

# IMAGINARY QUADRATIC FIELDS

DAVID SAVITT

## 1. LATTICES

We begin by recalling some basic facts about lattices. If  $v \in \mathbb{R}^n$ , let  $\|v\|$  denote the length of the vector  $v$ .

**Definition 1.1.** A set  $\Lambda \subset \mathbb{R}^n$  is a *lattice* if there exist linearly independent vectors  $v_1, \dots, v_n \in \mathbb{R}^n$  such that

$$\Lambda = \{m_1 v_1 + \dots + m_n v_n \mid m_i \in \mathbb{Z}\}.$$

In that case  $v_1, \dots, v_n$  are said to be a *basis* of  $\Lambda$ , and we will write  $\Lambda = [v_1, \dots, v_n]$ .

**Fact 1.2.** A set  $\Lambda \subset \mathbb{R}^n$  is a lattice if and only if

- $\Lambda$  is a group under addition (componentwise), i.e. if  $v_1, v_2$  are in  $\Lambda$  then  $v_1 + v_2$  and  $-v_1$  are in  $\Lambda$ ,
- $\Lambda$  is discrete, i.e., there exists  $\epsilon > 0$  so that  $\Lambda \cap \{v \in \mathbb{R}^n \mid \|v\| < \epsilon\} = \{0\}$ , and
- the vectors in  $\Lambda$  span  $\mathbb{R}^n$ .

(Without the third condition,  $\Lambda$  could live in a subspace of  $\mathbb{R}^n$  or even be  $\{0\}$ .)

**Fact 1.3.** For any distance  $d$ , the set  $\Lambda \cap \{v \in \mathbb{R}^n \mid \|v\| < d\}$  is finite.

**Fact 1.4.** If  $v \in \Lambda$  and there is no  $v' \in \Lambda$  such that  $v = kv'$  for some integer  $k > 1$ , then there is a basis for  $\Lambda$  which includes  $v$ .

## 2. ORDERS

**Definition 2.1.** A lattice  $\Lambda \subset \mathbb{C} = \mathbb{R}^2$  is called an *order* if  $1 \in \Lambda$  and if  $v, w \in \Lambda$  implies  $vw \in \Lambda$ .

**Proposition 2.2.** If  $\Lambda$  is an order, then there exists  $\tau \in \mathbb{C}$  so that  $\Lambda = [1, \tau]$ .

*Proof.* If  $\Lambda$  is an order, we will show that  $\Lambda \cap \mathbb{R} = \mathbb{Z}$ ; then the proposition follows by Fact 1.4 (there is a basis which includes 1). Since  $1 \in \Lambda$ , we know  $\mathbb{Z} \subset \Lambda \cap \mathbb{R}$ . Conversely, suppose that  $r \in \Lambda \cap \mathbb{R}$  is not an integer. Then the fractional part  $\{r\}$  of  $r$  is also in  $\Lambda$ , hence  $\{r\}^k \in \Lambda$  for all  $k > 0$ , since orders are closed under multiplication. Hence the intersection  $\Lambda \cap \{z \in \mathbb{C} \mid |z| < 1\}$  is infinite, contradicting Fact 1.3.  $\square$

**Proposition 2.3.** *The lattice with basis  $1, \tau$  is an order if and only if  $\tau$  is a complex quadratic algebraic integer, i.e.,  $\tau$  is the root of a monic quadratic polynomial with integer coefficients and negative discriminant.*

*Proof.* Suppose  $\tau \in \mathbb{C}$  is not real, and let  $\Lambda = [1, \tau]$ . To decide whether  $\Lambda$  is an order, we need to check if it is closed under multiplication; for this, it is necessary and sufficient that  $\tau^2 \in \Lambda$ . But  $\tau^2 \in \Lambda$  if and only if  $\tau^2 = b\tau + c$  for some integers  $c, b$ , i.e. if and only if  $\tau$  is the root of a monic quadratic polynomial with integer coefficients. Since  $\tau$  is not real, the discriminant must be negative.  $\square$

**Fact 2.4.** *Every complex quadratic algebraic integer is of the form  $a + b\sqrt{d}$  with  $a, b, d \in \mathbb{Z}$  and  $d < 0$  or of the form  $\frac{1}{2}(a + b\sqrt{d})$  with  $a, b$  odd integers and  $d \equiv 1 \pmod{4}$  a negative integer.*

Therefore if  $\Lambda = [1, \tau]$  is an order,  $\tau$  has the above form. Noting that we also have  $\Lambda = [1, m + \tau]$  for any integer  $m$ , we may assume without loss of generality that  $\tau = b\sqrt{d}$  for  $d < 0$ , or  $\tau = \frac{1}{2}(1 + b\sqrt{d})$  for  $b$  odd and  $d \equiv 1 \pmod{4}$  and negative. Absorbing  $b$  into the square root, we conclude the following theorem:

**Theorem 2.5.** *Every order  $\Lambda$  has one of the following two forms:  $\Lambda = [1, \sqrt{d}]$  for some integer  $d < 0$ , or else  $\Lambda = [1, \frac{1}{2}(1 + \sqrt{d})]$  for  $d \equiv 1 \pmod{4}$  and negative.*

We can check easily that the orders described in the above theorem are all distinct; for example, their fundamental regions all have different volumes. (For  $[1, \sqrt{d}]$  this volume is  $\sqrt{|d|}$ , while for  $[\frac{1}{2}(1 + \sqrt{d})]$  it is  $\frac{1}{2}\sqrt{|d|}$ .)

Let  $\Lambda$  be an order. We want to consider special sublattices of  $\Lambda$  called *ideal sublattices* (or simply *ideals*):

**Definition 2.6.** A lattice  $I \subset \Lambda$  is called an ideal if  $vw \in I$  for all  $v \in \Lambda$  and  $w \in I$ . That is, the sublattice  $I$  is closed under multiplication by *all* of  $\Lambda$ .

**Example 2.7.** If  $\lambda \in \Lambda$ , we can form the set  $\lambda\Lambda = \{\lambda w \mid w \in \Lambda\}$ . This is a lattice by Fact 1.2:  $\lambda\Lambda$  is a group under addition, it is discrete (for example, because it is a subset of  $\Lambda$ ), and it spans. Indeed, it is also an ideal, because if  $\lambda w \in \lambda\Lambda$  and  $v \in \Lambda$  then  $(\lambda w)v = \lambda(vw) \in \lambda\Lambda$ . We call  $\lambda\Lambda$  the *principal ideal generated by  $\lambda$* , and will often denote it by  $(\lambda)$ .

We can add and multiply ideals:

**Definition 2.8.** If  $I, I'$  are ideals of an order  $\Lambda$ , we set

$$I + I' = \{v + w \mid v \in I, w \in I'\}.$$

We cannot simply define  $II'$  as  $\{vw \mid v \in I, w \in I'\}$ , as this would not be a lattice (try to prove that it is!) so we modify this as follows:

$$II' = \left\{ \sum_i v_i w_i \mid v_i \in I, w_i \in I' \right\},$$

so that  $II'$  consists of *finite sums* of products of elements from  $I$  and  $I'$ .

**Proposition 2.9.**  *$I + I'$  and  $II'$  are both ideals.*

*Proof.* They are both groups under addition, they are both discrete (since they are contained in  $\Lambda$ ), and they both span  $\mathbb{C}$ , so they are both lattices by Fact 1.2. It is similarly straightforward to check that they are closed under multiplication by  $\Lambda$ , so they are indeed ideals.  $\square$

**Definition 2.10.** An ideal  $I \subset \Lambda$  is *prime* if  $I \neq \Lambda$  and there are no ideals  $I'$  satisfying  $I \subsetneq I' \subsetneq \Lambda$ .

**Proposition 2.11.** *If  $I$  is a prime,  $v, w \in \Lambda$ , and  $vw \in I$ , then either  $v \in I$  or  $w \in I$ .*

*Proof.* Suppose  $v, w \notin I$ . Let  $I_v = (v) + I$  and  $I_w = (w) + I$ . Since  $v \notin I$ , we have  $I \subsetneq I_v$ , so  $I_v = \Lambda$  since  $I$  is prime. Similarly  $I_w = \Lambda$ . But then  $I_v I_w = \Lambda \Lambda = \Lambda$ . However, we also have

$$I_v I_w = ((v) + I)((w) + I) \subset (vw) + (v)I + (w)I + II \subset I$$

since  $vw \in I$ , and this is a contradiction.  $\square$

**Proposition 2.12.** *If  $I$  is a prime and  $J, J'$  are ideals such that  $JJ' \subset I$ , then either  $J \subset I$  or  $J' \subset I$ .*

*Proof.* Suppose  $J \not\subset I$ , so there is some  $v$  in  $J$  which is not in  $I$ . Suppose  $w \in J'$ . Since  $JJ' \subset I$ , we have  $vw \in I$ . By the previous proposition, since  $v \notin I$  we have  $w \in I$ . Thus  $J' \subset I$ .  $\square$

We have thus motivated the following definition:

**Definition 2.13.** If  $I \subset I'$  are ideals in an order  $\Lambda$ , we say that  $I'$  *divides*  $I$  if there is an ideal  $J$  so that  $I'J = I$ . We say that  $I$  has a *prime factorization* if there are primes  $I_1, \dots, I_k$  so that  $I = I_1 \cdots I_k$ .

### 3. UNIQUE FACTORIZATION OF IDEALS IN MAXIMAL ORDERS

Suppose that  $d < 0$  is not square-free, say  $d = b^2 d'$  with  $b > 1$ . Then the lattice  $[1, \sqrt{d}] = [1, b\sqrt{d'}] \subsetneq [1, \sqrt{d'}]$ ; in fact, if  $d < 0$  is square-free but is  $1 \pmod{4}$ , then we even have  $[1, \sqrt{d}] \subsetneq [1, \frac{1}{2}(1 + \sqrt{d})]$ . Similarly, if  $d = b^2 d' < 0$  is not square-free and is  $1 \pmod{4}$ , then  $[1, \frac{1}{2}(1 + \sqrt{d})] \subsetneq [1, \frac{1}{2}(1 + \sqrt{d'})]$ . So, we define:

**Definition 3.1.** The orders

$$[1, \sqrt{d}]$$

with  $d < 0$  and  $d \not\equiv 1 \pmod{4}$  and

$$[1, \frac{1}{2}(1 + \sqrt{d})]$$

with  $d < 0$  and  $d \equiv 1 \pmod{4}$  are called *maximal orders*.

The remarkable theorem is:

**Theorem 3.2.** *If  $\Lambda$  is a maximal order, then every nonzero ideal in  $\Lambda$  has a unique factorization into prime ideals.*

To prove this theorem, we require a simple lemma with an ugly proof, which give in the following subsection.

**3.1. Norms.** If  $\Lambda$  is an order and  $I$  is an ideal in  $\Lambda$ , then both are lattices, so we can associate to each a volume. We have

**Definition 3.3.** The *norm* of the ideal  $I$  is defined to be

$$\text{Norm}(I) = \text{vol}(I)/\text{vol}(\Lambda).$$

Note that  $\text{Norm}(I) = 1$  implies that  $\text{vol}(I) = \text{vol}(\Lambda)$ ; since  $I \subset \Lambda$ , this forces  $I = \Lambda$ .

If  $I$  is an ideal in  $\Lambda$ , let  $\bar{I}$  be the complex conjugate of  $I$ ; that is,

$$\bar{I} = \{\bar{z} \mid z \in I\}.$$

It is not difficult to see that  $\bar{I}$  is also an ideal in  $\Lambda$ . The aforementioned ugly lemma is:

**Lemma 3.4.** *If  $\Lambda$  is a maximal order and  $I$  is an ideal in  $\Lambda$ , then  $\text{Norm}(I)$  is an integer and*

$$I\bar{I} = (\text{Norm}(I)),$$

where the right-hand side is the ideal generated by  $\text{Norm}(I)$ .

*Proof.* If  $z \in I$ , then since  $I$  is an ideal we have  $\bar{z}z \in I$ , so  $I$  contains an integer. Let  $n$  be the smallest positive integer contained in  $I$ . By Fact 1.4, we know that  $I = [n, \tau]$  for some non-real  $\tau \in I$ . Let's restrict ourselves to the case where the maximal order  $\Lambda = [1, \sqrt{d}]$  for some  $d < 0$  that is not  $1 \pmod{4}$ ; the proof in the case  $\Lambda = [1, \frac{1}{2}(1 + \sqrt{d})]$  with  $d < 0$  and  $d \equiv 1 \pmod{4}$  will be similar. Then

$$I = [n, a + b\sqrt{d}]$$

for  $a, b \in \mathbb{Z}$ . Now  $\text{vol}(I) = nb\sqrt{|d|}$  and  $\text{vol}(\Lambda) = \sqrt{|d|}$ , so  $\text{Norm}(I) = nb$  is an integer, which proves the first claim of the lemma.

The fact that  $I$  is an ideal places restrictions on  $a$ ,  $b$ , and  $n$ : indeed, the fact that  $n\sqrt{d}$  must be in  $I$  forces  $b$  to divide  $n$ , and the fact that  $\sqrt{d}(a + b\sqrt{d}) \in I$  forces  $b$  to divide  $a$ . Factoring out  $b$ , we write

$$I = (b)[n', a' + \sqrt{d}].$$

with  $n' = n/b$  and  $a' = a/b$ . Then the fact that  $(a' + \sqrt{d})(a' - \sqrt{d}) \in [n', a' + \sqrt{d}]$  forces  $n'$  to divide  $(a')^2 - d$ . Now

$$\bar{I} = (b)[n', a' - \sqrt{d}].$$

so

$$I\bar{I} = (b^2)[(n')^2, n'(a' + \sqrt{d}), n'(a' - \sqrt{d}), (a')^2 - d],$$

and we may factor out  $n'$  from the right-hand side and write

$$\begin{aligned} I\bar{I} &= (b^2 n') [n', a' + \sqrt{d}, a' - \sqrt{d}, \frac{(a')^2 - d}{n'}] \\ &= (nb) [n', 2a', \frac{(a')^2 - d}{n'}, a' + \sqrt{d}]. \end{aligned}$$

We must show that the ideal  $[n', 2a', \frac{(a')^2-d}{n'}, a' + \sqrt{d}]$  contains 1: any ideal which contains 1 automatically is equal to  $\Lambda$ , and so we would then have  $I\bar{I} = (nb) = (\text{Norm}(I))$ , as desired.

Suppose a prime  $p$  divides  $n'$ ,  $2a'$ , and  $((a')^2 - d)/n'$ . Then  $p^2$  divides  $(a')^2 - d$ . If  $p$  is odd, then  $p$  divides  $a'$ , so  $p^2$  divides  $(a')^2$  and consequently  $p^2$  divides  $d$ , contradicting that  $d$  is square-free. If  $p$  is even, then either  $a'$  is even, in which case we get the same contradiction as in the case  $p$  odd, or else  $a'$  is odd. But since  $(a')^2 - d$  is divisible by  $2^2 = 4$ , we would have  $d \equiv (a')^2 \equiv 1 \pmod{4}$ , contradicting our assumption that  $d$  is *not*  $1 \pmod{4}$ . Thus no prime divides all three of  $n'$ ,  $2a'$ , and  $(a')^2 - d)/n'$ , and the ideal  $[n', 2a', \frac{(a')^2-d}{n'}, a' + \sqrt{d}]$  must contain 1. This completes the proof in the case of  $\Lambda[1, \sqrt{d}]$ . The proof in the case  $\Lambda = [1, \frac{1}{2}(1 + \sqrt{d})]$  with  $d < 0$  and  $d \equiv 1 \pmod{4}$  is left as an exercise for the reader.  $\square$

Here is a useful consequences of this lemma:

**Proposition 3.5.** *If  $I, I'$  are ideals, then  $\text{Norm}(II') = \text{Norm}(I)\text{Norm}(I')$ .*

*Proof.* We compute

$$(\text{Norm}(II')) = II'\overline{II'} = (I\bar{I})(I'\bar{I}') = (\text{Norm}(I))(\text{Norm}(I')) = (\text{Norm}(I)\text{Norm}(I')),$$

whence the desired equality.  $\square$

**3.2. The proof of unique factorization.** We can now prove that if  $\Lambda$  is a maximal order, then non-zero ideals can be factored uniquely into prime ideals. We begin with a crucial observation:

**Lemma 3.6.** *If  $I \subset I'$ , then  $I'$  divides  $I$ ; that is, there exists  $J$  such that  $I'J = I$ .*

*Proof.* Note that  $I'\bar{I}' = (\text{Norm}(I'))$ , and so

$$I\bar{I} \subset I'\bar{I}' = (\text{Norm}(I')).$$

Thus every element in  $I\bar{I}$  is a multiple of  $\text{Norm}(I')$ , so we take

$$J = \frac{1}{\text{Norm}(I')} I\bar{I} \subset \Lambda.$$

Then

$$I'J = \frac{1}{\text{Norm}(I')} I\bar{I}I' = \frac{1}{\text{Norm}(I')} (\text{Norm}(I'))I = I.$$

as desired.  $\square$

Here are two immediate consequences for prime ideals.

**Proposition 3.7.** *An ideal  $I$  in a maximal order is prime if and only if for all factorizations  $I = JJ'$ , one of  $J$  and  $J'$  is  $\Lambda$ .*

*Proof.* If  $I$  is prime and  $I = JJ'$ , then  $J, J'$  both divide  $I$ , and in particular both contain  $I$ . Therefore  $J$  and  $J'$  are either  $I$  or  $\Lambda$ . But  $II \subsetneq I$  (why?), so one of  $J, J'$  must be  $\Lambda$ . Conversely, suppose  $I$  is not prime. Then there is some  $J$  satisfying

$I \subsetneq J \subsetneq \Lambda$ , and by Lemma 3.6 there exists  $J'$  so that  $JJ' = I$ . Since neither  $J$  nor  $J'$  can be  $\Lambda$ , this completes the proof.  $\square$

**Proposition 3.8.** *If  $I$  is a prime and  $I$  divides  $JJ'$ , then  $I$  divides  $J$  or  $I$  divides  $J'$ .*

*Proof.* If  $I$  divides  $JJ'$ , then  $JJ'$  is contained in  $I$ . By Proposition 2.12, we know that either  $J$  is contained in  $I$  or  $J'$  is contained in  $I$ . But if  $J$  is contained in  $I$ , then by Lemma 3.6 we know  $I$  divides  $J$ ; similarly, if  $J'$  is contained in  $I$  then  $I$  divides  $J'$ .  $\square$

Inductively, it follows that if a prime ideal  $I$  divides a product  $J_1 \cdots J_j$ , then  $I$  divides some  $J_l$ .

Now, suppose  $I$  is a non-zero ideal. We prove by induction on  $\text{Norm}(I)$  that  $I$  can be factored into prime ideals. If  $\text{Norm}(I) = 1$ , then  $I = \Lambda$ , the trivial factorization. The rest of the base case is:

**Proposition 3.9.** *If  $\text{Norm}(I)$  is prime, then  $I$  is prime. (Caution: the converse to this statement is false.)*

*Proof.* Suppose  $I = JJ'$ . Then since  $\text{Norm}(J)\text{Norm}(J') = \text{Norm}(I)$ , we must have either  $\text{Norm}(J) = 1$ , in which case  $J = \Lambda$  or  $\text{Norm}(J') = 1$ , in which case  $J' = \Lambda$ . By Proposition 3.7,  $I$  is prime.  $\square$

Now suppose that  $I$  is not prime; then by Proposition 3.7,  $I$  can be factored as  $I = JJ'$  where neither  $J$  nor  $J'$  is the entire maximal order  $\Lambda$ , and so  $\text{Norm}(J)$  and  $\text{Norm}(J')$  are both smaller than  $\text{Norm}(I)$ . By induction,  $J$  and  $J'$  can be factored into primes, and so  $I$  can. Therefore all non-zero ideals can be factored into primes. We still need to see that this factorization is unique. Suppose that

$$(3.10) \quad I_1 \cdots I_i = J_1 \cdots J_j$$

are two factorizations of the same ideal into primes. Since  $I_1$  divides  $J_1 \cdots J_j$ , we see that  $I_1$  divides  $J_l$  for some  $l$ . Since  $J_l$  is prime,  $I_1 = J_l$ . Suppose  $I_1$  has norm  $N$ , and renumber the  $J$ 's so that  $J_1 = I_1$ . Multiplying both sides of (3.10) by  $\overline{I_1} = \overline{J_1}$ , we get

$$(N)I_2 \cdots I_i = (N)J_2 \cdots J_j$$

and so

$$I_2 \cdots I_i = J_2 \cdots J_j.$$

Inductively we see  $i = j$  and the  $J$ 's are simply a permutation of the  $I$ 's, completing the proof of Theorem 3.2.