Chapter 4
Ideal Lattices

In Chap. 2, interesting lattices together with their parameters and applications were presented. In Chap. 3, one method to build such lattices was discussed, which consists of obtaining lattices from linear codes. This chapter presents two other methods to construct lattices, both called ideal lattices, because they both rely on the structure of ideals in rings. We recall that given a commutative ring R, an *ideal* of R is an additive subgroup of R which is also closed under multiplication by elements of R. The same terminology is used for two different viewpoints on lattices because of the communities that studied them. We will explain the first method using quadratic fields and refer to [79] for general number field constructions. We note that such a lattice construction from number fields can in turn be combined with Construction A to obtain further lattices, e.g., [59] and references therein. In the second method, "ideal lattices" refer to a family of lattices recently used in cryptography.

4.1 Ideal Lattices from Quadratic Fields

For $d > 1$ a squarefree integer, consider the field

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d},\ a, b \in \mathbb{Q}\}$$

which is called *quadratic* because it has dimension 2 as a vector space over $\mathbb{Q}$ (elements in $\mathbb{Q}(\sqrt{d})$ can be written as vectors (a, b), fixing, for example, $\{1, \sqrt{d}\}$ as a basis).

Since $d > 1$, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$. It is clear that we have this field inclusion, but what is maybe less clear is that there are actually two meaningful ways of embedding $\mathbb{Q}(\sqrt{d})$ into $\mathbb{R}$:

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5_4

$$\sigma_1 : a + b\sqrt{d} \mapsto a + b\sqrt{d}$$
$$\sigma_2 : a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

The first one, the identity map, is probably the one that everyone thinks of. However, the second one is just as “meaningful," in the sense that σ_2, just as σ_1, includes $\mathbb{Q}(\sqrt{d})$ into $\mathbb{R}$ while preserving (1) its ring structure ($\sigma_2(x+y) = \sigma_2(x) + \sigma_2(y)$ and $\sigma_2(xy) = \sigma_2(x)\sigma_2(y)$ for all $x, y \in \mathbb{Q}(\sqrt{d})$) (2) its vector space structure ($\sigma_2(a) = a$ for any $a \in \mathbb{Q}$). In fact, σ_1, σ_2 are the only two maps that satisfy the above (2) conditions. Suppose τ satisfies both of them, then:

$$\tau\left((\sqrt{d})^2\right) = \begin{cases} \tau(d) = d \\ \tau(\sqrt{d})^2 \end{cases}$$

and thus $\tau(\sqrt{d})$ must satisfy

$$\tau(\sqrt{d})^2 - d = 0$$

showing that $\tau(\sqrt{d}) = \pm\sqrt{d}$. As a consequence $\sigma = (\sigma_1, \sigma_2)$ gives an embedding of $\mathbb{Q}(\sqrt{d})$ into $\mathbb{R}^2$.

4.1.1 Lattice Constructions

Now our purpose is to obtain lattices, which are discrete structures. The above embedding suggests it may be possible to obtain 2-dimensional lattices, if we start from a discrete structure within $\mathbb{Q}(\sqrt{d})$. A natural candidate for this is

$$\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d}, a, b, \in \mathbb{Z}\right\}.$$

Now $\mathbb{Z}[\sqrt{d}]$ is not a vector space, but it has a basis, given, for example, by $\{1, \sqrt{d}\}$. Embedding this basis using σ gives,

$$B = \begin{bmatrix} 1 & \sigma_1(\sqrt{d}) \\ 1 & \sigma_2(\sqrt{d}) \end{bmatrix} = \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}$$

and integer linear combinations of rows of B do define a lattice (since the two rows are linearly independent). Note that

$$Bu = \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1 + u_2\sqrt{d} \\ u_1 - u_2\sqrt{d} \end{bmatrix} = \begin{bmatrix} \sigma_1(x) \\ \sigma_2(x) \end{bmatrix}, \ x = u_1 + u_2\sqrt{d} \qquad (4.1)$$

which gives a nice geometric interpretation of how an element $x \in \mathbb{Z}[\sqrt{d}]$ is embedded in the lattice $\sigma(\mathbb{Z}[\sqrt{d}])$.

The lattice construction proposed above only relies on having a "discrete structure"[1] in $\mathbb{Q}(\sqrt{d})$ with a $\mathbb{Z}$-basis. If $d \equiv 1(\text{mod}4)$, it is possible for example to take $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Let us give some examples, before discussing the meaning of the condition $d \equiv 1(\text{mod}4)$.

Example 4.1 The ring $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \{a + b\frac{1+\sqrt{5}}{2},\ a, b \in \mathbb{Z}\}$ is a subset of the field $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5},\ a, b \in \mathbb{Q}\}$. The two ways of embedding $\mathbb{Q}(\sqrt{5})$ into $\mathbb{R}$ are:

$$\sigma_1 : \sqrt{5} \mapsto \sqrt{5},\ \sigma_2 : \sqrt{5} \mapsto -\sqrt{5}.$$

We then embed $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ into $\mathbb{R}^2$ using $\sigma = (\sigma_1, \sigma_2)$, to get a generator matrix

$$B = \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{5}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}.$$

This lattice is shown in Fig. 4.2. Its corresponding Gram matrix is

$$G = B^T B = \begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{5}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}.$$

To compare, a Gram matrix for the lattice $\sigma(\mathbb{Z}[\sqrt{5}])$, shown in Fig. 4.1, is

$$\begin{bmatrix} 1 & 1 \\ \sigma_1(\sqrt{5}) & \sigma_2(\sqrt{5}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\sqrt{5}) \\ 1 & \sigma_2(\sqrt{5}) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 10 \end{bmatrix}.$$

Let us now consider $d \not\equiv 1(\text{mod}4)$.

Example 4.2 The two ways of embedding $\mathbb{Q}(\sqrt{2})$ into $\mathbb{R}$ are:

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2},\ \sigma_2 : \sqrt{2} \mapsto -\sqrt{2}.$$

We then embed $\mathbb{Z}[\frac{1+\sqrt{2}}{2}]$ into $\mathbb{R}^2$ using $\sigma = (\sigma_1, \sigma_2)$, to get as Gram matrix

$$\begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{2}}{2}) & \sigma_2(\frac{1+\sqrt{2}}{2}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{2}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{2}}{2}) \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 3/2 \end{bmatrix},$$

[1] Such suitable structures are orders (rings with a $\mathbb{Z}$-basis) and their ideals, which explains the terminology *ideal lattice*.

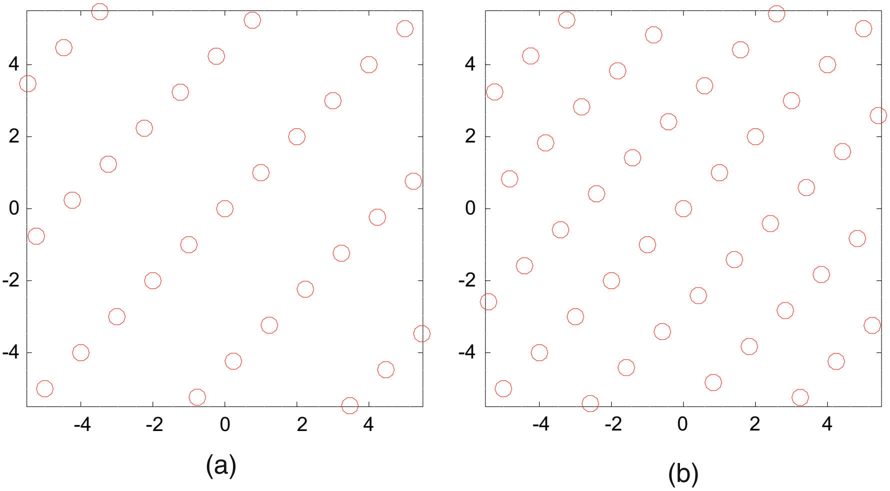

Fig. 4.1 Lattices from the quadratic fields $\mathbb{Z}[\sqrt{5}]$ and $\mathbb{Z}[\sqrt{2}]$, respectively. (**a**) The lattice obtained from $\{1, \sqrt{5}\}$. (**b**) The lattice obtained from $\{1, \sqrt{2}\}$

while a Gram matrix for the lattice $\sigma(\mathbb{Z}[\sqrt{2}])$ is

$$\begin{bmatrix} 1 & 1 \\ \sigma_1(\sqrt{2}) & \sigma_2(\sqrt{2}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\sqrt{2}) \\ 1 & \sigma_2(\sqrt{2}) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}.$$

This lattice is shown in Fig. 4.1.

The difference between the first example and the second is that in the first example, both Gram matrices have integer coefficients (the lattice is integral; see Definition 2.13), while in the second example, this is not the case.

The reason behind this is that the ring $\mathbb{Z}[\sqrt{d}]$ turns out to contain elements from $\mathbb{Q}(\sqrt{d})$ which all have the property of being the root of some monic polynomial whose coefficients live in $\mathbb{Z}$ (we recall that a polynomial $p(X)$ is monic if the coefficient of its leading term is equal to one). Now when $d \not\equiv 1(\mathrm{mod}4)$, it turns out (see Exercise 4.1) that $\mathbb{Z}[\sqrt{d}]$ is exactly the set of elements from $\mathbb{Q}(\sqrt{d})$ which are roots of monic polynomials with coefficients in $\mathbb{Z}$, while when $d \equiv 1(\mathrm{mod}4)$, this set is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Now for a $\mathbb{Z}$-basis $\{\theta_1, \theta_2\}$ (of, respectively, $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ depending on the congruence of $d(\mathrm{mod}4)$ or of (an ideal of) an order of these two rings), a Gram matrix is of the form

$$\begin{aligned} & \begin{bmatrix} \sigma_1(\theta_1) & \sigma_2(\theta_1) \\ \sigma_1(\theta_2) & \sigma_2(\theta_2) \end{bmatrix} \begin{bmatrix} \sigma_1(\theta_1) & \sigma_1(\theta_2) \\ \sigma_2(\theta_1) & \sigma_2(\theta_2) \end{bmatrix} \\ &= \begin{bmatrix} \sigma_1(\theta_1)^2 + \sigma_2(\theta_1)^2 & \sigma_1(\theta_1)\sigma_1(\theta_2) + \sigma_2(\theta_1)\sigma_2(\theta_2) \\ \sigma_1(\theta_1)\sigma_1(\theta_2) + \sigma_2(\theta_1)\sigma_2(\theta_2) & \sigma_1(\theta_2)^2 + \sigma_2(\theta_2)^2 \end{bmatrix} \\ &= \begin{bmatrix} \sigma_1(\theta_1^2) + \sigma_2(\theta_1^2) & \sigma_1(\theta_1\theta_2) + \sigma_2(\theta_1\theta_2) \\ \sigma_1(\theta_1\theta_2) + \sigma_2(\theta_1\theta_2) & \sigma_1(\theta_2^2) + \sigma_2(\theta_2^2) \end{bmatrix}. \end{aligned}$$

If we observe the coefficients of this matrix, they all are of the form

$$\sigma_1(a+b\sqrt{d})+\sigma_2(a+b\sqrt{d})=2a$$

for some $a, b \in \mathbb{Q}$, which explains why the Gram matrix coefficients are in $\mathbb{Q}$.

Now $\sigma_1(a+b\sqrt{d}), \sigma_2(a+b\sqrt{d})$ and thus $\sigma_1(a+b\sqrt{d})+\sigma_2(a+b\sqrt{d})$ belong to the intersection of $\mathbb{Z}[\sqrt{d}]$ (or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ depending on $d(\text{mod} 4)$) and $\mathbb{Q}$. We claim that this intersection is $\mathbb{Z}$, and therefore the Gram matrix has integer coefficients.

To prove that the intersection is $\mathbb{Z}$, recall that we are looking at elements in $\mathbb{Q}$, thus of the form u/v, $v \neq 0$, $u, v \in \mathbb{Z}$, and we can assume $\gcd(u, v) = 1$, which are roots of some monic polynomial $p(X)$ with coefficients in $\mathbb{Z}$. This means

$$p(u/v) = p_0 + p_1(u/v) + p_2(u/v)^2 + \cdots + p_{n-1}(u/v)^{n-1} + (u/v)^n = 0$$

which implies

$$v^n p_0 + p_1 u v^{n-1} + p_2 u^2 v^{n-2} + \cdots + p_{n-1} u^{n-1} v + u^n = 0.$$

Now it must be that

$$v^n p_0 + p_1 u v^{n-1} + p_2 u^2 v^{n-2} + \cdots + p_{n-1} u^{n-1} v = -u^n$$

but the left-hand side is divisible by v, while the right-hand side is not, a contradiction, apart for $v = 1$.

Canonical $\mathbb{Z}$-bases are $\{1, \sqrt{d}\}$ and $\{1, \frac{1+\sqrt{d}}{2}\}$ depending on d. A variety of interesting lattices can be obtained by introducing a “twisting" element α such that $\sigma_1(\alpha) > 0$ and $\sigma_2(\alpha) > 0$ as follows. Let θ denote $\sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$ depending on $d(\text{mod} 4)$. A generator matrix of a lattice using a twisting element α is given by

$$B = \begin{bmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_1(\alpha)}\sigma_1(\theta) \\ \sqrt{\sigma_2(\alpha)} & \sqrt{\sigma_2(\alpha)}\sigma_2(\theta) \end{bmatrix} = \begin{bmatrix} \sqrt{\sigma_1(\alpha)} & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} \end{bmatrix} \begin{bmatrix} \sigma_1(1) & \sigma_1(\theta) \\ \sigma_2(1) & \sigma_2(\theta) \end{bmatrix}$$

and a Gram matrix by

$$B^T B = \begin{bmatrix} \sigma_1(\alpha)+\sigma_2(\alpha) & \sigma_1(\alpha\theta)+\sigma_2(\alpha\theta) \\ \sigma_1(\alpha\theta)+\sigma_2(\alpha\theta) & \sigma_1(\alpha\theta^2)+\sigma_2(\alpha\theta^2) \end{bmatrix}.$$

Note that the conditions $\sigma_1(\alpha) > 0$ and $\sigma_2(\alpha) > 0$ ensure that the lattice remains real (and no complex value is introduced when taking the square root). Furthermore, by taking α in $\mathbb{Z}[\theta]$, the lattice will remain an integral lattice, even though $\sqrt{\alpha}$ typically has no reason to be in $\mathbb{Z}[\theta]$. By Definition 2.4, the volume of the lattice[2] $\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])$ is given by the square root of

[2] Writing $\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])$ is a slight abuse of notation, since σ cannot really be applied to $\sqrt{\alpha}$ when it does not belong to $\mathbb{Z}[\theta]$.

$$\left(\det\begin{bmatrix}\sigma_1(1) & \sigma_2(1)\\ \sigma_1(\theta) & \sigma_2(\theta)\end{bmatrix}\right)^2\left(\det\begin{bmatrix}\sqrt{\sigma_1(\alpha)} & 0\\ 0 & \sqrt{\sigma_2(\alpha)}\end{bmatrix}\right)^2 = \sigma_1(\alpha)\sigma_2(\alpha)(\sigma_2(\theta)-\sigma_1(\theta))^2,$$

thus

$$V(\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])) = \sqrt{|\sigma_1(\alpha)\sigma_2(\alpha)|}|\sigma_2(\theta)-\sigma_1(\theta)|.$$

We continue Example 4.1.

Example 4.3 Take

$$\alpha = 3 - \tfrac{1+\sqrt{5}}{2},\ \alpha\theta = -1 + 2\tfrac{1+\sqrt{5}}{2},\ \alpha\theta^2 = 2 + \tfrac{1+\sqrt{5}}{2}.$$

Then a generator matrix of $\sigma(\sqrt{\alpha}\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$, illustrated in Fig. 4.2 is

$$B = \begin{bmatrix}\sqrt{\alpha} & \sqrt{\alpha}\frac{1+\sqrt{5}}{2}\\ \sqrt{\sigma_2(\alpha)} & \sqrt{\sigma_2(\alpha)}\frac{1-\sqrt{5}}{2}\end{bmatrix}$$

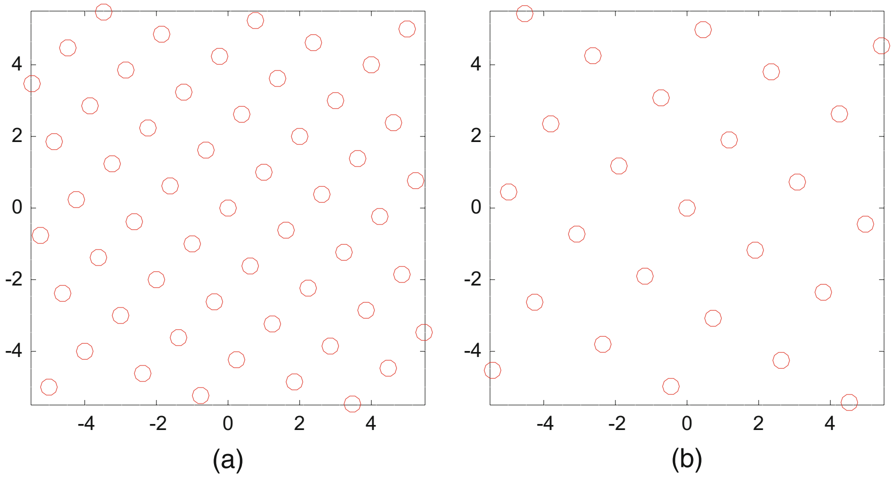

Fig. 4.2 Lattices from the quadratic field $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ with and without twisting. (**a**) The lattice obtained from $\{1, \frac{1+\sqrt{5}}{2}\}$. (**b**) The lattice obtained from $\{1, \frac{1+\sqrt{5}}{2}\}$ using a twisting element $\alpha = 3 - \frac{1+\sqrt{5}}{2}$

with corresponding Gram matrix

$$G = \begin{bmatrix} \sigma_1(3-\frac{1+\sqrt{5}}{2})+\sigma_2(3-\frac{1+\sqrt{5}}{2}) & \sigma_1(-1+2\frac{1+\sqrt{5}}{2})+\sigma_2(-1+2\frac{1+\sqrt{5}}{2}) \\ \sigma_1(-1+2\frac{1+\sqrt{5}}{2})+\sigma_2(-1+2\frac{1+\sqrt{5}}{2}) & \sigma_1(2+\frac{1+\sqrt{5}}{2})+\sigma_2(2+\frac{1+\sqrt{5}}{2}) \end{bmatrix}$$
$$= \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

and volume

$$V(\sigma(\sqrt{\alpha}\mathbb{Z}[\tfrac{1+\sqrt{5}}{2}])) = \sqrt{|\sigma_1(\alpha)\sigma_2(\alpha)|}|\sigma_2(\theta)-\sigma_1(\theta)|$$
$$= \sqrt{5}|\sqrt{5}| = 5.$$

This lattice is equivalent to (a scaled version of) $\mathbb{Z}^2$ (see Exercise 4.3).

4.1.2 Some Sublattices

Consider two lattices $\sigma(\beta\mathbb{Z}[\sqrt{d}])$ and $\sigma(\alpha\mathbb{Z}[\sqrt{d}])$, or $\sigma(\beta\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$ and $\sigma(\alpha\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$, with $\beta = \alpha\sigma(\alpha)$, $\alpha \neq \sigma(\alpha)$. Then $\sigma(\beta\mathbb{Z}[\sqrt{d}])$ is a sublattice of $\sigma(\alpha\mathbb{Z}[\sqrt{d}])$, or in the other case, $\sigma(\beta\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$ is a sublattice $\sigma(\alpha\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$. Indeed, consider, for the former case, the sets $I_1 = \{\alpha a + \alpha b\sqrt{d},\ a, b \in \mathbb{Z}\}$, $I_2 = \{\sigma(\alpha)a + \sigma(\alpha)b\sqrt{d},\ a, b \in \mathbb{Z}\}$, and $I = \{\beta a + \beta b\sqrt{d},\ a, b \in \mathbb{Z}\}$. Define the sets I, I_1, I_2 accordingly for the latter case, and the following argument also hold by replacing $\sqrt{d}$ by $\frac{1+\sqrt{d}}{2}$. Then $I_1 + I_2 = 1$, from which it follows that $I_1 I_2 = I_1 \cap I_2$ (see Exercise 4.4), and $I_1 I_2 = I$, where $I_1 I_2$ is the set formed by finite sums of terms of the form $i_1 i_2$, $i_1 \in I_1$, $i_2 \in I_2$. Take the lattice point

$$\begin{bmatrix} \sigma_1(\beta x) \\ \sigma_2(\beta x) \end{bmatrix}$$

in $\sigma(\beta\mathbb{Z}[\sqrt{d}])$. It is obtained by embedding $\beta x \in I$, with $I = I_1 I_2 = I_1 \cap I_2$. Thus βx also belongs to I_1, so its embedding will appear in the embedding of I_1, which yields $\sigma(\alpha\mathbb{Z}[\sqrt{d}])$. This is illustrated in Fig. 4.3.

4.1.3 Coding Applications

Recall from (4.1) that points in lattices obtained from quadratic fields are of the form

$$\begin{bmatrix} \sigma_1(x) \\ \sigma_2(x) \end{bmatrix}, \text{ or } \begin{bmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(x) \\ \sqrt{\sigma_2(\alpha)}\sigma_2(x) \end{bmatrix}$$

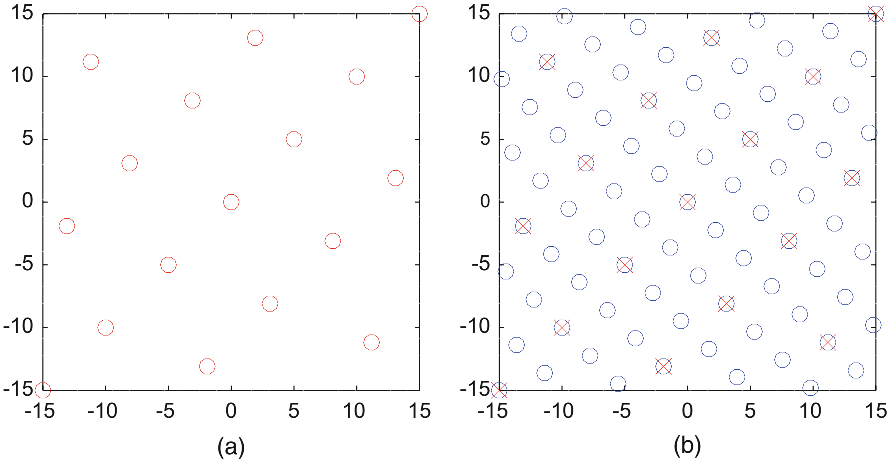

Fig. 4.3 The lattice $\sigma(5\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$ and a sublattice. (**a**) The lattice obtained from $\{5, 5\frac{1+\sqrt{5}}{2}\}$. (**b**) The sublattice obtained from $\{\alpha, \alpha\frac{1+\sqrt{5}}{2}\}$, $\alpha = 3 - \frac{1+\sqrt{5}}{2}$

for $x = u_1 + u_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, depending on the presence or not of a twisting element α. Such pairs of points satisfy the property that

$$\sigma_1(x) \neq 0,\ \sigma_2(x) \neq 0$$

for all $x \neq 0$, since $\sigma_1(x) = u_1 + u_2\sqrt{d} = 0$ if and only if $x = 0$, and similarly $\sigma_2(x) = u_1 - u_2\sqrt{d} = 0$ if and only if $x = 0$. Now take any two arbitrary distinct lattice points

$$\begin{bmatrix}\sigma_1(x)\\ \sigma_2(x)\end{bmatrix},\ \begin{bmatrix}\sigma_1(y)\\ \sigma_2(y)\end{bmatrix},\ \text{or}\ \begin{bmatrix}\sqrt{\sigma_1(\alpha)}\sigma_1(x)\\ \sqrt{\sigma_2(\alpha)}\sigma_2(x)\end{bmatrix},\ \begin{bmatrix}\sqrt{\sigma_1(\alpha)}\sigma_1(y)\\ \sqrt{\sigma_2(\alpha)}\sigma_2(y)\end{bmatrix},$$

then their difference belongs to the lattice and

$$\sqrt{\sigma_1(\alpha)}\sigma_1(x) - \sqrt{\sigma_1(\alpha)}\sigma_1(y) = \sqrt{\sigma_1(\alpha)}\sigma_1(x-y) \neq 0,$$
$$\sqrt{\sigma_2(\alpha)}\sigma_2(x) - \sqrt{\sigma_2(\alpha)}\sigma_2(y) = \sqrt{\sigma_2(\alpha)}\sigma_2(x-y) \neq 0.$$

Geometrically, this means that given any two distinct lattice points, they will always differ on both their components, as can be observed on the different earlier figures of this chapter.

This is meaningful when lattice points are used for transmission over fast-fading channels. We have already seen in Chap. 2 how lattice points are used for transmission over Gaussian channels. Over a fast-fading channel, communication is modeled by

$$\mathbf{y} = H\mathbf{x} + \mathbf{n},\ H = \begin{bmatrix} h_1 & 0 \\ 0 & h_2 \end{bmatrix}$$

where $\mathbf{n}$ is a random vector whose components are independent Gaussian random variables with mean 0 and variance σ^2, and h_1, h_2 are independently Rayleigh distributed. We notice that the model is very similar to (2.20), except for the matrix H which takes into account fading in a wireless environment. Assuming the receiver knows H (this is called a *coherent* channel), he is facing a channel similar to a Gaussian channel, only the lattice constellation transmitted is now twisted by the fading H. If $\mathbf{x}$ is a lattice point of the form $B\mathbf{u}$, then it is as if the lattice used for transmission had in fact generator matrix HB, and

$$H\mathbf{x} = \begin{bmatrix} h_1 & 0 \\ 0 & h_2 \end{bmatrix} \begin{bmatrix} \sigma_1(x) \\ \sigma_2(x) \end{bmatrix} = \begin{bmatrix} h_1\sigma_1(x) \\ h_2\sigma_2(x) \end{bmatrix}.$$

A lattice constellation for a Gaussian channel will make sure that lattice points are separated enough to resist the channel noise. However, even if $\sigma_j(x)$ and $\sigma_j(y)$ are designed to be apart, $h_j\sigma_j(x)$ and $h_j\sigma_j(y)$ could be arbitrarily close, depending on h_j, $j = 1, 2$.

The relevant distance in this case is the so-called *product distance*, which is the minimum of the absolute value of the product of the coordinates of non-zero vectors in the lattice. We may check (see Exercise 4.5) that the product distance, despite its name, is actually not a distance, as per Definition 3.2. It was shown that constellations in lattices with greater minimum product distance are associated to smaller error probability when used in signal transmission over Rayleigh fading channels [15]. The intuition is that the product distance captures the number of components in which lattice points (and therefore differences of lattice points) differ, guaranteeing that if the fading affects some components, the lattice points will still be distinguishable on their other non-zero components. Therefore lattices Λ in $\mathbb{R}^n$ with full diversity n are preferred, that is, lattices such that any of their vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, have $x_i \neq 0$, for any i. For a general lattice, it is computationally hard to determine its minimum product distance, which makes the interest of algebraic constructions of the type presented above; see, e.g., [9, 58]. Furthermore, since for a lattice in dimension n, its diversity is at most n, it can be increased by augmenting n, the dimension in which the lattice lives. One technique to do so is by considering tensor products, as explained next.

4.1.4 High-Dimensional Lattices

Consider two generator matrices

$$B_1 = \begin{bmatrix} \sigma_1(\theta_1) & \sigma_1(\theta_2) \\ \sigma_2(\theta_1) & \sigma_2(\theta_2) \end{bmatrix},\ B_2 = \begin{bmatrix} \tau_1(\nu_1) & \tau_1(\nu_2) \\ \tau_2(\nu_1) & \tau_2(\nu_2) \end{bmatrix}$$

and their Kronecker (tensor) product

$$B_1 \otimes B_2 = \begin{bmatrix} \sigma_1(\theta_1)B_2 & \sigma_1(\theta_2)B_2 \\ \sigma_2(\theta_1)B_2 & \sigma_2(\theta_2)B_2. \end{bmatrix}$$

Surely this defines the generator matrix of a 4-dimensional lattice, since the columns of this matrix are linearly independent: the determinant of the generator matrix is the product of the determinants of B_1 and B_2. Now in terms of diversity, it is harder to say something in general, though there is one case where we can easily show that the property of diversity is inherited from B_1 and B_2. Suppose that $\tau_i(\theta_j) = \theta_j$ and $\sigma_i(\nu_j) = \nu_j$, and we place ourselves in a large enough field[3] which contains θ_j, ν_j, and for which τ_i, σ_i are embeddings. Then

$$B_1 \otimes B_2 = \begin{bmatrix} \sigma_1\tau_1(\theta_1\nu_1) & \sigma_1\tau_1(\theta_1\nu_2) & \sigma_1\tau_1(\theta_2\nu_1) & \sigma_1\tau_1(\theta_2\nu_2) \\ \sigma_1\tau_2(\theta_1\nu_1) & \sigma_1\tau_2(\theta_1\nu_2) & \sigma_1\tau_2(\theta_2\nu_1) & \sigma_1\tau_2(\theta_2\nu_2) \\ \sigma_2\tau_1(\theta_1\nu_1) & \sigma_2\tau_1(\theta_1\nu_2) & \sigma_2\tau_1(\theta_2\nu_1) & \sigma_2\tau_1(\theta_2\nu_2) \\ \sigma_2\tau_2(\theta_1\nu_1) & \sigma_2\tau_2(\theta_1\nu_2) & \sigma_2\tau_2(\theta_2\nu_1) & \sigma_2\tau_2(\theta_2\nu_2) \end{bmatrix}$$

which is now the generator matrix of a lattice of dimension 4 and diversity 4. This process can be iterated to obtain lattices in dimensions which are powers of 2 (see Exercise 4.6).

Example 4.4 Take

$$B_1 = \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{5}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}, \; B_2 = \begin{bmatrix} 1 & \tau_1(\sqrt{2}) \\ 1 & \tau_2(\sqrt{2}) \end{bmatrix}.$$

We place ourselves in $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \{a_0+a_1\sqrt{5}+a_2\sqrt{2}+a_3\sqrt{5}\sqrt{2},\ a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$, so that $\sigma(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{5}) = \sqrt{5}$. Then $B_1 \otimes B_2$ is a 4-dimensional lattice with diversity 4.

4.2 Ideal Lattices for Cryptography

Consider a lattice Λ of dimension n living in $\mathbb{Z}^n$ instead of $\mathbb{R}^n$, meaning that all lattice points have integer coordinates. Now we ask for the following further *cyclic* property that for every $\mathbf{x} = (x_1, \ldots, x_n) \in \Lambda$, it must be that $(x_n, x_1, \ldots, x_{n-1})$ also belongs to Λ. Note that since the cyclic property is asked for every lattice point, it means that $(x_{n-1}, x_n, x_1, \ldots, x_{n-2}) \in \Lambda$ and, iteratively, all shifts of $\mathbf{x} = (x_1, \ldots, x_n)$ must be in Λ.

[3] We voluntarily skip the definition of compositum of two fields with coprime discriminants here, which would be the proper way to describe the suitable field extension.

Example 4.5 The lattice $\mathbb{Z}^2$ is cyclic. Indeed, if $(x_1, x_2) \in \mathbb{Z}^2$, this means that x_1, x_2 are integers, and (x_2, x_1) also belongs to $\mathbb{Z}^2$.

One way to obtain cyclic lattices is to use the following lemma.[4]

Lemma 4.1 *A lattice Λ in $\mathbb{Z}^n$ is a cyclic lattice if Λ is an ideal of $\mathbb{Z}[X]/(X^n - 1)$.*

Proof Given a lattice point $\mathbf{a} = (a_1, \cdots, a_n) \in \Lambda$, associate the polynomial in $\mathbb{Z}[X]$ given by $a_1 + a_2X + a_3X^2 + \ldots a_nX^{n-1}$. We notice that this polynomial belongs to $\mathbb{Z}[X]/(X^n - 1)$ since its degree is less than n. By definition of ideal, Λ is an ideal of $\mathbb{Z}[X]/(X^n - 1)$ means that it is closed under multiplication, that is, if we multiply $a_1 + a_2X + a_3X^2 + \ldots a_nX^{n-1}$ by X (and iteratively by powers of X), the result remains in Λ. But if we compute

$$(a_1 + a_2X + a_3X^2 + \ldots a_nX^{n-1})X = a_1X + a_2X^2 + a_3X^3 + \cdots a_nX^n,$$

we obtain $a_1X + a_2X^2 + a_3X^3 + \ldots a_n$ since $X^n \equiv 1$ in $\mathbb{Z}[X]/(X^n - 1)$. This shows that $(a_n, a_1, \ldots, a_{n_1}) \in \Lambda$ as desired.

Example 4.6 Consider $\mathbb{Z}[X]/(X^2 - 1)$, which is the set of polynomials $a_1 + a_2X$, $a_1, a_2 \in \mathbb{Z}$. Take the polynomial $g(X) = 2 + X \in \mathbb{Z}[X]/(X^2 - 1)$ and the ideal $(g(X))$ which is the set of all polynomials in $\mathbb{Z}[X]/(X^2 - 1)$ which are multiples of $g(X)$. It is indeed an ideal since it is closed under addition:

$$g(X)(a_1 + a_2X) + g(X)(a_1' + a_2'X)$$

is a multiple of $g(X)$. It is also clearly closed under multiplication: a multiple of $g(X)$ multiplied by any polynomial will remain a multiple of $g(X)$. Furthermore:

$$(2 + X)(a_1 + a_2X) = 2a_1 + 2a_2X + a_1X + a_2 = (a_2 + 2a_1) + (2a_2 + a_1)X.$$

This gives a set of vectors of the form $(a_2 + 2a_1, 2a_2 + a_1)$ corresponding to a generator matrix:

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

One may check explicitly (see Exercise 4.7) that this lattice is indeed cyclic.

Remark 4.1 The quotient $\mathbb{Z}[X]/(X^n - 1)$ does not have a field structure, therefore the underlying multiplicative structure of this construction is different from that of the previous "ideal lattices."

One interest in this construction of lattices is its succinct representation, since an n-dimensional lattice can be encoded with one vector. Furthermore, fast arithmetic

[4] A reader familiar with the theory of cyclic codes will notice the analogy between cyclic codes and cyclic lattices and their characterization.

is enabled using the fast Fourier transform (FFT). Yet unlike the q-ary lattices of Sect. 3.2.1, ideal lattices come with some guarantee in terms of complexity, e.g., the worst-case hardness of the SVP (see Problem 2.1) in cyclic lattices was analyzed in [71], to build one-way functions. Thus cyclic ideal lattices have been considered to build efficient cryptographic primitives and homomorphic encryption schemes. However, such lattice exhibit some weaknesses; see, e.g., [73, p.11], due to the fact that $X^n - 1$ is reducible over the rationals.

A natural generalization is to consider a polynomial[5] $p(X) \in \mathbb{Z}[X]$ other than $X^n - 1$, such as $X^n + 1$, for example, (in particular, the factor $X - 1$ of $X^n - 1$ is not present, and thus $X^n + 1$ tends to be preferred to $X^n - 1$). If $p(X)$ is instead a monic irreducible polynomial ($X^n - 1$ is not), then the quotient $\mathbb{Z}[X]/(p(X))$ becomes a field. A family of polynomials that has been considered in the literature is that of cyclotomic polynomials. The *m-th cyclotomic polynomial* $\phi_m(X)$ is by definition

$$\phi_m(X) = \prod_{k,\gcd(k,m)=1} (X - e^{\frac{2ik\pi}{m}}).$$

If m is prime, then $\phi_m(X) = \frac{X^m-1}{X-1}$. If m is a power of 2, then $\phi_m(X) = X^{m/2} + 1$ (see Exercise 4.8). We use the notation $\zeta_m = e^{\frac{2ik\pi}{m}}$. In that case, we have

$$\mathbb{Z}[X]/(\phi_m(X)) \simeq \mathbb{Z}[\zeta_m] \subset \mathbb{Q}(\zeta_m) \simeq \mathbb{Q}(X)/(\phi_m(X))$$

and $\mathbb{Q}(\zeta_m) = \{a_1 + a_2\zeta_m + \cdots + a_{d-1}\zeta_m^{d-1},\ a_1, \ldots, a_{d-1} \in \mathbb{Q}\}$ and $d = \varphi(n)$ is the Euler totient of n. The reason for considering cyclotomic polynomials is that they have been well studied.

Remark 4.2 Unlike for the quotient $\mathbb{Z}[X]/(X^n - 1)$, in this case of cyclotomic polynomials, both notions of "ideal lattices" coincide.

Thus to a vector, $(a_1, \ldots, a_{d-1})$ corresponds a polynomial $a_1 + a_2X + \cdots + a_{d-1}X^{d-1}$ in $\mathbb{Z}[X]/\phi_m(X)$, which in turn corresponds to an element $a_1 + a_2\zeta_m + \cdots + a_{d-1}X^{d-1} \in \mathbb{Q}(\zeta_m)$. The corresponding lattice is now obtained by embedding $\mathbb{Q}(\zeta_m)$ into $\mathbb{C}^n$. We illustrate this for the case $m = 4$, corresponding to the cyclotomic polynomial $\phi_4(X) = X^2 + 1$. Then $\mathbb{Q}(X)/(X^2 + 1) \simeq \mathbb{Q}(i)$.There are two embeddings (see the previous ideal construction):

$$\sigma_1 : i \mapsto i,\ \sigma_2 : i \mapsto -i.$$

A generator matrix is given by

$$\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}.$$

[5] For linear codes, we would call these pseudo-cyclic codes.

There is a similar problem to that of the shortest vector problem (see Problem 2.1) for ideal (see [102], [84], Sec. 4.3.4. and the references therein). Consider $\sigma = (\sigma_1, \ldots, \sigma_d)$ the vector of embeddings of a degree-d number field K.

Problem 4.1 Given an ideal I of $\mathscr{O}_K$, where K is a number field, find a non-zero element $b \in I$ which minimizes $\|\sigma(b)\|$.

The complexity of ideal lattice problems are summarized in [102], together with applications.

Exercises

Exercise 4.1 Show that the set of elements from $\mathbb{Q}(\sqrt{d})$ which are roots of monic polynomials with coefficients in $\mathbb{Z}$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ when $d \equiv 1(\text{mod}4)$ and $\mathbb{Z}[\sqrt{d}]$ when $d \not\equiv 1(\text{mod}4)$.

Exercise 4.2 Construct a 2-dimensional lattice from $\mathbb{Z}[\sqrt{3}]$.

Exercise 4.3 Show that the lattice $\sigma(\sqrt{\alpha}\mathbb{Z}[(1+\sqrt{5})/2])$ in Example 4.3 is equivalent to $\mathbb{Z}^2$. Exhibit the explicit orthogonal transformation matrix and scaling factor.

Exercise 4.4 Show that the sets $I_1 = \{\alpha a + \alpha b\sqrt{d},\ a, b \in \mathbb{Z}\}$, $I_2 = \{\sigma(\alpha)a + \sigma(\alpha)b\sqrt{d},\ a, b \in \mathbb{Z}\}$ and $I = \{\beta a + \beta b\sqrt{d},\ a, b \in \mathbb{Z}\}$ with $\beta = \alpha\sigma(\alpha), \alpha \neq \sigma(\alpha)$ satisfy $I_1 I_2 = I_1 \cap I_2$. Discuss what happens if $\alpha = \sigma(\alpha)$.

Exercise 4.5 Show that the product distance is not a mathematical distance.

Exercise 4.6 Construct an 8-dimensional lattice by tensor product.

Exercise 4.7 Show that the lattice with generator matrix

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

is cyclic.

Exercise 4.8 Prove that for m a power of 2, the cyclotomic polynomial is $\phi_m(X) = X^{m/2} + 1$.