Math 4527 (Number Theory 2)

Lecture #27 of 37 ∼ March 25, 2021

Factorization 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, I

Last time, we introduced divisibility of ideals:

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 $J = IK$.

Proposition (Properties of Ideal Divisibility)

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

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.*

Recap, II

We then proved that every nonzero ideal has a unique factorization as a product of prime ideals:

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 $P_i = Q_i$.

Our goal now is to discuss how to identify the prime ideals inside $\mathcal{O}_D$.

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

In fact, we can narrow down the possible norms of prime ideals in $\mathcal{O}_D$ quite substantially, and they all arise from primes in $\mathbb{Z}$.

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

If P is a nonzero prime ideal of $\mathcal{O}_D$, then $P \cap \mathbb{Z} = p\mathbb{Z}$ for a unique prime $p \in \mathbb{Z}$ (we say P "lies above" the prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$). Furthermore, every prime ideal in $\mathcal{O}_D$ lying above $p\mathbb{Z}$ divides the ideal (p) in $\mathcal{O}_D$, and the norm of any prime ideal is either p or p^2.

As a consequence, since (p) is a product of prime ideals, either (p) itself is prime (and has norm p^2) or (p) splits as the product of two prime ideals $(p) = P_1 P_2$ each of norm p.

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

Proof:

- Let $\varphi : \mathbb{Z} \to \mathcal{O}_D$ be the inclusion homomorphism, and observe that $\varphi^{-1}(P) = P \cap \mathbb{Z}$ is then an ideal of $\mathbb{Z}$, since the inverse image contains 0 and is closed under subtraction and arbitrary multiplication.
- Furthermore, if $ab \in \varphi^{-1}(P)$ then $\varphi(a)\varphi(b) = \varphi(ab) \in P$, so since P is prime we see $\varphi(a) \in P$ or $\varphi(b) \in P$: thus, either a or b is in $\varphi^{-1}(P)$.
- Also, since φ maps $1_{\mathbb{Z}}$ to $1_{\mathcal{O}_D}$, $\varphi^{-1}(P)$ does not contain 1, and since P contains the nonzero integer $N(P)$, we conclude that $\varphi^{-1}(P) = P \cap \mathbb{Z}$ is a nonzero prime ideal of $\mathbb{Z}$.

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

Proof (continued):

- The result of the last slide says that $P \cap \mathbb{Z} = p\mathbb{Z}$ for a unique prime $p \in \mathbb{Z}$.
- Thus, P contains $p \in \mathbb{Z}$ hence P contains (p), so by the equivalence of divisibility and containment, we see that P divides (p).
- For the last statement, since P divides (p) we see that $N(P)$ divides $N((p)) = N(p) = p^2$, so since $N(P) > 1$ we must have $N(p) = p$ or $N(p) = p^2$.

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

This last result tells us that we can find all the prime ideals in $\mathcal{O}_D$ by studying the factorization of the ideal (p) in $\mathcal{O}_D$.

- Let's work out some examples in the case $\mathcal{O}_D = \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, we just need to look at factorizations of the prime numbers p inside $\mathbb{Z}[i]$.
- Moreover, as we noted earlier, either p itself is prime, or it splits as the product of two prime ideals. If one of these ideals is $(a + bi)$ then we must have $(a + bi)(a - bi) = (p)$ and so $a^2 + b^2 = p$ (up to a unit factor, but this unit must be 1).
- So in fact we are reduced to determining whether p is the sum of two squares.

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

Examples: Find the factorizations of the ideals (2), (3), (5), (7), (11), (13), (17), (19), (23), and (29) in $\mathbb{Z}[i]$.

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

Examples: Find the factorizations of the ideals (2), (3), (5), (7), (11), (13), (17), (19), (23), and (29) in $\mathbb{Z}[i]$.

- We just have to decide which primes are the sum of two squares, and write the corresponding products of ideals.
- We see $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, and $29 = 5^2 + 2^2$, yielding the ideal factorizations
  $(2) = (1+i)(1-i) = (1+i)^2$,
  $(5) = (2+i)(2-i)$,
  $(13) = (3+2i)(3-2i)$,
  $(17) = (4+i)(4-i)$, and
  $(29) = (5+2i)(5-2i)$.
- Also, the other primes 3, 7, 11, 19, 23 are visibly not the sum of two squares (they are all 3 mod 4) and so each of the ideals (3), (7), (11), (19), (23) is prime in $\mathbb{Z}[i]$.

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

Based on these examples, we can make some fairly natural conjectures about what the prime ideals in $\mathbb{Z}[i]$ are. (We will do all of this rigorously later, of course; this discussion is just motivation.) So here are some reasonable guesses:

- There is a unique prime ideal $(1+i)$ above 2, with $(2) = (1+i)^2$ decomposing as a product with repeated factors.
- If $p \equiv 3 \bmod 4$ then the ideal (p) remains prime in $\mathbb{Z}[i]$.
- If $p \equiv 1 \bmod 4$ then $(p) = (\pi)(\overline{\pi})$ factors as the product of distinct ideals.

What we would like to do is reformulate these statements in a way that might be generalizable to other quadratic integer rings, because these statements really rely on unique factorization of elements.

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

We can give another way of describing the prime ideals and their behavior in $\mathbb{Z}[i]$ in terms of the behavior of the polynomial $q(x) = x^2 + 1$ modulo p, which (it just so happens) is the minimal polynomial of the generator $i \in \mathbb{Z}[i]$.

- If the polynomial $q(x)$ has a repeated root modulo p (which only happens with $p = 2$) then the ideal (p) decomposes as a product with repeated factors.
- If the polynomial $q(x)$ is irreducible modulo p (which is equivalent to saying that -1 is not a square modulo p, which occurs when $p \equiv 3 \bmod 4$) then (p) remains prime in $\mathbb{Z}[i]$.
- If the polynomial $q(x)$ factors with distinct roots modulo p (which is equivalent to saying that -1 is a square modulo p, which occurs when $p \equiv 1 \bmod 4$) then (p) factors as the product of two distinct conjugate ideals.

This is a statement that we can generalize to other $\mathcal{O}_D$.

Computing Ideal Factorizations in $\mathcal{O}_D$, I

Here is the main result, which is a special case of a general theorem of a result known as the Dedekind-Kummer factorization theorem:

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

Let p be a prime and let

$$q(x) = \begin{cases} x^2 - D & \text{for } D \equiv 2,3 \text{ mod } 4 \\ x^2 - x - (D-1)/4 & \text{for } D \equiv 1 \text{ mod } 4 \end{cases}, \text{ where}$$

$$\omega = \begin{cases} \sqrt{D} & \text{for } D \equiv 2,3 \text{ mod } 4 \\ (1+\sqrt{D})/2 & \text{for } D \equiv 1 \text{ mod } 4 \end{cases} \text{ is a root of } q(x).$$

If the polynomial $q(x)$ has a repeated root r modulo p then the ideal $(p) = (p, \omega - r)^2$ is the square of a prime ideal of norm p in $\mathcal{O}_D$, if $q(x)$ is irreducible modulo p then the ideal (p) is prime in $\mathcal{O}_D$ of norm p^2, and if $q(x)$ is reducible with distinct roots r, r' modulo p, then $(p) = (p, \omega - r) \cdot (p, \omega - r')$ factors as the product of two distinct ideals in $\mathcal{O}_D$ each of norm p.

Computing Ideal Factorizations in $\mathcal{O}_D$, II

Some comments before I launch into this long proof:

- Understanding the technical details of how this proof works are not at all necessary in order to understand how to use the results of the theorem. For the purposes of this class, it is fine if you want to view this theorem as akin to a "black box", the details of whose internal workings are entirely opaque.
- The starting point of the proof is the observation that if $q(x)$ is the minimal polynomial of the generator of $\mathcal{O}_D$, then as rings we have an isomorphism $\mathbb{Z}[x]/(q(x)) \cong \mathcal{O}_D$.
- This follows by applying the first isomorphism theorem to the evaluation homomorphism $\varphi : p \mapsto p(\alpha)$.
- We then make a bunch of manipulations of the quotient ring (in particular, we will use the Chinese remainder theorem when $q(x)$ factors) and use the ring isomorphism theorems.

Computing Ideal Factorizations in $\mathcal{O}_D$, III

Theorem (Second Isomorphism Theorem)

If A is a subring of R and B is an ideal of R, then $A + B = \{a + b : a \in A, b \in B\}$ is a subring of A, $A \cap B$ is an ideal of A, and $(A + B)/B$ is isomorphic to $A/(A \cap B)$.

Theorem (Third Isomorphism Theorem)

If I and J are ideals of R with $I \subseteq J$, then J/I is an ideal of R/I and $(R/I)/(J/I)$ is isomorphic to R/J.

Theorem (Fourth/Lattice Isomorphism Theorem)

If I is an ideal of R, then there is an inclusion-preserving bijection between subrings A of R containing I and the subrings $\overline{A} = A/I$ of R/I. Furthermore, a subring A of R containing I is an ideal of R if and only if A/I is an ideal of R/I.

Computing Ideal Factorizations in $\mathcal{O}_D$, IV

Proof:

- Observe that $\mathcal{O}_D \cong \mathbb{Z}[x]/(q(x))$.
- Thus, by the isomorphism theorems we see that

$$\begin{aligned} \mathcal{O}_D/(p) &\cong \left[\mathbb{Z}[x]/(q(x))\right]/(p) \\ &\cong \mathbb{Z}[x]/(p, q(x)) \\ &\cong \left[\mathbb{Z}[x]/(p)\right]/(q(x)) \\ &\cong \mathbb{F}_p[x]/(q(x)). \end{aligned}$$

- Thus, the ring structure of $\mathcal{O}_D/(p)$ is the same as the ring structure of $\mathbb{F}_p[x]/(q(x))$.
- Our task is now to unravel the structure of this ring.

Computing Ideal Factorizations in $\mathcal{O}_D$, V

Proof (continued):

- We have $\mathcal{O}_D/(p) \cong \mathbb{F}_p[x]/(q(x))$.
- The ideal (p) is prime (equivalently, maximal) in $\mathcal{O}_D$ precisely when the quotient ring is a field, and this occurs exactly when $q(x)$ is irreducible in $\mathbb{F}_p[x]$. In this case, $N((p)) = p^2$ so (p) is prime of norm p^2.
- If (p) is not prime, then since $N((p)) = p^2$, we see that (p) must factor as the product of two prime ideals I and I' each of norm p.
- Furthermore, since $I \cdot \overline{I} = (N(I)) = (p)$, by uniqueness of the prime ideal factorization we see that $I' = \overline{I}$, so the ideals in the factorization are conjugates.

Computing Ideal Factorizations in $\mathcal{O}_D$, VI

Proof (continued^2):

- We have $\mathcal{O}_D/(p) \cong \mathbb{F}_p[x]/(q(x))$ and are analyzing the case where $(p) = I\overline{I}$.
- If $I \neq \overline{I}$ then $I + \overline{I} = \mathcal{O}_D$ because I is maximal and $I + \overline{I} \neq I$.
- This means I and $\overline{I}$ are comaximal, so the Chinese remainder theorem implies that $\mathcal{O}_D/(p) \cong \mathcal{O}_D/I \times \mathcal{O}_D/\overline{I}$ is the direct product of two fields, and has no nonzero nilpotent elements.
- On the other hand, if $I = \overline{I}$, then $\mathcal{O}_D/(p) = \mathcal{O}_D/I^2$ has a nonzero nilpotent element (namely, the class of any element in I but not in I^2).
- Now we look at the ring $\mathbb{F}_p[x]/(q(x))$.

Computing Ideal Factorizations in $\mathcal{O}_D$, VII

Proof (continued[3]):

- We have $\mathcal{O}_D/(p) \cong \mathbb{F}_p[x]/(q(x))$, where $q(x)$ factors modulo p. There are two possible factorizations: either $q(x) = (x-r)^2$ or $q(x) = (x-r)(x-r')$ with $r \neq r'$.
- If $q(x) = (x-r)(x-r')$ in $\mathbb{F}_p[x]$, then the quotient ring $\mathcal{O}_D/(p) \cong \mathbb{F}_p[x]/(q(x)) \cong \mathbb{F}_p[x]/(x-r) \times \mathbb{F}_p[x]/(x-r') \cong \mathbb{F}_p \times \mathbb{F}_p$ is a direct product of two fields by the Chinese remainder theorem, and has no nonzero nilpotent elements.
- If $q(x) = (x-r)^2$ in $\mathbb{F}_p[x]$, then $\mathcal{O}_D/(p) \cong \mathbb{F}_p[x]/(x-r)^2$ does have a nonzero nilpotent element (namely $x-r$).
- Thus, comparing the ring structures in the two cases immediately shows that the case where $I = \overline{I}$ corresponds to the case where $q(x)$ has a repeated root, and $I \neq \overline{I}$ corresponds to the case where $q(x)$ has distinct roots.

Computing Ideal Factorizations in $\mathcal{O}_D$, VIII

Proof (continued[4]):

- For the remaining statements, if r is a root of $q(x)$ in $\mathbb{F}_p$, then $(p, \omega - r)$ divides (p) since it contains (p), and since $\omega - r \notin (p)$ we see that $(p, \omega - r)$ is a proper divisor of (p).
- Furthermore, $N((p, \omega - r))$ is the greatest common divisor of $N(p) = p^2$, $\mathrm{tr}(p(\omega - r)) = p\mathrm{tr}(\omega - r)$, and $N(\omega - r) = q(r) \equiv 0 \bmod p$. Since each of the terms is divisible by p, the gcd cannot be 1, and therefore $(p, \omega - r)$ is a proper ideal. By the uniqueness of the prime ideal factorization, $(p, \omega - r)$ must be a prime ideal dividing (p).
- If (p) is the square of a prime ideal, then $(p) = (p, \omega - r)^2$, while if (p) is the product of distinct ideals, we see that (p) is divisible by both $(p, \omega - r)$ and $(p, \omega - r')$, and since these ideals are comaximal we conclude $(p) = (p, \omega - r) \cdot (p, \omega - r')$. This establishes everything, so we are done.

Computing Ideal Factorizations in $\mathcal{O}_D$, IX

Example: Find the prime ideal factorizations of (2), (3), (5), and (7) in $\mathcal{O}_7 = \mathbb{Z}[\sqrt{7}]$.

Computing Ideal Factorizations in $\mathcal{O}_D$, IX

Example: Find the prime ideal factorizations of (2), (3), (5), and (7) in $\mathcal{O}_7 = \mathbb{Z}[\sqrt{7}]$.

- For (2) we consider $x^2 - 7$ modulo 2: since it has a repeated root 1, we see $(2) = (2, \sqrt{7} - 1)^2$ in $\mathbb{Z}[\sqrt{7}]$.
- For (3) we consider $x^2 - 7$ modulo 3: since its roots are 1 and 2, we get $(3) = (3, \sqrt{7} - 1) \cdot (3, \sqrt{7} - 2)$.
- For (5) we consider $x^2 - 7$ modulo 5: since it has no roots, we see that (5) remains prime in $\mathbb{Z}[\sqrt{7}]$.
- For (7) we consider $x^2 - 7$ modulo 7: since it has a repeated root 0, we see $(7) = (7, \sqrt{7})^2 = (\sqrt{7})^2$.

Computing Ideal Factorizations in $\mathcal{O}_D$, X

Example: Find the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_{\sqrt{5}} = \mathbb{Z}[\alpha]$ where $\alpha = (1+\sqrt{5})/2$.

Computing Ideal Factorizations in $\mathcal{O}_D$, X

Example: Find the prime ideal factorizations of (2), (3), (5), (7), and (11) in $\mathcal{O}_{\sqrt{5}} = \mathbb{Z}[\alpha]$ where $\alpha = (1+\sqrt{5})/2$.

- For (2) we consider $x^2 - x - 1$ modulo 2. It has no roots, so (2) remains prime in $\mathcal{O}_{\sqrt{5}}$.
- For (3) we consider $x^2 - x - 1$ modulo 3. It has no roots, so (3) remains prime in $\mathcal{O}_{\sqrt{5}}$.
- For (5) we consider $x^2 - x - 1$ modulo 5. It has a repeated root 3, so $(5) = (5, \alpha - 3)^2 = (5, \frac{-5+\sqrt{5}}{2})^2 = (\sqrt{5})^2$.
- For (7) we consider $x^2 - x - 1$ modulo 7. It has no roots, so (7) remains prime in $\mathcal{O}_{\sqrt{5}}$.
- For (11) we consider $x^2 - x - 1$ modulo 11. It has roots -3 and 4, so $(11) = (11, \alpha + 3)(11, \alpha - 4) = (11, \frac{7+\sqrt{5}}{2})(11, \frac{7-\sqrt{5}}{2})$ in $\mathcal{O}_{\sqrt{5}}$.

Computing Ideal Factorizations in $\mathcal{O}_D$, XI

Example: Compute the ideal factorization of (6) inside $\mathbb{Z}[\sqrt{-5}]$. Then show that the two element factorizations $6 = 2 \cdot 3$ and $6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ yield the same ideal factorization.

Computing Ideal Factorizations in $\mathcal{O}_D$, XI

Example: Compute the ideal factorization of (6) inside $\mathbb{Z}[\sqrt{-5}]$. Then show that the two element factorizations $6 = 2 \cdot 3$ and $6 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$ yield the same ideal factorization.

- We have $(6) = (2)(3)$ so we must factor the ideals (2) and (3). The minimal polynomial of the generator $\sqrt{-5}$ is $m(x) = x^2 + 5$.
- Modulo 2, we have $x^2 + 5 = (x-1)^2$, so we get the ideal factorization $(2) = (2, 1+\sqrt{-5})^2$.
- Modulo 3, we have $x^2 + 5 = (x+1)(x-1)$, so we get the ideal factorization $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$.
- Thus, $(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$.

Computing Ideal Factorizations in $\mathcal{O}_D$, XII

Example: Compute the ideal factorization of (6) inside $\mathbb{Z}[\sqrt{-5}]$. Then show that the two element factorizations $6 = 2 \cdot 3$ and $6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ yield the same ideal factorization.

Computing Ideal Factorizations in $\mathcal{O}_D$, XII

Example: Compute the ideal factorization of (6) inside $\mathbb{Z}[\sqrt{-5}]$. Then show that the two element factorizations $6 = 2 \cdot 3$ and $6 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$ yield the same ideal factorization.

- We have $(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$.
- Then $(2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$ $= (6,\ 2+2\sqrt{-5},\ 3+3\sqrt{-5},\ -4+2\sqrt{-5}) = (1+\sqrt{-5})$, since the ideal contains $1+\sqrt{-5}$ and all its generators are divisible by $1+\sqrt{-5}$.
- By taking conjugates and noting $\overline{(2, 1+\sqrt{-5})} = (2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5})$, we also have $(2, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (1-\sqrt{-5})$.
- So, both element factorizations reduce to the same ideal factorization, just regrouped.

Computing Ideal Factorizations in $\mathcal{O}_D$, XIII

To finish our discussion here, we will note that almost all of our analysis of the quadratic integer rings $\mathcal{O}_D$ can be extended to general rings of integers of algebraic number fields, as pioneered by Kummer, Dedekind, and Noether in their original development of the theory of rings and modules as applied to number theory.

- Explicitly, an algebraic number is a complex number that satisfies a polynomial with rational coefficients (such as $i/2$, $\sqrt[3]{2}$, and the roots of $x^5 - x - 1 = 0$).
- An algebraic integer is an algebraic number that satisfies a monic polynomial with integer coefficients (such as i and $\sqrt[3]{2}$, but not $i/2$).
- An algebraic number field is a subfield of $\mathbb{C}$ that is a finite-dimensional vector space over $\mathbb{Q}$ (examples include $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt[3]{2})$); all its elements are algebraic numbers.

Computing Ideal Factorizations in $\mathcal{O}_D$, XIV

It can be shown that the set of algebraic integers in an algebraic number field K is a subring of K, which is called the ring of integers of the number field. (For example, the ring of integers of $\mathbb{Q}(\sqrt{D})$ is $\mathcal{O}_D$.)

- Essentially all of the results we have proven then carry over to general rings of integers: ideal divisibility is equivalent to containment, nonzero prime ideals are maximal, nonzero ideals factor as a unique product of prime ideals, and nonzero prime ideals are precisely the ideal factors of (p).
- In number-theoretic language, if a prime ideal (p) remains prime in a ring of integers, we say (p) is inert. If (p) factors as a product of distinct prime ideals, we say (p) splits, while if (p) has repeated prime factors, we say that p ramifies. The question of when primes split, remain inert, or ramify is a fundamental object of study in algebraic number theory.

Summary

We proved a criterion for computing prime ideals in a quadratic integer ring.

We gave examples of how to compute the splitting of the ideal (p) in $\mathcal{O}_D$.

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