Theorem

For a number field $K$, the ideal class group $C_K$ is bounded by

$\kappa := \prod_{j=1}^{n} (\sum_{i=1}^{n} |v_i^{\sigma_j}|)$, hence finite.
Sketch of the proof.

Pick an \(\mathbb{Z}\)-basis \(v_1, \ldots, v_n\) of \(\mathcal{O}\).

Let \(c \in C_K\) be a class, we can pick an ideal \(a \in c^{-1}\). Let

\[
S := \{s \in \mathcal{O} | s = \sum m_i v_i, m_i \in \mathbb{Z}, 0 \leq m_i < (Na)^{1/n} + 1\}.
\]

Then \(|S| > Na\). There exist \(a, b \in S\) such that \(a - b \in a\). It follows that \((a - b) = ab\) for some \(b \in \mathcal{O}\).

Write \(a - b = \sum p_i v_i\), then

\[
N(a - b) \leq ((Na)^{1/n} + 1)^n \kappa.
\]

Replace \(a\) by \(aa\) with \(N(a)\) goes to infinity, then \(Na \leq \kappa\). \(\square\)
Example

Let $K = \mathbb{Q}(\omega)$. $d_K = -3$. $\{1, \omega\}$ is a basis. $\kappa = 4$. We look for ideals with norm $\leq 4$. They are principal, hence e get a PID.
Let $\mathcal{D}$ be a Dedekind domain and $K$ be its field of quotients. Let $\mathfrak{p}$ be a prime ideal. Then we have $v_{\mathfrak{p}} : K^* \to \mathbb{Z}$ such that:

$v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x)v_{\mathfrak{p}}(y)$. and $v_{\mathfrak{p}}(x + y) \geq \inf(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y))$.

Also this is surjective. We may extend the definition to $K$ by assign $v_{\mathfrak{p}}(0) = \infty$. 
It follows that $v(1) = 0$.
There is also another useful fact:
If $v(x) > v(y)$ then $v(x + y) = v(y)$.
To see this, first note that $v(x + y) \geq v(y)$. On the other hand, $v(y) \geq \inf(v(x + y), v(-x)) = v(x + y)$ since $v(-x) = v(x) > v(y)$. 
In general, for a given $K$ with a function $v : K \to \mathbb{Z} \cup \{\infty\}$ with above property is called a (discrete) valuation. For a valuation, let $R := \{x \in K | v(x) \geq 0\}$ and $m := \{x \in K | v(x) \geq 1\}$. Then $R$ is called the valuation ring. It’s easy to check that $m$ is a maximal ideal, called the valuation ideal.
Proposition

A discrete valuation ring $R$ is a local PID.
For Dedekind domain \( \mathcal{D} \), we can prove the following

**Proposition**

Let \( \mathcal{D} \) be a Dedekind domain and \( v \) be a valuation of \( K \) with \( \mathcal{D} \subset R \). Then \( v = v_p \) for some prime ideal \( p \). \( pR = m \) and \( R/m \cong \mathcal{D}/p \).
Proof.
Consider \( p := m \cap D \). It’s clearly a prime ideal of \( D \).
One can verify that \( p \neq 0 \), otherwise, \( v = 0 \).
If \( v_p(x) = 0 \), then \( v(x) = 0 \). We write \( x = \frac{b}{a} \). And
\( v_p(b) = v_p(a) = s \), that is \( (b) = p^s b \), \( (a) = p^s a \). Fix \( t \in p^s - p^{s+1} \),
then \( b = tb', a = ta' \) with \( a', b' \notin p \). So \( v(a') = v(b') = 0 \).
Next, we show that \( pR = m \). Since \( R \) is a DVR, \( pR = m^s \) for some
\( s \geq 1 \). Then one sees that \( v = sv_p \). Therefore, \( s = 1 \).
Finally, we show that \( D + m = R \).
Given \( x \in R - m \), we have \( v(x) = 0 \). We can write \( x = \frac{b}{a} \) with
\( b, a \in D - p \). Since \( D/p \) is a field. There is \( c \in D \) such that
\( ac \in 1 + p \). So
\[
x - bc = x(1 - ac) \in m.
\]
\( \square \)
Proposition

Let \( \mathcal{O} \) be the ring of algebraic integers of a number field \( K \). Let \( v \) be a valuation with valuation ring \( R \). Then \( \mathcal{O} \subset R \).
Proof.
First note that $v(x) \geq 0$ for all $x \in \mathbb{Z}$.
Next let $x \in \mathcal{D}$, $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. We have

$$nv(x) = v(x^n) \geq \inf(v(a_ix^i)) = \inf(v(a_i) + iv(x)) \geq \inf(iv(x)).$$

It follows that $v(x) \geq 0$. \qed
Corollary

Let $\mathcal{O}$ be the ring of algebraic integers of a number field $K$. Then there is an one to one correspondence between valuation of $K$ and prime ideals of $\mathcal{O}$. 
We would like to remark that this doesn’t holds for function field. Because the valuation $v_\infty$ by $v_\infty\left(\frac{f}{g}\right) = \deg g - \deg f$ is not coming from prime ideal.
In fact, we have

**Theorem**

Let $K = F(x)$. Let $p \triangleleft F[x]$ be prime ideals and $f_p := [R_p/m_p : F]$. Then $v_\infty$ with $v_p$ are the full set of valuations of $K$ which are zero on $F^*$. Moreover,

$$v_\infty + \sum f_p v_p = 0.$$
Sketch.
Suppose that $v(x) \geq 0$, then so if $v(f)$ for all $f \in F[x]$. We claim that there is a monic irreducible polynomial $f$ such that $v(f) > 0$. Then one can verify that $v = v_f$.

Next, suppose that $v(x) = s < 0$. We claim that $v(g) = s \deg g$, by induction on $\deg g$. We write $g = ax^d + g_1$ with $\deg g_1 < d$. Then $v(g_1) = s \deg g_1 > sd$. It follows that $v(g) = v(ax^d) = s \deg g$. Hence $s$ must be $-1$.

Finally, for any polynomial $g$, we clearly have:

$$\deg(g) = \sum \deg(p)v_p(g).$$

Since $\deg(p) = [R_p/m_p : F]$, the theorem follows.
We introduce the absolute value to justify the above formula. Given a field $K$, a function $| \cdot | : K \to \mathbb{R}_{\geq 0}$ is called an absolute value if for all $x, y \in K$,

1. $|x| = 0$ if and only if $x = 0$.
2. $|xy| = |x||y|
3. $|x + y| \leq |x| + |y|$. 

If 3 is replace by:

3’ $|x + y| \leq \sup(|x|, |y|)$ 
then we call it ultrametric. Note that for an ultrametric we have $|x| > |y|$ implies that $|x + y| = |x|$. We say an absolute value is discrete if $|K^*|$ is a discrete subgroup of $\mathbb{R}_{\geq 0}$.
Lemma

If $|·|$ is discrete then $|K^*|$ is cyclic generated by some $0 < \lambda < 1$. 
Proof.
Since $|1| = 1$ and thus $|K^*| \cap (0, 1) \neq \emptyset$. Discrete mean that intersection with any bounded set is finite. We pick maximal $\lambda$ in the intersection so that $|x| = \lambda$.
Now for any $y \in K^*$ with $|y| < 1$. Then $\lambda^{n+1} \leq |y| < \lambda^n$ for some $n$. Hence $\lambda \leq |yx^{-n}| < 1$. We must have $\lambda = |yx^{-n}|$ by maximality.
If $|y| > 1$, then we consider $y^{-1}$. This completes the proof. \qed
We have the following important examples:

**Example**

Let $\sigma : K \hookrightarrow \mathbb{R}$ be a real embedding. Then $|x|_\sigma := |\sigma(x)|_\mathbb{R}$ defines a absolute value.

Similarly $\sigma : K \hookrightarrow \mathbb{C}$ be an imaginary embedding. Then $|x|_\sigma := |\sigma(x)|_\mathbb{C}$ defines a absolute value.
Example

Let $\nu$ be a valuation and let $0 < \lambda < 1$, then $|x|_\nu := \lambda^\nu(x)$ defines an absolute value. We say that two absolute value $|\cdot|$, $|\cdot|'$ are equivalent if $|\cdot|^{\alpha} = |\cdot|'$ for some $\alpha$. An absolute value which is equivalent to Example 0.9 is called *Archimedean*. 
Lemma

Let $|·|_1, |·|_2$ be two non-trivial absolute values of $K$. Then they are equivalent if and only if

$$\{x \in K ||x||_1 > 1\} \subset \{x \in K ||x||_2 > 1\}.$$
Exercise

Given an absolute value, the $K$ is endowed with a metric. Show that the topology of two equivalent absolute values are the same.
Let’s consider the field $\mathbb{Q}$. We have $\cdot |_{\mathbb{R}}$. And we have $\cdot |_{p}$ by $|x|_p := p^{-\nu_p(x)}$.

Then we have the Product Formula

$$|x|_{\mathbb{R}} \prod |x|_p = 1.$$ 

**Theorem (Ostrowski)**

*An absolute value of $\mathbb{Q}$ is equivalent to exactly either $\cdot |_{\mathbb{R}}$ or $\cdot |_{p}$.***