# Quadratic forms, lattices, and ideal classes

Katherine E. Stange

March 1, 2021

## 1 Introduction

These notes are meant to be a self-contained, modern, simple and concise treatment of the very classical correspondence between quadratic forms and ideal classes. In my personal mental landscape, this correspondence is most naturally mediated by the study of complex lattices. I think taking this perspective breaks the equivalence between forms and ideal classes into discrete steps each of which is satisfyingly inevitable. These notes follow no particular treatment from the literature. But it may perhaps be more accurate to say that they follow all of them, because I am repeating a story so well-worn as to be pervasive in modern number theory, and nowdays absorbed osmotically.

These notes require a familiarity with the basic number theory of quadratic fields, including the ring of integers, ideal class group, and discriminant. I leave out some details that can easily be verified by the reader. A much fuller treatment can be found in Cox's book *Primes of the form $x^2 + ny^2$*.

## 2 Moduli of lattices

*We introduce the upper half plane and show that, under the quotient by a natural* $\mathrm{SL}(2,\mathbb{Z})$ *action, it can be interpreted as the moduli space of complex lattices.*

The upper half plane is defined as the 'upper' half of the complex plane, namely

$$\mathfrak{h} = \{x + iy : y > 0\} \subseteq \mathbb{C}.$$

If $\tau \in \mathfrak{h}$, we interpret it as a complex lattice $\Lambda_\tau := \mathbb{Z}+\tau\mathbb{Z} \subseteq \mathbb{C}$. Two complex lattices $\Lambda$ and $\Lambda'$ are said to be *homothetic* if one is obtained from the other by scaling by a complex number (geometrically, rotation and dilation). In this case we write $\Lambda \sim \Lambda'$.

If we are given a lattice $\Lambda = \alpha\mathbb{Z} + \beta\mathbb{Z}$, then up to homothety, it can be written as $\mathbb{Z} + \tau\mathbb{Z}$ for $\tau = \beta/\alpha$. By interchanging $\alpha$ and $\beta$, we can guarantee $\tau$ has positive real part. Therefore, every lattice, up to homothety, is represented by some $\tau \in \mathfrak{h}$.

However, many different $\tau$ give the same lattice. For example, $\tau$ and $\tau + 1$ clearly give the same lattice: this is essentially a change of basis. To address this, we define the natural action of $\mathrm{SL}(2,\mathbb{Z})$ on the upper half plane[1], as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}. \tag{1}$$

[1] The fact that $\mathrm{SL}(2,\mathbb{Z})$ stabilizes the upper half plane is due to the determinants being 1 and never $-1$, which would flip to the lower half plane.

Geometrically, this is the action of Möbius transformation[2]. Some important Möbius transformations include translation by 1 and inversion in the unit circle:

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \tau \mapsto \tau + 1,$$
$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \tau \mapsto -1/\tau.$$

**Proposition 1.** *$\Lambda_\tau \sim \Lambda_{\tau'}$ if and only if $\tau' = M \cdot \tau$ for some $M \in \mathrm{SL}(2, \mathbb{Z})$.*

*Proof.* The key to the proof is that $M$ implements a change of basis on the lattice, which alters $\tau$ but does not change the lattice. To see this explicitly, witness that

$$\Lambda_{M\cdot\tau} = \mathbb{Z} + \frac{a\tau + b}{c\tau + d}\mathbb{Z} \sim (c\tau + d)\mathbb{Z} + (a\tau + b)\mathbb{Z} = \mathbb{Z} + \tau\mathbb{Z}. \tag{2}$$

Conversely, if $\tau$ and $\tau'$ give the same lattice, then $\mathbb{Z} + \tau\mathbb{Z} \sim \mathbb{Z} + \tau'\mathbb{Z}$, which induces the relationship that

$$\alpha = c + d\tau, \quad \alpha\tau' = a + b\tau$$

for some $\alpha \in \mathbb{C}$. This is exactly the relationship (1). □

**We have now shown that the upper half plane, under the quotient by the action of $\mathrm{SL}(2, \mathbb{Z})$, is the moduli space of lattices up to homothety.**

A fundamental domain is given by

$$\mathcal{F} := \{z \in \mathfrak{h} : -1/2 \le |\operatorname{Re}(z)| \le 0, |z| \ge 1\} \cup \{z \in \mathfrak{h} : 0 < |\operatorname{Re}(z)| < 1/2, |z| > 1\}.$$

The fact that this is a fundamental domain, i.e. every $\mathrm{SL}(2, \mathbb{Z})$-orbit contains exactly one element of this set, is elementary, but somewhat lengthy. It appears in many books. Among those in frequent rotation for me, is Chapter 35 of Voight's *Quaternion Algebras*; another is the first chapter of Silverman's *Advanced Topics in the Arithmetic of Elliptic Curves*; there are many others.

Note that the matrix $-I$ acts trivially, so it is sometimes useful to think about the action of $\mathrm{PSL}(2, \mathbb{Z}) := \mathrm{SL}(2, \mathbb{Z})/\pm I$, which is faithful. One thing worth saying about the full story is that $\mathrm{PSL}(2, \mathbb{Z})$ is generated by the matrices $S$ and $T$ defined above. It is worth looking at the image of the fundamental domain and its images under small words in $S$ and $T$ in either of the references mentioned above.

[2] I recommend viewing the *Möbius Transformations Revealed* as an introduction to this topic more generally

## 3 Ideal Classes as $K$-Lattices

*We show that ideal classes of imaginary quadratic fields can naturally be interpreted as complex lattices up to homothety.*

I assume basic familiarity with ideal classes in the rings of integers of number fields. For the remainder of these notes, $K$ is an imaginary quadratic field.

The embeddings of $K$ into $\mathbb{C}$ can be obtained by extending scalars: $\mathbb{C} \cong \mathbb{R} \otimes_{\mathbb{Q}} K$. The metric topology induced by $\mathbb{C}$ on $K$ agrees with that of $K$ as a $\mathbb{Q}$-vector space. The salient point is that lattices of $K$ are still lattices in $\mathbb{C}$. This doesn't work for real quadratic fields or higher degree fields. We just get lucky here.

Recall that fractional ideals are, in particular, lattices in $K$. Therefore we may think of them as complex lattices generated by elements of $K$. Taking into account homothety, we arrive at the following definition.

**Definition 1.** *A complex lattice $\Lambda = \alpha\mathbb{Z} + \beta\mathbb{Z}$ is called a* $K$-lattice *if $\beta/\alpha \in K$.*

This property is insensitive to the choice of basis of the lattice, since if $\alpha' = a\alpha + b\beta$, $\beta' = c\alpha + d\beta$, then $\alpha/\beta \in K$ if and only if $\alpha'/\beta' \in K$ (i.e. the $\mathrm{SL}(2,\mathbb{Z})$ action on $\mathfrak{h}$ takes $K$ to $K$). Furthermore, being a $K$-lattice is an invariant under homothety. It is always possible to scale so that $\alpha, \beta \in K$ individually (e.g., take 1 and $\beta/\alpha$ as basis).

Finally, any $K$-lattice can be scaled to lie as a sublattice of $\mathcal{O}_K$. To see this, write $\Lambda = \alpha\mathbb{Z} + \beta\mathbb{Z}$, for $\alpha, \beta \in K$. The ideal $(\alpha, \beta)$ is a fractional ideal, and so there is some $d \in \mathcal{O}_K$ such that $d(\alpha, \beta) \subseteq \mathcal{O}_K$. Then[3] $d\Lambda \subseteq \mathcal{O}_K$.

Hence, the $K$-lattices are exactly those which arise from $\tau \in K$, under the theory of the upper half plane.

Next we wish to discuss the endomorphisms of a lattice; the collection of such is called the *order*.

**Definition 2.** *The* order *of a $K$-lattice is*

$$\mathrm{ord}(\Lambda) = \{x \in \mathbb{C} : x\Lambda \subseteq \Lambda\}.$$

The order of a lattice is clearly invariant under homothety. It is also insensitive to any choice of basis for the lattice, hence $\mathrm{ord}(\Lambda_\tau) = \mathrm{ord}(\Lambda_{M\cdot\tau})$ for $M \in \mathrm{SL}(2,\mathbb{Z})$, i.e. it is invariant under the $\mathrm{SL}(2,\mathbb{Z})$ action. So an element $\tau \in \mathfrak{h}$ can be said to have an order.

**Proposition 2.** *The order $\mathrm{ord}(\Lambda)$ is a subring of $\mathcal{O}_K$ with unity.*

*Proof.* First, $\mathrm{ord}(\Lambda) \subseteq K$, since, applying $x \in \mathrm{ord}(\Lambda_\tau)$ to the first basis element 1, we have $x \in \Lambda_\tau \subseteq \mathbb{Q}(\tau) \subseteq K$. The only difficult aspect is that $\mathrm{ord}(\Lambda) \subseteq \mathcal{O}_K$. By homothety, we may assume $\Lambda \subseteq \mathcal{O}_K$. Therefore if $x \in \mathrm{ord}(\Lambda)$, then $x^n\Lambda \subseteq \Lambda \subseteq \mathcal{O}_K$ for all positive integers $n$. Choosing $\lambda \in \Lambda$, we have $\lambda x^n \in \mathcal{O}_K$ for all $n$, which means that $\mathcal{O}_K[x]$ is a fractional ideal, hence finitely generated,

[3] Warning: $\Lambda$ need not equal $(\alpha, \beta)$ (one is a $\mathbb{Z}$-span of a basis, and the other an $\mathcal{O}_K$-span, hence there is a one-way inclusion).

implying $x$ is integral. Hence $\operatorname{ord}(\Lambda) \subseteq \mathcal{O}_K$. Finally, that it is a subring with unity is clear. □

We will focus this exposition on the case of lattices with order $\mathcal{O}_K$, but there is a rich theory when one includes other orders.

**Proposition 3.** *Fix an embedding of $K$ into $\mathbb{C}$. Under the embedding, every fractional ideal of $\mathcal{O}_K$ is a $K$-lattice with order $\mathcal{O}_K$. Furthermore, any $K$-lattice can be scaled to lie in $K$, and it has $\operatorname{ord}(\Lambda) = \mathcal{O}_K$ if and only if any such scaling is a fractional ideal of $\mathcal{O}_K$. Two $K$-lattices with order $\mathcal{O}_K$ are homothetic if and only if the corresponding fractional ideals are equivalent.*

*Proof.* A fractional ideal $I$ is naturally a $K$-lattice, and it has order $\mathcal{O}_K$ by the definition of an ideal. Conversely, consider a $K$-lattice $\Lambda$ with $\operatorname{ord}(\Lambda) = \mathcal{O}_K$. It is an $\mathcal{O}_K$-module, and finitely generated, hence a fractional ideal if scaled to lie in $K$. The ideals $I_1$ and $I_2$ are equivalent if and only if $I_1 = dI_2$ for some $d \in K$; this is exactly homothety. □

The following restatement is an immediate corollary.

**Corollary 1.** *Ideal classes of $\mathcal{O}_K$ are in bijection with $K$-lattices of order $\mathcal{O}_K$, up to homothety. The identification is obtained by considering an ideal class as a complex lattice under a fixed embedding of $K$ in $\mathbb{C}$.*

We use the notation $\operatorname{Cl}(K)$ for the ideal class group of $\mathcal{O}_K$.

Finally, we record a useful lemma for later.

**Lemma 1.** *Suppose $\tau$ is a complex root of a polynomial $ax^2 + bx + c \in \mathbb{Z}[x]$ where $\gcd(a, b, c) = 1$. Then $\operatorname{ord}(\Lambda_\tau) = \mathbb{Z}[a\tau]$.*

*Proof.* We verify that $a\tau\Lambda_\tau = \tau\mathbb{Z} + \tau^2\mathbb{Z} \subseteq \mathbb{Z} + \tau\mathbb{Z}$ because $\tau$ satisfies $a\tau^2 = -b\tau - c$. This shows $\mathbb{Z}[a\tau] \subseteq \operatorname{ord}(\Lambda_\tau)$. Conversely, suppose $\alpha = e + f\tau$ for $e, f \in \mathbb{Q}$. Then the endomorphism multiplication-by-$\alpha$ has matrix (in basis 1 and $\tau$),

$$\begin{pmatrix} e & -cf/a \\ f & e - bf/a \end{pmatrix}.$$

The condidition that $\alpha\Lambda_\tau \subseteq \Lambda_\tau$ is exactly the condition that the entries be integral. As $\gcd(a, b, c) = 1$, we find that $a \mid f$. So $\operatorname{ord}(\Lambda_\tau) \subseteq \mathbb{Z}[a\tau]$. □

# 4 Quadratic forms as $K$-Lattices

*In this section, we interpret primitive integral binary quadratic forms of fundamental discriminant $\Delta$ up to proper equivalence as $\mathbb{Q}(\Delta)$-lattices up to homothety.*

**Definition 3.** *An* integral binary quadratic form *is an expression $ax^2+bxy+cy^2$ in $\mathbb{Z}[x, y]$. The* discriminant *of the form is $\Delta = b^2 - 4ac$. If $\Delta < 0$, the form is* definite. *It is called* primitive *if $\gcd(a, b, c) = 1$.*

It is a fact of the theory of quadratic forms that definite forms take only values of a single sign. This is a consequence of the fact that, over $\mathbb{R}$, any binary quadratic form can be diagonalized[4]; the discriminant is negative if and only if the diagonalization is $x^2+y^2$ or $-x^2-y^2$. If the former, we call it *positive definite* (otherwise, predictably, *negative definite*).

One of the fundamental questions number theory seeks to answer is: What are the values taken by (*represented by*) a quadratic form? It is natural to consider quadratic forms up to change of variables, which shouldn't change the set of values a form represents. To this end, we define an action of $\mathrm{SL}(2, \mathbb{Z})$.

**Definition 4.** *Let $M \in \mathrm{SL}(2, \mathbb{Z})$. Then, $M$ acts on vectors in $\mathbb{Z}^2$. Writing $\mathbf{v} = (x, y)$ for the vector of indeterminates, considered a column vector, a quadratic form $f(x, y)$ can be given an action by $M$:*

$$M \cdot f(\mathbf{v}) = f(M \cdot \mathbf{v}).$$

*Two integral binary definite quadratic forms $f(x, y)$ and $g(x, y)$ are* properly equivalent *if they are in the same orbit. In that case we write $f \sim g$.*

Explicitly, this is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(x, y) = f(ax + by, cx + dy).$$

The action of $\mathrm{SL}(2, \mathbb{Z})$ doesn't change the discriminant of the form (this is simply a computation). Therefore we may define the *form class group* $\mathrm{Cl}(\Delta)$ to be the set of proper equivalence classes of primitive integral binary quadratic forms of discriminant $\Delta$.

Quadratic forms also give rise to complex lattices, although the association is slightly less obvious. A quadratic form $f(x, y) = ax^2 + bxy + cy^2$ has an associated polynomial $ax^2 + bx + c$ (by setting $y = 1$). If $\Delta < 0$, it has an associated pair of non-real complex conjugate roots $\tau_f, \overline{\tau_f}$, namely

$$\frac{-b \pm \sqrt{\Delta}}{2a}. \tag{3}$$

Let us assign these in such a way that $\tau_f \in \mathfrak{h}$. Note that the minimal polynomial of $\tau_f$ has discriminant $\Delta$, which implies $\mathbb{Z}[\tau_f]$ has discriminant $\Delta$.

**Proposition 4.** *Let $\Delta$ be a negative integer[5]. There is an $\mathrm{SL}(2, \mathbb{Z})$-equivariant bijection between primitive integral binary quadratic forms $f$ of discriminant $\Delta$ and quadratic irrationalities $\tau_f$ of discriminant $\Delta$. The equivariance is given by $\tau_{M \cdot f} = M^{-1}(\tau_f)$.*

*Proof.* We have seen how to associate to $f$ an element $\tau_f$ in the upper half plane which is a root of $f(x, 1)$. To invert this, one takes the minimal polynomial of

[4] Here I mean the Gram matrix.

[5] If $\Delta \equiv 2, 3 \pmod 4$, this bijection is vacuous.

$\tau_f$ (which is quadratic) and homogenizes to reintroduce the variable $y$. There's a small hitch here: any scaling of the quadratic form (i.e. $\lambda f$ in place of $f$) will produce the same $\tau_f$. So one must choose the *primitive* form amongst the scalar multiples.

We must also show that the action of $\mathrm{SL}(2,\mathbb{Z})$ on integral binary positive definite quadratic forms $f$ is equivariant with the inverse action of $\mathrm{SL}(2,\mathbb{Z})$ on the root $\tau_f$, explicitly, $\tau_{M\cdot f} = M^{-1}(\tau_f)$. This is a computation, so we omit the proof, but, for example, $\tau_{a(x-1)^2+b(x-1)+c} = \tau_{ax^2+bx+c} + 1$. □

Before we state the corollary giving a bijection between forms and lattices, we pause because we prefer to restrict our attention to $K$-lattices of the *maximal order* $\mathcal{O}_K$. The following definition will be useful for characterizing discriminants associated to the maximal order.

**Definition 5.** *A discriminant $\Delta$ is* fundamental *if it is of the form $\Delta = 4m$ for $m \equiv 2$ or $3 \pmod 4$ and squarefree, of the form $\Delta = m$ for $m \equiv 1 \pmod 4$ squarefree.*

It is a fact that these correspond (except for $\Delta = 1$) bijectively to quadratic number fields, as the discriminants of their rings of integers. (Non-fundamental non-square discriminants give other orders[6], i.e. full-rank subrings of $\mathcal{O}_K$ with unity.)

Now we can state the corollary.

**Corollary 2.** *Let $\Delta$ be a negative fundamental discriminant associated to quadratic imaginary field $K$. There is a bijection between proper equivalence classes of integral binary quadratic forms of discriminant $\Delta$ and homothety classes of $K$-lattices of order $\mathcal{O}_K$.*

*Proof.* From Proposition 4, there's a bijection between such forms and $\tau_f$ being quadratic of discriminant $\Delta$ in the upper half plane, taken modulo $\mathrm{SL}(2,\mathbb{Z})$.

Once we have associated $\tau_f$ to $f$, one also has an associated $K$-lattice

$$\Lambda_f := \Lambda_{\tau_f}.$$

This lattice has order $\mathbb{Z}[a\tau_f]$ (by Lemma 1), which has discriminant[7] $\Delta$. Therefore, since $\Delta$ is fundamental, it is a $K$-lattice of order $\mathcal{O}_K$.

Conversely, any $K$-lattice $\Lambda$ of order $\mathcal{O}_K$ is, up to homothety, of the form $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ where $\tau \in K$. Therefore $\tau$ is quadratic, and we have just seen that the discriminant of $\tau$ matches the discriminant of its order. If $\Lambda = \Lambda_{\tau_f}$ then $\tau_f \sim \tau$ and so this is a bijection. □

[6] These are also all the orders obtained from lattices as in Definition 2.

[7] In general, the discriminant of a power basis is the discriminant of the minimal polynomial. Hence the discriminants of a general polynomial $f$ of degree $n$ and of the power basis of its root $\tau$ are related by $\mathrm{disc}(f) = a^n \,\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$.

## 5 Quadratic forms and ideal classes

We now state the full bijection. We let $K$ be an imaginary quadratic field with discriminant $\Delta_K$.

**Theorem 1.** *We have bijections*

$$\mathrm{Cl}(K) \quad \leftrightarrow \quad \{K\text{-lattices of order } \mathcal{O}_K\}/\sim \quad \leftrightarrow \quad \mathrm{Cl}(\Delta_K)$$

*given by (left to right),*

$$\mathfrak{a} \mapsto \Lambda_{\mathfrak{a}} = \alpha\mathbb{Z} + \beta\mathbb{Z} \mapsto N(\alpha x - \beta y)/N(\mathfrak{a}). \tag{4}$$

*and by (right to left),*

$$ax^2 + bxy + cy^2 \mapsto \Lambda_f = \mathbb{Z} + \frac{-b+\sqrt{\Delta}}{2a}\mathbb{Z} \mapsto \left(a, \frac{-b+\sqrt{\Delta}}{2}\right) \tag{5}$$

*Proof.* The bijection is given by Corollaries 1 and 2, wherein we find the explicit maps. Tracing through these, it is easy to see the explicit map in the right-to-left direction, namely (5).

For the inverse, we pass from a $K$-lattice $\Lambda_{\mathfrak{a}} = \alpha\mathbb{Z} + \beta\mathbb{Z}$ representing an integral ideal $\mathfrak{a}$, to the corresponding quadratic form, which should arise from the minimal polynomial for $\beta/\alpha$. One slick way to obtain this minimal polynomial is to recover it as the characteristic polynomial of endomorphism $x \mapsto (\beta/\alpha)x$ on $K$, i.e. $\det(Ix - m_\beta m_\alpha^{-1}) = N(\alpha x - \beta y)/N(\alpha)$.

Thus the inverse map should be

$$\mathfrak{a} \mapsto \Lambda_{\mathfrak{a}} = \alpha\mathbb{Z} + \beta\mathbb{Z} \mapsto \kappa N(\alpha x - \beta y), \tag{6}$$

where $\kappa$ needs to be specified.

To set $\kappa$ and verify that we obtain an inverse, we use a nice choice of lattice homothety. Assume $\beta/\alpha$ satisfies the polynomial $ax^2 + bx + c \in \mathbb{Z}[x]$ with $\gcd(a,b,c) = 1$. Then,

$$\alpha\mathbb{Z} + \beta\mathbb{Z} \sim a\mathbb{Z} + \frac{-b+\sqrt{\Delta}}{2}\mathbb{Z}.$$

The rightmost coefficient, call it $\gamma$, is an algebraic integer generating $\mathcal{O}_K$ (it has minimal polynomial $x^2 + bx + \frac{b^2-\Delta}{4}$ of discriminant $\Delta$), and this lattice has covolume $a$ inside $\mathcal{O}_K = \mathbb{Z} + \gamma\mathbb{Z}$.

We compute

$$\begin{aligned} &N\left(ax - \frac{-b+\sqrt{\Delta}}{2}y\right) N\left(\left(a, \frac{-b+\sqrt{\Delta}}{2}\right)\right)^{-1} \\ &= \left(a^2x^2 + abxy + \frac{b^2-\Delta}{4}y^2\right)a^{-1} \\ &= ax^2 + bxy + cy^2. \end{aligned}$$

Hence, the correct scaling is more canonically given as

$$\frac{N(\alpha x - \beta y)}{N(\mathfrak{a})},$$

which is clearly invariant under homothety.

Thus the inverse to (5) is therefore (4). □

## 6 Finiteness of the class group

We now briefly indicate a few payoffs. Given a quadratic form $f$, we can apply the action of $\mathrm{SL}(2, \mathbb{Z})$ to place $\tau_f$ in the fundamental domain. This gives a *reduction theory*, i.e. an algorithm that replaces $f$ with a canonical representative of its equivalence class. Working this out explicitly, we obtain

**Proposition 5.** *Let $f(x, y) = ax^2 + bxy + cy^2$. Then $\tau_f \in \mathcal{F}$ if and only if $|b| \leq a \leq c$ with $b \geq 0$ whenever $|b| = a$ or $a = c$.*

Such a form is called *reduced*. In particular, this implies that for fixed discriminant $\Delta = b^2 - 4ac$, there are only finitely many reduced forms (to see this, note that $|\Delta| \geq 3a^2$ and so there are finitely many choices for $a$ and $b$; but any such choice determines at most one $c$).

We write $\mathrm{Cl}(\Delta)$ for the set of equivalence classes of quadratic forms of discriminant $\Delta$. We have just shown that $|\,\mathrm{Cl}(\Delta)| < \infty$. Via the bijection, this immediately implies $|\,\mathrm{Cl}(K)| < \infty$.

## 7 Composition of Quadratic Forms

Since the class group comes with a group operation, so must the set of equivalence classes of quadratic forms, inherited through this bijection. The composition of quadratic forms was actually observed long ago, before class groups. An example of this sort of thing is the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

which is essentially the multiplicativity of the Gaussian norm, but which we can now interpret as the identity $(1)(1) = (1)$ in the class group of $\mathbb{Z}[i]$. A general composition law that lines up with this story can be found in Cox's book *Primes of the form $x^2 + ny^2$*. Or you can derive it yourself from the bijection above.