INTRODUCTION TO ALGEBRAIC NUMBER THEORY

Contents

1. Algebraic Integers

In the following section, K is taken to be a number field and thus a subfield of $\overline{\mathbb{Q}}$

Definition 1.1. *Let $\alpha \in K$. Then α is said to be an* ***algebraic integer*** *if there exists $f(x) \in \mathbb{Z}[x]$ such that $f(x)$ is monic and $p(\alpha) = 0$. Define $O_K = \{\alpha \in K : \alpha \text{ is an algebraic integer}\}$.*

Theorem 1.2. *Let $\alpha \in K$. Then α is an algebraic integer iff $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$.*

Proof. If $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$, then clearly α is an algebraic integer.

Conversely, suppose that α is an algebraic integer. There exists $f(x) \in \mathbb{Z}[x]$ such that $f(x)$ is monic and $f(\alpha) = 0$. Since $\mathbb{Z}[x]$ is a unique factorization domain and $f(x)$ is not a unit and nonzero, there exist irreducible polynomials $(p_i(x))_{i=1}^n \subset \mathbb{Z}[x]$ such that $f(x) = \prod_{i=1}^n p_i(x)$. Since $f(x)$ is monic, for each $i \in \{1, 2, \cdots, n\}$, we may take $p_i(x)$ to be monic. Then there exists $k \in \{1, 2, \cdots, n\}$ such that $p_k(\alpha) = 0$. Then $m_{\alpha,\mathbb{Q}}(x) | p_k(x)$ in $\mathbb{Q}[x]$. Thus $p_k(x) = m_{\alpha,\mathbb{Q}}(x)$. Since $p_k(x)$ is monic and irreducible in $\mathbb{Z}[x]$, it is irreducible in $\mathbb{Q}[x]$. Thus $m_{\alpha,\mathbb{Q}}(x) = p_k(x)$. □

Lemma 1.3. *Let M be a finitely generated $\mathbb{Z}$-submodule of K. Then M is free.*

Proof. Since M is finitely genereated and torsion-free, the fundamental theorem of finitetly generated abelian groups shows that M is free. □

Note 1.4. *The previous result says that anytime we consider M, a finitely generated $\mathbb{Z}$-submodule of K, we may choose a basis for M.*

Theorem 1.5. *Let $\alpha \in K$. Then $\alpha \in O_K$ iff there exists a finitely generated $\mathbb{Z}$-submodule M of K such that $\alpha M \subset M$.*

Proof. Suppose that $\alpha \in O_K$. Then there exist $(a_i)_{i=0}^{n-1} \subset \mathbb{Z}$ such that such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Then $M = (1, \alpha, \alpha^2, \cdots, \alpha^{n-1})$ is a finitely generated $\mathbb{Z}$-submodule of K and $\alpha M \subset M$.

Conversely, Suppose that there exists a finitely generated $\mathbb{Z}$-submodule M of K such that $\alpha M \subset M$. Choose a basis $a = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ of M. Thus for each $i, j \in \{1, 2, \cdots, n\}$, there exists $a_{i,j} \in \mathbb{Z}$ such that $\alpha\alpha_j = \sum_{i=1}^n a_{i,j}\alpha_i$. Define $T : M \to M$ by $T(x) = \alpha x$. Then T is a linear with matrix representation $[T]_a = (a_{i,j})$ and eigen-value α. Thus $f(x) = \det(xI - T) \in \mathbb{Z}$ is a monic polynomial with root α. So $\alpha \in O_K$. □

Theorem 1.6. *Let $\alpha, \beta \in O_K$. Then $\alpha + \beta \in O_K$ and $\alpha\beta \in O_K$.*

Proof. Since $\alpha, \beta \in O_K$, there exist finitely generated $\mathbb{Z}$-submodules M and N of K such that $\alpha M \subset M$ and $\beta N \subset N$. Choose finite sets $X, Y \subset K$ such that $M = (X)$ and $N = (Y)$. Then $MN = (XY)$ is finitely generated. Let $x \in X$ and $y \in Y$. Then $(\alpha + \beta)(xy) = (\alpha x)y + x(\beta y)$ and $(\alpha\beta)(xy) = (\alpha x)(\beta y)$. Since $\alpha x \in M$ and $\beta y \in N$, we have that $(\alpha + \beta)(xy) \in MN$ and $(\alpha\beta)(xy) \in MN$. Hence $(\alpha + \beta)MN \subset MN$, $(\alpha\beta)MN \subset MN$ and thus $\alpha + \beta, \alpha\beta \in O_K$ □

Corollary 1.7. *We have that O_K is a ring.*

Lemma 1.8. *Let $\alpha \in O_K$, $(\alpha_i)_{i=1}$ the conjugates of α, $L = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$ an embedding. Then $\sigma(\alpha) \in O_L$*

Proof. Since $\alpha \in O_L$, there exists $f(x) \in \mathbb{Z}[x]$ such that $f(x)$ is monic and $f(\alpha) = 0$. Since σ permutes $(\alpha_i)_{i=1}$, $\sigma(\alpha) \in L$. Since σ fixes $\mathbb{Q}$ we haver that

$$\begin{aligned} f(\sigma(\alpha)) &= \sigma(f(\alpha)) \\ &= 0 \end{aligned}$$

so $\sigma(\alpha) \in O_L$. □

Lemma 1.9. *We have that $O_K \cap \mathbb{Q} = \mathbb{Z}$*

Proof. Clearly $\mathbb{Z} \subset O_K \cap \mathbb{Q}$. Let $\alpha \in O_K \cap \mathbb{Q}$. If $\alpha = 0$, then $\alpha \in \mathbb{Z}$. Suppose that $\alpha \neq 0$. Since $\alpha \in \mathbb{Q}$, there exists $a, b \in \mathbb{Z} \setminus \{0\}$ such that $\gcd(a, b) = 1$ and $\alpha = ab^{-1}$. Since $\alpha \in O_K$, there exist $a_0, a_1, \cdots, a_{n-1} \in \mathbb{Z}$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. The rational root theorem says that $b|1$, so $b \in \mathbb{Z}^\times$ and thus $\alpha \in \mathbb{Z}$. □

Lemma 1.10. *Let $\alpha \in O_K$, $(\alpha_i)_{i=1}^n \subset \overline{\mathbb{Q}}$ the conjugates of α and $f(X_1, X_2, \cdots, X_n) \in \mathbb{Z}[X_1, X_2, \cdots, X_n]$ a symmetric polynomial. Then $f(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{Z}$.*

Proof. Since O_K is a ring, it is clear that $f(\alpha_1, \alpha_2, \cdots, \alpha_n) \in O_K$. Let $L = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)$. Since O_L is a ring and for each embedding $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$ and $i \in \{1, 2, \cdots, n\}$, $\sigma(\alpha_i) \in O_L$, we know that for each embedding $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$, $\sigma(f(\alpha_1, \alpha_2, \cdots, \alpha_n)) \in O_L$. For each embedding $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$, there exists $\tau_\sigma \in S_n$ such that for each $i \in \{1, 2, \cdots, n\}$, $\sigma(\alpha_i) = \alpha_{\tau_\sigma(i)}$. So for each embedding $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$, we have

$$\begin{aligned} \sigma(f(\alpha_1, \alpha_2, \cdots, \alpha_n)) &= f(\sigma(\alpha_1), \sigma(\alpha_2), \cdots, \sigma(\alpha_n)) \\ &= f(\alpha_{\tau_\sigma(1)}, \alpha_{\tau_\sigma(2)}, \cdots, \alpha_{\tau_\sigma(n)}) \\ &= f(\alpha_1, \alpha_2, \cdots, \alpha_n) \end{aligned}$$

which implies that $f(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{Q}$. Since $\mathbb{Q} \cap O_L = \mathbb{Z}$, we have that $f(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{Z}$. □

Theorem 1.11. *Let $\alpha \in K$. Then there exists $c \in \mathbb{Z}$ such that $c\alpha \in O_K$.*

Proof. Consider $m_{\alpha,\mathbb{Q}}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$. For each $i \in \{1, 2, \cdots, n-1\}$, there exist $b_i, c_i \in Z$ such that $c_i \neq 0$ and $a_i = b_i c_i^{-1}$. Define $c = \text{lcm}\{c_i : i = 1, 2, \cdots, n-1\} \in \mathbb{Z}$ and $f(x) = c^n m_{\alpha,\mathbb{Q}}(c^{-1}x) = x^n + a_{n-1}cx^{n-1} + \cdots + a_1c^{n-1}x + a_0c^n \in \mathbb{Z}[x]$. Then $f(x)$ is monic and $f(c\alpha) = 0$. So $c\alpha \in O_K$. □

Corollary 1.12. *Let K be a number field. Then there exists $\alpha \in O_K$ such that $K = \mathbb{Q}(\alpha)$.*

Proof. Since K is a finite extension of $\mathbb{Q}$, there exists $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Then the previous result tells us that there exists $c \in \mathbb{Z}$ such that $c\theta \in O_K$. Choose $\alpha = c\theta$. Then $K = \mathbb{Q}(\theta) = \mathbb{Q}(\alpha)$. $\square$