Computing Integral Bases

by John Paul Cook

While the existence and concept of an integral basis is easy enough to understand, computing an integral basis for specific number fields is often not so easy. For this reason, as well as the desire to restrict this talk to an hour, we will focus mostly on examples and methods of computation for integral bases, while at the same time stating the necessary theory behind our methods (consult the listed references for proofs outside of what is included here). We assume only basic notions from field theory, such as the notions of field extensions, number fields, and algebraic integers.

1. Preliminaries

Thoughout, let $K = \mathbb{Q}(\beta)$ be a number field of degree n over $\mathbb{Q}$. Recall that for a number field $K = \mathbb{Q}(\beta)$ there are embeddings $\sigma : K \to \mathbb{C}$ which fix the groud field $\mathbb{Q}$ (also called monomorphisms, $\mathbb{Q}$-homomorphisms, automorphisms, etc. depending on the text). The following theorem allows us to explicitly describe these embeddings:

Theorem 1.1. Let $K = \mathbb{Q}(\beta)$ be a number field of degree n over $\mathbb{Q}$. Then there are n distinct embeddings $\sigma_i : K \to \mathbb{C}$, $i = 1, \ldots, n$, and $\sigma_i(\beta)$ is a distinct root of the minimum polynomial of β over $\mathbb{Q}$ for every such i.

Example 1.2. For $K = \mathbb{Q}(\sqrt[3]{5})$, the theorem gives that there are $[K : \mathbb{Q}] = 3$ distinct embeddings, and they are explicitly determined by the various mappings of $\sqrt[3]{5}$ to the roots of $X^3 - 5$, the minimum polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$:

$$\begin{aligned}\sigma_1(\sqrt[3]{5}) &= \sqrt[3]{5}\\ \sigma_2(\sqrt[3]{5}) &= \omega\sqrt[3]{5}\\ \sigma_3(\sqrt[3]{5}) &= \omega^2\sqrt[3]{5}\end{aligned}$$

where $\omega = e^{2\pi i/3}$.

Example 1.3. For $K = \mathbb{Q}(i, \sqrt{2})$, the theorem gives that there are $[K : \mathbb{Q}] = 4$ distinct embeddings, and they are explicitly determined by the various mappings of i to the roots of $X^2 + 1$, and the various mappings of $\sqrt{2}$ to the roots of $X^2 - 2$ (the respective minimum polynomials of i and $\sqrt{2}$ over $\mathbb{Q}$):

$$\sigma_1 : \begin{cases} i & \mapsto i \\ \sqrt{2} & \mapsto \sqrt{2} \end{cases} \quad \sigma_2 : \begin{cases} i & \mapsto -i \\ \sqrt{2} & \mapsto \sqrt{2} \end{cases} \quad \sigma_3 : \begin{cases} i & \mapsto i \\ \sqrt{2} & \mapsto -\sqrt{2} \end{cases} \quad \sigma_4 : \begin{cases} i & \mapsto -i \\ \sqrt{2} & \mapsto -\sqrt{2} \end{cases}$$

Definition 1.4. The elements $\sigma_i(\alpha)$ are called the *K-conjugates* of α over $\mathbb{Q}$.

It is worth noting that, as in the above example, the K-conjugates of α are not always elements of K. This notion of K-conjugates allows us to define the *norm* and *trace* of an element of a number field:

Definition 1.5. The *norm* of an element $\alpha \in K$ is given by

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

and the *trace* is given by:

$$T_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

In other words, the norm of α is the product of α and all its conjugates; the trace of α is the sum of α and all its conjugates. In the interests of saving time, we offer the following elementary properties of the norm and trace without proof (or, as the textbooks say, this is left to you "as an exercise"):

(1) The norm is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$
(2) The trace is additive, i.e. $T(\alpha + \beta) = T(\alpha) + T(\beta)$
(3) If α is an algebraic integer, then $N(\alpha)$, $T(\alpha) \in \mathbb{Z}$

The last few ideas we need to introduce involve the *ring of integers* of a number field K. We will take for granted (another exercise!) that the set of all algebraic integers, $\mathbb{B}$, is a subring of $\mathbb{C}$. Thus, the fact that the ring of integers is indeed a ring is immediate from the following definition:

Definition 1.6. The *ring of integers* of a number field $K/\mathbb{Q}$, denoted $\mathfrak{O}_K$, is $\mathfrak{O}_K = \mathbb{B} \cap K$. A $\mathbb{Z}$-basis for $\mathfrak{O}_K$ is called an *integral basis* for $\mathfrak{O}_K$.

Theorem 1.7. Every number field K has an integral basis.

Now that we know that an integral basis always exists for a number field K, it will be our primary device for finding the ring of integers.

2. Rings of Integers of Quadratic Fields

We are going to examine the case of quadratic fields first, before any heavier machinery is introduced. Before moving to a more general setting, let's look at an example:

Example 2.1. The ring of integers of $\mathbb{Q}(\sqrt{3})$ is $\mathbb{Z}[\sqrt{3}]$, with integral basis $\{1, \sqrt{3}\}$, which seems easy enough. However, the ring of integers of $\mathbb{Q}(\sqrt{5})$ is *not* $\mathbb{Z}[\sqrt{5}]$. For example,

$$\frac{1+\sqrt{5}}{2}$$

is a root of $X^2 - X - 1$ but is not an element of $\mathbb{Z}[\sqrt{5}]$. It turns out that $\mathfrak{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. In fact, there is a pattern which distinguishes which quadratic fields have a ring of integers like $\mathbb{Z}[\sqrt{3}]$ and which ones are like $\mathbb{Z}[\sqrt{5}]$, which we will look at in a moment.

This example hints that, in general, there is more to finding the ring of integers than just adjoining the generator to $\mathbb{Z}$. Before we can reveal the pattern by which one can immediately determine an integral basis for a quadratic field, we offer this characterization of quadratic fields:

Theorem 2.2. The quadratic fields are exactly those of the form $\mathbb{Q}(\sqrt{d})$, where d is a squarefree rational integer.

Proof. Let $K = \mathbb{Q}(\beta)$ be a quadratic field. Then β is the root of some monic quadratic polynomial

$$X^2 + bX + c$$

in $\mathbb{Z}[X]$ for some b, $c \in \mathbb{Z}$. Then

$$\beta = \frac{-b \pm r\sqrt{d}}{2}$$

where we put $b^2 - 4c = r^2 d$ and d is squarefree. Thus we have $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{d})$. □

This theorem is important because the ring of integers of a quadratic field depends only on d:

Theorem 2.3. Let $K = \mathbb{Q}(\sqrt{d})$, with d-squarefree. Then

$$\mathfrak{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \mod 4 \end{cases}$$

Cases beyond quadratic extensions, however, are not nearly as nice. We need some heavier machinery before we move on.

3. Methods for Finding Integral Bases

In this section we will cover the theory needed to compute integral bases of higher order. First, we recall the notion of discriminant of a number field:

Definition 3.1. Let K be number field of degree n over $\mathbb{Q}$, and let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K as a vector space over $\mathbb{Q}$. The *discriminant* of the given basis is

$$\Delta[\alpha_1, \ldots, \alpha_n] = \Big[\det \Big(\sigma_i(\alpha_j) \Big) \Big]^2.$$

Theorem 3.2. The discriminant of any basis $\{\alpha_1, \ldots, \alpha_n\}$ of a number field K is rational and non-zero. Moreover, if $\{\alpha_1, \ldots, \alpha_n\}$ consists of algebraic integers, then the discriminant is a rational integer.

Theorem 3.3. Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis for the number field K. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is squarefree, then $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis.

The problem with this seemingly useful theorem is that, practically speaking, it actually isn't very useful because a squarefree discriminant does not come up very often (at least in my experience). It is worth noting that the converse is *not* true, i.e. integral bases may have discriminants that are not squarefree. (For instance, any quadratic number field $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1 \mod 4$ has discriminant $4d$.) The following theorem, however, will prove much more useful:

Theorem 3.4. Suppose that $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers, and let p be a prime such that p^2 divides $\Delta[\alpha_1, \ldots, \alpha_n]$. Then there is an algebraic integer of the form

$$\frac{1}{p}(\lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n) \qquad (**)$$

where $0 \leq \lambda_i \leq p-1$, $\lambda_i \in \mathbb{Z}$.

Using the previous theorem, we can now write down a list of steps for computing an integral basis. These steps are are written in an informal, instructive, and hopefully practical manner. They have been listed here purely for reference – if any of the steps are unclear it may help to proceed to the examples.

(1) Start with a "natural" guess for an integral basis (make sure it is a $\mathbb{Q}$-basis for K consisting of algebraic integers).

(2) Calculate the discriminant of your guess. If this is squarefree, breathe a huge sigh of relief and move on with your life. Otherwise, proceed to step (3).

(3) Find all primes p such that p^2 divides the discriminant.

(4) Select one of the primes, p. Take the trace of a general "new" algebraic integer of the form $(**)$. Using the fact that the trace must be a rational integer, we can hopefully reduce the number of cases to check. *Note: order is important here; generally the norm is more difficult to compute than the trace, so we attempt to simplify the situation by using the trace first.*

(5) Take the norm of the resulting general form from the previous step. Similarly to the previous step, use this information to simplify as much as possible.

(6) Examine the remaining cases to see if they fit the criterion developed in the previous steps. If nothing else, exhausting all possible cases works, even if it isn't pleasant.

(7) If all cases are eliminated, then there are no new algebraic integers for the given p. If this is the case, return to step (3) and select another prime to repeat the process. If there are no other primes, then you have found an integral basis! However, if any numbers survived the process, proceed to the next step.

(8) Adjoin any new algebraic integers to your basis, and simplify. To elaborate, the set of elements you now have is $\mathbb{Z}$-linearly dependent, and to be a basis it obviously needs to be reduced so that it is $\mathbb{Z}$-linearly independent. Less formally, some of the old basis elements can be written as $\mathbb{Z}$-linear combinations of the newly adjoined elements, making them unnecessary.

(9) Calculate the discriminant of the new basis. If it is not squarefree, return to step (3) to repeat the process for any values of p such that p^2 divides the discriminant of the new basis. This process must be iterated even for already used values of p until no new algebraic integers are found. If you have done this for all such p, then congratulations, you have found an integral basis.

Example 3.5. Finding an integral basis for $K = \mathbb{Q}(\sqrt[3]{5})$:

(1) Start with a "natural" guess for an integral basis (make sure it is a $\mathbb{Q}$-basis for K consisting of algebraic integers).

A natural guess in this situation is $\{1, \sqrt[3]{5}, \sqrt[3]{5^2}\}$, which is clearly a $\mathbb{Q}$-basis for K, and all three elements are algebraic integers.

(2) Calculate the discriminant of your guess. If this is squarefree, breathe a huge sigh of relief and move on with your life. Otherwise, proceed to step (3).

We already found the embeddings $\sigma_i : K \to \mathbb{C}$ in section 1 (recall that $\omega = e^{2\pi i/3}$):

$$\begin{aligned}\Delta[1, \sqrt[3]{5}, \sqrt[3]{5^2}] &= \begin{vmatrix} 1 & \sqrt[3]{5} & \sqrt[3]{5^2} \\ 1 & \omega\sqrt[3]{5} & \omega^2\sqrt[3]{5^2} \\ 1 & \omega^2\sqrt[3]{5} & \omega\sqrt[3]{5^2} \end{vmatrix}^2 \\ &= -675 \\ &= -3^3 \cdot 5^2\end{aligned}$$

(3) Find all primes p such that p^2 divides the discriminant.

It is easy to see that 3 and 5 are the primes that need to be considered.

(4) Select one of the primes, p. Take the trace of a general "new" algebraic integer of the form $(**)$. Using the fact that the trace must be a rational integer, we can hopefully reduce the number of cases to check.

For no particular reason, we choose to start with $p = 5$. We want to examine the possibilities

$$\alpha = \frac{1}{5}(\lambda_1 + \lambda_2\sqrt[3]{5} + \lambda_3\sqrt[3]{5^2})$$

for $0 \leq \lambda_i \leq 4$ to see if any of them are algebraic integers. We compute the trace:

$$\begin{aligned}\mathrm{Tr}(\alpha) &= \Big(\frac{1}{5}\Big)\sum_{i=1}^{3} \sigma_i(\lambda_1 + \lambda_2\sqrt[3]{5} + \lambda_3\sqrt[3]{5^2}) \\ &= \frac{3\lambda_1}{5}\end{aligned}$$

which implies that $\lambda_1 \in 5\mathbb{Z}$.

(5) Take the norm of the resulting general form from the previous step. Similarly to the previous step, use this information to simplify as much as possible.

What remains from the previous step is

$$\alpha' = \frac{1}{5}(\lambda_2 \sqrt[3]{5} + \lambda_3 \sqrt[3]{5^2})$$

so that

$$\mathrm{N}(\alpha') = \Big(\frac{1}{125}\Big)\prod_{i=1}^{3} \sigma_i(\lambda_2 \sqrt[3]{5} + \lambda_3 \sqrt[3]{5^2}) = \frac{5\lambda_2^3 + 25\lambda_3^3}{125}$$

The information from this that we can use is that $\lambda_2^3 + 5\lambda_3^3$ must be divisible by 25 to be an algebraic integer.

(6) Examine the remaining cases to see if they fit the criterion developed in the previous steps. If nothing else, exhausting all possible cases works, even if it isn't pleasant.

There are probably better ways to do this, but one way to see if any of the remaining cases form algebraic integers is to try all of the cases:

λ_2	λ_3	$\lambda_2^3 + 5\lambda_3^2$	Divisible by 25?
0	1	5	NO
0	2	40	NO
0	3	135	NO
0	4	320	NO
1	0	1	NO
1	1	6	NO
1	2	41	NO
1	3	136	NO
1	4	321	NO
2	0	8	NO
2	1	13	NO
2	2	48	NO
2	3	143	NO
2	4	328	NO
3	0	27	NO
3	1	32	NO
3	2	67	NO
3	3	162	NO
3	4	347	NO
4	0	64	NO
4	1	69	NO
4	2	104	NO
4	3	199	NO
4	4	384	NO

(7) If all cases are eliminated, then there are no new algebraic integers for the given p. If this is the case, return to step (3) and select another prime to repeat the process. If there are no other primes, then you have found an integral basis! However, if any numbers survived the process, proceed to the next step.

As we saw, all cases for $p = 5$ are eliminated, so there are no new algebraic integers of the form

$$\alpha = \frac{1}{5}(\lambda_1 + \lambda_2\sqrt[3]{5} + \lambda_3\sqrt[3]{5^2})$$

Returning to step 3 and repeat this process for $p = 3$ also yields no new algebraic integers, eliminating all possibilities for new algebraic integers. Thus, an integral basis for $\mathbb{Q}(\sqrt[3]{5})$ is

$$\{1, \sqrt[3]{5}, \sqrt[3]{5^2}\}$$

Example 3.6. Finding an integral basis for $K = \mathbb{Q}(i, \sqrt{2})$:

(1) Start with a "natural" guess for an integral basis (make sure it is a $\mathbb{Q}$-basis for K consisting of algebraic integers).

A natural guess in this situation is $\{1, \sqrt{2}, i, i\sqrt{2}\}$, which is clearly a $\mathbb{Q}$-basis for K, and all four elements are algebraic integers.

(2) Calculate the discriminant of your guess. If this is squarefree, breathe a huge sigh of relief and move on with your life. Otherwise, proceed to step (3)

We already found the embeddings $\sigma_i : K \to \mathbb{C}$ in section 1:

$$\begin{aligned}\Delta[1, i\sqrt{2}, i, \sqrt{2}] &= \begin{vmatrix} 1 & \sqrt{2} & i & i\sqrt{2} \\ 1 & \sqrt{2} & -i & -i\sqrt{2} \\ 1 & -\sqrt{2} & i & -i\sqrt{2} \\ 1 & -\sqrt{2} & -i & \sqrt{2} \end{vmatrix}^2 \\ &= 1024 \\ &= 2^{10}\end{aligned}$$

(3) Find all primes p such that p^2 divides the discriminant.

Fortunately, $p = 2$ is the only case to consider.

(4) Select one of the primes, p. Take the trace of a general "new" algebraic integer of the form $(**)$. Using the fact that the trace must be a rational integer, we can hopefully reduce the number of cases to check.

Set $p = 2$, and examine the possibilities:

$$\alpha = \frac{1}{2}(\lambda_1 + \lambda_2\sqrt{2} + \lambda_3 i + \lambda_4 i\sqrt{2})$$

for $0 \leq \lambda_i \leq 1$ to see if any of them are algebraic integers. We compute the trace:

$$\mathrm{Tr}(\alpha) = \Big(\frac{1}{2}\Big)\sum_{k=1}^{4} \sigma_i(\lambda_1 + \lambda_2\sqrt{2} + \lambda_3 i + \lambda_4 i\sqrt{2}) = 2\lambda_1$$

which does not help! Begrudgingly, we proceed to the next step.

(5) Take the norm of the resulting general form from the previous step. Similarly to the previous step, use this information to simplify as much as possible.

$$\begin{aligned}\mathrm{N}(\alpha) &= \Big(\frac{1}{16}\Big)\prod_{k=1}^{4} \sigma_i(\lambda_1 + \lambda_2\sqrt{2} + \lambda_3 i + \lambda_4 i\sqrt{2}) \\ &= \frac{(\lambda_1^2 - \lambda_3^2 - 2\lambda_2^2 + 2\lambda_4^2)^2 + 4(\lambda_1\lambda_3 - 2\lambda_2\lambda_4)^2}{16}\end{aligned}$$

The information from this that we can use is that

$$(\lambda_1^2 - \lambda_3^2 - 2\lambda_2^2 + 2\lambda_4^2)^2 + 4(\lambda_1\lambda_3 - 2\lambda_2\lambda_4)^2$$

must be divisible by 16 to be an algebraic integer.

(6) Examine the remaining cases to see if they fit the criterion developed in the previous steps. If nothing else, exhausting all possible cases works, even if it isn't pleasant.

Again, we use brute force:

λ_1	λ_2	λ_3	λ_4	Is $N(\alpha)$ divisible by 16?
1	1	1	1	NO
0	1	1	1	NO
1	0	1	1	NO
0	0	1	1	NO
1	1	0	1	NO
0	1	0	1	YES
1	0	0	1	NO
0	0	0	1	NO
1	1	1	0	NO
0	1	1	0	NO
1	0	1	0	NO
0	0	1	0	NO
1	1	0	0	NO
0	1	0	0	NO
1	0	0	0	NO

(7) If all cases are eliminated, then there are no new algebraic integers for the given p. If this is the case, return to step (3) and select another prime to repeat the process. If there are no other primes, then you have found an integral basis! However, if any numbers survived the process, proceed to the next step.

This time, we find 1 new possibility for an algebraic integer (when $\lambda_2 = \lambda_4 = 1, \lambda_1 = \lambda_3 = 0$):

$$\beta = \frac{i\sqrt{2} + \sqrt{2}}{2}$$

which is a root of the monic polynomial

$$X^4 + 1$$

So we proceed to the next step.

(8) Adjoin any new algebraic integers to your basis, and simplify. To elaborate, the set of elements you now have is $\mathbb{Z}$-linearly dependent, and to be a basis it obviously needs to be reduced so that it is $\mathbb{Z}$-linearly independent. Less formally, some of the old basis elements can be written as $\mathbb{Z}$-linear combinations of the newly adjoined elements, making them unnecessary.

We now have

$$\{1, \sqrt{2}, i, i\sqrt{2}, \tfrac{i\sqrt{2}+\sqrt{2}}{2}\}$$

and we can easily reduce this back down to four elements, for $i\sqrt{2}$ is a linear combination of β and $\sqrt{2}$:

$$i\sqrt{2} = 2 \cdot \beta - \sqrt{2}$$

(9) Calculate the discriminant of the new basis. If it is not squarefree, return to step (3) to repeat the process for any values of p such that p^2 divides the discriminant of the new basis. This process must be iterated even for already used values of p until no new algebraic integers are found. If you have done this for all such p, then congratulations, you have found an integral basis.

Since we have added a new algebraic integer, we must repeat the process for $p = 2$, as, for example, there may be integers of the form

$$\frac{i\sqrt{2} + \sqrt{2}}{4}.$$

Repeating this process for $p = 2$ with the new basis, however, does not yield any new algebraic integers. This exhausts the case $p = 2$, so there are no other cases to check. Thus,

$$\{1, \sqrt{2}, i, \tfrac{i\sqrt{2}+\sqrt{2}}{2}\}$$

is an integral basis for $\mathbb{Q}(i, \sqrt{2})$.

$\sim$THE END$\sim$

References:

Stewart, Ian and Tall, David. Algebraic Number Theory and Fermats Last Theorem (3rd edition). A.K. Peters Ltd, Natick, MA, 2002.

Murty, M. and Esmonde, Jody. Problems in Algebraic Number Theory (2nd edition). Graduate Texts in Mathematics, 190. Springer-Verlag, New York, 2005.