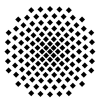


University of Stuttgart
Germany

Group rings for the dihedral group D_{2p}

Diploma thesis

Simon Klenk

2 January 2013

Contents

Introduction

The dihedral group

We aim to describe certain dihedral group rings. Let $p \in \mathbb{Z}_{\geq 3}$ be a prime. Write $n := \frac{p-1}{2}$.

We consider the dihedral group

$$\mathrm{D}_{2p} := \left\langle x, y : x^p, y^2, (yx)^2 \right\rangle ,$$

cf. Section 3.1.

Number theoretic preliminaries

Let $\zeta_p = \exp\left(\frac{2\pi \mathrm{i}}{p}\right) \in \mathbb{C}$ be a primitive p-th root of unity. Let $\vartheta_p := \zeta_p + \zeta_p^{-1} - 2$. Then

$$\mathbb{Q}(\zeta_p) \mid \mathbb{Q}(\vartheta_p) \mid \mathbb{Q} ,$$

where $\mathbb{Q}(\vartheta_p) = \mathbb{R} \cap \mathbb{Q}(\zeta_p)$. The corresponding rings of algebraic integers are

$$\mathbb{Z}[\zeta_p] \mid \mathbb{Z}[\vartheta_p] \mid \mathbb{Z} .$$

Cf. Lemma 22 and Lemma 24 *(i1)*. We obtain discrete valuation rings

$$\mathbb{Z}_{(p)}[\zeta_p] \mid \mathbb{Z}_{(p)}[\vartheta_p] \mid \mathbb{Z}_{(p)} ,$$

with maximal ideals generated by $\zeta_p - 1$, ϑ_p and p, respectively; cf. Remark 46 *(iii,iv)*.

Both extensions are totally ramified, with ramifications

$$\left((\zeta_p - 1)^2\right) = (\vartheta_p) \qquad \text{resp.} \qquad \left(\vartheta_p^n\right) = (p) .$$

Wedderburn

By Wedderburn's Theorem, we obtain the isomorphisms of algebras

Proposition 62 $\rightarrow$ $\quad \omega_{\mathbb{C}} : \mathbb{C}\mathrm{D}_{2p} \xrightarrow{\sim} \mathbb{C} \times \left(\mathbb{C}^{2\times 2}\right)^{\times n} \times \mathbb{C}$,

Proposition 63 $\rightarrow$ $\quad \omega_{\mathbb{Q}(\vartheta_p)} : \mathbb{Q}(\vartheta_p)\mathrm{D}_{2p} \xrightarrow{\sim} \mathbb{Q}(\vartheta_p) \times \left(\mathbb{Q}(\vartheta_p)^{2\times 2}\right)^{\times n} \times \mathbb{Q}(\vartheta_p)$,

Proposition 67 $\rightarrow$ $\quad \omega_{\mathbb{Q}} : \mathbb{Q}\mathrm{D}_{2p} \xrightarrow{\sim} \mathbb{Q} \times \mathbb{Q}(\vartheta_p)^{2\times 2} \times \mathbb{Q}$

over $\mathbb{C}$, $\mathbb{Q}(\vartheta_p)$ and $\mathbb{Q}$, respectively.

We want to describe the image $\omega_{\mathbb{Q}}(\mathbb{Z}\mathrm{D}_{2p})$, which is an isomorphic copy of $\mathbb{Z}\mathrm{D}_{2p}$.

We want to describe the image $\omega_{\mathbb{Q}(\vartheta_p)}(\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p})$, which is an isomorphic copy of $\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p}$.

The group rings $\mathbb{Z}\mathrm{D}_{2p}$ and $\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p}$

Aims

The image $\omega_{\mathbb{Q}}(\mathbb{Z}\mathrm{D}_{2p})$ is a proper subring of $\mathbb{Z} \times \mathbb{Z}[\vartheta_p]^{2\times 2} \times \mathbb{Z}$. We aim to describe this subring via congruences of matrix entries, called *ties*.

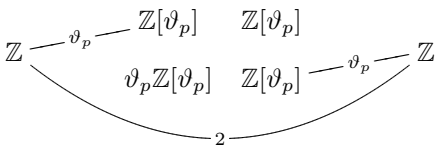
Similarly, the image $\omega_{\mathbb{Q}(\vartheta_p)}(\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p})$ is a proper $\mathbb{Z}[\vartheta_p]$-subalgebra of $\mathbb{Z}[\vartheta_p] \times \left(\mathbb{Z}[\vartheta_p]^{2\times 2}\right)^{\times n} \times \mathbb{Z}[\vartheta_p]$, which we want to describe via ties.

The integral group ring $\mathbb{Z}\mathrm{D}_{2p}$

In Theorem 70 we restrict $\omega_{\mathbb{Q}}$ to the isomorphism of rings

$$\begin{aligned}
\omega_{\mathbb{Z}} \,:\, \mathbb{Z}\mathrm{D}_{2p} &\xrightarrow{\sim} \left\{ (a\,, \begin{pmatrix} b & c \\ d & e \end{pmatrix}, f\,) \in \mathbb{Z} \times \mathbb{Z}[\vartheta_p]^{2\times 2} \times \mathbb{Z} \,:\, a \equiv_{\vartheta_p} b\,,\ d \equiv_{\vartheta_p} 0\,,\ e \equiv_{\vartheta_p} f\,,\ a \equiv_2 f \right\} \\
x &\longmapsto (1\,, \begin{pmatrix} 1 & 1 \\ \vartheta_p & \vartheta_p + 1 \end{pmatrix}, 1\,) \\
y &\longmapsto (1\,, \begin{pmatrix} 1 & 0 \\ \vartheta_p & -1 \end{pmatrix}, -1\,),
\end{aligned}$$

whose image is a subring of $\mathbb{Z} \times \mathbb{Z}[\vartheta_p]^{2\times 2} \times \mathbb{Z}$, which can be adumbrated as follows.



After tensoring with $\mathbb{Z}_p$, this can be compared with [Plesken 83, Ch. VIII, p. 138, Theorem (VIII.5)].

Using a related pullback description of $\mathbb{Z}\mathrm{D}_{2p}$, A. Zimmermann has investigated conjugacy classes of involutions in $\mathbb{Z}\mathrm{D}_{2p}$ in [Zimmermann 92, Abschnitt 3.9, p. 65, Satz 4].

The tensor product $\mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta_p]$

We will pass from the description of our isomorphic copy of the group ring $\mathbb{Z}\mathrm{D}_{2p}$ to that of $\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p}$ via $\mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} -$. There, tensor products of the form $\mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta_p]$ will occur, which need to be replaced as follows. For $i \in [0, n-1]$ and $k \in [1, n]$, we define

$$\left\langle \begin{matrix} i \\ k \end{matrix} \right\rangle := \begin{cases} (-1)^{i-k+1} \left(\binom{2i}{i-k+1} - \binom{2i}{i-k} \right) & \text{for } k \in [1, i+1]\,, \\ 0 & \text{for } k \in [i+2, n]\,. \end{cases}$$

Restricting the isomorphism of Dedekind's Lemma, cf. Lemma 109, we obtain the following

Proposition 41 We have the isomorphism of $\mathbb{Z}[\vartheta_p]$-algebras

$$f \,:\, \mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta_p] \xrightarrow{\sim} \left\{ (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n} \,:\, \sum_{k=1}^{n} \left\langle \begin{matrix} i \\ k \end{matrix} \right\rangle a_k \equiv_{\vartheta_p^i} 0 \text{ for } i \in [0, n-1] \right\} =: {}_p\Psi\,,$$

where ${}_p\Psi$ is a $\mathbb{Z}[\vartheta_p]$-subalgebra of $\mathbb{Z}[\vartheta_p]^{\times n}$.

EXAMPLE The subalgebra ${}_7\Psi$ of $\mathbb{Z}[\vartheta_7]^{\times 3}$ is given by

$$ {}_7\Psi \;=\; \left\{ (\,v\,,\,w\,,\,x\,) \in \mathbb{Z}[\vartheta_7]^{\times 3} \;:\; \begin{array}{rcl} -v+w & \equiv_{\vartheta_7^1} & 0 \\ 2v-3w+x & \equiv_{\vartheta_7^2} & 0 \end{array} \right\} . $$

A local and a global basis of a principal ideal

Write $\theta_p := f(1 \otimes \vartheta_p) \in {}_p\Psi$. In ${}_p\Psi$, we have the principal ideal

$$ {}_p\tilde{\Psi} \;:=\; \theta_p \cdot {}_p\Psi \;\subseteq\; {}_p\Psi \;\subseteq\; \mathbb{Z}[\vartheta_p]^{\times n} . $$

It also plays a role in the passage from $\mathbb{Z}\mathrm{D}_{2p}$ to $\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p}$ mentioned above. Its localization

$$ {}_p\tilde{\Psi}_{(p)} \;=\; \theta_p \cdot {}_p\Psi_{(p)} \;\subseteq\; {}_p\Psi_{(p)} \;\subseteq\; \mathbb{Z}_{(p)}[\vartheta_p]^{\times n} $$

will turn out to be easier to control than ${}_p\tilde{\Psi}$ itself.

Multiplying a $\mathbb{Z}[\vartheta_p]$-linear basis of ${}_p\Psi \subseteq \mathbb{Z}[\vartheta_p]^{\times n}$ of triangular shape with θ_p, we obtain a $\mathbb{Z}[\vartheta_p]$-linear basis $\mathrm{B}_{{}_p\tilde{\Psi}} = \mathrm{B}_{\theta_p \cdot {}_p\Psi}$ of ${}_p\tilde{\Psi}$.

Somewhat easier to handle is the description via ties, proven in

Proposition 52 The principal ideal of ${}_p\Psi$ generated by θ_p is given by

$$ {}_p\tilde{\Psi} \;=\; \theta_p \cdot {}_p\Psi \;=\; \left\{ (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n} \;:\; \sum_{k=1}^{n} \frac{(2i-1)^2}{(2k-1)^2} \cdot (2i)! \cdot \left\langle \begin{array}{c} i-1 \\ k \end{array} \right\rangle \cdot a_k \equiv_{\vartheta_p^{\,i}} 0 \text{ for } i \in [1,n] \right\} . $$

This description allows to deduce the $\mathbb{Z}_{(p)}[\vartheta_p]$-linear basis

$$ \mathrm{B}_{{}_p\tilde{\Psi}_{(p)}} \;:=\; \left(\left(\frac{(2k-1)^2}{l+k-1} \binom{l+k-1}{k-l} \cdot \vartheta_p^{\,l} \right)_{k\in[1,n]} \;:\; l \in [1,n] \right) $$

of the localized ideal ${}_p\tilde{\Psi}_{(p)}$.

Now $\mathrm{B}_{{}_p\tilde{\Psi}_{(p)}}$ is contained in ${}_p\tilde{\Psi}$, but not a $\mathbb{Z}[\vartheta_p]$-linear basis of ${}_p\tilde{\Psi}$ if $p \geq 5$, cf. Subsection 2.2.4, Corollary 53.

EXAMPLE We have the $\mathbb{Z}[\vartheta_7]$-linear basis

$$ \mathrm{B}_{{}_7\tilde{\Psi}} = \begin{pmatrix} (\; \vartheta_7^3 + 6\vartheta_7^2 + 9\vartheta_7 \;,\; \vartheta_7^2 + 4\vartheta_7 \;,\; \vartheta_7 \;) \,, \\ (\; 0 \;,\; \vartheta_7^3 + 4\vartheta_7^2 \;,\; 3\vartheta_7^2 \;) \,, \\ (\; 0 \;,\; 0 \;,\; \vartheta_7^3 \;) \end{pmatrix} $$

of ${}_7\tilde{\Psi}$, which is written using the $\mathbb{Z}$-linear basis $\left(\vartheta_7^i \;:\; i \in [1,3] \right)$ of $\vartheta_7\mathbb{Z}[\vartheta_7]$, cf. Lemma 24 *(i3)*.

The description via ties is given by

$$ {}_7\tilde{\Psi} \;=\; \left\{ (\,v\,,\,w\,,\,x\,) \in \mathbb{Z}[\vartheta_7]^{\times 3} \;:\; \begin{array}{rcl} 2v & \equiv_{\vartheta_7^1} & 0 \\ -216v + 24w & \equiv_{\vartheta_7^2} & 0 \\ 36000v - 6000w + 720x & \equiv_{\vartheta_7^3} & 0 \end{array} \right\} . $$

We deduce the $\mathbb{Z}_{(7)}[\vartheta_7]$-linear basis

$$ \mathrm{B}_{{}_7\tilde{\Psi}_{(7)}} \;=\; \left(\begin{array}{l} (\,\vartheta_7\,,\,9\vartheta_7\,,\,25\vartheta_7\,)\,, \\ (\;\;0\,,\,3\vartheta_7^2\,,\,25\vartheta_7^2\,)\,, \\ (\;\;0\,,\;\;\;0\,,\;\,5\vartheta_7^3\,) \end{array} \right) $$

of ${}_7\tilde{\Psi}_{(7)}$.

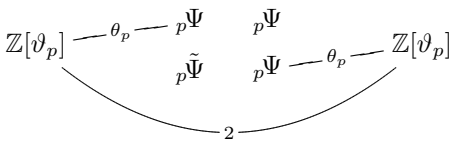
The group ring $\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p}$

Consider the $\mathbb{Z}[\vartheta_p]$-subalgebra

$$ {}_p\Omega := \left\{ (\xi, \begin{pmatrix} \psi_1 & \psi_2 \\ \psi_3 & \psi_4 \end{pmatrix}, \eta) \in \mathbb{Z}[\vartheta_p] \times {}_p\Psi^{2\times 2} \times \mathbb{Z}[\vartheta_p] \;:\; (\xi)_{i\in[1,n]} \equiv_{\theta_p} \psi_1\,,\; \psi_3 \equiv_{\theta_p} 0\,,\; \psi_4 \equiv_{\theta_p} (\eta)_{i\in[1,n]}\,,\; \xi \equiv_2 \eta \right\} $$

of $\mathbb{Z}[\vartheta_p] \times {}_p\Psi^{2\times 2} \times \mathbb{Z}[\vartheta_p]$. Here, for instance, $(\xi)_{i\in[1,n]} \equiv_{\theta_p} \psi_1$ means that $(\xi)_{i\in[1,n]} - \psi_1 \in \theta_p \cdot {}_p\Psi = {}_p\tilde{\Psi}$, which explains the interest in this principal ideal mentioned above. Cf. Notation 74.

The $\mathbb{Z}[\vartheta_p]$-algebra ${}_p\Omega$ can be adumbrated as follows.



So we can embed

$$ {}_p\Omega \;\subseteq\; \mathbb{Z}[\vartheta_p] \times {}_p\Psi^{2\times 2} \times \mathbb{Z}[\vartheta_p] \;\subseteq\; \mathbb{Z}[\vartheta_p] \times \left(\mathbb{Z}[\vartheta_p]^{\times n}\right)^{2\times 2} \times \mathbb{Z}[\vartheta_p] \;\xrightarrow{\sim}\; \mathbb{Z}[\vartheta_p] \times \left(\mathbb{Z}[\vartheta_p]^{2\times 2}\right)^{\times n} \times \mathbb{Z}[\vartheta_p]\,, $$

where the isomorphism " $\xrightarrow{\sim}$ " merely reorganizes the entries.

Theorem 80 We have the isomorphism of $\mathbb{Z}[\vartheta_p]$-algebras

$$ \begin{array}{rcccl} \omega_{\mathbb{Z}[\vartheta_p]} & : & \mathbb{Z}[\vartheta_p]\mathrm{D}_{2p} & \xrightarrow{\sim} & {}_p\Omega \\ & & x & \longmapsto & (\,1\,,\begin{pmatrix} 1 & 1 \\ \theta_p & \theta_p + 1 \end{pmatrix},\, 1\,) \\ & & y & \longmapsto & (\,1\,,\begin{pmatrix} 1 & 0 \\ \theta_p & -1 \end{pmatrix},\, -1\,)\,. \end{array} $$

Cf. also [Wingen 95, §4, p. 307, Theorem 3 and p. 309, Example 5].

Presentations via path algebras

Aim

We give a presentation of the group ring $\mathbb{Z}_{(p)}\mathrm{D}_{2p}$ by quiver and relations over $\mathbb{Z}_{(p)}$ in Chapter 6.

We derive a well-known presentation of the group ring $\mathbb{F}_p\mathrm{D}_{2p}$ by quiver and relations over $\mathbb{F}_p$.

Presentation of $\mathbb{Z}_{(p)}\mathrm{D}_{2p}$ by quiver and relations

Consider the quiver $\Xi := \left(E \bullet \underset{\beta}{\overset{\alpha}{\rightleftarrows}} \bullet F \right)$, cf. Notation 81.

Let $\mu_{\vartheta_p,\mathbb{Q}}(X) \in \mathbb{Z}[X]$ be the minimal polynomial of ϑ_p over $\mathbb{Q}$.

Consider the ideal

$$I \;:=\; \lhd\, \mu_{\vartheta_p,\mathbb{Q}}(\alpha\beta)\alpha\,,\, \mu_{\vartheta_p,\mathbb{Q}}(\beta\alpha)\beta \,\rhd_{\mathbb{Z}_{(p)}\Xi} \;\subseteq\; \mathbb{Z}_{(p)}\Xi\,,$$

cf. Convention 10, Notation 82. We denote the residue class of an element $\xi \in \mathbb{Z}_{(p)}\Xi$ by

$$\overline{\xi} \;:=\; \xi + I \;\in\; {}^{\mathbb{Z}_{(p)}\Xi}\!/_{I}\,.$$

Propositions 84, 85 We have the isomorphisms of $\mathbb{Z}_{(p)}$-algebras

$$\mathbb{Z}_{(p)}\mathrm{D}_{2p} \;\underset{\mathcal{P}_2}{\overset{\mathcal{P}_3}{\sim}}\; \mathbb{Z}_{(p)}\Xi/_{I}$$

which invert each other; cf. Remark 86.

The isomorphism of $\mathbb{Z}_{(p)}$-algebras $\mathcal{P}_3$ is given on the generators of $\mathrm{D}_{2p} = \langle\, x,\, y \,:\, x^p,\, y^2,\, (yx)^2 \,\rangle$ by

$$\mathcal{P}_3(x) \;=\; \overline{E} + \overline{F} + \overline{\alpha} + \overline{\beta} + \overline{\beta\alpha} \quad \text{and} \quad \mathcal{P}_3(y) \;=\; \overline{E} - \overline{F} + \overline{\beta}\,.$$

The isomorphism of $\mathbb{Z}_{(p)}$-algebras $\mathcal{P}_2$ is given on the generators by

$$\begin{aligned}
\mathcal{P}_2\big(\overline{E}\big) &= \frac{1}{2}\sum_{k=0}^{p-1}(-1)^k x^k(1+y)\\
\mathcal{P}_2\big(\overline{F}\big) &= \frac{1}{2}\left(1 - y - \sum_{k=1}^{p-1}(-1)^k x^k(1+y)\right)\\
\mathcal{P}_2(\overline{\alpha}) &= -x^{-1} - y - \sum_{k=1}^{p-2}(-1)^k x^k(1+y)\\
\mathcal{P}_2\big(\overline{\beta}\big) &= -\sum_{k=1}^{p-1}(-1)^k x^k(1+y)\,.
\end{aligned}$$

EXAMPLE The group ring $\mathbb{Z}_{(7)}\mathrm{D}_{14}$ is isomorphic to

$${}^{\mathbb{Z}_{(7)}\Xi}\!\Big/\!\lhd \big((\alpha\beta)^3 + 7(\alpha\beta)^2 + 14\alpha\beta + 7\big)\cdot\alpha\,,\, \big((\beta\alpha)^3 + 7(\beta\alpha)^2 + 14\beta\alpha + 7\big)\cdot\beta \,\rhd_{\mathbb{Z}_{(7)}\Xi}$$

as $\mathbb{Z}_{(7)}$-algebra.

Presentation of $\mathbb{F}_p\mathrm{D}_{2p}$ by quiver and relations

Using the presentation of the group ring $\mathbb{Z}_{(p)}\mathrm{D}_{2p}$ obtained above and the fact that the minimal polynomial of ϑ_p over $\mathbb{Q}$ is Eisenstein at p, we are able to derive a well-known presentation of the group ring $\mathbb{F}_p\mathrm{D}_{2p}$ via a reduction modulo p.

Consider the ideal

$$J \;:=\; \lhd\,(\alpha\beta)^n\alpha\,,\,(\beta\alpha)^n\beta\,\rhd_{\mathbb{F}_p\Xi} \;\subseteq\; \mathbb{F}_p\Xi\,,$$

cf. Convention 10, Notation 88. So J is the image of I under the reduction map $\mathbb{Z}_{(p)}\Xi \longrightarrow \mathbb{F}_p\Xi$ modulo p. We denote the residue class of an element $\xi \in \mathbb{F}_p\Xi$ by

$$\overline{\overline{\xi}} \;:=\; \xi + J \;\in\; {}^{\mathbb{F}_p\Xi}\!/_{J}\;.$$

We get isomorphisms of $\mathbb{F}_p$-algebras

$$\mathbb{F}_p\mathrm{D}_{2p} \;\underset{\mathcal{P}_5}{\overset{\mathcal{P}_4}{\sim}}\; {}^{\mathbb{F}_p\Xi}\!/_{J}$$

which invert each other; cf. Lemma 89.

The images of the generators of D_{2p} under $\mathcal{P}_4$ are given as

$$\mathcal{P}_4(x) \,=\, \overline{\overline{E}} + \overline{\overline{F}} + \overline{\overline{\alpha}} + \overline{\overline{\beta}} + \overline{\overline{\beta\alpha}} \qquad \text{and} \qquad \mathcal{P}_4(y) \,=\, \overline{\overline{E}} - \overline{\overline{F}} + \overline{\overline{\beta}}\;.$$

The images of the generators under $\mathcal{P}_5$ are given as

$$\begin{aligned}
\mathcal{P}_5\big(\overline{\overline{E}}\big) &= (n+1)\sum_{k=0}^{p-1}(-1)^k x^k(1+y)\\
\mathcal{P}_5\big(\overline{\overline{F}}\big) &= (n+1)\left(1-y-\sum_{k=1}^{p-1}(-1)^k x^k(1+y)\right)\\
\mathcal{P}_5\big(\overline{\overline{\alpha}}\big) &= -x^{-1}-y-\sum_{k=1}^{p-2}(-1)^k x^k(1+y)\\
\mathcal{P}_5\big(\overline{\overline{\beta}}\big) &= -\sum_{k=1}^{p-1}(-1)^k x^k(1+y)\,.
\end{aligned}$$

Acknowledgements

Definition We define the set $\mathcal{H}$ of *persons* and *institutions* as

$$\mathcal{H} := \left\{ \begin{array}{l} \text{Dr. Matthias Künzer, Prof. Dr. Richard Dipper, Dr. Friederike Stoll,} \\ \text{University of Stuttgart, Franziska Müller and Juliane Deißler,} \\ \text{staff of the department of mathematics and supervisors of the Stud-Pool} \end{array} \right\},$$

and the set $\mathcal{A}$ of *activities*

$$\mathcal{A} := \left\{ \begin{array}{l} \text{offering interesting lectures, giving these lectures, spending a lot of time,} \\ \text{arousing interest in algebra, giving an interesting topic for the diploma thesis,} \\ \text{advising in case of technical problems, giving constructive criticisms,} \\ \text{supporting professionally and mentally, having patience, having confidence,} \\ \text{creating or preserving a pleasant and stimulating work environment} \end{array} \right\}.$$

Lemma Let $H \in \mathcal{H}$ be an arbitrary element of the set of persons and institutions. Then there exists a nonempty subset $U_H \subseteq \mathcal{A}$, such that H has done the activity a for me, for all activities $a \in U_H$.

Due to this fact, we obtain a necessary consequence in the following

Corollary Let $H \in \mathcal{H}$. Then I am very grateful for all activities $a \in U_H$, which H has done.

My special thanks go to Prof. Dr. Richard Dipper, who taught me a great number of lectures, and this in an excellent way. During all these lectures I was extraordinarily well supported and supervised by Dr. Friederike Stoll. Moreover, in case of problems or questions, whatever the subject, she was helpful at all times. Therefore special thanks go to her, as well.

Most of all, I thank Dr. Matthias Künzer, who supervised my diploma thesis. In his case the subset $U_{\text{Dr. Matthias Künzer}}$ even equals $\mathcal{A}$. I thank him for his helpfulness, the constance and amount of his commitment, and for the whole support he gave to me while writing this diploma thesis.

Conventions

Convention 1 Let A, B be sets and $f : A \longrightarrow B$ be a map. Let $X \subseteq A$ and $f(X) \subseteq Y \subseteq B$.

Then we write

$$f\big|_X^Y : X \longrightarrow Y \text{ for the restriction of } f \text{ to } X \text{ in the domain and to } Y \text{ in the codomain.}$$

In addition, in the case $Y = B$ we denote $f\big|_X := f\big|_X^B$, and in the case $X = A$ we denote $f\big|^Y := f\big|_A^Y$.

Convention 2 Let f be an arbitrary map between commutative rings and $l \in \mathbb{Z}_{\geq 0}$.

Then we denote the *l-th difference* $\Delta^l f$ *at the point* x

$$\Delta^l f(x) := f(x) \text{ for } l = 0 ,$$

and recursively

$$\Delta^l f(x) := \Delta^{l-1} f(x+1) - \Delta^{l-1} f(x) \text{ for } l \in \mathbb{Z}_{\geq 1} .$$

Convention 3 Let $a, b \in \mathbb{Z}$. We denote $[a, b] := \{ z \in \mathbb{Z} : a \leq z \leq b \}$.

Convention 4 Given $a \in \mathbb{R}$ and $b \in \mathbb{Z}$. Then we denote

$$\binom{a}{b} := \begin{cases} \frac{a(a-1)\cdots(a-b+1)}{b!} & \text{for } b \geq 0 , \\ 0 & \text{for } b < 0 . \end{cases}$$

Note that if $a \in \mathbb{Z}_{\geq 0}$ and $b \notin [0, a]$, then $\binom{a}{b} = 0$.

Convention 5 Let $(A, +)$ be an abelian group and $m \in \mathbb{Z}_{\geq 1}$.

Then we write for the m-ary direct sum of A

$$\underbrace{A \oplus \cdots \oplus A}_{m} =: A^{\oplus m} .$$

Further, if A is a commutative ring, we write for the m-ary cartesian product of A

$$A^{1 \times m} = \underbrace{A \times \cdots \times A}_{m} =: A^{\times m} .$$

Let $a = (a_j)_{j \in [1,m]} \in A^{\times m}$. Then we consider a as a row vektor.

Convention 6

Given a commutative ring A and $m \in \mathbb{Z}_{\geq 1}$, we denote by E_m the identity matrix in $A^{m\times m}$.

Convention 7 Let K be a commutative ring and $m \in \mathbb{Z}_{\geq 1}$. Let $(A_i\,,\alpha_i\,)$ be K-algebras for $i \in [1,m]$. Then we consider $\prod\limits_{i=1}^{m} A_i$ as a K-algebra via

$$\begin{array}{ccc} K & \longrightarrow & \prod\limits_{i=1}^{m} A_i \\ \kappa & \longmapsto & (\,\alpha_1(\kappa)\,,\,\ldots\,,\,\alpha_m(\kappa)\,)\,. \end{array}$$

Furthermore, let A, B be K-algebras, where A is commutative. Then we consider $A \underset{K}{\otimes} B$ as an A-algebra via

$$\begin{array}{ccc} A & \longrightarrow & A \underset{K}{\otimes} B \\ a & \longmapsto & a \otimes 1_B\,, \end{array}$$

cf. Lemma 91 *(iii)*.

Convention 8 Let G be a finite group. We denote the *hermitian scalar product*

$$\begin{array}{rcccl} {}_G(\,\cdot\,,\,\cdot\,) & : & \mathrm{Cf}(G)\times\mathrm{Cf}(G) & \longrightarrow & \mathbb{C} \\ & & (\,\varphi\ ,\ \psi\,) & \longmapsto & {}_G(\,\varphi\,,\,\psi\,) \ := \ \frac{1}{|G|}\sum\limits_{g\in G}\varphi(g)\overline{\psi(g)}\,, \end{array}$$

where $\mathrm{Cf}(G)$ denotes the space of complex-valued class functions on G, i.e. the space of maps from G to $\mathbb{C}$ that are constant on conjugacy classes.

Convention 9 Let A be a commutative ring and $a \in A$. We write

$$(a) := aA = \{ax : x \in A\}$$

for the principal ideal of A generated by a if the ring is unambiguous.

We sometimes write $0 := (0) = \{0\} = 0A$.

Convention 10 Let A be a ring, not necessarily commutative. Let $m \in \mathbb{Z}_{\geq 1}$ and $a_i \in A$ for $i \in [1,m]$. Then we write $\lhd a_1\,,\ldots,a_m \rhd_A$ for the (both-sided) ideal of A that is generated by the set $\{a_1\,,\ldots,a_m\}$.

Convention 11 Let A be a commutative ring and $x,y,a \in A$.

Then we write

$$x \equiv_a y \iff x \equiv_a y \text{ in } A \iff x - y \in aA\,.$$

This also applies to the case where x is contained in some subring B of A.

Convention 12 Let A be a set, $s,t \in \mathbb{Z}_{\geq 1}$ and $a, x_i, y_j \in A$ for $i \in [1,s]$ and $j \in [1,t]$.

Then we write

$$\begin{aligned}
(x_1, \ldots, x_s) \sqcup (y_1, \ldots, y_t) &:= (x_1, \ldots, x_s, y_1, \ldots, y_t)\,, \\
a \in (x_1, \ldots, x_s) &\Leftrightarrow \text{there exists } i \in [1,s] \text{ with } a = x_i\,, \\
(x_1, \ldots, x_s) \subseteq (y_1, \ldots, y_t) &\Leftrightarrow \text{there exists } k \in [1, t-s] \text{ with } (x_1, \ldots, x_s) = (y_k, \ldots, y_{k+s})\,.
\end{aligned}$$

Convention 13

Let K be a commutative ring and V be a K-module. Further, let $s \in \mathbb{Z}_{\geq 0}$ and $v_1, \ldots, v_s \in V$.

$$\begin{array}{l}
\text{Then we call the tuple } (v_1, \ldots, v_s) \text{ a } \textit{K-basis of V} \\
\qquad\qquad\qquad\qquad\qquad\qquad \Updownarrow \\
\text{the } K\text{-linear map} \quad f \;:\; K^{\oplus s} \longrightarrow V \\
\qquad\qquad\qquad\qquad\qquad\qquad (\mu_1, \ldots, \mu_s) \longmapsto \sum_{i=1}^{s} \mu_i v_i \quad \text{is bijective.}
\end{array}$$

If there exists such a K-basis for the K-module V as explained above, then we call V a *finitely generated free* K-module.

Convention 14

In order to indicate explicitly which part of a statement is to be shown, we use the character "!".

Convention 15 Let $K \subseteq \mathbb{C}$ be a subfield. So K is a field extension of $\mathbb{Q}$.

Then we call K an *algebraic number field* (or simply *number field*) if K is a finite field extension of $\mathbb{Q}$.

Chapter 1

Number theoretic preliminaries

Definition 16 Let $K \subseteq \mathbb{C}$ be a subfield. Then we denote

$$\begin{aligned} \mathcal{O} &:= \{\, z \in \mathbb{C} : \text{there exists a monic polynomial } f(X) \in \mathbb{Z}[X] \text{ such that } f(z) = 0 \,\} \\ &\quad (\text{ the ring of algebraic integers }), \\ \mathcal{O}_K &:= \mathcal{O} \cap K \\ &\quad (\text{ the ring of algebraic integers of } K \,). \end{aligned}$$

Furthermore, we introduce the following definitions, which are valid throughout the main part of this work and for the part "On binomial coefficients" of the appendix, i.e. for the Chapters 1 to 6 and Chapter B.

Definition 17 Suppose given a prime $p \in \mathbb{Z}_{\geq 3}$. Then we denote

$$\begin{aligned} n &:= \tfrac{p-1}{2} \in \mathbb{Z}, \\ \zeta &:= \zeta_p \quad (\text{ primitive } p\text{-th root of unity }), \\ \mu_{\zeta,\mathbb{Q}}(X) = \Phi_p(X) &:= X^{p-1} + \cdots + X^0, \\ \vartheta = \vartheta_p &:= \zeta + \zeta^{-1} - 2 \;=\; \zeta + \overline{\zeta} - 2 \in \mathbb{R} \cap \mathbb{Q}(\zeta), \\ \gamma = \gamma_p &:= \vartheta + 2 \;=\; \zeta + \zeta^{-1}, \\ {}_j\gamma = {}_j\gamma_p &:= \zeta^j + \zeta^{-j} \quad \text{for } j \in \mathbb{Z}. \end{aligned}$$

1.1 The Dedekind domain $\mathbb{Z}[\vartheta_p]$

Remark 18

(i) For $l \in \mathbb{Z}$ we have $\gamma_p \cdot {}_l\gamma_p = {}_{l+1}\gamma_p + {}_{l-1}\gamma_p$.

(ii) We have $\mathbb{Z}[\vartheta_p] = \mathbb{Z}[\gamma_p]$.

Proof of *(i)*. For $l \in \mathbb{Z}$ we calculate

$$\begin{aligned} \gamma \cdot {}_l\gamma &= (\zeta + \zeta^{-1})(\zeta^l + \zeta^{-l}) = \zeta^{l+1} + \zeta^{-l+1} + \zeta^{l-1} + \zeta^{-l-1} \\ &= \zeta^{l+1} + \zeta^{-(l+1)} + \zeta^{l-1} + \zeta^{-(l-1)} = {}_{l+1}\gamma + {}_{l-1}\gamma \,. \end{aligned}$$

Proof of *(ii)*. This is a simple consequence of $\gamma = \vartheta + 2$. □

Lemma 19 *Suppose given $j \in \mathbb{Z}_{\geq 1}$. Then there exist $a_{j,k} \in \mathbb{Z}$ for $k \in [0, j-1]$ such that*

$$\gamma_p^j = {}_j\gamma_p + \sum_{k=0}^{j-1} a_{j,k} \cdot {}_k\gamma_p \,.$$

Proof. This is shown by induction on j. For $j = 1$, we obtain $\gamma^1 = \zeta + \zeta^{-1} = {}_1\gamma$.

For the inductive step $j \to j+1$, we calculate

$$\begin{aligned} \gamma^{j+1} = \gamma \cdot \gamma^j &\overset{\text{I.H.}}{=} \gamma \left({}_j\gamma + \sum_{k=0}^{j-1} a_{j,k} \cdot {}_k\gamma \right) \\ &= \gamma \cdot {}_j\gamma + \sum_{k=0}^{j-1} a_{j,k} \cdot \gamma \cdot {}_k\gamma \overset{\text{R.18}}{\underset{(i)}{=}} {}_{j+1}\gamma + {}_{j-1}\gamma + \sum_{k=0}^{j-1} a_{j,k}({}_{k+1}\gamma + {}_{k-1}\gamma) \,. \end{aligned}$$

(Note that ${}_{-1}\gamma = \zeta^{-1} + \zeta^1 = {}_1\gamma$.) □

Lemma 20

(i) For $j \in \mathbb{Z}$, the element ${}_j\gamma_p$ belongs to $\mathbb{Z}[\gamma_p]$.

(ii) Let $M := \{ x \in \mathbb{Z}[\zeta_p] : x = \overline{x} \} = \mathbb{R} \cap \mathbb{Z}[\zeta_p]$.
Then the tuple $({}_i\gamma_p : i \in [1, n])$ is a $\mathbb{Z}$-linear basis of M.

Proof of *(i)*. First we show the statement for $j \in \mathbb{Z}_{\geq 0}$. This is shown by induction on j.

For $j = 0$, we obtain ${}_0\gamma = \zeta^0 + \zeta^{-0} = 2 \in \mathbb{Z}[\gamma]$.

Suppose given $j \in \mathbb{Z}_{\geq 1}$. For the inductive step $j-1 \to j$, we note that by Lemma 19 there exist $a_{j,k} \in \mathbb{Z}$ for $k \in [0, j-1]$ such that

$$\gamma^j = {}_j\gamma + \sum_{k=0}^{j-1} a_{j,k} \cdot {}_k\gamma \,.$$

$$\text{So} \quad {}_j\gamma = \gamma^j - \underbrace{\sum_{k=0}^{j-1} a_{j,k} \cdot \overbrace{{}_k\gamma}^{\overset{\text{I.H.}}{\downarrow} \in \mathbb{Z}[\gamma]}}_{\in \mathbb{Z}[\gamma]} \in \mathbb{Z}[\gamma] \,.$$

Therefore the statement is true for $j \in \mathbb{Z}_{\geq 0}$. Since ${}_j\gamma = {}_{-j}\gamma$, cf. Definition 17, the statement is true for all $j \in \mathbb{Z}$.

Proof of *(ii)*. First we note that the tuple $({}_i\gamma : i \in [1, n])$ is linearly independent over $\mathbb{Z}$.

We choose the $\mathbb{Z}$-linear basis $(\zeta^1, \zeta^2, \zeta^3, \ldots, \zeta^{p-1})$ of $\mathbb{Z}[\zeta]$.

Let $y = a_1\zeta^1 + a_2\zeta^2 + a_3\zeta^3 + \cdots + a_{p-3}\zeta^{p-3} + a_{p-2}\zeta^{p-2} + a_{p-1}\zeta^{p-1} \in M$, where $a_i \in \mathbb{Z}$ for $i \in [1, p-1]$.

Then $y = \overline{y}$, i.e.

$$\begin{aligned} & a_1\zeta^1 + a_2\zeta^2 + a_3\zeta^3 + \cdots + a_{p-3}\zeta^{p-3} + a_{p-2}\zeta^{p-2} + a_{p-1}\zeta^{p-1} \\ = \; & \overline{a_1\zeta^1 + a_2\zeta^2 + a_3\zeta^3 + \cdots + a_{p-3}\zeta^{p-3} + a_{p-2}\zeta^{p-2} + a_{p-1}\zeta^{p-1}} \\ = \; & a_1\overline{\zeta^1} + a_2\overline{\zeta^2} + a_3\overline{\zeta^3} + \cdots + a_{p-3}\overline{\zeta^{p-3}} + a_{p-2}\overline{\zeta^{p-2}} + a_{p-1}\overline{\zeta^{p-1}} \\ = \; & a_{p-1}\zeta^1 + a_{p-2}\zeta^2 + a_{p-3}\zeta^3 + \cdots + a_3\zeta^{p-3} + a_2\zeta^{p-2} + a_1\zeta^{p-1}\,. \end{aligned}$$

This implies that $a_i = a_{p-i}$ for $i \in [1, p-1]$.

Thus every element $y \in M$ is of the form $y = \sum_{k=1}^{n} a_k \cdot (\zeta^k + \zeta^{-k}) = \sum_{k=1}^{n} a_k \cdot {}_k\gamma$. □

Corollary 21 *We have*

$$M \;=\; \{\, x \in \mathbb{Z}[\zeta_p] : x = \overline{x} \,\} \;=\; \mathbb{R} \cap \mathbb{Z}[\zeta_p] \;=\; \mathbb{Z}[\gamma_p] \;=\; \mathbb{Z}[\vartheta_p]\,.$$

In particular, $\mathbb{Z}[\vartheta_p]$ has the $\mathbb{Z}$-linear basis $({}_i\gamma_p : i \in [1,n])$.

Proof. In

$$M \overset{\text{L.20}}{\underset{(ii)}{=}} \{\, x \in \mathbb{Z}[\zeta_p] : x = \overline{x} \,\} \;=\; \mathbb{R} \cap \mathbb{Z}[\zeta_p] \overset{!}{=} \mathbb{Z}[\gamma_p] \overset{\text{R.18}}{\underset{(ii)}{=}} \mathbb{Z}[\vartheta_p]\,,$$

we only have to show "$\overset{!}{=}$".

We prove the inclusion "$\supseteq$". This is a consequence of $\gamma = \zeta + \zeta^{-1} = \zeta + \zeta^{p-1} = \zeta + \overline{\zeta} \in \mathbb{Z}[\zeta] \cap \mathbb{R}$.

We prove the inclusion "$\subseteq$". By Lemma 20 *(ii)* we get that every element $y \in M$ is of the form

$$y = \sum_{k=1}^{n} a_k \cdot \underbrace{{}_k\gamma}_{\substack{\in \mathbb{Z}[\gamma] \\ \uparrow \\ \text{L.20 } (i)}} \in \mathbb{Z}[\gamma]\,,$$

where $a_i \in \mathbb{Z}$ for $i \in [1,n]$.

Since M equals $\mathbb{Z}[\vartheta]$, we obtain by Lemma 20 *(ii)* that $\mathbb{Z}[\vartheta]$ has the $\mathbb{Z}$-linear basis $({}_i\gamma : i \in [1,n])$. □

Lemma 22 *We have that $\mathbb{Z}[\vartheta_p]$ is the ring of algebraic integers of $\mathbb{Q}(\vartheta_p)$, i.e.*

$$\mathbb{Z}[\vartheta_p] \;=\; \mathcal{O}_{\mathbb{Q}(\vartheta_p)}\,,$$

cf. Definition 16.

Proof. We prove the inclusion "$\subseteq$". We have $\mathbb{Z}[\vartheta] \subseteq \mathcal{O}$, because $\vartheta = \zeta + \zeta^{-1} - 2 \in \mathcal{O}$ and $\mathbb{Z}[\vartheta] \subseteq \mathbb{Q}(\vartheta)$.

We prove the inclusion "$\supseteq$". We obtain

$$\mathcal{O}_{\mathbb{Q}(\vartheta)} \;=\; \mathcal{O} \cap \mathbb{Q}(\vartheta) \overset{\vartheta \in \mathbb{Q}(\zeta) \cap \mathbb{R}}{\subseteq} \mathcal{O} \cap \mathbb{Q}(\zeta) \cap \mathbb{R} \;=\; \mathcal{O}_{\mathbb{Q}(\zeta)} \cap \mathbb{R} \overset{(*)}{=} \mathbb{Z}[\zeta] \cap \mathbb{R} \overset{\text{C.21}}{=} \mathbb{Z}[\vartheta]\,,$$

where in $(*)$ we refer to [Neukirch 99, Ch. I, p. 60, Proposition (10.2)]. □

Corollary 23 *The ring $\mathbb{Z}[\vartheta_p]$ is a Dedekind domain.*

Proof. By Lemma 22 we have that $\mathbb{Z}[\vartheta] = \mathcal{O}_{\mathbb{Q}(\vartheta)}$. Hence it is a Dedekind domain; cf. Remark 132. □

1.2 The discriminant $\Delta_{\mathbb{Q}(\vartheta_p)|\mathbb{Q}}$

Lemma 24

(i1) *The extension* $\mathbb{Q}(\zeta_p)|\mathbb{Q}(\vartheta_p)$ *has degree* $[\mathbb{Q}(\zeta_p):\mathbb{Q}(\vartheta_p)]=2$.

It follows that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}(\vartheta_p)) \;=\; \{\,\mathrm{id}_{\mathbb{Q}(\zeta_p)}\,,\,c\,\}\,,$$

where c *denotes the complex conjugation, restricted to* $\mathbb{Q}(\zeta_p)$.

(i2) *The extension* $\mathbb{Q}(\vartheta_p)|\mathbb{Q}$ *has degree* $[\mathbb{Q}(\vartheta_p):\mathbb{Q}]=\frac{p-1}{2}=n$.

(i3) $\mathbb{Z}[\vartheta_p]$ *has the* $\mathbb{Z}$*-linear basis* $\big(\,\vartheta_p^0\,,\,\ldots\,,\,\vartheta_p^{n-1}\,\big)$.

(ii) *We have* $\Delta_{\mathbb{Q}(\zeta_p)|\mathbb{Q}(\vartheta_p)} \;=\; \vartheta_p(\vartheta_p+4)$.

(iii) *We have* $\mathrm{N}_{\mathbb{Q}(\vartheta_p)|\mathbb{Q}}(\Delta_{\mathbb{Q}(\zeta_p)|\mathbb{Q}(\vartheta_p)}) \;=\; (-1)^n\cdot p$.

(iv) *The absolute term* a_0 *in* $\mu_{\vartheta_p,\mathbb{Q}}(X)$ *is* $a_0=(-1)^n\cdot \mathrm{N}_{\mathbb{Q}(\vartheta_p)|\mathbb{Q}}(\vartheta_p)=p$.

(v) *For* $i\in\mathbb{Z}$ *we have* $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}\big(\zeta_p^i\big) \;=\; \begin{cases} -1 & \text{for } i\not\equiv_p 0\,,\\ p-1 & \text{for } i\equiv_p 0\,. \end{cases}$

(vi) *We have* $\Delta_{\mathbb{Q}(\zeta_p)|\mathbb{Q}} \;=\; (-1)^n\cdot p^{p-2}$.

Proof of *(i1, i2, i3)* and *(ii)*. We have the minimal polynomial

$\mu_{\zeta,\mathbb{Q}(\vartheta)}(X)=X^2-(2+\vartheta)X+1$ of ζ over $\mathbb{Q}(\vartheta)$, because $\mu_{\zeta,\mathbb{Q}(\vartheta)}(\zeta)=0$ and $\zeta\notin\mathbb{R}\supseteq\mathbb{Q}(\vartheta)$.

And therefore we have $[\mathbb{Q}(\zeta):\mathbb{Q}(\vartheta)]=\deg(\mu_{\zeta,\mathbb{Q}(\vartheta)}(X))=2$.

So the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta))$ contains two elements. Of course $\mathrm{id}_{\mathbb{Q}(\zeta)}$ is contained in $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta))$. We have

$$c(\vartheta) \;=\; c\big(\zeta^1+\zeta^{-1}-2\big) \;=\; \overline{\zeta^1}+\overline{\zeta^{-1}}-2 \;=\; \zeta^{-1}+\zeta^1-2 \;=\; \vartheta\,.$$

So c is also contained in $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta))$. Moreover, $c(\zeta)=\zeta^{-1}\neq\zeta$. Hence $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta))=\{\mathrm{id}_{\mathbb{Q}(\zeta)},c\}$.

By the multiplicativity of degrees and knowing that $\deg(\mu_{\zeta,\mathbb{Q}}(X)) \overset{\text{D.17}}{=} \deg(X^{p-1}+\cdots+X^0)=p-1$, we get

$$[\mathbb{Q}(\vartheta):\mathbb{Q}] \;=\; \frac{[\mathbb{Q}(\zeta):\mathbb{Q}]}{[\mathbb{Q}(\zeta):\mathbb{Q}(\vartheta)]} \;=\; \frac{p-1}{2} \;=\; n\,.$$

So the tuple $(\,\vartheta^0,\ldots,\vartheta^{n-1}\,)$ is linearly independent over $\mathbb{Q}\supseteq\mathbb{Z}$ and since $\vartheta\in\mathcal{O}$ we have $\mu_{\vartheta,\mathbb{Q}}(X)\in\mathbb{Z}[X]$. Thus we get that $(\,\vartheta^0,\ldots,\vartheta^{n-1}\,)$ is a $\mathbb{Z}$-linear basis of $\mathbb{Z}[\vartheta]$.

Further we get with Remark 111 and $\mu_{\zeta,\mathbb{Q}(\vartheta)}(X)$ that

$$\Delta_{\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)} \;=\; (2+\vartheta)^2-4\cdot 1 \;=\; \vartheta^2+4\vartheta\,.$$

Proof of *(iii)* and *(iv)*. From *(ii)* it follows that

$$\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\Delta_{\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)}) \;=\; \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta(\vartheta+4)) \;=\; \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta)\,\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta+4)\,.$$

We prepare

$$(1)\qquad \mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)}(\zeta-1) \overset{(*)}{=} (\zeta-1)(\overline{\zeta}-1) \;=\; (\zeta-1)(\zeta^{-1}-1) \;=\; 2-\zeta-\zeta^{-1} \;=\; -\vartheta\,,$$

$$\mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)}(\zeta+1) \overset{(*)}{=} (\zeta+1)(\overline{\zeta}+1) = (\zeta+1)(\zeta^{-1}+1) = 2+\zeta+\zeta^{-1} = \vartheta+4\,, \tag{2}$$

and

$$\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(-1) = (-1)^n\,, \tag{3}$$

where in $(*)$ we refer to [Neukirch 99, Ch. I, p. 9, Proposition (2.6.iii)] and recall that by *(i1)* we have $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)) = \{\,\mathrm{id}_{\mathbb{Q}(\zeta)}\,, c\,\}$; cf. also Corollary 114 for the corresponding statement for the trace.

We have

$$\mu_{\zeta-1,\mathbb{Q}}(X) = \Phi_p(X+1) \overset{\text{D.17}}{=} \underbrace{(X+1)^{p-1}+(X+1)^{p-2}+\cdots+(X+1)^1+(X+1)^0}_{\text{has absolute term } p}\,,$$

whence

$$\mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta-1) = (-1)^{p-1}\cdot p = p\,. \tag{4}$$

Further we have

$$\mu_{\zeta+1,\mathbb{Q}}(X) = \Phi_p(X-1) \overset{\text{D.17}}{=} \underbrace{\underbrace{(X-1)^{p-1}}_{+1}+\underbrace{(X-1)^{p-2}}_{-1}+\cdots+\underbrace{(X-1)^1}_{-1}+\underbrace{(X-1)^0}_{+1}}_{\text{has absolute term } 1}\,,$$

whence

$$\mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta+1) = (-1)^{p-1}\cdot 1 = 1\,. \tag{5}$$

From (1) and (4) we get

$$\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(-\vartheta) = \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)}(\zeta-1)) = \mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta-1) = p\,. \tag{6}$$

So we get with (3) and (6)

$$\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta) = \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}((-1)(-\vartheta)) = \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(-1)\,\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(-\vartheta) = (-1)^n\cdot p\,. \tag{7}$$

Since $\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta) = (-1)^n\cdot a_0$ this shows *(iv)*.

From (2) and (5) we get

$$\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta+4) = \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)}(\zeta+1)) = \mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta+1) = 1\,. \tag{8}$$

And overall we get with (7) and (8)

$$\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\Delta_{\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)}) = \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta)\,\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta+4) = (-1)^n\cdot p\,.$$

Proof of *(v)*.

Case 1 : Let $i=0$. Then we have

$$\mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\zeta^0\right) = \mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(1) = [\mathbb{Q}(\zeta):\mathbb{Q}] = p-1\,. \tag{9}$$

Case 2 : Let $i\in[1,p-1]$. We choose the $\mathbb{Q}$-linear basis $(\,\zeta^0,\ldots,\zeta^{p-2}\,)$ of $\mathbb{Q}(\zeta)$.

- For $j\in[0,p-i-2]$ the exponent k of $\zeta^i\cdot\zeta^j = \zeta^k$ is in the set $[i,p-2]$. Therefore we have no contribution of the images of ζ^j to the trace.

- For $j = p-i-1$ we have $\zeta^i \cdot \zeta^j = \zeta^i \cdot \zeta^{p-i-1} = \zeta^{p-1} = -\sum_{l=0}^{p-2} \zeta^l$. Therefore we have a contribution of -1 to the trace.
- Finally let $j \in [p-i, p-2]$. Then the exponent k of $\zeta^i \cdot \zeta^j = \zeta^k$ is in the set $[1, i-2]$. Therefore we have no contribution of the images of ζ^j to the trace.

Thus, summarized we have $\mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\zeta^i\right) = -1$.

Now, we generalize the cases 1 and 2.

First, we consider the generalization of **Case 1**, that $i \in \mathbb{Z}$ with $i \equiv_p 0$. Then there exists $k \in \mathbb{Z}$ with $i = kp$ and so

$$\mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\zeta^i\right) = \mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\zeta^{kp}\right) = \mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(1) \overset{(9)}{=} p-1\,.$$

Finally, we consider the generalization of **Case 2**, that $i \in \mathbb{Z}$ with $i \not\equiv_p 0$. Then there exists $k \in \mathbb{Z}$ with $i + kp =: j \in [1, p-1]$ and so

$$\mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\zeta^i\right) = \mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\zeta^{j-kp}\right) = \mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\zeta^j\right) \overset{\textbf{Case 2}}{=} -1\,.$$

Proof of *(vi)*. For $p = 3$ we have

$$\Delta_{\mathbb{Q}(\zeta_3)|\mathbb{Q}} \overset{\mathrm{D.110}}{=} \det\begin{pmatrix} \mathrm{Tr}\left(\zeta_3^0\right) & \mathrm{Tr}\left(\zeta_3^1\right) \\ \mathrm{Tr}\left(\zeta_3^1\right) & \mathrm{Tr}\left(\zeta_3^2\right) \end{pmatrix} \overset{(v)}{=} \det\begin{pmatrix} 2 & -1 \\ -1 & -1 \end{pmatrix} = -3 = (-1)^{\frac{3-1}{2}} \cdot 3^{3-2}\,.$$

For $p > 3$ we have

$$\Delta_{\mathbb{Q}(\zeta)|\mathbb{Q}} \overset{\mathrm{D.110}}{=} \det\underbrace{\left(\left(\mathrm{Tr}_{\mathbb{Q}(\zeta)|\mathbb{Q}}\left(\zeta^i \cdot \zeta^j\right)\right)_{i,j\in[0,p-2]}\right)}_{\in \mathbb{Q}^{(p-1)\times(p-1)}}$$

$$= \det\begin{pmatrix} \mathrm{Tr}\left(\zeta^0\right) & \mathrm{Tr}\left(\zeta^1\right) & \mathrm{Tr}\left(\zeta^2\right) & \mathrm{Tr}\left(\zeta^3\right) & \cdots & \cdots & \cdots & \mathrm{Tr}\left(\zeta^{p-3}\right) & \mathrm{Tr}\left(\zeta^{p-2}\right) \\ \mathrm{Tr}\left(\zeta^1\right) & \mathrm{Tr}\left(\zeta^2\right) & \mathrm{Tr}\left(\zeta^3\right) & \mathrm{Tr}\left(\zeta^4\right) & \cdots & \cdots & \cdots & \mathrm{Tr}\left(\zeta^{p-2}\right) & \mathrm{Tr}\left(\zeta^{p-1}\right) \\ \mathrm{Tr}\left(\zeta^2\right) & \mathrm{Tr}\left(\zeta^3\right) & \mathrm{Tr}\left(\zeta^4\right) & \mathrm{Tr}\left(\zeta^5\right) & \cdots & \cdots & \cdots & \mathrm{Tr}\left(\zeta^{p-1}\right) & \mathrm{Tr}\left(\zeta^p\right) \\ \mathrm{Tr}\left(\zeta^3\right) & \mathrm{Tr}\left(\zeta^4\right) & \mathrm{Tr}\left(\zeta^5\right) & \mathrm{Tr}\left(\zeta^6\right) & \cdots & \cdots & \cdots & \mathrm{Tr}\left(\zeta^p\right) & \mathrm{Tr}\left(\zeta^{p+1}\right) \\ \vdots & \vdots & \vdots & \vdots & & & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \iddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \iddots & & & \vdots & \vdots \\ \mathrm{Tr}\left(\zeta^{p-3}\right) & \mathrm{Tr}\left(\zeta^{p-2}\right) & \mathrm{Tr}\left(\zeta^{p-1}\right) & \mathrm{Tr}\left(\zeta^p\right) & \cdots & \cdots & \cdots & \mathrm{Tr}\left(\zeta^{2p-6}\right) & \mathrm{Tr}\left(\zeta^{2p-5}\right) \\ \mathrm{Tr}\left(\zeta^{p-2}\right) & \mathrm{Tr}\left(\zeta^{p-1}\right) & \mathrm{Tr}\left(\zeta^p\right) & \mathrm{Tr}\left(\zeta^{p+1}\right) & \cdots & \cdots & \cdots & \mathrm{Tr}\left(\zeta^{2p-5}\right) & \mathrm{Tr}\left(\zeta^{2p-4}\right) \end{pmatrix}$$

$$\overset{(v)}{=} \det\begin{pmatrix} p-1 & -1 & -1 & -1 & \cdots & \cdots & \cdots & -1 & -1 \\ -1 & -1 & -1 & -1 & \cdots & \cdots & \cdots & -1 & -1 \\ -1 & -1 & -1 & -1 & \cdots & \cdots & \cdots & -1 & p-1 \\ -1 & -1 & -1 & -1 & \cdots & \cdots & \cdots & p-1 & -1 \\ \vdots & \vdots & \vdots & \vdots & & & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \iddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \iddots & & & \vdots & \vdots \\ -1 & -1 & -1 & p-1 & \cdots & \cdots & \cdots & -1 & -1 \\ -1 & -1 & p-1 & -1 & \cdots & \cdots & \cdots & -1 & -1 \end{pmatrix}$$

$$= \det \begin{pmatrix} p & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 \\ -1 & -1 & -1 & -1 & \cdots & \cdots & \cdots & -1 & -1 \\ 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & p \\ 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & p & 0 \\ \vdots & \vdots & \vdots & \vdots & & & \iddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \iddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \iddots & & & \vdots & \vdots \\ 0 & 0 & 0 & p & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & 0 & p & 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

$$= p^{p-2} \cdot \det \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 \\ -1 & -1 & -1 & -1 & \cdots & \cdots & \cdots & -1 & -1 \\ 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & & & \iddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \iddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \iddots & & & \vdots & \vdots \\ 0 & 0 & 0 & 1 & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

$$= p^{p-2} \cdot \det \left(\begin{array}{cc|ccccccc} 1 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & -1 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & & & \iddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \iddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \iddots & & & \vdots & \vdots \\ 0 & 0 & 0 & 1 & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 & 0 \end{array}\right)$$

$$= p^{p-2} \cdot \det \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \det \underbrace{\begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & 0 & 1 \\ 0 & 0 & \cdots & \cdots & \cdots & 1 & 0 \\ \vdots & \vdots & & & \iddots & \vdots & \vdots \\ \vdots & \vdots & & \iddots & & \vdots & \vdots \\ \vdots & \vdots & \iddots & & & \vdots & \vdots \\ 0 & 1 & \cdots & \cdots & \cdots & 0 & 0 \\ 1 & 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}}_{\in \mathbb{Q}^{(p-3)\times(p-3)}}$$

$$= p^{p-2} \cdot (-1) \cdot \operatorname{sgn}\left((1, p-3)(2, p-4) \cdots \left(\frac{p-3}{2} - 1, \frac{p-3}{2} + 2\right)\left(\frac{p-3}{2}, \frac{p-3}{2} + 1\right)\right)$$

$$= p^{p-2} \cdot (-1) \cdot (-1)^{\frac{p-3}{2}} = (-1)^{\frac{p-1}{2}} \cdot p^{p-2} = (-1)^n \cdot p^{p-2}\,.$$

□

Lemma 25 *We have*

$$\Delta_{\mathbb{Q}(\vartheta_p)|\mathbb{Q}} = \pm p^{\frac{p-3}{2}}.$$

Proof. We apply Lemma 112 to the case $(F|L|K) = (\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)|\mathbb{Q})$ to obtain

$$\Delta_{\mathbb{Q}(\zeta)|\mathbb{Q}} = \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}\left(\Delta_{\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)}\right) \cdot \Delta_{\mathbb{Q}(\vartheta)|\mathbb{Q}}^{[\mathbb{Q}(\zeta):\mathbb{Q}(\vartheta)]}.$$

By Lemma 24 *(i1, iii, vi)* it follows

$$(-1)^n \cdot p^{p-2} = (-1)^n \cdot p \cdot \Delta_{\mathbb{Q}(\vartheta)|\mathbb{Q}}^2 \cdot$$

So we get

$$\Delta_{\mathbb{Q}(\vartheta)|\mathbb{Q}} = \pm p^{\frac{p-3}{2}}.$$

□

1.3 The Galois group of $\mathbb{Q}(\vartheta_p)$ over $\mathbb{Q}$

Notation 26 We consider the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$, which has order $p-1$.

Denoting

$$\begin{array}{rccc} \hat{\sigma}_i & : & \mathbb{Q}(\zeta_p) & \longrightarrow & \mathbb{Q}(\zeta_p) \\ & & \zeta_p & \longmapsto & \zeta_p^i \end{array}$$

for $i \in [1, p-1]$, we get $\mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) = \{\, \hat{\sigma}_i \,:\, i \in [1, p-1] \,\}$.

Then the Galois group $\mathrm{Gal}(\mathbb{Q}(\vartheta_p)|\mathbb{Q})$ of $\mathbb{Q}(\vartheta_p)$ over $\mathbb{Q}$ is given by

$$\mathrm{Gal}(\mathbb{Q}(\vartheta_p)|\mathbb{Q}) \;=\; \{\, \sigma_i \,:\, i \in [1, n] \,\}\,,$$

where $\sigma_i := \hat{\sigma}_i\big|_{\mathbb{Q}(\vartheta_p)}^{\mathbb{Q}(\vartheta_p)}$ for $i \in [1, n]$; cf. Convention 1.

Proof. We have the short exact sequence

$$\overbrace{\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta))}^{\substack{\text{cf. L.24 } (i1) \\ \downarrow \\ |\cdot| = 2}} \;\hookrightarrow\; \overbrace{\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})}^{|\cdot| = p-1} \;\xrightarrow{f}\; \overbrace{\mathrm{Gal}(\mathbb{Q}(\vartheta)|\mathbb{Q})}^{\substack{\text{cf. L.24 } (i2) \\ \downarrow \\ |\cdot| = n}}$$

$$\hat{\sigma}_i \qquad\longmapsto\quad f(\hat{\sigma}_i) := \hat{\sigma}_i\big|_{\mathbb{Q}(\vartheta)}^{\mathbb{Q}(\vartheta)} \quad \text{for } i \in [1, p-1]\,,$$

cf. [Lang 02, Ch. VI, §1, p. 265, Theorem 1.10] applied to the case
$(K, k, G, F, H) = (\mathbb{Q}(\zeta), \mathbb{Q}, \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}), \mathbb{Q}(\vartheta), \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(\vartheta)))$.

For $i \in [1, n]$ we have

$$\hat{\sigma}_i(\vartheta + 2) = \hat{\sigma}_i\big(\zeta + \zeta^{-1}\big) = \zeta^i + \zeta^{-i} = \zeta^{i-p} + \zeta^{p-i} = \zeta^{-(p-i)} + \zeta^{p-i} = \hat{\sigma}_{p-i}\big(\zeta + \zeta^{-1}\big) = \hat{\sigma}_{p-i}(\vartheta + 2)\,,$$

whence $f(\hat{\sigma}_i) = f(\hat{\sigma}_{p-i})$ for $i \in [1, n]$. Writing $\sigma_i := \hat{\sigma}_i\big|_{\mathbb{Q}(\vartheta)}^{\mathbb{Q}(\vartheta)}$ for $i \in [1, n]$, we therefore get

$$\mathrm{Gal}(\mathbb{Q}(\vartheta)|\mathbb{Q}) \;=\; \{\, \sigma_i \,:\, i \in [1, n] \,\}\,.$$

□

1.4 Ramification

1.4.1 The ideal $\vartheta_p\mathbb{Z}[\vartheta_p]$ over $p\mathbb{Z}$

Lemma 27

(i) *We have the isomorphism of rings*

$$\mathbb{F}_p \xrightarrow{\sim} \mathbb{Z}[\vartheta_p]\Big/\vartheta_p\mathbb{Z}[\vartheta_p]\,,\ 1 \longmapsto 1+\vartheta_p\mathbb{Z}[\vartheta_p]\,.$$

In particular, $\vartheta_p\mathbb{Z}[\vartheta_p]$ is maximal ideal, hence a prime ideal of $\mathbb{Z}[\vartheta_p]$.

(ii) *We have the equality of ideals*

$$\vartheta_p\mathbb{Z}[\vartheta_p]\cap\mathbb{Z} = p\mathbb{Z}\,.$$

(iii) *We have the isomorphism of rings*

$$\mathbb{F}_p \xrightarrow{\sim} \mathbb{Z}[\zeta_p]\Big/(1-\zeta_p)\mathbb{Z}[\zeta_p]\,,\ 1 \longmapsto 1+(1-\zeta_p)\mathbb{Z}[\zeta_p]\,.$$

In particular, $(1-\zeta_p)\mathbb{Z}[\zeta_p]$ is maximal ideal, hence a prime ideal of $\mathbb{Z}[\zeta_p]$.

(iv) *We have the equality of ideals*

$$(1-\zeta_p)\mathbb{Z}[\zeta_p]\cap\mathbb{Z} = p\mathbb{Z}\,.$$

Proof of *(i)* and *(ii)*. We have

$$\det_{\mathbb{Z}}\begin{pmatrix}\mathbb{Z}[\vartheta] & \xrightarrow{(-)\vartheta} & \mathbb{Z}[\vartheta]\\ x & \longmapsto & x\vartheta\end{pmatrix} = \mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta) \overset{\text{L.24}}{\underset{(iv)}{=}} (-1)^n\cdot p\,.$$

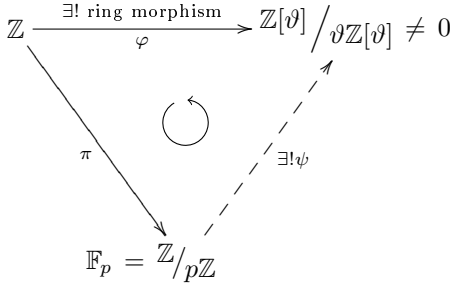
Therefore we get that

$$(*)\qquad \left|\mathbb{Z}[\vartheta]\Big/\vartheta\mathbb{Z}[\vartheta]\right| = |(-1)^n\cdot p| = p\,.$$

By Lemma 24 *(iv)* we get that $\vartheta|p$ and so $p\mathbb{Z}\subseteq\vartheta\mathbb{Z}[\vartheta]$.

By this we get that there exists a unique ring morphism ψ fitting into the following commutative triangle.

(1)



Since $\mathbb{F}_p$ is a field we get that ψ is injective. Considering the injectivity and through $(*)$ we get that ψ is surjective and this shows *(i)*.

Further we see that on the one hand

$$\ker(\varphi) = \left\{\, z\in\mathbb{Z} : z\in\vartheta\mathbb{Z}[\vartheta]\,\right\} = \mathbb{Z}\cap\vartheta\mathbb{Z}[\vartheta]\,,$$

and on the other hand with the commutativity in (1)

$$\ker(\varphi) = \ker(\psi\circ\pi) \overset{\psi\ \text{inj.}}{=} \ker(\pi) = p\mathbb{Z}\,.$$

Proof of *(iii)* and *(iv)*. We have

$$\mu_{1-\zeta,\mathbb{Q}}(X) = \Phi_p(1-X) \overset{\text{D.17}}{=} \underbrace{(1-X)^{p-1} + (1-X)^{p-2} + \cdots + (1-X)^1 + (1-X)^0}_{\text{has absolute term } p},$$

whence

$$\mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(1-\zeta) \;=\; \pm p.$$

Therefore we have

$$\det_{\mathbb{Z}}\begin{pmatrix} \mathbb{Z}[\zeta] & \overset{(-)(1-\zeta)}{\longrightarrow} & \mathbb{Z}[\zeta] \\ x & \longmapsto & x\cdot(1-\zeta) \end{pmatrix} \;=\; \mathrm{N}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(1-\zeta) \;=\; \pm p\,.$$

Therefore we get that

$$(**) \qquad \Big|\mathbb{Z}[\zeta]\Big/(1-\zeta)\mathbb{Z}[\zeta]\Big| = |\pm p| = p\,.$$

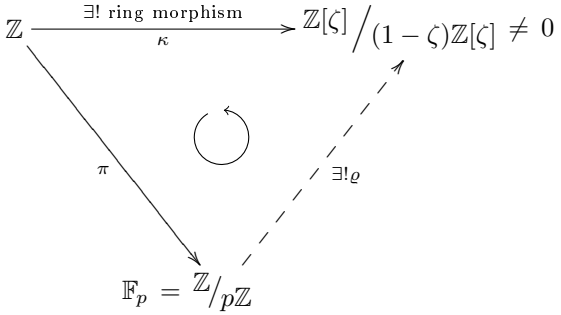
Since $(1-\zeta)\cdot(\zeta^{p-1}-1) = (1-\zeta)\cdot(\zeta^{-1}-1) = \zeta^{-1}-2+\zeta = \vartheta$, we get the divisor chain

$$1-\zeta \quad \text{divides} \quad \vartheta \quad \underset{\text{L.24}\,(iv)}{\overset{\uparrow}{\text{divides}}} \quad p\,,$$

so that $p\mathbb{Z} \subseteq (1-\zeta)\mathbb{Z}[\zeta]$.

By this we get that there exists a unique ring morphism ϱ fitting into the following commutative triangle.

(2)



Since $\mathbb{F}_p$ is a field we get that ϱ is injective. Considering the injectivity and through $(**)$ we get that ϱ is surjective and this shows *(iii)*.

Further we see that on the one hand

$$\ker(\kappa) \;=\; \big\{\, z\in\mathbb{Z} \,:\, z\in(1-\zeta)\mathbb{Z}[\zeta] \,\big\} \;=\; \mathbb{Z}\cap(1-\zeta)\mathbb{Z}[\zeta]\,,$$

and on the other hand with the commutativity in (2)

$$\ker(\kappa) \;=\; \ker(\varrho\circ\pi) \overset{\varrho \text{ inj.}}{=} \ker(\pi) \;=\; p\mathbb{Z}\,.$$

□

Remark 28

(i) *For* $x\in\mathbb{Z}[\vartheta_p]$ *we have* $x\mathbb{Z}[\zeta_p]\cap\mathbb{Z}[\vartheta_p] = x\mathbb{Z}[\vartheta_p]$.

(ii) *For* $i\in[1,p-1]$ *there exists* $u\in\mathrm{U}(\mathbb{Z}[\zeta_p])$ *such that* $\zeta_p^i - 1 = u(\zeta_p-1)$.

(iii) *For* $s\in\mathbb{Z}_{\geq 0}$ *and* $\sigma\in\mathrm{Gal}(\mathbb{Q}(\vartheta_p)|\mathbb{Q})$, *we have*

$$\sigma\big(\vartheta_p^s\mathbb{Z}[\vartheta_p]\big) \;=\; \vartheta_p^s\mathbb{Z}[\vartheta_p]\,.$$

Proof of *(i)*. The statement is true for $x = 0$. Given $x \in \mathbb{Z}[\vartheta] \setminus \{0\}$, then we have

$$\begin{aligned} x\mathbb{Z}[\zeta] \cap \mathbb{Z}[\vartheta] &\overset{\underset{(*)}{\text{L.22}}}{=} x\mathcal{O}_{\mathbb{Q}(\zeta)} \cap \mathcal{O}_{\mathbb{Q}(\vartheta)} &&= x\mathcal{O} \cap \underbrace{x\mathbb{Q}(\zeta)}_{=\mathbb{Q}(\zeta)\supseteq\mathbb{Q}(\vartheta)} \cap \underbrace{\mathcal{O}}_{\supseteq x\mathcal{O}} \cap \mathbb{Q}(\vartheta) \\ &= x\mathcal{O} \cap \underbrace{\mathbb{Q}(\vartheta)}_{=x\mathbb{Q}(\vartheta)} &&= x\mathcal{O} \cap x\mathbb{Q}(\vartheta) \\ &= x\mathcal{O}_{\mathbb{Q}(\vartheta)} &&\overset{\text{L.22}}{=} x\mathbb{Z}[\vartheta]\,, \end{aligned}$$

where in $(*)$ we refer to [Neukirch 99, Ch. I, p. 60, Proposition (10.2)].

Proof of *(ii)*. We have $\frac{\zeta^i-1}{\zeta-1} = \zeta^0 + \cdots + \zeta^{i-1} \in \mathbb{Z}[\zeta]$.

For $i \in [1, p-1]$ there exists $j \in \mathbb{Z}_{\geq 1}$ with $ij \equiv_p 1$, so that $\zeta^{ij} = \zeta^1$.

Hence we have

$$\frac{\zeta-1}{\zeta^i-1} = \frac{\left(\zeta^i\right)^j-1}{\zeta^i-1} = \left(\zeta^i\right)^0 + \left(\zeta^i\right)^1 + \left(\zeta^i\right)^2 + \cdots + \left(\zeta^i\right)^{j-1} \in \mathbb{Z}\left[\zeta^i\right] = \mathbb{Z}[\zeta]\,.$$

Thus our desired unit is $u := \frac{\zeta^i-1}{\zeta-1} \in \mathrm{U}(\mathbb{Z}[\zeta])$.

Proof of *(iii)*. We show that $\sigma_i(\vartheta\mathbb{Z}[\vartheta]) \overset{!}{=} \vartheta\mathbb{Z}[\vartheta]$ for $i \in [1, n]$; cf. Notation 26. In $\mathbb{Z}[\zeta]$ we have

$$(1)\quad \vartheta\mathbb{Z}[\zeta] = \underbrace{\big((\zeta-1)(\overline{\zeta}-1)\big)}_{=-\vartheta}\mathbb{Z}[\zeta] \overset{(ii)}{=} \big((\zeta^i-1)(\overline{\zeta}^i-1)\big)\mathbb{Z}[\zeta] = \hat{\sigma}_i\big(\big((\zeta-1)(\overline{\zeta}-1)\big)\mathbb{Z}[\zeta]\big) = \hat{\sigma}_i(\vartheta\mathbb{Z}[\zeta])\,.$$

We note that

$$\hat{\sigma}_i(\mathbb{Z}[\vartheta]) \overset{\text{L.22}}{=} \hat{\sigma}_i(\mathcal{O} \cap \mathbb{Q}(\vartheta)) \subseteq \mathbb{Z}[\vartheta] \text{ for } i \in [1, n]\,,$$

because $\hat{\sigma}_i$ maps an algebraic integer to an algebraic integer. Similarly, we have $\hat{\sigma}_i^{-1}(\mathbb{Z}[\vartheta]) \subseteq \mathbb{Z}[\vartheta]$, so that $\mathbb{Z}[\vartheta] \subseteq \hat{\sigma}_i(\mathbb{Z}[\vartheta])$, whence altogether

$$(2)\qquad \hat{\sigma}_i(\mathbb{Z}[\vartheta]) = \mathbb{Z}[\vartheta] \text{ for } i \in [1, n]\,.$$

So we get

$$(3)\qquad \sigma_i(\vartheta\mathbb{Z}[\vartheta]) \overset{(i)}{=} \hat{\sigma}_i(\vartheta\mathbb{Z}[\zeta] \cap \mathbb{Z}[\vartheta]) = \hat{\sigma}_i(\vartheta\mathbb{Z}[\zeta]) \cap \hat{\sigma}_i(\mathbb{Z}[\vartheta]) \overset{\underset{(2)}{(1)}}{=} \vartheta\mathbb{Z}[\zeta] \cap \mathbb{Z}[\vartheta] \overset{(i)}{=} \vartheta\mathbb{Z}[\vartheta]\,.$$

Hence, given $s \in \mathbb{Z}_{\geq 0}$, we obtain

$$\sigma_i(\vartheta^s\mathbb{Z}[\vartheta]) = \sigma_i((\vartheta\mathbb{Z}[\vartheta])^s) = (\sigma_i(\vartheta\mathbb{Z}[\vartheta]))^s \overset{(3)}{=} (\vartheta\mathbb{Z}[\vartheta])^s = \vartheta^s\mathbb{Z}[\vartheta]\,.$$

□

Lemma 29 *We have $(p) = (\vartheta_p)^n$. Therefore (p) is totally ramified in $\mathbb{Z}[\vartheta_p]$.*

Proof. By Corollary 23 there exist $s \in \mathbb{Z}_{\geq 1}$ and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of $\mathbb{Z}[\vartheta]$ such that

$$(1)\qquad (p) = \mathfrak{p}_1 \cdots \mathfrak{p}_s\,,$$

cf. Lemma 135 *(ii)*.

By Lemma 24 *(iv)* we get that $\vartheta | p$ in $\mathbb{Z}[\vartheta]$. So there exists $x \in \mathbb{Z}[\vartheta]$ with $p = \vartheta x$ and therefore

$$(p) = (\vartheta)(x)\,.$$

By this and by Lemma 27 *(i)* we can assume that the prime ideal $\mathfrak{p}_1$ is equal to (ϑ).

The Galois group $\mathrm{Gal}(\mathbb{Q}(\vartheta)|\mathbb{Q})$ permutes transitively the prime ideals in the prime ideal decomposition in (1), i.e. for $j \in [1,s]$ there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\vartheta)|\mathbb{Q})$ with $\sigma(\mathfrak{p}_1) = \sigma((\vartheta)) = \mathfrak{p}_j$; cf. [Neukirch 99, Ch. I, p. 54, Proposition (9.1)].

By Remark 28 *(iii)* we therefore get that

$$(p) \;=\; (\vartheta)^s\,. \tag{2}$$

Consider the embeddings

$$\vartheta^s\mathbb{Z}[\vartheta] \hookrightarrow \vartheta^{s-1}\mathbb{Z}[\vartheta] \hookrightarrow \ldots \hookrightarrow \vartheta^2\mathbb{Z}[\vartheta] \hookrightarrow \vartheta\mathbb{Z}[\vartheta] \hookrightarrow \mathbb{Z}[\vartheta]$$

By Lemma 27 *(i)* and using the isomorphism theorem each of these embeddings has index p and therefore the embeding $(\vartheta)^s = \vartheta^s\mathbb{Z}[\vartheta] \hookrightarrow \mathbb{Z}[\vartheta]$ has index p^s. (3)

So we get

$$\begin{array}{ccc} \left|\mathbb{Z}[\vartheta]\Big/(\vartheta)^s\right| & \overset{(3)}{=} & p^s \\ \| \ {\scriptstyle (2)} & & \\ \left|\mathbb{Z}[\vartheta]\Big/(p)\right| & \overset{(*)}{=} & \left|\mathbb{Z}^{\oplus n}\Big/p\mathbb{Z}^{\oplus n}\right| \;=\; p^n\,, \end{array}$$

where in $(*)$ we refer to Lemma 24 *(i3)*. So we have $s = n$. Consequently, (2) yields $(p) = (\vartheta)^n$. □

Remark 30 *For $k \in \mathbb{Z}_{\geq 0}$ we have*

$$(\zeta_p - 1)^{2k}\mathbb{Z}[\zeta_p] = \vartheta_p^k\mathbb{Z}[\zeta_p]\,.$$

Given $x, y \in \mathbb{Z}[\vartheta_p]$, then we have

$$x \equiv_{(\zeta_p-1)^{2k}} y \;\; \textit{in } \mathbb{Z}[\zeta_p] \iff x \equiv_{\vartheta_p^k} y \;\; \textit{in } \mathbb{Z}[\vartheta_p]\,.$$

Proof. For $k \in \mathbb{Z}_{\geq 0}$ we have

$$(*)\quad \vartheta^k\mathbb{Z}[\zeta] \;=\; (\vartheta\mathbb{Z}[\zeta])^k \;=\; ((-\vartheta)\mathbb{Z}[\zeta])^k \;=\; \big((\zeta-1)(\overline{\zeta}-1)\mathbb{Z}[\zeta]\big)^k \underset{(ii)}{\overset{\text{R.28}}{=}} \big((\zeta-1)^2\mathbb{Z}[\zeta]\big)^k \;=\; (\zeta-1)^{2k}\mathbb{Z}[\zeta]$$

Suppose given $x, y \in \mathbb{Z}[\vartheta]$. Then we have

$$\begin{array}{ll} & x \equiv_{(\zeta-1)^{2k}} y \text{ in } \mathbb{Z}[\zeta] \\ \iff & x - y \in (\zeta-1)^{2k}\mathbb{Z}[\zeta] \cap \mathbb{Z}[\vartheta] \overset{(*)}{=} \vartheta^k\mathbb{Z}[\zeta] \cap \mathbb{Z}[\vartheta] \underset{(i)}{\overset{\text{R.28}}{=}} \vartheta^k\mathbb{Z}[\vartheta] \\ \iff & x \equiv_{\vartheta^k} y \text{ in } \mathbb{Z}[\vartheta]. \end{array}$$

□

Remark 31 *We have*

$$(1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z}[\vartheta_p] \;=\; \vartheta_p\mathbb{Z}[\vartheta_p]\,.$$

Proof. We have that $(1-\zeta)\mathbb{Z}[\zeta] \cap \mathbb{Z}[\vartheta]$ is a proper ideal of $\mathbb{Z}[\vartheta]$. Because otherwise we had $1 \in (1-\zeta)\mathbb{Z}[\zeta]$, in contradiction to the fact that $(1-\zeta)\mathbb{Z}[\zeta] \subsetneq \mathbb{Z}[\zeta]$ is a maximal ideal of $\mathbb{Z}[\zeta]$; cf. Lemma 27 *(iii)*.

Therefore we get

$$(*) \qquad \vartheta\mathbb{Z}[\vartheta] \subseteq \vartheta\mathbb{Z}[\zeta]\cap\mathbb{Z}[\vartheta] \overset{\text{R.30}}{=} (1-\zeta)^2\mathbb{Z}[\zeta]\cap\mathbb{Z}[\vartheta] \subseteq (1-\zeta)\mathbb{Z}[\zeta]\cap\mathbb{Z}[\vartheta] \subsetneq \mathbb{Z}[\vartheta]\,.$$

By Lemma 27 *(i)* we know that $\vartheta\mathbb{Z}[\vartheta]$ is a maximal ideal of $\mathbb{Z}[\vartheta]$. So the sequence of ideals in $(*)$ yields that $\vartheta\mathbb{Z}[\vartheta] = (1-\zeta)\mathbb{Z}[\zeta]\cap\mathbb{Z}[\vartheta]$. □

1.4.2 Bases for $\vartheta_p\mathbb{Z}[\vartheta_p]$

Remark 32

(i) For $l \in \mathbb{Z}$ we define

$$ {}_l\gamma' = {}_l\gamma'_p := {}_l\gamma_p - {}_{l-1}\gamma_p\,.$$

Then we have for $i \in \mathbb{Z}_{\geq 1}$

$$\vartheta_p^i = \sum_{k=1}^{i}(-1)^{i-k}\cdot\binom{2i-1}{i-k}\cdot {}_k\gamma'_p\,.$$

(ii) The ideal $\vartheta_p\mathbb{Z}[\vartheta_p]$ of $\mathbb{Z}[\vartheta_p]$ has the $\mathbb{Z}$-linear basis

$$({}_k\gamma'_p : k \in [1,n])$$

and the $\mathbb{Z}$-linear basis

$$({}_k\gamma_p - 2 : k \in [1,n])\,.$$

Proof of *(i)*. This is shown by induction on i. For $i = 1$, the right hand side is

$$(-1)^{1-1}\cdot\binom{2\cdot 1-1}{1-1}\cdot {}_1\gamma' = {}_1\gamma' = {}_1\gamma - {}_0\gamma = \zeta+\zeta^{-1}-\zeta^0-\zeta^{-0} = \zeta+\zeta^{-1}-2 = \vartheta^1\,.$$

So the statement is true for $i = 1$.

Suppose given $i \in \mathbb{Z}_{\geq 1}$. To perform the inductive step $i \to i+1$, we make two preliminaries.

(a) For $l \in \mathbb{Z}$ we have

$$\begin{aligned}\vartheta\cdot {}_l\gamma' &\overset{\text{D.17}}{=} (\gamma-2)\cdot {}_l\gamma' = (\gamma-2)\cdot({}_l\gamma - {}_{l-1}\gamma)\\ &\overset{\text{R.18}}{\underset{(i)}{=}} {}_{l+1}\gamma + {}_{l-1}\gamma - {}_l\gamma - {}_{l-2}\gamma - 2\cdot({}_l\gamma - {}_{l-1}\gamma) = {}_{l+1}\gamma' + {}_{l-1}\gamma' - 2\cdot {}_l\gamma'\,.\end{aligned}$$

(b) For $k \in [1,i]$ we have

$$\begin{aligned}\binom{2i+1}{i+1-k} = \binom{2i}{i-k} + \binom{2i}{i+1-k} &= \binom{2i-1}{i-k-1} + \binom{2i-1}{i-k} + \binom{2i-1}{i-k} + \binom{2i-1}{i+1-k}\\ &= \binom{2i-1}{i-k-1} + 2\cdot\binom{2i-1}{i-k} + \binom{2i-1}{i+1-k}\,.\end{aligned}$$

Inductive step:

$$\sum_{k=1}^{i+1}(-1)^{i+1-k}\tbinom{2i+1}{i+1-k}\cdot {}_k\gamma' \overset{!}{=} \vartheta^{i+1} = \vartheta\vartheta^i \overset{\text{I.H.}}{=} \vartheta\sum_{k=1}^{i}(-1)^{i-k}\tbinom{2i-1}{i-k}\cdot {}_k\gamma'$$

$$\iff \quad -\sum_{k=1}^{i+1}(-1)^{k}\tbinom{2i+1}{i+1-k}\cdot {}_k\gamma' \overset{!}{=} \sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i-k}\cdot\vartheta\cdot {}_k\gamma'$$

$$\overset{\text{(a) on the right}}{\underset{\text{(b) on the left}}{\iff}} \quad -\sum_{k=1}^{i+1}(-1)^{k}\left(\tbinom{2i-1}{i-k-1}+2\tbinom{2i-1}{i-k}+\tbinom{2i-1}{i+1-k}\right)\cdot {}_k\gamma' \overset{!}{=} \sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i-k}\left({}_{k+1}\gamma'+{}_{k-1}\gamma'-2\cdot {}_k\gamma'\right)$$

$$\iff \quad -(-1)^{i+1}\tbinom{2i-1}{0}\cdot {}_{i+1}\gamma' - \sum_{k=1}^{i}(-1)^{k}\left(\tbinom{2i-1}{i-k-1}+2\tbinom{2i-1}{i-k}+\tbinom{2i-1}{i+1-k}\right)\cdot {}_k\gamma' \overset{!}{=} \sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i-k}\left({}_{k+1}\gamma'+{}_{k-1}\gamma'-2\cdot {}_k\gamma'\right) \quad \Big| + \sum_{k=1}^{i}(-1)^{k}\cdot 2\tbinom{2i-1}{i-k}\cdot {}_k\gamma'$$

$$\iff \quad (-1)^{i}\cdot {}_{i+1}\gamma' - \sum_{k=1}^{i}(-1)^{k}\left(\tbinom{2i-1}{i-k-1}+\tbinom{2i-1}{i+1-k}\right)\cdot {}_k\gamma' \overset{!}{=} \sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i-k}\left({}_{k+1}\gamma'+{}_{k-1}\gamma'\right)$$

$$\iff \quad (-1)^{i}\cdot {}_{i+1}\gamma' - \sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i-k-1}\cdot {}_k\gamma' - \sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i+1-k}\cdot {}_k\gamma' \overset{!}{=} \underbrace{\sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i-k}\cdot {}_{k+1}\gamma'}_{=:S_{\mathrm{L}}} + \underbrace{\sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i-k}\cdot {}_{k-1}\gamma'}_{=:S_{\mathrm{R}}} \quad \Big| \text{ subst. } \begin{cases} k\leftrightarrow k+1 \text{ in } S_{\mathrm{L}} \\ k\leftrightarrow k-1 \text{ in } S_{\mathrm{R}} \end{cases}$$

$$\iff \quad (-1)^{i}\cdot {}_{i+1}\gamma' - \sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i-k-1}\cdot {}_k\gamma' - \sum_{k=1}^{i}(-1)^{k}\tbinom{2i-1}{i+1-k}\cdot {}_k\gamma' \overset{!}{=} -\sum_{k=2}^{i+1}(-1)^{k}\tbinom{2i-1}{i+1-k}\cdot {}_k\gamma' - \sum_{k=0}^{i-1}(-1)^{k}\tbinom{2i-1}{i-k-1}\cdot {}_k\gamma' \quad \Big| \begin{array}{l} +\sum_{k=2}^{i}(-1)^{k}\tbinom{2i-1}{i+1-k}\cdot {}_k\gamma' \\ +\sum_{k=1}^{i-1}(-1)^{k}\tbinom{2i-1}{i-k-1}\cdot {}_k\gamma' \end{array}$$

$$\iff \quad (-1)^{i}\cdot {}_{i+1}\gamma' - \underbrace{(-1)^{i}\tbinom{2i-1}{i-i-1}\cdot {}_i\gamma'}_{\text{summand for } k=i} - \underbrace{(-1)^{1}\tbinom{2i-1}{i+1-1}\cdot {}_1\gamma'}_{\text{summand for } k=1} \overset{!}{=} -\underbrace{(-1)^{i+1}\tbinom{2i-1}{i+1-(i+1)}\cdot {}_{i+1}\gamma'}_{\text{summand for } k=i+1} - \underbrace{(-1)^{0}\tbinom{2i-1}{i-0-1}\cdot {}_0\gamma'}_{\text{summand for } k=0} \quad \Big| -(-1)^{i}\cdot {}_{i+1}\gamma'$$

$$\iff \quad \tbinom{2i-1}{i}\cdot {}_1\gamma' \overset{!}{=} -\tbinom{2i-1}{i-1}\cdot {}_0\gamma'$$

$$\iff \quad 0 \overset{!}{=} \tbinom{2i-1}{i}\cdot {}_1\gamma' + \tbinom{2i-1}{i-1}\cdot {}_0\gamma' = \tbinom{2i-1}{i}\cdot {}_1\gamma' + \tbinom{2i-1}{i}\cdot {}_0\gamma'$$

$$\iff \quad 0 \overset{!}{=} {}_1\gamma' + {}_0\gamma' = {}_1\gamma - {}_0\gamma + {}_0\gamma - {}_{-1}\gamma = 0\,.$$

Proof of *(ii)*. We define $B_2 := ({}_k\gamma' : k \in [1,n])$. By Lemma 24 *(i3)* it follows that $\vartheta\mathbb{Z}[\vartheta]$ has the $\mathbb{Z}$-linear basis $B_1 := (\vartheta^s : s \in [1,n])$. By this and using *(i)* we see that $\vartheta\mathbb{Z}[\vartheta] \subseteq \langle B_2 \rangle_{\mathbb{Z}}$.

Therefore we have $n = \mathrm{rk}_{\mathbb{Z}}(\langle B_1 \rangle_{\mathbb{Z}}) = \mathrm{rk}_{\mathbb{Z}}(\vartheta\mathbb{Z}[\vartheta]) \leq \mathrm{rk}_{\mathbb{Z}}(\langle B_2 \rangle_{\mathbb{Z}}) \leq n$. So $\mathrm{rk}_{\mathbb{Z}}(\langle B_2 \rangle_{\mathbb{Z}}) = n$, whence B_2 is $\mathbb{Z}$-linearly independent.

We consider the $\mathbb{Z}$-linear embedding $\iota_1 : \vartheta\mathbb{Z}[\vartheta] \hookrightarrow \langle B_2 \rangle_{\mathbb{Z}}$. It follows from *(i)* that the describing matrix A_1 of ι_1 with respect to B_1 and B_2 is upper triangular.

The diagonal entries of A_1 are $(-1)^{i-i} \cdot \binom{2i-1}{i-i} = 1$ for $i \in [1,n]$. Therefore A_1 has determinant 1, whence ι_1 is bijective.

Altogether, B_2 is a $\mathbb{Z}$-linear basis of $\vartheta\mathbb{Z}[\vartheta]$.

We define $B_3 := ({}_k\gamma - 2 : k \in [1,n])$. For $s \in [1,n]$ we have $\sigma_s(\vartheta) = \sigma_s({}_1\gamma - 2) = {}_s\gamma - 2$. Since $\sigma_s(\vartheta) \in \vartheta\mathbb{Z}[\vartheta]$, cf. Remark 28 *(iii)*, we therefore obtain that $\langle B_3 \rangle_{\mathbb{Z}} \subseteq \vartheta\mathbb{Z}[\vartheta] = \langle B_2 \rangle_{\mathbb{Z}}$.

On the other hand, we have

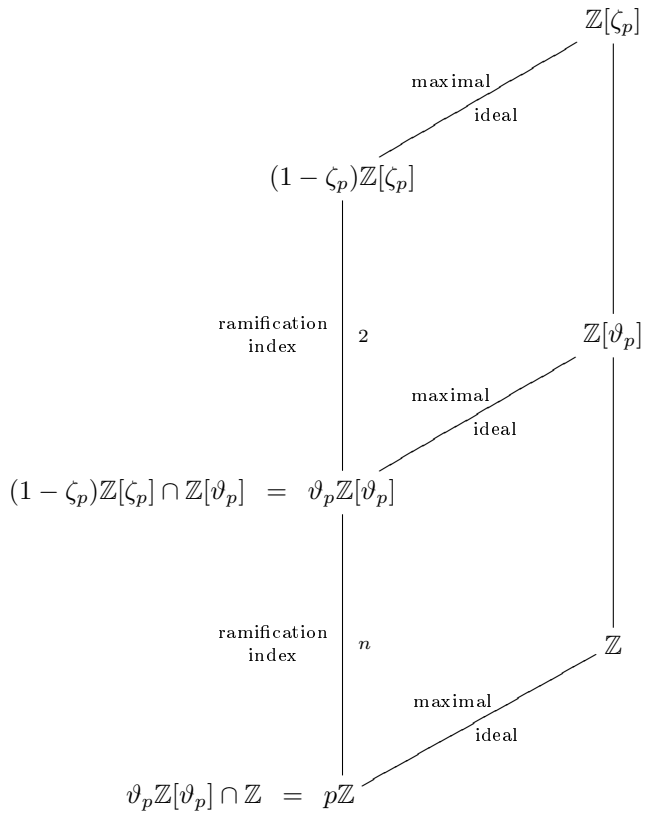
$${}_s\gamma' = {}_s\gamma - {}_{s-1}\gamma = ({}_s\gamma - 2) - ({}_{s-1}\gamma - 2) = \begin{cases} ({}_s\gamma - 2) - ({}_{s-1}\gamma - 2) & \text{for } s \in [2,n], \\ {}_1\gamma - 2 & \text{for } s = 1. \end{cases}$$

So $\vartheta\mathbb{Z}[\vartheta] = \langle B_2 \rangle_{\mathbb{Z}} \subseteq \langle B_3 \rangle_{\mathbb{Z}}$. Hence we get $\langle B_3 \rangle_{\mathbb{Z}} = \vartheta\mathbb{Z}[\vartheta]$. Since $n = \mathrm{rk}_{\mathbb{Z}}(\vartheta\mathbb{Z}[\vartheta]) = \mathrm{rk}_{\mathbb{Z}}(\langle B_3 \rangle_{\mathbb{Z}}) \leq n$, we have that $\mathrm{rk}_{\mathbb{Z}}(\langle B_3 \rangle_{\mathbb{Z}}) = n$. Thus B_3 is $\mathbb{Z}$-linearly independent.

Altogether, B_3 is a $\mathbb{Z}$-linear basis of $\vartheta\mathbb{Z}[\vartheta]$. □

1.4.3 Summary of Ramification

In summary, we obtain the following diagram



Chapter 2

Two tensor products

2.1 The tensor product $\mathbb{Q}(\vartheta_p) \underset{\mathbb{Q}}{\otimes} \mathbb{Q}(\vartheta_p)$

Lemma 33 *We have the isomorphism of $\mathbb{Q}(\vartheta_p)$-algebras*

$$\begin{aligned} \delta : \mathbb{Q}(\vartheta_p) \underset{\mathbb{Q}}{\otimes} \mathbb{Q}(\vartheta_p) \quad &\xrightarrow{\sim} \quad \mathbb{Q}(\vartheta_p) \quad \times \ldots \times \quad \mathbb{Q}(\vartheta_p) \\ y \quad \otimes \quad x \quad &\longmapsto (\sigma_n(x)y \ , \ \ldots \ , \ \sigma_1(x)y) \, , \end{aligned}$$

where $\mathrm{Gal}(\mathbb{Q}(\vartheta_p)|\mathbb{Q}) = \{\sigma_i \, : \, i \in [1,n]\}$ *; cf.* Notation 26.

Proof. By Lemma 24 *(i2)* we have $[\mathbb{Q}(\vartheta) : \mathbb{Q}] = n$. Hence, we apply Lemma 109 to the case $(L, K, m) = (\mathbb{Q}(\vartheta), \mathbb{Q}, n)$ to obtain the assertion. (Note that the order of the Galois automorphisms may be chosen arbitrarily.) □

2.2 The tensor product $\mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta_p]$

2.2.1 The tensor product $\mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta_p]$ as a $\mathbb{Z}[\vartheta_p]$-subalgebra ${}_p\Psi$ of $\mathbb{Z}[\vartheta_p]^{\times n}$

Definition 34 For $i \in [0, n-1]$ and $k \in [1, n]$, we define

$$\mathbb{Z} \ni \left\langle \begin{matrix} i \\ k \end{matrix} \right\rangle := \begin{cases} (-1)^{i-k+1} \left(\binom{2i}{i-k+1} - \binom{2i}{i-k} \right) & \text{for } k \in [1, i+1] \, , \\ 0 & \text{for } k \in [i+2, n] \, . \end{cases}$$

Note that the formula for $k \in [1, i+1]$ applies to the case $k \in [i+2, n]$ as well, if one prefers.

This enables us to define the $\mathbb{Z}[\vartheta_p]$-submodule of the $\mathbb{Z}[\vartheta_p]$-algebra $\mathbb{Z}[\vartheta_p]^{\times n}$

$$\Psi \ = \ {}_p\Psi := \left\{ (a_j)_{j \in [1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n} \, : \, \sum_{k=1}^{n} \left\langle \begin{matrix} i \\ k \end{matrix} \right\rangle a_k \equiv_{\vartheta_p^i} 0 \text{ for } i \in [0, n-1] \right\} ,$$

cf. Convention 7.

Example 35 Let us consider ${}_p\Psi$ in the case $p = 11$. Then ${}_{11}\Psi$ is given by

$$ {}_{11}\Psi \;=\; \left\{ (\,v\,,\,w\,,\,x\,,\,y\,,\,z\,) \in \mathbb{Z}[\vartheta_{11}]^{\times 5} \;:\; \begin{array}{rcl} -v+w & \equiv_{\vartheta_{11}^1} & 0 \\ 2v-3w+x & \equiv_{\vartheta_{11}^2} & 0 \\ -5v+9w-5x+y & \equiv_{\vartheta_{11}^3} & 0 \\ 14v-28w+20x-7y+z & \equiv_{\vartheta_{11}^4} & 0 \end{array} \right\} . $$

Remark 36

$$ \textit{Let} \quad D_\Psi \;=\; D_{{}_p\Psi} \;:=\; \mathrm{diag}\big(\,\vartheta_p^{n-1}\,,\,\vartheta_p^{n-2}\,,\,\ldots\,,\,\vartheta_p^0\,\big) \quad \in \mathbb{Z}[\vartheta_p]^{n\times n} \cap \mathrm{GL}_n(\mathbb{C})\,, $$

$$ \textit{and} \quad K_\Psi \;=\; K_{{}_p\Psi} \;:=\; \left(\left\langle \begin{matrix} i \\ k \end{matrix} \right\rangle \right)_{\substack{i\,\in\,[0,\,n-1],\\ k\,\in\,[1,\,n]}} \qquad \in \mathbb{Z}^{n\times n} \cap \mathrm{GL}_n(\mathbb{Q})\,. $$

Suppose given $a = (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n}$. *Then we have*

$$ a \in {}_p\Psi \iff D_{{}_p\Psi} K_{{}_p\Psi}\, a^{\mathrm{t}} \in \vartheta_p^{n-1}\mathbb{Z}[\vartheta_p]^{n\times 1}\,. $$

Proof. We have $K_\Psi \in \mathbb{Z}^{n\times n}$ by Definition 34. We see that $\left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle = \begin{cases} 0 \text{ for } k > i+1 \text{ and} \\ 1 \text{ for } k = i+1\,. \end{cases}$

Therefore K_Ψ is lower triangular and $\det(K_\Psi) = 1$. Hence, $K_\Psi \in \mathrm{GL}_n(\mathbb{Q})$.

For given $a = (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$, we have

$$ \begin{array}{rcl} a \in \Psi & \iff & a \text{ satisfies the defining congruences for } \Psi \\ & \iff & \displaystyle\sum_{k=1}^{n} \left\langle \begin{matrix} i \\ k \end{matrix} \right\rangle a_k \equiv_{\vartheta^i} 0 \text{ for } i \in [0,n-1] \quad \iff \quad D_\Psi K_\Psi a^{\mathrm{t}} \in \vartheta^{n-1}\mathbb{Z}[\vartheta]^{n\times 1}\,. \end{array} $$

□

Example 37 Let us consider $K_{{}_p\Psi}$ in the case $p = 11$. Then $K_{{}_{11}\Psi}$ is given by the lower triangular matrix

$$ K_{{}_{11}\Psi} \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 2 & -3 & 1 & 0 & 0 \\ -5 & 9 & -5 & 1 & 0 \\ 14 & -28 & 20 & -7 & 1 \end{pmatrix} . $$

Lemma 38 *The* $\mathbb{Z}[\vartheta_p]$*-submodule* ${}_p\Psi \subseteq \mathbb{Z}[\vartheta_p]^{\times n}$ *has the* $\mathbb{Z}[\vartheta_p]$*-linear basis*

$$ \mathrm{B}_\Psi \;=\; \mathrm{B}_{{}_p\Psi} \;:=\; \left(\vartheta_p^{l-1} \cdot \left(\binom{l+k-2}{2l-2} \right)_{k\in[1,n]} \;:\; l \in [1,n] \right) . $$

Proof. Let $i, l \in [1, n]$. First, note that the elements of B_Ψ are the rows of an upper triangular matrix, whence B_Ψ is $\mathbb{Z}[\vartheta]$-linearly independent.

The describing matrix L of the embedding $\iota : \langle \mathrm{B}_\Psi \rangle_{\mathbb{Z}[\vartheta]} \hookrightarrow \mathbb{Z}[\vartheta]^{\times n}$ with respect to B_Ψ and to the standard basis of $\mathbb{Z}[\vartheta]^{\times n}$ is

$$L = \left(\vartheta^{l-1} \cdot \binom{l+k-2}{2l-2} \right)_{k,l \in [1,n]} .$$

We consider the matrix K_Ψ defined in Remark 36 and note that $K_\Psi = \left(\left\langle \begin{smallmatrix} i-1 \\ k \end{smallmatrix} \right\rangle \right)_{i,k \in [1,n]}$. Then we have

$$\left.\begin{aligned} K_\Psi L \;=\; \left(\sum_{k=1}^{n} \left\langle \begin{smallmatrix} i-1 \\ k \end{smallmatrix} \right\rangle \cdot \vartheta^{l-1} \cdot \binom{l+k-2}{2l-2} \right)_{i,l \in [1,n]} &= \left(\vartheta^{l-1} \cdot \sum_{k=1}^{n} \left\langle \begin{smallmatrix} i-1 \\ k \end{smallmatrix} \right\rangle \cdot \binom{l+k-2}{2l-2} \right)_{i,l \in [1,n]} \\ \overset{\text{R.139}}{=} \left(\vartheta^{l-1} \cdot S(i,l) \right)_{i,l \in [1,n]} \overset{\text{R.139}}{=} \left(\vartheta^{l-1} \cdot \partial_{i,l} \right)_{i,l \in [1,n]} &= \operatorname{diag}\left(\vartheta^0, \vartheta^1, \ldots, \vartheta^{n-1} \right) =: F . \end{aligned}\right\} (1)$$

So we obtain for given $a = (a_j)_{j \in [1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$

$$\begin{aligned} a \in \Psi \overset{\text{R.36}}{\iff} D_\Psi \overbrace{K_\Psi}^{\overset{(1)}{=} FL^{-1}} a^{\mathrm{t}} \in \vartheta^{n-1}\mathbb{Z}[\vartheta]^{n \times 1} &\iff \overbrace{D_\Psi F}^{= \vartheta^{n-1} \cdot \mathrm{E}_n} L^{-1} a^{\mathrm{t}} \in \vartheta^{n-1}\mathbb{Z}[\vartheta]^{n \times 1} \\ \iff \vartheta^{n-1} L^{-1} a^{\mathrm{t}} \in \vartheta^{n-1}\mathbb{Z}[\vartheta]^{n \times 1} &\iff a^{\mathrm{t}} \in L\mathbb{Z}[\vartheta]^{n \times 1} \iff a \in \langle \mathrm{B}_\Psi \rangle_{\mathbb{Z}[\vartheta]} . \end{aligned}$$

Therefore we have $\Psi = \langle \mathrm{B}_\Psi \rangle_{\mathbb{Z}[\vartheta]}$. □

Example 39 In the case $p = 11$ the $\mathbb{Z}[\vartheta_{11}]$-linear basis $\mathrm{B}_{{}_{11}\Psi}$ of the submodule ${}_{11}\Psi$ of $\mathbb{Z}[\vartheta_{11}]^{\times 5}$ is given by

$$\mathrm{B}_{{}_{11}\Psi} = \begin{pmatrix} (1, & 1, & 1, & 1, & 1), \\ \vartheta_{11}^1 \cdot (0, & 1, & 3, & 6, & 10), \\ \vartheta_{11}^2 \cdot (0, & 0, & 1, & 5, & 15), \\ \vartheta_{11}^3 \cdot (0, & 0, & 0, & 1, & 7), \\ \vartheta_{11}^4 \cdot (0, & 0, & 0, & 0, & 1) \end{pmatrix} .$$

Remark 40 *Let* $\iota : {}_p\Psi \hookrightarrow \mathbb{Z}[\vartheta_p]^{\times n}$ *be the canonical embedding.*

Then we have

$$\det_{\mathbb{Z}[\vartheta_p]}(\iota) = \vartheta_p^{\frac{(n-1)n}{2}} .$$

Proof. By Lemma 38 we get that the describing matrix of ι with respect to the basis B_Ψ of Ψ and to the standard basis of $\mathbb{Z}[\vartheta]^{\times n}$ is

$$L = \left(\vartheta^{l-1} \cdot \binom{l+k-2}{2l-2} \right)_{k,l \in [1,n]} .$$

Since $\binom{l+k-2}{2l-2} = 0$ for $k < l$ the matrix L is lower triangular. Further we have that $\binom{l+k-2}{2l-2} = 1$ for $k = l$.

So we can calculate the determinant of ι as follows

$$\det_{\mathbb{Z}[\vartheta]}(\iota) \;=\; \det(L) \;=\; \prod_{i=0}^{n-1} \vartheta^i \;=\; \vartheta^{\sum_{i=0}^{n-1} i} \;=\; \vartheta^{\frac{(n-1)n}{2}} .$$

□

Proposition 41

The $\mathbb{Z}[\vartheta_p]$-submodule ${}_p\Psi$ of the $\mathbb{Z}[\vartheta_p]$-algebra $\mathbb{Z}[\vartheta_p]^{\times n}$, given in Definition 34*, is a subalgebra.*

We have the isomorphism of $\mathbb{Z}[\vartheta_p]$-algebras

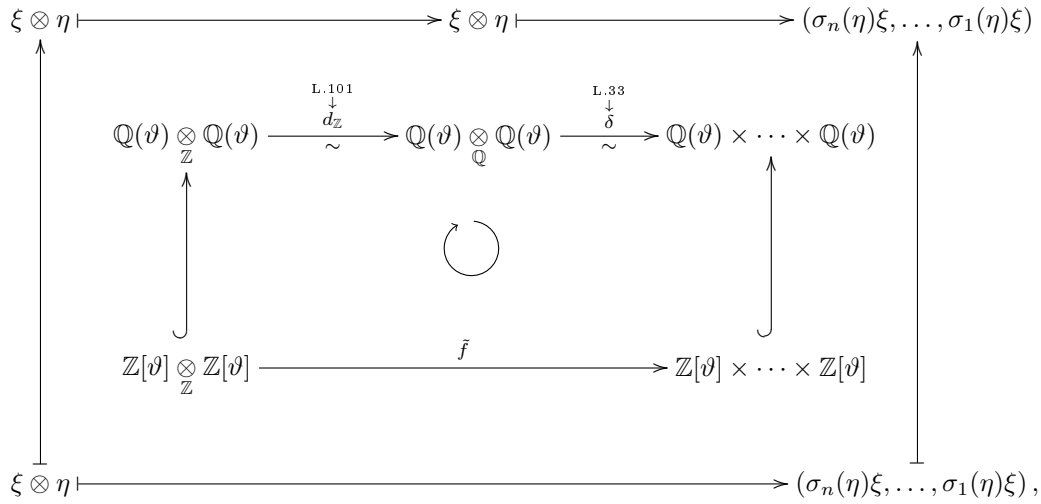
$$\begin{array}{rcccl} f & : & \mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta_p] & \xrightarrow{\sim} & \left\{ (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n} \,:\, \sum_{k=1}^{n} \left\langle \begin{matrix} i \\ k \end{matrix} \right\rangle a_k \equiv_{\vartheta_p^i} 0 \text{ for } i \in [0,n-1] \right\} \;=\; {}_p\Psi \\ & & \xi \otimes \eta & \longmapsto & (\,\sigma_{n-j+1}(\eta)\cdot\xi\,)_{j\in[1,n]}\,, \end{array}$$

where $\sigma_j \in \mathrm{Gal}(\mathbb{Q}(\vartheta_p)|\mathbb{Q})$ for $j \in [1,n]$; cf. Notation 26.

Proof. By Remark 28 *(iii)* (in the case $s = 0$) we get that σ restricts to an automorphism of $\mathbb{Z}[\vartheta]$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\vartheta)|\mathbb{Q})$.

So we can consider the map $\tilde{f} : \mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta] \longrightarrow \mathbb{Z}[\vartheta]^{\times n}$, $\xi \otimes \eta \longmapsto f(\xi\otimes\eta) = (\sigma_{n-j+1}(\eta)\cdot\xi)_{j\in[1,n]}$.

We have the commutative diagram



whence $\tilde{f}$ is an injective morphism of $\mathbb{Z}[\vartheta]$-algebras.

Now we want to show that $\tilde{f}(\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta]) \overset{!}{\subseteq} \Psi$.

We choose the $\mathbb{Z}$-linear basis $({}_1\gamma,\, {}_2\gamma, \ldots,\, {}_{n-1}\gamma,\, {}_n\gamma)$ of $\mathbb{Z}[\vartheta]$; cf. Corollary 21.

Therefore we can choose the $\mathbb{Z}[\vartheta]$-linear basis $B := (1\otimes {}_1\gamma, 1\otimes {}_2\gamma, \ldots, 1\otimes {}_{n-1}\gamma, 1\otimes {}_n\gamma)$ of $\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta]$; cf. Lemma 100 *(i)*.

By Remark 28 *(iii)* we have for $\tau \in \mathrm{Gal}(\mathbb{Q}(\vartheta)|\mathbb{Q})$

$$\tau\big(\vartheta^i\mathbb{Z}[\vartheta]\big) \;=\; \vartheta^i\mathbb{Z}[\vartheta] \text{ for } i \in [0,n-1]\,. \tag{1}$$

Given $(a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$ and $\tau \in \mathrm{Gal}(\mathbb{Q}(\vartheta)|\mathbb{Q})$ we write $\tau((a_j)_{j\in[1,n]}) := (\tau(a_j))_{j\in[1,n]}$.

For $(a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$, we obtain

$$\left.\begin{array}{lll}
(a_j)_{j\in[1,n]} \in \Psi & \overset{\text{D.34}}{\iff} & \sum_{k=1}^{n} \left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle a_k \equiv_{\vartheta^i} 0 \text{ for } i \in [0,n-1] \\
& \iff & \sum_{k=1}^{n} \left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle a_k \in \vartheta^i\mathbb{Z}[\vartheta] \overset{(1)}{=} \tau^{-1}\big(\vartheta^i\mathbb{Z}[\vartheta]\big) \text{ for } i \in [0,n-1] \\
& \iff & \tau\Bigg(\sum_{k=1}^{n} \underbrace{\left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle}_{\in\mathbb{Z}} a_k\Bigg) \in \vartheta^i\mathbb{Z}[\vartheta] \text{ for } i \in [0,n-1] \\
& \iff & \sum_{k=1}^{n} \left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle \tau(a_k) \in \vartheta^i\mathbb{Z}[\vartheta] \text{ for } i \in [0,n-1] \\
& \iff & \sum_{k=1}^{n} \left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle \tau(a_k) \equiv_{\vartheta^i} 0 \text{ for } i \in [0,n-1] \iff (\tau(a_j))_{j\in[1,n]} \in \Psi \\
& & \iff \tau((a_j)_{j\in[1,n]}) \in \Psi\,.
\end{array}\right\} (*)$$

Further we have for $s \in [1,n]$

$$\begin{array}{rcccl}
\tilde{f}(1 \otimes {}_s\gamma) & = & \tilde{f}(1 \otimes \sigma_s({}_1\gamma)) & = & (\sigma_{n-j+1}(\sigma_s({}_1\gamma)))_{j\in[1,n]} \\
& & & \overset{\text{Gal.gr. abelian}}{=} & (\sigma_s(\sigma_{n-j+1}({}_1\gamma)))_{j\in[1,n]} \\
& & & = & \sigma_s((\sigma_{n-j+1}({}_1\gamma))_{j\in[1,n]}) \;=\; \sigma_s\big(\tilde{f}(1 \otimes {}_1\gamma)\big)\,.
\end{array}$$

Since B is a $\mathbb{Z}[\vartheta]$-linear basis of $\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta]$ and because of $(*)$, we only have to show that

$$\tilde{f}(1 \otimes {}_1\gamma) = (\underbrace{\sigma_{n-j+1}({}_1\gamma)}_{={}_{n-j+1}\gamma})_{j\in[1,n]} = ({}_n\gamma, \ldots, {}_1\gamma) \overset{!}{\in} \Psi\,,$$

in order to prove the stated inclusion $\tilde{f}(\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta]) \overset{!}{\subseteq} \Psi$.

For this we shall verify that the tuple $({}_n\gamma, \ldots, {}_1\gamma)$ satisfies the defining congruences for Ψ.

For $i \in [0, n-1]$ we have

$$
\begin{aligned}
\mathbb{Z}[\vartheta] \overset{\text{D.34}}{\ni} & \sum_{k=1}^{n} \left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle \cdot {}_{n-k+1}\gamma \overset{\text{D.17}}{=} \sum_{k=1}^{n} \left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle \left(\zeta^{n-k+1} + \zeta^{-n+k-1}\right) \\
\overset{\text{D.34}}{=} & \ \zeta^{n-i} + \zeta^{-n+i} + \sum_{k=1}^{i} (-1)^{i-k+1} \left(\tbinom{2i}{i-k+1} - \tbinom{2i}{i-k} \right) \left(\zeta^{n-k+1} + \zeta^{-n+k-1}\right) \\
\overset{s=i-k+1}{=} & \ \zeta^{n-i} + \zeta^{-n+i} + \sum_{s=1}^{i} (-1)^{s} \left(\tbinom{2i}{s} - \tbinom{2i}{s-1} \right) \left(\zeta^{n-i+s} + \zeta^{-n+i-s}\right) \\
= & \ \zeta^{n-i} + \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{n-i+s} + \sum_{s=1}^{i} (-1)^{s+1} \tbinom{2i}{s-1} \zeta^{-n+i-s} + \zeta^{-n+i} + \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{-n+i-s} + \sum_{s=1}^{i} (-1)^{s+1} \tbinom{2i}{s-1} \zeta^{n-i+s} \\
= & \ \zeta^{n-i} + \zeta^{n-i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} + \zeta^{-n+i} \sum_{s=1}^{i} (-1)^{s+1} \tbinom{2i}{s-1} \zeta^{-s} + \zeta^{-n+i} + \zeta^{-n+i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} + \zeta^{n-i} \sum_{s=1}^{i} (-1)^{s+1} \tbinom{2i}{s-1} \zeta^{s} \\
\overset{j=2i-s+1}{=} & \ \zeta^{n-i} + \zeta^{n-i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} + \zeta^{-n+i} \sum_{j=i+1}^{2i} (-1)^{2i-j+2} \tbinom{2i}{j} \zeta^{-2i+j-1} + \zeta^{-n+i} + \zeta^{-n+i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} + \zeta^{n-i} \sum_{j=i+1}^{2i} (-1)^{2i-j+2} \tbinom{2i}{j} \zeta^{2i-j+1} \\
= & \ \zeta^{n-i} + \zeta^{n-i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} + \zeta^{-n-i} \sum_{j=i+1}^{2i} (-1)^{j} \tbinom{2i}{j} \zeta^{j-1} + \zeta^{-n+i} + \zeta^{-n+i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} + \zeta^{n+i} \sum_{j=i+1}^{2i} (-1)^{j} \tbinom{2i}{j} \zeta^{-j+1} \\
= & \ \zeta^{n-i} + \zeta^{n-i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} + \zeta^{-n-i} \sum_{j=i+1}^{2i} (-1)^{j} \tbinom{2i}{j} \zeta^{\overbrace{2n+1}^{p} + j - 1} + \zeta^{-n+i} + \zeta^{-n+i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} + \zeta^{n+i} \sum_{j=i+1}^{2i} (-1)^{j} \tbinom{2i}{j} \zeta^{\overbrace{-2n-1}^{-p} - j + 1} \\
= & \ \zeta^{n-i} + \zeta^{n-i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} + \zeta^{n-i} \sum_{j=i+1}^{2i} (-1)^{j} \tbinom{2i}{j} \zeta^{j} + \zeta^{-n+i} + \zeta^{-n+i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} + \zeta^{-n+i} \sum_{j=i+1}^{2i} (-1)^{j} \tbinom{2i}{j} \zeta^{-j} \\
\overset{s=j}{=} & \ \zeta^{n-i} + \zeta^{n-i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} + \zeta^{n-i} \sum_{s=i+1}^{2i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} + \zeta^{-n+i} + \zeta^{-n+i} \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} + \zeta^{-n+i} \sum_{s=i+1}^{2i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} \\
= & \ \zeta^{n-i} \left(1 + \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} + \sum_{s=i+1}^{2i} (-1)^{s} \tbinom{2i}{s} \zeta^{s} \right) + \zeta^{-n+i} \left(1 + \sum_{s=1}^{i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} + \sum_{s=i+1}^{2i} (-1)^{s} \tbinom{2i}{s} \zeta^{-s} \right) \\
= & \ \zeta^{n-i} \sum_{s=0}^{2i} \tbinom{2i}{s} (-\zeta)^{s} + \zeta^{-n+i} \sum_{s=0}^{2i} \tbinom{2i}{s} (-\zeta^{-1})^{s} \ = \ \zeta^{n-i} (1-\zeta)^{2i} + \zeta^{-n+i} (1-\zeta^{-1})^{2i} \ \equiv_{(\zeta-1)^{2i}} \ 0 \,,
\end{aligned}
$$

where the congruence at the end is true for $i = 0$, and for $i \in [1, n-1]$ it follows from Remark 28 *(ii)*.

Hence we get with Remark 30 that $\sum_{k=1}^{n} \left\langle \begin{smallmatrix} i \\ k \end{smallmatrix} \right\rangle_{n-k+1} \gamma \equiv_{\vartheta^i} 0$ for $i \in [0, n-1]$, and so $\tilde{f}(\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta]) \subseteq \Psi$.

So we can define $f := \tilde{f}\big|^{\Psi}$; cf. Convention 1. As a restriction of $\tilde{f}$, the map $f : \mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta] \longrightarrow \Psi$ is injective.

Now we calculate the principal ideal of $\mathbb{Z}[\vartheta]$ that is generated by the $\mathbb{Z}[\vartheta]$-linear determinant of $\tilde{f}$.

We choose the $\mathbb{Z}$-linear basis $(\,\vartheta^0, \vartheta^1, \ldots, \vartheta^{n-2}, \vartheta^{n-1}\,)$ of $\mathbb{Z}[\vartheta]$; cf. Lemma 24 *(i3)*.

Therefore we can choose the $\mathbb{Z}[\vartheta]$-linear basis $C := (\,1\otimes\vartheta^0, 1\otimes\vartheta^1, \ldots, 1\otimes\vartheta^{n-2}, 1\otimes\vartheta^{n-1}\,)$ of $\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta]$; cf. Lemma 100 *(i)*. Further we choose the standard basis of $\mathbb{Z}[\vartheta]^{\times n}$. So we obtain the describing matrix of the $\mathbb{Z}[\vartheta]$-linear map $\tilde{f} : \mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta] \longrightarrow \mathbb{Z}[\vartheta]^{\times n}$ as

$$A := \Big(\sigma_{n-j+1}\big(\vartheta^i\big)\Big)_{\substack{j \in [1,n],\\ i \in [0,n-1]}} .$$

We apply Lemma 115 to the case $\big(L, \mathbb{Q}, m, (x_j)_{j\in[1,m]}\big) = \big(\mathbb{Q}(\vartheta), \mathbb{Q}, n, (\vartheta^i)_{i\in[0,n-1]}\big)$ and get

$$\big(\det(A)\big)^2 \;=\; \Delta_{\mathbb{Q}(\vartheta)|\mathbb{Q}} \overset{\text{L.25}}{=} \pm p^{\frac{p-3}{2}} .$$

So we have

$$\big(\det(A)\big)^2\mathbb{Z}[\vartheta] \;=\; p^{\frac{p-3}{2}}\mathbb{Z}[\vartheta] \overset{\text{L.29}}{=} \vartheta^{n\cdot\frac{p-3}{2}}\mathbb{Z}[\vartheta] \;=\; \vartheta^{n\cdot\frac{2n+1-3}{2}}\mathbb{Z}[\vartheta] \;=\; \vartheta^{n(n-1)}\mathbb{Z}[\vartheta]\,,$$

whence

$$\det_{\mathbb{Z}[\vartheta]}\big(\tilde{f}\,\big)\mathbb{Z}[\vartheta] \;=\; \det(A)\mathbb{Z}[\vartheta] \;=\; \vartheta^{\frac{(n-1)n}{2}}\mathbb{Z}[\vartheta]\,.$$

By Remark 40 we know that $\det_{\mathbb{Z}[\vartheta]}(\iota : \Psi \hookrightarrow \mathbb{Z}[\vartheta]^{\times n}) \;=\; \vartheta^{\frac{(n-1)n}{2}}$.

So we have the following situation

$$\begin{array}{ccccc} & & \det_{\mathbb{Z}[\vartheta]}(\tilde{f})\mathbb{Z}[\vartheta]=\vartheta^{\frac{(n-1)n}{2}}\mathbb{Z}[\vartheta] & & \\ & & \downarrow & & \\ & \overset{\tilde{f}}{\nearrow} & & \overset{\tilde{f}}{\searrow} & \\ \mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta] & \xrightarrow{f=\tilde{f}|^{\Psi}} & \Psi & \xrightarrow{\iota} & \mathbb{Z}[\vartheta]^{\times n}\,. \\ & & \uparrow & & \\ & & \det_{\mathbb{Z}[\vartheta]}(\iota)\mathbb{Z}[\vartheta]=\vartheta^{\frac{(n-1)n}{2}}\mathbb{Z}[\vartheta] & & \end{array}$$

We have

$$\left.\begin{array}{rcl} \det_{\mathbb{Z}[\vartheta]}\big(\tilde{f}\,\big)\mathbb{Z}[\vartheta] & = & \det_{\mathbb{Z}[\vartheta]}(\iota\circ f)\mathbb{Z}[\vartheta] \\ = \quad (\det_{\mathbb{Z}[\vartheta]}(f)\cdot\det_{\mathbb{Z}[\vartheta]}(\iota))\mathbb{Z}[\vartheta] & = & \det_{\mathbb{Z}[\vartheta]}(f)\mathbb{Z}[\vartheta]\cdot\det_{\mathbb{Z}[\vartheta]}(\iota)\mathbb{Z}[\vartheta] \\ = \det_{\mathbb{Z}[\vartheta]}(f)\mathbb{Z}[\vartheta]\cdot\det_{\mathbb{Z}[\vartheta]}\big(\tilde{f}\,\big)\mathbb{Z}[\vartheta] & = & \big(\det_{\mathbb{Z}[\vartheta]}(f)\cdot\det_{\mathbb{Z}[\vartheta]}\big(\tilde{f}\,\big)\big)\mathbb{Z}[\vartheta]\,. \end{array}\right\} (2)$$

From the inclusion "$\subseteq$" in (2) we get that there exists an $x \in \mathbb{Z}[\vartheta]$ with

$$0 \;\overset{\tilde{f}\text{ inj.}}{\neq}\; \det_{\mathbb{Z}[\vartheta]}\big(\tilde{f}\,\big) \;=\; \det_{\mathbb{Z}[\vartheta]}(f)\cdot\det_{\mathbb{Z}[\vartheta]}\big(\tilde{f}\,\big)\cdot x \quad\Longleftrightarrow\quad 1 \;=\; \det_{\mathbb{Z}[\vartheta]}(f)\cdot x$$

$$\Longleftrightarrow\quad \det_{\mathbb{Z}[\vartheta]}(f) \in \mathrm{U}(\mathbb{Z}[\vartheta])\,.$$

Thus we get that f is surjective.

Altogether, f is bijective. Since $f = \tilde{f}\big|^{\Psi}$ and $\tilde{f}$ is a morphism of $\mathbb{Z}[\vartheta]$-algebras, we conclude that $\Psi = \mathrm{im}\big(\tilde{f}\,\big)$ is a $\mathbb{Z}[\vartheta]$-subalgebra of $\mathbb{Z}[\vartheta]^{\times n}$. □

2.2.2 A submodule ${}_p\tilde{\Psi}$ of $\mathbb{Z}[\vartheta_p]^{\times n}$

In the following two Subsections 2.2.2 and 2.2.3, we intend to describe a principal ideal of ${}_p\Psi$ via ties, which will help us later to describe the group ring $\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p}$ in Section 4.2 via ties.

Definition 42 We define the $\mathbb{Z}[\vartheta_p]$-submodule ${}_p\tilde{\Psi}$ of the $\mathbb{Z}[\vartheta_p]$-algebra $\mathbb{Z}[\vartheta_p]^{\times n}$

$$\tilde{\Psi} = {}_p\tilde{\Psi} := \left\{ (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n} : \sum_{k=1}^{n} \frac{(2i-1)^2}{(2k-1)^2}(2i)! \left\langle \begin{matrix} i-1 \\ k \end{matrix} \right\rangle \cdot a_k \equiv_{\vartheta_p^i} 0 \text{ for } i \in [1,n] \right\},$$

cf. Convention 7, Definition 34 and Remark 141.

Example 43 Let us consider ${}_p\tilde{\Psi}$ in the case $p = 11$. Then ${}_{11}\tilde{\Psi}$ is given by

$${}_{11}\tilde{\Psi} = \left\{ (v, w, x, y, z) \in \mathbb{Z}[\vartheta_{11}]^{\times 5} : \begin{array}{rcl} 2v & \equiv_{\vartheta_{11}^1} & 0 \\ -216v + 24w & \equiv_{\vartheta_{11}^2} & 0 \\ 36000v - 6000w + 720x & \equiv_{\vartheta_{11}^3} & 0 \\ -9878400v + 1975680w - 395136x + 40320y & \equiv_{\vartheta_{11}^4} & 0 \\ 4115059200v - 914457600w + 235146240x - 41990400y + 3628800z & \equiv_{\vartheta_{11}^5} & 0 \end{array} \right\}.$$

Remark 44

$$\textit{Let} \quad D_{\tilde{\Psi}} = D_{{}_p\tilde{\Psi}} := \mathrm{diag}\left(\vartheta_p^{n-1}, \vartheta_p^{n-2}, \ldots, \vartheta_p^0\right) \in \mathbb{Z}[\vartheta_p]^{n\times n} \cap \mathrm{GL}_n(\mathbb{C}),$$

$$\textit{and} \quad K_{\tilde{\Psi}} = K_{{}_p\tilde{\Psi}} := \left(\frac{(2i-1)^2}{(2k-1)^2}(2i)! \left\langle \begin{matrix} i-1 \\ k \end{matrix} \right\rangle \right)_{i,k\in[1,n]} \in \mathbb{Z}^{n\times n} \cap \mathrm{GL}_n(\mathbb{Q}).$$

Suppose given $a = (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n}$. Then we have

$$a \in {}_p\tilde{\Psi} \iff D_{{}_p\tilde{\Psi}} K_{{}_p\tilde{\Psi}} a^{\mathrm{t}} \in \vartheta_p^n \mathbb{Z}[\vartheta_p]^{n\times 1}.$$

Proof. We have $K_{\tilde{\Psi}} \in \mathbb{Z}^{n\times n}$ by Remark 141.

For $i,k \in [1,n]$ we denote the entries of $K_{\tilde{\Psi}}$ by $l_{i,k} := \frac{(2i-1)^2}{(2k-1)^2}(2i)!\left\langle \begin{smallmatrix} i-1 \\ k \end{smallmatrix} \right\rangle$. By Definition 34 we see that $l_{i,k} = 0$ for $k > i$ and $l_{i,k} \neq 0$ for $k = i$.

Therefore $K_{\tilde{\Psi}}$ is lower triangular and $\det(K_{\tilde{\Psi}}) \neq 0$, i.e. $K_{\tilde{\Psi}} \in \mathrm{GL}_n(\mathbb{Q})$.

For given $a = (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$, we have

$$\begin{aligned} a \in \tilde{\Psi} &\iff a \text{ satisfies the defining congruences for } \tilde{\Psi} \\ &\iff \sum_{k=1}^{n} \frac{(2i-1)^2}{(2k-1)^2}(2i)! \left\langle \begin{matrix} i-1 \\ k \end{matrix} \right\rangle a_k \equiv_{\vartheta^i} 0 \text{ for } i \in [1,n] \iff D_{\tilde{\Psi}} K_{\tilde{\Psi}} a^{\mathrm{t}} \in \vartheta^n \mathbb{Z}[\vartheta]^{n\times 1}. \end{aligned}$$

□

Example 45 Let us consider $K_{{}_p\tilde{\Psi}}$ in the case $p = 11$. Then $K_{{}_{11}\tilde{\Psi}}$ is given by the lower triangular matrix

$$K_{{}_{11}\tilde{\Psi}} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ -216 & 24 & 0 & 0 & 0 \\ 36000 & -6000 & 720 & 0 & 0 \\ -9878400 & 1975680 & -395136 & 40320 & 0 \\ 4115059200 & -914457600 & 235146240 & -41990400 & 3628800 \end{pmatrix}.$$

Remark 46 *We write* $(p) := p\mathbb{Z}$ *and* $(\vartheta_p) := \vartheta_p\mathbb{Z}[\vartheta_p]$.

(i) We have $\mathbb{Z}[\vartheta_p]_{(p)} = \mathbb{Z}[\vartheta_p]_{(\vartheta_p)}$ *as subrings of* $\mathbb{Q}(\vartheta_p)$.

(ii) We have $\mathbb{Z}[\vartheta_p]_{(p)} = \mathbb{Z}_{(p)}[\vartheta_p]$ *as subrings of* $\mathbb{Q}(\vartheta_p)$.

(iii) In particular, $\mathbb{Z}_{(p)}[\vartheta_p]$ *is a discrete valuation ring.*

(iv) Moreover, the maximal ideal of $\mathbb{Z}_{(p)}[\vartheta_p]$ *is generated by* ϑ_p .

Proof of *(i)*. Recall that $(p) \subseteq \mathbb{Z}$ and $(\vartheta) \subseteq \mathbb{Z}[\vartheta]$ are prime ideals; cf. Lemma 27 *(i)*. So the localizations of $\mathbb{Z}[\vartheta]$ at (ϑ) respective (p) are defined; cf. Definition 117. By Lemma 22 we have $\mathbb{Z}[\vartheta] = \mathcal{O}_{\mathbb{Q}(\vartheta)}$. By Lemma 27 *(ii)*, we have $(p) = \mathbb{Z} \cap (\vartheta)$. By Lemma 29 we have $\vartheta^n\mathbb{Z}[\vartheta] = p\mathbb{Z}[\vartheta]$. Therefore we can apply Lemma 137 to the case $(L, K, \mathcal{O}_K, \mathfrak{p}, \mathcal{O}_L, \mathfrak{q}, s) = (\mathbb{Q}(\vartheta), \mathbb{Q}, \mathbb{Z}, (p), \mathbb{Z}[\vartheta], (\vartheta), n)$ and obtain the assertion.

Proof of *(ii)*. Using Lemma 24 *(i3)* we have to show the vertical equality in

$$\begin{array}{rcl} \mathbb{Z}[\vartheta]_{(p)} & = & \left\{ \frac{\sum_{i=0}^{n-1} a_i\vartheta^i}{s} \,:\, a_i \in \mathbb{Z} \text{ for } i \in [0,n-1], s \in \mathbb{Z} \setminus (p) \right\} \quad \subseteq \quad \mathbb{Q}(\vartheta) \\ & & \qquad\qquad \| \; ! \\ \mathbb{Z}_{(p)}[\vartheta] & = & \left\{ \sum_{i=0}^{n-1} \frac{b_i}{s_i}\vartheta^i \,:\, b_i \in \mathbb{Z} \text{ for } i \in [0,n-1], s_i \in \mathbb{Z} \setminus (p) \text{ for } i \in [0,n-1] \right\} \quad \subseteq \quad \mathbb{Q}(\vartheta)\,. \end{array}$$

The inclusion "$\cap$|" holds using coefficients $\frac{a_i}{s}$ of ϑ^i for $i \in [0, n-1]$.

Ad "|$\cup$". Let $s := \prod_{i=0}^{n-1} s_i \in \mathbb{Z}\setminus(p)$. Then $ss_i^{-1} \in \mathbb{Z}$ for $i \in [0, n-1]$, and $\sum_{i=0}^{n-1} \frac{b_i}{s_i}\vartheta^i = \frac{\sum_{i=0}^{n-1}(b_i s s_i^{-1})\vartheta^i}{s} \in \mathbb{Z}[\vartheta]_{(p)}$.

Proof of *(iii)*. By Corollary 23 the ring $\mathbb{Z}[\vartheta]$ is a Dedekind domain. By Lemma 27 *(i)*, the ideal $(\vartheta) \neq 0$ of $\mathbb{Z}[\vartheta]$ is prime. Therefore we get with Definition 131 that $\mathbb{Z}[\vartheta]_{(\vartheta)} \overset{(i)}{=} \mathbb{Z}[\vartheta]_{(p)} \overset{(ii)}{=} \mathbb{Z}_{(p)}[\vartheta]$ is a discrete valuation ring.

Proof of *(iv)*. By Lemma 27 *(i)* we have that (ϑ) is a maximal ideal of $\mathbb{Z}[\vartheta]$. So we obtain by *(iii)* and Remark 126 that $(\vartheta)_{(\vartheta)}$ is the unique maximal of $\mathbb{Z}[\vartheta]_{(\vartheta)} = \mathbb{Z}_{(p)}[\vartheta]$. □

Lemma 47 *The* $\mathbb{Z}_{(p)}[\vartheta_p]$*-submodule* ${}_p\tilde{\Psi}_{(p)}$ *of* $\mathbb{Z}_{(p)}[\vartheta_p]^{\times n}$ *has the* $\mathbb{Z}_{(p)}[\vartheta_p]$*-linear basis*

$$\mathrm{B}_{\tilde{\Psi}_{(p)}} = \mathrm{B}_{{}_p\tilde{\Psi}_{(p)}} := \left(\vartheta_p^l \cdot \left(\frac{(2k-1)^2}{l+k-1} \binom{l+k-1}{k-l} \right)_{k\in[1,n]} \,:\, l \in [1,n] \right).$$

Proof. First, note that the elements of $\mathrm{B}_{\tilde{\Psi}_{(p)}}$ are the rows of an upper triangular matrix, whence $\mathrm{B}_{\tilde{\Psi}_{(p)}}$ is $\mathbb{Z}_{(p)}[\vartheta]$-linearly independent.

The describing matrix of the embedding $\iota : \langle \mathrm{B}_{\tilde{\Psi}_{(p)}} \rangle_{\mathbb{Z}_{(p)}[\vartheta]} \hookrightarrow \mathbb{Z}_{(p)}[\vartheta]^{\times n}$ with respect to $\mathrm{B}_{\tilde{\Psi}_{(p)}}$ and to the standard basis of $\mathbb{Z}_{(p)}[\vartheta]^{\times n}$ is

$$L \;=\; \left(\vartheta^l \cdot \frac{(2k-1)^2}{l+k-1} \binom{l+k-1}{k-l} \right)_{k,l\in[1,n]} .$$

Since $l+k-1 \leq 2n-1 < p$ for $l,k \in [1,n]$, we see that $L \in \big(\mathbb{Z}_{(p)}[\vartheta]\big)^{n\times n}$.

Note that by Remark 143 the matrix L is already contained in $\mathbb{Z}[\vartheta]^{n\times n}$. So $\mathrm{B}_{\tilde{\Psi}_{(p)}}$, which we find again in the columns of L, is already contained in $\mathbb{Z}[\vartheta]^{\times n}$. Cf. Subsection 2.2.4.

Further we consider the matrix

$$K_{\tilde{\Psi}} \;=\; \left(\frac{(2i-1)^2}{(2k-1)^2}(2i)! \left\langle {i-1 \atop k} \right\rangle \right)_{i,k\in[1,n]} \overset{\text{R.141}}{=} \left((-1)^{i-k} \binom{2i-1}{i-k} \frac{(2i)!}{2k-1}(2i-1) \right)_{i,k\in[1,n]} \overset{\text{R.141}}{\in} \mathbb{Z}^{n\times n},$$

defined in Remark 44.

Then we have

$$\left.\begin{aligned}
K_{\tilde{\Psi}}L =& \left(\sum_{k=1}^{n} (-1)^{i-k} \binom{2i-1}{i-k} \frac{(2i)!}{2k-1}(2i-1) \cdot \vartheta^l \cdot \frac{(2k-1)^2}{l+k-1} \binom{l+k-1}{k-l} \right)_{i,l\in[1,n]} \\
=& \left(\vartheta^l \cdot (2i-1)(2i)! \sum_{k=1}^{n} (-1)^{i-k} \underbrace{\binom{2i-1}{i-k}}_{=0 \text{ for } k>i} \frac{2k-1}{l+k-1} \underbrace{\binom{l+k-1}{k-l}}_{=0 \text{ for } k<l} \right)_{i,l\in[1,n]} \\
=& \left(\vartheta^l \cdot (2i-1)(2i)! \sum_{k=l}^{i} (-1)^{i-k} \binom{2i-1}{i-k} \frac{2k-1}{l+k-1} \binom{l+k-1}{k-l} \right)_{i,l\in[1,n]} \\
\overset{k'=k-l}{=}& \left(\vartheta^l \cdot (2i-1)(2i)! \sum_{k'=0}^{i-l} (-1)^{i-l-k'} \binom{2i-1}{i-l-k'} \frac{2l+2k'-1}{2l+k'-1} \binom{2l+k'-1}{k'} \right)_{i,l\in[1,n]} \\
\overset{k=k'}{=}& \left(\vartheta^l \cdot (2i-1)(2i)!(-1)^{i-l} \sum_{k=0}^{i-l} (-1)^{k} \binom{2i-1}{i-l-k} \frac{2l+2k-1}{2l+k-1} \frac{(2l+k-1)!}{k!(2l-1)!} \right)_{i,l\in[1,n]} \\
=& \left(\vartheta^l \cdot (2i-1)(2i)!(-1)^{i-l} \sum_{k=0}^{i-l} (-1)^{k} \binom{2i-1}{i-l-k} (2l+2k-1) \frac{(2l+k-2)!}{k!(2l-2)!} \frac{1}{2l-1} \right)_{i,l\in[1,n]} \\
=& \left(\vartheta^l \cdot (2i-1)(2i)! \frac{1}{2l-1}(-1)^{i-l} \sum_{k=0}^{i-l} (-1)^{k} \binom{2i-1}{i-l-k} (2l+2k-1) \binom{2l+k-2}{2l-2} \right)_{i,l\in[1,n]} \\
\overset{\text{C.140}}{=}& \left(\vartheta^l \cdot (2i-1)(2i)! \frac{1}{2l-1}(2i-1) \cdot \partial_{i,l} \right)_{i,l\in[1,n]} \\
=& \big(\vartheta^l \cdot (2i-1)(2i)! \cdot \partial_{i,l} \big)_{i,l\in[1,n]} \;=\; \mathrm{diag}\big(\vartheta^i (2i-1)(2i)! \,:\, i \in [1,n] \big) \;=:\; F .
\end{aligned}\right\} (1)$$

By Remark 44, we have, given $a = (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$,

$$a \in \tilde{\Psi} \iff D_{\tilde{\Psi}} K_{\tilde{\Psi}} a^{\mathrm{t}} \in \vartheta^n \mathbb{Z}[\vartheta]^{n\times 1} .$$

We apply Corollary 125 to the case $(A, B, \mathfrak{p}, x, k, M, N) = (\,\mathbb{Z},\, \mathbb{Z}[\vartheta],\, p\mathbb{Z},\, \vartheta^n,\, n,\, D_{\tilde{\Psi}} K_{\tilde{\Psi}}\,,\, \tilde{\Psi}^{\mathrm{t}}\,)$.
So given $a = (a_j)_{j\in[1,n]} \in \big(\mathbb{Z}[\vartheta]_{(p)}\big)^{\times n} \underset{\text{R.46}\,(ii)}{=} \big(\mathbb{Z}_{(p)}[\vartheta]\big)^{\times n}$, we have

$$a \in \tilde{\Psi}_{(p)} \iff D_{\tilde{\Psi}} K_{\tilde{\Psi}} a^{\mathrm{t}} \in \vartheta^n \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{n\times 1}\,.$$

Therefore we get

$$\left.\begin{array}{rcl}
a \in \tilde{\Psi}_{(p)} & \iff & D_{\tilde{\Psi}} \overbrace{K_{\tilde{\Psi}}}^{\overset{(1)}{=} FL^{-1}} a^{\mathrm{t}} \in \vartheta^n \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{n\times 1} \\
& \iff & (D_{\tilde{\Psi}} F) L^{-1} a^{\mathrm{t}} \in \vartheta^n \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{n\times 1} \\
& \overset{\text{R.44}}{\iff} & \vartheta^n \cdot \mathrm{diag}(\,(2i-1)(2i)! \,:\, i \in [1,n]\,) L^{-1} a^{\mathrm{t}} \in \vartheta^n \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{n\times 1} \\
& \iff & \underbrace{\mathrm{diag}(\,(2i-1)(2i)! \,:\, i \in [1,n]\,)}_{=:A} L^{-1} a^{\mathrm{t}} \in \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{n\times 1}
\end{array}\right\} \quad (2)$$

Since $2i-1 < 2i \le 2n < p$ for $i \in [1,n]$, we get that $p \nmid \det(A) \in \mathbb{Z}$. Therefore $A \in \mathrm{GL}_n\big(\mathbb{Z}_{(p)}\big)$, implying that $A^{-1}\left(\mathbb{Z}_{(p)}[\vartheta]\right)^{n\times 1} = \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{n\times 1}$.

So we get with (2)

$$a \in \tilde{\Psi}_{(p)} \iff a^{\mathrm{t}} \in L\left(\mathbb{Z}_{(p)}[\vartheta]\right)^{n\times 1} \iff a \in \langle \mathrm{B}_{\tilde{\Psi}_{(p)}} \rangle_{\mathbb{Z}_{(p)}[\vartheta]}\,.$$

Therefore we have $\tilde{\Psi}_{(p)} = \langle \mathrm{B}_{\tilde{\Psi}_{(p)}} \rangle_{\mathbb{Z}_{(p)}[\vartheta]}$. □

Example 48

In the case $p = 11$ the $\mathbb{Z}_{(11)}[\vartheta_{11}]$-linear basis $\mathrm{B}_{{}_{11}\tilde{\Psi}_{(11)}}$ of the submodule ${}_{11}\tilde{\Psi}_{(11)}$ of $\mathbb{Z}_{(11)}[\vartheta_{11}]^{\times 5}$ is given by

$$\mathrm{B}_{{}_{11}\tilde{\Psi}_{(11)}} = \begin{pmatrix}
\vartheta_{11}^1 \cdot (\,1\,, & 9\,, & 25\,, & 49\,, & 81\,)\,, \\
\vartheta_{11}^2 \cdot (\,0\,, & 3\,, & 25\,, & 98\,, & 270\,)\,, \\
\vartheta_{11}^3 \cdot (\,0\,, & 0\,, & 5\,, & 49\,, & 243\,)\,, \\
\vartheta_{11}^4 \cdot (\,0\,, & 0\,, & 0\,, & 7\,, & 81\,)\,, \\
\vartheta_{11}^5 \cdot (\,0\,, & 0\,, & 0\,, & 0\,, & 9\,)
\end{pmatrix}.$$

2.2.3 The principal ideal of ${}_p\Psi$ generated by the image of $1 \otimes \vartheta_p$ equals ${}_p\tilde{\Psi}$

Definition 49 We define

$$\theta = \theta_p := (\,\sigma_n(\vartheta_p)\,, \ldots, \sigma_1(\vartheta_p)\,) = f(1 \otimes \vartheta_p) \in {}_p\Psi\,,$$

where $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\vartheta_p)|\mathbb{Q})$ for $i \in [1,n]$; cf. Notation 26. For f we refer to Proposition 41.

We obtain the principal ideal $\theta\Psi = \theta_p \cdot {}_p\Psi$ in ${}_p\Psi$ generated by θ_p.

Remark 50 *The principal ideal of ${}_p\Psi$ generated by θ_p has the $\mathbb{Z}[\vartheta_p]$-linear basis*

$$\mathrm{B}_{\theta\Psi} \;=\; \mathrm{B}_{\theta_p\cdot {}_p\Psi} \;:=\; \left(\vartheta_p^{l-1}\cdot\left(\sigma_{n-k+1}(\vartheta_p)\cdot\binom{l+k-2}{2l-2}\right)_{k\in[1,n]} \;:\; l\in[1,n]\right).$$

Let $\iota : \theta_p\cdot {}_p\Psi \longhookrightarrow \mathbb{Z}[\vartheta_p]^{\times n}$ be the canonical embedding. Then we have

$$\det_{\mathbb{Z}[\vartheta_p]}(\iota) \;=\; \prod_{s=1}^{n}\left(\vartheta_p^{s-1}\cdot\sigma_{n-s+1}(\vartheta_p)\right) \qquad \textit{and} \qquad \det_{\mathbb{Z}}(\iota) \;=\; \pm p^{\frac{n(n+1)}{2}}\,.$$

Proof. By Lemma 38 we have a $\mathbb{Z}[\vartheta]$-linear basis of Ψ given by $\mathrm{B}_\Psi = \left(\vartheta^{l-1}\cdot\left(\binom{l+k-2}{2l-2}\right)_{k\in[1,n]} \;:\; l\in[1,n]\right)$. Therefore $\theta\Psi$ has the $\mathbb{Z}[\vartheta]$-linear basis $\theta\cdot\mathrm{B}_\Psi = \left(\vartheta^{l-1}\cdot\left(\sigma_{n-k+1}(\vartheta)\cdot\binom{l+k-2}{2l-2}\right)_{k\in[1,n]} \;:\; l\in[1,n]\right) = \mathrm{B}_{\theta\Psi}$.

Further we have $\displaystyle\binom{l+k-2}{2l-2} = \begin{cases} 0 \text{ for } k<l \text{ and} \\ 1 \text{ for } k=l\,. \end{cases}$

Therefore the describing matrix A of the $\mathbb{Z}[\vartheta]$-linear embedding $\iota : \theta\Psi \longhookrightarrow \mathbb{Z}[\vartheta]^{\times n}$ with respect to $\mathrm{B}_{\theta\Psi}$ and to the standard basis of $\mathbb{Z}[\vartheta]^{\times n}$ is lower triangular. Its diagonal entry at position (s,s) is $\vartheta^{s-1}\cdot\sigma_{n-s+1}(\vartheta)$ for $s\in[1,n]$. So A has the determinant

$$\det(A) \;=\; \prod_{s=1}^{n}\left(\vartheta^{s-1}\cdot\sigma_{n-s+1}(\vartheta)\right).$$

We have

$$\begin{aligned}
\det_{\mathbb{Z}}(\iota) \;&\overset{(1)}{=}\; \pm\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\det_{\mathbb{Z}[\vartheta]}(\iota)) \;=\; \pm\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\det(A)) \;=\; \pm\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}\left(\prod_{s=1}^{n}\left(\vartheta^{s-1}\cdot\sigma_{n-s+1}(\vartheta)\right)\right)\\
&=\; \pm\prod_{s=1}^{n}\left(\left(\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta)\right)^{s-1}\cdot\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\sigma_{n-s+1}(\vartheta))\right) \;\overset{(2)}{=}\; \pm\prod_{s=1}^{n}\left(\left(\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta)\right)^{s-1}\cdot\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta)\right)\\
&=\; \pm\prod_{s=1}^{n}\left(\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}(\vartheta)\right)^{s} \;\underset{(iv)}{\overset{\text{L.24}}{=}}\; \pm\prod_{s=1}^{n}p^s \;=\; \pm p^{\frac{n(n+1)}{2}}\,,
\end{aligned}$$

where in (1) we refer to Lemma 116 applied to the case

$$(K,s,A,B,r,\mathcal{O}_K,\varphi) \;=\; (\mathbb{Q}(\vartheta),n,\theta\Psi,\mathbb{Z}[\vartheta]^{\times n},n,\mathcal{O}_{\mathbb{Q}(\vartheta)},\iota)\,,$$

and recall that $\mathcal{O}_{\mathbb{Q}(\vartheta)} \overset{\text{L.22}}{=} \mathbb{Z}[\vartheta]$.

In (2) we refer to [Neukirch 99, Ch. I, p. 9, Proposition (2.6.iii)]; cf. also Corollary 114 for the corresponding statement for the trace. □

Example 51 In the case $p=11$ the $\mathbb{Z}[\vartheta_{11}]$-linear basis $\mathrm{B}_{\theta_{11}\cdot {}_{11}\Psi}$ of the submodule $\theta_{11}\cdot {}_{11}\Psi$ of $\mathbb{Z}[\vartheta_{11}]^{\times 5}$ is given by

$$\mathrm{B}_{\theta_{11}\cdot {}_{11}\Psi} \;=\; \begin{pmatrix}
(\,\sigma_5(\vartheta_{11}), & \sigma_4(\vartheta_{11}), & \sigma_3(\vartheta_{11}), & \sigma_2(\vartheta_{11}), & \sigma_1(\vartheta_{11}))\,,\\
\vartheta_{11}^1\cdot(\,0, & \sigma_4(\vartheta_{11}), & 3\cdot\sigma_3(\vartheta_{11}), & 6\cdot\sigma_2(\vartheta_{11}), & 10\cdot\sigma_1(\vartheta_{11}))\,,\\
\vartheta_{11}^2\cdot(\,0, & 0, & \sigma_3(\vartheta_{11}), & 5\cdot\sigma_2(\vartheta_{11}), & 15\cdot\sigma_1(\vartheta_{11}))\,,\\
\vartheta_{11}^3\cdot(\,0, & 0, & 0, & \sigma_2(\vartheta_{11}), & 7\cdot\sigma_1(\vartheta_{11}))\,,\\
\vartheta_{11}^4\cdot(\,0, & 0, & 0, & 0, & \sigma_1(\vartheta_{11}))
\end{pmatrix},$$

respectively, written using the $\mathbb{Z}$-linear basis $(\,\vartheta_{11}^i \,:\, i \in [1,5]\,)$ of $\vartheta_{11}\mathbb{Z}[\vartheta_{11}]$, cf. Lemma 24 *(i3)*,

$$\mathrm{B}_{\theta_{11}\cdot{}_{11}\Psi} = \begin{pmatrix} (\,\vartheta_{11}^5{+}10\vartheta_{11}^4{+}35\vartheta_{11}^3{+}50\vartheta_{11}^2{+}25\vartheta_{11},\ \vartheta_{11}^4{+}8\vartheta_{11}^3{+}20\vartheta_{11}^2{+}16\vartheta_{11},\ \vartheta_{11}^3{+}6\vartheta_{11}^2{+}9\vartheta_{11},\ \vartheta_{11}^2{+}4\vartheta_{11},\ \vartheta_{11}\,), \\ (\,0,\ \vartheta_{11}^5{+}8\vartheta_{11}^4{+}20\vartheta_{11}^3{+}16\vartheta_{11}^2,\ 3\vartheta_{11}^4{+}18\vartheta_{11}^3{+}27\vartheta_{11}^2,\ 6\vartheta_{11}^3{+}24\vartheta_{11}^2,\ 10\vartheta_{11}^2\,), \\ (\,0,\ 0,\ \vartheta_{11}^5{+}6\vartheta_{11}^4{+}9\vartheta_{11}^3,\ 5\vartheta_{11}^4{+}20\vartheta_{11}^3,\ 15\vartheta_{11}^3\,), \\ (\,0,\ 0,\ 0,\ \vartheta_{11}^5{+}4\vartheta_{11}^4,\ 7\vartheta_{11}^4\,), \\ (\,0,\ 0,\ 0,\ 0,\ \vartheta_{11}^5\,) \end{pmatrix}.$$

Proposition 52 *The principal ideal of* ${}_p\Psi$ *generated by* θ_p *is given by*

$$\theta_p \cdot {}_p\Psi \;=\; \left\{ (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n} \,:\, \sum_{k=1}^{n} \frac{(2i-1)^2}{(2k-1)^2} \cdot (2i)! \cdot \left\langle \begin{matrix} i-1 \\ k \end{matrix} \right\rangle \cdot a_k \equiv_{\vartheta_p^i} 0 \text{ for } i \in [1,n] \right\} \;=\; {}_p\tilde{\Psi}\,.$$

Proof. We have

$$\theta\Psi \overset{\text{P.41}}{\underset{\text{D.49}}{=}} f(1\otimes\vartheta)f(\mathbb{Z}[\vartheta]\otimes\mathbb{Z}[\vartheta]) \;=\; f(\mathbb{Z}[\vartheta]\otimes\vartheta\mathbb{Z}[\vartheta])\,. \tag{1}$$

We choose the $\mathbb{Z}$-linear basis $(\,{}_k\gamma - 2 \,:\, k\in[1,n]\,)$ of $\vartheta\mathbb{Z}[\vartheta]$; cf. Remark 32 *(ii)*. Therefore we can choose the $\mathbb{Z}[\vartheta]$-linear basis $B := (\,1\otimes({}_1\gamma-2)\,,\, 1\otimes({}_2\gamma-2)\,,\,\ldots\,,\, 1\otimes({}_{n-1}\gamma-2)\,,\, 1\otimes({}_n\gamma-2)\,)$ of $\mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\vartheta\mathbb{Z}[\vartheta]$; cf. Lemma 100 *(i)*. So we get by (1) that

$$\theta\Psi \;=\; \langle\, f(1\otimes({}_s\gamma-2)) \,:\, s\in[1,n]\,\rangle_{\mathbb{Z}[\vartheta]}\,. \tag{2}$$

Now we want to show that $\theta\Psi \overset{!}{\subseteq} \tilde{\Psi}$. Because of (2) it suffices to show that

$$f(1\otimes({}_s\gamma-2)) \overset{!}{\in} \tilde{\Psi} \text{ for } s\in[1,n]\,. \qquad (*)$$

Given $(a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$ and $\tau \in \mathrm{Gal}(\mathbb{Q}(\vartheta)|\mathbb{Q})$ we write $\tau((a_j)_{j\in[1,n]}) := (\tau(a_j))_{j\in[1,n]}$.

For $(a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$, we obtain

$$\left.\begin{aligned}
(a_j)_{j\in[1,n]} \in \tilde{\Psi} &\overset{\text{D.42}}{\iff} \sum_{k=1}^{n} \tfrac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot\left\langle\begin{matrix} i-1\\ k\end{matrix}\right\rangle\cdot a_k \equiv_{\vartheta^i} 0 \text{ for } i\in[1,n] \\
&\iff \sum_{k=1}^{n} \tfrac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot\left\langle\begin{matrix} i-1\\ k\end{matrix}\right\rangle\cdot a_k \in \vartheta^i\mathbb{Z}[\vartheta] \overset{\text{R.28}}{\underset{(iii)}{=}} \tau^{-1}\big(\vartheta^i\mathbb{Z}[\vartheta]\big) \text{ for } i\in[1,n] \\
&\iff \tau\left(\sum_{k=1}^{n} \tfrac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot\left\langle\begin{matrix} i-1\\ k\end{matrix}\right\rangle\cdot a_k\right) \in \vartheta^i\mathbb{Z}[\vartheta] \text{ for } i\in[1,n] \\
&\overset{\text{R.141}}{\iff} \sum_{k=1}^{n} \tfrac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot\left\langle\begin{matrix} i-1\\ k\end{matrix}\right\rangle\cdot \tau(a_k) \in \vartheta^i\mathbb{Z}[\vartheta] \text{ for } i\in[1,n] \\
&\iff \sum_{k=1}^{n} \tfrac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot\left\langle\begin{matrix} i-1\\ k\end{matrix}\right\rangle\cdot \tau(a_k) \equiv_{\vartheta^i} 0 \text{ for } i\in[1,n] \\
&\iff (\tau(a_j))_{j\in[1,n]} \in \tilde{\Psi} \iff \tau((a_j)_{j\in[1,n]}) \in \tilde{\Psi}\,.
\end{aligned}\right\} \tag{3}$$

Further we have for $s \in [1,n]$

$$\left.\begin{array}{rcl} f(1\otimes({}_s\gamma-2)) = f(1\otimes\sigma_s({}_1\gamma-2)) & = & (\sigma_{n-j+1}(\sigma_s({}_1\gamma-2)))_{j\in[1,n]} \\ & \overset{\text{Gal.gr.}}{\underset{\text{abelian}}{=}} & (\sigma_s(\sigma_{n-j+1}({}_1\gamma-2)))_{j\in[1,n]} \\ & = & \sigma_s((\sigma_{n-j+1}({}_1\gamma-2))_{j\in[1,n]}) = \sigma_s(f(1\otimes({}_1\gamma-2)))\,. \end{array}\right\} (4)$$

Because of (3) and (4) our task from $(*)$ reduces further to

$$f(1\otimes({}_1\gamma-2)) \;=\; (\sigma_{n-j+1}({}_1\gamma-2))_{j\in[1,n]} \;=\; ({}_{n-j+1}\gamma-2)_{j\in[1,n]} \overset{!}{\in} \tilde{\Psi}\,.$$

For this we shall verify that the tuple $({}_{n-j+1}\gamma-2)_{j\in[1,n]}$ satisfies the defining congruences for $\tilde{\Psi}$.

For $i \in [1,n]$ we have

$$\begin{array}{rcl} & & \sum_{k=1}^{n} \frac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot\left\langle {i-1 \atop k}\right\rangle\cdot({}_{n-k+1}\gamma-2) \\ \overset{\text{R.141}}{\underset{\text{D.17}}{=}} & & \sum_{k=1}^{n}(-1)^{i-k}\cdot\underbrace{\binom{2i-1}{i-k}}_{=0 \text{ for } k>i}\cdot\frac{(2i)!}{2k-1}\cdot(2i-1)\cdot\left(\zeta^{n-k+1}+\zeta^{-n+k-1}-2\right) \\ & = & (2i)!\cdot(2i-1)\cdot(-1)^i\cdot\sum_{k=1}^{i}(-1)^k\cdot\binom{2i-1}{i-k}\cdot\frac{1}{2k-1}\cdot\left(\zeta^{n-k+1}+\zeta^{\overbrace{2n+1}^{=p}-n+k-1}-2\right) \\ & = & (2i)!\cdot(2i-1)\cdot(-1)^i\cdot\sum_{k=1}^{i}(-1)^k\cdot\binom{2i-1}{i-k}\cdot\frac{1}{2k-1}\cdot\left(((\zeta-1)+1)^{n-k+1}+((\zeta-1)+1)^{n+k}-2\right) \\ & = & (2i)!\cdot(2i-1)\cdot(-1)^i\cdot\sum_{k=1}^{i}(-1)^k\cdot\binom{2i-1}{i-k}\cdot\frac{1}{2k-1}\cdot\left(\sum_{j=1}^{n-k+1}\underbrace{\binom{n-k+1}{j}}_{\substack{=0 \text{ for}\\ j>n-k+1}}(\zeta-1)^j+\sum_{j=1}^{n+k}\binom{n+k}{j}(\zeta-1)^j\right) \\ & = & (2i)!\cdot(2i-1)\cdot(-1)^i\cdot\sum_{k=1}^{i}(-1)^k\cdot\binom{2i-1}{i-k}\cdot\frac{1}{2k-1}\cdot\left(\sum_{j=1}^{n+k}\binom{n-k+1}{j}(\zeta-1)^j+\sum_{j=1}^{n+k}\binom{n+k}{j}(\zeta-1)^j\right) \\ & = & (2i)!\cdot(2i-1)\cdot(-1)^i\cdot\sum_{k=1}^{i}(-1)^k\cdot\binom{2i-1}{i-k}\cdot\frac{1}{2k-1}\cdot\sum_{j=1}^{n+k}\left(\binom{n-k+1}{j}+\binom{n+k}{j}\right)\cdot(\zeta-1)^j \;=:\; \mathrm{S}(i). \end{array}$$

We denote the coefficient of $(\zeta-1)^j$ in $\mathrm{S}(i)$ with $\mathrm{k}(i,j)$.

Considering the left side of the equation above we get with Remark 141 and Remark 32 *(ii)* that

$$\mathrm{S}(i) \in \vartheta\mathbb{Z}[\vartheta] \overset{\text{R.31}}{\subseteq} (\zeta-1)\mathbb{Z}[\zeta]\,.$$

Choosing the $\mathbb{Z}$-liner basis $(\,(\zeta-1)^l \,:\, l\in[0,\overbrace{2n-1}^{=p-2}]\,)$ of $\mathbb{Z}[\zeta]$ we get that $(\zeta-1)\mathbb{Z}[\zeta]$ has the $\mathbb{Z}$-liner basis $(\,(\zeta-1)^l \,:\, l\in[1,2n]\,)$. Since $j \le n+k \le n+i \le 2n$, we therefore get that all occurring coefficients $\mathrm{k}(i,j)$ in $\mathrm{S}(i)$ are integers.

Let us have a closer look at the coefficients $\mathrm{k}(i,s)$ for $s\in[1,2i-1]$. We calculate

$$\begin{array}{rcl} \mathbb{Z}\ni\mathrm{k}(i,s) & := & (2i)!\cdot(2i-1)\cdot(-1)^i\cdot\sum_{k=1}^{i}(-1)^k\cdot\binom{2i-1}{i-k}\cdot\frac{1}{2k-1}\cdot\left(\binom{n-k+1}{s}+\binom{n+k}{s}\right) \\ & \overset{\text{R.142}}{=} & (2i)!\cdot(2i-1)\cdot(-1)^i\cdot(-1)^i\cdot\sum_{k=0}^{2i-1}(-1)^k\cdot\binom{2i-1}{k}\cdot\frac{1}{2i-1-2k}\cdot\binom{n+i-k}{s} \end{array}$$

$$
\begin{aligned}
&= (2i)! \cdot (2i-1) \cdot (-1)^{i-1} \cdot (-1)^{i+1} \cdot \sum_{k=0}^{2i-1} (-1)^k \cdot \tbinom{2i-1}{k} \cdot \tfrac{1}{2i-1-2k} \cdot \tbinom{n+i-k}{s} \\
\overset{\text{R.147}}{=}\ & (2i)! \cdot (2i-1) \cdot (-1)^{i-1} \cdot 2^{4i-2-s} \cdot \tfrac{i!(i-1)!}{s!(2i)!} \cdot \prod_{u=0}^{s-1} (2n+1-2u) \\
=\ & (2i-1) \cdot (-1)^{i-1} \cdot 2^{4i-2-s} \cdot \tfrac{i!(i-1)!}{s!} \cdot \prod_{u=0}^{s-1} (p-2u) \\
=\ & p \cdot (2i-1) \cdot (-1)^{i-1} \cdot 2^{4i-2-s} \cdot \tfrac{i!(i-1)!}{s!} \cdot \prod_{u=1}^{s-1} (p-2u) \\
=\ & p \cdot \tfrac{1}{s!} \cdot (2i-1) \cdot (-1)^{i-1} \cdot 2^{4i-2-s} \cdot i!(i-1)! \cdot \prod_{u=1}^{s-1} (p-2u)\,. \qquad \leftarrow\ (**)
\end{aligned}
$$

So we have $\mathrm{k}(i,s) = p \cdot \frac{x}{y}$, with $x \in \mathbb{Z}$ and $y \in \mathbb{Z}_{\geq 1}$. Without loss of generality we suppose that x is coprime to y. Since $\mathrm{k}(i,s) \in \mathbb{Z}$ we know that $y \in \{1,p\}$. We further know from $(**)$ that y is a divisor of $s!$. But, since $s \leq 2i-1 \leq 2n-1 < p$, we get that y equals 1. Thus we have that $\frac{\mathrm{k}(i,s)}{p} = x \in \mathbb{Z}$ for $s \in [1, 2i-1]$.

So we can write $\mathrm{S}(i)$ as

$$
\mathrm{S}(i) = (\zeta-1)^{2i} \cdot w + p \cdot \sum_{j=1}^{2i-1} a_j (\zeta-1)^j \text{ , with } a_j \in \mathbb{Z} \text{ for } j \in [1,2i-1] \text{ and } w \in \mathbb{Z}[\zeta]\,. \qquad (***)
$$

By considering the divisor chain

$$
(\zeta-1)^{2i} \underset{\text{R.30}}{\overset{\uparrow}{\text{ divides }}} \vartheta^n \underset{\text{L.29}}{\overset{\uparrow}{\text{ divides }}} p \text{ in } \mathbb{Z}[\zeta] \text{ for } i \in [1,n]\,,
$$

and using $(***)$ we get that

$$
\mathrm{S}(i) \equiv_{(\zeta-1)^{2i}} 0 \text{ in } \mathbb{Z}[\zeta] \overset{\text{R.30}}{\iff} \mathrm{S}(i) \equiv_{\vartheta^i} 0 \text{ in } \mathbb{Z}[\vartheta]\,.
$$

Hence $\theta\Psi$ is a subset of $\tilde{\Psi}$.

Suppose given $a = (a_j)_{j \in [1,n]} \in \mathbb{Z}[\vartheta]^{\times n}$. Then we know from Remark 44 that

$$
\left.
\begin{aligned}
a \in \tilde{\Psi} &\iff D_{\tilde{\Psi}} K_{\tilde{\Psi}} a^{\mathrm{t}} \in \vartheta^n \mathbb{Z}[\vartheta]^{n \times 1} \\
&\iff a^{\mathrm{t}} \in \vartheta^n K_{\tilde{\Psi}}^{-1} D_{\tilde{\Psi}}^{-1} \mathbb{Z}[\vartheta]^{n \times 1}
\end{aligned}
\right\} \quad (5)
$$

We define $\tilde{\Psi}' := \left(\vartheta^n K_{\tilde{\Psi}}^{-1} D_{\tilde{\Psi}}^{-1} \mathbb{Z}[\vartheta]^{n \times 1}\right)^{\mathrm{t}}$. Using (5) we therefore get that $\tilde{\Psi} = \tilde{\Psi}' \cap \mathbb{Z}[\vartheta]^{\times n}$.

We choose the standard basis $(e_i : i \in [1,n])$ for $\mathbb{Z}[\vartheta]^{\times n}$ and the basis $\left(\det(K_{\tilde{\Psi}})^{-1} e_i : i \in [1,n]\right)$ for $\det(K_{\tilde{\Psi}})^{-1} \mathbb{Z}[\vartheta]^{\times n} \subseteq \mathbb{Q}(\vartheta)^{\times n}$. So the embedding $j : \mathbb{Z}[\vartheta]^{\times n} \hookrightarrow \det(K_{\tilde{\Psi}})^{-1} \mathbb{Z}[\vartheta]^{\times n}$ is given by the matrix $\det(K_{\tilde{\Psi}})\,\mathrm{E}_n$.
For $\tilde{\Psi}'$ we choose the basis $\left(\left(\vartheta^n K_{\tilde{\Psi}}^{-1} D_{\tilde{\Psi}}^{-1} e_i^{\mathrm{t}}\right)^{\mathrm{t}} : i \in [1,n]\right)$.

For fixed $i \in [1,n]$ we are looking for $\lambda_{j,i} \in \mathbb{Z}[\vartheta]$ for $j \in [1,n]$ with

$$
\vartheta^n K_{\tilde{\Psi}}^{-1} D_{\tilde{\Psi}}^{-1} e_i^{\mathrm{t}} = \sum_{j=1}^{n} \lambda_{j,i} \det(K_{\tilde{\Psi}})^{-1} e_j^{\mathrm{t}}\,,
$$

i.e. we are looking for a representation of the i-th basis element of $\tilde{\Psi}'$ in the basis of $\det(K_{\tilde{\Psi}})^{-1} \mathbb{Z}[\vartheta]^{\times n}$. This is equivalent to

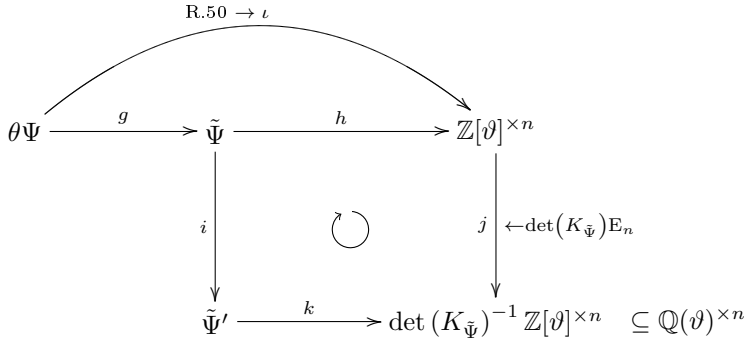
$$
\det(K_{\tilde{\Psi}})\, K_{\tilde{\Psi}}^{-1} \vartheta^n D_{\tilde{\Psi}}^{-1} e_i^{\mathrm{t}} = \sum_{j=1}^{n} \lambda_{j,i}\, e_j^{\mathrm{t}}\,.
$$

So the desired $\lambda_{1,i}\,,\,\ldots\,,\,\lambda_{n,i}$ can be found in the i-th column of the matrix $\det\left(K_{\tilde{\Psi}}\right) K_{\tilde{\Psi}}^{-1}\vartheta^n D_{\tilde{\Psi}}^{-1}$. Thus the latter is the describing matrix of the embedding $k : \tilde{\Psi}' \hookrightarrow \det\left(K_{\tilde{\Psi}}\right)^{-1}\mathbb{Z}[\vartheta]^{\times n}$.

Note, since $\vartheta^n D_{\tilde{\Psi}}^{-1} \in \mathbb{Z}[\vartheta]^{n\times n}$ and $\det\left(K_{\tilde{\Psi}}\right) K_{\tilde{\Psi}}^{-1} = \det\left(K_{\tilde{\Psi}}\right)\left(\det\left(K_{\tilde{\Psi}}\right)\right)^{-1}\underbrace{\operatorname{adj}\left(K_{\tilde{\Psi}}\right)}_{\in\mathbb{Z}^{n\times n}}$, cf. Remark 44, we see that the describing matrix of k is an element of $\mathbb{Z}[\vartheta]^{n\times n}$.

So we can consider the commutative diagram of the $\mathbb{Z}[\vartheta]$-linear embeddings with respect to the bases as explained above

(6)



Note that all occurring modules in diagram (6) are finitely generated free $\mathbb{Z}$-modules.

By Remark 50 we have

$$\det_{\mathbb{Z}}(h\circ g) \;=\; \det_{\mathbb{Z}}(\iota) \;=\; \pm p^{\frac{n(n+1)}{2}}\quad .$$

Since $\det_{\mathbb{Z}}(h\circ g) = \det_{\mathbb{Z}}(h)\det_{\mathbb{Z}}(g)$, we therefore get that

$$\left.\begin{aligned} \det_{\mathbb{Z}}(h)\det_{\mathbb{Z}}(g) \;&=\; \pm p^{\frac{n(n+1)}{2}} \\ \text{and hence}\quad |\det_{\mathbb{Z}}(h)| &\text{ is a power of } p\,. \end{aligned}\right\} \tag{7}$$

We further calculate

$$\left.\begin{aligned} \det_{\mathbb{Z}}(k) \;&\overset{(8)}{=}\; \pm\,\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}\left(\det\left(\det\left(K_{\tilde{\Psi}}\right)K_{\tilde{\Psi}}^{-1}\vartheta^n D_{\tilde{\Psi}}^{-1}\right)\right) \\ &=\; \pm\,\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}\Big(\underbrace{\det\left(K_{\tilde{\Psi}}\right)^n\det\left(K_{\tilde{\Psi}}^{-1}\right)}_{=\det\left(K_{\tilde{\Psi}}\right)^{n-1}\in\mathbb{Z}}\det\left(\vartheta^n D_{\tilde{\Psi}}^{-1}\right)\Big) \\ &=\; \pm\det\left(K_{\tilde{\Psi}}\right)^{(n-1)n}\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}\left(\det\left(\vartheta^n D_{\tilde{\Psi}}^{-1}\right)\right) \\ &\overset{\text{R.44}}{=}\; \pm\det\left(K_{\tilde{\Psi}}\right)^{(n-1)n}\mathrm{N}_{\mathbb{Q}(\vartheta)|\mathbb{Q}}\left(\vartheta^1\cdots\vartheta^n\right) \\ &\overset{\substack{\text{L.24}\\ (iv)}}{=}\; \pm\det\left(K_{\tilde{\Psi}}\right)^{(n-1)n}\cdot p^1\cdots p^n \;=\; \pm\det\left(K_{\tilde{\Psi}}\right)^{(n-1)n}\cdot p^{\frac{n(n+1)}{2}}\,, \end{aligned}\right\} \tag{9}$$

where in (8) we refer to Lemma 116 applied to the case

$$(K, s, A, B, r, \mathcal{O}_K\,, \varphi, F) \;=\; \left(\mathbb{Q}(\vartheta),\, n,\, \tilde{\Psi}',\, \det\left(K_{\tilde{\Psi}}\right)^{-1}\mathbb{Z}[\vartheta]^{\times n},\, n,\, \mathbb{Z}[\vartheta],\, k,\, \det\left(K_{\tilde{\Psi}}\right)K_{\tilde{\Psi}}^{-1}\vartheta^n D_{\tilde{\Psi}}^{-1}\right),$$

and recall that $\mathbb{Z}[\vartheta] \overset{\text{L.22}}{=} \mathcal{O}_{\mathbb{Q}(\vartheta)}$.

The matrix $K_{\tilde{\Psi}}$ is a lower triangular matrix with the diagonal entries $(2i)!$ for $i\in[1,n]$; cf. Remark 44 and Definition 34. Hence $\det\left(K_{\tilde{\Psi}}\right) \;=\; \prod_{i=1}^{n}(2i)!$. Since $2i \le 2n < p$ for $i\in[1,n]$, we get

$$p \nmid \det\left(K_{\tilde{\Psi}}\right)\,. \tag{10}$$

By the commutativity in (6) we get

$$\det_{\mathbb{Z}}(j)\det_{\mathbb{Z}}(h) \;=\; \det_{\mathbb{Z}}(j\circ h) \;=\; \det_{\mathbb{Z}}(k\circ i) \;=\; \det_{\mathbb{Z}}(k)\det_{\mathbb{Z}}(i)\,. \tag{11}$$

Now it is our aim to show that

$$\det_{\mathbb{Z}}(g) \overset{!}{=} \pm 1\,.$$

Since $|\det_{\mathbb{Z}}(h)|$ is a power of p, in particular $\neq 0$,
we see that it suffices to show that

$$\det_{\mathbb{Z}}(h)\det_{\mathbb{Z}}(g) \overset{!}{|}\, \det_{\mathbb{Z}}(h)\,.$$

Now $|\det_{\mathbb{Z}}(h)\det_{\mathbb{Z}}(g)|$ is a power of p, cf. (7), and
$\det_{\mathbb{Z}}(j)$ as a power of $\det\left(K_{\tilde{\Psi}}\right)$ is coprime to p,
cf. (10). So it suffices to show that

$$\det_{\mathbb{Z}}(h)\det_{\mathbb{Z}}(g) \overset{!}{|}\, \det_{\mathbb{Z}}(h)\det_{\mathbb{Z}}(j) \overset{(11)}{=} \det_{\mathbb{Z}}(k)\det_{\mathbb{Z}}(i)\,.$$

This is certainly satisfied if $\det_{\mathbb{Z}}(h)\det_{\mathbb{Z}}(g)$
already divides the factor $\det_{\mathbb{Z}}(k)$ in the product
$\det_{\mathbb{Z}}(k)\det_{\mathbb{Z}}(i)$. So it remains to show that

$$\det_{\mathbb{Z}}(h)\det_{\mathbb{Z}}(g) \overset{!}{|}\, \det_{\mathbb{Z}}(k)\,.$$

And this is true, cf. (7) and (9).

So we have reached our aim to show that $\det_{\mathbb{Z}}(g) = \pm 1$, whence $\theta\Psi = \tilde{\Psi}$. □

2.2.4 The local basis can not be used globally

In the previous Proposition 52 we have provided a description of the principal ideal $\theta_p \cdot {}_p\Psi$ as $\theta_p \cdot {}_p\Psi \;=\; {}_p\tilde{\Psi}$, where ${}_p\tilde{\Psi}$ is defined as a submodule of $\mathbb{Z}[\vartheta_p]^{\times n}$ via ties.

We have seen in Lemma 47 that, if we localize the $\mathbb{Z}$-module ${}_p\tilde{\Psi}$ at (p), we obtain the $\mathbb{Z}_{(p)}[\vartheta_p]$-linear basis $\mathrm{B}_{{}_p\tilde{\Psi}_{(p)}}$ of ${}_p\tilde{\Psi}_{(p)} \;=\; (\theta_p \cdot {}_p\Psi)_{(p)}$. By Remark 143 we get that $\mathrm{B}_{{}_p\tilde{\Psi}_{(p)}}$ is already contained in $\mathbb{Z}[\vartheta_p]^{\times n}$.
By Remark 50 we have the rather complicated $\mathbb{Z}[\vartheta_p]$-linear basis $\mathrm{B}_{\theta_p\cdot {}_p\Psi}$ of $\theta_p \cdot {}_p\Psi$, involving σ_i for $i \in [1,n]$.
So one might ask whether $\mathrm{B}_{{}_p\tilde{\Psi}_{(p)}}$ is already a $\mathbb{Z}[\vartheta_p]$-linear basis of $\theta_p \cdot {}_p\Psi$. But this is false for $p \in \mathbb{Z}_{\geq 5}$.

We show this exemplarily in the case $p = 11$.

The known $\mathbb{Z}[\vartheta_{11}]$-linear basis of the submodule $\theta_{11} \cdot {}_{11}\Psi$ of $\mathbb{Z}[\vartheta_{11}]^{\times 5}$ is given by

$$\mathrm{B}_{\theta_{11}\cdot {}_{11}\Psi} \;=\; \begin{pmatrix} (\,\sigma_5(\vartheta_{11}), & \sigma_4(\vartheta_{11}), & \sigma_3(\vartheta_{11}), & \sigma_2(\vartheta_{11}), & \sigma_1(\vartheta_{11}))\,, \\ \vartheta_{11}^1\cdot(\,0, & \sigma_4(\vartheta_{11}), & 3\cdot\sigma_3(\vartheta_{11}), & 6\cdot\sigma_2(\vartheta_{11}), & 10\cdot\sigma_1(\vartheta_{11}))\,, \\ \vartheta_{11}^2\cdot(\,0, & 0, & \sigma_3(\vartheta_{11}), & 5\cdot\sigma_2(\vartheta_{11}), & 15\cdot\sigma_1(\vartheta_{11}))\,, \\ \vartheta_{11}^3\cdot(\,0, & 0, & 0, & \sigma_2(\vartheta_{11}), & 7\cdot\sigma_1(\vartheta_{11}))\,, \\ \vartheta_{11}^4\cdot(\,0, & 0, & 0, & 0, & \sigma_1(\vartheta_{11}))\end{pmatrix},$$

cf. Example 51.

Therefore we obtain the principal ideal of the $\mathbb{Z}[\vartheta_{11}]$-linear determinant of the canonical embedding

$$\left.\begin{array}{rl} & \det_{\mathbb{Z}[\vartheta_{11}]}\big(\theta_{11}\cdot{}_{11}\Psi \hookrightarrow \mathbb{Z}[\vartheta_{11}]^{\times 5}\big)\mathbb{Z}[\vartheta_{11}] \;=\; \det_{\mathbb{Z}[\vartheta_{11}]}\big(\langle \mathrm{B}_{\theta_{11}\cdot{}_{11}\Psi}\rangle_{\mathbb{Z}[\vartheta_{11}]} \hookrightarrow \mathbb{Z}[\vartheta_{11}]^{\times 5}\big)\mathbb{Z}[\vartheta_{11}] \\ = & \left(\prod_{s=1}^{5}\big(\vartheta_{11}^{s-1}\cdot\sigma_{5-s+1}(\vartheta_{11})\big)\right)\mathbb{Z}[\vartheta_{11}] \;=\; \left(\prod_{s=1}^{5}\vartheta_{11}^{s-1}\right)\mathbb{Z}[\vartheta_{11}]\cdot\left(\prod_{s=1}^{5}\sigma_{5-s+1}(\vartheta_{11})\right)\mathbb{Z}[\vartheta_{11}] \\ = & \vartheta_{11}^{10}\mathbb{Z}[\vartheta_{11}]\cdot \mathrm{N}_{\mathbb{Q}(\vartheta_{11})|\mathbb{Q}}(\vartheta_{11})\mathbb{Z}[\vartheta_{11}] \overset{\text{L.24}}{\underset{(iv)}{=}} \vartheta_{11}^{10}\mathbb{Z}[\vartheta_{11}]\cdot 11\mathbb{Z}[\vartheta_{11}] \\ \overset{\text{L.29}}{=} & 11^2\mathbb{Z}[\vartheta_{11}]\cdot 11\mathbb{Z}[\vartheta_{11}] \;=\; 11^3\mathbb{Z}[\vartheta_{11}]\,. \end{array}\right\} (1)$$

We recall from Example 48 that

$$\mathrm{B}_{{}_{11}\tilde{\Psi}_{(11)}} = \begin{pmatrix} \vartheta_{11}^1\cdot(1, & 9, & 25, & 49, & 81), \\ \vartheta_{11}^2\cdot(0, & 3, & 25, & 98, & 270), \\ \vartheta_{11}^3\cdot(0, & 0, & 5, & 49, & 243), \\ \vartheta_{11}^4\cdot(0, & 0, & 0, & 7, & 81), \\ \vartheta_{11}^5\cdot(0, & 0, & 0, & 0, & 9) \end{pmatrix},$$

which is contained in $\mathbb{Z}[\vartheta_{11}]^{\times 5}$.

Therefore we obtain the principal ideal of the $\mathbb{Z}[\vartheta_{11}]$-linear determinant of the canonical embedding

$$\left.\begin{array}{rl} & \det_{\mathbb{Z}[\vartheta_{11}]}\left(\langle \mathrm{B}_{{}_{11}\tilde{\Psi}_{(11)}}\rangle_{\mathbb{Z}[\vartheta_{11}]} \hookrightarrow \mathbb{Z}[\vartheta_{11}]^{\times 5}\right)\mathbb{Z}[\vartheta_{11}] \\ = & \left(\prod_{s=1}^{5}\big((2s-1)\cdot\vartheta_{11}^{s}\big)\right)\mathbb{Z}[\vartheta_{11}] \;=\; (1\cdot 3\cdot 5\cdot 7\cdot 9)\mathbb{Z}[\vartheta_{11}]\cdot\vartheta_{11}^{15}\mathbb{Z}[\vartheta_{11}] \\ \overset{\text{L.29}}{=} & (1\cdot 3\cdot 5\cdot 7\cdot 9)\mathbb{Z}[\vartheta_{11}]\cdot 11^3\mathbb{Z}[\vartheta_{11}] \;=\; (1\cdot 3\cdot 5\cdot 7\cdot 9\cdot 11^3)\mathbb{Z}[\vartheta_{11}]\,. \end{array}\right\} (2)$$

We see that the ideals differ by the factor $1\cdot 3\cdot 5\cdot 7\cdot 9$, which is not a unit in $\mathbb{Z}[\vartheta_{11}]$. Therefore $\mathrm{B}_{{}_{11}\tilde{\Psi}_{(11)}}$ can not be a $\mathbb{Z}[\vartheta_{11}]$-linear basis of $\theta_{11}\cdot{}_{11}\Psi$, whence $\langle \mathrm{B}_{{}_{11}\tilde{\Psi}_{(11)}}\rangle_{\mathbb{Z}[\vartheta_{11}]} \neq \langle \mathrm{B}_{\theta_{11}\cdot{}_{11}\Psi}\rangle_{\mathbb{Z}[\vartheta_{11}]} = \theta_{11}\cdot{}_{11}\Psi$.

In the case of an arbitrary prime $p\in\mathbb{Z}_{\geq 5}$ we have the factor $\prod_{s=1}^{n}(2s-1)$ by which the ideals differ. Also this factor is not a unit in $\mathbb{Z}[\vartheta_p]$ and $\langle \mathrm{B}_{{}_{p}\tilde{\Psi}_{(p)}}\rangle_{\mathbb{Z}[\vartheta_p]} \neq \langle \mathrm{B}_{\theta_p\cdot{}_{p}\Psi}\rangle_{\mathbb{Z}[\vartheta_p]} = \theta_p\cdot{}_{p}\Psi$.

Locally, we of course have $\langle \mathrm{B}_{{}_{p}\tilde{\Psi}_{(p)}}\rangle_{\mathbb{Z}_{(p)}[\vartheta_p]} = (\theta_p\cdot{}_{p}\Psi)_{(p)} = \langle \mathrm{B}_{\theta_p\cdot{}_{p}\Psi}\rangle_{\mathbb{Z}_{(p)}[\vartheta_p]}$; cf. Lemma 47 and Remark 50.

But at least we get the following

Corollary 53 *We have*

$$\langle \mathrm{B}_{{}_{p}\tilde{\Psi}_{(p)}}\rangle_{\mathbb{Z}[\vartheta_p]} \subseteq \langle \mathrm{B}_{\theta_p\cdot{}_{p}\Psi}\rangle_{\mathbb{Z}[\vartheta_p]}\,.$$

Moreover, this is a proper inclusion for $p\in\mathbb{Z}_{\geq 5}$.

Proof. By Remark 50 we have $d := \det_{\mathbb{Z}}(\theta\Psi \hookrightarrow \mathbb{Z}[\vartheta]^{\times n}) = \pm p^{\frac{n(n+1)}{2}}$. Moreover, we have

$$d\cdot\mathbb{Z}[\vartheta]^{\times n} \subseteq \theta\Psi \subseteq \mathbb{Z}[\vartheta]^{\times n}\,.$$

So we can apply Lemma 128 to the case $(R, \pi, \alpha, M, N) = \left(\mathbb{Z},\, p,\, \frac{n(n+1)}{2},\, \mathbb{Z}[\vartheta]^{\times n},\, \theta\Psi\right)$ and get

$$(\theta\Psi)_{(p)} \cap \mathbb{Z}[\vartheta]^{\times n} = \theta\Psi\,. \tag{1}$$

We have

$$\langle \mathrm{B}_{\tilde{\Psi}_{(p)}} \rangle_{\mathbb{Z}[\vartheta]} \overset{\text{L.47}}{\underset{\downarrow}{\subseteq}} \tilde{\Psi}_{(p)} \overset{\text{P.52}}{=} (\theta\Psi)_{(p)}\,.$$

We have that $\mathrm{B}_{\tilde{\Psi}_{(p)}}$ is contained in $\mathbb{Z}[\vartheta]^{\times n}$; cf. Lemma 47 and Remark 143.

Altogether, we obtain

$$\langle \mathrm{B}_{\tilde{\Psi}_{(p)}} \rangle_{\mathbb{Z}[\vartheta]} \subseteq (\theta\Psi)_{(p)} \cap \mathbb{Z}[\vartheta]^{\times n} \overset{(1)}{=} \theta\Psi \overset{\text{R.50}}{=} \langle \mathrm{B}_{\theta\Psi} \rangle_{\mathbb{Z}[\vartheta]}\,.$$

Properness of the inclusion for $p \in \mathbb{Z}_{\geq 5}$ is a consequence of the inequality shown above by means of determinants. □

Chapter 3

Wedderburn

3.1 The dihedral group

Definition 54 For $m \in \mathbb{Z}_{\geq 1}$ we define the *dihedral group* via generators and relations as

$$\mathrm{D}_{2m} := \left\langle x, y : x^m, y^2, (yx)^2 \right\rangle,$$

cf. [Dummit 04, Sec. 1.2, p. 26, item (1.1)].

Remark 55 *The dihedral group, given in* Definition 54*, has the non-redundant list of elements*

$$\mathrm{D}_{2m} = \left\{ 1, x^1, x^2, \ldots, x^{m-1}, y, xy, x^2y, \ldots, x^{m-1}y \right\}.$$

In particular, the dihedral group D_{2m} *has order* $2m$*.*

Proof. We refer to [Dummit 04, Sec. 1.2, pp. 24-26]. □

3.2 Wedderburn over $\mathbb{C}$

Definition 56 For $i \in [1, n]$ we define

$$M_i := \begin{pmatrix} 1 & 1 \\ \zeta_p^i + \zeta_p^{-i} - 2 & \zeta_p^i + \zeta_p^{-i} - 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}[\vartheta_p]),$$

$$N_i := \begin{pmatrix} 1 & 0 \\ \zeta_p^i + \zeta_p^{-i} - 2 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}[\vartheta_p]),$$

$$A_i := \begin{pmatrix} 1 - \zeta_p^{-i} & 1 \\ \zeta_p^i - 1 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}),$$

cf. Definition 17 and Corollary 21.

In particular,

$$M_1 = \begin{pmatrix} 1 & 1 \\ \vartheta_p & \vartheta_p + 1 \end{pmatrix} \quad \text{and} \quad N_1 = \begin{pmatrix} 1 & 0 \\ \vartheta_p & -1 \end{pmatrix}.$$

Remark 57 *For the matrices, given in* Definition 56*, the following holds:*

(i) For $i \in [1, n]$ *we have*

$$A_i M_i A_i^{-1} = \begin{pmatrix} \zeta_p^i & 0 \\ 0 & \zeta_p^{-i} \end{pmatrix},$$

$$A_i N_i A_i^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

(ii) For $i \in [1, n]$ *we have*

$$M_i^p = N_i^2 = (N_i \cdot M_i)^2 = \mathrm{E}_2.$$

(iii) We have

$$M_1^{-1} = \begin{pmatrix} \vartheta_p + 1 & -1 \\ -\vartheta_p & 1 \end{pmatrix} \quad \textit{and} \quad A_1^{-1} = \frac{1}{\zeta_p^{-1} - \zeta_p} \begin{pmatrix} -1 & -1 \\ 1 - \zeta_p & 1 - \zeta_p^{-1} \end{pmatrix}.$$

(iv) For $k \in \mathbb{Z}_{\geq 0}$ *we have*

$$M_1^k (\mathrm{E}_2 + N_1) = \begin{pmatrix} \zeta_p^k + \zeta_p^{-k} & 0 \\ \zeta_p^{k+1} - \zeta_p^k + \zeta_p^{-(k+1)} - \zeta_p^{-k} & 0 \end{pmatrix}.$$

Proof of *(i)*. We have

$$A_i M_i = \begin{pmatrix} 1 - \zeta^{-i} & 1 \\ \zeta^i - 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \zeta^i + \zeta^{-i} - 2 & \zeta^i + \zeta^{-i} - 1 \end{pmatrix} = \begin{pmatrix} \zeta^i - 1 & \zeta^i \\ 1 - \zeta^{-i} & -\zeta^{-i} \end{pmatrix}$$

$$\| \quad \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix} A_i = \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix} \begin{pmatrix} 1 - \zeta^{-i} & 1 \\ \zeta^i - 1 & -1 \end{pmatrix} = \begin{pmatrix} \zeta^i - 1 & \zeta^i \\ 1 - \zeta^{-i} & -\zeta^{-i} \end{pmatrix},$$

and

$$A_i N_i = \begin{pmatrix} 1 - \zeta^{-i} & 1 \\ \zeta^i - 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \zeta^i + \zeta^{-i} - 2 & -1 \end{pmatrix} = \begin{pmatrix} \zeta^i - 1 & -1 \\ 1 - \zeta^{-i} & 1 \end{pmatrix}$$

$$\| \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 - \zeta^{-i} & 1 \\ \zeta^i - 1 & -1 \end{pmatrix} = \begin{pmatrix} \zeta^i - 1 & -1 \\ 1 - \zeta^{-i} & 1 \end{pmatrix}.$$

Proof of *(ii)*. This follows from *(i)*.

Proof of *(iii)*. This is shown by multiplication of the respective matrices.

Proof of *(iv)*. For $k \in \mathbb{Z}_{\geq 0}$ we have

$$M_1^k(\mathrm{E}_2 + N_1) \overset{(i)}{=} \left(A_1^{-1}\begin{pmatrix} \zeta^1 & 0 \\ 0 & \zeta^{-1} \end{pmatrix} A_1\right)^k (\mathrm{E}_2 + N_1) \;=\; A_1^{-1}\begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix} A_1(\mathrm{E}_2 + N_1)$$

$$\overset{(iii)}{=} \frac{1}{\zeta^{-1}-\zeta}\begin{pmatrix} -1 & -1 \\ 1-\zeta & 1-\zeta^{-1} \end{pmatrix}\begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix}\begin{pmatrix} 1-\zeta^{-1} & 1 \\ \zeta-1 & -1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ \zeta+\zeta^{-1}-2 & 0 \end{pmatrix}$$

$$= \frac{1}{\zeta^{-1}-\zeta}\begin{pmatrix} -\zeta^k & -\zeta^{-k} \\ \zeta^k-\zeta^{k+1} & \zeta^{-k}-\zeta^{-(k+1)} \end{pmatrix}\begin{pmatrix} \zeta-\zeta^{-1} & 0 \\ \zeta-\zeta^{-1} & 0 \end{pmatrix}$$

$$= \begin{pmatrix} -\zeta^k & -\zeta^{-k} \\ \zeta^k-\zeta^{k+1} & \zeta^{-k}-\zeta^{-(k+1)} \end{pmatrix}\begin{pmatrix} -1 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \zeta^k+\zeta^{-k} & 0 \\ \zeta^{k+1}-\zeta^k+\zeta^{-(k+1)}-\zeta^{-k} & 0 \end{pmatrix}.$$

□

Lemma 58 *We have the representations of the dihedral group* D_{2p}

(1)
$$\begin{aligned} \varrho_{\mathfrak{t}} \;:\; \mathrm{D}_{2p} &\longrightarrow \mathrm{GL}_1(\mathbb{C}) \\ x &\longmapsto 1\,, \\ y &\longmapsto 1\,, \end{aligned}$$

(2)
$$\begin{aligned} \varrho_{\mathfrak{a}} \;:\; \mathrm{D}_{2p} &\longrightarrow \mathrm{GL}_1(\mathbb{C}) \\ x &\longmapsto 1\,, \\ y &\longmapsto -1\,, \end{aligned}$$

and,

(3) *for* $i \in [1,n]$,
$$\begin{aligned} \varrho_i \;:\; \mathrm{D}_{2p} &\longrightarrow \mathrm{GL}_2(\mathbb{C}) \\ x &\longmapsto M_i\,, \\ y &\longmapsto N_i\,. \end{aligned}$$

A. Zimmermann has made use of the representing matrices M_1 and $-N_1$ in (3); cf. [Zimmermann 92, Abschnitt 3.9, pp. 60-63] and note that our $(\mathrm{D}_{2p}, x, y, {}_j\gamma_p)$ is denoted by $(\mathrm{D}_p, a, b, \eta_j(p))$ in his work.

We denote the characters of these representations by $\chi_{\varrho_{\mathfrak{t}}}$, $\chi_{\varrho_{\mathfrak{a}}}$ and χ_{ϱ_i} for $i \in [1,n]$, respectively.

Proof.
The relations required by Definition 54 have to be verified. For (3), they follow by Remark 57 *(ii)*. □

Remark 59 *Let* x *and* y *denote the generators of* D_{2p} *given in* Definition 54.

Then we have for $i \in [1,n]$ *and* $j \in [0, p-1]$

$$\chi_{\varrho_i}(x^j) \;=\; \zeta_p^{ji} + \zeta_p^{-ji} \qquad \textit{and} \qquad \chi_{\varrho_i}(x^j y) \;=\; 0\,,$$

cf. Lemma 58.

Proof. For $i \in [1,n]$ and $j \in [0,p-1]$ we have

$$\chi_{\varrho_i}\big(x^j\big) \;=\; \mathrm{tr}\big(\varrho_i\big(x^j\big)\big) \overset{\text{L.58}}{\underset{(3)}{=}} \mathrm{tr}\big(M_i^j\big) \overset{\text{R.57}}{\underset{(i)}{=}} \mathrm{tr}\left(\begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix}^j\right) = \zeta^{ji} + \zeta^{-ji}\,,$$

and

$$\chi_{\varrho_i}\big(x^j y\big) \;=\; \mathrm{tr}\big(\varrho_i\big(x^j y\big)\big) \overset{\text{L.58}}{\underset{(3)}{=}} \mathrm{tr}\big(M_i^j N_i\big) \overset{\text{R.57}}{\underset{(i)}{=}} \mathrm{tr}\left(\begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix}^j \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = \mathrm{tr}\left(\begin{pmatrix} 0 & \zeta^{ji} \\ \zeta^{-ji} & 0 \end{pmatrix}\right) = 0\,.$$

□

Lemma 60 *The characters of the representations given in* Lemma 58 *are irreducible.*

Proof. We only have to consider χ_{ϱ_i} for $i \in [1,n]$. Let x and y denote the generators of D_{2p} given in Definition 54. Then we have

$$\begin{aligned} 2p \cdot \underbrace{{}_{\mathrm{D}_{2p}}(\chi_{\varrho_i}, \chi_{\varrho_i})}_{\text{cf. C.8}} &= \sum_{d \in \mathrm{D}_{2p}} |\chi_{\varrho_i}(d)|^2 \overset{\text{R.55}}{\underset{\text{R.59}}{=}} \sum_{j=0}^{p-1} \big|\underbrace{\zeta^{ji} + \zeta^{-ji}}_{\in \mathbb{R}}\big|^2 = \sum_{j=0}^{p-1} \big(\zeta^{ji} + \zeta^{-ji}\big)^2 \\ &= \sum_{j=0}^{p-1} \zeta^{2ji} + 2\underbrace{\zeta^{ji}\zeta^{-ji}}_{=1} + \zeta^{-2ji} = 2p + \sum_{j=0}^{p-1} \big(\underbrace{\zeta^{2i}}_{\substack{\text{primitive } p\text{-th} \\ \text{roots of unity} \\ \text{since } 2i \not\equiv_p 0}}\big)^j + \big(\underbrace{\zeta^{-2i}}_{\text{''}}\big)^j = 2p\,, \end{aligned}$$

Therefore we have ${}_{\mathrm{D}_{2p}}(\chi_{\varrho_i}, \chi_{\varrho_i}) = 1$. □

Lemma 61 *The characters of the representations given in* Lemma 58 *are pairwise distinct.*

Proof. We only have to show that

$$\chi_{\varrho_k} \overset{!}{\neq} \chi_{\varrho_l} \quad \text{for } k,l \in [1,n] \text{ with } k \neq l.$$

For $k,l \in [1,n]$ with $k \neq l$ we have

$$\begin{array}{lllllll} \chi_{\varrho_k}(x) & = & \mathrm{tr}(\varrho_k(x)) & = & \mathrm{tr}(M_k) & \overset{\text{D.56}}{=} & \zeta^k + \zeta^{-k} \;=\; {}_k\gamma \\ \chi_{\varrho_l}(x) & = & \mathrm{tr}(\varrho_l(x)) & = & \mathrm{tr}(M_l) & \overset{\text{D.56}}{=} & \zeta^l + \zeta^{-l} \;=\; {}_l\gamma\,. \end{array} \qquad \not\parallel \text{ C.21}$$

□

Proposition 62 *We have the Wedderburn isomorphism of the semisimple* $\mathbb{C}$*-algebra* $\mathbb{C}\mathrm{D}_{2p}$

$$\begin{array}{rcccccl} \omega_{\mathbb{C}} \;:\; \mathbb{C}\mathrm{D}_{2p} & \xrightarrow{\sim} & \mathbb{C} & \times & \big(\mathbb{C}^{2\times 2}\big)^{\times n} & \times & \mathbb{C} \\ x & \longmapsto & (\,1 & , & (M_{n-i+1})_{i\in[1,n]} & , & 1\,) \\ y & \longmapsto & (\,1 & , & (N_{n-i+1})_{i\in[1,n]} & , & -1\,) \end{array} \begin{array}{l} = \;(\,\varrho_{\mathrm{t}}(x)\;,\;(\varrho_{n-i+1}(x))_{i\in[1,n]}\;,\;\varrho_{\mathrm{a}}(x)\,)\,, \\ = \;(\,\varrho_{\mathrm{t}}(y)\;,\;(\varrho_{n-i+1}(y))_{i\in[1,n]}\;,\;\varrho_{\mathrm{a}}(y)\,)\,, \end{array}$$

cf. Lemma 58.

Proof. The representations ϱ_{t}, ϱ_{a} and ϱ_i for $i \in [1,n]$ of D_{2p} over $\mathbb{C}$ are irreducible; cf. Lemma 60. Moreover, they are pairwise distinct; cf. Lemma 61.

Thus the Artin-Wedderburn theorem yields that there exists an isomorphism

$$(1) \qquad \mathbb{C}\mathrm{D}_{2p} \xrightarrow{\sim} \mathbb{C} \times \left(\mathbb{C}^{2\times 2}\right)^{\times n} \times \mathbb{C} \times \prod_{s=1}^{m} \mathbb{C}^{n_s \times n_s} \text{ , where } m \in \mathbb{Z}_{\geq 0} \text{ and } n_s \in \mathbb{Z}_{\geq 1} \text{ for } s \in [1,m] \text{ ,}$$

projecting to the $\mathbb{C}$-algebra morphism $\omega_{\mathbb{C}}$ on the first $n+2$ components of the cartesian product.

Considering the $\mathbb{C}$-dimensions in (1) we get by Remark 55

$$2p = 1^2 + 2^2 \cdot n + 1^2 + \sum_{s=1}^{m} n_s^2 = 2 + 4 \cdot \frac{p-1}{2} + \sum_{s=1}^{m} n_s^2 = 2p + \sum_{s=1}^{m} n_s^2 \,.$$

It follows that m has to be zero. □

3.3 Wedderburn over $\mathbb{Q}(\vartheta_p)$

Proposition 63 *We have the Wedderburn isomorphism of the semisimple $\mathbb{Q}(\vartheta_p)$-algebra $\mathbb{Q}(\vartheta_p)\mathrm{D}_{2p}$*

$$\begin{array}{rccccccc} \omega_{\mathbb{Q}(\vartheta_p)} & : & \mathbb{Q}(\vartheta_p)\mathrm{D}_{2p} & \xrightarrow{\sim} & \mathbb{Q}(\vartheta_p) & \times & \left(\mathbb{Q}(\vartheta_p)^{2\times 2}\right)^{\times n} & \times \mathbb{Q}(\vartheta_p) \\ & & x & \longmapsto & (1 & , & (M_{n-i+1})_{i\in[1,n]} & , \quad 1)\,, \\ & & y & \longmapsto & (1 & , & (N_{n-i+1})_{i\in[1,n]} & , -1)\,. \end{array}$$

Proof. We consider the Wedderburn isomorphism $\omega_{\mathbb{C}}$ of Proposition 62.

We restrict the domain of $\omega_{\mathbb{C}}$ from $\mathbb{C}\mathrm{D}_{2p}$ to $\mathbb{Q}(\vartheta)\mathrm{D}_{2p}$. Further, since $M_i, N_i \in \mathbb{Z}[\vartheta]^{2\times 2} \subseteq \mathbb{Q}(\vartheta)^{2\times 2}$ for $i \in [1,n]$, cf. Definition 56, we can restrict the codomain of $\omega_{\mathbb{C}}|_{\mathbb{Q}(\vartheta)\mathrm{D}_{2p}}$ from $\mathbb{C} \times \left(\mathbb{C}^{2\times 2}\right)^{\times n} \times \mathbb{C}$ to $\mathbb{Q}(\vartheta) \times \left(\mathbb{Q}(\vartheta)^{2\times 2}\right)^{\times n} \times \mathbb{Q}(\vartheta)$.

So we can define $\omega_{\mathbb{Q}(\vartheta)} := \omega_{\mathbb{C}}\Big|^{\mathbb{Q}(\vartheta)\times\left(\mathbb{Q}(\vartheta)^{2\times 2}\right)^{\times n}\times\mathbb{Q}(\vartheta)}_{\mathbb{Q}(\vartheta)\mathrm{D}_{2p}}$, whence $\omega_{\mathbb{Q}(\vartheta)}$ is a morphism of $\mathbb{Q}(\vartheta)$-algebras.

Moreover we obtain the commutative diagram of rings

$$\begin{array}{ccc} \mathbb{C}\mathrm{D}_{2p} & \xrightarrow[\sim]{\omega_{\mathbb{C}}} & \mathbb{C} \times \left(\mathbb{C}^{2\times 2}\right)^{\times n} \times \mathbb{C} \\ \uparrow & \circlearrowright & \uparrow \\ \mathbb{Q}(\vartheta)\mathrm{D}_{2p} & \xrightarrow{\omega_{\mathbb{Q}(\vartheta)}} & \mathbb{Q}(\vartheta) \times \left(\mathbb{Q}(\vartheta)^{2\times 2}\right)^{\times n} \times \mathbb{Q}(\vartheta)\,. \end{array}$$

As a restriction of $\omega_{\mathbb{C}}$, the map $\omega_{\mathbb{Q}(\vartheta)}$ is injective. Comparing $\mathbb{Q}(\vartheta)$-dimensions, it is also surjective; cf. Remark 55. □

3.4 Wedderburn over $\mathbb{Q}$

Lemma 64 *We have the isomorphism of* $\mathbb{Q}(\vartheta_p)$*-algebras*

$$\begin{array}{rcccl} f & : & \mathbb{Q}(\vartheta_p) \underset{\mathbb{Q}}{\otimes} \mathbb{Q}\mathrm{D}_{2p} & \xrightarrow{\sim} & \mathbb{Q}(\vartheta_p)\mathrm{D}_{2p} \\ & & x \otimes \sum\limits_{d\in\mathrm{D}_{2p}} q_d d & \longmapsto & \sum\limits_{d\in\mathrm{D}_{2p}} x q_d d\,, \end{array}$$

cf. Convention 7.

Proof. We apply Lemma 99 to the case $(K, L, G, \varphi) = (\mathbb{Q}, \mathbb{Q}(\vartheta), \mathrm{D}_{2p}, \mathbb{Q} \hookrightarrow \mathbb{Q}(\vartheta))$. □

Lemma 65 *We have the isomorphism of* $\mathbb{Q}(\vartheta_p)$*-algebras*

$$\begin{array}{rcccl} h & : & \mathbb{Q}(\vartheta_p) \underset{\mathbb{Q}}{\otimes} \left(\mathbb{Q}(\vartheta_p)^{2\times 2}\right) & \xrightarrow{\sim} & \mathbb{Q}(\vartheta_p)^{2\times 2} \times \ldots \times \mathbb{Q}(\vartheta_p)^{2\times 2} \\ & & x \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \left(\begin{pmatrix} \sigma_n(a)x & \sigma_n(b)x \\ \sigma_n(c)x & \sigma_n(d)x \end{pmatrix}, \ \ldots\ , \begin{pmatrix} \sigma_1(a)x & \sigma_1(b)x \\ \sigma_1(c)x & \sigma_1(d)x \end{pmatrix} \right). \end{array}$$

Proof. We have

$$\mathbb{Q}(\vartheta) \underset{\mathbb{Q}}{\otimes} \left(\mathbb{Q}(\vartheta)^{2\times 2}\right) \xrightarrow[\sim]{(*)} \left(\mathbb{Q}(\vartheta) \underset{\mathbb{Q}}{\otimes} \mathbb{Q}(\vartheta)\right)^{2\times 2} \xrightarrow[\sim]{\text{L.33}} (\mathbb{Q}(\vartheta) \times \ldots \times \mathbb{Q}(\vartheta))^{2\times 2} = (\mathbb{Q}(\vartheta)^{\times n})^{2\times 2}$$

$$x \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} x\otimes a & x\otimes b \\ x\otimes c & x\otimes d \end{pmatrix} \longmapsto \begin{pmatrix} (\sigma_n(a)x, \ldots, \sigma_1(a)x) & (\sigma_n(b)x, \ldots, \sigma_1(b)x) \\ (\sigma_n(c)x, \ldots, \sigma_1(c)x) & (\sigma_n(d)x, \ldots, \sigma_1(d)x) \end{pmatrix}$$

$$\xrightarrow[\sim]{\text{L.102}} \mathbb{Q}(\vartheta)^{2\times 2} \times \ldots \times \mathbb{Q}(\vartheta)^{2\times 2}$$

$$\longmapsto \left(\begin{pmatrix} \sigma_n(a)x & \sigma_n(b)x \\ \sigma_n(c)x & \sigma_n(d)x \end{pmatrix}, \ \ldots\ , \begin{pmatrix} \sigma_1(a)x & \sigma_1(b)x \\ \sigma_1(c)x & \sigma_1(d)x \end{pmatrix} \right),$$

where in $(*)$ we refer to Lemma 98 applied to the case $(A, B, K, m) = (\mathbb{Q}(\vartheta), \mathbb{Q}(\vartheta), \mathbb{Q}, 2)$. □

Corollary 66 *We have the isomorphism of* $\mathbb{Q}(\vartheta_p)$*-algebras*

$$\begin{array}{rcccl} k & : & \mathbb{Q}(\vartheta_p) \underset{\mathbb{Q}}{\otimes} \mathbb{Q}\mathrm{D}_{2p} & \xrightarrow{\sim} & \mathbb{Q}(\vartheta_p) \underset{\mathbb{Q}}{\otimes} (\,\mathbb{Q} \times \mathbb{Q}(\vartheta_p)^{2\times 2} \times \mathbb{Q}\,) \\ & & q \otimes x & \longmapsto & q \otimes (1, M_1, 1)\,, \\ & & q \otimes y & \longmapsto & q \otimes (1, N_1, -1)\,. \end{array}$$

Proof. We have

$$\begin{array}{ccccccccc} \mathbb{Q}(\vartheta) \underset{\mathbb{Q}}{\otimes} \mathbb{Q}\mathrm{D}_{2p} & \xrightarrow[\sim]{\text{L.64}} & \mathbb{Q}(\vartheta)\mathrm{D}_{2p} & \xrightarrow[\omega_{\mathbb{Q}(\vartheta)}]{\text{P.63}} & \mathbb{Q}(\vartheta) & \times & \left(\mathbb{Q}(\vartheta)^{2\times 2}\right)^{\times n} & \times & \mathbb{Q}(\vartheta) \\ q \otimes x & \longmapsto & qx & \longmapsto & (q & , & q\cdot(M_{n-i+1})_{i\in[1,n]} & , & q) \\ q \otimes y & \longmapsto & qy & \longmapsto & (q & , & q\cdot(N_{n-i+1})_{i\in[1,n]} & , & -q) \end{array}$$

$$\begin{array}{lllllllllllll}
\xrightarrow[\sim]{(*)} & \mathbb{Q}(\vartheta)\underset{\mathbb{Q}}{\otimes}\mathbb{Q} & \times & \mathbb{Q}(\vartheta)\underset{\mathbb{Q}}{\otimes}\left(\mathbb{Q}(\vartheta)^{2\times 2}\right) & \times & \mathbb{Q}(\vartheta)\underset{\mathbb{Q}}{\otimes}\mathbb{Q} & \xleftarrow[\sim]{\text{L.96}} & \mathbb{Q}(\vartheta) & \underset{\mathbb{Q}}{\otimes} & (\,\mathbb{Q} & \times & \mathbb{Q}(\vartheta)^{2\times 2} & \times & \mathbb{Q}\,) \\
\longmapsto & (\,q\otimes 1 & , & q\otimes M_1 & , & q\otimes 1\,) & \longmapsto & q & \otimes & (\,1 & , & M_1 & , & 1\,) \\
\longmapsto & (\,q\otimes 1 & , & q\otimes N_1 & , & -q\otimes 1\,) & \longmapsto & q & \otimes & (\,1 & , & N_1 & , & -1\,),
\end{array}$$

where in $(*)$ in the middle component we refer to Lemma 65 and note that

$$h(q\otimes M_1) \overset{\text{D.56}}{=} h\left(q\otimes\begin{pmatrix}1 & 1\\ \zeta^1+\zeta^{-1}-2 & \zeta^1+\zeta^{-1}-1\end{pmatrix}\right)$$

$$\overset{\substack{\text{L.65}\\ \text{N.26}}}{=}\left(\begin{pmatrix}q & q\\ (\zeta^{n-i+1}+\zeta^{-(n-i+1)}-2)q & (\zeta^{n-i+1}+\zeta^{-(n-i+1)}-1)q\end{pmatrix}\right)_{i\in[1,n]} \overset{\text{D.56}}{=} q(M_{n-i+1})_{i\in[1,n]}\,.$$

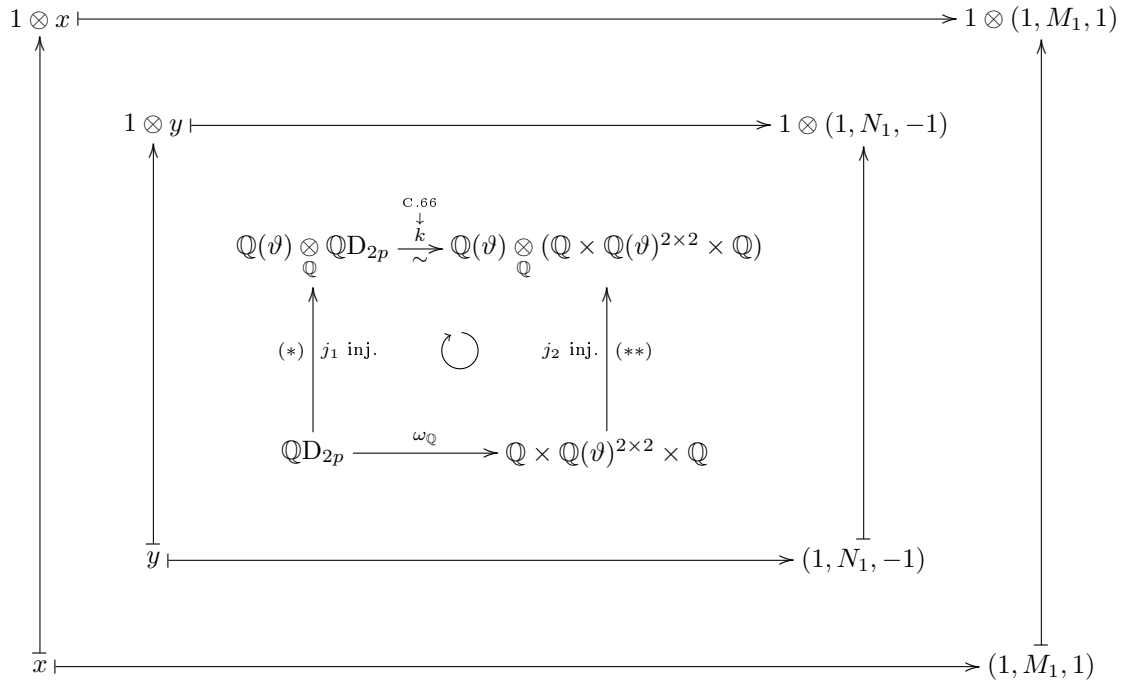
Similarly, we have $h(q\otimes N_1)=q(N_{n-i+1})_{i\in[1,n]}$. □

Proposition 67 *We have the Wedderburn isomorphism of the semisimple $\mathbb{Q}$-algebra $\mathbb{Q}\mathrm{D}_{2p}$*

$$\begin{array}{rcccccc}
\omega_{\mathbb{Q}} : \mathbb{Q}\mathrm{D}_{2p} & \xrightarrow{\sim} & \mathbb{Q} & \times & \mathbb{Q}(\vartheta_p)^{2\times 2} & \times & \mathbb{Q} \\
x & \longmapsto & (\,1 & , & M_1 & , & 1\,), \\
y & \longmapsto & (\,1 & , & N_1 & , & -1\,),
\end{array}$$

cf. Definition 56.

Proof. We have the commutative diagram

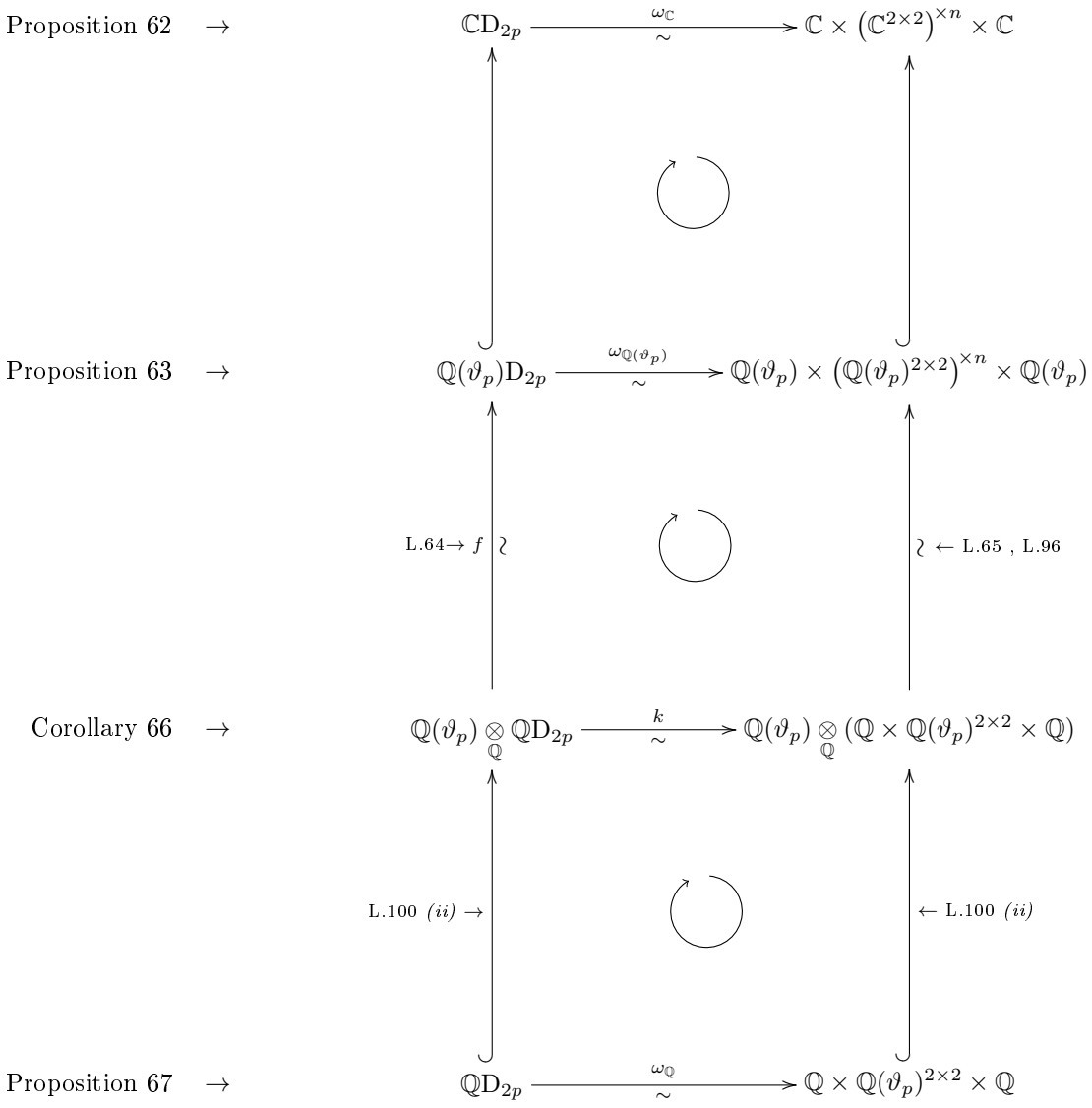


In $(*)$ and $(**)$ we refer to Lemma 100 *(ii)* applied to the case $(K,\,L,\,\varphi,\,V)=(\mathbb{Q},\,\mathbb{Q}(\vartheta),\,\mathbb{Q}\hookrightarrow\mathbb{Q}(\vartheta),\mathbb{Q}\mathrm{D}_{2p})$ and $(K,\,L,\,\varphi,V)=(\mathbb{Q},\,\mathbb{Q}(\vartheta),\,\mathbb{Q}\hookrightarrow\mathbb{Q}(\vartheta),\mathbb{Q}\times\mathbb{Q}(\vartheta)^{2\times 2}\times\mathbb{Q})$, respectively.

Therefore $\omega_{\mathbb{Q}}$ is an injective morphism of $\mathbb{Q}$-algebras. Comparing $\mathbb{Q}$-dimensions, it is also surjective; cf. Lemma 24 *(i2)* and Remark 55. □

3.5 Summary of Wedderburn

In summary, we obtain the following commutative diagram



Chapter 4

Group rings of D_{2p}

4.1 The integral group ring $\mathbb{Z}\mathrm{D}_{2p}$

Notation 68 Recall that $p \in \mathbb{Z}_{\geq 3}$ is a prime. Denote:

$$\Gamma \;=\; {}_p\Gamma \;:=\; \mathbb{Z} \times \mathbb{Z}[\vartheta_p]^{2\times 2} \times \mathbb{Z}\,,$$

$$\Lambda \;=\; {}_p\Lambda \;:=\; \left\{ (\,a\,, \begin{pmatrix} b & c \\ d & e \end{pmatrix}, f\,) \in \mathbb{Z} \times \mathbb{Z}[\vartheta_p]^{2\times 2} \times \mathbb{Z} \,:\, a \equiv_{\vartheta_p} b\,,\, d \equiv_{\vartheta_p} 0\,,\, e \equiv_{\vartheta_p} f\,,\, a \equiv_2 f \right\} \;\subseteq\; {}_p\Gamma.$$

Remark 69

(i) The additive subgroup ${}_p\Lambda$ of ${}_p\Gamma$ is a subring.

(ii) Let

$$G_{\mathrm{b}} \;:=\; \left((0, \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}, 0)\right) \quad \bigsqcup \left((0, \begin{pmatrix} \vartheta_p^i & 0 \\ 0 & 0 \end{pmatrix}, 0) : i \in [1, n-1]\right),$$

$$G_{\mathrm{c}} \;:=\; \left((0, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, 0)\right) \quad \bigsqcup \left((0, \begin{pmatrix} 0 & \vartheta_p^i \\ 0 & 0 \end{pmatrix}, 0) : i \in [1, n-1]\right),$$

$$G_{\mathrm{d}} \;:=\; \left((0, \begin{pmatrix} 0 & 0 \\ p & 0 \end{pmatrix}, 0)\right) \quad \bigsqcup \left((0, \begin{pmatrix} 0 & 0 \\ \vartheta_p^i & 0 \end{pmatrix}, 0) : i \in [1, n-1]\right),$$

$$G_{\mathrm{e}} \;:=\; \left((0, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 1-p)\right) \bigsqcup \left((0, \begin{pmatrix} 0 & 0 \\ 0 & \vartheta_p^i \end{pmatrix}, 0) : i \in [1, n-1]\right),$$

$$G_{\mathrm{f}} \;:=\; \left((0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, 2p)\right).$$

We define $G := \left(1_{{}_p\Gamma}\right) \sqcup G_{\mathrm{b}} \sqcup G_{\mathrm{c}} \sqcup G_{\mathrm{d}} \sqcup G_{\mathrm{e}} \sqcup G_{\mathrm{f}}$. *Cf.* Convention 12.

Then G is a $\mathbb{Z}$-linear basis of ${}_p\Lambda$ in ${}_p\Gamma$.

In particular, we have the $\mathbb{Z}$-linear determinant of the canonical embedding $\iota : {}_p\Lambda \hookrightarrow {}_p\Gamma$,

$$\det_{\mathbb{Z}}(\iota) \;=\; 2 \cdot p^3.$$

Proof of *(i)*. We have $1_\Gamma = (1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1) \in \Lambda$.

Suppose given $(a_1, \begin{pmatrix} b_1 & c_1 \\ d_1 & e_1 \end{pmatrix}, f_1)$, $(a_2, \begin{pmatrix} b_2 & c_2 \\ d_2 & e_2 \end{pmatrix}, f_2) \in \Lambda$. $\quad (*)$

We have to show that

$$(a_1, \begin{pmatrix} b_1 & c_1 \\ d_1 & e_1 \end{pmatrix}, f_1) \cdot (a_2, \begin{pmatrix} b_2 & c_2 \\ d_2 & e_2 \end{pmatrix}, f_2) = (a_1a_2, \begin{pmatrix} b_1b_2 + c_1d_2 & b_1c_2 + c_1e_2 \\ d_1b_2 + e_1d_2 & d_1c_2 + e_1e_2 \end{pmatrix}, f_1f_2) \overset{!}{\in} \Lambda \quad (**)$$

Because of $(*)$ there exist $k, l \in \mathbb{Z}$ and $z_1, z_2, w_1, w_2, u_1, u_2 \in \mathbb{Z}[\vartheta]$ with

$$\begin{array}{rclcrcl} a_1 &=& f_1 + 2k\,, & & a_1 - b_1 &=& \vartheta \cdot w_1\,, \\ a_2 &=& f_2 + 2l\,, & & a_2 - b_2 &=& \vartheta \cdot w_2\,, \\ d_1 &=& \vartheta \cdot z_1\,, & & e_1 - f_1 &=& \vartheta \cdot u_1\,, \\ d_2 &=& \vartheta \cdot z_2\,, & & e_2 - f_2 &=& \vartheta \cdot u_2\,. \end{array}$$

Now we consider the entries of the product.

(1) We have $a_1a_2 = (f_1 + 2k)(f_2 + 2l) = f_1f_2 + 2lf_1 + 2kf_2 + 4kl \equiv_2 f_1f_2$.

(2) We have $d_1b_2 + e_1d_2 = \vartheta z_1b_2 + \vartheta e_1z_2 = \vartheta(z_1b_2 + e_1z_2) \equiv_\vartheta 0$.

(3) We have

$$\begin{array}{rcll} a_1a_2 - b_1b_2 - c_1d_2 &=& a_1a_2 - b_1a_2 + b_1a_2 - b_1b_2 - c_1d_2 & \\ &=& (a_1 - b_1)a_2 + b_1(a_2 - b_2) - c_1d_2 & \\ &=& \vartheta w_1a_2 + b_1\vartheta w_2 - c_1\vartheta z_2 & \equiv_\vartheta 0\,. \end{array}$$

(4) The congruence $d_1c_2 + e_1e_2 \equiv_\vartheta f_1f_2$ is shown analogously to (3).

Overall this shows $(**)$ and so Λ is a ring.

Proof of *(ii)*. By Lemma 24 *(iv)* we get that $\vartheta | p$ in $\mathbb{Z}[\vartheta]$. So it is seen that G is a subset of Λ, because the defining congruences for Λ hold for every element in G. The tuple G is, by construction, linearly independent over $\mathbb{Z}$; cf. Lemma 24 *(i3)*.

Suppose given $\lambda = (a, \begin{pmatrix} b & c \\ d & e \end{pmatrix}, f) \in \Lambda$.

We have to show that λ is a $\mathbb{Z}$-linear combination of elements of G.

By subtraction of a $\mathbb{Z}$-multiple of $1_\Gamma \in G$ we can assume $a = 0$, whence $b \equiv_\vartheta 0$ and $f \in 2\mathbb{Z}$.

$\dashrightarrow \; (0, \begin{pmatrix} b & c \\ d & e \end{pmatrix}, f)$

By Lemma 24 *(i3)* and since $b \equiv_\vartheta 0$, there exist $s_i \in \mathbb{Z}$ for $i \in [0, n-1]$ with

$$b \;=\; \vartheta(s_{n-1}\vartheta^{n-1} + s_{n-2}\vartheta^{n-2} + \cdots + s_1\vartheta^1 + s_0) \;=\; s_{n-1}\vartheta^n + s_{n-2}\vartheta^{n-1} + \cdots + s_1\vartheta^2 + s_0\vartheta^1.$$

Because of Lemma 24 *(iv)* there exist $t_j \in \mathbb{Z}$ for $j \in [1, n-1]$ with

$$\vartheta^n \;=\; t_{n-1}\vartheta^{n-1} + t_{n-2}\vartheta^{n-2} + \cdots + t_1\vartheta^1 - p\,,$$

and therefore we get

$$\begin{aligned} b &= s_{n-1}(t_{n-1}\vartheta^{n-1} + t_{n-2}\vartheta^{n-2} + \cdots + t_1\vartheta^1 - p) + s_{n-2}\vartheta^{n-1} + \cdots + s_1\vartheta^2 + s_0\vartheta^1 \\ &= s_{n-1}t_{n-1}\vartheta^{n-1} + s_{n-1}t_{n-2}\vartheta^{n-2} + \cdots + s_{n-1}t_1\vartheta^1 - s_{n-1}p + s_{n-2}\vartheta^{n-1} + \cdots + s_1\vartheta^2 + s_0\vartheta^1 \,. \end{aligned}$$

So we can assume $b = 0$ by subtraction of $\mathbb{Z}$-multiples of elements of $G_\mathrm{b} \subseteq G$.

$\dashrightarrow\ (0, \begin{pmatrix} 0 & c \\ d & e \end{pmatrix}, f)$

By subtraction of $\mathbb{Z}$-multiples of elements of $G_\mathrm{c} \subseteq G$ we can assume $c = 0$; cf. Lemma 24 *(i3)*.

$\dashrightarrow\ (0, \begin{pmatrix} 0 & 0 \\ d & e \end{pmatrix}, f)$

Since $d \equiv_\vartheta 0$, we can assume $d = 0$ by subtraction of $\mathbb{Z}$-multiples of elements of $G_\mathrm{d} \subseteq G$;
cf. procedure for entry b.

$\dashrightarrow\ (0, \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix}, f)$

By subtraction of $\mathbb{Z}$-multiples of elements of $G_\mathrm{e} \subseteq G$ we can assume $e = 0$, cf. Lemma 24 *(i3)*, whence $f \equiv_\vartheta 0$. Recall that $a = 0$, whence $f \in 2\mathbb{Z}$. So we have

$$f \in \vartheta\mathbb{Z}[\vartheta] \cap 2\mathbb{Z} \;=\; \vartheta\mathbb{Z}[\vartheta] \cap \mathbb{Z} \cap 2\mathbb{Z} \overset{\text{L.27}}{\underset{(ii)}{=}} p\mathbb{Z} \cap 2\mathbb{Z} \;=\; 2p\mathbb{Z}\,.$$

$\dashrightarrow\ (0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, f)$

Since $f \in 2p\mathbb{Z}$ we can assume $f = 0$ by subtraction of a $\mathbb{Z}$-multiple of $G_\mathrm{f} \subseteq G$.

$\dashrightarrow\ (0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, 0)$

Therefore G is a $\mathbb{Z}$-linear basis of Λ in Γ.

Now we choose the $\mathbb{Z}$-linear basis G of Λ and the canonical $\mathbb{Z}$-linear basis of Γ; cf. Lemma 24 *(i3)*.

Then the describing matrix of the canonical embedding $\iota : \Lambda \hookrightarrow \Gamma$ is lower triangular.

We consider the contributing factors of the components of G to the determinant of ι:

component of G	1_Γ	G_b	G_c	G_d	G_e	G_f
contributing factor	1	p	1	p	1	$2p$

Therefore we have the determinant $\det_\mathbb{Z}(\iota) = 2 \cdot p^3$. □

Theorem 70 *We have the isomorphism of rings*

$$\omega_\mathbb{Z} : \mathbb{Z}\mathrm{D}_{2p} \xrightarrow{\sim} \left\{ (a, \begin{pmatrix} b & c \\ d & e \end{pmatrix}, f) \in \mathbb{Z} \times \mathbb{Z}[\vartheta_p]^{2\times 2} \times \mathbb{Z} : a \equiv_{\vartheta_p} b, d \equiv_{\vartheta_p} 0, e \equiv_{\vartheta_p} f, a \equiv_2 f \right\} = {}_p\Lambda$$

$$x \longmapsto (1, M_1, 1) = (1, \begin{pmatrix} 1 & 1 \\ \vartheta_p & \vartheta_p + 1 \end{pmatrix}, 1),$$

$$y \longmapsto (1, N_1, -1) = (1, \begin{pmatrix} 1 & 0 \\ \vartheta_p & -1 \end{pmatrix}, -1),$$

cf. Definitions 17, 56.

Proof. We consider the Wedderburn isomorphism $\omega_{\mathbb{Q}}$ of Proposition 67.

We restrict the domain of $\omega_{\mathbb{Q}}$ from $\mathbb{Q}\mathrm{D}_{2p}$ to $\mathbb{Z}\mathrm{D}_{2p}$. Further, since M_1, $N_1 \in \mathbb{Z}[\vartheta]^{2\times 2}$, we can restrict the codomain of $\omega_{\mathbb{Q}}\big|_{\mathbb{Z}\mathrm{D}_{2p}}$ from $\mathbb{Q} \times \mathbb{Q}(\vartheta)^{2\times 2} \times \mathbb{Q}$ to $\mathbb{Z} \times \mathbb{Z}[\vartheta]^{2\times 2} \times \mathbb{Z}$.

So we can define $\tilde{\omega}_{\mathbb{Z}} := \omega_{\mathbb{Q}}\big|_{\mathbb{Z}\mathrm{D}_{2p}}^{\mathbb{Z}\times\mathbb{Z}[\vartheta]^{2\times 2}\times\mathbb{Z}}$, whence $\tilde{\omega}_{\mathbb{Z}}$ is a morphism of rings.

Hence, we obtain the commutative diagram

$$\begin{array}{ccc} \mathbb{Q}\mathrm{D}_{2p} & \xrightarrow[\sim]{\omega_{\mathbb{Q}}} & \mathbb{Q} \times \mathbb{Q}(\vartheta)^{2\times 2} \times \mathbb{Q} \\ \uparrow & \circlearrowright & \uparrow \\ \mathbb{Z}\mathrm{D}_{2p} & \xrightarrow{\tilde{\omega}_{\mathbb{Z}}} & \mathbb{Z} \times \mathbb{Z}[\vartheta]^{2\times 2} \times \mathbb{Z} = \Gamma \quad \leftarrow \quad \text{N.68} \end{array}$$

As a restriction of $\omega_{\mathbb{Q}}$, the map $\tilde{\omega}_{\mathbb{Z}}$ is injective.

Since $\tilde{\omega}_{\mathbb{Z}}(x)$ and $\tilde{\omega}_{\mathbb{Z}}(y)$ are elements of Λ and using the fact of Remark 69 *(i)* that Λ is a ring we get that $\tilde{\omega}_{\mathbb{Z}}(\mathbb{Z}\mathrm{D}_{2p}) \subseteq \Lambda$.

By Remark 69 *(ii)* we have that the canonical $\mathbb{Z}$-linear embedding of Λ in Γ has determinant $2 \cdot p^3$.

So we have

$$\left|\Gamma/\Lambda\right| = |\det_{\mathbb{Z}}(\Lambda \hookrightarrow \Gamma)| = 2 \cdot p^3.$$

Further we calculate the index of the image of $\tilde{\omega}_{\mathbb{Z}}$ in Γ as

$$\left|\Gamma/\tilde{\omega}_{\mathbb{Z}}(\mathbb{Z}\mathrm{D}_{2p})\right| \overset{(*)}{=} \sqrt{\left|\frac{|\mathrm{D}_{2p}|^{|\mathrm{D}_{2p}|}}{1 \cdot \left(\Delta^4_{\mathbb{Q}(\vartheta)|\mathbb{Q}} \cdot 2^{2^2\cdot[\mathbb{Q}(\vartheta):\mathbb{Q}]}\right) \cdot 1}\right|} \underset{\text{L.25}}{\overset{\text{L.24}\,(i2)}{=}} \sqrt{\left|\frac{(2p)^{2p}}{\left(\pm p^{\frac{p-3}{2}}\right)^4 \cdot 2^{4\cdot\frac{p-1}{2}}}\right|} = \frac{(2p)^p}{p^{p-3} \cdot 2^{p-1}} = 2 \cdot p^3,$$

where in $(*)$ we refer to [Künzer 99, Ch. I, p. 4, Proposition 1.1.5 (total index formula II)] applied to the case $(G, R, K) = (\mathrm{D}_{2p}, \mathbb{Z}, \mathbb{Q})$; cf. Lemma 22.

Using that $\tilde{\omega}_{\mathbb{Z}}(\mathbb{Z}\mathrm{D}_{2p})$ is a subset of Λ we therefore obtain that $\tilde{\omega}_{\mathbb{Z}}(\mathbb{Z}\mathrm{D}_{2p}) = \Lambda$.

Hence we get that $\omega_{\mathbb{Z}} := \tilde{\omega}_{\mathbb{Z}}\big|^{\Lambda} = \omega_{\mathbb{Q}}\big|_{\mathbb{Z}\mathrm{D}_{2p}}^{\Lambda}$ is an isomorphism of rings. □

Corollary 71 *We have the isomorphism of* $\mathbb{Z}_{(p)}$*-algebras*

$$\begin{array}{rccl} \omega_{\mathbb{Z}_{(p)}} & : & \mathbb{Z}_{(p)}\mathrm{D}_{2p} & \xrightarrow{\sim} & {}_p\Lambda_{(p)} \\ & & x & \longmapsto & \omega_{\mathbb{Z}}(x)\,, \\ & & y & \longmapsto & \omega_{\mathbb{Z}}(y)\,. \end{array}$$

Proof. By Theorem 70 we have the isomorphism of rings $\omega_{\mathbb{Z}} : \mathbb{Z}\mathrm{D}_{2p} \xrightarrow{\sim} \Lambda$. So we get by Remark 122 that

$$\begin{array}{rccccc} & & & & \text{as subrings of } \mathbb{Q}\mathrm{D}_{2p} & \\ & & & & \downarrow & \\ \omega_{\mathbb{Z}_{(p)}} := (\omega_{\mathbb{Z}})_{(p)} & : & (\mathbb{Z}\mathrm{D}_{2p})_{(p)} & = & \mathbb{Z}_{(p)}\mathrm{D}_{2p} & \xrightarrow{\sim} \qquad \Lambda_{(p)} \\ & & & & \sum_{d\in\mathrm{D}_{2p}} \frac{z_d}{s_d}\cdot d & \longmapsto \quad \sum_{d\in\mathrm{D}_{2p}} \frac{z_d}{s_d}\cdot\omega_{\mathbb{Z}}(d) \end{array}$$

is an isomorphism of $\mathbb{Z}_{(p)}$-modules. Since $\omega_{\mathbb{Z}}$ is an isomorphism of rings, we see that $\omega_{\mathbb{Z}_{(p)}}$ preserves 1 and is multiplicative. So $\omega_{\mathbb{Z}_{(p)}}$ is an isomorphism of $\mathbb{Z}_{(p)}$-algebras. □

Remark 72 *We have the short exact sequence of abelian groups*

$$\begin{array}{ccccccc} {}_p\Lambda & \overset{\iota}{\hookrightarrow} & {}_p\Gamma & \overset{\varrho}{\longrightarrow} & \mathbb{Z}/2\mathbb{Z} & \oplus & \left(\mathbb{Z}[\vartheta_p]\Big/\vartheta_p\mathbb{Z}[\vartheta_p]\right)^{\oplus 3} \\ (a,\begin{pmatrix} b & c \\ d & e \end{pmatrix},f) & \longmapsto & (a,\begin{pmatrix} b & c \\ d & e \end{pmatrix},f) & \longmapsto & \Big((a-f)+2\mathbb{Z} & , & (a-b)+\vartheta_p\mathbb{Z}[\vartheta_p] \\ & & & & & , & d+\vartheta_p\mathbb{Z}[\vartheta_p] \\ & & & & & , & (e-f)+\vartheta_p\mathbb{Z}[\vartheta_p]\Big)\,. \end{array}$$

Proof. As embedding of Λ in Γ, the map ι is additive and injective. We see that ϱ is also additive. Suppose given $\left(r+2\mathbb{Z}, s+\vartheta\mathbb{Z}[\vartheta], t+\vartheta\mathbb{Z}[\vartheta], u+\vartheta\mathbb{Z}[\vartheta]\right) \in \mathbb{Z}/2\mathbb{Z} \oplus \left(\mathbb{Z}[\vartheta]\Big/\vartheta\mathbb{Z}[\vartheta]\right)^{\oplus 3}$. Then we have

$$\varrho\left((r,\begin{pmatrix} r-s & 0 \\ t & u \end{pmatrix},0)\right) \;=\; \left(r+2\mathbb{Z}, s+\vartheta\mathbb{Z}[\vartheta], t+\vartheta\mathbb{Z}[\vartheta], u+\vartheta\mathbb{Z}[\vartheta]\right).$$

Therefore ϱ is surjective. Further we have the equivalences

$$(a,\begin{pmatrix} b & c \\ d & e \end{pmatrix},f) \in \ker(\varrho) \iff a-f \in 2\mathbb{Z} \text{ and } a-b,\, d,\, e-f \in \vartheta\mathbb{Z}[\vartheta] \overset{\text{N.68}}{\iff} (a,\begin{pmatrix} b & c \\ d & e \end{pmatrix},f) \in \Lambda = \mathrm{im}(\iota)\,.$$

□

4.2 The group ring $\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p}$

Remark 73 First we recall some definitions and facts from Section 2.2 :

$$\Psi \;=\; {}_p\Psi \;\overset{\text{D.34}}{=}\; \left\{ (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n} \,:\, \sum_{k=1}^{n} \left\langle \begin{matrix} i \\ k \end{matrix} \right\rangle a_k \equiv_{\vartheta_p^i} 0 \text{ for } i \in [0,n-1] \right\} \subseteq \mathbb{Z}[\vartheta_p]^{\times n},$$

$$\theta \;=\; \theta_p \;\overset{\text{D.49}}{=}\; (\,\sigma_n(\vartheta_p)\,,\,\ldots\,,\,\sigma_1(\vartheta_p)\,) \;\overset{\text{P.41}}{=}\; f(1\otimes\vartheta_p) \,\in\, {}_p\Psi\,,$$

$$\theta\Psi \;=\; \theta_p\cdot{}_p\Psi \;\overset{\text{P.52}}{=}\; \left\{ (a_j)_{j\in[1,n]} \in \mathbb{Z}[\vartheta_p]^{\times n} \,:\, \sum_{k=1}^{n} \frac{(2i-1)^2}{(2k-1)^2}(2i)! \left\langle \begin{matrix} i-1 \\ k \end{matrix} \right\rangle a_k \equiv_{\vartheta_p^i} 0 \text{ for } i \in [1,n] \right\}.$$

Given $\xi,\,\eta \in {}_p\Psi$, we usually write $\xi \equiv_{\theta_p} \eta$ for $\xi-\eta \in \theta_p\cdot{}_p\Psi$; cf. Convention 11.

Notation 74 We have the $\mathbb{Z}[\vartheta_p]$-algebra

$$\mathfrak{K} \;=\; {}_p\mathfrak{K} \;:=\; \mathbb{Z}[\vartheta_p]\times{}_p\Psi^{2\times2}\times\mathbb{Z}[\vartheta_p]\,,$$

and its $\mathbb{Z}[\vartheta_p]$-submodule

$$\Omega \;=\; {}_p\Omega \;:=\; \left\{ (\xi,\begin{pmatrix}\psi_1 & \psi_2\\ \psi_3 & \psi_4\end{pmatrix},\eta) \in {}_p\mathfrak{K} \,:\, (\xi)_{i\in[1,n]} \equiv_{\theta_p} \psi_1\,,\, \psi_3 \equiv_{\theta_p} 0\,,\, \psi_4 \equiv_{\theta_p} (\eta)_{i\in[1,n]}\,,\, \xi \equiv_2 \eta \right\},$$

cf. Convention 7.

Remark 75 *Write* $I := [1,n]$. *We have the injective morphism of* $\mathbb{Z}[\vartheta_p]$*-algebras*

$$\begin{array}{rcl} \tilde{\nu} \;:\; {}_p\mathfrak{K} = \mathbb{Z}[\vartheta_p]\times {}_p\Psi^{2\times2} \times\mathbb{Z}[\vartheta_p] & \longrightarrow & \mathbb{Z}[\vartheta_p]\times\left(\mathbb{Z}[\vartheta_p]^{2\times2}\right)^{\times n}\times\mathbb{Z}[\vartheta_p] \\ (\,\xi\;,\;\begin{pmatrix}(a_i)_{i\in I} & (b_i)_{i\in I}\\ (c_i)_{i\in I} & (d_i)_{i\in I}\end{pmatrix}\;,\;\eta\,) & \longmapsto & (\,\xi\;,\;\begin{pmatrix}a_i & b_i\\ c_i & d_i\end{pmatrix}_{i\in I}\;,\;\eta\,) \end{array}$$

Proof. We obtain $\tilde{\nu}$ as the composite of the injective morphisms of $\mathbb{Z}[\vartheta]$-algebras

$$\begin{array}{ccccc} \mathbb{Z}[\vartheta]\times\Psi^{2\times2}\times\mathbb{Z}[\vartheta] & \overset{(*)}{\hookrightarrow} & \mathbb{Z}[\vartheta]\times\left(\mathbb{Z}[\vartheta]^{\times n}\right)^{2\times2}\times\mathbb{Z}[\vartheta] & \underset{\sim}{\overset{(**)}{\longrightarrow}} & \mathbb{Z}[\vartheta]\times\left(\mathbb{Z}[\vartheta]^{2\times2}\right)^{\times n}\times\mathbb{Z}[\vartheta] \\ (\,\xi\,,\,\begin{pmatrix}(a_i)_{i\in I} & (b_i)_{i\in I}\\ (c_i)_{i\in I} & (d_i)_{i\in I}\end{pmatrix},\,\eta\,) & \longmapsto & (\,\xi\,,\,\begin{pmatrix}(a_i)_{i\in I} & (b_i)_{i\in I}\\ (c_i)_{i\in I} & (d_i)_{i\in I}\end{pmatrix},\,\eta\,) & \longmapsto & (\,\xi\,,\,\begin{pmatrix}a_i & b_i\\ c_i & d_i\end{pmatrix}_{i\in I},\,\eta\,), \end{array}$$

where we note that Ψ is a $\mathbb{Z}[\vartheta]$-subalgebra of $\mathbb{Z}[\vartheta]^{\times n}$, cf. Proposition 41, so that the canonical embedding in $(*)$ is an injective morphism of $\mathbb{Z}[\vartheta]$-algebras. In $(**)$ we refer to Lemma 102. □

Remark 76 *Write* $I := [1,n]$. *We have the short exact sequence of* $\mathbb{Z}[\vartheta_p]$*-modules*

$$\begin{array}{ccccccc} {}_p\Omega & \overset{j}{\hookrightarrow} & {}_p\mathfrak{K} & \overset{r}{\longrightarrow} & \mathbb{Z}[\vartheta_p]\Big/2\mathbb{Z}[\vartheta_p] & \oplus & \left({}_p\Psi\Big/\theta_p\cdot{}_p\Psi\right)^{\oplus 3} \\ (\xi,\begin{pmatrix}\psi_1 & \psi_2\\ \psi_3 & \psi_4\end{pmatrix},\eta) & \longmapsto & (\xi,\begin{pmatrix}\psi_1 & \psi_2\\ \psi_3 & \psi_4\end{pmatrix},\eta) & \longmapsto & \Big((\xi-\eta)+2\mathbb{Z}[\vartheta_p] & , & ((\xi)_{i\in I}-\psi_1)+\theta_p\cdot{}_p\Psi \\ & & & & & , & \psi_3+\theta_p\cdot{}_p\Psi \\ & & & & & , & (\psi_4-(\eta)_{i\in I})+\theta_p\cdot{}_p\Psi\Big)\,. \end{array}$$

Proof. As embedding of Ω in $\mathfrak{K}$, the map j is a morphism of $\mathbb{Z}[\vartheta]$-modules and injective.

We see that r is also a morphism of $\mathbb{Z}[\vartheta]$-modules.

Suppose given $\left(w+2\mathbb{Z}[\vartheta], x+\theta\Psi, y+\theta\Psi, z+\theta\Psi\right) \in \mathbb{Z}[\vartheta]\Big/2\mathbb{Z}[\vartheta] \oplus \left(\Psi\Big/\theta\Psi\right)^{\oplus 3}$. Then we have

$$r\left(w,\begin{pmatrix}(w)_{i\in I}-x & 0\\ y & z\end{pmatrix},0\right) \;=\; \left(w+2\mathbb{Z}[\vartheta], x+\theta\Psi, y+\theta\Psi, z+\theta\Psi\right).$$

Therefore r is surjective. Further we have the equivalences

$$\begin{aligned}(\xi,\begin{pmatrix}\psi_1 & \psi_2\\ \psi_3 & \psi_4\end{pmatrix},\eta)\in\ker(r) &\iff \xi-\eta\in 2\mathbb{Z}[\vartheta] \text{ and } (\xi)_{i\in I}-\psi_1\,,\ \psi_3\,,\ \psi_4-(\eta)_{i\in I}\in\theta\Psi \\ &\overset{\text{N.74}}{\iff} (\xi,\begin{pmatrix}\psi_1 & \psi_2\\ \psi_3 & \psi_4\end{pmatrix},\eta)\in\Omega=\mathrm{im}(j)\,.\end{aligned}$$

□

Remark 77 *We have the isomorphism of* $\mathbb{Z}[\vartheta_p]$*-algebras*

$$\begin{array}{rcccccl} k\ :\ \mathbb{Z}[\vartheta_p]\mathrm{D}_{2p} & \overset{\sim}{\longrightarrow} & \mathbb{Z}[\vartheta_p] & \underset{\mathbb{Z}}{\otimes} & {}_p\Lambda & & \\ x & \longmapsto & 1 & \otimes\ \omega_{\mathbb{Z}}(x) & = 1\otimes(1,M_1,1) & = & 1\otimes(1,\begin{pmatrix}1 & 1\\ \vartheta_p & \vartheta_p+1\end{pmatrix},1) \\ y & \longmapsto & 1 & \otimes\ \omega_{\mathbb{Z}}(y) & = 1\otimes(1,N_1,-1) & = & 1\otimes\ (1,\begin{pmatrix}1 & 0\\ \vartheta_p & -1\end{pmatrix},-1)\,. \end{array}$$

For $\omega_{\mathbb{Z}}$ *we refer to* Theorem 70.

Proof. We compose the isomorphisms of $\mathbb{Z}[\vartheta_p]$-algebras

$$\begin{array}{ccccccccc} \mathbb{Z}[\vartheta]\mathrm{D}_{2p} & \underset{\text{L.99}}{\overset{\sim}{\longrightarrow}} & \mathbb{Z}[\vartheta] & \underset{\mathbb{Z}}{\otimes} & \mathbb{Z}\mathrm{D}_{2p} & \underset{\text{L.93, L.92}\textit{(ii)}}{\overset{\mathbb{Z}[\vartheta]\otimes\omega_{\mathbb{Z}}}{\overset{\sim}{\longrightarrow}}} & \mathbb{Z}[\vartheta] & \underset{\mathbb{Z}}{\otimes} & \Lambda \\ x & \longmapsto & 1 & \otimes & x & \longmapsto & 1 & \otimes & \omega_{\mathbb{Z}}(x) \\ y & \longmapsto & 1 & \otimes & y & \longmapsto & 1 & \otimes & \omega_{\mathbb{Z}}(y) \end{array}$$

For the matrices occurring in $\omega_{\mathbb{Z}}(x)$ and $\omega_{\mathbb{Z}}(y)$, we refer to Theorem 70. □

Lemma 78 *We have the isomorphism of* $\mathbb{Z}[\vartheta_p]$*-algebras*

$$\begin{array}{rcccccccccc} \tau_0\ :\ \mathbb{Z}[\vartheta_p] & \underset{\mathbb{Z}}{\otimes} & \left(\mathbb{Z}\ \times\ \mathbb{Z}[\vartheta_p]^{2\times 2}\ \times\ \mathbb{Z}\right) & \overset{\sim}{\longrightarrow} & \mathbb{Z}[\vartheta_p]\ \times & {}_p\Psi^{2\times 2} & \times\ \mathbb{Z}[\vartheta_p] & = & {}_p\mathfrak{K} \\ \xi\ \otimes\ (\,u\ , & \begin{pmatrix}\eta_1 & \eta_2\\ \eta_3 & \eta_4\end{pmatrix} & ,\ v\,) & \longmapsto & (\,\xi u\ , & \begin{pmatrix}f(\xi\otimes\eta_1) & f(\xi\otimes\eta_2)\\ f(\xi\otimes\eta_3) & f(\xi\otimes\eta_4)\end{pmatrix} & ,\ \xi v\,)\,. & & \end{array}$$

Proof. We compose the isomorphisms of $\mathbb{Z}[\vartheta]$-algebras

$$\begin{aligned}
&\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \left(\mathbb{Z} \times \mathbb{Z}[\vartheta]^{2\times 2} \times \mathbb{Z}\right) \xrightarrow[\text{L.96}]{\sim} \mathbb{Z}[\vartheta] \times \left(\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta]^{2\times 2}\right) \times \mathbb{Z}[\vartheta] \\
&\xi \otimes (u\ ,\ \begin{pmatrix}\eta_1 & \eta_2\\ \eta_3 & \eta_4\end{pmatrix}\ ,\ v) \longmapsto (\xi u\ ,\ \xi \otimes \begin{pmatrix}\eta_1 & \eta_2\\ \eta_3 & \eta_4\end{pmatrix}\ ,\ \xi v)
\end{aligned}$$

$$\begin{aligned}
&\xrightarrow[\text{L.98}]{\sim} \mathbb{Z}[\vartheta] \times \left(\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[\vartheta]\right)^{2\times 2} \times \mathbb{Z}[\vartheta] \xrightarrow[\text{P.41}]{\sim} \mathbb{Z}[\vartheta] \times \Psi^{2\times 2} \times \mathbb{Z}[\vartheta] \\
&\longmapsto (\xi u\ ,\ \begin{pmatrix}\xi\otimes\eta_1 & \xi\otimes\eta_2\\ \xi\otimes\eta_3 & \xi\otimes\eta_4\end{pmatrix}\ ,\ \xi v) \longmapsto (\xi u\ ,\ \begin{pmatrix}f(\xi\otimes\eta_1) & f(\xi\otimes\eta_2)\\ f(\xi\otimes\eta_3) & f(\xi\otimes\eta_4)\end{pmatrix}\ ,\ \xi v).
\end{aligned}$$

□

Lemma 79 *We have the isomorphisms of* $\mathbb{Z}[\vartheta_p]$*-algebras*

(i)
$$\begin{aligned}
\tau_1 \ :\ \mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} \left(\mathbb{Z}/2\mathbb{Z}\right) &\xrightarrow{\sim} \mathbb{Z}[\vartheta_p]\Big/2\mathbb{Z}[\vartheta_p] \\
\xi \otimes (z+2\mathbb{Z}) &\longmapsto \xi z + 2\mathbb{Z}[\vartheta_p],
\end{aligned}$$

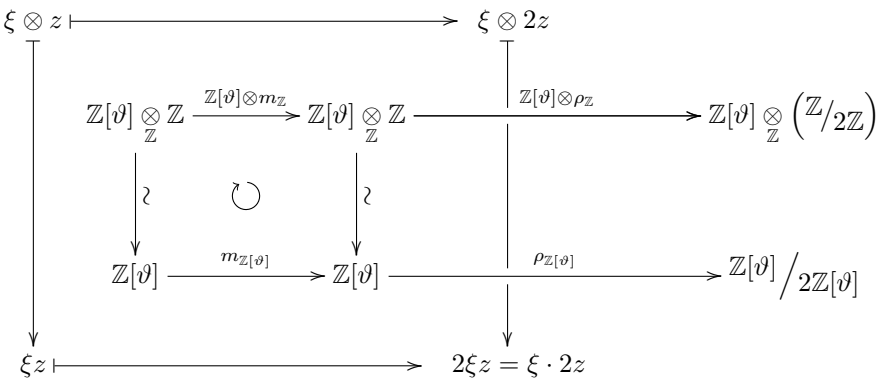
and

(ii)
$$\begin{aligned}
\tau_2 \ :\ \mathbb{Z}[\vartheta_p] \underset{\mathbb{Z}}{\otimes} \left(\mathbb{Z}[\vartheta_p]\Big/\vartheta_p\mathbb{Z}[\vartheta_p]\right) &\xrightarrow{\sim} {}_p\Psi\Big/\theta_p \cdot {}_p\Psi \\
\xi \otimes (\eta + \vartheta_p\mathbb{Z}[\vartheta_p]) &\longmapsto f(\xi\otimes\eta) + \theta_p \cdot {}_p\Psi,
\end{aligned}$$

where f *is the isomorphism of* $\mathbb{Z}[\vartheta_p]$*-algebras from* Proposition 41.

Proof of *(i).* We define the multiplication maps by $m_C : C \longrightarrow C$, $c \longmapsto 2c$ and the residue class maps by $\rho_C : C \longrightarrow C/2C$, $c \longmapsto c + 2C$ for $C = \mathbb{Z}$ respectively $C = \mathbb{Z}[\vartheta]$.

By Lemma 24 *(i3)* we have that $\mathbb{Z}[\vartheta]$ is a finitely generated free $\mathbb{Z}$-module. Therefore $\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} -$ is exact, cf. Lemma 94, and so the upper row in the following diagram is a right exact sequence of $\mathbb{Z}[\vartheta]$-modules.



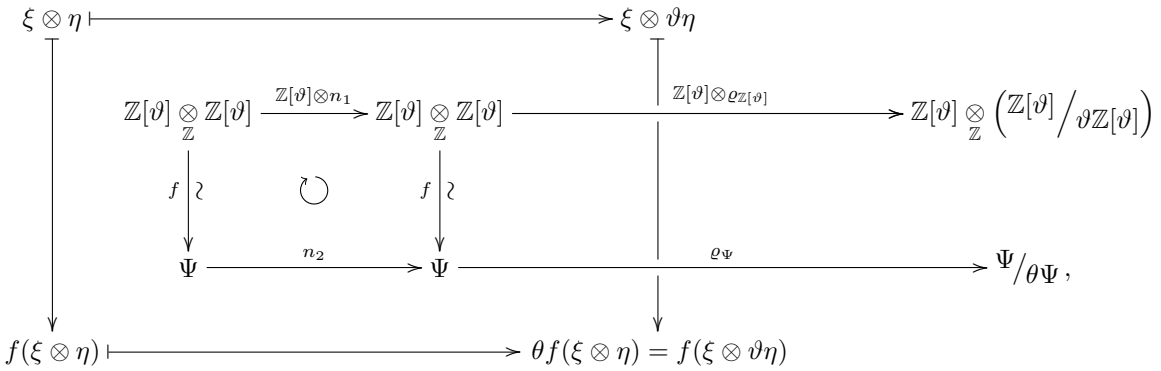
We see that the lower row is also a right exact sequence of $\mathbb{Z}[\vartheta]$-modules. Hence, there exists a unique $\mathbb{Z}[\vartheta]$-linear map $\mathbb{Z}[\vartheta] \underset{\mathbb{Z}}{\otimes} \left(\mathbb{Z}/2\mathbb{Z}\right) \longrightarrow \mathbb{Z}[\vartheta]\Big/2\mathbb{Z}[\vartheta]$ making the diagram commutative, which is an isomorphism. This map is just τ_1. We see that τ_1 preserves 1. For $\xi_1, \xi_2 \in \mathbb{Z}[\vartheta]$ and $z_1 + 2\mathbb{Z}$, $z_2 + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z}$

we have

$$\left.\begin{array}{rcccl} & \tau_1\big((\xi_1\otimes(z_1+2\mathbb{Z}))\cdot(\xi_2\otimes(z_2+2\mathbb{Z}))\big) & = & \tau_1\big((\xi_1\xi_2)\otimes(z_1z_2+2\mathbb{Z})\big) & = \ \xi_1\xi_2z_1z_2+2\mathbb{Z}[\vartheta] \\ = & (\xi_1z_1+2\mathbb{Z}[\vartheta])\cdot(\xi_2z_2+2\mathbb{Z}[\vartheta]) & = & \tau_1(\xi_1\otimes(z_1+2\mathbb{Z}))\cdot\tau_1(\xi_2\otimes(z_2+2\mathbb{Z}))\,. & \end{array}\right\}(1)$$

Since τ_1 is additive and every element of $\mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\left(\mathbb{Z}/2\mathbb{Z}\right)$ is a finite sum of elementary tensors, equation (1) shows that τ_1 is multiplicative.

Proof of *(ii)*. We define $n_1 : \mathbb{Z}[\vartheta]\longrightarrow\mathbb{Z}[\vartheta]$, $\xi\longmapsto\vartheta\xi$ and $n_2 : \Psi\longrightarrow\Psi$, $\psi\longmapsto\theta\psi$. The residue class maps we denote by $\varrho_{\mathbb{Z}[\vartheta]} : \mathbb{Z}[\vartheta]\longrightarrow{}^{\mathbb{Z}[\vartheta]}/_{\vartheta\mathbb{Z}[\vartheta]}$, $\xi\longmapsto\xi+\vartheta\mathbb{Z}[\vartheta]$ and $\varrho_\Psi : \Psi\longrightarrow{}^{\Psi}/_{\theta\Psi}$, $\psi\longmapsto\psi+\theta\Psi$. By Lemma 24 *(i3)* we have that $\mathbb{Z}[\vartheta]$ is a finitely generated free $\mathbb{Z}$-module. Therefore $\mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}-$ is exact, cf. Lemma 94, and so the upper row in the following diagram is a right exact sequence of $\mathbb{Z}[\vartheta]$-modules.



where we note that $\theta f(\xi\otimes\eta)=f(1\otimes\vartheta)\cdot f(\xi\otimes\eta)=f((1\otimes\vartheta)\cdot(\xi\otimes\eta))=f(\xi\otimes\vartheta\eta)$.

We see that the lower row is also a right exact sequence of $\mathbb{Z}[\vartheta]$-modules. Hence, there exists a unique $\mathbb{Z}[\vartheta]$-linear map $\mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\left(\mathbb{Z}[\vartheta]/\vartheta\mathbb{Z}[\vartheta]\right)\longrightarrow{}^{\Psi}/_{\theta\Psi}$ making the diagram commutative, which is an isomorphism. This map is just τ_2. Since f is a morphism of rings, we see that τ_2 preserves 1. For ξ_1, $\xi_2\in\mathbb{Z}[\vartheta]$ and $\eta_1+\vartheta\mathbb{Z}[\vartheta]$, $\eta_2+\vartheta\mathbb{Z}[\vartheta]\in{}^{\mathbb{Z}[\vartheta]}/_{\vartheta\mathbb{Z}[\vartheta]}$ we have

$$\left.\begin{array}{rl} & \tau_2\big((\xi_1\otimes(\eta_1+\vartheta\mathbb{Z}[\vartheta]))\cdot(\xi_2\otimes(\eta_2+\vartheta\mathbb{Z}[\vartheta]))\big) \ = \ \tau_2\big((\xi_1\xi_2)\otimes(\eta_1\eta_2+\vartheta\mathbb{Z}[\vartheta])\big) \\ = & f((\xi_1\xi_2)\otimes(\eta_1\eta_2))+\theta\Psi \ = \ f((\xi_1\otimes\eta_1)\cdot(\xi_2\otimes\eta_2))+\theta\Psi \ = \ (f(\xi_1\otimes\eta_1)\cdot f(\xi_2\otimes\eta_2))+\theta\Psi \\ = & (f(\xi_1\otimes\eta_1)+\theta\Psi)\cdot(f(\xi_2\otimes\eta_2)+\theta\Psi) \ = \ \tau_2(\xi_1\otimes(\eta_1+\vartheta\mathbb{Z}[\vartheta]))\cdot\tau_2(\xi_2\otimes(\eta_2+\vartheta\mathbb{Z}[\vartheta]))\,. \end{array}\right\}(2)$$

Since τ_2 is additive and every element of $\mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\left(\mathbb{Z}[\vartheta]/\vartheta\mathbb{Z}[\vartheta]\right)$ is a finite sum of elementary tensors, equation (2) shows that τ_2 is multiplicative. □

Theorem 80 *Write* $I:=[1,n]$. *We recall the* $\mathbb{Z}[\vartheta_p]$*-submodule* ${}_p\Omega$ *of the* $\mathbb{Z}[\vartheta_p]$*-algebra* ${}_p\mathfrak{K}$

$${}_p\Omega=\left\{(\xi,\begin{pmatrix}\psi_1&\psi_2\\ \psi_3&\psi_4\end{pmatrix},\eta)\in\mathbb{Z}[\vartheta_p]\times{}_p\Psi^{2\times2}\times\mathbb{Z}[\vartheta_p] \,:\, (\xi)_{i\in I}\equiv_{\theta_p}\psi_1\,,\ \psi_3\equiv_{\theta_p}0\,,\ \psi_4\equiv_{\theta_p}(\eta)_{i\in I}\,,\ \xi\equiv_2\eta\right\},$$

cf. Remark 73 *and* Notation 74.

Then ${}_p\Omega$ *is a* $\mathbb{Z}[\vartheta_p]$*-subalgebra of* ${}_p\mathfrak{K}$.

We have the isomorphism of $\mathbb{Z}[\vartheta_p]$*-algebras*

$$\begin{array}{rcccl} \omega_{\mathbb{Z}[\vartheta_p]} & : & \mathbb{Z}[\vartheta_p]\mathrm{D}_{2p} & \xrightarrow{\sim} & {}_p\Omega \\ & & x & \longmapsto & (\,1\,,\begin{pmatrix} 1 & 1 \\ \theta_p & \theta_p+1 \end{pmatrix},1\,) \\ & & y & \longmapsto & (\,1\,,\begin{pmatrix} 1 & 0 \\ \theta_p & -1 \end{pmatrix},-1\,). \end{array}$$

Moreover, we have the injective morphism of $\mathbb{Z}[\vartheta_p]$*-algebras*

$$\begin{array}{rcccl} \nu & : & {}_p\Omega & \longrightarrow & \mathbb{Z}[\vartheta_p]\times\left(\mathbb{Z}[\vartheta_p]^{2\times 2}\right)^{\times n}\times\mathbb{Z}[\vartheta_p] \\ & & (\,\xi\,,\begin{pmatrix} (a_i)_{i\in I} & (b_i)_{i\in I} \\ (c_i)_{i\in I} & (d_i)_{i\in I} \end{pmatrix},\eta\,) & \longmapsto & (\,\xi\;,\;\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}_{i\in I}\;,\;\eta\,). \end{array}$$

So altogether, we have the morphisms of $\mathbb{Z}[\vartheta_p]$*-algebras*

$$\mathbb{Z}[\vartheta_p]\mathrm{D}_{2p}\xrightarrow[\sim]{\omega_{\mathbb{Z}[\vartheta_p]}}{}_p\Omega\xrightarrow[\text{inj.}]{\nu}\mathbb{Z}[\vartheta_p]\times\left(\mathbb{Z}[\vartheta_p]^{2\times 2}\right)^{\times n}\times\mathbb{Z}[\vartheta_p]\,.$$

Proof. We have the short exact sequence of abelian groups $\Lambda\overset{\iota}{\hookrightarrow}\Gamma\overset{\varrho}{\longrightarrow}\mathbb{Z}/2\mathbb{Z}\oplus\left(\mathbb{Z}[\vartheta]\big/\vartheta\mathbb{Z}[\vartheta]\right)^{\oplus 3}$, where $\Gamma=\mathbb{Z}\times\mathbb{Z}[\vartheta]^{2\times 2}\times\mathbb{Z}$; cf. Remark 72 and Notation 68.

By Lemma 24 *(i3)* we have that $\mathbb{Z}[\vartheta]$ is a finitely generated free $\mathbb{Z}$-module. Therefore the upper row in the following diagram is a short exact sequence of $\mathbb{Z}[\vartheta]$-modules; cf. Lemma 94. By Remark 76 we get that the lower row is a short exact sequence of $\mathbb{Z}[\vartheta]$-modules; cf. Notation 74.

$$\begin{array}{ccccc} \mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\Lambda & \xrightarrow{\mathbb{Z}[\vartheta]\otimes\iota} & \mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\left(\mathbb{Z}\times\mathbb{Z}[\vartheta]^{2\times 2}\times\mathbb{Z}\right) & \xrightarrow{\mathbb{Z}[\vartheta]\otimes\varrho} & \mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\left(\mathbb{Z}/2\mathbb{Z}\oplus\left(\mathbb{Z}[\vartheta]\big/\vartheta\mathbb{Z}[\vartheta]\right)^{\oplus 3}\right) \\ & & \Big\downarrow{\scriptstyle \text{L.78}\to\tau_0}\wr & \circlearrowright & \Big\downarrow{\scriptstyle \begin{matrix}\text{L.95}\\+\\\text{L.79}\end{matrix}}\wr \\ \Omega & \xrightarrow{j} & \mathbb{Z}[\vartheta]\times\Psi^{2\times 2}\times\mathbb{Z}[\vartheta] & \xrightarrow{r} & \mathbb{Z}[\vartheta]/2\mathbb{Z}[\vartheta]\oplus\left(\Psi/\theta\Psi\right)^{\oplus 3} \end{array}$$

$$\begin{array}{ccc} \xi\otimes(u,\begin{pmatrix}\eta_1 & \eta_2\\ \eta_3 & \eta_4\end{pmatrix},v) & \longmapsto & \xi\otimes((u-v)+2\mathbb{Z},(u-\eta_1)+\vartheta\mathbb{Z}[\vartheta]\,, \\ & & \qquad\eta_3+\vartheta\mathbb{Z}[\vartheta]\,,(\eta_4-v)+\vartheta\mathbb{Z}[\vartheta]\,) \\ \Big\downarrow & \circlearrowright & \Big\downarrow \\ & & \big(\,\xi(u-v)+2\mathbb{Z}[\vartheta]\,,f(\xi\otimes(u-\eta_1))+\theta\Psi\,, \\ & & \qquad f(\xi\otimes\eta_3)+\theta\Psi\,,f(\xi\otimes(\eta_4-v))+\theta\Psi\,\big) \\ & & \qquad\qquad\| \ {\scriptstyle (1)} \\ (\xi u,\begin{pmatrix}f(\xi\otimes\eta_1) & f(\xi\otimes\eta_2)\\ f(\xi\otimes\eta_3) & f(\xi\otimes\eta_4)\end{pmatrix},\xi v) & \longmapsto & \big(\,(\xi u-\xi v)+2\mathbb{Z}[\vartheta]\,,((\xi u)_{i\in I}-f(\xi\otimes\eta_1))+\theta\Psi\,, \\ & & \qquad f(\xi\otimes\eta_3)+\theta\Psi\,,(f(\xi\otimes\eta_4)-(\xi v)_{i\in I})+\theta\Psi\,\big), \end{array}$$

where in equation (1) in the second entry, we note that

$$f(\xi\otimes(u-\eta_1)) \overset{\text{P.41}}{=} (\sigma_{n-i+1}(u-\eta_1)\xi)_{i\in I} = ((\overbrace{\sigma_{n-i+1}(u)}^{=u\in\mathbb{Z}}-\sigma_{n-i+1}(\eta_1))\xi)_{i\in I}$$
$$= (u\xi-\sigma_{n-i+1}(\eta_1)\xi)_{i\in I} = (\xi u)_{i\in I}-(\sigma_{n-i+1}(\eta_1)\xi)_{i\in I} \overset{\text{P.41}}{=} (\xi u)_{i\in I}-f(\xi\otimes\eta_1)\,,$$

and similarly for the fourth entry.

Therefore we get the induced isomorphism of $\mathbb{Z}[\vartheta]$-modules

$$(2)\qquad g\ :\ \mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\Lambda\ \xrightarrow{\sim}\ \Omega\ ,\ \xi\otimes(u,\begin{pmatrix}\eta_1&\eta_2\\ \eta_3&\eta_4\end{pmatrix},v)\ \longmapsto\ (\xi u,\begin{pmatrix}f(\xi\otimes\eta_1)&f(\xi\otimes\eta_2)\\ f(\xi\otimes\eta_3)&f(\xi\otimes\eta_4)\end{pmatrix},\xi v)\,.$$

We recall that $\mathfrak{K}=\mathbb{Z}[\vartheta]\times\Psi^{2\times2}\times\mathbb{Z}[\vartheta]$; cf. Remark 73 and Notation 74.

As embedding of Λ in Γ, the map ι is not only a morphism of $\mathbb{Z}$-modules, but also a morphism of $\mathbb{Z}$-algebras; cf. Remark 69 *(i)*. We apply Lemma 93 to the case $(K,\,L,\,\varphi,\,A,\,B)=(\mathbb{Z},\,\mathbb{Z}[\vartheta],\,\iota,\,\Lambda,\,\Gamma)$ and obtain that $\mathbb{Z}[\vartheta]\otimes\iota$ is a morphism of $\mathbb{Z}[\vartheta]$-algebras. We recall that $\mathbb{Z}[\vartheta]\otimes\iota$ is injective.

Hence we obtain the injective morphism of $\mathbb{Z}[\vartheta]$-algebras

$$g' := \tau_0\circ(\mathbb{Z}[\vartheta]\otimes\iota)\ :\ \mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\Lambda\ \longrightarrow\ \mathbb{Z}[\vartheta]\times\Psi^{2\times2}\times\mathbb{Z}[\vartheta]\ =\ \mathfrak{K}\,,$$

which acts just as g. I.e. we get the commutative diagram

$$\begin{array}{ccc}\mathbb{Z}[\vartheta]\underset{\mathbb{Z}}{\otimes}\Lambda & \xrightarrow[\sim]{g} & \Omega\\ & {\scriptstyle g'}\searrow\quad\circlearrowright\quad\swarrow & \\ & \mathfrak{K}\,, & \end{array}$$

whence $\Omega=\mathrm{im}(g')$ is a $\mathbb{Z}[\vartheta]$-subalgebra of $\mathfrak{K}$ and $g=g'\big|^{\Omega}$ is an isomorphism of $\mathbb{Z}[\vartheta]$-algebras.

Hence we get the isomorphism of $\mathbb{Z}[\vartheta]$-algebras

$$\begin{array}{rccc} g\circ k\ :\ \mathbb{Z}[\vartheta]\mathrm{D}_{2p} & \xrightarrow{\sim} & \Omega\\ x & \longmapsto & g(k(x))\\ y & \longmapsto & g(k(y))\,,\end{array}$$

cf. Remark 77. We have

$$(g\circ k)(x) = g(k(x)) \overset{\text{R.77}}{=} g\left(1\otimes(1,\begin{pmatrix}1&1\\ \vartheta&\vartheta+1\end{pmatrix},1)\right)$$
$$\overset{(2)}{=} (1,\begin{pmatrix}f(1\otimes1)&f(1\otimes1)\\ f(1\otimes\vartheta)&f(1\otimes(\vartheta+1))\end{pmatrix},1)$$
$$= (1,\begin{pmatrix}f(1\otimes1)&f(1\otimes1)\\ f(1\otimes\vartheta)&f(1\otimes\vartheta)+f(1\otimes1))\end{pmatrix},1) = (1,\begin{pmatrix}1&1\\ \theta&\theta+1\end{pmatrix},1)\,,$$

$$\text{and}\quad (g\circ k)(y) = g(k(y)) \overset{\text{R.77}}{=} g\left(1\otimes(1,\begin{pmatrix}1&0\\ \vartheta&-1\end{pmatrix},-1)\right)$$
$$\overset{(2)}{=} (1,\begin{pmatrix}f(1\otimes1)&f(1\otimes0)\\ f(1\otimes\vartheta)&f(1\otimes(-1))\end{pmatrix},-1) = (1,\begin{pmatrix}1&0\\ \theta&-1\end{pmatrix},-1)\,.$$

So $\omega_{\mathbb{Z}[\vartheta]} := g\circ k$ is the asserted isomorphism of $\mathbb{Z}[\vartheta]$-algebras.

We obtain the map ν as the composite of the injective morphisms of $\mathbb{Z}[\vartheta]$-algebras

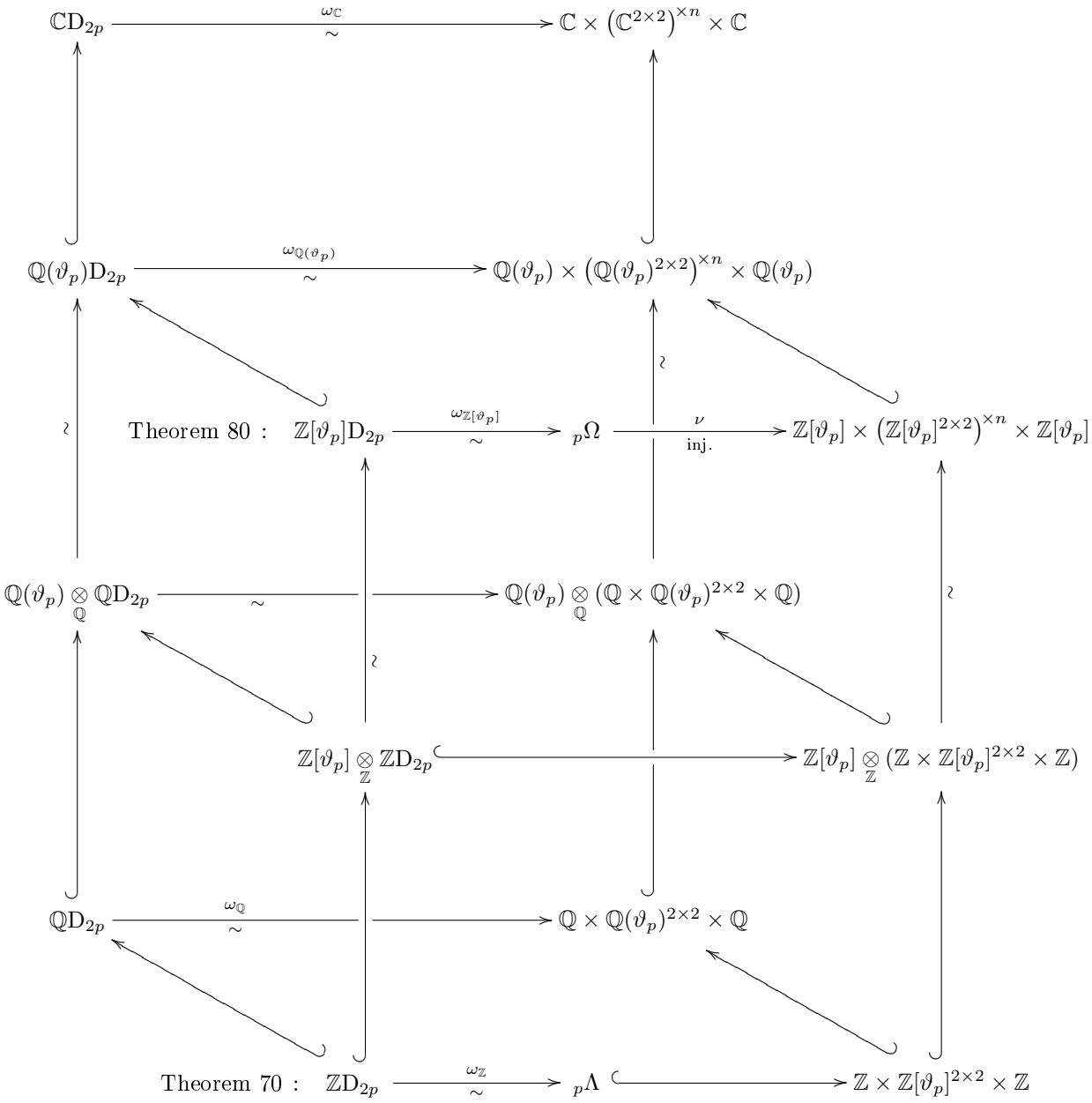
$$\begin{array}{ccccc} \Omega & \hookrightarrow & \mathfrak{K} & \xrightarrow{\tilde{\nu}} & \mathbb{Z}[\vartheta] \times \left(\mathbb{Z}[\vartheta]^{2\times 2}\right)^{\times n} \times \mathbb{Z}[\vartheta] \\ (\,\xi\,,\begin{pmatrix} (a_i)_{i\in I} & (b_i)_{i\in I} \\ (c_i)_{i\in I} & (d_i)_{i\in I} \end{pmatrix},\eta\,) & \longmapsto & (\,\xi\,,\begin{pmatrix} (a_i)_{i\in I} & (b_i)_{i\in I} \\ (c_i)_{i\in I} & (d_i)_{i\in I} \end{pmatrix},\eta\,) & \longmapsto & (\,\xi\,,\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}_{i\in I},\eta\,), \end{array}$$

where for $\tilde{\nu}$ we refer to Remark 75. □

Chapter 5

Overview of dihedral group rings

Summarizing Chapters 3 ("Wedderburn") and 4 ("Group rings of D_{2p}"), we obtain the following commutative diagram of rings and morphisms of rings.



Chapter 6

Presentations via path algebras

Notation 81

In this chapter we consider path algebras of the quiver $\Xi := \left(E \bullet \overset{\alpha}{\underset{\beta}{\rightleftarrows}} \bullet F \right)$.

We write composition of paths in such a way that e.g. $\alpha\beta$ is a path from E to E.

6.1 Presentation of $\mathbb{Z}_{(p)}\mathrm{D}_{2p}$ by quiver and relations

Notation 82 We denote by I the (both-sided) ideal of the path algebra $\mathbb{Z}_{(p)}\Xi$ that is generated by the set $\{ \mu_{\vartheta_p,\mathbb{Q}}(\alpha\beta)\alpha\,,\, \mu_{\vartheta_p,\mathbb{Q}}(\beta\alpha)\beta \}$, where $\mu_{\vartheta_p,\mathbb{Q}}(X) \in \mathbb{Z}[X]$ is the minimal polynomial of ϑ_p over $\mathbb{Q}$.

Using Convention 10 this means

$$I := \lhd\, \mu_{\vartheta_p,\mathbb{Q}}(\alpha\beta)\alpha\,,\, \mu_{\vartheta_p,\mathbb{Q}}(\beta\alpha)\beta \,\rhd_{\mathbb{Z}_{(p)}\Xi}\,.$$

Moreover, we denote the residue class of an element $\xi \in \mathbb{Z}_{(p)}\Xi$ by

$$\overline{\xi} := \xi + I \in {}^{\mathbb{Z}_{(p)}\Xi}\!/_{I}\,.$$

Proposition 83 *We have the isomorphism of $\mathbb{Z}_{(p)}$-algebras*

$$\mathcal{P}_1 :\quad {}^{\mathbb{Z}_{(p)}\Xi}\!/_{I} \;\xrightarrow{\sim}\; \left\{ (u, \begin{pmatrix} v & w \\ x & y \end{pmatrix}, z) \in \mathbb{Z}_{(p)} \times \left(\mathbb{Z}_{(p)}[\vartheta_p]\right)^{2\times 2} \times \mathbb{Z}_{(p)} : u \equiv_{\vartheta_p} v,\, x \equiv_{\vartheta_p} 0,\, y \equiv_{\vartheta_p} z \right\} = {}_p\Lambda_{(p)}$$

$$\overline{E} = E + I \;\longmapsto\; (1, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, 0) =: e$$

$$\overline{F} = F + I \;\longmapsto\; (0, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 1) =: f$$

$$\overline{\alpha} = \alpha + I \;\longmapsto\; (0, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, 0) =: a$$

$$\overline{\beta} = \beta + I \;\longmapsto\; (0, \begin{pmatrix} 0 & 0 \\ \vartheta_p & 0 \end{pmatrix}, 0) =: b\,.$$

For ${}_p\Lambda$ we refer to Notation 68.

Proof. We have the orthogonal decomposition into idempotents $1_{\Lambda_{(p)}} = e + f$. (1)

We see that $a \in e\Lambda_{(p)}f$ and $b \in f\Lambda_{(p)}e$. So the universal property of the path algebra yields that there exists a unique $\mathbb{Z}_{(p)}$-algebra morphism that maps

$$\begin{aligned}
\hat{\psi} \;:\; \mathbb{Z}_{(p)}\Xi \;&\longrightarrow\; \left\{ (\,u\,, \begin{pmatrix} v & w \\ x & y \end{pmatrix}, z\,) \in \mathbb{Z}_{(p)} \times \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{2\times 2} \times \mathbb{Z}_{(p)} \;:\; u \equiv_\vartheta v,\; x \equiv_\vartheta 0,\; y \equiv_\vartheta z \right\} \;=\; \Lambda_{(p)} \\
E \;&\longmapsto\; (\,1\,, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, 0\,) \;=\; e \\
F \;&\longmapsto\; (\,0\,, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 1\,) \;=\; f \\
\alpha \;&\longmapsto\; (\,0\,, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, 0\,) \;=\; a \\
\beta \;&\longmapsto\; (\,0\,, \begin{pmatrix} 0 & 0 \\ \vartheta & 0 \end{pmatrix}, 0\,) \;=\; b\,.
\end{aligned}$$

Using (1) we get the Peirce decomposition of $\Lambda_{(p)}$

$$\Lambda_{(p)} \;=\; e\Lambda_{(p)}e \oplus f\Lambda_{(p)}f \oplus f\Lambda_{(p)}e \oplus e\Lambda_{(p)}f\,. \tag{2}$$

We want to show that $\hat{\psi}$ is surjective. By (2) it suffices to show that $\hat{\psi}$ is surjective on each direct summand. We have

$$\begin{aligned}
\text{(S1)} \qquad e\Lambda_{(p)}e \;&=\; \left\{ (\,u\,, \begin{pmatrix} v & 0 \\ 0 & 0 \end{pmatrix}, 0\,) \in \mathbb{Z}_{(p)} \times \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{2\times 2} \times \mathbb{Z}_{(p)} \;:\; u \equiv_\vartheta v \right\} \\
\text{(S2)} \qquad f\Lambda_{(p)}f \;&=\; \left\{ (\,0\,, \begin{pmatrix} 0 & 0 \\ 0 & y \end{pmatrix}, z\,) \in \mathbb{Z}_{(p)} \times \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{2\times 2} \times \mathbb{Z}_{(p)} \;:\; y \equiv_\vartheta z \right\} \\
\text{(S3)} \qquad f\Lambda_{(p)}e \;&=\; \left\{ (\,0\,, \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}, 0\,) \in \mathbb{Z}_{(p)} \times \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{2\times 2} \times \mathbb{Z}_{(p)} \;:\; x \equiv_\vartheta 0 \right\} \\
\text{(S4)} \qquad e\Lambda_{(p)}f \;&=\; \left\{ (\,0\,, \begin{pmatrix} 0 & w \\ 0 & 0 \end{pmatrix}, 0\,) \in \mathbb{Z}_{(p)} \times \left(\mathbb{Z}_{(p)}[\vartheta]\right)^{2\times 2} \times \mathbb{Z}_{(p)} \right\}
\end{aligned}$$

We claim that

$$\begin{aligned}
\text{(C1)} \qquad e\Lambda_{(p)}e \;&\stackrel{!}{=}\; \left\langle e,\, (ab)^1,\, (ab)^2,\, \ldots,\, (ab)^{n-1},\, (ab)^n \right\rangle_{\mathbb{Z}_{(p)}} \\
\text{(C2)} \qquad f\Lambda_{(p)}f \;&\stackrel{!}{=}\; \left\langle f,\, (ba)^1,\, (ba)^2,\, \ldots,\, (ba)^{n-1},\, (ba)^n \right\rangle_{\mathbb{Z}_{(p)}} \\
\text{(C3)} \qquad f\Lambda_{(p)}e \;&\stackrel{!}{=}\; \left\langle b,\, b(ab)^1,\, b(ab)^2,\, \ldots,\, b(ab)^{n-2},\, b(ab)^{n-1} \right\rangle_{\mathbb{Z}_{(p)}} \\
\text{(C4)} \qquad e\Lambda_{(p)}f \;&\stackrel{!}{=}\; \left\langle a,\, a(ba)^1,\, a(ba)^2,\, \ldots,\, a(ba)^{n-2},\, a(ba)^{n-1} \right\rangle_{\mathbb{Z}_{(p)}}
\end{aligned}$$

Once this is shown, we have that $\hat{\psi}$ is surjective since each of the listed $\mathbb{Z}_{(p)}$-linear generators is in the image of $\hat{\psi}$.

$\mathbb{Z}_{(p)}[\vartheta]$ has the $\mathbb{Z}_{(p)}$-linear basis $(\,\vartheta^k \;:\; k \in [0, n-1]\,)$; cf. Lemma 24 *(i3)*. So $\vartheta\mathbb{Z}_{(p)}[\vartheta]$ has the $\mathbb{Z}_{(p)}$-linear basis $(\,\vartheta^k \;:\; k \in [1, n]\,)$. (3)

Ad (C1). We have

$$a \cdot b = (\,0\,, \begin{pmatrix} \vartheta & 0 \\ 0 & 0 \end{pmatrix}, 0\,)\,, \text{ whence } (ab)^k = (\,0\,, \begin{pmatrix} \vartheta^k & 0 \\ 0 & 0 \end{pmatrix}, 0\,) \text{ for } k \in [1, n]. \tag{4}$$

Considering (S1) we therefore see that the right side in (C1) is contained in the left.

Suppose given $(\,u\,,\begin{pmatrix} v & 0 \\ 0 & 0 \end{pmatrix},\,0\,) \in e\Lambda_{(p)}e$, so that $u \equiv_\vartheta v$; cf. (S1). By subtraction of a $\mathbb{Z}_{(p)}$-multiple of e we can set u to 0, whence $v \equiv_\vartheta 0$. Using (3) and (4) we can set v to 0, whence the claim (C1) is shown.

Ad (C2). We have

$$(4') \qquad b \cdot a = (\,0\,,\begin{pmatrix} 0 & 0 \\ 0 & \vartheta \end{pmatrix},\,0\,)\,,\ \text{whence}\ (ba)^k = (\,0\,,\begin{pmatrix} 0 & 0 \\ 0 & \vartheta^k \end{pmatrix},\,0\,)\ \text{for}\ k \in [1,n],$$

and so the proof is analogous to the proof of (C1).

Ad (C3). By (4) we get

$$(5) \qquad b(ab)^k = (\,0\,,\begin{pmatrix} 0 & 0 \\ \vartheta^{k+1} & 0 \end{pmatrix},\,0\,)\ \text{for}\ k \in [0,n-1].$$

Considering (S3) we therefore see that the right side in (C3) is contained in the left.

Suppose given $(\,0\,,\begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix},\,0\,) \in f\Lambda_{(p)}e$, so that $x \equiv_\vartheta 0$; cf. (S3). Using (3) and (5) we can set x to 0, whence the claim (C3) is shown.

Ad (C4). By (4′) we get

$$(5') \qquad a(ba)^k = (\,0\,,\begin{pmatrix} 0 & \vartheta^k \\ 0 & 0 \end{pmatrix},\,0\,)\ \text{for}\ k \in [0,n-1].$$

Suppose given $(\,0\,,\begin{pmatrix} 0 & w \\ 0 & 0 \end{pmatrix},\,0\,) \in f\Lambda_{(p)}e$, so that $w \in \mathbb{Z}_{(p)}[\vartheta]$; cf. (S4). Using (3) and (5′) we can set w to 0, whence the claim (C4) is shown.

So we have that $\hat{\psi}$ is surjective.

We want to show that $I \overset{!}{\subseteq} \ker\hat{\psi}$. We write

$$(6) \qquad \mu_{\vartheta,\mathbb{Q}}(X) = X^n + \sum_{j=0}^{n-1} c_j X^j \in \mathbb{Z}[X]\,,$$

cf. Lemma 24 *(i2)*.

Then we have

$$\begin{aligned}
\hat{\psi}\,(\mu_{\vartheta,\mathbb{Q}}(\alpha\beta)\cdot\alpha) \;&=\; \hat{\psi}\Big(\big((\alpha\beta)^n + \sum_{j=0}^{n-1} c_j(\alpha\beta)^j\big)\cdot\alpha\Big) \\
=\;& \Big((ab)^n + \sum_{j=0}^{n-1} c_j(ab)^j\Big)\cdot a \;=\; \Big((ab)^n + \sum_{j=1}^{n-1} c_j(ab)^j\Big)\cdot a + c_0\cdot a \\
\overset{(4)}{=}\;& \Big((\,0\,,\begin{pmatrix} \vartheta^n & 0 \\ 0 & 0 \end{pmatrix},\,0\,) + \sum_{j=1}^{n-1} c_j\cdot(\,0\,,\begin{pmatrix} \vartheta^j & 0 \\ 0 & 0 \end{pmatrix},\,0)\Big)\cdot(\,0\,,\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\,0\,) + c_0\cdot(\,0\,,\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\,0\,) \\
=\;& (\,0\,,\begin{pmatrix} 0 & \vartheta^n \\ 0 & 0 \end{pmatrix},\,0\,) + \sum_{j=1}^{n-1} c_j\cdot(\,0\,,\begin{pmatrix} 0 & \vartheta^j \\ 0 & 0 \end{pmatrix},\,0\,) + c_0\cdot(\,0\,,\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\,0\,) \\
=\;& (\,0\,,\begin{pmatrix} 0 & \mu_{\vartheta,\mathbb{Q}}(\vartheta) \\ 0 & 0 \end{pmatrix},\,0\,) \;=\; (\,0\,,\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\,0\,) \;=\; 0_{\Lambda_{(p)}}\,.
\end{aligned}$$

Similarly, we have that $\hat{\psi}\,(\mu_{\vartheta,\mathbb{Q}}(\beta\alpha)\beta) = 0_{\Lambda_{(p)}}$. Therefore we have that $I \subseteq \ker(\hat{\psi})$; cf. Notation 82.

So there exists a unique $\mathbb{Z}_{(p)}$-algebra morphism that maps

$$\begin{aligned}
\psi \;:\; {}^{\mathbb{Z}_{(p)}\Xi}\!/_{I} \;&\longrightarrow\; \Big\{ (\,u\,,\begin{pmatrix} v & w \\ x & y \end{pmatrix},\, z\,) \in \mathbb{Z}_{(p)} \times \big(\mathbb{Z}_{(p)}[\vartheta]\big)^{2\times 2} \times \mathbb{Z}_{(p)} \;:\; u \equiv_\vartheta v,\; x \equiv_\vartheta 0,\; y \equiv_\vartheta z \Big\} \;=\; \Lambda_{(p)} \\
E+I \;&\longmapsto\; (\,1\,,\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\, 0\,) \;=\; e \\
F+I \;&\longmapsto\; (\,0\,,\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},\, 1\,) \;=\; f \\
\alpha+I \;&\longmapsto\; (\,0\,,\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\, 0\,) \;=\; a \\
\beta+I \;&\longmapsto\; (\,0\,,\begin{pmatrix} 0 & 0 \\ \vartheta & 0 \end{pmatrix},\, 0\,) \;=\; b\,.
\end{aligned}$$

I.e. $\psi \circ \rho = \hat{\psi}$, where ρ denotes the residue class map $\rho : \mathbb{Z}_{(p)}\Xi \longrightarrow {}^{\mathbb{Z}_{(p)}\Xi}\!/_{I} : \kappa \longmapsto \kappa + I$. Since $\hat{\psi}$ is surjective, so is ψ.

For $k \in \mathbb{Z}_{\geq 0}$ we denote by G_k the $\mathbb{Z}_{(p)}$-linear span of residue classes of paths in Ξ of length less than or equal to k, i.e.

$$\begin{aligned}
G_0 \;&=\; \langle\, E+I\,,\, F+I \,\rangle_{\mathbb{Z}_{(p)}}\,, \\
G_1 \;&=\; \langle\, E+I\,,\, F+I\,,\, \alpha+I\,,\, \beta+I \,\rangle_{\mathbb{Z}_{(p)}}\,, \\
G_2 \;&=\; \langle\, E+I\,,\, F+I\,,\, \alpha+I\,,\, \beta+I\,,\, \alpha\beta+I\,,\, \beta\alpha+I \,\rangle_{\mathbb{Z}_{(p)}}\,, \\
G_3 \;&=\; \langle\, E+I\,,\, F+I\,,\, \alpha+I\,,\, \beta+I\,,\, \alpha\beta+I\,,\, \beta\alpha+I\,,\, \alpha\beta\alpha+I\,,\, \beta\alpha\beta+I \,\rangle_{\mathbb{Z}_{(p)}}\,, \\
&\;\;\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots
\end{aligned} \tag{7}$$

et cetera. Note that the number of $\mathbb{Z}_{(p)}$-linear generators given for G_s is $2s+2$ for $s \in \mathbb{Z}_{\geq 0}$. In particular, for G_{2n} this number equals $2 \cdot 2n + 2 = 2p$.

Since $G_r \subseteq G_s$ for $r \leq s$ we get that

$$ {}^{\mathbb{Z}_{(p)}\Xi}\!/_{I} \;=\; \bigcup_{k \geq 0} G_k\,. \tag{8}$$

For $s \geq n$ we have

$$(\alpha\beta)^s\alpha + I \;=\; \underbrace{(\alpha\beta)^{s-n}\left(-\sum_{j=0}^{n-1} c_j(\alpha\beta)^j\alpha\right) + I}_{\in\, G_{2s-1} \subseteq G_{2s}} \quad\text{and}\quad (\beta\alpha)^s\beta + I \;=\; \underbrace{(\beta\alpha)^{s-n}\left(-\sum_{j=0}^{n-1} c_j(\beta\alpha)^j\beta\right) + I}_{\in\, G_{2s-1} \subseteq G_{2s}}\,,$$

cf. Notation 82 and (6). Therefore we have $G_{2s+1} \subseteq G_{2s}$ for $s \geq n$.

For $s \geq n$ we have

$$(\alpha\beta)^{s+1} + I \;=\; \underbrace{(\alpha\beta)^{s-n}\left(-\sum_{j=0}^{n-1} c_j(\alpha\beta)^j\alpha\right)\beta + I}_{\in\, G_{2s} \subseteq G_{2s+1}} \quad\text{and}\quad (\beta\alpha)^{s+1} + I \;=\; \underbrace{(\beta\alpha)^{s-n}\left(-\sum_{j=0}^{n-1} c_j(\beta\alpha)^j\beta\right)\alpha + I}_{\in\, G_{2s} \subseteq G_{2s+1}}\,,$$

cf. Notation 82 and (6). Therefore we have $G_{2s+2} \subseteq G_{2s+1}$ for $s \geq n$.

Together this shows that $G_t = G_{2n}$ for $t \geq 2n$, so that (8) becomes ${}^{\mathbb{Z}_{(p)}\Xi}\!/_{I} = G_{2n}$.

So there exists a surjective $\mathbb{Z}_{(p)}$-linear map $\varphi : (\mathbb{Z}_{(p)})^{\times 2p} \longrightarrow {}^{\mathbb{Z}_{(p)}\Xi}\!/_{I}$, which maps the standard basis of $(\mathbb{Z}_{(p)})^{\times 2p}$ to the $\mathbb{Z}_{(p)}$-linear generating tuple of $G_{2n} = {}^{\mathbb{Z}_{(p)}\Xi}\!/_{I}$ mentioned above.

Note that $\mathrm{rk}_{\mathbb{Z}_{(p)}}(\Lambda_{(p)}) = \mathrm{rk}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_{(p)}\mathrm{D}_{2p}) = 2p$; cf. Corollary 71.

We have surjective $\mathbb{Z}_{(p)}$-linear maps

$$(\mathbb{Z}_{(p)})^{\times 2p} \xrightarrow[\text{surj.}]{\varphi} \mathbb{Z}_{(p)}\Xi/_I \xrightarrow[\text{surj.}]{\psi} \Lambda_{(p)}$$

The composite $\psi \circ \varphi$ is bijective, since $\mathrm{rk}_{\mathbb{Z}_{(p)}}(\ker(\psi \circ \varphi)) = \mathrm{rk}_{\mathbb{Z}_{(p)}}((\mathbb{Z}_{(p)})^{\times 2p}) - \mathrm{rk}_{\mathbb{Z}_{(p)}}(\Lambda_{(p)}) = 2p - 2p = 0$.

So φ is injective, hence bijective. Since $\psi \circ \varphi$ and φ are bijective, so is ψ.

Altogether ψ is the asserted isomorphism of $\mathbb{Z}_{(p)}$-algebras, which we rename to $\mathcal{P}_1 := \psi$. □

Proposition 84 *We have the isomorphism of $\mathbb{Z}_{(p)}$-algebras*

$$\begin{aligned}
\mathcal{P}_2 \;:\quad \mathbb{Z}_{(p)}\Xi/_I \quad &\xrightarrow{\sim} \quad \mathbb{Z}_{(p)}\mathrm{D}_{2p} \\
\overline{E} = E + I \quad &\longmapsto \quad \frac{1}{2}\sum_{k=0}^{p-1} (-1)^k x^k (1+y) \quad =:\; e' \\
\overline{F} = F + I \quad &\longmapsto \quad \frac{1}{2}\left(1 - y - \sum_{k=1}^{p-1} (-1)^k x^k (1+y)\right) \quad =:\; f' \\
\overline{\alpha} = \alpha + I \quad &\longmapsto \quad -x^{-1} - y - \sum_{k=1}^{p-2} (-1)^k x^k (1+y) \quad =:\; a' \\
\overline{\beta} = \beta + I \quad &\longmapsto \quad -\sum_{k=1}^{p-1} (-1)^k x^k (1+y) \quad =:\; b' \,,
\end{aligned}$$

where x and y denote the generators of D_{2p} given in Definition 54. *For the factor algebra of the path algebra, cf.* Notations 81, 82.

Proof. By Corollary 71 we have the isomorphism of $\mathbb{Z}_{(p)}$-algebras

$$\begin{aligned}
\omega_{\mathbb{Z}_{(p)}} \;:\quad \mathbb{Z}_{(p)}\mathrm{D}_{2p} \quad &\xrightarrow{\sim} \quad \Lambda_{(p)} \\
\sum_{d \in \mathrm{D}_{2p}} q_d \cdot d \quad &\longmapsto \quad \sum_{d \in \mathrm{D}_{2p}} q_d \cdot \omega_{\mathbb{Z}}(d) \,,
\end{aligned}$$

where $q_d \in \mathbb{Z}_{(p)}$ for $d \in \mathrm{D}_{2p}$. For $\omega_{\mathbb{Z}}$ we refer to Theorem 70.

By Proposition 83 we have the isomorphism of $\mathbb{Z}_{(p)}$-algebras $\mathcal{P}_1 : \mathbb{Z}_{(p)}\Xi/_I \xrightarrow{\sim} \Lambda_{(p)}$. Therefore it suffices to show that

$$\left.\begin{aligned}
(\omega^{-1}_{\mathbb{Z}_{(p)}} \circ \mathcal{P}_1)(E+I) = \omega^{-1}_{\mathbb{Z}_{(p)}}(e) \overset{!}{=} e' \quad &\Longleftrightarrow \quad \omega_{\mathbb{Z}_{(p)}}(e') \overset{!}{=} e \\
(\omega^{-1}_{\mathbb{Z}_{(p)}} \circ \mathcal{P}_1)(F+I) = \omega^{-1}_{\mathbb{Z}_{(p)}}(f) \overset{!}{=} f' \quad &\Longleftrightarrow \quad \omega_{\mathbb{Z}_{(p)}}(f') \overset{!}{=} f \\
(\omega^{-1}_{\mathbb{Z}_{(p)}} \circ \mathcal{P}_1)(\alpha+I) = \omega^{-1}_{\mathbb{Z}_{(p)}}(a) \overset{!}{=} a' \quad &\Longleftrightarrow \quad \omega_{\mathbb{Z}_{(p)}}(a') \overset{!}{=} a \\
(\omega^{-1}_{\mathbb{Z}_{(p)}} \circ \mathcal{P}_1)(\beta+I) = \omega^{-1}_{\mathbb{Z}_{(p)}}(b) \overset{!}{=} b' \quad &\Longleftrightarrow \quad \omega_{\mathbb{Z}_{(p)}}(b') \overset{!}{=} b \,,
\end{aligned}\right\} (1)$$

because then $\omega^{-1}_{\mathbb{Z}_{(p)}} \circ \mathcal{P}_1$ is the asserted isomorphism of $\mathbb{Z}_{(p)}$-algebras $\mathcal{P}_2$.

To show this we make two preparations. We have

$$\left.\begin{array}{rcl} \sum_{k=1}^{p-1}(-1)^k\left(\zeta^k+\zeta^{-k}\right) &=& \sum_{k=1}^{p-1}(-1)^k\zeta^k+\sum_{k=1}^{p-1}(-1)^k\zeta^{-k} \;=\; \sum_{k=1}^{p-1}(-1)^k\zeta^k+\sum_{k=1}^{p-1}(-1)^k\zeta^{p-k} \\ &\overset{\text{subst.}}{\underset{k'=p-k}{=}}& \sum_{k=1}^{p-1}(-1)^k\zeta^k+\sum_{k'=1}^{p-1}(-1)^{p-k'}\zeta^{k'} \;=\; \sum_{k=1}^{p-1}(-1)^k\zeta^k-\sum_{k'=1}^{p-1}(-1)^{k'}\zeta^{k'} \;=\; 0\,, \end{array}\right\} (2)$$

and

$$\left.\begin{array}{rl} & \sum_{k=0}^{p-1}(-1)^k\left(\zeta^{k+1}-\zeta^k+\zeta^{-(k+1)}-\zeta^{-k}\right) \\ = & -\sum_{k=0}^{p-1}(-1)^k\left(\zeta^k+\zeta^{-k}\right)+\sum_{k=0}^{p-1}(-1)^k\left(\zeta^{k+1}+\zeta^{-(k+1)}\right) \\ \overset{\text{(2) and subst.}}{\underset{k'=k+1}{=}} & -2-\sum_{k'=1}^{p}(-1)^{k'}\left(\zeta^{k'}+\zeta^{-k'}\right) \overset{(2)}{=} -2+2 \;=\; 0\,. \end{array}\right\} (3)$$

We have

$$\begin{aligned} \omega_{\mathbb{Z}_{(p)}}(e') &= \omega_{\mathbb{Z}_{(p)}}\Big(\tfrac{1}{2}\sum_{k=0}^{p-1}(-1)^k x^k(1+y)\Big) \;=\; \tfrac{1}{2}\sum_{k=0}^{p-1}(-1)^k\cdot\omega_{\mathbb{Z}_{(p)}}(x)^k\cdot\omega_{\mathbb{Z}_{(p)}}(1+y) \\ &= \tfrac{1}{2}\sum_{k=0}^{p-1}(-1)^k\cdot(1,M_1^k,1)\cdot\big((1,\mathrm{E}_2,1)+(1,N_1,-1)\big) \;=\; \tfrac{1}{2}\sum_{k=0}^{p-1}(-1)^k\cdot(1,M_1^k,1)\cdot(2,\mathrm{E}_2+N_1,0) \\ &= \tfrac{1}{2}\sum_{k=0}^{p-1}(-1)^k\cdot(2,M_1^k(\mathrm{E}_2+N_1),0) \overset{\text{R.57}}{\underset{(iv)}{=}} \tfrac{1}{2}\sum_{k=0}^{p-1}(-1)^k\cdot\Big(2,\begin{pmatrix}\zeta^k+\zeta^{-k} & 0\\ \zeta^{k+1}-\zeta^k+\zeta^{-(k+1)}-\zeta^{-k} & 0\end{pmatrix},0\Big) \\ &= \Big(1,\begin{pmatrix}\frac{1}{2}\sum_{k=0}^{p-1}(-1)^k\left(\zeta^k+\zeta^{-k}\right) & 0\\ \frac{1}{2}\sum_{k=0}^{p-1}(-1)^k\left(\zeta^{k+1}-\zeta^k+\zeta^{-(k+1)}-\zeta^{-k}\right) & 0\end{pmatrix},0\Big) \overset{(2)}{\underset{(3)}{=}} \Big(1,\begin{pmatrix}1&0\\0&0\end{pmatrix},0\Big) \;=\; e\,, \end{aligned}$$

$$\begin{aligned} \omega_{\mathbb{Z}_{(p)}}(f') &= \omega_{\mathbb{Z}_{(p)}}\Big(\tfrac{1}{2}\Big(1-y-\sum_{k=1}^{p-1}(-1)^k x^k(1+y)\Big)\Big) \;=\; \omega_{\mathbb{Z}_{(p)}}\Big(\tfrac{1}{2}\Big(1-y-2e'+(-1)^0x^0(1+y)\Big)\Big) \\ &= \omega_{\mathbb{Z}_{(p)}}(1-e') \;=\; \omega_{\mathbb{Z}_{(p)}}(1)-\underbrace{\omega_{\mathbb{Z}_{(p)}}(e')}_{=e} \;=\; \Big(1,\begin{pmatrix}1&0\\0&1\end{pmatrix},1\Big)-\Big(1,\begin{pmatrix}1&0\\0&0\end{pmatrix},0\Big) \\ &= \Big(0,\begin{pmatrix}0&0\\0&1\end{pmatrix},1\Big) \;=\; f\,, \end{aligned}$$

$$\begin{aligned} \omega_{\mathbb{Z}_{(p)}}(a') &= \omega_{\mathbb{Z}_{(p)}}\Big(-x^{-1}-y-\sum_{k=1}^{p-2}(-1)^k x^k(1+y)\Big) \\ &= \omega_{\mathbb{Z}_{(p)}}\big(-x^{-1}-y-2e'+(-1)^0x^0(1+y)+(-1)^{p-1}x^{p-1}(1+y)\big) \\ &= \omega_{\mathbb{Z}_{(p)}}\big(x^{-1}y+1-2e'\big) \;=\; \omega_{\mathbb{Z}_{(p)}}(x)^{-1}\cdot\omega_{\mathbb{Z}_{(p)}}(y)+\omega_{\mathbb{Z}_{(p)}}(1-2e') \\ &= (1,M_1^{-1},1)\cdot(1,N_1,-1)+\omega_{\mathbb{Z}_{(p)}}(1-2e') \\ &\overset{\text{R.57}\,(iii)}{\underset{\text{D.56}}{=}} \Big(1,\begin{pmatrix}\vartheta+1&-1\\-\vartheta&1\end{pmatrix},1\Big)\cdot\Big(1,\begin{pmatrix}1&0\\\vartheta&-1\end{pmatrix},-1\Big)+\omega_{\mathbb{Z}_{(p)}}(1-2e') \\ &= \Big(1,\begin{pmatrix}1&1\\0&-1\end{pmatrix},-1\Big)+\Big(-1,\begin{pmatrix}-1&0\\0&1\end{pmatrix},1\Big) \;=\; \Big(0,\begin{pmatrix}0&1\\0&0\end{pmatrix},0\Big) \;=\; a\,, \end{aligned}$$

and

$$\begin{aligned}\omega_{\mathbb{Z}_{(p)}}(b') &= \omega_{\mathbb{Z}_{(p)}}\Big(-\sum_{k=1}^{p-1}(-1)^k x^k(1+y)\Big) = \omega_{\mathbb{Z}_{(p)}}(-2e'+(-1)^0x^0(1+y))\\ &= \omega_{\mathbb{Z}_{(p)}}(y)+\omega_{\mathbb{Z}_{(p)}}(1-2e') = (1,N_1,-1)+\omega_{\mathbb{Z}_{(p)}}(1-2e')\\ &\overset{\text{D.56}}{=} (1,\begin{pmatrix}1&0\\ \vartheta&-1\end{pmatrix},-1)+(-1,\begin{pmatrix}-1&0\\0&1\end{pmatrix},1) = (0,\begin{pmatrix}0&0\\ \vartheta&0\end{pmatrix},0) = b\,.\end{aligned}$$

Hence all equations in (1) hold. □

Proposition 85 *We have the isomorphism of $\mathbb{Z}_{(p)}$-algebras*

$$\begin{aligned}\mathcal{P}_3 : \mathbb{Z}_{(p)}\mathrm{D}_{2p} &\xrightarrow{\sim} \mathbb{Z}_{(p)}\Xi/_I\\ x &\longmapsto \overline{E}+\overline{F}+\overline{\alpha}+\overline{\beta}+\overline{\beta\alpha}\,,\\ y &\longmapsto \overline{E}-\overline{F}+\overline{\beta}\,,\end{aligned}$$

where x and y denote the generators of D_{2p} given in Definition 54. *For the factor algebra of the path algebra, cf.* Notations 81, 82.

Proof. By Corollary 71 we have the isomorphism of $\mathbb{Z}_{(p)}$-algebras

$$\begin{aligned}\omega_{\mathbb{Z}_{(p)}} : \mathbb{Z}_{(p)}\mathrm{D}_{2p} &\xrightarrow{\sim} \Lambda_{(p)}\\ \sum_{d\in\mathrm{D}_{2p}} q_d\cdot d &\longmapsto \sum_{d\in\mathrm{D}_{2p}} q_d\cdot\omega_{\mathbb{Z}}(d)\,,\end{aligned}$$

where $q_d\in\mathbb{Z}_{(p)}$ for $d\in\mathrm{D}_{2p}$. For $\omega_{\mathbb{Z}}$ we refer to Theorem 70.

By Proposition 83 we have the isomorphism of $\mathbb{Z}_{(p)}$-algebras $\mathcal{P}_1 : {}^{\mathbb{Z}_{(p)}\Xi}/_I \xrightarrow{\sim} \Lambda_{(p)}$. Therefore it suffices to show that

$$\mathcal{P}_1^{-1}(\omega_{\mathbb{Z}_{(p)}}(x)) = \mathcal{P}_1^{-1}(\omega_{\mathbb{Z}}(x)) \overset{!}{=} \overline{E}+\overline{F}+\overline{\alpha}+\overline{\beta}+\overline{\beta\alpha} \iff \mathcal{P}_1\big(\overline{E}+\overline{F}+\overline{\alpha}+\overline{\beta}+\overline{\beta\alpha}\big) \overset{!}{=} \omega_{\mathbb{Z}}(x)$$

$$\mathcal{P}_1^{-1}(\omega_{\mathbb{Z}_{(p)}}(y)) = \mathcal{P}_1^{-1}(\omega_{\mathbb{Z}}(y)) \overset{!}{=} \overline{E}-\overline{F}+\overline{\beta} \iff \mathcal{P}_1\big(\overline{E}-\overline{F}+\overline{\beta}\big) \overset{!}{=} \omega_{\mathbb{Z}}(y)\,,$$

because then $\mathcal{P}_1^{-1}\circ\omega_{\mathbb{Z}_{(p)}}$ is the asserted isomorphism of $\mathbb{Z}_{(p)}$-algebras $\mathcal{P}_3$.

We have

$$\begin{aligned}\mathcal{P}_1\big(\overline{E}+\overline{F}+\overline{\alpha}+\overline{\beta}+\overline{\beta\alpha}\big) &= \mathcal{P}_1\big(\overline{E}\big)+\mathcal{P}_1\big(\overline{F}\big)+\mathcal{P}_1(\overline{\alpha})+\mathcal{P}_1\big(\overline{\beta}\big)+\mathcal{P}_1\big(\overline{\beta}\big)\cdot\mathcal{P}_1(\overline{\alpha})\\ &\overset{\text{P.83}}{=} (1,\begin{pmatrix}1&0\\0&0\end{pmatrix},0)+(0,\begin{pmatrix}0&0\\0&1\end{pmatrix},1)+(0,\begin{pmatrix}0&1\\0&0\end{pmatrix},0)\\ &\quad+(0,\begin{pmatrix}0&0\\ \vartheta&0\end{pmatrix},0)+(0,\begin{pmatrix}0&0\\ \vartheta&0\end{pmatrix},0)\cdot(0,\begin{pmatrix}0&1\\0&0\end{pmatrix},0)\\ &= (1,\begin{pmatrix}1&1\\0&1\end{pmatrix},1)+(0,\begin{pmatrix}0&0\\ \vartheta&\vartheta\end{pmatrix},0) = (1,\begin{pmatrix}1&1\\ \vartheta&\vartheta+1\end{pmatrix},1) \overset{\text{T.70}}{=} \omega_{\mathbb{Z}}(x)\,,\end{aligned}$$

and

$$\mathcal{P}_1\big(\overline{E}-\overline{F}+\overline{\beta}\,\big) = \mathcal{P}_1\big(\overline{E}\big)-\mathcal{P}_1\big(\overline{F}\big)+\mathcal{P}_1\big(\overline{\beta}\big)$$
$$\overset{\text{P.83}}{=} (1,\begin{pmatrix}1&0\\0&0\end{pmatrix},0)-(0,\begin{pmatrix}0&0\\0&1\end{pmatrix},1)+(0,\begin{pmatrix}0&0\\\vartheta&0\end{pmatrix},0) = (1,\begin{pmatrix}1&0\\\vartheta&-1\end{pmatrix},-1) \overset{\text{T.70}}{=} \omega_{\mathbb{Z}}(y)\,.$$

□

Remark 86 *The isomorphisms of $\mathbb{Z}_{(p)}$-algebras $\mathcal{P}_2$ and $\mathcal{P}_3$ invert each other, cf.* Propositions 84, 85.

Proof.
By construction, we have $\mathcal{P}_2 = \omega_{\mathbb{Z}_{(p)}}^{-1} \circ \mathcal{P}_1$ and $\mathcal{P}_3 = \mathcal{P}_1^{-1} \circ \omega_{\mathbb{Z}_{(p)}}$, cf. pfs. of Propositions 84, 85. □

6.2 Presentation of $\mathbb{F}_p\mathrm{D}_{2p}$ by quiver and relations

Lemma 87 *We consider the minimal polynomial $\mu_{\vartheta_p,\mathbb{Q}}(X) \in \mathbb{Z}[X]$ of ϑ_p over $\mathbb{Q}$.*

We have

$$\mu_{\vartheta_p,\mathbb{Q}}(X) \equiv_p X^n \quad \text{in } \mathbb{Z}[X]\,.$$

In particular, $\mu_{\vartheta_p,\mathbb{Q}}(X)$ is Eisenstein at p, cf. Lemma 24 *(iv).*

Proof. We write

$$\mu_{\vartheta,\mathbb{Q}}(X) = X^n + \left(\sum_{j=1}^{n-1} a_j X^j\right) + p \in \mathbb{Z}[X] \subseteq \mathbb{Z}_{(p)}[X]\,,$$

cf. Lemma 24 *(iv)*. So we have

$$\mathbb{Z}_{(p)}[\vartheta] \ni \mu_{\vartheta,\mathbb{Q}}(\vartheta) = \vartheta^n + \left(\sum_{j=1}^{n-1} a_j \vartheta^j\right) + p = 0\,. \tag{1}$$

By Remark 46 *(iii, iv)* we have that $\mathbb{Z}_{(p)}[\vartheta]$ is a discrete valuation ring and its maximal ideal is generated by ϑ. So we have a valuation $\mathrm{v}_\vartheta : \mathbb{Z}_{(p)}[\vartheta] \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ as in Remark 130 at our disposal.

We **assume** that there exists $i \in [1, n-1]$ with $p \nmid a_i$ in $\mathbb{Z}$, i.e. $p \nmid a_i$ in $\mathbb{Z}_{(p)}$.

Let i be minimal with this property. $(*)$

Then we have that $a_i \in \mathrm{U}(\mathbb{Z}_{(p)}) \subseteq \mathrm{U}(\mathbb{Z}_{(p)}[\vartheta])$, so that

$$\mathrm{v}_\vartheta\big(a_i\vartheta^i\big) = \underbrace{\mathrm{v}_\vartheta(a_i)}_{=0} + i = i\,.$$

By Lemma 29 we have that there exists $e \in \mathrm{U}(\mathbb{Z}[\vartheta]) \subseteq \mathrm{U}(\mathbb{Z}_{(p)}[\vartheta])$ with $p = e\vartheta^n$ $(**)$

By $(*)$ we obtain for $j \in [1, i-1]$ that $\frac{a_j}{p} \in \mathbb{Z}_{(p)}$, so that

$$\mathrm{v}_\vartheta\big(a_j\vartheta^j\big) = \mathrm{v}_\vartheta(a_j) + j = \mathrm{v}_\vartheta\Big(p\frac{a_j}{p}\Big) + j = \mathrm{v}_\vartheta(p) + \mathrm{v}_\vartheta\Big(\frac{a_j}{p}\Big) + j \overset{(**)}{=} \mathrm{v}_\vartheta(e\vartheta^n) + \mathrm{v}_\vartheta\Big(\frac{a_j}{p}\Big) + j \geq n + j \geq n > i\,.$$

For $j \in [i+1, n-1]$ we have

$$\mathrm{v}_\vartheta\big(a_j\vartheta^j\big) \geq \mathrm{v}_\vartheta(\vartheta^j) = j > i\,.$$

Hence we obtain on the one hand

$$\mathrm{v}_\vartheta\big(\vartheta^n + \cdots + a_i\vartheta^i + \cdots + a_1\vartheta^1\big) = \mathrm{v}_\vartheta\Big(\big(\underbrace{\vartheta^n + \cdots + a_{i+1}\vartheta^{i+1} + a_{i-1}\vartheta^{i-1} + \cdots + a_1\vartheta^1}_{\mathrm{v}_\vartheta(\,)>i}\big) + \underbrace{a_i\vartheta^i}_{\mathrm{v}_\vartheta(\,)=i}\Big) = i\,.$$

On the other hand we have

$$\mathrm{v}_\vartheta\big(\vartheta^n + \cdots + a_i\vartheta^i + \cdots + a_1\vartheta^1\big) \overset{(1)}{=} \mathrm{v}_\vartheta(-p) \overset{(**)}{=} \mathrm{v}_\vartheta(-e\vartheta^n) = n\,.$$

So we get $i = n$ in **contradiction** to $i \in [1, n-1]$. □

Notation 88 We denote by J the (both-sided) ideal of the path algebra $\mathbb{F}_p\Xi$ that is generated by the set $\big\{\,(\alpha\beta)^n\alpha\,,\,(\beta\alpha)^n\beta\,\big\}$.

Using Convention 10 this means

$$J := \lhd\,(\alpha\beta)^n\alpha\,,\,(\beta\alpha)^n\beta\,\rhd_{\mathbb{F}_p\Xi}\,.$$

Moreover, we denote the residue class of an element $\xi \in \mathbb{F}_p\Xi$ by

$$\overline{\overline{\xi}} := \xi + J \in {}^{\mathbb{F}_p\Xi}\big/_J\,.$$

We recover the following well-known description of $\mathbb{F}_p\mathrm{D}_{2p}$.

Lemma 89 *We have the isomorphism of $\mathbb{F}_p$-algebras*

$$\begin{aligned}
\mathcal{P}_4 \;:\quad \mathbb{F}_p\mathrm{D}_{2p} &\xrightarrow{\sim} \mathbb{F}_p\Xi\big/_J \\
x &\longmapsto \overline{\overline{E}} + \overline{\overline{F}} + \overline{\overline{\alpha}} + \overline{\overline{\beta}} + \overline{\overline{\beta\alpha}}\,, \\
y &\longmapsto \overline{\overline{E}} - \overline{\overline{F}} + \overline{\overline{\beta}}\,.
\end{aligned}$$

Its inverse map is given by

$$\begin{aligned}
\mathcal{P}_5 \;:\quad \mathbb{F}_p\Xi\big/_J &\xrightarrow{\sim} \mathbb{F}_p\mathrm{D}_{2p} \\
\overline{\overline{E}} = E + J &\longmapsto (n+1)\sum_{k=0}^{p-1}(-1)^k x^k(1+y) \\
\overline{\overline{F}} = F + J &\longmapsto (n+1)\left(1 - y - \sum_{k=1}^{p-1}(-1)^k x^k(1+y)\right) \\
\overline{\overline{\alpha}} = \alpha + J &\longmapsto -x^{-1} - y - \sum_{k=1}^{p-2}(-1)^k x^k(1+y) \\
\overline{\overline{\beta}} = \beta + J &\longmapsto -\sum_{k=1}^{p-1}(-1)^k x^k(1+y)\,.
\end{aligned}$$

Here x and y denote the generators of D_{2p} given in Definition 54. *For the factor algebra of the path algebra cf.* Notations 81, 88.

Proof. We denote the residue class map by $r : \mathbb{Z}_{(p)} \longrightarrow {}^{\mathbb{Z}_{(p)}}\big/_{p\mathbb{Z}_{(p)}}, w \longmapsto w + p\mathbb{Z}_{(p)}$. By Corollary 127 we therefore obtain the surjective morphism of rings $\varphi := \varrho^{-1} \circ r : \mathbb{Z}_{(p)} \longrightarrow \mathbb{F}_p$. We have

$$\ker(\varphi) = \ker(\underbrace{\varrho^{-1}}_{\text{iso.}} \circ r) = \ker(r) = p\mathbb{Z}_{(p)}\,.$$

We apply Lemma 105 to the case $(R, S, \varphi, \mathfrak{a}) = (\,\mathbb{Z}_{(p)}\,,\,\mathbb{F}_p\,,\,\varphi\,,\,p\mathbb{Z}_{(p)}\,)$ and get the surjective morphism of rings

$$\begin{aligned}
\psi \;:\quad \mathbb{Z}_{(p)}\Xi &\longrightarrow \mathbb{F}_p\Xi \\
\sum_{m\in\mathrm{Path}(\Xi)} q_m m &\longmapsto \sum_{m\in\mathrm{Path}(\Xi)} \varphi(q_m)m\,,
\end{aligned}$$

where $q_m \in \mathbb{Z}_{(p)}$, and $q_m = 0$ for almost all $m \in \mathrm{Path}(\Xi)$.

The kernel of ψ is given as $\ker(\psi) = p\mathbb{Z}_{(p)}(\mathbb{Z}_{(p)}\Xi) = p\mathbb{Z}_{(p)}\Xi$.

We have

$$\left.\begin{aligned}
\psi(I) &\overset{\text{N.82}}{=} \psi\big(\lhd \mu_{\vartheta,\mathbb{Q}}(\alpha\beta)\alpha\,,\,\mu_{\vartheta,\mathbb{Q}}(\beta\alpha)\beta \rhd_{\mathbb{Z}_{(p)}\Xi}\big) \overset{\psi\text{ surj.}}{=} \lhd \psi\big(\mu_{\vartheta,\mathbb{Q}}(\alpha\beta)\alpha\big)\,,\,\psi\big(\mu_{\vartheta,\mathbb{Q}}(\beta\alpha)\beta\big) \rhd_{\mathbb{F}_p\Xi} \\
&\overset{\text{L.87}}{=} \lhd \psi\Big((\alpha\beta)^n\alpha + p\cdot\sum_{k=0}^{n-1} b_k(\alpha\beta)^k\alpha\Big)\,,\,\psi\Big((\beta\alpha)^n\beta + p\cdot\sum_{k=0}^{n-1} b_k(\beta\alpha)^k\beta\Big) \rhd_{\mathbb{F}_p\Xi} \\
&= \lhd \psi\big((\alpha\beta)^n\alpha\big) + p\cdot\psi\Big(\sum_{k=0}^{n-1} b_k(\alpha\beta)^k\alpha\Big)\,,\,\psi\big((\beta\alpha)^n\beta\big) + p\cdot\psi\Big(\sum_{k=0}^{n-1} b_k(\beta\alpha)^k\beta\Big) \rhd_{\mathbb{F}_p\Xi} \\
&= \lhd \psi\big((\alpha\beta)^n\alpha\big)\,,\,\psi\big((\beta\alpha)^n\beta\big) \rhd_{\mathbb{F}_p\Xi} = \lhd (\alpha\beta)^n\alpha\,,\,(\beta\alpha)^n\beta \rhd_{\mathbb{F}_p\Xi} \overset{\text{N.88}}{=} J\,,
\end{aligned}\right\}(*)$$

where $b_k \in \mathbb{Z}$ for $k \in [0, n-1]$.

We apply Lemma 106 to the case $(A, B, I, \psi, K) = (\,\mathbb{Z}_{(p)}\Xi\,,\,\mathbb{F}_p\Xi\,,\,I\,,\,\psi\,,\,p\mathbb{Z}_{(p)}\Xi\,)$ and obtain the short exact sequence of abelian groups

$$\begin{array}{ccccccc}
\ker(\phi) = \big(p\mathbb{Z}_{(p)}\Xi + I\big)/_I & \hookrightarrow & \mathbb{Z}_{(p)}\Xi/_I & \xrightarrow{\phi} & \mathbb{F}_p\Xi/_J & \overset{(*)}{=} & \mathbb{F}_p\Xi/_{\psi(I)} \\
a + I & \longmapsto & a + I & \longmapsto & \psi(a) + J\,, & & \\
 & & \| & & \| & & \\
 & & \overline{a} & & \overline{\overline{\psi(a)}} & &
\end{array}$$

where ϕ is even a morphism of rings.

Since $p \in \ker(\phi) = \big(p\mathbb{Z}_{(p)}\Xi + I\big)/_I$, we have $p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big) \subseteq \big(p\mathbb{Z}_{(p)}\Xi + I\big)/_I$.

Suppose given $p\xi + i + I \in \big(p\mathbb{Z}_{(p)}\Xi + I\big)/_I$, where $\xi \in \mathbb{Z}_{(p)}\Xi$ and $i \in I$.

Then we have $p\xi + i + I = p\xi + I = p(\xi + I) \in p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big)$, whence $\big(p\mathbb{Z}_{(p)}\Xi + I\big)/_I \subseteq p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big)$.

So we have $\big(p\mathbb{Z}_{(p)}\Xi + I\big)/_I = p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big)$ $\qquad (**)$

We apply Lemma 103 to the case $(R, S, G, \varphi, \mathfrak{a}) = (\,\mathbb{Z}_{(p)}\,,\,\mathbb{F}_p\,,\,\mathrm{D}_{2p}\,,\,\varphi\,,\,p\mathbb{Z}_{(p)}\,)$ and obtain the short exact sequence of abelian groups

$$\begin{array}{ccccccc}
p\mathbb{Z}_{(p)}(\mathbb{Z}_{(p)}\mathrm{D}_{2p}) = p\mathbb{Z}_{(p)}\mathrm{D}_{2p} & \hookrightarrow & \mathbb{Z}_{(p)}\mathrm{D}_{2p} & \xrightarrow{\tilde{\varphi}} & \mathbb{F}_p\mathrm{D}_{2p} & & \\
\sum\limits_{d\in\mathrm{D}_{2p}} r_d d & \longmapsto & \sum\limits_{d\in\mathrm{D}_{2p}} r_d d & \longmapsto & \sum\limits_{d\in\mathrm{D}_{2p}} \varphi(r_d)d\,, & &
\end{array}$$

where $\tilde{\varphi}$ is even a morphism of rings.

We consider the isomorphisms of $\mathbb{Z}_{(p)}$-algebras

$$\mathcal{P}_2 : \mathbb{Z}_{(p)}\Xi/_I \xrightarrow{\sim} \mathbb{Z}_{(p)}\mathrm{D}_{2p} \quad\text{and}\quad \mathcal{P}_3 : \mathbb{Z}_{(p)}\mathrm{D}_{2p} \xrightarrow{\sim} \mathbb{Z}_{(p)}\Xi/_I\,,$$

cf. Propositions 84, 85. We have

$$\mathcal{P}_2\Big(p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big)\Big) = p\cdot\mathcal{P}_2\Big(\mathbb{Z}_{(p)}\Xi/_I\Big) = p\mathbb{Z}_{(p)}\mathrm{D}_{2p} \quad\text{and}\quad \mathcal{P}_3\big(p\mathbb{Z}_{(p)}\mathrm{D}_{2p}\big) = p\cdot\mathcal{P}_3\big(\mathbb{Z}_{(p)}\mathrm{D}_{2p}\big) = p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big).$$

So the restrictions

$$\mathcal{P}_2' := \mathcal{P}_2\Big|^{p\mathbb{Z}_{(p)}\mathrm{D}_{2p}}_{p(\mathbb{Z}_{(p)}\Xi/I)} : p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big) \xrightarrow{\sim} p\mathbb{Z}_{(p)}\mathrm{D}_{2p}\,,$$

and

$$\mathcal{P}_3' := \mathcal{P}_3\Big|^{p(\mathbb{Z}_{(p)}\Xi/I)}_{p\mathbb{Z}_{(p)}\mathrm{D}_{2p}} : p\mathbb{Z}_{(p)}\mathrm{D}_{2p} \xrightarrow{\sim} p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big)\,,$$

are isomorphisms of abelian groups. Since $\mathcal{P}_2$ and $\mathcal{P}_3$ invert each other, cf. Remark 86, the same applies to $\mathcal{P}_2'$ and $\mathcal{P}_3'$.

Altogether, the rows in the following commutative diagram are short exact sequences of abelian groups

$$\begin{array}{ccccc}
p\mathbb{Z}_{(p)}\mathrm{D}_{2p} & \hookrightarrow & \mathbb{Z}_{(p)}\mathrm{D}_{2p} & \xrightarrow{\tilde{\varphi}} & \mathbb{F}_p\mathrm{D}_{2p} \\
\uparrow \mathcal{P}_2' \;\wr\; \downarrow \mathcal{P}_3' & \circlearrowright & \uparrow \mathcal{P}_2 \;\wr\; \downarrow \mathcal{P}_3 & & \\
\big(p\mathbb{Z}_{(p)}\Xi + I\big)/_I \overset{(**)}{=} p\Big(\mathbb{Z}_{(p)}\Xi/_I\Big) & \hookrightarrow & \mathbb{Z}_{(p)}\Xi/_I & \xrightarrow{\phi} & \mathbb{F}_p\Xi/_J
\end{array}$$

So there exists a unique morphism of abelian groups $\mathcal{P}_4 : \mathbb{F}_p\mathrm{D}_{2p} \longrightarrow \mathbb{F}_p\Xi/_J$ making the diagram commutative, which is an isomorphism. Moreover, applying Remark 108 to the case $(A, B, A', B', \varphi, f, \varphi', g) = (\,\mathbb{Z}_{(p)}\mathrm{D}_{2p}\,,\,\mathbb{F}_p\mathrm{D}_{2p}\,,\,\mathbb{Z}_{(p)}\Xi/_I\,,\,\mathbb{F}_p\Xi/_J\,,\,\tilde{\varphi}\,,\,\mathcal{P}_3\,,\,\phi\,,\,\mathcal{P}_4\,)$ we get that $\mathcal{P}_4$ is an isomorphism of rings.

We see that $p\mathbb{F}_p\mathrm{D}_{2p} = 0$ and $p\Big(\mathbb{F}_p\Xi/_J\Big) = 0$. So we get by Remark 107 that $\mathcal{P}_4$ is an isomorphism of $\mathbb{F}_p$-algebras.

Since $\tilde{\varphi}(x) = x$ and $\tilde{\varphi}(y) = y$, we obtain

$$\begin{aligned}
\mathcal{P}_4(x) &= \mathcal{P}_4(\tilde{\varphi}(x)) = \phi\big(\mathcal{P}_3(x)\big) \overset{\text{P.85}}{=} \phi\big(\overline{E} + \overline{F} + \overline{\alpha} + \overline{\beta} + \overline{\beta\alpha}\big) \\
&= \overline{\overline{\psi(E)}} + \overline{\overline{\psi(F)}} + \overline{\overline{\psi(\alpha)}} + \overline{\overline{\psi(\beta)}} + \overline{\overline{\psi(\beta\alpha)}} = \overline{\overline{E}} + \overline{\overline{F}} + \overline{\overline{\alpha}} + \overline{\overline{\beta}} + \overline{\overline{\beta\alpha}}\,,
\end{aligned}$$

and

$$\begin{aligned}
\mathcal{P}_4(y) &= \mathcal{P}_4(\tilde{\varphi}(y)) = \phi\big(\mathcal{P}_3(y)\big) \overset{\text{P.85}}{=} \phi\big(\overline{E} - \overline{F} + \overline{\beta}\big) \\
&= \overline{\overline{\psi(E)}} - \overline{\overline{\psi(F)}} + \overline{\overline{\psi(\beta)}} = \overline{\overline{E}} - \overline{\overline{F}} + \overline{\overline{\beta}}\,.
\end{aligned}$$

We denote $\mathcal{P}_5 := \mathcal{P}_4^{-1} : \mathbb{F}_p\Xi/_J \longrightarrow \mathbb{F}_p\mathrm{D}_{2p}$.

We have $\psi(E) = E$, $\psi(F) = F$, $\psi(\alpha) = \alpha$ and $\psi(\beta) = \beta$, so that $\phi\big(\overline{E}\big) = \overline{\overline{E}}$, $\phi\big(\overline{F}\big) = \overline{\overline{F}}$, $\phi(\overline{\alpha}) = \overline{\overline{\alpha}}$ and $\phi\big(\overline{\beta}\big) = \overline{\overline{\beta}}$.

We have $2 \cdot (n+1) = p + 1 \equiv_p 1$, i.e. $(n+1) \equiv_p 2^{-1}$. So

$$(**) \qquad \varphi\left(\frac{1}{2}\right) = \varphi\big(2^{-1}\big) = \varrho^{-1}\big(r\big(2^{-1}\big)\big) = \varrho^{-1}\big(2^{-1} + p\mathbb{Z}_{(p)}\big) = \varrho^{-1}\big((n+1) + p\mathbb{Z}_{(p)}\big) \overset{\text{C.127}}{=} n+1\,.$$

Hence we have

$$\begin{aligned}
\mathcal{P}_5\big(\overline{\overline{E}}\big) &= \mathcal{P}_5\big(\phi\big(\overline{E}\big)\big) = \tilde{\varphi}\big(\mathcal{P}_2\big(\overline{E}\big)\big) \overset{\text{P.84}}{=} \tilde{\varphi}\left(\frac{1}{2}\sum_{k=0}^{p-1}(-1)^k x^k(1+y)\right) \\
&= \varphi\left(\frac{1}{2}\right)\sum_{k=0}^{p-1}(-1)^k x^k(1+y) \overset{(**)}{=} (n+1)\sum_{k=0}^{p-1}(-1)^k x^k(1+y)\,,
\end{aligned}$$

$$\begin{aligned}
\mathcal{P}_5\big(\overline{\overline{F}}\big) &= \mathcal{P}_5\big(\phi\big(\overline{F}\big)\big) = \tilde{\varphi}\big(\mathcal{P}_2\big(\overline{F}\big)\big) \overset{\text{P.84}}{=} \tilde{\varphi}\left(\frac{1}{2}\left(1 - y - \sum_{k=1}^{p-1}(-1)^k x^k(1+y)\right)\right) \\
&= \varphi\left(\frac{1}{2}\right)\left(1 - y - \sum_{k=1}^{p-1}(-1)^k x^k(1+y)\right) \overset{(**)}{=} (n+1)\left(1 - y - \sum_{k=1}^{p-1}(-1)^k x^k(1+y)\right),
\end{aligned}$$

$$\begin{aligned}\mathcal{P}_5(\overline{\overline{\alpha}}) &= \mathcal{P}_5\big(\phi(\overline{\alpha})\big) = \tilde{\varphi}\big(\mathcal{P}_2(\overline{\alpha})\big) \overset{\text{P.84}}{=} \tilde{\varphi}\Big(-x^{-1}-y-\sum_{k=1}^{p-2}(-1)^k x^k(1+y)\Big)\\ &= -x^{-1}-y-\sum_{k=1}^{p-2}(-1)^k x^k(1+y)\,,\end{aligned}$$

and

$$\mathcal{P}_5(\overline{\overline{\beta}}) = \mathcal{P}_5\big(\phi(\overline{\beta})\big) = \tilde{\varphi}\big(\mathcal{P}_2(\overline{\beta})\big) \overset{\text{P.84}}{=} \tilde{\varphi}\Big(-\sum_{k=1}^{p-1}(-1)^k x^k(1+y)\Big) = -\sum_{k=1}^{p-1}(-1)^k x^k(1+y)\,. \qquad \square$$

Appendix A

Algebraic facts

A.1 Compatibilities for tensor products

Lemma 90 *Let K be a commutative ring and A, B be K-algebras.*

Then $A \underset{K}{\otimes} B$ becomes a ring via the multiplication

$$\begin{array}{rcccccc} \mu & : & A \underset{K}{\otimes} B & \times & A \underset{K}{\otimes} B & \longrightarrow & A \underset{K}{\otimes} B \\ & & (\,\eta_1 \otimes \xi_1 & , & \eta_2 \otimes \xi_2\,) & \longmapsto & (\eta_1 \otimes \xi_1) \cdot (\eta_2 \otimes \xi_2) := (\eta_1 \eta_2) \otimes (\xi_1 \xi_2)\,. \end{array}$$

The identity element is $1_{A \underset{K}{\otimes} B} = 1_A \otimes 1_B$.

Proof. In the sequel, all occurring sums are finite. Suppose given $(a, b) \in A \times B$. A standard calculation shows that the map

$$\begin{array}{rccc} \hat{g}_{(a,b)} & : & A \times B & \longrightarrow & A \underset{K}{\otimes} B \\ & & (\,c\,,\,d\,) & \longmapsto & ac \otimes bd \end{array}$$

is K-bilinear. Therefore, the map

$$\begin{array}{rccc} g_{(a,b)} & : & A \underset{K}{\otimes} B & \longrightarrow & A \underset{K}{\otimes} B \\ & & c \otimes d & \longmapsto & ac \otimes bd \end{array}$$

is well-defined and $\mathbb{Z}$-linear.

Suppose given $\xi = \sum\limits_j c_j \otimes d_j \in A \underset{K}{\otimes} B$. Again a standard calculation shows that the map

$$\begin{array}{rccc} \hat{f}_{\xi} & : & A \times B & \longrightarrow & A \underset{K}{\otimes} B \\ & & (\,a\,,\,b\,) & \longmapsto & g_{(a,b)}(\xi) \end{array}$$

is K-bilinear. Therefore, the map

$$\begin{array}{rccc} f_{\xi} & : & A \underset{K}{\otimes} B & \longrightarrow & A \underset{K}{\otimes} B \\ & & a \otimes b & \longmapsto & g_{(a,b)}(\xi) = \sum\limits_j ac_j \otimes bd_j \end{array}$$

is well-defined and $\mathbb{Z}$-linear.

Hence we obtain for $\eta = \sum_i a_i \otimes b_i \in A \underset{K}{\otimes} B$ that

$$f_\xi(\eta) \;=\; f_\xi\left(\sum_i a_i \otimes b_i\right) \;=\; \sum_i f_\xi(a_i \otimes b_i) \;=\; \sum_i \sum_j a_i c_j \otimes b_i d_j \,.$$

Thus the stated multiplication

$$\begin{array}{rccccc} \mu \;:\; & A \underset{K}{\otimes} B & \times & A \underset{K}{\otimes} B & \longrightarrow & A \underset{K}{\otimes} B \\ & \Big(\underbrace{\sum_i a_i \otimes b_i}_{=\eta} & , & \underbrace{\sum_j c_j \otimes d_j}_{=\xi} \Big) & \longmapsto & \eta \cdot \xi \;:=\; f_\xi(\eta) \;=\; \sum_{i,j} a_i c_j \otimes b_i d_j \,, \end{array}$$

or on elementary tensors $\quad (\, a \otimes b \;\;,\;\; c \otimes d \,) \quad \longmapsto \quad (a \otimes b) \cdot (c \otimes d) = ac \otimes bd$
is well-defined.

We have

$$(1_A \otimes 1_B) \cdot \left(\sum_r a_r \otimes b_r\right) \;=\; \sum_r 1_A \cdot a_r \otimes 1_B \cdot b_r \;=\; \sum_r a_r \cdot 1_A \otimes b_r \cdot 1_B \;=\; \left(\sum_r a_r \otimes b_r\right) \cdot (1_A \otimes 1_B) \,,$$

and

$$\begin{aligned} \left(\sum_r a_r \otimes b_r\right) \cdot \left(\left(\sum_s c_s \otimes d_s\right) \cdot \left(\sum_t u_t \otimes v_t\right)\right) \;&=\; \left(\sum_r a_r \otimes b_r\right) \cdot \left(\sum_{s,t} c_s u_t \otimes d_s v_t\right) \\ &=\; \sum_{r,s,t} a_r c_s u_t \otimes b_r d_s v_t \,, \end{aligned}$$

and similarly in other brackets.

Further we have

$$\begin{aligned} \left(\sum_r a_r \otimes b_r\right) \cdot \left(\sum_s c_s \otimes d_s + \sum_t u_t \otimes v_t\right) &= \sum_{r,s} a_r c_s \otimes b_r d_s + \sum_{r,t} a_r u_t \otimes b_r v_t \\ &= \left(\sum_r a_r \otimes b_r\right) \cdot \left(\sum_s c_s \otimes d_s\right) + \left(\sum_r a_r \otimes b_r\right) \cdot \left(\sum_t u_t \otimes v_t\right) , \end{aligned}$$

and similarly on the other side. □

Lemma 91 *Let K be a commutative ring and (B, β), (L, φ) be K-algebras, where L is commutative. Further, let (A, ψ) be an L-algebra.* (*Note that $(A, \psi \circ \varphi)$ is a K-algebra.*)
Then we have

(i) $A \underset{K}{\otimes} B$ *becomes an L-algebra via*

$$\begin{array}{rccc} \rho \;:\; L & \longrightarrow & A \underset{K}{\otimes} B \\ \lambda & \longmapsto & \psi(\lambda) \cdot 1_A \otimes 1_B \,. \end{array}$$

Moreover, we have the two special cases

(ii) $L = K$ *and* $\varphi = \mathrm{id}_K$ *:*

Then $A \underset{K}{\otimes} B$ *becomes a* K*-algebra via*

$$\begin{array}{rccc} \nu & : & K & \longrightarrow & A \underset{K}{\otimes} B \\ & & \kappa & \longmapsto & \psi(\kappa) \cdot 1_A \otimes 1_B \,. \end{array}$$

(iii) Further, if A *is commutative, then we can set* $L = A$ *and* $\psi = \mathrm{id}_A$ *:*

Then $A \underset{K}{\otimes} B$ *becomes an* A*-algebra via*

$$\begin{array}{rccc} \eta & : & A & \longrightarrow & A \underset{K}{\otimes} B \\ & & a & \longmapsto & a \otimes 1_B \,. \end{array}$$

Proof of *(i)*. By Lemma 90 we know that $A \underset{K}{\otimes} B$ is a ring. For $\lambda_1 , \lambda_2 \in L$ we have

$$\begin{aligned} \rho(\lambda_1 + \lambda_2) \;&=\; \psi(\lambda_1 + \lambda_2) \cdot 1_A \otimes 1_B \;=\; (\psi(\lambda_1) + \psi(\lambda_2)) \cdot 1_A \otimes 1_B \\ &=\; (\psi(\lambda_1) \cdot 1_A + \psi(\lambda_2) \cdot 1_A) \otimes 1_B \;=\; \psi(\lambda_1) \cdot 1_A \otimes 1_B + \psi(\lambda_2) \cdot 1_A \otimes 1_B \;=\; \rho(\lambda_1) + \rho(\lambda_2) \,, \end{aligned}$$

and

$$\begin{aligned} \rho(\lambda_1 \cdot \lambda_2) \;&=\; \psi(\lambda_1 \cdot \lambda_2) \cdot 1_A \otimes 1_B \;=\; (\psi(\lambda_1) \cdot \psi(\lambda_2)) \cdot 1_A \otimes 1_B \\ &=\; (\psi(\lambda_1) \cdot 1_A \cdot \psi(\lambda_2) \cdot 1_A) \otimes 1_B \cdot 1_B \;=\; (\psi(\lambda_1) \cdot 1_A \otimes 1_B) \cdot (\psi(\lambda_2) \cdot 1_A \otimes 1_B) \;=\; \rho(\lambda_1) \cdot \rho(\lambda_2) \,. \end{aligned}$$

Further we have

$$\rho(1_L) \;=\; \psi(1_L) \cdot 1_A \otimes 1_B \;=\; 1_A \cdot 1_A \otimes 1_B \;=\; 1_{A \underset{K}{\otimes} B} \,.$$

Therefore ρ is a morphism of rings.

Now we finally prove that $\rho(L) \overset{!}{\subseteq} \mathrm{Z}(A \underset{K}{\otimes} B)$. Let $a \in A$, $b \in B$ and $\lambda \in L$. Then we have

$$\begin{aligned} \rho(\lambda) \cdot (a \otimes b) \;&=\; (\psi(\lambda) \cdot 1_A \otimes 1_B) \cdot (a \otimes b) \;=\; \overbrace{\psi(\lambda)}^{\in \mathrm{Z}(A)} \cdot 1_A \cdot a \otimes 1_B \cdot b \\ &=\; a \cdot \psi(\lambda) \cdot 1_A \otimes b \cdot 1_B \;=\; (a \otimes b) \cdot ((\psi(\lambda) \cdot 1_A \otimes 1_B)) \;=\; (a \otimes b) \cdot \rho(\lambda) \,. \end{aligned}$$

And so, $A \underset{K}{\otimes} B$ becomes an L-algebra.

The items *(ii)* and *(iii)* follow. □

Lemma 92 *Let* K*,* S *and* T *be commutative rings.*

Let ${}_S M_K \xrightarrow{f} {}_S M'_K \xrightarrow{f'} {}_S M''_K$ *be* S*-*K*-linear maps of* S*-*K*-bimodules.*

Let ${}_K N_T \xrightarrow{g} {}_K N'_T \xrightarrow{g'} {}_K N''_T$ *be* K*-*T*-linear maps of* K*-*T*-bimodules.*

(i) We have an S-T-linear map

$$\begin{aligned} f \otimes g \ : \ {}_SM_K \underset{K}{\otimes} {}_KN_T &\longrightarrow {}_SM'_K \underset{K}{\otimes} {}_KN'_T \\ m \quad \otimes \quad n \quad &\longmapsto f(m) \ \otimes \ g(n)\,. \end{aligned}$$

We write $M \otimes g := \mathrm{id}_M \otimes g$ *and* $f \otimes N := f \otimes \mathrm{id}_N$.

(ii) We have $(f' \otimes g') \circ (f \otimes g) = ((f' \circ f) \otimes (g' \circ g))$.

Further we have $\mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \underset{K}{\otimes} N}$.

Proof. This is well-known and can be shown along the lines of [Lang 02, Ch. XVI, §1, pp. 605/606]. □

Lemma 93 *Let* $K \subseteq L$ *be an extension of commutative rings. Let* $\varphi : A \longrightarrow B$ *be a morphism of* K*-algebras.*

Then we have the morphism of L*-algebras*

$$\begin{aligned} L \otimes \varphi \ : \ L \underset{K}{\otimes} A \ &\longrightarrow \ L \underset{K}{\otimes} B \\ \lambda \ \otimes \ a \ &\longmapsto \ \lambda \ \otimes \ \varphi(a)\,, \end{aligned}$$

cf. Lemma 91 *(iii).*

Proof. By Lemma 92 we have that $L \otimes \varphi$ is a morphism of L-modules.

Let $\lambda_1 \otimes a_1$, $\lambda_2 \otimes a_2 \in L \underset{K}{\otimes} A$. Then we have

$$\left.\begin{aligned} &(L \otimes \varphi)((\lambda_1 \otimes a_1) \cdot (\lambda_2 \otimes a_2)) \ = \ (L \otimes \varphi)((\lambda_1\lambda_2) \otimes (a_1a_2)) \ = \ (\lambda_1\lambda_2) \otimes \varphi(a_1a_2) \\ &= (\lambda_1\lambda_2) \otimes (\varphi(a_1)\varphi(a_2)) \ = \ (\lambda_1 \otimes \varphi(a_1)) \cdot (\lambda_2 \otimes \varphi(a_2)) \\ &= ((L \otimes \varphi)(\lambda_1 \otimes a_1)) \cdot ((L \otimes \varphi)(\lambda_2 \otimes a_2))\,, \end{aligned}\right\} (1)$$

and

$$(2) \qquad (L \otimes \varphi)\big(1_{L \underset{K}{\otimes} A}\big) \ = \ (L \otimes \varphi)(1_L \otimes 1_A) \ = \ 1_L \otimes \varphi(1_A) \ = \ 1_L \otimes 1_B \ = \ 1_{L \underset{K}{\otimes} B}\,.$$

Since $L \otimes \varphi$ is additive and every element of $L \underset{K}{\otimes} A$ is a finite sum of elementary tensors, equation (1) shows that $L \otimes \varphi$ is multiplicative.

This together with (2) shows that $L \otimes \varphi$ is a morphism of rings. □

Lemma 94 *Let* K, S *and* T *be commutative rings.*

Let M *be an* S*-*K*-module, such that* M *is finitely generated free over* K*; cf.* Convention 13.

Suppose given a short exact sequence $N' \xrightarrow{j} N \xrightarrow{q} N''$ *of* K*-*T*-bimodules.*

Then we have a short exact sequence of S*-*T*-bimodules*

$$M \underset{K}{\otimes} N' \xrightarrow{M \otimes j} M \underset{K}{\otimes} N \xrightarrow{M \otimes q} M \underset{K}{\otimes} N''\,,$$

i.e. $M \underset{K}{\otimes} -$ *is an exact functor.*

Proof. We have that K is a flat K-module; cf. [Lang 02, Ch. XVI, §3, p. 613, Proposition 3.1 (i)]. Therefore the finitely generated free K-module $M \simeq K^{\oplus s}$ is also a flat K-module, where $s \in \mathbb{Z}_{\geq 1}$; cf. [Lang 02, Ch. XVI, §3, p. 613, Proposition 3.1 (ii)]. So the statement follows by [Lang 02, Ch. XVI, §3, p. 613, F 2]. □

Lemma 95

Let K be a commutative ring and $m \in \mathbb{Z}_{\geq 1}$. Further, let X and Y_i be K-modules for $i \in [1,m] =: I$.

Then we have an isomorphism of $\mathbb{Z}$-modules

$$\begin{array}{ccccc} X \underset{K}{\otimes} & \left(\underset{i\in I}{\oplus} Y_i \right) & \xrightarrow{\sim} & \underset{i\in I}{\oplus} \left(X \underset{K}{\otimes} Y_i \right) \\ x \otimes & (y_i)_{i\in I} & \overset{\phi}{\longmapsto} & (\, x \otimes y_i \,)_{i\in I} \\ x \otimes (0,\ldots,0, \underset{\text{pos. } s}{\underset{\uparrow}{y_s}},0,\ldots,0) & & \overset{\psi}{\longmapsto} & (0,\ldots,0, \underset{\text{pos. } s}{\underset{\uparrow}{x \otimes y_s}},0,\ldots,0) \quad \textit{for } s \in I. \end{array}$$

Proof. We denote the projection onto the s-th direct summand by $\pi_s : \underset{i\in I}{\oplus} Y_i \longrightarrow Y_s, (y_i)_{i\in I} \longmapsto y_s$ and the inclusion by $\iota_s : Y_s \longrightarrow \underset{i\in I}{\oplus} Y_i, y_s \longmapsto (0,\ldots,0, \underset{\text{pos. } s}{\underset{\downarrow}{y_s}},0,\ldots,0)$, where $s \in I$. Hence we get

$$((X \otimes \pi_j)(x \otimes (y_i)_{i\in I}))_{j\in I} \,=\, (x \otimes y_j)_{j\in I} \,=\, (x \otimes y_i)_{i\in I} \,=\, \phi(x \otimes (y_i)_{i\in I}),$$

so that ϕ is well-defined and $\mathbb{Z}$-linear; cf. Lemma 92 *(i)*.

We consider the maps

$$\psi_s := X \otimes \iota_s \,:\, X \underset{K}{\otimes} Y_s \longrightarrow X \underset{K}{\otimes} \left(\underset{i\in I}{\oplus} Y_i \right), x \otimes y_s \longmapsto x \otimes (0,\ldots,0, \underset{\text{pos. } s}{\underset{\downarrow}{y_s}},0,\ldots,0) \text{ for } s \in I.$$

So we get that

$$\begin{array}{rccc} \psi \;:\; & \underset{i\in I}{\oplus} \left(X \underset{K}{\otimes} Y_i \right) & \longrightarrow & X \underset{K}{\otimes} \left(\underset{i\in I}{\oplus} Y_i \right) \\ & (\, x_i \otimes y_i \,)_{i\in I} & \longmapsto & \underset{s\in I}{\sum} \psi_s(x_s \otimes y_s) \end{array}$$

is also well-defined and $\mathbb{Z}$-linear.

Further we have for $x \otimes (y_i)_{i\in I} \in X \underset{K}{\otimes} \left(\underset{i\in I}{\oplus} Y_i \right)$ and $(0,\ldots,0, \underset{\text{pos. } s}{\underset{\downarrow}{x \otimes y_s}},0,\ldots,0) \in \underset{i\in I}{\oplus} (X \underset{K}{\otimes} Y_i)$ for $s \in I$

$$\left.\begin{array}{rcl} (\psi \circ \phi)(x \otimes (y_i)_{i\in I}) & = & \psi(\phi(x \otimes (y_i)_{i\in I})) \,=\, \psi((x \otimes y_i)_{i\in I}) \\ & = & \underset{s\in I}{\sum} \psi_s(x \otimes y_s) \,=\, \underset{s\in I}{\sum} x \otimes (0,\ldots,0, \underset{\text{pos. } s}{\underset{\uparrow}{y_s}},0,\ldots,0) \;=\; x \otimes (y_i)_{i\in I}, \end{array}\right\} (1)$$

and

$$\left.\begin{array}{rcl} (\phi \circ \psi)((0,\ldots,0, \underset{\text{pos. } s}{\underset{\downarrow}{x \otimes y_s}},0,\ldots,0)) & = & \phi(\psi((0,\ldots,0, \underset{\text{pos. } s}{\underset{\downarrow}{x \otimes y_s}},0,\ldots,0))) \\ = \quad \phi(\psi_s(x \otimes y_s)) \,=\, \phi(x \otimes (0,\ldots,0, \underset{\text{pos. } s}{\underset{\uparrow}{y_s}},0,\ldots,0)) & = & (0,\ldots,0, \underset{\text{pos. } s}{\underset{\uparrow}{x \otimes y_s}},0,\ldots,0). \end{array}\right\} (2)$$

Since ϕ and ψ are additive and every element of $X \underset{K}{\otimes} \left(\underset{i\in I}{\oplus} Y_i \right)$ respectively $\underset{i\in I}{\oplus} (X \underset{K}{\otimes} Y_i)$ is a finite sum of elements of the form as in (1) respectively (2), equations (1) and (2) show that

$$\psi \circ \phi \text{ is the identity on } X \underset{K}{\otimes} \left(\underset{i\in I}{\oplus} Y_i \right) \qquad \text{and} \qquad \phi \circ \psi \text{ is the identity on } \underset{i\in I}{\oplus} (X \underset{K}{\otimes} Y_i)\ .$$

Therefore ϕ is bijective. □

Lemma 96 *Let K be a commutative ring and (A,α), (B,β), (C,τ) be K-algebras.*

Then we have an isomorphism of K-algebras

$$\begin{array}{rcccc} g & : & A \underset{K}{\otimes} (B \times C) & \xrightarrow{\sim} & A \underset{K}{\otimes} B \times A \underset{K}{\otimes} C \\ & & a \otimes (\ b\ ,\ c\ ) & \longmapsto & (a \otimes b\ ,\ a \otimes c)\,. \end{array}$$

Further, if A is commutative, g is an isomorphism of A-algebras.

Proof. By Lemma 95 we know that g is an isomorphism of $\mathbb{Z}$-modules.

For $a_1\,, a_2 \in A$, $b_1\,, b_2 \in B$ and $c_1\,, c_2 \in C$ we have

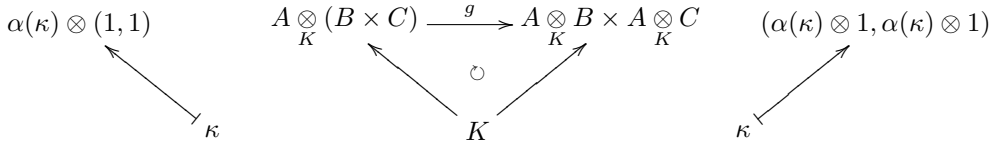
$$\left.\begin{array}{rcl} & g((a_1 \otimes (b_1\,, c_1)) \cdot (a_2 \otimes (b_2\,, c_2))) \ = \ g(a_1a_2 \otimes (b_1\,, c_1) \cdot (b_2\,, c_2)) \ = \ g(a_1a_2 \otimes (b_1b_2\,, c_1c_2)) \\ = & (a_1a_2 \otimes b_1b_2\,, a_1a_2 \otimes c_1c_2) \ = \ ((a_1 \otimes b_1) \cdot (a_2 \otimes b_2)\,, (a_1 \otimes c_1) \cdot (a_2 \otimes c_2)) \\ = & (a_1 \otimes b_1\,, a_1 \otimes c_1) \cdot (a_2 \otimes b_2\,, a_2 \otimes c_2) \ = \ g((a_1 \otimes (b_1\,, c_1))) \cdot g((a_2 \otimes (b_2\,, c_2)))\,, \end{array}\right\} (1)$$

and

$$g((1 \otimes (1,1))) = (1 \otimes 1, 1 \otimes 1) = 1_{A \underset{K}{\otimes} B \times A \underset{K}{\otimes} C}\,. \tag{2}$$

Since g is additive and every element of $A \underset{K}{\otimes} (B \times C)$ is a finite sum of elementary tensors of the form as in (1), equation (1) shows that g is multiplicative. This together with (2) shows that g is an isomorphism of rings.

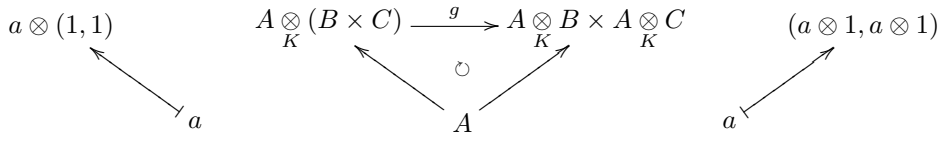
Note that $A \underset{K}{\otimes} (B \times C)$, together with $K \longrightarrow A \underset{K}{\otimes} (B \times C)$, $\kappa \longmapsto \alpha(\kappa) \otimes (1,1)$, is a K-algebra; cf. Lemma 91 *(ii)*. So we have the commutative diagram



Thus, g is a isomorphism of K-algebras.

Now let A be commutative.

Note that $A \underset{K}{\otimes} (B \times C)$, together with $A \longrightarrow A \underset{K}{\otimes} (B \times C)$, $a \longmapsto a \otimes (1,1)$, is an A-algebra; cf. Lemma 91 *(iii)*. So we have the commutative diagram



Therefore g is an isomorphism of A-algebras. □

Remark 97 *Let (B,β) be a K-algebra and $m \in \mathbb{Z}_{\geq 1}$. Then $B^{m\times m}$ becomes a K-algebra together with*

$$\begin{array}{rcccl} \beta_m & : & K & \longrightarrow & B^{m\times m} \\ & & \lambda & \longmapsto & \beta(\lambda)\cdot \mathrm{E}_m\,. \end{array}$$

Proof. Since β is a morphism of rings it is seen that β_m is also a morphism of rings. Further we have $\beta_m(K) \subseteq \mathrm{Z}(B^{m\times m})$. □

Lemma 98 *Let K be a commutative ring and (A,α), (B,β) be K-algebras with A commutative. Further, let $m \in \mathbb{Z}_{\geq 1}$.*

Then we have an isomorphism of A-algebras

$$\begin{array}{rcccl} h & : & A \underset{K}{\otimes} (B^{m\times m}) & \xrightarrow{\sim} & \left(A \underset{K}{\otimes} B\right)^{m\times m} \\ & & a \otimes (b_{i,j})_{i,j\in[1,m]} & \longmapsto & (a\otimes b_{i,j})_{i,j\in[1,m]}\,. \end{array}$$

Proof. We consider the map

$$\begin{array}{rcccl} \hat{h} & : & A \times (B^{m\times m}) & \longrightarrow & \left(A \underset{K}{\otimes} B\right)^{m\times m} \\ & & (\,a\ ,\ (b_{i,j})_{i,j\in[1,m]}\,) & \longmapsto & (a\otimes b_{i,j})_{i,j\in[1,m]}\,. \end{array}$$

A standard calculation shows that $\hat{h}$ is K-bilinear. Therefore h is well-defined and $\mathbb{Z}$-linear.

We have

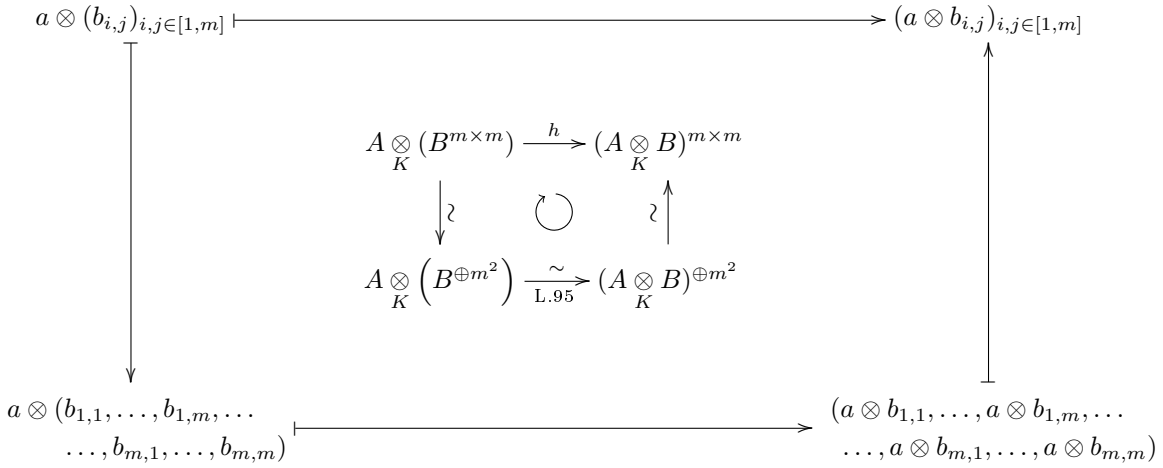
$$h(1_A \otimes \mathrm{E}_m) \;=\; (1_A \otimes 1_B\cdot \partial_{i,j})_{i,j\in[1,m]} \;=\; 1_{(A\underset{K}{\otimes}B)^{m\times m}}\,. \tag{1}$$

Let $a_1\,, a_2 \in A$ and $(b_{i,j})_{i,j\in[1,m]}\,, (c_{i,j})_{i,j\in[1,m]} \in B^{m\times m}$. Then we obtain

$$\left.\begin{array}{rcl} h\big((a_1\otimes (b_{i,j})_{i,j\in[1,m]})\cdot(a_2\otimes (c_{i,j})_{i,j\in[1,m]})\big) & = & h\big(a_1a_2\otimes ((b_{i,j})_{i,j\in[1,m]}\cdot (c_{i,j})_{i,j\in[1,m]})\big) \\ = \quad h\left(a_1a_2\otimes \left(\sum_{k=1}^{m} b_{i,k}\cdot c_{k,j}\right)_{i,j\in[1,m]}\right) & = & \left(a_1a_2\otimes \sum_{k=1}^{m} b_{i,k}\cdot c_{k,j}\right)_{i,j\in[1,m]} \\ = \quad \left(\sum_{k=1}^{m} a_1a_2\otimes b_{i,k}\cdot c_{k,j}\right)_{i,j\in[1,m]} & = & \left(\sum_{k=1}^{m} (a_1\otimes b_{i,k})\cdot(a_2\otimes c_{k,j})\right)_{i,j\in[1,m]} \\ = \quad (a_1\otimes b_{i,j})_{i,j\in[1,m]}\cdot(a_2\otimes c_{i,j})_{i,j\in[1,m]} & = & h\big(a_1\otimes (b_{i,j})_{i,j\in[1,m]}\big)\cdot h\big(a_2\otimes (c_{i,j})_{i,j\in[1,m]}\big)\,. \end{array}\right\} \tag{2}$$

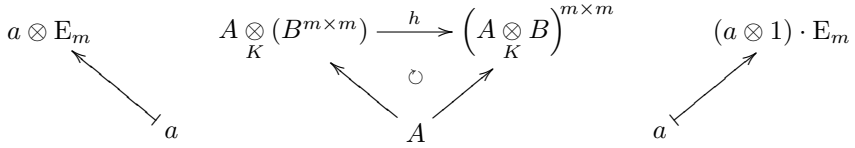
Since h is additive and every element of $A\underset{K}{\otimes}(B^{m\times m})$ is a finite sum of elementary tensors of the form as in (2), equation (2) shows that h is multiplicative. This together with (1) shows that h is a morphism of rings.

Further we have the commutative diagram of isomorphisms of abelian groups



Therefore h is an isomorphism of rings.

Recall that $A \underset{K}{\otimes} (B^{m\times m})$, together with $A \longrightarrow A \underset{K}{\otimes} (B^{m\times m})$, $a \longmapsto a \otimes \mathrm{E}_m$, is an A-algebra; cf. Remark 97, Lemma 91 *(iii)*. Recall that $\left(A \underset{K}{\otimes} B\right)^{m\times m}$, together with $A \longrightarrow \left(A \underset{K}{\otimes} B\right)^{m\times m}$, $a \longmapsto (a \otimes 1) \cdot \mathrm{E}_m$, is an A-algebra; cf. Lemma 91 *(iii)*, Remark 97. So we have the commutative diagram



Therefore h is an isomorphism of A-algebras. □

Lemma 99 *Let $\varphi : K \longrightarrow L$ be a morphism of commutative rings and G be a finite group.*

Then we have the isomorphism of L-algebras

$$\begin{array}{rcccc} f & : & L \underset{K}{\otimes} KG & \xrightarrow{\sim} & LG \\ & & \lambda \otimes \sum\limits_{g\in G} \kappa_g g & \longmapsto & \sum\limits_{g\in G} \lambda \cdot \varphi(\kappa_g) g\,. \end{array}$$

Proof. First we consider the map

$$\begin{array}{rcccc} \hat{f} & : & L \times KG & \longrightarrow & LG \\ & & \left(\lambda\ ,\ \sum\limits_{g\in G} \kappa_g g\right) & \longmapsto & \sum\limits_{g\in G} \lambda \cdot \varphi(\kappa_g) g\,. \end{array}$$

We see that $\hat{f}$ is additive in the first component. Using the additivity of φ, we get that $\hat{f}$ is additive in the second component.

Further we get for $\lambda \in L$, $\kappa \in K$ and $\sum\limits_{g\in G} \kappa_g g \in KG$ that

$$\begin{aligned} \hat{f}\Big(\Big(\lambda \cdot \kappa\,,\, \sum_{g\in G} \kappa_g g\Big)\Big) &= \hat{f}\Big(\Big(\lambda \cdot \varphi(\kappa)\,,\, \sum_{g\in G} \kappa_g g\Big)\Big) = \sum_{g\in G} \lambda \cdot \varphi(\kappa) \cdot \varphi(\kappa_g) g \\ &= \sum_{g\in G} \lambda \cdot \varphi(\kappa \cdot \kappa_g) g = \hat{f}\Big(\Big(\lambda\,,\, \sum_{g\in G} \kappa \cdot \kappa_g g\Big)\Big) = \hat{f}\Big(\Big(\lambda\,, \kappa \sum_{g\in G} \kappa_g g\Big)\Big)\,. \end{aligned}$$

Thus $\hat{f}$ is K-bilinear and consequently f is well-defined and $\mathbb{Z}$-linear.

For $\lambda_1 , \lambda_2 \in L$ and $g_1 , g_2 \in G$ we have

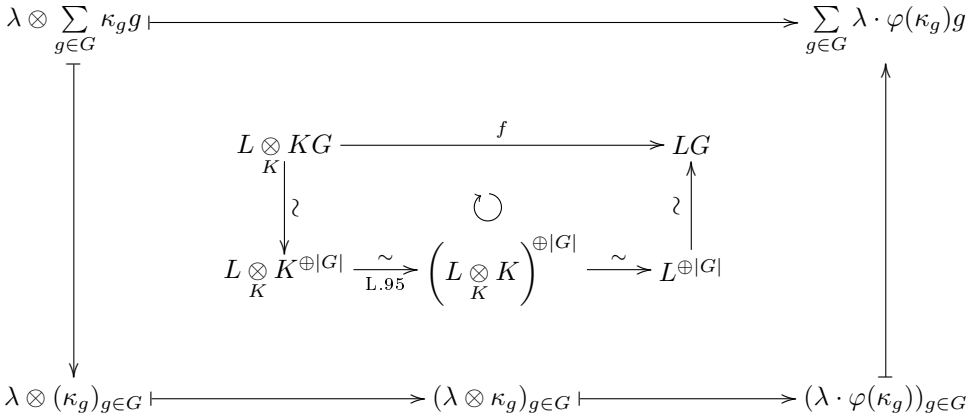
$$\left.\begin{array}{l} f((\lambda_1 \otimes g_1) \cdot (\lambda_2 \otimes g_2)) \;=\; f(\lambda_1\lambda_2 \otimes g_1 g_2) \;=\; \lambda_1 \cdot \lambda_2 \cdot \varphi(1_K) \cdot g_1 \cdot g_2 \;=\; \lambda_1 \cdot \lambda_2 \cdot g_1 \cdot g_2 \\ = \quad \lambda_1 \cdot g_1 \cdot \lambda_2 \cdot g_2 \;=\; \lambda_1 \cdot \varphi(1_K) \cdot g_1 \cdot \lambda_2 \cdot \varphi(1_K) \cdot g_2 \;=\; f(\lambda_1 \otimes g_1) \cdot f(\lambda_2 \otimes g_2) \,. \end{array}\right\} (1)$$

Since f is additive and every element of $L \underset{K}{\otimes} KG$ is a finite sum of tensors of the form as in (1), equation (1) shows that f is multiplicative. Further we have

$$f(1_L \otimes 1_{KG}) \;=\; f(1_L \otimes 1_K \cdot 1_G) \;=\; 1_L \cdot \varphi(1_K) \cdot 1_G \;=\; 1_{LG} \,.$$

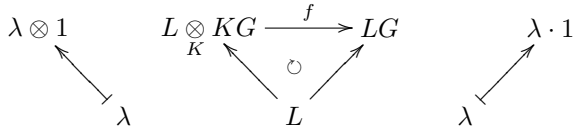
So f is a morphism of rings.

We have the commutative diagram of isomorphisms of abelian groups



Therefore f is an isomorphism of rings.

Recall that $L \underset{K}{\otimes} KG$, together with $L \longrightarrow L \underset{K}{\otimes} KG$, $\lambda \longmapsto \lambda \otimes 1$, is an L-algebra; cf. Lemma 91 *(iii)*. Therefore we have the following commutative diagram



So we get that f is an isomorphism of L-algebras. □

Lemma 100 *Let $\varphi : K \longrightarrow L$ be a morphism of commutative rings and V be a K-module.*

Further, let $s \in \mathbb{Z}_{\geq 1}$ and $(v_1 , \ldots , v_s)$ be a K-basis of V; cf. Convention 13.

Then we have

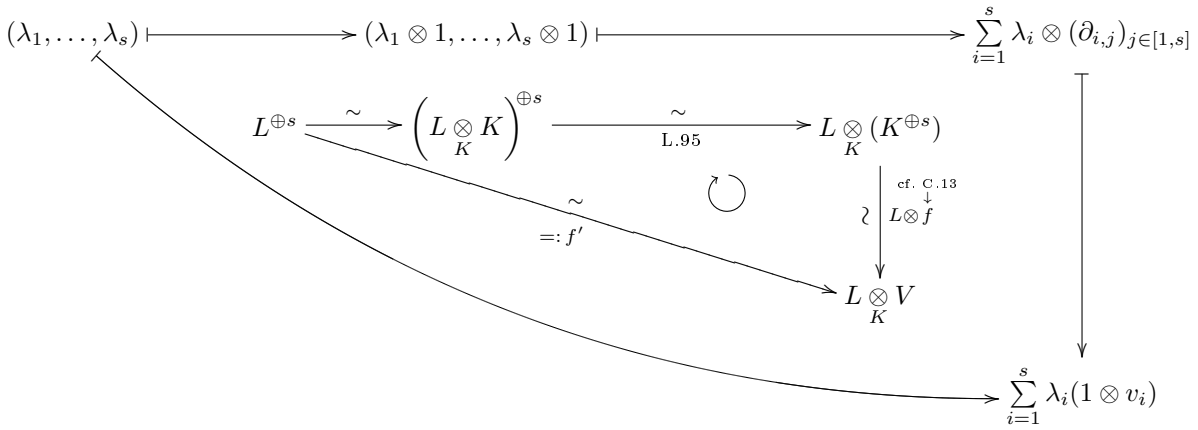
(i) The tuple $(1 \otimes v_1 , \ldots , 1 \otimes v_s)$ is an L-basis of $L \underset{K}{\otimes} V$.

(ii) Further, if φ is injective, then the map

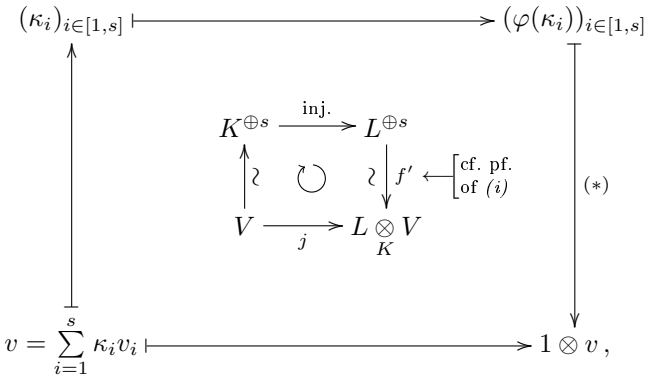
$$\begin{array}{ccccc} j & : & V & \longrightarrow & L \underset{K}{\otimes} V \\ & & v & \longmapsto & 1 \otimes v \quad \textit{is injective.} \end{array}$$

Moreover, if V is a K-algebra, we get that j is an injective morphism of K-algebras.

Proof of *(i)*. We obtain the asserted isomorphism of L-modules $f' : L^{\oplus s} \xrightarrow{\sim} L \underset{K}{\otimes} V$ as composite of the L-linear isomorphisms given in the following diagram



Proof of *(ii)*. We have the commutative diagram



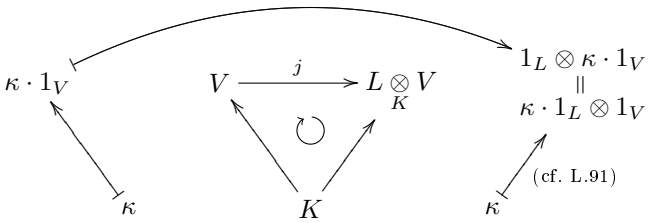
where in $(*)$ we remark that

$$f'\big((\varphi(\kappa_i))_{i\in[1,s]}\big) \;=\; \sum_{i=1}^{s} \varphi(\kappa_i) \otimes v_i \;=\; \sum_{i=1}^{s} 1_L \overset{\text{mult. of } K \text{ on } L}{\cdot} \kappa_i \otimes v_i \;=\; \sum_{i=1}^{s} 1 \otimes \kappa_i v_i \;=\; 1 \otimes \sum_{i=1}^{s} \kappa_i v_i \;=\; 1 \otimes v\,.$$

Therefore j is injective.

Now let V be a K-algebra. In this case, we see that j is multiplicative; cf. Lemma 90.

Further we have the commutative diagram



Therefore j is an injective morphism of K-algebras. □

Lemma 101 *Let S be a commutative ring. Let $R \subseteq S$ be a subring. Suppose that for all $s \in S$, there exists $r \in R \cap \mathrm{U}(S)$ with $rs \in R$. Furthermore, let A, B be S-algebras with A commutative.*

Then we have the isomorphisms of A-algebras

$$\begin{array}{ccc} A \underset{S}{\otimes} B & \xrightarrow{\sim} & A \underset{R}{\otimes} B \\ a \otimes b & \overset{d_S}{\longmapsto} & a \otimes b \\ a \otimes b & \overset{d_R}{\longmapsfrom} & a \otimes b\,. \end{array}$$

Proof. A standard calculation shows that d_R is well-defined and $\mathbb{Z}$-linear. We see that the map

$$\begin{array}{rcl} \hat{d}_S \;:\; A \times B & \longrightarrow & A \underset{R}{\otimes} B \\ (a\ ,\ b) & \longmapsto & a \otimes b \end{array}$$

is additive in both components.

Let $a \in A$, $b \in B$ and $s \in S$. Then there exists $r \in R \cap \mathrm{U}(S)$ with $rs \in R$. Note that $r^{-1} \in S$. Therefore we obtain

$$\begin{array}{rcccccl} \hat{d}_S\big((a \cdot s, b)\big) & = & a \cdot s \otimes b & = & a \cdot r^{-1}rs \otimes b & = & a \cdot r^{-1} \otimes rs \cdot b \\ & = & a \cdot r^{-1}r \otimes s \cdot b & = & a \otimes s \cdot b & = & \hat{d}_S\big((a, s \cdot b)\big)\,. \end{array}$$

Thus $\hat{d}_S$ is S-bilinear. Therefore d_S is well-defined and $\mathbb{Z}$-linear.

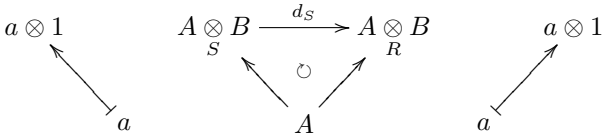
Let $a_1\,, a_2 \in A$ and $b_1\,, b_2 \in B$. Then we have

$$\begin{array}{rcccl} d_S\big((a_1 \otimes b_1) \cdot (a_2 \otimes b_2)\big) & = & d_S\big((a_1a_2) \otimes (b_1b_2)\big) & = & a_1a_2 \otimes b_1b_2 \\ & = & (a_1 \otimes b_1) \cdot (a_2 \otimes b_2) & = & d_S(a_1 \otimes b_1) \cdot d_S(a_2 \otimes b_2)\,. \end{array} \tag{1}$$

Since d_S is additive and every element of $A \underset{S}{\otimes} B$ is a finite sum of elementary tensors, equation (1) shows that d_S is multiplicative. We see that $d_S(1 \otimes 1) = 1_{A \underset{R}{\otimes} B}$.

In summary, we have that d_S is a morphism of rings.

Recall that $A \underset{S}{\otimes} B$, together with $A \longrightarrow A \underset{S}{\otimes} B\,,\ a \longmapsto a \otimes 1\,,$ is an A-algebra; cf. Lemma 91 *(iii)*. The similar applies to $A \underset{R}{\otimes} B$. Therefore we have the commutative diagram



Therefore d_S is a morphism of A-algebras. Finally, we see that d_S and d_R invert each other. □

A.2 Reordering an algebra

Lemma 102 *Let A be a commutative ring and $s,t \in \mathbb{Z}_{\geq 1}$.*

Then we have the isomorphisms of A-algebras

$$\begin{array}{ccc} (A^{\times s})^{t\times t} & \xrightarrow{\sim} & (A^{t\times t})^{\times s} \\ \big((b_{k,l;i})_{i\in[1,s]}\big)_{k,l\in[1,t]} & \overset{\phi}{\longmapsto} & \big((b_{k,l;i})_{k,l\in[1,t]}\big)_{i\in[1,s]} \\ \big((a_{i;k,l})_{i\in[1,s]}\big)_{k,l\in[1,t]} & \overset{\psi}{\longmapsto} & \big((a_{i;k,l})_{k,l\in[1,t]}\big)_{i\in[1,s]} . \end{array}$$

Proof. By construction, ϕ and ψ invert each other and therefore ϕ is bijective.

Moreover, we see that the map ϕ is additive and that $\phi(1_{(A^{\times s})^{t\times t}}) = 1_{(A^{t\times t})^{\times s}}$.

Let $\big((c_{k,l;i})_{i\in[1,s]}\big)_{k,l\in[1,t]}$, $\big((d_{k,l;i})_{i\in[1,s]}\big)_{k,l\in[1,t]} \in (A^{\times s})^{t\times t}$. Then we get

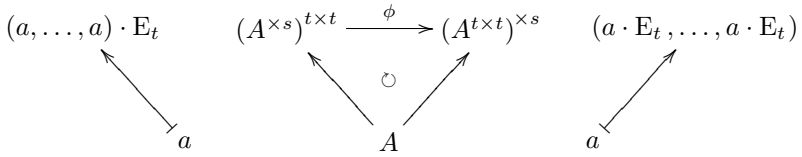
$$\begin{aligned} \phi\big(\big((c_{k,l;i})_{i\in[1,s]}\big)_{k,l\in[1,t]} \cdot \big((d_{k,l;i})_{i\in[1,s]}\big)_{k,l\in[1,t]}\big) &= \phi\Big(\Big(\sum_{j=1}^{t}(c_{k,j;i})_{i\in[1,s]} \cdot (d_{j,l;i})_{i\in[1,s]}\Big)_{k,l\in[1,t]}\Big) \\ = \qquad \phi\Big(\Big(\sum_{j=1}^{t}(c_{k,j;i} \cdot d_{j,l;i})_{i\in[1,s]}\Big)_{k,l\in[1,t]}\Big) &= \phi\Big(\Big(\Big(\sum_{j=1}^{t} c_{k,j;i} \cdot d_{j,l;i}\Big)_{i\in[1,s]}\Big)_{k,l\in[1,t]}\Big) \\ &= \Big(\Big(\sum_{j=1}^{t} c_{k,j;i} \cdot d_{j,l;i}\Big)_{k,l\in[1,t]}\Big)_{i\in[1,s]} , \end{aligned}$$

and

$$\begin{aligned} \phi\big(\big((c_{k,l;i})_{i\in[1,s]}\big)_{k,l\in[1,t]}\big) \cdot \phi\big(\big((d_{k,l;i})_{i\in[1,s]}\big)_{k,l\in[1,t]}\big) &= \big((c_{k,l;i})_{k,l\in[1,t]}\big)_{i\in[1,s]} \cdot \big((d_{k,l;i})_{k,l\in[1,t]}\big)_{i\in[1,s]} \\ = \qquad \big((c_{k,l;i})_{k,l\in[1,t]} \cdot (d_{k,l;i})_{k,l\in[1,t]}\big)_{i\in[1,s]} &= \Big(\Big(\sum_{j=1}^{t} c_{k,j;i} \cdot d_{j,l;i}\Big)_{k,l\in[1,t]}\Big)_{i\in[1,s]} . \end{aligned}$$

So ϕ is an isomorphism of rings.

Now we consider the A-algebra structures. We have commutative diagram



Hence ϕ is an isomorphism of A-algebras. □

A.3 Factor algebras

Lemma 103 *Let R, S be commutative rings and G be a finite group. Let $\varphi : R \longrightarrow S$ be a surjective morphism of rings. Write $\mathfrak{a} := \ker(\varphi)$.*

Then we have the short exact sequence of abelian groups

$$\begin{array}{ccccc} \mathfrak{a}RG & \hookrightarrow & RG & \xrightarrow{\tilde{\varphi}} & SG \\ \sum\limits_{g\in G} r_g g & \longmapsto & \sum\limits_{g\in G} r_g g & \longmapsto & \sum\limits_{g\in G} \varphi(r_g) g\,, \end{array}$$

where $\tilde{\varphi}$ is even a morphism of rings.

Proof. Since φ is a surjective morphism of rings we see that $\tilde{\varphi}$ is also surjective morphism of rings. The embedding of $\mathfrak{a}RG$ in RG is injective and additive. So it suffices to show that $\mathfrak{a}RG \stackrel{!}{=} \ker(\tilde{\varphi})$. We have

$$\begin{aligned} \ker(\tilde{\varphi}) &= \left\{ \sum_{g\in G} r_g g \in RG \,:\, \varphi(r_g) = 0 \text{ for } g \in G \right\} \\ &= \left\{ \sum_{g\in G} r_g g \in RG \,:\, r_g \in \ker(\varphi) = \mathfrak{a} \text{ for } g \in G \right\} \;=\; \mathfrak{a}RG\,. \end{aligned}$$

□

Notation 104 Recall from Notation 81 that $\Xi = \left(E \bullet \overset{\alpha}{\underset{\beta}{\rightleftarrows}} \bullet F \right)$ and that in this quiver, we write composition of paths in such a way that e.g. $\alpha\beta$ is a path from E to E.

Moreover, we denote the set of paths in Ξ by

$$\mathrm{Path}(\Xi) := \{E,\, F,\, \alpha,\, \beta,\, \alpha\beta,\, \beta\alpha,\, \dots\}\,.$$

Lemma 105 *Let R, S be commutative rings. Let $\varphi : R \longrightarrow S$ be a surjective morphism of rings. Write $\mathfrak{a} := \ker(\varphi)$.*

Then we have the short exact sequence of abelian groups

$$\begin{array}{ccccc} \mathfrak{a}R\Xi & \hookrightarrow & R\Xi & \xrightarrow{\psi} & S\Xi \\ \sum\limits_{m\in \mathrm{Path}(\Xi)} r_m m & \longmapsto & \sum\limits_{m\in \mathrm{Path}(\Xi)} r_m m & \longmapsto & \sum\limits_{m\in \mathrm{Path}(\Xi)} \varphi(r_m) m\,, \end{array}$$

where $r_m = 0$ for almost all $m \in \mathrm{Path}(\Xi)$.

The map ψ is even a morphism of rings. In particular, we have $\mathfrak{a}R\Xi = \ker(\psi)$.

Proof. The proof in analogous to the proof of Lemma 103. □

Lemma 106 *Let A, B be rings, not necessarily commutative, and I be an (both-sided) ideal of A. Let $\psi : A \longrightarrow B$ be a surjective morphism of rings. Write $K := \ker(\psi)$.*

Then we have the surjective morphism of rings

$$\begin{array}{rccc} \phi \;:\; & {}^{A}\!/_{I} & \longrightarrow & {}^{B}\!/_{\psi(I)} \\ & a + I & \longmapsto & \psi(a) + \psi(I)\,, \end{array}$$

with $\ker(\phi) = {}^{(K+I)}\!/_{I} \subseteq {}^{A}\!/_{I}$.

Proof. Since ψ is a surjective morphism of rings, $\psi(I)$ is an (both-sided) ideal of B and ϕ is a surjective morphism of rings.

Given $a \in A$, we have the equivalences

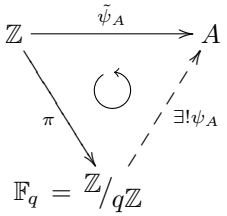
$$\begin{aligned} a+I \in \ker(\phi) &\iff \psi(a) \in \psi(I) \iff \text{there exists } z \in I \text{ with } \psi(a) = \psi(z) \\ &\iff \text{there exists } z \in I \text{ with } \psi(a-z) = 0 \\ &\iff \text{there exists } z \in I \text{ with } a - z \in K \iff a \in K + I\,. \end{aligned}$$ □

Remark 107 *Let $q \in \mathbb{Z}_{\geq 2}$ be a prime. Let A, B be rings with $qA = 0$ and $qB = 0$. Let $\varphi : A \longrightarrow B$ be a morphism of rings.*

Then A becomes an $\mathbb{F}_q$-algebra via $\mathbb{F}_q \longrightarrow A$, $k \cdot 1_{\mathbb{F}_q} \longmapsto k \cdot 1_A$, where $k \in \mathbb{Z}$. The same applies to B.

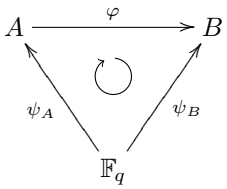
Moreover, φ becomes a morphism of $\mathbb{F}_q$-algebras.

Proof. Since A is a ring there exists a unique morphism of rings $\tilde{\psi}_A : \mathbb{Z} \longrightarrow A$, $1 \longmapsto 1_A$. Since $qA = 0$ we have $q\mathbb{Z} \subseteq \ker(\tilde{\psi}_A)$. So there exists a unique ring morphism ψ_A fitting into the following commutative triangle



mapping as stated above. Similarly B becomes an $\mathbb{F}_q$-algebra via a unique ring morphism ψ_B.

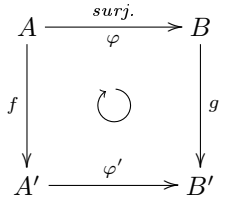
We have the commutative diagram



□

Remark 108 *Let A, B, A' and B' be rings. Let $\varphi : A \longrightarrow B$, $f : A \longrightarrow A'$ and $\varphi' : A' \longrightarrow B'$ be morphisms of rings, where φ is surjective. Let $g : B \longrightarrow B'$ be a morphism of abelian groups.*

Suppose that we have the following commutative diagram.



Then g is even a morphism of rings.

Proof. We have

$$g(1_B) = g(\varphi(1_A)) = \varphi'(f(1_A)) = \varphi'(1_{A'}) = 1_{B'}\,.$$

Let $b, \tilde{b} \in B$. Since φ is surjective, there exist $a, \tilde{a} \in A$ with $\varphi(a) = b$ and $\varphi(\tilde{a}) = \tilde{b}$. We obtain

$$\begin{aligned} g(b \cdot \tilde{b}) &= g(\varphi(a) \cdot \varphi(\tilde{a})) = g(\varphi(a \cdot \tilde{a})) = \varphi'(f(a \cdot \tilde{a})) = \varphi'(f(a) \cdot f(\tilde{a})) \\ &= \varphi'(f(a)) \cdot \varphi'(f(\tilde{a})) = g(\varphi(a)) \cdot g(\varphi(\tilde{a})) = g(b) \cdot g(\tilde{b})\,. \end{aligned}$$ □

A.4 Dedekind

Lemma 109 (Dedekind)

Let $L|K$ be a finite Galois extension. Write $m := [L : K]$.

Then we have the isomorphism of L-algebras

$$\begin{array}{rccc} f \;:\; L \underset{K}{\otimes} L & \xrightarrow{\sim} & L \times \ldots \times L \\ y \otimes x & \longmapsto & (\,\sigma_1(x)y \;,\; \ldots \;,\; \sigma_m(x)y\,)\,, \end{array}$$

where $\mathrm{Gal}(L|K) = \{\sigma_i \,:\, i \in [1,m]\}$.

Proof. First we prove that f is well-defined. For this we consider the map

$$\begin{array}{rccc} \hat{f} \;:\; L \times L & \longrightarrow & L \times \ldots \times L \\ (\,y \;,\; x\,) & \longmapsto & (\,\sigma_1(x)y \;,\; \ldots \;,\; \sigma_m(x)y\,)\,, \end{array}$$

We see that $\hat{f}$ is additive in both components. Let $y, x \in L$ and $\lambda \in K$. Then we have

$$\begin{array}{rcl} \hat{f}((y\lambda, x)) & = & (\sigma_1(x)y\lambda, \ldots, \sigma_m(x)y\lambda) \\ & \overset{\lambda\in K}{=} & (\sigma_1(x)y\sigma_1(\lambda), \ldots, \sigma_m(x)y\sigma_m(\lambda)) \\ & = & (\sigma_1(\lambda x)y, \ldots, \sigma_m(\lambda x)y) \qquad\qquad = \quad \hat{f}((y, \lambda x))\,. \end{array}$$

Therefore $\hat{f}$ is K-bilinear, whence f is well-defined and $\mathbb{Z}$-linear.

Let $y_1\,, y_2\,, x_1\,, x_2 \in L$. Then we get

$$\left.\begin{array}{rcl} & f((y_1 \otimes x_1)\cdot(y_2 \otimes x_2)) \;=\; f((y_1y_2 \otimes x_1x_2)) & \\ = & (\sigma_1(x_1x_2)y_1y_2\,, \ldots, \sigma_m(x_1x_2)y_1y_2) \;=\; (\sigma_1(x_1)y_1\sigma_1(x_2)y_2\,, \ldots, \sigma_m(x_1)y_1\sigma_m(x_2)y_2) & \\ = & (\sigma_1(x_1)y_1\,, \ldots, \sigma_m(x_1)y_1)\cdot(\sigma_1(x_2)y_2\,, \ldots, \sigma_m(x_2)y_2) \;=\; f((y_1 \otimes x_1))\cdot f((y_2 \otimes x_2))\,. & \end{array}\right\}(*)$$

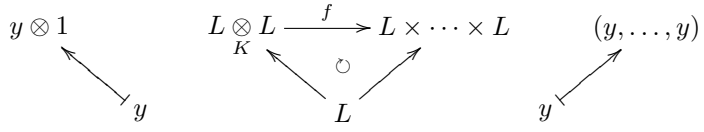
Since f is additive and every element of $L \underset{K}{\otimes} L$ is a finite sum of elementary tensors, equation $(*)$ shows that f is multiplicative.

Further we have

$$f(1 \otimes 1) \;=\; (\sigma_1(1)1, \ldots, \sigma_m(1)1) \;=\; 1_{L^{\times m}}\,.$$

Summarized we get that f is a morphism of rings.

Recall that $L \underset{K}{\otimes} L$, together with $L \longrightarrow L \underset{K}{\otimes} L$, $y \longmapsto y \otimes 1$, is an L-algebra; cf. Lemma 91 *(iii)*, applied to $(K, (A, \varphi), (B, \beta)) = (K, (L, \iota), (L, \iota))$, where $\iota : K \hookrightarrow L$ denotes the canonical embedding. Therefore we have the following commutative diagram



Therefore f is a morphism of L-algebras and so consequently L-linear.

So we can consider the matrix A describing f with respect to the following L-linear bases. Choose a K-linear basis $(x_1, \ldots, x_m)$ of L and consider the L-linear basis $(1 \otimes x_1, \ldots, 1 \otimes x_m)$ of $L \underset{K}{\otimes} L$; cf. Lemma 100 *(i)*. Furthermore, we choose the standard basis of $L^{\times m}$.

For $i \in [1, m]$ we have

$$1 \otimes x_i \overset{f}{\longmapsto} (\sigma_1(x_i), \ldots, \sigma_m(x_i)) .$$

And so we obtain A as

$$A = (\sigma_i(x_j))_{i,j \in [1,m]} \in L^{m \times m} .$$

Now we show that the rows in A are linearly independent.

For this we **assume** that the rows in A are linearly dependent.

Choose $\lambda_1, \ldots, \lambda_m \in L$ such that

$$\sum_{j=1}^{m} \lambda_j \sigma_j(x_i) \;=\; 0 \text{ for } i \in [1, m] , \qquad \text{with } |\underbrace{\{\, j \in [1, m] \,:\, \lambda_j \neq 0 \}}_{=:U}| \text{ minimal, but } \geq 1. \tag{1.1}$$

Since $(x_1, \ldots, x_m)$ is a K-linear basis of L and the map $\sum\limits_{j=1}^{m} \lambda_j \sigma_j$ is K-linear, (1.1) is equivalent to

$$\sum_{j=1}^{m} \lambda_j \sigma_j(x) \;=\; 0 \text{ for } x \in L , \qquad \text{with } |U| \text{ minimal, but } \geq 1. \tag{1.2}$$

Since $\sigma_j(1) = 1$ for $j \in [1, m]$, we know that $|U| \geq 2$. Choose $s, t \in U$ with $s \neq t$, so that $\lambda_s \neq 0$, $\lambda_t \neq 0$.

Since $s \neq t$, there exists $y \in L$ with $\sigma_s(y) \neq \sigma_t(y)$. $\qquad (**)$

Using (1.2) we therefore obtain

$$\sum_{j=1}^{m} \lambda_j \sigma_j(x) \sigma_s(y) \quad = \quad 0 \quad \text{for } x \in L , \tag{2}$$

and

$$\begin{array}{lcl} \displaystyle\sum_{j=1}^{m} \lambda_j \sigma_j(xy) & = & 0 \quad \text{for } x \in L . \\ \| & & \\ \displaystyle\sum_{j=1}^{m} \lambda_j \sigma_j(x) \sigma_j(y) & & \end{array} \tag{3}$$

The difference of (2) and (3) yields

$$\sum_{j=1}^{m} \lambda_j (\sigma_s(y) - \sigma_j(y)) \sigma_j(x) \quad = \quad 0 \quad \text{for } x \in L . \tag{4}$$

Writing $\lambda'_j := \lambda_j(\sigma_s(y) - \sigma_j(y))$ for $j \in [1, m]$ and $U' := \{\, j \in [1, m] \,:\, \lambda'_j \neq 0 \}$, we get $U' \subseteq U$. Since $t \in U'$, cf. $(**)$, and $s \in U \setminus U'$, we obtain $0 \neq |U'| < |U|$.

Hence, (4) is a shorter non-trivial linear combination than (1.2), in **contradiction** to the minimality of U.

Therefore the rows in A are linearly independent and A is invertible. And so f is bijective. $\square$

A.5 The discriminant of a finite Galois extension

Definition 110 Let $L|K$ be an extension of number fields of degree $m := [L : K]$. Suppose given an integral basis $(x_i)_{i\in[1,m]}$ of $\mathcal{O}_L|\mathcal{O}_K$; cf. Definition 16.

Then we define the (*relative*) *discriminant* of L over K

$$\Delta_{L|K} := \det\big((\mathrm{Tr}_{L|K}(x_i x_j))_{i,j\in[1,m]}\big)\,.$$

For the definition of an "*integral basis*" and that, if such a basis exists, its length equals the degree $[L : K]$ of the field extension, we refer to [Neukirch 99, Ch. I, p. 12, Remark before Proposition (2.10)].

Remark 111 *Let $L|K$ be an extension of number fields of degree 2.*

Suppose given $\alpha \in L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Write $X^2 + bX + c := \mu_{\alpha,K}(X) \in \mathcal{O}_K[X]$.

Then we have

$$\Delta_{L|K} = b^2 - 4c\,.$$

Proof. We choose the basis $(1, \alpha)$ of $\mathcal{O}_K[\alpha]$. Then we have

$$\Delta_{L|K} \overset{\text{D.110}}{=} \det\left(\begin{pmatrix} \mathrm{Tr}_{L|K}(1) & \mathrm{Tr}_{L|K}(\alpha) \\ \mathrm{Tr}_{L|K}(\alpha) & \mathrm{Tr}_{L|K}(\alpha^2) \end{pmatrix}\right) = \det\left(\begin{pmatrix} 2 & -b \\ -b & b^2 - 2c \end{pmatrix}\right) = 2b^2 - 4c - b^2 = b^2 - 4c\,.$$

□

Lemma 112 (Discriminant-product-formula)

In a tower of fields $F|L|K$, the relative discriminants are related by

$$\Delta_{F|K} = \mathrm{N}_{L|K}\big(\Delta_{F|L}\big) \cdot \Delta_{L|K}^{[F:L]}\,.$$

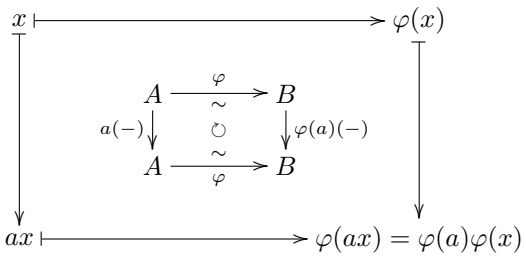
Proof. We refer to [Neukirch 99, Ch. III, p. 202, Corollary (2.10)]. □

Remark 113 *Let K be a commutative ring. Let A and B be K-algebras that are finitely generated free as modules over K. Let $\varphi : A \xrightarrow{\sim} B$ be an isomorphism of K-algebras.*

Then we have for $a \in A$

$$\mathrm{Tr}_{A|K}(a) = \mathrm{Tr}_{B|K}(\varphi(a))\,.$$

Proof. We have the commutative diagram



Therefore we have

$$\begin{aligned}\mathrm{Tr}_{A|K}(a) &= \mathrm{tr}_K(a(-) : A \longrightarrow A)\\ &= \mathrm{tr}_K(\varphi^{-1} \circ \varphi(a)(-) \circ \varphi : A \longrightarrow A)\\ &= \mathrm{tr}_K(\varphi(a)(-) : B \longrightarrow B) \qquad = \quad \mathrm{Tr}_{B|K}(\varphi(a))\,. \end{aligned}$$ □

Corollary 114 *Let $L|K$ be a finite Galois extension. Write $G := \mathrm{Gal}(L|K)$ and $m := |G|$.*

Then we have for $x \in L$

$$\mathrm{Tr}_{L|K}(x) \;=\; \sum_{\sigma \in G} \sigma(x)\,.$$

Proof. We have

$$\begin{aligned}\mathrm{Tr}_{L|K}(x) \;=\; \mathrm{tr}_K\big(L \xrightarrow{x(-)} L\big) &\overset{\text{L.100}}{\underset{(i)}{=}} \mathrm{tr}_L\big(L \underset{K}{\otimes} L \xrightarrow{1\otimes x(-)} L \underset{K}{\otimes} L\big)\\ &\overset{\text{L.109}}{\underset{\text{R.113}}{=}} \mathrm{tr}_L\big(L^{\times m} \xrightarrow{f(1\otimes x)(-)} L^{\times m}\big) \quad = \quad \mathrm{Tr}_{L^{\times m}|L}(f(1 \otimes x))\,.\end{aligned}$$

Write $G =: \{\sigma_1, \ldots, \sigma_m\}$ such that $f(1 \otimes x) = (\sigma_1(x), \ldots, \sigma_m(x))$. Choosing the standard L-linear basis of $L^{\times m}$ we therefore obtain the describing matrix A of $f(1 \otimes x)(-) : L^{\times m} \longrightarrow L^{\times m}$ as

$$A = \begin{pmatrix} \sigma_1(x) & & 0 \\ & \ddots & \\ 0 & & \sigma_m(x) \end{pmatrix}, \quad \text{so} \quad \mathrm{tr}(A) \;=\; \sum_{i=1}^{m} \sigma_i(x) \;=\; \sum_{\sigma \in G} \sigma(x)\,.$$

□

Lemma 115 *Let $L|\mathbb{Q}$ be a finite Galois extension.*

Write $\mathrm{Gal}(L|\mathbb{Q}) =: G =: \{\sigma_1, \ldots, \sigma_m\}$, where $m = |G|$. Suppose given a basis $(x_j)_{j\in[1,m]}$ of $\mathcal{O}_L|\mathbb{Z}$; cf. Definition 16.

Then we have

$$\big(\det\big((\sigma_i(x_j))_{i,j\in[1,m]}\big)\big)^2 \;=\; \Delta_{L|\mathbb{Q}}\,.$$

Proof. We have

$$\begin{aligned}(\sigma_i(x_j))_{j,i\in[1,m]} \cdot (\sigma_i(x_k))_{i,k\in[1,m]} &= \left(\sum_{i=1}^{m} \sigma_i(x_j)\sigma_i(x_k)\right)_{j,k\in[1,m]}\\ &= \left(\sum_{i=1}^{m} \sigma_i(x_j x_k)\right)_{j,k\in[1,m]} \overset{\text{C.114}}{=} (\mathrm{Tr}_{L|\mathbb{Q}}(x_j x_k))_{j,k\in[1,m]}\,.\end{aligned}$$

Therefore we have

$$\big(\det\big((\sigma_i(x_j))_{i,j\in[1,m]}\big)\big)^2 \;=\; \det\big((\mathrm{Tr}_{L|\mathbb{Q}}(x_j x_k))_{j,k\in[1,m]}\big) \;=\; \Delta_{L|\mathbb{Q}}\,.$$

□

A.6 Change of base ring for determinants

Lemma 116

Let K be a number field, i.e. $K \subseteq \mathbb{C}$ is a finite field extension of $\mathbb{Q}$; cf. Convention 15. *Write $s := [K : \mathbb{Q}]$.*

Let A, B be finitely generated free $\mathcal{O}_K$-modules of the same rank $r \in \mathbb{Z}_{\geq 0}$.

Let $(a_1 , \ldots , a_r)$ be an $\mathcal{O}_K$-linear basis of A and $(b_1 , \ldots , b_r)$ be an $\mathcal{O}_K$-linear basis of B.

Suppose given an $\mathcal{O}_K$-linear map $\varphi : A \longrightarrow B$. Let $F \in \mathcal{O}_K^{r \times r}$ be the describing matrix of φ with respect to the given $\mathcal{O}_K$-linear bases $(a_1 , \ldots , a_r)$ of A and $(b_1 , \ldots , b_r)$ of B.

Then we have

$$\det_{\mathbb{Z}}(\varphi) \;=\; \pm \mathrm{N}_{K|\mathbb{Q}}(\det(F)) \;=\; \pm \mathrm{N}_{K|\mathbb{Q}}(\det_{\mathcal{O}_K}(\varphi)) \,.$$

Proof. Let $(x_j)_{j \in [1,s]}$ be a $\mathbb{Z}$-linear basis of $\mathcal{O}_K$; cf. [Neukirch 99, Ch. I, p. 12, Proposition (2.10)].

Then we have the $\mathbb{Z}$-linear bases

$$\begin{aligned} (a_i x_j)_{\substack{i \,\in\, [1,\,r],\\ j \,\in\, [1,\,s]}} \quad &= \quad (a_1 x_1 , a_1 x_2 , \ldots , a_1 x_s \;\; , \;\; \ldots \;\; , \;\; a_r x_1 , a_r x_2 , \ldots , a_r x_s) \quad \text{of } A \text{ and} \\ (b_i x_j)_{\substack{i \,\in\, [1,\,r],\\ j \,\in\, [1,\,s]}} \quad &= \quad (b_1 x_1 , b_1 x_2 , \ldots , b_1 x_s \;\; , \;\; \ldots \;\; , \;\; b_r x_1 , b_r x_2 , \ldots , b_r x_s) \quad \text{of } B. \end{aligned}$$

For given $y \in K$ let $\hat{y} \in \mathbb{Q}^{s \times s}$ denote the $\mathbb{Q}$-linear describing matrix of $K \longrightarrow K$, $z \longmapsto zy$ with respect to the $\mathbb{Q}$-linear basis $(x_j)_{j \in [1,s]}$ of K; cf. [Neukirch 99, Ch. I, p. 8].

If $y \in \mathcal{O}_K$, then $\hat{y} \in \mathbb{Z}^{s \times s}$ is also the $\mathbb{Z}$-linear describing matrix of $\mathcal{O}_K \longrightarrow \mathcal{O}_K$, $z \longmapsto zy$ with respect to $(x_j)_{j \in [1,s]}$.

We further define for a given matrix $M = (m_{i,j})_{i,j \in [1,r]} \in K^{r \times r}$ the block matrix

$$\hat{M} \;=\; (\hat{m}_{k,l})_{k,l \in [1,r]} \;=\; \begin{array}{c} \\ s \\ r \end{array} \overbrace{\phantom{\begin{array}{|c|c|c|}\hat{m}_{1,1} & \hat{m}_{1,2} & \ldots \\ \hline \vdots & & \\ \hline & & \end{array}}}^{r} \left\{ \begin{array}{|c|c|c|} \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} \\ \multicolumn{1}{c}{s} & \hat{m}_{1,1} & \hat{m}_{1,2} & \ldots \\ \hline & \vdots & & \\ \hline & & & \end{array} \right. \quad \in \quad \mathbb{Q}^{sr \times sr}$$

A linear algebra calculation shows that the operation "$\hat{}$" is compatible with multiplication, i.e.

$$\begin{aligned} \hat{y}_1 \hat{y}_2 \quad &= \quad \widehat{y_1 y_2} \qquad \text{for } y_1 , y_2 \in K \text{ and} \\ \hat{M}_1 \hat{M}_2 \quad &= \quad \widehat{M_1 M_2} \quad \text{for } M_1 , M_2 \in K^{r \times r} \;\; . \end{aligned} \tag{1}$$

Let $F = (f_{k,l})_{k,l \in [1,r]}$. Then the $\mathbb{Z}$-linear describing matrix of φ with respect to the bases introduced above is given by

$$\hat{F} \;=\; \big(\hat{f}_{k,l}\big)_{k,l \in [1,r]} \;\in\; \mathbb{Z}^{sr \times sr} \,.$$

Let $\mathrm{SL}_r^{\pm}(K) := \big\{ S \in K^{r \times r} \,:\, \det(S) \in \{-1, +1\} \big\} \leq \mathrm{GL}_r(K)$.

Gaussian elimination over K yields a matrix $S \in \mathrm{SL}_r^{\pm}(K)$, arising as a product of elementary and permutation matrices, such that

$$SF \;=\; D \;:=\; \begin{pmatrix} d_1 & & * \\ & \ddots & \\ 0 & & d_r \end{pmatrix} \quad \text{, where } d_i \in K \text{ for } i \in [1, r] \,. \tag{2}$$

As both elementary matrices and permutation matrices yield matrices of determinant ± 1 under the operation "$\hat{}$", we have $\hat{S} \in \mathrm{SL}_{sr}^{\pm}(\mathbb{Q}) := \left\{ T \in \mathbb{Q}^{sr \times sr} \,:\, \det(T) \in \{-1,+1\} \right\} \leq \mathrm{GL}_{sr}(\mathbb{Q})$.

So we get

$$\pm\det(D) \overset{(2)}{=} \pm\det(\overset{\det=\pm 1}{\downarrow}\hat{S}F) = \pm\det(F) \overset{\text{def.}}{=} \pm\det_{\mathcal{O}_K}(\varphi) \qquad \text{and} \tag{3.1}$$

$$\pm\det\big(\hat{D}\big) \underset{(2)}{=} \pm\det\big(\widehat{SF}\big) \underset{(1)}{=} \pm\det\big(\hat{S}\hat{F}\big) = \pm\det\big(\hat{F}\big) \underset{\text{def.}}{=} \pm\det_{\mathbb{Z}}(\varphi)\,. \tag{3.2}$$

Therefore we have

$$\begin{aligned} \pm\det_{\mathbb{Z}}(\varphi) &\overset{(3.2)}{=} \pm\det\big(\overset{\text{block matrix}}{\downarrow}\hat{D}\big) = \pm\det\big(\hat{d}_1\big)\cdots\det\big(\hat{d}_r\big) = \pm\mathrm{N}_{K|\mathbb{Q}}(d_1)\cdots\mathrm{N}_{K|\mathbb{Q}}(d_r) \\ &= \pm\mathrm{N}_{K|\mathbb{Q}}(d_1\cdots d_r) \overset{(2)}{=} \pm\mathrm{N}_{K|\mathbb{Q}}(\det(D)) \overset{(3.1)}{=} \pm\mathrm{N}_{K|\mathbb{Q}}(\det_{\mathcal{O}_K}(\varphi))\,. \end{aligned}$$

□

A.7 Discrete valuation rings and other localizations

A.7.1 Localization

In this section we recall some facts and notations concerning localization of rings and modules.

If a statement or a part of a statement is not proven here, we refer to [Dummit 04, Sec. 15.4, pp. 706-730].

Definition 117 Let A be a commutative ring. Let $\mathfrak{p} \subseteq A$ be a prime ideal, and write $S := A \setminus \mathfrak{p}$. Further, let M be an A-module.

(1.1) We define the *localization* of M at $\mathfrak{p}$ as the set

$$M_{\mathfrak{p}} := {}^{(M \times S)}\!/_{\sim} ,$$

where the equivalence relation "$\sim$" is given by

$$(m,s) \sim (m',s') :\Longleftrightarrow \text{ there exists } u \in S \text{ with } \ us'm = usm' \ \text{ for } m,m' \in M \text{ and } s,s' \in S.$$

We write

$$\frac{m}{s} := [(m,s)]_{\sim} \ \text{ for the equivalence class of } (m,s) \in M \times S.$$

The set $M_{\mathfrak{p}}$ becomes an abelian group via

$$\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'} \ \text{ for } \ m,m' \in M \text{ and } s,s' \in S.$$

(1.2) Note that $0_{M_{\mathfrak{p}}} = \frac{0_M}{1_A}$. For $m \in M$ and $s \in S$ we have

$$\frac{m}{s} = \frac{0_M}{1_A} \iff \text{there exists } u \in S \text{ with } \ um = 0_M .$$

(1.3) We have the $\mathbb{Z}$-linear map $\lambda := \lambda_{M,\mathfrak{p}} : M \longrightarrow M_{\mathfrak{p}}$, $m \longmapsto \frac{m}{1_A}$.

(2.1) Considering A as an A-module, we obtain the abelian group $A_{\mathfrak{p}}$, on which we define the multiplication

$$\frac{a}{t} \cdot \frac{b}{s} := \frac{ab}{ts} \ \text{ for } \ a,b \in A \text{ and } t,s \in S.$$

So $A_{\mathfrak{p}}$ becomes a commutative ring with identity element $1_{A_{\mathfrak{p}}} = \frac{1_A}{1_A}$.

(2.2) The map $\lambda_{A,\mathfrak{p}}$ of (1.3) is a morphism of rings.

(2.3) The abelian group $M_{\mathfrak{p}}$ becomes an $A_{\mathfrak{p}}$-module via

$$\frac{a}{t} \cdot \frac{m}{s} := \frac{am}{ts} \ \text{ for } \ a \in A,\ m \in M \text{ and } t,s \in S.$$

More generally, let (B,φ) be a commutative A-algebra. Let M be a B-module. Everything else stays the same. Write $am := \varphi(a)m$ for $a \in A$ and $m \in M$.

(3.1) Considering B as an A-module via φ, we obtain the abelian group $B_{\mathfrak{p}}$, on which we define the multiplication

$$\frac{b}{s} \cdot \frac{c}{t} := \frac{bc}{st} \ \text{ for } \ b,c \in B,\ s,t \in S.$$

So $B_{\mathfrak{p}}$ becomes a commutative ring with identity element $1_{B_{\mathfrak{p}}} = \frac{1_B}{1_A}$.

(3.2) Then $B_{\mathfrak{p}}$ becomes an $A_{\mathfrak{p}}$-algebra via $\varphi_{\mathfrak{p}} : A_{\mathfrak{p}} \longrightarrow B_{\mathfrak{p}}$, $\frac{a}{s} \longmapsto \frac{\varphi(a)}{s}$, where $a \in A$ and $s \in S$.

(3.3) Moreover, $M_{\mathfrak{p}}$ becomes a $B_{\mathfrak{p}}$-module via

$$\frac{b}{t} \cdot \frac{m}{s} := \frac{bm}{ts} \quad \text{for} \quad b \in B,\, m \in M \text{ and } t, s \in S.$$

Proof of (3.1). Suppose given $\frac{b}{s}$, $\frac{b'}{s'} \in B_{\mathfrak{p}}$ with $\frac{b}{s} = \frac{b'}{s'}$, i.e. there exists $u \in S$ with $us'b = usb'$. For $c \in B$ and $t \in S$ we obtain $us'tbc = ustb'c$, whence $\frac{bc}{st} = \frac{b'c}{s't}$. So the multiplication is well-defined in the first component. The well-definedness in second component is shown analogously. Altogether, the multiplication is well-defined.

Since A, B are commutative rings we see that the multiplication is associative, commutative and unital. Distributivity is checked by a calculation.

Proof of (3.2). Suppose given $\frac{a}{s}$, $\frac{a'}{s'} \in A_{\mathfrak{p}}$ with $\frac{a}{s} = \frac{a'}{s'}$, i.e. there exists $u \in S$ with $us'a = usa'$. Then we have $us' \cdot \varphi(a) = \varphi(us')\varphi(a) = \varphi(us'a) = \varphi(usa') = us \cdot \varphi(a')$, so that $\frac{\varphi(a)}{s} = \frac{\varphi(a')}{s'}$. We have $\varphi_{\mathfrak{p}}\big(\frac{1_A}{1_A}\big) = \frac{\varphi(1_A)}{1_A} = \frac{1_B}{1_A}$. Since φ is additive and multiplicative we see that $\varphi_{\mathfrak{p}}$ is also additive and multiplicative. Cf. also Remark 122 below.

Proof of (3.3). By (1.1) $M_{\mathfrak{p}}$ is an abelian group.

Suppose given $\frac{b}{t}$, $\frac{b'}{t'} \in B_{\mathfrak{p}}$ with $\frac{b}{t} = \frac{b'}{t'}$, i.e. there exists $u \in S$ with $ut'b = utb'$. For $m \in M$ and $s \in S$ we obtain $ut'sbm = utsb'm$, whence $\frac{bm}{ts} = \frac{b'm}{t's}$. So the multiplication is well-defined in the first component.

Suppose given $\frac{m}{s}$, $\frac{m'}{s'} \in M_{\mathfrak{p}}$ with $\frac{m}{s} = \frac{m'}{s'}$, i.e. there exists $u \in S$ with $us'm = usm'$. For $b \in B$ and $t \in S$ we obtain $uts'bm = utsbm'$, whence $\frac{bm}{ts} = \frac{bm'}{ts'}$. So the multiplication is well-defined in the second component.

We have $\frac{1_B}{1_A} \cdot \frac{m}{s} = \frac{m}{s}$. The associativity follows by the associativities of A and the B-module structure of M. Distributivity is checked by a calculation. □

Remark 118

(i) The map $\lambda_{M,\mathfrak{p}}$, given in Definition 117 (1.3)*, is injective if and only if the multiplication map $t(-) : M \longrightarrow M$, $m \longmapsto tm$ is injective for $t \in S$.*

(ii) The map $\lambda_{A,\mathfrak{p}}$, cf. Definition 117 (1.3, 2.2)*, is injective if and only if S contains no zero divisors.*

In particular, if A is an integral domain then $\lambda_{A,\mathfrak{p}} : A \longrightarrow A_{\mathfrak{p}}$ is injective.

Remark 119 *Let A be integral domain. We consider the prime ideal $(0) \subseteq A$. Then we have*

$$A_{(0)} = \operatorname{frac}(A) =: K\,.$$

Suppose given a prime ideal $\mathfrak{p} \subseteq A$.

We consider A as a subring of $A_{\mathfrak{p}}$ via the identification $a = \frac{a}{1} = \lambda_{A,\mathfrak{p}}(a)$ for $a \in A$, cf. Remark 118 *(ii).*

Likewise, we consider $A_{\mathfrak{p}}$ as a subring of K.

So we have the identification

$$\begin{array}{ccccc} & & \frac{a}{s} & \longmapsto & \frac{a}{s} \\ A & \hookrightarrow & A_{\mathfrak{p}} & \hookrightarrow & K\,. \\ a & \longmapsto & \frac{a}{1} & & \end{array}$$

More generally, given an extension $A \subseteq B$ of integral domains, we write $L := \mathrm{frac}(B)$ and obtain the identification

$$\begin{array}{ccccc} & & \frac{b}{s} & \longmapsto & \frac{b}{s} \\ B & \hookrightarrow & B_{\mathfrak{p}} & \hookrightarrow & L\,. \\ b & \longmapsto & \frac{b}{1} & & \end{array}$$

Remark 120 *Let A be integral domain and $\mathfrak{p} \subseteq A$ be a prime ideal. Let M be a finitely generated free A-module. Then we may identify*

$$m \;=\; \frac{m}{1} \;=\; \lambda_{M,\mathfrak{p}}(m) \in M_{\mathfrak{p}}\,,$$

and view M as a subset of $M_{\mathfrak{p}}$.

Proof. Given $s \in A \setminus \mathfrak{p}$ and $m \in M$ such that $sm = 0$, then $m = 0$; cf. Remark 118 *(i)*. □

Corollary 121 *Let $A \subseteq B$ be an extension of integral domains. Let $\mathfrak{p} \subseteq A$ be a prime ideal. Let $k \in \mathbb{Z}_{\geq 1}$. As in* Remark 119 *we consider $(B_{\mathfrak{p}})^{\times k}$ and $\left(B^{\times k}\right)_{\mathfrak{p}}$ as subsets of $\mathrm{frac}(B)^{\times k}$. Then we have*

$$(B_{\mathfrak{p}})^{\times k} \;=\; \left(B^{\times k}\right)_{\mathfrak{p}} \text{ as subsets of } \mathrm{frac}(B)^{\times k}\,.$$

Proof. We have to show the vertical equality in

$$\begin{array}{rcccl} \left(B^{\times k}\right)_{\mathfrak{p}} & = & \left\{ \frac{(r_i)_{i\in[1,k]}}{s} \,:\, r_i \in B \text{ for } i \in [1,k], s \in A \setminus \mathfrak{p} \right\} & \subseteq & \mathrm{frac}(B)^{\times k} \\ & & \| \text{ !} & & \\ (B_{\mathfrak{p}})^{\times k} & = & \left\{ \left(\frac{r_i}{s_i}\right)_{i\in[1,k]} \,:\, r_i \in B \text{ for } i \in [1,k], s_i \in A \setminus \mathfrak{p} \text{ for } i \in [1,k] \right\} & \subseteq & \mathrm{frac}(B)^{\times k}\,. \end{array}$$

The inclusion "$\cap\mid$" holds using entries $\frac{r_i}{s}$ for $i \in [1,k]$.

Ad "$\mid\cup$". Let $s := \prod_{i=1}^{k} s_i \in A \setminus \mathfrak{p}$. Then $ss_i^{-1} \in A$ for $i \in [1,k]$, and $\left(\frac{r_i}{s_i}\right)_{i\in[1,k]} = \frac{(r_i s s_i^{-1})_{i\in[1,k]}}{s}$. □

Remark 122 *Let A be a commutative ring and $\mathfrak{p} \subseteq A$ be a prime ideal. Further, let $f : M \longrightarrow N$ and $g : N \longrightarrow P$ be morphisms of A-modules.*

Then we have

(i) The map $f_{\mathfrak{p}} : M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$, $\frac{m}{s} \longmapsto \frac{f(m)}{s}$ is a morphism of $A_{\mathfrak{p}}$-modules.

(ii) The localization of maps as in (i) is compatible with composition, i.e.

$$(g \circ f)_{\mathfrak{p}} \;=\; g_{\mathfrak{p}} \circ f_{\mathfrak{p}}\,.$$

Let $A \subseteq B$ be an extension of integral domains. Let $\mathfrak{p} \subseteq A$ be a prime ideal. Let $h : M' \longrightarrow N'$ be a morphism of B-modules.

Then we have

(iii) The map $h_{\mathfrak{p}} : M'_{\mathfrak{p}} \longrightarrow N'_{\mathfrak{p}}$, $\frac{m'}{s} \longmapsto \frac{h(m')}{s}$ is a morphism of $B_{\mathfrak{p}}$-modules.

For the $B_{\mathfrak{p}}$-module structures of $M'_{\mathfrak{p}}$ and $N'_{\mathfrak{p}}$ we refer to Definition 117 (3.1-3.3).

Proof of *(ii)*. For $\frac{m}{s} \in M_{\mathfrak{p}}$ we have $(g \circ f)_{\mathfrak{p}}\big(\frac{m}{s}\big) = \frac{g(f(m))}{s} = g_{\mathfrak{p}}\big(f_{\mathfrak{p}}\big(\frac{m}{s}\big)\big)$.

Proof of *(iii)*. By *(i)* we have that $h_{\mathfrak{p}}$ is well-defined and $\mathbb{Z}$-linear. For $\frac{b}{t} \in B_{\mathfrak{p}}$ and $\frac{m'}{s} \in M'_{\mathfrak{p}}$ we have

$$h_{\mathfrak{p}}\Big(\frac{b}{t} \cdot \frac{m'}{s}\Big) = h_{\mathfrak{p}}\Big(\frac{bm'}{ts}\Big) = \frac{h(bm')}{ts} = \frac{bh(m')}{ts} = \frac{b}{t} \cdot \frac{h(m')}{s} = \frac{b}{t} \cdot h_{\mathfrak{p}}\Big(\frac{m'}{s}\Big)\,.$$

□

Lemma 123 *Let A be a commutative ring and $\mathfrak{p} \subseteq A$ be a prime ideal. Suppose given a left exact sequence of A-modules*

$$(S1) \qquad M' \xrightarrow{g} M \xrightarrow{h} M''\,.$$

Then we have a left exact sequence of $A_{\mathfrak{p}}$-modules

$$(S2) \qquad M'_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} M_{\mathfrak{p}} \xrightarrow{h_{\mathfrak{p}}} M''_{\mathfrak{p}}\,.$$

If additionally h is surjective, i.e. $(S1)$ is a short exact sequence, then $(S2)$ is also a short exact sequence.

Proof. By Remark 122 *(i)* we have that $g_{\mathfrak{p}}$ and $h_{\mathfrak{p}}$ are morphisms of $A_{\mathfrak{p}}$-modules.

We show injectivity of $g_{\mathfrak{p}}$. Suppose given $\frac{m'}{s} \in M'_{\mathfrak{p}}$ such that $g_{\mathfrak{p}}\Big(\frac{m'}{s}\Big) = 0_{M_{\mathfrak{p}}}$.

Then $\frac{g(m')}{s} \overset{\text{R.122}}{\underset{(i)}{=}} g_{\mathfrak{p}}\Big(\frac{m'}{s}\Big) = 0_{M_{\mathfrak{p}}} = \frac{0}{1}$. Thus, by Definition 117 (1.2), there exists $u \in S$ with

$$g(um') \overset{g\ A\text{-lin.}}{=} ug(m') = 0\,.$$

Since g is injective we have $um' = 0$. By Definition 117 (1.2) we therefore have

$$\frac{m'}{s} = \frac{0}{1} = 0_{M'_{\mathfrak{p}}}\,.$$

We show that $\operatorname{im}(g_{\mathfrak{p}}) \overset{!}{=} \ker(h_{\mathfrak{p}})$.

We prove the inclusion "$\supseteq$". Suppose given $\frac{m}{s} \in \ker(h_{\mathfrak{p}})$. So we have

$$\frac{h(m)}{s} = h_{\mathfrak{p}}\Big(\frac{m}{s}\Big) = 0_{M''_{\mathfrak{p}}} = \frac{0}{1}\,.$$

Thus, by Definition 117 (1.2), there exists $u \in S$ with $h(um) \overset{h\ A\text{-lin.}}{=} uh(m) = 0$, so that $um \in \ker(h)$.

Since $\operatorname{im}(g) = \ker(h)$, we therefore get that there exists $m' \in M'$ with $g(m') = um$.

Hence

$$g_{\mathfrak{p}}\Big(\frac{m'}{su}\Big) = \frac{g(m')}{su} = \frac{um}{su} = \frac{m}{s}\,, \quad \text{i.e.} \quad \frac{m}{s} \in \operatorname{im}(g_{\mathfrak{p}})\,.$$

We prove the inclusion "$\subseteq$". We have

$$h_{\mathfrak{p}} \circ g_{\mathfrak{p}} \overset{\text{R.122}}{\underset{(ii)}{=}} (h \circ g)_{\mathfrak{p}} \overset{\operatorname{im}(g)=\ker(h)}{\downarrow} = 0_{\mathfrak{p}} = 0\,.$$

Therefore we have $\operatorname{im}(g_{\mathfrak{p}}) \subseteq \ker(h_{\mathfrak{p}})$. So we have shown that $(S2)$ is a left exact sequence.

Now let h additionally be surjective. We have to prove surjectivity of $h_{\mathfrak{p}}$. Suppose given $\frac{m''}{s} \in M''_{\mathfrak{p}}$. Since h is surjective there exists $m \in M$ with $h(m) = m''$.

Therefore we have

$$h_{\mathfrak{p}}\Big(\frac{m}{s}\Big) = \frac{h(m)}{s} = \frac{m''}{s}\,.$$

□

Corollary 124 *Let $A \subseteq B$ be an extension of integral domains. Let $\mathfrak{p} \subseteq A$ be a prime ideal and M be a B-module. Let $N \subseteq M$ be a submodule.*

Then we have the isomorphism of $B_\mathfrak{p}$-modules

$$\begin{array}{ccc} \left(M/N\right)_\mathfrak{p} & \xrightarrow{\sim} & M_\mathfrak{p}/N_\mathfrak{p} \\ \frac{m+N}{s} & \longmapsto & \frac{m}{s} + N_\mathfrak{p}\,. \end{array}$$

Proof. We have the short exact sequence of B-modules

$$N \xrightarrow{\iota} M \xrightarrow{\rho_\iota} M/N\,,$$

where ι is the canonical embedding, and ρ_ι is the residue class map. By Remark 122 *(iii)* and Lemma 123, the upper row in the following diagram is a short exact sequence of $B_\mathfrak{p}$-modules.

$$\begin{array}{ccccc} N_\mathfrak{p} & \xrightarrow{\iota_\mathfrak{p}} & M_\mathfrak{p} & \xrightarrow{(\rho_\iota)_\mathfrak{p}} & \left(M/N\right)_\mathfrak{p} \\ \| & \circlearrowright & \| & & \\ N_\mathfrak{p} & \xrightarrow{\iota_\mathfrak{p}} & M_\mathfrak{p} & \xrightarrow{\rho_{(\iota_\mathfrak{p})}} & M_\mathfrak{p}/N_\mathfrak{p} \end{array}$$

Here, $\rho_{(\iota_\mathfrak{p})}$ is the residue class map. So also the lower row is short exact. Hence there exists a unique $B_\mathfrak{p}$-linear map $(M/N)_\mathfrak{p} \longrightarrow M_\mathfrak{p}/N_\mathfrak{p}$ making the diagram commutative, which is an isomorphism. This map necessarily acts on elements as stated above. □

Corollary 125 *Let $A \subseteq B$ be an extension of integral domains. Let $\mathfrak{p} \subseteq A$ be a prime ideal. Let $x \in B$ and $k \in \mathbb{Z}_{\geq 1}$. We denote the residue class map by $\rho : B^{k\times 1} \longrightarrow B^{k\times 1}/xB^{k\times 1}$, $r \longmapsto r + xB^{k\times 1}$.*

Suppose given a matrix $M \in B^{k\times k}$.

Let $N \subseteq B^{k\times 1}$ be the kernel of $\rho \circ (M(-))$, i.e. $N = \left\{\, v \in B^{k\times 1} \,:\, Mv \in xB^{k\times 1} \,\right\}$.

Then $N_\mathfrak{p} = \left\{\, w \in B_\mathfrak{p}^{k\times 1} \,:\, Mw \in xB_\mathfrak{p}^{k\times 1} \,\right\}$.

Proof. The lower row in the following diagram is left exact.

$$\begin{array}{ccccc} & & & & B^{k\times 1} \\ & & & \overset{M(-)}{\nearrow} & \circlearrowright & \overset{\rho}{\searrow} \\ N & \xrightarrow{\iota} & B^{k\times 1} & & \xrightarrow[\rho\circ(M(-))]{} & & B^{k\times 1}/xB^{k\times 1}\,, \end{array}$$

where ι denotes the canonical embedding.

By Remark 122 *(iii)* and Lemma 123 we have the left exact sequence of $B_\mathfrak{p}$-modules

$$N_\mathfrak{p} \xrightarrow{\iota_\mathfrak{p}} \left(B^{k\times 1}\right)_\mathfrak{p} \xrightarrow[(\rho\circ(M(-)))_\mathfrak{p}]{} \left(B^{k\times 1}/xB^{k\times 1}\right)_\mathfrak{p}\,.$$

By Corollary 124 we have the isomorphism

$$\begin{array}{ccccccc} \varphi & : & \left(B^{k\times 1}/xB^{k\times 1}\right)_\mathfrak{p} & \xrightarrow{\sim} & (B^{k\times 1})_\mathfrak{p}/(xB^{k\times 1})_\mathfrak{p} & \overset{\text{C.121}}{=} & (B_\mathfrak{p})^{k\times 1}/x(B_\mathfrak{p})^{k\times 1} \\ & & \frac{v+xB^{k\times 1}}{s} & \longmapsto & \frac{v}{s} + (xB^{k\times 1})_\mathfrak{p} & \underset{\text{C.121}}{=} & \frac{v}{s} + x(B_\mathfrak{p})^{k\times 1}\,, \end{array}$$

where $v \in B^{k\times 1}$ and $s \in A \setminus \mathfrak{p}$.

Thus, viewing $N_{\mathfrak{p}}$ as a submodule of $(B^{k\times 1})_{\mathfrak{p}} \overset{\text{C.121}}{=} (B_{\mathfrak{p}})^{k\times 1}$ via $\iota_{\mathfrak{p}}$, we get

$$N_{\mathfrak{p}} \;=\; \ker((\rho\circ(M(-)))_{\mathfrak{p}}) \underset{(ii)}{\overset{\text{R.122}}{=}} \ker(\varphi\circ\rho_{\mathfrak{p}}\circ(M(-))_{\mathfrak{p}}) \;=\; \left\{\, w\in(B_{\mathfrak{p}})^{k\times 1} \;:\; Mw\in x(B_{\mathfrak{p}})^{k\times 1}\,\right\},$$

as asserted. □

Remark 126 *Let R be a commutative ring and $\mathfrak{m}\subseteq R$ be a maximal ideal of R.*

Then we have the isomorphism of rings

$$\begin{array}{rccc}\varphi: & {}^{R}\!/_{\mathfrak{m}} & \xrightarrow{\sim} & {}^{R_{\mathfrak{m}}}\!/_{\mathfrak{m}_{\mathfrak{m}}} \\ & r+\mathfrak{m} & \longmapsto & \frac{r}{1}+\mathfrak{m}_{\mathfrak{m}}\,.\end{array}$$

In particular, $\mathfrak{m}_{\mathfrak{m}}$ is a maximal ideal of $R_{\mathfrak{m}}$.

Proof. Write $S:=R\setminus\mathfrak{m}$. Let $r+\mathfrak{m}$, $r'+\mathfrak{m}\in\left({}^{R}\!/_{\mathfrak{m}}\right)$ with $r+\mathfrak{m}=r'+\mathfrak{m}$, i.e. $r-r'\in\mathfrak{m}$. $\quad(*)$

So we have

$$\left(\frac{r}{1}+\mathfrak{m}_{\mathfrak{m}}\right)-\left(\frac{r'}{1}+\mathfrak{m}_{\mathfrak{m}}\right) \;=\; \frac{r-r'}{1}+\mathfrak{m}_{\mathfrak{m}} \overset{(*)}{=} 0+\mathfrak{m}_{\mathfrak{m}}\,,$$

whence φ is well-defined.

We see that φ is additive, multiplicative and preserves 1; cf. Definition 117 (1.1,2.1). So altogether, φ is a morphism of rings.

We show injectivity of φ. Since ${}^{R}\!/_{\mathfrak{m}}$ is a field it suffices to show that $1\overset{!}{\notin}\mathfrak{m}_{\mathfrak{m}}$, because then ${}^{R_{\mathfrak{m}}}\!/_{\mathfrak{m}_{\mathfrak{m}}}$ is not the zero ring.

We **assume** that $\frac{1}{1}=\frac{m}{s}$, where $m\in\mathfrak{m}$ and $s\in S$. Then there exists $t\in S$ with $ts=tm\in\mathfrak{m}$. Since $\mathfrak{m}$ is a prime ideal we get $t\in\mathfrak{m}$ or $s\in\mathfrak{m}$ in **contradiction** to $t,s\in S$.

We show surjectivity of φ.

First, we need an auxiliary assertion. Suppose given $\frac{x}{s}\in R_{\mathfrak{m}}$. We claim that $\frac{x}{s}\in\mathfrak{m}_{\mathfrak{m}}$ if and only if $x\in\mathfrak{m}$. It suffices to show the direct implication. If $\frac{x}{s}=\frac{m}{t}$ for some $m\in\mathfrak{m}$ and $t\in S$, then there exists $u\in S$ such that $utx=usm\in\mathfrak{m}$. Since $\mathfrak{m}$ is a prime ideal and $u,t\in S$, we obtain $x\in\mathfrak{m}$. This proves the claim.

Now suppose given $\frac{r}{s}+\mathfrak{m}_{\mathfrak{m}}\in{}^{R_{\mathfrak{m}}}\!/_{\mathfrak{m}_{\mathfrak{m}}}$, where $r\in R$ and $s\in S$.

We have to show that there exists $x\in R$ with $\frac{x}{1}+\mathfrak{m}_{\mathfrak{m}}=\frac{r}{s}+\mathfrak{m}_{\mathfrak{m}}$, i.e. $\frac{x}{1}-\frac{r}{s}=\frac{xs-r}{s}\in\mathfrak{m}_{\mathfrak{m}}$, i.e., using the claim, $xs-r\in\mathfrak{m}$. This is equivalent to the existence of $x\in R$ with $(x+\mathfrak{m})(s+\mathfrak{m})=(r+\mathfrak{m})$. Since $s\notin\mathfrak{m}$ and ${}^{R}\!/_{\mathfrak{m}}$ is a field, we have $s+\mathfrak{m}\in\mathrm{U}\left({}^{R}\!/_{\mathfrak{m}}\right)$, so that our desired $x\in R$ can be chosen as an arbitrary representative of the residue class $(r+\mathfrak{m})(s+\mathfrak{m})^{-1}$. □

Corollary 127 *Let $q\in\mathbb{Z}_{\geq 2}$ be a prime. Then we have the isomorphism of $\mathbb{F}_q$-algebras*

$$\begin{array}{rccc}\varrho: & \mathbb{F}_q={}^{\mathbb{Z}}\!/_{q\mathbb{Z}} & \xrightarrow{\sim} & {}^{\mathbb{Z}_{(q)}}\!\big/_{q\mathbb{Z}_{(q)}} \\ & z+q\mathbb{Z} & \longmapsto & \frac{z}{1}+q\mathbb{Z}_{(q)}\,.\end{array}$$

Proof. We have $q\mathbb{Z}=:(q)\subseteq\mathbb{Z}$ is a maximal ideal. Further we have

$$(q)_{(q)}=\left\{\frac{a}{s}\;:\;a\in(q),\,s\in\mathbb{Z}\setminus(q)\right\}=\left\{q\cdot\frac{b}{s}\;:\;b\in\mathbb{Z},\,s\in\mathbb{Z}\setminus(q)\right\}=q\mathbb{Z}_{(q)}\,.$$

So we obtain by Remark 126 that ϱ is an isomorphism of rings.

Moreover, we have $q\mathbb{F}_q = 0$ and $q\Big(\mathbb{Z}_{(q)}\Big/q\mathbb{Z}_{(q)}\Big) = 0$. So we get by Remark 107 that ϱ is an isomorphism of $\mathbb{F}_q$-algebras. □

Lemma 128 *Let R be a principal ideal domain and $\pi R = (\pi) \subseteq R$ be a prime ideal of R. Let $\alpha \in \mathbb{Z}_{\geq 0}$ and M, N be finitely generated free R-modules with*

$$\pi^\alpha M \subseteq N \subseteq M\,, \quad \textit{i.e.} \ \ \pi^\alpha\Big(M\Big/N\Big) = 0\,.$$

So $N \subseteq M \subseteq M_{(\pi)}$ and $N \subseteq N_{(\pi)} \subseteq M_{(\pi)}$; cf. Remark 120.

Then we have

$$M \cap N_{(\pi)} = N\,.$$

Proof. We see that the inclusion "$\supseteq$" is true.

Ad "$\subseteq$". Suppose given $x \in M \cap N_{(\pi)}$. Then

$$\frac{m}{1} = x = \frac{n}{s} \quad \text{with } m \in M, n \in N \text{ and } s \in R \setminus (\pi)\,.$$

So there exists $u \in R \setminus (\pi)$ with $usm = un$. Since M is torsion-free we get $sm = n$. Hence we have $s(m+N) = sm + N = 0 + N = 0\,.$ (1)

By the structure theorem for finitely generated modules over a principal ideal domain we have a decomposition

$$M\Big/N \ \simeq \ \bigoplus_{i=1}^{k} R\Big/\Big(q_i^{\beta_i}\Big)\,, \tag{2}$$

where $k \in \mathbb{Z}_{\geq 0}$, $\beta_i \in \mathbb{Z}_{\geq 1}$ for $i \in [1,k]$ and $q_i \in R$ are prime elements of R for $i \in [1,k]$.

We **assume** that there exists $j \in [1,k]$ with $(q_j) \neq (\pi)$. By (2) and since $\pi^\alpha\Big(M\Big/N\Big) = 0$ we get

$$\pi^\alpha r + \Big(q_j^{\beta_j}\Big) = 0 + \Big(q_j^{\beta_j}\Big) \text{ for all } r \in R \text{ , i.e. } \pi^\alpha r \in \Big(q_j^{\beta_j}\Big) \text{ for all } r \in R.$$

Choosing $r = 1$ we get $\pi^\alpha \in \Big(q_j^{\beta_j}\Big)$. Since q_j is prime we therefore get that $q_j | \pi$. (3)

So there exists $x \in R$ with $q_j x = \pi$, in particular $\pi | q_j x$. Since π is prime we get $\pi | q_j$ or $\pi | x$.

In the case $\pi | q_j$ we get with (3) that $(q_j) = (\pi)$ in **contradiction** to our assumption.

In the case $\pi | x$ we get a **contradiction** to the fact that q_j, as a prime element, is not a unit.

So $(q_i) = (\pi)$ for $i \in [1,k]$, whence (2) becomes

$$M\Big/N \ \simeq \ \bigoplus_{i=1}^{k} R\Big/\big(\pi^{\beta_i}\big)\,. \tag{4}$$

We now **assume** that $m \notin N$. So we get by (1) that s annihilates $m + N \in \Big(M\Big/N\Big) \setminus \{0\}$. Hence we get with (4) that $s \in (\pi)$ in **contradiction** to the choice of $s \in R \setminus (\pi)$.

Therefore we have $m \in N$, whence $x = \frac{m}{1} = m \in N$. □

A.7.2 Dedekind domains and discrete valuation rings

Definition 129 A *discrete valuation ring* R is a local principal ideal domain that is not a field.

Remark 130 *Let R be a discrete valuation ring with maximal ideal generated by $\pi \in R$. Then every element $x \in R \setminus \{0\}$ is of the form $x = u\pi^a$, where $u \in \mathrm{U}(R) = R \setminus \pi R$ and $a \in \mathbb{Z}_{\geq 0}$.*

The exponent a in this representation of x is unique, whence we can define the valuation v_π as

$$\begin{aligned} \mathrm{v}_\pi \;:\; R \setminus \{0\} &\longrightarrow \mathbb{Z}_{\geq 0} \\ x = u\pi^a &\longmapsto \mathrm{v}_\pi\big(u\pi^a\big) := a\,. \end{aligned}$$

For $x, y \in R$, we have

$$\begin{aligned} &\textit{(i)} && \mathrm{v}_\pi(x \cdot y) &&= \mathrm{v}_\pi(x) + \mathrm{v}_\pi(y)\,, \\ &\textit{(ii)} && \mathrm{v}_\pi(x + y) &&\geq \min\{\,\mathrm{v}_\pi(x)\,,\,\mathrm{v}_\pi(y)\,\}\,, \quad \textit{and} \\ &\textit{(iii)} && \mathrm{v}_\pi(x + y) &&= \min\{\,\mathrm{v}_\pi(x)\,,\,\mathrm{v}_\pi(y)\,\} \quad \textit{if } \mathrm{v}_\pi(x) \neq \mathrm{v}_\pi(y)\,. \end{aligned}$$

Proof. We refer to [Serre 79, Ch. I, §1, pp. 5/6]. Concerning *(iii)*, note that given $0 \leq a < b$ in $\mathbb{Z}$ and $u,\, u' \in \mathrm{U}(R)$, we obtain $u\pi^a + u'\pi^b = (u + \pi^{b-a}u')\pi^a$, where $u + \pi^{b-a}u' \in R \setminus \pi R = \mathrm{U}(R)$. So $\mathrm{v}_\pi(u\pi^a + u'\pi^b) = a$.

Definition 131 Let A be a noetherian integral domain. Then we call A a *Dedekind domain* if $A_\mathfrak{p}$ is a discrete valuation ring for every prime ideal $\mathfrak{p} \neq 0$ of A.

Cf. [Serre 79, Ch. I, §3, p. 10, Proposition 4 and the subsequent definition].

Remark 132 *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. We refer to [Neukirch 99, Ch. I, pp. 17/18, Theorem (3.1), Definition (3.2)]. Note that the definition in loc. cit. is equivalent to our Definition 131 by [Serre 79, Ch. I, §3, p. 10, Proposition 4]. □

Definition 133 Let A be a Dedekind domain and $K := \mathrm{frac}(A)$.

(1) A *fractional ideal* of K is a finitely generated A-submodule $0 \neq \mathfrak{a}$ of K;
cf. [Neukirch 99, Ch. I, p. 21, Definition (3.7)].

(2) Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of K. Then we write $\mathfrak{a} \cdot \mathfrak{b}$ for the A-submodule of K that is generated by products of the form $a \cdot b$ with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

Lemma 134 *Let A be a Dedekind domain and $K := \mathrm{frac}(A)$. We denote by J_K the set of all fractional ideals of K. Then J_K becomes an abelian group with the multiplication as defined in* Definition 133 (2). *It is called the* ideal group *of K.*

The identity element is $1_{J_K} = A$, and the inverse of $\mathfrak{a} \in J_K$ is

$$\mathfrak{a}^{-1} = \{\, x \in K \,:\, x\mathfrak{a} \subseteq A \,\}\,.$$

Proof. We refer to [Neukirch 99, Ch. I, p. 21, Proposition (3.8)]. □

Lemma 135 *Let A be a Dedekind domain and $K := \mathrm{frac}(A)$. Denote by P the set of the nonzero prime ideals of A.*

(i) Let $\mathfrak{a}$ be a fractional ideal of K. Then $\mathfrak{a}$ admits a unique (up to the order of the factors) representation as a product

$$\mathfrak{a} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_\mathfrak{p}} \quad \text{with } \alpha_\mathfrak{p} \in \mathbb{Z} \text{ for } \mathfrak{p} \in P, \text{ and } \alpha_\mathfrak{p} = 0 \text{ for almost all } \mathfrak{p} \in P.$$

(ii) Let $0 \neq \mathfrak{a} \subseteq A$ be an ideal of A. Then $\mathfrak{a}$ admits a unique (up to the order of the factors) representation as a product

$$\mathfrak{a} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_\mathfrak{p}} \quad \text{with } \alpha_\mathfrak{p} \in \mathbb{Z}_{\geq 0} \text{ for } \mathfrak{p} \in P, \text{ and } \alpha_\mathfrak{p} = 0 \text{ for almost all } \mathfrak{p} \in P.$$

(iii) We have

$$\left\{ \mathfrak{a} \subseteq K : \mathfrak{a} \text{ is a fractional ideal of } K \text{ and } \mathfrak{a} \subseteq A \right\} = \left\{ \mathfrak{a} \subseteq A : \mathfrak{a} \text{ is an ideal of } A \text{ with } \mathfrak{a} \neq 0 \right\}.$$

Proof of *(i)* and *(ii)*. We refer to [Neukirch 99, Ch. I, p. 22, Corollary (3.9)] and [Neukirch 99, Ch. I, p. 18, Theorem (3.3)].

Proof of *(iii)*. The inclusion "$\supseteq$" follows from A being noetherian. The inclusion "$\subseteq$" follows since an ideal of A is just an A-submodule of A. □

Remark 136 *Let A be a Dedekind domain and $K := \mathrm{frac}(A)$. Denote by P the set of the nonzero prime ideals of A. Let $\alpha_\mathfrak{p}, \beta_\mathfrak{p} \in \mathbb{Z}$ for $\mathfrak{p} \in P$, where $\alpha_\mathfrak{p} = 0$ and $\beta_\mathfrak{p} = 0$ for almost all $\mathfrak{p} \in P$.*
Then we have the equivalence

$$\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_\mathfrak{p}} \subseteq \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\beta_\mathfrak{p}} \iff \alpha_\mathfrak{p} \geq \beta_\mathfrak{p} \text{ for } \mathfrak{p} \in P.$$

Proof. The implication "$\Longleftarrow$" is true since $\mathfrak{p}\mathfrak{a} \subseteq \mathfrak{a}$ for $\mathfrak{p} \in P$ and $\mathfrak{a} \in J_K$.

Ad "$\Longrightarrow$". By Lemma 134 we have

$$\mathfrak{r} := \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_\mathfrak{p}-\beta_\mathfrak{p}} = \left(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_\mathfrak{p}}\right) \cdot \left(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\beta_\mathfrak{p}}\right)^{-1} \subseteq \left(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_\mathfrak{p}}\right) \cdot \left(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_\mathfrak{p}}\right)^{-1} = A. \tag{1}$$

By Lemma 135 *(iii, ii)* the ideal $\mathfrak{r}$ of A admits a representation

$$\mathfrak{r} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\gamma_\mathfrak{p}} \text{ with } \gamma_\mathfrak{p} \in \mathbb{Z}_{\geq 0} \text{ for } \mathfrak{p} \in P, \text{ and } \gamma_\mathfrak{p} = 0 \text{ for almost all } \mathfrak{p} \in P.$$

Because of the uniqueness of the representation we therefore get with (1)

$$0 \leq \gamma_\mathfrak{p} = \alpha_\mathfrak{p} - \beta_\mathfrak{p} \text{ for } \mathfrak{p} \in P, \text{ and so } \alpha_\mathfrak{p} \geq \beta_\mathfrak{p} \text{ for } \mathfrak{p} \in P.$$

□

Lemma 137 *Let $L|K$ be an extension of number fields. Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal.*
Let $0 \neq \mathfrak{q} \subseteq \mathcal{O}_L$ be a prime ideal with $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$. Suppose that $\mathfrak{p}$ is totally ramified, more precisely, $\mathfrak{q}^s = \mathfrak{p}\mathcal{O}_L$, where $s \in \mathbb{Z}_{\geq 1}$.
Then we have

$$(\mathcal{O}_L)_\mathfrak{q} = (\mathcal{O}_L)_\mathfrak{p} \text{ considered as subrings of } L.$$

Proof. Write $A := \mathcal{O}_K$ and $B := \mathcal{O}_L$.

Ad $B_\mathfrak{p} \overset{!}{\subseteq} B_\mathfrak{q}$. We have

$$A \setminus \mathfrak{p} \;=\; A \setminus (\mathfrak{q} \cap A) \;=\; A \setminus \mathfrak{q} \;\overset{\substack{A \subseteq B \\ \downarrow}}{\subseteq}\; B \setminus \mathfrak{q}\,.$$

So every element $\frac{b}{s} \in B_\mathfrak{p}$, where $b \in B$ and $s \in A \setminus \mathfrak{p}$, is also an element of $B_\mathfrak{q}$.

Ad $B_\mathfrak{p} \overset{!}{\supseteq} B_\mathfrak{q}$. We want to show that every $t \in B \setminus \mathfrak{q}$ is invertible in $B_\mathfrak{p}$. Once this is shown, we obtain for $y \in B \subseteq B_\mathfrak{p}$ and $t \in B \setminus \mathfrak{q}$ that

$$\frac{y}{t} \;=\; y \cdot \overbrace{t^{-1}}^{\in B_\mathfrak{p}} \;\in B_\mathfrak{p}\,,$$

whence $B_\mathfrak{q} \subseteq B_\mathfrak{p}$, as required.

We have $t \in B \setminus \mathfrak{q}$ is invertible in $B_\mathfrak{p}$ if and only if $t \notin \mathfrak{m}$ for all maximal ideals $\mathfrak{m}$ of $B_\mathfrak{p}$. (1)

We see that $t = \frac{t}{1} \notin \mathfrak{q}_\mathfrak{p}$, since otherwise $t = \frac{q}{s}$ for some $q \in \mathfrak{q}$ and some $s \in A \setminus \mathfrak{p} \subseteq B \setminus \mathfrak{q}$, so $ts \in \mathfrak{q}$, but $\mathfrak{q}$ is prime and $s,\, t \notin \mathfrak{q}$, which is a contradiction.

Using (1) it therefore suffices to show that $\mathfrak{q}_\mathfrak{p}$ is the only maximal ideal of $B_\mathfrak{p}$.

By [Neukirch 99, Ch. I, p. 65, Proposition (11.1)] we get the bijection

$$\begin{array}{ccc} \{\,\text{prime ideals } \mathfrak{r} \text{ of } B \text{ with } \mathfrak{r} \cap (A \setminus \mathfrak{p}) = \emptyset\,\} & \longleftrightarrow & \{\,\text{prime ideals } \mathfrak{t} \text{ of } B_\mathfrak{p}\,\} \\ \mathfrak{r} & \longmapsto & \mathfrak{r}_\mathfrak{p} \\ \mathfrak{t} \cap B & \longmapsfrom & \mathfrak{t}\,. \end{array}$$

Since every prime ideal of $B_\mathfrak{p}$ is contained in a maximal ideal, it therefore suffices to show that

(2) $$\{\,\text{prime ideals } \mathfrak{r} \text{ of } B \text{ with } \mathfrak{r} \cap (A \setminus \mathfrak{p}) = \emptyset\,\} \overset{!}{=} \{\,0,\, \mathfrak{q}\,\}\,.$$

Now $A = \mathcal{O}_K$ and $B = \mathcal{O}_L$ are Dedekind domains; cf. Remark 132. Therefore every nonzero prime ideal of A respectively of B is maximal; cf. [Serre 79, Ch. I, §3, p. 10, Proposition 4(ii)]. (3)

Now, let $0 \neq \mathfrak{r}$ be a prime ideal of B. Then we claim

(4) $$\mathfrak{r} \cap (A \setminus \mathfrak{p}) = \emptyset \overset{!}{\iff} \mathfrak{p} \subseteq \mathfrak{r}\,.$$

Ad "$\Longrightarrow$". This will be proven by contraposition. Suppose that $\mathfrak{p} \nsubseteq \mathfrak{r}$.

Choose $y \in \mathfrak{r} \setminus \{0\}$. Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial having $f(y) = 0$. Dividing by a suitable power of y, we may assume that $f(0) \neq 0$. Then $f(0) = -(f(y) - f(0)) \in B$ is divisible by y. So $f(0) \in \mathbb{Z} \cap \mathfrak{r} \subseteq A \cap \mathfrak{r}$. In particular, $\mathfrak{p}' := A \cap \mathfrak{r} \neq 0$. Since $\mathfrak{p} \nsubseteq \mathfrak{r}$, we have $\mathfrak{p}' \neq \mathfrak{p}$. Since $\mathfrak{p}' \subseteq A$ is maximal by (3), there exists $x \in \mathfrak{p}' \setminus \mathfrak{p} = \mathfrak{r} \cap (A \setminus \mathfrak{p})$. So $\mathfrak{r} \cap (A \setminus \mathfrak{p}) \neq \emptyset$.

Ad "$\Longleftarrow$". Suppose that $\mathfrak{p} \subseteq \mathfrak{r}$. Then $\mathfrak{p} \subseteq \; A \cap \mathfrak{r} \; \subseteq A$. Since $\mathfrak{r} \subseteq B$ is prime, we have $1_A = 1_B \notin \mathfrak{r}$, whence $A \cap \mathfrak{r} \subsetneq A$. By (3) we obtain that $\mathfrak{p}$ is a maximal ideal. Therefore, $\mathfrak{p} = A \cap \mathfrak{r}$. Thus

$$\mathfrak{r} \cap (A \setminus \mathfrak{p}) \;=\; \mathfrak{r} \cap (A \setminus (A \cap \mathfrak{r})) \;=\; \mathfrak{r} \cap (A \setminus \mathfrak{r}) \;=\; \emptyset\,.$$

This proves claim (4).

So it suffices to show that

(2′) $$\{\,\text{prime ideals } \mathfrak{r} \text{ of } B \text{ with } \mathfrak{p} \subseteq \mathfrak{r}\,\} \overset{!}{=} \{\mathfrak{q}\}\,.$$

Assume that there exists a prime ideal $\mathfrak{r}$ of B with $\mathfrak{p} \subseteq \mathfrak{r}$ and $\mathfrak{r} \neq \mathfrak{q}$. So we get

$$\mathfrak{q}^s \cdot \mathfrak{r}^0 \;=\; \mathfrak{q}^s \;=\; \mathfrak{p}B \;\subseteq\; \mathfrak{r}B \;=\; \mathfrak{r} \;=\; \mathfrak{q}^0 \cdot \mathfrak{r}^1\,,$$

but this is in **contradiction** to Remark 136. □

Appendix B

On binomial coefficients

Lemma 138 (Vandermonde convolution) *Let $m \in \mathbb{Z}_{\geq 0}$ and $r, s \in \mathbb{Z}$. Then we have*

$$\sum_{k=0}^{m} \binom{r}{k} \cdot \binom{s}{m-k} = \binom{r+s}{m}.$$

Proof. To prove the statement we use the cauchy summation formula, which states the following.

Suppose given two power series

$$f(x) = \left(\sum_{i=0}^{\infty} t_i x^i \right) \quad \text{and} \quad g(x) = \left(\sum_{j=0}^{\infty} u_j x^j \right)$$

with the positive radii of convergence r_f and r_g. Then the product

$$(1) \quad f(x) \cdot g(x) = \left(\sum_{i=0}^{\infty} t_i x^i \right) \cdot \left(\sum_{j=0}^{\infty} u_j x^j \right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} t_j u_{i-j} \right) x^i =: h(x) \text{ for } |x| < \min\{ r_f , r_g \}$$

is also a power series with radius of convergence $r_h \geq \min\{ r_f , r_g \}$,

cf. [Walter 04, §7, p. 144, 7.8 Multiplikation von Potenzreihen].

Further we use the modified binomial theorem, wich states that for each $\alpha \in \mathbb{R}$ and $x \in \mathbb{R}$ with $|x| < 1$ we have

$$(2) \qquad (1+x)^{\alpha} = \sum_{m=0}^{\infty} \binom{\alpha}{m} x^m ,$$

cf. [Graham 94, Sec. 5.1, p. 163, Equation (5.13)].

So we obtain for $x \in \mathbb{R}$ with $|x| < 1$

$$\begin{aligned} \sum_{m=0}^{\infty} \binom{r+s}{m} x^m &\overset{(2)}{=} (1+x)^{r+s} = (1+x)^r \cdot (1+x)^s \\ &\overset{(2)}{=} \left(\sum_{i=0}^{\infty} \binom{r}{i} x^i \right) \cdot \left(\sum_{j=0}^{\infty} \binom{s}{j} x^j \right) \overset{(1)}{=} \sum_{m=0}^{\infty} \left(\sum_{k=0}^{m} \binom{r}{k} \cdot \binom{s}{m-k} \right) x^m , \end{aligned}$$

Since two power series are equal if and only if all of their coefficients are equal, comparing coefficients yields that the statement is true. □

Remark 139 *Let $i, l \in [1, n]$. Then we have*

$$S(i,l) := \sum_{k=1}^{n} \binom{l+k-2}{2l-2} \cdot \left\langle \begin{matrix} i-1 \\ k \end{matrix} \right\rangle = \partial_{i,l}\,.$$

For the term $\left\langle \begin{smallmatrix} i-1 \\ k \end{smallmatrix} \right\rangle$ *we refer to* Definition 34.

Proof. Since $\left\langle \begin{smallmatrix} i-1 \\ k \end{smallmatrix} \right\rangle = 0$ for $k > i$ and $\binom{l+k-2}{2l-2} = 0$ for $k < l$, we get

$$\begin{aligned} S(i,l) = \sum_{k=1}^{n} \binom{l+k-2}{2l-2} \cdot \left\langle \begin{matrix} i-1 \\ k \end{matrix} \right\rangle \quad &= \quad \sum_{k=l}^{i} \binom{l+k-2}{2l-2} \cdot \left\langle \begin{matrix} i-1 \\ k \end{matrix} \right\rangle \\ &\overset{\text{D.34}}{=} \quad \sum_{k=l}^{i} \binom{l+k-2}{2l-2} \cdot (-1)^{i-k} \cdot \left(\binom{2i-2}{i-k} - \binom{2i-2}{i-k-1} \right). \end{aligned}$$

For $i < l$ we have that $S(i,l)$ is an empty sum and the statement is true.

For $i = l$ we have

$$S(l,l) = \underbrace{\binom{l+l-2}{2l-2}}_{=1} \cdot \underbrace{(-1)^{l-l}}_{=1} \cdot \left(\underbrace{\binom{2l-2}{l-l}}_{=1} - \underbrace{\binom{2l-2}{l-l-1}}_{=0} \right) = 1\,,$$

and, again, the statement is true.

For $i > l$ we have to show that $S(i,l) \overset{!}{=} 0$. This is equivalent to

$$\sum_{k=l}^{i} \binom{l+k-2}{2l-2} \cdot (-1)^{i-k} \cdot \binom{2i-2}{i-k} \overset{!}{=} \sum_{k=l}^{i} \binom{l+k-2}{2l-2} \cdot (-1)^{i-k} \cdot \binom{2i-2}{i-k-1}.$$

We substitute $k' := k - l$ and $i' := i - l$. So we have to show for $i' > 0$ that

$$\sum_{k'=0}^{i'} \binom{2l+k'-2}{2l-2} \cdot (-1)^{i'-k'} \cdot \binom{2i'+2l-2}{i'-k'} \overset{!}{=} \sum_{k'=0}^{i'} \binom{2l+k'-2}{2l-2} \cdot (-1)^{i'-k'} \cdot \binom{2i'+2l-2}{i'-k'-1}.$$

By multiplication with $(-1)^{-i'}$ and further substitution $l' := 2l - 2$, we reformulate to

$$\sum_{k'=0}^{i'} \binom{l'+k'}{l'} \cdot (-1)^{k'} \cdot \binom{2i'+l'}{i'-k'} \overset{!}{=} \sum_{k'=0}^{i'} \binom{l'+k'}{l'} \cdot (-1)^{k'} \cdot \binom{2i'+l'}{i'-k'-1}.$$

For ease of notation, we rename $k := k'$, $i := i'$ and $l := l'$. Therefore it suffices to show that

$$\sum_{k=0}^{i} \binom{l+k}{l} \cdot (-1)^{k} \cdot \binom{2i+l}{i-k} \overset{!}{=} \sum_{k=0}^{i} \binom{l+k}{l} \cdot (-1)^{k} \cdot \binom{2i+l}{i-k-1} \tag{1}$$

for $l \geq 0$ and $i \geq 1$.

We have

$$\binom{l+k}{l} = \binom{l+k}{k} \overset{(*)}{=} (-1)^k \binom{-l-1}{k},$$

where the trick $(*)$ is taken from [Graham 94, Sec. 5.2, p. 174, Table 174 : "upper negation"].

Therefore equation (1) becomes

$$\underbrace{\sum_{k=0}^{i} \binom{-l-1}{k} \cdot \binom{2i+l}{i-k}}_{=:\,\mathrm{LS}} \overset{!}{=} \underbrace{\sum_{k=0}^{i} \binom{-l-1}{k} \cdot \binom{2i+l}{i-k-1}}_{=:\,\mathrm{RS}}. \tag{1'}$$

We have

$$\text{LS} \;=\; \sum_{k=0}^{i}\binom{-l-1}{k}\cdot\binom{2i+l}{i-k} \overset{\text{L.138}}{=} \binom{-l-1+2i+l}{i} \;=\; \binom{2i-1}{i} \quad \text{and}$$

$$\text{RS} \;=\; \sum_{k=0}^{i}\binom{-l-1}{k}\cdot\binom{2i+l}{i-k-1} \;=\; \binom{-l-1}{i}\cdot\underbrace{\binom{2i+l}{i-i-1}}_{=0}+\sum_{k=0}^{i-1}\binom{-l-1}{k}\cdot\binom{2i+l}{i-k-1}$$

$$\overset{\text{L.138}}{=} \binom{-l-1+2i+l}{i-1} \;=\; \binom{2i-1}{i-1} \;=\; \binom{2i-1}{i}.$$

Thus equation $(1')$ is shown.

In summary we have shown that $S(i,l) \;=\; \partial_{i,l}$ for $i,l\in[1,n]$. □

Corollary 140 *Let $i,l\in[1,n]$. Then we have*

$$(-1)^{i-l}\sum_{k=0}^{i-l}(-1)^k\binom{2i-1}{i-l-k}(2l+2k-1)\binom{2l+k-2}{2l-2} \;=\; (2i-1)\cdot\partial_{i,l}\,.$$

Proof. Let $i,k\in[1,n]$. Then we have

$$\left.\begin{aligned}
&\left\langle\begin{matrix} i-1 \\ k \end{matrix}\right\rangle \overset{\text{D.34}}{=} (-1)^{i-k}\left(\binom{2i-2}{i-k}-\binom{2i-2}{i-k-1}\right)\\
=\;& (-1)^{i-k}(2i-2)!\left(\frac{1}{(i-k)!(i+k-2)!}-\frac{1}{(i-k-1)!(i+k-1)!}\right)\\
=\;& (-1)^{i-k}(2i-2)!\frac{(i+k-1)-(i-k)}{(i-k)!(i+k-1)!} \;=\; (-1)^{i-k}(2i-2)!\frac{2k-1}{(i-k)!(i+k-1)!}\\
=\;& (-1)^{i-k}\frac{(2i-2)!(2i-1)}{(i-k)!(i+k-1)!}(2k-1)(2i-1)^{-1} \;=\; (-1)^{i-k}\binom{2i-1}{i-k}(2k-1)(2i-1)^{-1}.
\end{aligned}\right\}\ (*)$$

By Remark 139 we have for $i,l\in[1,n]$

$$\begin{aligned}
\partial_{i,l} \;&=\; \sum_{k=1}^{n}\underbrace{\binom{l+k-2}{2l-2}}_{=0\text{ for }k<l}\cdot\underbrace{\left\langle\begin{matrix} i-1 \\ k \end{matrix}\right\rangle}_{=0\text{ for }k>i}\\
&\overset{(*)}{=} \sum_{k=l}^{i}\binom{l+k-2}{2l-2}\cdot(-1)^{i-k}\binom{2i-1}{i-k}(2k-1)(2i-1)^{-1}\\
&\overset{\substack{k'=k-l\\ \downarrow}}{=} \sum_{k'=0}^{i-l}\binom{2l+k'-2}{2l-2}\cdot(-1)^{i-l-k'}\binom{2i-1}{i-l-k'}(2l+2k'-1)(2i-1)^{-1}\\
&\overset{\substack{k=k'\\ \downarrow}}{=} (-1)^{i-l}\sum_{k=0}^{i-l}\binom{2l+k-2}{2l-2}\cdot(-1)^{k}\binom{2i-1}{i-l-k}(2l+2k-1)(2i-1)^{-1}
\end{aligned}$$

□

Remark 141 *For $i,k\in[1,n]$ we have*

$$\frac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot\left\langle\begin{matrix}i-1\\k\end{matrix}\right\rangle=(-1)^{i-k}\cdot\binom{2i-1}{i-k}\cdot\frac{(2i)!}{2k-1}\cdot(2i-1)\in\mathbb{Z}\,.$$

Proof. For $k>i$, both sides equal 0; cf. Definition 34 and Convention 4. For $k=i$, both sides equal $(2i)!$. For $k<i$ we calculate the difference of the terms as

$$\begin{aligned}
&\tfrac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot\left\langle\begin{matrix}i-1\\k\end{matrix}\right\rangle-(-1)^{i-k}\cdot\tbinom{2i-1}{i-k}\cdot\tfrac{(2i)!}{2k-1}\cdot(2i-1)\\
\overset{\text{D.34}}{=}\;&\tfrac{(2i-1)^2}{(2k-1)^2}\cdot(2i)!\cdot(-1)^{i-k}\left(\tbinom{2i-2}{i-k}-\tbinom{2i-2}{i-k-1}\right)-(-1)^{i-k}\cdot\tbinom{2i-1}{i-k}\cdot\tfrac{(2i)!}{2k-1}\cdot(2i-1)\\
=\;&\tfrac{(2i-1)}{(2k-1)}\cdot(-1)^{i-k}\cdot(2i)!\cdot\left(\tfrac{(2i-1)}{(2k-1)}\cdot\left(\tbinom{2i-2}{i-k}-\tbinom{2i-2}{i-k-1}\right)-\tbinom{2i-1}{i-k}\right)\\
=\;&\tfrac{(2i-1)}{(2k-1)}\cdot(-1)^{i-k}\cdot(2i)!\cdot\left(\tfrac{(2i-1)}{(2k-1)}\cdot\left(\tfrac{(2i-2)!}{(i-k)!(i+k-2)!}-\tfrac{(2i-2)!}{(i-k-1)!(i+k-1)!}\right)-\tfrac{(2i-1)!}{(i-k)!(i+k-1)!}\right)\\
=\;&\tfrac{(2i-1)}{(2k-1)}\cdot(-1)^{i-k}\cdot(2i)!\cdot(2i-1)!\cdot\left(\tfrac{1}{(2k-1)}\cdot\left(\tfrac{1}{(i-k)!(i+k-2)!}-\tfrac{1}{(i-k-1)!(i+k-1)!}\right)-\tfrac{1}{(i-k)!(i+k-1)!}\right)\\
=\;&\tfrac{(2i-1)}{(2k-1)}\cdot(-1)^{i-k}\cdot(2i)!\cdot(2i-1)!\cdot\left(\tfrac{1}{(2k-1)}\cdot\tfrac{(i+k-1)-(i-k)}{(i-k)!(i+k-1)!}-\tfrac{1}{(i-k)!(i+k-1)!}\right)\\
=\;&\tfrac{(2i-1)}{(2k-1)}\cdot(-1)^{i-k}\cdot(2i)!\cdot(2i-1)!\cdot\left(\tfrac{1}{(i-k)!(i+k-1)!}-\tfrac{1}{(i-k)!(i+k-1)!}\right)\\
=\;&0\,.
\end{aligned}$$

In this case, we have $\frac{(2i)!}{2k-1}\in\mathbb{Z}$, so that the right hand side is an integer. □

Remark 142 *Let $i,s,t\in\mathbb{Z}_{\geq 0}$. Then we have*

$$\sum_{k=1}^{i}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\left(\binom{t-k+1}{s}+\binom{t+k}{s}\right)=(-1)^i\sum_{k=0}^{2i-1}(-1)^k\binom{2i-1}{k}\frac{1}{2i-1-2k}\binom{t+i-k}{s}.$$

Proof. For $i=0$, both sides equal 0. For $i\in\mathbb{Z}_{\geq 1}$ we have

$$\left.\begin{aligned}\sum_{k=1}^{i}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\binom{t-k+1}{s}&\overset{k'=1-k}{\underset{\downarrow}{=}}\sum_{k'=1-i}^{0}(-1)^{1-k'}\binom{2i-1}{i-1+k'}\frac{1}{-(2k'-1)}\binom{t+k'}{s}\\&\overset{k=k'}{\underset{\downarrow}{=}}\sum_{k=1-i}^{0}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\binom{t+k}{s}\,.\end{aligned}\right\}(*)$$

So we obtain

$$\begin{aligned}
&\sum_{k=1}^{i}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\left(\binom{t-k+1}{s}+\binom{t+k}{s}\right)\\
=\;&\sum_{k=1}^{i}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\binom{t-k+1}{s}+\sum_{k=1}^{i}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\binom{t+k}{s}
\end{aligned}$$

$$\begin{aligned}
&\overset{(*)}{=} \quad \sum_{k=1-i}^{0}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\binom{t+k}{s}+\sum_{k=1}^{i}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\binom{t+k}{s}\\
&= \quad \sum_{k=1-i}^{i}(-1)^k\binom{2i-1}{i-k}\frac{1}{2k-1}\binom{t+k}{s}\\
&\overset{k'=i-k}{=} \quad \sum_{k'=0}^{2i-1}(-1)^{i-k'}\binom{2i-1}{k'}\frac{1}{2i-2k'-1}\binom{t+i-k'}{s}\\
&\overset{k=k'}{=} \quad (-1)^i\sum_{k=0}^{2i-1}(-1)^k\binom{2i-1}{k}\frac{1}{2i-2k-1}\binom{t+i-k}{s}.
\end{aligned}$$

□

Remark 143 *Let $k,l\in\mathbb{Z}_{\geq 1}$. Then we have*

$$\frac{2k-1}{l+k-1}\binom{l+k-1}{k-l}=\binom{l+k-1}{k-l}+\binom{l+k-2}{k-l-1}\in\mathbb{Z}.$$

Proof. For $k<l$, both sides equal 0. For $k=l$, both sides equal 1. So let $k>l$. We calculate

$$\begin{aligned}
\frac{2k-1}{l+k-1}\binom{l+k-1}{k-l} &= \frac{((l+k-1)+(k-l))(l+k-1)!}{(l+k-1)(k-l)!(2l-1)!}\\
&= \frac{(l+k-1)(l+k-2)!}{(k-l)!(2l-1)!}+\frac{(k-l)(l+k-2)!}{(k-l)!(2l-1)!}\\
&= \frac{(l+k-1)!}{(k-l)!(2l-1)!}+\frac{(l+k-2)!}{(k-l-1)!(2l-1)!} = \binom{l+k-1}{k-l}+\binom{l+k-2}{k-l-1}.
\end{aligned}$$

□

Remark 144 *Let $m,j\in\mathbb{Z}_{\geq 0}$ with $m>j$. Then we have*

$$\sum_{k=0}^{m}(-1)^k\binom{m}{k}\binom{k}{j}=0.$$

Proof. We calculate

$$\begin{aligned}
&\sum_{k=0}^{m}(-1)^k\binom{m}{k}\overbrace{\binom{k}{j}}^{=0 \text{ for } k<j} &&= \sum_{k=j}^{m}(-1)^k\binom{m}{k}\binom{k}{j}\\
&= \sum_{k=j}^{m}(-1)^k\frac{m!}{k!(m-k)!}\cdot\frac{k!}{j!(k-j)!} &&= \sum_{k=j}^{m}(-1)^k\frac{(m-j)!}{(k-j)!(m-k)!}\cdot\frac{m!}{j!(m-j)!}\\
&= \sum_{k=j}^{m}(-1)^k\binom{m-j}{k-j}\binom{m}{j} &&\overset{k'=k-j}{=} \sum_{k'=0}^{m-j}(-1)^{k'+j}\binom{m-j}{k'}\binom{m}{j}\\
&= (-1)^j\binom{m}{j}\sum_{k'=0}^{m-j}(-1)^{k'}\binom{m-j}{k'} &&= (-1)^j\binom{m}{j}\cdot((1-1)^{m-j}) \overset{m\geq j}{=} 0.
\end{aligned}$$

□

Corollary 145 *Let $m, j \in \mathbb{Z}_{\geq 0}$ with $m > j$. Then we have*

$$\sum_{k=0}^{m} (-1)^k \binom{m}{k} k^j \;=\; 0\,.$$

In particular, for every polynomial $P(k) \in \mathbb{C}[k]$ of degree less than m we have

$$\sum_{k=0}^{m} (-1)^k \binom{m}{k} P(k) \;=\; 0\,.$$

Proof. Let $j \in [0, m-1]$. Suppose the statement to be true for all $s \in [1, m-1]$ with $s < j$ (I.H.). By Remark 144 we have

$$\begin{aligned} 0 \;=\; \sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{k}{j} \;&=\; \sum_{k=0}^{m} (-1)^k \binom{m}{k} \frac{k(k-1)\cdots(k-j+1)}{j!} \\ &=\; \frac{1}{j!} \sum_{k=0}^{m} (-1)^k \binom{m}{k} \underbrace{\big(k^j + g(k)\big)}_{\substack{\uparrow \\ \text{pol. in } k \text{ of} \\ \text{degree } < j, \text{ or } 0}} \;\overset{\text{I.H.}}{=}\; \frac{1}{j!} \sum_{k=0}^{m} (-1)^k \binom{m}{k} k^j\,. \end{aligned}$$

□

Remark 146 *Let $m \in \mathbb{Z}_{\geq 1}$ and $x \in \mathbb{R} \setminus [-m, 0]$. Then we have*

$$\sum_{k=0}^{m} (-1)^k \binom{m}{k} \frac{1}{x+k} \;=\; \frac{1}{x} \cdot \binom{x+m}{m}^{-1}\,.$$

Proof. We consider the map $g : \mathbb{R} \setminus \{0\} \longrightarrow \mathbb{R}$, $x \longmapsto \frac{1}{x}$. We now claim that

$$\Delta^l g(x) \;\overset{!}{=}\; (-1)^l \frac{l!}{x(x+1)\cdots(x+l)} \;\text{, for } l \in \mathbb{Z}_{\geq 0}\,. \qquad (\text{ for } \Delta^l \text{ cf. Convention 2 })$$

This is shown by induction on l. For $l = 0$ we have

$$\Delta^0 g(x) \;=\; g(x) \;=\; \frac{1}{x} \;=\; (-1)^0 \cdot \frac{0!}{x}\,.$$

For the inductive step $l \to l+1$, we calculate

$$\begin{aligned} \Delta^{l+1} g(x) \;&\overset{\text{C.2}}{=}\; \Delta^l g(x+1) - \Delta^l g(x) \\ &\overset{\text{I.H.}}{=}\; (-1)^l \cdot \frac{l!}{(x+1)(x+2)\cdots(x+l+1)} - (-1)^l \cdot \frac{l!}{x(x+1)\cdots(x+l)} \\ &=\; (-1)^l \cdot l! \cdot \frac{x - (x+l+1)}{x(x+1)(x+2)\cdots(x+l+1)} \\ &=\; (-1)^l \cdot l! \cdot \frac{-(l+1)}{x(x+1)(x+2)\cdots(x+l+1)} \\ &=\; (-1)^{l+1} \cdot \frac{(l+1)!}{x(x+1)\cdots(x+l+1)}\,. \end{aligned}$$

So our claim is shown.

Further we have

$$\Delta^l g(x) \;=\; \sum_{k=0}^{l} (-1)^{l-k} \binom{l}{k} g(x+k) \;\text{, for } l \in \mathbb{Z}_{\geq 0}\,,$$

cf. [Graham 94, Sec. 5.3, p. 188, Equation (5.40)].

Therefore, after setting $l = m$, we obtain

$$\begin{aligned} & \sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}g(x+k) &=& (-1)^m \cdot \frac{m!}{x(x+1)\cdots(x+m)} \\ \iff\quad & (-1)^m \sum_{k=0}^{m}(-1)^k\binom{m}{k}\frac{1}{x+k} &=& (-1)^m \cdot \frac{1}{x} \cdot \frac{m!}{((x+m)-m+1)\cdots(x+m)} \\ \iff\quad & \sum_{k=0}^{m}(-1)^k\binom{m}{k}\frac{1}{x+k} &=& \frac{1}{x}\cdot\binom{x+m}{m}^{-1}. \end{aligned}$$

□

Remark 147 *Suppose given $t \in \mathbb{Z}$, $i \in \mathbb{Z}_{\geq 1}$ and $s \in [0, 2i-1]$. Then we have*

$$\mathrm{L}_s := (-1)^{i+1}\sum_{k=0}^{2i-1}(-1)^k\binom{2i-1}{k}\frac{1}{2i-1-2k}\binom{t+i-k}{s} = 2^{4i-2-s}\cdot\frac{i!(i-1)!}{s!(2i)!}\cdot\prod_{u=0}^{s-1}(2t+1-2u) =: \mathrm{R}_s\,.$$

Proof. For $s = 0$ we have to show that

$$\mathrm{L}_0 = (-1)^{i+1}\sum_{k=0}^{2i-1}(-1)^k\binom{2i-1}{k}\frac{1}{2i-1-2k} \stackrel{!}{=} 2^{4i-2}\cdot\frac{i!(i-1)!}{(2i)!} = \mathrm{R}_0\,.$$

If $i = 1$, we obtain $2 = 2$.

If $i \geq 2$, we obtain

$$\begin{aligned} & (-1)^{i+1}\sum_{k=0}^{2i-1}(-1)^k\binom{2i-1}{k}\frac{1}{2i-1-2k} &=& (-1)^{i+1}\cdot\frac{1}{2}\cdot\sum_{k=0}^{2i-1}(-1)^k\binom{2i-1}{k}\frac{1}{\frac{2i-1}{2}-k} \\ =\ & (-1)^i\cdot\frac{1}{2}\cdot\sum_{k=0}^{2i-1}(-1)^k\binom{2i-1}{k}\frac{1}{-\frac{2i-1}{2}+k} &\stackrel{(*)}{=}& (-1)^i\cdot\frac{1}{2}\cdot\left(-\frac{2}{2i-1}\right)\binom{\frac{2i-1}{2}}{2i-1}^{-1} \\ =\ & \frac{(-1)^{i+1}}{2i-1}\binom{i-\frac{1}{2}}{2i-1}^{-1} &=& \frac{(-1)^{i+1}}{2i-1}\left(\frac{\left(i-\frac{1}{2}\right)\left(i-\frac{3}{2}\right)\left(i-\frac{5}{2}\right)\cdots\left(-i+\frac{3}{2}\right)}{(2i-1)!}\right)^{-1} \\ =\ & (-1)^{i+1}(2i-2)!\left((2i-1)(2i-3)\cdots 3\cdot 1\cdot(-1)\cdot(-3)\cdots(-2i+3)\cdot 2^{-(2i-1)}\right)^{-1} \\ =\ & (-1)^{i+1}(2i-2)!\left(\frac{(2i-1)!}{(i-1)!\cdot 2^{i-1}}\cdot\frac{(2i-3)!}{(i-2)!\cdot 2^{i-2}}\cdot(-1)^{i-1}\cdot 2^{-(2i-1)}\right)^{-1} \\ =\ & (2i-2)!\cdot 2^{4i-4}\cdot\frac{(i-1)!(i-2)!}{(2i-1)!(2i-3)!} &=& (2i-2)\cdot 2^{4i-4}\cdot\frac{(i-1)!(i-2)!}{(2i-1)!} \\ =\ & (i-1)\cdot 2^{4i-3}\cdot\frac{(i-1)!(i-2)!}{(2i-1)!} &=& 2^{4i-3}\cdot\frac{2i\cdot(i-1)!(i-1)!}{(2i)!} \\ =\ & 2^{4i-2}\cdot\frac{i!(i-1)!}{(2i)!}\ , \end{aligned}$$

where in $(*)$ we refer to Remark 146 applied to the case $(m, x) = \left(2i-1, -\frac{2i-1}{2}\right)$. So the statement is true for $s = 0$, i.e. $\mathrm{L}_0 = \mathrm{R}_0$.

Now let $s \in [1, 2i-1]$. We can transform L_s as follows.

$$
\begin{aligned}
\mathrm{L}_s &= (-1)^{i+1} \sum_{k=0}^{2i-1} (-1)^k \binom{2i-1}{k} \frac{1}{2i-1-2k} \binom{t+i-k}{s} \\
&= \frac{1}{2}(-1)^{i+1} \sum_{k=0}^{2i-1} (-1)^k \binom{2i-1}{k} \frac{(i-k+t)(i-k+t-1)\cdots(i-k+t-(s-2))(i-k+t-(s-1))}{(i-k-\frac{1}{2})s!} \\
&\overset{\substack{\text{write} \\ u=i-k-\frac{1}{2}}}{=} \frac{1}{2}(-1)^{i+1} \sum_{k=0}^{2i-1} (-1)^k \binom{2i-1}{k} \frac{(u+t+\frac{1}{2})(u+t+\frac{1}{2}-1)\cdots(u+t+\frac{1}{2}-(s-2))(u+t+\frac{1}{2}-(s-1))}{u \cdot s!} \\
&= \frac{1}{2s!}(-1)^{i+1} \sum_{k=0}^{2i-1} (-1)^k \binom{2i-1}{k} \Bigg(\overset{\substack{\text{pol. in } u \text{ (hence in } k) \\ \text{of degree} < 2i-1}}{\overset{\downarrow}{g(u)}} + \frac{(t+\frac{1}{2})(t+\frac{1}{2}-1)\cdots(t+\frac{1}{2}-(s-2))(t+\frac{1}{2}-(s-1))}{u} \Bigg) \\
&\overset{\text{C.145}}{=} \frac{1}{2s!}(-1)^{i+1} \sum_{k=0}^{2i-1} (-1)^k \binom{2i-1}{k} \frac{(t+\frac{1}{2})(t+\frac{1}{2}-1)\cdots(t+\frac{1}{2}-(s-2))(t+\frac{1}{2}-(s-1))}{u} \\
&= \frac{1}{s!}\left(t+\tfrac{1}{2}\right)\left(t+\tfrac{1}{2}-1\right)\cdots\left(t+\tfrac{1}{2}-(s-2)\right)\left(t+\tfrac{1}{2}-(s-1)\right)(-1)^{i+1} \sum_{k=0}^{2i-1} (-1)^k \binom{2i-1}{k} \frac{1}{2u} \\
&\overset{\substack{\text{write again} \\ i-k-\frac{1}{2}=u}}{=} \frac{1}{s!}\left(t+\tfrac{1}{2}\right)\left(t+\tfrac{1}{2}-1\right)\cdots\left(t+\tfrac{1}{2}-(s-2)\right)\left(t+\tfrac{1}{2}-(s-1)\right) \underbrace{(-1)^{i+1} \sum_{k=0}^{2i-1} (-1)^k \binom{2i-1}{k} \frac{1}{2i-1-2k}}_{=\mathrm{L}_0=\mathrm{R}_0} \\
&= \frac{1}{2^s s!}(2t+1-0)(2t+1-2)\cdots(2t+1-2(s-2))(2t+1-2(s-1)) \cdot \mathrm{R}_0 \;=\; \frac{1}{2^s s!}\left(\prod_{u=0}^{s-1}(2t+1-2u)\right) \cdot 2^{4i-2} \cdot \frac{i!(i-1)!}{(2i)!} \;=\; \mathrm{R}_s \qquad \square
\end{aligned}
$$

Bibliography

[Dummit 04] David S. Dummit & Richard M. Foote. Abstract algebra. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[Graham 94] Ronald L. Graham, Donald E. Knuth & Oren Patashnik. Concrete mathematics. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994.

[Künzer 99] Matthias Künzer. Ties for the integral group ring of the symmetric group. PhD thesis, Bielefeld, 1999.

[Lang 02] Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

[Neukirch 99] Jürgen Neukirch. Algebraic number theory, volume 322 of Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder.

[Plesken 83] Wilhelm Plesken. Group rings of finite groups over p-adic integers, volume 1026 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1983.

[Serre 79] Jean-Pierre Serre. Local fields, volume 67 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1979. Translated from the French by Marvin J. Greenberg.

[Walter 04] Wolfgang Walter. Analysis 1. Springer-Verlag, New York, seventh edition, 2004.

[Wingen 95] Herbert Wingen. On the Wedderburn structure of some integral Frobenius group rings. J. Algebra, vol. 171, no. 1, pages 294–327, 1995.

[Zimmermann 92] Alexander Zimmermann. Endliche Untergruppen der Einheitengruppe ganzzahliger Gruppenringe. PhD thesis, Universität Stuttgart, 1992.

Index

Symbols

A

B

D