Algebraic Integers

January 17, 2007

1 The ring of algebraic integers

An algebraic number is called an *algebraic integer* if it is a root of polynomial $x^n + a_1 x^{n-1} + ... + a_n$ with integer coefficients.

Lemma 1.1. *Let γ be any algebraic number. Then there exists a natural number a such that $a\gamma$ is an algebraic integer.*

Proof. We have $a_0\gamma^n + ... + a_n = 0$ for some integers a_i. Multiply by a_o^{n-1}, and get $(a_0\gamma)^n + a_1(a_0\gamma)^{n-1} + ... + a_n a_0^{n-1} = 0$. Hence $a_0\gamma$ is an algebraic integer. □

Lemma 1.2. *Let $\gamma_1, ..., \gamma_n$ be non-zero complex numbers and let M be the $\mathbb{Z}$-module generated by them, i.e. $\{a_1\gamma_1 + ... + a_n\gamma_n$, $a_i \in \mathbb{Z}$. Suppose that α has the property that $\alpha\gamma_i \in M$ for each i. Then α is an algebraic integer.*

Proof. We have $\alpha\gamma_i = \sum c_{i,j}\gamma_j$ for every i and some integers $c_{i,j}$. Hence γ_i are the solutions of the system of linear equations $C\vec{\gamma} - \alpha\vec{\gamma} = 0$ where $\vec{\gamma} = [\gamma_1, ..., \gamma_n]$, $C = [[c_{i,j}]]$ Therefore the determinant $\det(C - \alpha I)$ is 0. That determinant is a polynomial in α with integer coefficients and the highest coefficient 1. □

Theorem 1.3. *The set of algebraic integers is a ring.*

Proof. Let α be a root of $f(x)$, β be a root of $g(x)$, both algebraic integers. Let f be of degree m, g be of degree n. Consider the $\mathbb{Z}$-module generated by $\alpha^i\beta^j$, $0 \le i \le m-1, 0 \le j \le n-1$. Then $(\alpha \pm \beta)M \subseteq M$ and $(\alpha\beta)M \subseteq M$. Hence both $\alpha \pm \beta$ and $\alpha\beta$ are algebraic integers by Lemma 1.2. □

2 Rings of integers in finite extensions of $\mathbb{Q}$

Let K be a finite extension of $\mathbb{Q}$. The ring of integers $\mathcal{O} = \mathcal{O}(K)$ is the intersection of the ring of all algebraic integers with K.

Note that $K = \mathbb{Q}[\alpha]$ for some α where the degree of the minimal polynomial of α = the degree of the extension = the number of different embeddings of K into $\bar{\mathbb{Q}}$. The embeddings $\sigma_1, ..., \sigma_n$ extend the maps $\alpha \to \alpha_i$ where α_i are the roots of the minimal polynomial of α.

For every $\beta \in K$, the norm $N_K(\beta)$ (the trace $\mathrm{tr}_K(\beta)$) is the product (the sum) of all $\sigma_i(\beta)$. Both are rational numbers since these are the coefficients of the minimal polynomial for β. Note that the norm is multiplicative. As usual, the trace allows us to define a bi-linear non-degenerate form on K: $(\alpha, \beta) = \mathrm{tr}(\alpha\beta)$. The properties are easy to verify, including $\mathrm{tr}(\alpha^2) \neq 0$ if $\alpha \neq 0$. Note that for $\alpha, \beta \in \mathcal{O}(K)$ we have $\mathrm{tr}(\alpha\beta) \in \mathbb{Z}$.

For every $\alpha_1, ..., \alpha_n \in \mathcal{O}(K)$ let

$$D_K(\alpha_1, ..., \alpha_n) = \det(\sigma_j(a_i))^2 = \det(\mathrm{tr}_K(\alpha_i\alpha_j))) \in \mathbb{Z}.$$

The D_K is the *discriminant* of the numbers α_i.

Note that

Theorem 2.1. *Let I be an ideal in $\mathcal{O}(K)$ and let $\alpha_1, ..., \alpha_n$ be numbers in I that are linearly independent over $\mathbb{Q}$ such that $|D_K(\alpha_1, ..., \alpha_n)| \in \mathbb{N}$ is minimal. Then I is the Z-module generated by α_i's.*

Proof. Any $\alpha \in I$ is (unique) linear combination $a_1\alpha_1 + ... + a_n\alpha_n$. It is enough to show that $a_i \in \mathbb{Z}$. Suppose that, say, $a_1 \notin \mathbb{Z}$. Then $a_1 = b + \theta$, θ the fractional part of a_1 (strictly between 0 and 1).

Consider a new collection of numbers $\beta_1, ..., \beta_n$ from $\mathcal{O}(K)$:

$$\vec{\beta} = \vec{\alpha} \begin{pmatrix} \theta & 0 & 0 & ... & 0 \\ a_2 & 1 & 0 & ... & 0 \\ . & . & . & ... & . \\ . & . & . & ... & . \\ . & . & . & ... & . \\ a_n & 0 & 0 & ... & 1 \end{pmatrix}.$$

Note that $\beta_i = \alpha_i \in \mathcal{O}(K)$ if $i > 1$ and $\beta_1 = \theta\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n = \beta - b\alpha_1 \in \mathcal{O}(K)$. Clearly, β_i are linearly independent since $\theta \neq 0$.

Then, computing the determinant in the definition of D_K, we get

$$|D_K(\vec{\beta})| = \theta^2 |D_K(\vec{\alpha})| < |D_K(\vec{\alpha})|,$$

since $\theta < 1$, a contradiction. $\square$

Definition 2.2. The discriminant of K is $D_K(\vec{\alpha})$ for some (=any) integral basis $\vec{\alpha}$ of $\mathcal{O}(K)$.

More properties of $\mathcal{O}(K)$.

Proposition 2.3. *For every ideal I in $\mathcal{O}(K)$, $\mathcal{O}(K)/I$ is finite.*

Proof. I is an n-dim free Abelian group inside another n-dim. free Abelian group $\mathcal{O}(K)$. $\square$

Proposition 2.4. *$\mathcal{O}(K)$ is Noetherian.*

Proposition 2.5. *Every prime ideal P of $\mathcal{O}(K)$ is maximal.*

Proof. Indeed, $\mathcal{O}(K)/P$ is finite domain, hence a field. $\square$

Definition 2.6. If A and B are two ideals in $\mathcal{O}(K)$ then we say that A is equivalent to B (denote $A \sim B$) if

$$(\alpha)A = (\beta)B$$

for some non-zero α and β from $\mathcal{O}(K)$.

Remark 2.7. $\sim$ is an equivalence relation.

Remark 2.8. $(\alpha)A = \alpha A$.

Remark 2.9. $A \sim (1) = \mathcal{O}(K)$ iff A is principal. Indeed, $A \sim (1)$ means $\alpha A = (\beta)$ for some $\alpha, \beta \in \mathcal{O}(K)$. That implies $\beta = \alpha\delta$, $\delta \in A \subseteq \mathcal{O}(K)$. Hence $A = (\delta)$. The converse statement is obvious.

The equivalence classes of ideals are called *ideal classes* of K. We shall show that the number of ideal classes is finite.

Proposition 2.10 (Hurwitz)**.** *There exists $N > 0$ such that for every $\gamma \in K$, there exists $t \leq M$ and $\theta \in \mathcal{O}(K)$ such that*

$$N_K(t\gamma - \theta) < 1.$$

Proof. Let $\omega_1, ..., \omega_n$ be a basis of $\mathcal{O}(K)$. Then we have an isomorphism $K \to \mathbb{Q}^n$ (as vector spaces). If $\gamma = \sum c_i \omega_i$ then we set

$$||\gamma|| = \max_i |c_i|.$$

Then

$$N_K(\gamma) \leq \prod_j \left(\sum_i |x_i||\sigma_j(\omega_i)| \right) \leq ||\gamma||^n C \tag{1}$$

for some constant C.

Take any $M > C$ so that $m = M^{1/n}$ is an integer. For every i let $c_i = a_i + b_i$ where $0 \leq b_i < 1$, $a_i \in \mathbb{Z}$. The integral part of γ, $[\gamma] = \sum a_i \omega_i$. The fractional part is $\{\gamma\} = \gamma - [\gamma]$. Note that $[\gamma] \in \mathcal{O}(K)$. Note also that $\vec{b}$ is in the unit cube of $\mathbb{R}^n$. Divide the unit cube into M cubes with side $\frac{1}{m}$. Then for each $j = 1, ..., M+1$, the coordinate vector of $\{j\gamma\}$ is in one of these cubes. At least two of them must be in the same cube. Let it be $\{j_1\gamma\}$ and $\{j_2\gamma\}$, $j_1 > j_2$. Let $t = j_1 - j_2$. Then

$$t\gamma = \theta + \delta$$

with $\theta \in \mathcal{O}(K)$, and

$$M_K(\delta) \leq ||\delta||^n C \leq \left(\frac{1}{m}\right)^n C = \frac{C}{M} < 1$$

by (1) as required.

□

Theorem 2.11. *The number of ideal classes is finite.*

Proof. Let A be an ideal of $\mathcal{O}$. Choose $\beta \in A$ with minimal $|N_K(\beta)|$.

Take any $\alpha \in \mathcal{O}(K)$. Then by the proposition, there exists natural number $t \leq M$ and $\theta \in \mathcal{O}(K)$ such that $N_K(t\frac{\alpha}{\beta} - \theta) < 1$. Multiply by $N_K(\beta)$:

$$|N_K(t\alpha - \theta\beta)| < |N_K(\beta)|.$$

Hence for every $\alpha \in A$, $t\alpha \in (\beta)$. Since t divides $M!$, we get that

$$M!A \subseteq (\beta)$$

Therefore

$$B = \frac{M!}{\beta} A \subseteq \mathcal{O}(K).$$

Note that B is certainly an ideal of $\mathcal{O}(K)$. Moreover

$$(M!)A = (\beta)B,$$

so $A \sim B$.

Since $\beta \in A$, we have $M! \in B$. Hence $(M!) \subseteq B$. But there are only finitely many ideals bigger than $(M!)$ (the factor-ring is finite), so there are finitely many choices for B. □

Theorem 2.12. *The classes of ideals form a group under multiplication.*

Lemma 2.13. $A = AB \to B = (1)$.

Proof. Suppose that $A = \text{span}_{\mathbb{Z}}(\alpha_1, ..., \alpha_n)$. Since $A = AB$, we get $\alpha_i = \sum \beta_{i,j}\alpha_j$, $\beta_{i,j} \in B$. Hence $\vec{\alpha}$ is the 1-eigenvector of the matrix $U = [[\beta_{i,j}]]$. Thus $\det(U - I) = 0$. Expanding the determinant, we get $1 \in B$. □

Lemma 2.14. $(\beta)A = AB \to B = (\beta)$.

Proof. Let $\delta \in B$. Then $\delta A \subseteq (\beta)$. Hence $\frac{\delta}{\beta}A \subseteq A$. By Lemma 1.2, $\frac{\delta}{\beta} \in \mathcal{O}$. Hence $B \subseteq (\beta)$ and $\beta^{-1}B \subseteq \mathcal{O}$. Then $A = (\beta^{-1}B)A$, hence $\beta^{-1}B = \mathcal{O}(K)$, i.e. $(\beta) = B$. □

Lemma 2.15. $A^m \sim (1)$ *for some* m.

Proof. $A^i \sim A^{i+j}$ means $(\alpha)A^i = (\beta)A^{i+j}$. Hence $(\alpha)A^i = ((\beta)A^j)A^i$. Therefore by the previous lemma, $(\beta)A^j = (\alpha)$, so $A^j \sim (1)$. □

Proof of Theorem 2.12. It is easy to see that $\sim$ is stable under multiplication. So the set of classes is a finite semigroup. The previous lemma implies existence of inverses.

Corollary 2.16. *Let* h_K *be the ideal class number of* K. *Then* $A^{h_K} \sim (1)$.

Theorem 2.17 (Fundamental theorem of ideal theory.)**.** *Every ideal of* $\mathcal{O}(K)$ *can be written as a product of prime ideals; it can be written in a unique way except for the order of factors.*

Lemma 2.18. $AB = AC \to B = C$.

Proof. $A^h = (\alpha)$. Hence $\alpha B = \alpha C$ which trivially implies $B = C$.

Lemma 2.19. $A \subseteq B$ *implies that there exists an ideal* C *such that* $A = BC$.

Proof. $B^h = (\beta)$. Then $B^{h-1}A \subseteq (\beta)$. Hence $C = \frac{1}{\beta}B^{h-1}A \subseteq \mathcal{O}(K)$. Then $BC = \frac{1}{\beta}B^hA = A$. □

Proof of Theorem 2.17. $\mathcal{O}(K)/A$ is finite, hence there exists a maximal ideal $P_1 > A$. Then by the previous lemma there exists A_1: $P_1 A_1 = A$. We have $A \subset A_1$. If $A_1 \neq \mathcal{O}(K)$, we can continue. Hence $A = P_1 P_2 ... P_m$ for some m (by the Noetherian property).

For uniqueness: if $A = Q_1 ... Q_l$ then P_1 must divide one of the Q_i, etc.