1 Quadratic Fields

A *quadratic field* is defined as $\mathbb{Q}(\sqrt{-d}) = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Q}\}$ where $d \in \mathbb{Z}$. It can be verified to be a field over $\mathbb{Q}$ with the usual operations of $+, \times$, with respective identities $0, 1$ and inverses $-a - b\sqrt{-d}$ and $\frac{a}{a^2+b^2d} - \frac{b}{a^2+b^2d}\sqrt{-d}$.

An *integer* in a field is defined to be any element of the field which is the root of a *monic* polynomial with coefficients in $\mathbb{Z}$. The set of integers in a quadratic field form a ring. We will denote the ring of integers in $\mathbb{Q}(\sqrt{-d})$ by $\mathbb{Z}(\sqrt{-d})$.

Lemma 1.1. *1. If $d = 0$, i.e. $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q}$, then $\mathbb{Z}(\sqrt{-d}) = \mathbb{Z}$.*

2. If $d \equiv 1, 2 \mod 4$, then $\mathbb{Z}(\sqrt{-d}) = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$.

3. If $d \equiv 3 \mod 4$, then $\mathbb{Z}(\sqrt{-d}) = \{a + b\frac{1+\sqrt{-d}}{2} \mid a, b \in \mathbb{Z}\}$.

Note that if $d \equiv 0 \mod 4$, then $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(\sqrt{-d/4})$, so this case is covered by the above cases.

Proof. The elements of the given sets are integers in their respective fields:

1. Every $z \in \mathbb{Z}$ is the root of the monic polynomial $x - z$.
2. If $d \equiv 1, 2 \mod 4$, then $a + b\sqrt{-d}$ is a root of the monic polynomial $x^2 - 2ax + a^2 + db^2$.
3. If $d \equiv 3 \mod 4$, then $a + b\frac{1+\sqrt{-d}}{2}$ is a root of the monic polynomial $x^2 - (2a + b)x + a^2 + ab + \frac{d+1}{4}b^2$, and $\frac{d+1}{4} \in \mathbb{Z}$ as $4 \mid (d + 1)$.

Conversely these are the only integers because if x is a root of a monic polynomial $P(x)$ with integer coefficients, then:

- Irrational or complex roots of rational polynomials occur in conjugate pairs so x must be the root of a linear or quadratic factor of $P(x)$, where the coefficients of the factors are in $\mathbb{Q}$.
- The factors of an integer polynomial can be made to be monic with integer coefficients. This is Gauss' Lemma. Proof: Let $P(x) = Q(x)R(x)$, where $Q(x), R(x)$ are monic (we can assure this by dividing by the leading coefficients of $Q(x)$ and $R(x)$). Then there exist smallest positive integers m, n such that $mQ(x)$ and $nR(x)$ are integer polynomials, say $Q'(x) = mQ(x)$ and $R'(x) = nR(x)$. Thus $mnP(x) = Q'(x)R'(x)$. Now if $p|mn$, and p is a prime, then p divides all the coefficients of $mnP(x)$. Now suppose q_i, r_j are the first coefficients of $Q'(x), R'(x)$ such that $p \nmid q_i, p \nmid r_j$. Then p does not divide the coefficient of x^{i+j} in the product, which is a contradiction. Hence p must divide all the coefficients of $Q'(x)$ or all the coefficients of $R'(x)$. But this means that either m or n was not the smallest possible integers, as assumed. Hence $Q(x)$ and $R(x)$ must be integer polynomials.

- If a factor is linear monic with coefficients in $\mathbb{Z}$, then its root is in $\mathbb{Z}$, which is in the sets above for any d. Otherwise let the factor be $x^2 - ax + b$, $a, b \in \mathbb{Z}$. Its root is $x = \frac{a+\sqrt{a^2-4b}}{2}$ (the other root is analogous). In this case:

  1. If $d = 0$, then for x to be in $\mathbb{Q}$, $a^2 - 4b$ must be a square. If a is even, then the square root is even, so $x \in \mathbb{Z}$. If a is odd, then the square root is also odd, so $a + \sqrt{a^2 - 4b}$ is even, and again $x \in \mathbb{Z}$.
  2. If $d \equiv 1, 2 \mod 4$, and $a^2 - 4b$ is not a square, then $x \in \mathbb{Q}(\sqrt{-d})$ iff $a^2 - 4b = -m^2 d$ for some $m \in \mathbb{Z}$. If a is even, then m is even, and $x = \frac{a}{2} + \frac{m}{2}\sqrt{-d}$, which is in $\mathbb{Z}(\sqrt{-d})$. If a is odd and $a^2 = 4b - m^2 d$, then $a^2 \equiv 1 \mod 4$, whereas $4b - m^2 d \equiv 0, 2, 3 \mod 4$, which is not possible.
  3. If $d \equiv 3 \mod 4$, then as before $a^2 - 4b = -m^2 d$. In this case if a is odd, we get $x = \frac{a}{2} + \frac{m}{2}\sqrt{-d}$, where a, m are both odd. Then $x = \frac{a-m}{2} + m\frac{1+\sqrt{-d}}{2}$, which is in $\mathbb{Z}(\sqrt{-d})$.

$\square$

For any elements a, b in a ring R, define $a|b$ if there exists $c \in R$ such that $ac = b$. A *unit* $u \in R$ is any element such that $u|1$. For example in the ring $\mathbb{Z}$, the only units are ± 1, whereas in the ring $\mathbb{Z}(i)$ the units are $\pm 1, \pm i$. Note that the set of units in a ring form a subgroup of the ring. Two elements $a, b \in R$ are said to be associates if $a = ub$ where u is a unit in R. A *prime* $p \in R$ is any element which is not a unit such that $a|p$ iff a is a unit or an associate of p.

A ring R is a unique factorization domain if every integer can be written as a product of primes in a unique way, up to reorderings, units and associates.

2 Case $d = 0$ — Unique Factorization in $\mathbb{Z}$

Lemma 2.1. *Given any $a, b \in \mathbb{Z}$, $b \neq 0$, there exists $q, r \in \mathbb{Z}$ such that $a = bq + r$, and $|r| < |b|$.*

Proof. Consider $\frac{a}{b}$. This is an element of $\mathbb{Q}$, and hence lies between two consecutive elements of $\mathbb{Z}$. Thus there is some $q \in \mathbb{Z}$ such that $|\frac{a}{b} - q| < 1$. Multiplying by $|b|$, we have $|b||\frac{a}{b} - q| = |a - bq| < |b|$. Set $r = a - bq$, then q, r have the required property. $\square$

The gcd of $a, b \in \mathbb{Z} - \{0\}$ is any element $d \in \mathbb{Z}, d|a, d|b$ such that for any other element $d' \in \mathbb{Z}, d'|a, d'|b \Rightarrow d'|d$.

Lemma 2.2. *If d is a gcd of $a, b \in \mathbb{Z}$ then $d = ax + by$ for some $x, y \in \mathbb{Z}$.*

Proof. The proof follows by Euclid's algorithm and Lemma 2.1. $\square$

Lemma 2.3. *If $p \in \mathbb{Z}$ is a prime, then $p|ab$ implies $p|a$ or $p|b$.*

Proof. Suppose $p|ab$, and w.l.o.g. assume $p \nmid a$. Then 1 is a gcd of a, p, because if $d|a, d|p$, then d is a unit or an associate of p, but it cannot be an associate as $p \nmid a$ - so it is a unit i.e. $d|1$. By Lemma 2.2, $1 = ax + py$. Thus $b = abx + pby$. Since $p|abx, p|pby$, we have $p|b$. $\square$

Theorem 2.4. *$\mathbb{Z}$ is a unique factorization domain.*

Proof. Every element of $\mathbb{Z}$ is either prime, or the product of two numbers which are themselves products of primes. Hence inductively, every number can be written as a product of primes. If $n = p_1 p_2 \dots p_m = q_1 q_2 \dots q'_m$, where the p_i, q_j's are primes, then $p_1 | q_1 q_2 \dots q'_m$, so by Lemma 2.3 $p_1 | q_j$ for some $j \in 1 \dots m'$. Thus p_1 is an associate of q_j. Cancelling these out on both sides and repeating shows us that the prime factorization is unique. $\square$

3 Case $d = 1, 2$ — Unique Factorization in $\mathbb{Z}(i), \mathbb{Z}(\sqrt{-2})$

We only need to establish the analog of Lemma 2.1 for $\mathbb{Z}(i)$ and $\mathbb{Z}(\sqrt{-2})$ - the rest of the proof follows the case $d = 0$. Define the norm on $\mathbb{Q}(\sqrt{-d})$ as a function $N : \mathbb{Q}(\sqrt{-d}) \to \mathbb{Q}$ defined by $N(a + b\sqrt{-d}) = a^2 + db^2$. This has the following properties:

- $N(z) \geq 0$ and $N(z) = 0 \leftrightarrow z = 0$.
- $N(z) = 1$ iff z is a unit.
- $N(ab) = N(a)N(b)$.

Lemma 3.1. *For $d = 1, 2$, given any $a, b \in \mathbb{Z}(\sqrt{-d})$, $b \neq 0$, there exists $q, r \in \mathbb{Z}(\sqrt{-d}))$ such that $a = bq + r$, and $N(r) < N(b)$.*

Proof. The proof is analogous to the proof of Lemma 2.1. Consider $\gamma = \frac{a}{b}$. Then since $\mathbb{Q}(\sqrt{-d})$ is a field, $\gamma \in \mathbb{Q}(\sqrt{-d})$. Let $\gamma = x + y\sqrt{-d}$, where $x, y \in \mathbb{Q}$. Thus there exist $m, n \in \mathbb{Z}$ such that $|x - m| \leq \frac{1}{2}$ and $|y - n| \leq \frac{1}{2}$. Let $q = m + n\sqrt{-d}$. Thus

$$N(\gamma - q) = N((x - m) + (y - n)\sqrt{-d}) = (x - m)^2 + d(y - n)^2 \leq \frac{1 + d}{4} < 1$$

Thus $N(a - bq) = N(b(\gamma - q)) = N(b)N(\gamma - q) < N(b)$. Set $r = a - bq$ to get q, r that satisfy the properties required in the lemma. $\square$

4 Case $d = 3, 7, 11$ — Unique Factorization in $\mathbb{Z}(\sqrt{-3})$, $\mathbb{Z}(\sqrt{-7})$, $\mathbb{Z}(\sqrt{-11})$

Note that the above proof does not work since we showed that $N(\gamma - q) \leq \frac{1+d}{4}$, but this is less than 1 for $d \leq 2$. However if $d \equiv 3 \mod 4$, we have $\mathbb{Z}(\sqrt{-d}) = \{a + b\frac{1+\sqrt{-d}}{2} \mid a, b \in \mathbb{Z}\}$. A more careful analysis will show that in this case, $N(\gamma - q) \leq \frac{(1+d)^2}{16d}$, which is less than 1 for $d \leq 14$ and hence proves unique factorization for $d = 3, 7, 11$.

Lemma 4.1. *For $d = 3, 7, 11$, given any $a, b \in \mathbb{Z}(\sqrt{-d})$, $b \neq 0$, there exists $q, r \in \mathbb{Z}(\sqrt{-d}))$ such that $a = bq + r$, and $N(r) < N(b)$.*

Proof. As above, consider $\gamma = \frac{a}{b}$, once again, since $\gamma \in \mathbb{Q}(\sqrt{-d})$, we have $\gamma = x + y\sqrt{-d}$, where $x, y \in \mathbb{Q}$. Let us plot the elements of $\mathbb{Z}(\sqrt{-d})$ — these form a lattice in the plane as shown in Section 4. Each point in $\mathbb{Q}(\sqrt{-d})$ lies in one of the lattice cells. We can now compute the points in a cell that are maximally far from the vertices. Consider the cell with vertices $(0, 0), (1, 0), (0, 1), (1, -1)$. By symmetry and using basic calculus, we can see that the point farthest from all will lie on the vertical line connecting $(0, 1), (1, -1)$ and will be equidistant from $(0, 0), (0, 1)$ which correspond to the integers $0, \frac{1}{2} + \frac{\sqrt{-d}}{2}$. Let the point be $\frac{1}{2} + x\sqrt{-d}$. Then equating the norms to the two integers, we have $\frac{1}{4} + dx^2 = d(x - \frac{1}{2})^2$. Solving this we get $x = \frac{d-1}{4d}$, and its distance from the lattice points is $\frac{(1+d)^2}{16d}$.

Thus there is an element $q \in \mathbb{Z}(\sqrt{-d})$, such that $N(\gamma - q) \leq \frac{(1+d)^2}{16d} < 1$ for $d \leq 14$. Then by repeating the above argument, we get $N(a - bq) < N(b)$, and setting $r = a - bq$ we have the result. □

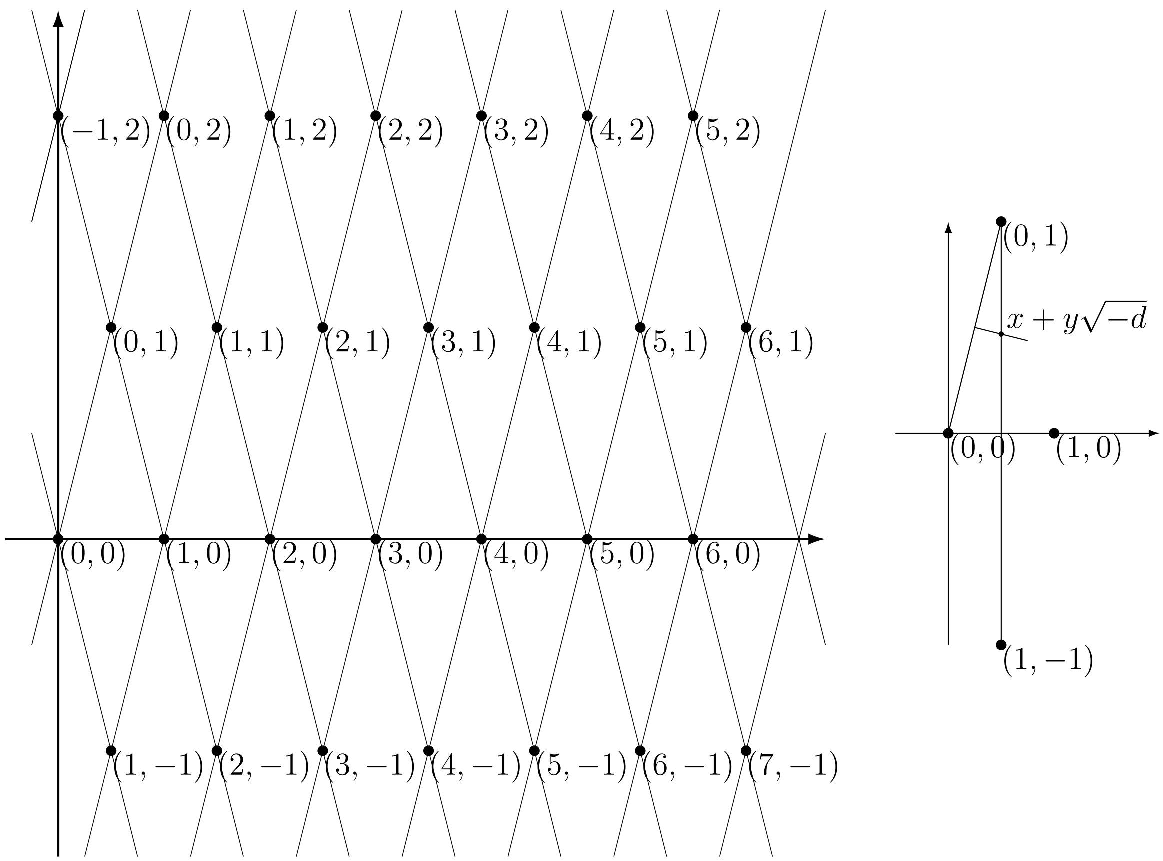

Figure 1: Left: Lattice of integers in $\mathbb{Z}(\sqrt{-d})$. Each point (a, b) represents the integer $a + b\frac{1+\sqrt{-d}}{2}$. Right: one lattice cell, with the point farthest from the lattice points.

5 Failure of Unique Factorization for $\mathbb{Z}(\sqrt{-5})$, $\mathbb{Z}(\sqrt{-6})$, $\mathbb{Z}(\sqrt{-10})$

The proof for $d = 1, 2$ did not work for any greater d, since it required $d + 1 < 4$. The proof for $d = 3, 7, 11$ worked only for these numbers because it required $d \equiv 3 \mod 4$ and $(d+1)^2 < 16d$. Thus we do not have a proof for $d = 5, 6, 10, 13, 14$ or any number larger than 14. Note that we do not consider d which have a square factor, as these are equivalent to smaller d. We now show that unique factorization fails for $d = 5, 6, 10, 13, 14$. The key fact we need is that $N(z)$ is multiplicative: $N(ab) = N(a)N(b)$.

$d = 5$: Observe that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. $N(2) = 4$, thus the only integers in $\mathbb{Z}(\sqrt{-5})$ that can divide 2 and are not units or associates must have norm 2. However since $N(a + b\sqrt{-5}) = a^2 + 5b^2$, and $a, b \in \mathbb{Z}$, we see that b must be 0, and hence there is no such a. Thus 2 is prime in $\mathbb{Z}(\sqrt{-5})$. Similarly we can verify that 3 is prime as there are no elements in $\mathbb{Z}(\sqrt{-5})$ with norm 3, and so are $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$, whose norms are 6. Thus 6 has two distinct factorizations in $\mathbb{Z}(\sqrt{-5})$.

$d = 6$: $10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$. Once again $\mathbb{Z}(\sqrt{-6})$ has no elements with norm 2 or 5, thus $2, 5, 2 + \sqrt{-6}, 2 - \sqrt{-6}$ are all prime in $\mathbb{Z}(\sqrt{-6})$.

$d = 10$: We use $14 = 2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10})$. Since $\mathbb{Z}(\sqrt{-10})$ has no elements with norm 2 or 7, the factors are all primes.

$d = 13$: Observe that $14 = 2 \cdot 7 = (1 + \sqrt{-13})(1 - \sqrt{-13})$. The conclusion follows as above.

$d = 14$: Observe that $15 = 3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$. The conclusion follows as above.

Unique factorization can be restored for these domains by considering ideals in the domains, we shall not consider those here.

For $d < 0$, there are infinitely many values for which unique factorization holds in $\mathbb{Z}(\sqrt{-d})$. However for $d > 0$, the only values for which unique factorization holds in $\mathbb{Z}(\sqrt{-d})$ are $d = 1, 2, 3, 7, 11$ (proved above) and $d = 19, 43, 67, 163$. We now turn to these remaining values.