Another Application of Minkowski’s Theorem

We will continue with the notation already set previously.

Recall that we proved Minkowski’s Theorem on Friday:

**Theorem (Minkowski’s First Convex Bodies Theorem)**

If $C$ is a convex body in $\mathbb{R}^n$ and $\Lambda$ is a full lattice in $\mathbb{R}^n$, then there is a non-zero lattice point $z \in C \cap \Lambda$ if

$$\text{Vol}(C) \geq 2^n \det(\Lambda).$$

**Theorem (1)**

Let $A$ be a non-zero fractional ideal of $K$. Then $\rho'(A)$ is a lattice in $\mathbb{R}^n$ with

$$\det(\rho'(A)) = N(A)^2 - r^2 \sqrt{|D_K|}.$$
Another Application of Minkowski’s Theorem

We will continue with the notation already set previously.
We will continue with the notation already set previously. Recall that we proved Minkowski’s Theorem on Friday:
We will continue with the notation already set previously. Recall that we proved Minkowski’s Theorem on Friday:

**Theorem (Minkowski’s First Convex Bodies Theorem)**

If $C$ is a convex body in $\mathbb{R}^n$ and $\Lambda$ is a full lattice in $\mathbb{R}^n$, then there is a non-zero lattice point $z \in C \cap \Lambda$ if $\text{Vol}(C) \geq 2^n \det(\Lambda)$. 

**Theorem (1)**

Let $A$ be a non-zero fractional ideal of $K$. Then $\rho'(A)$ is a lattice in $\mathbb{R}^n$ with $\det(\rho'(A)) = N(A)^2 - r^2 \sqrt{|D_K|}$. 

Math 681, Monday, February 8
Another Application of Minkowski’s Theorem

We will continue with the notation already set previously. Recall that we proved Minkowski’s Theorem on Friday:

**Theorem (Minkowski’s First Convex Bodies Theorem)**

*If $C$ is a convex body in $\mathbb{R}^n$ and $\Lambda$ is a full lattice in $\mathbb{R}^n$,

then there is a non-zero lattice point $z \in C \cap \Lambda$ if $\text{Vol}(C) \geq 2^n \det(\Lambda)$.*

**Theorem (1)**

Let $A$ be a non-zero fractional ideal of $K$. Then $\rho'(A)$ is a lattice in $\mathbb{R}^n$ with $\det(\rho'(A)) = N(A)^2 - r^2 \sqrt{|D_K|}$. 


Another Application of Minkowski’s Theorem

We will continue with the notation already set previously. Recall that we proved Minkowski’s Theorem on Friday:

**Theorem (Minkowski’s First Convex Bodies Theorem)**

*If $C$ is a convex body in $\mathbb{R}^n$ and $\Lambda$ is a full lattice in $\mathbb{R}^n$, then there is a non-zero lattice point $z \in C \cap \Lambda$.*
Another Application of Minkowski’s Theorem

We will continue with the notation already set previously. Recall that we proved Minkowski’s Theorem on Friday:

**Theorem (Minkowski’s First Convex Bodies Theorem)**

If $C$ is a convex body in $\mathbb{R}^n$ and $\Lambda$ is a full lattice in $\mathbb{R}^n$, then there is a non-zero lattice point $z \in C \cap \Lambda$ if

$$\text{Vol}(C) \geq 2^n \det(\Lambda).$$
We will continue with the notation already set previously. Recall that we proved Minkowski’s Theorem on Friday:

**Theorem (Minkowski’s First Convex Bodies Theorem)**

If $C$ is a convex body in $\mathbb{R}^n$ and $\Lambda$ is a full lattice in $\mathbb{R}^n$, then there is a non-zero lattice point $z \in C \cap \Lambda$ if

$$\text{Vol}(C) \geq 2^n \det(\Lambda).$$

**Theorem (1)**
Another Application of Minkowski’s Theorem

We will continue with the notation already set previously. Recall that we proved Minkowski’s Theorem on Friday:

**Theorem (Minkowski’s First Convex Bodies Theorem)**

If $C$ is a convex body in $\mathbb{R}^n$ and $\Lambda$ is a full lattice in $\mathbb{R}^n$, then there is a non-zero lattice point $z \in C \cap \Lambda$ if

$$\text{Vol}(C) \geq 2^n \det(\Lambda).$$

**Theorem (1)**

Let $\mathcal{A}$ be a non-zero fractional ideal of $K$. Then $\rho'(\mathcal{A})$ is a lattice in $\mathbb{R}^n$ with

$$\det(\rho'(\mathcal{A})) = N(\mathcal{A})2^{-r_2} \sqrt{|D_K|}.$$
Proof:

This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that
\[
\det(\rho(A)) = N(A) \sqrt{|D_K|}.
\]
Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.

Let \( f: \mathbb{R}^n \rightarrow \mathbb{R} \) be defined by
\[
f(x) = |x_1| + \cdots + |x_r_1| + 2 \sqrt{x_{r_1}^2} + x_{r_1+1} + \cdots + 2 \sqrt{x_{r_1+r_2}^2} + x_{r_1+r_2+1} + \cdots,
\]
where \( x = (x_1, \ldots, x_n) \).

Let \( C \subset \mathbb{R}^n \) be the set of \( x \) with \( f(x) \leq 1 \).

Lemma (1): The set \( C \) is a convex body.
Proof: This is almost exercise #1 from the fourth homework assignment;
**Proof:** This is almost exercise \#1 from the fourth homework assignment; the difference is that there you (essentially) prove that

\[
\det (\rho(\mathcal{A})) = N(\mathcal{A}) \sqrt{|D_K|}.
\]
Proof: This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that

\[ \det (\rho(\mathfrak{A})) = N(\mathfrak{A}) \sqrt{|D_K|}. \]

Theorem 1 follows via elementary row operations on the resulting bases for the lattices,
**Proof:** This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that

\[ \det(\rho(A)) = N(A) \sqrt{|D_K|}. \]

Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.
Proof: This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that
\[ \det (\rho(A)) = N(A) \sqrt{|D_K|}. \]

Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.

Let \( f : \mathbb{R}^n \to \mathbb{R} \) be defined by
Proof: This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that
\[ \det (\rho(\mathcal{A})) = N(\mathcal{A}) \sqrt{|D_K|}. \]

Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.

Let \( f : \mathbb{R}^n \to \mathbb{R} \) be defined by
\[
f(x) = |x_1| + \cdots + |x_{r_1}|
+ 2 \sqrt{x_{r_1+1}^2 + x_{r_1+r_2+1}^2 + \cdots + 2 \sqrt{x_{r_1+r_2}^2 + x_{r_1+2r_2}^2}},
\]
Proof: This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that

\[ \det (\rho(\mathcal{A})) = N(\mathcal{A}) \sqrt{|D_K|}. \]

Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.

Let \( f : \mathbb{R}^n \to \mathbb{R} \) be defined by

\[
f(x) = |x_1| + \cdots + |x_{r_1}| \]

\[
+ 2 \sqrt{x_{r_1+1}^2 + x_{r_1+r_2+1}^2 + \cdots + 2 \sqrt{x_{r_1+r_2}^2 + x_{r_1+2r_2}^2},}
\]

where \( x = (x_1, \ldots, x_n) \).
Proof: This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that

$$\det (\rho(\mathcal{A})) = N(\mathcal{A}) \sqrt{|D_K|}.$$ 

Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.

Let $f : \mathbb{R}^n \to \mathbb{R}$ be defined by

$$f(x) = |x_1| + \cdots + |x_{r_1}|$$

$$+ 2 \sqrt{x_{r_1+1}^2 + x_{r_1+r_2+1}^2 + \cdots + 2 \sqrt{x_{r_1+r_2}^2 + x_{r_1+2r_2}^2}},$$

where $x = (x_1, \ldots, x_n)$.

Let $C \subset \mathbb{R}^n$ be the set of $x$ with $f(x) \leq 1$. 
**Proof:** This is almost exercise \#1 from the fourth homework assignment; the difference is that there you (essentially) prove that

\[
\det (\rho(\mathfrak{A})) = N(\mathfrak{A}) \sqrt{|D_K|}.
\]

Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.

Let \( f : \mathbb{R}^{n} \to \mathbb{R} \) be defined by

\[
f(x) = |x_1| + \cdots + |x_{r_1}|
+ 2 \sqrt{x_{r_1+1}^2 + x_{r_1+r_2+1}^2} + \cdots + 2 \sqrt{x_{r_1+2r_2}^2 + x_{r_1+2r_2}^2},
\]

where \( x = (x_1, \ldots, x_n) \).

Let \( C \subset \mathbb{R}^n \) be the set of \( x \) with \( f(x) \leq 1 \).

**Lemma (1)**
**Proof:** This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that

$$\det (\rho(\mathcal{A})) = N(\mathcal{A}) \sqrt{|D_K|}.$$ 

Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.

Let \( f : \mathbb{R}^n \to \mathbb{R} \) be defined by

$$f(x) = |x_1| + \cdots + |x_{r_1}| + 2 \sqrt{x_{r_1+1}^2 + x_{r_1+r_2+1}^2 + \cdots + 2 \sqrt{x_{r_1+r_2}^2 + x_{r_1+2r_2}^2}},$$

where \( x = (x_1, \ldots, x_n) \).

Let \( C \subset \mathbb{R}^n \) be the set of \( x \) with \( f(x) \leq 1 \).

**Lemma (1)**

*The set \( C \) is a convex body.*
Proof:

One can show without much difficulty that
\[ f(x + y) \leq f(x) + f(y) \]
for all \( x, y \in \mathbb{R}^n \).

Since \( f \) is clearly continuous at the origin, we see that it is continuous everywhere and the set \( C \) is compact.

It is also clear that \( f(t x) = |t| f(x) \) for all \( t \in \mathbb{R} \) and \( x \in \mathbb{R}^n \).

The case \( t = -1 \) shows that \( C \) is symmetric about the origin.

Since
\[ f(tx + (1-t)y) \leq t f(x) + (1-t) f(y) \]
for all \( t \in \mathbb{R} \) and \( x, y \in \mathbb{R}^n \), \( C \) is convex.

Obviously the origin is an interior point of \( C \), so \( C \) is a convex body.

Lemma (2)

The volume of \( C \) is
\[ 2r_1 - r_2 \pi r_2^n ! \]
Proof: One can show without much difficulty that $f(x + y) \leq f(x) + f(y)$ for all $x, y \in \mathbb{R}^n$. 
Proof: One can show without much difficulty that \( f(x + y) \leq f(x) + f(y) \) for all \( x, y \in \mathbb{R}^n \). Since \( f \) is clearly continuous at the origin,
**Proof:** One can show without much difficulty that $f(x + y) \leq f(x) + f(y)$ for all $x, y \in \mathbb{R}^n$. Since $f$ is clearly continuous at the origin, we see that it is continuous everywhere and the set $C$ is compact.
Proof: One can show without much difficulty that $f(x + y) \leq f(x) + f(y)$ for all $x, y \in \mathbb{R}^n$. Since $f$ is clearly continuous at the origin, we see that it is continuous everywhere and the set $C$ is compact.

It is also clear that $f(tx) = |t|f(x)$ for all $t \in \mathbb{R}$ and $x \in \mathbb{R}^n$. 
Proof: One can show without much difficulty that \( f(x + y) \leq f(x) + f(y) \) for all \( x, y \in \mathbb{R}^n \). Since \( f \) is clearly continuous at the origin, we see that it is continuous everywhere and the set \( C \) is compact.

It is also clear that \( f(tx) = |t|f(x) \) for all \( t \in \mathbb{R} \) and \( x \in \mathbb{R}^n \). The case \( t = -1 \) shows that \( C \) is symmetric about the origin.
Proof: One can show without much difficulty that $f(x + y) \leq f(x) + f(y)$ for all $x, y \in \mathbb{R}^n$. Since $f$ is clearly continuous at the origin, we see that it is continuous everywhere and the set $C$ is compact.

It is also clear that $f(tx) = |t|f(x)$ for all $t \in \mathbb{R}$ and $x \in \mathbb{R}^n$. The case $t = -1$ shows that $C$ is symmetric about the origin.

Since

$$f(tx + (1 - t)y) \leq f(tx) + f((1 - t)y) = |t|f(x) + |1 - t|f(y)$$

for all $t \in \mathbb{R}$ and $x, y \in \mathbb{R}^n$, 

Lemma (2) The volume of $C$ is $2r_1 - r_2 \pi r_2^n$. 

Math 681, Monday, February 8
Proof: One can show without much difficulty that $f(x + y) \leq f(x) + f(y)$ for all $x, y \in \mathbb{R}^n$. Since $f$ is clearly continuous at the origin, we see that it is continuous everywhere and the set $C$ is compact.

It is also clear that $f(tx) = |t|f(x)$ for all $t \in \mathbb{R}$ and $x \in \mathbb{R}^n$. The case $t = -1$ shows that $C$ is symmetric about the origin.

Since

$$f(tx + (1 - t)y) \leq f(tx) + f((1 - t)y) = |t|f(x) + |1 - t|f(y)$$

for all $t \in \mathbb{R}$ and $x, y \in \mathbb{R}^n$, $C$ is convex.
Proof: One can show without much difficulty that $f(x + y) \leq f(x) + f(y)$ for all $x, y \in \mathbb{R}^n$. Since $f$ is clearly continuous at the origin, we see that it is continuous everywhere and the set $C$ is compact.

It is also clear that $f(tx) = |t|f(x)$ for all $t \in \mathbb{R}$ and $x \in \mathbb{R}^n$. The case $t = -1$ shows that $C$ is symmetric about the origin.

Since

$$f(tx + (1 - t)y) \leq f(tx) + f((1 - t)y) = |t|f(x) + |1 - t|f(y)$$

for all $t \in \mathbb{R}$ and $x, y \in \mathbb{R}^n$, $C$ is convex.

Obviously the origin is an interior point of $C$,
Proof: One can show without much difficulty that $f(x + y) \leq f(x) + f(y)$ for all $x, y \in \mathbb{R}^n$. Since $f$ is clearly continuous at the origin, we see that it is continuous everywhere and the set $C$ is compact.

It is also clear that $f(tx) = |t|f(x)$ for all $t \in \mathbb{R}$ and $x \in \mathbb{R}^n$. The case $t = -1$ shows that $C$ is symmetric about the origin.

Since

$$f(tx + (1 - t)y) \leq f(tx) + f((1 - t)y) = |t|f(x) + |1 - t|f(y)$$

for all $t \in \mathbb{R}$ and $x, y \in \mathbb{R}^n$, $C$ is convex.

Obviously the origin is an interior point of $C$, so $C$ is a convex body.
Proof: One can show without much difficulty that \( f(x + y) \leq f(x) + f(y) \) for all \( x, y \in \mathbb{R}^n \). Since \( f \) is clearly continuous at the origin, we see that it is continuous everywhere and the set \( C \) is compact.

It is also clear that \( f(tx) = \lvert t \rvert f(x) \) for all \( t \in \mathbb{R} \) and \( x \in \mathbb{R}^n \). The case \( t = -1 \) shows that \( C \) is symmetric about the origin.

Since

\[
f(tx + (1 - t)y) \leq f(tx) + f((1 - t)y) = \lvert t \rvert f(x) + \lvert 1 - t \rvert f(y)
\]

for all \( t \in \mathbb{R} \) and \( x, y \in \mathbb{R}^n \), \( C \) is convex.

Obviously the origin is an interior point of \( C \), so \( C \) is a convex body.

Lemma (2)
**Proof:** One can show without much difficulty that $f(x + y) \leq f(x) + f(y)$ for all $x, y \in \mathbb{R}^n$. Since $f$ is clearly continuous at the origin, we see that it is continuous everywhere and the set $C$ is compact.

It is also clear that $f(tx) = |t|f(x)$ for all $t \in \mathbb{R}$ and $x \in \mathbb{R}^n$. The case $t = -1$ shows that $C$ is symmetric about the origin.

Since

$$f(tx + (1 - t)y) \leq f(tx) + f((1 - t)y) = |t|f(x) + |1 - t|f(y)$$

for all $t \in \mathbb{R}$ and $x, y \in \mathbb{R}^n$, $C$ is convex.

Obviously the origin is an interior point of $C$, so $C$ is a convex body.

**Lemma (2)**

The volume of $C$ is $\frac{2(1-r_2)\pi r_2^n}{n!}$. 

Proof:

First let \( w_i = |x_i| \) for \( 1 \leq i \leq r_1 \) and convert to polar coordinates for the remaining subscripts:

\[
\begin{align*}
  x_i &= w_i \cos \theta_i \\
  x_i + r_2 &= w_i \sin \theta_i
\end{align*}
\]

for \( r_1 + 1 \leq i \leq r_1 + r_2 \), with \( w_i \geq 0 \) and \( 0 \leq \theta_i \leq 2\pi \).

The volume of \( C \) is equal to

\[
2r_1 (2\pi) r_2 \int \cdots \int_{D_1} \prod_{i=1}^{r_1} w_i - 1 \, dw_i,
\]

where \( D_1 \) is defined by \( w_i \geq 0 \) and \( \sum_{r_1 + r_2} = 1 \).

Letting \( z_i = e^{i w_i} \), one sees that the volume of \( C \) is equal to

\[
2r_1 - r_2 \pi r_2 \int \cdots \int_{D_2} \prod_{i=1}^{r_1} z_i e^{i - 1} \, dz_i,
\]

where \( D_2 \) is defined by \( z_i \geq 0 \) for all \( 1 \leq i \leq r_1 + r_2 \) and \( z_1 + \cdots + z_{r_1 + r_2} \leq 1 \).
Proof: First let $w_i = |x_i|$ for $1 \leq i \leq r_1$
Proof: First let \( w_i = |x_i| \) for \( 1 \leq i \leq r_1 \) and convert to polar coordinates for the remaining subscripts:
Proof: First let $w_i = |x_i|$ for $1 \leq i \leq r_1$ and convert to polar coordinates for the remaining subscripts: $x_i = w_i \cos \theta_i$ and $x_{i+r_2} = w_i \sin \theta_i$ for $r_1 + 1 \leq i \leq r_1 + r_2$. 
Proof: First let $w_i = |x_i|$ for $1 \leq i \leq r_1$ and convert to polar coordinates for the remaining subscripts: $x_i = w_i \cos \theta_i$ and $x_{i+r_2} = w_i \sin \theta_i$ for $r_1 + 1 \leq i \leq r_1 + r_2$, with $w_i \geq 0$ and $0 \leq \theta_i \leq 2\pi$. 
Proof: First let \( w_i = |x_i| \) for \( 1 \leq i \leq r_1 \) and convert to polar coordinates for the remaining subscripts: \( x_i = w_i \cos \theta_i \) and \( x_{i+r_2} = w_i \sin \theta_i \) for \( r_1 + 1 \leq i \leq r_1 + r_2 \), with \( w_i \geq 0 \) and \( 0 \leq \theta_i \leq 2\pi \).

The volume of \( C \) is equal to

\[
2^{r_1}(2\pi)^{r_2} \int \cdots \int_{D_1} \prod_{i=1}^{r_1+r_2} w_i^{e_i-1} \, dw_i,
\]
Proof: First let \( w_i = |x_i| \) for \( 1 \leq i \leq r_1 \) and convert to polar coordinates for the remaining subscripts: \( x_i = w_i \cos \theta_i \) and \( x_{i+r_2} = w_i \sin \theta_i \) for \( r_1 + 1 \leq i \leq r_1 + r_2 \), with \( w_i \geq 0 \) and \( 0 \leq \theta_i \leq 2\pi \).

The volume of \( C \) is equal to

\[
2^{r_1}(2\pi)^{r_2} \int \cdots \int_{D_1} \prod_{i=1}^{r_1+r_2} w_i^{e_i-1} \, dw_i,
\]

where \( D_1 \) is the region defined by \( w_i \geq 0 \) and \( \sum_{i=1}^{r_1+r_2} e_i w_i \leq 1 \).
Proof: First let $w_i = |x_i|$ for $1 \leq i \leq r_1$ and convert to polar coordinates for the remaining subscripts: $x_i = w_i \cos \theta_i$ and $x_{i+r_2} = w_i \sin \theta_i$ for $r_1 + 1 \leq i \leq r_1 + r_2$, with $w_i \geq 0$ and $0 \leq \theta_i \leq 2\pi$.

The volume of $C$ is equal to

$$2^{r_1} (2\pi)^{r_2} \int \cdots \int_{D_1} \prod_{i=1}^{r_1+r_2} w_i^{e_i-1} dw_i,$$

where $D_1$ is the region defined by $w_i \geq 0$ and $\sum_{i=1}^{r_1+r_2} e_i w_i \leq 1$.

Letting $z_i = e_i w_i$,
Proof: First let \( w_i = |x_i| \) for \( 1 \leq i \leq r_1 \) and convert to polar coordinates for the remaining subscripts: \( x_i = w_i \cos \theta_i \) and \( x_{i+r_2} = w_i \sin \theta_i \) for \( r_1 + 1 \leq i \leq r_1 + r_2 \), with \( w_i \geq 0 \) and \( 0 \leq \theta_i \leq 2\pi \).

The volume of \( C \) is equal to

\[
2^{r_1} (2\pi)^{r_2} \int \cdots \int_{D_1} \prod_{i=1}^{r_1+r_2} w_i^{e_i-1} \, dw_i,
\]

where \( D_1 \) is the region defined by \( w_i \geq 0 \) and \( \sum_{i=1}^{r_1+r_2} e_i w_i \leq 1 \).

Letting \( z_i = e_i w_i \), one sees that the volume of \( C \) is equal to

\[
2^{r_1-r_2} \pi^{r_2} \int \cdots \int_{D_2} \prod_{i=1}^{r_1+r_2} z_i^{e_i-1} \, dz_i,
\]
Proof: First let $w_i = |x_i|$ for $1 \leq i \leq r_1$ and convert to polar coordinates for the remaining subscripts: $x_i = w_i \cos \theta_i$ and $x_{i+r_2} = w_i \sin \theta_i$ for $r_1 + 1 \leq i \leq r_1 + r_2$, with $w_i \geq 0$ and $0 \leq \theta_i \leq 2\pi$.

The volume of $C$ is equal to

$$2^{r_1}(2\pi)^{r_2} \int \cdots \int_{D_1} \prod_{i=1}^{r_1+r_2} w_i^{e_i-1} \, dw_i,$$

where $D_1$ is the region defined by $w_i \geq 0$ and $\sum_{i=1}^{r_1+r_2} e_i w_i \leq 1$.

Letting $z_i = e_i w_i$, one sees that the volume of $C$ is equal to

$$2^{r_1-r_2}(2\pi)^{r_2} \int \cdots \int_{D_2} \prod_{i=1}^{r_1+r_2} z_i^{e_i-1} \, dz_i,$$

where $D_2$ is defined by $z_i \geq 0$ for all $1 \leq i \leq r_1 + r_2$ and $z_1 + \cdots + z_{r_1+r_2} \leq 1$. 

For $B \geq 0$ let

$$V(r_1, r_2, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r_1+r_2} y_i^{e_i-1} dy_i,$$

where the domain of integration $D_3$ is given by $y_i \geq 0$ for all $i$ and $y_1 + \cdots + y_{r_1+r_2} \leq B$.

We will use induction on $r_1 + r_2$ to show that $V(r_1, r_2, B) = B^{r_1+2r_2} (r_1 + 2r_2)!$.

Note that the case $B = 1$ will complete the proof of the lemma.

First set $r_1 + r_2 = 1$. Here we have two cases:

$V(1, 0, B) = \int_0^B 1 \, dy = B$

$V(0, 1, B) = \int_0^B y \, dy = B^2/2$.
For $B \geq 0$ let

$$V(r_1, r_2, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r_1+r_2} y_i^{e_i-1} dy_i,$$

where the domain of integration $D_3$ is given by $y_i \geq 0$ for all $i$ and $y_1 + \cdots + y_{r_1+r_2} \leq B.$
For $B \geq 0$ let

$$V(r_1, r_2, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r_1+r_2} y_i^{e_i-1} dy_i,$$

where the domain of integration $D_3$ is given by $y_i \geq 0$ for all $i$ and $y_1 + \cdots + y_{r_1+r_2} \leq B$.

We will use induction on $r_1 + r_2$ to show that

$$V(r_1, r_2, B) = \frac{B^{r_1+2r_2}}{(r_1 + 2r_2)!}.$$
For $B \geq 0$ let

$$V(r_1, r_2, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r_1+r_2} y_i^{e_i-1} dy_i,$$

where the domain of integration $D_3$ is given by $y_i \geq 0$ for all $i$ and $y_1 + \cdots + y_{r_1+r_2} \leq B$.

We will use induction on $r_1 + r_2$ to show that

$$V(r_1, r_2, B) = \frac{B^{r_1+2r_2}}{(r_1 + 2r_2)!}.$$

Note that the case $B = 1$ will complete the proof of the lemma.
For $B \geq 0$ let

$$V(r_1, r_2, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r_1+2r_2} y_i^{e_i-1} dy_i,$$

where the domain of integration $D_3$ is given by $y_i \geq 0$ for all $i$ and $y_1 + \cdots + y_{r_1+2r_2} \leq B$.

We will use induction on $r_1 + r_2$ to show that

$$V(r_1, r_2, B) = \frac{B^{r_1+2r_2}}{(r_1 + 2r_2)!}.$$

Note that the case $B = 1$ will complete the proof of the lemma.

First set $r_1 + r_2 = 1$. 
For $B \geq 0$ let

$$V(r_1, r_2, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r_1+r_2} y_i^{e_i-1} dy_i,$$

where the domain of integration $D_3$ is given by $y_i \geq 0$ for all $i$ and $y_1 + \cdots + y_{r_1+r_2} \leq B$.

We will use induction on $r_1 + r_2$ to show that

$$V(r_1, r_2, B) = \frac{B^{r_1+2r_2}}{(r_1 + 2r_2)!}.$$ 

Note that the case $B = 1$ will complete the proof of the lemma.

First set $r_1 + r_2 = 1$. Here we have two cases:
For $B \geq 0$ let

$$V(r_1, r_2, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r_1+r_2} y_i^{e_i-1} dy_i,$$

where the domain of integration $D_3$ is given by $y_i \geq 0$ for all $i$ and $y_1 + \cdots + y_{r_1+r_2} \leq B$.

We will use induction on $r_1 + r_2$ to show that

$$V(r_1, r_2, B) = \frac{B^{r_1+2r_2}}{(r_1 + 2r_2)!}.$$ 

Note that the case $B = 1$ will complete the proof of the lemma.

First set $r_1 + r_2 = 1$. Here we have two cases:

$$V(1, 0, B) = \int_0^B 1 \, dy = B$$
For $B \geq 0$ let

$$V(r_1, r_2, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r_1+r_2} y_i^{e_i-1} dy_i,$$

where the domain of integration $D_3$ is given by $y_i \geq 0$ for all $i$ and $y_1 + \cdots + y_{r_1+r_2} \leq B$.

We will use induction on $r_1 + r_2$ to show that

$$V(r_1, r_2, B) = \frac{B^{r_1+2r_2}}{(r_1 + 2r_2)!}.$$

Note that the case $B = 1$ will complete the proof of the lemma.

First set $r_1 + r_2 = 1$. Here we have two cases:

$$V(1, 0, B) = \int_0^B 1 \, dy = B$$

$$V(0, 1, B) = \int_0^B y \, dy = \frac{B^2}{2}.$$
Now suppose our claim is valid for $r_1 + r_2$. 

\[ \text{This shows the case where we increase } r_1 \text{ by 1.} \]
Now suppose our claim is valid for \( r_1 + r_2 \). We then have

\[
V(r_1 + 1, r_2, B) = \int_0^B V(r_1, r_2, B - y_0) \, dy_0
\]
Now suppose our claim is valid for \( r_1 + r_2 \). We then have

\[
V(r_1 + 1, r_2, B) = \int_0^B V(r_1, r_2, B - y_0) \, dy_0
\]

\[
= \int_0^B \frac{(B - y_0)^{r_1+2r_2}}{(r_1 + 2r_2)!} \, dy_0
\]

This shows the case where we increase \( r_1 \) by 1.
Now suppose our claim is valid for \( r_1 + r_2 \). We then have

\[
V(r_1 + 1, r_2, B) = \int_0^B V(r_1, r_2, B - y_0) \, dy_0
\]

\[
= \int_0^B \frac{(B - y_0)^{r_1 + 2r_2}}{(r_1 + 2r_2)!} \, dy_0
\]

\[
= \frac{-(B - y_0)^{r_1 + 1 + 2r_2}}{(r_1 + 1 + 2r_2)!} \bigg|_{y_0=0}^B
\]
Now suppose our claim is valid for $r_1 + r_2$. We then have

$$V(r_1 + 1, r_2, B) = \int_0^B V(r_1, r_2, B - y_0) \, dy_0$$

$$= \int_0^B \frac{(B - y_0)^{r_1+2r_2}}{(r_1 + 2r_2)!} \, dy_0$$

$$= \left. \frac{-(B - y_0)^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!} \right|_0^B$$

$$= \frac{B^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!}.$$
Now suppose our claim is valid for $r_1 + r_2$. We then have

$$V(r_1 + 1, r_2, B) = \int_0^B V(r_1, r_2, B - y_0) \, dy_0$$

$$= \int_0^B \frac{(B - y_0)^{r_1 + 2r_2}}{(r_1 + 2r_2)!} \, dy_0$$

$$= \left. -\frac{(B - y_0)^{r_1 + 1 + 2r_2}}{(r_1 + 1 + 2r_2)!} \right|_{y_0=0}^B$$

$$= \frac{B^{r_1 + 1 + 2r_2}}{(r_1 + 1 + 2r_2)!}.$$ 

This shows the case where we increase $r_1$ by 1.
For the case where we increase $r_2$ by 1
For the case where we increase $r_2$ by 1 we use the induction hypothesis together with integration by parts:
For the case where we increase $r_2$ by 1 we use the induction hypothesis together with integration by parts:

$$V(r_1, r_2 + 1, B) = \int_0^B V(r_1, r_2, B - y_0) y_0 \, dy_0$$
For the case where we increase $r_2$ by 1 we use the induction hypothesis together with integration by parts:

$$V(r_1, r_2 + 1, B) = \int_0^B V(r_1, r_2, B - y_0) y_0 \, dy_0$$

$$= \int_0^B \frac{(B - y_0)^{r_1+2r_2}}{(r_1 + 2r_2)!} y_0 \, dy_0$$
For the case where we increase $r_2$ by 1 we use the induction hypothesis together with integration by parts:

\[
V(r_1, r_2 + 1, B) = \int_0^B V(r_1, r_2, B - y_0)y_0 \, dy_0
\]

\[
= \int_0^B \frac{(B - y_0)^{r_1+2r_2}}{(r_1 + 2r_2)!} y_0 \, dy_0
\]

\[
= -y_0(B - y_0)^{r_1+1+2r_2} \bigg|_{y_0=0}^{B} + \int_0^B \frac{(B - y_0)^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!} \, dy_0
\]

This completes our proof.
For the case where we increase $r_2$ by 1 we use the induction hypothesis together with integration by parts:

$$V(r_1, r_2 + 1, B) = \int_0^B V(r_1, r_2, B - y_0) y_0 \, dy_0$$

$$= \int_0^B \frac{(B - y_0)^{r_1+2r_2}}{(r_1 + 2r_2)!} y_0 \, dy_0$$

$$= \frac{-y_0(B - y_0)^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!} \bigg|_{y_0=0}^B + \int_0^B \frac{(B - y_0)^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!} \, dy_0$$

$$= \frac{-(B - y_0)^{r_1+2+2r_2}}{(r_1 + 2 + 2r_2)!} \bigg|_{y_0=0}^B$$

This completes our proof.
For the case where we increase $r_2$ by 1 we use the induction hypothesis together with integration by parts:

\[
V(r_1, r_2 + 1, B) = \int_0^B V(r_1, r_2, B - y_0)y_0 \, dy_0
\]

\[
= \int_0^B \frac{(B - y_0)^{r_1+2r_2}}{(r_1 + 2r_2)!} y_0 \, dy_0
\]

\[
= \left[ -\frac{y_0(B - y_0)^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!} \right]_{y_0=0}^B + \int_0^B \frac{(B - y_0)^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!} \, dy_0
\]

\[
= \left[ -(B - y_0)^{r_1+2+2r_2} \right]_{y_0=0}^B + \frac{B^{r_1+2+2r_2}}{(r_1 + 2 + 2r_2)!}.
\]

This completes our proof.
For the case where we increase \( r_2 \) by 1 we use the induction hypothesis together with integration by parts:

\[
V(r_1, r_2 + 1, B) = \int_0^B V(r_1, r_2, B - y_0) y_0 \, dy_0
\]

\[
= \int_0^B \frac{(B - y_0)^{r_1+2r_2}}{(r_1 + 2r_2)!} y_0 \, dy_0
\]

\[
= -y_0(B - y_0)^{r_1+1+2r_2} \left|^{B}_{y_0=0} \right. + \int_0^B \frac{(B - y_0)^{r_1+1+2r_2}}{(r_1 + 1 + 2r_2)!} \, dy_0
\]

\[
= -\frac{(B - y_0)^{r_1+2+2r_2}}{(r_1 + 2 + 2r_2)!} \bigg|^{B}_{y_0=0}
\]

\[
= \frac{B^{r_1+2+2r_2}}{(r_1 + 2 + 2r_2)!}.
\]

This completes our proof.
Lemma (The arithmetic/geometric mean inequality)

For any non-negative $y_1, \ldots, y_m \in \mathbb{R}$ we have

\[
\left( \prod_{i=1}^{m} y_i \right)^{1/m} \leq \sum_{i=1}^{m} y_i^{m},
\]

with equality if and only if $y_1 = \cdots = y_m$.

Proof:
We use Lagrange multipliers to maximize the function

\[ f(y_1, \ldots, y_m) = y_1 \cdots y_m \]

subject to the constraint

\[ g(y_1, \ldots, y_m) = y_1 + \cdots + y_m = k. \]

(Here we assume $k > 0$).
Lemma (The arithmetic/geometric mean inequality)

For any non-negative $y_1, \ldots, y_m \in \mathbb{R}$ we have

$$\left( \prod_{i=1}^{m} y_i \right)^{1/m} \leq \frac{\sum_{i=1}^{m} y_i}{m},$$

Proof: We use Lagrange multipliers to maximize the function

$$f(y_1, \ldots, y_m) = y_1 \cdots y_m$$

subject to the constraint

$$g(y_1, \ldots, y_m) = y_1 + \cdots + y_m = k.$$
Lemma (The arithmetic/geometric mean inequality)

For any non-negative \( y_1, \ldots, y_m \in \mathbb{R} \) we have

\[
\left( \prod_{i=1}^{m} y_i \right)^{1/m} \leq \frac{\sum_{i=1}^{m} y_i}{m},
\]

with equality if and only if \( y_1 = \cdots = y_m \).
Lemma (The arithmetic/geometric mean inequality)

For any non-negative $y_1, \ldots, y_m \in \mathbb{R}$ we have

$$\left( \prod_{i=1}^{m} y_i \right)^{1/m} \leq \frac{\sum_{i=1}^{m} y_i}{m},$$

with equality if and only if $y_1 = \cdots = y_m$.

Proof:
Lemma (The arithmetic/geometric mean inequality)

For any non-negative $y_1, \ldots, y_m \in \mathbb{R}$ we have

$$
\left( \prod_{i=1}^{m} y_i \right)^{1/m} \leq \frac{\sum_{i=1}^{m} y_i}{m},
$$

with equality if and only if $y_1 = \cdots = y_m$.

Proof: We use Lagrange multipliers to maximize the function

$$
f(y_1, \ldots, y_m) = y_1 \cdots y_m
$$
Lemma (The arithmetic/geometric mean inequality)

For any non-negative $y_1, \ldots, y_m \in \mathbb{R}$ we have

$$\left(\prod_{i=1}^{m} y_i\right)^{1/m} \leq \frac{\sum_{i=1}^{m} y_i}{m},$$

with equality if and only if $y_1 = \cdots = y_m$.

Proof: We use Lagrange multipliers to maximize the function

$$f(y_1, \ldots, y_m) = y_1 \cdots y_m$$

subject to the constraint

$$g(y_1, \ldots, y_m) = y_1 + \cdots + y_m = k.$$
Lemma (The arithmetic/geometric mean inequality)

For any non-negative \( y_1, \ldots, y_m \in \mathbb{R} \) we have

\[
\left( \prod_{i=1}^{m} y_i \right)^{1/m} \leq \frac{\sum_{i=1}^{m} y_i}{m},
\]

with equality if and only if \( y_1 = \cdots = y_m \).

**Proof:** We use Lagrange multipliers to maximize the function

\[ f(y_1, \ldots, y_m) = y_1 \cdots y_m \]

subject to the constraint

\[ g(y_1, \ldots, y_m) = y_1 + \cdots + y_m = k. \]

(Here we assume \( k > 0 \)).
The gradient of $f$ is

$$\nabla (f) = (\prod_{1 \leq i \leq m} y_i, \prod_{1 \leq i \leq m} y_i, \ldots, \prod_{1 \leq i \leq m} y_i)$$

and the gradient of $g$ is

$$\nabla (g) = (1, \ldots, 1).$$

By the theory of Lagrange multipliers, $f$ has its extremum subject to $g = k$ when $\nabla (f) = \lambda \nabla (g)$ for some $\lambda \neq 0$. We readily see that this occurs exactly when all $y_i = \lambda - 1 \prod_{1 \leq j \leq m} y_j$ (in particular, all $y_i$ are equal).

This extremum is clearly a maximum, as opposed to a minimum, since we can easily make $f = 0$, for example. The lemma follows.
The gradient of $f$ is

$$\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)$$
The gradient of $f$ is

$$\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)$$

and the gradient of $g$ is
The gradient of $f$ is

$$\nabla(f) = \left(\frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m}\right)$$

and the gradient of $g$ is

$$\nabla(g) = (1, \ldots, 1).$$
The gradient of $f$ is

$$\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)$$

and the gradient of $g$ is

$$\nabla(g) = (1, \ldots, 1).$$

By the theory of Lagrange multipliers,
The gradient of $f$ is

$$\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)$$

and the gradient of $g$ is

$$\nabla(g) = (1, \ldots, 1).$$

By the theory of Lagrange multipliers, $f$ has its extremum subject to $g = k$ when $\nabla(f) = \lambda \nabla(g)$ for some $\lambda \neq 0$. 
The gradient of $f$ is

$$\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)$$

and the gradient of $g$ is

$$\nabla(g) = (1, \ldots, 1).$$

By the theory of Lagrange multipliers, $f$ has its extremum subject to $g = k$ when $\nabla(f) = \lambda \nabla(g)$ for some $\lambda \neq 0$. We readily see that this occurs exactly when all $y_i = \lambda^{-1} \prod_{1 \leq j \leq m} y_j$.
The gradient of $f$ is
\[
\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)
\]
and the gradient of $g$ is
\[
\nabla(g) = (1, \ldots, 1).
\]

By the theory of Lagrange multipliers, $f$ has its extremum subject to $g = k$ when $\nabla(f) = \lambda \nabla(g)$ for some $\lambda \neq 0$. We readily see that this occurs exactly when all $y_i = \lambda^{-1} \prod_{1 \leq j \leq m} y_j$ (in particular, all $y_i$ are equal).
The gradient of \( f \) is
\[
\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)
\]
and the gradient of \( g \) is
\[
\nabla(g) = (1, \ldots, 1).
\]

By the theory of Lagrange multipliers, \( f \) has its extremum subject to \( g = k \) when \( \nabla(f) = \lambda \nabla(g) \) for some \( \lambda \neq 0 \). We readily see that this occurs exactly when all \( y_i = \lambda^{-1} \prod_{1 \leq j \leq m} y_j \) (in particular, all \( y_i \) are equal). This extremum is clearly a maximum,
The gradient of $f$ is

$$\nabla(f) = \left(\frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m}\right)$$

and the gradient of $g$ is

$$\nabla(g) = (1, \ldots, 1).$$

By the theory of Lagrange multipliers, $f$ has its extremum subject to $g = k$ when $\nabla(f) = \lambda \nabla(g)$ for some $\lambda \neq 0$. We readily see that this occurs exactly when all $y_i = \lambda^{-1} \prod_{1 \leq j \leq m} y_j$ (in particular, all $y_i$ are equal). This extremum is clearly a maximum, as opposed to a minimum,
The gradient of $f$ is

$$\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)$$

and the gradient of $g$ is

$$\nabla(g) = (1, \ldots, 1).$$

By the theory of Lagrange multipliers, $f$ has its extremum subject to $g = k$ when $\nabla(f) = \lambda \nabla(g)$ for some $\lambda \neq 0$. We readily see that this occurs exactly when all $y_i = \lambda^{-1} \prod_{1 \leq j \leq m} y_j$ (in particular, all $y_i$ are equal). This extremum is clearly a maximum, as opposed to a minimum, since we can easily make $f = 0$, for example.
The gradient of $f$ is
\[
\nabla(f) = \left( \frac{\prod_{1 \leq i \leq m} y_i}{y_1}, \frac{\prod_{1 \leq i \leq m} y_i}{y_2}, \ldots, \frac{\prod_{1 \leq i \leq m} y_i}{y_m} \right)
\]
and the gradient of $g$ is
\[
\nabla(g) = (1, \ldots, 1).
\]

By the theory of Lagrange multipliers, $f$ has its extremum subject to $g = k$ when $\nabla(f) = \lambda \nabla(g)$ for some $\lambda \neq 0$. We readily see that this occurs exactly when all $y_i = \lambda^{-1} \prod_{1 \leq j \leq m} y_j$ (in particular, all $y_i$ are equal). This extremum is clearly a maximum, as opposed to a minimum, since we can easily make $f = 0$, for example. The lemma follows.
Theorem (2)

Let $A$ be a non-zero fractional ideal of $K$. Then there is a non-zero $\alpha \in A$ with 

$$|N_{K/Q}(\alpha)| \leq n!(4/\pi)^{r_2} \sqrt{|D_K|N(A)}.$$ 

Proof: By Theorem 1, Lemmas 1 and 2, and Minkowski's Theorem, the first successive minima $\lambda_1$ of $\rho'(A)$ with respect to $C$ satisfies 

$$\lambda_1 \leq n!(4/\pi)^{r_2} \sqrt{|D_K|N(A)}.$$ 

Now there is a non-zero $\alpha \in A$ with $\rho'(\alpha)$ contained in $\lambda_1 C$. By the definitions of $\rho'$ and $C$, we have 

$$\frac{1}{n} \sum_{i=1}^{n} |\sigma_i(\alpha)| \leq \lambda_1.$$ 

Applying the arithmetic/geometric mean inequality gives the result.
Theorem (2)

Let \( \mathfrak{A} \) be a non-zero fractional ideal of \( K \).
Theorem (2)

Let $\mathfrak{A}$ be a non-zero fractional ideal of $K$. Then there is a non-zero $\alpha \in \mathfrak{A}$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n_1}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|D_K|} N(\mathfrak{A})$. 
Theorem (2)

Let $\mathcal{A}$ be a non-zero fractional ideal of $K$. Then there is a non-zero $\alpha \in \mathcal{A}$ with $|N_{K/Q}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^r 2 \sqrt{|D_K|} N(\mathcal{A})$.

Proof:
Theorem (2)

Let $\mathfrak{A}$ be a non-zero fractional ideal of $K$. Then there is a non-zero $\alpha \in \mathfrak{A}$ with $|N_{K/Q}(\alpha)| \leq \frac{n!}{n^n} (4/\pi)^{r_2} \sqrt{|D_K|} |N(\mathfrak{A})|.$

Proof: By Theorem 1,
Theorem (2)

Let \( \mathfrak{A} \) be a non-zero fractional ideal of \( K \). Then there is a non-zero \( \alpha \in \mathfrak{A} \) with

\[
|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} (4/\pi)^{r_2} \sqrt{|D_K|} |N(\mathfrak{A})|.
\]

Proof: By Theorem 1, Lemmas 1 and 2,
**Theorem (2)**

Let $\mathcal{A}$ be a non-zero fractional ideal of $K$. Then there is a non-zero $\alpha \in \mathcal{A}$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|D_K|} |N(\mathcal{A})|.$

**Proof:** By Theorem 1, Lemmas 1 and 2, and Minkowski’s Theorem,
Theorem (2)

Let $\mathfrak{A}$ be a non-zero fractional ideal of $K$. Then there is a non-zero $\alpha \in \mathfrak{A}$ with $|N_{K/Q}(\alpha)| \leq \frac{n!}{n^n} (4/\pi)^{r_2} \sqrt{|D_K|} N(\mathfrak{A})$.

Proof: By Theorem 1, Lemmas 1 and 2, and Minkowski’s Theorem, the first successive minima $\lambda_1$ of $\rho'(\mathfrak{A})$ with respect to $C$ satisfies
Theorem (2)

Let $\mathfrak{A}$ be a non-zero fractional ideal of $K$. Then there is a non-zero $\alpha \in \mathfrak{A}$ with $|N_{K/Q}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|D_K|} \cdot N(\mathfrak{A})$.

Proof: By Theorem 1, Lemmas 1 and 2, and Minkowski’s Theorem, the first successive minima $\lambda_1$ of $\rho'(\mathfrak{A})$ with respect to $C$ satisfies

$$\lambda_1^n \leq n! \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|D_K|} \cdot N(\mathfrak{A}).$$
Theorem (2)

Let \( \mathcal{A} \) be a non-zero fractional ideal of \( K \). Then there is a non-zero \( \alpha \in \mathcal{A} \) with \( \left| N_{K/Q}(\alpha) \right| \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^{r^2} \sqrt{|D_K|} N(\mathcal{A}) \).

\[ \lambda_1^n \leq n! \left( \frac{4}{\pi} \right)^{r^2} \sqrt{|D_K|} N(\mathcal{A}). \]

Now there is a non-zero \( \alpha \in \mathcal{A} \) with \( \rho'(\alpha) \) contained in \( \lambda_1 C \).

**Proof:** By Theorem 1, Lemmas 1 and 2, and Minkowski’s Theorem, the first successive minima \( \lambda_1 \) of \( \rho'(\mathcal{A}) \) with respect to \( C \) satisfies
Theorem (2)

Let \( \mathcal{A} \) be a non-zero fractional ideal of \( K \). Then there is a non-zero \( \alpha \in \mathcal{A} \) with \( |N_{K/Q}(\alpha)| \leq \frac{n!}{n^n} (4/\pi)^{r_2} \sqrt{|D_K|} N(\mathcal{A}) \).

Proof: By Theorem 1, Lemmas 1 and 2, and Minkowski’s Theorem, the first successive minima \( \lambda_1 \) of \( \rho'(\mathcal{A}) \) with respect to \( C \) satisfies

\[ \lambda_1^n \leq n! (4/\pi)^{r_2} \sqrt{|D_K|} N(\mathcal{A}). \]

Now there is a non-zero \( \alpha \in \mathcal{A} \) with \( \rho'(\alpha) \) contained in \( \lambda_1 C \). By the definitions of \( \rho' \) and \( C \),
Theorem (2)

Let $\mathfrak{A}$ be a non-zero fractional ideal of $K$. Then there is a non-zero $\alpha \in \mathfrak{A}$ with $|N_{K/Q}(\alpha)| \leq \frac{n!}{n^n} (4/\pi)^{2r} \sqrt{|D_K|} N(\mathfrak{A})$.

Proof: By Theorem 1, Lemmas 1 and 2, and Minkowski’s Theorem, the first successive minima $\lambda_1$ of $\rho'(\mathfrak{A})$ with respect to $C$ satisfies

$$\lambda_1^n \leq n! (4/\pi)^{2r} \sqrt{|D_K|} N(\mathfrak{A}).$$

Now there is a non-zero $\alpha \in \mathfrak{A}$ with $\rho'(\alpha)$ contained in $\lambda_1 C$. By the definitions of $\rho'$ and $C$, we have

$$\frac{1}{n} \sum_{i=1}^{n} |\sigma_i(\alpha)| \leq \frac{\lambda_1}{n}.$$
Theorem (2)

Let \( \mathcal{A} \) be a non-zero fractional ideal of \( K \). Then there is a non-zero \( \alpha \in \mathcal{A} \) with \( |N_{K/Q}(\alpha)| \leq \frac{n!}{n^n} (4/\pi)^{r_2} \sqrt{|D_K|} N(\mathcal{A}). \)

**Proof:** By Theorem 1, Lemmas 1 and 2, and Minkowski’s Theorem, the first successive minima \( \lambda_1 \) of \( \rho'(\mathcal{A}) \) with respect to \( C \) satisfies

\[
\lambda_1^n \leq n! (4/\pi)^{r_2} \sqrt{|D_K|} N(\mathcal{A}).
\]

Now there is a non-zero \( \alpha \in \mathcal{A} \) with \( \rho'(\alpha) \) contained in \( \lambda_1 C \). By the definitions of \( \rho' \) and \( C \), we have

\[
\frac{1}{n} \sum_{i=1}^{n} |\sigma_i(\alpha)| \leq \frac{\lambda_1}{n}.
\]

Applying the arithmetic/geometric mean inequality gives the result.
The quantity

\[ \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^{r_2} \]

occurring in Theorem 2 is called the *Minkowski Constant*. 
The quantity
\[ \frac{n!}{n^n} \frac{(4/\pi)^{r_2}}{r_2} \]
occurring in Theorem 2 is called the *Minkowski Constant*. 

**Corollary (1)**
The quantity
\[ \frac{n!}{n^n (4/\pi)^{r_2}} \]
occurring in Theorem 2 is called the *Minkowski Constant*.

**Corollary (1)**

*If* \( K \neq \mathbb{Q} \) 

*Proof*: Exercise.
The quantity
\[ \frac{n!}{n^n (4/\pi)^{r_2}} \]
occuring in Theorem 2 is called the *Minkowski Constant*.

**Corollary (1)**

*If \( K \neq \mathbb{Q} \) (i.e., if \( n > 1 \))*
The quantity
\[ \frac{n!}{n^n (4/\pi)^r} \]
occuring in Theorem 2 is called the *Minkowski Constant*.

**Corollary (1)**

If \( K \neq \mathbb{Q} \) (i.e., if \( n > 1 \)) then \( \sqrt{|D_K|} > 1 \).
The quantity
\[
\frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2}
\]
occurring in Theorem 2 is called the *Minkowski Constant*.

**Corollary (1)**

If \( K \neq \mathbb{Q} \) (i.e., if \( n > 1 \)) then \( \sqrt{|D_K|} > 1 \).

**Proof:**

[Insert proof here]
The quantity
\[ \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^{\frac{r^2}{2}} \]
occurring in Theorem 2 is called the \textit{Minkowski Constant}.

\textbf{Corollary (1)}

\textit{If } \( K \neq \mathbb{Q} \) \textit{ (i.e., if } n > 1 \textit{) then } \sqrt{|D_K|} > 1. \textit{.}

\textbf{Proof: Exercise.}
The quantity
\[ \frac{n!}{n^n (4/\pi)^{r^2}} \]

occurring in Theorem 2 is called the *Minkowski Constant*.

**Corollary (1)**

If \( K \neq \mathbb{Q} \) (i.e., if \( n > 1 \)) then \( \sqrt{|D_K|} > 1 \).

**Proof**: Exercise.

**Corollary (2)**
The quantity
\[ \frac{n!}{n^n (4/\pi)^{r_2}} \]
occuring in Theorem 2 is called the \textit{Minkowski Constant}.

\textbf{Corollary (1)}

If \( K \neq \mathbb{Q} \) (i.e., if \( n > 1 \)) then \( \sqrt{|D_K|} > 1 \).

\textbf{Proof:} Exercise.

\textbf{Corollary (2)}

If \( \mathfrak{A} \) is a non-zero fractional ideal,
The quantity
\[ \frac{n!}{n^n (4/\pi)^{r_2}} \]
occurring in Theorem 2 is called the *Minkowski Constant*.

**Corollary (1)**

If \( K \neq \mathbb{Q} \) (i.e., if \( n > 1 \)) then \( \sqrt{|D_K|} > 1 \).

**Proof:** Exercise.

**Corollary (2)**

If \( \mathfrak{A} \) is a non-zero fractional ideal, then there is a non-zero \( \alpha \in K \) such that \( \alpha \mathfrak{A} \) is a non-zero ideal in \( \mathcal{O}_K \).
The quantity
\[ \frac{n!}{n^n (4/\pi)^{r_2}} \]
occuring in Theorem 2 is called the \textit{Minkowski Constant}.

\textbf{Corollary (1)}

If \( K \neq \mathbb{Q} \) (i.e., if \( n > 1 \)) then \( \sqrt{|D_K|} > 1 \).

\textbf{Proof:} Exercise.

\textbf{Corollary (2)}

If \( \mathfrak{A} \) is a non-zero fractional ideal, then there is a non-zero \( \alpha \in K \) such that \( \alpha \mathfrak{A} \) is a non-zero ideal in \( \mathcal{O}_K \) with
\[ N(\alpha \mathfrak{A}) \leq \frac{n!}{n^n (4/\pi)^{r_2}} \sqrt{|D_K|}. \]
Proof:

Apply Theorem 2 to the fractional ideal $A^{-1}$.

Since $\alpha \in A^{-1}$, we have $\alpha A \subseteq O_K$.

Clearly $\alpha A = \alpha O_K A$ (a product of fractional ideals), so that by a previous exercise $N(\alpha A) = N(\alpha O_K)$ $N(A)$ = $|N_K/Q(\alpha)| N(A)$.

The non-zero principal fractional ideals (those of the form $\alpha O_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the ideal class group of $K$.

The upshot of Corollary 2 is that this quotient group is finite.

The order of the quotient group is called the class number of the field $K$, and typically denoted $h_K$ or just $h$ if the field is understood.

Note that $h = 1$ is the same as saying $O_K$ is a principal ideal domain.

Corollary (3)

There is a positive integer $h$ (the class number, as defined above) such that $A^h$ is a principal ideal for all ideals $A \subseteq O_K$. 

Proof: Apply Theorem 2 to the fractional ideal \( \mathfrak{A}^{-1} \).
Proof: Apply Theorem 2 to the fractional ideal $\mathcal{A}^{-1}$. Since $\alpha \in \mathcal{A}^{-1}$,
Proof: Apply Theorem 2 to the fractional ideal $A^{-1}$. Since $\alpha \in A^{-1}$, we have $\alpha A \subseteq \mathcal{O}_K$. 
Proof: Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathcal{O}_K \mathfrak{A}$
Proof: Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathfrak{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathfrak{O}_K \mathfrak{A}$ (a product of fractional ideals),
Proof: Apply Theorem 2 to the fractional ideal \( \mathcal{A}^{-1} \). Since \( \alpha \in \mathcal{A}^{-1} \), we have \( \alpha \mathcal{A} \subseteq \mathfrak{O}_K \). Clearly \( \alpha \mathcal{A} = \alpha \mathfrak{O}_K \mathcal{A} \) (a product of fractional ideals), so that by a previous exercise \( N(\alpha \mathcal{A}) = N(\alpha \mathfrak{O}_K)N(\mathcal{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathcal{A}) \).
Proof: Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathcal{O}_K \mathfrak{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathfrak{A}) = N(\alpha \mathcal{O}_K)N(\mathfrak{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathfrak{A})$.

The non-zero principal fractional ideals

Math 681, Monday, February 8 February 8, 2021
Proof: Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathfrak{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathfrak{O}_K \mathfrak{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathfrak{A}) = N(\alpha \mathfrak{O}_K)N(\mathfrak{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathfrak{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathfrak{O}_K$ for some $\alpha \in K^\times$)
Proof: Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathcal{O}_K \mathfrak{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathfrak{A}) = N(\alpha \mathcal{O}_K)N(\mathfrak{A}) = |N_{K/Q}(\alpha)|N(\mathfrak{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.
Proof: Apply Theorem 2 to the fractional ideal $A^{-1}$. Since $\alpha \in A^{-1}$, we have $\alpha A \subseteq \mathcal{O}_K$. Clearly $\alpha A = \alpha \mathcal{O}_K A$ (a product of fractional ideals), so that by a previous exercise $N(\alpha A) = N(\alpha \mathcal{O}_K)N(A) = |N_{K/\mathbb{Q}}(\alpha)|N(A)$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group
**Proof:** Apply Theorem 2 to the fractional ideal $A^{-1}$. Since $\alpha \in A^{-1}$, we have $\alpha A \subseteq \mathcal{O}_K$. Clearly $\alpha A = \alpha \mathcal{O}_K A$ (a product of fractional ideals), so that by a previous exercise $N(\alpha A) = N(\alpha \mathcal{O}_K) N(A) = |N_{K/\mathbb{Q}}(\alpha)| N(A)$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here)
Proof: Apply Theorem 2 to the fractional ideal $\mathcal{A}^{-1}$. Since $\alpha \in \mathcal{A}^{-1}$, we have $\alpha \mathcal{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathcal{A} = \alpha \mathcal{O}_K \mathcal{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathcal{A}) = N(\alpha \mathcal{O}_K)N(\mathcal{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathcal{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the ideal class group of $K$. 

Math 681, Monday, February 8
**Proof:** Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathfrak{O}_K \mathfrak{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathfrak{A}) = N(\alpha \mathfrak{O}_K)N(\mathfrak{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathfrak{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathfrak{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the *ideal class group* of $K$.

The upshot of Corollary 2 is that this quotient group is finite.
Proof: Apply Theorem 2 to the fractional ideal \( \mathfrak{A}^{-1} \). Since \( \alpha \in \mathfrak{A}^{-1} \), we have \( \alpha \mathfrak{A} \subseteq \mathcal{O}_K \). Clearly \( \alpha \mathfrak{A} = \alpha \mathcal{O}_K \mathfrak{A} \) (a product of fractional ideals), so that by a previous exercise \( N(\alpha \mathfrak{A}) = N(\alpha \mathcal{O}_K)N(\mathfrak{A}) = |N_{K/Q}(\alpha)|N(\mathfrak{A}) \).

The non-zero principal fractional ideals (those of the form \( \alpha \mathcal{O}_K \) for some \( \alpha \in K^\times \)) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the ideal class group of \( K \).

The upshot of Corollary 2 is that this quotient group is finite. The order of the quotient group is called the class number of the field \( K \),
Proof: Apply Theorem 2 to the fractional ideal \( A^{-1} \). Since \( \alpha \in A^{-1} \), we have \( \alpha A \subseteq \mathcal{O}_K \). Clearly \( \alpha A = \alpha \mathcal{O}_K A \) (a product of fractional ideals), so that by a previous exercise \( N(\alpha A) = N(\alpha \mathcal{O}_K)N(A) = |N_{K/Q}(\alpha)|N(A) \).

The non-zero principal fractional ideals (those of the form \( \alpha \mathcal{O}_K \) for some \( \alpha \in K^\times \)) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the ideal class group of \( K \).

The upshot of Corollary 2 is that this quotient group is finite. The order of the quotient group is called the class number of the field \( K \), and typically denoted \( h_K \).
Proof: Apply Theorem 2 to the fractional ideal $\mathcal{A}^{-1}$. Since $\alpha \in \mathcal{A}^{-1}$, we have $\alpha \mathcal{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathcal{A} = \alpha \mathcal{O}_K \mathcal{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathcal{A}) = N(\alpha \mathcal{O}_K)N(\mathcal{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathcal{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the ideal class group of $K$.

The upshot of Corollary 2 is that this quotient group is finite. The order of the quotient group is called the class number of the field $K$, and typically denoted $h_K$ or just $h$ if the field is understood.
Proof: Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathcal{O}_K \mathfrak{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathfrak{A}) = N(\alpha \mathcal{O}_K)N(\mathfrak{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathfrak{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the ideal class group of $K$.

The upshot of Corollary 2 is that this quotient group is finite. The order of the quotient group is called the class number of the field $K$, and typically denoted $h_K$ or just $h$ if the field is understood.

Note that $h = 1$ is the same as saying $\mathcal{O}_K$ is a principal ideal domain.
**Proof:** Apply Theorem 2 to the fractional ideal $A^{-1}$. Since $\alpha \in A^{-1}$, we have $\alpha A \subseteq \mathfrak{O}_K$. Clearly $\alpha A = \alpha \mathfrak{O}_K A$ (a product of fractional ideals), so that by a previous exercise $N(\alpha A) = N(\alpha \mathfrak{O}_K)N(A) = |N_{K/\mathbb{Q}}(\alpha)|N(A)$.

The non-zero principal fractional ideals (those of the form $\alpha \mathfrak{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the *ideal class group* of $K$.

The upshot of Corollary 2 is that this quotient group is finite. The order of the quotient group is called the *class number* of the field $K$, and typically denoted $h_K$ or just $h$ if the field is understood.

Note that $h = 1$ is the same as saying $\mathfrak{O}_K$ is a principal ideal domain.

**Corollary (3)**
Proof: Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathcal{O}_K \mathfrak{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathfrak{A}) = N(\alpha \mathcal{O}_K)N(\mathfrak{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathfrak{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^{\times}$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the ideal class group of $K$.

The upshot of Corollary 2 is that this quotient group is finite. The order of the quotient group is called the class number of the field $K$, and typically denoted $h_K$ or just $h$ if the field is understood.

Note that $h = 1$ is the same as saying $\mathcal{O}_K$ is a principal ideal domain.

Corollary (3)

There is a positive integer $h$
**Proof:** Apply Theorem 2 to the fractional ideal $A^{-1}$. Since $\alpha \in A^{-1}$, we have $\alpha A \subseteq \mathcal{O}_K$. Clearly $\alpha A = \alpha \mathcal{O}_K A$ (a product of fractional ideals), so that by a previous exercise $N(\alpha A) = N(\alpha \mathcal{O}_K)N(A) = |N_{K/Q}(\alpha)|N(A)$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the *ideal class group* of $K$.

The upshot of Corollary 2 is that *this quotient group is finite*. The order of the quotient group is called the *class number* of the field $K$, and typically denoted $h_K$ or just $h$ if the field is understood.

Note that $h = 1$ is the same as saying $\mathcal{O}_K$ is a principal ideal domain.

**Corollary (3)**

*There is a positive integer $h$ (the class number, as defined above)*
Proof: Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathcal{O}_K \mathfrak{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathfrak{A}) = N(\alpha \mathcal{O}_K)N(\mathfrak{A}) = |N_{K/\mathbb{Q}}(\alpha)|N(\mathfrak{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals.

The quotient group (our group is abelian, so no problems here) is called the ideal class group of $K$.

The upshot of Corollary 2 is that this quotient group is finite. The order of the quotient group is called the class number of the field $K$, and typically denoted $h_K$ or just $h$ if the field is understood.

Note that $h = 1$ is the same as saying $\mathcal{O}_K$ is a principal ideal domain.

**Corollary (3)**

There is a positive integer $h$ (the class number, as defined above) such that $\mathfrak{A}^h$ is a principal ideal for all ideals $\mathfrak{A} \subseteq \mathcal{O}_K$. 
Example:

Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$. If $D \equiv 1 \pmod{4}$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $A$ contains a non-zero element $\alpha$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq N(A)\sqrt{D}$. If $D \equiv 2, 3 \pmod{4}$, then $\sqrt{|D_K|} = 2\sqrt{D}$ and every non-zero ideal $A$ contains a non-zero element $\alpha$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq N(A)\sqrt{D}$. It's known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields (when $D < 0$). It's famously conjectured, but still unproven, that $h_K = 1$ for infinitely many real quadratic number fields.
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. 
**Example:** Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$. 

It's known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields (when $D < 0$). It's famously conjectured, but still unproven, that $h_K = 1$ for infinitely many real quadratic number fields.
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|D_K|} = \sqrt{D}$
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A}) \sqrt{D}}{2}.$$
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$ 

If $D \equiv 2, 3 \mod 4$, it's known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields (when $D < 0$). It's famously conjectured, but still unproven, that $h_K = 1$ for infinitely many real quadratic number fields.
**Example:** Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$ 

If $D \equiv 2, 3 \mod 4$, then $\sqrt{|D_K|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(\mathfrak{A})\sqrt{D}.$$
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$ 

If $D \equiv 2, 3 \mod 4$, then $\sqrt{|D_K|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(\mathfrak{A})\sqrt{D}.$$ 

It’s known
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$ 

If $D \equiv 2, 3 \mod 4$, then $\sqrt{|D_K|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(\mathfrak{A})\sqrt{D}.$$ 

It’s known (you looked this up in the first homework assignment)
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \pmod{4}$, then $\sqrt{|DK|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$ 

If $D \equiv 2, 3 \pmod{4}$, then $\sqrt{|DK|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(\mathfrak{A})\sqrt{D}.$$ 

It’s known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields.
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$

If $D \equiv 2, 3 \mod 4$, then $\sqrt{|D_K|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(\mathfrak{A})\sqrt{D}.$$

It’s known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields (when $D < 0$).
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$ 

If $D \equiv 2, 3 \mod 4$, then $\sqrt{|D_K|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(\mathfrak{A})\sqrt{D}.$$ 

It’s known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields (when $D < 0$). It’s famously conjectured,
**Example:** Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \mod 4$, then $\sqrt{|DK|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$ 

If $D \equiv 2, 3 \mod 4$, then $\sqrt{|DK|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(\mathfrak{A})\sqrt{D}.$$ 

It’s known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields (when $D < 0$). It’s famously conjectured, but still unproven,
Example: Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$.

If $D \equiv 1 \pmod{4}$, then $\sqrt{|D_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{N(\mathfrak{A})\sqrt{D}}{2}.$$ 

If $D \equiv 2, 3 \pmod{4}$, then $\sqrt{|D_K|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq N(\mathfrak{A})\sqrt{D}.$$ 

It’s known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields (when $D < 0$). It’s famously conjectured, but still unproven, that $h_K = 1$ for infinitely many real quadratic number fields.