Integral Bases
Overview

Integral Bases

Norms and Traces

Existence of Integral Bases
Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree $n$. By Theorem 6.5, we may assume without loss of generality that $\theta$ is an algebraic integer.

**Definition**

A set of numbers $\beta_1, \ldots, \beta_s$ in $K$ is said to form a basis for $K$ over $F$ if for each element $\beta$ in $K$ there exists a unique set of numbers $d_1, \ldots, d_s$ such that

$$\beta = d_1 \beta_1 + \cdots + d_s \beta_s.$$
Integral Basis

Definition
A set of algebraic integers $\alpha_1, \ldots, \alpha_s$ in $K$ is called an integral basis of $K$ if every algebraic integer $\gamma$ in $K$ can be written uniquely in the form

$$\gamma = b_1\alpha_1 + \cdots + b_s\alpha_s$$

where $b_1, \ldots, b_s \in \mathbb{Z}$. 
Integral Bases are Bases

Lemma 6.7
An integral basis is a basis.

Proof Idea
Let $\alpha_1, \cdots, \alpha_s$ be an integral basis of $K$.
Let $\beta \in K$ and choose $r \in \mathbb{Z}$ so that $r\beta$ is an algebraic integer.
We may write

$$r\beta = b_1\alpha_1 + \cdots + b_s\alpha_s$$

$$\beta = \frac{b_1}{r}\alpha_1 + \cdots + \frac{b_s}{r}\alpha_s$$

It remains to show that $\alpha_1, \cdots, \alpha_s$ is linearly independent over $\mathbb{Q}$.
Conjugates for $\mathbb{Q}(\theta)$

Let $\theta$ be algebraic of degree $n$ over $\mathbb{Q}$, with conjugates $\theta_1, \ldots, \theta_n$ over $\mathbb{Q}$.

Let $\beta \in \mathbb{Q}(\theta)$, with $\beta = \sum_{i=0}^{n-1} c_i \theta^i = r(\theta)$. Suppose that $\beta$ has minimum polynomial $g(x)$ of degree $m$ over $\mathbb{Q}$.

**Definition**

The **conjugates of $\beta$ for $\mathbb{Q}(\theta)$** are the numbers $\beta_i = r(\theta_i)$ for $1 \leq i \leq n$.

**Note**

Observe that $\beta$ has $m$ conjugates over $\mathbb{Q}$, but has $n$ conjugates for $\mathbb{Q}(\theta)$. By Theorem 5.7, we also have that $m$ divides $n$. 
Norms and Traces

Let $\beta \in \mathbb{Q}(\theta)$, where $\theta$ is algebraic of degree $n$ over $\mathbb{Q}$.
Let $\beta_1, \ldots, \beta_n$ be the conjugates of $\beta$ for $\mathbb{Q}(\theta)$.

**Definition**
The norm of $\beta$ for $\mathbb{Q}(\theta)$ is defined to be

$$N(\beta) = N_{\mathbb{Q}(\theta)}(\beta) = \beta_1 \cdots \beta_n.$$ 

The trace of $\beta$ for $\mathbb{Q}(\theta)$ is defined to be

$$Tr(\beta) = Tr_{\mathbb{Q}(\theta)}(\beta) = \beta_1 + \cdots + \beta_n.$$
Let $\beta \in \mathbb{Q}(\theta)$, where $\theta$ is algebraic of degree $n$ over $\mathbb{Q}$.

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ be the minimum polynomial for $\beta$ over $\mathbb{Q}$ with roots $\beta_1, \ldots, \beta_m$.

Then

$$N(\beta) = \left(\beta_1 \cdots \beta_m\right)^{n/m} = (-1)^n b_0^{n/m}$$

and

$$Tr(\beta) = \frac{n}{m} (\beta_1 + \cdots + \beta_m) = -\frac{n}{m} b_{m-1}.$$
Theorem

Let $\beta, \gamma \in \mathbb{Q}(\theta)$. Then

$$N(\beta \gamma) = N(\beta)N(\gamma)$$

and

$$Tr(\beta + \gamma) = Tr(\beta) + Tr(\gamma).$$
**Theorem**

Let $\beta \in \mathbb{Q}(\theta)$. Then $N(\beta) \in \mathbb{Q}$ and $Tr(\beta) \in \mathbb{Q}$. If $\beta$ is an algebraic integer, then $N(\beta) \in \mathbb{Z}$ and $Tr(\beta) \in \mathbb{Z}$.
Lemma 6.8
If $\alpha_1, \ldots, \alpha_n$ is any basis of $\mathbb{Q}(\theta)$ over $\mathbb{Q}$ consisting only of algebraic integers, then $\Delta[\alpha_1, \ldots, \alpha_n]$ is a rational integer.

Proof Idea
This result follows from the last theorem since

\[
\Delta[\alpha_1, \ldots, \alpha_n] = \det((\alpha_j^i)^T)\det((\alpha_j^i)) = \det(\alpha_i^{(1)}\alpha_j^{(1)} + \alpha_i^{(2)}\alpha_j^{(2)} + \cdots + \alpha_i^{(n)}\alpha_j^{(n)}) = \det(Tr(\alpha_i\alpha_j)).
\]
Existence of Integral Bases

Theorem 6.9
Every algebraic number field has at least one integral basis.

Proof Idea
From the collection of all bases for $\mathbb{Q}(\theta)$ consisting of algebraic integers, choose one whose discriminant has smallest (nonzero) magnitude. Let its elements be $\omega_1, \ldots, \omega_n$.

Suppose FTSOC that $\omega_1, \ldots, \omega_n$ is not an integral basis, and let $\omega$ be an algebraic integer which is not a $\mathbb{Z}$-linear combination. We may suppose WLOG that

$$\omega = (a + r)\omega_1 + a_2\omega_2 \cdots + a_n\omega_n$$

where $a \in \mathbb{Z}$ and $0 < r < 1$.

But then defining $\omega_1^* = \omega - a\omega_1$ and $\omega_i^* = \omega_i$ for $2 \leq i \leq n$, we deduce that $\omega_1^*, \ldots, \omega_n^*$ is an integral basis with discriminant of smaller magnitude.
Invariance of Discriminants of Integral Bases

**Theorem 6.10**

All integral bases for a given algebraic number field have the same discriminant.
Acknowledgement

Statements of results follow the notation and wording of Pollard and Diamond’s *Theory of Algebraic Numbers*. 