Johannes Bartenschlager 11.11.2022

# On the Application of a Result about Lattices to Algebraic Number Theory

In the following we consider $\mathbb{Z}^n \subseteq \mathbb{R}^n$ for some $n \in \mathbb{N}$ with the canonical basis $e_1, ..., e_n$.

**Definition 1.** We say $x \in \mathbb{R}^n$ has dimensionality $d$ if it has exactly $d$ non-zero coefficients in the canonical basis.

For convenience we introduce the following notion.

**Definition 2.** For a lattice $\Lambda \subseteq \mathbb{Q}^n$ and $x \in \Lambda$ we say $x \neq 0$ is reduced if it is of the form

$$x = \sum_{j=1}^{n} \frac{a_j}{b_j} e_j$$

with $0 \leq a_j < b_j$ and $(a_j, b_j) = 1$ for all $j = 1, ..., n$.

Note that if $\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Q}^n$ every element $x$ therin is of the form $x = x' + y$ for $x' \in \Lambda - \mathbb{Z}^n$ reduced and $y \in \mathbb{Z}^n$. Further we observe that elements in $\mathbb{Z}^n$ are not reduced by definition.

**Lemma 1.** *Consider a lattice $\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Q}^n$. Assume there is some $d \in \mathbb{Z}$ and a map*

$$\begin{aligned} \sigma : \Lambda &\to \Lambda, \\ e_j &\mapsto e_{j+1} \text{ for } j = 1, ..., n-1, \\ e_n &\mapsto d e_1. \end{aligned}$$

*Assume $\Lambda$ has no reduced elements of dimensionalities $n-m, ..., n-1$, then the reduced elements of dimensionality $n$ are of the form*

$$x = \frac{1}{b} \sum_{j=1}^{n} a_j e_j$$

*and for all $i = 1, ..., n-1$, at least $m$ of the expressions*

$$\frac{a_i a_1 - a_{i+1} a_n d}{b} \text{ or}$$

$$\frac{a_i a_j - a_{i+1} a_{j-1}}{b} \text{ for } j = 2, ..., n,$$

*are integral.*

*Proof.* Assume $\Lambda$ has a reduced element $x$ of dimensinality $n$:

$$x = \sum_{j=1}^{d} \frac{a_j}{b_j} e_j$$

with the coefficients being reduced fractions, at least two are different, and all non-zero.

First we may assume that there is some $b_i \leq b_j$ for all $i \neq j$ but strictly for at least one $j$. Then $\frac{a_j b_i}{b_j} \in \mathbb{Q} - \mathbb{Z}$, hence

$$b_i x - a_i e_i = \sum_{j=1, i \neq j}^{d} \frac{a_j b_i}{b_j} e_j \in \Lambda - \mathbb{Z}^n$$

is reduced and of dimensionality $d-1$, which violates the assumption.

Hence $x$ is of the form

$$x = \frac{1}{b} \sum_{j=1}^{n} a_j e_j.$$

Consider for $i \neq n$ the element

$$\begin{aligned}(a_i \,\mathrm{id} - a_{i+1}\sigma)x =& \frac{1}{b}\left((a_i a_1 - a_{i+1}a_n d)e_1 + \sum_{j=2}^{n}(a_i a_j - a_{i+1}a_{j-1})e_j\right) \\ =& \frac{1}{b}\left((a_i a_1 - a_{i+1}a_n d)e_1 + \sum_{j=2, j\neq i+1}^{n}(a_i a_j - a_{i+1}a_{j-1})e_j\right) \in \Lambda.\end{aligned}$$

By assumption the reduction of this element has dimensionality at most $n-m-1$, hence at least $m$ coefficient lie in $\mathbb{Z}$. □

**Remark.** Note that diagonal elements, i.e., elements where all nominators are equal, satisfy this condition, but other reduced elements could exist. There is a restriction nevertheless, in some cases there are either diagonal elements or non-diagonal elements. If we have both, we could reduce the dimensionality, but not necessarily to dimension one less but more, where the assumption does not hold anyway.

We lastly state another theorem which simplifies some cases.

**Lemma 2.** *Let $\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Q}^n$ be a lattice and $x \in \Lambda$ be reduced and of the form*

$$x = \frac{1}{b} \sum_{j=1}^{d} a_j e_j.$$

*Then there is some reduced $\tilde{x}$ with $a_i = 1$ for at least one $i = 1, ..., n$.*

*Proof.* Since $x$ is reduced at least one $a_i$ is non-zero and $(a_i, b) = 1$. Let $\mathbf{1} = \sum_{j=1}^{d} e_j$, then $y = \mathbf{1} - x$ can be reduced to $y'$ since $\mathbb{Z}^n \subseteq \Lambda$. Now

$$y' = \frac{1}{b} \sum_{j=1}^{d} c_j e_j$$

and $c_i = b - a_i$. We can now apply the Euclidean Algorithm, since $(a_i, b) = (b - a_i, b) = 1$, to construct some element $z \in \Lambda$ which has $i$th coefficient $\frac{1}{b}$. We set $\tilde{x} = z'$ the reduction of $z$. □

**Remark.** This also applies to diagonal elements, i.e., if all numerators are the same, we can choose it to be 1.

**Application.** We can apply the results above to compute rings of integers for some small radical extensions. For a number field $K = \mathbb{Q}(\sqrt[n]{d})$ of degree $n$, $d \neq \pm 1$ free of an $n$th power, we have the canonical order $\mathbb{Z}[\sqrt[n]{d}] \subseteq \mathcal{O}_K$ and the powers of $\sqrt[n]{d}$ serve as canonical basis elements.

In $\mathcal{O}_K$ a symmetry as in Lemma 1 holds: Multiplication with $\sqrt[n]{d}$ almost only cyclically permutes the basis, but in addition it also changes the coefficient of 1, hence in the canonical basis multiplication with $\sqrt[n]{d}$ is the same as the map $\sigma : \Lambda \to \Lambda$ from above.

Note that w.l.o.g., we can assume that the coefficient of 1 of a non-zero element is always non-zero since multiplication with $\sqrt[n]{d}$ cyclically permutes the coefficients.

The assumption of dimensionality for an element allowed to write it with only non-zero coefficients, we now have to consider zero coefficients. The multiplication with powers of $\sqrt[n]{d}$ cyclically permutes the zero coefficients but does not allow to change their distribution. For example multiplication with powers of $\sqrt[4]{d}$ cannot change an element of the form $a + b\sqrt[4]{d}$ to an element of the form $c + d\sqrt[4]{d^2}$. So we have to consider all possible combinations for all dimensionalities up to cyclic permutations.

The strategy is now the following:

1. We apply Lemma 2 and check in any dimensionality, in all possible combinations of basis elements, that do not admit a symmetry as in Lemma 1, whether reduced elements are integral, by computing the characteristic polynomial. This might not suffice, but here further investigations can be made.

2. In the cases that admit a symmetry as in Lemma 1, we check diagonal elements.

3. If there are no diagonal elements and no reduced elements of fewer dimensionality, we have to apply Lemma 1 and check for elements with the restrictions on the coefficients.

4. At the end we collect as many different linearly independent elements as we find and check for linearly independence to get an integral basis.

**Example 1.** We compute the ring of integers of $K = \mathbb{Q}(\sqrt{d})$, for $d$ square-free. We follow the path from before and start by elements of dimensionality 1: Since $\mathbb{Z}$ is integrally closed and $d$ is square-free there canot be reduced elements of dimensionality 1.

We check for reduced elements of dimensionality 2.

$$\frac{1}{b}\left(1 + a_2\sqrt{d}\right) \rightsquigarrow \frac{1}{b}\begin{pmatrix} 1 & a_2 d \\ a_2 & 1 \end{pmatrix} \rightsquigarrow \lambda^2 - \frac{2}{b}\lambda + \frac{1 - a_2^2 d}{b^2}.$$

Thus only $b = 2$ is possible. Hence there are no reduced non-diagonal elements because $0 < a_2 < 2$ forces $a_2 = 1$.

This now gives

$$\lambda^2 - \frac{2}{b}\lambda + \frac{1 - d}{b^2}$$

for the characteristic polynomial. Hence for $d \equiv 1 (\mathrm{mod}\, 4)$ we conclude that $\omega = \frac{1+\sqrt{d}}{2}$ is integral.

Since the degree of the number field is 2 and there are no other diagonal elements we conclude that $\mathcal{O}_K = \mathbb{Z}[\omega]$.

**Example 2.** We compute the ring of integers of $K = \mathbb{Q}(\sqrt[3]{d})$ for $d \neq \pm 1$ cubic-free. We follow the path from the application and start by elements of dimensionality 1: Since $\mathbb{Z}$ is integrally closed and $d$ is cube-free, there canot be reduced elements of dimensionality 1.

We check for reduced elements of dimensionality 2:

$$\frac{1}{b}(1 + a_2\sqrt[3]{d}) \rightsquigarrow \frac{1}{b}\begin{pmatrix} 1 & 0 & a_2 d \\ a_2 & 1 & 0 \\ 0 & a_2 & 1 \end{pmatrix} \rightsquigarrow \lambda^3 - \frac{3}{b}\lambda^2 + \frac{3}{b^2}\lambda - \frac{1 + a_2^3 d}{b^3}.$$

Thus $b = 1$ since 3 is square-free from the third coefficient and there are no reduced elements of dimensionality 2.

We consider reduced elements of dimensionality 3:

$$\frac{1}{b}(1 + a_2\sqrt[3]{d} + a_3\sqrt[3]{d^2}) \rightsquigarrow \frac{1}{b}\begin{pmatrix} 1 & a_3 d & a_2 d \\ a_2 & 1 & a_3 d \\ a_3 & a_2 & 1 \end{pmatrix}$$

$$\rightsquigarrow \lambda^3 - \frac{3}{b}\lambda^2 + \frac{3(1 - a_2 a_3 d)}{b^2}\lambda - \frac{1 - 3a_2 a_3 d + a_2^3 d + a_3^3 d^2}{b^3}.$$

Thus only $b = 3$ is allowed because of the second coefficient.

The diagonal case reduces the characteristic polynomial to

$$\lambda^3 - \frac{3}{b}\lambda^2 + \frac{3(1 - d)}{b^2}\lambda - \frac{(1 - d)^2}{b^3}.$$

But then the third coefficient demands $3|1-d$ and with the fourth we conclude $d \equiv 1 (\mathrm{mod}\, 9)$ has to be satisfied for diagonal elements. Hence in this case $\omega = \frac{1 + \sqrt[3]{d} + \sqrt[3]{d^2}}{3}$ is integral.

Since there are no elements of dimensionality 1 and 2 and no diagonal elements if $d \not\equiv 1 (\mathrm{mod}\, 9)$, reduced elements could exist. Reducedness implies $0 < a_2, a_3 < 3$. The third coefficient in the non-diagonal case now requires $3|1 - a_2 a_3 d$. If $3|d$ this cannot hold and there are no reduced integral elements.

We now apply Lemma 1 for $i = 1$ and need all expressions therin to be integral. For $j = 2$ the expression vanishes by construction. For $j = 3$ we get $3|a_3 - a_2^2$ which means, since non-zero squares mod 3 are 1, that $a_3 = 1$. Since we are in the non-diagonal case $a_2 = 2$. The coefficients of the characteristic polynomial now give the conditions $3|1+d$, and $27|1 + 2d + d^2 = (1 + d)^2$, i.e., $9|(1 + d)$. We conclude that

$$\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{d}] \text{ for } d \not\equiv \pm 1 \bmod 9$$

and

$$\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{d}, \omega] \text{ for } \omega = \begin{cases} \frac{1 + \sqrt[3]{d} + \sqrt[3]{d^2}}{3}, & d \equiv 1 \bmod 9, \\ \frac{1 + 2\sqrt[3]{d} + \sqrt[3]{d^2}}{3}, & d \equiv 8 \bmod 9. \end{cases}$$