7. The ideal class group

Definition: Let $b_1,\dots,b_n \in \mathbb{R}^n$ be linearly independent over $\mathbb{R}$. Then $\Lambda = \mathbb{Z}b_1+\dots+\mathbb{Z}b_n$ is called a lattice [dt. Gitter] and $\{b_1,\dots,b_n\}$ is called a basis of Λ.

Remarks: 1) Clearly $(\Lambda,+) = (\mathbb{Z}b_1+\dots+\mathbb{Z}b_n,+)$ is a free abelian group of rank n (and $\{b_1,\dots,b_n\}$ is a $\mathbb{Z}$-basis of Λ).

2) The basis of a lattice is not uniquely determined. More precisely, Lemma 4 implies the following: If $c_{ij}\in\mathbb{Z}$ (with $1\le i,j\le n$) and $g_i = \sum_{j=1}^n c_{ij}b_j$ then $\{g_1,\dots,g_n\}$ is also a basis of Λ if and only if the matrix $C = (c_{ij})_{1\le i,j\le n}$ is unimodular (i.e., $\det C \in \{1,-1\}$).

Definition: Let $b_1,\dots,b_n\in\mathbb{R}^n$ be linearly independent over $\mathbb{R}$. Then $F = \{\sum_{i=1}^n x_i b_i \mid 0\le x_i<1 \ (1\le i\le n)\}$ is called the fundamental parallelopiped [dt Fundamentalparallelopiped] of the basis $\{b_1,\dots,b_n\}$ of the lattice $\mathbb{Z}b_1+\dots+\mathbb{Z}b_n$ and its volume $v(F)$ is called the lattice constant [dt. Gitterkonstante] of the lattice $\mathbb{Z}b_1+\dots+\mathbb{Z}b_n$. (More precisely, $v(F)$ denotes the Jordan measure of F.)

Lemma 122 Let $b_1,\dots,b_n\in\mathbb{R}^n$ be linearly independent over $\mathbb{R}$ and let F be the fundamental parallelopiped of the basis $\{b_1,\dots,b_n\}$ of the lattice $\mathbb{Z}b_1+\dots+\mathbb{Z}b_n$. Then

$$v(F) = |\det(b_1,\dots,b_n)|.$$

Proof: Using the transformation formula for multiple integrals we get

$$v(F) = \int_F d(x_1,\dots,x_n) = \int_0^1\cdots\int_0^1 |\det(b_1,\dots,b_n)|\,dx_1\dots dx_n = |\det(b_1,\dots,b_n)|.$$

Lemma 123 Let Λ be a lattice in $\mathbb{R}^n$ and $\{b_1,\dots,b_n\}$ and $\{g_1,\dots,g_n\}$ two bases of Λ. Then $|\det(b_1,\dots,b_n)| = |\det(g_1,\dots,g_n)|$, i.e., the lattice constant of Λ does not depend on the basis.

Proof: Let $g_i = \sum_{j=1}^n c_{ij}b_j$ with $c_{ij}\in\mathbb{Z}$ (for $1\le i,j\le n$) and $C = (c_{ij})_{1\le i,j\le n}$. Then

$$|\det(g_1,\dots,g_n)| = |\det(b_1,\dots,b_n)|\cdot\underbrace{|\det C|}_{=1} = |\det(b_1,\dots,b_n)|.$$

Definition: If $\Lambda\subseteq\mathbb{R}^n$ is a lattice its lattice constant is denoted by $d(\Lambda)$.

Definition: A set $K\subseteq\mathbb{R}^n$ is called symmetric about the origin [dt symmetrisch bezüglich des Ursprungs] if $-x\in K \ \forall x\in K$.

Theorem 124 (Minkowski's (convex body) theorem [dt. Gitterpunktsatz von Minkowski])
Let $K\subseteq\mathbb{R}^n$ be a bounded convex body with Jordan measure $v(K)$ that is symmetric about the origin and $\Lambda\subseteq\mathbb{R}^n$ a lattice. If $v(K) > 2^n d(\Lambda)$ then there exists an $x\in(\Lambda\cap K)\setminus\{0\}$. (i.e., K contains a lattice point different from the origin).

(Sketch of) **Proof** (Modell): First we assume $\Lambda = \mathbb{Z}^n$ ($\Rightarrow d(\Lambda)=1$). For $m\in\mathbb{N}$ let $K_m := \{(\frac{a_1}{m},\dots,\frac{a_n}{m})\in K \mid a_1,\dots,a_n\in\mathbb{Z}\}$. As K has Jordan measure we get $\lim_{m\to\infty}\frac{|K_m|}{m^n} = v(K)$.

As $v(K) > 2^n$ we get that $|K_m| > 2^n m^n$ for all sufficiently large m. For such an m we have $\exists \left(\frac{a_1}{m}, \dots, \frac{a_n}{m}\right), \left(\frac{b_1}{m}, \dots, \frac{b_n}{m}\right) \in K_m$ with $\left(\frac{a_1}{m}, \dots, \frac{a_n}{m}\right) \neq \left(\frac{b_1}{m}, \dots, \frac{b_n}{m}\right)$ and $a_i \equiv b_i \pmod{2m}$ for $1 \le i \le n$ by a bot argument [dt. Schubfachschluss]. Let $x := \frac{1}{2}\left(\frac{a_1}{m}, \dots, \frac{a_n}{m}\right) - \frac{1}{2}\left(\frac{b_1}{m}, \dots, \frac{b_n}{m}\right) = \left(\frac{a_1 - b_1}{2m}, \dots, \frac{a_n - b_n}{2m}\right)$. Then $x \in \mathbb{Z}^n$ as $(2m) \mid (a_i - b_i)$ for $1 \le i \le n$. As K is symmetric about the origin $-\left(\frac{b_1}{m}, \dots, \frac{b_n}{m}\right) \in K$ and as K is convex $x \in K$. As $(a_1, \dots, a_n) \neq (b_1, \dots, b_n)$ we get $x \neq 0$.

Now we consider an arbitrary lattice $\Lambda = \mathbb{Z} b_1 + \dots + \mathbb{Z} b_n$. Let $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ be the linear map that is defined by $\varphi(b_i) = e_i$ for $1 \le i \le n$ (where $e_i = (0, \dots, 0, \underset{i\text{th entry}}{1}, 0, \dots, 0)$). Then $|\det \varphi| = \frac{1}{d(\Lambda)}$ (as $d(\Lambda) = |\det \varphi^{-1}|$)

As $v(\varphi(K)) = |\det \varphi| \, v(K) = \frac{v(K)}{d(\Lambda)} > 2^n$ there is an $x \in (\mathbb{Z}^n \cap \varphi(K)) \setminus \{0\}$ and therefore $\varphi^{-1}(x) \in (\Lambda \cap K) \setminus \{0\}$ (where we used $\varphi(\Lambda) = \mathbb{Z}^n$).

Remarks: 1) In fact Theorem 124 proves the existence of two different lattice points $\neq 0$ in K as $x \in (\Lambda \cap K) \setminus \{0\} \Rightarrow -x \in (\Lambda \cap K) \setminus \{0\}$.

2) If $K = (-1, 1)^n$ and $\Lambda = \mathbb{Z}^n$ then $v(K) = 2^n d(\Lambda)$ but 0 is the only lattice point in K. I.e., Theorem 124 is best possible.

Definition: Let K be an algebraic number field with $[K : \mathbb{Q}] = n$ and $\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}} : K \hookrightarrow \mathbb{C}$ the different homomorphisms (with $\sigma_i(K) \subseteq \mathbb{R}$ for $1 \le i \le r$ and $\sigma_{r+i}(K) \not\subseteq \mathbb{R}$ for $1 \le i \le s$). Set

$$\sigma : K \to \mathbb{R}^n, \quad \sigma(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re}\sigma_{r+1}(\alpha), \operatorname{Im}\sigma_{r+1}(\alpha), \dots, \operatorname{Re}\sigma_{r+s}(\alpha), \operatorname{Im}\sigma_{r+s}(\alpha)).$$

Theorem 125 Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. If $\{\alpha_1, \dots, \alpha_n\}$ is a basis of K as a $\mathbb{Q}$-vector space then $\sigma(\alpha_1), \dots, \sigma(\alpha_n) \in \mathbb{R}^n$ are linearly independent over $\mathbb{R}$.

Proof: By Theorem 33

$$\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \sigma_{r+1}(\alpha_1) & \overline{\sigma_{r+1}}(\alpha_1) & \cdots & \sigma_{r+s}(\alpha_1) & \overline{\sigma_{r+s}}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \sigma_{r+1}(\alpha_n) & \overline{\sigma_{r+1}}(\alpha_n) & \cdots & \sigma_{r+s}(\alpha_n) & \overline{\sigma_{r+s}}(\alpha_n) \end{vmatrix}^2 = \Delta_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) \neq 0$$

and therefore

$$0 \neq \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) + i \operatorname{Im}\sigma_{r+1}(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) - i \operatorname{Im}\sigma_{r+1}(\alpha_1) & \cdots & \sigma_{r+s}(\alpha_1) & \overline{\sigma_{r+s}}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) + i \operatorname{Im}\sigma_{r+1}(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) - i \operatorname{Im}\sigma_{r+1}(\alpha_n) & \cdots & \sigma_{r+s}(\alpha_n) & \overline{\sigma_{r+s}}(\alpha_n) \end{vmatrix}$$

$$= \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & 2\operatorname{Re}\sigma_{r+1}(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) - i \operatorname{Im}\sigma_{r+1}(\alpha_1) & \cdots & \sigma_{r+s}(\alpha_1) & \overline{\sigma_{r+s}}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & 2\operatorname{Re}\sigma_{r+1}(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) - i \operatorname{Im}\sigma_{r+1}(\alpha_n) & \cdots & \sigma_{r+s}(\alpha_n) & \overline{\sigma_{r+s}}(\alpha_n) \end{vmatrix}$$

$$= 2 \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) - i \operatorname{Im}\sigma_{r+1}(\alpha_1) & \cdots & \sigma_{r+s}(\alpha_1) & \overline{\sigma_{r+s}}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) - i \operatorname{Im}\sigma_{r+1}(\alpha_n) & \cdots & \sigma_{r+s}(\alpha_n) & \overline{\sigma_{r+s}}(\alpha_n) \end{vmatrix}$$

$$= 2 \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) & -i\operatorname{Im}\sigma_{r+1}(\alpha_1) & \cdots & \sigma_{r+s}(\alpha_1) & \overline{\sigma_{r+s}}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) & -i\operatorname{Im}\sigma_{r+1}(\alpha_n) & \cdots & \sigma_{r+s}(\alpha_n) & \overline{\sigma_{r+s}}(\alpha_n) \end{vmatrix}$$

$$= -2i \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) & \operatorname{Im}\sigma_{r+1}(\alpha_1) & \cdots & \sigma_{r+s}(\alpha_1) & \overline{\sigma_{r+s}}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) & \operatorname{Im}\sigma_{r+1}(\alpha_n) & \cdots & \sigma_{r+s}(\alpha_n) & \overline{\sigma_{r+s}}(\alpha_n) \end{vmatrix}$$

$$= \cdots = (-2i)^s \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) & \operatorname{Im}\sigma_{r+1}(\alpha_1) & \cdots & \operatorname{Re}\sigma_{r+s}(\alpha_1) & \operatorname{Im}\sigma_{r+s}(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) & \operatorname{Im}\sigma_{r+1}(\alpha_n) & \cdots & \operatorname{Re}\sigma_{r+s}(\alpha_n) & \operatorname{Im}\sigma_{r+s}(\alpha_n) \end{vmatrix}$$

$$= (-2i)^s \det(\sigma(\alpha_1), \dots, \sigma(\alpha_n)),$$

i.e., $\det(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) \neq 0$ which implies the assertion.

23.1.2023

Lemma 126 Let Λ be a lattice in $\mathbb{R}^n$ with $n = r+2s$ (for some $r, s \in \mathbb{N}\cup\{0\}$). If $c_1, \dots, c_{r+s} > 0$ satisfy $c_1 \cdots c_{r+s} > \left(\frac{4}{\pi}\right)^s d(\Lambda)$ then there is an $x = (x_1, \dots, x_n) \in \Lambda \setminus \{0\}$ such that

$$|x_1| < c_1, \dots, |x_r| < c_r, \; x_{r+1}^2 + x_{r+2}^2 < c_{r+1}, \dots, x_{r+2s-1}^2 + x_{r+2s}^2 < c_{r+s}.$$

Proof: Let

$$K = \left\{(x_1, \dots, x_n) \in \mathbb{R}^n \;\middle|\; |x_1| < c_1, \dots, |x_r| < c_r, \; x_{r+1}^2 + x_{r+2}^2 < c_{r+1}, \dots, x_{r+2s-1}^2 + x_{r+2s}^2 < c_{r+s}\right\}.$$

Then K is bounded, convex and symmetric about the origin and has Jordan measure

$v(K) = (2c_1)\cdots(2c_r)(\pi c_{r+1})\cdots(\pi c_{r+s}) = 2^r \pi^s c_1 \cdots c_{r+s}$. As

$$v(K) > 2^{r+2s} d(\Lambda) \iff 2^r \pi^s c_1 \cdots c_{r+s} > 2^{r+2s} d(\Lambda) \iff c_1 \cdots c_{r+s} > \frac{2^{2s}}{\pi^s} d(\Lambda)$$

the assertion follows by Theorem 124.

Definition: Let K be an algebraic number field. Let

$\mathcal{F}_K := \{M \mid M$ is a fractional ideal of K, $M \neq \{0\}\}$ (which appeared already in Lemma 92(v) and Theorem 97),

$\mathcal{P}_K := \left\{\frac{1}{\alpha}(\beta) \;\middle|\; \alpha, \beta \in \mathcal{O}_K \setminus \{0\}\right\}$ (i.e., the subgroup of principal fractional ideals),

$\mathcal{H}_K := \mathcal{F}_K / \mathcal{P}_K$ (i.e., the quotient group of $\mathcal{F}_K$ by $\mathcal{P}_K$) and $h_K := |\mathcal{F}_K / \mathcal{P}_K|$ (i.e., the order of $\mathcal{H}_K$).

The group $\mathcal{H}_K$ is called the ideal class group of K and h_K the class number of K.

If $M \neq (0)$ is a fractional ideal of K, the notation $[M]$ will denote the coset $M\mathcal{P}_K =: [M]$ and is called an ideal class.

Remarks: 1) We will show that $\mathcal{H}_K$ is always a finite group, i.e., $h_K \in \mathbb{N}$.

2) The map $\mathcal{F}_K \to \mathcal{H}_K = \mathcal{F}_K/\mathcal{P}_K$, $M \mapsto [M]$ is a group homomorphism. Therefore, if $M, N (\neq \{0\})$ are fractional ideals of K, we have $[M\cdot N] = [M]\cdot[N]$ and $[M]^{-1} = [M^{-1}]$.

3) The identity element of $\mathcal{H}_K$ is the ideal class $[\mathcal{O}_K] = [(1)] = [(\alpha)]$ $\forall \alpha \in \mathcal{O}_K \setminus \{0\}$.

Lemma 127 Let K be an algebraic number field and $M (\neq \{0\})$ a fractional ideal of K. Then there is an integral ideal $I (\neq (0))$ of $\mathcal{O}_K$ such that $[I] = [M]$.

Proof: Let $M = \alpha^{-1} I$ (where $\alpha \in \mathcal{O}_K \setminus \{0\}$ and $I \neq (0)$ is an integral ideal). Then $I = \alpha M = (\alpha) M$ and therefore $[I] = [M]$ (as $(\alpha) \in P_K$).

Theorem 128 Let K be an algebraic number field. Then the following are equivalent:

(i) $\mathcal{O}_K$ is a unique factorization domain,

(ii) $h_K = 1$.

Proof: $\mathcal{O}_K$ is a unique factorization domain $\overset{\text{Th 121}}{\Longleftrightarrow}$ $\mathcal{O}_K$ is a principal ideal domain $\Longleftrightarrow$ $\mathcal{F}_K = P_K$ $\Longleftrightarrow$ $h_K = 1$

Theorem 129 Let K be an algebraic number field with $[K:\mathbb{Q}] = n = r + 2s$. If $I \neq (0)$ is an ideal of $\mathcal{O}_K$ then $\sigma(I)$ is a lattice in $\mathbb{R}^n$ with lattice constant $d(\sigma(I)) = 2^{-s} N(I) \sqrt{|d_K|}$.

Proof: By Theorem 86 I has a $\mathbb{Z}$-basis $\{\alpha_1, \dots, \alpha_n\}$, which is also a basis of K as a $\mathbb{Q}$-vector space. Because of Theorem 125 $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ are linearly independent over $\mathbb{R}$. As $\sigma : (K,+) \to (\mathbb{R}^n, +)$ is a group homomorphism, we get that $\sigma(I) = \sigma(\mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n) = \mathbb{Z}\sigma(\alpha_1) + \dots + \mathbb{Z}\sigma(\alpha_n)$ is a lattice. Using the proof of Theorem 125 we get

$$d(\sigma(I)) = \left| \det(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) \right|$$

$$= 2^{-s} \left| \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \sigma_{r+1}(\alpha_1) & \overline{\sigma_{r+1}(\alpha_1)} & \cdots & \sigma_{r+s}(\alpha_1) & \overline{\sigma_{r+s}(\alpha_1)} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \sigma_{r+1}(\alpha_n) & \overline{\sigma_{r+1}(\alpha_n)} & \cdots & \sigma_{r+s}(\alpha_n) & \overline{\sigma_{r+s}(\alpha_n)} \end{pmatrix} \right|$$

$$\overset{\text{Th 110}}{=} 2^{-s} \sqrt{|\Delta_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n)|} = 2^{-s} N(I) \sqrt{|d_K|}.$$

Theorem 130 Let K be an algebraic number field with $[K:\mathbb{Q}] = n = r + 2s$. If $I \neq (0)$ is an ideal of $\mathcal{O}_K$ then there is an $\alpha \in I \setminus \{0\}$ such that $|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|}$.

Proof: Let $\varepsilon > 0$. Choose $c_1, \dots, c_{r+s} > 0$ such that $c_1 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|} + \varepsilon$. By Theorem 129 $\sigma(I)$ is a lattice with lattice constant $d(\sigma(I)) = 2^{-s} N(I) \sqrt{|d_K|}$ and therefore $\frac{4^s}{\pi^s} d(\sigma(I)) = \left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|} < c_1 \cdots c_{r+s}$. By Lemma 126 there is an $\alpha \in I \setminus \{0\}$ (and thus $\sigma(\alpha) \in \sigma(I) \setminus \{0\}$) satisfying

$$|\sigma_1(\alpha)| < c_1, \dots, |\sigma_r(\alpha)| < c_r, |\sigma_{r+1}(\alpha)|^2 = (\operatorname{Re} \sigma_{r+1}(\alpha))^2 + (\operatorname{Im} \sigma_{r+1}(\alpha))^2 < c_{r+1}, \dots$$

$$\dots, |\sigma_{r+s}(\alpha)|^2 = (\operatorname{Re} \sigma_{r+s}(\alpha))^2 + (\operatorname{Im} \sigma_{r+s}(\alpha))^2 < c_{r+s}$$

which implies

$$|N_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha) \cdots \sigma_r(\alpha) \sigma_{r+1}(\alpha) \overline{\sigma_{r+1}(\alpha)} \cdots \sigma_{r+s}(\alpha) \overline{\sigma_{r+s}(\alpha)}|$$

$$= |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)| \, |\sigma_{r+1}(\alpha)|^2 \cdots |\sigma_{r+s}(\alpha)|^2 < c_1 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|} + \varepsilon.$$

Now choose $\varepsilon > 0$ so small that $\left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|} + \varepsilon < \left[\left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|}\right] + 1$.

As $|N_{K/\mathbb{Q}}(\alpha)| \in \mathbb{N}$ the inequality $|N_{K/\mathbb{Q}}(\alpha)| < \left[\left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|}\right] + 1$ implies

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left[\left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|}\right] \leq \left(\frac{2}{\pi}\right)^s N(I) \sqrt{|d_K|}.$$

Corollary 131 Let K be an algebraic number field and $I \neq (0)$ an ideal of $\mathcal{O}_K$. Then there is an ideal $J \neq (0)$ of $\mathcal{O}_K$ such that $[J] = [I]$ and $N(J) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$.

Proof: By Lemma 127 there is an integral ideal $\tilde{J} \neq (0)$ such that $[I^{-1}] = [\tilde{J}]$. By Theorem 130 there is an $\alpha \in \tilde{J} \setminus \{0\}$ such that $|N_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s N(\tilde{J}) \sqrt{|d_K|}$. As $\tilde{J} \mid (\alpha)$ there is an integral ideal $J \neq (0)$ such that $J\tilde{J} = (\alpha)$. Therefore $|N_{K|\mathbb{Q}}(\alpha)| = N((\alpha)) = N(J)N(\tilde{J})$. This implies $N(J)N(\tilde{J}) = |N_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s N(\tilde{J}) \sqrt{|d_K|}$ and thus $N(J) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Finally, we have

$$[J] = [\tilde{J}^{-1}] = [I].$$

Lemma 132 Let K be an algebraic number field.

(i) Let $I \neq (0)$ be an ideal of $\mathcal{O}_K$. There are only finitely many ideals J of $\mathcal{O}_K$ such that $J \mid I$,

(ii) Let $k \in \mathbb{Z} \setminus \{0\}$. There are only finitely many ideals J of $\mathcal{O}_K$ such that $k \in J$,

(iii) Let $k \in \mathbb{N}$. There are only finitely many ideals J of $\mathcal{O}_K$ such that $N(J) = k$.

Proof: (i) Let $I = P_1^{\alpha_1} \cdots P_\ell^{\alpha_\ell}$ be the factorization of I into prime ideals. Then $\{J \mid J \text{ is ideal of } \mathcal{O}_K, J \mid I\} = \left\{P_1^{\beta_1} \cdots P_\ell^{\beta_\ell} \mid 0 \leq \beta_i \leq \alpha_i \text{ for } 1 \leq i \leq \ell\right\}$ is finite.

(ii) Follows from (i) as $k \in J \iff (k) \subseteq J \iff J \mid (k)$.

(iii) By Theorem 116 (iii) $N(J) = k$ implies $k \in J$ and the assertion follows from (ii).

Theorem 133 For every algebraic number field K the ideal class group $\mathcal{H}_K$ is finite, i.e., $h_K \in \mathbb{N}$.

Proof: Let $[K:\mathbb{Q}] = n+2s$ and let $M \neq \{0\}$ be a fractional ideal of K. By Lemma 127 there is an integral ideal I with $[I] = [M]$. By Corollary 131 there is an integral ideal J such that $[J] = [I]$ $(= [M])$ and $N(J) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Because of Lemma 132 (iii) there are only finitely many integral ideals J with that property.

Corollary 134 Let K be an algebraic number field and $I \neq (0)$ an ideal of $\mathcal{O}_K$.

(i) I^{h_K} is a principal ideal,

(ii) If p is prime such that $p \nmid h_K$ and I^p is a principal ideal then I is a principal ideal.

Proof: (i) Follows from $[I^{h_K}] = [I]^{h_K} = [\mathcal{O}_K] = [(1)]$.

(ii) As $\gcd(p, h_K) = 1$ there are $x, y \in \mathbb{Z}$ such that $px + h_K y = 1$. As I^p is a principal ideal we have $[I]^p = [I^p] = [\mathcal{O}_K]$. As $[I] = [I]^{px + h_K y} = ([I]^p)^x ([I]^{h_K})^y = [\mathcal{O}_K]^x [\mathcal{O}_K]^y = [\mathcal{O}_K]^2 = [\mathcal{O}_K]$ we get that I is a principal ideal.

Definition: Let K be an algebraic number field. The quantity $M_K := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$ is called Minkowski bound.

Remark: Using better estimates Corollary 131 can be improved to show the following: For every fractional ideal $M \neq \{0\}$ of K there is an integral ideal $I \neq (0)$ such that $[I] = [M]$ and $N(I) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}$. As $N(I) \geq 1$ and $s \leq \frac{n}{2}$ this yields $1 \leq \left(\frac{4}{\pi}\right)^{n/2} \frac{n!}{n^n} \sqrt{|d_K|}$ and therefore $\sqrt{|d_K|} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}$. This in turn leads to the following results:

- $|d_K| > 1$ for all algebraic number fields $K \neq \mathbb{Q}$ (Minkowski)

• Let $k \in \mathbb{Z}$. There are only finitely many algebraic number fields K such that $d_K = k$. (Hermite) 23.1.2023

Algorithm to find the ideal class group $\mathcal{H}_K$ of an algebraic number field K

The input is an algebraic number field K and the quantities $n = [K:\mathbb{Q}]$, r, s and d_K.
By Corollary 131 it is sufficient to consider integral ideals $I \neq (0)$ with $N(I) \leq M_K$.
If $I \neq (0)$ is an ideal with $N(I) \leq M_K$ and P a prime ideal with $P \mid I$ then $N(P) \leq M_K$.
If $P \neq (0)$ is prime ideal with $N(P) \leq M_K$ and $N(P) = p^f$ (with p a prime) then $p \leq M_K$.

1. Determine all primes $p \leq M_K$.
2. For each prime $p \leq M_K$ determine the factorization of $(p) = p\mathcal{O}_K$ into prime ideals.
3. Determine all products of prime ideals found in step 2 having norm $\leq M_K$.
4. The set of ideals determined in step 3 contains generators of $\mathcal{H}_K$ which are determined.

If, for every prime $p \leq M_K$, the factorization of $(p) = p\mathcal{O}_K$ contains only prime ideals that are principal ideals of $\mathcal{O}_K$, we have $h_K = 1$.

Corollary 135 If $K = \mathbb{Q}(i\sqrt{19})$ then $h_K = 1$, i.e., $\mathcal{O}_{\mathbb{Q}(i\sqrt{19})} = \mathbb{Z}\left[\frac{1}{2}(1+i\sqrt{19})\right]$ is a principal ideal domain.

Proof: As $n=2$, $r=0$, $s=1$ and $d_K = -19$ we have $M_K = \frac{2\sqrt{19}}{\pi} = 2{,}774\ldots$ The only prime $\leq M_K$ is 2. By Theorem 119 the prime 2 is inert (as $-19 \equiv 5 \pmod 8$), i.e., (2) is a prime ideal and $h_K = 1$ by the remark above

Corollary 136 If $K = \mathbb{Q}(i\sqrt{163})$ then $h_K = 1$, i.e., $\mathcal{O}_{\mathbb{Q}(i\sqrt{163})} = \mathbb{Z}\left[\frac{1}{2}(1+i\sqrt{163})\right]$ is a principal ideal domain.

Proof: As $n=2$, $r=0$, $s=1$ and $d_K = -163$ we have $M_K = \frac{2\sqrt{163}}{\pi} = 8{,}127\ldots$ The primes $\leq M_K$ are 2, 3, 5 and 7. By Theorem 119 the prime 2 is inert (as $-163 \equiv 5 \pmod 8$) and the primes 3, 5 and 7 are inert (as $\left(\frac{-163}{3}\right) = \left(\frac{-163}{5}\right) = \left(\frac{-163}{7}\right) = -1$), i.e., (2), (3), (5) and (7) are all prime ideals and $h_K = 1$ by the remark above.

Remark: Both $\mathbb{Z}\left[\frac{1}{2}(1+i\sqrt{19})\right]$ and $\mathbb{Z}\left[\frac{1}{2}(1+i\sqrt{163})\right]$ are therefore principal ideal domains but not euclidean domains (by Theorem 77 and Corollaries 135 and 136).

Corollary 137 If $K = \mathbb{Q}(i\sqrt{5})$ then $h_K = 2$ (and therefore $(\mathcal{H}_K, \cdot) \cong (\mathbb{Z}/2\mathbb{Z}, +)$).

Proof: As $n=2$, $r=0$, $s=1$ and $d_K = -20$ we have $M_K = \frac{2\sqrt{20}}{\pi} = \frac{4\sqrt{5}}{\pi} = 2{,}847\ldots$ The only prime $\leq M_K$ is 2. By Theorem 119 the prime 2 ramifies (as $-5 \equiv 3 \pmod 4$) and $(2) = (2, 1+i\sqrt{5})^2$ where $P = (2, 1+i\sqrt{5})$ is a prime ideal with $N(P) = 2$. Clearly P is the only ideal $(\neq (1))$ whose norm is $\leq M_K$. If P were a principal ideal, $\mathcal{O}_K$ would be a unique factorization domain (which contradicts Theorem 76). Therefore $\mathcal{H}_K = \left\{[(1)], [(2, 1+i\sqrt{5})]\right\}$.

Remarks: 1) Dirichlet has given formulae for the class number h_K of a quadratic number field K:

$$h_K = -\frac{w_K}{2|d_K|} \sum_{1 \leq r < |d_K|} r \left(\frac{d_K}{r}\right) \quad \text{if } d_K < 0 \text{ (i.e., } K \text{ is an imaginary quadratic field)}$$

and

$$h_K = -\frac{1}{\log \eta} \sum_{1 \leq r < \frac{d_K}{2}} \left(\frac{d_K}{r}\right) \log\left(\sin \frac{\pi r}{d_K}\right) \quad \text{if } d_K > 0 \text{ (i.e., } K \text{ is a real quadratic field).}$$

Here

$$w_k = |\mathcal{O}^*_{\mathbb{Q}(\sqrt{d_k})}| = \begin{cases} 6 & \text{if } d_k = -3, \\ 4 & \text{if } d_k = -4, \\ 2 & \text{if } d_k < -4, \end{cases}$$

$\left(\frac{d_k}{\nu}\right)$ denotes (an extension of) the Kronecker symbol and $\eta > 1$ the fundamental unit, i.e., $\mathcal{O}_k^* = \{\pm \eta^k \mid k \in \mathbb{Z}\}$. This is a special case of an analytic class number formula that holds for all algebraic number fields.

2) We have $\lim_{|d_k| \to \infty} \frac{\log h_k}{\log |d_k|} = \frac{1}{2}$ for imaginary quadratic fields. This implies that $h_k = 1$ holds for only finitely many imaginary quadratic fields.