Minkowski's geometry of numbers


Lattices

Let $V$ be a real vector space of dimension $n$. By a lattice $L$ in $V$ we mean a discrete, additive subgroup. We say that $L$ is a full lattice if it spans $V$. Of course, any lattice is a full lattice in the subspace it spans.

The lattice $L$ is discrete in the induced topology, meaning that for any point $x \in L$ there is an open subset $U$ of $V$ whose intersection with $L$ is just $x$. For the subgroup $L$ to be discrete it is sufficient that this holds for the origin, i.e., that there is an open neighbourhood $U$ about $0$ with $U \cap L = \{0\}$. Indeed, if $x \in L$, then the translate $U' = U + x$ is open and intersects $L$ in the set $\{x\}$.

A often useful property of a lattice is that it has only finitely many points in any bounded subset of $V$. To see this, let $S \subseteq V$ be a bounded set and assume that $L \cap S$ is infinite. One may then pick a sequence $\{x_n\}$ of different elements from $L \cap S$ and assume that $(S \cap L \cap S')$ is infinite. One may then pick a sequence $\{x_n\}$ of different elements from $L \cap S$. Since $S$ is bounded, its closure is compact and $\{x_n\}$ has a subsequence that converges, say to $x$. Then $x$ is an accumulation point in $L$; every neighbourhood contains elements from $L$ distinct from $x$.

The lattice associated to a basis

If $B = \{v_1, \ldots, v_n\}$ is any basis for $V$, one may consider the subgroup $L_B = \sum_i \mathbb{Z}v_i$ of $V$ consisting of all linear combinations of the $v_i$'s with integral coefficients. Clearly $L_B$ is a discrete subspace of $V$; if one takes $U$ to be an open ball centered at the origin and having radius less than $\min_i \|v_i\|$, then $U \cap L = \{0\}$. Hence $L_B$ is a full lattice in $V$.

If might very well happen that another basis $B'$ generates the same lattice as $B$. If this occurs, the vectors $v'_i$ of $B'$ lies in $L$ and they can be expressed as linear combinations $v'_i = \sum_i a_i v_i$ with coefficients in $\mathbb{Z}$, and symmetrically, the vectors from $B$ are integral linear combinations of those from $B'$. Thus the transition matrix $(a_{ij})$ must lie in $\text{Gl}(n, \mathbb{Z})$, and we observe that its determinant equals $\pm 1$.

It might also happen that the lattice generated by $B'$ is contained, but not necessarily equal to $L_B$. Then the transition matrix $(a_{ij})$ still has integral coefficients, but the determinant is an integer different from $\pm 1$. The quotient group $L_B/L_{B'}$ is a finite group whose order equals $|\det(a_{ij})|$. This number is also called the index of $L_B$ in $L_{B'}$ and written $[L_B : L_{B'}]$.

The fundamental domain There is a particular subset of $V$ associated to the lattice $L_B$. It is the subset $T \subseteq V$ of real linear combinations of the $v_i$'s whose coefficients are
confined to the interval $[0, 1 >$, that is

$$T = \{ \sum_{i} a_i v_i \mid 0 \leq a_i < 1 \}.$$  

This set is called the \textit{the fundamental domain of $L_B$}. It depends on the basis $B$, so a lattice has many fundamental domain, one for each basis.

Assume now that $V$ comes equipped with a \textit{metric}, that is a scalar product. We can then speak about metric properties of subsets in $V$, like length, area and volume, etc. The etc stands for the the \textit{n-dimensional volume}—or just \textit{volume} or \textit{measure} for short—and we denote by $\mu(S)$ the measure of a subset $S$ (since it is in fact the Lebesgue measure). The sets we shall meet are extremely nice from a measure-theoretical point of view, so there is never a question about they being measurable.

Assume that $\mathcal{E}$ is an orthonormal basis. Any other basis $B$ may of course be expressed in terms of $\mathcal{E}$ by means of the transition matrix $M$. A fundamental property of the measure on $V$, is that the volume of the fundamental domain $T$ of the lattice $L_B$ is equal to the absolute value of the determinant of $M$, that is

$$\mu(T) = |\det M|.$$  

The translates of $T + v$ of the fundamental domain by elements $v \in L_B$ are disjoint and their union equals the whole of $V$, so they form a \textit{covering} of $V$. This is not an open covering since $T$ is not open (neither close for that matter), a part of the border is contained in $T$ and a part is not. To see that the translate are disjoint, assume that

$$\sum_{i} a_i v_i = \sum_{i} a'_i v_i + \sum_{i} n_i v_i,$$

with $a_i, a'_i \in [0, 1 >$. Then $n_i = a_i - a'_i \in <-1, 1 >$. So if the $n_i$’s in addition are integers, they must all be zero. That the translates cover $V$, follows since

$$\sum a_i v_i = \sum i < a_i > v_i + \sum [a_i] v_i = t + v,$$

where $< t >$ (resp. $[t]$) denotes the fractional (resp integral value) of a number $t$.

\textbf{Every lattice has a basis}

In fact, the previous collection $L_B$ of examples of lattices is exhaustive—any full lattice is of the type described there:

\textbf{Proposition 1} Let $L$ be a full lattice in the real vector space $V$. Then there is a basis $B$ for $V$ such that $L = L_B$.

\textbf{Proof:} Since $L$ spans $V$, we may find a basis $C$ for $V$ contained in $L$. Let $L_0 = L_C$ be the lattice spanned by $C$.  

— 2 —
The main point of the proof, is that $L_0$ is of finite index in $L$. Indeed, let $T$ be the fundamental domain of $L_0$. Now, $L \cap T$ is a finite set since $L$ is discrete and $T$ bounded. Any $x \in L$ is of the form $x = t + v$ with $v \in L_0$ and $t \in T$, and therefore $t = x - v$ is among the finitely many elements in $T \cap L$, and $x$ is congruent modulo $L_0$ to one of the elements in $T \cap L$.

The index $m = [L : L_0]$ kills the quotient $L/L_0$ and therefore $mL \subseteq L_0$, or $L \subseteq \frac{1}{m}L_0$ if one wants. But $\frac{1}{m}L_0$ has the basis $\{\frac{1}{m}v_i\}$ and is hence a finitely generated free abelian group. By a standard result about such groups, it follows that $L$ is finitely generated and free, and thus has a basis.

**Blichfeldt-Minkowski theory**

There is a whole industry producing results about the number of lattice points of a given lattice $L$ in $V$ lying in a given bounded set $S$. One may, for example, ask for the asymptotic behavior of the cardinality of $S \cap L$ as a function of $r$ (where $s = \{rx \mid x \in S\}$). This question goes back to Gauss and his circle problem, in which $n = 2$ and $S$ is the unit circle. We take a slightly different point of view in this paragraph, merely asking for the intersection $S \cap L$ to be non empty—or more precisely having a non-zero element.

We present a lemma, usually contributed to Hans Frederik Blichfeldt. He was an danish-american mathematician, born in the small village Iller close to Viborg on Jutland, whose parents emigrated to America in 1888. And we present what usually is called Minkowski’s theorem, a result due to the much more known Königsberg- and Göttingen-mathematician Hermann Minkowski.

**Blichfeldt’s lemma** We work with at full lattice $L$ in the real vector space $V$ which is equipped with a metric, i.e., an inner product—you may have $\mathbb{R}^n$ with the standard inner product in mind. We choose a basis $v_1, \ldots, v_n$ for $L$ and let $T$ denote the corresponding fundamental domain. It is an absolutely obvious observation that if $S \subseteq V$ is a bounded subset and $S \subseteq T$, then $\mu(S) \leq \mu(T)$. Elaborating this, we obtain the following slightly more subtle statement, known as Blichfeldt’s lemma:

**Lemma 1** Assume that $L \subseteq V$ is a full lattice and that $S \subseteq V$ is a bounded set. If $\mu(S) > \mu(T)$, then there are two different elements $x, y \in S$ such that $x - y \in L$.

**Proof:** For any $v \in L$ let $S_v = S \cap (T + v)$, that is, the part of the translate $T + v$ lying with in $S$. As the different translates $T - v$ form a disjoint covering of $V$ as $v$ runs through the lattice $L$, one has $S = \bigcup_{v \in L} S \cap (T + v)$.

Moving the set $S \cap (T + v)$ back into $T$ we get the set

$$S_v = S \cap (T + v) - v = \{ t \in T \mid t + v \in S \}.$$ 

Two such sets share a common element $t$ if and only if $x = t + v$ and $y = t + w$ both lie in $S$. Clearly their difference lies in $L$, so this is what we are aiming for.
Assume then that the $S_v$’s are disjoint, and let $S' = \bigcup_{v \in L} S_v$. Then

$$\mu(S') = \sum \mu(S_v) = \sum \mu(S \cap (T + v)) = \mu(S) > \mu(T),$$

contradicting the fact that $S' \subseteq S$.

For those acquainted with the world of manifolds and the general machinery of volume elements, there is a shorter way (which may be also reveals the mystery; once the machinery is in place, it is just the stupid statement we stated with) to present this proof: The quotient map $V \to V/L$ is a local isometry, and the interior $T$ is isometric to an open dense subset of $V/L$, hence $\mu(V/L) = \mu(T)$. But if $\mu(S) > \mu(T)$, the set $S$ can not map injectively into $V/L$, hence two of its members differ by an element in $L$.

For those who enjoy illustration, we have made a picture illustrating the first way of presenting the proof—the others can show it to their kids. The set $S$ is the yellow square to the left. The four triangles to the right are the different intersection of $S$ with the translates of $T$, moved back to $T$. The quotient $V/L$ is a torus. The quotient the map $T \to V/L$ identifies the four corners of $T$, the parallel parts of the border are pairwise identified, and the four triangles are reunited to the yellow square.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{minkowski_diagram.png}
\caption{Illustration of Minkowski’s theorem.}
\end{figure}

**Minkowski’s theorem** The point of this theorem is to give conditions on the subset $S \subseteq V$ to ensure that $S$ contains a non-zero lattice point. The conditions come in two flavors; a regularity condition on the geometry of $S$ and a metric condition on $S$. The set can not be too wild, and it must be of a certain size.

Recall that a set $S$ is said to be **convex** if the line segment between any two of its points is contained in $S$. It is said to be **central symmetric** if invariant under the inversion map $x \mapsto -x$ of $V$, i.e., if $x \in S$, then $-x \in S$.

**Theorem 1** Let $L \subseteq V$ be a full lattice in the $n$-dimensional vector space $V$ equipped with a metric, and let $S \subseteq V$ be a subset. Assume that $S$ satisfies the following two conditions

- $S$ is convex and central symmetric,
- $\mu(S) > 2^n \mu(L)$.

Then there is a non-zero lattice point contained in $S$.
Proof: The idea of the proof is to apply Blichfeldt’s lemma to the scaled set $\frac{1}{2}S$. As $\mu(\frac{1}{2}S) = 2^{-n}\mu(S)$, the metric condition on $S$ is exactly what is needed to get the condition $\mu(\frac{1}{2}S) > \mu(L)$ in Blichfeldt’s lemma. One concludes that there are two different points $x, y \in S$ such that $x/2 - y/2 \in L$. But $S$ being central symmetric, it follows that $-y \in S$, and $S$ being convex, the convex combination $x/2 - y/2$ lies in $S$. Thus we see that $x/2 - y/2 \in S \cap L$.

Lattices and number fields

The reason we are interested in lattices is of course that they play a fundamental role in the theory of numbers. So, given a number field $K$ of degree $n$ with ring of integers $A$, the question is: Can one associate a lattice $L_A$ to $A$? The additive group structure of $A$ is as requested of a lattice, namely it is a finitely generated free abelian group, that is $A \cong \mathbb{Z}^n$, but the remaining substantial part of the question is: How do we embedded it into a real vector space? And what space?

To get inspired, we start with two examples, both of quadratic fields:

An imaginary quadratic field The first example is an easy case. We look at the field of the Eisenstein numbers $K = \mathbb{Q}(\sqrt{-3})$. As $-3 \equiv 1 \mod 4$, the discriminant $\Delta$ equals $-3$, and the ring of integers is $A = \mathbb{Z}\left[(1 + \sqrt{-3})/2\right]$. The ring $A$ is already contained in $\mathbb{C}$, so $A$ is born as a lattice. This lattice is generated by any $\mathbb{Z}$-basis for $A$, for example by $1, (1 + \sqrt{-3})/2$. We depicted it in the figure below, where the fundamental parallelogram is coloured red. We remark that the area of $L_A$ is $\sqrt{3}/2$, which equals $\sqrt{|\Delta|}/2$.

A real quadratic field The case of real quadratic fields is more subtle. The ring $A$ of integers in such a field is not born as a lattice. Being contained in the one dimensional object $\mathbb{R}$, and basically being a two dimensional object itself, it must show some accumulation behavior. And in fact, $A$ dense in $\mathbb{R}$. 

The lattice corresponding to the Eisenstein numbers $\mathbb{Z}[\sqrt{-3}]$
We take a closer look at the example $\mathbb{Q}(\sqrt{3})$. The discriminant is 12, and the ring of integers is $A = \mathbb{Z}[\sqrt{3}]$. The field has two real embeddings differing by the sign of the square root, and using those, we can realize $A$ as a lattice $L_A$ in $\mathbb{R}^2$ by using the map $\Sigma: \mathbb{Q}(\sqrt{3}) \to \mathbb{R}^2$ defined as

$$\Sigma(x + y\sqrt{3}) = (x + y\sqrt{3}, x - y\sqrt{3}),$$

that is, the coordinates of $\Sigma(\alpha)$ are the values the two embeddings take on $\alpha$. Clearly the image of $A$ is the lattice $L_A$ generated by the vectors $(1, 1)$ and $(\sqrt{3}, -\sqrt{3})$. It is illustrated below. The red area is the fundamental domain. Its measure is $2\sqrt{3}$, which we observe equals $\sqrt{\Delta}$.

**Problem 1.** Show that for any $\alpha \in \mathbb{Q}(\sqrt{3})$ there is an $a \in \mathbb{Z}[\sqrt{3}]$ such that $|\alpha - a| < 2\sqrt{2}$. Show that $u = 2 - \sqrt{3}$ is a unit in $\mathbb{Z}[\sqrt{3}]$ and that $u_n = u^n$ is a sequence of units converging to 0. Show that $\mathbb{Z}[\sqrt{3}]$ is dense in $\mathbb{R}$. **HINT:** Find $a_n$ such that $|\alpha u_n^{-1} - a_n| < 2\sqrt{2}$.

**Problem 2.** Define and draw the lattice $L_A$ when $A$ is the ring of integer in $\mathbb{Q}(\sqrt{5})$.

**The lattice associated to a number field**

We proceed to attack the general situation when $K$ is any number field of degree $n$. It has $n$ embeddings in $\mathbb{C}$, and some of these are real and some complex. The complex ones come in complex conjugate pairs. Let us say that there are $r$ real embeddings and $2s$ complex ones. Then $n = r + 2s$.

It is customary to list the embeddings in a particular way. The real embeddings are listed in any order $\sigma_1, \ldots, \sigma_r$. When it comes to the complex ones, we choose...
one embedding from each pair of complex conjugate ones, and list these in any order: \( \sigma_{r+1}, \ldots, \sigma_{r+s} \). Then the total list of embeddings appears as

\[
\sigma, \ldots, \sigma_r, \sigma_{r+1}, \overline{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma}_{r+s}
\]

(\star)

These choices give us the map \( \sigma: K \rightarrow \mathbb{R}^r \times \mathbb{C}^s \) by sending \( \alpha \) to \( (\sigma_i(\alpha)) \). This is injective e.g., by Artins theorem on independence of characters. As usual, \( \mathbb{C} \simeq \mathbb{R}^2 \) via \( z \mapsto (\text{Re } z, \text{Im } z) \), and composing this with \( \sigma \) we get the map

\[
\Sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \text{Re } \sigma_{r+1}(\alpha), \text{Im } \sigma_{r+1}(\alpha), \ldots, \text{Re } \sigma_{r+s}(\alpha), \text{Im } \sigma_{r+s}(\alpha))
\]

which is an embedding of \( K \) into \( \mathbb{R}^r \times \mathbb{R}^{2s} = \mathbb{R}^n \).

Any \( \mathbb{Z} \)-basis for \( A \) is a \( \mathbb{Q} \)-basis for \( K \), hence a \( \mathbb{R} \)-basis for \( \mathbb{R}^n \), and the image \( L_A = \Sigma(A) \) is therefore a full lattice in \( \mathbb{R}^n \). More generally, let \( a \subseteq K \) be a fractional ideal. It is a free abelian group of rank \( n \) and has a \( \mathbb{Z} \)-basis which is a \( \mathbb{Q} \)-basis for \( K \). Hence the image \( L_a = \Sigma(a) \) also is a lattice in \( \mathbb{R}^n \).

**The volume of the lattice \( L_A \)** One of the most important invariants of a lattice is the volume, so after having defined the lattice \( L_A \), the first question that arises: Express the volume of \( L_A \) in terms of invariants of \( K \). The answer is

**Proposition 2** Let \( K \) be a number field with \( s \) complex embeddings and let \( A \) denote the ring of integers. The volume of the lattice \( L_A \) associated to \( A \) is given by

\[
\mu(L_A) = 2^{-s}\sqrt{|\Delta_K|}
\]

**PROOF:** We work with a \( \mathbb{Z} \)-basis \( A = \{\alpha_1, \ldots, \alpha_n\} \) of \( A \). The volume of \( L_A \) that we want to compute, is given as the determinant of the matrix \( C = (\Sigma(\alpha_1), \ldots, \Sigma(\alpha_n)) \) whose columns are the vectors \( \Sigma(\alpha_i) \).

The proof hangs on two points. The first, and deepest, is the formula for the discriminant we proved in \( xxx \)

\[
\Delta_K = \det(\sigma_j(\alpha_j))^2
\]

where \( \sigma_i \)'s are all the embeddings of \( K \) in \( \mathbb{C} \) listed in the manner of (\star) above (so for a moment we break with the convention adopted above). For later reference, we let \( D = (\sigma_j(\alpha_i)) \).

The second point, is a general formula from linear algebra, relating the two matrices \( C \) and \( D \). It is easy to prove, but to formulate it is somehow messy and takes some space, so prefer to treat it apart. It states that \( C = ED \) where \( E \) is an almost diagonal matrix. it has \( r \) diagonal entries equal to 1, and then \( s \) diagonal blocks, each block being equal to the \( 2 \times 2 \) matrix

\[
\begin{pmatrix}
1/2 & 1/2i
\end{pmatrix}
\]

Taking determinants, we obtain

\[
\det C = (-\frac{1}{2i})^{-s} \det D
\]

which in turn gives the proposition.
The volume of the lattice $L_\alpha$ Assume that $\alpha$ is an ideal in $A$. It has a $\mathbb{Z}$-basis, say $B = \{\beta_1, \ldots, \beta_n\}$, and each of the $\beta_i$’s may be expresses as $\beta_i = \sum_j m_{ij} \alpha_j$ with integral coefficients $m_{ij} \in \mathbb{Z}$. The transition matrix $M = (m_{ij})$ is just the matrix of the inclusion map relative to the basis $B$ and $A$. We have the commutative diagram

$$
\begin{array}{ccc}
\mathbb{Z}^n & \xrightarrow{\phi_M} & \mathbb{Z}_n \\
\downarrow & & \downarrow \\
\alpha & \rightarrow & A
\end{array}
$$

where the vertical maps are given by the coordinates in the two basises $A$ and $B$ respectively, and the map $\phi_M$ is just multiplication by $M$. The two horizontal maps have the same cokernel, and therefore by $\text{xxx}$, it holds that the counting norm of $\alpha$ satisfies $\mathcal{N}(\alpha) = \# A/\alpha = |\det M|$.

Relating this to the embedding $\Sigma$ of $K$ in $\mathbb{R}^n$, we see that in the image $\Sigma(\beta_i)$ of the basis vector $\beta_i$ is the vector $M \cdot (\Sigma(\alpha_i))$. Hence it follows that $\det(\Sigma(\beta_i)) = \det M \det(\Sigma(\alpha_i))$, and we have proven the following proposition, at least in the case of an integral ideal:

**Proposition 3** If $\alpha$ is a fractional ideal, we have

$$
\mu(L_\alpha) = \mathcal{N}(\alpha) 2^{-s} \sqrt{|\Delta|_K}.
$$

If the ideal $\alpha$ is really fractional, that is, if $A \subseteq \alpha$, one proceeds in a similar way. The difference being, that if $M$ is the transition matrix between a $\mathbb{Z}$-basis $B$ of $\alpha$ and the basis $A$ of $A$, then $(\Sigma(\beta_i)) = M^{-1}(\Sigma(\alpha_i))$. On the other hand, $\mathcal{N}(\alpha) = |\det M|^{-1}$ in this case, so the result holds.

### The Minkowski bound

We are now in the position to formulate and prove the main theorem of this section. It is an application of Minkowski’s theorem to the lattices $L_\alpha$ associated to fractional ideals $\alpha$, with the set $S$ chosen in an appropriate way.

One of the sets $S$ we shall use is the following. It depends on a positive real parameter $t$:

$$
S_t = \{ (t_1, \ldots, t_r, z_1, \ldots, z_s) \mid \sum_{1 \leq i \leq r} |t_i| + 2 \sum_{1 \leq i \leq s} |z_i| < t \}.
$$

This is a subset of $\mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^n$, and we prefer using a mix of real and complex coordinates. Recall that for a point $\Sigma(\alpha)$ in the image of $K$, the coordinates are the values $\sigma_i(\alpha)$ the $r+s$ the chosen embeddings $\sigma_i$ take at $\alpha$. Due to the fact that $|z| = |\Sigma|$ and the occurrence of the factor 2, the sum in the definition of $S_t$ evaluates to $\sum_\sigma \sigma(\alpha)$ at $\Sigma(\alpha)$ where the sum is over all embeddings $\sigma$ (and that is of course precisely the reason for that factor 2).

One finds the volume of $S_t$ by an easy but tiresome and not very instructive exercise in multiple integration. The result is
Lemma 2

\[ \mu(S_t) = \frac{2^{r-s} \pi^s t^n}{n!}. \]

We are free to choose the parameter \( t \), and we do this in the manner that \( \mu(S_t) > 2^n \mu(L_a) \), which means

\[ \frac{2^{r-s} \pi^s t^n}{n!} > 2^n \mathcal{N}(a) 2^{-s} \sqrt{|\Delta|_K} \]

or

\[ t^n = \frac{4^n n!}{\pi^s} \mathcal{N}(a) 2^{-s} \sqrt{|\Delta|_K} - \epsilon \]

for some positive \( \epsilon \). Minkowski’s theorem tells us then that there is a non-zero element \( a \in \mathfrak{a} \) lying in \( S_t \), that is, the element \( a \) satisfies

\[ \sum_{\sigma} |\sigma(a)| < t \]

where the sum is over all embeddings of \( K \). The last ingredient in the proof is the classical relation between the geometric and the arithmetical mean. For any positive numbers \( b_1, \ldots, b_m \) there is an inequality

\[ \left( \prod_i b_i \right)^{1/n} \leq \left( \sum_i b_i \right)/n. \]

Substituting the \( |\sigma(a)| \)'s for the \( b_i \)'s one obtains

\[ \mathcal{N}(a) = \prod_{\sigma} \sigma(a) < \left( \sum_{\sigma} \sigma(a) \right)^n/n^n < t^n/n^n = \frac{4^n n!}{\pi^s} \mathcal{N}(a) \sqrt{|\Delta|_K} - \epsilon/n^n, \]

and letting \( \epsilon \) tend to zero, we show the following theorem:

**Theorem 2** Let \( K \) be a number field and let \( \mathfrak{a} \) be a non-zero fractional ideal in \( K \). Then there is a non-zero element \( a \in \mathfrak{a} \) such that

\[ \mathcal{N}(a) \leq \frac{4^n n!}{\pi^s} \mathcal{N}(a) \sqrt{|\Delta|_K}. \]

**Application to the class group**

One of the main applications of Minkowski’s theorem in algebraic number theory is to the study of the class group (another important application is Dirichlet’s unit theorem which we shall come back to later). It follows from the theorem that any class \( \mathcal{C} \) in the class group, contains an ideal whose norm is bounded by a constant—called the Minkowski bound—that only depends on the field. And it is easily accessible. This reduces the study of the class group to study of a finite number of prime ideal.
**Theorem 3** Let \( C \) be any class in the class group \( C_A \). Then there is an integral ideal \( a \) in \( A \) such that

\[
\frac{4^n n!}{n^n \pi^n} \sqrt{|\Delta_K|} \leq a
\]

**Proof:** Let \( b \in C \) and apply theorem 2 above to the fractional ideal \( b^{-1} \), to get an element \( b \in b^{-1} \) such that

\[
N(b) \leq \frac{4^n n!}{n^n \pi^n} N(b^{-1}) \sqrt{|\Delta_K|}.
\]

Let \( a = bb \). Then \( a \subseteq A \) (since \( b \in b^{-1} \)), and since \( N(ab) = N(a)N(b) \) and \( N(b^{-1}) = N(b)^{-1} \), we get from ( \( \ast \) ) that

\[
N(a) = N(b)N(b) \leq \frac{4^n n!}{n^n \pi^n} \sqrt{|\Delta_K|}.
\]

There are some immediate and important consequences to be drawn. The first one is that the class group of a number field is finite. In general this is not true for Dedekind rings—rings of functions on most complex Riemann surfaces for example, have class groups with cardinality of the continuum—so this is a specific result for number fields. The Minkowski’s theorem tells us that any class may be represented by an ideal of bounded norm, so what is missing is that the number of ideals with bounded norm is finite, that is the following lemma:

**Lemma 3** Given a constant \( M \). The number of ideals in \( A \) with \( N(a) \leq M \) is finite.

**Proof:** First of all, the number of prime ideals in \( A \) lying over a given rational prime \( p \) is bounded by the degree \( n \) of \( K \)—for example, this follows from the fundamental relation \( N = \sum e_i f_i \)—and since \( p|N(p) \), if \( p \) lies over \( p \), we see that there are only finitely many possibilities for \( p \), and hence finitely many prime ideals whose norm is bounded by \( M \). If \( a = \prod p_i^{e_i} \), the \( p_i \)'s must be among the primes with norm bounded by \( M \), and clearly the \( e_i \)'s are also bounded, e.g., \( e_i \leq \log M/\log N(p_i) \).

We have proven

**Theorem 4** Let \( K \) be a number field whose ring of integer is \( A \). Then the class group \( C_A \) is finite.

**Ramification over \( \mathbb{Q} \)** Since the norm of any ideal is a positive integer, the inequality in theorem 3 above gives a lower bound on the discriminant \( \Delta_K \) of a number field. Solving for the discriminant, we get\(^1\)

\[
\sqrt{|\Delta_K|} > \frac{n^n \pi^n}{n!} \frac{4^n}{n^n 4^s} \geq 1
\]

\(^1\)Use induction on \( n \) and that \( \frac{(n+1)^n}{n^n} = \exp(n(\log(n + 1) - \log n)) \) is an increasing function, e.g., since the derivative of \( x(\log(x+1) - \log x) \) is on the form \( 1/(x+C) - 1/(x+1) \) for a \( C \) with \( 0 < C < 1 \).
and we conclude that \( \Delta_K \neq \pm 1 \). Hence the following theorem which is contributed to Minkowski:

**Theorem 5** If \( K \) is a number field different from \( \mathbb{Q} \), then the discriminant \( \Delta_K \) is not equal to \( \pm 1 \), i.e., \( K \) is not unramified over \( \mathbb{Q} \).

Of course extensions of other fields than \( \mathbb{Q} \) can very well be unramified. A nice and simple example is the biquadratic field \( K = \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \) which is unramified over \( \mathbb{Q}(\sqrt{-15}) \). The fields fit onto the diagram

\[
\begin{array}{ccc}
\mathbb{Q}(\sqrt{-3}) & \mathbb{Q}(\sqrt{-15}) & \mathbb{Q}(\sqrt{5}) \\
\mathbb{Q}(\sqrt{-3}, \sqrt{5})
\end{array}
\]

where the discriminants are indicated. The three numbers involved are all congruent 1 mod 4, so the discriminants of the three quadratic extensions of \( \mathbb{Q} \) are \(-3, -5 \) and \(-15 \). The moral of the example is that all the ramification is picked up in \( \mathbb{Q}(\sqrt{-15}) \).

Outside \( 3 \) and \( 5 \) all the three quadratic fields are unramified, so the same applies to \( \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \) over \( \mathbb{Q}(-15) \).

We shall check that \( \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \) is unramified at \( 3 \) over \( \mathbb{Q}(-15) \) (leaving the completely analogous case of \( 5 \) to the reader), and we shall do that by decomposing \( 3 \) in \( \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \) in two ways, one passing by \( \mathbb{Q}(\sqrt{-3}) \) and one by \( \mathbb{Q}(\sqrt{-15}) \).

In \( \mathbb{Q}(\sqrt{-3}) \) the prime \( 3 \) decomposes as \( (3) = p^2 \) for some prime \( p \). As the discriminant of \( \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \) over \( \mathbb{Q}(\sqrt{-3}) \) is 5 we see that \( \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \) is unramified over \( \mathbb{Q}(\sqrt{-3}) \) at \( p \), and there are two different primes \( p = \mathfrak{p}_1 \mathfrak{p}_2 \) lying over \( p \); the decomposition of \( 3 \) in \( \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \) then being \( (3) = \mathfrak{p}_1^2 \mathfrak{p}_2^2 \).

Now we analyze the decomposition of \( 3 \) by going via \( \mathbb{Q}(\sqrt{-15}) \). There \( 3 \) decomposes as \( (3) = q^2 \) (the discriminant is \(-15 \)). But then \( q \) can not ramify in \( \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \), since if it did, we would have \( q = \mathfrak{Q}^2 \) for a prime \( \mathfrak{Q} \) in \( \mathbb{Q}(\sqrt{-3}, \sqrt{5}) \), and therefore \( (3) = \mathfrak{Q}^4 \). This contradicts that \( (3) = \mathfrak{p}_1^2 \mathfrak{p}_2^2 \) with \( \mathfrak{p}_1 \) and \( \mathfrak{p}_2 \) distinct primes.

**Problem 3.** Generalize this example to the situation of \( \mathbb{Q}(\sqrt{a}, \sqrt{b}) \) where \( a \) and \( b \) are two relatively prime numbers, both congruent 1 modulo 4. Discuss the general case when \( a \) and \( b \) just are different numbers.

**The class number of some quadratic fields**

The virtue of the Minkowski theorem, is that any class is represented by an ideal, \( \mathfrak{a} \) say, of norm less than the Minkowski bound. And this ideal is a product of prime ideals of norm less than \( N(\mathfrak{a}) \). Hence to control the class group, it sufficient to understand the prime ideals lying over the primes \( p \) less then the Minkowski bound. Those prime ideals which are principal do not contribute to the class group, those that are not do.
In the quadratic case, if \( p \) remains prime, the only prime ideal lying over \( p \) is generated by \( p \) and does not contribute. In case \( p \) splits or is ramified, one has to do the work it is to decide whether the ideals in the decomposition are principal or not.

For a quadratic field \( K \) the Minkowski bound \( M \) becomes simple, and is given as

\[
M = \begin{cases} 
\frac{1}{2} \sqrt{|\Delta|} & \text{if } K \text{ is real} \\
\frac{2}{\pi} \sqrt{|\Delta|} & \text{if } K \text{ is complex}
\end{cases}
\]

**The nine imaginary quadratic fields with class number one** We start with checking the famous list of the nine imaginary quadratic fields with class number one, that is \( \mathbb{Q}(\sqrt{-d}) \) for \( d = 2, 3, 7, 11, 19, 43, 67 \) and 163. That is, we shall see that all these nine fields have class number one, and then for among fields with a relatively small discriminant, \( |\Delta| < 523 \), see that they are the only ones. The result that they are only among all imaginary quadratic fields is deep, and has a long and twisted history, starting with Gauss.

First one observation. Assume that \( p \) is a rational prime, with \( p = 2, 3, 5 \) and \( 7 \) are of current interest. If \( p \neq 2 \), the quadratic status of \(-d\) modulo \( p \) determines if \( p \) splits or not, that is \( x^2 + d \) is irreducible in \( \mathbb{F}_p[x] \) is and only if \(-d\) is not a square mod \( p \). If \( p = 2 \), one has to check the status of \( x^2 + x + m \), which is irreducible modulo 2 precisely when \( m \) is odd. Now, we are done since the only non-zero square mod 3 is 1. And, in terms of lowest residues, there are two modulo 5, namely 1 and \(-1\), and modulo 7 the three non-zero squares are 1, \(-3\) and 3.
We proceed to see that for $d < 400$, the other fields than the nine have class number greater than one. By the observation above, 2 cannot ramify, so $d = -1 \mod 4$.

If $4p < d$, we know that $p$ must be inert. So if $d \geq 20$, we can take $p = 2, 3$ and 5. For $p = 2$. Then $d = -1 \mod 4$ since 2 does not ramify and since $(1 + d)/4 = 1 \mod 8$. We have that $-d$ is not a square neither mod 3 nor mod 5, so $d = 1 \mod 3$ and $d = \pm 2 \mod 5$. To summarize, we have the three simultaneous congruences

\[
\begin{align*}
    d &= 3 \mod 8 \\
    d &= 1 \mod 3 \\
    d &= \pm 2 \mod 5
\end{align*}
\]

and solving them, we see that $d = 43 \mod 120$ or $d = 67 \mod 120$. So 43, 67, 163, 187, 283, 307, are the only solution less than 400, and the three last are not primes. Of course, one could continue this sequence of numbers, but as Dirichlet showed us, every congruence class has an infinite number of primes in it, so—helas—sooner or later a prime looms (523 being the first one).

A QUADRATIC FIELD WITH CLASS GROUP $\mathbb{Z}/4\mathbb{Z}$ We take a look at $\mathbb{Q}(\sqrt{-14})$. The discriminant is $\Delta = -4 \cdot 14$, and the Minkowski bound $M = 2/\pi \sqrt{14} = 4.7640$. Hence we have to examine the two primes 2 and 3. The prime 2 ramifies, and $(2) = p^2$ with $p = (2, \sqrt{-14})$. If we put $b = [p]$, then $b^2 = 1$ in the class group, and $b$ is non trivial.

The prime 3 splits, and $(3) = qq'$ where $q = (3, \sqrt{-14} - 1)$ and $q' = (3, \sqrt{-14} + 1)$. Non of these primes are principal, since norms of integral non-units are at least 14. It we put $a = [q]$, then $a^{-1} = [q']$.

The element $\alpha = 2 + \sqrt{-14}$ has norm 18 and is obviously contained in $p$ and $q$, and it is not in $q'$. Hence one has the decomposition $(\alpha) = pq^2$. It follows that $b = a^2$, and we are done.

THE CLASS NUMBER OF SOME REAL FIELDS We do some real examples:

- $\mathbb{Q}(\sqrt{6})$ has class number one.

In this case $\Delta = 2^3 \cdot 3$, and the Minkowski bound is $\sqrt{6} = 2.44949$, and all classes are represented by ideals of norm less than two, that is ideals lying over 2. As 2 ramifies, $(2, \sqrt{6})$ is the only such ideal, and as $2 + \sqrt{6}$ is of norm $-2$, it generates $(2, \sqrt{6})$.

- $\mathbb{Q}(\sqrt{7})$ has class number one.
The discriminant of \( \mathbb{Q}(\sqrt{7}) \) is \( \Delta = 2^2 \cdot 7 \), so \( \frac{1}{2} \sqrt{\Delta} = \sqrt{7} < 2.7 \), so classes are represented by the ideals of norm at most two, that is those lying over 2. As \( \Delta = 4 \cdot 7 \), the prime 2 ramifies there is only one lying over it, namely \( (2, \sqrt{7} + 1) \). One checks that the element \( \alpha = 3 + \sqrt{7} \) is of norm 2, hence \( \alpha \) is a prime element lying in \( (2, \sqrt{7} + 1) \), and it follows that \( (2, \sqrt{7} + 1) = (3 + \sqrt{7}) \). Hence \( \mathbb{Q}(\sqrt{7}) \) has class number one.

\( \Box \) \( \mathbb{Q}(\sqrt{10}) \) has class group \( \mathbb{Z}/2\mathbb{Z} \).

The discriminant is \( \Delta = 4 \cdot 20 \), so the Minkowski bound is \( \sqrt{10} = 3.16 \). The ideals to examine are therefore those lying over 2 and 3.

We have \((2) = (2, \sqrt{10})\), and \((2, \sqrt{10})\) is not principal. This follows since there are no elements of norm \( \pm 2 \), if \( \alpha = x + y\sqrt{10} \) was one, one would have \( \pm 2 = x^2 - 10y^2 \), but the only squares mod 5 are \( \pm 1 \) and 0. Now, \((3) = (3, \sqrt{10} + 1)(3, \sqrt{10} - 1) \). Now the element \( \alpha = 2 + \sqrt{10} \) is of norm \(-6 \), and hence \((2 + \sqrt{10}) = (2, \sqrt{10})(3, \sqrt{10} - 1) \) and \((2 - \sqrt{10}) = (2, \sqrt{10})(3, \sqrt{10} + 1) \). Hence all the three ideals are in the same class which is non-trivial, and the class number is two.

\( \Box \) \( \mathbb{Q}(\sqrt{11}) \) has class number one.

Then \( \Delta = 4 \cdot 11 \) and the Minkowski bound is \( \sqrt{11} = 3.31662 \), and classes are represented by ideals lying over 2 or 3. As \( x^2 - 11 \equiv x^2 + 1 \mod 3 \), and \(-1\) is not a square in \( \mathbb{F}_3 \) we see that 3 remains prime in \( \mathbb{Q}(\sqrt{11}) \) and generates the only prime ideal lying over 3.

Over 2 there is the ideal \((2, \sqrt{11} + 1)\) whose square is (2). Now \( 3 + \sqrt{11} \) has norm \(-2 \), and hence generates \((2, \sqrt{11} + 1)\). The class number is 1.

**Problem 4**. Determine the class groups of the following fields: \( \mathbb{Q}(79), \mathbb{Q}(82), \mathbb{Q}(-30) \) and \( \mathbb{Q}(-65) \) HINT: The answers are \( \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \) and \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \). *

**A formula from linear algebra**

We start with \( n = 2 \) case. One easily verifies the identity

\[
\begin{pmatrix}
    z_1 & \overline{z}_1 \\
    z_2 & \overline{z}_2
\end{pmatrix}
\begin{pmatrix}
    1/2 & 1/2i \\
    1/2 & -1/2i
\end{pmatrix}
= \begin{pmatrix}
    \text{Re } z_1 & \text{Im } z_1 \\
    \text{Re } z_2 & \text{Im } z_2
\end{pmatrix}
\]

In general, let there be given complex numbers \( z_{ij} \) with \( 1 \leq i \leq 2s \) and \( 1 \leq j \leq s \). Put \( w_{ij} = z_{i,j/2} \) if \( j \) is even and \( z_{i,(j-1)/2} \) if \( j \) is odd, and let the matrix \( D \) be given by \( D = (w_{ij}) \). That is

\[
D = \begin{pmatrix}
    \cdots & z_{1j} & \overline{z}_{1j} & \cdots \\
    z_{2j} & \overline{z}_{2j} & \cdots \\
    \vdots & \cdots & \cdots \\
    z_{2s,j} & \overline{z}_{2s,j}
\end{pmatrix}
\]

In our context, the matrix \( D \) corresponds to \( (\sigma_j \alpha_i) \) On the other hand let \( y_{ij} = \text{Re } z_{i,j/2} \)
if \( j \) is even and \( y_{ij} = \text{Im} \, z_{i,(j-1)/2} \) if \( j \) is odd. Let \( C \) be the matrix \( C = (y_{ij}) \), that is
\[
C = \begin{pmatrix}
\cdots & \text{Re} \, z_{1j} & \text{Im} \, z_{1j} & \cdots \\
\text{Re} \, z_{2j} & \text{Im} \, z_{2j} & \cdots \\
\vdots & \vdots & \ddots & \vdots \\
\text{Re} \, z_{2s,j} & \text{Im} \, z_{2s,j} & \cdots & \text{Re} \, z_{2s,j}
\end{pmatrix}.
\]

The relation xxx above generalizes to \( C = ED \) where \( E \) is the \( 2s \times 2s \)-matrix having \( s \) blocks along the diagonal each being a copy of the matrix
\[
\begin{pmatrix}
1/2 & 1/2i \\
1/2 & -1/2i
\end{pmatrix}
\]. Hence we get
\[
\det C = (-1/2i)^s \det D
\].