ISRAEL JOURNAL OF MATHEMATICS **265** (2025), 79–113
DOI: 10.1007/s11856-023-2577-6

POWER-FREE POINTS IN QUADRATIC NUMBER FIELDS: STABILISER, DYNAMICS AND ENTROPY

BY

Michael Baake

Fakultät für Mathematik, Universität Bielefeld
Postfach 100131, 33501 Bielefeld, Germany
e-mail: mbaake@math.uni-bielefeld.de

AND

Álvaro Bustos

School of Mathematics and Statistics, The Open University
Walton Hall, Milton Keynes MK7 6AA, UK
e-mail: abustos@math.uni-bielefeld.de

AND

Andreas Nickel*

Fakultät für Mathematik, Universität Duisburg-Essen
Thea-Leymann-Str. 9, 45127 Essen, Germany
e-mail: andreas.nickel@unibw.de

ABSTRACT

The sets of k-free integers in general quadratic number fields are studied, with special emphasis on (extended) symmetries and their impact on the topological dynamical systems induced by such integers. We establish correspondences between number-theoretic and dynamical quantities, and use symmetries and entropy to distinguish the systems.

* Current address: Institut für Theoretische Informatik, Mathematik und Operations Research, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85579 Neubiberg, Germany.
Received December 20, 2021 and in revised form March 30, 2022

1. Introduction

Topological and measure-theoretic dynamical systems have been studied for a long time, both in one and in higher dimensions. Powerful connections between such systems and number theory are known since the pioneering work of Furstenberg; see [17] for a concise introduction, and [27] for an account of some of the complications that show up in the innocently looking step from one to more than one dimension.

Here, we revisit one particular aspect of this connection, namely the structure of certain two-dimensional shift spaces of number-theoretic origin. More precisely, motivated by the properties of square-free integers and visible lattice points [1, 8, 26], we are interested in the planar shifts of k-free integers in arbitrary quadratic number fields, thus putting some of the observations from [3] into a more general setting. Here, given an arbitrary quadratic field K with ring of integers $\mathcal{O}_K$, an element $x \in \mathcal{O}_K$ is called k-free for some fixed natural number $k \geqslant 2$ when the principal ideal generated by x is not divisible by the k-th power of any prime ideal in $\mathcal{O}_K$.

The set of k-free integers gives rise to a natural topological dynamical system via its Minkowski embedding into $\mathbb{R}^2$ and the topological closure of the $\mathcal{O}_K$-orbit of the resulting discrete point set in the standard local topology. These shifts have interesting properties that are known from the set of visible lattice points [8] and various generalisations to $\mathcal{B}$-free lattice systems [5, 12, 3], where the latter are also generalisations of the recently much-studied $\mathcal{B}$-free integers [15, 14]. In fact, via the Minkowski embedding, previously studied extensions to number fields [12, 3] can also be viewed as $\mathcal{B}$-free lattice systems.

It is an interesting general observation that such systems can also be described in the setting of weak model sets [4, 6, 20, 19], which builds on the pioneering work of Meyer [23] and gives rapid access to various spectral and dynamical properties of such systems [6, 18]. Among these results is the statement that the dynamical spectrum is pure point, though no eigenfunction except the trivial one is continuous, and also a general formula for the spectrum and for the topological entropy of such shift spaces.

Clearly, one natural goal is the investigation of these shifts up to topological conjugacy, where some fairly simple groups come in handy, namely the topological centraliser and normaliser of the translation group in the group of homeomorphisms; see [9, 2, 11] and references therein. Generalising a result of

Mentzen [22] for the square-free integers on the line, it was shown in previous work [3] that the centraliser is trivial for many of these k-free shifts, while the normaliser is not. Therefore, certain results can already be obtained from this relatively simple invariant, which has the advantage of being explicitly computable.

In all our cases, we deal with examples of single orbit dynamics [30], which implies that we can derive many properties from the defining point set V of k-free integers (in its Minkowski embedding). Our strategy thus is to first study the stabiliser of the set V and later derive the extended symmetries of the induced dynamical system. This provides an interesting connection between an algebraic and a dynamical property, here via the connection between the normaliser, the unit group $\mathcal{O}^\times$, and the Galois group of $K/\mathbb{Q}$. Later, when we consider the induced shift spaces more closely, another connection of this kind shows up, then between topological entropy and the values of Dedekind zeta functions at integer values.

The paper is organised as follows. In Section 2, we set the scene with some initial examples of quadratic fields, where we determine the stabiliser for the k-free integers in $\mathbb{Q}(\sqrt{-2}\,)$ and recall previous results from [3]. Then, Section 3 covers the case of all quadratic fields, where the special cases treated before will come in handy as they turn out to be the ones that indeed need special treatment.

Afterwards, in Section 4, we construct the shift spaces that emerge as the orbit closure of the k-free points under the lattice translation action in the Minkowski embedding. Here, we use a special variant of the embedding such that all systems are acted on by the same group, namely the integer lattice $\mathbb{Z}^2$. This allows to determine the centraliser and the normaliser of the k-free shifts for arbitrary quadratic fields in a unified way.

Next, we address the question of how to classify the shifts up to topological conjugacy. While some distinctions are possible on the basis of the normaliser, we need topological entropy for a finer distinction, as we discuss in Section 5. Here, the entropy is expressed in terms of special values of the Dedekind zeta function, thus providing another link between an algebraic and a dynamical quantity. We also refine our viewpoint by considering factor maps, hence semiconjugacies, some of which can be excluded as well.

2. Initial examples of quadratic fields

Let us begin with the example of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-2})$, which has ring of integers

$$\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[\sqrt{-2}].$$

Its unit group is the smallest one possible, which is to say that $\mathcal{O}^\times = \{\pm 1\} \simeq C_2$. Here and below, C_n denotes the cyclic group of order n. The Galois group is another C_2, with complex conjugation (denoted by $\bar{\cdot}$) as the non-trivial automorphism, and the field norm is $N(x) = x\bar{x}$. Since $\mathcal{O}$ has class number 1, we can use numbers (rather than ideals) for this initial example. For an integer $k \geqslant 2$, we say that $x \in \mathcal{O}$ is **k-free** if it is not divisible by the k-th power of any prime in $\mathcal{O}$.

PROPOSITION 2.1: *Let $2 \leqslant k \in \mathbb{N}$ be fixed and consider the set $V = V_k$ of k-free integers in $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$. Let A be a $\mathbb{Z}$-linear bijection of $\mathcal{O}$ with $A(V) \subseteq V$. Then, A is of the form $A(x) = \varepsilon\sigma(x)$ with $\varepsilon \in \mathcal{O}^\times \simeq C_2$ and $\sigma \in \{\mathrm{id}, \bar{\cdot}\} \simeq C_2$. Consequently, $A(V) = V$, and these maps form the group* $\mathrm{stab}(V) \simeq C_2 \times C_2$.

Proof. Let A be a $\mathbb{Z}$-linear bijection of $\mathcal{O}$ with $A(V) \subseteq V$. If $x \in V$ is coprime with a rational prime p that is unramified, so $\gcd_{\mathcal{O}}(x, p) = 1$ where the $\gcd_{\mathcal{O}}$ in $\mathcal{O}$ is unique up to units, we know that $p^\ell x \in V$ for every $1 \leqslant \ell < k$, hence also $A(p^{k-1}x) = p^{k-1}A(x) \in V$, which implies $\gcd_{\mathcal{O}}(A(x), p) = 1$. Since no odd rational prime is ramified in K, this observation provides a powerful coprimality structure.

Let $U = \mathcal{O}^\times = \{\pm 1\}$ and set $\xi = \sqrt{-2}$. For $p = 2 = -\xi^2$, which is the only ramified prime in this case, we may now conclude from the above coprimality structure that

$$A(U) \subseteq U \cup \xi U \cup \cdots \cup \xi^{k-1}U,$$

which we will now reduce to $A(U) \subseteq U$, and thus to $A(U) = U$ since U is finite. Without loss of generality, we may assume $A(1) = \xi^m$ for some $0 \leqslant m < k$, possibly after replacing A by $-A$, which is a map of the same kind. Also, we know that $A(\xi) = a + b\xi$ for some $a, b \in \mathbb{Z}$.

If we compute $\det(A)$ with respect to the basis $\{1, \xi\}$, we get $\det(A) = (-2)^r b$ when $m = 2r$ and $\det(A) = -(-2)^r a$ when $m = 2r + 1$. Since A is bijective on $\mathcal{O}$, it is unimodular as an integer matrix, so $\det(A) = \pm 1$. This forces $r = 0$, and we either get $m = 0$, together with $b = \pm 1$, or $m = 1$, then with $a = \pm 1$.

If $m = 1$, we thus have $A(\xi) = \pm 1 + b\xi$, which has norm $N(\pm 1 + b\xi) = 1 + 2b^2$. This must be a power of 2 by coprimality, which is only possible for $b = 0$. But $A(1) = \xi$ and $A(\xi) = \pm 1$ implies $A(3 + \xi) = \pm 1 + 3\xi$, thus mapping an element of V of norm 11 to an image of norm 19, which is impossible by the coprimality structure. This rules out $m = 1$.

Finally, if $m = 0$ and $b = \pm 1$, we get $A(\xi) = a \pm \xi$ with $a \in \mathbb{Z}$ and

$$N(A(\xi)) = a^2 + 2,$$

which is a power of 2 only for $a = 0$. This leads to $A(1) = 1$ together with $A(\xi) = \pm\xi$, or to $-A$, which are the four elements of the form $A(x) = \varepsilon\sigma(x)$ stated in the proposition. They clearly map units to units, and all remaining claims are clear. ∎

Here and below, given a set U, the notation $\mathrm{stab}(U)$ refers to the monoid of $\mathbb{Z}$-linear mappings that send U *into* itself. It is thus part of the above result that the stabiliser of $V_k \subset \mathbb{Z}[\sqrt{-2}\,]$ is actually a group. In [3], the corresponding result was proved for the imaginary quadratic fields $\mathbb{Q}(\sqrt{d}\,)$ with $d \in \{-1, -3\}$, which are statements about the k-free elements of the Gaussian and the Eisenstein ring of integers, $\mathbb{Z}[\mathrm{i}]$ and $\mathbb{Z}[\rho]$ with $\rho = \frac{1}{2}(-1 + \mathrm{i}\sqrt{3}\,)$. Let us first recall the Gaussian case from [3, Lemma 6.1]. Here and below, $D_n = C_n \rtimes C_2$ denotes the dihedral group of order $2n$.

Fact 2.2: *Let V_k be the set of k-free Gaussian integers, for some fixed $2 \leqslant k \in \mathbb{N}$. Then, any $\mathbb{Z}$-linear bijection A of $\mathbb{Z}[\mathrm{i}]$ that satisfies $A(V_k) \subseteq V_k$ is of the form $A(x) = \varepsilon\sigma(x)$ with $\varepsilon \in \mathbb{Z}[\mathrm{i}]^\times = \{1, \mathrm{i}, -1, -\mathrm{i}\} \simeq C_4$ and $\sigma \in \{\mathrm{id}, \bar{\cdot}\} \simeq C_2$.*

These mappings are bijections of V_k and form the group

$$\mathrm{stab}(V_k) \simeq C_4 \rtimes C_2 = D_4,$$

which is a maximal finite subgroup of $\mathrm{GL}(2, \mathbb{Z})$, and independent of k. ∎

The analogous statement for the Eisenstein integers reads as follows; see [3, Thm. 6.5].

Fact 2.3: *Let V_k be the set of k-free Eisenstein integers, for some fixed $2 \leqslant k \in \mathbb{N}$. Then, any $\mathbb{Z}$-linear bijection A of $\mathbb{Z}[\rho]$ that satisfies $A(V_k) \subseteq V_k$ is of the form $A(x) = \varepsilon\sigma(x)$ with $\varepsilon \in \mathbb{Z}[\rho]^\times = \{(-\rho)^m : 0 \leqslant m \leqslant 5\} \simeq C_6$ and $\sigma \in \{\mathrm{id}, \bar{\cdot}\} \simeq C_2$.*

These mappings are bijections of V_k and form the group

$$\mathrm{stab}(V_k) \simeq C_6 \rtimes C_2 = D_6,$$

which is also a maximal finite subgroup of $\mathrm{GL}(2,\mathbb{Z})$, again independent of k. ∎

Also, the stabiliser was determined for some real quadratic fields, namely for $\mathbb{Q}(\sqrt{d}\,)$ with $d \in \{2,3,5\}$. The corresponding results from [3, Sec. 7] can be summarised as follows, where C_∞ denotes the infinite cyclic group.

FACT 2.4: *Consider $K = \mathbb{Q}(\sqrt{d}\,)$ for fixed $d \in \{2,3,5\}$, and let V_k be the set of k-free integers in $\mathcal{O}_K$, that is, in $\mathbb{Z}[\sqrt{2}\,]$, in $\mathbb{Z}[\sqrt{3}\,]$, or in $\mathbb{Z}[\tau]$ with $\tau = \frac{1}{2}(1+\sqrt{5}\,)$. Then, the $\mathbb{Z}$-linear bijections A of $\mathcal{O}_K$ with $A(V_k) \subseteq V_k$ are precisely the mappings $A(x) = \varepsilon\sigma(x)$ with $\varepsilon \in \mathcal{O}_K^\times \simeq C_2 \times C_\infty$ and $\sigma \in \{\mathrm{id}, (\cdot)'\}$, where $(\cdot)'$ denotes algebraic conjugation in K.*

These mappings are bijections of V_k and form the group

$$\mathrm{stab}(V_k) = \mathcal{O}_K^\times \rtimes C_2 \simeq C_2 \times D_\infty,$$

which is a proper infinite subgroup of $\mathrm{GL}(2,\mathbb{Z})$ that does not depend on k. ∎

All examples so far have class number 1. The natural next step is to extend the analysis to all quadratic fields, where key notions have to be formulated via ideals. In this process, the above examples will emerge as cases that need special treatment, in one way or another.

3. General quadratic fields

Let us recall some notation and basic results on quadratic fields, all of which can be found in [31]. We use the standard parameterisation by a square-free integer $d \in \mathbb{Z} \setminus \{0,1\}$ and consider $K = \mathbb{Q}(\sqrt{d}\,)$. The field discriminant d_K and the ring of integers $\mathcal{O}_K$ (which is the maximal order of K) are given by

$$d_K = \begin{cases} d, & \text{if } d \equiv 1 \bmod 4, \\ 4d, & \text{if } d \equiv 2,3 \bmod 4, \end{cases} \quad \text{and} \quad \mathcal{O}_K = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \bmod 4, \\ \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}, & \text{if } d \equiv 2,3 \bmod 4. \end{cases}$$

The Galois group is $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, (\cdot)'\} \simeq C_2$, where $(\cdot)'$ denotes algebraic conjugation in K, as induced by $\sqrt{d} \mapsto -\sqrt{d}$. This simply is complex conjugation for all imaginary quadratic fields. The field norm is given by $N(x) = xx'$, which can be negative for real fields.

Let us recall Dirichlet's unit theorem for quadratic fields as follows.

FACT 3.1: *The unit group $\mathcal{O}_K^\times$ for imaginary quadratic fields is always finite, and isomorphic with C_4 for $d = -1$, with C_6 for $d = -3$, and with C_2 for all remaining $d < 0$.*

For all real quadratic fields, the unit group is infinite, $\mathcal{O}_K^\times \simeq C_2 \times C_\infty$. ∎

For $x \neq 0$, the principal ideal (x) generated by x has the unique decomposition

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$$

into powers of prime ideals, where the product runs over all prime ideals of $\mathcal{O}_K$, but the valuation $v_{\mathfrak{p}}(x)$ vanishes for all but (at most) finitely many of them. For quadratic fields, a rational prime p is **ramified** if and only if $p|d_K$. In particular, one has

$$(\sqrt{d}\,) = \prod_{\mathfrak{p}|d} \mathfrak{p}. \tag{3.1}$$

Definition 3.2: Let $2 \leqslant k \in \mathbb{N}$ be fixed. An element $0 \neq x \in \mathcal{O}_K$ is called k**-free** if $v_{\mathfrak{p}}(x) < k$ for all prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$. The set of all k-free integers is denoted by V_k.

When the class number is 1, which is to say that all ideals in $\mathcal{O}$ are principal, our above definition agrees with the traditional one that x is k-free if it is not divisible by the k-th power of a prime in $\mathcal{O}$. However, beyond the class number 1 situation, one needs to employ ideals and valuations as above. By definition, 0 is never an element of V_k, and the following result justifies why the study of $k = 2$ plays a special role, for any fixed square-free $d \in \mathbb{Z} \setminus \{0, 1\}$.

LEMMA 3.3: *Let A be a $\mathbb{Z}$-linear bijection of $\mathcal{O} = \mathcal{O}_K$ that satisfies $A(V_k) \subseteq V_k$ for some integer $k \geqslant 2$. Then, one also has $A(V_2) \subseteq V_2$.*

Proof. Assume $A(V_k) \subseteq V_k$, let $x \in V_2$ and consider any non-ramified (rational) prime p, so $p \nmid d_K$. Then, $p^{k-2}x \in V_k$, and $\mathbb{Z}$-linearity of A implies

$$p^{k-2}A(x) = A(p^{k-2}x) \in V_k,$$

thus giving $v_{\mathfrak{p}}(A(x)) \leqslant 1$ for all $\mathfrak{p}|p$.

It remains to consider the ramified primes, that is, primes with $p|d_K$. For any such prime, we have $(p) = p\mathcal{O} = \mathfrak{p}^2$, with $\mathfrak{p}$ denoting the corresponding prime ideal over p in $\mathcal{O}$. When k is even and $x \in V_2$, one has

$$v_{\mathfrak{p}}(p^{\frac{k}{2}-1}x) = v_{\mathfrak{p}}(p^{\frac{k}{2}-1}) + v_{\mathfrak{p}}(x) = k - 2 + v_{\mathfrak{p}}(x) \leqslant k - 1 < k,$$

so $p^{\frac{k}{2}-1}x \in V_k$, hence also $A(p^{\frac{k}{2}-1}x) = p^{\frac{k}{2}-1}A(x) \in V_k$. With $v_{\mathfrak{p}}(p^{\frac{k}{2}-1}) = k-2$, this implies $v_{\mathfrak{p}}(A(x)) \leqslant 1$, and we get $A(V_2) \subseteq V_2$ for k even.

Now, consider k odd and $x \in V_2$, so $v_{\mathfrak{p}}(x) \in \{0,1\}$. Here, we have

$$v_{\mathfrak{p}}(p^{\frac{k-1}{2}-v_{\mathfrak{p}}(x)}) = k-1-2v_{\mathfrak{p}}(x) < k-2v_{\mathfrak{p}}(x),$$

and thus $p^{\frac{k-1}{2}-v_{\mathfrak{p}}(x)}x \in V_k$. Now, $p^{\frac{k-1}{2}-v_{\mathfrak{p}}(x)}A(x) = A(p^{\frac{k-1}{2}-v_{\mathfrak{p}}(x)}x) \in V_k$ gives

$$v_{\mathfrak{p}}(A(x)) \leqslant 2v_{\mathfrak{p}}(x). \tag{3.2}$$

When $v_{\mathfrak{p}}(x) = 0$, we also get $v_{\mathfrak{p}}(A(x)) = 0$, and we are good in this case, too. Next, consider $v_{\mathfrak{p}}(x) = 1$, where $v_{\mathfrak{p}}(A(x)) \leqslant 2$. From (3.1), if $\mathfrak{p}|d$, we see that $v_{\mathfrak{p}}(x\sqrt{d}\,) = 2$. As $\mathfrak{p}^2 = (p)$, we have $x\sqrt{d} = py$ for some $y \in \mathcal{O}$, hence $A(x\sqrt{d}\,) = pA(y) \in p\mathcal{O} = (p)$. Suppose $v_{\mathfrak{p}}(A(x)) \geqslant 2$, which means $v_{\mathfrak{p}}(A(x)) = 2$ by (3.2). Then, we also have $A(x) \in p\mathcal{O}$ and

$$A(x(\mathbb{Z} \oplus \mathbb{Z}\sqrt{d}\,)) = \mathbb{Z}A(x) \oplus \mathbb{Z}A(x\sqrt{d}\,).$$

Consequently, p^2 divides the index $[\mathcal{O} : A(x\mathbb{Z}[\sqrt{d}\,])]$.

When $d \equiv 1 \bmod 4$, we know that 2 is not ramified, so any ramified prime p must be odd. Here, we have $[\mathcal{O} : \mathbb{Z}[\sqrt{d}\,]] = 2$, hence also $[A(x\mathcal{O}) : A(x\mathbb{Z}[\sqrt{d}\,])] = 2$, which implies

$$p^2 \mid [\mathcal{O} : A(x\mathcal{O})] = [\mathcal{O} : x\mathcal{O}] = \mathrm{N}(x\mathcal{O}),$$

where $\mathrm{N}(\mathfrak{b}) := [\mathcal{O} : \mathfrak{b}]$ denotes the absolute norm of an ideal $\mathfrak{b}$ in $\mathcal{O}$. When $\mathfrak{b}$ is a principal ideal, hence $\mathfrak{b} = (z) = z\mathcal{O}$ for some $z \in \mathcal{O}$, the absolute norm is related to the field norm by $\mathrm{N}(\mathfrak{b}) = |N(z)|$, so we get $p^2|N(x)$.

When $d \equiv 2, 3 \bmod 4$, the condition $p^2|N(x)$ follows directly, without the extra index-2 argument. In fact, it then also applies to $p = 2$ for $d \equiv 2$. On the other hand, since $v_{\mathfrak{p}}(x) = 1$, we know that $N(x)$ is exactly divisible by p, hence not by p^2. This contradiction shows that $v_{\mathfrak{p}}(A(x)) \geqslant 2$ is impossible for any odd ramified prime, as well as for $p = 2$ when $d \equiv 2 \bmod 4$.

Finally, when $d \equiv 3 \bmod 4$, the prime 2 is ramified, and we need to check what happens with the corresponding prime ideal $\mathfrak{p}_2$, where $\mathfrak{p}_2^2 = 2\mathcal{O}$. Here, $\mathcal{O} = \mathbb{Z}[\sqrt{d}\,]$, and one has

$$x^2 - d \equiv x^2 - 1 \equiv (x-1)^2 \mod 2.$$

Invoking [24, Thm. I.8.3], we get that $\mathfrak{p}_2 = (2, \sqrt{d}-1)$, which comprises $\sqrt{d}-1 \in \mathfrak{p}_2$, so that $v_{\mathfrak{p}_2}(\sqrt{d}-1) \geqslant 1$. Since $v_{\mathfrak{p}_2}(2) = 2$, we then actually have $v_{\mathfrak{p}_2}(\sqrt{d}-1) = 1$, as we would otherwise get $(2, \sqrt{d}-1) \subseteq \mathfrak{p}_2^2$ and hence a contradiction. Now, $v_{\mathfrak{p}_2}(x) = 1$ implies $v_{\mathfrak{p}_2}(x(\sqrt{d}-1)) = 2$, and thus $x(\sqrt{d}-1) = 2y$ for some $y \in \mathcal{O}$.

Now, suppose $v_{\mathfrak{p}_2}(A(x)) \geqslant 2$, hence $v_{\mathfrak{p}_2}(A(x)) = 2$ by (3.2) again. As we now have $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}(\sqrt{d}-1)$, we see that $A(x\mathcal{O}) = \mathbb{Z}A(x) \oplus \mathbb{Z}A(x(\sqrt{d}-1)) \subseteq 2\mathcal{O}$. This gives

$$4 \mid [\mathcal{O} : A(x\mathcal{O})] = [\mathcal{O} : x\mathcal{O}] = \mathrm{N}(x\mathcal{O}) = |N(x)|,$$

but 4 cannot divide $N(x)$ for $x \in V_2$, whence $v_{\mathfrak{p}_2}(A(x)) \geqslant 2$ is impossible as well. ∎

In view of Lemma 3.3, we now concentrate our attention on the case $k = 2$, and set $V = V_2$.

Definition 3.4: Let K be a quadratic field, with ring of integers $\mathcal{O} = \mathcal{O}_K$ and $V \subset \mathcal{O}$ the subset of square-free elements. A $\mathbb{Z}$-linear bijection A of $\mathcal{O}$ is called a **preserving map** (PM) for V if $A(V) \subseteq V$, and a **strongly preserving map** (SPM) if $A(V) = V$.

The set of all PMs for V constitute the **stabiliser** of V, denoted by $\mathrm{stab}(V)$.

Note that the restriction of a PM to V is obviously injective, but it is not clear a priori whether it is also surjective. Since the $\mathbb{Z}$-linear bijections of $\mathcal{O}$ form a group, the subset of PMs for V inherits a semi-group structure with a unit, which is to say that $\mathrm{stab}(V)$ is a monoid. However, whether or when $\mathrm{stab}(V)$ is a group remains to be determined.

Let us first look at the coprimality structure within V. We say that two elements $x, y \in \mathcal{O}$ are *coprime*, denoted by $(x, y) = 1$, if the principal ideals (x) and (y) have disjoint decompositions into prime ideals of $\mathcal{O}$.

Lemma 3.5: *Let p be a rational prime with $p \nmid d_K$, and let $x \in V$ be coprime with p, so $(p, x) = 1$. Then, for any $A \in \mathrm{stab}(V)$, one also has $(p, A(x)) = 1$.*

Proof. By assumption, p is not ramified, and thus not a square, so the condition $x \in V$ together with $(p, x) = 1$ implies $px \in V$, hence also $pA(x) = A(px) \in V$ due to $A(V) \subseteq V$ together with $\mathbb{Z}$-linearity. But this is only possible if $(p, A(x)) = 1$ as claimed. ∎

In generalisation of previous arguments, we now need to consider the set

$$W := \{x \in V : v_{\mathfrak{p}}(x) > 0 \Rightarrow \mathfrak{p} | (d_K)\}.$$

The norms of elements in W have a prime decomposition into ramified primes only. In particular, given $x \in W$ and any prime ideal $\mathfrak{p}$ over a ramified p, one has $v_{\mathfrak{p}}(x) \in \{0, 1\}$, while all other valuations vanish.

LEMMA 3.6: *If A is a* PM *for V, it satisfies $A(W) = W$.*

Proof. Due to the coprimality structure stated in Lemma 3.5, it is clear that $A(W) \subseteq W$. When K is imaginary quadratic, W is a finite set, and bijectivity of A then implies $A(W) = W$. So, it remains to consider the case that K is real quadratic, where the unit group, and then also W, is an infinite set.

The norm on W takes only finitely many distinct values. This is so because there are only finitely many ramified primes that can show up in the prime decomposition of $N(x)$ for any $x \in W$, with powers 0 or 1, while units have norm ± 1. Let C be the set of these values and

$$S'_c := \{x \in W : N(x) = c\},$$

so that

$$W = \bigcup_{c \in C} S'_c$$

is a finite union of disjoint sets, where each S'_c itself is infinite, because the unit group is already infinite.

Let us write $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\delta = \mathbb{Z}[\delta]$ with

$$\delta = \begin{cases} \sqrt{d}, & d \equiv 2, 3 \bmod 4, \\ \frac{1}{2}(1 + \sqrt{d}\,), & d \equiv 1 \bmod 4. \end{cases} \tag{3.3}$$

With this choice of an integral basis for $\mathcal{O}$, we have $x = a + b\delta$ with $a, b \in \mathbb{Z}$ for any $x \in \mathcal{O}$, and the field norm is $N(x) = Q(a, b)$, where Q is a non-degenerate quadratic form in a and b. Thus, we have

$$S_c := \{(a, b) \in \mathbb{Z}^2 : a + b\delta \in S'_c\} = \{(a, b) \in \mathbb{Z}^2 : Q(a, b) = c\}, \tag{3.4}$$

where the equality follows because any element $a + b\delta$ with $Q(a, b) = c$ is square-free by construction.

Written in the $\mathbb{Z}$-basis $\{1, \delta\}$, our map A is represented by a $\mathrm{GL}(2, \mathbb{Z})$-matrix, also called A for simplicity, which acts linearly on all of $\mathbb{R}^2$. We thus see that S_c is the intersection of a quadratic curve (or conic) $\widehat{S}_c \subset \mathbb{R}^2$ with $\mathbb{Z}^2$. Since A maps $\bigcup_{c \in C} S_c$ into itself, any point from S_c must be mapped to a point from $S_{c'}$ for some $c' \in C$. Clearly, C is finite but S_c is not, because $(a, b) \leftrightarrow a + b\delta$ is a bijection between S_c and S'_c, where the latter is infinite. Now, Dirichlet's pigeon hole principle implies that, for some power A^n of A, there exists a $c_1 \in C$ such that $S_{c_1} \cap A^n(S_{c_1})$ is an infinite set, so also $\widehat{S}_{c_1} \cap A^n(\widehat{S}_{c_1})$ is infinite.

Now, $A^n(\widehat{S}_{c_1})$ is a non-degenerate conic as well, because it is the image of one under a linear bijection. Since non-degenerate conics cannot intersect in infinitely many points unless these conics are equal, because 5 points determine a conic, see [13, Sec. 14.7], we get $\widehat{S}_{c_1} = A^n(\widehat{S}_{c_1})$. Now, we have

$$A^n(S_{c_1}) = A^n(\widehat{S}_{c_1} \cap \mathbb{Z}^2) = A^n(\widehat{S}_{c_1}) \cap A^n(\mathbb{Z}^2) = \widehat{S}_{c_1} \cap \mathbb{Z}^2 = S_{c_1},$$

which also implies that A^n maps $\bigcup_{c \in C \setminus \{c_1\}} S_c$ into itself.

At this point, we can repeat the argument for the smaller union, where we get some power of A^n that maps some $S_{c'}$ into itself. After finitely many steps, a single $S_{c''}$ remains, which is then automatically invariant, by a simplified argument of the above type. So, we see that some power of A, say A^m, satisfies

$$A^m(S_c) = S_c$$

for all $c \in C$ and thus maps W onto itself. Now, if $A(W)$ were a strict subset of W, this would imply

$$W = A^m(W) = A^{m-1}(A(W)) \subsetneq A^{m-1}(W) \subseteq W,$$

which is a contradiction, so we also get $A(W) = W$ as claimed. ∎

Since algebraic conjugation maps W onto itself, the following consequence is immediate.

Fact 3.7: *One has $\sigma(W) = W$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.* ∎

We will also make use of the following easy observation.

Fact 3.8: *Let $x \in W$. Then, $N(x)$ is a square-free divisor of d_K.* ∎

If ε is a unit in $\mathcal{O}$, we use m_ε to denote the mapping $x \mapsto m_\varepsilon(x) := \varepsilon x$.

Proposition 3.9: *Let K be a quadratic field and $\mathcal{O} = \mathcal{O}_K$ its ring of integers. Then, for any $A \in \mathrm{stab}(V)$, the following statements are equivalent.*

(1) *$A = m_\varepsilon \circ \sigma$ for some $\varepsilon \in \mathcal{O}^\times$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.*
(2) *$A(1) \in \mathcal{O}^\times$.*

Proof. The implication (1) ⇒ (2) is clear. To show the converse direction, we observe that $A(1) = \varepsilon \in \mathcal{O}^\times$ implies that $A' = m_{\varepsilon^{-1}} \circ A$ is a mapping of the same type, wherefore we may assume $A(1) = 1$ without loss of generality. Now, we have to distinguish two cases.

Case 1: $d \equiv 1 \bmod 4$, so $\mathcal{O} = \mathbb{Z}[\delta]$ with $\delta = \frac{1+\sqrt{d}}{2}$. Let $A(\delta) = a + b\delta$ with $a, b \in \mathbb{Z}$. Since A is a bijection of $\mathcal{O}$, $A(1) = 1$ and $A(\delta)$ must generate $\mathcal{O}$ as a $\mathbb{Z}$-module, so A is represented by the matrix $\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$, hence $b = \det(A) = \pm 1$. Set $\tilde{a} = a + \frac{1}{2}(b-1)$.

Now, we have

$$A(\sqrt{d}\,) = A(2\delta - 1) = 2a - 1 \pm (1 + \sqrt{d}\,) = 2\tilde{a} \pm \sqrt{d},$$

which has norm $4\tilde{a}^2 - d$. Since $\sqrt{d}^2 = d = d_K$ in this case, we have

$$(\sqrt{d}\,) = \prod_{p \mid d_K} \mathfrak{p},$$

where $(p) = \mathfrak{p}^2$ for each factor, which implies $\sqrt{d} \in W$, hence also $A(\sqrt{d}\,) \in W$ by Lemma 3.6. Moreover, the norm of $A(\sqrt{d}\,)$ must be a divisor of $d = d_K$ by Fact 3.8.

We now claim that $2n\tilde{a} \pm \sqrt{d} \in W$ for all $n \in \mathbb{N}_0$. Indeed, since $\pm\sqrt{d} \in W$, this is clear for $n = 0$. Assuming the claim to hold for n, we have $x_n = 2n\tilde{a} \pm \sqrt{d} \in W$, and also its image must be in W, again by Lemma 3.6. But this means that $A(x_n) = 2(n+1)\tilde{a} \pm \sqrt{d} \in W$, for one of the signs, and then actually for both of them, by an application of Fact 3.7. This settles the claim inductively.

As a result, we see that $N(2n\tilde{a} + \sqrt{d}\,)$ divides d for all $n \in \mathbb{N}$, where the norm is $4n^2\tilde{a}^2 - d$. Since this is unbounded unless $\tilde{a} = 0$, we may conclude that $A(\sqrt{d}\,) = \pm\sqrt{d}$. Consequently, when $b = 1$, we get $a = 0$ and $A = \mathrm{id}$, while $b = -1$ forces $a = 1$, which gives $A(\delta) = \delta'$ with $(\cdot)' \in \mathrm{Gal}(K/\mathbb{Q})$ being algebraic conjugation. This settles the proposition for Case 1.

Case 2: $d \equiv 2, 3 \bmod 4$, so $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. Let $A(\sqrt{d}\,) = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. Here, $A(1) = 1$ and $A(\sqrt{d}\,)$ generate $\mathcal{O}$, so

$$b = \det\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) = \pm 1,$$

because A is a bijection of $\mathcal{O}$. In complete analogy to the first case, one shows by induction that $na + \sqrt{d} \in W$ for all $n \in \mathbb{N}_0$. Since $na + \sqrt{d}$ has norm $n^2a^2 - d$, but divides $2\,|d|$ by Fact 3.8, a contradiction is only avoided if $a = 0$, which gives $A(\sqrt{d}\,) = \pm\sqrt{d}$, and we are done. ∎

To continue, we shall need the following property of the splitting primes.

FACT 3.10: *For any quadratic number field K, there are infinitely many rational primes q that split in K in such a way that the prime ideals over q are principal.*

Proof. This is a consequence of Dirichlet's density theorem [24, Thm. VII.13.2] as follows. Let M be a set of prime ideals of K. As explained in [24, p. 543], the Dirichlet density of M is given by

$$d(M) = \lim_{s \searrow 1} \frac{\sum_{\mathfrak{q} \in M} N(\mathfrak{q})^{-s}}{\log \frac{1}{s-1}}.$$

Let S_{ram} be the set of all rational primes which are ramified in K, and let $S_{\mathrm{ram}}(K)$ be the set of primes (meaning prime ideals) in K above those in S_{ram}. We recall that $N(\mathfrak{q}) = q^f$, where q is the rational prime below $\mathfrak{q}$ and f is called the degree of $\mathfrak{q}$, which is equal to 2 if q is inert in K and equal to 1 otherwise. As the sum $\sum N(\mathfrak{q})^{-s}$ over all prime ideals in M of degree 2 converges and the set $S_{\mathrm{ram}}(K)$ is finite, the definition of $d(M)$ only depends upon primes $\mathfrak{q} \notin S_{\mathrm{ram}}(K)$ of degree 1. So if M has positive density, there are infinitely many primes $\mathfrak{q} \in M$ such that the rational prime q below $\mathfrak{q}$ splits in K.

We now apply this observation to the set of all primes which are principal, which has positive density by [24, Thm. VII.13.2]. Consequently, there are infinitely many rational primes q, which split in K, such that one prime above q is principal. But if one prime above q is principal, so is the other. ∎

PROPOSITION 3.11: *Let d be a square-free element of $\mathbb{Z} \setminus \{0, 1\}$ and further assume that $d \neq -1$. Let A be a $\mathbb{Z}$-linear bijection of $\mathcal{O}$ such that $A(W) = W$. Then, $A(1) \notin \sqrt{d}\mathcal{O}^\times$. In particular, this conclusion holds for any $A \in \mathrm{stab}(V)$.*

Proof. If A is a PM for V, we have $A(W) = W$ by Lemma 3.6. So, let us more generally assume A to be a $\mathbb{Z}$-linear bijection of $\mathcal{O}$ such that $A(W) = W$, where we also know that $\sqrt{d}\mathcal{O}^\times \subseteq W$. Since $d \neq -1$ by assumption, $\sqrt{d}$ is not a unit, and $\mathcal{O}^\times \neq \sqrt{d}\mathcal{O}^\times$. Now, suppose to the contrary of our claim that $A(1) \in \sqrt{d}\mathcal{O}^\times$, where we may then assume $A(1) = \sqrt{d}$ without loss of generality, because multiplying A by a unit does not change the type of mapping. Now, we have to consider two situations.

CASE 1: $d \equiv 1 \bmod 4$, where we set $\delta = \frac{1+\sqrt{d}}{2}$ and then get $A(1) = -1 + 2\delta$. Now, let $A(\delta) = a + b\delta$ with $a, b \in \mathbb{Z}$, wherefore A is represented by the matrix $\left(\begin{smallmatrix} -1 & a \\ 2 & b \end{smallmatrix}\right)$, which must lie in $\mathrm{GL}(2, \mathbb{Z})$ due to bijectivity of A on $\mathcal{O} = \mathbb{Z}[\delta]$. So,

this gives

$$\pm 1 = \det(A) = -2a - b,$$

and thus $A(\delta) = \pm\frac{1}{2} + \frac{b}{2}\sqrt{d}$. With $\sqrt{d} \in W$, we also get

$$A(\sqrt{d}\,) = A(2\delta - 1) = \pm 1 + (b-1)\sqrt{d} \in W,$$

which implies that its norm,

$$1 - d(b-1)^2 =: d',$$

divides $d_K = d$ by Fact 3.8.

Now, we claim that $d' = 1$: Suppose to the contrary that $d' \neq 1$, hence $0 \neq 1 - d' = d(b-1)^2$. If $d > 0$, we have $d + d' \geqslant 0$ because $d' | d$, and this gives $1 + d \geqslant 1 - d' = d(b-1)^2 \geqslant d$, where $d(b-1)^2 \neq 1 + d$. Then, $1 - d' = d$, and d and d' are coprime. Since $d' | d$, this forces $d' = \pm 1$ and thus $d = 0$ or $d = 2$, which is impossible because $d \equiv 1 \bmod 4$. Likewise, if $d < 0$, we get $d + d' \leqslant 0$ and then $1 + d \leqslant 1 - d' = d(b-1)^2 \leqslant d$, which is a contradiction. Consequently, we must indeed have $d' = 1$ and hence $b = 1$, so $A(\sqrt{d}\,) = \pm 1$, where one also gets $a \in \{-1, 0\}$.

Next, choose a prime $q \gg 1$ according to Fact 3.10 and let $\mathfrak{p} = (\pi)$ be a prime ideal over q, where $\pi \notin W$ by construction. Write $\pi = u + v\delta$ with $u, v \in \mathbb{Z}$, which has norm

$$N(\pi) = u^2 + uv + \frac{1-d}{4}v^2 = \pm q, \tag{3.5}$$

where $\frac{1-d}{4}$ is an integer. Now, q cannot divide $u^2 + uv$, as otherwise $q \gg 1$ implies $q | v^2$, hence $q | v$ and thus also $q | u$. But this would give $q^2 | q$, which is impossible. So, q and $u^2 + uv$ are coprime. Next, we have

$$A(\pi) = u\sqrt{d} + v\Big(\pm\frac{1}{2} + \frac{1}{2}\sqrt{d}\Big)$$

with norm

$$N(A(\pi)) = \frac{v^2}{4} - d\Big(u^2 + uv + \frac{v^2}{4}\Big) = \pm q - (d+1)(u^2 + uv),$$

where (3.5) was used for the second step. Clearly, q can be chosen sufficiently large so that it does not divide $d + 1$. Since q is coprime with $u^2 + uv$, we see that $q \nmid N(A(\pi))$. Since we know from Lemma 3.5 that $A(\pi)$ is coprime with any other non-ramified prime, we must have $A(\pi) \in W = A(W)$. As A is bijective on W, we get $\pi \in W$ and thus a contradiction, which rules out $A(1) \in \sqrt{d}\mathcal{O}^\times$ in this case.

Case 2: $d \equiv 2, 3 \bmod 4$, where we consider $A(1) = \sqrt{d}$ and $A(\sqrt{d}\,) = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. Here, the determinant condition gives $\pm 1 = \det\left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right) = -a$, and thus $a = \pm 1$. Consequently, $A(\sqrt{d}\,) = \pm 1 + b\sqrt{d} \in W$. Its norm is given by

$$N(A(\sqrt{d}\,)) = 1 - db^2 =: d',$$

which must divide d (if $d \equiv 2 \bmod 4$) or $2d$ (if $d \equiv 3 \bmod 4$) by Fact 3.8.

When $d < 0$, so $d' > 0$, we have $b \in \{0, \pm 1\}$, as otherwise, due to $d' | 2d$, the inequality $1 + 2d \leqslant 1 - d' = db^2 \leqslant 4d$ gives a contradiction. Likewise, when $d > 0$, so $d' < 0$, we again get $b \in \{0, \pm 1\}$, as any other value would lead to $4d \leqslant db^2 = 1 - d' = 1 + |d'| \leqslant 1 + 2d$ and thus to $2d \leqslant 1$, which is impossible.

Subcase $b = 0$: Here, we have $A(\sqrt{d}\,) = \pm 1$. By Fact 3.10, we may choose a rational prime $q \gg 1$ such that $(q) = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p}$ principal, so $\mathfrak{p} = (\pi)$ for some $\pi = u + v\sqrt{d}$. Then, we get

$$\pm q = N(\pi) = u^2 - dv^2 = u^2 - v^2 - (d-1)v^2.$$

Now, we must have $q \nmid (u^2 - v^2)$: Otherwise, $q \gg 1$ forces $q | v$, which implies $q | u$ and then $q^2 | q$, and thus a contradiction. Next, we calculate $A(\pi) = u\sqrt{d} \pm v$ and thus

$$N(A(\pi)) = v^2 - du^2 = \pm q + (d+1)(v^2 - u^2).$$

Since q does not divide either of the two bracketed terms, we see that $q \nmid N(A(\pi))$. As before, we conclude that $A(\pi) \in W = A(W)$ and hence $\pi \in W$ by the bijectivity of A. This contradicts the original choice of π, with the same conclusion as in Case 1.

Subcase $b = \pm 1$: Here, we have $d = 1 - d'$, so d and d' are coprime integers. Then, $d' | 2d$ with $d > 0$ means $d' \in \{-1, -2\}$, and thus $d = 2$ or $d = 3$, which are two of the cases from Fact 2.4. In its proof, $A(W) = W$ was used to show $A(V) \subseteq V$, and our claim holds. Likewise, when $d < 0$, we can only have $d' \in \{1, 2\}$, and thus $d = 0$, which is excluded, or $d = -1$, which is the excluded case of the Gaussian integers (where the claim actually does not hold). ∎

At this point, recalling Fact 2.2 for $d = -1$, we can completely answer the question for the stabiliser of V in imaginary quadratic fields as follows.

THEOREM 3.12: *Let $K = \mathbb{Q}(\sqrt{d})$, with $d < 0$ square-free, be an imaginary quadratic field, with ring of integers $\mathcal{O} = \mathcal{O}_K$. Then, any $A \in \mathrm{stab}(V)$ is of the form $A = m_\varepsilon \circ \sigma$ for some $\varepsilon \in \mathcal{O}^\times$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \simeq C_2$. Every such mapping is bijective on V, and we obtain that the stabiliser of V is a group,*

$$\mathrm{stab}(V) = \mathcal{O}^\times \rtimes \mathrm{Gal}(K/\mathbb{Q}) \simeq C_n \rtimes C_2 = D_n,$$

where D_n is the dihedral group, here with $n = 4$ for $d = -1$, $n = 6$ for $d = -3$, and $n = 2$ in all remaining cases.

Proof. The cases $d \in \{-1, -2, -3\}$ are known from Proposition 2.1 and Facts 2.2 and 2.3, so we may restrict to $d \leqslant -5$, as -4 is not square-free. Let A be a PM for V, so we know that $A(W) = W$ from Lemma 3.6. In view of Proposition 3.9, we now need to show $A(1) \in \mathcal{O}^\times$.

Suppose to the contrary that $A(1) \notin \mathcal{O}^\times$. Then, there exists a ramified prime p such that $A(1) \in \mathfrak{p}$ where $\mathfrak{p}$ is the prime ideal over p, so $(p) = \mathfrak{p}^2$. As $A(1)$ is square-free, we know that $N(A(1))$ is exactly divisible by p, hence not by p^2.

CASE 1: $d \equiv 2, 3 \bmod 4$, with $\mathcal{O} = \mathbb{Z}[\sqrt{d}\,]$ and $d_K = 4d$. Let $A(1) = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$, so

$$N(A(1)) = a^2 - db^2 =: d' \mid 2d$$

because $A(1) \in W$.

If we had $b = 0$, we would get $d' = a^2 | 2d$. But d is square-free and $A(1) \notin \mathcal{O}^\times$ by assumption, which implies $d' = 4$ and $a = \pm 2$. Consequently, $A(1) = \pm 2 \in \mathfrak{p}_2^2$, which is not square-free because 2 is ramified. So, we see that $b \neq 0$, and we actually must have $b = \pm 1$ (otherwise, $d' = a^2 - db^2 \geqslant -db^2 \geqslant 4|d| > 2|d| \geqslant d'$ would give a contradiction). So, with $b = \pm 1$, we get $d' = a^2 - d > 0$.

Now, we see that $a \neq 0$, as otherwise $A(1) = \pm\sqrt{d}$, which contradicts Proposition 3.11. Also, d' must be even (otherwise, $d' | d$ and $d' = a^2 - d > -d \geqslant d'$ gives a contradiction). So, write $d' = 2\tilde{d}$, where $\tilde{d} | d$ with $\tilde{d} > 0$. Since d is square-free, $\tilde{d}$ must divide a, and we get

$$2\tilde{d} = a^2 - d \geqslant \tilde{d}^2 + \tilde{d} = (\tilde{d} + 1)\tilde{d},$$

which implies $\tilde{d} = 1$. But this means $2 = a^2 - d \geqslant 5$, which is absurd, so $A(1) \notin \mathcal{O}^\times$ is ruled out in this case.

CASE 2: $d \equiv 1 \bmod 4$, where $\mathcal{O} = \mathbb{Z}[\delta]$ with $\delta = \frac{1+\sqrt{d}}{2}$ and $d_K = d$. Let $A(1) = a + b\delta$ with $a, b \in \mathbb{Z}$. Here, we get

$$N(A(1)) = \Big(a + \frac{b}{2}\Big)^2 - d\Big(\frac{b}{2}\Big)^2 =: d',$$

which divides d.

As before, $b = 0$ is impossible, as it would imply $a^2 | d$ with d square-free, so $a = \pm 1$ and thus $A(1) \in \mathcal{O}^\times$ in contradiction to our assumption. We claim that, once again, we must have $b = \pm 1$: Otherwise, we would have $d' \geqslant -d(\frac{b}{2})^2 \geqslant -d$, hence $d' = -d$ and $b = \pm 2$ together with $a = -\frac{b}{2}$. This, in turn, would give $A(1) = \pm\sqrt{d}$, in contradiction to Proposition 3.11.

So, we have $0 \leqslant (a \pm \frac{1}{2})^2 = d' + \frac{d}{4}$, which implies $|d| \geqslant d' \geqslant \frac{|d|}{4}$, hence $d' = |d|$ or $d' = \frac{|d|}{3}$ because d is odd. In the first case, we get

$$\Big(a \pm \frac{1}{2}\Big)^2 = |d| - \frac{|d|}{4} = \frac{3|d|}{4},$$

which forces $3|d|$ to be a square in $\mathbb{Z}$. With d being square-free, this is only possible for $d = -3$, which was excluded. When $d' = \frac{|d|}{3}$, we obtain

$$\Big(a \pm \frac{1}{2}\Big)^2 = \frac{|d|}{3} - \frac{|d|}{4} = \frac{|d|}{12},$$

and $\frac{|d|}{3}$ is a square in $\mathbb{Z}$, which again leads to the excluded case $d = -3$. So, $A(1) \notin \mathcal{O}^\times$ is ruled out also in this case, and we have $A(1) \in \mathcal{O}^\times$.

As each mapping of the form $A = m_\varepsilon \circ \sigma$ is in the stabiliser, the structure of $\mathrm{stab}(V)$ derives from the unit group (as stated early in this chapter) together with $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_2$ and the relation

$$\sigma \circ m_\varepsilon = m_{\sigma(\varepsilon)} \circ \sigma. \qquad \blacksquare$$

Let us next attack the more complicated case of real quadratic fields, where we begin with an observation that follows by elementary arguments from our previous results.

PROPOSITION 3.13: *Let $d = p > 0$ be a rational prime, and consider $K = \mathbb{Q}(\sqrt{d})$. Then, any $A \in \mathrm{stab}(V)$ is of the form*

$$A = m_\varepsilon \circ \sigma$$

with $\varepsilon \in \mathcal{O}^\times$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Proof. The case $d = 2$, where $d_K = 8$, is covered by Fact 2.4. Next, consider the case $d_K = d = p \equiv 1 \bmod 4$, where we know that $W = \mathcal{O}^\times \dot\cup \sqrt{p}\,\mathcal{O}^\times$ is a disjoint union. From Lemma 3.6, we get $A(1) \in W$, while Proposition 3.11 asserts that $A(1) \notin \sqrt{p}\,\mathcal{O}^\times$, so $A(1) \in \mathcal{O}^\times$. Then, Proposition 3.9 shows that A is of the form claimed.

Next, let $p \equiv 3 \bmod 4$, where $(2) = \mathfrak{p}_2^2$ is ramified. Consequently, we have

$$W = \mathcal{O}^\times \dot\cup \sqrt{p}\,\mathcal{O}^\times \dot\cup W'$$

for some subset $W' \subseteq \mathfrak{p}_2$. In view of Proposition 3.9, we now have to show that $A(1) \in \mathcal{O}^\times$.

Here, we know that $A(1) \in W$, but $A(1) \notin \sqrt{p}\,\mathcal{O}^\times$ by Proposition 3.11. Suppose we had $A(1) \in W'$, hence $A(1) \in \mathfrak{p}_2$. Since $A(\mathcal{O}) = \mathcal{O}$, we must have $A(\sqrt{p}\,) \notin \mathfrak{p}_2$, while we still have the inclusion $A(\sqrt{p}\,) \in W$ by Lemma 3.6. If $A(\sqrt{p}\,) = \epsilon \in \mathcal{O}^\times$, we get $(A^{-1} \circ m_\epsilon)(1) = \sqrt{p}$, in contradiction to Proposition 3.11 applied to the mapping $A^{-1} \circ m_\epsilon$, which clearly is a $\mathbb{Z}$-linear bijection of $\mathcal{O}$ that maps W onto itself. Consequently, we have $A(\sqrt{p}\,) \in \sqrt{p}\,\mathcal{O}^\times$.

Possibly after multiplying by a unit, which means no loss of generality, we may assume $A(\sqrt{p}\,) = \sqrt{p}$. Now, let $A(1) = a + b\sqrt{p}$ with $a, b \in \mathbb{Z}$. Since $A(1) \in W'$, its norm must satisfy $N(A(1)) \in \{\pm 2, \pm 2p\}$. Moreover, we have $a = \det(\left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right)) = \det(A) = \pm 1$, so we get $N(A(1)) = 1 - pb^2$. This never equals 2 or $\pm 2p$, while it can agree with -2 only for $p = 3$. Since $p = 3$ is known from Fact 2.4, we get $A(1) \in \mathcal{O}^\times$ in all cases, and we are done. ∎

The simplest cases not yet covered are $\mathbb{Q}(\sqrt{6}\,)$ and $\mathbb{Q}(\sqrt{15}\,)$, which can be treated by explicit arguments similar to those used for our previous cases from Fact 2.4, taking into account that one now has two ramified primes (as in the case of $\mathbb{Z}[\sqrt{3}\,]$ treated in [3]). The result is the expected one, and completely in line with the above. To generalise this now to all real quadratic fields, we invoke another result on quadratic forms of a more geometric origin. If Q is a given quadratic form, we (uniquely) represent it by the corresponding symmetric matrix B_Q, and call $\det(B_Q)$ the *determinant* of Q.

LEMMA 3.14: *Let Q_1 and Q_2 be two binary quadratic forms over $\mathbb{R}^2$ with negative determinant, and assume that they share a non-empty level curve, which is to say that, for some $c_1, c_2 \in \mathbb{R}$, the non-empty curves $\{Q_1(x, y) = c_1\}$ and $\{Q_2(x, y) = c_2\}$ agree. Then, there exists a constant $0 \neq c^* \in \mathbb{R}$ such that $Q_2 = c^*\, Q_1$.*

Remark 3.15: Note that the assertion of Lemma 3.14 holds for any pair of conics, not necessarily hyperbolic, under the assumption that the common level curve is infinite.

Proof. Due to the determinant condition, the curves $\{Q_i(x,y) = c\}$ are hyperbolas, with the limiting (degenerate) case $c = 0$ consisting of two straight lines each. If $\{Q_1(x,y) = c_1\}$ and $\{Q_2(x,y) = c_2\}$ agree as curves, they must have the same asymptotes, which are two straight lines passing through the origin. They are determined by the equation $Q_i(x,y) = 0$, for either choice of i, where we have a factorisation

$$Q_i(x,y) = (a_{i,1}x + b_{i,1}y)(a_{i,2}x + b_{i,2}y)$$

for suitable real numbers $a_{i,j}$ and $b_{i,j}$ with $i,j \in \{1,2\}$.

Now, possibly after interchanging the two factors for one of the forms, we may assume that $a_{i,1}x + b_{i,1}y = 0$, for both i, is the equation for the first asymptote, which means that $a_{i,2}x + b_{i,2}y = 0$ determines the other one. Observe that two non-degenerate linear equations determine the same line if and only if one equation is a constant (and non-zero) multiple of the other. In our case at hand, this means that there are constants $\kappa_j \neq 0$ such that

$$a_{2,j}x + b_{2,j}y = \kappa_j(a_{1,j}x + b_{1,j}y),$$

hence

$$Q_2(x,y) = \kappa_1\kappa_2\, Q_1(x,y),$$

which gives our claim by taking $c^* = \kappa_1\kappa_2$. ∎

In the context of real quadratic fields, $Q(a,b) = N(a + b\delta)$ with $a,b \in \mathbb{Z}$ defines a quadratic form over $\mathbb{Z}^2$, where δ is chosen as in Eq. (3.3). Clearly, Q extends to a quadratic form over $\mathbb{R}^2$, and we have $\det(B_Q) = -\frac{1}{4}d_K < 0$ in all cases under consideration. This can now be used as follows.

PROPOSITION 3.16: *Let K be a real quadratic field with $\mathcal{O} = \mathcal{O}_K$ as its ring of integers, and let W be the set of square-free elements of $\mathcal{O}$ that are coprime with all non-ramified rational primes. If A is a $\mathbb{Z}$-linear bijection of $\mathcal{O}$ with $A(W) = W$, one also has $A(\mathcal{O}^\times) = \mathcal{O}^\times$.*

Proof. As in the proof of Lemma 3.6, we can write W as a finite disjoint union of level sets $S'_c = \{a + b\delta : a,b \in \mathbb{Z} \text{ and } Q(a,b) = c\}$ with the δ from (3.3), where c divides $2d$. We identify S'_c with a subset S_c of $\mathbb{Z}^2$ as in (3.4). Then

each S_c is the intersection of the curve $\{(x,y) \in \mathbb{R}^2 : Q(x,y) = c\}$ with $\mathbb{Z}^2$, where we are in the situation of Lemma 3.14. In particular, the non-trivial level curves are hyperbolas.

As before, we use A both for the given mapping and for its $\mathrm{GL}(2,\mathbb{Z})$-representation after the identification of $\mathcal{O}$ with $\mathbb{Z}^2$ via the $\mathbb{Z}$-basis $\{1,\delta\}$ of $\mathcal{O}$. Since $A(W) = W$, we get

$$A(S_1) = \bigcup_{c|2d} S_c \cap A(S_1),$$

which is a finite union of disjoint sets. Consequently, for some $c|2d$, the set $S_c \cap A(S_1)$ must be infinite. This implies that the hyperbolas $\{Q(x,y) = c\}$ and $\{(Q \circ A^{-1})(x,y) = 1\}$ match in more than five points and thus have to agree as curves, where the latter corresponds to the image of $\{Q(x,y) = 1\}$ under A. By Lemma 3.14, there must be a real number $c^* \neq 0$ such that $Q \circ A^{-1} = c^* Q$.

Now, again inspecting the proof of Lemma 3.6, we know that some power of A maps units to units. In fact, from the above argument, we know that $A^k(S_1) = S_1$ must hold for some $k \in \mathbb{N}$. Then, A^{-k} maps S_1 into itself and $A^{-k}(1)$ has norm 1. This implies

$$1 = Q(A^{-k}(1)) = (c^*)^k Q(1) = (c^*)^k,$$

which means that c^* is a root of unity, as Q is non-degenerate. But $c^* \in \mathbb{R}$ by construction, so $c^* \in \{\pm 1\}$, which implies that A maps elements of norm ± 1 to elements of norm ± 1, that is, units to units. ∎

We can now wrap up this part as follows.

THEOREM 3.17: *Let $K = \mathbb{Q}(\sqrt{d})$, with $d > 1$ square-free, be a real quadratic field, with ring of integers $\mathcal{O} = \mathcal{O}_K$. Then, any $A \in \mathrm{stab}(V)$ is of the form $A = m_\varepsilon \circ \sigma$ with $\varepsilon \in \mathcal{O}^\times$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \simeq C_2$. Every such mapping is bijective on V, and the stabiliser is a group,*

$$\mathrm{stab}(V) = \mathcal{O}^\times \rtimes \mathrm{Gal}(K/\mathbb{Q}) \simeq (C_2 \times C_\infty) \rtimes C_2 \simeq C_2 \times D_\infty,$$

where $D_\infty = C_\infty \rtimes C_2$ is the infinite dihedral group.

Proof. If A is a PM for V, we once again know $A(W) = W$ from Lemma 3.6. Then, A maps units to units by Proposition 3.16, and A is of the claimed form as a result of Proposition 3.9, hence clearly a bijection on V.

The group property of $\mathrm{stab}(V)$ is then obvious, and its calculation follows from the standard properties mentioned earlier, including the structure of the unit group, $\mathcal{O}^\times$. ∎

Given any quadratic field, we know from Lemma 3.3 that $\mathrm{stab}(V_k) \subseteq \mathrm{stab}(V_2)$ holds for all $k \geqslant 2$. Now, $\mathrm{stab}(V_2)$ is a group, all elements of which also preserve V_k, by Theorems 3.12 and 3.17, so $\mathrm{stab}(V_k) = \mathrm{stab}(V_2)$, and we obtain the following conclusion.

Corollary 3.18: *Let K be a quadratic field, imaginary or real, with ring of integers $\mathcal{O}$. Then, for any $k \in \mathbb{N}$ with $k \geqslant 2$, the set $\mathrm{stab}(V_k)$ is a group that is independent of k, namely the group $\mathrm{stab}(V)$ characterised by Theorems 3.12 and 3.17.* ∎

4. The subshift of k-free integers

The connection to dynamical systems emerges from the observation that $V = V_k$ defines an element of $\mathbb{X}_{\mathcal{O}} := \{0,1\}^{\mathcal{O}}$, which is compact in the product topology, by identifying V with the function (or configuration) 1_V. As usual, we write elements of $\mathbb{X}_{\mathcal{O}}$ as $u = (u_x)_{x\in\mathcal{O}}$. Now, one can define an $\mathcal{O}$-action $\alpha\colon \mathcal{O}\times\mathbb{X}_{\mathcal{O}} \longrightarrow \mathbb{X}_{\mathcal{O}}$ via $(t,u) \mapsto \alpha_t(u)$ with $(\alpha_t(u))_x := u_{x+t}$. This action is continuous and turns $(\mathbb{X}_{\mathcal{O}}, \mathcal{O})$ into a **topological dynamical system** (TDS).

For a function $f : \mathbb{X}_{\mathcal{O}} \longrightarrow \mathbb{C}$, we define the translation action via

$$(\alpha_t f)(u) = f(\alpha_{-t}u).$$

With this, we get $\alpha_t(1_V) = 1_{t+V}$, where 1_S denotes the characteristic function of a set $S \subseteq \mathbb{Z}^2$. Now, the orbit closure in the product topology,

$$\mathbb{X}_V := \overline{\{\alpha_t(1_V) : t \in \mathcal{O}\}},$$

is a closed and hence compact subset of $\mathbb{X}_{\mathcal{O}}$ that is invariant under the above $\mathcal{O}$-action, so $(\mathbb{X}_V, \mathcal{O})$ is a TDS as well. At this point, it is useful to employ the Minkowski embedding of $\mathcal{O}$ as a lattice $\varGamma \subset \mathbb{R}^2$, for which there are several possibilities.

To establish the link with symbolic dynamics, it is more convenient to employ the standard $\mathbb{Z}$-basis $\{1, \delta\}$ of $\mathcal{O}$ with the δ from (3.3) and then consider

$$V_k' := \{(m_1, m_2) \in \mathbb{Z}^2 : m_1 + m_2\delta \in V_k\}, \tag{4.1}$$

which is now a subset of $\mathbb{Z}^2$. This also identifies $\mathcal{O}$ with $\varGamma = \mathbb{Z}^2$ in a specific way. We are now working with binary subshifts of $\{0,1\}^{\mathbb{Z}^2}$, hence in the usual setting of symbolic dynamics [21, 27]. In particular, for fixed k, we now have

$$\mathbb{X} = \mathbb{X}_{V_k'} = \overline{\{t + V_k' : t \in \mathbb{Z}^2\}},$$

where we tacitly identify subsets of $\mathbb{Z}^2$ with their characteristic functions. This gives us the TDS $(\mathbb{X}, \mathbb{Z}^2)$, which we call the subshift induced by the k-free integers of $\mathcal{O}$. It is unique up to isomorphism.

Let $\iota : \mathcal{O} \longrightarrow \mathbb{Z}^2$ be the embedding defined as above by $1 \mapsto (1,0)$ and $\delta \mapsto (0,1)$. When $\mathfrak{b}$ is an ideal in $\mathcal{O}$, its embedding $\varGamma_{\mathfrak{b}} := \iota(\mathfrak{b})$ is a sublattice of $\mathbb{Z}^2$ of index

$$[\mathbb{Z}^2 : \varGamma_{\mathfrak{b}}] = \mathrm{N}(\mathfrak{b}).$$

Now, $\mathbb{X}$ can also be seen as an algebraic $\mathcal{B}$-free lattice system in the sense of [3, Def. 5.1] as follows, where we assume $k \geqslant 2$ to be fixed. Let $\mathfrak{P}$ denote the set of prime ideals of $\mathcal{O}$ and consider

$$\mathcal{B} := \{\varGamma_{\mathfrak{p}^k} : \mathfrak{p} \in \mathfrak{P}\} \quad \text{with } \varGamma_{\mathfrak{p}^k} = \iota(\mathfrak{p}^k) \subset \mathbb{Z}^2. \tag{4.2}$$

Here, $\mathcal{B}$ is an infinite set of coprime sublattices of $\mathbb{Z}^2$, which is to say that $\varGamma_{\mathfrak{p}^k} + \varGamma_{\mathfrak{q}^k} = \mathbb{Z}^2$ whenever the prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ are different. The defining set from (4.1) can now be rewritten as

$$V_k' = V_{\mathcal{B}} := \mathbb{Z}^2 \setminus \bigcup_{\mathfrak{p} \in \mathfrak{P}} \varGamma_{\mathfrak{p}^k}. \tag{4.3}$$

This gives another way to view our subshift as an orbit closure, namely

$$\mathbb{X} = \mathbb{X}_{\mathcal{B}} = \overline{\mathbb{Z}^2 + V_{\mathcal{B}}},$$

where the latter is a shorthand for the translation orbit closure of $V_{\mathcal{B}}$ under the shift action. In our special setting, where $k \geqslant 2$, we also get

$$\sum_{\mathfrak{p} \in \mathfrak{P}} \frac{1}{[\mathbb{Z}^2 : \varGamma_{\mathfrak{p}}]} = \sum_{\mathfrak{p} \in \mathfrak{P}} \frac{1}{\mathrm{N}(\mathfrak{p})^k} < \infty,$$

which is to say that the $\mathcal{B}$-free system $(\mathbb{X}_{\mathcal{B}}, \mathbb{Z}^2)$ is automatically Erdős; compare [3].

Lemma 4.1: *Let K be a quadratic field, with ring of integers $\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[\delta]$, and let $V_k' \subset \mathbb{Z}^2$ with $k \geqslant 2$ be the set defined in* (4.1)*. Then, the set V_k' has tied density $1/\zeta_K(k)$, where ζ_K denotes the Dedekind zeta function of K.*

Proof. Tied density means that one considers $\mathrm{card}(V_k' \cap B_r(0))/\pi r^2$ in the limit $r \to \infty$, or with disks replaced by centred squares and their areas, which is known to exist and to be independent of the averaging sequence, once it is centred and of van Hove type. In [8], the arguments are spelled out in detail for the visible lattice points of $\mathbb{Z}^2$, and the same approach works here as well.

Indeed, looking at (4.3), it is clear that V_k' is a point set that is the limit, in the local topology, of a nested sequence of lattices by considering $\mathbb{Z}^2 \setminus \bigcup_{\mathfrak{p}:\mathrm{N}(\mathfrak{p})\leqslant n} \varGamma_{\mathfrak{p}^k}$ as $n \to \infty$. Clearly, the density of each lattice in this sequence exists with respect to the averaging sequence and, via a standard inclusion-exclusion argument, is given by

$$\prod_{\mathfrak{p}:\mathrm{N}(\mathfrak{p})\leqslant n} (1 - \mathrm{N}(\mathfrak{p})^{-k}),$$

which decreases in n and converges to $1/\zeta_K(k)$ as claimed. ∎

Also, the set V_k' is a weak model set of maximal density in the sense of [6]. Indeed, with k fixed, we can set $H_{\mathfrak{p}^k} = \mathbb{Z}^2/\varGamma_{\mathfrak{p}^k}$ for each prime ideal $\mathfrak{p}$ in $\mathcal{O}$, which defines an Abelian group of order $\mathrm{N}(\mathfrak{p})^k$. Then, $H := \prod_{\mathfrak{p}\in\mathfrak{P}} H_{\mathfrak{p}^k}$ is a compact Abelian group, which serves as internal space for the **cut and project scheme** (CPS)

$$\begin{array}{ccccc} \mathbb{R}^2 & \xleftarrow{\ \pi\ } & \mathbb{R}^2 \times H & \xrightarrow{\ \pi_{\mathrm{int}}\ } & H \\ \cup & & \cup & & \cup \ \text{dense} \\ \mathbb{Z}^2 & \xleftarrow{\ 1-1\ } & \mathcal{L} & \longrightarrow & \pi_{\mathrm{int}}(\mathcal{L}) \\ \| & & & & \| \\ L & & \xrightarrow{\qquad\star\qquad} & & L^\star \end{array} \tag{4.4}$$

where $\mathcal{L}$ is the standard diagonal embedding of $\mathbb{Z}^2$ into $\mathbb{R}^2 \times H$; see [4] for background.

Now, defining the $\star$-image of $x \in \mathbb{Z}^2$ as the lift of x into H by using its value modulo $\varGamma_{\mathfrak{p}^k}$ at place $\mathfrak{p}^k$, one obtains

$$V_k' = \{x \in \mathbb{Z}^2 : x \bmod \varGamma_{\mathfrak{p}^k} \neq 0 \text{ for all } \mathfrak{p} \in \mathfrak{P}\}.$$

In other words, the subset

$$W = \{(h_{\mathfrak{p}^k})_{\mathfrak{p}\in\mathfrak{P}} : h_{\mathfrak{p}^k} \neq 0 \text{ for all } \mathfrak{p} \in \mathfrak{P}\}$$

provides a coding for V_k', in the sense that W is the window for the description of V_k' as a model set in the CPS (4.4). In particular, V_k' and many of its properties can be retrieved from W via the CPS. In the natural (and normalised) Haar measure of H, this set has volume

$$\operatorname{vol}(W) = \prod_{\mathfrak{p}\in\mathfrak{P}} \frac{\mathrm{N}(\mathfrak{p})^k - 1}{\mathrm{N}(\mathfrak{p})^k} = \prod_{\mathfrak{p}\in\mathfrak{P}} (1 - \mathrm{N}(\mathfrak{p})^{-k}) = \frac{1}{\zeta_K(k)},$$

where ζ_K denotes the Dedekind zeta function of our quadratic field under consideration. Note that this is nothing but a variant of the argument used in the proof of Lemma 4.1.

In this setting, we get the reformulation of V_k' as

$$V_k' = \{x \in \mathbb{Z}^2 : x^\star \in W\},$$

which means that we have recognised it as a weak model set. The term 'weak' here emerges from the observation that the set W, which is also known as the **window**, is a compact subset of H that has no interior. It thus consists of boundary only, and the latter has Haar measure $1/\zeta_K(k)$ as derived above. Now, by the density formula for weak model sets [18, Prop. 3.4], the density of our set is bounded from above by $\operatorname{dens}(\mathbb{Z}^2)\operatorname{vol}(W) = \operatorname{vol}(W)$, which agrees with the density of V_k' by Lemma 4.1.

Next, we call a set $U \subset \mathbb{Z}^2$ **admissible** for $\mathcal{B}$ from (4.2) if, for every $\varGamma_\mathfrak{p} \in \mathcal{B}$, the set U meets at most $\mathrm{N}(\mathfrak{p})^k - 1$ cosets of $\varGamma_\mathfrak{p}$ in $\mathbb{Z}^2$, that is, misses at least one. The collection of all admissible subsets of $\mathbb{Z}^2$ constitutes again a subshift, denoted by $\mathbb{A}$, which clearly contains $\mathbb{X}_\mathcal{B}$ by construction.

PROPOSITION 4.2: *Let K be a quadratic field, with ring of integers $\mathcal{O} = \mathcal{O}_K$ and k-free elements V_k for some fixed $k \geqslant 2$. If $\mathbb{X}_\mathcal{B}$ is the $\mathcal{B}$-free shift induced by V_k, and $\mathbb{A}$ the corresponding shift of admissible sets, one has $\mathbb{X}_\mathcal{B} = \mathbb{A}$. In particular, $\mathbb{X}_\mathcal{B}$ is hereditary: Arbitrary subsets of elements of $\mathbb{X}_\mathcal{B}$ are again elements of $\mathbb{X}_\mathcal{B}$.*

Proof. While the relation $\mathbb{X}_\mathcal{B} \subseteq \mathbb{A}$ is clear by construction, the converse is the non-trivial part of the statement. If follows via [3, Prop. 5.2], which rests on an asymptotic density argument that holds because our system is Erdős. As such, the claim is a special case of [3, Thm. 5.3].

Since subsets of admissible sets clearly remain admissible, $\mathbb{X}_\mathcal{B}$ is hereditary. ∎

The action of $\mathcal{G} := \mathbb{Z}^2$ on $\mathbb{X} = \mathbb{X}_{V_k'}$ is faithful. We now consider the groups

$$\mathcal{S}(\mathbb{X}) := \mathrm{cent}_{\mathrm{Aut}(\mathbb{X})}(\mathcal{G}) = \{H \in \mathrm{Aut}(\mathbb{X}) : GH = HG \text{ for all } G \in \mathcal{G}\}$$

and

$$\mathcal{R}(\mathbb{X}) := \mathrm{norm}_{\mathrm{Aut}(\mathbb{X})}(\mathcal{G}) = \{H \in \mathrm{Aut}(\mathbb{X}) : H\mathcal{G}H^{-1} = \mathcal{G}\},$$

where $\mathrm{Aut}(\mathbb{X})$ refers to the group of all homeomorphisms of $\mathbb{X}$. These two groups are also known as the (topological) **centraliser** and **normaliser**, respectively.

PROPOSITION 4.3: *Let $k \geqslant 2$ be fixed, and let $(\mathbb{X}_{\mathcal{B}}, \mathbb{Z}^2)$ be the $\mathcal{B}$-free system from Proposition 4.2. Then, the centraliser is the trivial one, $\mathcal{S}(\mathbb{X}_{\mathcal{B}}) = \mathcal{G}$, and the normaliser is of the form $\mathcal{R}(\mathbb{X}_{\mathcal{B}}) = \mathcal{S}(\mathbb{X}_{\mathcal{B}}) \rtimes \mathcal{H}$, where $\mathcal{H}$ is isomorphic with a non-trivial subgroup of* $\mathrm{GL}(2, \mathbb{Z})$.

Proof. This is a consequence of [3, Thm. 5.3]. In fact, the triviality (or minimality) of the centraliser employs an argument put forward by Mentzen [22] for the subshift of square-free integers, which was then extended to lattice systems in [3].

With this structure of the centraliser, a variant of the Curtis–Hedlund–Lyndon (CHL) theorem, compare [21], can be used to prove that any element of $\mathcal{R}(\mathbb{X}_{\mathcal{B}})$ must be affine, which gives the semi-direct product structure as claimed; compare [3, Thm. 5.3], of which this is a special case.

That $\mathcal{H}$ must be non-trivial follows from the observation that the unit group $\mathcal{O}^\times$ always at least contains the elements ± 1. Via the embedding ι, this maps to a non-trivial subgroup of $\mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}(2, \mathbb{Z})$. ∎

Finally, we can wrap the stabiliser structure as follows.

THEOREM 4.4: *Let K be a quadratic field, with ring of integers $\mathcal{O}$, and let $(\mathbb{X}_{\mathcal{B}}, \mathbb{Z}^2)$ be the $\mathcal{B}$-free TDS from Proposition 4.2. Then, the normaliser is $\mathcal{R} = \mathcal{S} \rtimes \mathcal{H}$ with*

$$\mathcal{S} = \mathcal{G} = \mathbb{Z}^2 \quad \textit{and} \quad \mathcal{H} \simeq \mathcal{O}^\times \rtimes \mathrm{Aut}_{\mathbb{Q}}(K),$$

where $\mathrm{Aut}_{\mathbb{Q}}(K) = \mathrm{Gal}(K/\mathbb{Q})$.

Proof. It is clear from Theorems 3.12 and 3.17 that $\mathcal{S} \rtimes \mathcal{H}$ with $\mathcal{S} = \mathbb{Z}^2$ and $\mathcal{H}$ as stated is a subgroup of $\mathcal{R}$. We need to prove that no other element from $\mathbb{Z}^2 \rtimes \mathrm{GL}(2, \mathbb{Z})$ can lie in $\mathcal{R}$.

Assume, contrary to our claim, that some (t, M) with $t \in \mathbb{Z}^2$ and $M \in \mathrm{GL}(2,\mathbb{Z}) \setminus \mathrm{stab}(V_k')$ lies in $\mathcal{R}$. Since clearly also $(-t, \mathbb{1}) \in \mathcal{R}$, we may assume $t = 0$. Now, we will generalise the method employed in the proof of [3, Thm. 6.4] and construct an admissible set $S' \in V_k'$ such that its image $M(S')$ is not admissible. Then, the unique $\mathbb{Z}$-linear bijection A_M of $\mathcal{O}$ that corresponds to M is not an element of $\mathrm{Aut}(\mathbb{X}_{\mathcal{B}})$. From here on, we formulate our arguments with $\mathcal{O}$ and $V_k \subset \mathcal{O}$ directly, because we need to work with ideals anyhow.

Since $A_M \notin \mathrm{stab}(V_k)$ by assumption, there is a prime ideal $\mathfrak{p}_0$ in $\mathcal{O}$ and an element $w \in V_k$ such that $\mathfrak{p}_0^k$ divides the principal ideal generated by $A_M(w)$. Let P be a non-empty finite set of prime ideals of $\mathcal{O}$ that contains all primes $\mathfrak{p}$ with $\mathrm{N}(\mathfrak{p}) < \mathrm{N}(\mathfrak{p}_0)$, but none with $\mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{p}_0)$. Then, the ideal

$$\mathfrak{L} := \prod_{\mathfrak{p} \in P} \mathfrak{p}^k$$

is a submodule of $\mathcal{O}$ of index $\mathrm{N}(\mathfrak{L}) = \prod_{\mathfrak{p}\in P} \mathrm{N}(\mathfrak{p})^k$. Since this index is coprime to $n := \mathrm{N}(\mathfrak{p}_0^k) = \mathrm{N}(\mathfrak{p}_0)^k$, the ideal $\mathfrak{L}$, and likewise its translate $1 + \mathfrak{L}$, meet all cosets of $A_M^{-1}(\mathfrak{p}_0^k)$. We set $s_1 := w$ and choose numbers $s_2, \dots, s_n \in 1 + \mathfrak{L}$ such that $A_M(s_2), \dots, A_M(s_n)$ meet all non-zero cosets of $\mathfrak{p}_0^k$. We define $S := \{s_1, \dots, s_n\}$. Then, $A_M(S)$ clearly meets all cosets of $\mathfrak{p}_0^k$ and thus is not admissible.

Next, we modify the set S such that it becomes admissible, but without changing $A_M(S)$ modulo $\mathfrak{p}_0^k$. Note that S is clearly admissible for all primes $\mathfrak{q}$ with $\mathrm{N}(\mathfrak{q}) > \mathrm{N}(\mathfrak{p}_0)$ by cardinality. If S happens to meet all cosets of $\mathfrak{p}_0^k$, each of them must occur precisely once. We then replace s_2 by $s_2' := s_2 + w$ which does not change $A_M(S)$ modulo $\mathfrak{p}_0^k$, but reduces the number of cosets of $\mathfrak{p}_0^k$ in S by one.

If there is a second prime $\overline{\mathfrak{p}}_0$ of the same norm, $\mathrm{N}(\overline{\mathfrak{p}}_0) = \mathrm{N}(\mathfrak{p}_0)$, and if S happens to meet all cosets of $\overline{\mathfrak{p}}_0^k$, we play the same game as above. However, due to the previous step, we can neither use s_2' nor the second element of S which is congruent to s_2' modulo $\mathfrak{p}_0^k$. Nevertheless, we still have enough freedom, as n is at least 4.

It remains to show that S is admissible for all primes $\mathfrak{p}$ with $\mathrm{N}(\mathfrak{p}) < \mathrm{N}(\mathfrak{p}_0)$. We know by construction that all $s_i \in S$ are congruent to 1, w or $1 + w$ modulo $\mathfrak{p}^k$ (indeed modulo $\mathfrak{L}$). It follows that S meets at most 3 cosets of $\mathfrak{p}^k$ and is thus admissible for $\mathfrak{p}$ as $\mathrm{N}(\mathfrak{p}^k) \geqslant 2^k \geqslant 4$. Consequently, $S' = \iota(S) \subset \mathbb{Z}^2$ is the set we were after, and we are done. ∎

Both the centraliser and the normaliser are invariants of topological dynamical systems, which is to say that topologically conjugate systems must have isomorphic centralisers and normalisers, respectively. While the centraliser is always the same in Theorem 4.4, hence a toothless tiger in our setting, the normaliser allows a simple distinction between imaginary quadratic fields, where $\mathcal{O}^\times$ is a finite group, and real quadratic fields, where it is not.

COROLLARY 4.5: *Let $k, \ell \geqslant 2$ be arbitrary integers. Then, the k-free shift induced by a real quadratic field can never be topologically conjugate to the ℓ-free shift induced by an imaginary quadratic field.* ∎

Let us start with a k-free shift induced by an arbitrary quadratic field, $\mathbb{X}$ say, and consider the hypothetic situation of a factor shift according to the commutative diagram

$$\begin{array}{ccc} \mathbb{X} & \xrightarrow{\mathbb{Z}^2} & \mathbb{X} \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ \mathbb{Y} & \xrightarrow{\mathbb{Z}^2} & \mathbb{Y} \end{array} \tag{4.5}$$

where we assume $\mathbb{Y}$ to be another shift of this kind, hence with the same translation group acting on $\mathbb{X}$ and $\mathbb{Y}$. Here, ϕ is a continuous surjection.

While the topological normaliser proves Corollary 4.5, it is a more difficult question whether one such shift can be a factor of another, according to the diagram in (4.5). While one direction can usually be excluded via the topological entropy, as we shall explain in Section 5 below, also the opposite one looks highly unlikely. This is so because a factor map in the presence of such different normalisers would imply an extremely complicated fibre structure for the mapping ϕ. We shall discuss one particular example later.

For a classification of the k-free shifts up to topological conjugacy, we obviously need more than the normaliser. This is clear from Corollary 3.18 already for a fixed field K and different values of k. While there are many advanced invariants around, few of them are easy to determine, and hence of limited explicit use. One exception is topological entropy, which is a powerful invariant for the classification task, as we shall discuss next.

5. Entropy

It is well known [25] that dynamical systems of this kind have nice spectral properties, which allow to use the Halmos–von Neumann theorem for a distinction up to measure-theoretic isomorphism, but not immediately up to topological conjugacy. Fortunately, one can also determine the topological entropy. In our number-theoretic setting with quadratic fields, the result reads as follows.

THEOREM 5.1: *Let K be a quadratic field, and let V_k' with $k \geqslant 2$ be the set defined in Eq.* (4.1). *Then, the topological entropy of the induced $\mathcal{B}$-free TDS $(\mathbb{X}_{\mathcal{B}}, \mathbb{Z}^2)$ agrees with the patch counting entropy of V_k' and is given by*

$$\log(2)\,\mathrm{dens}(V_k') = \log(2)/\zeta_K(k).$$

Proof. It is well known for this type of dynamical systems that the topological entropy agrees with the patch-counting entropy; see [7, Thm. 1 and Rem. 2] in conjunction with [18, Rem. 4.3]. As $\mathbb{X}_{\mathcal{B}}$ is obtained as an orbit closure of the single set V_k', we can derive the entropy from this set and its properties.

Since V_k' is hereditary, we can 'knock out' each point individually without leaving the space $\mathbb{X}_{\mathcal{B}}$, which immediately implies that $\log(2)\,\mathrm{dens}(V_k')$ is a lower bound for the entropy.

On the other hand, the set V_k' is a weak model set of maximal density, with window W in internal space. In this case, since we used a formulation with a lattice of density 1, we know from [18, Thm. 4.5] that $\log(2)\,\mathrm{vol}(W)$ is an upper bound for the patch counting entropy of V_k'. It also applies to the topological entropy of the dynamical system, see [18, Rem. 4.3 and 4.6]. Since

$$\mathrm{vol}(W) = 1/\zeta_K(k) = \mathrm{dens}(V_k')$$

by Lemma 4.1, our claim follows. ∎

LEMMA 5.2: *Let K be a real quadratic field and let $k = 2\ell \in \mathbb{N}$ be an even integer. Then, K and k are uniquely determined by the number $\zeta_K(k)$.*

Proof. By a result due to Siegel [28], see also [24, Ch. VII, Cor. 9.9], we know that

$$\zeta_K(2\ell) = \frac{p\,\pi^{4\ell}}{q\sqrt{d_K}}$$

holds for some coprime $p, q \in \mathbb{N}$, where d_K is the discriminant of K as before. Now, if K and K' are both real quadratic fields, the identity $\zeta_K(2\ell) = \zeta_{K'}(2\ell')$

implies that $\pi^{4(\ell'-\ell)}$ is algebraic, which forces $\ell' = \ell$. Then, we get the identity $m^2 d_K = n^2 d_{K'}$ for some coprime $m, n \in \mathbb{N}$, hence $m^2 | d_{K'}$ and $n^2 | d_K$. Consequently, one must have $m, n \in \{1, 2\}$, and by checking the possible cases one finds that $m = n = 1$ is the only option. ∎

This has an interesting consequence on the role of topological entropy for our dynamical systems as follows.

PROPOSITION 5.3: *Among the k-free shifts that emerge from real quadratic fields, with k even, no two are topologically conjugate unless they are equal. In particular, topological entropy is a complete invariant within the class.*

Proof. By Theorem 5.1 the entropy has the form $s = \log(2)/\zeta_K(k)$, from which we can derive the value $\zeta_K(k)$. The latter determines K and k by Lemma 5.2. ∎

A more general result of this kind involving arbitrary integers $k \geqslant 2$ might still hold, but deciding this seems to require new ideas in view of the fact that the known formulas for $\zeta_K(k)$ at odd positive integers k are too cumbersome; compare [10].

Next, let us show that a folklore conjecture on zeta values predicts that the entropy is a complete invariant within the class of k-free shifts in imaginary quadratic fields with k odd. To this end, let K be an imaginary quadratic field and write $k = 2m + 1$ with $m \in \mathbb{N}$. We want to determine K and k from the value $\zeta_K(k)$.

Let $\chi\colon \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \{\pm 1\}$ be the unique non-trivial character of $\mathrm{Gal}(K/\mathbb{Q})$. Let f be the conductor of χ, so f is the smallest positive integer such that K is contained in the cyclotomic field $\mathbb{Q}(\xi_f)$, where ξ_f denotes a primitive f-th root of unity. Then, one has $f = |d_K|$, as follows from [24, Ch. VII, Conductor-Discriminant-Formula 11.9], but can also be seen more directly as follows.

We first show that K is contained in $\mathbb{Q}(\xi_{|d_K|})$. Let $K = \mathbb{Q}(\sqrt{d})$, where $d < 0$ is square-free. If p is an odd prime dividing d_K, the field $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}\, p}\,)$ is contained in $\mathbb{Q}(\xi_{|d_K|})$; see [16, p. 51]. Now, consider the case $d \equiv 1 \bmod 4$. Then, $-d$ is a product of distinct (positive) odd primes p_i, and the number of those p_i which are $\equiv 3 \bmod 4$ is odd. Hence, we have

$$d = d_K = \prod_i (-1)^{(p_i-1)/2}\, p_i$$

and thus $\sqrt{d} \in \mathbb{Q}(\xi_{|d_K|})$ as desired. The cases $d \equiv 2, 3 \bmod 4$ can be treated similarly, using the additional observation that $\mathbb{Q}(\sqrt{\pm 2}\,)$ both are contained in $\mathbb{Q}(\xi_8)$.

Conversely, let f be the minimal integer such that K is contained in $\mathbb{Q}(\xi_f)$. By minimality, one has $f \not\equiv 2 \bmod 4$, as $\mathbb{Q}(\xi_f) = \mathbb{Q}(\xi_{f/2})$ otherwise. Moreover, a prime p is ramified in $\mathbb{Q}(\xi_f)$ if and only if p divides f. Since the primes dividing d_K already ramify in K, it follows that f must be divisible by d_K, which shows the claim. Only if d_K is divisible by 8, this requires a small additional argument that relies on the fact that none of the fields $\mathbb{Q}(\sqrt{\pm 2}\,)$ is contained in $\mathbb{Q}(\xi_4) = \mathbb{Q}(\mathrm{i})$.

Recall that there is a natural isomorphism $(\mathbb{Z}/f\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\xi_f)/\mathbb{Q})$ that maps $a \bmod f$ to the automorphism $\xi_f \mapsto \xi_f^a$. Then, χ may be viewed as a Dirichlet character $(\mathbb{Z}/f\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ with kernel $\mathrm{Gal}(\mathbb{Q}(\xi_f)/K)$. Since K is imaginary, the character χ is odd (or has exponent 1 in the terminology of [24, Ch. VII, § 2]), as $\chi(-1) = -1 = -\chi(1)$.

Let $\zeta(s) = \zeta_{\mathbb{Q}}(s)$ and $L(\chi, s)$ be the Riemann zeta function and the Dirichlet L-series attached to χ, respectively. Since k is odd and thus congruent to the exponent of χ mod 2, [24, Ch. VII, Cor. 10.5 and 2.10] imply that

$$\frac{\zeta_K(k)}{\zeta(k)} = L(\chi, k) = (-1)^{m+1}\, \frac{\tau(\chi)}{2\mathrm{i}} \Big(\frac{2\pi}{f}\Big)^k \frac{B_{k,\chi}}{k!}. \tag{5.1}$$

Here, $B_{k,\chi}$ denotes the associated generalised Bernoulli number which is rational because the image of χ is, compare [24, p. 441], and $\tau(\chi)$ is the Gauss sum given by

$$\tau(\chi) := \sum_{a \in (\mathbb{Z}/f\mathbb{Z})^\times} \chi(a)\, \xi_f^a = \sum_{a \in \ker(\chi)} (\xi_f^a - \xi_f^{-a}) \in \mathrm{i}\mathbb{R}.$$

By [24, Ch. VII, Prop. 2.6], its absolute value is $\sqrt{f}$, so that indeed

$$\tau(\chi) = \pm \mathrm{i}\sqrt{f} = \pm \mathrm{i}\sqrt{|d_K|}. \tag{5.2}$$

It now follows from (5.1) and (5.2) that

$$\alpha_k := \frac{\zeta_K(k)}{\zeta(k)\pi^k} = q\sqrt{|d_K|} \tag{5.3}$$

for some (explicit) non-zero rational number q. It is now conjectured that the numbers

$$\pi, \zeta(3), \zeta(5), \zeta(7), \ldots$$

are algebraically independent (see [16] for a survey). Assuming this, Eq. (5.3) shows that the value $\zeta_K(k)$ determines k uniquely. Once we know k, we retrieve K from $K = \mathbb{Q}(\sqrt{|d_K|}\,) = \mathbb{Q}(\alpha_k)$, where α_k via (5.3) is clearly determined by $\zeta_K(k)$ and k. Let us sum this up as follows.

COROLLARY 5.4: *Let $k, \ell \geqslant 3$ be arbitrary odd integers. Under the assumption that the numbers $\pi, \zeta(3), \zeta(5), \zeta(7), \ldots$ are algebraically independent, no k-free shift induced by an imaginary quadratic field K can be topologically conjugate to the ℓ-free shift induced by K or, in fact, by any other imaginary quadratic field.* ∎

Next, observe that, for $a > 1$, the fraction $\frac{1}{1-a^{-s}}$ is strictly decreasing on the set $\{s > 1\}$. Consequently, the Dedekind zeta function

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathrm{N}(\mathfrak{p})^{-s}}$$

of a quadratic field, which is absolutely convergent on the half-plane $\{\mathrm{Re}(s) > 1\}$, is strictly decreasing on $\{s > 1\}$ as well, with $\lim_{s\to\infty} \zeta_K(s) = 1$. This has the following consequence.

COROLLARY 5.5: *Let K be any quadratic field, and $\mathbb{X}_k$ the k-free shift induced by it. Then, the TDS $(\mathbb{X}_k, \mathbb{Z}^2)$ can never be a factor of $(\mathbb{X}_\ell, \mathbb{Z}^2)$ when $k > \ell$.*

Proof. The entropy of $\mathbb{X}_k$ is $\log(2)/\zeta_K(k)$ by Theorem 5.1. As such, via the above observation, it is strictly increasing on $\{k \in \mathbb{N} : k \geqslant 2\}$, with limiting value $\log(2)$ as $k \to \infty$.

Since no factor of a TDS, in the sense of (4.5), can have a larger entropy than the original TDS, compare [29, Prop. 10.1.3], the claim is immediate. ∎

Let us close with another example, where we consider the shift $\mathbb{X}_V$ induced by the visible lattice points

$$V = \{(m, n) \in \mathbb{Z}^2 : (m, n) = 1\} = \mathbb{Z}^2 \setminus \bigcup_p p\mathbb{Z}^2,$$

where p runs through the rational primes, in comparison to the shift $\mathbb{X}_{\mathrm{G}}$ induced by the square-free Gaussian integers.

PROPOSITION 5.6: *Neither of the two shifts $(\mathbb{X}_V, \mathbb{Z}^2)$ and $(\mathbb{X}_{\mathrm{G}}, \mathbb{Z}^2)$ can be a topological factor of the other in the sense of the diagram in* (4.5).

Proof. The entropy of $(\mathbb{X}_V, \mathbb{Z}^2)$ is $\log(2)/\zeta(2)$; compare [5]. Now,

$$\zeta_{\mathbb{Q}(\mathrm{i})}(2) = \zeta(2)\, L(\chi, 2)$$

with χ the principal character of $\mathbb{Q}(\mathrm{i})$, where $L(\chi, 2) < 1$. Consequently, as the topological entropy of the Gaussian shift is larger than that of $\mathbb{X}_V$, one direction is ruled out immediately.

For the other direction, assuming that we have a surjective factor map $\phi\colon \mathbb{X}_{\mathrm{G}} \longrightarrow \mathbb{X}_V$, we now construct a configuration that is legal in $\mathbb{X}_{\mathrm{G}}$ whose image under ϕ cannot lie in $\mathbb{X}_V$. Due to the CHL theorem, ϕ is a sliding block map, hence given by a local function $\Phi\colon \{0,1\}^M \longrightarrow \{0,1\}$, where $M \subset \mathbb{Z}^2$ is the **memory set** or **local window** of ϕ.

Since ϕ is surjective, the singleton pattern $1_{\{\mathbf{0}\}} \in \mathbb{X}_V$ must have some preimage in $\mathbb{X}_{\mathrm{G}}$. This, in turn, implies the existence of some point pattern P such that $\Phi(P) = 1$. As P is a pattern that appears in some element of $\mathbb{X}_{\mathrm{G}}$, we may identify P with a G-admissible finite subset of M, which we also call P by slight abuse of notation. Thus, for every Gaussian prime q, there is some coset $r_q + (q^2)$ whose intersection with P is empty.

In what follows, let p be an inert rational prime such that $p^2 > \mathrm{card}(P)$. Let $\{q_1, q_2, \ldots, q_k\}$ be the set of all Gaussian primes of norm less than p^2, which is a finite set. By the Chinese Remainder Theorem, for every element (m,n) with $0 \leqslant m,n \leqslant p-1$, there exists a unique solution $\bmod(q_1^2 q_2^2 \cdots q_k^2 p^2)$ in $\mathbb{Z}[\mathrm{i}] \simeq \mathbb{Z}^2$ for the system of equations given by

$$x \equiv 0 \bmod (q_i^2) \qquad \text{for all } 1 \leqslant i \leqslant k$$

and

$$x \equiv (m,n) \bmod (p^2).$$

Let $x^{(m,n)} \in \mathbb{Z}^2$ be one solution of this system of congruences. Then, the set of *all* solutions is the lattice coset $x^{(m,n)} + (q_1^2 q_2^2 \cdots q_k^2 p^2)$. Clearly, no translation by an element of the lattice $(q_1^2 q_2^2 \cdots q_k^2 p^2)$ changes the equivalence class $\bmod(q_i^2)$ of any element of P. Now, for any $q \in \{q_1, \ldots, q_k\}$, there is some coset $r_q + (q^2)$ that has empty intersection with P, whence we also have the relation

$$(x^{(m,n)} + P) \cap (r_q + (q^2)) = \varnothing.$$

Clearly, $x^{(m,n)} + (q_1^2 q_2^2 \cdots q_k^2 p^2)$ is a relatively dense subset of $\mathbb{Z}[\mathrm{i}]$. Then, for every (m,n) with $0 \leqslant m,n \leqslant p-1$, we can choose an element $y^{(m,n)} \in x^{(m,n)} + (q_1^2 q_2^2 \cdots q_k^2 p^2)$ such that

$$\|y^{(m,n)} - y^{(m',n')}\|_2 > 2\,\mathrm{diam}(M)$$

holds for $(m,n) \neq (m',n')$. Let us now consider the set

$$P^* = \bigcup_{0 \leqslant m,n \leqslant p-1} y^{(m,n)} + P,$$

where we recall that we identify P with a subset of M. Since every term of this disjoint union has empty intersection with $r_q + (q^2)$, where q is any of the q_i, the set P^* has empty intersection with this coset as well.

Furthermore, $\operatorname{card}(P^*) = p^2 \operatorname{card}(P) < p^4$, due to our choice of p. Since the prime p is inert, and thus also a Gaussian prime, we have

$$[\mathbb{Z}[\mathrm{i}] : (p^2)] = \mathrm{N}(p)^2 = p^4,$$

so P^* necessarily misses a coset of (p^2). The same holds for every Gaussian prime of norm larger than p^2. Since any Gaussian prime of norm smaller than p^2 is one of the q_i's, we conclude that P^* is G-admissible, whence $u = 1_{P^*} \in \mathbb{X}_{\mathrm{G}}$. By the choice of Φ and the CHL theorem, we then have

$$\phi(u)_{y^{(m,n)}} = \Phi(u|_{y^{(m,n)}+M}) = \Phi(P) = 1,$$

for every $0 \leqslant m, n \leqslant p-1$, where we use that the p^2 translates of P in P^* are separated by more than $2\operatorname{diam}(M)$ by construction. Thus, they locally (for a disk-like window that covers the set M) look like a translate of 1_P. Consequently, if $\phi(u) = 1_U$, we have the inclusion

$$U \supseteq \{y^{(m,n)} : 0 \leqslant m, n \leqslant p-1\}.$$

Since we have $y^{(m,n)} \equiv (m,n) \bmod (p^2)$, with $(p^2) = p^2\mathbb{Z}^2$, we also have

$$y^{(m,n)} \equiv (m,n) \bmod p\mathbb{Z}^2.$$

Thus, U contains a complete set of representatives of $\mathbb{Z}^2/p\mathbb{Z}^2$, hence cannot be V-admissible. This contradiction implies that the factor map ϕ cannot exist. ∎

It is clear that this argument can be adapted to other quadratic fields as well, which we leave to the interested reader. It seems quite plausible that most if not all of the shift spaces we have analysed above are independent of each other in this stronger sense.

At this point, it is also natural to cover more field extensions that are Galois, and consider general cyclotomic fields in particular. Here, we expect that the result on the (extended) symmetries is structurally the same, which suggests that it might hold more generally. On the other hand, it looks doubtful whether entropy can be as strong as it seems here.

Acknowledgements. It is our pleasure to thank Uwe Grimm, Jürgen Klüners, Christoph Richard, Dan Rust and Johannes Sprang for helpful discussions. We thank an anonymous referee for several thoughtful comments that helped us to improve the presentation. AB was supported by the EPSRC (grant no. EP/S010335/1). He is also grateful to the Research Centre for Mathematical Modelling (RCM^2) at Bielefeld University for hospitality, and AN acknowledges financial support by the German Research Foundation (DFG) through its Heisenberg program (project no. 437113953).

Open Access. This article is distributed under the terms of the Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution and reproduction in any medium, provided the appropriate credit is given to the original authors and the source, and a link is provided to the Creative Commons license, indicating if changes were made (`https://creativecommons.org/licenses/by/4.0/`).
Open Access funding enabled and organized by Projekt DEAL.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer, New York–Heidelberg, 1968.

[2] M. Baake, *A brief guide to reversing and extended symmetries of dynamical systems*, in *Ergodic Theory and Dynamical Systems in their Interactions with Arithmetics and Combinatorics*, Lecture Notes in Mathematics, Vol. 2213, Springer, Cham, 2018, pp. 117–135.

[3] M. Baake, Á. Bustos, C. Huck, M. Lemańczyk and A. Nickel, *Number-theoretic positive entropy shifts with small centraliser and large normaliser*, Ergodic Theory and Dynamical Systems **41** (2021), 3201–3226.

[4] M. Baake and U. Grimm, *Aperiodic Order. Vol. 1*, Encyclopedia of Mathematics and its Applications, Vol. 149, Cambridge University Press, Cambridge, 2013.

[5] M. Baake and C. Huck, *Ergodic properties of visible lattice points*, Trudy Matematicheskogo Instituta Imeni V. A. Steklova **288** (2015), 184–208.

[6] M. Baake, C. Huck and N. Strungaru, *On weak model sets of extremal density*, Indagnationes Mathematicae **28** (2017), 3–31.

[7] M. Baake, D. Lenz and C. Richard, *Pure point diffraction implies zero entropy for Delone sets with uniform cluster frequencies*, Letters in Mathematical Physics **82** (2007), 61–77.

[8] M. Baake, R. V. Moody and P. A. B. Pleasants, *Diffraction of visible lattice points and kth power free integers*, Discrete Mathematics **221** (2000), 3–42.

[9] M. Baake, J. A. G. Roberts and R. Yassawi, *Reversing and extended symmetries of shift spaces*, Discrete and Continuous Dynamical Systems. Series A **38** (2018), 835–866.

[10] S. Banerjee, K. Chakraborty and A. Hoque, *An analogue of Wilton's formula and values of Dedekind zeta functions*, Journal of Mathematical Analysis and Applications **495** (2021), Article no. 124675.

[11] Á. Bustos, *Extended symmetry groups of multidimensional subshifts with hierarchical structure*, Discrete and Continuous Dynamical Systems. Series A **40** (2020), 5869–5895.

[12] F. Cellarosi and I. Vinogradov, *Ergodic properties of k-free integers in number fields*, Journal of Modern Dynamics **7** (2013), 461–488.

[13] H. S. M. Coxeter, *Introduction to Geometry*, Wiley, New York–London–Sydney, 1969.

[14] A. Dymek, S. Kasjan, J. Kułaga-Przymus and M. Lemańczyk, *$\mathcal{B}$-free sets and dynamics*, Transactions of the American Mathematical Society **370** (2018), 5425–5489.

[15] E. H. El Abdalaoui, M. Lemańczyk and T. de La Rue, *A dynamical point of view on the set of $\mathcal{B}$-free integers*, International Mathematics Research Notices **16** (2015), 7258–7286.

[16] S. Fischler, *Irrationalité de valeurs de zêta (d'après Apéry, Rivoal,...)*, Astérisque **294** (2004), 27–62.

[17] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton University Press, Princeton, 1981.

[18] C. Huck and C. Richard, *On pattern entropy of weak model sets*, Discrete & Computational Geometry **64** (2015), 741–757.

[19] S. Kasjan, G. Keller and M. Lemańczyk, *Dynamics of $\mathcal{B}$-free sets: a view through the window*, International Mathematics Research Notices **9** (2019), 2690–2734.

[20] G. Keller, *Maximal equicontinuous generic factors and weak model sets*, Discrete and Continuous Dynamical Systems. Series A **40** (2020), 6855–6875.

[21] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge University Press, New York, 1995.

[22] M. K. Mentzen, *Automorphisms of subshifts defined by $\mathcal{B}$-free sets of integers*, Colloquium Mathematicum **147** (2017), 87–94.

[23] Y. Meyer, *Algebraic Numbers and Harmonic Analysis*, North-Holland Mathematical Library, Vol. 2, North-Holland, Amsterdam, 1972.

[24] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, Vol. 322, Springer, Berlin, 1999.

[25] P. A. B. Pleasants and C. Huck, *Entropy and diffraction of the k-free points in n-dimensional lattices*, Discrete & Computational Geometry **50** (2013), 39–68.

[26] P. Sarnak, *Möbius randomness and dynamics*, Lecture slides, `https://publications.ias.edu/sarnak/paper/518`.

[27] K. Schmidt, *Dynamical Systems of Algebraic Origin*, Progress in Mathematics, Vol. 128, Birkhäuser, Basel, 1995.

[28] C.-L. Siegel, *Über die Fourierschen Koeffizienten von Modulformen*, Nachrichten der Akademie der Wissenschaften zu Göttingen. II. Mathematisch-Physikalische Klasse **1970** (1970), 15–56.

[29] M. Viana and K. Oliveira, *Foundations of Ergodic Theory*, Cambridge Studies in Advanced Mathematics, Vol. 151, Cambridge University Press, Cambridge, 2016.

[30] B. Weiss, *Single Orbit Dynamics*, American Mathematical Society, Providence, RI, 2000.

[31] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Hochschultext, Springer, Berlin–New York, 1981.