Indices of Algebraic Integers in Cubic Fields

Jeremy Smith, Department of Mathematics, Texas Christian University

Advisor: Dr. George Gilbert

Rings of Algebraic Integers

An algebraic integer is a complex number that 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 $\mathbb{A}$. If F is a number field (a field extension of $\mathbb{Q}$), then the set of all algebraic integers in F is given by $\mathscr{O}_F = F \cap \mathbb{A}$.

Just as F is a $\mathbb{Q}$-vector space, $\mathscr{O}_F$ is a $\mathbb{Z}$-module. A $\mathbb{Z}$-module is like a vector space where the scalars are integers. In fact, if $[F:\mathbb{Q}] = n$, then $\mathscr{O}_F$ is a free $\mathbb{Z}$-module of rank *n*. This means that $\mathscr{O}_F$ has a basis over $\mathbb{Z}$. Such a basis is called integral basis.

Examples

1. If $F = \mathbb{Q}(i)$, then $\mathscr{O}_F = \mathbb{Z}[i] = \{a + bi : a,\ b \in \mathbb{Z}\}$. These are known as the Gaussian Integers.

2. If $F = \mathbb{Q}(\sqrt{5})$, then $\mathscr{O}_F = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{5}}{2}\right) : a, b \in \mathbb{Z}\right\} \neq \mathbb{Z}[\sqrt{5}]$.

3. If $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $\mathscr{O}_F = \left\{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\frac{\sqrt{2}+\sqrt{6}}{2} : a_i \in \mathbb{Z}\right\} \neq \mathbb{Z}[\sqrt{2}, \sqrt{3}]$.

Power Bases

It is well-known that any number field may be generated by a single element.

The Primitive Element Theorem: If F is a number field of degree *n*, then there exists some $\theta \in F$ such that

$$F = \mathbb{Q}(\theta) = \{a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0 : a_i \in \mathbb{Q}\}$$

In other words, if θ is a root of a degree *n* irreducible polynomial over $\mathbb{Q}$, then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis for F as a vector space over $\mathbb{Q}$. For instance, we have that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

An integral basis $\mathscr{B}$ for $\mathscr{O}_F$ is said to be a power basis if $\mathscr{B} = \{1, \theta, \ldots, \theta^{n-1}\}$ for some $\theta \in \mathscr{O}_F$ and $n \in \mathbb{N}$. When this is the case, we write

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

Fact: If F is a quadratic field (a number field of degree 2) or cyclotomic field (a number field generated by a primitive root of unity), then $\mathscr{O}_F$ has a power basis.

Question: Do all number fields have power bases for their rings of integers?

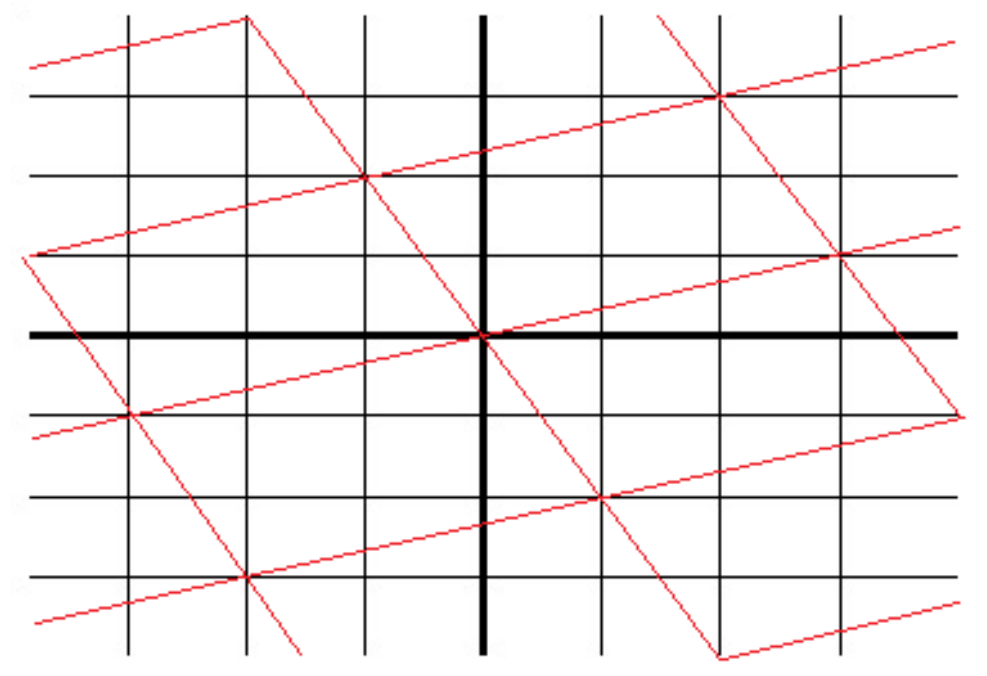
Answer: No! For instance, the field F generated by the polynomial $x^3 - x^2 - 2x - 8$ has ring of integers without a power basis. In fact, if θ is a root, then one such basis is given by $\{1, \theta, (\theta + \theta^2)/2\}$. Certainly $\mathscr{O}_F \neq \mathbb{Z}[\theta]$ but it turns out no other algebraic integer is a primitive element either.

Indices of Algebraic Integers

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

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

If an algebraic integer generates a number field, its index tells us how "close" it is to generating its ring of integers. In particular, $\mathscr{O}_F$ has a power basis if and only if it possesses an element of index 1.



Geometrically, $\operatorname{ind}(\theta)$ is the ratio between the volume of a fundamental parallelepiped in the $\mathbb{Z}$-lattice generated by $\{1, \theta, \ldots, \theta^{n-1}\}$ and the volume of a fundamental parallelepiped in the $\mathbb{Z}$-lattice generated by an integral basis for $\mathscr{O}_F$. As such, $\operatorname{ind}(\theta)$ is essentially a determinant calculation. An integral basis for $\mathscr{O}_F$ may be written in terms of θ in such a way that $\operatorname{ind}(\theta)$ will be the product of the denominators appearing in the basis.

Examples

1. $F = \mathbb{Q}(\sqrt[3]{2})$ has integral basis given by $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ so that $\operatorname{ind}(\sqrt[3]{2}) = 1$ and $\operatorname{ind}(2\sqrt[3]{2}) = 8$.

2. $F = \mathbb{Q}(\sqrt[3]{19})$ has integral basis given by $\left\{1, \sqrt[3]{19}, \frac{1 + \sqrt[3]{19} + \sqrt[3]{361}}{3}\right\}$ so that $\operatorname{ind}(\sqrt[3]{19}) = 3$.

Sets of Indices over Cubic Fields

We restrict our attention to cubic fields (number fields of degree 3). Given a quadratic field $L = \mathbb{Q}(\sqrt{d})$ with *d* squarefree, we say a cubic field F is associated to L if L is contained in the normal closure of F.

Example: The set of pure cubic fields (cubic fields of the form $F = \mathbb{Q}(\sqrt[3]{ab^2})$ with $a, b > 0$ and relatively prime) are associated to the quadratic field $\mathbb{Q}(\sqrt{-3})$.

Rather than look at a particular cubic field, we fix a quadratic field $L = \mathbb{Q}(\sqrt{d})$ and factorization of the prime ideal (2) in $\mathscr{O}_L$, and ask which natural numbers occur as indices in the family of cubic fields associated to L with the given factorization of (2). This will give us a set of indices over a set of cubic fields.

$$\begin{tikzcd}
 & LF \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
L = \mathbb{Q}(\sqrt{d}) \arrow[dr, dash, "2"'] & & F \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Results

Given a fixed quadratic field (described in terms of congruence conditions on *d*), and prime ideal factorization of (2) in $\mathscr{O}_L$ (note that not every factorization is possible in every case), the sets of indices are given 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	$8^n\{2\mathbb{N} - 1\} \cup 2 \cdot 8^n\{2\mathbb{N} - 1\}$

Observe that these are well-structured subsets of $\mathbb{N}$. For perspective, note that the set of indices in any particular cubic field would (more or less) be a random collection of natural numbers. In addition, we have that for each element in a given set, there exist infinitely many cubic fields in the corresponding family containing an algebraic integer with that index. This gives some idea of the frequency with which each index occurs.