Math 4527 (Number Theory 2)

Lecture $\#25$ of 37 $\sim$ March 18, 2021

The Chinese Remainder Theorem + Factorization in $\mathcal{O}_D$

- The Chinese Remainder Theorem for Rings
- Unique Factorization of Elements in $\mathcal{O}_D$
- Ideals in $\mathcal{O}_D$

This material represents §8.1.9-8.2.1 from the course notes.

Recap

We have now successfully[1] studied general ring versions of many classical constructions from elementary number theory in $\mathbb{Z}$:

1. Our construction of quotient rings generalizes the notion of modular arithmetic to arbitrary rings.
2. Our analysis of Euclidean domains generalizes the notion of a division-with-remainder algorithm to arbitrary domains.
3. Our analysis of principal ideal domains generalizes properties of GCDs and linear combinations to arbitrary domains.
4. Our analysis of unique factorization domains generalizes the notion of unique factorization to arbitrary domains.

We now conclude our tour by studying the generalization of the Chinese remainder theorem to arbitrary rings.

[1] Your level of success may vary

The Chinese Remainder Theorem, I

We first require a few preliminary definitions:

Definition

If R is commutative with 1 and I and J are ideals of R, then the sum $I + J = \{a + b \, : \, a \in I, \, b \in J\}$ is defined to be the set of all sums of elements of I and J, and the product $IJ = \{a_1 b_1 + \cdots + a_n b_n, \, : \, a_i \in I, \, b_i \in J\}$ is the set of finite sums of products of an element of I with an element of J.

- It is not difficult to verify[2] that $I + J$ and IJ are both ideals of R, and that IJ contains the intersection $I \cap J$.
- If I and J are finitely generated, with $I = (a_1, a_2, \dots, a_n)$ and $J = (b_1, b_2, \dots, b_m)$, it is also not hard to see that $I + J = (a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m)$ and $IJ = (a_1 b_1, a_1 b_2, \dots, a_1 b_m, a_2 b_1, \dots, a_2 b_m, \dots, a_n b_m)$.

[2] This is code for "This appears on the homework".

The Chinese Remainder Theorem, II

Examples:

1. If $I = (a)$ and $J = (b)$ inside $\mathbb{Z}$, then $I + J = (a, b) = (d)$ where $d = \gcd(a, b)$ and $IJ = (ab)$.
2. If $I = (x)$ and $J = (x^2)$ inside $F[x]$, then $I + J = (x, x^2) = (x) = I$ and $IJ = (x^3)$.
3. If $I = (x)$ and $J = (x + 1)$ inside $F[x]$, then $I + J = (x, x + 1) = (1) = F[x]$ and $IJ = (x^2 + x)$.

We can also speak of sums and products of more than two ideals.

- These are defined recursively, so that (for example) $I + J + K = (I + J) + K$ and $IJK = (IJ)K$.
- One can verify easily that these operations are associative, commutative, obey the distributive law, etc.

The Chinese Remainder Theorem, III

We also need the analogous notion of coprimality for ideals, which is defined as follows:

Definition

If R is commutative with 1, the ideals I and J are comaximal if $I + J = R$.

- Note that $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ precisely when a and b are relatively prime.
- The appropriate notion in general rings is not "primality" but "maximality", so we use the term comaximal rather than coprime.

The Chinese Remainder Theorem, IV

We can now state the general Chinese remainder theorem:

Theorem (Chinese Remainder Theorem for Rings)

Let R be commutative with 1 and $I_1, I_2, \dots, I_n$ be ideals of R. Then the map $\varphi : R \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$ defined by $\varphi(r) = (r + I_1,\ r + I_2,\ \dots,\ r + I_n)$ is a ring homomorphism with kernel $I_1 \cap I_2 \cap \cdots \cap I_n$. If all of the ideals $I_1, I_2, \dots, I_n$ are pairwise comaximal, then φ is surjective and $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$, and thus $R/(I_1 I_2 \cdots I_n) \cong (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$.

To prove that the given map is an isomorphism, we will invoke the first isomorphism theorem. Everything else is just some careful bookkeeping.

The Chinese Remainder Theorem, V

Proof:

- First, φ is a homomorphism since $\varphi(a+b) = (a+b+I_1, \dots, a+b+I_n) = (a+I_1, \dots, a+I_n) + (b+I_1, \dots, b+I_n) = \varphi(a) + \varphi(b)$ and similarly $\varphi(ab) = (ab+I_1, \dots, ab+I_n) = (a+I_1, \dots, a+I_n) \cdot (b+I_1, \dots, b+I_n) = \varphi(a)\varphi(b)$.
- The kernel of φ is the set of elements $r \in R$ such that $\varphi(r) = (0+I_1, \dots, 0+I_n)$, which is equivalent to requiring $r \in I_1$, $r \in I_2$, ... , and $r \in I_n$: thus, $\ker\varphi = I_1 \cap I_2 \cap \cdots \cap I_n$.
- This establishes the first part of the theorem.
- For the second part, we will prove the results for two ideals and then deduce the general statement via induction.

The Chinese Remainder Theorem, VI

Proof (continued):

- So suppose I and J are ideals of R and $\varphi : R \to (R/I) \times (R/J)$ has $\varphi(r) = (r + I, r + J)$. We must show that if $I + J = R$, then $I \cap J = IJ$ and φ is surjective.
- If $I + J = R$ then by definition there exist elements $x \in I$ and $y \in J$ with $x + y = 1$.
- Then for any $r \in I \cap J$, we can write $r = r(x + y) = rx + yr$, and both rx and yr are in IJ: hence $I \cap J \subseteq IJ$, and since $IJ \subseteq I \cap J$ we conclude $IJ = I \cap J$.

The Chinese Remainder Theorem, VII

Proof (continued more):

- So suppose I and J are ideals of R and $\varphi : R \to (R/I) \times (R/J)$ has $\varphi(r) = (r + I, r + J)$, with $I + J = R$. We just showed that $I \cap J = IJ$ and must now show that φ is surjective.
- For any $a, b \in R$ we can write $ay + bx = a(1 - x) + bx = a + (b - a)x$ so $ay + bx \in a + I$, and likewise $ay + bx = ay + b(1 - y) = b + (a - b)y \in b + J$.
- Then $\varphi(ay + bx) = (ay + bx + I,\ ay + bx + J) = (a + I,\ b + J)$, and therefore φ is surjective as claimed.
- Finally, the statement that $R/IJ \cong (R/I) \times (R/J)$ then follows immediately by the first isomorphism theorem. This establishes all of the results for two ideals.

The Chinese Remainder Theorem, VIII

Proof (continueder morer):

- Finally, we establish the general statement by on n. We just did the base case $n = 2$.
- For the inductive step, it is enough to show that the ideals I_1 and $I_2 \cdots I_n$ are comaximal, since then we may write $R/(I_1 I_2 \cdots I_n) \cong (R/I_1) \times (R/I_2 \cdots I_n)$ and apply the induction hypothesis to $R/I_2 \cdots I_n$.
- If I_1 and I_i are comaximal for $2 \leq i \leq n$, then there exist elements $x_i \in I_1$ and $y_i \in I_i$ such that $x_i + y_i = 1$. Then $1 = (x_2 + y_2)(x_3 + y_3) \cdots (x_n + y_n) \equiv y_2 y_3 \cdots y_n$ modulo I_1. But since $y_2 y_3 \cdots y_n$ is in $I_2 I_3 \cdots I_n$, this means that $I_1 + I_2 I_3 \cdots I_n$ contains 1 and is therefore all of R, as required.

The Chinese Remainder Theorem, IX

This result really is a direct generalization of the result we give the same name about solving simultaneous congruences.

- Explicitly, if $m_1, m_2, \dots m_n$ are relatively prime positive integers, then $\varphi : \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$ given by $\varphi(a) = (a \bmod m_1,\ a \bmod m_2, \dots, a \bmod m_n)$ is a surjective homomorphism with kernel $m_1 m_2 \cdots m_n \mathbb{Z}$.
- The fact that this map is surjective says that the system of simultaneous congruences $x \equiv a_1 \bmod m_1$, $x \equiv a_2 \bmod m_2$, ... , $x \equiv a_n \bmod m_n$ always has a solution in $\mathbb{Z}$. Furthermore, the characterization of the kernel says that the solution is unique modulo $m_1 m_2 \cdots m_n$.
- This is exactly the statement of the classical Chinese remainder theorem as we usually pose it for $\mathbb{Z}$.

The Chinese Remainder Theorem, X

We record our observations from the last slide, which allow us to decompose $\mathbb{Z}/m\mathbb{Z}$ as a direct product when m is composite.

Corollary (Chinese Remainder Theorem for $\mathbb{Z}$)

If m is a positive integer with prime factorization $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, then $\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{a_n}\mathbb{Z})$.

By counting the units in the Cartesian product, we see that the number of units in $\mathbb{Z}/m\mathbb{Z}$ is $m(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_n)$.

- This gives us a formula for the Euler φ-function $\varphi(m)$.

Overview, I

As we have seen, some of the quadratic integer rings (like $\mathbb{Z}[i]$) are unique factorization domains, while others (like $\mathbb{Z}[\sqrt{-5}]$) are not.

- More specifically, by extending the argument used for $\mathbb{Z}[i]$, it can be shown that the quadratic integer ring $\mathcal{O}_D = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{for } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[(1+\sqrt{D})/2] & \text{for } D \equiv 1 \pmod 4 \end{cases}$ is Euclidean (with norm given by the field norm) for a known list of negative $D = -1, -2, -3, -7, -11$ and for various positive D, including $D = 2, 3, 5, 6, 7, 11, \dots$.
- We would like to know whether it is possible to recover some sort of "unique factorization" property in the quadratic integer rings, even when they are not unique factorization domains.

Overview, II

The question of when $\mathcal{O}_D$ is a UFD was (and is) of substantial interest in applications to solving equations in number theory.

- As we already saw in our study of Pell's equation, the characterization of the ring structure and the units in $\mathbb{Z}[\sqrt{D}]$ tells us how to solve $x^2 - Dy^2 = r$.
- Likewise, we can sometimes use properties of rings (e.g., $\mathbb{Z}[i]$) to characterize the solutions to other Diophantine equations, as we saw earlier in the case of the equation $a^2 + b^2 = c^2$.

Overview, III

As another example, if p is an odd prime, we may study the Fermat equation $x^p + y^p = z^p$ in the ring $\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1} \,:\, a_i \in \mathbb{Z}\}$ where $\zeta_p = e^{2\pi i/p} = \cos(2\pi/p) + i\sin(2\pi/p)$ is a nonreal pth root of unity (satisfying $\zeta_p^p = 1$).

- We may rearrange the equation as $z^p - y^p = x^p$ and then factor the left-hand side as the product $(z-y)(z-\zeta_p y)(z-\zeta_p^2 y)\cdots(z-\zeta_p^{p-1}y)$ of linear terms inside $\mathbb{Z}[\zeta_p]$.
- If $\mathbb{Z}[\zeta_p]$ were a unique factorization domain, then since the terms on the left-hand side are essentially relatively prime, each of them would have to be a pth power in $\mathbb{Z}[\zeta_p]$, up to some small factors. This can be shown not to be possible unless $y = 0$, which would show that Fermat's equation $x^p + y^p = z^p$ has no nontrivial integer solutions.

Overview, IV

Unfortunately, the ring $\mathbb{Z}[\zeta_p]$ is not always a unique factorization domain.

- But the study of Diophantine equations in number theory, and associated questions about unique factorization, were (historically speaking) the impetus for much of the development of modern algebra, including ring theory.
- We will touch on a number of these topics, although we will primarily focus our attention on quadratic integer rings, since we can give concrete arguments in these cases.

Factorization in $\mathcal{O}_D$, I

As a first step, we show that every nonzero element in $\mathcal{O}_D$ does possess at least one factorization:

Proposition (Element Factorizations in $\mathcal{O}_D$)

If $R = \mathcal{O}_D$ is a quadratic integer ring, then every nonzero nonunit in R has at least one factorization as a product of irreducible elements.

As a consequence, this result means that the failure of $\mathcal{O}_D$ to be a UFD lies entirely with non-uniqueness.

Factorization in $\mathcal{O}_D$, II

Proof:

- We show the result by (strong) induction on the absolute value of the norm $N(r)$. If $N(r) = 0$ then $r = 0$, while if $N(r) = \pm 1$ then r is a unit.
- For the base case we take $|N(r)| = 2$: then r is irreducible, since the absolute value of its norm is a prime.
- For the inductive step, suppose that $|N(r)| = n$ for $n \geq 3$. If r is irreducible we are done: otherwise we have $r = ab$ for some a, b with $1 < |N(a)|, |N(b)| < n$.
- By the inductive hypothesis, both a and b have factorizations as a product of irreducibles, so r does too.

Factorization in $\mathcal{O}_D$, III

It would appear that we are essentially at an impasse regarding factorization of elements, beyond simply computing their norms and attempting to search for possible elements that could appear in a factorization.

- However, if we shift our focus instead to ideals, it turns out that these rings do possess unique prime factorizations on the level of *ideals*, rather than elements.
- In fact, this is where the name "ideal" originally arose: in Kummer's study of unique factorization, he constructed "ideal numbers" (essentially as sets of linear combinations of elements of $\mathcal{O}_D$) and proved that they did possess unique prime factorization. These "ideal numbers" were the prototype of the modern definition of an ideal.

Factorization in $\mathcal{O}_D$, IV

To illustrate using an example I have already discussed, the element $6 \in \mathbb{Z}[\sqrt{-5}]$ has two different factorizations into irreducibles, as $2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

- This yields the equivalent ideal factorization $(6) = (2) \cdot (3) = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.
- However, as ideals, we can factor further: explicitly, one can verify that $(2) = (2, 1 + \sqrt{-5})^2$, that $(1 \pm \sqrt{-5}) = (2, 1 + \sqrt{-5}) \cdot (3, 1 \pm \sqrt{-5})$, and that $(3) = (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$.

Factorization in $\mathcal{O}_D$, V

Here is an example of one of these calculations:

- We have $(2, 1+\sqrt{-5}) \cdot (3, 1+\sqrt{-5})$ $= (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5})$ by properties of ideal products.
- We can reduce the generating set by observing that this ideal contains $(3+3\sqrt{-5}) - (2+2\sqrt{-5}) = 1+\sqrt{-5}$, and that each of the four generators of the product ideal is a multiple of $1+\sqrt{-5}$.
- Thus, in fact, $(2, 1+\sqrt{-5}) \cdot (3, 1+\sqrt{-5}) = (1+\sqrt{-5})$, as claimed. The other calculations are similar.

Factorization in $\mathcal{O}_D$, VI

On the level of ideals, therefore, we see that these two factorizations $6 = 2 \cdot 3$ and $6 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$ are really "the same".

- Explicitly, both of them reduce to the factorization $(6) = (2, 1+\sqrt{-5})^2 \cdot (3, 1+\sqrt{-5}) \cdot (3, 1-\sqrt{-5})$; we have just regrouped the factors in the computations above using
$(2) = (2, 1+\sqrt{-5})^2$,
$(1 \pm \sqrt{-5}) = (2, 1+\sqrt{-5}) \cdot (3, 1 \pm \sqrt{-5})$, and
$(3) = (3, 1+\sqrt{-5}) \cdot (3, 1-\sqrt{-5})$.
- Furthermore, each of the ideals $(2, 1+\sqrt{-5})$, $(3, 1+\sqrt{-5})$, and $(3, 1-\sqrt{-5})$ can be shown to be prime (the quotient ring of $\mathbb{Z}[\sqrt{-5}]$ by each is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/3\mathbb{Z}$ respectively).
- Thus, we have found a factorization of the ideal (6) as a product of prime ideals of $\mathbb{Z}[\sqrt{-5}]$.

Factorization in $\mathcal{O}_D$, VII

Our goal is to show that the behavior in this last example holds in general: namely, that we can write any nonzero ideal in a quadratic integer ring as a product of prime ideals, and that this factorization is unique up to rearrangement.

- After first establishing some important properties of prime ideals, our model will be similar to our proofs that PIDs have unique factorization: we will discuss some properties of divisibility, show that every nonzero ideal can be written as a product of prime ideals, and then show that the factorization is unique.
- We will then give some applications of unique factorization into prime ideals, and in particular describe how to compute the prime ideals of $\mathcal{O}_D$.

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

To begin our study of ideals in $\mathcal{O}_D$, we show that every ideal in $\mathcal{O}_D$ is generated by at most 2 elements:

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 $(n, a + b \cdot \dfrac{1+\sqrt{D}}{2})$ for some $a, b, n \in \mathbb{Z}$.
(Note that if $D \equiv 2, 3$ (mod 4) then b is necessarily even.)

There is a short proof of this fact that uses some facts about finitely generated abelian groups. It goes as follows: the additive group of $\mathcal{O}_D$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$, and since an ideal of R is a subgroup, it is generated by at most 2 elements as a subgroup, hence also as an ideal. (One can then obtain the proposition by taking R-linear combinations of the generators.)

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

Proof:

- Let I be an ideal of $\mathcal{O}_D$, and define $I_0 = I \cap \mathbb{Z}$ and I_1 to be the set of $r \in \mathbb{Z}$ such that there exists some $s \in \mathbb{Z}$ with $s + r \cdot \dfrac{1+\sqrt{D}}{2} \in I$.
- Observe that I_0 and I_1 are both ideals of $\mathbb{Z}$ since they clearly contain 0, are closed under subtraction, and are closed under arbitrary $\mathbb{Z}$-multiplication. So suppose $I_0 = (n)$ and $I_1 = (b)$: then $n \in I$, and by definition of I_1, there exists $a \in \mathbb{Z}$ such that $a + b \cdot \dfrac{1+\sqrt{D}}{2} \in I$.
- We claim that n and $a + b \cdot \dfrac{1+\sqrt{D}}{2}$ generate I.

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

Proof (continued):

- We claim that n and $a + b \cdot \frac{1+\sqrt{D}}{2}$ generate I.
- So, suppose $s + r \cdot \frac{1+\sqrt{D}}{2}$ is an arbitrary element of I.
- By definition of I_1 we see that $r \in I_1$, whence $r = yb$ for some $y \in \mathbb{Z}$. Then $\left[\left(s + r \cdot \frac{1+\sqrt{D}}{2}\right) - y \cdot \left(a + b \cdot \frac{1+\sqrt{D}}{2}\right)\right] = s - ay$ is in $I \cap \mathbb{Z} = I_0$, so this quantity is equal to xn for some $x \in \mathbb{Z}$.
- Thus, $s + r \cdot \frac{1+\sqrt{D}}{2} = xn + y\left(a + b \cdot \frac{1+\sqrt{D}}{2}\right)$, and so n and $a + b \cdot \frac{1+\sqrt{D}}{2}$ generate I as claimed.

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 $\{1, r, r^2, \dots, r^n, \dots\}$ 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[3] 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.

[3] 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 $I \cdot \overline{I}$ is always principal.

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

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

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

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.

Summary

We proved the general Chinese remainder theorem for rings.

We started our discussion of factorization in quadratic integer rings.

Next lecture: Factorization of ideals in $\mathcal{O}_D$.