FRACTIONAL IDEALS

1. Definition of fractional ideals

Let α be a nonzero element of the quadratic integer ring R inside a quadratic field $\mathbf{Q}(\delta)$. The reciprocal $\alpha^{-1} = \overline{\alpha}/\mathrm{N}(\alpha)$ of α is contained in $\mathbf{Q}(\delta)$, but in general it will no longer be contained in R. Nonetheless, it is very convenient to have the ability to divide two elements of R.

We have seen that in many ways, ideals in R behave better than the elements of R. However, most ideals of R do not have a multiplicative inverses, just like most elements of R do not. Fractional ideals are a generalization of ordinary ideals which do admit inverses. A fractional ideal is to an ordinary ideal as $\mathbf{Q}$ is to $\mathbf{Z}$.

Definition 1.1. Let R be the quadratic integer ring inside $\mathbf{Q}(\delta)$. A *fractional ideal* of R is a nonzero subgroup $A \subset \mathbf{Q}(\delta)$ such that:

(1) [Ideal] $\beta A \subset A$ for all $\beta \in R$, and
(2) [Clearing denominators] there exists $\beta \in R \setminus \{0\}$ such that $\beta A \subset R$.

We will sometimes call ordinary ideals of R *integral ideals* in order to differentiate them from fractional ideals.

Remark. (1) A fractional ideal A which is contained in R is the same as an integral ideal of R.
(2) If A is a fractional ideal of R and $\beta \in R$ is a nonzero element such that $B = \beta A \subset R$, then B is an integral ideal of R. Hence any fractional ideal has the form $A = \alpha B$ for an integral ideal $B \subset R$ and a nonzero element $\alpha = \beta^{-1}$ of $\mathbf{Q}(\delta)$.
(3) With the notation in (2), if $\beta A \subset R$ then $\overline{\beta}\beta A \subset R$ as well. But $\overline{\beta}\beta$ is the ordinary nonzero integer $n = N(\beta) \in \mathbf{Z}$, so we have $nA \subset R$. Therefore we can replace condition (2) in Definition 1.1 with the equivalent condition "there exists a nonzero integer n such that $nA \subset R$." Hence any fractional ideal has the form $A = n^{-1}B$ for $n \in \mathbf{Z} \setminus \{0\}$ and $A \subset R$ an integral ideal.
(4) If $\mathbf{Q}(\delta)$ is an imaginary quadratic field, then every ideal B of R is a lattice in $\mathbf{C}$. Since any fractional ideal has the form $A = n^{-1}B$ for an integral ideal B, this is also a lattice in $\mathbf{C}$, so fractional ideals are lattices as well.

Example 1.2. Let $R = \mathbf{Z}$. This is more of an analogy than an example since we have not defined fractional ideals in $\mathbf{Q}$, but the definition is the same as Definition 1.1. A fractional ideal has the from rA for $r \in \mathbf{Q}^\times$ and $A \subset \mathbf{Z}$ a nonzero ideal. Since any ideal is principal, we have $A = (n)$ for $n \in \mathbf{Z} \setminus \{0\}$, and hence $rA = r(n) = (rn)\mathbf{Z}$. Since rn is an arbitrary element of $\mathbf{Q}^\times$, we have

$$\{\text{fractional ideals in } \mathbf{Q}\} = \{r\mathbf{Z} \ : \ r \in \mathbf{Q}^\times\}.$$

See Figure 1.

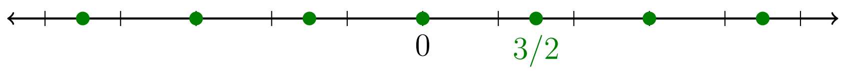

FIGURE 1. The fractional ideal $\frac{3}{2}\mathbf{Z}$ in $\mathbf{Q}$.

Example 1.3. Now let $R = \mathbf{Z}[i]$, the Gauss integers. This is a PID, so as in Example 1.2, any fractional ideal has the form $\alpha(\beta) = (\alpha\beta)\mathbf{Z}[i]$ for $\alpha \in \mathbf{Q}(i)^\times$ and $\beta \in \mathbf{Z}[i] \setminus \{0\}$. Therefore

$$\{\text{fractional ideals in } \mathbf{Q}(i)\} = \{(a+bi)\mathbf{Z}[i] \;:\; a+bi \in \mathbf{Q}(i)^\times\}.$$

See Figure 2.

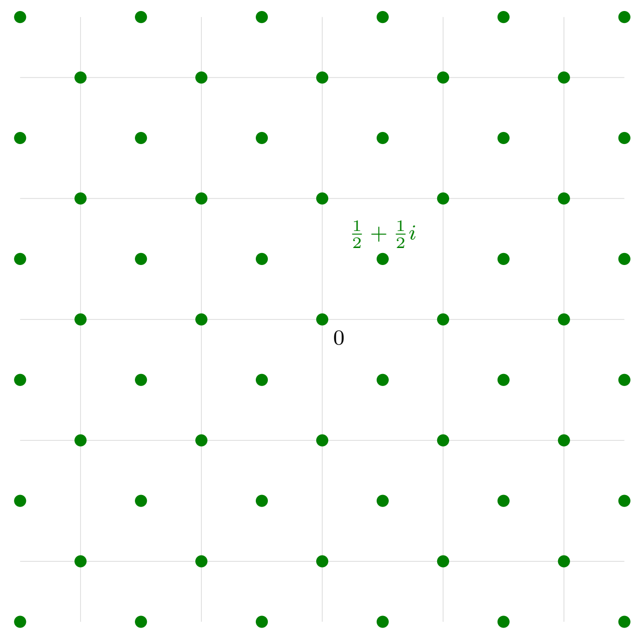

FIGURE 2. The fractional ideal $(\frac{1}{2}+\frac{1}{2}i)\mathbf{Z}[i]$ in $\mathbf{Q}(i)$. This fractional ideal happens to contain $\mathbf{Z}[i]$, but this is a coincidence; see Figure 1.

Example 1.4. Let $\delta = \sqrt{-5}$ and $R = \mathbf{Z}[\delta]$. Let $A \subset \mathbf{C}$ be the lattice $\langle 1, \frac{1}{2}(1+\delta)\rangle$. Then A is a fractional ideal in $\mathbf{Q}(\delta)$, since $2A = \langle 2, 1+\delta\rangle = (2, 1+\delta)$ is an ideal in R. See Figure 3.

Example 1.5. The full additive group $\mathbf{Q}(\delta)$ is not a fractional ideal. It satisfies condition (1) of Definition 1.1, but it does not satisfy condition (2): there does not a exist a single element $\beta \in R \setminus \{0\}$ such that $\beta\mathbf{Q}(\delta) \subset \mathbf{R}$, for the same reason that there does not exist a single $n \in \mathbf{Z} \setminus \{0\}$ such that $n\mathbf{Q} \subset \mathbf{Z}$.

Most of the constructions we made for integral ideals work equally well for fractional ideals.

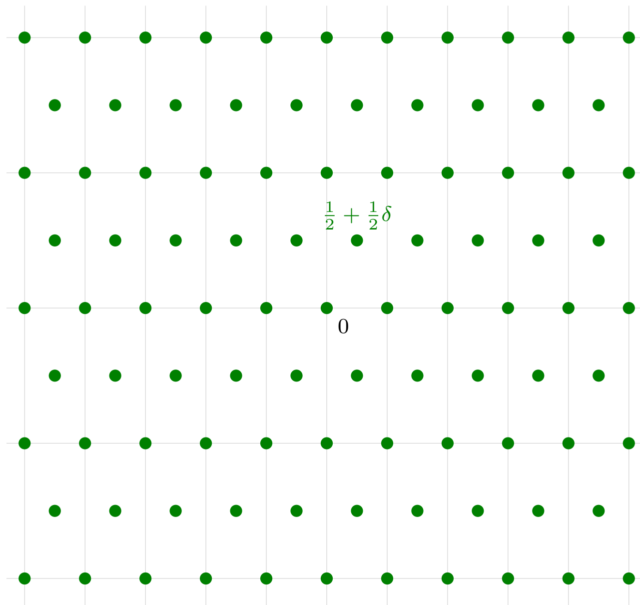

FIGURE 3. The fractional ideal $\langle 1, \frac{1}{2}(1+\delta)\rangle$ in $\mathbf{Q}(\sqrt{-5})$.

Definition 1.6. Let R be the quadratic integer ring inside $\mathbf{Q}(\delta)$ and let $\alpha_1, \ldots, \alpha_n \in \mathbf{Q}(\delta)$, not all equal to zero. The *fractional ideal generated by* $\alpha_1, \ldots, \alpha_n$ is

$$(\alpha_1, \ldots, \alpha_n) \coloneqq \big\{\beta_1\alpha_1 + \cdots + \beta_n\alpha_n \ : \ \beta_1, \ldots, \beta_n \in R\big\}.$$

A fractional ideal of the form (α) for $\alpha \in \mathbf{Q}(\delta)^\times$ is called *principal*.

It is clear that if $\alpha_1, \ldots, \alpha_n \in \mathbf{Q}(\delta)^\times$ are not all zero then $(\alpha_1, \ldots, \alpha_n)$ is a subgroup of $\mathbf{Q}(\delta)$ which is closed under multiplication by R. There exists an integer $m \in \mathbf{Z}\setminus\{0\}$ such that $m\alpha_i \in R$ for each i: indeed, $\alpha_i = a_i + b_i\delta$ for $a_i, b_i \in \mathbf{Q}$; just choose m to clear the denominators of all of the a_i, b_i. Then $m(\alpha_1, \ldots, \alpha_n) = (m\alpha_1, \ldots, m\alpha_n)$ is an integral ideal.

Any fractional ideal $A \subset \mathbf{Q}(\delta)$ has a lattice basis $\{\alpha, \beta\}$; then clearly $A = (\alpha, \beta)$. (Compare with the proof of the Main Lemma, 13.4.8 in Artin.) In other words, any fractional ideal can be generated by two elements.

Definition 1.7. Let $A, B \subset \mathbf{Q}(\delta)$ be two fractional ideals. The *product fractional ideal* is

$$AB = \big\{\alpha_1\beta_1 + \cdots + \alpha_n\beta_n \ : \ n \geq 0, \alpha_i \in A, \beta_i \in B\big\}.$$

If $A, B \subset R$ are integral ideals then AB is just the product ideal. As with ordinary ideals, multiplication is associative and commutative: $AB = BA$ and $(AB)C = A(BC)$ for fractional ideals $A, B, C \subset \mathbf{Q}(\delta)$. Moreover, one can calculate the product on generators: if $A = (\alpha_1, \alpha_2)$ and $B = (\beta_1, \beta_2)$ then

$$AB = (\alpha_1\beta_1,\ \alpha_1\beta_2,\ \alpha_2\beta_1,\ \alpha_2\beta_2).$$

Written this way, it is clear that AB is a fractional ideal. Note also that if $A = (\alpha)$ then

$$AB = \alpha B = \{\alpha\beta \ : \ \beta \in B\}.$$

Now we come to the main result about fractional ideals, which says that an integral ideal has a multiplicative inverse which is a fractional ideal.

Proposition 1.8. *Let R be the quadratic integer ring inside $\mathbf{Q}(\delta)$. The set of all fractional ideals in $\mathbf{Q}(\delta)$ is an abelian group under multiplication of fractional ideals, with unit element R.*

Proof. As mentioned above, multiplication is associative and commutative, so we only need to show that inverses exist. Let A be a fractional ideal, and choose $n \in \mathbf{Z} \setminus \{0\}$ such that $nA = B \subset R$ is an integral ideal. Then $B\overline{B} = (m)$ for some $m \in \mathbf{Z} \setminus \{0\}$, and we have

$$A\left(\frac{n}{m}\overline{B}\right) = (nA)\left(\frac{1}{m}\overline{B}\right) = B\left(\frac{1}{m}\overline{B}\right) = \frac{1}{m}(B\overline{B}) = \frac{1}{m}(m) = (1).$$

Hence $\frac{n}{m}\overline{B} = A^{-1}$. □

As an abstract group, the group of fractional ideals in $\mathbf{Q}(\delta)$ is not very interesting, as we will see in a moment. On the other hand, as the next example shows, neither is the multiplicative group $\mathbf{Q}_{>0}$.

Recall that the *direct sum* of an infinite family $G_1, G_2, \ldots$ of abelian groups is defined as

$$\bigoplus_{i=1}^{\infty} G_i = \big\{(x_1, x_2, \ldots) \ : \ x_i \in G_i, \text{ only finitely many } x_i \text{ are nonzero}\big\}.$$

The group law is just componentwise addition, and the additive identity is $(0, 0, \ldots)$. If $G_1 = G_2 = \cdots = \mathbf{Z}$ then every element of $\bigoplus_{i=1}^{\infty} \mathbf{Z}$ can be written uniquely as

$$a_1e_1 + \cdots + a_ne_n$$

for some $n \geq 0$ and $a_1, \ldots, a_n \in \mathbf{Z}$, where $e_i = (0, \ldots, 0, 1, 0, \ldots)$ is the "ith unit coordinate vector." We call $\bigoplus_{i=1}^{\infty} \mathbf{Z}$ the *free abelian group on countably many generators*.

Example 1.9. Define $\varphi : \bigoplus_{p \text{ prime}} \mathbf{Z} \to \mathbf{Q}_{>0}$ by

$$\varphi(a_2, a_3, a_5, \ldots) = 2^{a_2}3^{a_3}5^{a_5} \cdots .$$

Since only finitely many of the a_i are nonzero, this is a finite product. Clearly $\varphi(a + b) = \varphi(a)\varphi(b)$, so φ is a group homomorphism. Suppose that $\varphi(a_2, a_3, a_5, \ldots) = 1$. Then

$$2^{a_2}3^{a_3}5^{a_5} \cdots = 1.$$

Moving the terms with negative exponent to the other side of this equation gives two different prime factorizations of the same integer, unless all of the $a_i = 0$. Hence φ is injective, by uniqueness of prime factorizations. Since any fraction can be written in the form

$$r = \frac{2^{a_2}3^{a_3}5^{a_5} \cdots}{2^{b_2}3^{b_3}5^{b_5} \cdots}$$

by factoring the numerator and the denominator, we have $r = \varphi(a_2 - b_2, a_3 - b_3, \ldots)$, so φ is surjective and hence an isomorphism. We have shown that $\mathbf{Q}_{>0}$ is isomorphic to the free abelian group on countably many generators.

The ideal-theoretic version of Example 1.9 essentially says that unique factorization extends from ideals to fractional ideals.

Proposition 1.10. *Let R be the quadratic integer ring inside $\mathbf{Q}(\delta)$, let Π be the set of all nonzero prime ideals in R, and let $\mathcal{I}$ be the group of fractional ideals in $\mathbf{Q}(\delta)$. Define $\varphi : \bigoplus_{P\in\Pi} \mathbf{Z} \to \mathcal{I}$ by*

$$\varphi(\ldots, a_P, \ldots) = \prod_{P\in\Pi} P^{a_P}.$$

Then φ is an isomorphism of abelian groups.

In particular, for every fractional ideal I there are distinct prime ideals $P_1, \ldots, P_n \subset R$ and $a_1, \ldots, a_n \in \mathbf{Z}$ such that $I = P_1^{e_1} \cdots P_n^{e_n}$, and this expression is unique up to reordering the factors.

Proof. The proof is almost identical to Example 1.9. It is clear that φ is a homomorphism. If $\varphi(\ldots, a_P, \ldots) = R$ then we have an expression of the form $\prod P_i^{a_i} = R$; moving the terms with negative exponents to the right hand side of the equation gives two different factorizations of the same (integral) ideal, which by unique factorization of ideals is a contradiction unless all of the $a_i = 0$. For surjectivity, let $A \subset \mathbf{Q}(\delta)$ be a fractional ideal, and let $m \in \mathbf{Z} \setminus \{0\}$ be an integer such that $mA = B$ is an integral ideal. Let $(m) = \cdots P^{a_P} \cdots$ and $B = \cdots P^{b_P} \cdots$ be the prime factorizations of the (integral) ideals (m) and B. Then

$$A = (m)^{-1}B = \cdots P^{b_P - a_P} \cdots = \varphi(\ldots, b_P - a_P, \ldots).$$

Hence φ is an isomorphism, so fractional ideals have unique factorization. □

2. Fractional ideals and ideal classes

Now we use the group structure on the set of fractional ideals in $\mathbf{Q}(\delta)$ to define the class group, and we discuss the relation with similarity classes.

Definition 2.1. Let R be the quadratic integer ring inside $\mathbf{Q}(\delta)$, let $\mathcal{I}$ be the group of fractional ideals in $\mathbf{Q}(\delta)$, and let $\mathcal{P} \subset \mathcal{I}$ be the subgroup of principal fractional ideals. The *class group* of $\mathbf{Q}(\delta)$ is the quotient

$$\mathrm{Cl}(\mathbf{Q}(\delta)) := \mathcal{I}/\mathcal{P}.$$

Since $(\alpha)(\beta)^{-1} = (\alpha\beta^{-1})$, it is clear that $\mathcal{P}$ is in fact a subgroup of $\mathcal{I}$. Hence $\mathrm{Cl}(\mathbf{Q}(\delta))$ is an abelian group, which we will soon see is *finite*.

Recall that two ideals $A, B \subset R$ (resp. fractional ideals $A, B \subset \mathbf{Q}(\delta)$) are *similar* provided that there exists $z \in \mathbf{Q}(\delta)^\times$ such that $zA = B$. Similarity is an equivalence relation on the set of all ideals (resp. fractional ideals). An *ideal class* (resp. *fractional ideal class*) is an equivalence class under this relation. If A is a fractional ideal, we write $\langle A \rangle$ for its fractional ideal class.

Remark 2.2. Artin only defines similarity for ideals in *imaginary* quadratic integer rings: he says that A is similar to B if there exists $z \in \mathbf{C}^\times$ such that $zA = B$. If $\alpha \in A$ is nonzero and $\beta = z\alpha \in B$, then $z = \beta/\alpha$ is necessarily in $\mathbf{Q}(\delta)^\times$. Hence his definition is equivalent to the one given above, except our definition also works for fractional ideals and for real quadratic fields.

Proposition 2.3. *Let R be the quadratic integer ring inside $\mathbf{Q}(\delta)$, let $\mathcal{I}$ be the group of fractional ideals in $\mathbf{Q}(\delta)$, and let $\mathcal{P} \subset \mathcal{I}$ be the subgroup of principal fractional ideals. For $A \in \mathcal{I}$ the coset $A\mathcal{P}$ is equal to the fractional ideal class $\langle A \rangle$. Therefore the class group $\mathrm{Cl}(\mathbf{Q}(\delta))$ is equal to the set of fractional ideal classes, and we have $\langle A \rangle \langle B \rangle = \langle AB \rangle$ for $A, B \in \mathcal{I}$.*

Proof. We have $B \in \langle A \rangle$ if and only if there exists $z \in \mathbf{Q}(\delta)^\times$ such that $B = zA$. But $zA = (z)A = A(z) \in A\mathcal{P}$, so $B \in A\mathcal{P}$. Conversely, if $B = A(z) \in A\mathcal{P}$ then $B = zA \in \langle A \rangle$. □

Exercise 2.4. Prove that $\langle A \rangle^{-1} = \langle \overline{A} \rangle$ for a fractional ideal A.

The next lemma clarifies that there is essentially no difference between ideal classes and fractional ideal classes. Its proof is immediate.

Lemma 2.5. *Let R be the quadratic integer ring inside $\mathbf{Q}(\delta)$.*

(1) *If $A, B \subset R$ are integral ideals, then A and B are similar as integral ideals if and only if they are similar as fractional ideals.*
(2) *Every fractional ideal class contains an integral ideal.*
(3) *The set of fractional ideal classes is in bijection with the set of (integral) ideal classes.*

Therefore we can think of $\mathrm{Cl}(\mathbf{Q}(\delta))$ as the set of integral ideal classes if we like, as Artin does.