On twisted group rings and Galois-stable ideals

Bachelor's thesis

in partial fulfillment of the requirements for the degree of
Bachelor of Science in Mathematics

Universität Stuttgart

Nora Krauß

November 2015

Contents

0 Introduction

0.1 Outline

Let A be a Dedekind domain with perfect field of fractions K, and let B be the integral closure of A in a finite Galois extension L of K, with Galois group $G := \operatorname{Gal}(L|K)$.

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[d, dash, "{G,\ |G|=n}"] \\
B \arrow[d, dash] & K \arrow[dl, dash] \\
A &
\end{tikzcd}$$

In this setting, we consider the twisted group ring $L \wr G$. It carries the multiplication given by $\alpha\sigma \cdot \beta\rho := \alpha\sigma(\beta)(\sigma \circ \rho)$ for $\alpha, \beta \in L$, $\sigma, \rho \in G$, extended K-bilinearly, cf. Definition 2.

Suppose there exists an A-linear basis $\underline{y}$ of B, which is also a K-linear basis of L. Let $\omega_0 : L \wr G \to \operatorname{End}_K L$, $\alpha\sigma \mapsto (x \mapsto \alpha\sigma(x))$, which is a Wedderburn isomorphism for $L \wr G$. Let $\omega_{1,\underline{y}} : \operatorname{End}_K L \to K^{n\times n}$ map an endomorphism to its representation matrix with respect to $\underline{y}$. Let $\omega_{\underline{y}} := \omega_{1,\underline{y}} \circ \omega_0$. Then it is possible to restrict the Wedderburn isomorphism $\omega_{\underline{y}} : L \wr G \to K^{n\times n}$ to the injective A-algebra morphism $\omega_{\underline{y}}^A : B \wr G \to A^{n\times n}$, cf. Remark 7.

$$\begin{tikzcd}
L \wr G \arrow[r, "\omega_0", "\sim"'] \arrow[rr, bend left, "\omega_{\underline{y}}", "\sim"'] & \operatorname{End}_K L \arrow[r, "\omega_{1,\underline{y}}", "\sim"'] & K^{n\times n} \\
B \wr G \arrow[u, hook] \arrow[rr, "\omega_{\underline{y}}^A := \omega_{\underline{y}}|_{B\wr G}^{A^{n\times n}}"] \arrow[dr, "\sim"'] & & A^{n\times n} \arrow[u, hook] \\
 & \omega_{\underline{y}}^A(B \wr G) \arrow[ur] &
\end{tikzcd}$$

We ask for a description of the image $\omega_{\underline{y}}^A(B \wr G)$ in $A^{n\times n}$ via congruences of matrix entries. The complexity of this description depends heavily on the choice of a suitable basis $\underline{y}$, cf. §0.2.3, §0.2.4.

By means of the description of $\omega_{\underline{y}}^A(B \wr G)$ we show that there are non-zero ideals in $B \wr G$ that are not of the form $\mathfrak{b}(B \wr G)$ for some Galois-stable ideal $\mathfrak{b} \subseteq B$, cf. §0.2.5.

0.2 Results

0.2.1 Wedderburn inversion formula and index formula

In case of $[L : K]$ being invertible in K, we obtain an inversion formula of the Wedderburn isomorphism $\omega_0 : L \wr G \to \operatorname{End}_K L$, $\sum\limits_{\sigma\in G} \alpha_\sigma\sigma \mapsto \left(x \mapsto \sum\limits_{\sigma\in G} \alpha_\sigma\sigma(x)\right)$, cf. Lemma 12.

With this formula we are able to prove that, if A is a finite extension of $\mathbf{Z}$, then the index of $\omega_{\underline{y}}^{A}(B \wr G)$ in $A^{n\times n}$ is given by $|\,\mathrm{N}_{K|\mathbf{Q}}(\Delta_{L|K,\underline{y}})|^{\frac{n}{2}}$, where $\Delta_{L|K,\underline{y}}$ denotes the discriminant of $L|K$ with respect to $\underline{y}$, cf. Theorem 16.

In particular, if $K = \mathbf{Q}$, then the index is given by $|\Delta_{L|\mathbf{Q},\underline{y}}|^{\frac{n}{2}}$, cf. Corollary 17.

0.2.2 Quadratic extensions

Let $d \in \mathbf{Z} \setminus \{0\}$ be squarefree. Consider the Galois extension $\mathbf{Q}(\sqrt{d})|\mathbf{Q}$ with Galois group $G \cong \mathrm{C}_2$.

In case of $d \equiv_4 2$ or $d \equiv_4 3$, the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{d})$ is given by $\mathbf{Z}[\sqrt{d}]$. If we employ the $\mathbf{Z}$-linear basis $\underline{y} = (1, \sqrt{d})$ of $\mathbf{Z}[\sqrt{d}]$, then

$$\mathbf{Z}[\sqrt{d}] \wr \mathrm{C}_2 \cong \omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\sqrt{d}] \wr \mathrm{C}_2) = \{\left(\begin{smallmatrix} s & dw \\ u & v \end{smallmatrix}\right) : s, w, u, v \in \mathbf{Z},\ s \equiv_2 v,\ w \equiv_2 u\}\ ,$$

cf. Proposition 20. Note that the index of $\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\sqrt{d}]\wr\mathrm{C}_2)$ in $\mathbf{Z}^{2\times 2}$ equals $4d$, cf. Corollary 17.

In case of $d \equiv_4 1$, the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{d})$ is given by $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. The description of $\omega_{\underline{y}}^{A}(\mathbf{Z}[\frac{1+\sqrt{d}}{2}]\wr\mathrm{C}_2)$ takes a rather simple form if we use the $\mathbf{Z}$-linear basis $\underline{y} = (1, x + \frac{1+\sqrt{d}}{2})$ of $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ for $x \in \mathbf{Z}$ chosen such that $2x \equiv_d -1$. We obtain

$$\mathbf{Z}[\tfrac{1+\sqrt{d}}{2}] \wr \mathrm{C}_2 \cong \omega_{\underline{y}}^{A}(\mathbf{Z}[\tfrac{1+\sqrt{d}}{2}] \wr \mathrm{C}_2) = \{\left(\begin{smallmatrix} s & dw \\ u & v \end{smallmatrix}\right) : s, w, u, v \in \mathbf{Z}\} = \left(\begin{smallmatrix} \mathbf{Z} & (d) \\ \mathbf{Z} & \mathbf{Z} \end{smallmatrix}\right),$$

cf. Proposition 22. Note that the index of $\omega_{\underline{y}}^{\mathbf{Z}}([\frac{1+\sqrt{d}}{2}]\wr\mathrm{C}_2)$ in $\mathbf{Z}^{2\times 2}$ equals d, cf. Corollary 17.

For instance, if $d = -15$ and if we employ the $\mathbf{Z}$-linear basis $\underline{y} = (1, 7 + \frac{1+\sqrt{-15}}{2})$, then $\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\frac{1+\sqrt{-15}}{2}] \wr \mathrm{C}_2) = \left(\begin{smallmatrix} \mathbf{Z} & (-15) \\ \mathbf{Z} & \mathbf{Z} \end{smallmatrix}\right) = \left(\begin{smallmatrix} \mathbf{Z} & (15) \\ \mathbf{Z} & \mathbf{Z} \end{smallmatrix}\right)$.

0.2.3 Cyclotomic extensions

Let $m \in \mathbf{Z}_{>0}$ and $\zeta_m := \exp(2\pi\,\mathrm{i}\,/m)$. Consider the Galois extension $\mathbf{Q}(\zeta_m)|\mathbf{Q}$ with Galois group $G \cong \mathrm{U}(\mathbf{Z}/(m))$ of order $|G| = \Phi(m)$. The integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\zeta_m)$ is given by $\mathbf{Z}[\zeta_m]$.

In case of $m = p$ for $p \in \mathbf{Z}_{>0}$ prime, we have $G \cong \mathrm{C}_{p-1}$. For the $\mathbf{Z}$-linear basis

$$\underline{y} = ((\zeta_p - 1)^0, \ldots, (\zeta_p - 1)^{p-2})$$

of $\mathbf{Z}[\zeta_p]$, we obtain

$$\mathbf{Z}[\zeta_p] \wr \mathrm{C}_{p-1} \cong \omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\zeta_p] \wr \mathrm{C}_{p-1}) = \begin{pmatrix} \mathbf{Z} & (p) & \cdots & (p) \\ \mathbf{Z} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & (p) \\ \mathbf{Z} & \cdots & \mathbf{Z} & \mathbf{Z} \end{pmatrix} \subseteq \mathbf{Z}^{(p-1)\times(p-1)}\ ,$$

cf. Theorem 25.

In case of m not being a prime, the $\mathbf{Z}$-linear basis $\underline{y} = ((\zeta_m - 1)^0, \ldots, (\zeta_m - 1)^{\Phi(m)-1})$ of $\mathbf{Z}[\zeta_m]$ does not necessarily provide such a simple description of $\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\zeta_m] \wr G)$.

Suppose, for instance, $m = 9$. Then the $\mathbf{Z}$-linear basis $\underline{y'} = ((\zeta_9 - 1)^0, \ldots, (\zeta_9 - 1)^5)$ of $\mathbf{Z}[\zeta_9]$ leads to a rather complicated structure, involving congruences of length up to eleven matrix entries, cf. Remark 28. Therefore, we exhibit another basis $\underline{y'}$ of $\mathbf{Z}[\zeta_9]$ for which the description of $\omega_{\underline{y'}}^{\mathbf{Z}}(\mathbf{Z}[\zeta_9] \wr G)$ involves shorter congruences, cf. Proposition 30.

To obtain a neat description of the image of $\mathbf{Z}[\zeta_9] \wr G$, it surprisingly turned out to be convenient not to map $\mathbf{Z}[\zeta_9] \wr G$ into $\mathbf{Z}^{6\times 6}$, but only into $\mathbf{Q}^{6\times 6}$, accepting non-integral matrix entries at one matrix position. This is done by means of a $\mathbf{Q}$-linear basis $\underline{q}$ of $\mathbf{Q}(\zeta_9)$ that is contained in $\mathbf{Z}[\zeta_9]$ but that is not a $\mathbf{Z}$-linear basis thereof, cf. Remark 29.

Then $\omega_{\underline{q}}(\mathbf{Z}[\zeta_9] \wr G)$ admits a neat decomposition into matrix blocks:

$$\mathbf{Z}[\zeta_9] \wr G \cong \omega_{\underline{q}}(\mathbf{Z}[\zeta_9] \wr G) = \begin{pmatrix} \Xi & \xi^2 \Xi \\ \\ \xi^{-1}\Xi & \Xi \end{pmatrix} \subseteq \mathbf{Q}^{6\times 6} ,$$

where $\Xi := \left\{ (y_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \end{pmatrix} : \begin{array}{rl} y_{1,1} \equiv_3 y_{2,2} & \equiv_3 \; y_{3,3} \\ y_{1,3} + 3y_{2,1} + 3y_{3,2} & \equiv_9 \; 0 \end{array} \right\} \subseteq \mathbf{Z}^{3\times 3}$ and

$\xi := \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, cf. Corollary 32.

0.2.4 Example: $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)|\mathbf{Q}$

We consider the Galois extension $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)|\mathbf{Q}$ with Galois group $G \cong \mathrm{S}_3$.

Write $\delta := \sqrt[3]{2}$, $\zeta := \zeta_3$, $\eta := \frac{\zeta - 1}{\delta + 1}$. The integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\delta, \zeta)$ is given by $\mathbf{Z}[\delta, \eta]$. If we used the $\mathbf{Z}$-linear basis $\underline{y} = (1, \delta, \delta^2, \eta, \delta\eta, \delta^2\eta)$ of $\mathbf{Z}[\delta, \eta]$, then the congruences describing $\omega_{\underline{y}}(\mathbf{Z}[\delta, \eta] \wr G)$ would be rather complicated.

A $\mathbf{Z}$-linear basis for which the appearing congruences take a simpler form was calculated using the computer algebra system Magma [7]. This way, the complexity of the congruences could be decreased from a maximal length of 9 matrix entries to a maximal length of 3 matrix entries, cf. Proposition 34.

0.2.5 Galois-stable ideals

An ideal $\mathfrak{b}$ is called Galois-stable if $\sigma(\mathfrak{b}) = \mathfrak{b}$ for $\sigma \in G$. We denote by $\mathrm{Ideals}^{\times,G}(B)$ the set of non-zero Galois-stable ideals of B and by $\mathrm{Ideals}^{\times}(B \wr G)$ the set of non-zero ideals of $B \wr G$.

We have an injective map

$$\begin{array}{rcl}\iota : \mathrm{Ideals}^{\times,G}(B) & \to & \mathrm{Ideals}^{\times}(B \wr G) \\ \mathfrak{b} & \mapsto & \mathfrak{b}(B \wr G)\ .\end{array}$$

It is shown that in case of $\mathbf{Q}(\sqrt{-15})$ the map

$$\iota : \mathrm{Ideals}^{\times,G}(\mathbf{Z}[\tfrac{1+\sqrt{-15}}{2}]) \to \mathrm{Ideals}^{\times}(\mathbf{Z}[\tfrac{1+\sqrt{-15}}{2}] \wr \mathrm{C}_2)$$

is not surjective, i.e. that there are non-zero ideals in $\mathbf{Z}[\frac{1+\sqrt{-15}}{2}] \wr \mathrm{C}_2$ that are not of the form $\mathfrak{b}(\mathbf{Z}[\frac{1+\sqrt{-15}}{2}] \wr \mathrm{C}_2)$ for some $\mathfrak{b} \in \mathrm{Ideals}^{\times,G}(\mathbf{Z}[\frac{1+\sqrt{-15}}{2}])$, cf. Proposition 55.

For this purpose, we first determine a list of ideals in $\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\frac{1+\sqrt{-15}}{2}] \wr \mathrm{C}_2)$, where $\underline{y} = (1, 7 + \frac{1+\sqrt{-15}}{2})$.
We subsequently list those ideals contained in $\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\frac{1+\sqrt{-15}}{2}]))\right)$.
We find that

$$\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\tfrac{1+\sqrt{-15}}{2}]))\right) \subsetneq \omega_{\underline{y}}^{\mathbf{Z}}(\mathrm{Ideals}^{\times}(\mathbf{Z}[\tfrac{1+\sqrt{-15}}{2}] \wr \mathrm{C}_2))\ ,$$

so that we have

$$\iota(\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\tfrac{1+\sqrt{-15}}{2}])) \subsetneq \mathrm{Ideals}^{\times}(\mathbf{Z}[\tfrac{1+\sqrt{-15}}{2}] \wr \mathrm{C}_2)$$

and thus the map ι is not surjective.
In case of $\mathbf{Q}(\sqrt{-5})$, it is analogously shown that the map

$$\iota : \mathrm{Ideals}^{\times,G}(\mathbf{Z}[\sqrt{-5}]) \to \mathrm{Ideals}^{\times}(\mathbf{Z}[\sqrt{-5}] \wr \mathrm{C}_2)$$

is not surjective either, cf. Proposition 60.

As the index of $\iota(\mathfrak{b})$ in $B \wr G$ is given by a $|G|$-th power for $\mathfrak{b} \in \mathrm{Ideals}^{\times,G}(B)$, cf. Remark 48, we asked whether every ideal in $B \wr G$ of index a $|G|$-th power is contained in the image of ι.

This question is answered in the negative, for we find a non-zero ideal in $\mathbf{Z}[\sqrt{-5}] \wr \mathrm{C}_2$ of index 4 that is not contained in the image of ι, cf. Proposition 60.

0.3 Conventions

Let A be a Dedekind domain. Let R be a commutative ring. Let K be a field.

- We freely use standard notation from algebraic number theory.
- Morphisms will be written on the left, i.e $(\xrightarrow{a}\xrightarrow{b}) = (\xrightarrow{b\circ a})$.
- Given elements i, j of some set I, we let $\delta_{i,j} = 1$ in case $i = j$ and $\delta_{i,j} = 0$ in case $i \neq j$.
- For $a, b \in \mathbf{Z}$ we denote by $[a, b] := \{z \in \mathbf{Z} : a \leq z \leq b\}$ the integral interval.
- Write $R^\times := R \setminus \{0\}$.
- We denote by $\mathrm{U}(R) := \{r \in R : \text{ it exists } s \in R \text{ such that } rs = sr = 1_R\}$ the group of units of R.
- Suppose $x, y, z \in R$. We write $x \equiv_z y$ if there exists $a \in R$ such that $x - y = az$.
- Given $n, m \geq 1$, we denote by $R^{n\times m}$ the ring of $n \times m$ matrices over R.
- The standard R-linear basis $(\mathrm{e}_{i,j})_{i\in[1,n],j\in[1,m]}$ of $R^{n\times m}$ consists of the $n\times m$ matrices with entry 1 at position (i, j) and entry 0 elsewhere. In case of $m = 1$ we write $\mathrm{e}_{i,1} =: \mathrm{e}_i$ and $(\mathrm{e}_i)_{i\in[1,n]}$ is basis of $R^{n\times 1}$.
- Let K be a field and V be a K-vector space. Let $\varphi \in \mathrm{End}_K V$. We denote the K-linear trace of φ by $\mathrm{Tr}_K(\varphi)$.
- Let $M \in R^{n\times n}$. We denote the trace of M by $\mathrm{tr}(M)$.
- If R is an integral domain, then we denote by $R_\mathfrak{p}$ the localization of the ring R at a prime ideal $\mathfrak{p}$, that is, $R_\mathfrak{p} := \{\frac{r}{s} : r \in R,\ s \in R \setminus \mathfrak{p}\} \subseteq \mathrm{frac}(R)$.
- By an *R-order*, we understand a finitely generated free R-algebra.
- Let $L|K$ be a finite extension of fields and $K = \mathrm{frac}(A)$.

  For $\alpha \in L$ we write $\mathrm{Tr}_{L|K}(\alpha) = \mathrm{Tr}_K(L \xrightarrow{\alpha(-)} L)$.

  We denote by $\Gamma_L(A)$ the integral closure of A in L.

  Let $\underline{y} := (y_1, \ldots, y_n)$ be a K-linear basis of L. We write

  $$\mathrm{Gram}_{L|K,\underline{y}} := \mathrm{Tr}_{L|K}(y_i y_j))_{i,j\in[1,n]} \in K^{n\times n}.$$

  We denote the discriminant of $L|K$ with respect to $\underline{y}$ by $\Delta_{L|K,\underline{y}}$.
- Let $L|K$ be a Galois extension of fields. Let $G := \mathrm{Gal}(L|K)$ be its Galois group.

  By $L \wr G$ we denote the twisted group ring of G with coefficients in L, cf. Definition 2.

- We denote by $\mathrm{Ideals}^{\times}(A)$ the set of non-zero ideals of A.

  We denote by $\mathrm{Rightideals}^{\times}(A)$ the set of non-zero right ideals of A.

  We denote by $\mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)$ the set of non-zero prime ideals of A.

- Given a group G that acts on A, we write:

  $\mathrm{Ideals}^{\times,G}(A) := \{\mathfrak{a} \subseteq A :$ is an ideal and $\sigma(\mathfrak{a}) = \mathfrak{a}$ for $\sigma \in G\} \subseteq \mathrm{Ideals}^{\times}(A)$, cf. Definition 38.

  $\mathrm{Ideals}^{\times,G}_{\mathrm{principal}}(A) := \{\mathfrak{a} \subseteq A :$ is a principal ideal and $\sigma(\mathfrak{a}) = \mathfrak{a}$ for $\sigma \in G\} \subseteq \mathrm{Ideals}^{\times,G}(A)$.

- Let $\mathfrak{p} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)$ and $\mathfrak{a} \in \mathrm{Ideals}^{\times}(A)$. We denote by $v_{\mathfrak{p}}(\mathfrak{a})$ the valuation of $\mathfrak{a}$ at $\mathfrak{p}$. In addition we write $v_{\mathfrak{p}}((0)) = +\infty$.

  Likewise for elements instead of ideals.

- For $n \geq 1$, let $\zeta_n := \exp(2\pi\,\mathrm{i}\,/n)$.

- For a prime q, let $\mathbf{F}_q$ denote the finite field containing q elements.

- Let Y be a group and $X \leq Y$ a subgroup. We denote by $[Y : X] := |Y/X|$ the index of X in Y.

- Suppose given $a_{i,j} \in \mathbf{Q}^{\times}$ for $i, j \in [1, n]$. We form the fractional ideal $(a_{i,j}) := \{z a_{i,j} : z \in \mathbf{Z}\} \subseteq \mathbf{Q}$. In particular, $(1) = \mathbf{Z}$. We write the additive subgroup

$$\begin{pmatrix} (a_{1,1}) & (a_{1,2}) & \dots & (a_{1,n}) \\ \vdots & \vdots & \vdots & \vdots \\ (a_{n,1}) & (a_{n,2}) & \dots & (a_{n,n}) \end{pmatrix} := \{(x_{i,j})_{i,j} \in \mathbf{Q}^{n\times n} : x_{i,j} \in (a_{i,j}) \text{ for } i, j \in [1, n]\} \subseteq \mathbf{Q}^{n\times n} \ .$$

0.4 Acknowledgments

I would like to thank Matthias Künzer, who has supported me with his knowledge and patience. I thank him for the constructive conversations we had, his annotations vastly helped improving the quality of this text.

1 Preliminaries

Setting 1. Let A be a Dedekind domain with perfect field of fractions $K = \mathrm{frac}(A)$. Let $L|K$ be a finite Galois extension with Galois group $G := \mathrm{Gal}(L|K)$. Write $n := |G| = [L : K]$. Let $B := \Gamma_L(A)$ be the integral closure of A in L.

In case of $A = \mathbf{Z}$ we denote $\Gamma_L(\mathbf{Z}) = \mathcal{O}_L$.

$$\begin{tikzcd}
 & L \arrow[d, dash, "{G,\ |G|=n}"] \\
B \arrow[ur, dash] \arrow[d, dash] & K \\
A \arrow[ur, dash] &
\end{tikzcd}$$

We identify along the A-algebra isomorphism

$$\begin{array}{rcl} \{\varphi \in \mathrm{End}_K L : \varphi(B) \subseteq B\} & \xrightarrow{\sim} & \mathrm{End}_A B \\ \varphi & \mapsto & \varphi|_B^B \ . \end{array}$$

Let $\underline{y} = (y_1, ..., y_n)$ be a K-linear basis of L and let $\underline{y}^* = (y_1^*, ..., y_n^*)$ be its dual basis with respect to $\mathrm{Tr}_{L|K}$, i.e. $\mathrm{Tr}_{L|K}(y_i y_j^*) = \delta_{i,j}$ for $i, j \in [1, n]$.

Definition 2. For a subring $R \subseteq L$ such that $\sigma(R) = R$ for $\sigma \in G$, the *twisted group ring*[1] is defined as the set of formal sums

$$R \wr G := \{\sum_{\sigma \in G} \alpha_\sigma \sigma : \ \alpha_\sigma \in R\} \ .$$

The addition in $R \wr G$ is given by

$$\left(\sum_{\sigma \in G} \alpha_\sigma \sigma\right) + \left(\sum_{\sigma \in G} \beta_\sigma \sigma\right) := \sum_{\sigma \in G} (\alpha_\sigma + \beta_\sigma)\sigma$$

and the multiplication is defined by

$$\left(\sum_{\sigma \in G} \alpha_\sigma \sigma\right) \cdot \left(\sum_{\rho \in G} \beta_\rho \rho\right) := \sum_{\sigma \in G} \sum_{\rho \in G} \alpha_\sigma \sigma(\beta_\rho) \sigma \circ \rho$$

where $\alpha_\sigma, \ \beta_\sigma \in R$ for $\sigma \in G$.

We have an injective ring morphism

$$\begin{array}{rcl} R & \rightarrow & R \wr G \\ x & \mapsto & x \, \mathrm{id} \end{array}$$

*along which we identify x with $x\,$*id.

[1] We use the terminology *twisted group ring* as in [1, §28].

We have an injective map

$$\begin{array}{rcl} G & \to & R \wr G \\ \sigma & \mapsto & 1 \cdot \sigma \end{array}$$

along which we identify σ with $1 \cdot \sigma$.

In the following, we give a proof of the fact that the twisted group ring $L \wr G$ is isomorphic to $K^{n \times n}$.

Lemma 3. *We have an isomorphism of K-algebras*

$$\begin{array}{rcl} \omega_{1,\underline{y}} : \operatorname{End}_K L & \to & K^{n \times n} \\ \left(\sum\limits_{i \in [1,n]} b_i y_i \mapsto \sum\limits_{i \in [1,n]} \sum\limits_{j \in [1,n]} a_{i,j} b_j y_i \right) & \leftarrow\!\shortmid & (a_{i,j})_{i,j} \\ \varphi & \mapsto & (a^{\varphi}_{i,j})_{i,j} \end{array}$$

where $(a^{\varphi}_{i,j})_{i,j}$ is the representation matrix of φ, with respect to $\underline{y}$, i.e. $a^{\varphi}_{i,j}$ is determined by $\varphi(y_j) = \sum\limits_{i \in [1,n]} a^{\varphi}_{i,j} y_i$ for $j \in [1, n]$.

In particular, $\operatorname{End}_K L$ is of dimension n^2 over K.

Lemma 4. *The map*

$$\begin{array}{c} \omega_0 : L \wr G \to \operatorname{End}_K L \\ \sum\limits_{\sigma \in G} \alpha_\sigma \sigma \mapsto \left(x \mapsto \sum\limits_{\sigma \in G} \alpha_\sigma \sigma(x) \right) \end{array}$$

is a K-algebra isomorphism.

Proof. Let $\alpha_\sigma,\ \beta_\sigma \in L$ for $\sigma \in G$ and let $\lambda \in K$. For $x \in L$, we obtain the following.

$$\begin{aligned} (\omega_0(\sum_{\sigma \in G} \alpha_\sigma \sigma) + \omega_0(\sum_{\sigma \in G} \beta_\sigma \sigma))(x) &= \sum_{\sigma \in G} \alpha_\sigma \sigma(x) + \sum_{\sigma \in G} \beta_\sigma \sigma(x) \\ &= \sum_{\sigma \in G} (\alpha_\sigma + \beta_\sigma) \sigma(x) \\ &= \omega_0(\sum_{\sigma \in G} (\alpha_\sigma + \beta_\sigma) \sigma)(x) \\ &= \omega_0(\sum_{\sigma \in G} \alpha_\sigma \sigma + \sum_{\sigma \in G} \beta_\sigma \sigma)(x) \end{aligned}$$

$$\begin{aligned} \omega_0(\lambda \sum_{\sigma \in G} \alpha_\sigma \sigma)(x) &= \omega_0(\sum_{\sigma \in G} \lambda \alpha_\sigma \sigma)(x) \\ &= \sum_{\sigma \in G} \lambda \alpha_\sigma \sigma(x) \end{aligned}$$

$$\begin{aligned} &= \lambda \sum_{\sigma\in G} \alpha_\sigma \sigma(x) \\ &= \lambda \omega_0(\sum_{\sigma\in G} \alpha_\sigma \sigma)(x) \end{aligned}$$

$$\begin{aligned} \omega_0(\sum_{\sigma\in G} \alpha_\sigma \sigma) \circ \omega_0(\sum_{\rho\in G} \beta_\rho \rho)(x) &= \omega_0(\sum_{\sigma\in G} \alpha_\sigma \sigma)(\sum_{\rho\in G} \beta_\rho \rho(x)) \\ &= \sum_{\sigma\in G} \alpha_\sigma \sigma(\sum_{\rho\in G} \beta_\rho \rho(x)) \\ &= \sum_{\sigma\in G}\sum_{\rho\in G} \alpha_\sigma \sigma(\beta_\rho \rho(x)) \\ &= \sum_{\sigma\in G}\sum_{\rho\in G} \alpha_\sigma \sigma(\beta_\rho)(\sigma\circ\rho)(x) \\ &= \omega_0((\sum_{\sigma\in G} \alpha_\sigma \sigma)\cdot(\sum_{\rho\in G} \beta_\rho \rho))(x) \end{aligned}$$

So ω_0 is a K-algebra morphism.

Since $L \wr G$ and $\operatorname{End}_K L$ are of dimension n^2 over K it remains to show that ω_0 is injective. This results of Dedekind's Lemma, see e.g. [2, Lemma 7.5.1]. We recall the arguments:

Let $1 \le m \le n$. Let $\sigma_1, ..., \sigma_m \in G$ be pairwise distinct and $\xi := \sum_{i\in[1,m]} \alpha_{\sigma_i}\sigma_i$ be an element of the kernel of ω_0, where $\alpha_{\sigma_i} \in L$ for $i \in [1,m]$. Then $(\omega_0(\xi))(x) = \sum_{i\in[1,m]} \alpha_{\sigma_i}\sigma_i(x) = 0$ for all $x \in L$.

We will show that $\alpha_{\sigma_i} = 0$ for every $i \in [1,m]$, using induction on $m \ge 1$.

Initial step: Suppose $m = 1$. Since $\sigma_1(1_L) = 1_L$ it follows that $\alpha_{\sigma_1} = \alpha_{\sigma_1}\sigma_1(1_L) = 0$.

Induction step: Let $m \ge 2$. *Assume* $\xi \ne 0$. Without loss of generality, we have $\alpha_{\sigma_1} \ne 0$.

Since $\sigma_1 \ne \sigma_m$ there exists $a \in L$ such that $\sigma_1(a) \ne \sigma_m(a)$. We obtain

$$\begin{aligned} (1)\ 0 = \sum_{i\in[1,m]} \alpha_{\sigma_i}\sigma_i(ax) &= \alpha_{\sigma_1}\sigma_1(a)\sigma_1(x) + \cdots + \alpha_{\sigma_{m-1}}\sigma_{m-1}(a)\sigma_{m-1}(x) + \alpha_{\sigma_m}\sigma_m(a)\sigma_m(x) \\ (2)\ 0 = \sigma_m(a)\sum_{i\in[1,m]} \alpha_{\sigma_i}\sigma_i(x) &= \alpha_{\sigma_1}\sigma_m(a)\sigma_1(x) + \cdots + \alpha_{\sigma_{m-1}}\sigma_m(a)\sigma_{m-1}(x) + \alpha_{\sigma_m}\sigma_m(a)\sigma_m(x) \end{aligned}$$

and so, forming the difference of (1) and (2),

$$0 = \alpha_{\sigma_1}(\sigma_1(a) - \sigma_m(a))\sigma_1(x) + \cdots + \alpha_{\sigma_{m-1}}(\sigma_{m-1}(a) - \sigma_m(a))\sigma_{m-1}(x) \quad \text{for } x \in L.$$

By induction hypothesis we have $\alpha_{\sigma_i}(\sigma_i(a) - \sigma_m(a)) = 0$ for $i \in [1, m-1]$. As $\sigma_1(a) - \sigma_m(a) \ne 0$ it follows that $\alpha_{\sigma_1} = 0$. Which is a *contradiction*.

Therefore $\alpha_{\sigma_i} = 0$ for $i \in [1,m]$ and thus $\xi = 0$.

Hence ω_0 is injective. □

Corollary 5. *We have the K-algebra isomorphism*

$$\omega_{\underline{y}} : L \wr G \ \ \rightarrow \ \ K^{n\times n}$$

where

$$\omega_{\underline{y}} \ \ = \ \ \omega_{1,\underline{y}} \circ \omega_0 \ .$$

Lemma 6. *We have*

$$\omega_0(B \wr G) \subseteq \operatorname{End}_A B \ .$$

Proof. The assertion $\omega_0(B \wr G) \overset{!}{\subseteq} \operatorname{End}_A B$ is equivalent to $(\omega_0(\xi))(B) \overset{!}{\subseteq} B$ for $\xi \in B \wr G$. Suppose given $b \in B$ and $\xi = \sum\limits_{\sigma \in G} \alpha_\sigma \sigma \in B \wr G$, where $\alpha_\sigma \in B$.

Then

$$(\omega_0(\xi))(b) = \sum_{\sigma \in G} \underbrace{\alpha_\sigma}_{\in B} \underbrace{\sigma(b)}_{\in B} \in B \ .$$

□

Remark 7. Suppose $\underline{y} = (y_1, \ldots, y_n)$ to be an A-linear basis of B. Using Lemma 6 it is possible to restrict $\omega_{\underline{y}} : L \wr G \rightarrow K^{n\times n}$ to the injective A-algebra morphism $\omega_{\underline{y}}^A := \omega_{\underline{y}}|_{B\wr G}^{A^{n\times n}} : B \wr G \rightarrow A^{n\times n}$.

$$\begin{tikzcd}
L \wr G \arrow[r, "\omega_0", "\sim"'] \arrow[rr, bend left, "\omega_{\underline{y}}", "\sim"'] & \operatorname{End}_K L \arrow[r, "\omega_{1,\underline{y}}", "\sim"'] & K^{n\times n} \\
B \wr G \arrow[u, hook] \arrow[r, "\omega_0|_{B\wr G}^{\operatorname{End}_A B}"] \arrow[rr, bend right, "\omega_{\underline{y}}^A := \omega_{\underline{y}}|_{B\wr G}^{A^{n\times n}}"'] & \operatorname{End}_A B \arrow[u] \arrow[r, "\omega_{1,\underline{y}}|_{\operatorname{End}_A B}^{A^{n\times n}}", "\sim"'] & A^{n\times n} \arrow[u, hook]
\end{tikzcd}$$

Lemma 8. *Let $I \in \operatorname{Ideals}^\times(B \wr G)$. Then $I \cap A \neq (0)$.*

Proof. Let $I \in \operatorname{Ideals}^\times(B \wr G)$. As each element $y \in L$ is of the form $\frac{b}{a}$, for $b \in B$, $a \in A^\times$, cf. [4, VII. Proposition 1.1], the set

$$KI := \{\tfrac{1}{a} \cdot x : a \in A^\times, \ x \in I\}$$

is an ideal in $L \wr G \cong K^{n\times n}$.

Thus, $KI = (0)$ or $KI = L \wr G$. As $I \neq (0)$ it follows that $KI \neq (0)$ and therefore $KI = L \wr G$. Note that $KI \cap L = L$.

We have $1_L \in KI$ and therefore

$$1_L = \tfrac{1}{a} \cdot x \text{ for some } a \in A^\times, x \in I \ .$$

So $x = a \in A^\times$ and hence $x \in I \cap A$. □

2 A Wedderburn inversion formula

We use Setting 1.

Lemma 9. *Let V be a K-vector space of dimension n. Let $\varphi \in \operatorname{End}_K V$. Then*

$$n \cdot \operatorname{Tr}_K(\varphi) = \operatorname{Tr}_K(\ \operatorname{End}_K V \xrightarrow{\varphi\circ(-)} \operatorname{End}_K V\ )\ .$$

Proof. Let $\underline{v} = (v_1, \dots, v_n)$ be a K-linear basis of V. Let $\varepsilon_{i,j} \in \operatorname{End}_K V$ be defined by

$$\varepsilon_{i,j}(v_k) := \left\{ \begin{array}{cl} v_i & \text{for } j = k \\ 0 & \text{for } j \neq k \end{array} \right\} = \delta_{j,k} v_i\ .$$

Then $(\varepsilon_{i,j})_{i,j\in[1,n]}$ is a K-linear basis of $\operatorname{End}_K V$.

Let $\varphi(v_i) =: \sum\limits_{s\in[1,n]} a_{s,i} v_s$, where $a_{s,i} \in K$ for $i, s \in [1, n]$. We have $\operatorname{Tr}_K(\varphi) = \sum\limits_{i\in[1,n]} a_{i,i}$.

Consider $\varepsilon_{i,j} \overset{\varphi\circ(-)}{\longmapsto} \varphi \circ \varepsilon_{i,j}$ for $i, j \in [1, n]$. We have

$$(\varphi \circ \varepsilon_{i,j})(v_k) \;=\; \varphi(\delta_{j,k} v_i) \;=\; \delta_{j,k} \sum_{s\in[1,n]} a_{s,i} v_s \;=\; \sum_{s\in[1,n]} a_{s,i} \delta_{j,k} v_s \;=\; \sum_{s\in[1,n]} a_{s,i} \varepsilon_{s,j}(v_k)$$

for $k \in [1, n]$. As $\underline{v}$ is a basis of V it follows that

$$\varphi \circ \varepsilon_{i,j} = \sum_{s\in[1,n]} a_{s,i} \varepsilon_{s,j}\ .$$

So the diagonal coefficient of $\varphi \circ (-)$ at $\varepsilon_{i,j}$ is $a_{i,i}$.

Altogether we have

$$\operatorname{Tr}_K(\ \operatorname{End}_K V \xrightarrow{\varphi\circ(-)} \operatorname{End}_K V\ ) = \sum_{i,j\in[1,n]} a_{i,i} = n \cdot \sum_{i\in[1,n]} a_{i,i} = n \cdot \operatorname{Tr}_K(\varphi)\ .$$

□

Lemma 10. *Suppose given $\xi \in L \wr G$. We have*

$$\operatorname{Tr}_K(\ \operatorname{End}_K L \xrightarrow{\omega_0(\xi)\circ(-)} \operatorname{End}_K L\ ) = \operatorname{Tr}_K(\ L \wr G \xrightarrow{\xi\cdot(-)} L \wr G\ )\ .$$

Proof. The quadrangle

$$\begin{tikzcd}
\operatorname{End}_K L \arrow[r, "\omega_0(\xi)\circ(-)"] & \operatorname{End}_K L \\
L \wr G \arrow[u, "\omega_0", "\wr"'] \arrow[r, "\omega_0^{-1}\circ(\omega_0(\xi)\circ(-))\circ\omega_0"] & L \wr G \arrow[u, "\omega_0", "\wr"']
\end{tikzcd}$$

commutes. Since ω_0 is an isomorphism by Lemma 4, we know that

$$\mathrm{Tr}_K(\omega_0(\xi)\circ(-)) = \mathrm{Tr}_K(\omega_0^{-1}\circ(\omega_0(\xi)\circ(-))\circ\omega_0)\ .$$

Let $\eta \in L \wr G$. Then

$$\begin{aligned} \omega_0^{-1}\circ(\omega_0(\xi)\circ(-))\circ\omega_0(\eta) &= \omega_0^{-1}\circ(\omega_0(\xi)\circ\omega_0(\eta)) \\ &= \omega_0^{-1}(\omega_0(\xi\cdot\eta)) = \xi\cdot\eta\ . \end{aligned}$$

Hence $\omega_0^{-1}\circ(\omega_0(\xi)\circ(-))\circ\omega_0 = \xi\cdot(-)$.

So we have $\mathrm{Tr}_K(\ \mathrm{End}_K L \xrightarrow{\omega_0(\xi)\circ(-)} \mathrm{End}_K L\ ) = \mathrm{Tr}_K(\ L\wr G \xrightarrow{\xi\cdot(-)} L\wr G\ )$. □

Lemma 11. *Suppose that* $\mathrm{char}\, K$ *does not divide* n *(e.g.* $\mathrm{char}\, K = 0$*). Let* $\alpha \in L$ *and* $\sigma \in G$*. Then*

$$\mathrm{Tr}_K(\omega_0(\alpha\sigma)) = \delta_{\sigma,\mathrm{id}}\,\mathrm{Tr}_{L|K}(\alpha)\ .$$

Proof. Consider the K-linear basis $(y_i\rho)_{i\in[1,n],\rho\in G}$ of $L\wr G$. By Lemma 9 and Lemma 10 the assertion $\mathrm{Tr}_K(\omega_0(\alpha\sigma)) \overset{!}{=} \delta_{\sigma,\mathrm{id}}\,\mathrm{Tr}_{L|K}(\alpha)$ is equivalent to

$$\mathrm{Tr}_K(L\wr G \xrightarrow{\alpha\sigma\cdot(-)} L\wr G) \ \overset{!}{=}\ \begin{cases} n\cdot\mathrm{Tr}_{L|K}(\alpha) & \text{for } \sigma = \mathrm{id} \\ 0 & \text{for } \sigma \neq \mathrm{id}\ . \end{cases}$$

Given $i \in [1,n]$ and $\rho \in G$, we have

$$(\alpha\sigma\cdot(-))(y_i\rho) \ = \ \alpha\sigma\cdot y_i\rho \ = \ \alpha\sigma(y_i)\sigma\circ\rho\ .$$

Since $\underline{y}$ is a K-linear basis of L, we find $b_{j,i} \in K$ for $j \in [1,n]$ such that $\alpha\sigma(y_i) = \sum\limits_{j\in[1,n]} b_{j,i}y_j$. So we have

$$(\alpha\sigma\cdot(-))(y_i\rho) \ = \ \sum_{j\in[1,n]} b_{j,i}y_j\sigma\circ\rho\ .$$

The diagonal coefficient at $y_i\rho$ now is given by $\delta_{\sigma\circ\rho,\rho}b_{i,i} = \delta_{\sigma,\mathrm{id}}b_{i,i}$.

Therefore we have

$$\mathrm{Tr}_K(L\wr G \xrightarrow{\alpha\sigma\cdot(-)} L\wr G) = \begin{cases} \sum\limits_{\rho\in G,\ i\in[1,n]} b_{i,i} = n\cdot\sum\limits_{i\in[1,n]} b_{i,i} & \text{for } \sigma = \mathrm{id} \\ 0 & \text{for } \sigma \neq \mathrm{id}\ . \end{cases}$$

It now remains to show that in case of $\sigma = \mathrm{id}$, we have $\sum\limits_{i\in[1,n]} b_{i,i} \overset{!}{=} \mathrm{Tr}_{L|K}(\alpha)$.

We have $\alpha y_i = \alpha\sigma(y_i) = \sum\limits_{j\in[1,n]} b_{j,i}y_j$. So the diagonal coefficient at y_i is given by $b_{i,i}$.

Therefore we obtain $\sum\limits_{i\in[1,n]} b_{i,i} = \mathrm{Tr}_K(L \xrightarrow{\alpha(-)} L) = \mathrm{Tr}_{L|K}(\alpha)$.

So we have $\mathrm{Tr}_K(L \wr G \xrightarrow{\alpha\sigma\cdot(-)} L \wr G) = \begin{cases} n \cdot \mathrm{Tr}_{L|K}(\alpha) & \text{for } \sigma = \mathrm{id} \\ 0 & \text{for } \sigma \neq \mathrm{id}\end{cases}$. □

Lemma 12. *The inverse of ω_0 is given by*

$$\begin{aligned} \omega_0^{-1} : \mathrm{End}_K L &\to L \wr G \\ \varphi &\mapsto \sum_{\sigma\in G,\ l\in[1,n]} \mathrm{Tr}_K(\omega_0(y_l^*\sigma^{-1}) \circ \varphi)\sigma y_l \ . \end{aligned}$$

This was already shown in a wider context by M. Künzer in [3, Corollary 1.18].

Proof. Write $\tilde{\omega}_0 : \mathrm{End}_K L \to L \wr G$, $\varphi \mapsto \sum\limits_{\sigma\in G,\ l\in[1,n]} \mathrm{Tr}_K(\omega_0(y_l^*\sigma^{-1}) \circ \varphi)\sigma y_l$. By Lemma 4 we know that ω_0 is an isomorphism of K-algebras. Therefore it suffices to show that

$$\tilde{\omega}_0 \circ \omega_0 = \mathrm{id}_{L\wr G} \ .$$

Consider the K-linear basis $(\sigma y_l)_{l\in[1,n],\sigma\in G}$ of $L \wr G$. Given $\rho \in G$ and $k \in [1,n]$, we verify

$$\begin{aligned} \tilde{\omega}_0 \circ \omega_0(\rho y_k) &= \sum_{\sigma\in G,\ l\in[1,n]} \mathrm{Tr}_K\left(\omega_0(y_l^*\sigma^{-1}) \circ \omega_0(\rho y_k)\right)\sigma y_l \\ &= \sum_{\sigma\in G,\ l\in[1,n]} \mathrm{Tr}_K\left(\omega_0(y_l^*\sigma^{-1} \cdot \rho y_k)\right)\sigma y_l \\ &= \sum_{\sigma\in G,\ l\in[1,n]} \mathrm{Tr}_K\left(\omega_0(y_l^*\sigma^{-1}(\rho(y_k))\sigma^{-1} \circ \rho)\right)\sigma y_l \\ &\overset{\text{Lemma 11}}{=} \sum_{\sigma\in G,\ l\in[1,n]} \delta_{\sigma^{-1}\circ\rho,\mathrm{id}}\,\mathrm{Tr}_{L|K}\left(y_l^* \cdot \sigma^{-1}(\rho(y_k))\right)\sigma y_l \\ &= \sum_{l\in[1,n]} \mathrm{Tr}_{L|K}(y_l^* y_k)\rho y_l \\ &= \sum_{l\in[1,n]} \delta_{l,k}\rho y_l \\ &= \rho y_k \ . \end{aligned}$$

□

3 An index formula

Setting 13. Let $A|\mathbf{Z}$ be a ring extension such that A is a principal ideal domain. Let $K := \mathrm{frac}(A)$ and suppose $K|\mathbf{Q}$ to be a finite extension of fields. Write $r := [K : \mathbf{Q}]$. Let $L|K$ be a Galois extension with Galois group $G := \mathrm{Gal}(L|K)$. Write $n := |G| = [L : K]$. Let $B = \Gamma_L(A)$ be the integral closure of A in L.

$$\begin{tikzcd}
 & L \arrow[dl, no head] \arrow[d, no head, "{G,\ |G|=n}"] \\
B \arrow[d, no head] & K \arrow[dl, no head] \arrow[d, no head, "r"] \\
A \arrow[d, no head] & \mathbf{Q} \arrow[dl, no head] \\
\mathbf{Z} &
\end{tikzcd}$$

Let $\underline{y} = (y_1, ..., y_n)$ be an A-linear basis of B, which is also a K-linear basis of L. Let $\underline{y}^* = (y_1^*, ..., y_n^*)$ be its dual basis with respect to $\mathrm{Tr}_{L|K}$, i.e. $\mathrm{Tr}_{L|K}(y_i y_j^*) = \delta_{i,j}$ for $i, j \in [1, n]$.

Lemma 14. *Let $d \in A^\times$. Then*

$$|A/(d)| = |\,\mathrm{N}_{K|\mathbf{Q}}(d)|\ .$$

Proof. Let $(a_i)_{i\in[1,r]}$ be a $\mathbf{Z}$-linear basis of A, which is also a $\mathbf{Q}$-linear basis of K. We have the $\mathbf{Z}$-linear isomorphism

$$\varphi : \mathbf{Z}^{r\times 1} \to A,\ \mathrm{e}_i \mapsto a_i\ .$$

Let $\lambda : A \to A$, $a \mapsto da$. Let $P \in \mathbf{Z}^{r\times r}$ be the representation matrix of λ with respect to $(a_i)_{i\in[1,r]}$.

Then we get the commutative diagram of $\mathbf{Z}$-linear maps

$$\begin{tikzcd}
A \arrow[r, "\lambda"] & A \arrow[r] & A/(d) \\
\mathbf{Z}^{r\times 1} \arrow[u, "\wr"', "\varphi"] \arrow[r, "P(-)"] & \mathbf{Z}^{r\times 1} \arrow[u, "\wr"', "\varphi"] \arrow[r] & \mathbf{Z}^{r\times 1}/P\mathbf{Z}^{r\times 1} \arrow[u, "\wr"']
\end{tikzcd}$$

cf. Lemma A 1.

By the elementary divisor theorem there exist matrices $S, T \in \mathrm{GL}_n(\mathbf{Z})$ such that $SPT = D = \mathrm{diag}(d_1, ..., d_r)$ for some $d_1, \dots, d_r \in \mathbf{Z}$, see e.g. [4, III. Theorem 7.8.]. So we get the commutative diagram of $\mathbf{Z}$- linear maps

$$\begin{tikzcd}
\mathbf{Z}^{r\times 1} \arrow[r, "P(-)"] & \mathbf{Z}^{r\times 1} \arrow[r] & \mathbf{Z}^{r\times 1}/P\mathbf{Z}^{r\times 1} \\
\mathbf{Z}^{r\times 1} \arrow[u, "\wr"', "T(-)"] \arrow[r, "D(-)"] & \mathbf{Z}^{r\times 1} \arrow[u, "\wr"', "S^{-1}(-)"] \arrow[r] & \mathbf{Z}^{r\times 1}/D\mathbf{Z}^{r\times 1} \arrow[u, "\wr"']
\end{tikzcd}$$

cf. Lemma A 1.

Moreover we have

$$\mathbf{Z}^{r\times 1}/D\mathbf{Z}^{r\times 1} \cong \bigoplus_{i\in[1,r]} \mathbf{Z}/(d_i)$$

via $\begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} + D\mathbf{Z}^{r\times 1} \mapsto (z_1 + (d_1), ..., z_n + (d_r))$.

Altogether we have $A/(d) \cong \bigoplus\limits_{i\in[1,r]} \mathbf{Z}/(d_i)$ and therefore

$$|A/(d)| = |\bigoplus_{i\in[1,r]} \mathbf{Z}/(d_i)| = |\prod_{i\in[1,r]} d_i| = |\det(D)| = |\det(P)| \ .$$

We have $|\,\mathrm{N}_{K|\mathbf{Q}}(d)| = |\det(P)|$ by definition of $\mathrm{N}_{K|\mathbf{Q}}$. □

Lemma 15. *Let P and Q be free A-modules of rank n and bases $(p_i)_{i\in[1,n]}$ respectively $(q_i)_{i\in[1,n]}$. Let $\mu : P \to Q$ be injective and A-linear. Let M be the representation matrix of μ with respect to $(p_i)_{i\in[1,n]}$ and $(q_i)_{i\in[1,n]}$. Then the index of $\mu(P)$ in Q is given by*

$$[Q : \mu(P)] := |Q/\mu(P)| = |\,\mathrm{N}_{K|\mathbf{Q}}(\det(M))| \ .$$

Proof. Consider the basis $(\mathrm{e}_i)_{i\in[1,n]}$ of $A^{n\times 1}$. We have the A-linear isomorphisms

$$\begin{aligned} f : A^{n\times 1} &\to P \\ \mathrm{e}_i &\mapsto p_i \text{ , for } i \in [1,n] \end{aligned}$$

$$\begin{aligned} g : A^{n\times 1} &\to Q \\ \mathrm{e}_i &\mapsto q_i \text{ , for } i \in [1,n] \ . \end{aligned}$$

Since A is a principal ideal domain there exist, by the elementary divisor theorem, matrices $S, T \in \mathrm{GL}_n(A)$ such that $TM = DS$ and such that $D = \mathrm{diag}(d_1, ..., d_n)$ is a diagonal matrix, where $d_i \in A$ for $i \in [1,n]$, see e.g. [4, III. Theorem 7.8.].

We have the following commutative diagram of A-linear maps.

$$\begin{tikzcd}
P \arrow[r, "\mu"] & Q \\
A^{n\times 1} \arrow[u, "f", "\wr"'] \arrow[r, "M(-)"] \arrow[d, "S(-)"', "\wr"] & A^{n\times 1} \arrow[u, "g", "\wr"'] \arrow[d, "T(-)"', "\wr"] \\
A^{n\times 1} \arrow[r, "D(-)"] & A^{n\times 1}
\end{tikzcd}$$

We have

$$\det(M) = \det(T^{-1}DS) = \det(T^{-1})\det(D)\det(S) \ .$$

Note that $\det(S) \in \mathrm{U}(A)$ and thus $\mathrm{N}_{K|\mathbf{Q}}(\det(S)) \in \{-1, +1\}$.

Likewise, $\mathrm{N}_{K|\mathbf{Q}}(\det(T^{-1})) \in \{-1, +1\}$. So

$$\begin{aligned} |\,\mathrm{N}_{K|\mathbf{Q}}(\det(M))| &= |\,\mathrm{N}_{K|\mathbf{Q}}(\det(T^{-1})\det(D)\det(S))| \\ &= |\,\mathrm{N}_{K|\mathbf{Q}}(\det(T^{-1})|\,|\,\mathrm{N}_{K|\mathbf{Q}}(\det(D))|\,|\,\mathrm{N}_{K|\mathbf{Q}}(\det(S))| \\ &= |\,\mathrm{N}_{K|\mathbf{Q}}(\det(D))|\ . \end{aligned}$$

Since D is diagonal, we have $\det(D) = \prod\limits_{i\in[1,n]} d_i$. This leads to

$$\begin{aligned} |\,\mathrm{N}_{K|\mathbf{Q}}(\det(D))| &= |\,\mathrm{N}_{K|\mathbf{Q}}(\prod_{i\in[1,n]} d_i)| \\ &= \prod_{i\in[1,n]} |\,\mathrm{N}_{K|\mathbf{Q}}(d_i)| \\ &\overset{\text{Lemma 14}}{=} \prod_{i\in[1,n]} |A/(d_i)| \\ &= |\bigoplus_{i\in[1,n]} A/(d_i)|\ . \end{aligned}$$

It suffices to show that $\bigoplus\limits_{i\in[1,n]} A/(d_i) \cong Q/\mu(P)$, because then

$$|\bigoplus_{i\in[1,n]} A/(d_i)| = |Q/\mu(P)|\ .$$

We have $A^{n\times 1}/DA^{n\times 1} \cong \bigoplus\limits_{i\in[1,n]} A/(d_i)$ via $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + DA^{n\times 1} \mapsto (a_1 + (d_1), ..., a_n + (d_n))$.

We get the commutative diagram of A- linear maps

$$\begin{tikzcd} A^{n\times 1} \arrow[r, "D(-)"] \arrow[d, "f"', "\wr"] & A^{n\times 1} \arrow[r] \arrow[d, "g"', "\wr"] & A^{n\times 1}/DA^{n\times 1} \arrow[d, "\wr"] \\ P \arrow[r, "\mu"] & Q \arrow[r] & Q/\mu(P) \end{tikzcd}$$

cf. Lemma A 1.

Altogether, we have

$$|\,\mathrm{N}_{K|\mathbf{Q}}(\det(M))| = |\,\mathrm{N}_{K|\mathbf{Q}}(\det(D))| = |\bigoplus_{i\in[1,n]} A/(d_i)| = |Q/\mu(P)|\ .$$

□

Theorem 16. *Recall that we use Setting 13.*

Let $\Lambda := \omega_{\underline{y}}(B \wr G) = \omega_{\underline{y}}^{A}(B \wr G) \subseteq A^{n\times n}$, *cf.* Remark 7. *Then we have an isomorphism of* A*-algebras*

$$\begin{aligned} B \wr G &\overset{\sim}{\to} \Lambda \\ \xi &\mapsto \omega_{\underline{y}}(\xi) = \omega_{\underline{y}}^{A}(\xi)\ . \end{aligned}$$

Moreover, the index of Λ *in* $A^{n\times n}$ *is given by*

$$[A^{n\times n}:\Lambda] := |A^{n\times n}/\Lambda| = |\,\mathrm{N}_{K|\mathbf{Q}}(\Delta_{L|K,\underline{y}})|^{\frac{n}{2}} \ .$$

This result can also be attained by specifying the result of M. Künzer concerning the colength of the Wedderburn embedding, see [3, Theorem 2.15].

Proof. We have

$$\begin{tikzcd}
L\wr G \arrow[r, "\omega_0", "\sim"'] \arrow[rr, bend left, "\omega_{\underline{y}}", "\sim"'] & \mathrm{End}_K L \arrow[r, "\omega_{1,\underline{y}}", "\sim"'] & K^{n\times n} \\
\xi \arrow[rr, mapsto] & & \omega_{\underline{y}}(\xi) =: (\omega_{\underline{y};\,i,j}(\xi))_{i,j} \ .
\end{tikzcd}$$

Write $G=\{\sigma_1,...,\sigma_n\}$.

Let $\beta=(\beta_{(i,j),(l,t)})_{(i,j),(l,t)}\in A^{n^2\times n^2}$ be the representation matrix of $\omega_{\underline{y}}^{A}$, with respect to the A-linear basis $(y_l\sigma_t)_{l,t\in[1,n]}$ of $B\wr G$ and the A-linear basis $(\mathrm{e}_{i,j})_{i,j\in[1,n]}$ of $A^{n\times n}$.

Then $\beta=(\beta_{(i,j),(l,t)})_{(i,j),(l,t)}\in K^{n^2\times n^2}$ is also the representation matrix of $\omega_{\underline{y}}$, with respect to the K-linear basis $(y_l\sigma_t)_{l,t\in[1,n]}$ of $L\wr G$ and the K-linear basis $(\mathrm{e}_{i,j})_{i,j\in[1,n]}$ of $K^{n\times n}$.

We obtain

$$\beta_{(i,j),(l,t)}=\omega_{\underline{y};\,i,j}(y_l\sigma_t) \ ,$$

for $i,j,l,t\in[1,n]$. We aim to determine the coefficients of the representation matrix $\gamma=(\gamma_{(t,l),(j,i)})_{(t,l),(j,i)}\in K^{n^2\times n^2}$ of $\omega_{\underline{y}}^{-1}$, with respect to the K-linear bases $(\mathrm{e}_{j,i})_{j,i\in[1,n]}$ of $K^{n\times n}$ and $(\sigma_t y_l)_{t,l\in[1,n]}$ of $L\wr G$.

Write

$$y_l^* =: \sum_{m\in[1,n]} a_{l,m}y_m \ , \text{ where } a_{l,m}\in K \text{ for } l,m\in[1,n] \ .$$

Recall that

$$\begin{array}{rcl}
(a_{l,m})_{l,m} & = & (\mathrm{Gram}_{L|K,\underline{y}})^{-1} \\
\det(\mathrm{Gram}_{L|K,\underline{y}}) & = & \Delta_{L|K,\underline{y}} \ .
\end{array}$$

Given $i, j \in [1, n]$, we have

$$\begin{aligned}
\omega_{\underline{y}}^{-1}(\mathrm{e}_{j,i}) &= \omega_0^{-1}(\omega_{1,\underline{y}}^{-1}(\mathrm{e}_{j,i})) \\
&\overset{\text{Lemma 12}}{=} \sum_{t,l\in[1,n]} \mathrm{Tr}_K(\omega_0(y_l^*\sigma_t^{-1}) \circ \omega_{1,\underline{y}}^{-1}(\mathrm{e}_{j,i}))\sigma_t y_l \\
&= \sum_{t,l\in[1,n]} \mathrm{tr}\,\big(\omega_{1,\underline{y}}(\omega_0(y_l^*\sigma_t^{-1}) \circ \omega_{1,\underline{y}}^{-1}(\mathrm{e}_{j,i}))\big)\sigma_t y_l \\
&= \sum_{t,l\in[1,n]} \mathrm{tr}\,\big(\omega_{1,\underline{y}}(\omega_0(y_l^*\sigma_t^{-1})) \cdot \omega_{1,\underline{y}}(\omega_{1,\underline{y}}^{-1}(\mathrm{e}_{j,i}))\big)\sigma_t y_l \\
&= \sum_{t,l\in[1,n]} \mathrm{tr}\,\big(\omega_{\underline{y}}(y_l^*\sigma_t^{-1})\,\mathrm{e}_{j,i}\,\big)\sigma_t y_l \\
&= \sum_{t,l\in[1,n]} \mathrm{tr}\,\big((\omega_{\underline{y}_{u,v}}(y_l^*\sigma_t^{-1}))_{u,v}\,\mathrm{e}_{j,i}\,\big)\sigma_t y_l \\
&= \sum_{t,l\in[1,n]} \omega_{\underline{y}_{i,j}}(y_l^*\sigma_t^{-1})\sigma_t y_l \\
&= \sum_{t,l\in[1,n]} \omega_{\underline{y}_{i,j}}(\sum_{m\in[1,n]} a_{l,m} y_m \sigma_t^{-1})\sigma_t y_l \\
&= \sum_{t,l,m\in[1,n]} a_{l,m}\omega_{\underline{y}_{i,j}}(y_m\sigma_t^{-1})\sigma_t y_l \ .
\end{aligned}$$

So the coefficient at $\sigma_t y_l$ is given by

$$\gamma_{(t,l),(j,i)} = \sum_{m\in[1,n]} a_{l,m}\omega_{\underline{y}_{i,j}}(y_m\sigma_t^{-1}) \ .$$

Hence

$$\gamma = \begin{pmatrix} (a_{u,v}) & & \\ & \ddots & \\ & & (a_{u,v}) \end{pmatrix} (\omega_{\underline{y}_{i,j}}(y_m\sigma_t^{-1}))_{(t,m),(j,i)} \ ,$$

where we have ordered $\{(t, m) : t, m \in [1, n]\}$ lexicographically.

Write $\gamma' := (\omega_{\underline{y}_{i,j}}(y_m\sigma_t^{-1}))_{(t,m),(j,i)}$. As γ' results from β by transposition, row permutation and column permutation, we have $\det(\gamma') = \mu \det(\beta)$, for some $\mu \in \{-1, +1\}$.

We have

$$\omega_{\underline{y}}^{-1} \circ \omega_{\underline{y}} = \mathrm{id}_{L\wr G}$$

and therefore

$$\begin{aligned}
1 &= \det(\gamma)\det(\beta) \\
&= (\det((a_{u,v})_{u,v}))^n \det(\gamma')\det(\beta) \\
&= (\det((a_{u,v})_{u,v}))^n \mu \det(\beta)\det(\beta) \\
&= \mu\Delta_{L|K,\underline{y}}^{-n}\det(\beta)^2 \ .
\end{aligned}$$

Hence we have

$$\begin{aligned}[A^{n\times n} : \Lambda]^2 = |A^{n\times n}/\Lambda|^2 &\overset{\text{Lemma 15}}{=} |\,\mathrm{N}_{K|\mathbf{Q}}(\det(\beta))|^2 &&= |\,\mathrm{N}_{K|\mathbf{Q}}(\det(\beta)^2)| \\ &= |\,\mathrm{N}_{K|\mathbf{Q}}(\mu^{-1}\Delta_{L|K,\underline{y}})| &&= |\,\mathrm{N}_{K|\mathbf{Q}}(\Delta_{L|K,\underline{y}})|^n\ .\end{aligned}$$

□

Corollary 17. *Keep the notation of* Theorem 16*. Let* $A = \mathbf{Z}$*. Then*

$$[\mathbf{Z}^{n\times n} : \Lambda] := |\mathbf{Z}^{n\times n}/\Lambda| = |\Delta_{L|K,\underline{y}}|^{\frac{n}{2}}\ .$$

4 Quadratic extensions

Setting 18. Let $d \in \mathbf{Z}^\times$ be squarefree. Consider the Galois extension $\mathbf{Q}(\sqrt{d})|\mathbf{Q}$ with Galois group $G = \{\mathrm{id}, \sqrt{d} \overset{\sigma}{\mapsto} -\sqrt{d})\} \cong \mathrm{C}_2$.

$$\begin{tikzcd} & \mathbf{Q}(\sqrt{d}) \arrow[dl, dash] \arrow[d, dash, "G,\ |G|=2"] \\ \mathcal{O}_{\mathbf{Q}(\sqrt{d})} \arrow[d, dash] & \mathbf{Q} \\ \mathbf{Z} \arrow[ur, dash] & \end{tikzcd}$$

Recall that the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{d})$ is given by

$$\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \begin{cases} \mathbf{Z}[\frac{1+\sqrt{d}}{2}] & \text{if} \quad d \equiv_4 1 \\ \mathbf{Z}[\sqrt{d}] & \text{if} \quad d \equiv_4 2 \text{ or } d \equiv_4 3\ . \end{cases}$$

Note that the requirements of Setting 1 and Setting 13 are also met, letting $A = \mathbf{Z}$ and $B = \mathcal{O}_{\mathbf{Q}(\sqrt{d})}$.

Example 19. Regard the extension $\mathbf{Q}(\mathrm{i})|\mathbf{Q}$.

We have $\mathcal{O}_{\mathbf{Q}(\mathrm{i})} = \mathbf{Z}[\mathrm{i}]$ and $G = \{\mathrm{id}, \sigma\}$. Consider the $\mathbf{Z}$-linear basis $\underline{y} = (1, \mathrm{i})$ of $\mathbf{Z}[\mathrm{i}]$ and the $\mathbf{Z}$-linear basis $\underline{z} = (1, \mathrm{i}, \sigma, \mathrm{i}\,\sigma)$ of $\mathbf{Z}[\mathrm{i}] \wr G$.

Then $\omega_{\underline{y}}^{\mathbf{Z}} : \mathbf{Z}[\mathrm{i}] \wr G \to \mathbf{Z}^{2\times 2}$, maps

$$\begin{array}{lllll} 1 & \mapsto \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) & \qquad\qquad & \mathrm{i} & \mapsto \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right) \\ \sigma & \mapsto \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right) & & \mathrm{i}\,\sigma & \mapsto \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right) \quad . \end{array}$$

The image of $\omega_{\underline{y}}^{\mathbf{Z}}$ is given by the subring $\Lambda := \{\left(\begin{smallmatrix}s&t\\u&v\end{smallmatrix}\right) \in \mathbf{Z}^{2\times 2} : s \equiv_2 v \text{ and } t \equiv_2 u\}$.

In fact, the image of the basis elements of $\underline{z}$ are contained in Λ, and the index of Λ in $\mathbf{Z}^{2\times 2}$ is $[\mathbf{Z}^{2\times 2} : \Lambda] = 4 = |\Delta_{\mathbf{Q}(\mathrm{i})|\mathbf{Q},\underline{y}}|^{\frac{2}{2}}$; cf. Corollary 17.

More generally, we have the

Proposition 20. *Suppose that $d \equiv_4 2$ or $d \equiv_4 3$.*

We consider the $\mathbf{Z}$-linear basis $\underline{y} = (1, \sqrt{d})$ of $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[\sqrt{d}]$.

Consider the map $\omega_{\underline{y}}^{\mathbf{Z}} : \mathbf{Z}[\sqrt{d}] \wr G \to \mathbf{Z}^{2\times 2}$.

Then the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ is given by $\Lambda := \left\{ \left(\begin{smallmatrix} s & dw \\ u & v \end{smallmatrix}\right) : s, w, u, v \in \mathbf{Z}, s \equiv_2 v,\ w \equiv_2 u \right\}$.

In particular, we have an isomorphism of rings $\mathbf{Z}[\sqrt{d}] \wr G \xrightarrow{\sim} \Lambda$.

Proof. We consider the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ on the $\mathbf{Z}$-linear basis $\underline{z} = (1, \sqrt{d}, \sigma, \sqrt{d}\sigma)$ of $\mathbf{Z}[\sqrt{d}] \wr G$.

$$\begin{array}{llcll} 1 & \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) & \qquad & \sqrt{d} & \mapsto \left(\begin{smallmatrix} 0 & d \\ 1 & 0 \end{smallmatrix}\right) \\ \sigma & \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) & & \sqrt{d}\sigma & \mapsto \left(\begin{smallmatrix} 0 & -d \\ 1 & 0 \end{smallmatrix}\right) \end{array}$$

Let A be the representation matrix of $\omega_{\underline{y}}^{\mathbf{Z}}$ with respect to the bases $\underline{z}$ of $\mathbf{Z}[\sqrt{d}] \wr G$ and $(\mathrm{e}_{i,j})_{i,j\in[1,2]}$ of $\mathbf{Z}^{2\times 2}$. We obtain

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & d & 0 & -d \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \text{ and } A^{-1} = \frac{1}{2d} \begin{pmatrix} d & 0 & 0 & d \\ 0 & 1 & d & 0 \\ d & 0 & 0 & -d \\ 0 & -1 & d & 0 \end{pmatrix}.$$

So for $\left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \mathbf{Z}^{2\times 2}$ we get

$$\begin{aligned} \left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \Lambda \Leftrightarrow & \begin{pmatrix} d & 0 & 0 & d \\ 0 & 1 & d & 0 \\ d & 0 & 0 & -d \\ 0 & -1 & d & 0 \end{pmatrix} \begin{pmatrix} s \\ t \\ u \\ v \end{pmatrix} \in 2d\mathbf{Z}^{4\times 1} \\ \Leftrightarrow & \left\{ \begin{array}{rcrcl} sd & + & vd & \equiv_{2d} & 0 \\ t & + & ud & \equiv_{2d} & 0 \\ sd & - & vd & \equiv_{2d} & 0 \\ -t & + & ud & \equiv_{2d} & 0 \end{array} \right. \\ \Leftrightarrow & \left\{ \begin{array}{rcl} s & \equiv_2 & v \\ t + ud & \equiv_{2d} & 0 \\ t & \equiv_d & 0\,. \end{array} \right. \qquad\qquad (\star) \end{aligned}$$

Since $t \equiv_d 0$ there is $w \in \mathbf{Z}$ such that $t = dw$. So in $(\star)$ we obtain $dw + du \equiv_{2d} 0$, i.e. $w \equiv_2 u$. The congruences for s, v, w, u now read as follows

$$\begin{array}{rcl} s & \equiv_2 & v \\ t & \equiv_d & 0 \\ w & \equiv_2 & u\,. \end{array}$$

Hence the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ is given by the subring

$$\Lambda = \left\{ \left(\begin{smallmatrix} s & dw \\ u & v \end{smallmatrix} \right) : s, w, u, v \in \mathbf{Z}, s \equiv_2 v,\ w \equiv_2 u \right\} .$$

□

Remark 21. Theorem 16 states that the index of Λ in $\mathbf{Z}^{2\times 2}$ is

$$[\mathbf{Z}^{2\times 2} : \Lambda] = |\Delta_{\mathbf{Q}(\sqrt{d})|\mathbf{Q},\underline{y}}| = |(\sqrt{d} - (-\sqrt{d}))^2| = |4d| .$$

We will verify this by a direct calculation

$$[\mathbf{Z}^{2\times 2} : \Lambda] = |\det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & d & 0 & -d \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \end{pmatrix} | = |4d| .$$

Proposition 22. *Suppose that $d \equiv_4 1$.*
Write $\alpha := \frac{1+\sqrt{d}}{2}$. Choose $x \in \mathbf{Z}$ such that $2x \equiv_d -1$.
We consider the $\mathbf{Z}$-linear basis $\underline{y} = (1, \alpha + x)$ of $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[\alpha]$.
Consider the map $\omega_{\underline{y}}^{\mathbf{Z}} : \mathbf{Z}[\alpha] \wr G \to \mathbf{Z}^{2\times 2}$.
Then the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ is given by $\Lambda := \left\{ \left(\begin{smallmatrix} s & dw \\ u & v \end{smallmatrix} \right) : s, w, u, v \in \mathbf{Z} \right\} = \left(\begin{smallmatrix} \mathbf{Z} & (d) \\ \mathbf{Z} & \mathbf{Z} \end{smallmatrix} \right) \subseteq \mathbf{Z}^{2\times 2}$.
In particular, we have an isomorphism of rings $\mathbf{Z}[\alpha] \wr G \xrightarrow{\sim} \Lambda$.

Proof. Define $a := \frac{d-1}{4}$. It follows that

$$\alpha^2 = \tfrac{1}{4}(1 + 2\sqrt{d} + d) = \tfrac{2+2\sqrt{d}}{4} + \tfrac{d-1}{4} = \alpha + \tfrac{d-1}{4} = \alpha + a .$$

We consider the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ on the $\mathbf{Z}-$linear basis $\underline{z} = (1, \alpha + x, \sigma, (\alpha + x)\sigma)$ of $\mathbf{Z}[\alpha] \wr G$.

$$\begin{array}{lll} 1 & \mapsto & \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right) \\ \sigma & \mapsto & \left(\begin{smallmatrix} 1 & 2x+1 \\ 0 & -1 \end{smallmatrix} \right) \end{array} \qquad \begin{array}{rll} \alpha + x & \mapsto & \left(\begin{smallmatrix} 0 & a-x^2-x \\ 1 & 2x+1 \end{smallmatrix} \right) \\ (\alpha + x)\sigma & \mapsto & \left(\begin{smallmatrix} 0 & x^2+x-a \\ 1 & 0 \end{smallmatrix} \right) \end{array}$$

Let A be the representation matrix of $\omega_{\underline{y}}^{\mathbf{Z}}$, with respect to the bases $\underline{z}$ of $\mathbf{Z}[\alpha] \wr G$ and $(\mathrm{e}_{i,j})_{i,j \in [1,2]}$ of $\mathbf{Z}^{2\times 2}$. We obtain

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & a - x^2 - x & 2x + 1 & x^2 + x - a \\ 0 & 1 & 0 & 1 \\ 1 & 2x + 1 & -1 & 0 \end{pmatrix}$$

and

$$A^{-1} = \frac{1}{d}\begin{pmatrix} 2x^2+2x+1+2a & -2x-1 & -(2x+1)(-x^2+a-x) & -2x^2+2a-2x \\ -2x-1 & 2 & -2x^2+2a-2x & 2x+1 \\ -2x^2+2a-2x & 2x+1 & (2x+1)(-x^2+a-x) & 2x^2-2a+2x \\ 2x+1 & -2 & 2x^2+2a+2x+1 & -2x-1 \end{pmatrix}.$$

Since $2x \equiv_d -1$ we obtain for $\left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \mathbf{Z}^{2\times 2}$ that:

$$\left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \Lambda \Leftrightarrow \begin{pmatrix} 2x^2+2a & 0 & 0 & -2x^2+2a+1 \\ 0 & 2 & -2x^2+2a+1 & 0 \\ -2x^2+2a+1 & 0 & 0 & 2x^2-2a-1 \\ 0 & -2 & 2x^2+2a & 0 \end{pmatrix}\begin{pmatrix} s \\ t \\ u \\ v \end{pmatrix} \in d\mathbf{Z}^{4\times 1}$$

$$\Leftrightarrow \left\{\begin{array}{ccccc} (2x^2+2a)s & + & (-2x^2+2a+1)v & \equiv_d & 0 \qquad (1) \\ 2t & + & (-2x^2+2a+1)u & \equiv_d & 0 \qquad (2) \\ (-2x^2+2a+1)s & + & (2x^2-2a-1)v & \equiv_d & 0 \qquad (3) \\ -2t & + & (2x^2+2a)u & \equiv_d & 0 \qquad (4) \end{array}\right.$$

The sum of (1) and (3) yields: $(4a+1)s \equiv_d 0$, which is redundant since $4a+1 = d$.

The sum of (2) and (4) yields: $(4a+1)u \equiv_d 0$, which is redundant since $4a+1 = d$.

Therefore we obtain

$$\begin{array}{lcl} \left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \Lambda & \Leftrightarrow & \left\{\begin{array}{ccccc} (2x^2+2a)s & + & (-2x^2+2a+1)v & \equiv_d & 0 \\ 2t & + & (-2x^2+2a+1)u & \equiv_d & 0 \end{array}\right. \\ & \overset{d \not\equiv_2 0}{\Longleftrightarrow} & \left\{\begin{array}{ccccc} (4x^2+4a)s & + & (-4x^2+4a+2)v & \equiv_d & 0 \\ 4t & + & (-4x^2+4a+2)u & \equiv_d & 0 \end{array}\right. \\ & \underset{4a+1=d}{\overset{4x^2 \equiv_d 1}{\Longleftrightarrow}} & \left\{\begin{array}{l} ds + dv \equiv_d 0 \\ 4t + du \equiv_d 0 \end{array}\right. \\ & \overset{d \not\equiv_4 0}{\Longleftrightarrow} & \left\{ t \equiv_d 0 \right. . \end{array}$$

Hence the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ is given by the subring

$$\Lambda := \{\left(\begin{smallmatrix} s & dw \\ u & v \end{smallmatrix}\right) : s,w,u,v \in \mathbf{Z}\} = \left(\begin{smallmatrix} \mathbf{Z} & (d) \\ \mathbf{Z} & \mathbf{Z} \end{smallmatrix}\right) .$$

□

Remark 23. Theorem 16 states that the index of Λ in $\mathbf{Z}^{2\times 2}$ is

$$[\mathbf{Z}^{2\times 2} : \Lambda] = |\Delta_{\mathbf{Q}(\sqrt{d})|\mathbf{Q},\underline{y}}| = |(\alpha - (1-\alpha))^2| = |(2\alpha - 1)^2| = |(\sqrt{d})^2| = |d| \ .$$

We will verify this by a direct calculation

$$[\mathbf{Z}^{2\times 2} : \Lambda] = |\det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & a - x^2 - x & 2x+1 & x^2 + x - a \\ 0 & 1 & 0 & 1 \\ 1 & 2x+1 & -1 & 0 \end{pmatrix} | = |d| \ .$$

5 Cyclotomic extensions

Setting 24. Let $m \in \mathbf{Z}_{>0}$. Consider the Galois extension $\mathbf{Q}(\zeta_m)|\mathbf{Q}$ with Galois group $G = \{\mathbf{Q}(\zeta_m) \xrightarrow{\sim} \mathbf{Q}(\zeta_m),\ \zeta_m \mapsto \zeta_m^k : k \in [0, m-1],\ \gcd(k,m) = 1\} \cong \mathrm{U}(\mathbf{Z}/(m))$.

$$\begin{tikzcd}
& \mathbf{Q}(\zeta_m) \arrow[ld, dash] \arrow[d, dash, "{G,\ |G|=\varphi(m):=|\{k\in[0,m-1]:\ \gcd(k,m)=1\}|}"] \\
\mathcal{O}_{\mathbf{Q}(\zeta_m)} \arrow[d, dash] & \mathbf{Q} \\
\mathbf{Z} \arrow[ru, dash] &
\end{tikzcd}$$

Recall that the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\zeta_m)$ is given by $\mathcal{O}_{\mathbf{Q}(\zeta_m)} = \mathbf{Z}[\zeta_m]$, see [6, I. Proposition (10.2)].

Note that the requirements of Setting 1 and Setting 13 are also met, letting $A = \mathbf{Z}$ and $B = \mathcal{O}_{\mathbf{Q}(\zeta_m)}$.

Theorem 25. *Let $p \in \mathbf{Z}_{>0}$ be a prime.*

Consider the Galois extension $\mathbf{Q}(\zeta_p)|\mathbf{Q}$ with Galois group C_{p-1} . Consider the $\mathbf{Z}$-linear basis $\underline{y} = ((\zeta_p - 1)^0, \ldots, (\zeta_p - 1)^{p-2})$ of $\mathbf{Z}[\zeta_p]$. We have

$$\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\zeta_p] \wr \mathrm{C}_{p-1}) =: \Lambda = \begin{pmatrix} \mathbf{Z} & (p) & \cdots & (p) \\ \mathbf{Z} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & (p) \\ \mathbf{Z} & \cdots & \mathbf{Z} & \mathbf{Z} \end{pmatrix} \subseteq \mathbf{Z}^{(p-1)\times(p-1)} \ .$$

In particular, we have an isomorphism of rings $\mathbf{Z}[\zeta_p] \wr \mathrm{C}_{p-1} \xrightarrow{\sim} \Lambda$.

Proof. Consider the map $\omega_{\underline{y}}^{\mathbf{Z}} : \mathbf{Z}[\zeta] \wr \mathrm{C}_{p-1} \to \mathbf{Z}^{(p-1)\times(p-1)}$. Let Λ be the image of $\omega_{\underline{y}}^{\mathbf{Z}}$. We need to show

$$\Lambda \overset{!}{=} \begin{pmatrix} \mathbf{Z} & (p) & \cdots & (p) \\ \mathbf{Z} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & (p) \\ \mathbf{Z} & \cdots & \mathbf{Z} & \mathbf{Z} \end{pmatrix} =: \Lambda' \ .$$

Step 1. We show $\Lambda \overset{!}{\subseteq} \Lambda'$.

For this we *claim* that the additive subgroup Λ' of $\mathbf{Z}^{(p-1)\times(p-1)}$ is a subring.

Consider the surjective ring morphism

$$\begin{aligned} \tau : \mathbf{Z}^{(p-1)\times(p-1)} &\to \mathbf{F}_p^{(p-1)\times(p-1)} \\ (z_{i,j})_{i,j} &\mapsto (z_{i,j} + (p))_{i,j} \ . \end{aligned}$$

We obtain $\tau(\Lambda') = \begin{pmatrix} \mathbf{F}_p & 0 & \cdots & 0 \\ \mathbf{F}_p & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \mathbf{F}_p & \cdots & \mathbf{F}_p & \mathbf{F}_p \end{pmatrix}$, which is a subring of $\mathbf{F}_p^{(p-1)\times(p-1)}$. Moreover, we have $\Lambda' = \tau^{-1}(\tau(\Lambda'))$. Since τ is a ring morphism, the pre-image Λ' is a subring of $\mathbf{Z}^{(p-1)\times(p-1)}$. This proves the *claim.*

Choose $j \in [1, p-1]$ such that $\mathrm{U}(\mathbf{F}_p) = \langle j + (p) \rangle$. Then $\sigma : \mathbf{Q}(\zeta_p) \to \mathbf{Q}(\zeta_p)$, $\zeta_p \mapsto \zeta_p^j$ is a generator of C_{p-1} i.e. $\mathrm{C}_{p-1} = \langle \sigma \rangle$.

Since Λ' is a subring of $\mathbf{Z}^{(p-1)\times(p-1)}$ it now suffices to show that $\omega_{\underline{y}}^{\mathbf{Z}}$ maps the ring generators ζ_p and σ of $\mathbf{Z}[\zeta_p] \wr \mathrm{C}_{p-1}$ to Λ'.

The minimal polynomial of $\zeta_p - 1$ is given by

$$\mu_{\zeta_p - 1, \mathbf{Q}}(x) = \mu_{\zeta_p, \mathbf{Q}}(x+1) = \frac{(x+1)^p - 1}{(x+1) \ \ - 1} = \sum_{k \in [1,p]} \tbinom{p}{k} x^{k-1}$$

and therefore it follows that

$$\mu_{\zeta_p - 1, \mathbf{Q}}(x) \equiv_p x^{p-1} \ .$$

So

$$\zeta_p - 1 \overset{\omega_{\underline{y}}}{\longmapsto} \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -\binom{p}{1} \\ 1 & 0 & 0 & \cdots & 0 & -\binom{p}{2} \\ 0 & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & 0 & -\binom{p}{p-2} \\ 0 & 0 & 0 & 0 & 1 & -\binom{p}{p-1} \end{pmatrix} \in \Lambda' \,.$$

Let $\pi := (\zeta_p - 1)$. Recall that $(\pi)^{p-1} = (p)$ in $\mathbf{Z}[\zeta_p]$, see e.g. [6, I. Lemma (10.1)]. We have $(p) \subseteq \mathbf{Z} \cap (\pi)$. Since (p) is a maximal ideal in $\mathbf{Z}$ and because of $1 \notin (\pi)$, and therefore $1 \notin \mathbf{Z} \cap (\pi)$, we have $(\pi) \cap \mathbf{Z} = (p)$.

We show that $\sigma(\pi^k)$ is divisible by π^k for $k \in [1, p-2]$.

We have

$$\sigma(\pi) = \zeta_p^j - 1 = (\zeta_p - 1) \sum_{i \in [0, j-1]} \zeta_p^i =: \pi\theta$$

with $\theta \in \mathbf{Z}[\zeta_p]$. Suppose given $k \in [1, p-2]$. Then

$$\sigma(\pi^k) = (\sigma(\pi))^k = (\pi\theta)^k = \pi^k \theta^k$$

is divisible by π^k.

Write $x := \sigma(\pi^k) := a_0 + a_1\pi + a_2\pi^2 + \cdots + a_{p-2}\pi^{p-2}$, where $a_0, \ldots, a_{p-2} \in \mathbf{Z}$. We show that a_l is divisible by p using induction on $l \in [0, k-1]$.

Initial step: Suppose $l = 0$. Since x is divisible by π, a_0 has to be divisible by π in $\mathbf{Z}[\zeta_p]$ and therefore lie in $(\pi) \subseteq \mathbf{Z}[\zeta_p]$. This leads to $a_0 \in (\pi) \cap \mathbf{Z} = (p)$.

Induction step: Let $l \in [1, k-1]$. We have that for $a_0, \ldots, a_{p-2} \in \mathbf{Z}$

$$x = a_0 + a_1\pi + a_2\pi^2 + \cdots + a_{k-1}\pi^{k-1} + a_k\pi^k + \cdots + a_{p-2}\pi^{p-2}$$

is divisible by π^k, hence by π^{l+1}.

By induction hypothesis it follows that $a_0, \ldots, a_{l-1}$ are divisible by p and so divisible in $\mathbf{Z}[\zeta_p]$ by π^{l+1}.

Therefore $a_i\pi^i$ is divisible by π^{l+1} for $i \in [0, p-2] \setminus \{l\}$.

Hence $a_l\pi^l$ is divisible by π^{l+1} and so a_l needs to be divisible by π in $\mathbf{Z}[\zeta_p]$.

This leads to $a_l \in (\pi) \cap \mathbf{Z} = (p)$. This concludes the induction.

Note that the column of $\omega_{\underline{y}}(\sigma)$ belonging to the basis element π^k is given by $\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{p-2} \end{pmatrix}$.

So it follows that $\omega_{\underline{y}}(\sigma) \in \Lambda'$.

Altogether, we have $\Lambda \subseteq \Lambda'$.

Step 2. We show $[\mathbf{Z}^{(p-1)\times(p-1)} : \Lambda'] \overset{!}{=} [\mathbf{Z}^{(p-1)\times(p-1)} : \Lambda]$.

Since $[\mathbf{Z} : \mathbf{Z}] = 1$ and $[\mathbf{Z} : (p)] = p$, it follows that $[\mathbf{Z}^{(p-1)\times(p-1)} : \Lambda'] = p^{\frac{(p-1)(p-2)}{2}}$.

We have $|\Delta_{\mathbf{Q}(\zeta_p)|\mathbf{Q},\underline{y}}| = p^{p-2}$, cf. [6, I. Lemma (10.1)].

By Corollary 17 it follows that

$$[\mathbf{Z}^{(p-1)\times(p-1)} : \Lambda] = |\Delta_{\mathbf{Q}(\zeta_p)|\mathbf{Q},\underline{y}}|^{\frac{p-1}{2}} = |p^{p-2}|^{\frac{p-1}{2}} = p^{\frac{(p-1)(p-2)}{2}} \; .$$

Conclusion.
Since $\Lambda \subseteq \Lambda' \subseteq \mathbf{Z}^{(p-1)\times(p-1)}$ by *Step 1*, we have

$$[\mathbf{Z}^{(p-1)\times(p-1)} : \Lambda'][\Lambda' : \Lambda] = [\mathbf{Z}^{(p-1)\times(p-1)} : \Lambda] \; .$$

Since $[\mathbf{Z}^{(p-1)\times(p-1)} : \Lambda'] = [\mathbf{Z}^{(p-1)\times(p-1)} : \Lambda]$ by *Step 2*, we conclude that

$$[\Lambda' : \Lambda] = 1, \text{ i.e. } \Lambda' = \Lambda \; .$$

□

Example 26. Regard the extension $\mathbf{Q}(\zeta_3)|\mathbf{Q}$. Write $\zeta := \zeta_3 = \frac{-1+\sqrt{-3}}{2}$.

Its Galois group is given by $G = \{\mathrm{id}, \zeta \mapsto \zeta^2\}$.

We have $\mathbf{Q}(\zeta) = \mathbf{Q}(\sqrt{-3})$ and $\mathcal{O}_{\mathbf{Q}(\zeta)} = \mathbf{Z}[\zeta] = \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$.

Choose the $\mathbf{Z}$-linear basis $\underline{y} = (1, \frac{-3+\sqrt{-3}}{2}) = ((\zeta-1)^0, (\zeta-1)^1) = (1, \frac{1+\sqrt{-3}}{2} + (-2))$ of $\mathbf{Z}[\zeta]$, where $2(-2) \equiv_{-3} -1$. So $\underline{y}$ may be used in Proposition 22 and Theorem 25.

By Proposition 22, the image of $\omega_{\underline{y}}^{\mathbf{Z}} : \mathbf{Z}[\zeta] \to \mathbf{Z}^{2\times 2}$ is given by

$$\Lambda = \{\left(\begin{smallmatrix} s & -3w \\ u & v \end{smallmatrix}\right) \in \mathbf{Z}^{2\times 2}\} = \left(\begin{smallmatrix} \mathbf{Z} & (-3) \\ \mathbf{Z} & \mathbf{Z} \end{smallmatrix}\right) = \left(\begin{smallmatrix} \mathbf{Z} & (3) \\ \mathbf{Z} & \mathbf{Z} \end{smallmatrix}\right) \; ,$$

which confirms the statement of Theorem 25 in this case.

Example 27. Consider the Galois extension $\mathbf{Q}(\zeta_5)|\mathbf{Q}$. Define $\zeta := \zeta_5$.

Its Galois group is given by $G = \{\mathrm{id}, \zeta \overset{\sigma}{\mapsto} \zeta^2, \sigma^2, \sigma^3\}$.

We consider the $\mathbf{Z}$-linear basis $\underline{y} = (1, \zeta-1, (\zeta-1)^2, (\zeta-1)^3)$ of $\mathcal{O}_{\mathbf{Q}(\zeta)} = \mathbf{Z}[\zeta]$ and the $\mathbf{Z}$-linear basis $\underline{z} = (1, \zeta, \zeta^2, \zeta^3, \sigma, \zeta\sigma, \zeta^2\sigma, \zeta^3\sigma, \sigma^2, \zeta\sigma^2, \zeta^2\sigma^2, \zeta^3\sigma^2, \sigma^3, \zeta\sigma^3, \zeta^2\sigma^3, \zeta^3\sigma^3)$ of $\mathbf{Z}[\zeta] \wr G$.

Then $\omega_{\underline{y}}^{\mathbf{Z}} : \mathbf{Z}[\zeta] \wr G \to \mathbf{Z}^{4\times 4}$ maps

$$\zeta^j\sigma^k \quad \mapsto \quad \begin{pmatrix} 1 & 0 & 0 & -5 \\ 1 & 1 & 0 & -10 \\ 0 & 1 & 1 & -10 \\ 0 & 0 & 1 & -4 \end{pmatrix}^j \begin{pmatrix} 1 & 0 & -5 & 15 \\ 0 & 2 & -10 & 25 \\ 0 & 1 & -6 & 15 \\ 0 & 0 & -1 & 3 \end{pmatrix}^k \quad \text{for } j,k \in [0,3] \; .$$

Let Λ be the image of $\omega_{\underline{y}}^{\mathbf{Z}}$. We want to illustrate and confirm Theorem 25 by a direct calculation.

Let A be the representation matrix of $\omega_{\underline{y}}^{\mathbf{Z}}$ with respect to the bases $\underline{z}$ of $\mathbf{Z}[\zeta] \wr G$ and $(\mathrm{e}_{i,j})_{i,j\in[1,4]}$ of $\mathbf{Z}^{4\times 4}$. We obtain by a direct calculation
$A =$

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & -5 & 0 & 0 & -5 & 0 & -5 & 0 & 0 & 0 & 0 & -5 & 0 & 0 \\
0 & 0 & -5 & 10 & -5 & 0 & 10 & 0 & 10 & -5 & 0 & 0 & 0 & 10 & 0 & -5 \\
0 & -5 & 15 & -15 & 15 & 0 & -15 & -5 & -15 & 15 & -5 & 0 & -5 & -15 & 0 & 15 \\
0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\
1 & 1 & 1 & -9 & 2 & 2 & -8 & -3 & -6 & -1 & -1 & -1 & 3 & -7 & -2 & -2 \\
0 & 0 & -10 & 15 & -10 & -5 & 15 & 5 & 15 & -5 & 0 & 0 & -5 & 15 & 5 & -5 \\
0 & -10 & 25 & -20 & 25 & 10 & -20 & -15 & -25 & 20 & -5 & 0 & 0 & -25 & -10 & 20 \\
0 & 0 & 1 & 3 & 0 & 0 & 1 & 3 & 0 & 0 & 1 & 3 & 0 & 0 & 1 & 3 \\
0 & 1 & 2 & -7 & 1 & 3 & -5 & -3 & -4 & 0 & -1 & -2 & 3 & -4 & -1 & -3 \\
1 & 1 & -9 & 11 & -6 & -6 & 9 & 4 & 11 & -4 & 1 & 1 & -6 & 9 & 4 & -1 \\
0 & -10 & 20 & -15 & 15 & 10 & -10 & -10 & -20 & 15 & -5 & 0 & 5 & -15 & -10 & 10 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & -2 & 0 & 1 & -1 & -1 & -1 & 0 & 0 & -1 & 1 & -1 & 0 & -1 \\
0 & 1 & -3 & 3 & -1 & -2 & 2 & 1 & 3 & -1 & 0 & 1 & -2 & 2 & 1 & 0 \\
1 & -4 & 6 & -4 & 3 & 3 & -2 & -2 & -6 & 4 & -1 & -1 & 2 & -3 & -3 & 2
\end{pmatrix}$$

and
$A^{-1} =$

$$\frac{1}{5}\begin{pmatrix}
0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 5 & 10 & 10 & 5 \\
-5 & -7 & -4 & -1 & 5 & 5 & 3 & 1 & -5 & -5 & -5 & -2 & 10 & 15 & 15 & 5 \\
0 & 2 & 3 & 1 & -5 & -10 & -8 & -2 & 10 & 15 & 10 & 2 & -10 & -10 & -5 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & -5 & -10 & -10 & -4 & 20 & 35 & 30 & 10 \\
0 & -3 & -3 & -1 & 0 & 5 & 6 & 2 & 5 & 0 & -5 & -2 & -20 & -20 & -5 & 0 \\
0 & -1 & -2 & -1 & 0 & 0 & 2 & 1 & 5 & 10 & 5 & 1 & -15 & -30 & -20 & -5 \\
-5 & -9 & -7 & -2 & 5 & 10 & 8 & 2 & 0 & -5 & -5 & -1 & -10 & -5 & 0 & 0 \\
0 & -2 & -3 & -1 & -5 & -5 & -1 & 0 & 15 & 20 & 10 & 2 & -30 & -45 & -25 & -5 \\
5 & 6 & 4 & 1 & -10 & -15 & -11 & -3 & 15 & 25 & 20 & 6 & -20 & -35 & -30 & -10 \\
5 & 7 & 4 & 1 & -5 & -10 & -7 & -2 & 0 & 5 & 5 & 2 & 10 & 10 & 5 & 0 \\
5 & 8 & 5 & 1 & -5 & -10 & -8 & -2 & 5 & 10 & 10 & 3 & -10 & -15 & -15 & -5 \\
5 & 9 & 7 & 2 & -5 & -10 & -9 & -3 & 5 & 10 & 10 & 4 & -5 & -10 & -10 & -5 \\
0 & -2 & -1 & 0 & 5 & 10 & 6 & 1 & -15 & -25 & -15 & -3 & 30 & 45 & 25 & 5 \\
0 & 1 & 2 & 1 & 5 & 5 & 2 & 0 & -10 & -10 & -5 & -1 & 10 & 5 & 0 & 0 \\
0 & -1 & -1 & 0 & 5 & 10 & 8 & 2 & -10 & -20 & -15 & -4 & 15 & 30 & 20 & 5 \\
-5 & -8 & -5 & -1 & 10 & 15 & 9 & 2 & -15 & -20 & -10 & -2 & 20 & 20 & 5 & 0
\end{pmatrix}.$$

We have for $X = (x_{i,j})_{i,j\in[1,4]} \in \mathbf{Z}^{4\times 4}$

$$\begin{aligned}
X \in \Lambda &\Leftrightarrow \omega_{\underline{y}}^{-1}(X) \in \mathbf{Z}[\zeta] \wr G \\
&\Leftrightarrow A^{-1} \cdot \begin{pmatrix} x_{1,1} \\ x_{1,2} \\ \vdots \\ x_{4,4} \end{pmatrix} \in \mathbf{Z}^{16\times 1}
\end{aligned}$$

$$\Leftrightarrow \begin{pmatrix} 0 & 4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 3 & 1 & 4 & 0 & 0 & 3 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 2 & 3 & 1 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 4 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 4 & 3 & 4 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 3 & 0 & 0 & 3 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 3 & 2 & 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 4 & 1 & 0 & 0 & 4 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 1 & 0 & 0 & 3 & 3 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 4 & 2 & 2 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 3 & 4 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 4 & 4 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 4 & 0 & 0 & 4 & 2 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_{1,1} \\ x_{1,2} \\ x_{1,3} \\ x_{1,4} \\ x_{2,1} \\ x_{2,2} \\ x_{2,3} \\ x_{2,4} \\ x_{3,1} \\ x_{3,2} \\ x_{3,3} \\ x_{3,4} \\ x_{4,1} \\ x_{4,2} \\ x_{4,3} \\ x_{4,4} \end{pmatrix} \in 5\mathbf{Z}^{16\times 1}$$

$$\Leftrightarrow \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_{1,1} \\ x_{1,2} \\ \vdots \\ \vdots \\ x_{4,4} \end{pmatrix} \in 5\mathbf{Z}^{6\times 1}$$

$$\Leftrightarrow \left\{ \begin{array}{rcl} x_{1,2} & \equiv_5 & 0 \\ x_{1,3} & \equiv_5 & 0 \\ x_{1,4} & \equiv_5 & 0 \\ x_{2,3} & \equiv_5 & 0 \\ x_{2,4} & \equiv_5 & 0 \\ x_{3,4} & \equiv_5 & 0 \end{array} \right. \Leftrightarrow X \in \Lambda := \begin{pmatrix} \mathbf{Z} & (5) & (5) & (5) \\ \mathbf{Z} & \mathbf{Z} & (5) & (5) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (5) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \end{pmatrix}$$

Hence the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ is given by Λ, confirming the result of Theorem 25 in this case.

Remark 28. Theorem 25 shows that in case of m being a prime the $\mathbf{Z}$-linear basis

$$\underline{y} = ((\zeta_m - 1)^0, \ldots, (\zeta_m - 1)^{m-2})$$

of $\mathbf{Z}[\zeta_m]$ leads to a quite simple description of $\Lambda = \omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\zeta_m \wr G)$.

If m is not a prime this is different.

In case of $m = 9$, for instance, the $\mathbf{Z}$-linear basis $\underline{y} = ((\zeta_9 - 1)^0, \ldots, (\zeta_9 - 1)^5)$ of $\mathbf{Z}[\zeta_9]$ leads to a rather complicated structure. Our result using this basis involves congruences of length up to eleven matrix entries.

In this case the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ is given by

$$\Lambda := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (3) & (3) & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} & (3) & (3) & \mathbf{Z} & \mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \end{pmatrix} \subseteq \mathbf{Z}^{6\times 6} : \right.$$

$$\left. \begin{array}{rcl} x_{1,1} & \equiv_3 & x_{3,3} \equiv_3 x_{5,5} \\ x_{2,1} + x_{5,5} + 2x_{6,5} + 2x_{6,6} & \equiv_3 & 0 \\ x_{2,2} & \equiv_3 & x_{4,4} \equiv_3 x_{6,6} \\ x_{3,2} + 2x_{5,4} + x_{5,5} + 2x_{6,6} & \equiv_3 & 0 \\ x_{4,3} + 2x_{5,5} + 2x_{6,5} + x_{6,6} & \equiv_3 & 0 \\ x_{1,4} + 3x_{3,1} + x_{3,6} + 6x_{4,2} + 6x_{5,2} + 6x_{5,3} + 3x_{5,4} + 3x_{5,5} + 3x_{6,4} + 6x_{6,5} + 6x_{6,6} & \equiv_9 & 0 \\ x_{1,5} + 6x_{3,1} + 6x_{5,3} + 6x_{5,5} + 3x_{6,6} & \equiv_9 & 0 \\ x_{1,6} + 3x_{5,4} + 3x_{5,5} + 6x_{6,6} & \equiv_9 & 0 \\ x_{2,5} + 6x_{3,1} + 6x_{4,1} + 3x_{4,2} + 3x_{5,3} + 6x_{5,4} + 3x_{5,5} + 6x_{6,3} + 6x_{6,4} + 3x_{6,5} + 6x_{6,6} & \equiv_9 & 0 \\ x_{2,6} + 6x_{4,2} + 3x_{5,5} + 6x_{6,4} + 6x_{6,6} & \equiv_9 & 0 \end{array} \right\} .$$

Therefore we shall present another $\mathbf{Z}$-linear basis of $\mathbf{Z}[\zeta_9]$ for which the appearing congruences are less intricate, cf. Proposition 30.

Remark 29. Write $\zeta_9 = \zeta$. Define $\pi := (\zeta - 1)(\zeta^{-1} - 1) = 2 - \zeta - \zeta^{-1}$. We have $\mu_{\pi,\mathbf{Q}}(x) = x^3 - 6x^2 + 9x - 3$. Regard the extensions

$$\begin{tikzcd}
 & \mathbf{Q}(\zeta) \arrow[d, equal] & \\
 & \mathbf{Q}(\pi, \zeta^3) \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\mathbf{Q}(\zeta) \cap \mathbf{R} = \mathbf{Q}(\pi) \arrow[dr, dash, "3"'] & & \mathbf{Q}(\zeta^3) \arrow[dl, dash, "2"] \\
 & \mathbf{Q} &
\end{tikzcd} .$$

We consider the $\mathbf{Q}$-linear bases $(1, \pi, \pi^2)$ of $\mathbf{Q}(\pi)$ and $(1, \zeta^3 - 1)$ of $\mathbf{Q}(\zeta^3)$. Since

$$[\mathbf{Q}(\pi, \zeta^3) : \mathbf{Q}] = 6 = 3 \cdot 2 = [\mathbf{Q}(\pi) : \mathbf{Q}] \cdot [\mathbf{Q}(\zeta^3) : \mathbf{Q}]$$

the extensions $\mathbf{Q}(\pi)|\mathbf{Q}$ and $\mathbf{Q}(\zeta^3)|\mathbf{Q}$ are linearly disjoint. Therefore we obtain the $\mathbf{Q}$-linear basis $\underline{q} = (1, \pi, \pi^2, \zeta^3 - 1, (\zeta^3 - 1)\pi, (\zeta^3 - 1)\pi^2)$ of $\mathbf{Q}(\pi, \zeta^3) = \mathbf{Q}(\zeta)$ which is as well a $\mathbf{Z}$-linear basis of $\mathbf{Z}[\pi, \zeta^3] \subseteq \mathbf{Z}[\zeta]$.

However, $\underline{q}$ is not a $\mathbf{Z}$-linear basis of $\mathbf{Z}[\zeta]$ since

$$\zeta = 4 - 5\pi + \pi^2 + 2(\zeta^3 - 1) - 3(\zeta^3 - 1)\pi + \tfrac{2}{3}(\zeta^3 - 1)\pi^2 \notin \mathbf{Z}[\pi, \zeta^3] \ .$$

Consider the adjusted $\mathbf{Q}$-linear basis $\underline{t} = (1, \pi, \pi^2, \zeta^3 - 1, (\zeta^3 - 1)\pi, \frac{1}{3}(\zeta^3 - 1)\pi^2)$ of $\mathbf{Q}[\zeta]$. Its base-change matrix to the $\mathbf{Z}$-linear basis $\underline{z} = (\zeta^0, \zeta^1, \zeta^2, \zeta^3, \zeta^4, \zeta^5)$ of $\mathbf{Z}[\zeta]$ is given by

$$\begin{pmatrix} 1 & 2 & 6 & -1 & -2 & -2 \\ 0 & -1 & -5 & 0 & 1 & 2 \\ 0 & 1 & 5 & 0 & -2 & -3 \\ 0 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & -1 & 0 & -1 & -1 \\ 0 & 1 & 4 & 0 & -1 & -1 \end{pmatrix},$$

where the columns are indexed by $\underline{t}$, the rows by $\underline{z}$. Since it has determinant 1, $\underline{t}$ is a $\mathbf{Z}$-linear basis of $\mathbf{Z}[\zeta]$.

Proposition 30. *Consider the Galois extension* $\mathbf{Q}(\zeta_9)|\mathbf{Q}$. *Write* $\zeta := \zeta_9$.

Its Galois group is given by $G = \{\mathrm{id}, \zeta \overset{\sigma}{\mapsto} \zeta^5, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$.

Consider the $\mathbf{Z}$*-linear basis* $\underline{t} = (1, \pi, \pi^2, \zeta^3 - 1, (\zeta^3 - 1)\pi, \frac{1}{3}(\zeta^3 - 1)\pi^2)$ *of* $\mathcal{O}_{\mathbf{Q}(\zeta)} = \mathbf{Z}[\zeta]$, *cf.* Remark 29.

Consider the map $\omega_{\underline{t}}^{\mathbf{Z}} : \mathbf{Z}[\zeta] \wr G \to \mathbf{Z}^{6\times 6}$.

Then the image of $\omega_{\underline{t}}^{\mathbf{Z}}$ *is given by*

$$\Lambda := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (3) & (3) & (3) & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & (3) & (3) & (3) & \mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) & \mathbf{Z} \\ & & & & & \\ \mathbf{Z} & \mathbf{Z} & (3) & \mathbf{Z} & (3) & \mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \\ \mathbf{Z} & (3) & (3) & (3) & (3) & \mathbf{Z} \end{pmatrix} : \begin{array}{r} x_{1,1} \equiv_3 x_{2,2} \equiv_3 x_{3,3} \\ x_{1,3} + 3x_{2,1} + 3x_{3,2} \equiv_9 0 \\ \\ x_{1,4} + x_{2,5} + 3x_{3,6} \equiv_9 0 \\ x_{1,5} \equiv_9 3x_{2,6} \equiv_9 3x_{3,4} \\ \\ x_{4,2} \equiv_3 x_{5,3} \equiv_3 x_{6,1} \\ x_{6,3} + 3x_{4,1} + 3x_{5,2} \equiv_9 0 \\ \\ x_{4,4} \equiv_3 x_{5,5} \equiv_3 x_{6,6} \\ x_{6,5} + 3x_{4,6} + 3x_{5,4} \equiv_9 0 \end{array} \right\}.$$

In particular, we have an isomorphism of rings $\mathbf{Z}[\zeta_9] \wr G \xrightarrow{\sim} \Lambda$.

Consider the $\mathbf{Q}$*-linear basis* $\underline{q} = (1, \pi, \pi^2, \zeta^3 - 1, (\zeta^3 - 1)\pi, (\zeta^3 - 1)\pi^2)$ *of* $\mathbf{Q}[\zeta]$*, cf.* Remark 29*.*

Consider the map $\omega_{\underline{q}}|_{\mathbf{Z}[\zeta]\wr G} : \mathbf{Z}[\zeta] \wr G \to \mathbf{Q}^{6\times 6}$ *.*

Then the image of $\omega_{\underline{q}}|_{\mathbf{Z}[\zeta]\wr G}$ *is given by*

$$\Lambda' := \left\{ (y_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (3) & (3) & (3) & (3) & (9) \\ \mathbf{Z} & \mathbf{Z} & (3) & (3) & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) & (3) \\ & & & & & \\ \mathbf{Z} & \mathbf{Z} & (3) & \mathbf{Z} & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) \\ (1/3) & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \end{pmatrix} : \begin{array}{r} y_{1,1} \equiv_3 y_{2,2} \equiv_3 y_{3,3} \\ y_{1,3} + 3y_{2,1} + 3y_{3,2} \equiv_9 0 \\ \\ y_{1,4} + y_{2,5} + y_{3,6} \equiv_9 0 \\ y_{1,5} \equiv_9 y_{2,6} \equiv_9 3y_{3,4} \\ \\ y_{4,2} \equiv_3 y_{5,3} \equiv_3 3y_{6,1} \\ y_{4,1} + y_{5,2} + y_{6,3} \equiv_3 0 \\ \\ y_{4,4} \equiv_3 y_{5,5} \equiv_3 y_{6,6} \\ y_{4,6} + 3y_{5,4} + 3y_{6,5} \equiv_9 0 \end{array} \right\}.$$

In particular, we have an isomorphism of rings $\mathbf{Z}[\zeta_9] \wr G \xrightarrow{\sim} \Lambda'$.

Proof. Consider the $\mathbf{Z}$-linear basis $\underline{z} = (\zeta^j \sigma^k : j, k \in [0, 5])$ of $\mathbf{Z}[\zeta] \wr G$.

Then $\omega_{\underline{t}}^{\mathbf{Z}} : \mathbf{Z}[\zeta] \wr G \to \mathbf{Z}^{6\times 6}$ maps for $j, k \in [0, 5]$

$$\zeta^j \sigma^k \quad \mapsto \quad \begin{pmatrix} 4 & 3 & 3 & -6 & -6 & -3 \\ -5 & -5 & -6 & 9 & 12 & 7 \\ 1 & 1 & 1 & -2 & -3 & -2 \\ 2 & 2 & 3 & -2 & -3 & -2 \\ -3 & -4 & -7 & 4 & 7 & 5 \\ 2 & 3 & 6 & -3 & -6 & -5 \end{pmatrix}^{j} \begin{pmatrix} 1 & 6 & 24 & -3 & -18 & -24 \\ 0 & -5 & -21 & 0 & 15 & 21 \\ 0 & 1 & 4 & 0 & -3 & -4 \\ 0 & 0 & 0 & -1 & -6 & -8 \\ 0 & 0 & 0 & 0 & 5 & 7 \\ 0 & 0 & 0 & 0 & -3 & -4 \end{pmatrix}^{k}.$$

Let A be the representation matrix of $\omega_{\underline{t}}^{\mathbf{Z}}$, with respect to the bases $\underline{z}$ of $\mathbf{Z}[\zeta] \wr G$ and $(\mathrm{e}_{i,j})_{i,j\in[1,6]}$ of $\mathbf{Z}^{6\times 6}$. A direct calculation leads to

$$A =$$

$$\begin{pmatrix}
1 & 4 & 4 & 1 & -2 & -2 & 1 & 4 & 4 & 1 & -2 & -2 & 1 & 4 & 4 & 1 & -2 & -2 & 1 & 4 & 4 & 1 & -2 & -2 & 1 & 4 & 4 & 1 & -2 & -2 & 1 & 4 & 4 & 1 & -2 & -2 \\
0 & 3 & 3 & 0 & -3 & 0 & 6 & 12 & 12 & 6 & -3 & -9 & 0 & 9 & 9 & 0 & -6 & -3 & 0 & 3 & 3 & 0 & -3 & 0 & 6 & 12 & 12 & 6 & -3 & -9 & 0 & 9 & 9 & 0 & -6 & -3 \\
0 & 3 & 3 & 0 & -6 & 3 & 24 & 45 & 45 & 24 & -9 & -36 & -6 & 24 & 24 & -6 & -21 & -3 & 0 & 3 & 3 & 0 & -6 & 3 & 24 & 45 & 45 & 24 & -9 & -36 & -6 & 24 & 24 & -6 & -21 & -3 \\
0 & -6 & -6 & -3 & 0 & 0 & -3 & -6 & -6 & 0 & 6 & 6 & 0 & -6 & -6 & -3 & 0 & 0 & -3 & -6 & -6 & 0 & 6 & 6 & 0 & -6 & -6 & -3 & 0 & 0 & -3 & -6 & -6 & 0 & 6 & 6 \\
0 & -6 & -3 & 0 & 3 & -3 & -18 & -21 & -15 & 0 & 15 & 21 & 0 & -15 & -12 & 0 & 3 & -3 & 0 & -3 & -6 & 0 & 6 & 3 & 0 & -15 & -21 & -18 & -6 & 6 & 0 & -12 & -15 & 0 & 15 & 12 \\
0 & -3 & 0 & 0 & 3 & -3 & -24 & -27 & -18 & 0 & 18 & 27 & 0 & -15 & -9 & 6 & 6 & -6 & 0 & 0 & -3 & 0 & 3 & 0 & 0 & -18 & -27 & -24 & -9 & 9 & 6 & -9 & -15 & 0 & 15 & 9 \\
0 & -5 & -5 & 0 & 4 & 1 & 0 & -5 & -5 & 0 & 4 & 1 & 0 & -5 & -5 & 0 & 4 & 1 & 0 & -5 & -5 & 0 & 4 & 1 & 0 & -5 & -5 & 0 & 4 & 1 & 0 & -5 & -5 & 0 & 4 & 1 \\
1 & -5 & -5 & 1 & 7 & -2 & -5 & -11 & -11 & -5 & 4 & 7 & 4 & -14 & -14 & 4 & 13 & 1 & 1 & -5 & -5 & 1 & 7 & -2 & -5 & -11 & -11 & -5 & 4 & 7 & 4 & -14 & -14 & 4 & 13 & 1 \\
0 & -6 & -6 & 0 & 15 & -9 & -21 & -39 & -39 & -21 & 9 & 30 & 21 & -45 & -45 & 21 & 48 & -3 & 0 & -6 & -6 & 0 & 15 & -9 & -21 & -39 & -39 & -21 & 9 & 30 & 21 & -45 & -45 & 21 & 48 & -3 \\
0 & 9 & 6 & 0 & -3 & 3 & 0 & 6 & 9 & 0 & -9 & -6 & 0 & 9 & 6 & 0 & -3 & 3 & 0 & 6 & 9 & 0 & -9 & -6 & 0 & 9 & 6 & 0 & -3 & 3 & 0 & 6 & 9 & 0 & -9 & -6 \\
0 & 12 & 3 & -3 & -9 & 9 & 15 & 18 & 15 & 0 & -15 & -18 & 0 & 27 & 15 & -12 & -12 & 12 & -3 & 3 & 12 & 0 & -12 & -3 & 0 & 15 & 18 & 15 & 3 & -3 & -12 & 15 & 27 & 0 & -27 & -15 \\
0 & 7 & -1 & 0 & -8 & 8 & 21 & 23 & 16 & 0 & -16 & -23 & 0 & 31 & 14 & -21 & -17 & 17 & 0 & -1 & 7 & 0 & -7 & 1 & 0 & 16 & 23 & 21 & 7 & -7 & -21 & 14 & 31 & 0 & -31 & -14 \\
0 & 1 & 1 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & -1 & 0 & 0 & 1 & 1 & 0 & -1 & 0 \\
0 & 1 & 1 & 0 & -2 & 1 & 1 & 2 & 2 & 1 & -1 & -1 & -1 & 3 & 3 & -1 & -3 & 0 & 0 & 1 & 1 & 0 & -2 & 1 & 1 & 2 & 2 & 1 & -1 & -1 & -1 & 3 & 3 & -1 & -3 & 0 \\
1 & 1 & 1 & 1 & -5 & 4 & 4 & 7 & 7 & 4 & -2 & -5 & -5 & 10 & 10 & -5 & -11 & 1 & 1 & 1 & 1 & 1 & -5 & 4 & 4 & 7 & 7 & 4 & -2 & -5 & -5 & 10 & 10 & -5 & -11 & 1 \\
0 & -2 & -1 & 0 & 1 & -1 & 0 & -1 & -2 & 0 & 2 & 1 & 0 & -2 & -1 & 0 & 1 & -1 & 0 & -1 & -2 & 0 & 2 & 1 & 0 & -2 & -1 & 0 & 1 & -1 & 0 & -1 & -2 & 0 & 2 & 1 \\
0 & -3 & 0 & 0 & 3 & -3 & -3 & -3 & -3 & 0 & 3 & 3 & 0 & -6 & -3 & 3 & 3 & -3 & 0 & 0 & -3 & 0 & 3 & 0 & 0 & -3 & -3 & -3 & 0 & 0 & 3 & -3 & -6 & 0 & 6 & 3 \\
0 & -2 & 1 & -1 & 3 & -3 & -4 & -4 & -3 & 0 & 3 & 4 & 0 & -7 & -3 & 5 & 4 & -4 & -1 & 1 & -2 & 0 & 2 & -1 & 0 & -3 & -4 & -4 & -1 & 1 & 5 & -3 & -7 & 0 & 7 & 3 \\
0 & 2 & 2 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 & 0 & 2 & 2 & 1 & 0 & 0 \\
0 & 2 & 1 & 0 & -1 & 1 & 0 & 5 & 7 & 6 & 2 & -2 & 0 & 5 & 4 & 0 & -1 & 1 & 0 & 2 & 1 & 0 & -1 & 1 & 0 & 5 & 7 & 6 & 2 & -2 & 0 & 5 & 4 & 0 & -1 & 1 \\
0 & 3 & 0 & 0 & -3 & 3 & 0 & 18 & 27 & 24 & 9 & -9 & 0 & 15 & 9 & -6 & -6 & 6 & 0 & 3 & 0 & 0 & -3 & 3 & 0 & 18 & 27 & 24 & 9 & -9 & 0 & 15 & 9 & -6 & -6 & 6 \\
1 & -2 & -2 & -2 & -2 & -2 & -1 & -4 & -4 & -1 & 2 & 2 & 1 & -2 & -2 & -2 & -2 & -2 & -1 & -4 & -4 & -1 & 2 & 2 & 1 & -2 & -2 & -2 & -2 & -2 & -1 & -4 & -4 & -1 & 2 & 2 \\
0 & -3 & 0 & 0 & 0 & -3 & -6 & -12 & -12 & -6 & 3 & 9 & 0 & -6 & -3 & 0 & -3 & -6 & 0 & -3 & -3 & 0 & 3 & 0 & 6 & -3 & -9 & -12 & -9 & -3 & 0 & -9 & -9 & 0 & 6 & 3 \\
0 & -2 & 1 & 0 & 1 & -2 & -8 & -15 & -15 & -8 & 3 & 12 & -2 & -7 & -1 & 4 & -1 & -7 & 0 & -1 & -1 & 0 & 2 & -1 & 8 & -3 & -12 & -16 & -12 & -3 & 2 & -8 & -8 & 2 & 7 & 1 \\
0 & -3 & -2 & 0 & 1 & -1 & 0 & -3 & -2 & 0 & 1 & -1 & 0 & -3 & -2 & 0 & 1 & -1 & 0 & -3 & -2 & 0 & 1 & -1 & 0 & -3 & -2 & 0 & 1 & -1 & 0 & -3 & -2 & 0 & 1 & -1 \\
0 & -4 & -1 & 1 & 3 & -3 & 0 & -5 & -6 & -5 & -1 & 1 & 0 & -9 & -5 & 4 & 4 & -4 & 0 & -4 & -1 & 1 & 3 & -3 & 0 & -5 & -6 & -5 & -1 & 1 & 0 & -9 & -5 & 4 & 4 & -4 \\
0 & -7 & 1 & 0 & 8 & -8 & 0 & -16 & -23 & -21 & -7 & 7 & 0 & -31 & -14 & 21 & 17 & -17 & 0 & -7 & 1 & 0 & 8 & -8 & 0 & -16 & -23 & -21 & -7 & 7 & 0 & -31 & -14 & 21 & 17 & -17 \\
0 & 4 & 1 & 0 & 1 & 4 & 0 & 5 & 5 & 0 & -4 & -1 & 0 & 4 & 1 & 0 & 1 & 4 & 0 & 5 & 5 & 0 & -4 & -1 & 0 & 4 & 1 & 0 & 1 & 4 & 0 & 5 & 5 & 0 & -4 & -1 \\
1 & 7 & -2 & -2 & -2 & 7 & 5 & 11 & 11 & 5 & -4 & -7 & 4 & 13 & 1 & -8 & 1 & 13 & -1 & 5 & 5 & -1 & -7 & 2 & -5 & 4 & 7 & 10 & 7 & 4 & -4 & 14 & 14 & -4 & -13 & -1 \\
0 & 5 & -3 & 0 & -3 & 5 & 7 & 13 & 13 & 7 & -3 & -10 & 7 & 16 & -1 & -14 & -1 & 16 & 0 & 2 & 2 & 0 & -5 & 3 & -7 & 3 & 10 & 14 & 10 & 3 & -7 & 15 & 15 & -7 & -16 & 1 \\
0 & 2 & 1 & 0 & -1 & 1 & 0 & 2 & 1 & 0 & -1 & 1 & 0 & 2 & 1 & 0 & -1 & 1 & 0 & 2 & 1 & 0 & -1 & 1 & 0 & 2 & 1 & 0 & -1 & 1 & 0 & 2 & 1 & 0 & -1 & 1 \\
0 & 3 & 0 & 0 & -3 & 3 & 0 & 3 & 3 & 3 & 0 & 0 & 0 & 6 & 3 & -3 & -3 & 3 & 0 & 3 & 0 & 0 & -3 & 3 & 0 & 3 & 3 & 3 & 0 & 0 & 0 & 6 & 3 & -3 & -3 & 3 \\
0 & 6 & -3 & 3 & -9 & 9 & 0 & 9 & 12 & 12 & 3 & -3 & 0 & 21 & 9 & -15 & -12 & 12 & 0 & 6 & -3 & 3 & -9 & 9 & 0 & 9 & 12 & 12 & 3 & -3 & 0 & 21 & 9 & -15 & -12 & 12 \\
0 & -3 & 0 & 0 & 0 & -3 & 0 & -3 & -3 & 0 & 3 & 0 & 0 & -3 & 0 & 0 & 0 & -3 & 0 & -3 & -3 & 0 & 3 & 0 & 0 & -3 & 0 & 0 & 0 & -3 & 0 & -3 & -3 & 0 & 3 & 0 \\
0 & -6 & 3 & 0 & 3 & -6 & -3 & -6 & -6 & -3 & 3 & 3 & -3 & -9 & 0 & 6 & 0 & -9 & 0 & -3 & -3 & 0 & 6 & -3 & 3 & -3 & -3 & -6 & -3 & -3 & 3 & -9 & -9 & 3 & 9 & 0 \\
1 & -5 & 4 & -2 & 4 & -5 & -4 & -7 & -7 & -4 & 2 & 5 & -5 & -11 & 1 & 10 & 1 & -11 & -1 & -1 & -1 & -1 & 5 & -4 & 4 & -2 & -5 & -8 & -5 & -2 & 5 & -10 & -10 & 5 & 11 & -1
\end{pmatrix}$$

and $9A^{-1} =$

$$\begin{pmatrix}
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -3 & 3 & 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 & 0 & 1 & 0 & 0 & 3 \\
-6 & 9 & -2 & -4 & 5 & -3 & -6 & 12 & -3 & -3 & 5 & -3 & -9 & 21 & -6 & -3 & 6 & -3 & 12 & -15 & 3 & 6 & -6 & 3 & 9 & -15 & 3 & 3 & -3 & 0 & 3 & -6 & 1 & 0 & 1 & -3 \\
-6 & 6 & -1 & -4 & 5 & -3 & -3 & 3 & 0 & -3 & 5 & -3 & 0 & -3 & 3 & -3 & 6 & -3 & 12 & -15 & 3 & 6 & -9 & 6 & 9 & -15 & 3 & 6 & -12 & 9 & 3 & -6 & 1 & 3 & -7 & 6 \\
-3 & 0 & 0 & -2 & 0 & 0 & 0 & -3 & 0 & 0 & -2 & 0 & 0 & 0 & -3 & 0 & 0 & -6 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 2 & 0 & 0 & 3 \\
-6 & 6 & -1 & -2 & 1 & 0 & -3 & 3 & 0 & 0 & -2 & 3 & 0 & -3 & 3 & 3 & -9 & 12 & 6 & -3 & 0 & 0 & 3 & -3 & 0 & 6 & -3 & -3 & 9 & -9 & -3 & 9 & -4 & -3 & 8 & -9 \\
-6 & 9 & -2 & -2 & 4 & -3 & -6 & 12 & -3 & -3 & 7 & -6 & -9 & 21 & -6 & -6 & 15 & -15 & 6 & -12 & 3 & 0 & -3 & 3 & 9 & -21 & 6 & 3 & -9 & 9 & 6 & -15 & 5 & 3 & -8 & 9 \\
3 & 0 & 0 & 1 & 0 & 0 & 0 & 12 & -3 & 0 & 4 & -3 & -18 & 63 & -15 & -6 & 21 & -15 & -6 & 0 & 0 & -3 & 0 & 0 & 0 & -24 & 6 & 0 & -12 & 9 & 12 & -42 & 10 & 6 & -21 & 15 \\
0 & -3 & 1 & -2 & 1 & 0 & 3 & -12 & 3 & -3 & 1 & 0 & 18 & -51 & 12 & -3 & -3 & 3 & -6 & 12 & -3 & 0 & 3 & -3 & -18 & 39 & -9 & -3 & 12 & -9 & -21 & 48 & -11 & -6 & 17 & -12 \\
-6 & 6 & -1 & -2 & 1 & 0 & -12 & 15 & -3 & -3 & 1 & 0 & -27 & 42 & -9 & -3 & -3 & 3 & 12 & -15 & 3 & 6 & -6 & 3 & 27 & -42 & 9 & 12 & -15 & 9 & 24 & -45 & 10 & 9 & -14 & 9 \\
3 & 0 & 0 & 2 & 0 & 0 & 0 & 12 & -3 & 0 & 8 & -6 & -18 & 63 & -15 & -12 & 42 & -30 & -3 & 0 & 0 & -3 & 0 & 0 & 0 & -12 & 3 & 0 & -12 & 9 & 6 & -21 & 5 & 6 & -21 & 15 \\
6 & -9 & 2 & 2 & -4 & 3 & 15 & -27 & 6 & 6 & -13 & 9 & 45 & -93 & 21 & 21 & -48 & 33 & -12 & 15 & -3 & -6 & 9 & -6 & -27 & 42 & -9 & -15 & 27 & -18 & -24 & 45 & -10 & -15 & 31 & -21 \\
-6 & 9 & -2 & -4 & 5 & -3 & -15 & 27 & -6 & -9 & 14 & -9 & -45 & 93 & -21 & -24 & 45 & -30 & 6 & -12 & 3 & 6 & -9 & 6 & 18 & -39 & 9 & 15 & -27 & 18 & 21 & -48 & 11 & 15 & -31 & 21 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -6 & 5 & -3 & 0 & 0 & 0 & -24 & 21 & -12 & 3 & 0 & 0 & 3 & 0 & 0 & 18 & -15 & 3 & 18 & -15 & 9 & 24 & -21 & 4 & 24 & -21 & 12 \\
0 & -3 & 1 & 2 & -4 & 3 & -6 & 3 & 0 & 3 & -4 & 3 & -27 & 21 & -3 & 9 & -9 & 6 & -6 & 12 & -3 & -6 & 9 & -6 & -9 & 12 & -3 & -15 & 15 & -9 & -9 & 9 & -2 & -18 & 16 & -9 \\
6 & -9 & 2 & 2 & -4 & 3 & 15 & -15 & 3 & 3 & -4 & 3 & 54 & -48 & 9 & 9 & -9 & 6 & -6 & 12 & -3 & 0 & 3 & -3 & -9 & 12 & -3 & 6 & -3 & 0 & -9 & 9 & -2 & 9 & -7 & 3 \\
-3 & 0 & 0 & -2 & 0 & 0 & -18 & 15 & -3 & -12 & 10 & -6 & -72 & 63 & -12 & -48 & 42 & -24 & 6 & 0 & 0 & 3 & 0 & 0 & 36 & -30 & 6 & 18 & -15 & 9 & 48 & -42 & 8 & 24 & -21 & 12 \\
6 & -9 & 2 & 4 & -5 & 3 & 15 & -15 & 3 & 12 & -11 & 6 & 54 & -48 & 9 & 45 & -39 & 21 & -12 & 15 & -3 & -6 & 6 & -3 & -36 & 33 & -6 & -21 & 18 & -9 & -45 & 39 & -7 & -27 & 23 & -12 \\
0 & -3 & 1 & -2 & 1 & 0 & -6 & 3 & 0 & -9 & 7 & -3 & -27 & 21 & -3 & -36 & 30 & -15 & 6 & -3 & 0 & 6 & -6 & 3 & 27 & -21 & 3 & 21 & -18 & 9 & 36 & -30 & 5 & 27 & -23 & 12 \\
3 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 3 & -6 & 0 & 0 & -3 & 0 & 0 & 0 & -6 & 0 & 0 & -3 & 0 & 0 & 0 & -2 & 0 & 0 & -3 \\
6 & -6 & 1 & 4 & -5 & 3 & 3 & -3 & 0 & 3 & -5 & 3 & 0 & 3 & -3 & 3 & -6 & 3 & -6 & 3 & 0 & -6 & 6 & -3 & 0 & -6 & 3 & -3 & 3 & 0 & 3 & -9 & 4 & 0 & -1 & 3 \\
6 & -9 & 2 & 4 & -5 & 3 & 6 & -12 & 3 & 3 & -5 & 3 & 9 & -21 & 6 & 3 & -6 & 3 & -6 & 12 & -3 & -6 & 9 & -6 & -9 & 21 & -6 & -6 & 12 & -9 & -6 & 15 & -5 & -3 & 7 & -6 \\
3 & 0 & 0 & 2 & 0 & 0 & 0 & 3 & 0 & 0 & 2 & 0 & 0 & 0 & 3 & 0 & 0 & 6 & -3 & 0 & 0 & -3 & 0 & 0 & 0 & -3 & 0 & 0 & -3 & 0 & 0 & 0 & -1 & 0 & 0 & -3 \\
0 & 3 & -1 & 2 & -1 & 0 & -3 & 9 & -3 & 0 & 2 & -3 & -9 & 24 & -9 & -3 & 9 & -12 & 6 & -12 & 3 & 0 & -3 & 3 & 9 & -21 & 6 & 3 & -9 & 9 & 6 & -15 & 5 & 3 & -8 & 9 \\
0 & -3 & 1 & 2 & -4 & 3 & 3 & -9 & 3 & 3 & -7 & 6 & 9 & -24 & 9 & 6 & -15 & 15 & 6 & -3 & 0 & 0 & 3 & -3 & 0 & 6 & -3 & -3 & 9 & -9 & -3 & 9 & -4 & -3 & 8 & -9 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & 3 & 0 & 0 & 0 & 6 & -21 & 15 & 3 & 0 & 0 & 3 & 0 & 0 & 0 & 12 & -3 & 0 & 12 & -9 & -6 & 21 & -5 & -6 & 21 & -15 \\
6 & -6 & 1 & 2 & -1 & 0 & 12 & -15 & 3 & 3 & -1 & 0 & 27 & -42 & 9 & 3 & 3 & -3 & -6 & 3 & 0 & 0 & -3 & 3 & -9 & 3 & 0 & 3 & -12 & 9 & -3 & -3 & 1 & 6 & -17 & 12 \\
0 & 3 & -1 & 2 & -1 & 0 & -3 & 12 & -3 & 3 & -1 & 0 & -18 & 51 & -12 & 3 & 3 & -3 & -6 & 3 & 0 & -6 & 6 & -3 & -9 & 3 & 0 & -12 & 15 & -9 & -3 & -3 & 1 & -9 & 14 & -9 \\
-3 & 0 & 0 & -2 & 0 & 0 & 0 & -12 & 3 & 0 & -8 & 6 & 18 & -63 & 15 & 12 & -42 & 30 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 24 & -6 & 0 & 12 & -9 & -12 & 42 & -10 & -6 & 21 & -15 \\
0 & 3 & -1 & -2 & 4 & -3 & -3 & 12 & -3 & -6 & 13 & -9 & -18 & 51 & -12 & -21 & 48 & -33 & 6 & -12 & 3 & 6 & -9 & 6 & 18 & -39 & 9 & 15 & -27 & 18 & 21 & -48 & 11 & 15 & -31 & 21 \\
6 & -6 & 1 & 4 & -5 & 3 & 12 & -15 & 3 & 9 & -14 & 9 & 27 & -42 & 9 & 24 & -45 & 30 & -12 & 15 & -3 & -6 & 9 & -6 & -27 & 42 & -9 & -15 & 27 & -18 & -24 & 45 & -10 & -15 & 31 & -21 \\
3 & 0 & 0 & 1 & 0 & 0 & 18 & -15 & 3 & 6 & -5 & 3 & 72 & -63 & 12 & 24 & -21 & 12 & -6 & 0 & 0 & -3 & 0 & 0 & -36 & 30 & -6 & -18 & 15 & -9 & -48 & 42 & -8 & -24 & 21 & -12 \\
-6 & 9 & -2 & -2 & 4 & -3 & -15 & 15 & -3 & -3 & 4 & -3 & -54 & 48 & -9 & -9 & 9 & -6 & 12 & -15 & 3 & 6 & -9 & 6 & 36 & -33 & 6 & 15 & -15 & 9 & 45 & -39 & 7 & 18 & -16 & 9 \\
0 & 3 & -1 & -2 & 4 & -3 & 6 & -3 & 0 & -3 & 4 & -3 & 27 & -21 & 3 & -9 & 9 & -6 & -6 & 3 & 0 & 0 & -3 & 3 & -27 & 21 & -3 & -6 & 3 & 0 & -36 & 30 & -5 & -9 & 7 & -3 \\
3 & 0 & 0 & 2 & 0 & 0 & 18 & -15 & 3 & 12 & -10 & 6 & 72 & -63 & 12 & 48 & -42 & 24 & -3 & 0 & 0 & -3 & 0 & 0 & -18 & 15 & -3 & -18 & 15 & -9 & -24 & 21 & -4 & -24 & 21 & -12 \\
-6 & 6 & -1 & -4 & 5 & -3 & -21 & 18 & -3 & -12 & 11 & -6 & -81 & 69 & -12 & -45 & 39 & -21 & 6 & -3 & 0 & 6 & -6 & 3 & 27 & -21 & 3 & 21 & -18 & 9 & 36 & -30 & 5 & 27 & -23 & 12 \\
6 & -6 & 1 & 2 & -1 & 0 & 21 & -18 & 3 & 9 & -7 & 3 & 81 & -69 & 12 & 36 & -30 & 15 & -12 & 15 & -3 & -6 & 6 & -3 & -36 & 33 & -6 & -21 & 18 & -9 & -45 & 39 & -7 & -27 & 23 & -12
\end{pmatrix}.$$

Let $X = (x_{i,j})_{i,j\in[1,6]} \in \mathbf{Z}^{6\times 6}$. We have

$$X \in \Lambda \quad\Leftrightarrow\quad \omega_{\underline{t}}^{-1}(X) \in \mathbf{Z}[\zeta] \wr G \Leftrightarrow A^{-1} \cdot \begin{pmatrix} x_{1,1} \\ x_{1,2} \\ \vdots \\ x_{6,6} \end{pmatrix} \in \mathbf{Z}^{36\times 1}$$

$$\Leftrightarrow \quad \left(\begin{array}{cccccccccccccccccccccccccccccccccccc}
3&0&0&0&0&0&0&0&0&0&0&0&0&0&6&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&3&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&6&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&3&0&0&0&0&0&0&6&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&6&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&3&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&6&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0&6\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&3&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&6&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&0&0&0&6\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3&0
\end{array}\right)
\begin{pmatrix} x_{1,1} \\ \vdots \\ x_{1,6} \\ x_{2,1} \\ \vdots \\ x_{2,6} \\ \vdots \\ x_{3,1} \\ \vdots \\ x_{3,6} \\ x_{4,1} \\ \vdots \\ x_{4,6} \\ x_{5,1} \\ \vdots \\ x_{5,6} \\ x_{6,1} \\ \vdots \\ x_{6,6} \end{pmatrix} \in 9\mathbf{Z}^{24\times 1}$$

$$\Leftrightarrow \left\{\begin{array}{rcl}
3x_{1,1}+6x_{3,3} & \equiv_9 & 0 \\
3x_{1,2} & \equiv_9 & 0 \\
x_{1,3}+3x_{2,1}+3x_{3,2} & \equiv_9 & 0 \\
x_{1,4}+x_{2,5}+3x_{3,6} & \equiv_9 & 0 \\
x_{1,5}+6x_{3,4} & \equiv_9 & 0 \\
3x_{1,6} & \equiv_9 & 0 \\
3x_{2,2}+6x_{3,3} & \equiv_9 & 0 \\
3x_{2,3} & \equiv_9 & 0 \\
3x_{2,4} & \equiv_9 & 0 \\
3x_{2,5} & \equiv_9 & 0 \\
3x_{2,6}+6x_{3,4} & \equiv_9 & 0 \\
3x_{3,5} & \equiv_9 & 0 \\
3x_{4,1}+3x_{5,2}+x_{6,3} & \equiv_9 & 0 \\
3x_{4,2}+6x_{6,1} & \equiv_9 & 0 \\
3x_{4,3} & \equiv_9 & 0 \\
3x_{4,4}+6x_{6,6} & \equiv_9 & 0 \\
3x_{4,5} & \equiv_9 & 0 \\
3x_{4,6}+3x_{5,4}+x_{6,5} & \equiv_9 & 0 \\
3x_{5,3}+6x_{6,1} & \equiv_9 & 0 \\
3x_{5,5}+6x_{6,6} & \equiv_9 & 0 \\
3x_{6,2} & \equiv_9 & 0 \\
3x_{6,3} & \equiv_9 & 0 \\
3x_{6,4} & \equiv_9 & 0 \\
3x_{6,5} & \equiv_9 & 0
\end{array}\right.
\Leftrightarrow \left\{\begin{array}{rcccl}
x_{1,1} & \equiv_3 & x_{2,2} & \equiv_3 & x_{3,3} \\
x_{1,2} & \equiv_3 & 0 & & \\
x_{1,3}+3x_{2,1}+3x_{3,2} & \equiv_9 & 0 & & \\
x_{2,3} & \equiv_3 & 0 & & \\
 & & & & \\
x_{1,4}+x_{2,5}+3x_{3,6} & \equiv_9 & 0 & & \\
x_{1,5} & \equiv_9 & 3x_{2,6} & \equiv_9 & 3x_{3,4} \\
x_{1,6} & \equiv_3 & 0 & & \\
x_{2,4} & \equiv_3 & 0 & & \\
x_{2,5} & \equiv_3 & 0 & & \\
x_{3,5} & \equiv_3 & 0 & & \\
 & & & & \\
3x_{4,1}+3x_{5,2}+x_{6,3} & \equiv_9 & 0 & & \\
x_{4,2} & \equiv_3 & x_{5,3} & \equiv_3 & x_{6,1} \\
x_{4,3} & \equiv_3 & 0 & & \\
x_{5,3} & \equiv_3 & x_{6,1} & & \\
x_{6,2} & \equiv_3 & 0 & & \\
 & & & & \\
x_{4,4} & \equiv_3 & x_{5,5} & \equiv_3 & x_{6,6} \\
x_{4,5} & \equiv_3 & 0 & & \\
3x_{4,6}+3x_{5,4}+x_{6,5} & \equiv_9 & 0 & & \\
x_{6,4} & \equiv_3 & 0 & &
\end{array}\right.$$

Hence the image of $\omega_{\underline{t}}^{\mathbf{Z}}$ is given by

$$\Lambda := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (3) & (3) & (3) & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & (3) & (3) & (3) & \mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) & \mathbf{Z} \\ & & & & & \\ \mathbf{Z} & \mathbf{Z} & (3) & \mathbf{Z} & (3) & \mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \\ \mathbf{Z} & (3) & (3) & (3) & (3) & \mathbf{Z} \end{pmatrix} : \begin{array}{rcl} x_{1,1} & \equiv_3 & x_{2,2} \equiv_3 x_{3,3} \\ x_{1,3} + 3x_{2,1} + 3x_{3,2} & \equiv_9 & 0 \\ & & \\ x_{1,4} + x_{2,5} + 3x_{3,6} & \equiv_9 & 0 \\ x_{1,5} & \equiv_9 & 3x_{2,6} \equiv_9 3x_{3,4} \\ & & \\ x_{4,2} & \equiv_3 & x_{5,3} \equiv_3 x_{6,1} \\ x_{6,3} + 3x_{4,1} + 3x_{5,2} & \equiv_9 & 0 \\ & & \\ x_{4,4} & \equiv_3 & x_{5,5} \equiv_3 x_{6,6} \\ x_{6,5} + 3x_{4,6} + 3x_{5,4} & \equiv_9 & 0 \end{array} \right\}.$$

This system of congruences is less intricate than the result that was obtained using the $\mathbf{Z}$-linear basis $\underline{y} = ((\zeta_9 - 1)^0, \ldots, (\zeta_9 - 1)^5)$ of $\mathbf{Z}[\zeta_9]$, cf. Remark 28.

In comparison, we consider the $\mathbf{Q}$-linear basis $\underline{q} = (1, \pi, \pi^2, \zeta^3 - 1, (\zeta^3 - 1)\pi, (\zeta^3 - 1)\pi^2)$ of $\mathbf{Q}[\zeta]$.

Since $\underline{q}$ is not a $\mathbf{Z}$-linear basis of $\mathbf{Z}[\zeta]$ the image $\tilde{\Lambda}'$ of $\omega_{\underline{q}}|_{\mathbf{Z}[\zeta] \wr G} : \mathbf{Z}[\zeta] \wr G$ now is not contained in $\mathbf{Z}^{6 \times 6}$, but is only a subring of $\mathbf{Q}^{6 \times 6}$.

The congruences appearing in the description of $\tilde{\Lambda}'$ will be calculated by using the congruences appearing in the description of Λ.

Let S be the base-change matrix of the $\mathbf{Q}$-linear bases $\underline{t}$ and $\underline{q}$ of $\mathbf{Q}(\zeta)$, i.e.

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix},$$

where the columns of S are indexed by $\underline{q}$, the rows by $\underline{t}$.

Let $(y_{i,j})_{i,j} \in \mathbf{Q}^{6 \times 6}$. We have

$$(y_{i,j})_{i,j} \in \tilde{\Lambda}' \Leftrightarrow S(y_{i,j})_{i,j}S^{-1} \in \Lambda \Leftrightarrow$$

$$\begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} & y_{1,4} & y_{1,5} & \frac{1}{3}y_{1,6} \\ y_{2,1} & y_{2,2} & y_{2,3} & y_{2,4} & y_{2,5} & \frac{1}{3}y_{2,6} \\ y_{3,1} & y_{3,2} & y_{3,3} & y_{3,4} & y_{3,5} & \frac{1}{3}y_{3,6} \\ & & & & & \\ y_{4,1} & y_{4,2} & y_{4,3} & y_{4,4} & y_{4,5} & \frac{1}{3}y_{4,6} \\ y_{5,1} & y_{5,2} & y_{5,3} & y_{5,4} & y_{5,5} & \frac{1}{3}y_{5,6} \\ 3y_{6,1} & 3y_{6,2} & 3y_{6,3} & 3y_{6,4} & 3y_{6,5} & y_{6,6} \end{pmatrix} \in \Lambda = \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (3) & (3) & (3) & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & (3) & (3) & (3) & \mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) & \mathbf{Z} \\ & & & & & \\ \mathbf{Z} & \mathbf{Z} & (3) & \mathbf{Z} & (3) & \mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \\ \mathbf{Z} & (3) & (3) & (3) & (3) & \mathbf{Z} \end{pmatrix} : \begin{array}{rcl} x_{1,1} & \equiv_3 & x_{2,2} \equiv_3 x_{3,3} \\ x_{1,3} + 3x_{2,1} + 3x_{3,2} & \equiv_9 & 0 \\ & & \\ x_{1,4} + x_{2,5} + 3x_{3,6} & \equiv_9 & 0 \\ x_{1,5} & \equiv_9 & 3x_{2,6} \equiv_9 3x_{3,4} \\ & & \\ x_{4,2} & \equiv_3 & x_{5,3} \equiv_3 x_{6,1} \\ x_{5,3} & \equiv_3 & x_{6,1} \\ x_{6,3} + 3x_{4,1} + 3x_{5,2} & \equiv_9 & 0 \\ & & \\ x_{4,4} & \equiv_3 & x_{5,5} \equiv_3 x_{6,6} \\ x_{6,5} + 3x_{4,6} + 3x_{5,4} & \equiv_9 & 0 \end{array} \right\}.$$

So we obtain

$$\tilde{\Lambda}' = \left\{ (y_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (3) & (3) & (3) & (3) & (9) \\ \mathbf{Z} & \mathbf{Z} & (3) & (3) & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & (3) & \mathbf{Z} & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) \\ (1/3) & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \end{pmatrix} : \begin{array}{rcl} y_{1,1} & \equiv_3 & y_{2,2} \equiv_3 y_{3,3} \\ y_{1,3} + 3y_{2,1} + 3y_{3,2} & \equiv_9 & 0 \\ & & \\ y_{1,4} + y_{2,5} + y_{3,6} & \equiv_9 & 0 \\ y_{1,5} & \equiv_9 & y_{2,6} \equiv_9 3y_{3,4} \\ & & \\ y_{4,2} & \equiv_3 & y_{5,3} \equiv_3 3y_{6,1} \\ y_{4,1} + y_{5,2} + y_{6,3} & \equiv_3 & 0 \\ & & \\ y_{4,4} & \equiv_3 & y_{5,5} \equiv_3 y_{6,6} \\ y_{4,6} + 3y_{5,4} + 3y_{6,5} & \equiv_9 & 0 \end{array} \right\} = \Lambda'.$$

Attention: Since $y_{6,1} \in (1/3)$, the congruence $y_{5,3} \equiv_3 3y_{6,1}$ does not imply $y_{5,3} \equiv_3 0$. □

Remark 31. The index of Λ in $\mathbf{Z}^{6\times 6}$ is directly calculated to be

$$[\mathbf{Z}^{6\times 6} : \Lambda] = |\det(A)| = 3^{27} = (3^9)^3 = |\Delta_{\mathbf{Q}(\zeta_9)|\mathbf{Q},\underline{t}}|^{6/2} ,$$

confirming the statement of Theorem 16 in this case, cf. Proposition 30, [6, I. Lemma (10.1)].

Proposition 30 shows that it is not always convenient to employ a $\mathbf{Z}$-linear basis of $\mathcal{O}_{\mathbf{Q}(\zeta_m)}$. In fact, Λ' is only a subring of $\mathbf{Q}^{6\times 6}$ but its structure is rather symmetric.

Corollary 32.

Let $\Xi := \left\{ (y_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (3) & (3) \\ \mathbf{Z} & \mathbf{Z} & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \end{pmatrix} : \begin{array}{rcl} y_{1,1} \equiv_3 y_{2,2} & \equiv_3 & y_{3,3} \\ y_{1,3} + 3y_{2,1} + 3y_{3,2} & \equiv_9 & 0 \end{array} \right\} \subseteq \mathbf{Z}^{3\times 3}$.

Let $\xi := \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. *Then the ring* Λ' *from* Proposition 30 *can be written as*

$$\Lambda' = \begin{pmatrix} \Xi & \xi^2 \Xi \\ \xi^{-1}\Xi & \Xi \end{pmatrix} \subseteq \mathbf{Q}^{6\times 6} .$$

Note that Ξ *is a subring of* $\mathbf{Z}^{3\times 3}$ *and that* $\xi\Xi = \Xi\xi$.

Proof. We need to show that

$$\xi^2\Xi \overset{!}{=} \tilde{\Xi} := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} (3) & (3) & (9) \\ (3) & (3) & (3) \\ \mathbf{Z} & (3) & (3) \end{pmatrix} : \begin{array}{rcl} x_{1,1}+x_{2,2}+x_{3,3} & \equiv_9 & 0 \\ x_{1,2} \equiv_9 x_{2,3} & \equiv_9 & 3x_{3,1} \end{array} \right\},$$

cf. Proposition 30.

Ad ($\subseteq$). Let $\begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} \in \Xi$. We have $\xi^2 = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 3 \\ 1 & 0 & 0 \end{pmatrix}$.
Therefore we obtain

$$\begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 3 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} = \begin{pmatrix} 3y_{2,1} & 3y_{2,2} & 3y_{2,3} \\ 3y_{3,1} & 3y_{3,2} & 3y_{3,3} \\ y_{1,1} & y_{1,2} & y_{1,3} \end{pmatrix},$$

which is an element of $\tilde{\Xi}$ as

$$\begin{array}{lll} y_{2,1} \in \mathbf{Z}, & y_{2,2} \in \mathbf{Z}, & y_{2,3} \in (3) \\ y_{3,1} \in \mathbf{Z}, & y_{3,2} \in \mathbf{Z}, & y_{3,3} \in \mathbf{Z} \\ y_{1,1} \in \mathbf{Z}, & y_{1,2} \in (3), & y_{1,3} \in (3) \end{array}$$

and since $y_{1,3} + 3y_{2,1} + 3y_{3,2} \equiv_9 0$ as well as $y_{1,1} \equiv_3 y_{2,2} \equiv_3 y_{3,3}$.
So we have $\xi^2\Xi \subseteq \tilde{\Xi}$.

Ad ($\supseteq$). Let $\begin{pmatrix} z_{1,1} & z_{1,2} & z_{1,3} \\ z_{2,1} & z_{2,2} & z_{2,3} \\ z_{3,1} & z_{3,2} & z_{3,3} \end{pmatrix} \in \tilde{\Xi}$. We show that $\xi^{-2} \begin{pmatrix} z_{1,1} & z_{1,2} & z_{1,3} \\ z_{2,1} & z_{2,2} & z_{2,3} \\ z_{3,1} & z_{3,2} & z_{3,3} \end{pmatrix} \overset{!}{\in} \Xi$. We have $\xi^{-2} = \begin{pmatrix} 0 & 0 & 1 \\ \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 \end{pmatrix}$.
Therefore we obtain

$$\begin{pmatrix} 0 & 0 & 1 \\ \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 \end{pmatrix} \begin{pmatrix} z_{1,1} & z_{1,2} & z_{1,3} \\ z_{2,1} & z_{2,2} & z_{2,3} \\ z_{3,1} & z_{3,2} & z_{3,3} \end{pmatrix} = \begin{pmatrix} z_{3,1} & z_{3,2} & z_{3,3} \\ \frac{1}{3}z_{1,1} & \frac{1}{3}z_{1,2} & \frac{1}{3}z_{1,3} \\ \frac{1}{3}z_{2,1} & \frac{1}{3}z_{2,2} & \frac{1}{3}z_{2,3} \end{pmatrix},$$

which is an element of Ξ because of

$$\begin{array}{ccc} z_{3,1} \in \mathbf{Z}, & z_{3,2} \in (3), & z_{3,3} \in (3) \\ z_{1,1} \in (3), & z_{1,2} \in (3), & z_{1,3} \in (9) \\ z_{2,1} \in (3), & z_{2,2} \in (3), & z_{2,3} \in (3) \end{array}$$

and since

$$\begin{array}{rcl} 3z_{3,1} \equiv_9 z_{2,3} \equiv_9 z_{1,2} & \Rightarrow & z_{3,1} \equiv_3 \frac{1}{3}z_{2,3} \equiv_3 \frac{1}{3}z_{1,2} \\ z_{1,1} + z_{2,2} + z_{3,3} \equiv_9 0 & \Rightarrow & z_{3,3} + 3\frac{1}{3}z_{1,1} + 3\frac{1}{3}z_{2,2} \equiv_9 0 \ . \end{array}$$

Hence we have $\Xi \supseteq \xi^{-2}\tilde{\Xi}$.

Altogether we obtain $\xi^2\Xi = \tilde{\Xi}$.

We need to show that

$$\xi^{-1}\Xi \overset{!}{=} \tilde{\Xi}' := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & \mathbf{Z} & (3) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \\ (1/3) & \mathbf{Z} & \mathbf{Z} \end{pmatrix} : \begin{array}{rcl} x_{1,1} + x_{2,2} + x_{3,3} & \equiv_3 & 0 \\ x_{1,2} \equiv_3 x_{2,3} & \equiv_3 & 3x_{3,1} \end{array} \right\}$$

cf. Proposition 30.

Ad ($\subseteq$). Let $\begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} \in \Xi$. We have $\xi^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \frac{1}{3} & 0 & 0 \end{pmatrix}$.

Therefore we obtain

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \frac{1}{3} & 0 & 0 \end{pmatrix} \begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} = \begin{pmatrix} y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \\ \frac{1}{3}y_{1,1} & \frac{1}{3}y_{1,2} & \frac{1}{3}y_{1,3} \end{pmatrix} ,$$

which is an element of $\tilde{\Xi}'$ since

$$\begin{array}{ccc} y_{2,1} \in \mathbf{Z}, & y_{2,2} \in \mathbf{Z}, & y_{2,3} \in (3) \\ y_{3,1} \in \mathbf{Z}, & y_{3,2} \in \mathbf{Z}, & y_{3,3} \in \mathbf{Z} \\ y_{1,1} \in \mathbf{Z}, & y_{1,2} \in (3), & y_{1,3} \in (3) \end{array}$$

and since

$$\begin{array}{rcl} y_{1,3} + 3y_{2,1} + 3y_{3,2} \equiv_9 0 & \Rightarrow & \frac{1}{3}y_{1,3} + y_{2,1} + y_{3,2} \equiv_3 0 \\ y_{1,1} \equiv_3 y_{2,2} \equiv_3 y_{3,3} & \Rightarrow & 3\frac{1}{3}y_{1,1} \equiv_3 y_{2,2} \equiv_3 y_{3,3} \ . \end{array}$$

Hence we have $\xi^{-1}\Xi \subseteq \tilde{\Xi}$.

Ad ($\supseteq$) Let $\begin{pmatrix} z_{1,1} & z_{1,2} & z_{1,3} \\ z_{2,1} & z_{2,2} & z_{2,3} \\ z_{3,1} & z_{3,2} & z_{3,3} \end{pmatrix} \in \tilde{\Xi}'$. We show that $\xi \begin{pmatrix} z_{1,1} & z_{1,2} & z_{1,3} \\ z_{2,1} & z_{2,2} & z_{2,3} \\ z_{3,1} & z_{3,2} & z_{3,3} \end{pmatrix} \overset{!}{\in} \Xi$.

Therefore we obtain

$$\begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} z_{1,1} & z_{1,2} & z_{1,3} \\ z_{2,1} & z_{2,2} & z_{2,3} \\ z_{3,1} & z_{3,2} & z_{3,3} \end{pmatrix} = \begin{pmatrix} 3z_{3,1} & 3z_{3,2} & 3z_{3,3} \\ z_{1,1} & z_{1,2} & z_{1,3} \\ z_{2,1} & z_{2,2} & z_{2,3} \end{pmatrix} ,$$

which is an element of Ξ because of

$$\begin{array}{lcllcllcl} z_{3,1} & \in & (1/3), & z_{3,2} & \in \mathbf{Z}, & z_{3,3} & \in & \mathbf{Z} \\ z_{1,1} & \in & \mathbf{Z}, & z_{1,2} & \in \mathbf{Z}, & z_{1,3} & \in & (3) \\ z_{2,1} & \in & \mathbf{Z}, & z_{2,2} & \in \mathbf{Z}, & z_{2,3} & \in & \mathbf{Z} \end{array}$$

and since

$$\begin{array}{l} 3z_{3,1} \equiv_3 z_{2,3} \equiv_3 z_{1,2} \\ z_{1,1} + z_{2,2} + z_{3,3} \equiv_3 0 \quad \Rightarrow \quad 3z_{3,3} + 3z_{1,1} + 3z_{2,2} \equiv_9 0 \ . \end{array}$$

So $\Xi \supseteq \xi\tilde{\Xi}'$.

Altogether we have $\xi^{-1}\Xi = \tilde{\Xi}$.

We have $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \Xi \neq \emptyset$ and $\Xi \subseteq \mathbf{Z}^{3\times 3}$. As Λ' is a subring of $\mathbf{Q}^{6\times 6}$ and as $\begin{pmatrix} 0 & 0 \\ 0 & \Xi \end{pmatrix} \subseteq \Lambda'$, it follows that Ξ is closed under multiplication and subtraction. Because

$$\begin{pmatrix} 0 & 0 \\ 0 & \Xi \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \Xi \end{pmatrix} \subseteq \Lambda' \cap \left(\begin{smallmatrix} 0 & 0 \\ 0 & \mathbf{Z}^{2\times 2} \end{smallmatrix}\right) = \begin{pmatrix} 0 & 0 \\ 0 & \Xi \end{pmatrix}$$

and therefore $\Xi \cdot \Xi \subseteq \Xi$, respectively

$$\begin{pmatrix} 0 & 0 \\ 0 & \Xi \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & \Xi \end{pmatrix} \subseteq \Lambda' \cap \left(\begin{smallmatrix} 0 & 0 \\ 0 & \mathbf{Z}^{2\times 2} \end{smallmatrix}\right) = \begin{pmatrix} 0 & 0 \\ 0 & \Xi \end{pmatrix}$$

and therefore $\Xi - \Xi \subseteq \Xi$. So Ξ is a subring of $\mathbf{Z}^{3\times 3}$.

We need to show that $\xi\Xi \overset{!}{=} \Xi\xi$

Ad $(\subseteq)$. Let $\begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} \in \Xi$.

We have

$$\begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \frac{1}{3} & 0 & 0 \end{pmatrix} = \begin{pmatrix} y_{3,3} & 3y_{3,1} & 3y_{3,2} \\ \frac{1}{3}y_{1,3} & y_{1,1} & y_{1,2} \\ \frac{1}{3}y_{2,3} & y_{2,1} & y_{2,2} \end{pmatrix},$$

which is an element of Ξ since

$$\begin{array}{ccc} y_{3,3} \in \mathbf{Z}, & y_{3,1} \in \mathbf{Z}, & y_{3,2} \in \mathbf{Z} \\ y_{1,3} \in (3), & y_{1,1} \in \mathbf{Z}, & y_{1,2} \in (3) \\ y_{2,3} \in (3), & y_{2,1} \in \mathbf{Z}, & y_{2,2} \in \mathbf{Z} \end{array}$$

and since $y_{3,3} \equiv_3 y_{1,1} \equiv_3 y_{2,2}$ as well as $3y_{3,2} + y_{1,3} + 3y_{2,1} \equiv_9 0$.

So we have $\xi\Xi\xi^{-1} \subseteq \Xi$.

Ad $(\supseteq)$. Let $\begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} \in \Xi$.

We have

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \frac{1}{3} & 0 & 0 \end{pmatrix} \begin{pmatrix} y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} y_{2,2} & y_{2,3} & 3y_{2,1} \\ y_{3,2} & y_{3,3} & 3y_{3,1} \\ \frac{1}{3}y_{1,2} & \frac{1}{3}y_{1,3} & y_{1,1} \end{pmatrix},$$

which is an element of Ξ since

$$\begin{array}{ccc} y_{2,2} \in \mathbf{Z}, & y_{2,3} \in (3), & y_{2,1} \in \mathbf{Z} \\ y_{3,2} \in \mathbf{Z}, & y_{3,3} \in \mathbf{Z}, & y_{3,1} \in \mathbf{Z} \\ y_{1,2} \in (3), & y_{1,3} \in (3), & y_{1,1} \in \mathbf{Z} \end{array}$$

and since $y_{2,2} \equiv_3 y_{3,3} \equiv_3 y_{1,1}$ as well as $3y_{2,1} + 3y_{3,2} + y_{1,3} \equiv_9 0$.

So we have $\xi^{-1}\Xi\xi \subseteq \Xi$.

Altogether we have $\xi\Xi = \Xi\xi$. □

6 Example: $\mathbf{Q}(\sqrt[3]{2},\zeta_3)$

Setting 33. Consider the Galois extension $\mathbf{Q}(\sqrt[3]{2},\zeta_3)|\mathbf{Q}$ with Galois group $G \cong \mathrm{S}_3$.

$$\begin{tikzcd}
 & \mathbf{Q}(\sqrt[3]{2},\zeta_3) \arrow[d, dash, "{G,\ |G|=6}"] \\
\mathcal{O}_{\mathbf{Q}(\sqrt[3]{2},\zeta_3)} \arrow[ur, dash] \arrow[d, dash] & \mathbf{Q} \\
\mathbf{Z} \arrow[ur, dash] &
\end{tikzcd}$$

Write $\delta := \sqrt[3]{2},\ \zeta := \zeta_3,\ \eta := \frac{\zeta-1}{\delta+1}$.

The integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\delta,\zeta)$ is given by $\mathcal{O}_{\mathbf{Q}(\delta,\zeta)} = \mathbf{Z}[\delta,\eta]$, as I have learned from K. Conrad [5]. Note that the requirements of Setting 1 and Setting 13 are met, letting $A = \mathbf{Z}$ and $B = \mathcal{O}_{\mathbf{Q}(\delta,\zeta)}$.

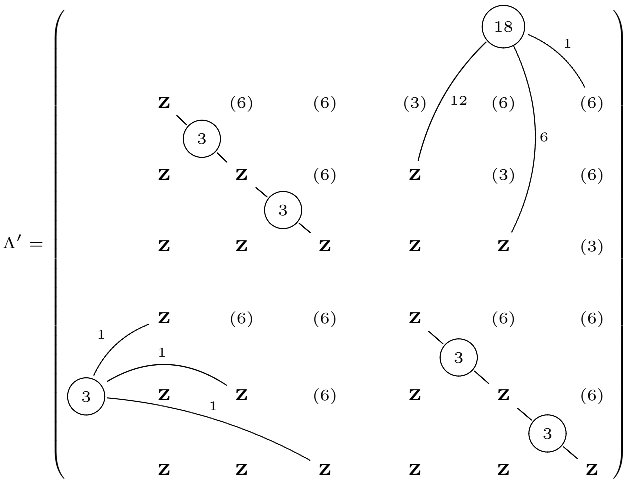
Proposition 34. *Consider the extension* $\mathbf{Q}(\delta,\zeta)|\mathbf{Q}$.

Choose the $\mathbf{Z}$*-linear basis* $\underline{y'} = (1-\delta, 2-\delta, -2+2\delta+\delta^2, \eta, 4\eta+\delta\eta, 4\eta+2\delta\eta+\delta^2\eta)$ *of* $\mathbf{Z}[\delta,\eta]$. *Consider the map* $\omega^{\mathbf{Z}}_{\underline{y'}} : \mathbf{Z}[\delta,\eta] \wr G \hookrightarrow \mathbf{Z}^{6\times 6}$. *Then the image of* $\omega^{\mathbf{Z}}_{\underline{y'}}$ *is given by*

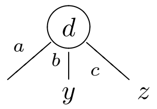
$$\Lambda' := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (6) & (6) & (3) & (6) & (6) \\ \mathbf{Z} & \mathbf{Z} & (6) & \mathbf{Z} & (3) & (6) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) \\ \\ \mathbf{Z} & (6) & (6) & \mathbf{Z} & (6) & (6) \\ \mathbf{Z} & \mathbf{Z} & (6) & \mathbf{Z} & \mathbf{Z} & (6) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \end{pmatrix} : \begin{array}{r} x_{1,1} \equiv_3 x_{2,2} \equiv_3 x_{3,3} \\ \\ x_{1,6} - 6x_{2,4} + 6x_{3,5} \equiv_{18} 0 \\ \\ x_{4,1} + x_{5,2} - x_{6,3} \equiv_3 0 \\ \\ x_{4,4} \equiv_3 x_{5,5} \equiv_3 x_{6,6} \end{array} \right\} .$$

In particular, we have $\mathbf{Z}[\delta,\eta] \wr G \cong \Lambda'$ *as rings.*

More symbolically written, we have



wherein



means $a\cdot x+b\cdot y+c\cdot z \equiv_d 0$.

If we considered the $\mathbf{Z}$-linear basis $\underline{y} = (y_1, ..., y_6) = (1, \delta, \delta^2, \eta, \delta\eta, \delta^2\eta)$ of $\mathbf{Z}[\delta, \eta]$ the congruences appearing in $\omega_{\underline{y}}$ would be rather complicated.

The $\mathbf{Z}$-linear basis $\underline{y'} = (1-\delta, 2-\delta, -2+2\delta+\delta^2, \eta, 4\eta+\delta\eta, 4\eta+2\delta\eta+\delta^2\eta)$, for which the appearing congruences take a simpler form, was calculated using the computer algebra system Magma [7], cf. Magma Code A 2.

Proof. The Galois group of the extension $\mathbf{Q}(\delta, \zeta)|\mathbf{Q}$ is given by $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ where

$$\begin{array}{rclllll}
 & & \sigma_1 : & \delta & \mapsto \delta, & \eta \mapsto & \eta \\
 & & \sigma_2 : & \delta & \mapsto \delta, & \eta \mapsto & (\zeta+1)\eta \\
 & & \sigma_3 : & \delta & \mapsto \zeta\delta, & \eta \mapsto & \dfrac{(\zeta-1)}{\zeta\delta+1} \\
\sigma_4 & = & \sigma_3\sigma_2 : & \delta & \mapsto \zeta\delta, & \eta \mapsto & (\zeta+1)\dfrac{(\zeta-1)}{\zeta\delta+1} \\
\sigma_5 & = & \sigma_3^2 : & \delta & \mapsto \zeta^2\delta, & \eta \mapsto & \dfrac{(\zeta-1)}{\zeta^2\delta+1} \\
\sigma_6 & = & \sigma_2\sigma_3 : & \delta & \mapsto \zeta^2\delta, & \eta \mapsto & (\zeta+1)\dfrac{(\zeta-1)}{\zeta^2\delta+1} \; .
\end{array}$$

We consider the image of $\omega_{\underline{y'}}^{\mathbf{Z}}$ on the $\mathbf{Z}$-linear basis $\underline{z'} = (y'_i\sigma_j : j, k \in [1,6])$ of $\mathbf{Z}[\delta, \eta] \wr G$.

$$\delta \;\mapsto\; \begin{pmatrix} -4 & -6 & 6 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ -1 & -1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 & -12 & -6 \\ 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix} \qquad \eta \;\mapsto\; \begin{pmatrix} 0 & 0 & 0 & -3 & -12 & -6 \\ 0 & 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & -1 & -4 & -3 \\ 5 & 6 & -6 & -9 & -30 & -18 \\ -1 & -1 & 0 & 3 & 9 & 6 \\ 0 & 0 & 1 & -1 & -3 & -3 \end{pmatrix}$$

$$\sigma_2 \;\mapsto\; \begin{pmatrix} 1 & 0 & 0 & -3 & -6 & 0 \\ 0 & 1 & 0 & 0 & -3 & -6 \\ 0 & 0 & 1 & -1 & -3 & -3 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \qquad \sigma_3 \;\mapsto\; \begin{pmatrix} 1 & 0 & -6 & 0 & 0 & 6 \\ 0 & 1 & 0 & 1 & 3 & 0 \\ 0 & 0 & -2 & 1 & 3 & 3 \\ 0 & 0 & -6 & 1 & 0 & 0 \\ 1 & 1 & 0 & -1 & -2 & 0 \\ -1 & -1 & 1 & 1 & 3 & 1 \end{pmatrix}$$

Let A be the representation matrix of $\omega_{\underline{y}}^{\mathbf{Z}}$, with respect to the bases $\underline{z'}$ of $\mathbf{Z}[\delta, \eta] \wr G$ and $(e_{i,j})_{i,j \in [1,6]}$ of $\mathbf{Z}^{6\times 6}$.

A=

$$\begin{pmatrix}
1 & -4 & 4 & 0 & 0 & 0 & 1 & -4 & 4 & 0 & 0 & 0 & 1 & -4 & 4 & -6 & 0 & 6 & 1 & -4 & 4 & -6 & 0 & 6 & -5 & 2 & -2 & 6 & 0 & -6 & -5 & 2 & -2 & 6 & 0 & -6 \\
0 & -6 & 6 & 0 & 0 & 0 & 0 & -6 & 6 & 0 & 0 & 0 & 0 & -6 & 6 & -6 & 0 & 6 & 0 & -6 & 6 & -6 & 0 & 6 & -6 & 0 & 0 & 6 & 0 & -6 & -6 & 0 & 0 & 6 & 0 & -6 \\
0 & 6 & -12 & 0 & 0 & 0 & 0 & 6 & -12 & 0 & 0 & 0 & -6 & 12 & 0 & 12 & 6 & -24 & -6 & 12 & 0 & 12 & 6 & -24 & 12 & -6 & 0 & -12 & -6 & 24 & 12 & -6 & 0 & -12 & -6 & 24 \\
0 & 0 & 0 & -3 & 0 & 6 & -3 & 6 & 0 & 3 & 0 & -6 & 0 & 0 & -6 & 3 & 0 & 0 & 3 & 0 & -6 & 3 & -6 & 6 & 0 & 0 & 6 & -3 & 6 & -6 & 3 & 0 & 0 & -3 & 0 & 0 \\
0 & 0 & 0 & -12 & 6 & 18 & -6 & 24 & -6 & 12 & -6 & -18 & 0 & 0 & -18 & 6 & 6 & 0 & 12 & 6 & -24 & 12 & -24 & 18 & 0 & 0 & 18 & -12 & 24 & -18 & 12 & 6 & -6 & -6 & -6 & 0 \\
0 & 0 & 0 & -6 & 6 & 12 & 0 & 18 & 0 & 6 & -6 & -12 & 6 & -6 & -12 & -6 & 6 & 12 & 12 & 6 & -24 & 6 & -24 & 24 & -6 & 6 & 12 & -6 & 24 & -24 & 6 & 12 & -12 & 6 & -6 & -12 \\
0 & 1 & -2 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 & 1 & -2 & 3 & 0 & 0 & 0 & 1 & -2 & 3 & 0 & 0 & 3 & 1 & 4 & -3 & 0 & 0 & 3 & 1 & 4 & -3 & 0 & 0 \\
1 & 2 & -2 & 0 & 0 & 0 & 1 & 2 & -2 & 0 & 0 & 0 & 1 & 2 & -2 & 3 & 0 & 0 & 1 & 2 & -2 & 3 & 0 & 0 & 4 & 2 & 4 & -3 & 0 & 0 & 4 & 2 & 4 & -3 & 0 & 0 \\
0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & -6 & 0 & -6 & 0 & 6 & 0 & -6 & 0 & -6 & 0 & 6 & -6 & 0 & -6 & 6 & 0 & -6 & -6 & 0 & -6 & 6 & 0 & -6 \\
0 & 0 & 0 & 1 & -1 & -2 & 0 & -3 & 0 & -1 & 1 & 2 & 1 & 2 & 4 & -2 & -1 & -2 & -1 & 1 & 2 & -1 & 1 & -4 & -1 & -2 & -4 & 1 & -1 & 4 & -2 & -1 & -2 & 2 & 1 & 2 \\
0 & 0 & 0 & 3 & -6 & -6 & -3 & -12 & 0 & -3 & 6 & 6 & 3 & 6 & 12 & -6 & -6 & -6 & -6 & 0 & 6 & -3 & 6 & -12 & -3 & -6 & -12 & 3 & -6 & 12 & -9 & -6 & -6 & 6 & 6 & 6 \\
0 & 0 & 0 & 0 & -6 & -6 & -6 & -12 & -6 & 0 & 6 & 6 & 0 & 6 & 6 & 0 & -6 & -6 & -6 & 0 & 6 & 0 & 6 & -12 & 0 & -6 & -6 & 0 & -6 & 12 & -6 & -6 & 0 & 0 & 6 & 6 \\
0 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & 2 & 0 & -1 & 1 & -1 & 1 & 2 & 0 & 2 & 1 & 1 & -1 & -2 & 0 & 2 & 1 & 1 & -1 & -2 \\
0 & -1 & 2 & 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 1 & 2 & 0 & -1 & 2 & -1 & 1 & 2 & 0 & 2 & 2 & 1 & -1 & -2 & 0 & 2 & 2 & 1 & -1 & -2 \\
1 & 2 & -2 & 0 & 0 & 0 & 1 & 2 & -2 & 0 & 0 & 0 & -2 & 2 & -2 & 3 & 0 & -6 & -2 & 2 & -2 & 3 & 0 & -6 & 1 & -4 & -2 & -3 & 0 & 6 & 1 & -4 & -2 & -3 & 0 & 6 \\
0 & 0 & 0 & -1 & 0 & 1 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & 1 & 0 & 0 & -1 & -1 & 1 & 0 & -1 & 0 & -2 & 1 & -1 & -1 & 0 & 0 & 2 & -1 & 0 & -1 & -1 & 0 & 1 & 1 \\
0 & 0 & 0 & -4 & 1 & 2 & -3 & 3 & -6 & 4 & -1 & -2 & 3 & 3 & 0 & -1 & -2 & -4 & 3 & 0 & -6 & 1 & -7 & 4 & -3 & -3 & 0 & -1 & 7 & -4 & 0 & -3 & -6 & 1 & 2 & 4 \\
0 & 0 & 0 & -3 & 0 & 0 & -3 & 0 & -6 & 3 & 0 & 0 & 3 & 0 & 0 & -3 & 0 & 0 & 3 & 0 & -6 & 0 & -6 & 6 & -3 & 0 & 0 & 0 & 6 & -6 & 0 & 0 & -6 & 3 & 0 & 0 \\
0 & 0 & 0 & 5 & -8 & 2 & 0 & 0 & 0 & 5 & -8 & 2 & 0 & -6 & 6 & -7 & 4 & 8 & 0 & -6 & 6 & -7 & 4 & 8 & 0 & 6 & -6 & 5 & -8 & 2 & 0 & 6 & -6 & 5 & -8 & 2 \\
0 & 0 & 0 & 6 & -12 & 6 & 0 & 0 & 0 & 6 & -12 & 6 & 0 & -6 & 6 & -6 & 0 & 12 & 0 & -6 & 6 & -6 & 0 & 12 & 0 & 6 & -6 & 6 & -12 & 6 & 0 & 6 & -6 & 6 & -12 & 6 \\
0 & 0 & 0 & -6 & 18 & -12 & 0 & 0 & 0 & -6 & 18 & -12 & -6 & 18 & -12 & 18 & -6 & -24 & -6 & 18 & -12 & 18 & -6 & -24 & 6 & -18 & 12 & -18 & 12 & 12 & 6 & -18 & 12 & -18 & 12 & 12 \\
1 & -4 & 4 & -9 & 6 & 6 & -1 & 4 & -4 & 0 & 0 & 0 & 1 & 2 & -2 & 3 & 0 & -6 & 5 & -2 & -4 & 0 & -6 & 6 & -5 & 2 & 4 & 3 & 6 & -12 & -1 & -2 & 2 & 0 & 6 & -6 \\
0 & -12 & 18 & -30 & 30 & 6 & 0 & 12 & -18 & 0 & 0 & 0 & 0 & 6 & 0 & 6 & 12 & -30 & 18 & -6 & -18 & 0 & -18 & 18 & -18 & 6 & 18 & 6 & 30 & -48 & 0 & -6 & 0 & 0 & 18 & -18 \\
0 & -6 & 12 & -18 & 18 & 0 & 0 & 6 & -12 & 0 & 0 & 0 & 0 & -6 & 12 & -6 & 24 & -24 & 18 & -12 & -12 & -12 & -6 & 24 & -18 & 12 & 12 & 6 & 30 & -48 & 0 & 6 & -12 & 12 & 6 & -24 \\
0 & 0 & 0 & -1 & 3 & -2 & 0 & 0 & 0 & -1 & 3 & -2 & 1 & 2 & -2 & 2 & -3 & -2 & 1 & 2 & -2 & 2 & -3 & -2 & -1 & -2 & 2 & -1 & 3 & -2 & -1 & -2 & 2 & -1 & 3 & -2 \\
0 & 0 & 0 & -1 & 4 & -4 & 0 & 0 & 0 & -1 & 4 & -4 & 1 & 2 & -2 & 2 & -2 & -4 & 1 & 2 & -2 & 2 & -2 & -4 & -1 & -2 & 2 & -1 & 4 & -4 & -1 & -2 & 2 & -1 & 4 & -4 \\
0 & 0 & 0 & 0 & -6 & 6 & 0 & 0 & 0 & 0 & -6 & 6 & 0 & -6 & 6 & -6 & 6 & 6 & 0 & -6 & 6 & -6 & 6 & 6 & 0 & 6 & -6 & 6 & -6 & 0 & 0 & 6 & -6 & 6 & -6 & 0 \\
0 & 1 & -2 & 3 & -3 & 0 & 0 & -1 & 2 & 0 & 0 & 0 & -1 & -1 & 0 & -1 & 1 & 2 & -2 & 1 & 0 & 1 & 2 & -2 & 2 & -1 & 0 & -2 & -1 & 4 & 1 & 1 & 0 & -1 & -2 & 2 \\
1 & 2 & -8 & 9 & -12 & 6 & -1 & -2 & 8 & 0 & 0 & 0 & -2 & -4 & -2 & -3 & 0 & 12 & -7 & 4 & 2 & 3 & 6 & -6 & 7 & -4 & -2 & -6 & -6 & 18 & 2 & 4 & 2 & -3 & -6 & 6 \\
0 & 0 & -6 & 6 & -6 & 6 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & -6 & 0 & -6 & 12 & -6 & 6 & 0 & 6 & 0 & -6 & 6 & -6 & 0 & -6 & -6 & 18 & 0 & 0 & 6 & -6 & 0 & 6 \\
0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & -1 & -1 & 0 & 0 & 2 & 1 & -1 & -1 & 0 & 0 & 2 & 1 & 1 & 1 & 0 & 0 & -1 & 1 & 1 & 1 & 0 & 0 & -1 & 1 \\
0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & -1 & 0 & 0 & 2 & 2 & -1 & -1 & 0 & 0 & 2 & 2 & 1 & 1 & 0 & 0 & -1 & 2 & 1 & 1 & 0 & 0 & -1 & 2 \\
0 & 0 & 0 & 1 & 2 & -2 & 0 & 0 & 0 & 1 & 2 & -2 & 1 & 2 & -2 & 1 & -4 & -2 & 1 & 2 & -2 & 1 & -4 & -2 & -1 & -2 & 2 & -2 & 2 & -2 & -1 & -2 & 2 & -2 & 2 & -2 \\
0 & 0 & 1 & -1 & 1 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & -1 & -1 & 1 & 0 & 1 & -1 & -1 & 0 & -1 & 0 & -1 & 1 & 0 & -1 & -1 & -1 & -1 & 1 & 1 & 0 \\
0 & 1 & 4 & -3 & 3 & -6 & 0 & -1 & -4 & 0 & 0 & 0 & 3 & 4 & 4 & 0 & -3 & -6 & 3 & -1 & 2 & -3 & -3 & 0 & -3 & 1 & -2 & 3 & 0 & -6 & -3 & -4 & -4 & 3 & 3 & 0 \\
1 & 2 & 4 & -3 & 0 & -6 & -1 & -2 & -4 & 0 & 0 & 0 & 1 & 2 & 4 & 0 & 0 & -6 & 2 & -2 & 2 & -3 & 0 & 0 & -2 & 2 & -2 & 3 & 0 & -6 & -1 & -2 & -4 & 3 & 0 & 0
\end{pmatrix}$$

and $18A^{-1}=$

$$\begin{pmatrix}
-6 & 0 & 0 & 18 & -12 & 6 & 0 & -6 & 0 & 36 & -18 & 6 & 0 & 0 & -6 & -72 & 36 & -18 & 18 & 0 & 6 & 12 & 0 & 0 & 36 & 18 & 18 & 0 & 12 & 0 & 0 & 36 & 18 & 0 & 0 & 12 \\
-12 & 6 & -3 & -36 & 12 & -3 & -18 & 6 & -6 & -54 & 18 & -6 & 36 & -18 & 6 & 72 & -18 & 0 & 0 & 0 & 3 & 24 & -12 & 6 & 18 & 0 & 18 & 108 & -48 & 24 & 0 & 18 & 18 & 72 & -36 & 24 \\
12 & -3 & 3 & 18 & -3 & 0 & 18 & -6 & 3 & 18 & 0 & -3 & -18 & 0 & -6 & -18 & 0 & 0 & -18 & 9 & -3 & -24 & 6 & 0 & -72 & 36 & -9 & -72 & 12 & 6 & -54 & 36 & 0 & -36 & 0 & 12 \\
18 & -6 & 6 & 36 & -12 & 4 & 36 & -18 & 6 & 48 & -12 & 0 & -36 & 0 & -18 & -72 & 24 & -12 & -12 & 12 & 0 & -18 & 6 & 0 & -72 & 60 & 0 & -72 & 18 & 6 & -72 & 72 & 12 & -36 & 0 & 18 \\
-18 & 6 & -3 & -12 & 0 & 2 & -18 & 0 & -6 & -12 & 0 & 0 & 36 & -18 & 0 & 0 & 12 & -12 & 12 & 0 & 6 & 18 & -6 & 3 & 36 & 12 & 24 & 54 & -18 & 12 & 0 & 36 & 24 & 36 & -18 & 18 \\
0 & 3 & 0 & -12 & 6 & -2 & 0 & 0 & -3 & -24 & 12 & -6 & 18 & -18 & 0 & 36 & -12 & 0 & -12 & 6 & 0 & 0 & -3 & 3 & -36 & 24 & 6 & 18 & -18 & 15 & -36 & 36 & 12 & 18 & -18 & 18 \\
12 & 0 & 0 & -18 & 12 & -6 & 0 & 12 & 0 & -36 & 18 & -6 & 0 & 0 & 12 & 72 & -36 & 18 & -18 & 0 & -6 & -12 & 0 & 0 & -36 & -18 & -18 & 0 & -12 & 0 & 0 & -36 & -18 & 0 & 0 & -12 \\
24 & -12 & 6 & 36 & -12 & 3 & 36 & -12 & 12 & 54 & -18 & 6 & -72 & 36 & -12 & -72 & 18 & 0 & 0 & 0 & -3 & -24 & 12 & -6 & -18 & 0 & -18 & -108 & 48 & -24 & 0 & -18 & -18 & -72 & 36 & -24 \\
-24 & 6 & -6 & -18 & 3 & 0 & -36 & 12 & -6 & -18 & 0 & 3 & 36 & 0 & 12 & 18 & 0 & 0 & 18 & -9 & 3 & 24 & -6 & 0 & 72 & -36 & 9 & 72 & -12 & -6 & 54 & -36 & 0 & 36 & 0 & -12 \\
-18 & 6 & -6 & -36 & 12 & -4 & -36 & 18 & -6 & -48 & 12 & 0 & 36 & 0 & 18 & 72 & -24 & 12 & 6 & -6 & 0 & 18 & -6 & 0 & 36 & -30 & 0 & 72 & -18 & -6 & 36 & -36 & -6 & 36 & 0 & -18 \\
18 & -6 & 3 & 12 & 0 & -2 & 18 & 0 & 6 & 12 & 0 & 0 & -36 & 18 & 0 & 0 & -12 & 12 & -6 & 0 & -3 & -18 & 6 & -3 & -18 & -6 & -12 & -54 & 18 & -12 & 0 & -18 & -12 & -36 & 18 & -18 \\
0 & -3 & 0 & 12 & -6 & 2 & 0 & 0 & 3 & 24 & -12 & 6 & -18 & 18 & 0 & -36 & 12 & 0 & 6 & -3 & 0 & 0 & 3 & -3 & 18 & -12 & -3 & -18 & 18 & -15 & 18 & -18 & -6 & -18 & 18 & -18 \\
-6 & 0 & 0 & 18 & -6 & 0 & 0 & -6 & 0 & 36 & -12 & 0 & 36 & 0 & 12 & 0 & 0 & 6 & -18 & 6 & -6 & -24 & 6 & 0 & -72 & 36 & -18 & -108 & 30 & 0 & -72 & 36 & -18 & -108 & 36 & -6 \\
6 & 6 & 6 & 0 & 0 & 3 & 18 & 6 & 12 & 18 & -6 & 6 & 0 & -18 & -12 & 0 & 0 & -6 & 0 & -6 & -3 & 6 & 0 & -3 & -18 & -18 & -18 & 0 & 6 & -12 & -36 & 0 & -18 & -36 & 18 & -12 \\
-6 & -3 & -6 & -18 & 6 & -3 & 0 & -6 & -6 & -18 & 6 & -3 & 18 & 0 & 12 & 54 & -18 & 6 & 0 & 6 & 3 & -6 & 3 & 0 & 0 & 18 & 9 & -18 & 12 & -3 & -18 & 18 & 0 & -36 & 18 & -6 \\
-6 & -6 & -6 & 0 & 0 & -2 & 0 & -12 & -6 & 12 & -6 & 0 & 36 & 0 & 18 & 36 & -12 & 6 & -12 & 12 & 0 & -18 & 6 & 0 & -36 & 42 & 0 & -72 & 30 & -6 & -36 & 36 & -6 & -72 & 36 & -12 \\
6 & 0 & 3 & 6 & 0 & -1 & 18 & -6 & 6 & 24 & -6 & 0 & 0 & 0 & 0 & 0 & -6 & 6 & -6 & 0 & -3 & 0 & 0 & 0 & -36 & 12 & -12 & -18 & 6 & 0 & -36 & 18 & -12 & -36 & 18 & -6 \\
-6 & 6 & 0 & -12 & 3 & 1 & 0 & 6 & 3 & -6 & 0 & 3 & 18 & -18 & 0 & 36 & -12 & 0 & 6 & -3 & 0 & 0 & 3 & -3 & 18 & -12 & -3 & 0 & 12 & -12 & 0 & 0 & -6 & -18 & 18 & -12 \\
-24 & 18 & 0 & -18 & 6 & 0 & -36 & 30 & 0 & -36 & 12 & 0 & 36 & -36 & -6 & 0 & 0 & -6 & 18 & -12 & 0 & 24 & -6 & 0 & 72 & -54 & 0 & 108 & -30 & 0 & 36 & -36 & 0 & 108 & -36 & 6 \\
6 & -12 & -3 & 0 & 0 & -3 & 0 & -12 & -6 & -18 & 6 & -6 & 0 & 18 & 6 & 0 & 0 & 6 & -18 & 12 & 0 & -6 & 0 & 3 & -54 & 36 & 0 & 0 & -6 & 12 & -36 & 18 & 0 & 36 & -18 & 12 \\
12 & -3 & 3 & 18 & -6 & 3 & 18 & -6 & 3 & 18 & -6 & 3 & -36 & 18 & -6 & -54 & 18 & -6 & 0 & -3 & 0 & 6 & -3 & 0 & -18 & 0 & 0 & 18 & -12 & 3 & -18 & 0 & 0 & 36 & -18 & 6 \\
-6 & 6 & 0 & 0 & 0 & 2 & 0 & 6 & 0 & -12 & 6 & 0 & 0 & 0 & 0 & -36 & 12 & -6 & 6 & -6 & 0 & 18 & -6 & 0 & 0 & -12 & 0 & 72 & -30 & 6 & -36 & 0 & -6 & 72 & -36 & 12 \\
-12 & 6 & 0 & -6 & 0 & 1 & -18 & 12 & 0 & -24 & 6 & 0 & 36 & -18 & 0 & 0 & 6 & -6 & -6 & 0 & -3 & 0 & 0 & 0 & -18 & -6 & -12 & 18 & -6 & 0 & -36 & 0 & -12 & 36 & -18 & 6 \\
12 & -9 & 0 & 12 & -3 & -1 & 18 & -12 & 0 & 6 & 0 & -3 & -18 & 18 & 0 & -36 & 12 & 0 & -12 & 6 & 0 & 0 & -3 & 3 & -54 & 24 & -3 & 0 & -12 & 12 & -54 & 18 & -6 & 18 & -18 & 12 \\
30 & -18 & 0 & 18 & 0 & -6 & 36 & -24 & 0 & 36 & -6 & -6 & -72 & 36 & -6 & -36 & 0 & 12 & -18 & 12 & 0 & -24 & 6 & 0 & -72 & 54 & 0 & -108 & 30 & 0 & -36 & 36 & 0 & -108 & 36 & -6 \\
-12 & 6 & -3 & -18 & 6 & 0 & -18 & 6 & -6 & -18 & 6 & 0 & 0 & 0 & 6 & 36 & -18 & 6 & 18 & -12 & 0 & 6 & 0 & -3 & 54 & -36 & 0 & 0 & 6 & -12 & 36 & -18 & 0 & -36 & 18 & -12 \\
-6 & 6 & 3 & 0 & -3 & 3 & -18 & 12 & 3 & 0 & -6 & 6 & 18 & -18 & -6 & 18 & 0 & -6 & 0 & 3 & 0 & -6 & 3 & 0 & 18 & 0 & 0 & -18 & 12 & -3 & 18 & 0 & 0 & -36 & 18 & -6 \\
6 & -6 & 0 & 0 & 0 & -2 & 0 & -6 & 0 & 12 & -6 & 0 & 0 & 0 & 0 & 36 & -12 & 6 & -12 & 12 & 0 & -18 & 6 & 0 & -36 & 42 & 0 & -72 & 24 & 0 & -36 & 36 & -6 & -108 & 36 & -6 \\
12 & -6 & 0 & 6 & 0 & -1 & 18 & -12 & 0 & 24 & -6 & 0 & -36 & 18 & 0 & 0 & -6 & 6 & -6 & 0 & -3 & -18 & 6 & -3 & -36 & 12 & -12 & -90 & 30 & -12 & -36 & 18 & -12 & -108 & 36 & -12 \\
-12 & 9 & 0 & -12 & 3 & 1 & -18 & 12 & 0 & -6 & 0 & 3 & 18 & -18 & 0 & 36 & -12 & 0 & 6 & -3 & 0 & 0 & 0 & 0 & 18 & -12 & -3 & -18 & 6 & -3 & 0 & 0 & -6 & -54 & 18 & -6 \\
-24 & 18 & 0 & -18 & 0 & 6 & -36 & 30 & 0 & -36 & 6 & 6 & 36 & -36 & -6 & 36 & 0 & -12 & 18 & -6 & 6 & 24 & -6 & 0 & 72 & -36 & 18 & 108 & -30 & 0 & 72 & -36 & 18 & 108 & -36 & 6 \\
6 & -12 & -3 & 18 & -6 & 0 & 0 & -12 & -6 & 18 & -6 & 0 & 0 & 18 & 6 & -36 & 18 & -6 & 0 & 6 & 3 & -6 & 0 & 3 & 18 & 18 & 18 & 0 & -6 & 12 & 36 & 0 & 18 & 36 & -18 & 12 \\
12 & -3 & 3 & 0 & 3 & -3 & 18 & -6 & 3 & 0 & 6 & -6 & -36 & 18 & -6 & -18 & 0 & 6 & 0 & -6 & -3 & 6 & -3 & 0 & 0 & -18 & -9 & 18 & -12 & 3 & 18 & -18 & 0 & 36 & -18 & 6 \\
6 & 6 & 6 & 0 & 0 & 2 & 0 & 12 & 6 & -12 & 6 & 0 & -36 & 0 & -18 & -36 & 12 & -6 & 6 & -6 & 0 & 18 & -6 & 0 & 36 & -30 & 0 & 72 & -24 & 0 & 72 & -36 & 12 & 108 & -36 & 6 \\
-6 & 0 & -3 & -6 & 0 & 1 & -18 & 6 & -6 & -24 & 6 & 0 & 0 & 0 & 0 & 0 & 6 & -6 & 12 & 0 & 6 & 18 & -6 & 3 & 54 & -6 & 24 & 90 & -30 & 12 & 72 & -18 & 24 & 108 & -36 & 12 \\
6 & -6 & 0 & 12 & -3 & -1 & 0 & -6 & -3 & 6 & 0 & -3 & -18 & 18 & 0 & -36 & 12 & 0 & 6 & -3 & 0 & 0 & 0 & 0 & 36 & -12 & 6 & 18 & -6 & 3 & 54 & -18 & 12 & 54 & -18 & 6
\end{pmatrix}$$

Let $X = (x_{i,j})_{i,j} \in \mathbf{Z}^{6\times 6},\ i,j \in [1,6]$. We have

$$X \in \Lambda \quad \Leftrightarrow \qquad \omega_{\underline{y}}^{-1}(X) \in \mathbf{Z}[\delta,\eta] \wr G \Leftrightarrow A^{-1} \cdot \begin{pmatrix} x_{1,1} \\ x_{1,2} \\ \vdots \\ x_{6,6} \end{pmatrix} \in \mathbf{Z}^{36\times 1}$$

$$\Leftrightarrow \quad \begin{pmatrix}
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 12 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\begin{pmatrix} x_{1,1} \\ \vdots \\ x_{1,6} \\ x_{2,1} \\ \vdots \\ x_{2,6} \\ x_{3,1} \\ \vdots \\ x_{3,6} \\ x_{4,1} \\ \vdots \\ x_{4,6} \\ x_{5,1} \\ \vdots \\ x_{5,6} \\ x_{6,1} \\ \vdots \\ x_{6,6} \end{pmatrix} \in 18\mathbf{Z}^{20\times 1}$$

$$\Leftrightarrow \qquad \left\{ \begin{aligned}
6x_{1,1} + 12x_{3,3} &\equiv_{18} 0 \\
3x_{1,2} &\equiv_{18} 0 \\
3x_{1,3} &\equiv_{18} 0 \\
6x_{1,4} &\equiv_{18} 0 \\
3x_{1,5} &\equiv_{18} 0 \\
x_{1,6} + 12x_{2,4} + 6x_{3,5} &\equiv_{18} 0 \\
6x_{2,2} + 12x_{3,3} &\equiv_{18} 0 \\
3x_{2,3} &\equiv_{18} 0 \\
6x_{2,5} &\equiv_{18} 0 \\
3x_{2,6} &\equiv_{18} 0 \\
6x_{3,6} &\equiv_{18} 0 \\
6x_{4,1} + 6x_{5,2} + 12x_{6,3} &\equiv_{18} 0 \\
3x_{4,2} &\equiv_{18} 0 \\
3x_{4,3} &\equiv_{18} 0 \\
6x_{4,4} + 12x_{6,6} &\equiv_{18} 0 \\
3x_{4,5} &\equiv_{18} 0 \\
3x_{4,6} &\equiv_{18} 0 \\
3x_{5,3} &\equiv_{18} 0 \\
6x_{5,5} + 12x_{6,6} &\equiv_{18} 0 \\
3x_{5,6} &\equiv_{18} 0
\end{aligned} \right.
\Leftrightarrow
\left\{ \begin{aligned}
x_{1,1} &\equiv_3 x_{2,2} \equiv_3 x_{3,3} \\
x_{1,2} &\equiv_6 x_{1,3} \equiv_6 x_{2,3} \equiv_6 0 \\
\\
x_{1,4} &\equiv_3 x_{1,5} \equiv_6 0 \\
x_{1,6} - 6x_{2,4} + 6x_{3,5} &\equiv_{18} 0 \\
x_{2,5} &\equiv_3 x_{2,6} \equiv_6 x_{3,6} \equiv_3 0 \\
\\
x_{4,1} + x_{5,2} - x_{6,3} &\equiv_3 0 \\
x_{4,2} &\equiv_6 x_{4,3} \equiv_6 x_{5,3} \equiv_6 0 \\
\\
x_{4,4} &\equiv_3 x_{5,5} \equiv_3 x_{6,6} \\
x_{4,5} &\equiv_6 x_{4,6} \equiv_6 x_{5,6} \equiv_6 0
\end{aligned} \right.
.$$

Hence the image of $\omega_{\underline{y}}^{\mathbf{Z}}$ is given by

$$\Lambda' := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} \mathbf{Z} & (6) & (6) & (3) & (6) & (6) \\ \mathbf{Z} & \mathbf{Z} & (6) & \mathbf{Z} & (3) & (6) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & (3) \\ \mathbf{Z} & (6) & (6) & \mathbf{Z} & (6) & (6) \\ \mathbf{Z} & \mathbf{Z} & (6) & \mathbf{Z} & \mathbf{Z} & (6) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & \mathbf{Z} \end{pmatrix} : \begin{array}{r} x_{1,1} \equiv_3 x_{2,2} \equiv_3 x_{3,3} \\ x_{1,6} - 6x_{2,4} + 6x_{3,5} \equiv_{18} 0 \\ x_{4,1} + x_{5,2} + x_{6,3} \equiv_3 0 \\ x_{4,4} \equiv_3 x_{5,5} \equiv_3 x_{6,6} \end{array} \right\}.$$

□

Remark 35. The index of Λ in $\mathbf{Z}^{6\times 6}$ is directly calculated to be

$$[\mathbf{Z}^{6\times 6} : \Lambda] := |\mathbf{Z}^{6\times 6}/\Lambda| = 2^{12} \cdot 3^{21} = (2^4 \cdot 3^7)^3 = |\Delta_{\mathbf{Q}(\sqrt[3]{2},\zeta_3)|\mathbf{Q},\underline{y}}|^{6/2} ,$$

confirming the statement of Corollary 17 in this case.

Corollary 36. *In the case of* Proposition 34 *we have the following.*

(1) *Write* $R := \mathbf{Z}_{(2)}$. *Then* $\Lambda'_{(2)} := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} R & (2) & (2) & R & (2) & (2) \\ R & R & (2) & R & R & (2) \\ R & R & R & R & R & R \\ R & (2) & (2) & R & (2) & (2) \\ R & R & (2) & R & R & (2) \\ R & R & R & R & R & R \end{pmatrix} \right\}$.

(2) *Write* $R := \mathbf{Z}_{(3)}$. *Then*

$$\Lambda'_{(3)} := \left\{ (x_{i,j})_{i,j} \in \begin{pmatrix} R & (3) & (3) & (3) & (3) & (3) \\ R & R & (3) & R & (3) & (3) \\ R & R & R & R & R & (3) \\ R & (3) & (3) & R & (3) & (3) \\ R & R & (3) & R & R & (3) \\ R & R & R & R & R & R \end{pmatrix} : \begin{array}{r} x_{1,1} \equiv_3 x_{2,2} \equiv_3 x_{3,3} \\ x_{1,6} + 3x_{2,4} - 3x_{3,5} \equiv_9 0 \\ x_{4,1} + x_{5,2} + x_{6,3} \equiv_3 0 \\ x_{4,4} \equiv_3 x_{5,5} \equiv_3 x_{6,6} \end{array} \right\}.$$

7 Ideals

Setting 37. Let A be a Dedekind domain with perfect field of fractions $K = \mathrm{frac}(A)$. Let $L|K$ be a Galois extension with Galois group $G := \mathrm{Gal}(L|K)$. Write $n := |G| = [L : K]$. Let $B = \Gamma_L(A)$ be the integral closure of A in L.
In case of $A = \mathbf{Z}$ we denote $\Gamma_L(\mathbf{Z}) = \mathcal{O}_L$.

$$\begin{tikzcd}
 & L \arrow[d, dash, "{G,\ |G|=n}"] \\
B \arrow[ur, dash] \arrow[d, dash] & K \\
A \arrow[ur, dash] &
\end{tikzcd}$$

Let $\underline{y} = (y_1, ..., y_n)$ be a $\mathbf{Z}$-linear basis of B, which is also a K-linear basis of L.

Note that the requirements of Setting 1 are also met.

Let $\Lambda := \omega_{\underline{y}}^A(B \wr G) \subseteq A^{n\times n}$, cf. Remark 7.

7.1 Galois-stability

Definition 38. An ideal $\mathfrak{b} \subseteq B$ is called *Galois-stable* if it satifies the condition $\sigma(\mathfrak{b}) = \mathfrak{b}$ for all $\sigma \in G$. We denote the set of all non-zero Galois-stable ideals in B by $\mathrm{Ideals}^{\times,G}(B)$.

Example 39.

(1) Let $L = \mathbf{Q}(\sqrt{-5})$. We have $G = \{\mathrm{id}, \sqrt{-5} \overset{\sigma}{\mapsto} -\sqrt{-5}\}$ and $B = \mathbf{Z}[\sqrt{-5}]$.

The ideal $\mathfrak{b} = (2, 1 + \sqrt{-5}) \subseteq B$ is Galois-stable since

$$\sigma(\mathfrak{b}) = (2, 1 - \sqrt{-5}) = (2, 1 + \sqrt{-5}) \ .$$

(2) Let $L = \mathbf{Q}(\mathrm{i})$. We have $G = \{\mathrm{id}, \mathrm{i} \overset{\sigma}{\mapsto} -\mathrm{i}\}$ and $B = \mathbf{Z}[\mathrm{i}]$.

The ideal $\mathfrak{b} = (2 + \mathrm{i}) \subseteq B$ is not Galois-stable because

$$\mathfrak{b}^2 = (3 + 4\,\mathrm{i}) \neq (5) = (2 + \mathrm{i})(2 - \mathrm{i}) = \mathfrak{b}\sigma(\mathfrak{b})$$

since $3 + 4\,\mathrm{i}$ is not divisible by 5 in $\mathbf{Z}[\mathrm{i}]$.

Lemma 40. *We have the map*

$$\begin{array}{ccc} \mathrm{Ideals}^{\times}(B) & \to & \mathrm{Rightideals}^{\times}(B \wr G) \\ \mathfrak{b} & \mapsto & \mathfrak{b}(B \wr G) \end{array}$$

where $\mathfrak{b}(B \wr G) \subseteq B \wr G$ is a right ideal. If $\mathfrak{b} \in \mathrm{Ideals}^{\times,G}(B)$ then $\mathfrak{b}(B \wr G)$ is an ideal, so that we obtain the map

$$\begin{array}{rcl} \mathrm{Ideals}^{\times,G}(B) & \xrightarrow{\iota} & \mathrm{Ideals}^{\times}(B \wr G) \\ \mathfrak{b} & \mapsto & \mathfrak{b}(B \wr G)\ . \end{array}$$

Proof. Suppose given $x, x' \in \mathfrak{b}(B \wr G)$ and $r \in B \wr G$. Write $x =: \sum\limits_{\sigma\in G} \alpha_\sigma \sigma,\ x' =: \sum\limits_{\sigma\in G} \beta_\sigma\sigma$ where $\alpha_\sigma, \beta_\sigma \in \mathfrak{b}$ and $r =: \sum\limits_{\rho\in G} \gamma_\rho\rho$ where $\gamma_\rho \in B$.

We obtain

$$\begin{array}{rclcl} x + x' &=& \sum\limits_{\sigma\in G} \alpha_\sigma\sigma + \sum\limits_{\sigma\in G} \beta_\sigma\sigma &=& \sum\limits_{\sigma\in G} (\alpha_\sigma + \beta_\sigma)\sigma \in \mathfrak{b}(B \wr G) \qquad \text{since } \alpha_\sigma + \beta_\sigma \in \mathfrak{b} \\ xr &=& \sum\limits_{\sigma\in G} \alpha_\sigma\sigma \sum\limits_{\rho\in G} \gamma_\rho\rho &=& \sum\limits_{\sigma\in G}\sum\limits_{\rho\in G} \alpha_\sigma\sigma(\gamma_\rho)\sigma\circ\rho \in \mathfrak{b}(B \wr G) \ \ \text{since } \sigma(\gamma_\rho) \in B,\ \alpha_\sigma\sigma(\gamma_\rho) \in \mathfrak{b}. \end{array}$$

So $\mathfrak{b}(B \wr G) \subseteq B \wr G$ is a right ideal.

Suppose $\mathfrak{b} \in \mathrm{Ideals}^{\times,G}(B)$. In that case

$$rx = \sum_{\rho\in G} \gamma_\rho\rho \sum_{\sigma\in G} \alpha_\sigma\sigma = \sum_{\rho\in G}\sum_{\sigma\in G} \gamma_\rho\rho(\alpha_\sigma)\rho\circ\sigma \in \mathfrak{b}(B \wr G) \text{ since } \rho(\alpha_\sigma) \in \mathfrak{b} \text{ we have } \gamma_\rho\rho(\alpha_\sigma) \in \mathfrak{b}.$$

So $\mathfrak{b}(B \wr G) \subseteq B \wr G$ is an ideal. □

Example 41. The ideal $(2 + \mathrm{i}) \subseteq \mathbf{Z}[\mathrm{i}]$ is not Galois-stable, cf. Example 39.

Indeed $(2 + \mathrm{i})(\mathbf{Z}[\mathrm{i}] \wr G)$ is not an ideal in $\mathbf{Z}[\mathrm{i}] \wr G$:

For $\sigma : \mathrm{i} \mapsto -\mathrm{i}$ and $(2 + \mathrm{i})\sigma \in (2 + \mathrm{i})(\mathbf{Z}[\mathrm{i}] \wr G)$ we obtain

$$\sigma \cdot (2 + \mathrm{i})\sigma = \sigma(2 + \mathrm{i})(\sigma\circ\sigma) = 2 - \mathrm{i} \notin (2 + \mathrm{i})(\mathbf{Z}[\mathrm{i}] \wr G)\ ,$$

since $2 - \mathrm{i} \notin (2 + \mathrm{i})$ because of $(2 - \mathrm{i}) \neq (2 + \mathrm{i})$, cf. Example 39.

Lemma 42. *The map*

$$\begin{array}{rcl} \iota : \mathrm{Ideals}^{\times,G}(B) & \rightarrow & \mathrm{Ideals}^{\times}(B \wr G) \\ \mathfrak{b} & \mapsto & \mathfrak{b}(B \wr G) \end{array}$$

satisfies $\iota(\mathfrak{bc}) = \iota(\mathfrak{b})\iota(\mathfrak{c})$ *for* $\mathfrak{b}, \mathfrak{c} \in \mathrm{Ideals}^{\times,G}(B)$.

Proof. Let $\mathfrak{b}, \mathfrak{c} \in \mathrm{Ideals}^{\times,G}(B)$. Then $\iota(\mathfrak{bc}) = \mathfrak{bc}(B \wr G) \overset{!}{=} \mathfrak{b}(B \wr G)\mathfrak{c}(B \wr G) = \iota(\mathfrak{b})\iota(\mathfrak{c})$.

So we need to show that $\mathfrak{bc}(B \wr G) \overset{!}{=} \mathfrak{b}(B \wr G)\mathfrak{c}(B \wr G)$.

Therefore it suffices to show that $\mathfrak{c}(B \wr G) \overset{!}{=} (B \wr G)\mathfrak{c}(B \wr G)$.

We surely have

$$\mathfrak{c}(B \wr G) \subseteq (B \wr G)\mathfrak{c}(B \wr G)\ .$$

As $\mathfrak{c}$ is Galois-stable, $\mathfrak{c}(B \wr G)$ is an ideal in $B \wr G$ by Lemma 40, and so we also get

$$(B \wr G)\mathfrak{c}(B \wr G) \subseteq B \wr G \ .$$

□

Lemma 43. ([6, I. Proposition (9.1)])
Let $\mathfrak{p} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)$. *The group* G *acts transitively on*

$$\mathrm{Ideals}^{\times}_{\mathrm{prime}}(B, \mathfrak{p}) := \{\mathfrak{q} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(B) : \mathfrak{q} \cap A = \mathfrak{p}\} \ ,$$

the set of all prime ideals of B *lying above* $\mathfrak{p} \subseteq A$, *i.e. these prime ideals are pairwise conjugate.*

Remark 44. Let $\mathfrak{p} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)$. We have the product decomposition

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_m^{e_m}$$

for some $m \in \mathbf{Z}_{>0}$, $\mathfrak{q}_j \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(B)$, $e_j \in \mathbf{Z}_{\geq 1}$ for $j \in [1, m]$. The exponent e_j for $j \in [1, m]$ denotes the ramification index.

By Lemma 43, the prime ideals $\mathfrak{q}_j$ for $j \in [1, m]$ form an orbit. So we have $e_1 = \dots = e_m =: e_{\mathfrak{p}}$. Hence

$$\mathfrak{p} = (\mathfrak{q}_1 \dots \mathfrak{q}_m)^{e_{\mathfrak{p}}} \ .$$

Recall that $e_{\mathfrak{p}} = 1$ if $\Delta_{L|K,\underline{y}} \not\equiv_{\mathfrak{p}} 0$, see e.g. [6, Proposition (8.4)].

We denote $(\mathfrak{p}^{\frac{1}{e_{\mathfrak{p}}}})^k := \mathfrak{p}^{\frac{k}{e_{\mathfrak{p}}}} := (\mathfrak{q}_1 \dots \mathfrak{q}_m)^k$ for $k \in \mathbf{Z}_{\geq 0}$.

Lemma 45. *Let*

$$\begin{array}{rcl} P_{\mathrm{r}} & := & \{\mathfrak{p} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(A) : \Delta_{L|K,\underline{y}} \equiv_{\mathfrak{p}} 0\} \ \textit{and} \\ P_{\mathrm{u}} & := & \{\mathfrak{p} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(A) : \Delta_{L|K,\underline{y}} \not\equiv_{\mathfrak{p}} 0\} \ . \end{array}$$

Suppose given $\mathfrak{b} \in \mathrm{Ideals}^{\times}(B)$. *Then*

$$\mathfrak{b} \in \mathrm{Ideals}^{\times, G}(B)$$

if and only if there exists $\mathfrak{a} \in \mathrm{Ideals}^{\times}(A)$ *with* $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ *for* $\mathfrak{p} \in P_{\mathrm{r}}$ *and* $\varepsilon_{\mathfrak{p}} \in \mathbf{Z}_{\geq 0}$ *for* $\mathfrak{p} \in P_{\mathrm{r}}$, *such that*

$$\mathfrak{b} = \mathfrak{a} \prod_{\mathfrak{p} \in P_{\mathrm{r}}} \mathfrak{p}^{\frac{\varepsilon_{\mathfrak{p}}}{e_{\mathfrak{p}}}} \ .$$

Cf. Remark 44.

Proof. Write

$$\mathfrak{b} = \prod_{\mathfrak{p}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)} \ \prod_{\mathfrak{q}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(B,\mathfrak{p})} \mathfrak{q}^{\alpha_\mathfrak{q}} \ ,$$

where $\alpha_\mathfrak{q} \in \mathbf{Z}_{\geq 0}$, with $\{\mathfrak{q} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(B) : \alpha_\mathfrak{q} \neq 0\}$ finite, cf. Lemma 43.

For $\sigma \in G$, we obtain

$$\begin{array}{rcl} \sigma(\mathfrak{b}) & = & \displaystyle\prod_{\mathfrak{p}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)} \ \prod_{\mathfrak{q}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(B,\mathfrak{p})} \sigma(\mathfrak{q})^{\alpha_\mathfrak{q}} \\ & = & \displaystyle\prod_{\mathfrak{p}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)} \ \prod_{\mathfrak{q}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(B,\mathfrak{p})} \mathfrak{q}^{\alpha_{\sigma^{-1}(\mathfrak{q})}} \ . \end{array}$$

Hence $\mathfrak{b} = \sigma(\mathfrak{b})$ for $\sigma \in G$

$$\begin{array}{rrcl} \Leftrightarrow & \alpha_\mathfrak{q} & = & \alpha_{\sigma(\mathfrak{q})} \text{ for } \sigma \in G \\ \overset{\text{Remark 44}}{\Longleftrightarrow} & \alpha_\mathfrak{q} & = & \alpha_{\tilde{\mathfrak{q}}} \text{ for } \mathfrak{q}, \tilde{\mathfrak{q}} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(B,\mathfrak{p}) \\ \Leftrightarrow & \mathfrak{b} & = & \displaystyle\prod_{\mathfrak{p}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)} \ \prod_{\mathfrak{q}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(B,\mathfrak{p})} \mathfrak{q}^{\varepsilon_\mathfrak{p}} \\ & & = & \displaystyle\prod_{\mathfrak{p}\in\mathrm{Ideals}^{\times}_{\mathrm{prime}}(A)} \mathfrak{p}^{\frac{\varepsilon_\mathfrak{p}}{e_\mathfrak{p}}} \\ & & = & \displaystyle\left(\prod_{\mathfrak{p}\in P_\mathrm{u}} \mathfrak{p}^{\varepsilon_\mathfrak{p}}\right)\left(\prod_{\mathfrak{p}\in P_\mathrm{r}} \mathfrak{p}^{\frac{\varepsilon_\mathfrak{p}}{e_\mathfrak{p}}}\right) \end{array}$$

for some $\varepsilon_\mathfrak{p} \in \mathbf{Z}_{\geq 0}$, with $\{\mathfrak{p} \in \mathrm{Ideals}^{\times}_{\mathrm{prime}}(A) : \varepsilon_\mathfrak{p} \neq 0\}$ finite. □

Lemma 46. *We have the map*

$$\begin{array}{rcl} \psi : \mathrm{Ideals}^{\times}(B \wr G) & \to & \mathrm{Ideals}^{\times,G}(B) \\ I & \mapsto & I \cap B \ . \end{array}$$

Proof. Suppose given $I \in \mathrm{Ideals}^{\times}(B \wr G)$. Then $I \cap B$ is an ideal in B. Moreover, $I \cap B \neq (0)$ by Lemma 8.

It remains to show that $I \cap B$ is Galois-stable.

Suppose given $\sigma \in G$. Then $I = \sigma \cdot I \cdot \sigma^{-1}$.

We *claim* that $\sigma \cdot B = B \cdot \sigma$. Suppose given $b \in B$. Then

$$\begin{array}{ll} Ad(\subseteq). & \sigma \cdot b = \sigma(b) \cdot \sigma \subseteq B \cdot \sigma \\ Ad(\supseteq). & b \cdot \sigma = \sigma \cdot \sigma^{-1}(b) \subseteq \sigma \cdot B \end{array}$$

This proves the *claim.*

Thus

$$I \cap B = \sigma \cdot I \cdot \sigma^{-1} \cap B = \sigma \cdot I \cdot \sigma^{-1} \cap \sigma \cdot B \cdot \sigma^{-1} = \sigma \cdot (I \cap B) \cdot \sigma^{-1} \ .$$

We obtain for $x \in I \cap B$ that

$$\sigma(x) = \sigma(x) \cdot \sigma \circ \sigma^{-1} = \sigma \cdot x \cdot \sigma^{-1} \in \sigma \cdot (I \cap B) \cdot \sigma^{-1} = I \cap B \ .$$

□

Remark 47. Suppose given a Galois-stable ideal $\mathfrak{b} \subseteq B$. Then $\psi \circ \iota(\mathfrak{b}) = \mathfrak{b}$, cf. Lemma 42, Lemma 46. In particular, ι is injective.

Proof. We have

$$\begin{array}{rcl} \psi \circ \iota(\mathfrak{b}) & = & \psi(\mathfrak{b}(B \wr G)) = B \cap (\mathfrak{b}(B \wr G)) \\ & = & B \cap \{ \sum\limits_{\sigma \in G} \alpha_\sigma \sigma : \alpha_\sigma \in \mathfrak{b} \} \\ & = & \{ \sum\limits_{\sigma \in G} \alpha_\sigma \sigma : \alpha_\sigma = 0 \text{ for } \sigma \in G \backslash \{\mathrm{id}\} \} \\ & = & \mathfrak{b} \ . \end{array}$$

□

Remark 48. *Suppose that $A = \mathbf{Z}$. Let $\mathfrak{d} \in \mathrm{Ideals}^{\times, G}(\mathcal{O}_L)$. Then*

$$[(\mathcal{O}_L \wr G) : \mathfrak{d}(\mathcal{O}_L \wr G)] = [\mathcal{O}_L : \mathfrak{d}]^{|G|} \ .$$

In particular, the index of $\mathfrak{d}(\mathcal{O}_L \wr G)$ in $\mathcal{O}_L \wr G$ is a $|G|$-th power of a natural number.

Proof. We have $\bigoplus\limits_{\sigma \in G} \mathfrak{d}\sigma = \mathfrak{d}(\mathcal{O}_L \wr G) \subseteq \mathcal{O}_L \wr G = \bigoplus\limits_{\sigma \in G} \mathcal{O}_L \sigma$ and therefore

$$(\mathcal{O}_L \wr G)/\mathfrak{d}(\mathcal{O}_L \wr G) \cong \bigoplus_{\sigma \in G} (\mathcal{O}_L \sigma / \mathfrak{d}\sigma) \cong (\mathcal{O}_L/\mathfrak{d})^{\bigoplus |G|} \ .$$

So the index $|(\mathcal{O}_L \wr G)/\mathfrak{d}(\mathcal{O}_L \wr G)| = |\mathcal{O}_L/\mathfrak{d}|^{|G|}$ is a $|G|$-th power. □

7.2 Ideals in case of quadratic extensions $\mathbf{Q}(\sqrt{d})|\mathbf{Q}$

In the following we aim to show that ι is not surjective. Therefore we first try to determine $\mathrm{Ideals}(\Lambda)$.

Let $d \in \mathbf{Z}^\times$ be squarefree.

7.2.1 Ideals in $\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\frac{1+\sqrt{d}}{2}] \wr G)$ for $d \equiv_4 1$

Suppose that $d \equiv_4 1$.

Lemma 49. *Let $p \in \mathbf{Z}_{>0}$ be a prime and $R := \mathbf{Z}_{(p)}$. Let $R' := \left(\begin{smallmatrix} R & R \\ R & R \end{smallmatrix}\right)$. Then*

$$\mathrm{Ideals}^{\times}(R') = \{p^k R' : k \in \mathbf{Z}_{\geq 0}\} \ .$$

Proof. It suffices to show the inclusion ($\subseteq$).

Let $I \subseteq R'$ be a non-zero ideal.

For $a, b, c, e \in R$ define $\mathrm{v}_p(\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right)) := \min\{\mathrm{v}_p(a), \mathrm{v}_p(b), \mathrm{v}_p(c), \mathrm{v}_p(e)\}$.

Since $I \neq (0)$ there exists an element $X \in I$ satisfying $\mathrm{v}_p(X) \neq +\infty$. Choose $X_0 = \left(\begin{smallmatrix} a_0 & b_0 \\ c_0 & e_0 \end{smallmatrix}\right) \in I$ such that $k := \mathrm{v}_p(X_0) \in \mathbf{Z}_{\geq 0}$ is minimal.

As $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in R'$ we can assume without loss of generality that $\mathrm{v}_p(X_0) = \mathrm{v}_p(a_0)$, by using permutation of rows and columns. We obtain

$$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} a_0 & b_0 \\ c_0 & e_0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I \ .$$

Since $a_0 = p^k u$ for some $u \in \mathrm{U}(R)$, it follows that $p^k \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I$.

Moreover,

$$\begin{array}{rcl} p^k \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) & = & p^k \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in I \\ p^k \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) & = & p^k \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in I \\ p^k \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) & = & p^k \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in I \quad . \end{array}$$

This shows $p^k R' \subseteq I$.

Suppose given $X = \left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) \in I$. Then we have $\mathrm{v}_p(X) \geq k$ and therefore $\mathrm{v}_p(a) \geq k$, $\mathrm{v}_p(b) \geq k$, $\mathrm{v}_p(c) \geq k$, $\mathrm{v}_p(e) \geq k$. Hence a, b, c, e are divisible by p^k in R and consequently $\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) \in p^k R'$.

This shows $I \subseteq p^k R'$.

So $I = p^k R'$.

Taken as a whole we have $\mathrm{Ideals}^{\times}(R') = \{p^k R' : k \in \mathbf{Z}_{\geq 0}\}$. □

Lemma 50. *Let $p \in \mathbf{Z}_{>0}$ be a prime and $R := \mathbf{Z}_{(p)}$. Consider the subring $R' := \left(\begin{smallmatrix} R & (p) \\ R & R \end{smallmatrix}\right) \subseteq \left(\begin{smallmatrix} R & R \\ R & R \end{smallmatrix}\right)$. Let $I \in \mathrm{Ideals}^{\times}(R')$.*

(1) *Suppose that $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in I$, where $a, b, c, e \in R$ and $a \not\equiv_p 0$, then $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I$.*

(2) *Suppose that $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in I$, where $a, b, c, e \in R$ and $b \not\equiv_p 0$, then $\left(\begin{smallmatrix} 0 & p \\ 0 & 0 \end{smallmatrix}\right) \in I$.*

(3) *Suppose that $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in I$, where $a, b, c, e \in R$ and $c \not\equiv_p 0$, then $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in I$.*

(4) *Suppose that $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in I$, where $a, b, c, e \in R$ and $e \not\equiv_p 0$, then $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in I$.*

Proof.

(1) Suppose that $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in I$, where $a, b, c, e \in R$ and $a \not\equiv_p 0$. Then $a \in \mathrm{U}(R)$ and we obtain

$$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I \overset{a\in \mathrm{U}(R)}{\rightsquigarrow} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I \ .$$

(2) Suppose that $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in I$, where $a, b, c, e \in R$ and $b \not\equiv_p 0$. Then $b \in \mathrm{U}(R)$ and we obtain

$$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & pb \\ 0 & 0 \end{smallmatrix}\right) \in I \overset{b\in \mathrm{U}(R)}{\rightsquigarrow} \left(\begin{smallmatrix} 0 & p \\ 0 & 0 \end{smallmatrix}\right) \in I \ .$$

(3) Suppose that $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in I$, where $a, b, c, e \in R$ and $c \not\equiv_p 0$. Then $c \in \mathrm{U}(R)$ and we obtain

$$\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ c & 0 \end{smallmatrix}\right) \in I \overset{c\in \mathrm{U}(R)}{\rightsquigarrow} \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in I \ .$$

(4) Suppose that $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in I$, where $a, b, c, e \in R$ and $e \not\equiv_p 0$. Then $e \in \mathrm{U}(R)$ and we obtain

$$\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & e \end{smallmatrix}\right) \in I \overset{e\in \mathrm{U}(R)}{\rightsquigarrow} \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in I \ .$$

□

Lemma 51. *Let $p \in \mathbf{Z}_{>0}$ be a prime and $R := \mathbf{Z}_{(p)}$. Consider the subring $R' := \left(\begin{smallmatrix} R & (p) \\ R & R \end{smallmatrix}\right) \subseteq \left(\begin{smallmatrix} R & R \\ R & R \end{smallmatrix}\right)$. Then*

$$\mathrm{Ideals}^{\times}(R') = \{p^k \left(\begin{smallmatrix} R & (p) \\ R & R \end{smallmatrix}\right),\ p^k \left(\begin{smallmatrix} (p) & (p) \\ R & R \end{smallmatrix}\right),\ p^k \left(\begin{smallmatrix} (p) & (p) \\ (p) & (p) \end{smallmatrix}\right),\ p^k \left(\begin{smallmatrix} R & (p) \\ R & (p) \end{smallmatrix}\right),\ p^k \left(\begin{smallmatrix} (p) & (p) \\ R & (p) \end{smallmatrix}\right),\ p^k \left(\begin{smallmatrix} (p) & (p^2) \\ R & (p) \end{smallmatrix}\right) : k \in \mathbf{Z}_{\geq 0}\} \ .$$

Proof. It suffices to show the inclusion ($\subseteq$).

Let $I \subseteq R'$ be a non-zero ideal.

Let $k \in \mathbf{Z}_{\geq 0}$ be maximal such that $p^{-k}I \subseteq R'$. Then $J := p^{-k}I$ is an ideal in R'.

We may choose an element $\left(\begin{smallmatrix} a & pb \\ c & e \end{smallmatrix}\right) \in J$ where $a \not\equiv_p 0 \vee b \not\equiv_p 0 \vee c \not\equiv_p 0 \vee e \not\equiv_p 0$.

Case 1: $a \not\equiv_p 0$.

By Lemma 50, we obtain that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in J$. Moreover, it follows that

$$\begin{aligned} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & p \\ 0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & p \\ 0 & 0 \end{smallmatrix}\right) \in J \\ \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in J \\ \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & p \\ 0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & p \end{smallmatrix}\right) \in J \ . \end{aligned}$$

So we have $\left(\begin{smallmatrix} R & (p) \\ R & (p) \end{smallmatrix}\right) \subseteq J \subseteq R'$.

Subcase 1.1 We have $J = \left(\begin{smallmatrix} R & (p) \\ R & (p) \end{smallmatrix}\right)$ if for every $\left(\begin{smallmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{smallmatrix}\right) \in J$ the element $\tilde{e}$ is divisible by p.

Subcase 1.2 If there exists an element $\left(\begin{smallmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{smallmatrix}\right) \in J$ such that $\tilde{e} \not\equiv_p 0$, then it follows by Lemma 50 that $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in J$. Since $\left(\begin{smallmatrix} R & (p) \\ R & (p) \end{smallmatrix}\right) \subseteq J$ we obtain $R' = \left(\begin{smallmatrix} R & (p) \\ R & R \end{smallmatrix}\right) \subseteq J \subseteq R'$. So $J = R'$.

Case 2: $b \not\equiv_p 0$.

By Lemma 50 we obtain that $\left(\begin{smallmatrix} 0 & p \\ 0 & 0 \end{smallmatrix}\right) \in J$. Moreover, it follows that

$$\begin{aligned}
\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & p \\ 0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & p \end{smallmatrix}\right) \in J \\
\left(\begin{smallmatrix} 0 & p \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} p & 0 \\ 0 & 0 \end{smallmatrix}\right) \in J \\
\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ p & 0 \end{smallmatrix}\right) \in J\ .
\end{aligned}$$

So we have $\left(\begin{smallmatrix} (p) & (p) \\ (p) & (p) \end{smallmatrix}\right) \subseteq J \subseteq R'$.

Subcase 2.1 We have $J = \left(\begin{smallmatrix} (p) & (p) \\ (p) & (p) \end{smallmatrix}\right)$ if for every $\left(\begin{smallmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{smallmatrix}\right) \in J$ the elements $\tilde{a}, \tilde{c}, \tilde{e}$ are divisible by p.

Subcase 2.2 If there is no element $\left(\begin{smallmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{smallmatrix}\right) \in J$ such that $\tilde{a} \not\equiv_p 0$ or $\tilde{e} \not\equiv_p 0$, but an element $\left(\begin{smallmatrix} \tilde{a}' & p\tilde{b}' \\ \tilde{c}' & \tilde{e}' \end{smallmatrix}\right) \in J$ such that $\tilde{c}' \not\equiv_p 0$, then it follows by Lemma 50 that $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in J$.

Hence $J = \left(\begin{smallmatrix} (p) & (p) \\ R & (p) \end{smallmatrix}\right)$.

Subcase 2.3 If there exists an element $\left(\begin{smallmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{smallmatrix}\right) \in J$ such that $\tilde{a} \not\equiv_p 0$ and an element $\left(\begin{smallmatrix} \tilde{a}' & p\tilde{b}' \\ \tilde{c}' & \tilde{e}' \end{smallmatrix}\right) \in J$ such that $\tilde{e}' \not\equiv_p 0$, then we have by Lemma 50 that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in J$ and that $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in J$. Besides, $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in J$. Since $\left(\begin{smallmatrix} (p) & (p) \\ (p) & (p) \end{smallmatrix}\right) \subseteq J$ we obtain $J = R'$.

Subcase 2.4 If there exists an element $\left(\begin{smallmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{smallmatrix}\right) \in J$ such that $\tilde{a} \not\equiv_p 0$, but no element $\left(\begin{smallmatrix} \tilde{a}' & p\tilde{b}' \\ \tilde{c}' & \tilde{e}' \end{smallmatrix}\right) \in J$ such that $\tilde{e}' \not\equiv_p 0$, then we have by Lemma 50 that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in J$. Therefore it follows that $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in J$.

Hence $J = \left(\begin{smallmatrix} R & (p) \\ R & (p) \end{smallmatrix}\right)$.

Subcase 2.5 If there exists an element $\left(\begin{smallmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{smallmatrix}\right) \in J$ such that $\tilde{e} \not\equiv_p 0$, but no element $\left(\begin{smallmatrix} \tilde{a}' & p\tilde{b}' \\ \tilde{c}' & \tilde{e}' \end{smallmatrix}\right) \in J$ such that $\tilde{a}' \not\equiv_p 0$, then it follows by Lemma 50 that $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in J$. Therefore it follows that $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in J$.
Hence $J = \left(\begin{smallmatrix} (p) & (p) \\ R & R \end{smallmatrix}\right)$.

Case 3: $c \not\equiv_p 0$.

By Lemma 50, we obtain that $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) \in J$. Moreover,

$$\begin{aligned}
\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) &= \left(\begin{smallmatrix}0&0\\0&p\end{smallmatrix}\right) &\in J\\
\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) &= \left(\begin{smallmatrix}p&0\\0&0\end{smallmatrix}\right) &\in J\\
\left(\begin{smallmatrix}p&0\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) &= \begin{pmatrix}0&p^2\\0&0\end{pmatrix} &\in J\ .
\end{aligned}$$

So it follows that$\begin{pmatrix}(p)&(p^2)\\R&(p)\end{pmatrix} \subseteq J \subseteq R'$.

Subcase 3.1 We have $J = \begin{pmatrix}(p)&(p^2)\\R&(p)\end{pmatrix}$ if for every $\begin{pmatrix}\tilde{a}&p\tilde{b}\\\tilde{c}&\tilde{e}\end{pmatrix} \in J$ the elements $\tilde{a}, \tilde{b}, \tilde{e}$ are divisible by p.

Subcase 3.2 If there is no element $\begin{pmatrix}\tilde{a}&p\tilde{b}\\\tilde{c}&\tilde{e}\end{pmatrix} \in J$ such that $\tilde{a} \not\equiv_p 0$ or $\tilde{e} \not\equiv_p 0$, but an element $\begin{pmatrix}\tilde{a}'&p\tilde{b}'\\\tilde{c}'&\tilde{e}'\end{pmatrix} \in J$ such that $\tilde{b}' \not\equiv_p 0$, then it follows by Lemma 50 that $\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) \in J$.
Because of $\begin{pmatrix}(p)&(p^2)\\R&(p)\end{pmatrix} \subseteq J$ this leads to $J = \begin{pmatrix}(p)&(p)\\R&(p)\end{pmatrix}$.

Subcase 3.3 If there exists an element $\begin{pmatrix}\tilde{a}&p\tilde{b}\\\tilde{c}&\tilde{e}\end{pmatrix} \in J$ such that $\tilde{a} \not\equiv_p 0$ and an element $\begin{pmatrix}\tilde{a}'&p\tilde{b}'\\\tilde{c}'&\tilde{e}'\end{pmatrix} \in J$ such that $\tilde{e}' \not\equiv_p 0$, then we have by Lemma 50 that $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) \in J$ and that $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right) \in J$. Besides, $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) \in J$.

Since $\begin{pmatrix}(p)&(p^2)\\R&(p)\end{pmatrix} \subseteq J$ we obtain $J = R'$.

Subcase 3.4 If there exists an element $\begin{pmatrix}\tilde{a}&p\tilde{b}\\\tilde{c}&\tilde{e}\end{pmatrix} \in J$ such that $\tilde{a} \not\equiv_p 0$, but no element $\begin{pmatrix}\tilde{a}'&p\tilde{b}'\\\tilde{c}'&\tilde{e}'\end{pmatrix} \in J$ such that $\tilde{e}' \not\equiv_p 0$, then we obtain by Lemma 50 that $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) \in J$. Therefore it follows that $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) \in J$.

Because of $\begin{pmatrix}(p)&(p^2)\\R&(p)\end{pmatrix} \subseteq J$ this leads to $J = \begin{pmatrix}R&(p)\\R&(p)\end{pmatrix}$.

Subcase 3.5 If there exists an element $\begin{pmatrix}\tilde{a}&p\tilde{b}\\\tilde{c}&\tilde{e}\end{pmatrix} \in J$ such that $\tilde{e} \not\equiv_p 0$, but no element $\begin{pmatrix}\tilde{a}'&p\tilde{b}'\\\tilde{c}'&\tilde{e}'\end{pmatrix} \in J$ such that $\tilde{a}' \not\equiv_p 0$, then it follows by Lemma 50 that $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right) \in J$. Besides, $\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) \in J$.

Because of $\begin{pmatrix}(p)&(p^2)\\R&(p)\end{pmatrix} \subseteq J$ this leads to $J = \left(\begin{smallmatrix}(p)&(p)\\R&R\end{smallmatrix}\right)$.

Case 4: $e \not\equiv_p 0$.

By Lemma 50, we obtain that $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right) \in J$. Moreover,

$$\begin{aligned}
\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) &= \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) \in J\\
\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right) &= \left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right) \in J\\
\left(\begin{smallmatrix}0&p\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) &= \left(\begin{smallmatrix}p&0\\0&0\end{smallmatrix}\right) \in J\ .
\end{aligned}$$

So we have $\left(\begin{smallmatrix} (p) & (p) \\ R & R \end{smallmatrix}\right) \subseteq J \subseteq R'$.

Subcase 4.1 We have $J = \left(\begin{smallmatrix} (p) & (p) \\ R & R \end{smallmatrix}\right)$ if for every $\begin{pmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{pmatrix} \in J$ the element $\tilde{a}$ is divisible by p.

Subcase 4.2 If there exists an element $\begin{pmatrix} \tilde{a} & p\tilde{b} \\ \tilde{c} & \tilde{e} \end{pmatrix} \in J$ such that $\tilde{a} \not\equiv_p 0$, then we have by Lemma 50 that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in J$. Since $\left(\begin{smallmatrix} (p) & (p) \\ R & R \end{smallmatrix}\right) \subseteq J$ we obtain $J = R'$.

Taken as a whole we obtain

$$\mathrm{Ideals}^{\times}(R') = \{p^k \begin{pmatrix} (p) & (p^2) \\ R & (p) \end{pmatrix},\ p^k \left(\begin{smallmatrix} (p) & (p) \\ R & R \end{smallmatrix}\right),\ p^k \begin{pmatrix} (p) & (p) \\ (p) & (p) \end{pmatrix},\ p^k \begin{pmatrix} R & (p) \\ R & (p) \end{pmatrix},\ p^k \begin{pmatrix} (p) & (p) \\ R & (p) \end{pmatrix},\ p^k \left(\begin{smallmatrix} R & (p) \\ R & R \end{smallmatrix}\right) : k \in \mathbf{Z}_{\geq 0}\} .$$

□

Remark 52. Recall that d is squarefree and that $d \equiv_4 1$. Let $p \in \mathbf{Z}_{>0}$ be a prime. Let $R = \mathbf{Z}_{(p)}$. Let $\underline{y}$ be as in Proposition 22.

In case of $d \equiv_p 0$, the R-algebra $R' := \left(\begin{smallmatrix} R & (p) \\ R & R \end{smallmatrix}\right)$ is isomorphic to $R[\frac{1+\sqrt{d}}{2}] \wr \mathrm{C}_2$ via $\omega_{\underline{y}}^{R}$, cf. Proposition 22.

In case of $d \not\equiv_p 0$, the R-algebra $R' := \left(\begin{smallmatrix} R & R \\ R & R \end{smallmatrix}\right)$ is isomorphic to $R[\frac{1+\sqrt{d}}{2}] \wr \mathrm{C}_2$ via $\omega_{\underline{y}}^{R}$, cf. Proposition 22.

We now obtain the ideals in $\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\frac{1+\sqrt{d}}{2}] \wr G)$ with the help of

Lemma 53. *Let M be a $\mathbf{Z}$-order and $J \subseteq M$ be an ideal. Then*

$$J = \bigcap_{p \text{ prime}} J_{(p)} \ .$$

Proof. It suffices to show the inclusion $(\supseteq)$. Suppose given $x \in M$ such that $x \in J_{(p)}$ for all primes p. We need to show that $x \overset{!}{\in} J$.

Assume that $x \notin J$. Let $\mathfrak{a} := \{a \in \mathbf{Z} : ax \in J\}$. Then $\mathfrak{a}$ is an ideal in $\mathbf{Z}$ as $0 \in \mathfrak{a}$ and as $(za + z'a')x = z(ax) + z'(a'x) \in J$ and thus $za + z'a' \in \mathfrak{a}$ for $z, z' \in \mathbf{Z}$, $a, a' \in \mathfrak{a}$.

Suppose given a prime p.

Since $x \in J_{(p)}$, there exists $y \in J$ and $s \in \mathbf{Z} \setminus (p)$ such that $x = \frac{y}{s}$. Hence $sx = y \in J$, i.e. $s \in \mathfrak{a}$. Therefore $\mathfrak{a} \not\subseteq (p)$.

So $\mathfrak{a}$ is not contained in a maximal ideal of $\mathbf{Z}$, whence $\mathfrak{a} = \mathbf{Z}$. In particular, $1 \in \mathfrak{a}$, i.e. $1 \cdot x \in J$, which is a *contradiction.* □

Remark 54. Let $m \in \mathbf{Z}_{\geq 1}$. Let $p_1, \ldots, p_m \in \mathbf{Z}_{>0}$ be prime. Let $l_i \in \mathbf{Z}_{\geq 0}$ for $i \in [1, m]$. Write $t_i := p_i^{l_i}$ for $i \in [1, m]$ and $t := \prod_{i \in [1,m]} t_i$. Let s be coprime to $p_1, \ldots, p_m$. We have

$$\begin{array}{cl} & t_1\mathbf{Z}_{(p_1)} \cap \cdots \cap t_m\mathbf{Z}_{(p_m)} \cap s\mathbf{Z} \\ \overset{\text{Lemma 53}}{=} & t_1\mathbf{Z}_{(p_1)} \cap \cdots \cap t_m\mathbf{Z}_{(p_m)} \cap \bigcap_{p \text{ prime}} s\mathbf{Z}_{(p)} \\ = & t_1\mathbf{Z}_{(p_1)} \cap \cdots \cap t_m\mathbf{Z}_{(p_m)} \cap s\mathbf{Z}_{(p_1)} \cap \cdots \cap s\mathbf{Z}_{(p_m)} \cap \bigcap_{p \text{ prime},\ p \notin \{p_1,\ldots,p_m\}} s\mathbf{Z}_{(p)} \\ = & st_1\mathbf{Z}_{(p_1)} \cap \cdots \cap st_m\mathbf{Z}_{(p_m)} \cap \bigcap_{p \text{ prime},\ p \notin \{p_1,\ldots,p_m\}} s\mathbf{Z}_{(p)} \\ = & st\mathbf{Z}_{(p_1)} \cap \cdots \cap st\mathbf{Z}_{(p_m)} \cap \bigcap_{p \text{ prime},\ p \notin \{p_1,\ldots,p_m\}} st\mathbf{Z}_{(p)} \\ = & st(\bigcap_{p \text{ prime}} \mathbf{Z}_{(p)}) = st\mathbf{Z}\ . \end{array}$$

Proposition 55. *Let $L = \mathbf{Q}(\sqrt{-15})$ and $K = \mathbf{Q}$. Let $A = \mathbf{Z}$. Write $\alpha := \frac{1+\sqrt{-15}}{2}$. Then $B = \mathcal{O}_L = \mathbf{Z}[\alpha]$. The Galois group is given by $G = \{\mathrm{id}, \sqrt{-15} \overset{\sigma}{\mapsto} -\sqrt{-15}\}$.*

Consider the $\mathbf{Z}$-linear basis $\underline{y} = (1, \alpha + 7)$ of $\mathbf{Z}[\alpha]$. By Proposition 22 *we obtain that*

$$\Lambda := \omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\alpha] \wr G) = \left(\begin{smallmatrix} \mathbf{Z} & (15) \\ \mathbf{Z} & \mathbf{Z} \end{smallmatrix}\right)\ .$$

Then the map ι : $\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha]) \to \mathrm{Ideals}^{\times}(\mathbf{Z}[\alpha] \wr G)$ is not surjective, cf. Lemma 40, Remark 47.

More specifically we have

$$\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha]))\right) = \{z\Lambda,\ z\begin{pmatrix} (15) & (15) \\ \mathbf{Z} & (15) \end{pmatrix},\ z\begin{pmatrix} (5) & (15) \\ \mathbf{Z} & (5) \end{pmatrix},\ z\begin{pmatrix} (3) & (15) \\ \mathbf{Z} & (3) \end{pmatrix} : z \in \mathbf{Z}^{\times}\}$$

and therein

$$\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathrm{Ideals}^{\times,G}_{\mathrm{principal}}(\mathbf{Z}[\alpha]))\right) = \{z\Lambda,\ z\begin{pmatrix} (15) & (15) \\ \mathbf{Z} & (15) \end{pmatrix} : z \in \mathbf{Z}^{\times}\}$$

and both are proper subfields of $\omega_{\underline{y}}^{\mathbf{Z}}(\mathrm{Ideals}^{\times}(\mathbf{Z}[\alpha] \wr G)) = \mathrm{Ideals}^{\times}(\Lambda)$, listed in $(\star)$ below.

Proof. First we determine $\mathrm{Ideals}^{\times}(\Lambda)$.

Let $p \in \mathbf{Z}_{>0}$ be a prime.

Case $p \notin \{3, 5\}$. Then we have $\Lambda_{(p)} = \begin{pmatrix} \mathbf{Z}_{(p)} & \mathbf{Z}_{(p)} \\ \mathbf{Z}_{(p)} & \mathbf{Z}_{(p)} \end{pmatrix}$ since 15 is a unit in $\mathbf{Z}_{(p)}$. By Lemma 49 we have

$$\mathrm{Ideals}^{\times}(\Lambda_{(p)}) = \{p^k\Lambda_{(p)} : k \in \mathbf{Z}_{\geq 0}\}\ .$$

Case $p = 3$. Then $\Lambda_{(3)} = \begin{pmatrix} \mathbf{Z}_{(3)} & (3) \\ \mathbf{Z}_{(3)} & \mathbf{Z}_{(3)} \end{pmatrix}$ since 5 is a unit in $\mathbf{Z}_{(3)}$. By Lemma 51 we have

$$\mathrm{Ideals}^{\times}(\Lambda_{(3)}) =$$
$$\{3^k \underbrace{\begin{pmatrix} \mathbf{Z}_{(3)} & (3) \\ \mathbf{Z}_{(3)} & \mathbf{Z}_{(3)} \end{pmatrix}}_{=:J_1},\ 3^k \underbrace{\begin{pmatrix} (3) & (3) \\ \mathbf{Z}_{(3)} & \mathbf{Z}_{(3)} \end{pmatrix}}_{=:J_2},\ 3^k \underbrace{\begin{pmatrix} (3) & (3) \\ (3) & (3) \end{pmatrix}}_{=:J_3},\ 3^k \underbrace{\begin{pmatrix} \mathbf{Z}_{(3)} & (3) \\ \mathbf{Z}_{(3)} & (3) \end{pmatrix}}_{=:J_4},\ 3^k \underbrace{\begin{pmatrix} (3) & (3) \\ \mathbf{Z}_{(3)} & (3) \end{pmatrix}}_{=:J_5},\ 3^k \underbrace{\begin{pmatrix} (3) & (3^2) \\ \mathbf{Z}_{(3)} & (3) \end{pmatrix}}_{=:J_6} : k \in \mathbf{Z}_{\geq 0}\}\ .$$

Case $p = 5$. Then $\Lambda_{(5)} = \left(\begin{smallmatrix} \mathbf{Z}_{(5)} & (5) \\ \mathbf{Z}_{(5)} & \mathbf{Z}_{(5)} \end{smallmatrix}\right)$ since 3 is a unit in $\mathbf{Z}_{(5)}$. By Lemma 51 we have

$$\begin{aligned}&\mathrm{Ideals}^{\times}(\Lambda_{(5)}) = \\ &\{5^k \underbrace{\left(\begin{smallmatrix} \mathbf{Z}_{(5)} & (5) \\ \mathbf{Z}_{(5)} & \mathbf{Z}_{(5)} \end{smallmatrix}\right)}_{=:I_1},\ 5^k \underbrace{\left(\begin{smallmatrix} (5) & (5) \\ \mathbf{Z}_{(5)} & \mathbf{Z}_{(5)} \end{smallmatrix}\right)}_{=:I_2},\ 5^k \underbrace{\left(\begin{smallmatrix} (5) & (5) \\ (5) & (5) \end{smallmatrix}\right)}_{=:I_3},\ 5^k \underbrace{\left(\begin{smallmatrix} \mathbf{Z}_{(5)} & (5) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right)}_{=:I_4},\ 5^k \underbrace{\left(\begin{smallmatrix} (5) & (5) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right)}_{=:I_5},\ 5^k \underbrace{\left(\begin{smallmatrix} (5) & (5^2) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right)}_{=:I_6} : k \in \mathbf{Z}_{\geq 0}\} \ .\end{aligned}$$

We *claim* that

$$\mathrm{Ideals}^{\times}(\Lambda) \overset{!}{=} \{5^k I_a \cap 3^l J_b \cap c\mathbf{Z}^{2\times 2} : a \in [1,6],\ b \in [1,6],\ k,l \in \mathbf{Z}_{\geq 0},\ c \in \mathbf{Z}_{>0},\ c \not\equiv_3 0,\ c \not\equiv_5 0\} \ .$$

We only need to show $(\subseteq)$.

Suppose given $M \in \mathrm{Ideals}^{\times}(\Lambda)$. We have

$$M \overset{\text{Lemma 53}}{=} \bigcap_{p \text{ prime}} M_{(p)} = M_{(5)} \cap M_{(3)} \cap \bigcap_{p \text{ prime},\ p \notin \{3,5\}} M_{(p)} \ .$$

For $p \notin \{3,5\}$ we have $\Lambda_{(p)} = \mathbf{Z}_{(p)}^{2\times 2}$ and $M_{(p)} = p^{\alpha_p}\mathbf{Z}_{(p)}^{2\times 2}$, where $\alpha_p \in \mathbf{Z}_{\geq 0}$ and $\alpha_p = 0$ for all but finitely many p.

Write $M_{(5)} = 5^k I_a$ and $M_{(3)} = 3^l J_b$ for some $a \in [1,6]$, $b \in [1,6]$, $k,l \in \mathbf{Z}_{\geq 0}$. Then

$$M = 5^k I_a \cap 3^l J_b \cap \bigcap_{p \text{ prime},\ p \notin \{3,5\}} p^{\alpha_p}\mathbf{Z}_{(p)}^{2\times 2} \ .$$

Define $c := \prod_{q \text{ prime},\ q \notin \{3,5\}} q^{\alpha_q}$. We obtain for $p \notin \{3,5\}$ that

$$\begin{aligned} c\mathbf{Z}_{(p)}^{2\times 2} &= p^{\alpha_p}\mathbf{Z}_{(p)}^{2\times 2} \\ 5^k I_a &\subseteq \mathbf{Z}_{(5)}^{2\times 2} = c\mathbf{Z}_{(5)}^{2\times 2} \\ 3^l J_b &\subseteq \mathbf{Z}_{(3)}^{2\times 2} = c\mathbf{Z}_{(3)}^{2\times 2} \ . \end{aligned}$$

So

$$\begin{aligned} M &= 5^k I_a \cap 3^l J_b \cap \bigcap_{p \text{ prime},\ p \notin \{3,5\}} c\mathbf{Z}_{(p)}^{2\times 2} \\ &= 5^k I_a \cap c\mathbf{Z}_{(5)}^{2\times 2} \cap 3^l J_b \cap c\mathbf{Z}_{(3)}^{2\times 2} \cap \bigcap_{p \text{ prime},\ p \notin \{3,5\}} c\mathbf{Z}_{(p)}^{2\times 2} \\ &= 5^k I_a \cap 3^l J_b \cap \bigcap_{p \text{ prime}} c\mathbf{Z}_{(p)}^{2\times 2} \\ &= 5^k I_a \cap 3^l J_b \cap c(\bigcap_{p \text{ prime}} \mathbf{Z}_{(p)}^{2\times 2}) \\ &= 5^k I_a \cap 3^l J_b \cap c(\bigcap_{p \text{ prime}} \mathbf{Z}_{(p)})^{2\times 2} \\ &= 5^k I_a \cap 3^l J_b \cap c\mathbf{Z}^{2\times 2} \ . \end{aligned}$$

This proves the *claim.*

By Remark 54 we obtain

$(\star)$

$$\mathrm{Ideals}^\times(\Lambda) = \left\{ \begin{array}{l}
z\begin{pmatrix} \mathbf{Z} & (15) \\ \mathbf{Z} & \mathbf{Z} \end{pmatrix},\ z\begin{pmatrix} (5) & (15) \\ \mathbf{Z} & \mathbf{Z} \end{pmatrix},\ z\begin{pmatrix} (5) & (15) \\ (5) & (5) \end{pmatrix},\ z\begin{pmatrix} \mathbf{Z} & (15) \\ \mathbf{Z} & (5) \end{pmatrix},\ z\begin{pmatrix} (5) & (15) \\ \mathbf{Z} & (5) \end{pmatrix},\ z\begin{pmatrix} (5) & (75) \\ \mathbf{Z} & (5) \end{pmatrix}, \\
z\begin{pmatrix} (3) & (15) \\ \mathbf{Z} & \mathbf{Z} \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ \mathbf{Z} & \mathbf{Z} \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ (5) & (5) \end{pmatrix},\ z\begin{pmatrix} (3) & (15) \\ \mathbf{Z} & (5) \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ \mathbf{Z} & (5) \end{pmatrix},\ z\begin{pmatrix} (15) & (75) \\ \mathbf{Z} & (5) \end{pmatrix}, \\
z\begin{pmatrix} (3) & (15) \\ (3) & (3) \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ (3) & (3) \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ (15) & (15) \end{pmatrix},\ z\begin{pmatrix} (3) & (15) \\ (3) & (15) \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ (3) & (15) \end{pmatrix},\ z\begin{pmatrix} (15) & (75) \\ (3) & (15) \end{pmatrix}, \\
z\begin{pmatrix} \mathbf{Z} & (15) \\ \mathbf{Z} & (3) \end{pmatrix},\ z\begin{pmatrix} (5) & (15) \\ \mathbf{Z} & (3) \end{pmatrix},\ z\begin{pmatrix} (5) & (15) \\ (5) & (15) \end{pmatrix},\ z\begin{pmatrix} \mathbf{Z} & (15) \\ \mathbf{Z} & (15) \end{pmatrix},\ z\begin{pmatrix} (5) & (15) \\ \mathbf{Z} & (15) \end{pmatrix},\ z\begin{pmatrix} (5) & (75) \\ \mathbf{Z} & (15) \end{pmatrix}, \\
z\begin{pmatrix} (3) & (15) \\ \mathbf{Z} & (3) \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ \mathbf{Z} & (3) \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ (5) & (15) \end{pmatrix},\ z\begin{pmatrix} (3) & (15) \\ \mathbf{Z} & (15) \end{pmatrix},\ z\begin{pmatrix} (15) & (15) \\ \mathbf{Z} & (15) \end{pmatrix},\ z\begin{pmatrix} (15) & (75) \\ \mathbf{Z} & (15) \end{pmatrix}, \\
z\begin{pmatrix} (3) & (45) \\ \mathbf{Z} & (3) \end{pmatrix},\ z\begin{pmatrix} (15) & (45) \\ \mathbf{Z} & (3) \end{pmatrix},\ z\begin{pmatrix} (15) & (45) \\ (5) & (15) \end{pmatrix},\ z\begin{pmatrix} (3) & (45) \\ \mathbf{Z} & (15) \end{pmatrix},\ z\begin{pmatrix} (15) & (45) \\ \mathbf{Z} & (15) \end{pmatrix},\ z\begin{pmatrix} (15) & (225) \\ \mathbf{Z} & (15) \end{pmatrix}\ :\ z \in \mathbf{Z}^\times
\end{array} \right\} .$$

In Lemma 45, we considered $P_{\mathrm{r}} := \{\mathfrak{p} \in \mathrm{Ideals}^\times_{\mathrm{prime}}(\mathbf{Z}) : \Delta_{\mathbf{Q}(\sqrt{-15})|\mathbf{Q},\underline{y}} \equiv_{\mathfrak{p}} 0\}$ and obtained that $\mathfrak{b} \in \mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha])$ if and only if we can write $\mathfrak{b} = \mathfrak{a} \prod\limits_{\mathfrak{p}\in P_{\mathrm{r}}} \mathfrak{p}^{\frac{\varepsilon_{\mathfrak{p}}}{e_{\mathfrak{p}}}}$, where $\mathfrak{a} \in \mathrm{Ideals}^\times(\mathbf{Z})$ with $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for $\mathfrak{p} \in P_{\mathrm{r}}$ and $\varepsilon_{\mathfrak{p}} \in \mathbf{Z}_{\geq 0}$ for $\mathfrak{p} \in P_{\mathrm{r}}$. Concerning the ramification indices $e_{\mathfrak{p}}$, see Remark 44.

We have $|\Delta_{\mathbf{Q}(\sqrt{-15})|\mathbf{Q},\underline{y}}| = 15$ and therefore $e_p = 1$ for $p \not\in \{3, 5\}$, cf. Remark 44.

We have $\mu_{\alpha,\mathbf{Q}}(x) = x^2 - x + 4$. As

$$\mu_{\alpha,\mathbf{Q}}(x) \equiv_3 (x+1)^2 \text{ and } \mu_{\alpha,\mathbf{Q}}(x) \equiv_5 (x+2)^2 \ ,$$

the prime ideal factorizations of (3) and (5) in $\mathbf{Z}[\alpha]$ are given by

$$\begin{array}{rcl} (3) & = & (3, \alpha+1)^2 \\ (5) & = & (5, \alpha+2)^2 \ . \end{array}$$

Write $\mathfrak{d}_3 := (3, \alpha+1) = {}_{\mathbf{Z}}\langle 3, \alpha+1\rangle$ and $\mathfrak{d}_5 := (5, \alpha+2) = {}_{\mathbf{Z}}\langle 5, \alpha+2\rangle$.

By Lemma 45 we know that every non zero Galois-stable ideal has the form

$$\mathfrak{d}_3^{\varepsilon_3}\mathfrak{d}_5^{\varepsilon_5}(z)$$

for some $\varepsilon_3 \in \{0, 1\}$, $\varepsilon_5 \in \{0, 1\}$, $z \in \mathbf{Z}_{>0}$.

We have $\omega_{\underline{y}}^{\mathbf{Z}}(\iota(z)) = z\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\alpha] \wr G) = z\Lambda$.

We *claim* that $\omega_{\underline{y}}^{\mathbf{Z}}\,(\iota(\mathfrak{o}_3)) = \left(\begin{smallmatrix}(3) & (15)\\ \mathbf{Z} & (3)\end{smallmatrix}\right)$.

We have the $\mathbf{Z}$-linear basis $(\left(\begin{smallmatrix}3&0\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&15\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&0\\0&3\end{smallmatrix}\right))$ of $\left(\begin{smallmatrix}(3) & (15)\\ \mathbf{Z} & (3)\end{smallmatrix}\right)$.

Consider the $\mathbf{Z}$-linear basis $\underline{r} = (3, \alpha+1, 3\sigma, (\alpha+1)\sigma)$ of $\iota(\mathfrak{o}_3) = \mathfrak{o}_3(\mathbf{Z}[\alpha]\wr G)$. It is mapped by $\omega_{\underline{y}}^{\mathbf{Z}}$ to

$$\begin{array}{rcl}
3 & \mapsto & \left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)\\
(\alpha+1) & \mapsto & \left(\begin{smallmatrix}-6&-60\\1&9\end{smallmatrix}\right)\\
3\sigma & \mapsto & \left(\begin{smallmatrix}3&45\\0&-3\end{smallmatrix}\right)\\
(\alpha+1)\sigma & \mapsto & \left(\begin{smallmatrix}-6&-30\\1&6\end{smallmatrix}\right)\ .
\end{array}$$

We have ${}_{\mathbf{Z}}\langle\left(\begin{smallmatrix}3&0\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&15\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&0\\0&3\end{smallmatrix}\right)\rangle \subseteq {}_{\mathbf{Z}}\langle\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right),\ \left(\begin{smallmatrix}-6&-60\\1&9\end{smallmatrix}\right),\ \left(\begin{smallmatrix}3&45\\0&-3\end{smallmatrix}\right),\ \left(\begin{smallmatrix}-6&-30\\1&6\end{smallmatrix}\right)\rangle$ because of

$$\begin{array}{rcl}
\left(\begin{smallmatrix}3&0\\0&0\end{smallmatrix}\right) & = & -\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right) + 3\left(\begin{smallmatrix}-6&-60\\1&9\end{smallmatrix}\right) + 2\left(\begin{smallmatrix}3&45\\0&-3\end{smallmatrix}\right) - 3\left(\begin{smallmatrix}-6&-30\\1&6\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}0&15\\0&0\end{smallmatrix}\right) & = & \left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right) - 2\left(\begin{smallmatrix}-6&-60\\1&9\end{smallmatrix}\right) - \left(\begin{smallmatrix}3&45\\0&-3\end{smallmatrix}\right) + 2\left(\begin{smallmatrix}-6&-30\\1&6\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) & = & -4\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right) + 8\left(\begin{smallmatrix}-6&-60\\1&9\end{smallmatrix}\right) + 6\left(\begin{smallmatrix}3&45\\0&-3\end{smallmatrix}\right) - 7\left(\begin{smallmatrix}-6&-30\\1&6\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}0&0\\0&3\end{smallmatrix}\right) & = & 2\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right) - 3\left(\begin{smallmatrix}-6&-60\\1&9\end{smallmatrix}\right) - 2\left(\begin{smallmatrix}3&45\\0&-3\end{smallmatrix}\right) + 3\left(\begin{smallmatrix}-6&-30\\1&6\end{smallmatrix}\right)\ .
\end{array}$$

Conversely, we have ${}_{\mathbf{Z}}\langle\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right),\ \left(\begin{smallmatrix}-6&-60\\1&9\end{smallmatrix}\right),\ \left(\begin{smallmatrix}3&45\\0&-3\end{smallmatrix}\right),\ \left(\begin{smallmatrix}-6&-30\\1&6\end{smallmatrix}\right)\rangle \subseteq \left(\begin{smallmatrix}(3) & (15)\\ \mathbf{Z} & (3)\end{smallmatrix}\right)$. This proves the *claim.*

We *claim* that $\omega_{\underline{y}}^{\mathbf{Z}}\,(\iota(\mathfrak{o}_5)) = \left(\begin{smallmatrix}(5) & (15)\\ \mathbf{Z} & (5)\end{smallmatrix}\right)$.

We have the $\mathbf{Z}$-linear basis $(\left(\begin{smallmatrix}5&0\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&15\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&0\\0&5\end{smallmatrix}\right))$ of $\left(\begin{smallmatrix}(5) & (15)\\ \mathbf{Z} & (5)\end{smallmatrix}\right)$.

Consider the $\mathbf{Z}$-linear basis $\underline{r} = (5, \alpha+2, 5\sigma, (\alpha+2)\sigma)$ of $\iota(\mathfrak{o}_5) = \mathfrak{o}_5(\mathbf{Z}[\alpha]\wr G)$. It is mapped by $\omega_{\underline{y}}^{\mathbf{Z}}$ to

$$\begin{array}{rcl}
5 & \mapsto & \left(\begin{smallmatrix}5&0\\0&5\end{smallmatrix}\right)\\
(\alpha+2) & \mapsto & \left(\begin{smallmatrix}-5&-60\\1&10\end{smallmatrix}\right)\\
5\sigma & \mapsto & \left(\begin{smallmatrix}5&75\\0&-5\end{smallmatrix}\right)\\
(\alpha+2)\sigma & \mapsto & \left(\begin{smallmatrix}-5&-15\\1&5\end{smallmatrix}\right)\ .
\end{array}$$

We have ${}_{\mathbf{Z}}\langle\left(\begin{smallmatrix}5&0\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&15\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&0\\0&5\end{smallmatrix}\right)\rangle \subseteq {}_{\mathbf{Z}}\langle\left(\begin{smallmatrix}5&0\\0&5\end{smallmatrix}\right),\ \left(\begin{smallmatrix}-5&-60\\1&10\end{smallmatrix}\right),\ \left(\begin{smallmatrix}5&75\\0&-5\end{smallmatrix}\right),\ \left(\begin{smallmatrix}-5&-15\\1&5\end{smallmatrix}\right)\rangle$ because of

$$\begin{array}{rcl}
\left(\begin{smallmatrix}5&0\\0&0\end{smallmatrix}\right) & = & -2\left(\begin{smallmatrix}5&0\\0&5\end{smallmatrix}\right) + 5\left(\begin{smallmatrix}-5&-60\\1&10\end{smallmatrix}\right) + 3\left(\begin{smallmatrix}5&75\\0&-5\end{smallmatrix}\right) - 5\left(\begin{smallmatrix}-5&-15\\1&5\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}0&15\\0&0\end{smallmatrix}\right) & = & \left(\begin{smallmatrix}5&0\\0&5\end{smallmatrix}\right) - 2\left(\begin{smallmatrix}-5&-60\\1&10\end{smallmatrix}\right) - 1\left(\begin{smallmatrix}5&75\\0&-5\end{smallmatrix}\right) + 2\left(\begin{smallmatrix}-5&-15\\1&5\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) & = & -4\left(\begin{smallmatrix}5&0\\0&5\end{smallmatrix}\right) + 8\left(\begin{smallmatrix}-5&-60\\1&10\end{smallmatrix}\right) + 5\left(\begin{smallmatrix}5&75\\0&-5\end{smallmatrix}\right) - 7\left(\begin{smallmatrix}-5&-15\\1&5\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}0&0\\0&5\end{smallmatrix}\right) & = & 3\left(\begin{smallmatrix}5&0\\0&5\end{smallmatrix}\right) - 5\left(\begin{smallmatrix}-5&-60\\1&10\end{smallmatrix}\right) - 3\left(\begin{smallmatrix}5&75\\0&-5\end{smallmatrix}\right) + 5\left(\begin{smallmatrix}-5&-15\\1&5\end{smallmatrix}\right)\ .
\end{array}$$

Conversely, we have ${}_{\mathbf{Z}}\langle \left(\begin{smallmatrix} 5 & 0 \\ 0 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} -5 & -60 \\ 1 & 10 \end{smallmatrix}\right), \left(\begin{smallmatrix} 5 & 75 \\ 0 & -5 \end{smallmatrix}\right), \left(\begin{smallmatrix} -5 & -15 \\ 1 & 5 \end{smallmatrix}\right)\rangle \subseteq \left(\begin{smallmatrix} (5) & (15) \\ \mathbf{Z} & (5) \end{smallmatrix}\right)$. This proves the *claim*.

Now we consider

$$\begin{aligned} \mathfrak{d}_5\mathfrak{d}_3 &= (5,\alpha+2)(3,\alpha+1) = (15, 3\alpha+6, 5\alpha+5, 4\alpha-2) = (15, 5\alpha+5, 2\alpha-1) \\ &= (15, 1-2\alpha) = (1-2\alpha)\ . \end{aligned}$$

As $\omega_{\underline{y}}^{\mathbf{Z}}$ is a ring isomorphism, we obtain

$$\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathfrak{d}_5\mathfrak{d}_3)\right) \;=\; \omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathfrak{d}_5)\right)\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathfrak{d}_3)\right) = \left(\begin{smallmatrix} (5) & (15) \\ \mathbf{Z} & (5) \end{smallmatrix}\right)\left(\begin{smallmatrix} (3) & (15) \\ \mathbf{Z} & (3) \end{smallmatrix}\right) = \left(\begin{smallmatrix} (15) & (15) \\ \mathbf{Z} & (15) \end{smallmatrix}\right)\ .$$

Since

$$\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha])\right) \subsetneq \mathrm{Ideals}^{\times}(\Lambda) = \omega_{\underline{y}}^{\mathbf{Z}}(\mathrm{Ideals}^{\times}(\mathbf{Z}[\alpha] \wr G))\ ,$$

we have

$$\iota(\mathrm{Ideals}^{\times,G}) \subsetneq \mathrm{Ideals}^{\times}(\mathbf{Z}[\alpha] \wr G)\ ,$$

and so the map ι is not surjective. □

7.2.2 Ideals in $\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\sqrt{d}] \wr G)$ for $d \equiv_4 2$ or $d \equiv_4 3$

Suppose that $d \equiv_4 2$ or $d \equiv_4 3$.

Lemma 56. *Let* $R := \mathbf{Z}_{(2)}$. *Let* $R' := \{\left(\begin{smallmatrix} s & w \\ u & v \end{smallmatrix}\right) : s, w, u, v \in R,\ s \equiv_2 v,\ w \equiv_2 u\}$. *Then*

$$\mathrm{Ideals}^{\times}(R') = \{2^k J_i : i \in [1,8],\ k \in \mathbf{Z}_{\geq 0}\}\ ,$$

where

$J_1 = {}_R\langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 2 \end{smallmatrix}\right)\rangle = R'$

$J_2 = {}_R\langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 2 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 4 \end{smallmatrix}\right)\rangle = \{\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) : a, b, c, e \in R,\ a \equiv_2 e \equiv_2 b \equiv_2 c,\ a + e \equiv_4 b + c\}$

$J_3 = {}_R\langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 2 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 4 \end{smallmatrix}\right)\rangle = \{\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) : a, b, c, e \in R,\ a \equiv_2 e \equiv_2 b \equiv_2 c,\ e \equiv_4 a + b + c\}$

$J_4 = {}_R\langle \left(\begin{smallmatrix} 2 & 2 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 4 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 2 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 4 \end{smallmatrix}\right)\rangle = \{\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) : a, b, c, e \in R,\ a \equiv_2 e \equiv_2 b \equiv_2 c \equiv_2 0,\ a \equiv_4 b,\ c \equiv_4 e\}$

$J_5 = {}_R\langle \left(\begin{smallmatrix} 2 & 0 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 4 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 4 \end{smallmatrix}\right)\rangle = \{\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) : a, b, c, e \in R,\ a \equiv_2 e \equiv_2 b \equiv_2 c \equiv_2 0,\ a \equiv_4 c,\ b \equiv_4 e\}$

$J_6 = {}_R\langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 2 \end{smallmatrix}\right)\rangle = \left(\begin{smallmatrix} (2) & (2) \\ (2) & (2) \end{smallmatrix}\right)$

$J_7 = {}_R\langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 2 \end{smallmatrix}\right)\rangle = \{\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) : a, b, c, e \in R,\ a \equiv_2 e \equiv_2 b \equiv_2 c\}$

$J_8 = {}_R\langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 2 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 4 \end{smallmatrix}\right)\rangle = \{\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) : a, b, c, e \in R,\ a \equiv_2 e \equiv_2 b \equiv_2 c \equiv_2 0,\ a + b + c \equiv_4 e\}$.

Proof. It suffices to show the inclusion ($\subseteq$).

Let $I \subseteq R'$ be a non-zero ideal.

Let $k \in \mathbf{Z}_{\geq 0}$ be maximal such that $2^{-k}I \subseteq R'$. Then $J := 2^{-k}I$ is an ideal in R'.

We *claim* that there exists $\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) \in J$ with $a \not\equiv_4 0 \vee b \not\equiv_4 0 \vee c \not\equiv_4 0 \vee e \not\equiv_4 0$.

In fact, if we *assume* that $a \equiv_4 0,\ b \equiv_4 0,\ c \equiv_4 0,\ e \equiv_4 0$ for $\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) \in J$, then we have $\left(\begin{smallmatrix} a/2 & b/2 \\ c/2 & e/2 \end{smallmatrix}\right) \in R'$ and therefore $2^{-1}J \subseteq R'$, which is a *contradiction* to the maximality of k. This proves the *claim.*

So we may choose an element $\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) \in J$ with $a \not\equiv_4 0 \vee b \not\equiv_4 0 \vee c \not\equiv_4 0 \vee e \not\equiv_4 0$. As $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in R'$ we can assume without loss of generality that $a \not\equiv_4 0$, by using permutation of rows and colums.

We have

$$\left(\begin{smallmatrix} 2 & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right)\left(\begin{smallmatrix} 2 & 0 \\ 0 & 0 \end{smallmatrix}\right) \quad = \quad \left(\begin{smallmatrix} 4a & 0 \\ 0 & 0 \end{smallmatrix}\right) \in J$$

and therefore $\left(\begin{smallmatrix} 8 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in J$.

Because of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 8 & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 8 \end{smallmatrix}\right) \in J$, it follows that $\left(\begin{smallmatrix} 8 & 0 \\ 0 & 8 \end{smallmatrix}\right) \in J$, whence $8R' \subseteq J$.

So it suffices to find those ideals of R' that contain $2^3R'$ and that are not divisible by 2.

We determined these ideals J_i for $i \in [1, 8]$ using the computer algebra system Magma [7], Magma Code A 3. □

Lemma 57. *Let* $R := \mathbf{Z}_{(2)}$. *Consider* $R'' := \{\left(\begin{smallmatrix} s & 2w \\ u & v \end{smallmatrix}\right) : s, w, u, v \in R,\ s \equiv_2 v,\ w \equiv_2 u\}$. *Let* $I \subseteq R''$ *be an ideal.*

(1) *Suppose that* $\left(\begin{smallmatrix} a_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I$, *where* $a_0 \in R$. *Then* $\left(\begin{smallmatrix} (a_0) & (2a_0) \\ (a_0) & (2a_0) \end{smallmatrix}\right) \subseteq I$.

(2) *Suppose that* $\left(\begin{smallmatrix} 0 & 2b_0 \\ 0 & 0 \end{smallmatrix}\right) \in I$, *where* $b_0 \in R$. *Then* $\left(\begin{smallmatrix} (2b_0) & (2b_0) \\ (2b_0) & (2b_0) \end{smallmatrix}\right) \subseteq I$.

(3) *Suppose that* $\left(\begin{smallmatrix} 0 & 0 \\ c_0 & 0 \end{smallmatrix}\right) \in I$, *where* $c_0 \in R$. *Then* $\left(\begin{smallmatrix} (2c_0) & (4c_0) \\ (c_0) & (2c_0) \end{smallmatrix}\right) \subseteq I$.

(4) *Suppose that* $\left(\begin{smallmatrix} 0 & 0 \\ 0 & e_0 \end{smallmatrix}\right) \in I$, *where* $e_0 \in R$. *Then* $\left(\begin{smallmatrix} (2e_0) & (2e_0) \\ (e_0) & (e_0) \end{smallmatrix}\right) \subseteq I$.

Proof.

(1) Suppose that $\left(\begin{smallmatrix} a_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I$, where $a_0 \in R$. Then

$$\begin{aligned}
\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ a_0 & 0 \end{smallmatrix}\right) \in I \\
\left(\begin{smallmatrix} a_0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 2a_0 \\ 0 & 0 \end{smallmatrix}\right) \in I \\
\left(\begin{smallmatrix} 0 & 0 \\ a_0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & 2a_0 \end{smallmatrix}\right) \in I\ .
\end{aligned}$$

So we have $\begin{pmatrix} (a_0) & (2a_0) \\ (a_0) & (2a_0) \end{pmatrix} \subseteq I$.

(2) Suppose that $\left(\begin{smallmatrix} 0 & 2b_0 \\ 0 & 0 \end{smallmatrix}\right) \in I$, where $b_0 \in R$. Then

$$\begin{aligned} \left(\begin{smallmatrix} 0 & 2b_0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 2b_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I \\ \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 2b_0 \\ 0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & 2b_0 \end{smallmatrix}\right) \in I \\ \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 2b_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ 2b_0 & 0 \end{smallmatrix}\right) \in I \ . \end{aligned}$$

So we have $\begin{pmatrix} (2b_0) & (2b_0) \\ (2b_0) & (2b_0) \end{pmatrix} \subseteq I$.

(3) Suppose that $\left(\begin{smallmatrix} 0 & 0 \\ c_0 & 0 \end{smallmatrix}\right) \in I$, where $c_0 \in R$. Then

$$\begin{aligned} \left(\begin{smallmatrix} 0 & 0 \\ c_0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & 2c_0 \end{smallmatrix}\right) \in I \\ \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 0 \\ c_0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 2c_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I \\ \left(\begin{smallmatrix} 2c_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 4c_0 \\ 0 & 0 \end{smallmatrix}\right) \in I \ . \end{aligned}$$

So we have $\begin{pmatrix} (2c_0) & (4c_0) \\ (c_0) & (2c_0) \end{pmatrix} \subseteq I$.

(4) Suppose that $\left(\begin{smallmatrix} 0 & 0 \\ 0 & e_0 \end{smallmatrix}\right) \in I$, where $e_0 \in R$. Then

$$\begin{aligned} \left(\begin{smallmatrix} 0 & 0 \\ 0 & e_0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 0 \\ e_0 & 0 \end{smallmatrix}\right) \in I \\ \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 0 \\ 0 & e_0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & 2e_0 \\ 0 & 0 \end{smallmatrix}\right) \in I \\ \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 0 \\ e_0 & 0 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 2e_0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in I \ . \end{aligned}$$

So we have $\begin{pmatrix} (2e_0) & (2e_0) \\ (e_0) & (e_0) \end{pmatrix} \subseteq I$.

□

Lemma 58. *Let* $R := \mathbf{Z}_{(2)}$. *Let* $R'' := \{ \left(\begin{smallmatrix} s & 2w \\ u & v \end{smallmatrix}\right) : s, w, u, v \in R,\ s \equiv_2 v,\ w \equiv_2 u \}$. *Then*

$$\mathrm{Ideals}^{\times}(R'') = \{ 2^k J_i : k \in \mathbf{Z}_{\geq 0},\ i \in [1, 12] \} \ ,$$

where

$$\begin{aligned}
J_1 &= {}_R\langle \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&2\end{smallmatrix}\right)\rangle &&= R'' \\
J_2 &= {}_R\langle \left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&2\\1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle &&= \{\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right) : a,b,c,e \in R,\ a \equiv_2 0 \equiv_2 e,\ a+2b \equiv_4 e,\ b \equiv_2 c\} \\
J_3 &= {}_R\langle \left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle &&= \{\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right) : a,b,c,e \in R,\ a \equiv_2 0 \equiv_2 e,\ a \equiv_4 e,\ b \equiv_2 c\} \\
J_4 &= {}_R\langle \left(\begin{smallmatrix}2&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&4\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle &&= \begin{pmatrix}\scriptstyle(2)&\scriptstyle(4)\\\scriptstyle(2)&\scriptstyle(4)\end{pmatrix} \\
J_5 &= {}_R\langle \left(\begin{smallmatrix}4&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&4\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&2\end{smallmatrix}\right)\rangle &&= \begin{pmatrix}\scriptstyle(4)&\scriptstyle(4)\\\scriptstyle(2)&\scriptstyle(2)\end{pmatrix} \\
J_6 &= {}_R\langle \left(\begin{smallmatrix}2&0\\2&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&4\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\4&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle &&= \{\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right) : a,b,c,e \in R,\ a \equiv_2 0 \equiv_2 e, \\
& &&\qquad\qquad a \equiv_4 e,\ b \equiv_2 0 \equiv_2 c,\ a+b \equiv_4 c\} \\
J_7 &= {}_R\langle \left(\begin{smallmatrix}4&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&4\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\4&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle &&= \begin{pmatrix}\scriptstyle(4)&\scriptstyle(4)\\\scriptstyle(4)&\scriptstyle(4)\end{pmatrix} \\
J_8 &= {}_R\langle \left(\begin{smallmatrix}4&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&8\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle &&= \begin{pmatrix}\scriptstyle(4)&\scriptstyle(8)\\\scriptstyle(2)&\scriptstyle(4)\end{pmatrix} \\
J_9 &= {}_R\langle \left(\begin{smallmatrix}2&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&2\end{smallmatrix}\right)\rangle &&= \{\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right) : a,b,c,e \in R,\ a \equiv_2 0 \equiv_2 e,\ b \equiv_2 c\} \\
J_{10} &= {}_R\langle \left(\begin{smallmatrix}2&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&4\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&2\end{smallmatrix}\right)\rangle &&= \begin{pmatrix}\scriptstyle(2)&\scriptstyle(4)\\\scriptstyle(2)&\scriptstyle(2)\end{pmatrix} \\
J_{11} &= {}_R\langle \left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&4\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle &&= \{\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right) : a,b,c,e \in R,\ a \equiv_2 0 \equiv_2 e,\ a \equiv_4 e,\ b \equiv_2 0 \equiv_2 c\} \\
J_{12} &= {}_R\langle \left(\begin{smallmatrix}4&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&4\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle &&= \begin{pmatrix}\scriptstyle(4)&\scriptstyle(4)\\\scriptstyle(2)&\scriptstyle(4)\end{pmatrix}\ .
\end{aligned}$$

Proof. It suffices to show the inclusion $(\subseteq)$.

Let $I \subseteq R''$ be a non-zero ideal.

Let $k \in \mathbf{Z}_{\geq 0}$ be maximal such that $2^{-k}I \subseteq R''$. Then $J := 2^{-k}I$ is an ideal in R''.

We *claim* that there exists $\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right) \in J$ with $a \not\equiv_4 0 \vee b \not\equiv_4 0 \vee c \not\equiv_4 0 \vee e \not\equiv_4 0$. In fact, if we *assume* that $a \equiv_4 0,\ b \equiv_4 0,\ c \equiv_4 0,\ e \equiv_4 0$, for $\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right) \in J$, then we have $\begin{pmatrix}\scriptstyle a/2&\scriptstyle 2(b/2)\\\scriptstyle c/2&\scriptstyle e/2\end{pmatrix} \in R''$ and therefore $2^{-1}J \subseteq R''$, which is a *contradiction* to the maximality of k. This proves the *claim.*

So we may choose an element $\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right) \in J$ with $a \not\equiv_4 0 \vee b \not\equiv_4 0 \vee c \not\equiv_4 0 \vee e \not\equiv_4 0$.

We *claim* that $16R'' \subseteq J$.

Case 1. Suppose that $a \not\equiv_4 0$.

We have $\left(\begin{smallmatrix}2&0\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right)\left(\begin{smallmatrix}2&0\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}4a&0\\0&0\end{smallmatrix}\right) \in J$ and therefore $\left(\begin{smallmatrix}8&0\\0&0\end{smallmatrix}\right) \in J$.

By Lemma 57 (1), we obtain that $\begin{pmatrix}\scriptstyle(8)&\scriptstyle(16)\\\scriptstyle(8)&\scriptstyle(16)\end{pmatrix} \in J$. Hence we have $\left(\begin{smallmatrix}16&0\\0&16\end{smallmatrix}\right) \in J$ and consequently $16R'' \subseteq J$.

Case 2. Suppose that $b \not\equiv_4 0$.

We have $\left(\begin{smallmatrix}2&0\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}a&2b\\c&e\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\0&2\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&8b\\0&0\end{smallmatrix}\right) \in J$ and therefore $\left(\begin{smallmatrix}0&16\\0&0\end{smallmatrix}\right) \in J$.

By Lemma 57 (2), we obtain that $\begin{pmatrix}\scriptstyle(16)&\scriptstyle(16)\\\scriptstyle(16)&\scriptstyle(16)\end{pmatrix} \in J$. Hence we have $\left(\begin{smallmatrix}16&0\\0&16\end{smallmatrix}\right) \in J$ and consequently $16R'' \subseteq J$.

Subcase 2.3 Suppose that $c \not\equiv_4 0$.

We have $\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & 2b \\ c & e \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 4c & 0 \end{pmatrix} \in J$ and therefore $\begin{pmatrix} 0 & 0 \\ 8 & 0 \end{pmatrix} \in J$.

By Lemma 57 (3), we obtain that $\begin{pmatrix} (16) & (32) \\ (8) & (16) \end{pmatrix} \in J$. Hence we have $\begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix} \in J$ and consequently $16R'' \subseteq J$.

Subcase 2.4 Suppose that $d \not\equiv_4 0$.

We have $\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & 2b \\ c & e \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 4e \end{pmatrix} \in J$ and therefore $\begin{pmatrix} 0 & 0 \\ 0 & 8 \end{pmatrix} \in J$.

By Lemma 57 (4), we obtain that $\begin{pmatrix} (16) & (16) \\ (8) & (8) \end{pmatrix} \in J$. Hence we have $\begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix} \in J$ and consequently $16R'' \subseteq J$.

This proves the *claim*.

So it suffices to find those ideals of R'' that contain $2^4 R''$ and that are not divisble by 2. We determined these ideals J_i for $i \in [1, 12]$, using the computer algebra system Magma [7], Magma Code A 4. □

Remark 59. Recall that d is squarefree and that $d \equiv_4 2$ or $d \equiv_4 3$. Let $\underline{y}$ be as in Proposition 20.

(1) Let $p \in \mathbf{Z}_{\geq 3}$ be a prime. Let $R = \mathbf{Z}_{(p)}$.

In case of $d \equiv_p 0$, the R-algebra $R' := \begin{pmatrix} R & (p) \\ R & R \end{pmatrix}$ is isomorphic to $R[\sqrt{d}] \wr \mathrm{C}_2$ via $\omega_{\underline{y}}^R$, cf. Proposition 20.

In case of $d \not\equiv_p 0$, the R-algebra $R' := \begin{pmatrix} R & R \\ R & R \end{pmatrix}$ is isomorphic to $R[\sqrt{d}] \wr \mathrm{C}_2$ via $\omega_{\underline{y}}^R$, cf. Proposition 20.

(2) Let $R = \mathbf{Z}_{(2)}$.

If $d \not\equiv_2 0$, the R-algebra $R' := \{\begin{pmatrix} s & w \\ u & v \end{pmatrix} : s, w, u, v \in R,\ s \equiv_2 v,\ w \equiv_2 u\}$ is isomorphic to $R[\sqrt{d}] \wr \mathrm{C}_2$ via $\omega_{\underline{y}}^R$, cf. Proposition 20.

If $d \equiv_2 0$, the R-algebra $R'' = \{\begin{pmatrix} s & 2w \\ u & v \end{pmatrix} : s, w, u, v \in R,\ s \equiv_2 v,\ w \equiv_2 u\}$ is isomorphic to $R[\sqrt{d}] \wr \mathrm{C}_2$ via $\omega_{\underline{y}}^R$.

Proposition 60. *Let* $L = \mathbf{Q}(\sqrt{-5})$ *and* $K = \mathbf{Q}$. *Let* $A = \mathbf{Z}$. *Write* $\alpha := \sqrt{-5}$. *Then* $B = \mathcal{O}_L = \mathbf{Z}[\alpha]$. *The Galois group is given by* $G = \{\mathrm{id}, \sqrt{-5} \overset{\sigma}{\mapsto} -\sqrt{-5}\}$.

Consider the $\mathbf{Z}$*-linear basis* $\underline{y} = (1, \alpha)$ *of* $\mathbf{Z}[\alpha]$.

By Proposition 20 *we know that*

$$\begin{aligned} \Lambda := \omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\alpha \wr G]) &= \{\begin{pmatrix} s & -5w \\ u & v \end{pmatrix} : s, w, u, v \in \mathbf{Z}, s \equiv_2 v,\ w \equiv_2 u\} \\ &= \{\begin{pmatrix} s & 5w \\ u & v \end{pmatrix} : s, w, u, v \in \mathbf{Z}, s \equiv_2 v,\ w \equiv_2 u\}\ . \end{aligned}$$

We remind of

$$\begin{array}{rcl} J_1 & = & \{\left(\begin{smallmatrix} s & w \\ u & v \end{smallmatrix}\right) : s, w, u, v \in \mathbf{Z}_{(2)},\ s \equiv_2 v,\ w \equiv_2 u\} \\ J_3 & = & \{\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) : a, b, c, e \in \mathbf{Z}_{(2)},\ a \equiv_2 e \equiv_2 b \equiv_2 c,\ e \equiv_4 a+b+c\},\ \textit{cf.}\ \text{Lemma 56.} \end{array}$$

Then the map $\iota : \mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha]) \to \mathrm{Ideals}^{\times}(\mathbf{Z}[\alpha] \wr G)$ *is not surjective, cf.* Lemma 40, Remark 47*.*

More specifically, we have

$$\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha]))\right) =$$
$$\{z\Lambda,\ z(\left(\begin{smallmatrix} (5) & (5) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right) \cap J_1 \cap \mathbf{Z}^{2\times 2}),\ z(\left(\begin{smallmatrix} \mathbf{Z}_{(5)} & (5) \\ \mathbf{Z}_{(5)} & \mathbf{Z}_{(5)} \end{smallmatrix}\right) \cap J_3 \cap \mathbf{Z}^{2\times 2}),\ z(\left(\begin{smallmatrix} (5) & (5) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right) \cap J_3 \cap \mathbf{Z}^{2\times 2}) : z \in \mathbf{Z}^{\times}\}$$

and therein

$$\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathrm{Ideals}^{\times,G}_{\mathrm{principal}}(\mathbf{Z}[\alpha]))\right) = \{z\Lambda,\ z(\left(\begin{smallmatrix} (5) & (5) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right) \cap J_1 \cap \mathbf{Z}^{2\times 2}) : z \in \mathbf{Z}^{\times}\}\ .$$

Moreover, there exists a non-zero ideal in $\mathbf{Z}[\alpha] \wr G$ *whose index is a square and that is not contained in the image of* ι*,* cf. Remark 48.

Proof. First we determine $\mathrm{Ideals}^{\times}(\Lambda)$.

Let $p \in \mathbf{Z}_{>0}$ be a prime.

Case $p \notin \{2, 5\}$. Then we have $\Lambda_{(p)} = \left(\begin{smallmatrix} \mathbf{Z}_{(p)} & \mathbf{Z}_{(p)} \\ \mathbf{Z}_{(p)} & \mathbf{Z}_{(p)} \end{smallmatrix}\right)$ since 2 and 5 are units in $\mathbf{Z}_{(p)}$. By Lemma 49 we have

$$\mathrm{Ideals}^{\times}(\Lambda_{(p)}) = \{p^k \Lambda_{(p)} : k \in \mathbf{Z}_{\geq 0}\}\ .$$

Case $p = 5$. Then $\Lambda_{(5)} = \left(\begin{smallmatrix} \mathbf{Z}_{(5)} & (5) \\ \mathbf{Z}_{(5)} & \mathbf{Z}_{(5)} \end{smallmatrix}\right)$ since 2 is a unit in $\mathbf{Z}_{(5)}$. By Lemma 51 we have

$$\mathrm{Ideals}^{\times}(\Lambda_{(5)}) =$$
$$\{5^k \underbrace{\left(\begin{smallmatrix} \mathbf{Z}_{(5)} & (5) \\ \mathbf{Z}_{(5)} & \mathbf{Z}_{(5)} \end{smallmatrix}\right)}_{=:I_1},\ 5^k \underbrace{\left(\begin{smallmatrix} (5) & (5^2) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right)}_{=:I_2},\ 5^k \underbrace{\left(\begin{smallmatrix} (5) & (5) \\ \mathbf{Z}_{(5)} & \mathbf{Z}_{(5)} \end{smallmatrix}\right)}_{=:I_3},\ 5^k \underbrace{\left(\begin{smallmatrix} (5) & (5) \\ (5) & (5) \end{smallmatrix}\right)}_{=:I_4},\ 5^k \underbrace{\left(\begin{smallmatrix} \mathbf{Z}_{(5)} & (5) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right)}_{=:I_5},\ 5^k \underbrace{\left(\begin{smallmatrix} (5) & (5) \\ \mathbf{Z}_{(5)} & (5) \end{smallmatrix}\right)}_{=:I_6} : k \in \mathbf{Z}_{\geq 0}\}\ .$$

Case $p = 2$. Then $\Lambda_{(2)} = \{\left(\begin{smallmatrix} s & w \\ u & v \end{smallmatrix}\right) : s, w, u, v \in \mathbf{Z}_{(2)},\ s \equiv_2 v,\ w \equiv_2 u\}$ since 5 is a unit in $\mathbf{Z}_{(2)}$. By Lemma 56, in the notation used there, we have

$$\mathrm{Ideals}(\Lambda_{(2)}) = \{2^k J_i : i \in [1, 8],\ k \in \mathbf{Z}_{\geq 0}\}\ .$$

We *claim* that

$$\mathrm{Ideals}^\times(\Lambda) \overset{!}{=} \{5^k I_a \cap 2^l J_b \cap c\mathbf{Z}^{2\times 2} : a \in [1,6],\ b \in [1,8],\ k,l \in \mathbf{Z}_{\geq 0},\ c \in \mathbf{Z}_{>0},\ c \not\equiv_2 0,\ c \not\equiv_5 0\}\ .$$

We only need to show $(\subseteq)$.

Suppose given $M \in \mathrm{Ideals}^\times(\Lambda)$. We have

$$M \overset{\text{Lemma 53}}{=} \bigcap_{p \text{ prime}} M_{(p)} = M_{(5)} \cap M_{(2)} \cap \bigcap_{p \text{ prime},\ p \notin \{2,5\}} M_{(p)}\ .$$

For $p \notin \{2,5\}$ we have $\Lambda_{(p)} = \mathbf{Z}_{(p)}^{2\times 2}$ and $M_{(p)} = p^{\alpha_p}\mathbf{Z}_{(p)}^{2\times 2}$, where $\alpha_p \in \mathbf{Z}_{\geq 0}$ and $\alpha_p = 0$ for all but finitely many p.

Write $M_{(5)} = 5^k I_a$ and $M_{(2)} = 2^l J_b$ for some $a \in [1,6]$, $b \in [1,8]$, $k,l \in \mathbf{Z}_{\geq 0}$. Then

$$M = 5^k I_a \cap 2^l J_b \cap \bigcap_{p \text{ prime},\ p \notin \{2,5\}} p^{\alpha_p}\mathbf{Z}_{(p)}^{2\times 2}\ .$$

Define $c := \prod_{q \text{ prime},\ q \notin \{2,5\}} q^{\alpha_q}$. We obtain for $p \notin \{2,5\}$

$$\begin{array}{rcl} c\mathbf{Z}_{(p)}^{2\times 2} & = & p^{\alpha_p}\mathbf{Z}_{(p)}^{2\times 2} \\ 5^k I_a & \subseteq & \mathbf{Z}_{(5)}^{2\times 2} = c\mathbf{Z}_{(5)}^{2\times 2} \\ 2^l J_b & \subseteq & \mathbf{Z}_{(2)}^{2\times 2} = c\mathbf{Z}_{(2)}^{2\times 2}\ . \end{array}$$

So

$$\begin{array}{rcl} M & = & 5^k I_a \cap 2^l J_b \cap \bigcap_{p \text{ prime},\ p \notin \{2,5\}} c\mathbf{Z}_{(p)}^{2\times 2} \\ & = & 5^k I_a \cap c\mathbf{Z}_{(5)}^{2\times 2} \cap 2^l J_b \cap c\mathbf{Z}_{(2)}^{2\times 2} \cap \bigcap_{p \text{ prime},\ p \notin \{2,5\}} c\mathbf{Z}_{(p)}^{2\times 2} \\ & = & 5^k I_a \cap 2^l J_b \cap \bigcap_{p \text{ prime}} c\mathbf{Z}_{(p)}^{2\times 2} \\ & = & 5^k I_a \cap 2^l J_b \cap c(\bigcap_{p \text{ prime}} \mathbf{Z}_{(p)}^{2\times 2}) \\ & = & 5^k I_a \cap 2^l J_b \cap c(\bigcap_{p \text{ prime}} \mathbf{Z}_{(p)})^{2\times 2} \\ & = & 5^k I_a \cap 2^l J_b \cap c\mathbf{Z}^{2\times 2}\ . \end{array}$$

This proves the *claim*.

In Lemma 45, we considered $P_{\mathrm{r}} := \{\mathfrak{p} \in \mathrm{Ideals}^\times_{\mathrm{prime}}(\mathbf{Z}) : \Delta_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q},\underline{y}} \equiv_{\mathfrak{p}} 0\}$ and obtained that $\mathfrak{b} \in \mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha])$ if and only if we can write $\mathfrak{b} = \mathfrak{a}\prod_{\mathfrak{p}\in P_{\mathrm{r}}} \mathfrak{p}^{\frac{\varepsilon_{\mathfrak{p}}}{e_{\mathfrak{p}}}}$, where $\mathfrak{a} \in \mathrm{Ideals}^\times(\mathbf{Z})$ with $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for $\mathfrak{p} \in P_{\mathrm{r}}$ and $\varepsilon_{\mathfrak{p}} \in \mathbf{Z}_{\geq 0}$ for $\mathfrak{p} \in P_{\mathrm{r}}$. Concerning the ramification indices $e_{\mathfrak{p}}$, see Remark 44.

We have $|\Delta_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q},\underline{y}}| = 20$ and therefore $e_p = 1$ for $p \notin \{2,5\}$, cf. Remark 44.

We have $\mu_{\alpha,\mathbf{Q}}(x) = x^2 + 5$. As

$$\mu_{\alpha,\mathbf{Q}}(x) \equiv_2 (x+1)^2 \text{ and } \mu_{\alpha,\mathbf{Q}}(x) \equiv_5 x^2,$$

the prime ideal factorizations of (2) and (5) in $\mathbf{Z}[\alpha]$ are given by

$$\begin{array}{rcl} (2) & = & (2, \alpha+1)^2 \\ (5) & = & (\alpha)^2 \ . \end{array}$$

Write $\mathfrak{d}_2 := (2, \alpha+1) = {}_{\mathbf{Z}}\langle 2, \alpha+1\rangle$ and $\mathfrak{d}_5 = (\alpha) = {}_{\mathbf{Z}}\langle -5, \alpha\rangle$.

By Lemma 45 we know that every Galois-stable ideal has the form

$$\mathfrak{d}_2^{\varepsilon_2}\mathfrak{d}_5^{\varepsilon_5}(z)$$

for some $\varepsilon_2 \in \{0,1\}$, $\varepsilon_5 \in \{0,1\}$, $z \in \mathbf{Z}_{>0}$.

We have $\omega_{\underline{y}}^{\mathbf{Z}}(\iota(z)) = z\omega_{\underline{y}}^{\mathbf{Z}}(\mathbf{Z}[\alpha] \wr G) = z\Lambda$.

To determine $\omega_{\underline{y}}^{\mathbf{Z}}(\iota(\mathfrak{d}_2))$, it is sufficient to determine the image of $\iota((\mathfrak{d}_2)_{(p)})$ in $\Lambda_{(p)}$ for p prime.

For $p \neq 2$ prime we have $(\mathfrak{d}_2)_{(p)} = \mathbf{Z}[\alpha]_{(p)}$ and therefore $\omega_{\underline{y}}^{\mathbf{Z}_{(p)}}\big(\iota((\mathfrak{d}_2)_{(p)})\big) = \Lambda_{(p)}$.

We *claim* that the image of $(\mathfrak{d}_2)_{(2)}$ in $\Lambda_{(2)}$ is given by

$$J_3 = {}_{\mathbf{Z}_{(2)}}\langle \left(\begin{smallmatrix}1&1\\1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}0&2\\0&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle = \{\left(\begin{smallmatrix}a&b\\c&e\end{smallmatrix}\right) : a,b,c,e \in \mathbf{Z}_{(2)},\ a \equiv_2 e \equiv_2 b \equiv_2 c,\ e \equiv_4 a+b+c\} \ .$$

Consider the images of the $\mathbf{Z}_{(2)}$-linear basis $\underline{r} = (2, \alpha+1, 2\sigma, (\alpha+1)\sigma)$ of $(\mathfrak{d}_2)_{(2)}(\mathbf{Z}_{(2)}[\alpha]\wr G)$.

$$\begin{array}{rcl} 2 & \mapsto & \left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right) \\ \alpha+1 & \mapsto & \left(\begin{smallmatrix}1&-5\\1&1\end{smallmatrix}\right) \\ 2\sigma & \mapsto & \left(\begin{smallmatrix}2&0\\0&-2\end{smallmatrix}\right) \\ (\alpha+1)\sigma & \mapsto & \left(\begin{smallmatrix}1&5\\1&-1\end{smallmatrix}\right) \ . \end{array}$$

We have ${}_{\mathbf{Z}_{(2)}}\langle \left(\begin{smallmatrix}1&1\\1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}0&2\\0&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\2&2\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right)\rangle \subseteq {}_{\mathbf{Z}_{(2)}}\langle \left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&-5\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}2&0\\0&-2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&5\\1&-1\end{smallmatrix}\right)\rangle$ because of

$$\begin{array}{rcl} \left(\begin{smallmatrix}1&1\\1&3\end{smallmatrix}\right) & = & \frac{1}{5}\left(4\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right) + 2\left(\begin{smallmatrix}1&-5\\1&1\end{smallmatrix}\right) - 4\left(\begin{smallmatrix}2&0\\0&-2\end{smallmatrix}\right) + 3\left(\begin{smallmatrix}1&5\\1&-1\end{smallmatrix}\right)\right) \\ \left(\begin{smallmatrix}0&2\\0&2\end{smallmatrix}\right) & = & \frac{1}{5}\left(3\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right) - 1\left(\begin{smallmatrix}1&-5\\1&1\end{smallmatrix}\right) - 3\left(\begin{smallmatrix}2&0\\0&-2\end{smallmatrix}\right) + 1\left(\begin{smallmatrix}1&5\\1&-1\end{smallmatrix}\right)\right) \\ \left(\begin{smallmatrix}0&0\\2&2\end{smallmatrix}\right) & = & \left(\begin{smallmatrix}1&-5\\1&1\end{smallmatrix}\right) - \left(\begin{smallmatrix}2&0\\0&-2\end{smallmatrix}\right) + \left(\begin{smallmatrix}1&5\\1&-1\end{smallmatrix}\right) \\ \left(\begin{smallmatrix}0&0\\0&4\end{smallmatrix}\right) & = & \left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right) - \left(\begin{smallmatrix}2&0\\0&-2\end{smallmatrix}\right) \ . \end{array}$$

Conversely, we have

$$_{\mathbf{Z}_{(2)}}\langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -5 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & -2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 5 \\ 1 & -1 \end{smallmatrix}\right)\rangle \subseteq \{\left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right) : a, b, c, e \in \mathbf{Z}_{(2)},\ a \equiv_2 e \equiv_2 b \equiv_2 c,\ e \equiv_4 a + b + c\} = J_3 \ .$$

This proves the *claim.*

So we have $\omega_{\underline{y}}^{\mathbf{Z}}(\iota(\mathfrak{d}_2)) = I_1 \cap J_3 \cap \mathbf{Z}^{2\times 2}$.

To determine $\omega_{\underline{y}}^{\mathbf{Z}}(\iota(\mathfrak{d}_5))$, it is sufficient to determine the image of $\iota(\mathfrak{d}_5)_{(p)}$ in $\Lambda_{(p)}$ for p prime.

For $p \neq 5$ prime we have $(\mathfrak{d}_5)_{(p)} = \mathbf{Z}[\alpha]_{(p)}$ and therefore $\omega_{\underline{y}}^{\mathbf{Z}_{(p)}}\big(\iota((\mathfrak{d}_5)_{(p)})\big) = \Lambda_{(p)}$.

We *claim* that the image of $(\mathfrak{d}_5)_{(5)}$ in $\Lambda_{(5)}$ is given by

$$I_6 = \begin{pmatrix} \mathbf{Z}_{(5)} & (5) \\ (5) & (5) \end{pmatrix} = {}_{\mathbf{Z}_{(5)}}\langle \left(\begin{smallmatrix} 5 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 5 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 5 \end{smallmatrix}\right)\rangle \ .$$

Consider the images of the $\mathbf{Z}_{(5)}$-linear basis $\underline{r} = (-5, \alpha, -5\sigma, \alpha\sigma)$ of $(\mathfrak{d}_5)_{(5)}(\mathbf{Z}[\alpha] \wr G)$.

$$\begin{array}{rcl} -5 & \mapsto & \left(\begin{smallmatrix} -5 & 0 \\ 0 & -5 \end{smallmatrix}\right) \\ \alpha & \mapsto & \left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right) \\ -5\sigma & \mapsto & \left(\begin{smallmatrix} -5 & 0 \\ 0 & 5 \end{smallmatrix}\right) \\ \alpha\sigma & \mapsto & \left(\begin{smallmatrix} 0 & 5 \\ 1 & 0 \end{smallmatrix}\right) \ . \end{array}$$

We have ${}_{\mathbf{Z}_{(5)}}\langle \left(\begin{smallmatrix} 5 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 5 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 5 \end{smallmatrix}\right)\rangle \subseteq {}_{\mathbf{Z}_{(5)}}\langle \left(\begin{smallmatrix} -5 & 0 \\ 0 & -5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -5 & 0 \\ 0 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 5 \\ 1 & 0 \end{smallmatrix}\right)\rangle$ because of

$$\begin{array}{rcl} \left(\begin{smallmatrix} 5 & 0 \\ 0 & 0 \end{smallmatrix}\right) & = & \frac{1}{2}\big(-\left(\begin{smallmatrix} -5 & 0 \\ 0 & -5 \end{smallmatrix}\right) - \left(\begin{smallmatrix} -5 & 0 \\ 0 & 5 \end{smallmatrix}\right)\big) \\ \left(\begin{smallmatrix} 0 & 5 \\ 0 & 0 \end{smallmatrix}\right) & = & \frac{1}{2}\big(-\left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 5 \\ 1 & 0 \end{smallmatrix}\right)\big) \\ \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) & = & \frac{1}{2}\big(\left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 5 \\ 1 & 0 \end{smallmatrix}\right)\big) \\ \left(\begin{smallmatrix} 0 & 0 \\ 0 & 5 \end{smallmatrix}\right) & = & \frac{1}{2}\big(-\left(\begin{smallmatrix} -5 & 0 \\ 0 & -5 \end{smallmatrix}\right) + \left(\begin{smallmatrix} -5 & 0 \\ 0 & 5 \end{smallmatrix}\right)\big) \ . \end{array}$$

Conversely, we have ${}_{\mathbf{Z}_{(5)}}\langle \left(\begin{smallmatrix} -5 & 0 \\ 0 & -5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -5 & 0 \\ 0 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 5 \\ 1 & 0 \end{smallmatrix}\right)\rangle \subseteq \begin{pmatrix} \mathbf{Z}_{(5)} & (5) \\ (5) & (5) \end{pmatrix}$.

This proves the *claim.*

So we have $\omega_{\underline{y}}^{\mathbf{Z}}(\iota(\mathfrak{d}_5)) = I_6 \cap J_1 \cap \mathbf{Z}^{2\times 2}$.

Now we consider $\mathfrak{d}_2\mathfrak{d}_5 = (2, \alpha + 1)(\alpha) = (2\alpha, \alpha - 5) = (10, \alpha - 5)$.

As $\omega_{\underline{y}}^{\mathbf{Z}}$ is a ring isomorphism, we obtain

$$\begin{array}{rcl} \omega_{\underline{y}}^{\mathbf{Z}}(\iota(\mathfrak{d}_2\mathfrak{d}_5)) & = & \omega_{\underline{y}}^{\mathbf{Z}}(\iota(\mathfrak{d}_2))\,\omega_{\underline{y}}^{\mathbf{Z}}(\iota(\mathfrak{d}_5)) \\ & = & (I_1 \cap J_3 \cap \mathbf{Z}^{2\times 2})(I_6 \cap J_1 \cap \mathbf{Z}^{2\times 2}) \\ & = & I_6 \cap J_3 \cap \mathbf{Z}^{2\times 2} \ . \end{array}$$

Since

$$\omega_{\underline{y}}^{\mathbf{Z}}\left(\iota(\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha]))\right) \subsetneq \mathrm{Ideals}^{\times}(\Lambda) = \omega_{\underline{y}}^{\mathbf{Z}}(\mathrm{Ideals}^{\times}(\mathbf{Z}[\alpha] \wr G)) \ ,$$

we have

$$\iota(\mathrm{Ideals}^{\times,G}(\mathbf{Z}[\alpha])) \subsetneq \mathrm{Ideals}^{\times}(\mathbf{Z}[\alpha] \wr G) \ ,$$

and so the map ι is not surjective.

The ideal

$$\left(\begin{smallmatrix} \mathbf{Z}_{(5)} & (5) \\ \mathbf{Z}_{(5)} & \mathbf{Z}_{(5)} \end{smallmatrix}\right) \cap \left(\begin{smallmatrix} (2) & (2) \\ (2) & (2) \end{smallmatrix}\right) \cap \mathbf{Z}^{2\times 2} = I_1 \cap J_6 \cap \mathbf{Z}^{2\times 2}$$

is of index 2^2 in Λ, but it is not contained in the image of $\omega_{\underline{y}}^{\mathbf{Z}} \circ \iota$. □

8 Appendix

Lemma A 1. *Let R be a ring. Let*

$$\begin{tikzcd}
M' \arrow[r, "\mu"] \arrow[d, "\varphi'"'] & M \arrow[d, "\varphi"'] \\
N' \arrow[r, "\nu"] & N
\end{tikzcd}$$

be a commutative quadrangle of R-modules and R-linear maps. Write $\overline{M} := M/\mu(M')$ and $\overline{N} := N/\nu(N')$. Consider the R-linear maps

$$\begin{array}{rcl} \rho_M : M & \to & \overline{M} \\ m & \mapsto & m + \mu(M')\ , \end{array}$$

$$\begin{array}{rcl} \rho_N : N & \to & \overline{N} \\ n & \mapsto & n + \nu(N')\ . \end{array}$$

Then there exists a unique R-linear map $\overline{\varphi} : \overline{M} \to \overline{N}$, such that

$$\begin{tikzcd}
M' \arrow[r, "\mu"] \arrow[d, "\varphi'"'] & M \arrow[r, "\rho_M"] \arrow[d, "\varphi"'] & \overline{M} \arrow[d, "\overline{\varphi}"'] \\
N' \arrow[r, "\nu"] & N \arrow[r, "\rho_N"] & \overline{N}
\end{tikzcd}$$

commutes, i.e. $\overline{\varphi} \circ \rho_M = \rho_N \circ \varphi$.

If φ' and φ are isomorphisms, then $\overline{\varphi}$ is an isomorphism as well.

Proof. Set

$$\begin{array}{rcl} \overline{\varphi} : \overline{M} & \to & \overline{N} \\ m + \mu(M') & \mapsto & \varphi(m) + \nu(N')\ . \end{array}$$

We show that this is well-defined. Suppose $m + \mu(M') = \tilde{m} + \mu(M')$ for $m, \tilde{m} \in M$. We have $m - \tilde{m} = \mu(m')$ for some $m' \in M'$ and therefore

$$\varphi(m) - \varphi(\tilde{m}) = \varphi(m - \tilde{m}) = \varphi(\mu(m')) = \nu(\varphi'(m')) \in \nu(N')\ .$$

So $\varphi(m) + \nu(N') = \varphi(\tilde{m}) + \nu(N')$. Since φ is R-linear, $\overline{\varphi}$ is R-linear as well.

Since ρ_M is surjective, $\overline{\varphi}$ is unique with respect to $\overline{\varphi} \circ \rho_M = \rho_N \circ \varphi$.

Suppose that φ' and φ are isomorphisms. Since φ is surjective, so is $\rho_N \circ \varphi = \overline{\varphi} \circ \rho_M$ and hence so is $\overline{\varphi}$.

It remains to show that $\overline{\varphi}$ is injective, i.e. that kernel of $\overline{\varphi}$ is zero. Therefor we need to show that for $m \in M$ with $\varphi(m) \in \nu(N')$ it follows that $m \overset{!}{\in} \mu(M')$. Choose $n' \in N'$ with $\varphi(m) = \nu(n')$. Since φ' is surjective, we may choose $m' \in M'$ with $\varphi'(m') = n'$. We get

$$\varphi(m) = \nu(n') = \nu(\varphi'(m')) = \varphi(\mu(m')) \ .$$

Because of φ being injective, it follows that $m = \mu(m') \in \mu(M')$. □

Magma Code A 2 (for Proposition 34)**.**
Consider the $\mathbf{Z}$-linear basis $\underline{y} = (1, \delta, \delta^2, \eta, \delta\eta, \delta^2\eta)$ of $\mathbf{Z}[\delta, \eta]$. We determine the congruences describing the image of $\omega_{\underline{y}}^{\mathbf{Z}}$. Then we simplify them by conjugating with elementary matrices and counting the number of emerging zeroes.

```
MRZ6 := MatrixRing(Integers(),6);

de:=MRZ6!Matrix([[0,0,2,0,0,0], [1,0,0,0,0,0], [0,1,0,0,0,0],
                 [0,0,0,0,0,2],[0,0,0,1,0,0],[0,0,0,0,1,0]]);
et:=MRZ6!Matrix([[0,0,0,1,-2,0],[0,0,0,0,1,-2], [0,0,0,-1,0,1],
                 [1,0,0,-1,-2,2],[0,1,0,1,-1,-2],[0,0,1,-1,1,-1]]);
I :=MRZ6!Matrix([[1,0,0,0,0,0], [0,1,0,0,0,0], [0,0,1,0,0,0],
                 [0,0,0,1,0,0],[0,0,0,0,1,0],[0,0,0,0,0,1]]);
s2:=MRZ6!Matrix([[1,0,0,-1,-2,2], [0,1,0,1,-1,-2], [0,0,1,-1,1,-1],
                 [0,0,0,-1,0,0],[0,0,0,0,-1,0],[0,0,0,0,0,-1]]);
s3:=MRZ6!Matrix([[1,0,0,0,0,0], [0,1,0,1,-1,-2], [0,0,-2,1,-1,1],
                 [0,0,-2,1,0,0],[0,1,0,1,0,-2],[0,1,-1,1,-1,-1]]);

im_list_mat:=[I, de, de^2, et, de*et, de^2*et,
              s2, de*s2, de^2*s2, et*s2, de*et*s2,
              de^2*et*s2,s3, de*s3, de^2*s3, et*s3, de*et*s3,
              de^2*et*s3, s3*s2, de*s3*s2, de^2*s3*s2, et*s3*s2,
              de*et*s3*s2, de^2*et*s3*s2, s3^2, de*s3^2, de^2*s3^2,
              et*s3^2, de*et*s3^2, de^2*et*s3^2,s2*s3, de*s2*s3,
              de^2*s2*s3, et*s2*s3, de*et*s2*s3, de^2*et*s2*s3];

im_list:=[ElementToSequence(x): x in im_list_mat];

MRQ36 := MatrixRing(Rationals(),36);
A := Transpose(MRQ36!im_list);
MR18_36 := MatrixRing(Integers(18),36);
AI := MR18_36!(18*A^-1); //contains the congruences modulo 18
AI := EchelonForm(AI);
AI := RowSubmatrix(AI,[1..Rank(AI)]);




//Determination of elementary matrices for conjugation
P := [];
for k in [1..6] do
 for l in [1..6] do
```

```
  if k ne l then
   for x in [1,-1,2,-2,3,-3,4,-4,5,-5,6,-6,7,-7,8,-8,9] do
    P cat:= [<k,l,x>];
   end for;
  end if;
 end for;
end for;
P := [<1,2,0>] cat P; // trivial operation


Mat_L := function(k,l,x)
 L := MR18_36!1;
 for i in [0..5] do
  L[k+6*i,l+6*i] := x;
 end for;
 return L;
end function;

Mat_R := function(k,l,x)
 R := MR18_36!1;
 for i in [1..6] do
  R[6*(l-1)+i,6*(k-1)+i] := x;
 end for;
 return R;
end function;


number_of_zeroes := function(B);
 return #[B[i,j] : i in [1..NumberOfRows(B)],
                   j in [1..NumberOfColumns(B)] | B[i,j] eq 0];
end function;

Z:=AI;
k:=0;
repeat
    k:=k+1;
    noz_min := number_of_zeroes(Z);
    p_min := <1,2,0>;
    q_min := <1,2,0>;
    AI_min := Z;
    for p in P do // p[1] = k, p[2] = l, p[3] = x
      for q in P do
        if <p[1],p[2]> ne  <q[1],q[2]> then
           AI_test := EchelonForm(Z * Mat_R(p[1],p[2],-p[3])
                                    * Mat_L(p[1],p[2],p[3])
                                    * Mat_R(q[1],q[2],-q[3])
                                    * Mat_L(q[1],q[2],q[3]) );
```

```
          noz_test := number_of_zeroes(AI_test);
             if noz_test gt noz_min then
                noz_min := noz_test;
                p_min := p;
                q_min := q;
                AI_min := AI_test;
// to monitor the progress
                print "k, noz_min, q_min, p_min := ",k, noz_min, q_min, p_min;

             end if;
        end if;
      end for;
    end for;
    Z:=AI_min;
until (p_min eq <1,2,0>) and (q_min eq <1,2,0>);


index := function(A,n) // An integer matrix containing congruences modulo n
 D,S,T := SmithForm(A);
 G:=DiagonalMatrix(Integers(), Diagonal(D));
 return &*[n/Gcd(n,x) : x in Diagonal(G)];
end function;

index(Z,18);
```

Magma Code A 3 (for Lemma 56).

```
Z := Integers();
R := loc< Z | 2>;
M := MatrixRing(R,2);

b1 := M!Matrix([[1,0],[0,1]]);//R-linear basis
b2 := M!Matrix([[0,0],[0,2]]);
b3 := M!Matrix([[0,1],[1,0]]);
b4 := M!Matrix([[0,0],[2,0]]);
RS,f := sub<M | b1,b2,b3,b4>;




//Representatives of elements of RS/RS8

Interval := [-3..4];
RepList := [a1 * b1 + a2 * b2 + a3 * b3 + a4 * b4 : a1 in Interval,
                                                     a2 in Interval,
                                                     a3 in Interval,
                                                     a4 in Interval];
RS8 := ideal<RS | 8>;
IdealList := [RS8];
i := 1;
while i le #IdealList do
 for r in RepList do
  I_new := ideal<RS|IdealList[i],r>;
  if not I_new in IdealList then
   IdealList := IdealList cat [I_new];
  end if;
 end for;
 print #IdealList, i; // to monitor the progress
 i +:= 1;
end while;

Ideals_2Power := [ideal< RS | 2^k> : k in [1..3]];
RemovePos := {};
for i in [1..#IdealList] do
 for j in [1..#IdealList] do
  for IP in Ideals_2Power do
   if IdealList[i] eq IdealList[j] * IP then
    RemovePos := RemovePos join {i};
   end if;
  end for;
 end for;
end for;

IdealList_short := [IdealList[i] : i in [1..#IdealList] | not i in RemovePos];

Bases_IdealList_short := [Basis(I) : I in IdealList_short];
```

Magma Code A 4 (for Lemma 58).

```
Z := Integers();
R := loc< Z | 2>;
M := MatrixRing(R,2);

b1 := M!Matrix([[1,0],[0,1]]);// R- linear basis
b2 := M!Matrix([[0,0],[0,2]]);
b3 := M!Matrix([[0,2],[1,0]]);
b4 := M!Matrix([[0,0],[2,0]]);
RS,f := sub<M | b1,b2,b3,b4>;
```

```
//Representatives of elements of RS/RS16

Interval := [-7..8];
RepList := [a1 * b1 + a2 * b2 + a3 * b3 + a4 * b4 : a1 in Interval,
                                                    a2 in Interval,
                                                    a3 in Interval,
                                                    a4 in Interval];
RS16 := ideal<RS | 16>;
IdealList := [RS16];
i := 1;
while i le #IdealList do
   for r in RepList do
     I_new := ideal<RS|IdealList[i],r>;
     if not I_new in IdealList then
        IdealList := IdealList cat [I_new];
     end if;
   end for;
   print  #IdealList, i; // to monitor the progress
   i +:= 1;
end while;

Ideals_2Power := [ideal< RS | 2^k> : k in [1..4]];
RemovePos := {};
for i in [1..#IdealList] do
   for j in [1..#IdealList] do
      for IP in Ideals_2Power do
         if IdealList[i] eq IdealList[j] * IP then
            RemovePos := RemovePos join {i};
         end if;
      end for;
   end for;
end for;

IdealList_short := [IdealList[i] : i in [1..#IdealList] | not i in RemovePos];

Bases_IdealList_short := [Basis(I) : I in IdealList_short];
```

Bibliography

[1] Charles W. Curtis, Irving Reiner, *Methods of representation theory I,* Wiley, 1990.

[2] Paul M. Cohn, *Basic algebra: groups, rings and fields,* Springer, 2003.

[3] Matthias Künzer, *On representations of twisted group rings,* arXiv:math/0301125v1, 2008. http://arxiv.org/pdf/math/0301125.pdf

[4] Serge Lang, *Algebra*, Addison-Wesley, 3. ed., repr. with corrections, 1993.

[5] Keith Conrad, *The splitting field of* $X^3 - 2$ *over* $\mathbf{Q}$, www.math.uconn.edu/~kconrad/blurbs/gradnumthy/Qw2.pdf, 2006 (last access 31.08.2015)

[6] Jürgen Neukirch, *Algebraic number theory*, Springer, 1999.

[7] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235-265.

Zusammenfassung

Sei A ein Dedekind-Bereich mit perfektem Quotientenkörper K. Sei B der ganze Abschluss von A in einer Galois-Erweiterung L von K von Grad n, mit Galois-Gruppe G.

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[d, dash, "{G,\ |G|=n}"] \\
B \arrow[d, dash] & K \\
A \arrow[ur, dash] &
\end{tikzcd}$$

Wir untersuchen den getwisteten Gruppenring $L \wr G$. Dieser hat G als L-lineare Basis und die Multiplikation involviert die Gruppenoperation von G auf L.

Wir betrachten den Wedderburn-Isomorphismus $\omega_{\underline{y}} : L \wr G \to K^{n\times n}$, wobei $\underline{y}$ eine K-lineare Basis von L ist. Gibt es eine Basis $\underline{y}$, die zugleich eine A-lineare Basis von B ist, dann kann $\omega_{\underline{y}}$ auf $B \wr G$ und $A^{n\times n}$ eingeschränkt werden. Dann ist

$$B \wr G \xrightarrow{\sim} \omega_{\underline{y}}(B \wr G) \subseteq A^{n\times n} \ .$$

Im Fall von quadratischen Erweiterungen $\mathbf{Q}(\sqrt{d})|\mathbf{Q}$ für $d \in \mathbf{Z}^\times$ quadratfrei, im Fall von Kreisteilungskörpern $\mathbf{Q}(\zeta_p)|\mathbf{Q}$ für $p \in \mathbf{Z}_{>0}$ prim, sowie für $\mathbf{Q}(\zeta_9)|\mathbf{Q}$ und $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)|\mathbf{Q}$ geben wir eine explizite Beschreibung des Bildes dieser Einschränkung $\omega_{\underline{y}}(B \wr G)$ in $A^{n\times n}$ über Kongruenzen von Matrixeinträgen an. Die Komplexität dieser Beschreibung hängt stark von der gewählten Basis $\underline{y}$ ab.

Für $\mathbf{Q}(\zeta_9)|\mathbf{Q}$ und daher $B = \mathbf{Z}[\zeta_9]$ ist es wider Erwarten vorteilhaft, anstelle einer Beschreibung von $\omega_{\underline{y}}(\mathbf{Z}[\zeta_9] \wr G)$ in $\mathbf{Z}^{6\times 6}$ eine Beschreibung in $\mathbf{Q}^{6\times 6}$ zu suchen. Hierfür wird eine $\mathbf{Q}$-lineare Basis von $\mathbf{Q}(\zeta_9)$ verwendet, die in $\mathbf{Z}[\zeta_9]$ enthalten ist, aber keine $\mathbf{Z}$-lineare Basis davon ist.

Falls A eine endliche Erweiterung von $\mathbf{Z}$ ist, geben wir eine explizite Formel zur Bestimmung des Index von $\omega_{\underline{y}}(B \wr G)$ in $A^{n\times n}$ an.

Mit Hilfe der Beschreibung von $\omega_{\underline{y}}(B \wr G)$ wird gezeigt, dass es in $B \wr G$ nichtverschwindende Ideale gibt, die nicht von der Form $\mathfrak{b}(B \wr G)$ sind für ein Galois-stabiles Ideal $\mathfrak{b} \subseteq B$. D.h. die injektive Abbildung $\mathfrak{b} \mapsto \mathfrak{b}(B \wr G)$ von der Menge der nichtverschwindenden Galois-stabilen Ideale von B in die Menge der nichtverschwindenden Ideale von $B \wr G$ ist im Allgemeinen nicht surjektiv.

Ist A eine endliche Erweiterung von $\mathbf{Z}$, dann ist der Index von $\mathfrak{b}(B \wr G)$ in $B \wr G$ eine $|G|$-te Potenz einer natürlichen Zahl. Die Annahme, dass alle Ideale in $B \wr G$, deren Index dies erfüllt, im Bild unserer Abbildung liegen, erweist sich beispielsweise im Fall von $B = \mathbf{Z}[\sqrt{-5}]$ als nicht zutreffend.

Hiermit versichere ich,

1. dass ich meine Arbeit selbstständig verfasst habe,
2. dass ich keine anderen als die angegebenen Quellen benutzt und alle wörtlich oder sinngemäß aus anderen Werken übernommenen Aussagen als solche gekennzeichnet habe,
3. dass die eingereichte Arbeit weder vollständig noch in wesentlichen Teilen Gegenstand eines anderen Prüfungsverfahrens gewesen ist und
4. dass das elektronische Exemplar mit den anderen Exemplaren übereinstimmt.

Stuttgart, im November 2015

Nora Krauß