Math 4527 (Number Theory 2)

Lecture #26 of 37 $\sim$ March 22, 2021

Factorization of Ideals in $\mathcal{O}_D$

- Properties of Ideals in $\mathcal{O}_D$
- Divisibility of Ideals in $\mathcal{O}_D$
- Factorization of Ideals in $\mathcal{O}_D$

This material represents §8.2.2-8.2.3 from the course notes.

Recap

Last time, we showed a fact about the ideals of $\mathcal{O}_D$:

Proposition (Ideal Generators in $\mathcal{O}_D$)

If $R = \mathcal{O}_D$ is a quadratic integer ring, then every ideal in R is of the form $(n, a + b \cdot \frac{1+\sqrt{D}}{2})$ for some $a, b, n \in \mathbb{Z}$.

(Note that if $D \equiv 2, 3 \pmod 4$ then b is necessarily even.)

We now continue our analysis of the ideals of $\mathcal{O}_D$.

Ideals in $\mathcal{O}_D$, X

As a corollary, nonzero prime ideals of $\mathcal{O}_D$ are maximal:

Corollary (Quotients of $\mathcal{O}_D$)

If $R = \mathcal{O}_D$ is a quadratic integer ring and I is a nonzero ideal, then $\mathcal{O}_D/I$ is finite. Thus, every nonzero prime ideal of $\mathcal{O}_D$ is maximal.

To prove this we first require a lemma:

Lemma (Finite Integral Domains are Fields)

A finite integral domain is a field.

Proof:

- Suppose R is a finite domain and let $r \in R$ be nonzero.
- Then the set $\{1, r, r^2, \ldots, r^n, \ldots\}$ is finite. If $r^a = r^b$ with $a < b$, since $r \neq 0$ we may cancel to see $r^{b-a} = 1$, and so r^{b-a-1} is a multiplicative inverse of r.
- Hence every nonzero element of R is a unit, so R is a field.

Ideals in $\mathcal{O}_D$, XI

Proof (of corollary):

- For the first statement, if I is a nonzero ideal in $\mathcal{O}_D$, then $I \cap \mathbb{Z}$ is nonzero (since if $r \in I$ is any nonzero element, $N(r) \in I$ is a nonzero integer) and so by our proposition, $I = (n, a + b \cdot \frac{1+\sqrt{D}}{2})$ where $n \neq 0$ is a generator of $I \cap \mathbb{Z}$.
- There are finitely many residue classes in $\mathcal{O}_D/(n)$, since each residue class has (exactly) one representative by an element of the form $s + t \cdot \frac{1+\sqrt{D}}{2}$ for some integers $0 \leq s, t \leq n - 1$.
- It is a general fact[1] that $\mathcal{O}_D/I \cong [\mathcal{O}_D/(n)]/[I/(n)]$. The latter expression is a quotient of a finite ring, hence also finite.
- For the second statement, if P is a nonzero prime ideal of $\mathcal{O}_D$, then $\mathcal{O}_D/P$ is a finite integral domain, hence is a field.

[1] This is called the third isomorphism theorem: for a general ring R and ideals I and J containing I, it is true that R/J is isomorphic to $(R/I)/(J/I)$.

Ideals in $\mathcal{O}_D$, XII

We also require a few additional properties about the conjugation map in $\mathcal{O}_D$:

Definition

If $a + b\sqrt{D}$ is an element of $\mathcal{O}_D$, its conjugate is $\overline{a + b\sqrt{D}} = a - b\sqrt{D}$. For any $r \in \mathcal{O}_D$, we have $N(r) = r \cdot \overline{r}$, and we also define the trace of r as $\mathrm{tr}(r) = r + \overline{r}$.

Examples:

1. In $\mathbb{Z}[i]$, we have $\overline{2+i} = 2 - i$, $N(2+i) = (2+i)(2-i) = 5$, and $\mathrm{tr}(2+i) = (2+i) + (2-i) = 4$.
2. In $\mathcal{O}_{\sqrt{13}}$, we have $\overline{1+\sqrt{13}} = 1 - \sqrt{13}$, $N(1+\sqrt{13}) = (1+\sqrt{13})(1-\sqrt{13}) = -12$, and $\mathrm{tr}(1+\sqrt{13}) = (1+\sqrt{13}) + (1-\sqrt{13}) = 2$.
3. In $\mathcal{O}_{\sqrt{13}}$, $\overline{\frac{3+\sqrt{13}}{2}} = \frac{3-\sqrt{13}}{2}$ and $\mathrm{tr}(\frac{3+\sqrt{13}}{2}) = 3$.

Ideals in $\mathcal{O}_D$, XIII

For any $r \in \mathcal{O}_D$, both $N(r)$ and $\mathrm{tr}(r)$ are integers.

- Conversely, the elements $r \in \mathbb{Q}(\sqrt{D})$ with the property that $N(r)$ and $\mathrm{tr}(r)$ are both in $\mathbb{Z}$ are precisely the elements of $\mathcal{O}_D$.
- To see this, if $r = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, then $N(r) = a^2 - Db^2$ and $\mathrm{tr}(r) = 2a$. If both of these values are integers, then $2a$ is an integer, and then $4N(r) - (2a)^2 = -4Db^2$ is also an integer. Since D is squarefree, this means $4b^2$ hence $2b$ is an integer as well.
- Finally, if $D \equiv 2, 3 \pmod 4$ then $N(r)$ will only be an integer when a and b are themselves integers, while if $D \equiv 1 \pmod 4$ then $N(r)$ will be an integer when $2a$ and $2b$ are integers of the same parity. In both cases, we see $r \in \mathcal{O}_D$ as claimed.

Ideals in $\mathcal{O}_D$, XIV

We can also apply the conjugation map to ideals:

Definition

If I is an ideal of $\mathcal{O}_D$, then its conjugate is the ideal $\overline{I} = \{\overline{r} : r \in I\}$.

It is straightforward to see that the conjugate of an ideal is also an ideal.

- More specifically, if $I = (r, s)$, then $\overline{I} = (\overline{r}, \overline{s})$.
- Thus, for example, in $\mathbb{Z}[\sqrt{-5}]$ we have $\overline{(3, 1 + \sqrt{-5})} = (3, 1 - \sqrt{-5})$.
- Likewise, it is a straightforward calculation that for any ideals I and J, we have $\overline{IJ} = \overline{I} \cdot \overline{J}$ and $\overline{\overline{I}} = I$.

Ideals in $\mathcal{O}_D$, XV

Our first key result is that the product of an ideal with its conjugate is always principal:

Theorem (Ideals and Conjugates in $\mathcal{O}_D$)

If I is any ideal of $\mathcal{O}_D$, then $I \cdot \bar{I}$ is always principal.

Example: In $\mathbb{Z}[\sqrt{-5}]$, for $I = (3, 1 + \sqrt{-5})$, show that $I\bar{I}$ is principal.

Ideals in $\mathcal{O}_D$, XV

Our first key result is that the product of an ideal with its conjugate is always principal:

Theorem (Ideals and Conjugates in $\mathcal{O}_D$)

If I is any ideal of $\mathcal{O}_D$, then $I \cdot \bar{I}$ is always principal.

Example: In $\mathbb{Z}[\sqrt{-5}]$, for $I = (3, 1 + \sqrt{-5})$, show that $I\bar{I}$ is principal.

- Since $\bar{I} = (3, 1 - \sqrt{-5})$ we have $I\bar{I} = (3, 1+\sqrt{-5}) \cdot (3, 1-\sqrt{-5}) = (9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6)$.
- This ideal contains $9 - 6 = 3$, but in fact, every element is a multiple of 3. Thus we see $I\bar{I} = (3)$.

Ideals in $\mathcal{O}_D$, XVI

Proof:

- If $I = 0$ we are done. Otherwise, suppose that $I = (r, s)$ for some nonzero $r, s \in \mathcal{O}_D$: then $\overline{I} = (\overline{r}, \overline{s})$ and $I \cdot \overline{I} = (r\overline{r}, r\overline{s}, \overline{r}s, s\overline{s})$.
- We claim in fact that $I \cdot \overline{I} = (r\overline{r}, r\overline{s} + \overline{r}s, s\overline{s}) = (N(r),\ \mathrm{tr}(r\overline{s}),\ N(s))$.
- This will imply the desired result (namely that $I\overline{I}$ is principal), because $N(r)$, $\mathrm{tr}(r\overline{s})$, and $N(s)$ are each in $\mathbb{Z}$.
- Explicitly, if we let their greatest common divisor in $\mathbb{Z}$ be d, then $d = xN(r) + y\mathrm{tr}(r\overline{s}) + zN(s)$ for some $x, y, z \in \mathbb{Z}$.
- Then $(d) = (N(r),\ \mathrm{tr}(r\overline{s}),\ N(s))$ in $\mathcal{O}_D$ since d divides each of $N(r)$, $\mathrm{tr}(r\overline{s})$, and $N(s)$.

Ideals in $\mathcal{O}_D$, XVII

Proof (continued):

- In order to show that $I \cdot \overline{I} = (r\overline{r}, r\overline{s} + \overline{r}s, s\overline{s})$, we must show that $r\overline{s}$ is in the ideal $(r\overline{r}, r\overline{s} + \overline{r}s, s\overline{s}) = (d)$.
- Observe that $\mathrm{tr}(r\overline{s}/d) = \dfrac{r\overline{s} + \overline{r}s}{d} = \dfrac{\mathrm{tr}(r\overline{s})}{d}$ is an integer, as is $N(r\overline{s}/d) = \dfrac{r\overline{s}}{d} \cdot \dfrac{\overline{r}s}{d} = \dfrac{N(r)}{d} \cdot \dfrac{N(s)}{d}$, since d divides each of $N(r)$, $\mathrm{tr}(r\overline{s})$, and $N(s)$.
- Then, by our characterization of the elements in $\mathcal{O}_D$ as those having integral trace and norm, we conclude that $r\overline{s}/d$ is in $\mathcal{O}_D$, so that $r\overline{s} \in (d)$.
- Therefore, $I \cdot \overline{I} = (r\overline{r}, r\overline{s} + \overline{r}s, s\overline{s}) = (N(r), \mathrm{tr}(r\overline{s}), N(s)) = (d)$ is principal, as claimed.

Divisibility of Ideals in $\mathcal{O}_D$, I

Now we can discuss divisibility of ideals. Our definition is the same as for divisibility of elements:

Definition

If I and J are ideals of $\mathcal{O}_D$, we say that I divides J, written $I|J$, if there is some ideal K such that $J = IK$.

Examples:

1. If $I = (a)$ and $J = (b)$ are principal, then I divides J if and only if $a|b$. So in the case of principal ideals, we recover the usual notion of divisibility of elements.
2. If $I = (2)$ and $J = (4, 2 + 2\sqrt{7})$ inside $\mathbb{Z}[\sqrt{7}]$, then I divides J: for $K = (2, 1 + \sqrt{7})$ we have $IK = (4, 2 + 2\sqrt{7}) = J$.
3. If $I = (2, 1 + \sqrt{-5})$ and $J = (2)$ inside $\mathbb{Z}[\sqrt{-5}]$, then I divides J: for $K = (2, 1 - \sqrt{-5})$, we have $IK = (4, 2(1 + \sqrt{-5}), 2(1 - \sqrt{-5}), 6) = (2) = J$.

Divisibility of Ideals in $\mathcal{O}_D$, II

Now some properties of ideal divisibility:

Proposition (Properties of Ideal Divisibility)

Suppose I and J are ideals of $\mathcal{O}_D$ and $r \in \mathcal{O}_D$.

1. *If I divides J, then I contains J.*
2. *We have $I|J$ and $J|I$ if and only if $I = J$.*
3. *The principal ideal (r) divides I if and only if (r) contains I.*
4. *If $(r)J = (r)K$ and $r \neq 0$, then $J = K$.*
5. *If $IJ = IK$ and $I \neq 0$, then $J = K$.*
6. *The ideal I divides J if and only if I contains J.*

The main result is (6), which you can remember using the shorter statement "to divide is to contain".

Divisibility of Ideals in $\mathcal{O}_D$, III

1. If I divides J, then I contains J.

Proof:

- If $J = IK$ then every element in J is a sum of multiples of elements in I, hence is in I.

---

2. We have $I|J$ and $J|I$ if and only if $I = J$.

Proof:

- Since $I = IR$, $I = J$ implies $I|J$ and $J|I$.
- Conversely, if $I|J$ and $J|I$, then $I \subseteq J$ and $J \subseteq I$ so $I = J$.

---

3. The principal ideal (r) divides I if and only if (r) contains I.

Proof:

- The forward direction follows from (1). For the reverse, if (r) contains $I = (s, t)$ then $r|s$ and $r|t$, so $I = (r) \cdot (s/r, t/r)$.

Divisibility of Ideals in $\mathcal{O}_D$, IV

4. If $(r)J = (r)K$ and $r \neq 0$, then $J = K$.

Proof:

- If $s \in J$, then $rs \in (r)J$: then $rs \in (r)K$ and so $s \in K$.
- Thus, $J \subseteq K$, and by the same argument in reverse, $K \subseteq J$, so $J = K$.

---

5. If $IJ = IK$ and $I \neq 0$, then $J = K$.

Proof:

- If $I \neq 0$ then $I \cdot \bar{I} = (r)$ is a nonzero principal ideal as we proved earlier.
- Then $IJ = IK$ implies $(I\bar{I})J = (I\bar{I})K$ so that $(r)J = (r)K$, whence $J = K$ by (4).

Divisibility of Ideals in $\mathcal{O}_D$, V

6. The ideal I divides J if and only if I contains J.

Proof:

- The forward direction is given by (1), and it is easy to see that the result also holds if I is zero (since every ideal divides the zero ideal, but the zero ideal only divides itself).
- If I and J are nonzero ideals and I contains J, then $I \cdot \overline{I} = (r)$ contains $J \cdot \overline{I}$.
- Then by (3) we see that $(r) = I \cdot \overline{I}$ divides $J \cdot \overline{I}$, so $J \cdot \overline{I} = I \cdot \overline{I} \cdot K$ for some K.
- Then since $I \neq 0$ (whence $\overline{I} \neq 0$), by (5) we may cancel to conclude that $J = IK$, meaning that I divides J.

Unique Factorization of Ideals in $\mathcal{O}_D$, I

We are now tantalizingly close to being able to establish unique factorization of ideals.

- From this description of ideal divisibility, and the fact that nonzero prime ideals are maximal that we proved earlier, we can immediately conclude that the "irreducible" ideals (namely, ideals that have no nontrivial factorization, which is to say $I = JK$ implies $J = \mathcal{O}_D$ or $K = \mathcal{O}_D$) are the same as the maximal ideals, which are in turn the same as the nonzero prime ideals.
- To show that factorizations exist, we mimic the proof we gave earlier for elements by defining an "ideal norm".
- For elements we use the norm $N(r) = |r \cdot \overline{r}|$, so a natural guess for ideals would be to use $I \cdot \overline{I}$, which (conveniently) is principal and generated by an integer.

Unique Factorization of Ideals in $\mathcal{O}_D$, II

Definition

If I is an ideal of $\mathcal{O}_D$, then the norm $N(I)$ of I is the nonnegative integer generator of the principal ideal $I \cdot \overline{I}$.

The ideal norm obeys the same properties as the norm on elements:

- First, it is multiplicative:
  $(N(IJ)) = IJ \cdot \overline{IJ} = I\overline{I} \cdot J\overline{J} = (N(I)N(J))$.
- Also notice that the only ideal with norm 0 is the zero ideal, while the only ideal with norm 1 is $\mathcal{O}_D$ (since $I\overline{I} = (1)$ implies that I contains a unit).
- Thus, in particular, if $N(I)$ is a prime integer then I has no nontrivial factorization, and thus I is a prime ideal.

Unique Factorization of Ideals in $\mathcal{O}_D$, III

We can now establish that every ideal has a factorization as a product of prime ideals:

Proposition (Prime Factorization of Ideals in $\mathcal{O}_D$)

Every nonzero ideal in $\mathcal{O}_D$ can be written as the product of prime ideals of $\mathcal{O}_D$.

As usual, we take the convention that the empty product represents the multiplicative identity element, which for ideals is $\mathcal{O}_D$.

Unique Factorization of Ideals in $\mathcal{O}_D$, IV

Proof:

- We use (strong) induction on the norm of the ideal. Since $I \neq 0$ we have $N(I) \geq 1$.
- For the base case $N(I) = 1$, we have $I = \mathcal{O}_D$ so we may take the empty product of prime ideals.
- For the inductive step, suppose the result holds for every ideal of norm less than n and suppose $N(I) = n$.
- If I is a prime ideal we are done, so assume I is not prime (hence not maximal). Then I is properly contained in some other proper ideal J, so by our results on divisibility we may write $I = JK$ where J and K are both proper.
- Then $N(I) = N(J) \cdot N(K)$ and $1 < N(J), N(K) < n$. By the inductive hypothesis, both J and K are the product of some number of prime ideals, so I is as well.

Unique Factorization of Ideals in $\mathcal{O}_D$, V

As our final step, we show that the factorization is unique. To do this we require the prime divisibility property of prime ideals:

Proposition (Divisibility and Prime Ideals in $\mathcal{O}_D$)

If P is a prime ideal of $\mathcal{O}_D$ and I and J are any ideals with $P|IJ$, then $P|I$ or $P|J$.

We will reformulate this result into a statement that actually holds in an arbitrary commutative ring with 1: namely, that if P is prime and P contains IJ, then P contains I or P contains J.

Unique Factorization of Ideals in $\mathcal{O}_D$, VI

Proof:

- By the equivalence of divisibility and containment in $\mathcal{O}_D$, we need to show that if P is a prime ideal with P containing IJ, then P contains I or P contains J.
- Suppose that P contains neither I nor J: then there is some $x \in I$ that is not in P and some $y \in J$ that is not in P.
- But then $xy \in IJ$ is contained in P, which contradicts the assumption that P was prime.
- Thus, P contains I or P contains J, as required.

Unique Factorization of Ideals in $\mathcal{O}_D$, VII

Now it is just a matter of putting all of our results together and doing some bookkeeping:

Theorem (Uniqueness of Prime Ideal Factorization in $\mathcal{O}_D$)

Every nonzero ideal in $\mathcal{O}_D$ can be written as the product of prime ideals of $\mathcal{O}_D$. Furthermore, this representation is unique up to rearrangement: if $I = P_1 P_2 \cdots P_n = Q_1 Q_2 \cdots Q_k$, then $n = k$ and there is some rearrangement of the Q_i so that $P_i = Q_i$.

This result is even a little bit better than our unique factorization theorem for elements, since we don't even have to worry about associates.

Unique Factorization of Ideals in $\mathcal{O}_D$, VIII

Proof:

- We already proved that every nonzero ideal can be written as a product of prime ideals. For uniqueness, we induct on the minimal number of terms n in the prime factorization.
- For the base case $n = 0$, we have $I = \mathcal{O}_D$. Every prime ideal is proper, so I cannot be a nonempty product of prime ideals.
- For the inductive step, suppose representations with $< n$ terms are unique and let $I = P_1 P_2 \cdots P_n = Q_1 Q_2 \cdots Q_k$.
- Since P_1 is prime and divides $Q_1 Q_2 \cdots Q_k$, we see that P_1 must divide one of the Q_i; without loss of generality, rearrange so that P_1 divides Q_1.
- But since P_1 and Q_1 are both nonzero prime ideals, they are maximal. Since P_1 divides Q_1 we see that P_1 contains Q_1, but since Q_1 is maximal and $P_1 \neq \mathcal{O}_D$, we must have $P_1 = Q_1$.
- Cancelling yields $P_2 \cdots P_n = Q_2 \cdots Q_k$: then the inductive hypothesis yields the uniqueness of the factorization.

Unique Factorization of Ideals in $\mathcal{O}_D$, IX

So, we see that by working with ideals, rather than elements, we recover the existence of unique factorizations in all of the quadratic integer rings $\mathcal{O}_D$.

- As a historical matter, the study of unique factorization of elements (and its failures) quite substantially predates the modern notion of a ring.
- In fact, it was precisely in trying to "fix" the failure of numbers to have unique factorization that led Kummer to develop a new notion of a number, which he called an "ideal number", that did provide the missing terms that could further decompose these non-unique factorizations of elements.
- It is exactly Kummer's "ideal numbers" that were formalized by Dedekind, who proved that the general class of rings known as Dedekind domains possess unique factorization of ideals into products of prime ideals.

Unique Factorization of Ideals in $\mathcal{O}_D$, X

Thus, in fact, the modern notion of rings, ideals, and quotient rings all arose, historically, from this very problem of non-uniqueness of factorizations we have just been discussing.

- Furthermore, the formulation of the general notion of a ring also brought together the study of these classical questions from number theory with classical questions from algebraic geometry about polynomials in several variables[2].
- A great deal of this synthesis of commutative algebra was done in the late 19th and early 20th centuries by Dedekind, Hilbert, and (especially) Noether.
- We will use some of these connections shortly to give methods for calculating factorizations in $\mathcal{O}_D$.

[2] In fact, many of the questions about elliptic curves that we discussed in the last chapter can be posed about more general algebraic curves.

Unique Factorization of Ideals in $\mathcal{O}_D$, XI

As a corollary of the unique factorization of ideals, we can give a characterization of when $\mathcal{O}_D$ is a unique factorization domain:

Theorem (Unique Factorization in $\mathcal{O}_D$)

The ring $\mathcal{O}_D$ is a unique factorization domain if and only if it is a principal ideal domain.

This theorem (in its inverse formulation) tells us that every example of non-unique factorization of elements in $\mathcal{O}_D$ ultimately arises from the presence of nonprincipal ideals, which is something I remarked on a while ago.

Unique Factorization of Ideals in $\mathcal{O}_D$, XII

Proof:

- If $\mathcal{O}_D$ is a PID then it is a UFD.
- Now suppose $\mathcal{O}_D$ is a UFD and let P be a prime ideal. Then P divides the principal ideal $(N(P))$.
- By the unique factorization of elements in $\mathcal{O}_D$, we can write $N(P) = \pi_1\pi_2\cdots\pi_n$ for some irreducibles $\pi_1, \ldots, \pi_n \in \mathcal{O}_D$.
- Therefore, P divides the ideal product $(N(P)) = (\pi_1)\cdots(\pi_n)$, and hence P divides one of the ideals (π_i).
- But since irreducibles are prime in UFDs, the ideal (π_i) is also prime, and so we must have $P = (\pi_i)$. Thus, P is principal.
- Then any nonzero ideal in $\mathcal{O}_D$ is a product of prime (hence principal) ideals hence is also principal. Since the zero ideal is also principal, every ideal in $\mathcal{O}_D$ is principal, so it is a PID.

Unique Factorization of Ideals in $\mathcal{O}_D$, XIII

Having a general theorem about the existence of unique prime factorization for ideals is nice, but we would really like to be able to compute these factorizations.

- If we have some ideal $I = P_1 \cdots P_n$, then by taking norms we see that $N(I) = N(P_1) \cdots N(P_n)$.
- Thus, for each i, we see that P_i divides the principal ideal $(N(P_i))$, and the integer $N(P_i)$ is a divisor of the integer $N(I)$.
- Thus, if we can factor the integer $N(I)$ and then identify all of the possible prime ideal factors in $\mathcal{O}_D$ of this integer, we will have a list of all possible prime ideals that could divide I.

We will discuss this next time.

Summary

We continued our discussion of ideals in quadratic integer rings.

We proved that nonzero ideals in quadratic integer rings can be factored uniquely as a product of prime ideals.

Next lecture: Computing ideal factorizations in $\mathcal{O}_D$.

Note that all classes are cancelled on Wednesday, so our next lecture is on Thursday. In the spirit of actually taking the day off, I am also cancelling office hours on Wednesday, and I'm extending the homework due date by 24 hours.