Math 4527 (Number Theory 2)

Lecture #21 of 38 $\sim$ March 10, 2021

Arithmetic in Domains + Quadratic Integer Rings

- Prime Ideals
- Arithmetic in Integral Domains
- Quadratic Integer Rings

This material represents §8.1.4-8.1.5 from the course notes.

Recall, I

Last time, we discussed maximal ideals:

Definition

If R is a ring, a maximal ideal of R is an ideal $M \neq R$ with the property that the only ideals of R containing M are M and R.

Commutative rings with 1 always have maximal ideals, and we can detect them using quotient rings:

Proposition (Maximal Ideals and Quotients)

If R is a commutative ring with 1, then the ideal M is maximal if and only if R/M is a field.

Prime Ideals, I

In addition to maximal ideals, we have another important class of ideals in commutative rings:

Definition

If R is a commutative ring with 1, a prime ideal of R is an ideal $P \neq R$ with the property that for any $a, b \in R$ with ab in P, at least one of a and b is in P.

As naturally suggested by the name, prime ideals are a generalization of the idea of a prime number in $\mathbb{Z}$.

- Explicitly, for $n > 1$, the ideal $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ precisely when $ab \in n\mathbb{Z}$ implies $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$.
- Equivalently (in the language of divisibility) this means $n|ab$ implies $n|a$ or $n|b$, and this is precisely the condition that n is either a prime number (or zero).

Prime Ideals, II

Examples:

1. The prime ideals of $\mathbb{Z}$ are (0) and the ideals $p\mathbb{Z}$ where p is a prime number.
2. In $R = F[x]$, the ideal (p) is prime precisely when p is not a unit and $p|ab$ implies $p|a$ or $p|b$. This latter condition, per facts about polynomial factorization, is equivalent to saying that p is either irreducible or zero.
3. The prime ideals of $F[x]$ are (0) and the ideals (p) where p is an irreducible polynomial of positive degree.

Prime Ideals, III

Like with maximal ideals, there is an easy way to test whether an ideal is prime using quotient rings:

Proposition (Prime Ideals and Quotients)

If R is a commutative ring with 1, then the ideal P is prime if and only if R/P is an integral domain[a][b].

[a] Recall that an integral domain is a commutative ring with $1 \neq 0$ that has no zero divisors.

[b] Recall that a zero divisor is a nonzero element x such that there exists a nonzero element y with $xy = 0$

The proof is essentially just a restatement of the definition of a prime ideal using residue classes in the quotient ring.

- The key is to observe that $r \in P$ if and only if $\overline{r} = \overline{0}$ in R/P.

Prime Ideals, IV

Proof:

- If R is commutative with 1 and $P \neq R$, then R/P is also commutative with 1, so we need only test for zero divisors.
- If P is a prime ideal, then $ab \in P$ implies $a \in P$ or $b \in P$. In the quotient ring R/P, this says that $\overline{ab} = \overline{0}$ implies $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, which is precisely the statement that R/P has no zero divisors.
- Conversely, if R/P has no zero divisors, then $\overline{ab} = \overline{0}$ implies $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, which is to say, $ab \in P$ implies $a \in P$ or $b \in P$. Furthermore, since R/P is not the zero ring (since this possibility is excluded by the definition of integral domain), we see $P \neq R$, and therefore P is a prime ideal of R.

Prime Ideals, V

Our characterization of prime ideals yields two nice corollaries:

Corollary (Characterization of Domains)

A commutative ring with 1 is an integral domain if and only if (0) *is a prime ideal.*

Proof:

- Note that (0) is prime if and only if the quotient ring $R/0 \cong R$ is an integral domain.

Corollary (Maximal Ideals are Prime)

In a commutative ring with 1, every maximal ideal is prime.

Proof:

- If M is a maximal ideal, then R/M is a field. Every field is an integral domain, so M is a prime ideal.

Prime Ideals, VI

Example: Determine whether the ideals (x), (x^2), and (x^2+1) in $\mathbb{Z}[x]$ are prime ideals.

Prime Ideals, VI

Example: Determine whether the ideals (x), (x^2), and (x^2+1) in $\mathbb{Z}[x]$ are prime ideals.

- By the division algorithm, the residue classes in $\mathbb{Z}[x]/(x)$ are of the form $\overline{a}$ for $a \in \mathbb{Z}$. This means $\mathbb{Z}[x]/(x)$ is an integral domain (it is isomorphic to $\mathbb{Z}$, as can be shown directly or via the first isomorphism theorem), so (x) is a prime ideal.
- On the other hand, also by the division algorithm, we see that the residue classes in $\mathbb{Z}[x]/(x^2)$ are of the form $\overline{a+bx}$ where $a, b \in \mathbb{Z}$. Since $\overline{x} \cdot \overline{x} = \overline{0}$ but $\overline{x} \neq \overline{0}$, we see that $\mathbb{Z}[x]/(x^2)$ has zero divisors, and so (x^2) is not a prime ideal.
- Finally, as we showed before, $\mathbb{Z}[x]/(x^2+1)$ is isomorphic to the Gaussian integers $\mathbb{Z}[i]$, which is an integral domain, so (x^2+1) is a prime ideal.

Prime Ideals, VII

Example: For $R = \mathbb{Z}[\sqrt{3}]$ with the ideal $I = (2)$, identify explicitly the residue classes and operations in the quotient ring R/I, and determine whether I is (a) prime, and (b) maximal.

Prime Ideals, VII

Example: For $R = \mathbb{Z}[\sqrt{3}]$ with the ideal $I = (2)$, identify explicitly the residue classes and operations in the quotient ring R/I, and determine whether I is (a) prime, and (b) maximal.

- Note that I consists of the multiples of 2, so, explicitly, $I = \{2a + 2b\sqrt{3} : a, b \in \mathbb{Z}\}$.
- There are then four residue classes in R/I: they are
  $0 + I = \{2a + 2b\sqrt{3} : a, b \in \mathbb{Z}\}$,
  $1 + I = \{(2a + 1) + 2b\sqrt{3} : a, b \in \mathbb{Z}\}$,
  $\sqrt{3} + I = \{2a + (2b + 1)\sqrt{3} : a, b \in \mathbb{Z}\}$,
  $1 + \sqrt{3} + I = \{(2a + 1) + (2b + 1)\sqrt{3} : a, b \in \mathbb{Z}\}$.
- The addition operations are straightforward: we just add up the coefficients using the relation $2 = 0$.
- Thus for example,
  $(\sqrt{3} + I) + (1 + \sqrt{3} + I) = 1 + 2\sqrt{3} + I = 1 + I$.

Prime Ideals, VIII

Example: For $R = \mathbb{Z}[\sqrt{3}]$ with the ideal $I = (2)$, identify explicitly the residue classes and operations in the quotient ring R/I, and determine whether I is (a) prime, and (b) maximal.

- For multiplication, the nontrivial cases are
  $(\sqrt{3} + I) \cdot (\sqrt{3} + I) = 3 + I = 1 + I$,
  $(1 + \sqrt{3} + I) \cdot (\sqrt{3} + I) = 3 + \sqrt{3} + I = (1 + \sqrt{3}) + I$, and
  $(1 + \sqrt{3} + I) \cdot (1 + \sqrt{3} + I) = 4 + 2\sqrt{3} + I = 0 + I$.
- From this, we can see that the element $1 + \sqrt{3} + I$ is a zero divisor, meaning that I is neither prime nor maximal.
- Remark: From this calculation, we can see that the quotient ring R/I contains the nontrivial ideal $\overline{(1 + \sqrt{3})}$. This means I is contained in the ideal $I' = (2, 1 + \sqrt{3})$; in fact, I' is maximal. Our goal in this chapter is to understand how to make calculations like this systematically.

Arithmetic in Integral Domains, I

Our next goal is to translate a number of fundamental properties of arithmetic into general integral domains.

- In fact, I have already implicitly used this language a number of times (but informally).
- Today, we will start by formulating notions of divisibility, common divisors, and factorization in integral domains, and we will relate them to the language of ideals we have developed.
- We will then study various types of integral domains having various convenient properties: the existence of a Euclidean algorithm, having every ideal be principal, and having unique factorization (respectively).
- We will also pose the Chinese remainder theorem in great generality using our ring language.

Arithmetic in Integral Domains, II

First, we make a number of definitions precise:

Definition

Suppose that R is an integral domain and $a, b, d \in R$.

1. *We say that d <u>divides</u> a, written $d|a$, if there exists some $r \in R$ such that $a = rd$.*
2. *We say d is a <u>common divisor</u> of a and b if $d|a$ and $d|b$.*
3. *We say that a common divisor $d \in R$ is a <u>greatest common divisor</u> of a and b if $d \neq 0$ and for any other common divisor d', it is true that $d'|d$.*
4. *If 1 is a greatest common divisor of a and b, then we say a and b are <u>relatively prime</u>.*
5. *If $a = ub$ for some unit u, then we say a and b are <u>associates</u>.*

Arithmetic in Integral Domains, II

Examples:

1. Inside $\mathbb{Z}$, we have $2|6$, $5|-10$, $3|0$, and $0|0$.
   1 is a common divisor of 6 and 16, and 2 is a greatest common divisor (as is -2).
   3 and 5 are relatively prime.
   6 and -6 are associates.
2. Inside $\mathbb{Z}[i]$, we have $(1+i)|2$ because $2 = (1+i)(1-i)$.
   $1+i$ is a common divisor of 2 and $3+i$, since $(3+i) = (1+i)(2-i)$.
   In fact, $1+i$ is a greatest common divisor of 2 and $3+i$, although this is harder to show.
   The elements $2+i$, $-1+2i = i(2+i)$, $-2-i$, and $1-2i$ are all associates.

Arithmetic in Integral Domains, III

We will focus more tightly on the question of how to compute greatest common divisors later.

- In the definition we gave, it is not at all clear how one would establish that a particular value of d is a greatest common divisor of the elements a and b.
- One could resort to the method of writing down all possible divisors of a and b and then searching for a greatest one. But of course, if the ring R is complicated, this might be very difficult. (For example: try writing down all the divisors of $95 + 67i$ inside $\mathbb{Z}[i]$.)

In fact, an even worse scenario exists: it can happen that elements a and b do not have a greatest common divisor at all!

Arithmetic in Integral Domains, IV

Example: Show that $2 + 2\sqrt{-5}$ and 6 do not possess a greatest common divisor in $\mathbb{Z}[\sqrt{-5}]$.

- First, observe that 2 and $1 + \sqrt{-5}$ are both common divisors of $2 + 2\sqrt{-5}$ and 6.
- Now suppose that $2 + 2\sqrt{-5}$ and 6 had a gcd d: then d would divide $2(1 + \sqrt{-5})$ and 6, and also be divisible by 2 and $1 + \sqrt{-5}$.
- By taking norms, we see that $N(d)$ divides both $N(2 + 2\sqrt{-5}) = 24$ and $N(6) = 36$, hence divides 12.
- Also, $N(d)$ would also necessarily be a multiple of $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, hence be a multiple of 12.
- The only possibility is $N(d) = 12$... but there are no elements of norm 12 in $\mathbb{Z}[\sqrt{-5}]$, since there are no integer solutions to $a^2 + 5b^2 = 12$. This is a contradiction, so $2 + 2\sqrt{-5}$ and 6 do not possess a greatest common divisor in $\mathbb{Z}[\sqrt{-5}]$.

Arithmetic in Integral Domains, V

The point of this last example is that greatest common divisors are a bit more subtle in arbitrary integral domains.

- You might also recall from a few lectures ago when I mentioned a non-principal ideal $(2, 1 + \sqrt{-5})$ in this same ring, and identified a non-unique factorization $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.
- Given this reminder, you might then notice that the elements appearing there and in this last example, namely, $2(1 + \sqrt{-5})$ and 6, seem very suspiciously similar.
- Indeed, the lack of greatest common divisors in this example is quite intimately tied to the existence of a non-principal ideal in this ring. (We will return to this question later.)

Arithmetic in Integral Domains, V

We have some basic properties of divisibility:

Proposition (Properties of Divisibility)

Let R be an integral domain. Then for any elements $a, b, d \in R$, the following are true:

1. *The element d divides a if and only if the principal ideal (a) is contained in the principal ideal (d).*
2. *The elements a and b are associate if and only if $a|b$ and $b|a$, if and only if $(a) = (b)$.*
3. *If a and b have a gcd d, the collection of greatest common divisors of a and b is precisely the set of associates of d.*
4. *The element d is a gcd of a and b if and only if (d) is the smallest principal ideal containing (a, b). In particular, if (a, b) is a principal ideal, then any generator is a gcd of a and b.*

Arithmetic in Integral Domains, VI

1. The element d divides a if and only if the principal ideal (a) is contained in the principal ideal (d).

Proof:

- Note $(a) \subseteq (d)$ if and only if $a \in (d)$ if and only if $a = dk$ for some $k \in R$.

---

2. The elements a and b are associate if and only if $a|b$ and $b|a$, if and only if $(a) = (b)$.

Proof:

- Note $(a) = (b)$ if and only if $(a) \subseteq (b)$ and $(b) \subseteq (a)$, which is equivalent to $a|b$ and $b|a$ by (1).
- Also, $a = ub$ for some unit u clearly implies $a|b$ and $b|a$.
- Conversely if $a|b$ and $b|a$, then $a = rb$ and $b = sa$: then $a = rsa$. If $a = 0$ then $b = 0$ also and we are done; otherwise we may cancel to see $rs = 1$ and so r is a unit.

Arithmetic in Integral Domains, VII

3. If a and b have a gcd d, then then the collection of greatest common divisors of a and b is precisely the set of associates of d.

Proof:

- If d is a gcd of a and b and u is any unit, then $(ud)|a$ and $(ud)|b$, and also if $d'|d$ then $d'|(ud)$ so ud is also a gcd.
- Furthermore, if d and e are both gcds of a and b, then $d|e$ and $e|d$ so that d and e are associates by (2).

Arithmetic in Integral Domains, VIII

4. The element d is a gcd of a and b if and only if (d) is the smallest principal ideal containing (a, b). In particular, if (a, b) is a principal ideal, then any generator is a gcd of a and b.

Proof:

- By (1), d is a common divisor of a and b if and only if (d) contains both (a) and (b), which is equivalent to saying $(a, b) \subseteq (d)$.
- Then by (1) again, if d is a gcd of a and b and d' is any other common divisor, we must have $(d) \subseteq (d')$: thus, d is a gcd of a and b if and only if (d) is the smallest principal ideal containing (a, b).
- Finally, if $(a, b) = (d)$ is itself principal, then clearly (d) is the smallest principal ideal containing (a, b).

Arithmetic in Integral Domains, IX

Now that we have established some basic properties of divisibility, we can talk about factorizations.

Definition

Let R be an integral domain. A nonzero element $r \in R$ is irreducible if it is not a unit and, for any "factorization" $r = bc$ with $b, c \in R$, one of b and c must be a unit. A ring element that is not irreducible and not a unit is called reducible: it can be written as $r = ab$ where neither a nor b is a unit.

Examples:

1. The irreducible elements of $\mathbb{Z}$ are precisely the prime numbers (and their negatives).
2. The irreducible elements of $F[x]$ are the irreducible polynomials of positive degree.

Arithmetic in Integral Domains, X

Examples:

3. The element 5 is reducible in $\mathbb{Z}[i]$, since we can write $5 = (2+i)(2-i)$ and neither $2+i$ nor $2-i$ is a unit in $\mathbb{Z}[i]$.
4. The element $2+i$ is irreducible in $\mathbb{Z}[i]$: if $2+i = bc$ for some $z, w \in \mathbb{Z}[i]$, then taking norms yields $5 = N(2+i) = N(b)N(c)$, and since 5 is a prime number, one of $N(b)$ and $N(c)$ would necessarily be ± 1, and then b or c would be a unit. Likewise, $2-i$ is also irreducible.
5. The element 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$: if $2 = bc$ then taking norms yields $4 = N(2) = N(b)N(c)$, and since there are no elements of norm 2 in $\mathbb{Z}[\sqrt{-5}]$, one of $N(b)$ and $N(c)$ would necessarily be ± 1, and then b or c would be a unit.

Arithmetic in Integral Domains, XI

Inside $\mathbb{Z}$, the irreducible elements are the prime numbers. However, we have a different notion of a prime element in an arbitrary integral domain:

Definition

Let R be an integral domain. A nonzero element $p \in R$ is prime if p is nonzero and not a unit, and for any $a, b \in R$, if $p|ab$ then $p|a$ or $p|b$. Equivalently, p is prime if p is nonzero and the ideal (p) is a prime ideal of R.

Arithmetic in Integral Domains, XI

Examples:

1. The prime elements of $\mathbb{Z}$ are precisely the prime numbers (and their negatives).
2. The prime elements of $F[x]$ are the irreducible polynomials of positive degree.
3. The element $2+i$ is prime in $\mathbb{Z}[i]$: if $ab \in (2+i)$ then $2+i = bc$ for some $z, w \in \mathbb{Z}[i]$. Taking norms yields $5 = N(2+i) = N(b)N(c)$, and since 5 is a prime number, one of $N(b)$ and $N(c)$ would necessarily be ± 1, and then b or c would be a unit.
4. The element 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$: note that $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ is divisible by 2, but neither $1+\sqrt{-5}$ nor $1-\sqrt{-5}$ is divisible by 2.

Arithmetic in Integral Domains, XII

As suggested by the examples above, prime elements are always irreducible, but irreducible elements are not necessarily prime:

Proposition (Primes are Irreducible)

In an integral domain, prime elements are always irreducible.

Proof:

- Suppose $p \in R$ is a prime element.
- If $p = bc$ then since $p|bc$, we conclude that $p|b$ or $p|c$; without loss of generality suppose $b = pr$.
- Then $p = prc$, so since $p \neq 0$ we may cancel to conclude $rc = 1$, so that c is a unit. Thus, p is irreducible.

Later, we will discuss under what conditions irreducible elements will be prime.

Quadratic Integer Rings, I

We now have enough background to discuss some facts about the rings that we will be analyzing in this chapter. First, we (re-)introduce quadratic fields:

Definition

Let D be a squarefree integer not equal to 1. The quadratic field $\mathbb{Q}(\sqrt{D})$ is the set of complex numbers of the form $a + b\sqrt{D}$, where a and b are rational numbers.

- Recall that an integer is squarefree if it is not divisible by the square of any prime, and not equal to 1.
- We lose nothing here by assuming that D is a squarefree integer, since two different integers differing by a square factor would generate the same set of complex numbers $a + b\sqrt{D}$.

Quadratic Integer Rings, II

For explicitness, the operations in $\mathbb{Q}(\sqrt{D})$ are as follows:
$(a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$, and
$(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + Dbd) + (ad + bc)\sqrt{D}$.

- Since $\mathbb{Q}(\sqrt{D})$ is clearly closed under subtraction and multiplication, and contains $0 = 0 + 0\sqrt{D}$, it is a subring of $\mathbb{C}$ and hence an integral domain, since it contains 1.
- It is in fact a field (justifying the name "quadratic field") because we can write $(a + b\sqrt{D})^{-1} = \dfrac{a - b\sqrt{D}}{a^2 - Db^2}$, and $a^2 - Db^2 \neq 0$ provided that a and b are not both zero because $\sqrt{D}$ is irrational by the assumption that D is squarefree and not equal to 1.

Quadratic Integer Rings, III

We can also construct this ring[1] as a quotient ring of a polynomial ring.

- Specifically, $\mathbb{Q}(\sqrt{D})$ is isomorphic to the quotient ring $\mathbb{Q}[x]$ modulo the principal ideal $(x^2 - D)$.
- The isomorphism is given explicitly by mapping $p(x) \in \mathbb{Q}[x]$ to $p(\sqrt{D}) \in \mathbb{Q}(\sqrt{D})$.
- This "evaluation map" can be seen to be a ring homomorphism, and its kernel is the ideal $(x^2 - D)$ of $\mathbb{Q}[x]$.
- Since the evaluation map is clearly surjective, the first isomorphism theorem tells us that $\mathbb{Q}(\sqrt{D})$ is isomorphic to the quotient ring $\mathbb{Q}[x]/(x^2 - D)$, as claimed.

[1] Or, depending on how pedantic you wish to be, a ring isomorphic to it.

Quadratic Integer Rings, IV

We have already made use of the field norm, but we record its definition again here:

Definition

The field norm $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ *is defined to be the function* $N(a + b\sqrt{D}) = a^2 - Db^2 = (a + b\sqrt{D})(a - b\sqrt{D})$.

The fundamental property of the field norm is that it is multiplicative (i.e., that $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Q}(\sqrt{D})$), as we showed back during the first week of class.

Quadratic Integer Rings, V

A fundamental subring of the quadratic field $\mathbb{Q}(\sqrt{D})$ is its associated "quadratic integer ring".

- The most obvious choice for an analogy of the integers $\mathbb{Z}$ inside $\mathbb{Q}(\sqrt{D})$ would be $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$.
- However, notice that if $D \equiv 1 \pmod 4$, then the slightly larger subset $\mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{a + b\frac{1+\sqrt{D}}{2} : a, b \in \mathbb{Z}\}$ is actually also a subring: closure under subtraction is obvious, and for multiplication we can write $(a + b\frac{1+\sqrt{D}}{2})(c + d\frac{1+\sqrt{D}}{2}) = (ac + \frac{D-1}{4}bd) + (ad + bc + bd)\frac{1+\sqrt{D}}{2}$.
- One reason that this larger set turns out to give a slightly better analogy for the integers $\mathbb{Z}$ when $D \equiv 1 \pmod 4$ is that $\frac{1+\sqrt{D}}{2}$ satisfies a monic polynomial with integer coefficients: specifically, it is a root of $x^2 - x + \frac{1-D}{4} = 0$.

Quadratic Integer Rings, VI

So, with this minor enlargement when $D \equiv 1 \pmod 4$, we have our definition of a quadratic integer ring:

Definition

The ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ in the quadratic field $\mathbb{Q}(\sqrt{D})$ is defined as $\mathbb{Z}[\sqrt{D}]$ if $D \equiv 2$ or $3 \pmod 4$ and as $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ when $D \equiv 1 \pmod 4$. Each of these rings is an integral domain.

- For $D \equiv 2, 3 \pmod 4$, observe that $N(a + b\sqrt{D}) = a^2 - Db^2$ is an integer for every $a + b\sqrt{D} \in \mathcal{O}_{\sqrt{D}}$.
- Likewise, if $D \equiv 1 \pmod 4$, we have $N(a + b\frac{1+\sqrt{D}}{2}) = a^2 + ab + \frac{1-D}{4}b^2$ is also an integer for every $a + b\frac{1+\sqrt{D}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.
- Thus, the field norm N is always integer-valued on $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

Quadratic Integer Rings, VII

Since the field norm is integer-valued on $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, we can use it to identify units:

Proposition (Units in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$)

An element r in the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a unit if and only if $N(r) = \pm 1$.

Example:

- The units in $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$: for $r = a + bi$ we have $N(r) = a^2 + b^2$, and $a^2 + b^2 = \pm 1$ has four solutions yielding the four listed units.

We essentially proved this result already, but let's do it again.

Quadratic Integer Rings, VIII

Proof:

- Suppose $r = a + b\sqrt{D}$ and let $\overline{r} = a - b\sqrt{D}$, so that $N(r) = r\overline{r}$.
- Note that $\overline{r} = 2a - r$, so that even when $D \equiv 1 \pmod 4$ (with a and b possibly half-integers), $\overline{r}$ is still in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.
- If $N(r) = \pm 1$, then we see that $r\overline{r} = \pm 1$, so (by multiplying by -1 if necessary) we obtain a multiplicative inverse for r.
- Conversely, suppose r is a unit and $rs = 1$. Taking norms yields $N(r)N(s) = N(rs) = 1$. Since $N(r)$ and $N(s)$ are both integers, we see that $N(r)$ must either be 1 or -1.

Quadratic Integer Rings, IX

Example: Find the units in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[(1+\sqrt{-3})/2]$.

Quadratic Integer Rings, IX

Example: Find the units in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[(1+\sqrt{-3})/2]$.

- For $r = a + b\dfrac{1+\sqrt{-3}}{2}$ we see $N(r) = a^2 + ab + b^2$.
- We must therefore solve $a^2 + ab + b^2 = 1$ in $\mathbb{Z}$.
- By multiplying by 4 and completing the square, this equation is equivalent to $(2a+b)^2 + 3b^2 = 4$, which has six solutions corresponding to $r = 1, -1, \omega, -\omega, \omega^2, -\omega^2$, where $\omega = \dfrac{1+\sqrt{-3}}{2}$ is seen to be a sixth root of unity satisfying $\omega^6 = 1$. (If you prefer, you can also think of this list as $\{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$.)

Quadratic Integer Rings, X

In general, determining the full set of units in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a nontrivial computation.

- When $D < 0$ it is not too difficult to see (by completing the square in a similar way to above when $D \equiv 1 \pmod 4$) that if $D \neq -1, -3$, then the only units in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ are ± 1.
- When $D > 0$ and $D \equiv 2, 3 \pmod 4$, solving $N(\alpha) = \pm 1$ is equivalent to solving Pell's equation $x^2 - Dy^2 = \pm 1$, which we have already described at length.
- For $D > 0$ with $D \equiv 1 \pmod 4$, we see $N(\frac{a+b\sqrt{D}}{2}) = \pm 1$ is equivalent to the Pell's equation $a^2 - Db^2 = \pm 4$, whose solutions can also be found using continued fractions.
- In particular, the same sort of analysis we gave for $x^2 - Dy^2 = \pm 1$ will show that the solutions are of the form $\pm u^n$ where u is the fundamental unit.

Quadratic Integer Rings, XI

We will return to discuss these rings after we have developed some additional results about ideals and factorizations in integral domains, which is our next major topic.

For notational convenience, I will often write $\mathcal{O}_{\sqrt{D}}$ as shorthand for $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, since it is marginally faster to typeset.

Summary

We discussed some properties of arithmetic and factorization in integral domains.

We defined the quadratic integer rings and remarked on some of their basic properties.

Next lecture: Euclidean domains, principal ideal domains.