason the matrix  $D_\zeta$  corresponds to the identity  $Id$  and the inverse  $F_\zeta^{-1}$  of the matrix of factorials divides the  $i$ -th row of  $L$  by  $i!$ .  $\square$

**Remark 3.21.** (i)  $T \in \Lambda$  (Definition 3.14) is a unit of order  $p$ , satisfying:

$$T = Id - NW, \quad WN - NW = (1-\zeta)T.$$

For  $p \in \{2, 3\}$  we will use this unit  $T$  to construct an non inner automorphism of the integral group ring  $\mathbb{Z}G$ .



Then the multiplicative structure of  $\Lambda$  is given by:

$$(i) \text{ For } 0 \leq j \leq i < p: \quad W^i \cdot N^j = \sum_{l=0}^j (\mathfrak{M}_i)_{j+1, l+1} N^{j-l} W^{i-l}.$$

$$(ii) \text{ For } 0 \leq i \leq j < p: \quad W^i \cdot N^j = \sum_{l=0}^i (\mathfrak{M}_j)_{i+1, l+1} N^{j-l} W^{i-l}.$$

*Proof.* (i) With Theorem 3.20 (ii) one shows inductively that:

$$W^i \cdot N = \zeta^i \cdot N W^i + (1 - \zeta^i) \cdot W^{i-1}.$$

Then  $W^i \cdot N^j = (W^i \cdot N) \cdots N$  leads to the recursive definition.

(ii) This follows analogously with  $W \cdot N^j = \zeta^j \cdot N^j W + (1 - \zeta^j) \cdot N^{j-1}$ .  $\square$

**Example 3.24.** Let  $p > 3 = i \geq j$ . Then

$$\mathfrak{M}_3 = \begin{pmatrix} 1 \\ \zeta^3 & 1 - \zeta^3 \\ \zeta^6 & (\zeta^2 + \zeta^3)(1 - \zeta^3) & (1 - \zeta^2)(1 - \zeta^3) \\ \zeta^9 & (\zeta^4 + \zeta^5 + \zeta^6)(1 - \zeta^3) & (\zeta + \zeta^2 + \zeta^3)(1 - \zeta^2)(1 - \zeta^3) & (1 - \zeta)(1 - \zeta^2)(1 - \zeta^3) \end{pmatrix}.$$

Especially for  $j \leq 3$  we get

$$W^3 N^j = \sum_{l=0}^j (\mathfrak{M}_3)_{j+1, l+1} N^{j-l} W^{3-l}.$$

**Remark 3.25.** (i) Since  $N \cdot W = \zeta^{-1} \cdot W N + 1 - \zeta^{-1}$  one gets also formulas for the multiplication "from the other side", where  $\overline{\mathfrak{M}_t}$  is complex conjugate to  $\mathfrak{M}_t$ .

$$\text{For } 0 \leq j \leq i < p: \quad N^i \cdot W^j = \sum_{l=0}^j (\overline{\mathfrak{M}_i})_{j+1, l+1} W^{j-l} N^{i-l}.$$

$$\text{For } 0 \leq i \leq j < p: \quad N^i \cdot W^j = \sum_{l=0}^i (\overline{\mathfrak{M}_j})_{i+1, l+1} W^{j-l} N^{i-l}.$$

(ii) After localizing at  $p$  the radical of  $R$ -order  $\Lambda$  is precisely the ideal  $\langle W, N \rangle$  with an  $R$ -basis

$$\{N^i W^j \mid 0 \leq i, j < p, i + j \neq 0\}.$$

We get this result from Theorem 3.22 and from

$$\Lambda / \langle W, N \rangle \simeq R / \pi \simeq \mathbb{F}_p.$$

In the next chapter we describe  $\langle W, N \rangle$  more general (see Theorem 6.5).

- (iii) Since every  $N^i W^j$  lies in exactly one diagonal, there are no congruences between different diagonals.

To describe the congruences inside the  $i$ -th diagonal, we use:

**Definition 3.26.** Let  $0 \leq i < p$ .

- (i) Let  $\tilde{D}_i$  be the  $p \times p$  diagonal matrix

$$(\tilde{D}_i)_{j,j} := \begin{cases} 1 & \text{if } j \leq p - i, \\ \pi & \text{if } j > p - i. \end{cases}$$

- (ii)  $\Lambda_i := \{\lambda \in \Lambda \mid \lambda \text{ lies on the } i\text{-th diagonal of } \Lambda\}$ .  
 (iii)  $\tilde{\Lambda}_i := \tilde{D}_i^{-1} \Lambda_i$ .

**Example 3.27.**  $\tilde{D}_0$  is the identity,

$$\tilde{D}_1 = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \pi \end{pmatrix}, \dots, \tilde{D}_{p-1} = \begin{pmatrix} 1 & & & \\ & \pi & & \\ & & \ddots & \\ & & & \pi \end{pmatrix}.$$

**Remark 3.28.** Since  $\tau$  (Definition 3.17) turns diagonals into columns and

$$\Lambda \subseteq \begin{pmatrix} R & \dots & R \\ (\pi) & R & \vdots \\ \vdots & \ddots & \ddots \\ (\pi) & \dots & (\pi) & R \end{pmatrix}$$

we identify  $\tilde{\Lambda}_i^\tau$  as subset of  $R^p$ . Especially we can describe the congruences in  $\Lambda$  by considering  $\tilde{\Lambda}_i^\tau$ .

**Example 3.29.** With  $W \in \Lambda_1$  and  $N \in \Lambda_{p-1}$  we get that  $\tilde{D}_1^{-1} W^\tau \in \tilde{\Lambda}_1^\tau$  and  $\tilde{D}_{p-1}^{-1} N^\tau \in \tilde{\Lambda}_{p-1}^\tau$  are corresponding to the vectors:

$$\tilde{D}_1^{-1} W^\tau \sim \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \text{ and } \tilde{D}_{p-1}^{-1} N^\tau \sim \frac{1}{\pi} \begin{pmatrix} 0 \\ 1 - \zeta \\ \vdots \\ 1 - \zeta^{p-1} \end{pmatrix}.$$

**Theorem 3.30.** By decomposing the  $R$ -order  $\Lambda = \bigoplus_{i=0}^{p-1} \Lambda_i$  one gets:

- (i) An  $R$ -basis of  $\tilde{\Lambda}_i^\tau$  is given by the columns of  $\hat{P} D_{1-\zeta} \tilde{D}_i^{-1}$ .  
 (ii) Let  $v \in R^p$ . Then  $v \in \tilde{\Lambda}_i^\tau$  if and only if  $\tilde{D}_i D_{1-\zeta}^{-1} \hat{P} \cdot v \in R^p$ .

*Proof.* (i) Theorem 3.22 implies, that  $\Lambda_i$  has the  $R$ -basis

$$\{N^0 W^i, \dots, N^{p-1-i} W^{p-1}, N^{p-i} W^0, \dots, N^{p-1} W^{i-1}\}.$$

By applying  $\tilde{D}_i^{-1}$  and  $\tau$  to this basis one easily sees that the first  $p-i$  basis vectors are given by the first  $p-i$  columns of  $\hat{K}$ , while the others are the remaining columns of  $\hat{K}$  divided by  $\pi$ . Hence an  $R$ -basis of  $\tilde{\Lambda}_i^\tau$  is given by the columns of  $\hat{K}\tilde{D}_i^{-1}$ . We conclude with  $\hat{P} = PD_{-1}$  and Remark 2.19 that

$$\hat{K} \cdot \tilde{D}_i^{-1} = \hat{P}D_{1-\zeta} \cdot X \cdot \tilde{D}_i^{-1}$$

with the lower triangular matrix  $X := D_{-1}\bar{L}_\zeta^{-1}F_\zeta \in GL_p(R)$ , because the matrix of factorials  $F_\zeta$  is of diagonal shape, with cyclotomic units as entries and  $\bar{L}_\zeta^{-1}$  is a lower triangular matrix with entries 1 on the diagonal. Then one easily determines  $X'_i := \tilde{D}_i X \tilde{D}_i^{-1}$  as

$$(X'_i)_{k,l} := \begin{cases} \pi(X)_{k,l} & \text{if } p-i < k \leq p \text{ and } 1 \leq l \leq p-i, \\ (X)_{k,l} & \text{else.} \end{cases}$$

Especially this operation does not affect the entries on the diagonal, hence  $X'_i$  is a lower triangular matrix with units on the diagonal, which shows that  $X'_i \in GL_p(R)$  and we are done with

$$\hat{K}\tilde{D}_i^{-1} = \hat{P}D_{1-\zeta}\tilde{D}_i^{-1} \cdot X'_i.$$

(ii) By (i)  $\tilde{\Lambda}_i^\tau$  is given as the image of  $\hat{P}D_{1-\zeta}\tilde{D}_i^{-1}$ . Hence we get for  $v \in R^p$  that

$$v \in \tilde{\Lambda}_i^\tau \iff (\hat{P}D_{1-\zeta}\tilde{D}_i^{-1})^{-1} \cdot v \in R^p.$$

We are done since  $\hat{P}$  is an involution (Lemma 1.2 (ii)).  $\square$

**Example 3.31.** Let  $p = 5$ ,  $n > 1$ ,  $\zeta$  and  $\pi$  as above. Then by denoting

$$\hat{v}_0 := \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \hat{v}_1 := \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \hat{v}_2 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 3 \\ 6 \end{pmatrix}, \hat{v}_3 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 4 \end{pmatrix}, \hat{v}_4 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

and  $v_i := (1-\zeta)^i \hat{v}_i$  we get the following  $R$ -bases  $\mathfrak{B}_{\tilde{\Lambda}_i^\tau}$ : for  $\tilde{\Lambda}_i^\tau$ :

$$\mathfrak{B}_{\tilde{\Lambda}_0^\tau} = \{v_0, \dots, v_4\}, \mathfrak{B}_{\tilde{\Lambda}_1^\tau} = \{v_0, \dots, v_3, v_4/\pi\}, \dots, \mathfrak{B}_{\tilde{\Lambda}_4^\tau} = \{v_0, v_1/\pi, \dots, v_4/\pi\}.$$

Now we give an impression, how to apply part (ii) of the last theorem, by checking whether  $W$  and  $N$  are elements of  $\Lambda$ . Then  $W^i \in \Lambda_i$  corresponds to  $v_0 \in \mathfrak{B}_{\tilde{\Lambda}_i^\tau}$

and  $N \in \Lambda_{p-1}$  to

$$\widehat{v} = \frac{1}{\pi}(v_0 - v_\zeta) \text{ with } v_\zeta := \begin{pmatrix} \zeta^0 \\ \zeta^1 \\ \zeta^2 \\ \zeta^3 \\ \zeta^4 \end{pmatrix}.$$

And, as expected, we have

- with  $\widehat{P}^2 = Id$  and  $\widehat{P}_{*,1} = v_0$ , that

$$\widehat{P} \cdot v_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \text{ and hence } \widetilde{D}_1 D_{1-\zeta}^{-1} \widehat{P} \cdot v_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \in R^p,$$

- with

$$\widehat{P} \cdot v_\zeta = \begin{pmatrix} (1-\zeta)^0 \\ (1-\zeta)^1 \\ (1-\zeta)^2 \\ (1-\zeta)^3 \\ (1-\zeta)^4 \end{pmatrix} \text{ that } \widetilde{D}_4 D_{1-\zeta}^{-1} \widehat{P} \cdot \widehat{v} = - \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \in R^p.$$

## 4. AUTOMORPHISMS AND UNITS

## 4.1. Automorphisms of integral group rings.

One can use the following strategy to construct outer central automorphisms of the integral group ring  $\mathbb{Z}C_{p^{n+1}} \rtimes C_p$  by the pullback

$$\begin{array}{ccc} \mathbb{Z}C_{p^{n+1}} \rtimes C_p & \longrightarrow & \mathbb{Z}C_{p^n} \times C_p \\ \beta \downarrow & & \downarrow \gamma \\ \Lambda & \xrightarrow{\delta} & \mathbb{F}_p C_{p^n} \times C_p. \end{array}$$

Assume there is a unit  $\lambda \in \Lambda^\times$ , such that the preimage of  $\delta(\lambda)$  under  $\gamma$  contains no unit. Since conjugation with  $\lambda$  in  $\Lambda$  induces the identity in the modular image, one can lift this inner automorphism of  $\Lambda$  to an outer automorphism of  $\mathbb{Z}C_{p^{n+1}} \rtimes C_p$  by conjugation with  $\lambda$  in  $\Lambda$  and the identity on  $\mathbb{Z}C_{p^n} \times C_p$ .

We apply this method to  $T \in \Lambda$ , a unit of order  $p$  (see Definition 3.14):

Since  $T = Id - NW$  (see Remark 3.21), we get  $\delta(T)$  with Theorem 3.20 (iii).

Then there is the **problem**:

- Is there a unit  $u \in \mathbb{Z}C_{p^n} \times C_p$  with  $\gamma(u) = \delta(T)$ ?

To get outer automorphisms we are interested in a negative answer. We don't have a result for general  $p$  but one can check it for some special primes.

**Theorem 4.1.** Let  $p \in \{2, 3\}$ . Then conjugation with  $T$  on  $\Lambda$  together with the identity on  $\mathbb{Z}C_{p^n} \times C_p$  provides an outer automorphism of the integral group ring  $\mathbb{Z}C_{p^{n+1}} \rtimes C_p$ .

*Proof.* From the discussion above it follows that  $T$  induces an automorphism for general  $p$ . Now Theorem 3.20 provides

$$\delta(T) = \begin{cases} \bar{a}^{-1} + \bar{b} + \bar{a}^{-1}\bar{b} & \text{if } p = 2, \\ \bar{b} - \bar{a}^{-1} + \bar{a}^{-1}\bar{b}^2 - \bar{a}^{-2} - \bar{a}^{-2}\bar{b} - \bar{a}^{-2}\bar{b}^2 & \text{if } p = 3. \end{cases}$$

By a classical theorem of Higman there are only trivial units in  $\mathbb{Z}C_p \times C_p$  for  $p \in \{2, 3\}$ . Hence we are done for  $n = 1$ . For general  $n \in \mathbb{N}$  we consider the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & (1 - \bar{a}^p) & \longrightarrow & \mathbb{Z}C_{p^n} \times C_p & \longrightarrow & \mathbb{Z}C_p \times C_p \longrightarrow 0 \\ & & & & \downarrow \gamma & & \downarrow \gamma' \\ 0 & \longrightarrow & (1 - \bar{a}^p) & \longrightarrow & \mathbb{F}_p C_{p^n} \times C_p & \xrightarrow{\alpha} & \mathbb{F}_p C_p \times C_p \longrightarrow 0. \end{array}$$

The case  $n = 1$  shows, that the preimage of  $\alpha(\delta(T))$  under  $\gamma'$  contains no unit, and hence the preimage of  $\delta(T)$  under  $\gamma$  contains no unit, and  $T$  does not lift to an unit in the integral group ring  $\mathbb{Z}G$ .

Now we assume that this automorphism is inner, hence there is an unit  $u \in \mathbb{Z}G^\times$ , which we can choose with augmentation 1, such that  $\beta(u) = T \cdot c$  for a central unit  $c \in \Lambda$ , where the center of  $\Lambda$  is given by the ring  $R = \mathbb{Z}[\zeta_{p^n}]$ . Then we consider the commutative diagram

$$\begin{array}{ccccccc}
 & & \mathbb{Z}G & \longrightarrow & \mathbb{Z}C_{p^n} \times C_p & \longrightarrow & \mathbb{Z}C_p \times C_p \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \beta & & & & \\
 R & \xrightarrow{\iota} & \Lambda & \xrightarrow{\delta} & \mathbb{F}_p C_{p^n} \times C_p & \xrightarrow{\alpha} & \mathbb{F}_p C_p \times C_p.
 \end{array}$$

We conclude with  $c \in \iota(R)$  and  $\text{Im}(\iota\delta\alpha) = \mathbb{F}_p$  that

$$\alpha(\delta(\beta(u))) = \alpha(\delta(T)) = \begin{cases} a + b + ab & \text{if } p = 2, \\ b - a^2 + a^2b^2 - a - ab - ab^2 & \text{if } p = 3, \end{cases}$$

which contradicts the theorem of Higman.  $\square$

**Remark 4.2.** Let us point out, where the problem to generalize this proof to arbitrary prime  $p$  lies:

- (i) There is no generic description for the group of units in  $\mathbb{Z}C_p \times C_p$  for an arbitrary prime  $p$ . Even the integral group ring  $\mathbb{Z}C_p$  doesn't allow such a description of the group of units, since one can consider  $\mathbb{Z}C_p$  as pullback

$$\begin{array}{ccc}
 \mathbb{Z}C_p & \longrightarrow & \mathbb{Z} \\
 \downarrow & & \downarrow \\
 \mathbb{Z}[\zeta] & \xrightarrow{\text{mod } 1-\zeta} & \mathbb{F}_p
 \end{array}$$

and there is no explicit description of  $\mathbb{Z}[\zeta]^\times$ .

- (ii) One can also describe  $\mathbb{Z}C_p \times C_p$  by a pullback diagram, which reduces the problem to determine the units in  $\mathbb{Z}[\zeta]$ . For some explicit given primes  $p$  one can do this by using computer algebra systems.

As an application of the last theorem we first give Lemma 3.5. of [RoTa]:

**Lemma 4.3.** Let  $D_4$  be the dihedral group of order 8. Then there are two conjugacy classes of group bases in  $\mathbb{Z}D_4$ .

Hereby

- conjugacy class means conjugation in  $V(\mathbb{Z}D_4)$ , the group of units in  $\mathbb{Z}D_4$  of augmentation 1.
- a group basis of  $\mathbb{Z}G$  is a subgroup  $H$  of  $V(\mathbb{Z}G)$  with  $|H| = |G|$ .

Then one gets

**Lemma 4.4.** Conjugation with the involution  $T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  induces an automorphism of  $\mathbb{Z}D_4$ , which permutes the conjugacy classes of group bases.

This automorphism is most easily described using a pullback:

- (i) By Lemma 3.11 we consider  $a, b \in \mathbb{Z}D_4$  as

$$a \sim \left( \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}, \bar{a} \right) \text{ and } b \sim \left( \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}, \bar{b} \right).$$

Applying the automorphism given by conjugation with  $T$  one gets:

$$a^T \sim \left( \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix}, \bar{a} \right) \text{ and } b^T \sim \left( \begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix}, \bar{b} \right).$$

- (ii) With respect to the group basis  $G$  one gets:

$$\begin{aligned} ()^T : \mathbb{Z}D_4 &\rightarrow \mathbb{Z}D_4 \\ a &\mapsto a + (1 - a^2)(b - ab - 2a) \\ b &\mapsto b - (1 - a^2)(a + ab). \end{aligned}$$

#### 4.2. Automorphisms of twisted group rings.

Now we will consider automorphisms of the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p \simeq \Lambda$ . Later on, these results will be applied to get projective resolutions of some  $\Lambda$ -lattices.

From  $W^p = \pi$  follows that  $W$  is no unit in  $\Lambda$  but a rational unit. Hence we can conjugate with  $W$  and get

**Theorem 4.5.** The conjugation with  $W$  provides an automorphism of the  $R$ -order  $\Lambda$ .

*Proof.* Since  $\Lambda = \langle N, W \rangle$ , (Theorem 3.20 (i)) one just has to show, that

$$N_1 := {}^W N \in \Lambda.$$

One easily calculates

$$N_1 = \begin{pmatrix} & & & (1-\zeta)/\pi \\ 1-\zeta^2 & & & \\ & \ddots & & \\ & & 1-\zeta^{p-1} & \\ & & & 0 \end{pmatrix}.$$

Then  $N$  and  $N_1$  are lying on the  $(p-1)$ -th diagonal, (Definition 3.15 ), and correspond to (see Definition 3.26, Remark 3.28 and Example 3.29 )

$$\hat{n}_0 := \frac{1}{\pi} \begin{pmatrix} 0 \\ 1-\zeta \\ 1-\zeta^2 \\ \vdots \\ 1-\zeta^{p-1} \end{pmatrix} \in \tilde{\Lambda}_{p-1}^\tau \quad \text{and} \quad \hat{n}_1 := \frac{1}{\pi} \begin{pmatrix} 1-\zeta \\ 1-\zeta^2 \\ \vdots \\ 1-\zeta^{p-1} \\ 0 \end{pmatrix} \in \tilde{\Lambda}_{p-1}^\tau.$$

By Theorem 3.30 we have to show, that

$$\tilde{D}_{p-1} D_{1-\zeta}^{-1} \hat{P} \cdot \hat{n}_1 \in R^p \text{ holds.}$$

Then  $(\hat{P}) = 1$ ,  $(D_{1-\zeta}^{-1}) = 1$  and  $\tilde{D}_{p-1} = 1$  implies that the entry of the first position of this product is given by  $1 - \zeta/\pi \in R$ . Let  $n_i := \pi \hat{n}_i$  and  $1 < j \leq p$ . Then we have to show that the  $j$ -th entry of  $\hat{P} \cdot n_1$  lies in  $(1 - \zeta)^{j-1}$ .

Let  $1 < j < p$ : Since  $n_1$  is the vector  $n_0$  shifted by one position we get with Definition 2.15 that

$$\hat{P} \cdot n_1 = (\hat{P})_{*,*+1} \cdot n_0.$$

From the recursive definition of the Pascal matrix follows that the  $j+1$ -row of  $\hat{P}$  is equal to the  $j$ -row of  $\hat{P}$  minus the  $j$ -row of  $(\hat{P})_{*,*+1}$ . Hence we get

$$(\hat{P})_{j,*} \cdot n_1 = (\hat{P})_{j,*+1} \cdot n_0 = (\hat{P})_{j,*} \cdot n_0 - (\hat{P})_{j+1,*} \cdot n_0.$$

Now  $N \in \Lambda$  implies that  $(\hat{P})_{j,*} \cdot n_0 \in ((1-\zeta)^{j-1})$  and  $(\hat{P})_{j+1,*} \cdot n_0 \in ((1-\zeta)^j)$ , which shows that  $(\hat{P})_{j,*} \cdot n_1 \in (1 - \zeta)^{j-1}$ .

Let  $j = p$ : Observe that  $(1 - \zeta)^{p-1} \sim p$  and that the entries  $(-1)^i \binom{p-1}{i}$  in the  $p$ -th row of  $\hat{P}$  are equivalent to 1 modulo  $p$ . Then we are done since  $\text{Tr}(1 - \zeta) = p$ .  $\square$

#### 4.3. Units in integral and in twisted group rings.

For the rest of this chapter we will use the notation  $\Delta(G)$  for the augmentation ideal of the integral group ring  $\mathbb{Z}G$ .

A classical theorem of Higman describes the units for an abelian group in the integral group ring:

**Theorem 4.6.** (i) Let  $H$  be an abelian group. The group of units with augmentation 1 is given by

$$V(\mathbb{Z}H) \simeq H \times N,$$

where  $N$  is a free abelian group, with elements congruent to 1 mod  $(\Delta^2(H))$ ,  
 $N := U(1 + \Delta^2(H))$ .

(ii) Let  $G$  be an arbitrary group with commutator subgroup  $G'$ .

Then  $V(\mathbb{Z}G)/U(1 + \Delta^2(G)) \simeq G/G'$ .

**Remark 4.7.** (i) A proof of (i) is given by Cliff, Sehgal and Weiss, who considered the exponential type homomorphism

$$e : \sum_{h \in H} z_h h \rightarrow \prod_{h \in H} h^{z_h}.$$

Part (ii) of the theorem follows with the same arguments.

(ii) The following theorem is a special case of a well known theorem of Cliff, Sehgal and Weiss [ClSeWe]. But the proof given here for the group  $C_{p^{n+1}} \rtimes C_p$  is more elementary. One is interested if the following theorem is also true for nilpotent groups (see [Se] Problem 28).

**Theorem 4.8.** Let  $G \simeq C_{p^{n+1}} \rtimes C_p$ . Then the group of units with augmentation 1 is given by

$$V(\mathbb{Z}G) \simeq N \rtimes G,$$

where  $N := U(1 + \Delta(A)\Delta(G) + \Delta^2(B))$  is torsion free.

Hereby we set  $\Delta(A) := \langle a - 1 \rangle$  and  $\Delta(B) := \langle b - 1 \rangle$ .

*Proof.* Theorem 4.6 (ii) shows that  $N' := U(1 + \Delta^2(G)) \trianglelefteq V(\mathbb{Z}G)$  with

$$V(\mathbb{Z}G)/N' \simeq C_{p^n} \times C_p.$$

First we show that  $N \times \langle a^{p^n} \rangle \simeq N'$ . With  $I := \Delta(A)\Delta(G) + \Delta^2(B)$  we get

$$(b-1)(a-1) \equiv (b-1)(a-1) - (a-1)(b-1) \equiv ba(1-a^{p^n}) \equiv (1-a^{p^n}) \pmod{I}.$$

and conclude with

$$(1-a^{p^n}) \notin I \text{ and } p \cdot (1-a^{p^n}) \equiv (1+a^{p^n} + \dots + a^{p^n(p-1)})(1-a^{p^n}) = 0 \pmod{I},$$

that  $a^{p^n} \notin N$ , and that  $N$  is of index  $p$  in  $N'$ .

It remains to show that  $N$  is torsion free:

Let  $x \in N$  be a torsion element. Then Theorem 4.6 (i) implies that

$$\alpha : \begin{array}{ccc} \mathbb{Z}G & \rightarrow & \mathbb{Z}C_{p^n} \times C_p \\ x & \mapsto & 1 \end{array}.$$

Since  $x$  is conjugate in  $\widehat{\mathbb{Z}}_p G$  to an element of  $G$  (by a theorem of Weiss [Wei]) we get  $x \sim a^{p^{n \cdot j}}$ . We are done, since  $a^{p^n}$  is central.  $\square$

#### 4.4. Explicit calculations.

**Proposition 4.9.** The elements

$$X := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \text{ and } Y := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

of  $\mathrm{SL}_2(\mathbb{Z})$  are generating a group, which is isomorphic to

$$V = \langle x, y \mid (xy^{-1})^2 = -1, (yx^{-1})^2 = -1 \rangle.$$

*Proof.* One easily checks the relations for the given matrices.

This relations are implying that

$$X \cdot Y = -Y \cdot X^{-1}Y^2 \text{ and } X^{-1} \cdot Y = -Y \cdot Y^{-2}X.$$

It is well known, that  $X$  and  $Y^2$  are generators of a free group  $\Gamma(2)$  [New], (where  $\Gamma(2) \leq \mathrm{PSL}_2(\mathbb{Z})$ , with odd entries on the diagonal and even entries on the codiagonal.) Hence there are no other relations, since one can express  $v \in V$  uniquely as

$$v = (-1)^\varepsilon Y^\tau \gamma, \text{ with } \varepsilon, \tau \in \{0, 1\} \text{ and } \gamma \in \Gamma(2).$$

□

**Theorem 4.10.** The unit group of the twisted group ring  $\mathbb{Z}[i] \rtimes C_2$  is given by

$$U \simeq V \rtimes C_2 := \langle x, y, t \mid (xy^{-1})^2 = -1, t^2 = 1, x^t = x^{-1}, y^t = y^{-1} \rangle.$$

*Proof.* Theorem 3.30 provides that

$$\mathbb{Z}[i] \rtimes C_2 \simeq \Lambda := \left\{ \begin{pmatrix} a & b \\ 2c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, a \equiv d \pmod{2} \right\}.$$

With  $T := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  and Proposition 4.9 one verifies the relations above.

Let  $\Lambda' := \langle X, Y, T \rangle$ . Then one has to show, that

$$\forall \lambda := \begin{pmatrix} a & b \\ 2c & d \end{pmatrix} \in \Lambda^\times \implies \lambda \in \Lambda'.$$

Since  $-1, T \in \Lambda'$  one can assume that  $a, b \geq 0$  and  $\det(\lambda) = 1$  holds. Because of

$$\lambda \cdot X^n = \begin{pmatrix} a+2n \cdot b & b \\ * & * \end{pmatrix} \text{ and } \lambda \cdot Y^m = \begin{pmatrix} a & b+m \cdot a \\ * & * \end{pmatrix}$$

one can apply Euclid's algorithm for the elements of the first row. Since  $\lambda$  is a unit one gets that  $a$  is odd and that  $\gcd(a, b) = 1$ . Hence

$$\exists \lambda' \in \Lambda' : \lambda \cdot \lambda' = \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix} = X^n.$$

□

**Remark 4.11.** (i) There is a split exact short sequence

$$1 \longrightarrow V \longrightarrow \Lambda^* \xrightarrow{\det} \langle -1 \rangle \longrightarrow 1,$$

where a retraction  $\phi$  defined by  $\phi(-1) = T$ .

- (ii) Conjugation with  $W = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$  is an automorphism on  $\Lambda^*$  (see Theorem 4.5), which multiplies  $T$  by  $-1$  and permutes  $X$  and  $Y$ .
- (iii) From  $|\mathrm{PSL}_2(\mathbb{Z})/\Gamma(2)| = 6$ , see [New], and the proof of Proposition 4.9 follows that  $V$  has the index 3 in  $\mathrm{SL}_2(\mathbb{Z})$ .
- (iv) Conjugation with  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  shows, that  $V$  is not normal in  $\mathrm{SL}_2(\mathbb{Z})$ .

Let  $V(RG)$  denote the units in  $RG$  with augmentation 1.

Then again the group ring  $\mathbb{Z}D_4$  is written as a pullback

$$\begin{array}{ccc} \mathbb{Z}D_4 & \longrightarrow & \mathbb{Z}C_2 \times C_2 \\ \downarrow & & \downarrow \\ \mathbb{Z}[i] \rtimes C_2 & \longrightarrow & \mathbb{F}_2C_2 \times C_2 \end{array} .$$

Then the augmentation map  $\epsilon : \mathbb{Z}D_4 \rightarrow \mathbb{Z}$  factors through  $\mathbb{Z}C_2 \times C_2$  and since  $V(\mathbb{Z}C_2 \times C_2) \simeq C_2 \times C_2$  we get a diagram with an exact row

$$\begin{array}{ccccccc} & & & & (\mathbb{Z}[i] \rtimes C_2)^* & & \\ & & & & \downarrow \alpha & & \\ 1 & \longrightarrow & V(\mathbb{Z}C_2 \times C_2) & \xrightarrow{\beta} & (\mathbb{F}_2C_2 \times C_2)^* & \xrightarrow{\gamma} & C_2 \longrightarrow 1, \end{array}$$

where  $\alpha, \beta$  are induced from the factor map mod(2) and  $\gamma$  from the cokernel of  $\beta$ . One easily sees that  $\alpha$  is surjective.

Then Lemma 1.9 (ii) implies  $V(\mathbb{Z}D_4) \simeq \ker \alpha\gamma \leq (\mathbb{Z}[i] \rtimes C_2)^*$ . Theorem 3.11 provides the representations

$$A = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} .$$

By using the representations of Theorem 4.10 we get  $A = XY^{-1}$ ,  $B = XT$  and  $BA = YT$ .

**Theorem 4.12.** Let  $D_4 := \langle a, b \mid a^4 = 1, b^2 = 1, a^b = a^{-1} \rangle$  be the dihedral group. Then the group of units with augmentation 1 of  $\mathbb{Z}D_4$  is given by:

- (i)  $V(\mathbb{Z}D_4) \simeq V' \rtimes C_2$  with

$$V' \simeq \langle x^2, xy^{-1}, y^2 \mid (xy^{-1})^2 = -1, (yx^{-1})^2 = -1 \rangle \quad C_2 = \langle b \rangle$$

and the operations

$$(x^2)^b = x^{-2}, \quad (xy^{-1})^b = (xy^{-1})^{-1}, \quad (y^2)^b = (xy^{-1}) \cdot y^{-2} \cdot (xy^{-1})^{-1}.$$

(ii)  $V(\mathbb{Z}D_4) \simeq V'' \rtimes D_4$ , where  $V''$  is the free group on 3 generators

$$V'' \simeq \langle x^2, y^{-1}x^2y^{-1}, y^2 \rangle$$

and  $D_4 = \langle a, b \mid a^4 = 1, b^2 = 1, a^b = a^{-1} \rangle$  acts via

$$\begin{aligned} (x^2)^a &= y^2 \cdot (y^{-1}x^2y^{-1}) & (y^{-1}x^2y^{-1})^a &= (y^{-1}x^2y^{-1})^{-1} & (y^2)^a &= x^2 \cdot (y^{-1}x^2y^{-1}) \\ (x^2)^b &= x^{-2} & (y^{-1}x^2y^{-1})^b &= x^2 \cdot y^{-2} & (y^2)^b &= (y^{-1}x^2y^{-1})^{-1} \cdot x^{-2}. \end{aligned}$$

*Proof.* (i) One easily computes

$$\alpha(x) = 1 + a + ab, \quad \alpha(y) = 1 + a + b, \quad \alpha(t) = a + b + ab.$$

Hence  $\alpha(V' \rtimes C_2) \subseteq \text{Ker}(\gamma)$ . Since  $V' \rtimes C_2$  is of index 2 in  $(\mathbb{Z}[i] \rtimes C_2)^*$  one just has to check the given operations. This can be done with Theorem 4.10 .

(ii) From  $V' = V'' \cdot \langle a \rangle$  follows  $V'' \cdot D_4 \simeq V(\mathbb{Z}D_4)$ . The operations are again verified by using Theorem 4.10.  $\square$

**Remark 4.13.** (i) The description above is symmetric in  $x$  and  $y$ . Especially one has:

$$y^{-1}x^2y^{-1} = x^{-1}y^2x^{-1}.$$

This equation follows from Theorem 4.12 (i):  $(xy^{-1})^2 = (yx^{-1})^2$ , or from an explicite calculation with matrices.

(ii) The isomorphism  $V(\mathbb{Z}D_4) \simeq V'' \rtimes D_4$  is shown by Jespers and Leal, also by Parmenter, see also [Se]. They give the generators of  $V''$  by bicyclic units, but they don't describe the operation of  $D_4$  on them. Indeed one can easily verify that  $x^2$  and  $y^2$  are bicyclic units, and  $y^{-1}x^2y^{-1}$  is not.

(iii) From Theorem 4.1 follows, that  $T \in \Lambda^*$  provides an automorphism  $\sigma_T$  on  $\mathbb{Z}D_4$ , which is not inner. One computes the following relations for the generators of the free group  $V''$ :

$$b \cdot b^{\sigma_T} = x^2, \quad ab \cdot (ab)^{\sigma_T} = y^2, \quad a^{\sigma_T} a^3 = y^{-1}x^2y^{-1}.$$

Especially the group bases  $D_4$  and  $D_4^{\sigma_T}$  are generating  $V(\mathbb{Z}D_4)$ .

(iv) By denoting the embedding  $\iota : V(\mathbb{Z}D_4) \rightarrow \Lambda^\times$ , one gets the descriptions of  $V(\mathbb{Z}D_4)$  as semi direct products.

Case (i): Let  $\det: \Lambda^* \rightarrow \langle -1 \rangle$ . Then one has the split exact sequence

$$1 \longrightarrow V' \longrightarrow V(\mathbb{Z}D_4) \xrightarrow{\iota \cdot \det} \langle -1 \rangle \longrightarrow 1.$$

Case (ii): Let  $\phi$  be the map induced by the factorization  $\Lambda \rightarrow \Lambda/2\langle W, N \rangle$ .

Then one has the split exact sequence

$$1 \longrightarrow V'' \longrightarrow V(\mathbb{Z}D_4) \xrightarrow{\iota \cdot \phi} \Lambda/2\langle W, N \rangle^\times \longrightarrow 1.$$

5. THE TWISTED GROUP RING  $\Lambda$  AND A BILINEAR FORM

From the following result one reads off the discriminant of  $\Lambda$ . In Chapter 6, this will serve as starting point to construct over orders of  $\Lambda$  in the hereditary  $R$ -order  $\Gamma$ .

In Chapter 7, the result is used to give injective resolutions of certain  $\Lambda$ -lattices, where it turns out, that these resolutions are ‘the same’ as the projective ones. Glueing together these resolutions allows to calculate Tate cohomology.

**Proposition 5.1.** The  $R$ -order  $\Lambda$  is self dual with respect to the following non-degenerate, associative, symmetric bilinear form:

$$\begin{aligned} \langle \cdot, \cdot \rangle : \Lambda \times \Lambda &\rightarrow R \\ (\lambda, \lambda') &\mapsto \frac{1}{p} \text{Tr}(\lambda \lambda') \end{aligned}$$

*Proof.* From Theorem 3.22 it follows that  $\{W^i N^i \mid 0 \leq i < p\}$  is an  $R$ -basis of the diagonal of  $\Lambda$ , and by Corollary 2.24

$$\text{Tr}(W^i N^i) = \sum_{k=0}^{p-i-1} (1-\zeta^{1+k}) \dots (1-\zeta^{i+k}) = p.$$

In particular  $\langle \cdot, \cdot \rangle$  takes values in  $R$ , as claimed.

Let  $0 \leq i, j, k, l < p$ , and assume that  $\text{Tr}(W^i N^j \cdot N^k W^l) \neq 0$ . Then  $j + k < p$  as  $N^p = 0$  or equivalently  $k \in \{0, 1, \dots, p-j-1\}$ .

Since  $\text{Tr}(W^i N^j \cdot N^k W^l) = \text{Tr}(W^l \cdot W^i N^j N^k)$  the matrix  $W^{i+l} N^{j+k}$  lies on the diagonal, which means that  $i + l \equiv j + k \pmod{p}$  or  $l = \overline{j+k-i}$ .

Order the elements of the  $R$ -bases  $\mathfrak{B}'_\Lambda$  and  $\mathfrak{B}_\Lambda$  given in Theorem 3.22 as follows:

$$\begin{aligned} \mathfrak{B}'_\Lambda &= \{b'_1, \dots, b'_{p^2}\} \\ &= \{W^{p-1}N^{p-1}, W^{p-2}N^{p-1}, \dots, W^0N^{p-1}, W^{p-1}N^{p-2}, \dots, W^0N^{p-2}, \dots, W^{p-1}N^0, \dots, W^0N^0\}, \\ \mathfrak{B}_\Lambda &= \{b_1, \dots, b_{p^2}\} \\ &= \{N^0W^0, N^0W^1, \dots, N^0W^{p-1}, N^1W^0, \dots, N^1W^{p-1}, \dots, N^{p-1}W^0, \dots, N^{p-1}W^{p-1}\}. \end{aligned}$$

The matrix  $M := (\langle b'_i, b_j \rangle)$  describes  $\langle \cdot, \cdot \rangle$  with respect to this ordered bases. Then the discussion above shows that  $M$  is a lower triangular  $(p^2 \times p^2)$ -matrix with ones on the diagonal. Hence  $M$  is invertible, and  $\Lambda$  is self dual with respect to  $\langle \cdot, \cdot \rangle$ .  $\square$

**Remark 5.2.** Hence there is the following isomorphism as  $\Lambda$ -left modules between  $\Lambda$  and its contragredient  $(\Lambda_\Lambda)^*$  (see Proposition 9.5 of [CuRe])

$$\begin{aligned}\Lambda &\rightarrow (\Lambda_\Lambda)^* \\ \lambda &\mapsto \langle \cdot, \lambda \rangle.\end{aligned}$$

Since  $\Lambda$  is projective as  $\Lambda$ -right module every short exact sequence of  $\Lambda$ -right modules

$$0 \longrightarrow M \longrightarrow N \longrightarrow \Lambda \longrightarrow 0$$

splits. To get an exact functor  $\text{Hom}_R(\cdot, R)$  we restrict ourselves to the category of  $\Lambda$ -lattices. Now we apply  $\text{Hom}_R(\cdot, R)$  and get the split exact sequence

$$0 \longrightarrow \Lambda^* \longrightarrow N^* \longrightarrow M^* \longrightarrow 0.$$

Since  $\text{Hom}_R(\cdot, R)$  yields a duality between left and right  $\Lambda$ -lattices we conclude that  $\Lambda$  is self-injective in the category of  $\Lambda$ -lattices.

6. OVER ORDERS OF  $\Lambda$ 

In chapter 3, we obtain an embedding of the  $R$ -order  $\Lambda$  in the hereditary  $R$ -order

$$\Gamma := \begin{pmatrix} R & \dots & & R \\ \pi & R & & \vdots \\ \vdots & \ddots & \ddots & \\ \pi & \dots & \pi & R \end{pmatrix}.$$

In this chapter we are concerned with the following questions:

- What is the index  $[\Gamma/\Lambda]$  of  $\Lambda$  in  $\Gamma$ ?
- Is there a generic construction for a chain of orders from  $\Lambda$  to  $\Gamma$  with maximal length?
- Can one describe all intermediate orders between  $\Lambda$  and  $\Gamma$ ?

### 6.1. The radical idealisator process.

For the moment, let us assume that  $R$  is a local Dedekind ring, and that  $\Lambda$  is an arbitrary  $R$ -order in a separable algebra  $A$ .

**Definition 6.1.** Let  $I$  be an two-sided  $\Lambda$ -ideal in  $\Lambda$ .

- (i) The left order of  $I$  is the  $R$ -order

$$\mathfrak{D}_l(I) := \{a \in A \mid a \cdot I \subseteq I\}.$$

Similarly, the right order of  $I$  is the  $R$ -order

$$\mathfrak{D}_r(I) := \{a \in A \mid I \cdot a \subseteq I\}.$$

- (ii) The idealisator of  $I$  is the  $R$ -order

$$\mathfrak{J}(I) := \mathfrak{D}_l(I) \cap \mathfrak{D}_r(I).$$

Set  $\Lambda_0 := \Lambda$  and  $\Lambda_{n+1} := \mathfrak{J}(\text{rad}(\Lambda))$  for  $n \geq 0$ . The radical idealisator chain is the ascending chain  $\Lambda_0 \subsetneq \Lambda_1 \subsetneq \dots$  of  $R$ -orders, which eventually becomes stationary:

$$\Lambda_0 \subsetneq \Lambda_1 \subsetneq \dots \subsetneq \Lambda_N = \Lambda_{N+1}.$$

Then, the  $R$ -order  $\Lambda_N$  is hereditary. (For details, we refer the reader to I. Reiners Maximal Orders [Re] or to [Nebe].)

If the Dedekind ring  $R$  is assumed to have infinitely many prime ideals, then the Jacobson radical of  $\Lambda$  is the zero ideal. In this situation, Benz and Zassenhaus gave the notation of arithmetic radical of  $\Lambda$ . The reader may wish to recall the definition of the discriminant  $d(\Lambda, R)$  of the  $R$ -order  $\Lambda$  from [Re], Section 10.

**Definition 6.2.** (i) The arithmetic radical  $\text{arad}_R(\Lambda)$  of the  $R$ -order  $\Lambda$  is the intersection of the maximal ideals of  $\Lambda$  containing the discriminant  $d(\Lambda, R)$ .

- (ii) We say that the  $R$ -order  $\Lambda$  is arithmetic local if there is a unique maximal ideal of  $\Lambda$  containing the discriminant  $d(\Lambda, R)$ .

Now one has again a radical idealisator process, that is, one can form a radical idealisator chain, using the arithmetic radical instead of the Jacobson radical. Let us return to our situation, where  $R = \mathbb{Z}[\zeta_{p^n}]$  and  $\Lambda \simeq \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$ . Then the discriminant  $d(\Lambda, R)$  is the principal ideal generated by  $\det(\text{Tr}(b_i b_j))$ , where  $\{b_1, \dots, b_{p^2}\}$  is an  $R$ -basis of  $\Lambda$ . Thus it follows from theorem 5.1 that

**Corollary 6.3.** The discriminant of the  $R$ -order  $\Lambda$  is given by

$$d(\Lambda, R) = (p^{p^2}).$$

Likewise, it follows that  $(p)$  is the different of the  $R$ -order  $\Lambda$  (for the definition of the different see [Re], p.150).

**Remark 6.4.** Therefore we get the surprising fact that the different and the discriminant of the  $R$ -order  $\Lambda$  does not depend on  $n$ .

**Proposition 6.5.** The  $R$ -order  $\Lambda$  is arithmetic local, with arithmetic radical

$$\text{arad}_R(\Lambda) = (W, N).$$

*Proof.* Let  $M$  be a maximal ideal containing  $p^{p^2}$ . Since  $W^p = \pi$  and  $N^p = 0$ , the images of  $W$  and  $N$  in  $\Lambda/M$  are nilpotent. Hence  $W, N \in M$ . On the other hand, it follows from Theorem 3.22 that

$$\Lambda/(W, N) \simeq R/\pi \simeq \mathbb{F}_p.$$

So  $M = (W, N) = \text{arad}_R(\Lambda)$ . □

**Definition 6.6.** Set  $\Lambda_0 := \Lambda$  and for  $i \geq 0$

$$\Lambda_{i+1} := \mathfrak{I}(\text{arad}_R(\Lambda_i)).$$

**Remark 6.7.** Since any two elements of  $\Lambda$ , and therefore also any two elements of an over order of  $\Lambda$ , are commuting modulo  $(1-\zeta)$ , one easily sees that

$$\mathfrak{D}_l(\text{arad}_R(\Lambda_i)) = \mathfrak{D}_r(\text{arad}_R(\Lambda_i)).$$

For  $p=2$  and arbitrary  $n \in \mathbb{N}$  we have the following result:

**Theorem 6.8.** Let  $\Lambda \simeq \mathbb{Z}[\zeta_{2^{n+1}}] \rtimes C_2$ .

- (i) The radical idealisator process provides a chain of orders

$$\Lambda = \Lambda_0 \subsetneq \dots \subsetneq \Lambda_{2^n-1} = \Gamma.$$

An  $R$  basis of order  $\Lambda_i$  is given by

$$\begin{aligned}\mathfrak{B}_{2k} &:= \{1, W, \pi^{-k}N, \pi^{-k}NW\} && \text{if } i=2k \text{ is even,} \\ \mathfrak{B}_{2k+1} &:= \{1, W, \pi^{-k}N, \pi^{-(k+1)}NW\} && \text{if } i=2k+1 \text{ is odd.}\end{aligned}$$

For  $i < 2^n - 1$ , the arithmetic radical of  $\Lambda_i$  is given by

$$\begin{aligned}\text{arad}_R(\Lambda_{2k}) &:= {}_R\langle \pi, W, \pi^{-k}N, \pi^{-k}NW \rangle && \text{if } i=2k \text{ is even,} \\ \text{arad}_R(\Lambda_{2k+1}) &:= {}_R\langle \pi, W, \pi^{-k}N, \pi^{-(k+1)}NW \rangle && \text{if } i=2k+1 \text{ is odd.}\end{aligned}$$

with  $i < 2^n - 1$  and for the hereditary order  $\Gamma = \Lambda_{2^n - 1}$  by

$$\text{arad}_R(\Gamma) = \text{arad}_R(\Lambda_{2^n - 1}) = \text{arad}_R(\Lambda_{2^n - 2}).$$

- (ii) The chain of intermediate orders in (i) is of maximal length. Every intermediate order  $\tilde{\Lambda}$  is an element of this chain.

*Proof.* (i) The proof is done by induction on  $i$ . The statement for  $i=0$  follows from Proposition 6.5. Assume that  $i=2k+1$  is odd, and let

$$X := \alpha + \beta W + \gamma N + \delta NW \in \Lambda_{2i+1} \quad (\alpha, \beta, \gamma, \delta \in \mathbb{Q}(\zeta_{p^n})).$$

Inductively, we may assume that  $\text{arad}_R(\Lambda_{2k})$  has an  $R$ -basis as stated, so  $W \in \text{arad}_R(\Lambda_{2k})$  implies that

$$X \cdot W = \alpha W + \beta \pi + \gamma NW + \delta \pi N \in \Lambda_{2k},$$

and hence  $\alpha, \beta, \pi^k \gamma, \pi^{k+1} \delta \in R$ . One easily checks the multiplication of  $X$  with the remaining (basis) elements does not lead to stronger congruences, which give the  $R$ -basis  $B_{2k+1}$  of  $\Lambda_{2k+1}$ . Now the arithmetic radical of  $\Lambda_{2k+1}$  is computed in the same way as  $\text{arad}_R(\Lambda)$  was computed in Proposition 6.5. The case  $i$  is even is treated similar.

- (ii) Let  $\tilde{\Lambda}$  be an intermediate order between  $\Lambda$  and  $\Gamma$ ; we wish to show that  $\tilde{\Lambda} = \Lambda_i$  for some  $0 \leq i \leq 2^{n-1} - 1$ .

Note that  $\pi^{2^{n-1}} = 2u$  for some  $u \in R^\times$ . The  $R$ -order  $\Gamma$  has the  $R$ -basis

$$1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \quad W = \begin{pmatrix} & 1 \\ \pi & \end{pmatrix}, \quad \frac{u}{\pi^{2^{n-1}-1}}N = \begin{pmatrix} & \\ \pi & \end{pmatrix}, \quad \frac{u}{\pi^{2^{n-1}}}WN = \begin{pmatrix} & \\ & 1 \end{pmatrix}.$$

Since  $1, W \in \Lambda \subseteq \tilde{\Lambda}$ , we only need to know what  $R$ -linear combinations of  $\begin{pmatrix} & \\ \pi & \end{pmatrix}$  and  $\begin{pmatrix} & \\ & 1 \end{pmatrix}$  are contained in  $\tilde{\Lambda}$ .

Note that each non-zero element of  $R$  can be written uniquely as  $\alpha \pi^s$  where  $s \geq 0$  and  $\alpha$  has norm  $\text{Nr}_{R/\mathbb{Z}}(\alpha)$  not divisible by 2. Since  $N \in \tilde{\Lambda}$ , there are  $0 \neq \alpha \in R$

and  $\beta \in R$  whose norm, if non-zero, is not divisible by 2 and  $s, t \geq 0$ , such that  $\tilde{\Lambda}$  contains the element

$$X = \alpha\pi^s \begin{pmatrix} \pi \\ 1 \end{pmatrix} + \beta\pi^t \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Choose such an  $X$  with minimal  $s$ . We will show that  $\pi^s \begin{pmatrix} \pi \\ 1 \end{pmatrix} \in \tilde{\Lambda}$ .

Write  $m = \text{Nr}_{R/\mathbb{Z}}(\alpha) = \alpha \cdot \alpha'$ . If  $\beta = 0$  then  $\tilde{\Lambda}$  contains

$$\alpha'X = m \begin{pmatrix} \pi^{s+1} \\ 1 \end{pmatrix} \quad \text{and} \quad \pi^{s+1}N = \pi^{s+1} \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

and since  $(m, 2) = 1$ ,  $\begin{pmatrix} \pi^{s+1} \\ 1 \end{pmatrix}$  is an integral linear combination of these elements, and we are done.

So assume that  $\beta \neq 0$ . Since

$$X \cdot W = \beta\pi^t \begin{pmatrix} \pi \\ 1 \end{pmatrix} + \alpha\pi^{s+1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \tilde{\Lambda},$$

we have  $s \leq t$  since  $s$  is minimal.

If  $s = t$ , then

$$X' := \beta X - \alpha XW = \gamma\pi^s \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \tilde{\Lambda} \quad \text{with} \quad \gamma := \beta^2 - \alpha^2\pi.$$

Write  $n = \text{Nr}_{R/\mathbb{Z}}(\gamma) = \gamma \cdot \gamma'$ . Then  $\tilde{\Lambda}$  contains

$$\gamma'X = n \begin{pmatrix} \pi^s \\ 1 \end{pmatrix} \quad \text{and} \quad \pi^s NW = 2 \begin{pmatrix} \pi^s \\ 1 \end{pmatrix},$$

and since  $(n, 2) = 1$ ,  $\hat{X} := \begin{pmatrix} \pi^s \\ 1 \end{pmatrix}$  is an integral linear combination of these elements.

Hence also  $\hat{X}W = \pi^s \begin{pmatrix} \pi \\ 1 \end{pmatrix} \in \tilde{\Lambda}$ .

If  $s < t$ , then

$$\alpha X - \beta\pi^{t-s-1}XW = (\alpha^2 - \beta^2\pi^{2(t-s)-1}) \begin{pmatrix} \pi^{s+1} \\ 1 \end{pmatrix} \in \tilde{\Lambda},$$

and therefore  $\pi^s \begin{pmatrix} \pi \\ 1 \end{pmatrix} \in \tilde{\Lambda}$  by the already familiar argument.

Now it readily follows that  $\tilde{\Lambda}$  has an  $R$ -basis

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \pi \\ 1 \end{pmatrix}, \begin{pmatrix} \pi^{s+1} \\ 1 \end{pmatrix}, \begin{pmatrix} \pi^t \\ 1 \end{pmatrix}$$

for some  $t \geq s \geq 0$ . From

$$\begin{pmatrix} \pi^{s+1} \\ 1 \end{pmatrix} \begin{pmatrix} \pi \\ 1 \end{pmatrix} = \begin{pmatrix} \pi^{s+1} \\ 1 \end{pmatrix}$$

one gets  $s \leq t \leq s+1$ . The given basis elements of  $\tilde{\Lambda}$  are, up to units of  $R$ , the elements

$$1, \quad W, \quad \frac{1}{\pi^{2^{n-1}-1-s}}N, \quad \frac{1}{\pi^{2^{n-1}-t}}NW.$$

Since  $N \in \tilde{\Lambda}$ , we have  $s \leq 2^{n-1} - 1$ . Altogether, we have

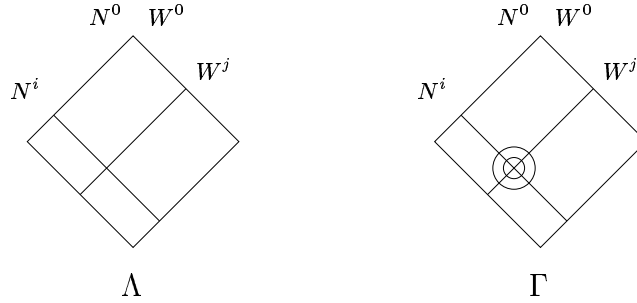
$$0 \leq s \leq t \leq s + 1 \leq 2^{n-1} - 1,$$

and each of the  $2^n$  possible choices for  $s, t$  gives one of the orders  $\Lambda_0, \dots, \Lambda_{2^n-1}$ . As a trivial consequence, the chain  $\Lambda_0 \subseteq \dots \subseteq \Lambda_{2^n-1}$  is maximal.  $\square$

The radical idealisator process does not yield a satisfactory result when  $p$  is odd, because we do not get a chain of over orders of maximal length. This is illustrated by the example of remark 6.30 (ii), where we use a graphical description of intermediate orders, which we introduce in the following.

## 6.2. Embedding of twisted group rings in hereditary orders.

Now we give a graphical description of the  $R$ -order  $\Lambda$ , with respect to the  $R$ -basis of Theorem 3.22 (i). Therefore we use the following diagram, whereby the position  $(i, j)$  corresponds to  $N^i W^j$ . One can use the same diagram to describe intermediate orders between  $\Lambda$  and the hereditary over-order  $\Gamma$  by adjoining 'some' circles to the position  $(i, j)$ , where  $\nu(i, j)$  circles are corresponding to the element  $N^i W^j / \pi^{\nu(i, j)}$ :



Now we give some rules for intermediate orders, which we will need in the following.

**Lemma 6.9.** Let  $\tilde{\Lambda}$  be an intermediate order (i.e.  $\Lambda \subseteq \tilde{\Lambda} \subseteq \Gamma$ ), which can be described by adjoining circles to a diagram and denoting  $\nu(i, j)$  the number of circles at the position  $(i, j)$ . For  $0 \leq i, j, k < p$  we get:

- (i) Let  $j \leq k$ . Then  $\nu(i, j) \leq \nu(i, k)$ .
- (ii) Let  $0 \leq i \leq p-1$ . Then  $\nu(i, p-1) - \nu(i, 0) \leq 1$ .
- (iii) Let  $i \leq k$ . Then  $\nu(i, j) \leq \nu(k, j)$ .
- (iv) Let  $i \geq 1$ . Then  $\nu(i, j) - \nu(i-1, j) \leq p^{n-1}$ .

*Proof.* Since  $N, W \in \tilde{\Lambda}$ , one concludes :

(i) Obviously

$$\frac{N^i W^j}{\pi^{\nu(i, j)}} \cdot W^{k-j} = \frac{N^i W^k}{\pi^{\nu(i, j)}} \in \tilde{\Lambda}.$$

By assumption there is the following  $R$ -basis of  $\tilde{\Lambda}$

$$\left\{ \frac{N^r W^s}{\pi^{\nu(r,s)}} \mid 0 \leq r, s < p \right\},$$

and hence there exist an  $r \in R$  such that

$$\frac{N^i W^k}{\pi^{\nu(i,j)}} = r \cdot \frac{N^i W^k}{\pi^{\nu(i,k)}}.$$

Hence  $\nu(i, j) \leq \nu(i, k)$ .

(ii) From

$$\frac{N^i W^{p-1}}{\pi^{\nu(i,p-1)}} \cdot W = \frac{N^i}{\pi^{\nu(i,j)-1}} \in \tilde{\Lambda},$$

follows, as in part (i), that  $\nu(i, p-1) - 1 \leq \nu(i, 0)$ .

(iii) It is proved as part (i) by analyzing the product

$$N^{k-i} \cdot \frac{N^i W^j}{\pi^{\nu(i,j)}} = \frac{N^k W^j}{\pi^{\nu(i,j)}} \in \tilde{\Lambda}.$$

(iv) Theorem 3.23 shows that  $W \cdot N^i = \zeta^i N^i W + (1 - \zeta^i) N^{i-1}$  and hence

$$W \cdot \frac{N^i W^j}{\pi^{\nu(i,j)}} = \zeta^i \cdot \frac{N^i W^{j+1}}{\pi^{\nu(i,j)}} + (1 - \zeta^i) \cdot \frac{N^{i-1} W^j}{\pi^{\nu(i,j)}},$$

where both summands are elements of  $\tilde{\Lambda}$ . Then we consider the second summand and are done with the even well known arguments as above and since  $(1 - \zeta^i)$  is totally ramified over  $\pi$  of degree  $p^{n-1}$ .  $\square$

**Theorem 6.10.** (i) The  $R$ -order  $\Gamma$  has the  $R$ -basis  $\{b_{i,j}\}$  for  $0 \leq i, j < p$  and

$$b_{i,j} := \frac{N^i W^j}{\pi^{\nu(i,j)}}, \text{ with } \nu(i, j) = \begin{cases} i \cdot p^{n-1} & \text{if } i \leq j, \\ i \cdot p^{n-1} - 1 & \text{if } i > j. \end{cases}$$

(ii) The index of the  $R$ -order  $\Lambda$  in the hereditary  $R$ -order  $\Gamma$  is given by

$$|\Gamma/\Lambda| = p^{(p^n-1)\binom{p}{2}}.$$

*Proof.* (i) First we show that  $b_{i,j} \in \Gamma$ :

The elements  $N^i$  and  $W^j$  are lying on the  $\overline{p-i}$ -th and on the  $j$ -th diagonal with

entries

$$(N^i)_{[l+i],l} = \begin{cases} (1-\zeta^l)(1-\zeta^{l+1})\cdots(1-\zeta^{l+i-1}), & \text{if } l \leq p-i, \\ 0 & \text{else,} \end{cases}$$

$$(W^j)_{l,[l+j]} = \begin{cases} 1 & \text{if } l \leq p-j, \\ \pi & \text{if } l > p-j. \end{cases}$$

Now we define  $\sigma_{j,l} := 1$  if  $l \leq p-j$  and  $\sigma_{j,l} := \pi$  if  $l > p-j$ . Then  $N^i W^j$  lies on the  $\overline{j-i}$ -th diagonal where the non zero entries are given, if  $l \leq p-i$ , by

$$(*) \quad (N^i W^j)_{[l+i],[l+j]} = (1-\zeta^l)(1-\zeta^{l+1})\cdots(1-\zeta^{l+i-1})\sigma_{j,l}.$$

Since for  $0 < k < p$  the element  $1 - \zeta^k$  is totally ramified over the prime  $\pi := 1 - \zeta_{p^n} \in R$  of degree  $p^{n-1}$  we get

$$\pi^{-i \cdot p^{n-1}} \cdot N^i W^j \in (R)_{p \times p}.$$

Obviously we have  $\pi^{-(i \cdot p^{n-1} - 1)} \cdot N^i W^j \in \Gamma$ . Now we prove

$$\pi^{-i \cdot p^{n-1}} \cdot N^i W^j \in \Gamma \iff i \leq j :$$

Now we have to verify that the entries beyond the diagonal of the matrix  $\pi^{-i \cdot p^{n-1}} \cdot N^i W^j$  are divisible by  $\pi$  if and only if  $i \leq j$ . By the discussion above we just have to consider  $l \in \{1, \dots, p-i\}$  :

For  $i \leq j$  we conclude from  $[l+i] > [l+j]$  that  $l+j > p$ , which shows that  $\sigma_{j,l} = \pi$ , and we are done by formula (\*).

Since  $l \in \{1, \dots, p-i\}$  we conclude for  $i > j$  that  $p-l \geq i > j$ , which shows that  $\sigma_{j,l} = 1$ , and we are done with formula (\*).

Hence  $b_{i,j} \in \Gamma$ . It remains to show that

$$\mathfrak{B}_k := \{b_{0,k}, b_{1,k+1}, \dots, b_{p-k-1,p-1}, b_{p-k,0}, \dots, b_{p-1,k-1}\}$$

is an  $R$ -basis of the  $k$ -th diagonal.

For  $0 \leq i, j < p$  we define the  $p \times p$ -matrices

$$(\tilde{b}_{i,j})_{k+1,l+1} := \begin{cases} \pi \cdot \delta_{i,k} \cdot \delta_{j,l} & \text{if } i > j, \\ \delta_{i,k} \cdot \delta_{j,l} & \text{otherwise,} \end{cases}$$

and get obviously an  $R$ -basis for the  $k$ -th diagonal of  $\Gamma$  by

$$\tilde{\mathfrak{B}}_k := \{\tilde{b}_{0,k}, \tilde{b}_{1,k+1}, \dots, \tilde{b}_{p-k-1,p-1}, \tilde{b}_{p-k,0}, \dots, \tilde{b}_{p-1,k-1}\}.$$

Now let  $J_k$  be the matrix, which  $(l+1)$ -th column coincides with  $k$ -th diagonal of  $b_{l,[l+k]}$  and  $\tilde{J}_k$  the matrix, which  $(l+1)$ -th column coincides with  $k$ -th diagonal of  $\tilde{b}_{l,[l+k]}$ .

We get  $\tilde{J}_k = \tilde{D}_k$ , see Definition 3.26, and that  $J_k$  is a lower triangular  $p \times p$ -matrix with the following entries on the diagonal:

$$(J_k)_{l+1,l+1} = \begin{cases} \pi^{-lp^{n-1}} \cdot (1-\zeta) \cdots (1-\zeta^l) & \text{if } l < p-k, \\ \pi^{-(lp^{n-1}-1)} \cdot (1-\zeta) \cdots (1-\zeta^l) & \text{otherwise.} \end{cases}$$

Since

$$\frac{(1-\zeta) \cdots (1-\zeta^l)}{\pi^{lp^{n-1}}} \in R^\times$$

we conclude that

$$J_k \cdot \tilde{D}_k^{-1} \in \text{Gl}_p(R)$$

describes the basis transformation from  $\tilde{\mathfrak{B}}_k$  to  $\mathfrak{B}_k$ .

(ii) With the formula of (i) there are

$$\sum_{j=0}^{i-1} (ip^{n-1} - 1) + \sum_{j=i}^{p-1} ip^{n-1} = i(ip^{n-1} - 1) + (p-i)ip^{n-1} = i(p^n - 1)$$

circles in the line of to  $N^i$ . We are done since  $\sum_{i=0}^{p-1} i = \binom{p}{2}$  and  $R/\pi \simeq \mathbb{F}_p$ .  $\square$

**Corollary 6.11.** (i) There is the following identity of  $R$ -orders:  $\Gamma = \Lambda \left[ \frac{NW}{1-\zeta} \right]$ .

(ii) There is an  $R$ -basis of  $\Gamma$  given by  $\left\{ \left( \frac{NW}{1-\zeta} \right)^i W^j \mid 0 \leq i, j < p \right\}$ .

*Proof.* (i) We have that  $(1-\zeta)^i$  is totally ramified over  $\pi$  of degree  $ip^{n-1}$ . Then Theorem 6.10 (i) and Lemma 6.9 (i), (ii) show that

$$\Gamma = \Lambda \left[ \frac{NW}{1-\zeta}, \frac{N^2W^2}{(1-\zeta)^2}, \dots, \frac{N^{p-1}W^{p-1}}{(1-\zeta)^{p-1}} \right].$$

Now we show inductively that

$$(NW)^i = \sum_{j=1}^i r_{i,j} N^j W^j$$

with  $r_{i,i} \in R^\times$ , explicetely  $r_{i,i} = \zeta \cdot \zeta^2 \cdots \zeta^{i-1}$ .

This is trivially true for  $i = 1$ . Now let the statement hold for  $i$ . Then

$$(NW)^{i+1} = (NW)^i \cdot NW = \sum_{j=1}^i r_{i,j} N^j W^j \cdot NW,$$

with  $r_{i,i} = \zeta \zeta^2 \dots \zeta^{i-1}$ . Now Theorem 3.23 shows that

$$W^i \cdot N = \zeta^i N W^i + (1 - \zeta^i) W^{i-1}$$

and hence  $r_{i+1,i+1} = r_{i,i} \cdot \zeta^i = \zeta \dots \zeta^{i-1} \zeta^i$ .

(ii) Theorem 6.10 (i) shows that an  $R$ -basis of  $\Gamma$  is given by the elements

$$\gamma_{i,j} := \begin{cases} \frac{N^i W^i}{(1-\zeta)^i} \cdot W^{j-i} & \text{if } 0 \leq i \leq j < p, \\ \frac{N^i W^i}{(1-\zeta)^i} \cdot W^{p+j-i} & \text{if } 0 \leq j < i < p. \end{cases}$$

Then the proof of part (i) shows that it does not matter, whether one considers elements  $N^i W^i$  or  $(NW)^i$ .  $\square$

### 6.3. Ideals in hereditary orders.

For the rest of this section we will construct a generic chain of over-orders from  $\Lambda$  to  $\Gamma$ . For this we will need a chain of two-sided  $\Gamma$ -ideals.

So first we will study those  $\Gamma$ -ideals which we can describe by the same diagrams as before, explicitly let  $\mathfrak{I}$  an two-sided  $\Gamma$ -ideal which has an  $R$ -basis of the form

$$\{\pi^{\mu(i,j)} N^i W^j \mid 0 \leq i, j < p, \mu(i, j) \in \mathbb{Z}\}.$$

Since  $\mathfrak{I} \subseteq \Gamma$  we conclude from Theorem 6.10 (i) that  $\mu(i, j) \geq -\nu(i, j)$ .

**Proposition 6.12.** Let  $\mathfrak{L}$  be an  $R$ -sub-lattice of  $\Gamma$  with  $R$ -basis

$$\{\pi^{\mu(i,j)} N^i W^j \mid 0 \leq i, j < p, \mu(i, j) \geq -\nu(i, j)\}.$$

Then  $\mathfrak{L}$  is an two-sided  $\Gamma$ -ideal if and only if the following conditions are satisfied

- (i)  $\mu(i, 0) \geq \mu(i, 1) \geq \dots \geq \mu(i, p-1) \geq \mu(i, 0) - 1$ .
- (ii) For  $i > 0$  we have  $\mu(i, j) + p^{n-1} \geq \mu(i-1, j)$ .
- (iii) For  $i, j < p-1$  we have  $\mu(i, j) \geq \mu(i+1, j+1) + p^{n-1}$  and also  $\mu(i, p-1) + 1 \geq \mu(i+1, 0) + p^{n-1}$ .

*Proof.* Let  $\mathfrak{L}$  be an two-sided  $\Gamma$ -ideal. Then we get:

(i) The equation

$$\pi^{\mu(i,j)} N^i W^j \cdot W = \pi^{\mu(i,j)-\mu(i,j+1)} \cdot \pi^{\mu(i,j+1)} N^i W^{j+1} \in \mathfrak{L}$$

shows that  $\mu(i, j) \geq \mu(i, j+1)$  for  $j < p-1$  and  $\mu(i, p-1) \geq \mu(i, 0) - 1$  since  $W^p = \pi$ .

(ii) Theorem 3.23 shows for  $i > 0$  that

$$\begin{aligned} W \cdot \pi^{\mu(i,j)} N^i W^j \\ = \zeta^i \cdot \pi^{\mu(i,j)} N^i W^{j+1} + \frac{1 - \zeta^i}{\pi p^{n-1}} \cdot \pi^{\mu(i,j)+p^{n-1}} N^{i-1} W^j. \end{aligned}$$

Since an  $R$ -basis of  $\mathfrak{L}$  can be taken as above we conclude that especially the second summand is an element of  $\mathfrak{L}$ . Now  $\frac{1-\zeta^i}{\pi p^{n-1}} \in R^\times$  shows that  $\mu(i, j) + p^{n-1} \geq \mu(i-1, j)$ .

(iii) Theorem 3.23 shows that

$$\begin{aligned} & \pi^{\mu(i,j)} N^i W^j \cdot \frac{NW}{1-\zeta} \\ &= \frac{\pi^{\mu(i,j)-\mu(i+1,j+1)}}{1-\zeta} \zeta^j \cdot \pi^{\mu(i+1,j+1)} N^{i+1} W^{j+1} + \frac{1-\zeta^j}{1-\zeta} \cdot \pi^{\mu(i,j)} N^i W^j. \end{aligned}$$

With the same argument as above we have that the first summand is an element of  $\mathfrak{L}$ . Since  $1-\zeta$  is totally ramified over  $\pi$  of degree  $p^{n-1}$  we get, using the notation of Definition 3.15:

$$\mu(i, j) - \mu(i+1, \overline{j+1}) \geq \begin{cases} p^{n-1} & \text{if } j < p-1 \\ p^{n-1} - 1 & \text{if } j = p-1 \end{cases}.$$

So one direction of the proof is done.

By using Corollary 6.11 (ii) we show that a given  $R$ -basis, which satisfies the conditions (i),(ii) and (iii), is closed under multiplying by  $W$  and  $\frac{NW}{1-\zeta}$ :

(Therefore we use the same equations as in the first part of the proof.)

We get from (i) for  $j < p-1$  that

$$\pi^{\mu(i,j)} N^i W^j \cdot W = \pi^{\mu(i,j)-\mu(i,j+1)} \cdot \pi^{\mu(i,j+1)} N^i W^{j+1} \in \mathfrak{L},$$

since  $\mu(i, j) \geq \mu(i, j+1)$ . Let  $j = p-1$ . Then we get

$$\pi^{\mu(i,p-1)} N^i W^{p-1} \cdot W = \pi^{\mu(i,p-1)+1-\mu(i,0)} \cdot \pi^{\mu(i,0)} N^i W^0 \in \mathfrak{L},$$

since  $\mu(i, p-1) + 1 \geq \mu(i, 0)$ .

The left-multiplication by  $W$  is handled as in Lemma 6.9 (iv):

Theorem 3.23 shows that

$$\begin{aligned} & W \cdot \pi^{\mu(i,j)} N^i W^j \\ &= \zeta^i \cdot \pi^{\mu(i,j)} N^i W^{j+1} + \frac{1-\zeta^i}{\pi p^{n-1}} \cdot \pi^{\mu(i,j)+p^{n-1}} N^{i-1} W^j. \end{aligned}$$

The first summand is element of  $\mathfrak{L}$ , because  $\mathfrak{L}$  is closed under right multiplication by  $W$  and the second summand because  $\frac{1-\zeta^i}{\pi p^{n-1}} \in R$  and  $\mu(i, j) + p^{n-1} \geq \mu(i-1, j)$  by (ii).

For the right-multiplication with  $\frac{NW}{1-\zeta}$  we get from Theorem 3.23 that

$$\begin{aligned} & \pi^{\mu(i,j)} N^i W^j \cdot \frac{NW}{1-\zeta} \\ &= \frac{\pi^{\mu(i,j)-\mu(i+1,j+1)}}{1-\zeta} \zeta^j \cdot \pi^{\mu(i+1,j+1)} N^{i+1} W^{j+1} + \frac{1-\zeta^j}{1-\zeta} \cdot \pi^{\mu(i,j)} N^i W^j. \end{aligned}$$

The second summand is element of  $\mathfrak{L}$  since  $\frac{1-\zeta^j}{1-\zeta} \in R$ . Also the first summand is element of  $\mathfrak{L}$  since by (iii)  $\mu(i,j) - \mu(i+1,j+1) \geq p^{n-1}$  and since  $1-\zeta$  is totally ramified over  $\pi$  of degree  $p^{n-1}$ . The case  $j = p-1$  follows with  $W^p = \pi$ .

The left-multiplication by  $\frac{NW}{1-\zeta}$  is handled similar.  $\square$

Now we give an equivalent criterium, to decide whether  $R$ -lattices are even  $\Gamma$ -ideals. We can use this new criterium to identify some  $R$ -lattices as  $\Gamma$ -ideals and use them to construct a chain of intermediate orders of maximal length from  $\Lambda$  to  $\Gamma$ .

**Proposition 6.13.** Let  $\mathfrak{L}$  be an  $R$ -sub-lattice of  $\Gamma$  with  $R$ -basis

$$\{\pi^{\mu(i,j)} N^i W^j \mid 0 \leq i, j < p, \mu(i,j) \geq -\nu(i,j)\}.$$

Then  $\mathfrak{L}$  is an two-sided  $\Gamma$ -ideal if and only if the following conditions are satisfied:

(i')  $\mathfrak{L}$  is free as  $R[W]$ -right-module of rank  $p$  with basis

$$\{\pi^{\mu(i,j(i))} N^i W^{j(i)} \mid 0 \leq i < p\}.$$

Hereby  $0 \leq j(i) < p$  is defined as follows:

If  $\mu(i,0) = \mu(i,1) = \dots = \mu(i,p-1)$  then  $j(i) := 0$ ,

else let  $j(i)$  be determined by  $\mu(i, j(i)-1) - \mu(i, j(i)) = 1$ .

(ii') Let  $i > 0$ . Then  $j(i) = j(i-1)$  or

$$j(i) = \begin{cases} j(i-1) + 1 & \text{if } j(i-1) < p-1 \\ 0 & \text{if } j(i-1) = p-1 \end{cases}$$

(iii') Let  $i > 0$ . Then we have that

$$\mu(i-1, j(i-1)) = \mu(i, j(i)) + p^{n-1}, \quad (\alpha)$$

except in the case  $j(i) = 0$  and  $j(i-1) = p-1$ , where we get

$$\mu(i-1, j(i-1)) = \mu(i, j(i)) + p^{n-1} - 1. \quad (\beta)$$

*Proof.* With Proposition 6.12 we have to show that the conditions (i),(ii) and (iii), which are given there, are equivalent to (i'),(ii') and (iii').

First let us assume that the conditions (i),(ii) and (iii) are satisfied.

(i'): From (i) follows that  $j(i)$  is well-defined. Then we get for  $0 \leq k < p$  that

$$\pi^{\mu(i,j(i))} N^i W^{j(i)} \cdot W^k = \begin{cases} \pi^{\mu(i,j(i)+k)} N^i W^{j(i)+k} & \text{if } j(i) + k < p, \\ \pi^{\mu(i,j(i)+k-p)} N^i W^{j(i)+k-p} & \text{else,} \end{cases}$$

where we identify  $W^p = \pi \in R$ .

(ii'): Let  $j > 0$ . We conclude from (ii) and (iii) the following equation

$$\mu(i-1, j-1) \geq \mu(i, j) + p^{n-1} \geq \mu(i-1, j),$$

and (i') shows that these three terms are equal exactly if  $j \neq j(i-1)$ , especially we have

$$(*)' \quad j \neq j(i-1) : \mu(i-1, j) - \mu(i, j) = p^{n-1}.$$

Let  $j = j(i-1) > 0$ , hence

$$\mu(i-1, j-1) - \mu(i-1, j) = 1.$$

Then there are two cases.

Let case (I) be given by

$$\mu(i-1, j-1) > \mu(i, j) + p^{n-1} = \mu(i-1, j), \quad (\alpha_1)$$

we conclude that

$$\mu(i-1, j-1) - \mu(i, j) = p^{n-1} + 1.$$

Since (ii) implies that  $\mu(i-1, j-1) - \mu(i, j-1) \leq p^{n-1}$ , we get

$$\mu(i, j-1) - \mu(i, j) = 1$$

and hence  $j(i) = j(i-1)$ .

Now we consider case (II) :

$$\mu(i-1, j-1) = \mu(i, j) + p^{n-1} > \mu(i-1, j).$$

Then  $\mu(i-1, j-1) = \mu(i-1, j) + 1$  implies that

$$(*) : \mu(i-1, j) - \mu(i, j) = p^{n-1} - 1.$$

For  $j < p-1$  we conclude from  $j+1 \neq j := j(i-1)$  that  $\mu(i-1, j+1) = \mu(i-1, j)$  and with statement (\*) that  $\mu(i-1, j+1) - \mu(i, j+1) = p^{n-1}$ . This shows us

$$(**) : \mu(i-1, j) - \mu(i, j+1) = p^{n-1}. \quad (\alpha_2)$$

The difference of the last equations (\*\*) and (\*) gives

$$(**) - (*) : \mu(i, j) - \mu(i, j+1) = 1,$$

and hence we get  $j(i) = j(i-1) + 1$ .

If  $j = p-1$  we have  $\mu(i, p-1) \geq \mu(i, 0)$  since

$$\begin{aligned} \mu(i, p-1) + p^{n-1} &= \mu(i-1, p-2) && \text{(case (II))} \\ &= 1 + \mu(i-1, p-1) && (j = p-1) \\ &\geq \mu(i, 0) + p^{n-1} && \text{(iii)}. \end{aligned} \tag{\beta}$$

Then (i) shows  $\mu(i, p-1) = \mu(i, 0)$  and  $j(i) = 0$ .

Hence we showed (ii') for the case  $j(i-1) > 0$ .

Now we conclude from (ii) and (iii) the following equation

$$1 + \mu(i-1, p-1) \geq \mu(i, 0) + p^{n-1} \geq \mu(i-1, 0),$$

and (i') shows that these three terms are equal exactly if  $j(i-1) \neq 0$ .

Now let  $j(i-1) = 0$ . As above there are two cases: The case  $(I)_0$  is given by

$$1 + \mu(i-1, p-1) > \mu(i, 0) + p^{n-1} = \mu(i-1, 0). \tag{\alpha_3}$$

With (\*') we have also for  $j > 0$

$$\mu(i, j) + p^{n-1} = \mu(i-1, j).$$

Then  $j(i-1) = 0$  provides

$$\mu(i-1, 0) = \mu(i-1, 1) = \dots = \mu(i-1, p-1),$$

hence also

$$\mu(i, 0) = \mu(i, 1) = \dots = \mu(i, p-1),$$

which shows  $j(i) = 0$ .

The case  $(II)_0$  is given by

$$1 + \mu(i-1, p-1) = \mu(i, 0) + p^{n-1} > \mu(i-1, 0)$$

which implies

$$(*)_0 : \mu(i-1, 0) - \mu(i, 0) = p^{n-1} - 1.$$

Then (\*') shows, since  $j(i-1) = 0$ , that

$$(**)_0 : \mu(i-1, 1) - \mu(i, 1) = p^{n-1}. \tag{\alpha_4}$$

Hence the difference between  $(**)_0$  and  $(*)_0$ , by using  $\mu(i-1, 0) = \mu(i-1, 1)$ , gives

$$\mu(i, 0) - \mu(i, 1) = 1,$$

so we get  $j(i) = 1$ . Hence (ii') is proved.

(iii') There are four cases, proved in (ii'), which together give equation  $(\alpha)$ .

Hereby we set again  $j := j(i-1)$ .

(1): In case (I) we have for  $j := j(i-1) > 0$  that

$$\mu(i, j) + p^{n-1} = \mu(i-1, j), \quad (\alpha_1)$$

with  $j(i) = j(i-1)$ .

(2): In case (II) we have for  $0 < j < p-1$  that

$$\mu(i-1, j) - \mu(i, j+1) = p^{n-1}, \quad (\alpha_2)$$

with  $j(i) = j(i-1) + 1$ .

Hence it remains to prove  $(\alpha)$  for  $j(i-1) = 0$ .

(3): In case (I<sub>0</sub>) we get  $j(i) = 0$  and the equation

$$\mu(i, 0) + p^{n-1} = \mu(i-1, 0). \quad (\alpha_3)$$

(4): In case (II<sub>0</sub>) we have  $j(i) = 1$  and

$$\mu(i-1, 1) - \mu(i, 1) = p^{n-1} \quad (\alpha_4)$$

Then we are done, because for  $j(i-1) = 0$  holds  $\mu(i-1, 0) = \mu(i-1, 1)$ .

(β): In case (II) we get for  $j := j(i-1) = p-1$  that

$$\mu(i, p-1) + p^{n-1} = 1 + \mu(i-1, p-1) \quad (\beta)$$

and  $j(i) = 0$ , which shows that  $\mu(i, 0) = \mu(i, p-1)$  and we conclude

$$\mu(i-1, p-1) = \mu(i, 0) + p^{n-1} - 1.$$

Hence we proved (iii').

Now we assume the conditions (i'), (ii') and (iii').

(i): Since  $\{W^k \mid 0 \leq k < p\}$  is a  $R$ -basis of  $R[W]$  we get with (i') the following  $R$ -basis of  $\mathfrak{L}$

$$\{\pi^{\mu(i, j(i))} N^i W^{j(i)+k} \mid 0 \leq i, k < p\}.$$

By assumption there is an  $R$ -basis of  $\mathfrak{L}$  given by

$$\{\pi^{\mu(i, j)} N^i W^j \mid 0 \leq i, j < p\}.$$

Hence we get

$$(***) \quad \mu(i, k) = \begin{cases} \mu(i, j(i)) & \text{if } j(i) \leq k < p \\ \mu(i, j(i)) + 1 & \text{if } 0 \leq k < j(i) \end{cases}$$

which shows that

$$\mu(i, 0) \geq \mu(i, 1) \geq \dots \geq \mu(i, p-1) \geq \mu(i, 0) - 1.$$

(ii): We assume  $i > 0$ . Then by (ii') there are three cases.

For  $j := j(i) = j(i-1)$  we get with (iii') that

$$\mu(i-1, j) = \mu(i, j) + p^{n-1}.$$

Now (\*\*\*) implies

$$\mu(i-1, k) = \mu(i, k) + p^{n-1} \text{ for } 0 \leq k < p,$$

and we have verified (ii) in the first case.

For  $j(i) = j(i-1) + 1$  we show the equation of (ii),  $\mu(i-1, k) \leq \mu(i, k) + p^{n-1}$ , by considering the cases  $k = j(i-1)$ ,  $k \geq j(i)$  and  $k < j(i-1)$ .

Now we recall equation ( $\alpha$ ), given in (iii'):

$$\mu(i-1, j(i-1)) = \mu(i, j(i)) + p^{n-1}. \quad (\alpha)$$

By definition we get

$$\mu(i, j(i-1)) = \mu(i, j(i)) + 1,$$

and hence we get, after summing  $p^{n-1}$  to the last and 1 to equation ( $\alpha$ ):

$$\mu(i-1, j(i-1)) < \mu(i-1, j(i-1)) + 1 = \mu(i, j(i-1)) + p^{n-1}.$$

Now (\*\*\*) shows for  $k$ , with  $j(i) \leq k < p$ , that  $\mu(i-1, k) = \mu(i-1, j(i-1))$  and  $\mu(i-1, k) = \mu(i, j(i))$ , hence ( $\alpha$ ) shows

$$\mu(i-1, k) = \mu(i, k) + p^{n-1} \text{ for } j(i) \leq k < p.$$

Similar (\*\*\*) shows for  $0 \leq k < j(i-1)$  that  $\mu(i-1, k) = \mu(i-1, j(i-1)) + 1$  and  $\mu(i, k) = \mu(i, j(i)) + 1$ , hence ( $\alpha$ ) shows

$$\mu(i-1, k) = \mu(i, k) + p^{n-1} \text{ for } 0 \leq k < j(i-1).$$

For  $j(i) = 0$  and  $j(i-1) = p-1$  we consider equation ( $\beta$ ) of (iii'):

$$\mu(i-1, p-1) = \mu(i, 0) + p^{n-1} - 1.$$

Then  $j(i) = 0$  implies that  $\mu(i, 0) = \mu(i, 1) = \dots = \mu(i, p-1)$ , hence

$$\mu(i-1, p-1) = \mu(i, p-1) + p^{n-1} - 1 < \mu(i, p-1) + p^{n-1},$$

and  $j(i-1) = p-1$  shows that  $\mu(i-1, k) = \mu(i-1, p-1) + 1$  for  $0 \leq k < p-1$ , hence

$$\mu(i-1, k) = \mu(i, k) + p^{n-1}.$$

So in all cases we have for  $i > 0$  that

$$\mu(i, j) + p^{n-1} \geq \mu(i-1, j).$$

(iii) The proof of this part is done by similar arguments as in part(ii).

Again we use the equation  $(\alpha)$  of (iii'), which is equivalent to

$$\mu(i, j(i)) = \mu(i+1, j(i+1)) + p^{n-1}. \quad (\alpha')$$

With (ii') we have to consider some different cases.

First let  $j := j(i) = j(i+1)$ .

For  $j \leq k < p-1$  we have  $\mu(i, k) = \mu(i, j)$  and  $\mu(i+1, k+1) = \mu(i+1, j)$  hence  $(\alpha')$  implies that

$$\mu(i, k) = \mu(i+1, k+1) + p^{n-1}.$$

For  $j > 0$  we need to consider additional cases: With the equation

$$\mu(i, j-1) = \mu(i, j) + 1,$$

and  $(\alpha')$  we conclude that

$$\mu(i, j-1) > \mu(i, j-1) - 1 = \mu(i+1, j) + p^{n-1}.$$

For  $k < j-1$  we get that  $\mu(i, k) = \mu(i, j) + 1$  and  $\mu(i+1, k+1) = \mu(i+1, j) + 1$ . Hence again  $(\alpha')$  implies

$$\mu(i, k) = \mu(i+1, k+1) + p^{n-1},$$

which provides the first equation of (iii) in the case  $j := j(i) = j(i+1)$ .

Now we consider the second equation of (iii) in this case:

We have  $\mu(i, p-1) = \mu(i, j)$  and  $\mu(i+1, 0) = \mu(i+1, j) + 1$  for  $j > 0$ . Hence  $(\alpha')$  implies for  $j > 0$  that

$$\mu(i, p-1) + 1 = \mu(i+1, 0) + p^{n-1},$$

and for  $j = 0$  we get

$$\mu(i, p-1) + 1 > \mu(i, p-1) = \mu(i+1, 0) + p^{n-1}.$$

With (ii') we consider the case  $j(i+1) = j(i) + 1 \leq p-1$ .

For  $j(i) \leq k < p-1$  we get  $\mu(i, k) = \mu(i, j(i))$  and  $\mu(i+1, k+1) = \mu(i+1, j(i+1))$ , and hence with  $(\alpha')$  that

$$\mu(i, k) = \mu(i+1, k+1) + p^{n-1}.$$

For  $0 \leq k < j(i)$  we get  $\mu(i, k) = \mu(i, j(i)) + 1$  and  $\mu(i+1, k+1) = \mu(i+1, j(i+1)) + 1$ , hence again with  $(\alpha')$  that

$$\mu(i, k) = \mu(i+1, k+1) + p^{n-1}.$$

Now we prove the second equation of (iii) in the case  $j(i+1) = j(i) + 1 \leq p-1$ : Again we have  $\mu(i, p-1) = \mu(i, j)$  and  $\mu(i+1, 0) = \mu(i+1, j) + 1$  since  $j(i+1) > 0$ . So we get with equation  $(\alpha')$  that

$$\mu(i, p-1) + 1 = \mu(i+1, 0) + p^{n-1}.$$

In the case  $j(i+1) = 0$  and  $j(i) = p-1$ , we get by the equation  $(\beta)$  of (iii') that

$$\mu(i, p-1) + 1 = \mu(i+1, 0) + p^{n-1},$$

the second equation of (iii), and for  $0 \leq k < p-1$  that  $\mu(i, k) = \mu(i, p-1) + 1$  and  $\mu(i+1, k) = \mu(i+1, 0)$ . This shows

$$\mu(i, k) = \mu(i+1, k) + p^{n-1}.$$

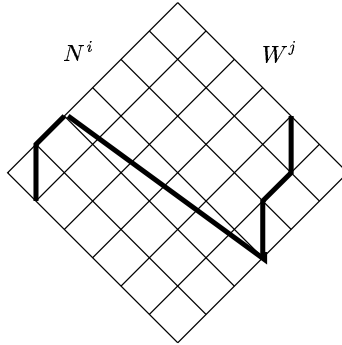
□

With help of the last proposition we graphically describe the  $\Gamma$ -ideals, which have an  $R$ -basis

$$\{\pi^{\mu(i,j)} N^i W^j \mid 0 \leq i, j < p, \mu(i, j) \geq -\nu(i, j)\},$$

by drawing a thick line through the points  $(i, j(i))$ .

**Example 6.14.** The following diagram describes such an typical  $\Gamma$ -ideal, especially it satisfies condition (ii) of Proposition 6.13. Here we are in the case  $p = 7$  (and  $n \geq 1$ ). Proposition 6.13 (iii) shows that  $\mu(i_0, j_0)$  for some fixed  $0 \leq i_0, j_0 < p$  determines  $\mu(i, j)$  for arbitrary  $0 \leq i, j < p$  hence the following diagram describes the  $\Gamma$ -ideal up to an constant factor  $\pi^k$ .



**Definition 6.15.** Let  $0 \leq i, j < p$  and

$$k \geq \begin{cases} -p^{n-1} \cdot i & \text{if } i \leq j \\ -p^{n-1} \cdot i + 1 & \text{if } i > j. \end{cases}$$

Then let  $\mathfrak{J}_{i,j,k}$  be the following two-sided  $\Gamma$ -principal-ideal  $\mathfrak{J}_{i,j,k} := (\pi^k \cdot N^i W^j)$ .

The ideals  $\mathfrak{J}_{i,j,k}$  are well defined, because Theorem 6.10 (i) shows that  $\mathfrak{J}_{i,j,k} \subseteq \Gamma$ . Now we use the notation of Proposition 6.13 and Definition 3.15 and get:

**Proposition 6.16.** The  $\Gamma$ -ideal  $\mathfrak{J}_{i_0,j_0,k}$  is uniquely described by

$$j(i) = \begin{cases} j_0 & \text{if } i \leq i_0 \\ \frac{j_0 + i - i_0}{1} & \text{if } i > i_0, \end{cases}$$

and

$$\mu(i, j(i)) = \begin{cases} k - p^{n-1} \cdot (i - i_0) & \text{if } i < p + i_0 - j_0 \\ k - p^{n-1} \cdot (i - i_0) + 1 & \text{if } i \geq p + i_0 - j_0. \end{cases}$$

*Proof.* The  $\Gamma$ -ideal  $\mathfrak{J}_{i_0,j_0,k}$  has an  $R$ -basis

$$\{\pi^{\mu(i,j)} N^i W^j \mid 0 \leq i, j < p\},$$

with  $\mu(i, j) \geq -\nu(i, j)$ .

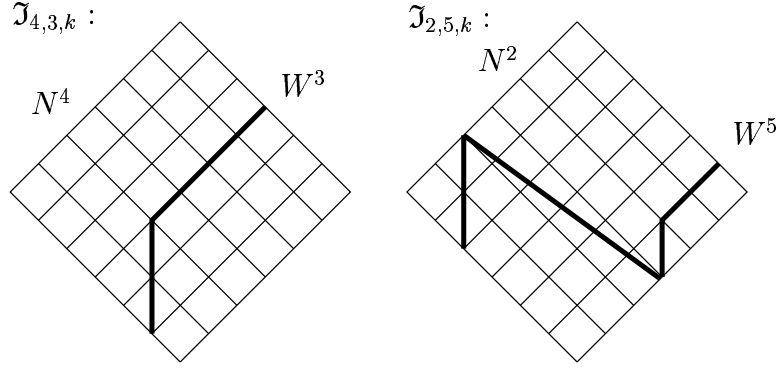
With Corollary we have 6.11  $\Gamma = \Lambda \left[ W, \frac{NW}{1-\zeta} \right]$  and in the proof of Proposition 6.12 we determined the products  $\pi^{\mu(i,j)} N^i W^j \cdot W$ ,  $W \cdot \pi^{\mu(i,j)} N^i W^j$ ,  $\pi^{\mu(i,j)} N^i W^j \cdot \frac{NW}{1-\zeta}$  and  $\frac{NW}{1-\zeta} \cdot \pi^{\mu(i,j)} N^i W^j$  as  $R$ -linear combination of the given  $R$ -basis.

By using Theorem 3.23 we see that multiplying  $\pi^k \cdot N^{i_0} W^{j_0}$  from the left with  $W^r$  for  $0 \leq r \leq i_0$  and  $\left( \frac{NW}{1-\zeta} \right)^s$  for  $0 \leq s < p - i_0$  describes  $\mathfrak{J}_{i_0,j_0,k}$  as  $R[W]$ -right module as in Proposition 6.13 (i).

Since  $\mathfrak{J}_{i_0,j_0,k}$  is minimal with  $\pi^k \cdot N^{i_0} W^{j_0} \in \mathfrak{J}_{i_0,j_0,k}$  we get with Proposition 6.13 (ii) and (iii) the description above.  $\square$

Proposition 6.16 shows that the graphical description of the principal-ideal  $\mathfrak{J}_{i,j,k}$  depends if  $i \geq j$  or if  $i < j$ . We illustrate this in the following example.

**Example 6.17.** Let  $p = 7$ . Then we describe the ideals  $\mathfrak{J}_{4,3,k}$  and  $\mathfrak{J}_{2,5,k}$  by the following diagrams.



By setting  $i := p - 1$  we get the following chain of  $\Gamma$ -principal ideals

$$\mathfrak{I}_{p-1,0,0} \subset \mathfrak{I}_{p-1,p-1,-1} \subset \mathfrak{I}_{p-1,p-2,-1} \subset \dots \subset \mathfrak{I}_{p-1,0,-1} \subset \mathfrak{I}_{p-1,p-1,-2} \subset \dots$$

$$\subset \mathfrak{I}_{p-1,p-1,-p^{n-1}(p-1)+1} \subset \dots \subset \mathfrak{I}_{p-1,0,-p^{n-1}(p-1)+1} \subset \mathfrak{I}_{p-1,p-1,-p^{n-1}(p-1)} \subset \Gamma,$$

which can also be written as

$$(N^{p-1}) \subset (N^{p-1}W^{-1}) \subset (N^{p-1}W^{-2}) \subset \dots \subset (N^{p-1}W^{-p}) \subset (N^{p-1}W^{-(p+1)}) \subset \dots$$

$$\subset (N^{p-1}W^{-p^n(p-1)+p}) \subset \dots \subset (N^{p-1}W^{-p^n(p-1)+1}) \subset (N^{p-1}W^{-p^n(p-1)}) \subset \Gamma.$$

This chain of ideals respects the  $R$ -basis

$$\{\pi^{\mu(i,j)} N^i W^j \mid 0 \leq i, j < p\},$$

which allows us to describe these ideals and later on some over orders graphically. Proposition 6.16 shows that the quotient of any two successive ideals is isomorphic as  $R$ -module to a direct sum of  $p$  copies of  $R/\pi \simeq \mathbb{F}_p$ . (This result is illustrated in example 6.18.)

We need a refinement of this chain to get a chain of  $\Gamma$ -ideals of maximal length. Then we get for  $0 \leq j < p - 1$  and  $0 < r < p^{n-1}(p - 1)$  with Proposition 6.16 the following chain of  $\Gamma$ -ideals between the two successive ideal  $\widehat{\mathfrak{I}} := \mathfrak{I}_{p-1,j+1,-r}$  and  $\mathfrak{I}_{p-1,j,-r}$  of the last chain:

$$(I_j) : \widehat{\mathfrak{I}} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{0,j,-r+(p-1) \cdot p^{n-1}} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{1,j,-r+(p-2) \cdot p^{n-1}} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{2,j,-r+(p-3) \cdot p^{n-1}} \subset$$

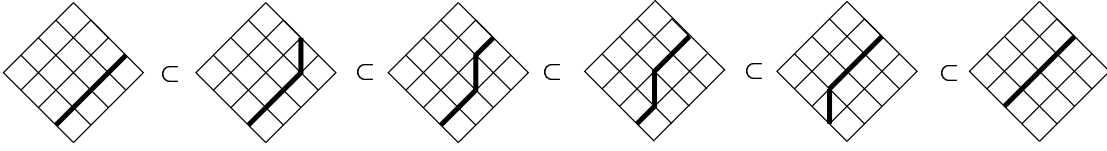
$$\dots \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{p-3,j,-r+2 \cdot p^{n-1}} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{p-2,j,-r+p^{n-1}} = \mathfrak{I}_{p-2,j,-r+p^{n-1}} \subset \mathfrak{I}_{p-1,j,-r},$$

where the quotient of any two successive ideals is isomorphic as  $R$ -module to  $R/\pi \simeq \mathbb{F}_p$ .

**Example 6.18.** Let  $p = 5$  and  $j = 3$  and  $\widehat{\mathfrak{I}} := \mathfrak{I}_{4,3,*}$ . Then the chain of  $\Gamma$ -ideals

$$\widehat{\mathfrak{I}} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{0,2,*} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{1,2,*} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{2,2,*} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{3,2,*} = \mathfrak{I}_{3,2,*} \subset \mathfrak{I}_{4,2,*}$$

corresponds to the diagrams



The refinement of maximal length between  $\widehat{\mathfrak{J}} := \mathfrak{J}_{p-1,0,-r+1}$  and  $\mathfrak{J}_{p-1,p-1,-r}$  is done analogously:

$$(\iota_{p-1} : ) \quad \widehat{\mathfrak{J}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{0,p-1,-r+(p-1) \cdot p^{n-1}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{1,p-1,-r+(p-2) \cdot p^{n-1}} \subset \dots$$

$$\dots \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{p-2,p-1,-r+p^{n-1}} = \mathfrak{J}_{p-2,p-1,-r+p^{n-1}} \subset \mathfrak{J}_{p-1,p-1,-r}.$$

So altogether we have constructed a chain of  $\Gamma$ -ideals of maximal length between  $\mathfrak{J}_{p-1,0,0}$  and  $\mathfrak{J}_{p-1,p-1,(p-1)p^{n-1}}$ , but we will need also a refinement between  $\mathfrak{J}_{p-1,p-1,(p-1)p^{n-1}}$  and  $\Gamma$ . Therefore we consider the chain

$$\mathfrak{J}_{p-1,p-1,(p-1)p^{n-1}} \subset \mathfrak{J}_{p-2,p-2,(p-2)p^{n-1}} \subset \dots \subset \mathfrak{J}_{2,2,2p^{n-1}} \subset \mathfrak{J}_{1,1,p^{n-1}} \subset \Gamma.$$

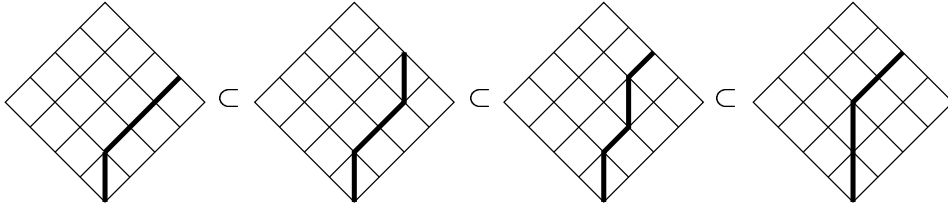
which is even not of maximal length, but we are done by constructing a refinement between  $\widehat{\mathfrak{J}} := \mathfrak{J}_{i+1,i+1,-(i+1)p^{n-1}}$  and  $\mathfrak{J}_{i,i,-ip^{n-1}}$  of maximal length analogously as before:

$$\widehat{\mathfrak{J}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{i,0,0} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{i,1,-p^{n-1}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{i,2,-2p^{n-1}} \subset \dots \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{i,i-1,-(i-1)p^{n-1}} \subset \mathfrak{J}_{i,i,-ip^{n-1}}.$$

**Example 6.19.** Let  $p = 5$ . Then a chain of maximal length between  $\widehat{\mathfrak{J}} := \mathfrak{J}_{3,3,-3 \cdot 5^{n-1}}$  and  $\mathfrak{J}_{2,2,-2 \cdot 5^{n-1}}$  is given by

$$\widehat{\mathfrak{J}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{0,2,0} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{1,2,-5^{n-1}} \subset \mathfrak{J}_{2,2,-2 \cdot 5^{n-1}},$$

which corresponds to the diagrams



Hence we have proved

**Theorem 6.20.** There is a generic chain of  $\Gamma$ -ideals of maximal length between  $\mathfrak{J}_{0,0,0}$  and  $\Gamma$ , where the quotient of any two successive ideals is isomorphic as  $R$ -module to  $R/\pi \simeq \mathbb{F}_p$ .

**Proposition 6.21.** Let  $\mathfrak{J}$  be an  $\Gamma$ -ideal.

- (i) Then  $\Lambda[\mathfrak{J}]$  is an intermediate order between  $\Lambda$  and  $\Gamma$ .

(ii) Let  $\{\pi^{\mu(i,j)}N^iW^j \mid 0 \leq i, j < p, \mu(i, j) \geq \nu(i, j)\}$  be an  $R$ -basis of  $\mathfrak{J}$ . Then  $\Lambda[\mathfrak{J}]$  has an  $R$ -basis

$$\{\pi^{\rho(i,j)}N^iW^j \mid 0 \leq i, j < p, \text{ with } \rho(i, j) := \min(\mu(i, j), 0)\}.$$

*Proof.* (i)  $\Lambda[\mathfrak{J}]$  is multiplicatively closed since  $\Lambda \subset \Gamma$ .

(ii) follows by comparing the  $R$ -basis of  $\mathfrak{J}$  with  $\mathfrak{B}_\Lambda := \{N^iW^j \mid 0 \leq i, j < p\}$ , an  $R$ -basis of  $\Lambda$ , which is given in Theorem 3.22.  $\square$

**Corollary 6.22.** The generic chain of strictly increasing  $\Gamma$ -ideals of maximal length

$$\mathfrak{J}_{p-1,0,0} \subset \mathfrak{J}_{p-1,0,0} + \mathfrak{J}_{0,p-1,(p-1)p^{n-1}-1} \subset \dots \subset \mathfrak{J}_{1,1,-p^{n-1}} \subset \Gamma,$$

which is given in Theorem 6.20, provides by adjoining these  $\Gamma$ -ideals to the  $R$ -order  $\Lambda$ , a generic chain of increasing intermediate  $R$ -orders between  $\Lambda$  and  $\Gamma$ .

*Proof.* This follows from Proposition 6.21 (i).  $\square$

**Remark 6.23.** Let  $\mathfrak{J}_1 \subset \mathfrak{J}_2$  are two successive  $\Gamma$ -ideals in the generic chain of  $\Gamma$ -ideals of Corollary 6.22 with the  $R$ -bases  $\mathfrak{B}_1 = \{\pi^{\mu_1(i,j)}N^iW^j \mid 0 \leq i, j < p\}$  and  $\mathfrak{B}_2 = \{\pi^{\mu_2(i,j)}N^iW^j \mid 0 \leq i, j < p\}$ . Then there is exactly one pair  $(i_0, j_0)$  with  $0 \leq i_0, j_0 < p$ , such that

$$\mu_2(i, j) = \begin{cases} \mu_1(i_0, j_0) - 1 & \text{if } (i, j) = (i_0, j_0), \\ \mu_1(i_0, j_0) & \text{else,} \end{cases}$$

and Proposition 6.21 (ii) shows that  $\Lambda[\mathfrak{J}_1]$  and  $\Lambda[\mathfrak{J}_2]$  coincide if and only if  $\mu_2(i_0, j_0) \geq 0$ .

Now let  $\Lambda[\mathfrak{J}_1] \subset \Lambda[\mathfrak{J}_2]$ . Then this is a minimal extension of  $R$ -orders since  $\mathfrak{J}_1$  has index  $p$  in  $\mathfrak{J}_2$ .

#### 6.4. Graphical description of intermediate orders.

Now we describe a chain of intermediate orders between  $\Lambda$  and  $\Gamma$  with maximal length graphically. Thereby we use the graphical description of Lemma 6.9, that means we use the diagram of the size  $p \times p$ , whereby the position  $(i, j)$  corresponds to  $N^iW^j$ . To this positions we are adjoining circles, where one circle corresponds to 'dividing by  $\pi$ '.

**Example 6.24.** Let  $\Lambda \simeq \mathbb{Z}[\zeta_{2^{n+1}}] \rtimes C_2$ . Then with Theorem 6.8 and by setting

$$\diamond := \overset{N^0}{N} \overset{W^0}{W} \diamond ,$$

the unique chain of intermediate orders (of length  $2^n$ ) is given by:

$$\Lambda := \diamond - \diamond - \diamond - \diamond - \dots - \Gamma .$$

To give an analog result for  $p > 2$ , we describe the chain of intermediate orders, which is given in Corollary 6.22, graphically. Therefore we use the following technics:

**Definition 6.25.** (i) Let  $0 < k < p$ . Then by 'going up with width  $k$ ' one adjoins  $k \cdot p$  circles to the  $p \times p$  diagram, according to the following algorithm:

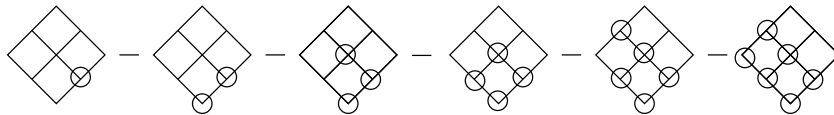
```

for  $j$  from  $p - 1$  to  $0$  by step  $-1$  do
  for  $i$  from  $p - k$  to  $p - 1$  do
    print a circle at the position  $(i, j)$ 
  next  $i$ 
next  $j$ .

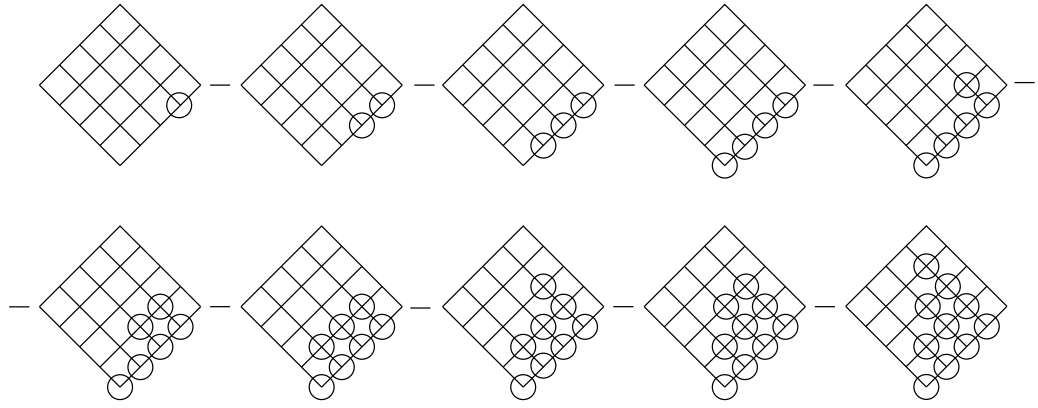
```

(ii) By 'going up to the middle' one adjoins  $\binom{p}{2}$  circles to the  $p \times p$  diagram. Hereby one is 'going up with wide  $p - 1$ ', but only adjoins circles at the position  $(i, j)$ , if  $i \leq j$ .

**Example 6.26.** (i) Let  $p = 3$ . Then going up with width 2 is given by:



(ii) Let  $p = 5$ . Then going up to the middle is given by:



**Theorem 6.27.** Let  $\Lambda \simeq \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$ . There is the following generic construction of over orders from  $\Lambda$  to  $\Gamma$  with maximal length, by adjoining circles to the  $p \times p$  diagram corresponding to the  $R$ -basis  $\mathfrak{B}$ :

- First: Going up with width 1 for  $p^{n-1}$  times.
- Then: Going up with width 2 for  $p^{n-1}$  times.
- ...
- Then: Going up with width  $p - 2$  for  $p^{n-1}$  times.
- Then: Going up with width  $p - 1$  for  $p^{n-1} - 1$  times.
- Finally: Going up to the middle.

*Proof.* We decompose the chain of strictly increasing  $\Gamma$ -ideals of Corollary 6.22 into :

$$\begin{array}{llll}
(\mathfrak{w}_0) : & & \mathfrak{I}_{p-1,0,0} & \subset \\
(\mathfrak{w}_1) : & \mathfrak{I}_{p-1,0,0} + \mathfrak{I}_{0,p-1,(p-1)p^{n-1}-1} & \subset \dots \subset \mathfrak{I}_{p-1,0,-p^{n-1}} & \subset \\
(\mathfrak{w}_2) : & \mathfrak{I}_{p-1,0,-p^{n-1}} + \mathfrak{I}_{0,p-1,(p-2)p^{n-1}-1} & \subset \dots \subset \mathfrak{I}_{p-1,0,-2p^{n-1}} & \subset \\
& \dots & \dots & \dots \\
(\mathfrak{w}_{p-2}) : & \mathfrak{I}_{p-1,0,-(p-3)p^{n-1}} + \mathfrak{I}_{0,p-1,2p^{n-1}-1} & \subset \dots \subset \mathfrak{I}_{p-1,0,-(p-2)p^{n-1}} & \subset \\
(\mathfrak{w}_{p-1}) : & \mathfrak{I}_{p-1,0,-(p-2)p^{n-1}} + \mathfrak{I}_{0,p-1,p^{n-1}-1} & \subset \dots \subset \mathfrak{I}_{p-1,0,-(p-1)p^{n-1}+1} & \subset \\
(\mathfrak{m}_{p-1}) : & \mathfrak{I}_{p-1,0,-(p-1)p^{n-1}+1} + \mathfrak{I}_{0,p-1,0} & \subset \dots \subset \mathfrak{I}_{p-1,p-1,-(p-1)p^{n-1}} & \subset \\
(\mathfrak{m}_{p-2}) : & \mathfrak{I}_{p-1,p-1,-(p-1)p^{n-1}} + \mathfrak{I}_{0,p-2,0} & \subset \dots \subset \mathfrak{I}_{p-2,p-2,-(p-2)p^{n-1}} & \subset \\
& \dots & & \\
(\mathfrak{m}_1) : & \mathfrak{I}_{2,2,-2p^{n-1}} + \mathfrak{I}_{0,1,0} & \subset \mathfrak{I}_{1,1,-p^{n-1}} & \subset \\
(\mathfrak{m}_0) : & \Gamma, & & 
\end{array}$$

and adjoin this chain of ideals to the  $R$ -order  $\Lambda$  and get therefore the increasing chain of intermediate orders of Corollary 6.22.

With Proposition 6.21 (ii) we get in line  $(\mathfrak{w}_0)$  that  $\Lambda[\mathfrak{I}_{p-1,0,0}] = \Lambda$ .

Now we prove that for  $1 \leq k < p-1$  the line  $(\mathfrak{w}_k)$  corresponds to 'going up with width  $k$ ' for  $p^{n-1}$  times,  $(\mathfrak{w}_{p-1})$  corresponds to 'going up with width  $p-1$ ' for  $p^{n-1}-1$  times and that the lines from  $(\mathfrak{m}_{p-1})$  to  $(\mathfrak{m}_1)$  correspond to 'going up to the middle':

Line  $(\mathfrak{w}_k)$  is given by

$$(\mathfrak{w}_k) : \mathfrak{I}_{p-1,0,-(k-1)p^{n-1}} + \mathfrak{I}_{0,p-1,(p-k)p^{n-1}-1} \subset \dots \subset \mathfrak{I}_{p-1,0,-kp^{n-1}} ,$$

and decomposes for  $k < p-1$  into  $p^{n-1}$  lines

$$\begin{aligned} (\mathfrak{k}_1) : & \mathfrak{I}_{p-1,0,-(k-1)p^{n-1}} + \mathfrak{I}_{0,p-1,(p-k)p^{n-1}-1} \subset \dots \subset \mathfrak{I}_{p-1,0,-(k-1)p^{n-1}-1} \subset \\ (\mathfrak{k}_2) : & \mathfrak{I}_{p-1,0,-(k-1)p^{n-1}-1} + \mathfrak{I}_{0,p-1,(p-k)p^{n-1}-2} \subset \dots \subset \mathfrak{I}_{p-1,0,-(k-1)p^{n-1}-2} \subset \\ & \dots \qquad \qquad \qquad \dots \qquad \qquad \dots \\ (\mathfrak{k}_{p^{n-1}}) : & \mathfrak{I}_{p-1,0,-(k-1)p^{n-1}-p^{n-1}+1} + \mathfrak{I}_{0,p-1,(p-k)p^{n-1}-p^{n-1}} \subset \dots \subset \mathfrak{I}_{p-1,0,-kp^{n-1}} , \end{aligned}$$

and for  $k = p-1$  into  $p^{n-1}-1$  lines, where we submit the last line  $(\mathfrak{k}_{p^{n-1}})$ .

Now we prove for  $1 \leq l \leq p^{n-1}$  that the line ( in the case  $k = p-1$  we have  $1 \leq l < p^{n-1}$ )

$$(\mathfrak{k}_l) : \mathfrak{I}_{p-1,0,-(k-1)p^{n-1}-(l-1)} + \mathfrak{I}_{0,p-1,(p-k)p^{n-1}-l} \subset \dots \subset \mathfrak{I}_{p-1,0,-(k-1)p^{n-1}-l}$$

corresponds to 'going up with width  $k$ '.

Therefore we set  $r := (k-1)p^{n-1} + l$  and decompose the  $p^2$  ideals of  $(\mathfrak{k}_l)$  into

$$\begin{aligned} (l_{p-1}) : & \mathfrak{I}_{p-1,0,-r+1} + \mathfrak{I}_{0,p-1,-r+(p-1)p^{n-1}} \subset \dots \subset \mathfrak{I}_{p-1,p-1,-r} \subset \\ (l_{p-2}) : & \mathfrak{I}_{p-1,p-1,-r} + \mathfrak{I}_{0,p-2,-r+(p-1)p^{n-1}} \subset \dots \subset \mathfrak{I}_{p-1,p-2,-r} \subset \\ & \dots \qquad \qquad \qquad \dots \qquad \qquad \dots \\ (l_0) : & \mathfrak{I}_{p-1,1,-r} + \mathfrak{I}_{0,0,-r+(p-1)p^{n-1}} \subset \dots \subset \mathfrak{I}_{p-1,0,-r} , \end{aligned}$$

where the lines  $(l_j)$  correspond to the outer 'for next'-loop of Definition 6.25 (i) and hence to the line in the diagram, which corresponds to  $W^j$ .

We even have given the lines  $(l_j)$  in the proof of Theorem 6.20, explicitly for  $j = p-1$  with  $\widehat{\mathfrak{I}} := \mathfrak{I}_{p-1,0,-r+1}$  between Example 6.18 and Example 6.19

$$\begin{aligned} (l_{p-1} : ) \quad \widehat{\mathfrak{I}} \subset & \widehat{\mathfrak{I}} + \mathfrak{I}_{0,p-1,-r+(p-1)p^{n-1}} \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{1,p-1,-r+(p-2)p^{n-1}} \subset \dots \\ & \dots \subset \widehat{\mathfrak{I}} + \mathfrak{I}_{p-2,p-1,-r+p^{n-1}} = \mathfrak{I}_{p-2,p-1,-r+p^{n-1}} \subset \mathfrak{I}_{p-1,p-1,-r} \end{aligned}$$

and for  $j < p - 1$  with  $\widehat{\mathfrak{J}} := \mathfrak{J}_{p-1, j+1, -r}$  between Example 6.17 and Example 6.18:

$$(l_j) : \widehat{\mathfrak{J}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{0, j, -r+(p-1) \cdot p^{n-1}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{1, j, -r+(p-2) \cdot p^{n-1}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{2, j, -r+(p-3) \cdot p^{n-1}} \subset \\ \dots \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{p-3, j, -r+2 \cdot p^{n-1}} \subset \widehat{\mathfrak{J}} + \mathfrak{J}_{p-2, j, -r+p^{n-1}} = \mathfrak{J}_{p-2, j, -r+p^{n-1}} \subset \mathfrak{J}_{p-1, j, -r} .$$

Now for  $0 \leq j < p$  and  $\widehat{\mathfrak{J}}(i) := \widehat{\mathfrak{J}} + \mathfrak{J}_{i, j, -r+(p-1-i) \cdot p^{n-1}}$  we get the chain

$$(l_j) \quad \widehat{\mathfrak{J}}(-1) := \widehat{\mathfrak{J}} \subset \widehat{\mathfrak{J}}(0) \subset \widehat{\mathfrak{J}}(1) \subset \dots \subset \widehat{\mathfrak{J}}(p-1) .$$

We denote  $\mathfrak{B}_i$  the  $R$ -basis of  $\widehat{\mathfrak{J}}(i)$  of the form  $\{\pi^{\mu_i(i', j')} N^{i'} W^{j'} \mid 0 \leq i', j'\}$ . Then for two successive ideals  $\widehat{\mathfrak{J}}(i-1)$  and  $\widehat{\mathfrak{J}}(i)$  we have

$$\mu_i(i', j') = \begin{cases} \mu_{i-1}(i', j') - 1 & \text{if } (i', j') = (i, j), \\ \mu_{i-1}(i', j') & \text{else.} \end{cases}$$

Hence in the diagrams, which we used to describe  $\Gamma$ -ideals we have to consider the position  $(i, j)$ . Since  $(l_j)$  is ordered by inclusion we consider first  $(0, j)$  and then  $(1, j)$  and so on up to  $(p-1, j)$ . This correspond to the inner 'for next'-loop of Definition 6.25.

In the diagram which we use to describe intermediate-orders we have to print a circle at the position  $(i, j)$  if the  $R$ -order  $\Lambda[\widehat{\mathfrak{J}}(i)]$  is bigger then  $\Lambda[\widehat{\mathfrak{J}}(i-1)]$ . Remark 6.23 shows that this is the cases if and only if  $\mu(i, j) < 0$ , where  $\mu(i, j)$  is given in the line  $(l_j)$  as  $\mu(i, j) = -r + (p-1-i) \cdot p^{n-1}$ .

With  $r = (k-1)p^{n-1} + l$  and  $1 \leq l \leq p^{n-1}$  we first get

$$-(k-1)p^{n-1} > -r \geq -kp^{n-1} :$$

Then, after adding  $(p-1-i)p^{n-1}$  we conclude that

$$(p-i-k)p^{n-1} > \mu(i, j) \geq (p-1-i-k)p^{n-1} .$$

Hence  $\mu(i, j) < 0$  if and only if  $i+k \geq p$  or equivalently if

$$i \in \{p-k, \dots, p-1\} .$$

So just in this case we have to print a circle at the position  $(i, j)$ , which verifies our construction 'going up with width  $k$ '.

It remains to prove, that the lines  $(\mathfrak{m}_{p-1})$  to  $(\mathfrak{m}_1)$  corresponds to 'going up to the middle':

Now we will show that  $(\mathfrak{m}_k)$  for  $p-1 \geq k \geq 1$  corresponds to the inner 'for

next'-loop of 'going up to the middle', which is induced by the line of  $N^*W^k$  in the diagram. Therefore we set

$$\widehat{\mathfrak{J}} := \begin{cases} \mathfrak{J}_{p-1,0,-(p-1)p^{n-1}+1} & \text{for } k = p - 1, \\ \mathfrak{J}_{k+1,k+1,-(k+1)p^{n-1}} & \text{else,} \end{cases}$$

and  $\widehat{\mathfrak{J}}(i) := \widehat{\mathfrak{J}} + \mathfrak{J}_{i,k,-i \cdot p^{n-1}}$  for  $0 \leq i \leq k$ . Then the line  $(\mathbf{m}_k)$ , which corresponds to the points from  $(0, k)$  to  $(k, k)$  in the diagram provides the chain (as above in the chase of  $(l_j)$ )

$$(\mathbf{m}_k) : \widehat{\mathfrak{J}}(-1) := \widehat{\mathfrak{J}} \subset \widehat{\mathfrak{J}}(0) \subset \widehat{\mathfrak{J}}(1) \subset \dots \subset \widehat{\mathfrak{J}}(k).$$

Then two successive ideals  $\widehat{\mathfrak{J}}(i-1) \subset \widehat{\mathfrak{J}}(i)$  are just differing at the position  $(i, k)$ . Since  $\mu(i, k) = -i \cdot p^{n-1} < 0$  if and only if  $i > 0$  we have, by the same arguments as in the discussion above, to print circles for all  $i$  with  $0 < i \leq k$ . This verifies our construction 'going up to the middle'.  $\square$

**Remark 6.28.** For intermediate orders  $\widetilde{\Lambda}$  ( $\Lambda \subset \widetilde{\Lambda} \subset \Gamma$ ), which can be described by adjoint circles to a diagram, that means these orders have an  $R$ -bases

$$\{\pi^{\mu(i,j)} N^i W^j \mid 0 \leq i, j < p, 0 \geq \mu(i, j) \geq -\nu(i, j)\},$$

with  $\nu(i, j)$  defined in Theorem 6.10 as

$$\nu(i, j) = \begin{cases} p^{n-1} \cdot i & \text{if } i \leq j, \\ p^{n-1} \cdot i - 1 & \text{if } i > j, \end{cases}$$

we get

- (i) an unique intermediate order  $\Lambda_{\min}$ , which is minimal over  $\Lambda$ , and
- (ii) an unique intermediate order  $\Lambda_{\max}$ , which is maximal under  $\Gamma$ .

(i): This follows directly from Lemma 6.9 with  $\Lambda_{\min} := \Lambda \left[ \frac{N^{p-1}W^{p-1}}{\pi} \right]$ .

(ii): We get  $\Lambda_{\max}$  by submitting the last circle in the construction algorithm of Theorem 6.27. Hence  $\Lambda_{\max}$  has the following basis as  $R[W]$ -right module

$$\left\{ 1, \frac{NW^2}{\pi p^{n-1}}, \frac{N^2W^2}{\pi 2p^{n-1}}, \dots, \frac{N^{p-1}W^{p-1}}{\pi (p-1)p^{n-1}} \right\}.$$

The uniqueness follows from  $\Gamma = \Lambda \left[ \frac{NW}{1-\zeta} \right]$ , which was shown in Corollary 6.11 (i).

Now we are interested whether the intermediate orders  $\Lambda_{\min}$  and  $\Lambda_{\max}$  remain unique by comparing them with arbitrary intermediate orders  $\widetilde{\Lambda}$ . Hence we give up the assumption that the intermediate orders  $\widetilde{\Lambda}$  have  $R$ -bases

$$\{\pi^{\mu(i,j)} N^i W^j \mid 0 \leq i, j < p, 0 \geq \mu(i, j) \geq -\nu(i, j)\}.$$

**Lemma 6.29.** The  $R$ -order  $\Lambda_{\min}$  is the uniquely minimal over-order over  $\Lambda$  of all intermediate orders between  $\Lambda$  and  $\Gamma$ .

*Proof.* Let  $\Lambda'$  be another minimal over-order of  $\Lambda$ . Then  $\Lambda$  has the index  $p$  in  $\Lambda'$  as  $R$ -module. Then there exist a

$$\lambda' := \frac{1}{\pi} \cdot \sum_{\substack{i,j \geq 0 \\ i+j \leq p-1}} r_{i,j} N^i W^j,$$

with  $(\pi, r_{i,j}) = 1$ , such that  $\Lambda'$  is generated as  $R$ -lattice by

$$\{N^i W^j \mid 0 \leq i, j < p\} \cup \{\lambda'\}.$$

Now we choose the index  $i_0$  minimal under the indices of the non zero coefficients  $r_{i,j}$  and the index  $j_0$  minimal under the indices of the non zero coefficients  $r_{i_0,j}$  and get

$$N^{p-1-i_0} \cdot \lambda' \cdot W^{p-1-i_0} = \frac{r_{i_0,j_0} N^{p-1} W^{p-1}}{\pi} + \lambda,$$

with  $\lambda \in \Lambda$ . Then we set

$$\hat{\lambda} := \frac{r_{i_0,j_0} N^{p-1} W^{p-1}}{\pi}$$

and get the inclusions

$$\Lambda \subset \Lambda[\hat{\lambda}] \subseteq \Lambda'.$$

Then  $(\pi, r_{i_0,j_0}) = 1$  implies that  $\Lambda[\hat{\lambda}] \subseteq \Lambda_{\min}$  and the minimality of  $\Lambda'$  and  $\Lambda_{\min}$  shows that these orders coincide.  $\square$

**Remark 6.30.** Now we want to point out that there some differences depending if the prime  $p$  is odd or even. Therefore we compare the results of Theorem 6.8 and Example 6.24 with the following results.

(i) There is no unique maximal suborder of  $\Gamma$  for odd  $p$ .

We will prove this in the case  $p = 3$ . The arbitrary case is handled analogously.

The radical of  $\Gamma$  is well known and given by

$$\text{rad}(\Gamma) = \begin{pmatrix} \pi & R & R \\ \pi & \pi & R \\ \pi & \pi & \pi \end{pmatrix},$$

and we get

$$\begin{array}{ccccccc}
 & & \Lambda_{\max} & & & & \\
 & & \downarrow \iota & & & & \\
 0 & \longrightarrow & \text{rad}(\Gamma) & \longrightarrow & \Gamma & \xrightarrow{\phi} & \mathbb{F}_3^3 \longrightarrow 0,
 \end{array}$$

where an  $F_3$ -basis of the image  $\text{Im}(\iota\phi)$  is given by the elements

$$\left\{ \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & & \\ & & 1 \end{pmatrix} \right\}.$$

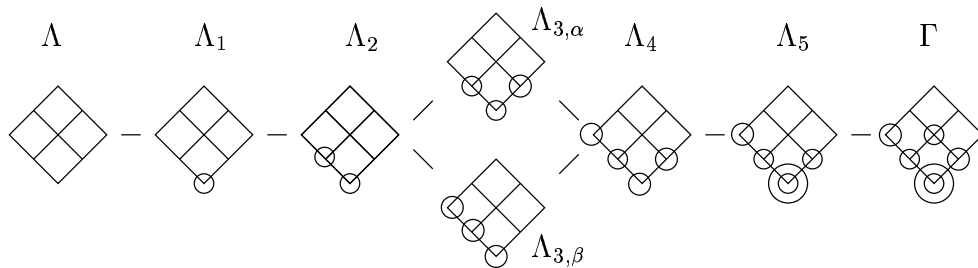
Conjugation with  $W$  provides an automorphism of  $\Gamma$ , which does not fix the maximal suborder  $\Lambda_{\max}$ , since one easily calculates that the image  $\text{Im}(\iota\phi)$  of the conjugate suborder  $\Lambda_{\max}^W$  has an  $F_3$ -basis given by the elements

$$\left\{ \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & & \\ & & 1 \end{pmatrix} \right\}.$$

(ii) For  $\Lambda \simeq \mathbb{Z}[\zeta_9] \rtimes C_3$  we get with  $\pi = 1 - \zeta_3 \in R = \mathbb{Z}[\zeta_3]$ , and by setting

$$\begin{array}{c} \diamond \end{array} := \begin{array}{c} \begin{array}{ccc} & N^0 & W^0 \\ N^2 & \diamond & W \\ & & W^2 \end{array} \end{array}$$

the following chain of all intermediate orders, which can be described by adjoint circles to a diagram:



Since

$$\frac{NW^2}{\pi} \cdot \frac{NW^2}{\pi} = \zeta^2 \cdot \frac{N^2W}{\pi} + (1 + \zeta) \cdot N,$$

we are allowed to adjoin a circle at the position  $(1, 2)$  if there is just a circle at the position  $(2, 1)$ . The other steps are easily verified with Lemma 6.9.

One easily calculates the intermediate orders given by the radical idealisator process:

$$\Lambda - \Lambda_1 - \Lambda_{3,\alpha} - \Lambda_4 - \Gamma ,$$

especially we do not get a chain of maximal length.

Theorem 6.27 provides the following chain of intermediate orders:

$$\Lambda - \Lambda_1 - \Lambda_2 - \Lambda_{3,\beta} - \Lambda_4 - \Lambda_5 - \Gamma .$$

## 7. COHOMOLOGY OF TWISTED GROUP RINGS

In this section we consider left modules. There are analogous results for right modules by replacing column vectors through row vectors. As general reference we use Carlsons 'Modules and Group Algebras' [Ca].

## 7.1. Projective and injective resolutions, Ext-groups.

Trivially  $\Lambda$  is projective as  $\Lambda$ -module. We will use this to construct projective resolutions for some modules we are interested in. To construct analogous injective resolutions we will need that  $\Lambda$  is injective as  $\Lambda$ -module. With Remark 5.2 we restrict ourselves to the category of  $\Lambda$ -lattices.

We are interested in modules of the form  $\Lambda e$ , where  $e$  runs through a chosen set of rational primitive idempotents. These can be interpreted as the columns of  $\Lambda$ , equipped with the natural  $\Lambda$ -operation. They are natural objects in the following sense:

For  $0 \leq i < p$  we denote by  $e_i := (\delta_{p-i,j})_j$  the column vectors:

$$e_{p-1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_{p-2} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, e_0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

By multiplying  $\Lambda$  with the vector  $e_i$  we get the projection on the  $p-i$ -th column

$$\Lambda \cdot e_{p-1} \simeq \begin{pmatrix} R \\ \pi \\ \vdots \\ \pi \end{pmatrix}, \dots, \Lambda \cdot e_1 \simeq \begin{pmatrix} R \\ \vdots \\ R \\ \pi \end{pmatrix}, \Lambda \cdot e_0 \simeq \begin{pmatrix} R \\ R \\ \vdots \\ R \end{pmatrix}$$

and hence an isomorphism of left  $\Lambda$ -lattices

$$\Gamma \simeq \bigoplus_{i=0}^{p-1} \Lambda \cdot e_i.$$

**Remark 7.1.** (i) The automorphism of Theorem 4.5, which is given by the conjugation with  $W$  on  $\Lambda$ , and the equation  $e_i = W^i \cdot e_0$  provide an isomorphism of  $\Lambda$ -modules

$$\Lambda \cdot e_i = \Lambda \cdot W^i e_0 \simeq W^{p-i} \Lambda \cdot e_0.$$

(ii) Then conjugation with  $W^i$  from the left leads to  $N_i := W^i N$ , explicitly to

$$N_0 = \begin{pmatrix} 1-\zeta & & & 0 \\ & 1-\zeta^2 & & \\ & & \ddots & \\ & & & 1-\zeta^{p-1} \end{pmatrix}, N_1 = \begin{pmatrix} & & & 1-\zeta/\pi \\ 1-\zeta^2 & & & \\ & \ddots & & \\ & & 1-\zeta^{p-1} & \\ & & & 0 \end{pmatrix},$$

$$\dots, N_{p-1} = \begin{pmatrix} & & & 1-\zeta^{p-1}/\pi \\ 0 & & & \\ & 1-\zeta^1 & & \\ & & \ddots & \\ & & & 1-\zeta^{p-2} \end{pmatrix}.$$

Hence  $N_i$  lies on the  $p-1$ -th diagonal. More precisely, we obtain

$$(N_i)_{1,p} = \frac{1-\zeta^i}{\pi} \text{ and } (N_i)_{r+1,r} = 1-\zeta^{i+r} \text{ for } 0 < r < p,$$

or equivalently written in a compact form, where we use the notation, which we will introduce just before Lemma 7.4

$$(N_i)_{[r+1],[r]} = \frac{1-\zeta^{i+r}}{\tau_{[r],[r+1]}}.$$

(iii)  $N_i^{p-1}$  lies on the first diagonal, exactly one calculates for  $1 \leq i < p$ :

$$(N_i^{p-1})_{j,k} = \delta_{p-i,j} \cdot \delta_{p+1-i,k} \cdot p/\pi.$$

(iv) Soon we will see that for  $p$  odd the projective resolution for the  $\Lambda$ -lattice  $\Lambda \cdot e_i$  are cyclic of degree 2, while it is constant for  $p=2$ . In this case the following calculations to determine Ext-groups and cohomology rings are getting more simple.

**Suppose that  $p \geq 3$ .** (The case  $p=2$  will be treated at the end of the section.)

Therefore one has the projective and injective resolutions (with  $e_i^T$  the transpose vector to  $e_i$ ).

**Proposition 7.2.** (i) The  $\Lambda$ -lattice  $\Lambda \cdot e_i$  with  $0 \leq i < p$  has a projective resolution of the form

$$\dots \Lambda \xrightarrow{\cdot N_i} \Lambda \xrightarrow{\cdot N_i^{p-1}} \Lambda \xrightarrow{\cdot N_i} \Lambda \xrightarrow{\cdot e_i} \Lambda \cdot e_i \longrightarrow 0.$$

(ii) The  $\Lambda$ -lattice  $\Lambda \cdot e_0$  has an injective resolution of the form

$$0 \longrightarrow \Lambda \cdot e_0 \xrightarrow{\cdot p \cdot e_{p-1}^T} \Lambda \xrightarrow{\cdot N} \Lambda \xrightarrow{\cdot N^{p-1}} \Lambda \xrightarrow{\cdot N} \Lambda \dots$$

(iii) The  $\Lambda$ -lattice  $\Lambda \cdot e_i$  with  $0 < i < p$  has an injective resolution of the form

$$0 \longrightarrow \Lambda \cdot e_i \xrightarrow{\cdot \frac{p}{\pi} \cdot e_{i-1}^T} \Lambda \xrightarrow{\cdot N_i} \Lambda \xrightarrow{\cdot N_i^{p-1}} \Lambda \xrightarrow{\cdot N_i} \Lambda \cdots$$

*Proof.* (i) With the isomorphism  $\Lambda \cdot e_i \simeq {}^{W^{p-i}}\Lambda \cdot e_0$  of Remark 7.1, we just have to consider the case  $i = 0$ .

We have a complex because of  $N^p = 0$ .

The exactness follows since  $\{W^i N^j \mid 0 \leq i, j \leq p-1\}$  is an  $R$ -basis of  $\Lambda$  (Theorem 3.22 (ii)). Precisely

$$\lambda = \sum_{i,j=0}^{p-1} r_{i,j} W^i N^j \in \ker(\cdot N) \implies 0 = \lambda \cdot N = \sum_{i,j=0}^{p-1} r_{i,j} W^i N^{j+1}$$

and hence  $r_{i,j} = 0$  for all  $j < p-1$ .

From  $N^{p-1} = (p\delta_{(p,1),(j,k)})_{j,k}$ , i.e. just  $p$  in the lower left corner, it follows that  $\ker(\cdot e_0) = \ker(\cdot N^{p-1})$  and hence the exactness at the rightmost copy of  $\Lambda$ .

(ii) follows with the same arguments as in part (i) and since  $N^{p-1}$  factors through  $\Lambda \cdot e_0$ :

$$\begin{array}{ccccccc} \cdots & \Lambda & \xrightarrow{\cdot N} & \Lambda & \xrightarrow{\cdot N^{p-1}} & \Lambda & \xrightarrow{\cdot N} & \Lambda & \cdots \\ & & & \searrow \cdot e_0 & & \nearrow \cdot p e_{p-1}^T & & & \\ & & & & \Lambda \cdot e_0 & & & & \end{array}$$

Assertion (iii) follows analogous to (ii).  $\square$

**Remark 7.3.** Hence by splicing together the projective and injective resolution of  $\Lambda \cdot e_i$  one gets the following exact sequence, cyclic of degree 2

$$\cdots \Lambda \xrightarrow{\cdot N_i} \Lambda \xrightarrow{\cdot N_i^{p-1}} \Lambda \xrightarrow{\cdot N_i} \Lambda \xrightarrow{\cdot N_i^{p-1}} \Lambda \cdots,$$

which we will use to calculate the Tate cohomology.

We describe the elements of the cohomology ring as to  $p$ -dimensional vectors, where we use the notation:

- Let  $z \in \mathbb{Z}$ . Then  $\bar{z}, [z]$  are introduced in Definition 3.15 (i) as

$$\bar{z} \equiv [z] \equiv z \pmod{p} \quad \text{with } 0 \leq \bar{z} < p \text{ and } 0 < [z] \leq p.$$

- $\tau_{j,i} := 1$  for  $j \leq i$  and  $\tau_{j,i} := \pi$  for  $j > i$ .

**Lemma 7.4.** Let  $p$  be odd  $n \in \mathbb{Z}$  and  $0 \leq i, j, k < p$ . Then

- (i) Via the isomorphism  $\text{Hom}_\Lambda(\Lambda, \Lambda \cdot e_j) \simeq \Lambda \cdot e_j$ , we get an  $R$ -basis of  $\text{Hom}_\Lambda(\Lambda, \Lambda \cdot e_j)$  by  $\{\tau_{j,i} \cdot e_i \mid 0 \leq i < p\}$ .
- (ii)  $\widehat{\text{Ext}}_\Lambda^{2n}(\Lambda \cdot e_i, \Lambda \cdot e_j)$  is generated by  $\{\tau_{j,i} e_i\}$ , which is an  $R$ -basis for the cocycles, and we get

$$\widehat{\text{Ext}}_\Lambda^{2n}(\Lambda \cdot e_i, \Lambda \cdot e_j) \simeq \begin{cases} R/(p) & \text{if } i = j, \\ R/(p \cdot \pi^{-1}) & \text{else.} \end{cases}$$

- (iii)  $\widehat{\text{Ext}}_\Lambda^{2n+1}(\Lambda \cdot e_i, \Lambda \cdot e_j)$  is generated by  $\{\tau_{j,k} e_k \mid k \not\equiv i-1 \pmod{p}\}$ , which is an  $R$ -basis for the cocycles and is isomorphic to a direct sum of the quotients  $\mathfrak{E}_k \cdot e_k$ , with  $k \not\equiv \overline{i-1}$  and

$$\mathfrak{E}_k \simeq \begin{cases} R/(1-\zeta) & \text{if } k \not\equiv \overline{j-1}, \\ R/((1-\zeta)\pi^{-1}) & \text{if } k \equiv \overline{j-1}. \end{cases}$$

*Proof.* (i) Follows easily by the isomorphisms between  $\Lambda \cdot e_j$  with vectors, we have given at the begin of this chapter.

(ii) We use the identification of (i) and get the cocycles by  $v \in \Lambda \cdot e_j$  with  $N_i \cdot v = 0$ , so the cocycles are generated as  $R$ -module by  $\tau_{j,i} e_i$ .

Now we consider the diagram

$$\begin{array}{ccccc} \dots & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \dots \\ & & & \downarrow \tau_{j,i} \cdot e_i & \nearrow \tau_{j,\overline{i-1}} \cdot e_{\overline{i-1}} & & \\ & & & \Lambda \cdot e_j & & & \end{array}$$

and get the non zero coboundaries generated by the vector  $N_i^{p-1} \cdot \tau_{j,\overline{i-1}} e_{\overline{i-1}}$ . We determine the Ext-group by verifying

$$\tau_{j,i} \cdot e_i / \tau_{j,\overline{i-1}} \cdot N_i^{p-1} \cdot e_{\overline{i-1}} = \begin{cases} 1/p \cdot e_i & \text{if } i = j, \\ \pi/p \cdot e_i & \text{else.} \end{cases}$$

In the case  $i = 0$  we get  $N_i^{p-1} \cdot e_{p-1} = p \cdot e_0$  and are done since  $\tau_{j,p-1} = 1$  and

$$\tau_{j,0} = \begin{cases} 1 & \text{if } j = 0, \\ \pi & \text{else.} \end{cases}$$

If  $i > 0$  we get with Remark 7.1 (iii) that  $N_i^{p-1} \cdot e_{i-1} = p/\pi \cdot e_i$ , which gives the result, because we have for  $i \neq j$ , that  $\tau_{j,i} = \tau_{j,i-1}$  and for  $i = j$  that  $\tau_{j,i} = 1$  and

$\tau_{j,i-1} = \pi$ .

(iii) As above we get the cocycles by  $v \in \Lambda e_j$  with  $N_i^{p-1} \cdot v = 0$ . Remark 7.1 (iii) provides an  $R$ -basis for the cocycles by  $\{\tau_{j,k} e_k \mid k \not\equiv i-1 \pmod{p}\}$  and hence we consider for  $k \not\equiv i-1 \pmod{p}$  the diagram

$$\begin{array}{ccccc}
 \dots & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \dots \\
 & & & \downarrow \tau_{j,k} \cdot e_k & \searrow \tau_{j,k+1} \cdot e_{k+1} & & \\
 & & & \Lambda \cdot e_j & & & .
 \end{array}$$

Hence the coboundaries have an  $R$ -basis  $\{N_i \cdot \tau_{j,\overline{k+1}} e_{\overline{k+1}} \mid k \not\equiv i-1 \pmod{p}\}$ . We recall that the non zero entries of  $N_i$  generate the ideal  $(1-\zeta)$ , except if there is an entry in the last column, which provides  $((1-\zeta)\pi^{-1})$ . Now we determine the Ext-group as above:

First let  $i = 0$  and hence  $k < p-1$ , which shows that

$$\tau_{j,k} = \tau_{j,\overline{k+1}} \iff j \neq k+1$$

and this yields the quotient  $R/(1-\zeta)$ .

For  $j = k+1$  we have  $\tau_{k+1,k} = \pi$  and  $\tau_{k+1,k+1} = 1$ . This yields to the quotient  $R/((1-\zeta)\pi^{-1})$ .

The case  $i > 0$  and  $k \neq p-1$  is done by the same arguments as the case  $i = 0$ .

Now let  $i > 0$  and  $k = p-1$ . For the cocycles we get  $\tau_{j,p-1} = 1$  for all  $j$ . The coboundaries are determined as before by  $N^i \cdot \tau_{j,0} e_0 = \tau_{j,0}(1-\zeta^i)/\pi \cdot e_{p-1}$  and our result follows from

$$\tau_{j,0} = \begin{cases} 1 & \text{if } j = 0, \\ \pi & \text{else.} \end{cases}$$

□

## 7.2. Products in Cohomology.

We will describe products in cohomology by using the composition of chain maps, whereby we first consider the more difficult case  $p$  odd.

Since the resolution belonging to  $\Lambda \cdot e_i$  is cyclic of degree 2, one just has to consider the cases  $\text{Ext}_\Lambda^0(\Lambda \cdot e_i, \Lambda \cdot e_j)$  and  $\text{Ext}_\Lambda^1(\Lambda \cdot e_i, \Lambda \cdot e_j)$ .

**Proposition 7.5.** Let  $p$  be odd.

(i) The chain map corresponding to  $\gamma \in \text{Ext}_\Lambda^0(\Lambda \cdot e_i, \Lambda \cdot e_j)$  with  $\gamma = \tau_{j,i} \cdot e_i$  is given by

$$\begin{array}{ccccccccccc}
 \dots & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot e_i} & \Lambda \cdot e_i & \longrightarrow & 0 \\
 & \downarrow \cdot W^{i-j} & & \downarrow \cdot W^{i-j} & & \downarrow \cdot W^{i-j} & & \downarrow \cdot W^{i-j} & \searrow \cdot \tau_{j,i} e_i & & & \\
 \dots & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \xrightarrow{\cdot e_j} & \Lambda \cdot e_j & \longrightarrow & 0
 \end{array}$$

(ii) The chain map corresponding to  $\gamma_k \in \text{Ext}_\Lambda^1(\Lambda \cdot e_i, \Lambda \cdot e_j)$  with  $k \not\equiv i-1 \pmod p$  and  $\gamma_k = \tau_{j,k} \cdot e_k$  is given by

$$\begin{array}{ccccccccccc}
 \dots & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot e_i} & \Lambda \cdot e_i & \longrightarrow & 0 \\
 & \downarrow \cdot W^{k-j} & & \downarrow \cdot X_{i,j,k} & & \downarrow \cdot W^{k-j} & & \downarrow \cdot W^{k-j} & \searrow \cdot \tau_{j,k} e_k & & & \\
 \dots & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \xrightarrow{\cdot e_j} & \Lambda \cdot e_j & \longrightarrow & 0
 \end{array}$$

where  $X_{i,j,k} \in \Lambda$  lies on the  $\mu$ -th diagonal with  $\mu := \overline{2+k-j}$ , and is always zero except at the two different positions

$$(X_{i,j,k})_{p-i, [\mu-i]} = \frac{\nu_{p-i, [\mu-i]} \cdot p}{1 - \zeta^{1+k-i}}$$

and

$$(X_{i,j,k})_{[-1-k], [1-j]} = \frac{\nu_{[-1-k], [1-j]} \cdot p}{1 - \zeta^{-1-k+i}},$$

with

$$\nu_{j,k} = \begin{cases} \frac{1}{\pi} & \text{if } k-j > 1, \\ 1 & \text{if } -p+1 < k-j \leq 1, \\ \pi & \text{if } k-j = -p+1. \end{cases}$$

**Remark 7.6.** The coefficients  $\nu_{j,k}$  correspond to the matrix

$$(\nu_{j,k}) = \begin{pmatrix} 1 & 1 & \frac{1}{\pi} & \dots & \frac{1}{\pi} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \frac{1}{\pi} \\ 1 & & & & 1 \\ \pi & 1 & \dots & \dots & 1 \end{pmatrix}.$$

They can also given by

$$(*) \quad (\nu_{j,k}) = \sum_{i=2-p}^1 W^i.$$

The matrix  $X_{i,j,k}$  is determined by two non zero entries  $\frac{p}{1-\zeta^\alpha}$  and the coefficient  $\nu_{j,k}$ , which we get most easily from the matrix above.

*Proof.* (i) First one verifies that  $W^{\overline{i-j}} \cdot e_j = \tau_{j,i} \cdot e_i$ :  
 $W^{\overline{i-j}}$  lies on the  $\overline{i-j}$ -th diagonal with entries

$$(*_1) \quad (W^{\overline{i-j}})_{r,[r+i-j]} = \tau_{r,[r+i-j]} \text{ for } 1 \leq r \leq p,$$

and the vector  $e_j$  has exactly one non zero entry  $(e_j)_k = \delta_{k,p-j}$ .

Hence we get a non zero entry in the product if and only if  $[r+i-j] = p-j$  or equivalently if  $r = p-i$ . Exactly we get

$$W^{\overline{i-j}} \cdot e_j = \tau_{p-i,p-j} \cdot e_i,$$

and are done, since  $\tau_{p-i,p-j} = \tau_{j,i}$ .

For  $i \geq j$  and arbitrary  $\alpha$  one gets

$$N_i^\alpha \cdot W^{i-j} = \frac{1}{\pi} W^i \cdot N^\alpha \cdot W^{p-j} = W^{i-j} \cdot N_j^\alpha.$$

For  $i < j$  the commutativity of the diagram follows by multiplying this equation with the central element  $W^p = \pi$ .

(ii) As above one gets  $W^{\overline{k-j}} \cdot e_j = \tau_{j,k} \cdot e_k$ .

We set

$$\Delta_1 := N_i^{p-1} \cdot W^{\overline{k-j}}.$$

Remark 7.1 (iii) shows, that only the  $p-i$ -th row of  $\Delta_1$  has nonzero entries. Then  $N_i^{p-1}$  lies on the first,  $W^{\overline{k-j}}$  on the  $\overline{k-j}$ -th and hence  $\Delta_1$  on the  $\overline{1+k-j}$ -th diagonal. Now we conclude, that  $\Delta_1$  has exactly one nonzero entry. Now we show that this entry is given by

$$(*_2) \quad (\Delta_1)_{r,s} = \frac{p}{\tau_{s,r}} \cdot \delta_{r,p-i} \delta_{s,[1+k-j-i]} :$$

We have that  $(N_i^{p-1})_{r,s} = \frac{p}{\tau_{i,0}} \cdot \delta_{r,p-i} \cdot \delta_{s,[1-i]}$  ( see Remark 7.1 (iii)) and hence equation  $(*_1)$  of (i) shows that the unique nonzero entry of  $\Delta_1$  lies at the position  $(p-i, [1+k-i-j])$  and is given by

$$\frac{p}{\tau_{i,0}} \cdot \tau_{[1-i],[1+k-i-j]}.$$

For  $i = 0$  we verify formula  $(*_2)$  with  $\tau_{i,0} = 1$ ,  $\tau_{[1-i],[1+k-i-j]} = 1$ ,  $r = p$  and  $s \leq p$  and hence  $\tau_{s,r} = 1$ .

For  $i > 0$  we have  $\tau_{i,0} = \pi$  and  $[1 - i] = [-i] + 1 > [-i]$ . The position of the non zero entry of  $\Delta_1$  is at the position  $r = [-i]$  and  $s = [1 + k - i - j]$ . Then we have

$$\tau_{[1-i],s} = 1 \iff [1 - i] \leq s \iff r < s,$$

and the formula  $(*_2)$  follows from

$$\frac{\tau_{[1-i],s}}{\pi} = \frac{1}{\tau_{s,r}}.$$

Now we consider the equation

$$(*_3) \quad X_{i,j,k} \cdot N_j = \Delta_1,$$

which implies that  $X_{i,j,k}$  lies on the  $\mu$ -th diagonal and has a non zero entry in the  $p-i$ -th row, so at the position  $(p-i, [\mu-i])$ . Remark 7.1 (ii) shows, that the nonzero entry of the  $[\mu-i]$ -th row of  $N_j$  is given by

$$\frac{1 - \zeta^{1+k-i}}{\tau_{[\mu-1-i],[\mu-i]}},$$

and hence we conclude with  $[\mu-1-i] > [\mu-i] \iff [\mu-1-i] = p$  that

$$(X_{i,j,k})_{p-i,[\mu-i]} = \frac{p}{\tau_{[\mu-1-i],p-i}} \frac{\tau_{[\mu-1-i],p-1}}{1 - \zeta^{1+k-i}}.$$

Next we show, that

$$\nu_{p-i,[\mu-i]} = \frac{\tau_{[\mu-1-i],p-1}}{\tau_{[\mu-1-i],p-i}}.$$

For this we use

$$(*_4) \quad [\mu - i] = \begin{cases} \mu - i & \text{if } \mu > i, \\ p + \mu - i & \text{if } \mu \leq i. \end{cases}$$

First let  $[\mu - i] - (p - i) > 1$ , which is with  $(*_4)$  equivalent to  $1 < \mu \leq i$ . So we conclude, that  $\mu \not\equiv i + 1 \pmod{p}$  and get

$$p > [\mu - i - 1] = p + \mu - i - 1 > p - i,$$

which implies, that

$$\frac{\tau_{[\mu-1-i],p-1}}{\tau_{[\mu-1-i],p-i}} = \frac{1}{\pi} = \nu_{p-i,[\mu-i]} \text{ for } [\mu - i] - (p - i) > 1.$$

We get for  $[\mu - i] - (p - i) \leq 1 \iff [\mu - i] - 1 \leq (p - i)$ , that

$$[\mu - i - 1] = \begin{cases} [\mu - i] - 1 & \text{if } \mu \not\equiv i + 1 \pmod{p}, \\ p & \text{if } \mu \equiv i + 1 \pmod{p}. \end{cases}$$

So we get for  $\mu \not\equiv i + 1 \pmod{p}$  that

$$\frac{\tau_{[\mu-1-i],p-1}}{\tau_{[\mu-1-i],p-i}} = \frac{1}{1} = \nu_{p-i, [\mu-i]} \text{ for } 1 - p < [\mu - i] - (p - i) \leq 1.$$

For  $\mu \equiv i + 1 \pmod{p}$  we get for  $i > 0$ , that

$$\frac{\tau_{[\mu-1-i],p-1}}{\tau_{[\mu-1-i],p-i}} = \frac{\pi}{\pi} = \nu_{p-i, [\mu-i]} \text{ for } 1 - p < [\mu - i] - (p - i) \leq 1,$$

and for  $i = 0$ , that

$$\frac{\tau_{[\mu-1-i],p-1}}{\tau_{[\mu-1-i],p-i}} = \frac{\pi}{1} = \nu_{p-i, [\mu-i]} \text{ for } 1 - p = [\mu - i] - (p - i).$$

Hence we determined the first non zero entry of  $X_{i,j,k}$ .

Remark 7.1 (ii) shows that the  $[1-j]$ -th row is the only one of  $N_j$  which is identically zero, so we get by equation  $(*_3)$  that all other non zero entries of  $X_{i,j,k}$  have to lie on the  $[1-j]$ -th column. Since  $X_{i,j,k}$  lies on the  $\mu$ -th diagonal, we have to consider the position  $([-1-k], [1-j])$  and determine this entry by the equation

$$N_i \cdot X_{i,j,k} = W^{\overline{k-j}} \cdot N_j^{p-1} =: \Delta_2.$$

By similar calculations as above one gets

$$(\Delta_2)_{r,s} := \frac{p}{\tau_{s,r}} \cdot \delta_{r,p-k} \delta_{s,[1-j]},$$

and Remark 7.1 (ii) shows that

$$(N_i)_{p-k, [-1-k]} = \frac{1 - \zeta^{i-1-k}}{\tau_{[-1-k], p-k}}.$$

So we have

$$(X_{i,j,k})_{[-1-k], [1-j]} = \frac{p}{\tau_{[1-j], p-k}} \frac{\tau_{[-1-k], p-k}}{1 - \zeta^{i-1-k}}.$$

Then we have to show with

$$(*_5) \quad \tau_{[-1-k], p-k} = \begin{cases} \pi & \text{if } k = p - 1 \\ 1 & \text{if } k < p - 1, \end{cases}$$

and

$$(*_6) \quad \tau_{[1-j], p-k} = \begin{cases} \pi & \text{if } k \geq j \geq 1, \\ 1 & \text{else,} \end{cases}$$

that

$$(*_7) \quad \nu_{[-1-k], [1-j]} = \frac{\tau_{[-1-k], p-k}}{\tau_{[1-j], p-k}}.$$

For  $[1-j] - [-1-k] > 1$  we get, that  $[1-j] > 1$  and  $[-1-k] < p$  hence  $j \geq 1$ , a condition of  $(*_6)$ , and  $k < p-1$ , so we get with  $(*_5)$  that  $\tau_{[-1-k], p-k} = 1$ . Now

$$[1-j] = p+1-j \text{ and } [-1-k] = p-1-k$$

imply that

$$[1-j] - [-1-k] > 1 \iff p+1-j - (p-1-k) > 1 \iff k \geq j > 0,$$

hence we get with  $(*_6)$ , that  $\tau_{[1-j], p-k} = \pi$ , which yields to the equation  $(*_7)$  in the first case.

Now let  $[1-j] - [-1-k] \leq 1$ . As above we get for  $k < p-1$ , that  $[-1-k] = p-1-k$ , hence  $\tau_{[-1-k], p-k} = 1$  and

$$[1-j] - [-1-k] \leq 1 \iff [1-j] - (p-1-k) \leq 1 \iff [1-j] \leq p-k,$$

which shows that  $\tau_{[1-j], p-k} = 1$ . So we verified equation  $(*_7)$  in the case  $k < p-1$ . If  $k = p-1$  we have  $\tau_{[-1-k], p-k} = \pi$  and

$$\tau_{[1-j], p-k} = \begin{cases} \pi & \text{if } j \geq 1, \\ 1 & \text{if } j = 0, \end{cases}$$

hence equation  $(*_7)$  is verified.

The matrix  $X_{i,j,k}$  has nonzero entries exactly at two different positions since we assumed that  $k \not\equiv i-1 \pmod{p}$ , so the diagram in (ii) commutes. Now we have to prove, that the multiplication with  $X_{i,j,k}$  provides a homomorphism of  $\Lambda$ -modules, which is done by showing  $X_{i,j,k} \in \Lambda$ . For this we use the notation of Definition 3.26 and Theorem 3.30.

Since  $X_{i,j,k}$  lies on the  $\mu$ -th diagonal we have to show that

$$X_{i,j,k} \in \Lambda_\mu.$$

By Definition 3.26 (iii) we get

$$X_{i,j,k} \in \Lambda_\mu \iff \tilde{D}_\mu^{-1} \cdot X_{i,j,k} \in \tilde{\Lambda}_\mu.$$

This is, by denoting  $\hat{X}_{i,j,k}$  the nonzero column of  $\tilde{D}_\mu^{-1} X_{i,j,k}^\tau$ , with Theorem 3.30 (ii), equivalent to show

$$(*) \quad \tilde{D}_\mu D_{1-\zeta}^{-1} \hat{P} \cdot \hat{X}_{i,j,k} \in R^p.$$

For any  $p \times p$ -matrix  $Y$  lying on the  $l$ -th diagonal one easily computes

$$(\tilde{D}_l^{-1} \cdot Y)_{r, [l+r]} = (Y)_{r, [l+r]} / \tau_{r, p-l}.$$

We apply this to our matrix  $X_{i,j,k}$ , and get the column vector  $\widehat{X}_{i,j,k}$ , which is identically zero, except in the  $p-i$ -th and in the  $[-1-k]$ -th row, with entries

$$\begin{aligned} (\widehat{X}_{i,j,k})_{p-i} &= \begin{cases} \frac{p}{1-\zeta^{1-i+k}} & \text{if } \mu \in \{0, 1\}, \\ \frac{1}{\pi} \frac{p}{(1-\zeta^{1-i+k})} & \text{else,} \end{cases} \\ (\widehat{X}_{i,j,k})_{[-1-k]} &= \begin{cases} \frac{p}{1-\zeta^{-1+i-k}} & \text{if } \mu \in \{0, 1\}, \\ \frac{1}{\pi} \frac{p}{(1-\zeta^{-1+i-k})} & \text{else.} \end{cases} \end{aligned}$$

Since these entries are depending whether  $\mu \in \{0, 1\}$  or not, we just have to prove equation (\*) for the strongest congruences, hence we have to consider the cases  $\mu \in \{0, 2\}$ .

In the case  $\mu = 0$  we have an equivalence between equation (\*) and that

$$(\widehat{P} \cdot \widehat{X}_{i,j,k})_l \equiv 0 \pmod{(1-\zeta)^{l-1}},$$

holds for  $1 \leq l \leq p$ . Now we just have to consider the case  $l = p$ , since  $(1-\zeta)^{p-2}$  divides the entries of  $\widehat{X}_{i,j,k}$ . Now  $p$  is totally ramified over  $(1-\zeta)$  of degree  $p-1$  and the entries of the  $p$ -th row of  $\widehat{P}$  are equal to  $1 \pmod{p}$  since

$$(-1)^i \binom{p-1}{i} \equiv 1 \pmod{p} \text{ for } 0 \leq i < p,$$

which can easily be proved by induction on  $i$ . So we are done, since

$$\frac{p}{1-\zeta^\alpha} + \frac{p}{1-\zeta^{-\alpha}} = p \text{ for } 0 < \alpha < p.$$

The case  $\mu = 2$  follows by the same arguments since the entries of  $\widehat{X}_{i,j,k}$  are divisible by  $\frac{(1-\zeta)^{p-2}}{\pi}$  for  $\mu > 1$ . For  $l = p$  we work as in the case  $\mu = 0$ , after multiplying the analogue equations with  $\pi$ .  $\square$

Immediately we get the Tate-cohomology  $\widehat{\text{Ext}}_{\Lambda}^*(\Lambda \cdot e_i, \Lambda \cdot e_j)$ , by using Proposition 7.5.

**Corollary 7.7.** Let  $p$  be odd.

- (i) The chain map corresponding to  $\gamma \in \widehat{\text{Ext}}_{\Lambda}^{2n}(\Lambda \cdot e_i, \Lambda \cdot e_j)$  with  $\gamma = \tau_{j,i} \cdot e_i$  is given by

$$\begin{array}{ccccccccc} \dots & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \dots \\ \cdot W^{\overline{i-j}} \downarrow & & \cdot W^{\overline{i-j}} \downarrow & & \cdot W^{\overline{i-j}} \downarrow & & \cdot W^{\overline{i-j}} \downarrow & & \cdot W^{\overline{i-j}} \downarrow & & \\ \dots & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \dots \end{array}$$

- (ii) The chain map corresponding to  $\gamma_k \in \widehat{\text{Ext}}_{\Lambda}^{2m+1}(\Lambda \cdot e_i, \Lambda \cdot e_j)$  with  $k \not\equiv i-1 \pmod{p}$  and  $\gamma_k = \tau_{j,k} \cdot e_k$  is given by

$$\begin{array}{ccccccccc} \dots & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \dots \\ \cdot W^{\overline{k-j}} \downarrow & & \cdot X_{i,j,k} \downarrow & & \cdot W^{\overline{k-j}} \downarrow & & \cdot X_{i,j,k} \downarrow & & \cdot W^{\overline{k-j}} \downarrow & & \\ \dots & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \dots \end{array}$$

We use the previous results to describe the cohomology ring  $H_{\Lambda}^*(\Gamma)$ :

**Theorem 7.8.** Let  $p$  be odd and  $\gamma \in \widehat{\text{Ext}}_{\Lambda}^n(\Lambda \cdot e_i, \Lambda \cdot e_j)$  and  $\nu \in \widehat{\text{Ext}}_{\Lambda}^m(\Lambda \cdot e_j, \Lambda \cdot e_k)$  are given as  $p$  dimensional vectors as described in Lemma 7.4. Then we get the product  $\gamma \cdot \nu \in \widehat{\text{Ext}}_{\Lambda}^{n+m}(\Lambda \cdot e_i, \Lambda \cdot e_k)$  as the following  $p$  dimensional vector:

- (i) For  $n$  and  $m$  even,  $\gamma = \tau_{j,i} \cdot e_i$  and  $\nu = \tau_{k,j} \cdot e_j$  we get

$$\gamma \cdot \nu = \begin{cases} \tau_{k,i} \cdot e_i & \text{if } \overline{i-j} + \overline{j-k} < p, \\ \pi \tau_{k,i} \cdot e_i & \text{if } \overline{i-j} + \overline{j-k} \geq p. \end{cases}$$

- (ii) For  $n$  even,  $m$  odd,  $\gamma = \tau_{j,i} \cdot e_i$  and  $\nu = \tau_{k,l} \cdot e_l$  with  $l \not\equiv j-1 \pmod{p}$  we get

$$\gamma \cdot \nu = \begin{cases} \tau_{k,\overline{l+i-j}} \cdot e_{\overline{l+i-j}} & \text{if } \overline{i-j} + \overline{l-k} < p, \\ \pi \tau_{k,\overline{l+i-j}} \cdot e_{\overline{l+i-j}} & \text{if } \overline{i-j} + \overline{l-k} \geq p, \end{cases}$$

where we get  $\overline{l+i-j} \not\equiv i-1 \pmod{p}$ .

- (iii) For  $n$  odd,  $m$  even,  $\gamma = \tau_{j,l} \cdot e_l$  with  $l \not\equiv i-1 \pmod{p}$  and  $\nu = \tau_{k,j} \cdot e_j$  we get

$$\gamma \cdot \nu = \begin{cases} \tau_{k,l} \cdot e_l & \text{if } \overline{l-j} + \overline{j-k} < p, \\ \pi \cdot \tau_{k,l} \cdot e_l & \text{if } \overline{l-j} + \overline{j-k} \geq p. \end{cases}$$

(iv) For  $n$  and  $m$  odd,  $\gamma = \tau_{j,l} \cdot e_l$  with  $l \not\equiv i-1 \pmod{p}$  and  $\nu = \tau_{k,t} \cdot e_t$  with  $t \not\equiv j-1 \pmod{p}$  we get

$$\gamma \cdot \nu = \begin{cases} \frac{p}{1-\zeta^{1+l-i}} \eta_{\overline{l-j}, \overline{t-k}} \cdot \tau_{k,i} e_i & \text{if } t+l+2 \equiv j+i \pmod{p}, \\ 0 & \text{else,} \end{cases}$$

where the coefficients  $\eta_{r,s}$  are given for  $0 \leq r, s < p$  by

$$\eta_{r,s} := \begin{cases} \frac{1}{\pi} & \text{if } r+s < p-2, \\ 1 & \text{if } p-2 \leq r+s < 2p-2, \\ \pi & \text{if } r=s=p-1. \end{cases}$$

Hence the coefficients  $\eta_{r,s}$  correspond to the  $p \times p$ -matrix

$$(\eta_{r,s}) = \begin{pmatrix} \frac{1}{\pi} & \dots & \frac{1}{\pi} & 1 & 1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \frac{1}{\pi} & & & 1 & \\ 1 & & & & 1 \\ 1 & \dots & \dots & 1 & \pi \end{pmatrix}.$$

*Proof.* (i) The product  $\gamma \cdot \nu$  corresponds to the diagram

$$\begin{array}{ccccccc} \dots & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \dots \\ \cdot W^{\overline{i-j}} \downarrow & & & \cdot W^{\overline{i-j}} \downarrow & & \cdot W^{\overline{i-j}} \downarrow & & \cdot W^{\overline{i-j}} \downarrow & \\ \dots & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \dots \\ \cdot W^{\overline{j-k}} \downarrow & & & \cdot W^{\overline{j-k}} \downarrow & & \cdot W^{\overline{j-k}} \downarrow & & \cdot W^{\overline{j-k}} \downarrow & \\ \dots & \Lambda & \xrightarrow{\cdot N_k} & \Lambda & \xrightarrow{\cdot N_k^{p-1}} & \Lambda & \xrightarrow{\cdot N_k} & \Lambda & \xrightarrow{\cdot \tau_{k,j} e_j} & \Lambda \cdot e_k, \\ & & & & & & & & \cdot e_k & \end{array}$$

exactly to the vector

$$W^{\overline{i-j}} \tau_{k,j} e_j = W^{\overline{i-j+j-k}} e_k = \begin{cases} \tau_{k,i} \cdot e_i & \text{if } \overline{i-j} + \overline{j-k} < p, \\ \pi \tau_{k,i} \cdot e_i & \text{if } \overline{i-j} + \overline{j-k} \geq p. \end{cases}$$

(ii) and (iii) are proved analogously.

(iv) The product  $\gamma \cdot \nu$  corresponds to the diagram

$$\begin{array}{ccccccc}
\cdots & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \xrightarrow{\cdot N_i^{p-1}} & \Lambda & \xrightarrow{\cdot N_i} & \Lambda & \cdots \\
\downarrow \cdot W^{\overline{l-j}} & & & \downarrow \cdot X_{i,j,l} & & \downarrow \cdot W^{\overline{l-j}} & & \downarrow \cdot X_{i,j,l} & \\
\cdots & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \xrightarrow{\cdot N_j} & \Lambda & \xrightarrow{\cdot N_j^{p-1}} & \Lambda & \cdots \\
\downarrow \cdot X_{j,k,t} & & & \downarrow \cdot W^{\overline{t-k}} & & \downarrow \cdot X_{j,k,t} & & \downarrow \cdot W^{\overline{t-k}} & \\
\cdots & \Lambda & \xrightarrow{\cdot N_k} & \Lambda & \xrightarrow{\cdot N_k^{p-1}} & \Lambda & \xrightarrow{\cdot N_k} & \Lambda & \xrightarrow{\cdot \tau_{k,t} e_t} & \Lambda \cdot e_k,
\end{array}$$

or by using the description as vectors to

$$\gamma \cdot \nu = X_{i,j,l} \tau_{k,t} e_t.$$

Now Proposition 7.5 (ii) provides that the  $[\mu - i]$ -th and the  $[1 - j]$ -th column are exactly the non zero columns of  $X_{i,j,l}$ , and that  $X_{i,j,l}$  lies on the  $\mu$ -th diagonal with  $\mu := \overline{2 + l - j}$ . Especially these are two different columns since  $l \not\equiv i - 1 \pmod{p}$ . We conclude with  $t \not\equiv j - 1 \pmod{p}$ , that the vector above is different from zero exactly if  $t = \overline{i - \mu}$  and we get in this case with formula (\*) of remark 7.6, that

$$\gamma \cdot \nu = \begin{cases} \frac{p}{1-\zeta^{1+t-i}} W^{\mu+t-k} \cdot e_k & \text{if } \mu \in \{0, 1\}, \\ \frac{p}{1-\zeta^{1+t-i}} \frac{1}{\pi} W^{\mu+t-k} \cdot e_k & \text{if } \mu > 1. \end{cases}$$

Now we determine  $\gamma \cdot \nu$ , which depends on  $\mu$  and  $\rho := \overline{2 + t - k}$ , so  $\mu$  belongs to the first and  $\rho$  to the second chain complex. ( $X_{j,k,t}$  lies on the  $\rho$ -th diagonal.)

We get for  $\mu = 1$  that:

$$\mu + \overline{t - k} \geq p \iff \overline{t - k} = p - 1 \iff \rho = 1,$$

which yields to the last row of  $(\eta_{r,s})$ .

The row above,  $(\eta_{p-2,*})$ , is induced by  $\mu = 0 \iff \overline{l - j} = p - 2$ .

For  $\mu > 1$  we get  $\mu = 2 + \overline{l - j}$  and hence

$$\mu + \overline{t - k} < p \iff \overline{l - j} + \overline{t - k} < p - 2,$$

which gives the row  $\eta_{\overline{l-j},*}$ . □

As an application we also get the cohomology ring  $H_{\Lambda}^*(\Lambda \cdot e_i)$ .

**Definition 7.9.** Let  $\varepsilon_i \in \widehat{\text{Ext}}_{\Lambda}^0(\Lambda \cdot e_i, \Lambda \cdot e_i)$  be the element of the cohomology ring  $H_{\Lambda}^*(\Gamma)$  corresponding to  $e_i$ .

**Corollary 7.10.** Then  $\varepsilon_i$  is an idempotent with

$$\varepsilon_i \cdot H_{\Lambda}^*(\Gamma) \cdot \varepsilon_i \simeq H_{\Lambda}^*(\Lambda \cdot e_i).$$

*Proof.* Lemma 7.4 (i) shows that  $\varepsilon_i$  is well defined. Then we are done by the last theorem and by  $W^{\overline{i-i}} = Id$ .  $\square$

Theorem 7.8 provides also a description of the cohomology ring  $H_{\Lambda}^*(\Lambda \cdot e_i)$ , which is more explicit, because one just has to consider matrices  $X_{i,i,k}$  instead of  $X_{i,j,k}$ :

**Corollary 7.11.** Let  $p$  be odd. With the notation

- ${}_{2n}\varepsilon \in \widehat{\text{Ext}}_{\Lambda}^{2n}(\Lambda \cdot e_i, \Lambda \cdot e_i)$  and
- ${}_{2m+1}\delta_k \in \widehat{\text{Ext}}_{\Lambda}^{2m+1}(\Lambda \cdot e_i, \Lambda \cdot e_i)$  for  $0 \leq k \leq p-1, k \not\equiv i-1 \pmod{p}$ ,

where  ${}_{2n}\varepsilon$  corresponds to  $e_i$  and  ${}_{2m+1}\delta_k$  to  $\tau_{i,k}e_k$  (see Prop. 7.4), one gets the multiplicative structure of  $H_{\Lambda}^*(\Lambda \cdot e_i)$  as

(i)  ${}_{2n}\varepsilon$  is central and

$${}_{2n}\varepsilon \cdot {}_{2n'}\varepsilon = {}_{2(n+n')}\varepsilon \quad \text{and} \quad {}_{2n}\varepsilon \cdot {}_{2m+1}\delta_k = {}_{2(n+m)+1}\delta_k.$$

(ii) the non central  ${}_{2m+1}\delta_k$ 's are multiplied in the following way:

$${}_{2m+1}\delta_k \cdot {}_{2m'+1}\delta_{k'} = \begin{cases} \frac{p}{1-\zeta^{\overline{1+k-i}}} \cdot {}_{2(m+m'+1)}\varepsilon & \text{if } k+k' \equiv 2(i-1) \pmod{p}, \\ 0 & \text{else.} \end{cases}$$

*Proof.* (i) This is most easily seen by using the description of chain complexes, where we have the identity as vertical maps.

(ii) We get from Theorem 7.8 (iv) that  $\overline{k-i} \neq p-1, \overline{k'-i} \neq p-1$  and  $k+k' \equiv 2(i-1) \pmod{p}$ . This implies that  $\overline{k-i} + \overline{k'-i} = p-2$  and hence we get  $\eta_{\overline{k-i}, \overline{k'-i}} = 1$ .  $\square$

**Remark 7.12.** (i) For  $k+k' \equiv 2(i-1) \pmod{p}$  one gets

$${}_{2m+1}\delta_{k'} \cdot {}_{2m'+1}\delta_k = \frac{p}{1-\zeta^{-(1+k-i)}} \cdot {}_{2(m+m'+1)}\varepsilon.$$

Hence the complex conjugation is the only obstruction for  $H_{\Lambda}^*(\Lambda \cdot e_i)$  to be commutative.

In the case  $p=2$  we have  $\zeta = -1$ , which is the only case in which the cohomology rings  $H_{\Lambda}^*(\Lambda \cdot e_i)$  are commutative.

- (ii) It is surprising that the cohomology rings  $H_{\Lambda}^*(\Lambda \cdot e_i)$ , for  $0 \leq i < p$  are independent of  $n$ , where  $\Lambda \simeq \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$ .

**Example 7.13.** Let  $\Lambda$  be the twisted group ring corresponding to  $p = 5$  and an arbitrary  $n > 1$ . Then  $H_{\Lambda}^*(\Lambda \cdot e_2)$  is additively generated by

$${}_{2n}\varepsilon \text{ and } {}_{2m+1}\delta_k \text{ with } k \in \{0, 2, 3, 4\}.$$

The multiplicative structure is given by

- ${}_{2n}\varepsilon$  is central and

$${}_{2n}\varepsilon \cdot {}_{2n'}\varepsilon = {}_{2(n+n')}\varepsilon \text{ and } {}_{2n}\varepsilon \cdot {}_{2m+1}\delta_k = {}_{2(n+m)+1}\delta_k.$$

- the non central  ${}_{2m+1}\delta_k$  are multiplied as

$$\begin{aligned} {}_{2m+1}\delta_2 \cdot {}_{2m'+1}\delta_k &= \begin{cases} \frac{5}{1-\zeta} \cdot {}_{2(m+m'+1)}\varepsilon & \text{if } k=0, \\ 0 & \text{else,} \end{cases} \\ {}_{2m+1}\delta_3 \cdot {}_{2m'+1}\delta_k &= \begin{cases} \frac{5}{1-\zeta^2} \cdot {}_{2(m+m'+1)}\varepsilon & \text{if } k=4, \\ 0 & \text{else,} \end{cases} \\ {}_{2m+1}\delta_4 \cdot {}_{2m'+1}\delta_k &= \begin{cases} \frac{5}{1-\zeta^3} \cdot {}_{2(m+m'+1)}\varepsilon & \text{if } k=3, \\ 0 & \text{else,} \end{cases} \\ {}_{2m+1}\delta_0 \cdot {}_{2m'+1}\delta_k &= \begin{cases} \frac{5}{1-\zeta^4} \cdot {}_{2(m+m'+1)}\varepsilon & \text{if } k=2, \\ 0 & \text{else.} \end{cases} \end{aligned}$$

**Remark 7.14.** Now we consider the case  $p = 2$ :

- (i) Proposition 7.2 remains true.
- (ii) In Lemma 7.4 and in Proposition 7.5 one has not to distinguish the cases if the index of the Ext-groups is even or odd. In Lemma 7.4 case (i) is equivalent to cases (ii) and (iii). Consider that in Proposition 7.5 we have  $X_{i,j,k} = W^{\overline{k-j}}$ . hence the statements (i), (ii), (iii) and (iv) of Theorem 7.8 are equivalent. Also part (i) and (ii) of Corollary 7.11 are equivalent.

## 8. THE REPRESENTATION TYPE OF SOME TWISTED GROUP RINGS

First we state some well known results, where we use chapter 33 of [CuRe] as reference. We denote by  $\Omega$  an  $\mathcal{O}$ -order in a separable  $K$ -algebra, where  $K$  is a global field or the completion of a global field, and  $R$  is a Dedekind domain with quotient field  $K$ . We assume that  $R \neq K$ . For each maximal ideal  $p$  of  $\mathcal{O}$ , let the subscript  $P$  denote completion. Then we set

$$S(\Omega) = \{P \mid \Omega_P \neq \text{maximal } \mathcal{O}_P\text{-order in } A_p\},$$

and get

**Proposition 8.1.** Let  $\Omega$  be a hereditary or maximal order. Then the number of non-isomorphic indecomposable  $\Omega$ -lattices is finite, and equals to the number of isomorphism classes of full  $\Omega$ -lattices in simple  $A$ -modules.

By the following theorem of Jones [Jo] we just have to consider the  $p$ -adic case:

**Theorem 8.2.** Let  $\Omega$  be an  $\mathcal{O}$ -order in a separable  $K$ -algebra, where  $K$  is a global field: Let  $n(\Omega)$  be the number of non-isomorphic indecomposable left  $\Omega$ -lattices: Then

$$n(\Omega) < \infty \iff n(\Omega_P) < \infty \text{ for each } P \in S(\Omega).$$

For integral group rings holds

**Theorem 8.3.** Let  $G$  be a finite group. Then  $\mathbb{Z}G$  has finite representation type if and only if for each prime  $p$  dividing  $|G|$ , the Sylow  $p$ -subgroups of  $G$  are cyclic of order  $p$  or  $p^2$ .

Hence the integral group rings  $\mathbb{Z}C_{p^{n+1}} \rtimes C_p$  have infinite representation type. Now we consider twisted group rings  $\Lambda \simeq \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$ , which we studied in the preceding chapters, especially we are in the totally ramified case. With Theorem 8.2 we are interested whether the  $p$ -adic completion of  $\Lambda$  which we denote by  $\Lambda_P$  has finite representation type.

First we apply the following result of Drozd [Dr]:

**Theorem 8.4.** Let  $R$  be a discrete valuation ring and let  $\Omega$  be an  $R$ -order in a separable  $K$ -algebra  $A$ . Suppose that  $\Omega$  is a local ring, and set  $D = \Omega/\text{rad}(\Omega)$  (a skewfield). Let  $\Omega'$  be an  $R$ -order in  $A$  containing  $\Omega$ , and suppose that  $J$  is a two-sided ideal of  $\Omega'$  for which

$$\text{rad}(\Omega) \subseteq J \subseteq \text{rad}(\Omega').$$

Let  $m$  be the dimension over  $D$  of the  $D$ -vector space  $\Omega'/J$ . Then

- (i)  $\Omega$  has infinite representation type if  $m \geq 4$ .

- (ii) If  $\Omega'$  is itself a local order, and if  $(\text{rad}(\Omega')) \subseteq J$ , then  $\Omega$  has infinite representation type whenever  $m \geq 3$ .

Then we conclude

**Corollary 8.5.** Let  $p$  be prime  $p \geq 5$  and  $n \geq 1$ . Then the twisted group ring  $\mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p \simeq \Lambda$  has infinite representation type.

*Proof.* We get that  $\Omega := \Lambda_p$  and  $\Omega' := \Gamma_p$  are  $\mathbb{Z}_p[\zeta_{p^n}]$ -orders, where we have shown in Remark 3.25 (ii), that  $\Omega$  is local with maximal ideal  $\langle W, N \rangle$  and residue class field  $\mathbb{F}_p$ . Now we set  $R = \mathbb{Z}_p[\zeta_{p^n}]$   $J := \text{rad}(\Gamma_p)$  and get with

$$\Gamma_p := \begin{pmatrix} R & \dots & R \\ (\pi) & R & \vdots \\ \vdots & \ddots & \ddots \\ (\pi) & \dots & (\pi) & R \end{pmatrix} \text{ and } \text{rad}(\Gamma_p) := \begin{pmatrix} (\pi) & R & \dots & R \\ (\pi) & (\pi) & \ddots & \vdots \\ \vdots & & \ddots & R \\ (\pi) & \dots & & (\pi) \end{pmatrix}$$

that

$$\Omega'/J \simeq \mathbb{F}_p.$$

Hence we are done with part (i) of Theorem 8.4.  $\square$

It remains to study the case  $p \in \{2, 3\}$ . For this we use the following Theorem of Drozd and Kiričenko, where we use the notation  $\mu_R(M)$  for the minimal number of generators of the  $R$ -module  $M$ .

**Theorem 8.6.** Let  $\Omega$  be a  $\mathbb{Z}$ -order in a f.d.  $\mathbb{Q}$ -algebra  $A$ , and let  $C$  be the center of  $\Omega$ . Suppose that for each prime ideal  $P$  of  $C$ , the localisation  $\Omega_p$  is primary (that is  $\Omega_p/\text{rad}(\Omega_p)$  is a simple artinian ring.) Let  $\tilde{\Omega}$  be the intersection of all maximal  $\mathbb{Z}$ -orders in  $A$  which contains  $\Omega$ , and let  $I$  be the  $\Omega$ -module  $\tilde{\Omega}/\Omega$ .

Then  $\Omega$  is of finite representation type if and only if the following conditions hold:

- (i)  $\tilde{\Omega}$  is a hereditary ring.
- (ii)  $\mu_{\Omega}(I) \leq 2$ .
- (iii)  $\mu_{\Omega}(\text{rad}(I)) \leq 1$ .

Then we will show the main result of this chapter:

**Theorem 8.7.** Let  $p$  be prime and  $n \geq 1$ . Then the representation type of the twisted group ring  $\Lambda \simeq \mathbb{Z}[\zeta_{p^{n+1}}] \rtimes C_p$  is finite if and only if  $p = 2$ .

*Proof.* Theorem 8.2 allows us to consider  $R$ -orders over the  $p$ -adic numbers  $R = \mathbb{Z}_p[\zeta_{p^n}]$ .

First let  $p = 2$ . Then we shall show that there are exactly two maximal orders

$\Omega_1$  and  $\Omega_2$  over  $\Lambda$  with

$$\Omega_1 = \begin{pmatrix} R & R \\ R & R \end{pmatrix} \text{ and } \Omega_2 = \begin{pmatrix} R & (\pi^{-1}) \\ (\pi) & R \end{pmatrix}.$$

It is well known ( see [Re]) that all maximal orders over  $\Lambda$  are given up to conjugation by the maximal order  $\Omega_1$ . Then  $\Omega_2$  is maximal, because

$$\begin{pmatrix} \pi^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R & R \\ R & R \end{pmatrix} \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} R & (\pi^{-1}) \\ (\pi) & R \end{pmatrix}.$$

We denote by  $K$  the field of quotients of  $R$ . Then every

$$u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with  $a, b, c, d \in K$  and  $\det u \neq 0$  provides a maximal order  $u^{-1}\Omega_1u$ . By multiplying  $u$  with the central matrix

$$u = \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}$$

we can assume that  $u$  has the valuation  $\nu_\pi(\det u) \in \{0, 1\}$ . Now let  $u^{-1}\Omega_1u$  an arbitrary maximal order over  $\Lambda$ . Then  $W \in \Lambda$  shows that

$$\frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} \pi bd - ac & a^2 - \pi b^2 \\ \pi d^2 - c^2 & ac - bd\pi \end{pmatrix} \in \begin{pmatrix} R & R \\ R & R \end{pmatrix}.$$

We get for  $k \in K$  that  $\nu_\pi(k^2) \in 2\mathbb{Z}$  and  $\nu_\pi(\pi k^2) \in 1 + 2\mathbb{Z}$ .

Now let  $\nu_\pi(\det u) = 0$ . Then  $a^2 - \pi b^2 \in R$  implies that  $\nu_\pi(a) \geq 0$  and  $\nu_\pi(b) \geq 0$ , and  $\pi d^2 - c^2 \in R$  implies that  $\nu_\pi(c) \geq 0$  and  $\nu_\pi(d) \geq 0$ . Hence we get  $u \in \text{Gl}_2(R)$  and  $u^{-1}\Omega_1u = \Omega_1$ .

Now let  $\nu_\pi(\det u) = 1$ . Then  $a^2 - \pi b^2 \in (\pi)$  implies that  $\nu_\pi(a) \geq 1$  and  $\nu_\pi(b) \geq 0$ , and  $\pi d^2 - c^2 \in R$  implies that  $\nu_\pi(c) \geq 1$  and  $\nu_\pi(d) \geq 0$ . We set  $a = \pi a'$ ,  $c = \pi c'$  and we get with

$$u' = \begin{pmatrix} a' & b \\ c' & d \end{pmatrix} \in \text{Gl}_2(R)$$

that

$$u^{-1}\Omega_1u = \begin{pmatrix} \pi^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b \\ c' & d \end{pmatrix}^{-1} \begin{pmatrix} R & R \\ R & R \end{pmatrix} \begin{pmatrix} a' & b \\ c' & d \end{pmatrix} \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} = \Omega_2.$$

Hence

$$\tilde{\Omega} = \Omega_1 \cap \Omega_2 = \Gamma$$

verifies condition (i) of Theorem 8.6.

Theorem 6.10 shows that  $I = \Gamma/\Lambda$  has the  $R$ -basis  $\left\{ \frac{N}{\pi^{p^{n-1}-1}}, \frac{NW}{\pi^{p^n-1}} \right\}$ . From Theorem 3.20 we get  $WN = -NW + 2$ . Then  $\frac{2}{\pi^{p^n-1}} \in R$  shows the following identity

in  $I$ :

$$W \cdot \frac{NW}{\pi^{p^{n-1}}} = \frac{N}{\pi^{p^{n-1}-1}}.$$

Then  $I$  is generated as  $\Lambda$ -module by  $\frac{NW}{\pi^{p^{n-1}}}$  and  $\text{rad}(I) = \text{rad}(\Lambda)I$  by  $\frac{N}{\pi^{p^{n-1}-1}}$ , which verifies the condition (ii) and (iii) of Theorem 8.6.

Now we sketch the proof for  $p = 3$ :

Obviously there are the following maximal suborders over  $\Lambda$ :

$$\Omega_1 = \begin{pmatrix} R & R & R \\ R & R & R \\ R & R & R \end{pmatrix}, \Omega_2 = \begin{pmatrix} R & (\pi^{-1}) & (\pi^{-1}) \\ (\pi) & R & R \\ (\pi) & R & R \end{pmatrix}, \Omega_3 = \begin{pmatrix} R & R & (\pi^{-1}) \\ R & R & (\pi^{-1}) \\ (\pi) & (\pi) & R \end{pmatrix}.$$

Then we conclude that

$$\tilde{\Omega} \subseteq \Omega_1 \cap \Omega_2 \cap \Omega_3 = \Gamma.$$

By applying Theorem 8.6 we want to prove that  $\Lambda$  has an infinite representation type. Since there is no hereditary suborder of  $\Gamma$  we can assume that  $\tilde{\Omega} = \Gamma$ .

As above we apply Theorem 6.10 and conclude that  $I = \Gamma/\Lambda$  is generated as  $\Lambda$ -module by

$$\left\{ \frac{NW}{\pi^{p^{n-1}}}, \frac{N^2W^2}{\pi^{2p^{n-1}}} \right\}.$$

Since  $\Lambda$  is semilocal we get that

$$\text{rad}(I) = \text{rad}(\Lambda)I = \left\langle \frac{NW^2}{\pi^{p^{n-1}}}, \frac{N^2}{\pi^{2p^{n-1}-1}} \right\rangle$$

is not cyclic, which contradicts condition (iii) of Theorem 6.10.

The case  $p \geq 5$  is done in Corollary 8.5. □

**Remark 8.8.** (i) Hence we received finite representation type in the non commutativ and totally ramified case for  $p = 2$ . It should be no problem to examine the representation type of the twisted group rings  $\mathbb{Z}[\zeta_{2^{n+1}}] \rtimes C_2$ , which are induced from the dihedral group with

$$\zeta_{2^{n+1}}^b = \zeta_{2^{n+1}}^{-1},$$

or from the semidihedral group with

$$\zeta_{2^{n+1}}^b = \zeta_{2^{n+1}}^{2^n-1}$$

by the methods of this work.

(ii) In Theorem 6.8 we get in the case  $p = 2$  the following unique chain of intermediate orders

$$\Lambda = \Lambda_0 \subsetneq \dots \subsetneq \Lambda_{2^n-1} = \Gamma.$$

Now one can ask if these intermediate orders classify the nonisomorphic indecomposable  $\Lambda$ -lattices.

- (iii) Now let  $p > 2$ . Since  $\Gamma$  is hereditary it has finite representation type. Now one can ask for which  $R$ -orders given in the chain of intermediate orders between  $\Lambda$  and  $\Gamma$  (see Theorem 6.27) we get a finite representation typ.

## REFERENCES

- [An] Andrews G.E.; *Theory of partitions*, Encyclopedia of Math. Appl., Vol. 2, Addison-Wesley, (1976).
- [CuRe] Curti C.W.,Reiner I.; *Methods of Representation Theory*, Vol I,II, Wiley-Interscience, New York, (1981,1987). **20** (1985), 282-298.
- [BeZa] Benz H., Zassenhaus H.; *Über verschränkte Produktordnungen*, J. Number Theory **20** (1985), 282-298.
- [Ca] Carlson J.F.;; *Modules and Group Algebras*, Lectures of Mathematics ETH Zürich, Birkhäuser, (1996).
- [ClSeWe] Cliff G.,Sehgal S.,Weiss A.; *Units of integral group rings of metabelian groups*, J. Algebra **73**, (1981), 167-185.
- [Dr] Drozd Ju. A.; *Generalisation of a theorem of Dade*, Dopovidi Akad. Nauk RSR Ser. A, **3**, (1974), 204-207.
- [DrKi] Drozd, Ju. A. and Kiričenko, V. V., *Primary orders with a finite number of indecomposable representations*, Izv. Akad. Nauk SSSR Ser. Mat., **37**, (1973), 715-736.
- [IrRo] Ireland K., Rosen M.; *A Classical Introduction to Modern Number Theory*, Springer GTM **84**, (1990).
- [Ja] James G.D.,*Representations of General Linear Groups*, London Mathematical Society Lecture Notes Series **94**, (1984).
- [Jo] Jones A.;*Groups with a finite number of indecomposable integral representations*, Michigan Math. J. **10**,(1963), 257-261.
- [Kl] Kleinert E.; *Handling integral p-group rings*, Comm. Algebra **24**, (1996), 3193-3210.
- [Kü] Künzer M.; *Ties for the  $\mathbb{Z}S_n$* , PhD-thesis, Bielefeld, (1999).
- [KüWe] Künzer M.,Weber H.; *On the cyclotomic Dedekind embedding and the cyclic Wedderburn embedding*, To appear in Algebras and Representation Theory.
- [Nebe] Nebe G.; *Orthogonale Darstellungen endlicher Gruppen und Gruppenringe*, Aachener Beiträge zur Mathematik, (1999).
- [Neu] Neukirch J.;*Algebraische Zahlentheorie*, Springer (1991).
- [New] Newman M.;*Integral Matrices*, Academic Press Vol. **45**, (1972).
- [PaWa] Parshall W., Wang J.; *Quantum linear groups*, Memoires of the American Mathematical Society, Number **439**, (1991).
- [Re] Reiner I.; *Maximal Orders*, Academic Press, (1975).
- [Rim] Rim D.S.; *Modules over finite groups*, Ann. Math. (2) **69**, (1959), 700-712.
- [RiSe] Ritter J., Sehgal S.K.; *Integral group rings of some p-groups*, Canad. J. Math. **34**, (1982), 233-246.
- [Ro] Roggenkamp K.W.; *Subgroup rigidity of p-adic group rings (Weiss arguments revisited)*, J. London Math. Soc.(2) **46**, (1992), 432-448.
- [Ro2] Roggenkamp K.W.; *Integral representations and structure of finite group rings*, Sem. Math. Sup.(71), Montreal (1980).

- [Rob] Robinson D.; *A Course in the Theory of Groups*, Springer GTM **80**
- [RoTa] Roggenkamp K.W., Taylor M.J.; *Group Rings and Class Groups*, DMV-Seminar Bd. **18**, Birkhäuser, (1992).
- [Se] Sehgal S.K.; *Units in Integral Group Rings*, Longman Scientific & Technical, (1993).
- [Wa] Washington; *Introduction to Cyclotomic Fields*, Springer GTM **83**
- [We] Weber Heinrich; *Lehrbuch der Algebra*,
- [Wei] Weiss A.; *p-adic rigidity of p-torsion*; Annals of Mathematics **126**, (1987), 317-332.
- [Zi] Zimmermann A.; *Untergruppen der Einheitsgruppen ganzzahliger Gruppenringe*; Dissertation Universität Stuttgart (1992).



## LEBENS LAUF

**Harald Weber**

**geboren**

am 7. Juni 1967 in Radolfzell.

**Eltern**

Ewald Weber und Elfriede Weber, geborene Wieser.

**Schulbildung**

Grundschule Stahringen von 1973 bis 1977.

Realschule Radolfzell von 1977 bis 1984.

Technisches Gymnasium in Konstanz von 1984 bis 1987.

**Reifeprüfung**

im Mai 1987.

**Zivildienst**

Altersheim Radolfzell.

**Studium**

Mathematik mit Nebenfach Physik an der Universität Stuttgart.

Beginn im Wintersemester 1989/90.

Vordiplom im Sommersemester 1991.

**Diplomprüfung**

am 3. März 1996 an der Universität Stuttgart.

**Berufstätigkeit**

Juni 1996 – April 1998 Stipendiat (Landesgraduiertenförderung)  
an der Universität Stuttgart.

Seit April 1998 Mitarbeiter an der Universität Stuttgart.