#A74 INTEGERS 21 (2021)

AN ELEMENTARY COMPUTER ASSISTED UNIQUE FACTORIZATION TEST

Sándor Szabó
Institute of Mathematics and Informatics, University of Pécs, Hungary
sszabo7@hotmail.com

Received: 8/3/20, Accepted: 7/5/21, Published: 7/9/21

Abstract

It will be shown that the unique factorization property of the algebraic integers in certain algebraic number fields can be verified by a relatively straightforward computer assisted computation. The argument is based on a systematic use of the Dedekind-Hasse criterion and a less systematic geometric representation of the tested ring of the algebraic integers.

1. Introduction

Let R be the ring of integers of a number field F. We say that $\tau \in F$ has the Dedekind-Hasse property or satisfies the Dedekind-Hasse criterion if either $\tau \in R$ or there are $\gamma, \delta \in R$ such that $0 < |N(\tau\gamma + \delta)| < 1$. Here $N(\alpha)$ is the norm of α. It is known that if each element of F has the Dedekind-Hasse property, then R is a unique factorization domain. This is the so-called Dedekind-Hasse criterion. The proposed procedure is based on the following plan. We establish that there is a positive integer s such that checking the Dedekind-Hasse property of the elements of F reduces to checking the property for the elements of the test sets

$$T_p = \{(1/p)(i_1\alpha_1 + \cdots + i_n\alpha_n) : 0 \leq i_1, \ldots, i_n \leq p-1\},$$

where $p \leq s$ is a rational prime and $\alpha_1, \ldots, \alpha_n$ is an integral basis of R. Elements of T_p stay in T_p after multiplying them by an element of R if we reduce the coefficients modulo 1. First we establish the Dedekind-Hasse property of some elements of T_p by a simple inspection of the norms of the elements. Then we choose an element $\beta \in T_p$ for which we consider the map $f_\beta : T_p \to T_p$ defined by $f_\beta(x) = \beta x$. If $\tau \in T_p$ has the Dedekind-Hasse property, then so does τ', where $\tau = f_\beta(\tau')$. In the case when f_β is a permutation of the elements of T_p, then one can verify the Dedekind-Hasse property of elements forming complete cycles of this permutation. The element β is chosen by trial and error.

We illustrate the test working out three examples.

The ring R of all integers of an algebraic number field F is known to be a unique factorization domain if and only if F has a class number $h_F = 1$. There are efficient algorithms for computing h_F. The paper develops certain guide lines for trying to prove that $h_F = 1$. The essential point is that we do not use ideal theory and we do not even mention such a concept as class number. In this sense our approach is very elementary. The merit of our approach is that the price of the basic arithmetic operations as addition, subtraction, and multiplication is going down rapidly with the increase of the capabilities of the computers and we are replacing concepts that require considerable time to master with completely mechanical number crunching. It makes accessible proving of the unique factorization property for a technically less sophisticated audience. We would like to point out that there is no guarantee that our approach works in connection with a particular given number field at all. However, when it works one can try to extend it to compute the class number h_F. But the resulting computation does not compare well with the more advanced techniques of computational algebraic number theory.

2. The Dedekind-Hasse property

We will use two observations about the Dedekind-Hasse property. For easier reference we spell these out as lemmas.

Lemma 1. *If $\rho \in R$, $\tau, \tau' \in F$ and $\tau' = \tau + \rho$ has the Dedekind-Hasse property, then so does τ.*

Proof. Suppose that τ' has the Dedekind-Hasse property. If $\tau' \in R$, then $\tau \in R$ and so it has the Dedekind-Hasse property by definition. We may assume that $\tau' \notin R$ and so there are $\gamma', \delta' \in R$ such that $0 < |N(\tau'\gamma' + \delta')| < 1$. Now $\tau \notin R$ and we have to show that there are $\gamma, \delta \in R$ with $0 < |N(\tau\gamma + \delta)| < 1$. Set $\gamma = \gamma'$ and $\delta = \delta' + \rho\gamma'$ and compute $\tau\gamma + \delta$:

$$\tau\gamma + \delta = (\tau' - \rho)\gamma' + \delta' + \rho\gamma' = \tau'\gamma' - \rho\gamma' + \delta' + \rho\gamma' = \tau'\gamma' + \delta'$$

Hence $0 < |N(\tau\gamma + \delta)| < 1$. This completes the proof. □

Lemma 2. *If $\rho \in R$, $\tau, \tau' \in F$ and $\tau' = \tau\rho \notin R$ has the Dedekind-Hasse property, then so does τ.*

Proof. Suppose that τ' has the Dedekind-Hasse property. Since $\tau' \notin R$ there are $\gamma', \delta' \in R$ with $0 < |N(\tau'\gamma' + \delta')| < 1$. Clearly $\tau \notin R$. We should show that there are $\gamma, \delta \in R$ with $0 < |N(\tau\gamma + \delta)| < 1$. Set $\gamma = \rho\gamma'$ and $\delta = \delta'$ and compute $\tau\gamma + \delta$:

$$\tau\gamma + \delta = \tau(\rho\gamma') + \delta' = \tau'\gamma' + \delta'.$$

Hence $0 < |N(\tau\gamma + \delta)| < 1$. This completes the proof. □

3. Covering by Spheres

Let r be a fixed positive real number and let l be a positive integer. Cover the point i/l with the open interval of radius r/l centered at the point for each i, $0 \leq i \leq l$. Repeat this procedure for $l = 1, 2, 3, \ldots$.

Lemma 3. *The unit interval* $[0, 1]$ *will be covered by open intervals after a finite number of steps.*

Proof. We use Farey sequences to prove this claim. The 1st Farey sequence is $0/1, 1/1$. The 2nd Farey sequence is $0/1, 1/2, 1/1$. The 3rd Farey sequence is $0/1, 1/3, 1/2, 2/3, 1/1$. In general the sth Farey sequence is constructed from the $(s-1)$th one by inserting new elements. If a/b and a'/b' are adjacent elements in the $(s-1)$th Farey sequence and $b + b' \leq s$, then we insert $(a + a')/(b + b')$ between a/b and a'/b'. We need only the next two properties of the Farey sequences. If a/b and a'/b' are adjacent elements in the sth Farey sequence, then $b + b' \geq s + 1$ and $(a'/b') - (a/b) = 1/bb'$.

There is an s such that $1/(s + 1) < r \leq 1/s$. Cover the element a/b of the sth Farey sequence with the open interval of radius r/b centered at a/b. Since

$$\frac{a'}{b'} - \frac{a}{b} = \frac{1}{bb'} < \frac{r(s+1)}{bb'} \leq \frac{r(b+b')}{bb'} = \frac{r}{b} + \frac{r}{b'},$$

these open intervals cover the whole unit interval. □

Example 1. Let $r = 0.21$. As $1/5 < r \leq 1/4$ we choose s to be equal to 4. The 4th Farey sequence $0/1, 1/4, 1/3, 2/5, 1/2, 2/3, 3/4, 1/1$ can be used to cover the closed unit interval $[0, 1]$ with the following nine open intervals:

$$\begin{array}{ccc}
\left(\frac{0}{1} - \frac{0.21}{1}, \frac{0}{1} + \frac{0.21}{1}\right), & \left(\frac{1}{4} - \frac{0.21}{4}, \frac{1}{4} + \frac{0.21}{4}\right), & \left(\frac{1}{3} - \frac{0.21}{3}, \frac{1}{3} + \frac{0.21}{3}\right), \\
\left(\frac{2}{5} - \frac{0.21}{5}, \frac{2}{5} + \frac{0.21}{5}\right), & \left(\frac{1}{2} - \frac{0.21}{2}, \frac{1}{2} + \frac{0.21}{2}\right), & \left(\frac{3}{5} - \frac{0.21}{5}, \frac{3}{5} + \frac{0.21}{5}\right), \\
\left(\frac{2}{3} - \frac{0.21}{3}, \frac{2}{3} + \frac{0.21}{3}\right), & \left(\frac{3}{4} - \frac{0.21}{4}, \frac{3}{4} + \frac{0.21}{4}\right), & \left(\frac{1}{1} - \frac{0.21}{1}, \frac{1}{1} + \frac{0.21}{1}\right).
\end{array}$$

We computed the endpoints of the intervals for a few decimal places:

$$\begin{array}{rrr}
(-0.2100, 0.2100), & (0.1975, 0.3025), & (0.2633, 0.4033), \\
(0.3580, 0.4420), & (0.3950, 0.6050), & (0.5580, 0.6420), \\
(0.5966, 0.7366), & (0.6975, 0.8025), & (0.7900, 1.2100),
\end{array}$$

and depict them in Figure 1.

Let r be a fixed positive real number and $\mathbf{a}$, $\mathbf{b}$ independent vectors on the plane. Cover the point $(i/l)\mathbf{a} + (j/l)\mathbf{b}$ with an open circular disc of radius r/l centered at the point for each i, j, $0 \leq i, j \leq l$. Repeat this procedure for $l = 1, 2, 3, \ldots$.

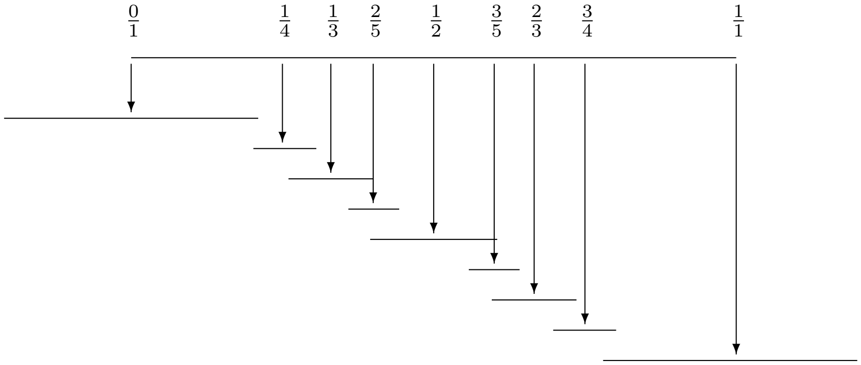

Figure 1: The intervals in Example 1.

Lemma 4. *The parallelogram P spanned by* $\mathbf{a}$ *and* $\mathbf{b}$ *will be covered by open circular discs after a finite number of steps.*

Proof. By Lemma 3, there is a v such that the discs of radius r/l centered at $(i/l)\mathbf{a}$ cover the line of $\mathbf{a}$ as l varies over $1, 2, \dots, v$ and i varies over the integers. Also there is a strip parallel to $\mathbf{a}$ covered by the discs. The line of $\mathbf{b}$ and the strip intersect in an interval, say of radius t. There is an s such that the intervals of radius t/l centered at $(j/l)\mathbf{b}$ cover the line of $\mathbf{b}$ as l runs over $1, 2, \dots, s$ and j runs over the integers. Thus P can be covered by strips and consequently by discs. □

Example 2. Let $r = 0.3$. As $1/4 < r \leq 1/3$ we choose s to be equal to 3. The 3rd Farey sequence $0/1, 1/3, 1/2, 2/3, 1/1$ can be used to cover the closed unit interval $[0, 1]$ with the following five open intervals:

$$\left(\tfrac{0}{1} - \tfrac{0.3}{1}, \tfrac{0}{1} + \tfrac{0.3}{1}\right), \quad \left(\tfrac{1}{3} - \tfrac{0.3}{3}, \tfrac{1}{3} + \tfrac{0.3}{3}\right), \quad \left(\tfrac{1}{2} - \tfrac{0.3}{2}, \tfrac{1}{2} + \tfrac{0.3}{2}\right),$$
$$\left(\tfrac{2}{3} - \tfrac{0.3}{3}, \tfrac{2}{3} + \tfrac{0.3}{3}\right), \quad \left(\tfrac{1}{1} - \tfrac{0.3}{1}, \tfrac{1}{1} + \tfrac{0.3}{1}\right).$$

We computed the endpoints of the intervals for a few decimal places:

$$(-0.3000, 0.3000), \quad (0.2333, 0.4333), \quad (0.3500, 0.6500),$$
$$(0.5666, 0.7666), \quad (0.7000, 1.3000),$$

and we consider five circular discs centered at the elements of the 3rd Farey sequence. The diameters of the circles are equal to intervals we listed. Instead of circular discs in Figure 2 we used squares inscribed into the circles. In this situation a strip appears whose width is equal to

$$\left(\frac{0}{1} + \frac{0.3}{1}\right) - \left(\frac{1}{3} - \frac{0.3}{3}\right) = \frac{0.2}{3}.$$

Of course the strip is wider when we do not replace the circles with squares.

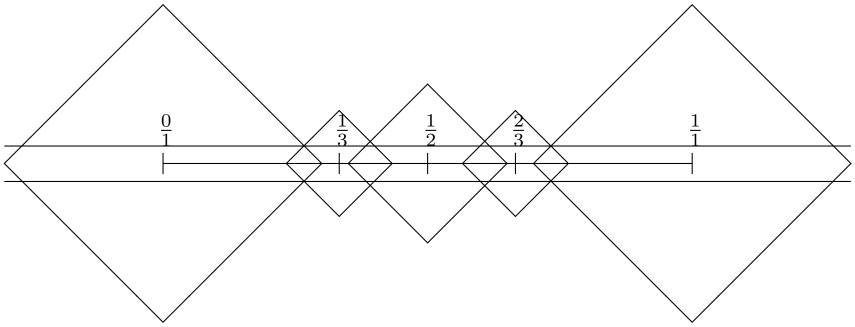

Figure 2: The strip in Example 2.

We can extend Lemma 4 for higher dimensional cases. The 3-dimensional version reads as follows. Let r be a positive real number and let P be the parallelepiped spanned by the independent $\mathbf{a}, \mathbf{b}, \mathbf{c}$ vectors in the 3-space. Cover the point $(i/l)\mathbf{a} + (j/l)\mathbf{b} + (k/l)\mathbf{c}$ with an open sphere of radius r/l centered at the point for each i, j, k, $0 \leq i, j, k \leq l$. Repeat this procedure for $l = 1, 2, 3 \ldots$.

Lemma 5. *After a finite number of steps the parallelepiped P will be covered by open balls.*

4. The Test Sets T_p

Let R be the ring of integers of a number field F. To an integral basis $\alpha_1, \ldots, \alpha_n$ of R we assign the linearly independent vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$. Linear combinations of $\mathbf{a}_1, \ldots, \mathbf{a}_n$ with integer coefficients represent elements of R and with rational coefficients they represent elements of F. In this way we have a geometric version of R and F. Let Q be the field of rational numbers and let Q^n be the n-dimensional space over Q. Consider the linear map $f : Q^n \to F$ defined by $f(\mathbf{a}_i) = \alpha_i$, for each i, $1 \leq i \leq n$.

Lemma 6. *Assume that the unit norm domain $\{\mathbf{a} : \ |N(f(\mathbf{a}))| < 1, \ \mathbf{a} \in Q^n\}$ contains an n-dimensional open sphere of radius r centered at the origin, where $0 < r \leq 1$. Then there is a positive integer s such that if the elements of the test sets T_p has the Dedekind-Hasse property for each prime p, $p \leq s$, then each $\tau \in F$ has the Dedekind-Hasse property.*

A word of caution seems to be appropriate at this juncture. The weakness of our approach lies in the fact that we are not able to provide a mechanical procedure for how to assign the vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$ to the elements $\alpha_1, \ldots, \alpha_n$. The only thing we do here is to establish that if an ad hoc assignment satisfies the above conditions, then we can be sure that each element of F has the Dedekind-Hasse property.

Proof. We would like to show that each $\tau \in F$ has the Dedekind-Hasse property. By Lemma 1 it is enough to deal with the points of the parallelepiped P spanned by the vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$. Cover the point $(1/l)(i_1\mathbf{a}_1 + \cdots + i_n\mathbf{a}_n)$ with the open sphere of radius (r/l) centered at the point for each $0 \le i_1, \ldots, i_n \le l$. Repeat the procedure for $l = 1, 2, 3, \ldots$. By the covering result there is an s such that after s steps P will be covered. Thus each $\tau \in F$ is covered by an open sphere of radius $r/l \le 1/l$ centered at μ for some l, $1 \le l \le s$. In other words $|N(\tau - \mu)| < (1/l^2)$ or $|N(l\tau - l\mu)| < 1$. Note that $l\tau$ has the Dedekind-Hasse property. Indeed, if $l\tau \in R$, then by definition and if $l\tau \notin R$, then $0 < |N(\gamma(l\tau) + \delta)| < 1$ is satisfied with $\gamma = 1$ and $\delta = -l\mu$. In particular, τ has the Dedekind-Hasse property when $l = 1$. If $l \ne 1$, then by Lemma 2, τ has the Dedekind-Hasse property if $l\tau \notin R$. This leaves only the elements of the test sets

$$T_l = \{(1/l)(i_1\alpha_1 + \cdots + i_n\alpha_n) : 0 \le i_1, \ldots, i_n \le l - 1\}$$

undecided for l, $2 \le l \le s$.

We claim that if the elements of T_p have the Dedekind-Hasse property for each prime $p \le s$, then so do the elements of T_l for each l, $2 \le l \le s$. We prove this claim by induction on $e(l)$, the number of the not necessarily distinct prime factors of l. There is nothing to prove when $e(l) = 1$ so we assume that $e(l) \ge 2$ and write l in the form $l = uv$, where $u \ge 2$, $v \ge 2$. Consider $u\tau$, where $\tau \in T_l$. If $u\tau \notin R$, then $u\tau \in T_v$ and by the inductive assumption $u\tau$ has the Dedekind-Hasse property. Then by Lemma 2, τ has the Dedekind-Hasse property. If $u\tau \in R$, then $\tau \in T_u$ and by the inductive assumption it has the Dedekind-Hasse property. □

5. Unique Factorization in $Q(\sqrt{-67})$

Elements of $F = Q(\sqrt{-67})$ are linear combinations of 1 and $\sqrt{-67}$ with rational coefficients. We represent 1 and $\sqrt{-67}$ by the points $\mathbf{a} = (1, 0)$ and $\mathbf{b} = (0, \sqrt{67})$ on the plane respectively. So the number $\alpha = a + b\sqrt{-67}$ and the point $U = (u, v)$ correspond to each other if and only if $u = a$ and $v = b\sqrt{67}$. In other words, the linear map $f : Q^2 \to F$ is defined by $f(\mathbf{a}) = 1$, $f(\mathbf{b}) = \sqrt{-67}$. Since

$$N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{-67})(a - b\sqrt{-67}) = a^2 + 67b^2 = u^2 + v^2,$$

the unit norm domain $\{\mathbf{a} : \ |N(f(\mathbf{a}))| < 1, \ \mathbf{a} \in Q^2\}$ contains (the rational points of) the open unit circle $u^2 + v^2 < 1$.

The ring of integers of $Q(\sqrt{-67})$ is $Z[\vartheta] = \{a + b\vartheta : a, b \in Z\}$, where $\vartheta = (1 + \sqrt{-67})/2$. $Z[\vartheta]$ is represented by the lattice spanned by the vectors $\mathbf{a} = (1, 0)$ and

x	$f_\vartheta(x)$
$(0/2)+(0/2)\vartheta$	$(0/2)+(0/2)\vartheta$
$(0/2)+(1/2)\vartheta$	$(1/2)+(1/2)\vartheta$
$(1/2)+(0/2)\vartheta$	$(0/2)+(1/2)\vartheta$
$(1/2)+(1/2)\vartheta$	$(1/2)+(0/2)\vartheta$

Table 1: The map $f_\vartheta : T_2 \to T_2$

$\mathbf{b} = (1/2, \sqrt{67}/2)$. We would like to show that each $\tau \in Q(\sqrt{-67})$ has the Dedekind-Hasse property. By Lemma 1, we may focus our attention to the parallelogram spanned by **a** and **b**. Cover the point $(i/l)\mathbf{a} + (j/l)\mathbf{b}$ with the open circular disc of radius $1/l$ centered at the point for each integer i, j. Repeat this procedure for $l = 1, 2, 3, \ldots$. For $l = 1$ the discs cover strips parallel to the 1st coordinate axis having width $\sqrt{3}$. Now we wish to cover the interval $[0, \sqrt{67}/2]$ on the 2nd coordinate axis with intervals of radius $\big(\sqrt{3}/2\big)/l$, where l varies over $1, 2, 3, \ldots$. If $s = 4$, then

$$\frac{1}{s+1} < \frac{\sqrt{3}/2}{\sqrt{67}/2} \leq \frac{1}{s}$$

and so using the 4th Farey sequence we can cover the interval $[0, \sqrt{67}/2]$. This leaves only the elements of the test sets

$$T_p = \{(1/p)(i + j\vartheta) : 0 \leq i, j \leq p-1\}$$

unsettled for primes $p \leq 4$.

Table 1 shows that the map $f_\vartheta : T_2 \to T_2$ defined by $f_\vartheta(x) = x\vartheta$ permutes the elements of T_2. After coding the element $(i/p) + (j/p)\vartheta$ of T_p by $[i, j]$ the above permutation is in the following form:

$$\begin{pmatrix} [0,0] & [0,1] & [1,0] & [1,1] \\ [0,0] & [1,1] & [0,1] & [1,0] \end{pmatrix} = \big([0,0]\big)\big([0,1],[1,1],[1,0]\big).$$

$$\begin{pmatrix} [0,0] & [0,1] & [1,0] & [1,1] \\ [0,0] & [1,1] & [0,1] & [1,0] \end{pmatrix} = \big([0,0]\big)\big([0,1],[1,1],[1,0]\big).$$

Since $[0,0]$ and $[1,0]$ have the Dedekind-Hasse property because of their norms, all have the Dedekind-Hasse property.

The map $f_\vartheta : T_3 \to T_3$ defined by $f_\vartheta(x) = x\vartheta$ permutes the elements of T_3. The map after coding is the following:

$$\begin{pmatrix} [0,0] & [0,1] & [0,2] & [1,0] & [1,1] & [1,2] & [2,0] & [2,1] & [2,2] \\ [0,0] & [1,1] & [2,2] & [0,1] & [1,2] & [2,0] & [0,2] & [1,0] & [2,1] \end{pmatrix}$$

$$= \big([0,0]\big)\big([0,1],[1,1],[1,2],[2,0],[0,2],[2,2],[2,1],[1,0]\big).$$

Since $[0,0]$, $[1,0]$, $[2,0]$ have the Dedekind-Hasse property by their norms, all have the Dedekind-Hasse property.

In a similar way one can verify the unique factorization property in $Q(\sqrt{d})$ for

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

6. Unique Factorization in $Q(\sqrt{14})$

The ring of integers R of $F = Q(\sqrt{14})$ is $Z[\sqrt{14}]$. We assign the vectors $\mathbf{a} = (1,0)$ and $\mathbf{b} = (0,\sqrt{14})$ to the numbers 1 and $\sqrt{14}$ in $Q(\sqrt{14})$. In other words, the linear map $f : Q^2 \to F$ is defined by $f(\mathbf{a}) = 1$, $f(\mathbf{b}) = \sqrt{14}$. As a result the number $\alpha = a + b\sqrt{14}$ and the point $U = (u,v)$ correspond to each other if and only if $u = a$ and $v = b\sqrt{14}$. Since

$$\begin{aligned} N(\alpha) &= \alpha\overline{\alpha} \\ &= (a + b\sqrt{14})(a - b\sqrt{14}) \\ &= a^2 - 14b^2 \\ &= u^2 - v^2, \end{aligned}$$

the unit norm domain $\{\mathbf{a} : \ |N(f(\mathbf{a}))| < 1, \ \mathbf{a} \in Q^2\}$ is bounded by the hyperbolas $u^2 - v^2 = \pm 1$ and so it contains (the rational points of) the open unit circle $u^2 + v^2 < 1$. The unit circles centered at elements of $Z[\sqrt{14}]$ cover strips parallel to the 1st coordinate axis having width $\sqrt{3}$. If $s = 4$, then

$$\frac{1}{s+1} < \frac{\sqrt{3}/2}{\sqrt{14}} \leq \frac{1}{s}$$

and so with the help of the 4th Farey sequence we can cover the plane by strips and consequently by open circles. It is enough to check the elements of the test sets

$$T_p = \{(1/p)(i + j\sqrt{14}) : 0 \leq i, j \leq p - 1\}$$

for prime $p \leq 4$.

Let $\beta = 1 + \sqrt{14}$ and consider the map $f_\beta : T_2 \to T_2$ defined by $f_\beta(x) = x\beta$. This map permutes the elements of T_2.

$$\begin{pmatrix} [0,0] & [0,1] & [1,0] & [1,1] \\ [0,0] & [0,1] & [1,1] & [1,0] \end{pmatrix} = \big([0,0]\big)\big([0,1]\big)\big([1,0],[1,1]\big)$$

The elements $[0,0]$, $[1,0]$ have the Dedekind-Hasse property because of their norms. The element $\tau = (0/2) + (1/2)\sqrt{14}$ coded by $[0,1]$ also have the Dedekind-Hasse property since $0 < |N(\tau\gamma + \delta)| < 1$ holds with $\gamma = -1$, $\delta = 2 + \sqrt{14}$.

The map $f_\beta : T_3 \to T_3$ defined by $f_\beta(x) = x\beta$ permutes the elements of T_3:

$$\begin{pmatrix} [0,0] & [0,1] & [0,2] & [1,0] & [1,1] & [1,2] & [2,0] & [2,1] & [2,2] \\ [0,0] & [2,1] & [1,2] & [1,1] & [0,2] & [2,0] & [2,2] & [1,0] & [0,1] \end{pmatrix}$$

$$= \big([0,0]\big)\big([0,1],[2,1],[1,0],[1,1],[0,2],[1,2],[2,0],[2,2]\big)$$

As $[0,0]$, $[1,0]$ have the Dedekind-Hasse property because of their norms, each element of T_3 has the Dedekind-Hasse property.

7. Unique Factorization in $Q(\sqrt[3]{2})$

Elements of $F = Q(\sqrt[3]{2})$ are linear combinations of 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ with rational coefficients and the linear combinations with integer coefficients give the ring R of the algebraic integers of F. To the numbers 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ we assign the vectors

$$\mathbf{a} = (1,0,0) \qquad \mathbf{b} = (0,\sqrt[3]{2},0) \qquad \mathbf{c} = (0,0,\sqrt[3]{4}).$$

The number $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ and the point $U = (u,v,w)$ correspond to each other if and only if $u = a$, $v = b\sqrt[3]{2}$, $w = c\sqrt[3]{4}$. In other words, the linear map $f : Q^3 \to F$ is defined by $f(\mathbf{a}) = 1$, $f(\mathbf{b}) = \sqrt[3]{2}$, $f(\mathbf{c}) = \sqrt[3]{4}$. Now

$$\begin{aligned} N(\alpha) &= a^3 + 2b^3 + 4c^3 - 6abc \\ &= u^3 + v^3 + w^3 - 3uvw. \end{aligned}$$

The unit norm domain $\{\mathbf{a} : \ |N(f(\mathbf{a}))| < 1, \ \mathbf{a} \in Q^3\}$ contains (the rational points of) the open unit sphere $u^2 + v^2 + w^2 < 1$.

The open unit spheres centered at elements of $Z[\sqrt[3]{2}]$ cover cylinders parallel to the 1st coordinate axis. The coordinate plane perpendicular to the 1st axis intersects these cylinders in circles of radius $\sqrt{3}/2$. The circles cover strips parallel to the 2nd coordinate axis. The width of the strips is $\sqrt{3 - \sqrt[3]{4}}$. If $s = 2$, then

$$\frac{1}{s+1} < \frac{\big(\sqrt{3-\sqrt[3]{4}}\big)/2}{\sqrt[3]{4}} \leq \frac{1}{s}.$$

Therefore using the 2nd Farey sequence we can cover the $[0, \sqrt[3]{4}]$ interval on the 3rd coordinate axis by strips and consequently the whole 3-space by open spheres. Only the elements of the test set

$$T_2 = \{(1/2)(i + j\sqrt[3]{2} + k\sqrt[3]{4}) : 0 \leq i,j,k \leq 1\}$$

need to be checked. Table 2 shows that $|N(\tau)| < 1$ for each $\tau \in T_2 \setminus \{0\}$ and so each τ has the Dedekind-Hasse property.

τ	$N(\tau)$
$(0/2)+(0/2)\sqrt[3]{2}+(0/2)\sqrt[3]{4}$	0/8
$(0/2)+(0/2)\sqrt[3]{2}+(1/2)\sqrt[3]{4}$	4/8
$(0/2)+(1/2)\sqrt[3]{2}+(0/2)\sqrt[3]{4}$	2/8
$(0/2)+(1/2)\sqrt[3]{2}+(1/2)\sqrt[3]{4}$	6/8
$(1/2)+(0/2)\sqrt[3]{2}+(0/2)\sqrt[3]{4}$	1/8
$(1/2)+(0/2)\sqrt[3]{2}+(1/2)\sqrt[3]{4}$	5/8
$(1/2)+(1/2)\sqrt[3]{2}+(0/2)\sqrt[3]{4}$	3/8
$(1/2)+(1/2)\sqrt[3]{2}+(1/2)\sqrt[3]{4}$	1/8

Table 2: The norms of the elements of T_2

8. Totally Real Fields

Suppose $F = Q(\vartheta)$ is a totally real field of degree n and

$$\alpha_i = \sum_{j=1}^{n} a_{i,j}\vartheta^{j-1}, \quad 1 \le i \le n$$

is an integral basis of the ring of algebraic integers R of F. Sections 6 and 7 suggest to choose the vector $\mathbf{a}_i$ to be $(a_{i,1}, a_{i,2}\vartheta, \dots, a_{i,n}\vartheta^{n-1})$. Define the linear map $f : Q^n \to F$ by

$$f(\mathbf{a}_i) = \alpha_i = \sum_{j=1}^{n} a_{i,j}\vartheta^{j-1}$$

for each i, $1 \le i \le n$. In Lemma 6 we assumed that the unit norm domain $\{\mathbf{a} : \ |N(f(\mathbf{a}))| < 1, \ \mathbf{a} \in Q^n\}$ contains an n-dimensional open sphere of radius r centered at the origin, where $0 < r \le 1$. The following argument shows that in this particular case, that is, in the case of F being a totally real number field, this assumption can be proved.

Let $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ be all the conjugates of ϑ such that $\vartheta = \vartheta_1$ and $F = Q(\vartheta)$. Set

$$v = \Big[\prod_{i=1}^{n}\sum_{j=1}^{n}\Big|\frac{\vartheta_i}{\vartheta}\Big|^{2(j-1)}\Big]^{-1/(2n)}.$$

Then for

$$\alpha = \sum_{j=1}^{n} a_j\vartheta^{j-1}, \quad a_j \in Q, \quad x_j = a_j\vartheta^{j-1}$$

the inequality

$$\sum_{j=1}^{n} x_j^2 < v^2$$

implies

$$\begin{aligned}
[N(\alpha)]^2 = \prod_{i=1}^{n}\Big|\sum_{j=1}^{n} a_j\vartheta_i^{j-1}\Big|^2 &= \prod_{i=1}^{n}\Big|\sum_{j=1}^{n} a_j\vartheta^{j-1}\Big(\frac{\vartheta_i}{\vartheta}\Big)^{j-1}\Big|^2 \\
&= \prod_{i=1}^{n}\Big|\sum_{j=1}^{n} x_j\Big(\frac{\vartheta_i}{\vartheta}\Big)^{j-1}\Big|^2 \\
&= \prod_{i=1}^{n}\Big|\sum_{j=1}^{n}\Big(\frac{\vartheta_i}{\vartheta}\Big)^{j-1}x_j\Big|^2 \\
&\leq \prod_{i=1}^{n}\Big[\sum_{j=1}^{n}\Big|\frac{\vartheta_i}{\vartheta}\Big|^{j-1}|x_j|\Big]^2 \\
&\leq \prod_{i=1}^{n}\Big\{\Big[\sum_{j=1}^{n}\Big|\frac{\vartheta_i}{\vartheta}\Big|^{2(j-1)}\Big]\Big[\sum_{j=1}^{n} x_j^2\Big]\Big\} \\
&= \Big\{\prod_{i=1}^{n}\Big[\sum_{j=1}^{n}\Big|\frac{\vartheta_i}{\vartheta}\Big|^{2(j-1)}\Big]\Big\}\Big\{\prod_{i=1}^{n}\Big[\sum_{j=1}^{n} x_j^2\Big]\Big\} \\
&< \Big\{\prod_{i=1}^{n}\Big[\sum_{j=1}^{n}\Big|\frac{\vartheta_i}{\vartheta}\Big|^{2(j-1)}\Big]\Big\}\Big\{\prod_{i=1}^{n} v^2\Big\} \\
&= \Big\{\prod_{i=1}^{n}\Big[\sum_{j=1}^{n}\Big|\frac{\vartheta_i}{\vartheta}\Big|^{2(j-1)}\Big]\Big\}v^{2n} \\
&= v^{-2n}v^{2n} \\
&= 1.
\end{aligned}$$

Thus in the special case of totally real number fields our procedure is more complete than in the general case. However, the elements $\beta \in T_p$ used in the definition of the maps $f_\beta : T_p \to T_p$ are still chosen by trial and error and not in a systematic manner.

References

[1] F. Lemmermeyer, An application of the Dedekind-Hasse criterion, arXiv:1205.1147 [math.NT]

[2] K. Spindler, *Abstract Algebra with Applications*, Marcel Dekker, Inc., New York, 1994.

[3] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*, Chapman and Hall, London, 1987.