CHAPTER 4

Class Group and Class Number

4.1. Fractional Ideals

Suppose that K is an algebraic number field, with ring of integers $\mathfrak{O}$. A subset $\mathfrak{g}$ of K is a fractional ideal in K if the following two conditions are satisfied:

(i) If $\alpha, \beta \in \mathfrak{g}$, then $\lambda\alpha + \mu\beta \in \mathfrak{g}$ for every $\lambda, \mu \in \mathfrak{O}$.
(ii) There exists $m \in \mathbb{N}$ such that $m\alpha \in \mathfrak{O}$ for every $\alpha \in \mathfrak{g}$.

Note that ideals in K are also fractional ideals in K, so that this is a generalization of the notion of ideals in K.

THEOREM 4.1. *Every fractional ideal $\mathfrak{g}$ in an algebraic number field K is of the form*

$$\mathfrak{g} = \langle \alpha_1, \ldots, \alpha_s \rangle, \quad \alpha_1, \ldots, \alpha_s \in \mathfrak{g}.$$

In other words, $\mathfrak{g}$ is the range of values of a linear form $\lambda_1\alpha_1 + \ldots + \lambda_s\alpha_s$, where $\lambda_1, \ldots, \lambda_s \in \mathfrak{O}$, the ring of integers in K, and $\alpha_1, \ldots, \alpha_s \in \mathfrak{g}$.

PROOF. Let $m \in \mathbb{N}$ be chosen to satisfy (ii) above. Then the set $\mathfrak{a} = \{m\alpha : \alpha \in \mathfrak{g}\}$ is an ideal in K. Let $\mathfrak{a} = \langle \gamma_1, \ldots, \gamma_s \rangle$. Clearly $\mathfrak{g} = \langle \gamma_1/m, \ldots, \gamma_s/m \rangle$. ◯

If $\mathfrak{g} = \langle \alpha_1, \ldots, \alpha_s \rangle$, then we say that the fractional ideal $\mathfrak{g}$ is generated by $\alpha_1, \ldots, \alpha_s$. We also say that a fractional ideal in an algebraic number field K is principal if it is generated by a single element.

We can also define $\mathbb{Z}$-basis for fractional ideals in an algebraic number field in the obvious way. In the notation of the proof of Theorem 4.1, if $\{\gamma_1, \ldots, \gamma_s\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$, then $\{\gamma_1/m, \ldots, \gamma_s/m\}$ is obviously a $\mathbb{Z}$-basis for $\mathfrak{g}$.

Suppose that $\mathfrak{g} = \langle \alpha_1, \ldots, \alpha_s \rangle$ and $\mathfrak{h} = \langle \beta_1, \ldots, \beta_t \rangle$ are fractional ideals in an algebraic number field K. Then the fractional ideal

$$\mathfrak{gh} = \langle \alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_s\beta_t \rangle$$

is called the product of $\mathfrak{g}$ and $\mathfrak{h}$.

It is obvious that every non-zero fractional ideal $\mathfrak{g}$ in an algebraic number field K can be made into an ideal in K by multiplication by a suitable ideal $\langle m \rangle$, where $m \in \mathbb{N}$. Consequently, in view of Theorem 3.5, $\mathfrak{g}$ can be made into a principal ideal in K. The result below follows in analogy to Theorem 3.6(i).

THEOREM 4.2. *Suppose that $\mathfrak{g}$, $\mathfrak{h}$ and $\mathfrak{k}$ are fractional ideals in an algebraic number field K. Suppose further that $\mathfrak{gh} = \mathfrak{gk}$ and $\mathfrak{g} \neq \langle 0 \rangle$. Then $\mathfrak{h} = \mathfrak{k}$.*

THEOREM 4.3. *Suppose that $\mathfrak{g}$ and $\mathfrak{h}$ are fractional ideals in an algebraic number field K. Suppose further that $\mathfrak{g} \neq \langle 0 \rangle$. Then there exists a unique fractional ideal $\mathfrak{r}$ such that $\mathfrak{gr} = \mathfrak{h}$.*

We call the fractional ideal $\mathfrak{r}$ in Theorem 4.3 the quotient of $\mathfrak{h}$ and $\mathfrak{g}$, and write $\mathfrak{r} = \mathfrak{h}/\mathfrak{g}$.

PROOF OF THEOREM 4.3. We choose a non-zero ideal $\mathfrak{a}$ in K such that $\mathfrak{ag} = \langle m \rangle$, where $m \in \mathbb{N}$, is principal. If $\mathfrak{ah} = \langle \rho_1, \ldots, \rho_t \rangle$, let $\mathfrak{r} = \langle \rho_1/m, \ldots, \rho_t/m \rangle$. Then $\mathfrak{ah} = \langle m \rangle \mathfrak{r} = \mathfrak{agr}$, so that $\mathfrak{h} = \mathfrak{gr}$ by Theorem 4.2. To show uniqueness, note that if $\mathfrak{h} = \mathfrak{gs}$ for some fractional ideal $\mathfrak{s}$ in K, then $\mathfrak{gr} = \mathfrak{gs}$, and so $\mathfrak{r} = \mathfrak{s}$ by Theorem 4.2. ◯

A consequence of the above is that every fractional ideal in an algebraic number field K can be expressed as the quotient of two relatively prime ideals in K.

Suppose that $\mathfrak{g}$ and $\mathfrak{h}$ are fractional ideals in an algebraic number field K. We say that $\mathfrak{g}$ divides $\mathfrak{h}$, denoted by $\mathfrak{g} \mid \mathfrak{h}$, if $\mathfrak{h}/\mathfrak{g}$ is an ideal in K.

Suppose that $\mathfrak{g}$ is a fractional ideal in an algebraic number field K. Suppose further that $\mathfrak{g} = \mathfrak{a}/\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime ideals in K. We define the norm of $\mathfrak{g}$, denoted by $N(\mathfrak{g})$, by $N(\mathfrak{g}) = N(\mathfrak{a})/N(\mathfrak{b})$. It is clear that this remains valid even when $\mathfrak{a}$ and $\mathfrak{b}$ are not relatively prime. Note also that $N(\mathfrak{gh}) = N(\mathfrak{g})N(\mathfrak{h})$ for all fractional ideals $\mathfrak{g}$ and $\mathfrak{h}$ in K. It is also not difficult to establish the following analogue of Theorem 3.20.

THEOREM 4.4. *Suppose that $\mathfrak{g}$ is a non-zero fractional ideal in an algebraic number field K, and that $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{g}$. Then*

$$N(\mathfrak{g}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{\frac{1}{2}},$$

where Δ is the discriminant of K.

4.2. Some Geometric Input

Whereas everything up to now has depended on the concept of divisibility and algebraic processes, the concept of magnitude now plays a crucial rôle in the further development of algebraic number theory. We next establish a result related to Minkowski's work on the geometry of numbers.

THEOREM 4.5 (Minkowski's theorem on linear forms). *Suppose that*

$$F_i(\mathbf{x}) = \sum_{j=1}^{n} a_{ij} x_j,$$

where $i = 1, \ldots, n$ and $\mathbf{x} = (x_1, \ldots, x_n)$, are linear forms with real coefficients a_{ij} and with non-zero determinant $D = |(a_{ij})|$. Suppose further that $c_1, \ldots, c_n$ are positive numbers such that $c_1 \ldots c_n \geqslant |D|$. Then there exists $\mathbf{x} \in \mathbb{Z}^n$, different from $\mathbf{0} = (0, \ldots, 0)$, such that for every $i = 1, \ldots, n$, we have

$$|F_i(\mathbf{x})| \leqslant c_i. \tag{4.1}$$

PROOF. We establish he result by contradiction.

(i) Consider a parallelotope

$$\mathcal{P}(\mathbf{0}) = \{\mathbf{x} \in \mathbb{R}^n : |F_i(\mathbf{x})| \leqslant \tfrac{1}{2} c_i,\ i = 1, \ldots, n\},$$

centred at $\mathbf{0}$. For $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{Z}^n$, let

$$\mathcal{P}(\mathbf{b}) = \{\mathbf{x} \in \mathbb{R}^n : |F_i(\mathbf{x} - \mathbf{b})| \leqslant \tfrac{1}{2} c_i,\ i = 1, \ldots, n\}. \tag{4.2}$$

Note that $\mathcal{P}(\mathbf{b})$ is obtained from $\mathcal{P}(\mathbf{0})$ through a translation by a vector $\mathbf{b}$. Suppose, on the contrary, that no $\mathbf{x} \in \mathbb{Z}^n$ such that $\mathbf{x} \neq \mathbf{0}$ satisfies (4.1) simultaneously for every $i = 1, \ldots, n$. We claim that no two parallelotopes of the form (4.2), where $\mathbf{b} \in \mathbb{Z}^n$, have a point in common. Indeed, if $\mathbf{x} \in \mathcal{P}(\mathbf{b}') \cap \mathcal{P}(\mathbf{b}'')$, then it follows from

$$-\tfrac{1}{2} c_i \leqslant F_i(\mathbf{x} - \mathbf{b}') \leqslant \tfrac{1}{2} c_i \quad \text{and} \quad -\tfrac{1}{2} c_i \leqslant F_i(\mathbf{x} - \mathbf{b}'') \leqslant \tfrac{1}{2} c_i$$

that $|F_i(\mathbf{b}' - \mathbf{b}'')| \leqslant c_i$ for every $i = 1, \ldots, n$. Consequently, $\mathbf{b}' - \mathbf{b}''$ satisfies (4.1) simultaneously for every $i = 1, \ldots, n$.

(ii) Let V denote the n-dimensional volume of $\mathcal{P}(\mathbf{0})$, and hence of $\mathcal{P}(\mathbf{b})$ for every $\mathbf{b} \in \mathbb{Z}^n$. We next show that $V \leqslant 1$. Let $c > 0$ be a constant such that $\mathcal{P}(\mathbf{0}) \subseteq [-c, c]^n$. Consider a set of the form $[-L, L]^n$, where $L \in \mathbb{N}$ is "large" compared to c. The number of integer lattice points $\mathbf{b} \in \mathbb{Z}^n \cap [-L, L]^n$ is precisely $(2L + 1)^n$. Also, the total n-dimensional volume of $\mathcal{P}(\mathbf{b})$ over these values of $\mathbf{b}$ does not exceed the volume of $[-L - c, L + c]^n$. In other words, we must have

$$(2L + 1)^n V \leqslant (2L + 2c)^n. \tag{4.3}$$

The inequality $V \leqslant 1$ follows immediately on dividing both sides of (4.3) by L^n and letting $L \to \infty$.

(iii) We next express V in terms of the determinant D and $c_1, \ldots, c_n$. We have

$$V = \int\limits_{\substack{F_i(\mathbf{x}) \leqslant \frac{1}{2}c_i \\ i=1,\ldots,n}} \ldots \int\limits \mathrm{d}x_1 \ldots \mathrm{d}x_n = \frac{1}{|D|} \int\limits_{\substack{|y_i| \leqslant \frac{1}{2}c_i \\ i=1,\ldots,n}} \ldots \int\limits \mathrm{d}y_1 \ldots \mathrm{d}y_n = \frac{c_1 \ldots c_n}{|D|}.$$

It now follows that $c_1 \ldots c_n \leqslant |D|$.

(iv) To obtain a contradiction, we need to deduce that $c_1 \ldots c_n < |D|$. To achieve this, we apply continuity arguments. Suppose that no $\mathbf{x} \in \mathbb{Z}^n$ such that $\mathbf{x} \neq \mathbf{0}$ satisfies (4.1) simultaneously for every $i = 1, \ldots, n$. By continuity, there exist $\epsilon_i > 0$, $i = 1, \ldots, n$, such that no $\mathbf{x} \in \mathbb{Z}^n$ such that $\mathbf{x} \neq \mathbf{0}$ satisfies $|F_i(\mathbf{x})| \leqslant c_i + \epsilon_i$ simultaneously for every $i = 1, \ldots, n$. Hence $(c_1 + \epsilon_1) \ldots (c_n + \epsilon_n) \leqslant |D|$. This gives $c_1 \ldots c_n < |D|$, and we have the required contradiction. ◯

We use a somewhat modified version of this result.

THEOREM 4.6. *Suppose that the linear forms*

$$F_i(\mathbf{x}) = \sum_{j=1}^{n} a_{ij} x_j, \tag{4.4}$$

where $i = 1, \ldots, n$ and $\mathbf{x} = (x_1, \ldots, x_n)$, and positive numbers $c_1, \ldots, c_n$ satisfy the following four conditions:

(i) *The coefficients a_{ij} are complex and the determinant $D = |(a_{ij})|$ is non-zero.*
(ii) *If one of the linear forms is not real, then its complex conjugate, i.e. the linear form obtained by replacing every coefficient by its complex conjugate, also occurs among the collection.*
(iii) *If the linear forms $F_\alpha(\mathbf{x})$ abd $F_\beta(\mathbf{x})$ are complex conjugates, then $c_\alpha = c_\beta$.*
(iv) *We have $c_1 \ldots c_n \geqslant |D|$.*

Then there exists $\mathbf{x} \in \mathbb{Z}^n$, different from $\mathbf{0} = (0, \ldots, 0)$, such that $|F_i(\mathbf{x})| \leqslant c_i$ for every $i = 1, \ldots, n$.

PROOF. We construct real linear forms from the system (4.4), where $i = 1, \ldots, n$. If $F_i(\mathbf{x})$ is a real linear form, then we write $G_i(\mathbf{x}) = F_i(\mathbf{x})$, and let $d_i = c_i$. If $F_\alpha(\mathbf{x})$ is not real, let $F_\beta(\mathbf{x})$ denote its complex conjugate, and we write

$$G_\alpha(\mathbf{x}) = \frac{F_\alpha(\mathbf{x}) + F_\beta(\mathbf{x})}{2} \quad \text{and} \quad G_\beta(\mathbf{x}) = \frac{F_\alpha(\mathbf{x}) - F_\beta(\mathbf{x})}{2\mathrm{i}},$$

and let $d_\alpha = d_\beta = c_\alpha/\sqrt{2}$. The system of real linear forms $G_i(\mathbf{x})$, where $i = 1, \ldots, n$, now has determinant D' satisfying $|D'| = 2^{-t}|D|$, where t denotes the number of pairs of complex conjugate forms $F_i(\mathbf{x})$. Clearly $d_1 \ldots d_n \geqslant |D'|$. It now follows from Theorem 4.5 that there exists $\mathbf{x} \in \mathbb{Z}^n$, different from $\mathbf{0} = (0, \ldots, 0)$, such that $|G_i(\mathbf{x})| \leqslant d_i$ for every $i = 1, \ldots, n$. Clearly, if $F_\alpha(\mathbf{x})$ is not real, with conjugate form $F_\beta(\mathbf{x})$, we have

$$|F_\alpha(\mathbf{x})|^2 = |G_\alpha(\mathbf{x})|^2 + |G_\beta(\mathbf{x})|^2 \leqslant d_\alpha^2 + d_\beta^2 = c_\alpha^2.$$

The result follows. ◯

4.3. Ideal Classes

Suppose that K is an algebraic number field. Two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ in K are said to be equivalent, denoted by $\mathfrak{a} \sim \mathfrak{b}$, if there is a principal fractional ideal $\langle w \rangle \neq \langle 0 \rangle$ such that $\mathfrak{a} = \langle w \rangle \mathfrak{b}$.

We immediately have the following result.

THEOREM 4.7. *Suppose that $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ are non-zero fractional ideals in an algebraic number field K. Then*

(i) $\mathfrak{a} \sim \mathfrak{a}$;
(ii) *if $\mathfrak{a} \sim \mathfrak{b}$, then $\mathfrak{b} \sim \mathfrak{a}$;*
(iii) *if $\mathfrak{a} \sim \mathfrak{b}$ and $\mathfrak{b} \sim \mathfrak{c}$, then $\mathfrak{a} \sim \mathfrak{c}$;*
(iv) *if $\mathfrak{a} \sim \mathfrak{b}$, then $\mathfrak{ac} \sim \mathfrak{bc}$; and*
(v) *if $\mathfrak{ac} \sim \mathfrak{bc}$ and $\mathfrak{c} \neq \langle 0 \rangle$, then $\mathfrak{a} \sim \mathfrak{b}$.*

Conditions (i)–(iii) above imply that the equivalence of non-zero fractional ideals in an algebraic number field is an equivalence relation. The equivalence classes are called the ideal classes. Furthermore, all non-zero principal fractional ideals are equivalent to each other. They form the principal class.

On the other hand, it follows from conditions (iv) and (v) above that the equivalence classes, or ideal classes, can be made into an abelian group in the following way: If $[\mathfrak{a}]$ and $[\mathfrak{b}]$ denote respectively the idral classes containing the fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$, then $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$. This abelian group is called the class group of the algebraic number field K. The unit element is clearly the principal class.

REMARK. The passage from ideals to ideal classes is the analogue of the passage from integers to residue classes with respect to a given modulus. The collection of all non-zero fractional ideals in an algebraic number field K forms an infinite abelian group $\mathfrak{F}$ under multiplication. Clearly $\mathfrak{F}$ contains the subgroup $\mathfrak{P}$ of all non-zero principal fractional ideals in K. The class group of K is in fact the factor group $\mathfrak{F}/\mathfrak{P}$, whose elements are the different cosets consisting of fractional ideals in K which differ only by an element of $\mathfrak{P}$, *i.e.* a non-zero principal fractional ideal in K.

The class number h of an algebraic number field K is the order of the class group of K.

Our main task in this section is to establish the following important result.

THEOREM 4.8. *Suppose that K is an algebraic number field. Then every ideal class of K contains an (integral) ideal $\mathfrak{a}$ such that*

$$N(\mathfrak{a}) \leqslant |\Delta|^{\frac{1}{2}}, \tag{4.5}$$

where Δ is the discriminant of K. Furthermore, the class number H of K is finite.

PROOF. For any ideal class A of K, let $\mathfrak{b}$ be an (integral) ideal in the ideal class A^{-1}, and let $\{\beta_1, \ldots \beta_n\}$ be a $\mathbb{Z}$-basis of $\mathfrak{b}$. For every $j = 1, \ldots, n$, denote by $\beta_j^{(1)}, \ldots, \beta_j^{(n)}$ the K-conjugates of β_j, with the convention that $\beta_j = \beta_j^{(1)}$. Then by Theorem 4.6, there exists $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that $\mathbf{x} \neq \mathbf{0}$ and

$$|w^{(i)}| = \left| \sum_{j=1}^{n} \beta_j^{(i)} x_j \right| \leqslant |\Delta[\beta_1, \ldots \beta_n]|^{\frac{1}{2n}}$$

simultaneously for every $i = 1, \ldots, n$. It follows from Theorem 3.20 that the number

$$w = \beta_1 x_1 + \ldots + \beta_n x_n$$

satisfies

$$|N(w)| = |w^{(1)} \ldots w^{(n)}| \leqslant |\Delta[\beta_1, \ldots, \beta_n]|^{\frac{1}{2}} = N(\mathfrak{b})|\Delta|^{\frac{1}{2}}. \tag{4.6}$$

Clearly $w \in \mathfrak{b}$, so that $\langle w \rangle \subseteq \mathfrak{b}$ and so $\mathfrak{b} \mid \langle w \rangle$. It follows that $\langle w \rangle = \mathfrak{a}\mathfrak{b}$ for some non-zero ideal $\mathfrak{a}$ in K. Clearly $\mathfrak{a}\mathfrak{b} \sim \langle 1 \rangle$, so that $\mathfrak{a} \in A$. By Theorem 3.22, we have $N(\mathfrak{a})N(\mathfrak{b}) = N(\langle w \rangle) = |N(w)|$, so it follows from (4.6) that $N(\mathfrak{a}) \leqslant |\Delta|^{\frac{1}{2}}$, proving the first assertion. To complete the proof, recall first Theorem 3.25(iii), that there are only finitely many ideals in K of a given norm. Since these norms are natural numbers, there are only finitely many ideals $\mathfrak{a}$ in K that satisfy (4.5). Hence the number h of distinct ideal classes in K is finite. ◯

4.4. Consequences of the Finiteness of the Class Number

A little basic group theory enables us to establish the following result.

THEOREM 4.9. *Suppose that K is an algebraic number field with class number h, and that $\mathfrak{a}$ is an ideal in K. Then*

(i) *$\mathfrak{a}^h$ is principal; and*
(ii) *$\mathfrak{a}$ is principal if $\mathfrak{a}^q$ is principal for some natural number q prime to h.*

PROOF. (i) Since h is the order of the class group of K, we have $[\mathfrak{a}]^h = [\mathfrak{O}]$, where $\mathfrak{O}$ is the ring of integers in K and $[\mathfrak{O}]$ denotes the principal class. Hence $[\mathfrak{a}^h] = [\mathfrak{O}]$, so that $\mathfrak{a}^h \sim \mathfrak{O}$, and so $\mathfrak{a}^h$ is principal.

(ii) There exist $u, v \in \mathbb{Z}$ such that $qu + hv = 1$. If $\mathfrak{a}^q$ is principal, then $[\mathfrak{a}]^q = [\mathfrak{O}]$, so that

$$[\mathfrak{a}] = [\mathfrak{a}]^{qu+hv} = ([\mathfrak{a}]^q)^u([\mathfrak{a}]^h)^v = [\mathfrak{O}]^u[\mathfrak{O}]^v = [\mathfrak{O}],$$

and so $\mathfrak{a}$ is principal. ◯

The last result in this chapter is a precise description of the brief discussion in Section 3.1.

THEOREM 4.10. *Suppose that K is an algebraic number field, with ring of integers $\mathfrak{O}$. Suppose also that $\mathbb{A}$ denotes the ring of all algebraic integers. For every non-zero ideal $\mathfrak{a}$ in K, there exists $\kappa \in \mathbb{A}$ such that if $\mathfrak{O}'$ is the ring of integers of the extended algebraic number field $K(\kappa)$, then*

(i) $\mathfrak{O}'\langle\kappa\rangle = \mathfrak{O}'\mathfrak{a}$;
(ii) $\mathfrak{O}'\langle\kappa\rangle \cap \mathfrak{O} = \mathfrak{a}$; *and*
(iii) $\mathbb{A}\langle\kappa\rangle \cap K = \mathfrak{a}$.

Furthermore, κ is unique to within units in $\mathbb{A}$.

PROOF. By Theorem 4.9(i), the ideal $\mathfrak{a}^h$ is principal. Suppose that $\mathfrak{a}^h = \langle w\rangle$, where $w \in \mathfrak{O}$. Let κ be a root of the polynomial $t^h - w$. Then $\kappa \in \mathbb{A}$ by Theorem 2.18, and so $\kappa \in \mathfrak{O}'$ also. Hence $\mathfrak{O}'\kappa$ is an ideal in $K(\kappa)$. Note now that viewed within $K(\kappa)$, we have

$$(\mathfrak{O}'\langle\kappa\rangle)^h = \mathfrak{O}'\langle\kappa\rangle^h = \mathfrak{O}'\langle w\rangle = \mathfrak{O}'\mathfrak{a}^h = (\mathfrak{O}'\mathfrak{a})^h.$$

The assertion (i) now follows from uniqueness of factorization in $K(\kappa)$.

On the other hand, assertion (ii) clearly follows from assertion (iii), so we now prove the latter. The inclusion $\mathfrak{a} \subseteq \mathbb{A}\langle\kappa\rangle \cap K$ is obvious. To prove the opposite inclusion, suppose now that $\alpha \in \mathbb{A}\langle\kappa\rangle \cap K$. Since $\alpha \in \mathbb{A}\langle\kappa\rangle$, there exists $\lambda \in \mathbb{A}$ such that $\alpha = \lambda\kappa$, so that $\alpha^h = \lambda^h\kappa^h = \lambda^h w$. In particular, we have $\lambda^h = \alpha^h/w \in K$, so that $\lambda^h \in \mathbb{A} \cap K = \mathfrak{O}$. Note also that $\alpha \in \mathbb{A} \cap K = \mathfrak{O}$. To summarize, we have

$$\alpha^h = \lambda^h w, \quad \alpha, \lambda^h, w \in \mathfrak{O}.$$

Taking ideals in $\mathfrak{O}$, we obtain

$$\langle\alpha\rangle^h = \langle\lambda^h\rangle\langle w\rangle = \langle\lambda^h\rangle\mathfrak{a}^h.$$

It follows immediately from uniqueness of factorization in $\mathfrak{O}$ that $\langle\lambda^h\rangle = \mathfrak{b}^h$ for some ideal $\mathfrak{b}$ in $\mathfrak{O}$, so that $\langle\alpha\rangle^h = \mathfrak{b}^h\mathfrak{a}^h$, and so $\langle\alpha\rangle = \mathfrak{b}\mathfrak{a}$. Hence $\alpha \in \mathfrak{a}$, and this completes the proof of assertion (iii).

Finally, suppose that $\gamma \in \mathbb{A}$ and the ring of integers $\mathfrak{O}''$ of the extended algebraic number field $K(\gamma)$ satisfy conditions analogous to (i), (ii) and (iii) above. In view of Theorem 3.15, write $\mathfrak{a} = \langle\alpha, \beta\rangle$, where $\alpha, \beta \in \mathfrak{O}$. Then $\mathfrak{O}''\langle\gamma\rangle = \mathfrak{O}''\langle\alpha, \beta\rangle$, and so $\gamma = \lambda\alpha + \mu\beta$ for some $\lambda, \mu \in \mathfrak{O}'' \subseteq \mathbb{A}$. But then from (iii), we have $\alpha = \xi\kappa$ and $\beta = \eta\kappa$ for some $\xi, \eta \in \mathbb{A}$. Hence we have $\gamma = \lambda\xi\kappa + \mu\eta\kappa$, and so $\kappa \mid \gamma$ in $\mathbb{A}$. Interchanging the roles of κ and γ, we have $\gamma \mid \kappa$ in $\mathbb{A}$. Hence κ and γ are associates in $\mathbb{A}$. ◯