Indices of Algebraic Integers in Cubic Fields

Jeremy Smith, Department of Mathematics, Texas Christian University

Advisor: Dr. George Gilbert

Algebraic Integers

An *algebraic integer* is a complex number that is a root of a monic polynomial with integer coefficients. In other words, it is a root of a polynomial of the form

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

for some $n \in \mathbb{N}$. The set of all algebraic integers is a subring of $\mathbb{C}$, denoted by $\mathbb{A}$. This means that sums and products of algebraic integers are also algebraic integers.

$\sqrt{-1} = i \in \mathbb{A}$ because it is a root of $x^2 + 1$.
$\sqrt[3]{2} \in \mathbb{A}$ because it is a root of $x^3 - 2$.
$\frac{\sqrt[3]{2}}{2} \notin \mathbb{A}$ because it is a root of $4x^3 - 1$ and not the root of any monic polynomial in $\mathbb{Z}[x]$.

Number Rings

A *number field* is a finite field extension of $\mathbb{Q}$. We can think of any number field F as a $\mathbb{Q}$-vector space. This means F has a basis over $\mathbb{Q}$. The number of basis elements is called the *degree* of F over $\mathbb{Q}$. Number fields of degree 2 and degree 3 over $\mathbb{Q}$ are called *quadratic fields* and *cubic fields*, respectively.

The set of all algebraic integers in F is called a *number ring* and is given by $\mathcal{O}_F = F \cap \mathbb{A}$. If F is of degree *n* over $\mathbb{Q}$, then $\mathcal{O}_F$ has a basis over $\mathbb{Z}$ consisting of *n* elements, called an *integral basis*.

Examples

1. If $F = \mathbb{Q}(i)$, then $\mathcal{O}_F = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
2. If $F = \mathbb{Q}(\sqrt{5})$, then $\mathcal{O}_F = \left\{ a + b\left(\frac{1+\sqrt{5}}{2}\right) : a, b \in \mathbb{Z} \right\}$.
3. If $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $\mathcal{O}_F = \left\{ a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\frac{\sqrt{2}+\sqrt{6}}{2} : a_i \in \mathbb{Z} \right\}$.

Let F be a number field of degree n. For any $\theta \in \mathcal{O}_F$, we define

$$\mathbb{Z}[\theta] := \{a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} : a_i \in \mathbb{Z}\}.$$

Certainly we have that $\mathbb{Z}[\theta] \subset \mathcal{O}_F$, but the reverse containment may not hold. A number ring $\mathcal{O}_F$ is called *monogenic* if there exists some $\theta \in \mathcal{O}_F$ such that $\mathcal{O}_F = \mathbb{Z}[\theta]$. Not all number rings are monogenic. This is different from the case of number fields in which there always exists some $\theta \in \mathcal{O}_F$ such that $F = \mathbb{Q}(\theta)$.

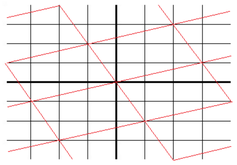
All number rings of quadratic fields are monogenic. However, there are some cubic fields whose number rings are not monogenic. One such example is the number ring of the field generated by a root of the polynomial $x^3 + x^2 - 2x + 8$.

Indices

If $F = \mathbb{Q}(\theta)$ where $\theta \in \mathcal{O}_F$, then the *index* of θ in $\mathcal{O}_F$ is the $\mathbb{Z}$-module index, given by

$$\mathrm{ind}(\theta) = [\mathcal{O}_F : \mathbb{Z}[\theta]]$$

The index of an algebraic integer tells us how close it is to generating it number ring. The close the index is to 1, the closer $\mathcal{O}_F$ is to being monogenic.



If F is of degree n over $\mathbb{Q}$, then $\mathrm{ind}(\theta)$ is the ratio between the volume of a fundamental parallelepiped in the $\mathbb{Z}$-lattice generated by $\{1, \theta, \ldots, \theta^{n-1}\}$ to the volume of a fundamental parallelepiped in the $\mathbb{Z}$-lattice generated by an integral basis for $\mathcal{O}_F$. Thus, $\mathrm{ind}(\theta)$ is essentially a determinant calculation. An integral basis for $\mathcal{O}_F$ may be written in terms of θ in such a way that $\mathrm{ind}(\theta)$ is the product of the denominators appearing in the basis.

Examples

1. $F = \mathbb{Q}(\sqrt{5})$ has an integral basis given by $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ so that $\mathrm{ind}\left(\frac{1+\sqrt{5}}{2}\right) = 1$ and $\mathrm{ind}(\sqrt{5}) = 2$.
2. $F = \mathbb{Q}(\sqrt[3]{10})$ has an integral basis given by $\left\{1, \sqrt[3]{10}, \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}\right\}$ so that $\mathrm{ind}(\sqrt[3]{10}) = 3$.

Main Results

We prove two major results pertaining to indices of algebraic integers in cubic fields.

Let $d \in \mathbb{Z}$ be squarefree. If $d \neq 1$, let $C(d)$ be the set of all non-cyclic cubic fields whose normal closure contains the unique quadratic subfield $\mathbb{Q}(\sqrt{d})$. Let $C(1)$ be the set of all cyclic cubic fields. For each congruence class of d modulo 8 and factorization of the ideal (2) into prime $\mathcal{O}_F$-ideals, we determine the set of all indices of algebraic integers in each $F \in C(d)$. The results are given in the table below.

d	factorization of (2)	set of indices
$d \equiv 2, 3 \pmod 4$	$P_1^2 P_1'$	$\mathbb{N}$
$d \equiv 1 \pmod 8$	$P_1 P_1' P_1''$	$2\mathbb{N}$
	P_3	$8^n\{2\mathbb{N} - 1\}$
$d \equiv 5 \pmod 8$	$P_1 P_2$	$\mathbb{N}$
	P_1^3	$8^n\{2\mathbb{N} - 1\} \cup 2 \cdot 8^n\{2\mathbb{N} - 1\}$

Furthermore, we show that for each index in each index set, there exist infinitely $F \in C(d)$ with the given factorization of (2) containing an algebraic integer with that index.

For any cubic field F, the *minimal index* of F is given by

$$m(F) = \min_{\theta \in \mathcal{O}_F} \mathrm{ind}(\theta)$$

For each squarefree $d \in \mathbb{Z}$ and for each $n \in \mathbb{N}$ we also prove that there exists some $F \in C(d)$ such that $m(F) > N$. This shows that the minimal index is unbounded as we run through the set of all cubic fields in $C(d)$.