Quadratic Integers

Riccardo Brasca Pietro Monticone

December 12, 2025

Chapter 1

Ring of Integers of a Quadratic Field (Formalisation-Oriented)

Let d be an integer different from 0 and 1. We also assume that d is squarefree. We write K for the $\mathbb{Q}$-algebra generated by $\sqrt{d}$: to be precise, we implement K using `QuadraticAlgebra` $\mathbb{Q}$ `d 0`.

Lemma 1. *For all rational r, we have $r^2 \neq d$, so K is a field.*

Proof. Clear since we assume that d is squarefree. □

Lemma 2. *We have that $d = \pm 1 \bmod 4$ or $d = 2 \bmod 4$.*

Proof. If $d = 0 \bmod 4$ then d would not be squarefree. □

We now write R for $\mathbb{Z}[\sqrt{d}]$: we have that K is an R-algebra in the obvious way. Note that R is implemented as `QuadraticAlgebra` $\mathbb{Z}$ `d 0`.

Lemma 3. *We have that $\sqrt{d}$ is an integral element of K.*

Proof. Clear since $\sqrt{d}$ is a root of $x^2 - d$. □

Note that, in Lean, the above proposition technically says that the image in K of $\sqrt{d}$ *as element of* R is integral.

1.1 Trace and norm

We fix in this section two rational numbers $a, b \in \mathbb{Q}$ and we write z for $a + b\sqrt{d} \in K$.

Lemma 4. *We have that $z \in \mathbb{Q}$ if and only if $b = 0$.*

Proof. Clear. □

Lemma 5. *If $b \neq 0$ then the minimal polynomial of z over $\mathbb{Q}$ is*

$$X^2 - 2aX + (a^2 - db^2)$$

Proof. It's clear that z is a root of P and that $P \in \mathbb{Q}[X]$ is monic. Irreducibility follows by the fact that P has a root that is irrational. □

Lemma 6. *We have that the trace of z is $2a$.*

Proof. If $b = 0$ then $z = a \in \mathbb{Q}$ and the trace is $2a$ since $[K : \mathbb{Q}] = 2$. Otherwise this is clear by Lemma 5. □

Lemma 7. *We have that the norm of z is $a^2 - db^2$.*

Proof. If $b = 0$ then $z = a \in \mathbb{Q}$ and the norm is a^2 since $[K : \mathbb{Q}] = 2$. Otherwise this is clear by Lemma 5. □

1.1.1 Integrality

We now suppose that $z \in \mathcal{O}_K$.

Lemma 8. *We have that $2a \in \mathbb{Z}$.*

Proof. Since the trace of an algebraic integer is an integers, this follows by Lemma 6. □

Definition 9. We write t (for trace) to denote $2a$ as an integer. Mathematically we have $t = 2a$.

Lemma 10. *We have that $a^2 - db^2 \in \mathbb{Z}$.*

Proof. Since the norm of an algebraic integer is an integers, this follows by Lemma 7. □

Definition 11. We write n (for norm) to denote $a^2 - db^2$ as an integer. Mathematically we have $n = a^2 - db^2$.

Lemma 12. *We have that $4n = (2a)^2 - d(2b)^2$.*

Proof. Obvious by applying 11. □

Lemma 13. *Let n be a squarefree integer and let r be a rational such that br^2 is an integer. Then r is itself an integer.*

Proof. Easy. □

Lemma 14. *We have that $2b \in \mathbb{Z}$.*

Proof. By Lemma 12, $(2a)^2 - d(2b)^2$ is an integer and so, by Lemma 8, we know that $d(2b)^2 \in \mathbb{Z}$. Since d is squarefree, we conclude that $2b \in \mathbb{Z}$ by Lemma 13. □

Definition 15. We write B_2 to denote $2b$ as an integer. Mathematically we have $B_2 = 2b$.

Lemma 16. *If $a \in \mathbb{Z}$ then $b \in \mathbb{Z}$.*

Proof. By Lemma 12 and our assumption, both $(2a)^2$ and $(2a)^2 - d(2b)^2$ are integers divisible by 4, so the same holds for $d(2b)^2$. In particular $db^2 \in \mathbb{Z}$ and $b \in \mathbb{Z}$ by Lemma 13 since d is squarefree. □

Definition 17. If a is an integer, we write B to denote b as an integer. Mathematically we have $B = b$.

Lemma 18. *If $a \notin \mathbb{Z}$ then $d = 1 \bmod 4$.*

Proof. We have that $2a$, that is an integer, must be odd. By Lemmas 12 and 14, we have $(2a)^2 = d(2b)^2 \bmod 4$, so $2b$ must be odd and $d = 1 \bmod 4$ as required. □

1.2 The case $d \neq 1 \bmod 4$

Theorem 19. *Assume that $d = 2 \bmod 4$ or $d = 3 \bmod 4$. Then*

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$$

Proof. By Lemma 3 we know that $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. Let $z = a + b\sqrt{d} \in \mathcal{O}_K$, with $a, b \in \mathbb{Q}$. By Lemma 18 we have that $a \in \mathbb{Z}$ (since by Lemma 2 we cannot have $d = 1 \bmod 4$), and so by Lemma 16 we have $b \in \mathbb{Z}$, so $z \in \mathbb{Z}[\sqrt{d}]$. □

1.3 The case $d = 1 \bmod 4$

We assume in this section that $d = 1 \bmod 4$ and we write $e = \frac{d-1}{4}$.

Lemma 20. *We have that e is an integer and $4e = d - 1$.*

Proof. Obvious. □

We write S for the ring $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, implemented as `QuadraticAlgebra ℤ e 1`.

Lemma 21. *We have that*

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

so that S is an R-algebra.

Proof. Obvious by Lemma 20. □

Lemma 22. *We have that*

$$\left(\frac{1+\sqrt{d}}{2}\right)^2 = \left(\frac{1+\sqrt{d}}{2}\right) + e$$

so that K is an S-algebra.

Proof. Obvious by Lemma 20. □

Lemma 23. *The obvious diagram between R, S and K commutes.*

Proof. Clear. □

Lemma 24. *We have that $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$.*

Proof. Clear since $\frac{1+\sqrt{d}}{2}$ is a root of $X^2 - X - e \in \mathbb{Z}[X]$. □

Lemma 25. *Take $z = a + b\sqrt{d} \in \mathcal{O}_K$ with $a, b \in \mathbb{Q}$. If $a \in \mathbb{Z}$ then $z \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.*

Proof. By Lemma 16 we have that $b \in \mathbb{Z}$ and so $z \in \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. □

Theorem 26. *We have*

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

Proof. By Lemma 24 we know that $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq \mathcal{O}_K$. Let $z = a + b\sqrt{d} \in \mathcal{O}_K$, with $a, b \in \mathbb{Q}$.

- If $a \in \mathbb{Z}$ we conclude by Lemma 25.
- If $a \notin \mathbb{Z}$, let us consider

$$z' = z - \frac{1+\sqrt{d}}{2} = a - \frac{1}{2} + \left(b - \frac{1}{2}\right)\sqrt{d} \in \mathcal{O}_K$$

Since $2a \in \mathbb{Z}$ and $a \notin \mathbb{Z}$, we have that $a - \frac{1}{2} \in \mathbb{Z}$, so by Lemma 25, we have that $z' \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and so $z \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

□

Chapter 2

Ring of Integers of a Quadratic Field (Human-Oriented)

Let d be an integer different from 0 and 1. We also assume that d is squarefree. We write K for the subring of $\mathbb{C}$ generated by $\sqrt{d}$. By our assumptions on d, we have that $K = \mathbb{Q}(\sqrt{d})$ is a field.

Lemma 27. *We have that $d = \pm 1 \bmod 4$ or $d = 2 \bmod 4$.*

Proof. If $d = 0 \bmod 4$ then d would not be squarefree. □

Lemma 28. *We have that $\sqrt{d} \in \mathcal{O}_K$.*

Proof. Clear since $\sqrt{d}$ is a root of $x^2 - d$. □

Lemma 29. *If $d = 1 \bmod 4$ then $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$.*

Proof. Write $d = 4a + 1$, with $a \in \mathbb{Z}$. Then $\frac{1+\sqrt{d}}{2}$ is a root of $x^2 - x - a \in \mathbb{Z}[x]$. □

Let $t \in K$, so $t = a + b\sqrt{d}$ for some $a, b \in \mathbb{Q}$. We assume that $t \notin \mathbb{Q}$, i.e. that $b \neq 0$.

Lemma 30. *The minimal polynomial of t over $\mathbb{Q}$ is*

$$P(x) = x^2 - 2at + (a^2 - db^2)$$

Proof. It's clear that t is a root of P and that $P \in \mathbb{Q}[x]$ is monic.
Irreducibility follows by the fact that P has a root that is not rational. □

Lemma 31. *We have that the trace of t is $2a$.*

Proof. Clear by Lemma 30. □

Lemma 32. *We have that the norm of t is $a^2 - db^2$.*

Proof. Clear by Lemma 30. □

We suppose now that $t \in \mathcal{O}_K$.

Lemma 33. *We have that $2a \in \mathbb{Z}$*

Proof. Since the trace of an algebraic integer is an integers, this follows by Lemma 31. □

Lemma 34. *We have that* $a^2 - db^2 \in \mathbb{Z}$

Proof. Since the norm of an algebraic integer is an integers, this follows by Lemma 32. □

Lemma 35. *We have that* $(2a)^2 - d(2b)^2$ *is an integer divisible by* 4.

Proof. Clear since $(2a)^2 - d(2b)^2 = 4(a^2 - db^2)$ and $a^2 - db^2 \in \mathbb{Z}$ by Lemma 34. □

Lemma 36. *We have that* $2b \in \mathbb{Z}$.

Proof. By Lemma 35, $(2a)^2 - d(2b)^2$ is an integer and so, by Lemma 33, we know that $d(2b)^2 \in \mathbb{Z}$. Since d is squarefree, we conclude that $2b \in \mathbb{Z}$. □

Lemma 37. *If* $a \in \mathbb{Z}$ *then* $b \in \mathbb{Z}$.

Proof. By Lemma 35 and our assumption, both $(2a)^2$ and $(2a)^2 - d(2b)^2$ are integers divisible by 4, so the same holds for $d(2b)^2$. In particular $db^2 \in \mathbb{Z}$ and $b \in \mathbb{Z}$ since d is squarefree. □

Lemma 38. *If* $a \notin \mathbb{Z}$ *then* $d = 1 \bmod 4$.

Proof. We have that $2a$, that is an integer, must be odd. By Lemmas 35 and 36, we have $(2a)^2 = d(2b)^2 \bmod 4$, so $2b$ must be odd and $d = 1 \bmod 4$ as required. □

Theorem 1. *Assume that* $d = 2 \bmod 4$ *or* $d = 3 \bmod 4$. *Then*

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$$

Proof. By Lemma 28 we know that $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. Let $t = a + b\sqrt{d} \in \mathcal{O}_K$, with $a, b \in \mathbb{Q}$. By Lemma 38 we have that $a \in \mathbb{Z}$ (since by Lemma 27 we cannot have $d = 1 \bmod 4$), and so by Lemma 37 we have $b \in \mathbb{Z}$, so $t \in \mathbb{Z}[\sqrt{d}]$. □

Lemma 39. *Assume that* $d = 1 \bmod 4$ *and take* $t = a + b\sqrt{d} \in \mathcal{O}_K$ *with* $a, b \in \mathbb{Q}$. *If* $a \in \mathbb{Z}$ *then* $t \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Proof. By Lemma 37 we have that $b \in \mathbb{Z}$ and so $t \in \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. □

Theorem 2. *Assume that* $d = 1 \bmod 4$. *Then*

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

Proof. By Lemma 29 we know that $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq \mathcal{O}_K$. Let $t = a + b\sqrt{d} \in \mathcal{O}_K$, with $a, b \in \mathbb{Q}$.

- If $a \in \mathbb{Z}$ we conclude by Lemma 39.
- If $a \notin \mathbb{Z}$, let us consider

$$t' = t - \frac{1+\sqrt{d}}{2} = a - \frac{1}{2} + \left(b - \frac{1}{2}\right)\sqrt{d} \in \mathcal{O}_K$$

  Since $2a \in \mathbb{Z}$ and $a \notin \mathbb{Z}$, we have that $a - \frac{1}{2} \in \mathbb{Z}$, so by Lemma 39, we have that $t' \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and so $t \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

□