Ring of Integers in a Quadratic Field

Courtney Guo

November 20

1 Ring of Integers Definition

Definition 1 Let \( \alpha = a + b\sqrt{D} \) be an element in \( \mathbb{Q}[\sqrt{D}] \). Then, let \( f_\alpha \) be the polynomial of degree 2 that has \( \alpha \) as a root:

\[
f_\alpha(x) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} = x^2 - 2a + (a^2 - Db^2)
\]

Definition 2 The ring of integers in a quadratic field \( \mathbb{Q}[\sqrt{D}] \) is defined as the set \( O(\sqrt{D}) \) such that \( f_\alpha \) has integer coefficients:

\[
O(\sqrt{D}) = \{ \alpha \mid f_\alpha \in \mathbb{Z}[x] \}
\]

which is equivalent to:

\[
O(\sqrt{D}) = \{ a + b\sqrt{D} \mid 2a \in \mathbb{Z}, a^2 - Db^2 \in \mathbb{Z} \}
\]

2 Casework on \( D \mod 4 \)

Theorem 1 If \( D \not\equiv 1 \mod 4 \), then the set \( O(\sqrt{D}) \) is the set \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \), the ring \( O(\sqrt{D}) \) is the union of the following sets:

\[
O(\sqrt{D}) = \{ a + b\sqrt{D} \mid a, b \in \mathbb{Z} \} \cup \{ a + b\sqrt{D} \mid a - \frac{1}{2}, b - \frac{1}{2} \in \mathbb{Z} \}
\]

Proof: We will show the two cases separately.

2.1 \( D \equiv 1 \mod 4 \)

To show this, we first consider the possible values of \( a \). We know that \( 2a \in \mathbb{Z} \), so either \( a \in \mathbb{Z} \) or \( a = \frac{p}{2} \) for some \( p \not\equiv 0 \mod 2 \).

If \( a \in \mathbb{Z} \):
We are given that \( a^2 - Db^2 \) is an integer. Since \( a \) is an integer, \( Db^2 \) must be an integer. Since \( D \) is square-free, \( b \) must be an integer. This set of solutions is the first set in the union in Theorem 1.
If $a = \frac{p^2}{2}$ for some odd $p$:
We are given that $a^2 - Db^2 = \frac{1}{4}(p^2 - 4Db^2)$ is an integer. Since $p^2$ is an integer, $4Db^2$ must be an integer, and since $D$ is square-free, $4b^2$ must be an integer. Therefore, $b$ must be of the form $\frac{q}{2}$ for some integer $q$. Then, our constraint becomes $\frac{1}{4}(p^2 - Dq^2) \in \mathbb{Z}$.

Since $\frac{1}{4}(p^2 - Dq^2)$ is an integer, we must have $p^2 \equiv Dq^2 \mod 4$. Since $p$ is odd, we must have $p^2 \equiv 1 \mod 4$, so we must have $Dq^2 \equiv 0 \mod 4$. We are given that $D \equiv 1 \mod 4$, so $q^2 \equiv 1 \mod 4$. This is true for any odd integer $q$. Therefore, if $a = \frac{p^2}{2}$ for some odd $p$, we get that $b = \frac{q}{2}$ for some odd $q$. This set of solutions is the second set in the union in Theorem 1.

Combining the two cases above, we see that $O(\sqrt{D})$ is the union of two sets that are exactly the two sets in Theorem 1.

2.2 $D \not\equiv 1 \mod 4$

Similar to the proof above, we first consider the possible values of $a$. We know that $2a \in \mathbb{Z}$, so either $a \in \mathbb{Z}$ or $a = \frac{p^2}{2}$ for some $p \not\equiv 0 \mod 2$.

If $a \in \mathbb{Z}$:
By the same argument in the previous section, if $a \in \mathbb{Z}$ then $b \in \mathbb{Z}$. Therefore this set of solutions is $\mathbb{Z}[\sqrt{D}]$.

If $a = \frac{p^2}{2}$ for some odd $p$:
We are given that $a^2 - Db^2$ is an integer. By the same argument from earlier, $b$ must be of the form $\frac{q}{2}$ for some integer $q$, and as before, we must have $p^2 \equiv Dq^2 \mod 4$. Since $p$ is odd, we must have $p^2 \equiv 1 \mod 4$, so we must have $Dq^2 \equiv 0 \mod 4$.

Since $q^2$ is a perfect square, we must have either $q^2 \equiv 1 \mod 4$ or $q^2 \equiv 0 \mod 4$. Since $Dq^2 \equiv 0 \mod 4$, we must have $q^2 \equiv 0 \mod 4$, which implies that $D \equiv 1 \mod 4$, a contradiction. Therefore, $a$ must be an integer, and there are no solutions for this case.

Therefore, $O(\sqrt{D})$ is equal to $\mathbb{Z}[\sqrt{D}]$.

3 The Ring Structure of $O(\sqrt{D})$

We’ve defined $O(\sqrt{D})$ and called it a ring, but we haven’t shown that it in fact is a ring. We will now show this, again for the two different cases of $D \equiv 1 \mod 4$ and $D \not\equiv 1 \mod 4$.

Theorem 2 The set $O(\sqrt{D})$ is a ring.
Proof: Again we will do casework on $D \mod 4$.

3.1 $D \not\equiv 1 \mod 4$

As shown in Theorem 1, when $D \not\equiv 1 \mod 4$, we have that $O(\sqrt{D}) = \mathbb{Z}[\sqrt{D}]$.

- Addition: $\alpha + \beta = a_1 + b_1\sqrt{D} + a_2 + b_2\sqrt{D} = (a_1 + a_2)\sqrt{D} + (b_1 + b_2)\sqrt{D}$. Since $\alpha + \beta$ has integer coefficients, $\mathbb{Z}[\sqrt{D}]$ is closed under addition.
Multiplication: $\alpha \beta = (a_1 + b_1 \sqrt{D})(a_2 + b_2 \sqrt{D}) = (a_1 a_2 + D b_1 b_2) + (a_1 b_2 + b_1 a_2) \sqrt{D}$. Since $\alpha \beta$ has integer coefficients, $\mathbb{Z}[\sqrt{D}]$ is closed under multiplication.

Addition and multiplication are clearly associative and commutative, and multiplication is clearly distributive. Additive and multiplicative identities are the same as those in $\mathbb{Z}$. Additive inverses exist because additive inverses exist in $\mathbb{Z}$.

Therefore, $\mathbb{Z}$ is a ring, so $O(\sqrt{D})$ is a ring when $D \not\equiv 1 \mod 4$.

### 3.2 $D \equiv 1 \mod 4$

Let’s define $\mathbb{Z}'[\sqrt{D}]$ to be the following set:

$$\mathbb{Z}'[\sqrt{D}] = \{(a + \frac{1}{2}) + (b + \frac{1}{2})\sqrt{D} \mid a, b \in \mathbb{Z}\}$$

Then, from Theorem 1, $O(\sqrt{D}) = \mathbb{Z}[\sqrt{D}] \cup \mathbb{Z}'[\sqrt{D}]$. We want to show that $O(\sqrt{D})$ is a ring, so we need to show that it is closed under addition and multiplication.

**Addition:**

- If $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$, then by the previous subsection, $\alpha + \beta \in \mathbb{Z}[\sqrt{D}] \in O(\sqrt{D})$.
- If $\alpha \in \mathbb{Z}[\sqrt{D}]$ and $\beta \in \mathbb{Z}'[\sqrt{D}]$: 
  $\alpha + \beta = a_1 + b_1 \sqrt{D} + (a_2 + \frac{1}{2}) + (b_2 + \frac{1}{2}) \sqrt{D} = (a_1 + a_2 + \frac{1}{2}) + (b_1 + b_2 + \frac{1}{2}) \sqrt{D}$ 
  Therefore, $\alpha + \beta \in \mathbb{Z}'[\sqrt{D}] \in O(\sqrt{D})$.
- If $\alpha \in \mathbb{Z}'[\sqrt{D}]$ and $\beta \in \mathbb{Z}[\sqrt{D}]$: 
  Addition is commutative, so by the same argument as above, $\alpha + \beta \in O(\sqrt{D})$.
- If $\alpha, \beta \in \mathbb{Z}'[\sqrt{D}]$: 
  $\alpha + \beta = (a_1 + \frac{1}{2}) + (b_1 + \frac{1}{2}) \sqrt{D} + (a_2 + \frac{1}{2}) + (b_2 + \frac{1}{2}) \sqrt{D} = (a_1 + a_2 + 1) + (b_1 + b_2 + 1) \sqrt{D}$ 
  Therefore, $\alpha + \beta \in \mathbb{Z}[\sqrt{D}] \in O(\sqrt{D})$.

**Multiplication:**

- If $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$, then by the previous subsection, $\alpha \beta \in \mathbb{Z}[\sqrt{D}] \in O(\sqrt{D})$.
- If $\alpha \in \mathbb{Z}[\sqrt{D}]$ and $\beta \in \mathbb{Z}'[\sqrt{D}]$: 
  $$\alpha \beta = (a_1 + b_1 \sqrt{D})((a_2 + \frac{1}{2}) + (b_2 + \frac{1}{2}) \sqrt{D})$$
  $$= (a_1 a_2 + D b_1 b_2 + \frac{1}{2}(a_1 + D b_1)) + (a_1 b_2 + a_2 b_1 + \frac{1}{2}(a_1 + b_1)) \sqrt{D}$$

Since we are given that $D \equiv 1 \mod 4$, we have that $a_1 + D b_1 \equiv a_1 + b_1 \mod 2$. If $a_1 + b_1 \equiv 0 \mod 2$, then $\alpha \beta \in \mathbb{Z}[\sqrt{D}]$. Otherwise, $\alpha \beta \in \mathbb{Z}'[\sqrt{D}]$. Therefore, regardless of the value of $a_1 + b_1 \mod 2$, we have that $\alpha \beta \in O(\sqrt{D})$.
- If $\alpha \in \mathbb{Z}'[\sqrt{D}]$ and $\beta \in \mathbb{Z}[\sqrt{D}]$: 
  Multiplication is commutative, so by the same argument as above, $\alpha \beta \in O(\sqrt{D})$. 

3
If $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$:

$$\alpha \beta = ((a_1 + \frac{1}{2}) + (b_1 + \frac{1}{2})\sqrt{D})((a_2 + \frac{1}{2}) + (b_2 + \frac{1}{2})\sqrt{D})$$

$$= (a_1a_2 + Db_1b_2 + \frac{1}{2}(a_1 + a_2 + Db_1 + Db_2 + \frac{D+1}{2}))$$

$$+ (a_1b_2 + a_2b_1 + \frac{1}{2}(a_1 + a_2 + b_1 + b_2 + 1))\sqrt{D}$$

We know that $D \equiv 1 \mod 4$, so $Db_1 + Db_2 \equiv b_1 + b_2 \mod 2$. Also, we know that $\frac{D+1}{2} \equiv 1 \mod 2$. Therefore, $a_1 + a_2 + Db_1 + Db_2 + \frac{D+1}{2} \equiv a_1 + a_2 + b_1 + b_2 + 1 \mod 2$. This means that $\alpha \beta$ is in either $\mathbb{Z}[\sqrt{D}]$ or $\mathbb{Z}'[\sqrt{D}]$, so $\alpha \beta \in O(\sqrt{D})$.

The other properties of a ring (associativity, commutativity, identities, additive inverse) are all true with the same arguments as before.