Ring of Integers

Definition: Algebraic Integer

To say that an algebraic number is an *algebraic integer* means that its minimal polynomial has coefficients in $\mathbb{Z}$.

Theorem

Let $\overline{\mathbb{Z}}$ be the set of algebraic integers:

$\overline{\mathbb{Z}}$ is a ring (but not a field).

Definition: Ring of Integers

Let d be a squarefree integer. The *ring of integers* of $\mathbb{Q}(\sqrt{d})$ is given by:

$$R_d = \mathbb{Q}(\sqrt{d}) \cap \overline{\mathbb{Z}}$$

Theorem: Integer Criterion

Let $\alpha \in \mathbb{Q}(\sqrt{d})$:

$$\alpha \in R_d \iff N(\alpha), T(\alpha) \in \mathbb{Z}$$

Proof

Assume $\alpha \in \mathbb{Q}(\sqrt{d})$

α is a zero of the monic polynomial:

$$f(x) = (x-\alpha)(x-\alpha') = x^2 - (\alpha+\alpha')x + (\alpha\alpha') = x^2 - T(\alpha)x + N(\alpha)$$

which has all rational coefficients

Thus, $x - \alpha$ or $f(x)$ is the minimal polynomial for a and it is then clear that $N(\alpha), T(\alpha) \in \mathbb{Z}$.

Theorem

$$R_d = \begin{cases} \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}], & d \equiv 2, 3 \pmod 4 \end{cases}$$

Proof

$\implies$ Assume $\alpha \in R_d$

Let $\alpha = r + \sqrt{d}$

By the integer criterion:

$$N(\alpha) = r^2 - ds^2 \in \mathbb{Z}$$

$$T(\alpha) = 2r \in \mathbb{Z}$$

Then:

$$-4N(\alpha) + T(\alpha)^2 = 4(ds^2 - r^2) + (2r)^2 = 4ds^2 = d(2s)^2 \in \mathbb{Z}$$

Since $s \in \mathbb{Q}$, let $2s = \frac{a}{c}$ where $(a, c) = 1$ and $c \neq 0$
Let $d\left(\frac{a}{c}\right)^2 = k \in \mathbb{Z}$
$da^2 = kc^2$
Now, ABC that there exists prime p such that $p \mid c$
$p^2 \mid c^2$
But $(a, c) = 1$, so $p^2 \nmid a^2$, and thus $p^2 \mid d$
CONTRADICTION! Since d is squarefree
Thus, $c = 1$ and $d\left(\frac{a}{c}\right)^2 = d(2s)^2 \in \mathbb{Z}$
And since $d \in \mathbb{Z}$, we have $2s \in \mathbb{Z}$

Now, let $a = 2s \in \mathbb{Z}$ amd $b = 2r \in \mathbb{Z}$
$\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{d}$
$N(\alpha) = \left(\frac{a}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = \frac{a^2 - db^2}{4}$
$a^2 - db^2 = 4N(\alpha) \equiv 0 \pmod 4$
and so: $a^2 \equiv db^2 \pmod 4$

Now, consider the even/odd cases for a and b
Recall: $\forall\, n \in \mathbb{Z}, n$ is even $\iff n^2$
Assume $n \in \mathbb{Z}$:

Case 1: n even

Case 1a: $n \equiv 0 \pmod 4$

$$n^2 \equiv 0 \cdot 0 \pmod 4 \equiv 0 \pmod 4$$

Case 1b: $n \equiv 2 \pmod 4$

$$n^2 \equiv 2 \cdot 2 \pmod 4 \equiv 0 \pmod 4$$

Thus, n even $\implies n^2 \equiv 0 \pmod 4$

Case 2: n odd

Case 2a: $n \equiv 1 \pmod 4$

$$n^2 \equiv 1 \cdot 1 \pmod 4 \equiv 1 \pmod 4$$

Case 2b: $n \equiv 3 \pmod 4$

$$n^2 \equiv (-1) \cdot (-1) \pmod 4 \equiv 1 \pmod 4$$

Thus, n odd $\implies n^2 \equiv 1 \pmod 4$

Now, apply this information to a and b based on d:

Case 1: $d \equiv 1 \pmod 4$

$a^2 \equiv b^2 \pmod 4$
Thus a and b must have the same parity, and so:

$$\alpha = \frac{a + b\sqrt{d}}{2} = \frac{a+b}{2} + b\left(\frac{-1+\sqrt{d}}{2}\right)$$

But since a and b have the same parity: $\frac{a+b}{2} \in \mathbb{Z}$
Also $b \in \mathbb{Z}$
$\therefore \alpha \in \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$

Case 2: $d \equiv 2 \pmod 4$

$a^2 \equiv 2b^2 \pmod 4$
and so $a^2, b^2 \equiv 0 \pmod 4$, and thus a and b must both be even
Thus $r = \frac{a}{2}$ and $s = \frac{b}{2}$ are both integers

$\therefore \alpha \in \mathbb{Z}[\sqrt{d}]$

Case 3: $d \equiv 3 \pmod 4$

$a^2 \equiv -b^2 \pmod 4$
and so $a^2, b^2 \equiv 0 \pmod 4$, and thus a and b must both be even and this is the same as the previous case

$\therefore \alpha \in \mathbb{Z}[\sqrt{d}]$

$\Longleftarrow$ Assume $\alpha \in \begin{cases} \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}], & d \equiv 2, 3 \pmod 4 \end{cases}$

Case 1: $d \equiv 1 \pmod 4$

$\alpha \in \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$
Let $\alpha = m + n\left(\frac{-1+\sqrt{d}}{2}\right)$ where $m, n \in \mathbb{Z}$
$\alpha = m - \frac{n}{2} + \frac{n\sqrt{d}}{2}$
$N(\alpha) = \left(m - \frac{n}{2}\right)^2 - d\left(\frac{n}{2}\right)^2 = m^2 - mn + \frac{n^2}{4} - \frac{dn^2}{4} = m^2 - mn + n^2\left(\frac{1-d}{4}\right) \in \mathbb{Z}$
$T(\alpha) = 2\left(m - \frac{n}{2}\right) = 2m - n \in \mathbb{Z}$

Therefore, by the integer criterion, $\alpha \in R_d$

Case 2: $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$

$\alpha \in \mathbb{Z}[\sqrt{d}]$
Let $\alpha = m + n\sqrt{d}$ where $m, n \in \mathbb{Z}$

$N(\alpha) = m^2 - dn^2 \in \mathbb{Z}$

$T(\alpha) = 2m \in \mathbb{Z}$

Therefore, by the integer criterion, $\alpha \in R_d$