Math 4527 (Number Theory 2)

Lecture #23 of ~~38~~ 37 $\sim$ March 15, 2021

Quadratic Integer Rings + Euclidean Domains

- Quadratic Integer Rings
- Euclidean Domains

This material represents §8.1.5-8.1.6 from the course notes.

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

By using norms, we can also study possible factorizations and establish the irreducibility of elements. The following special case is often helpful:

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

If $r \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ has $N(r) = \pm p$ where p is a prime number, then r is irreducible in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

Examples:

1. The elements $1 + i$ and $2 + i$ in $\mathbb{Z}[i]$ are irreducible, since their norms are 2 and 5 respectively.
2. The elements $\dfrac{5 + \sqrt{5}}{2}$ and $4 + \sqrt{5}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ are irreducible since their norms are 5 and 11 respectively.

Quadratic Integer Rings, XI

Proof:

- Suppose $N(r) = \pm p$ and we had a factorization $r = s_1 s_2$.
- Taking norms yields $\pm p = N(s_1 s_2) = N(s_1)N(s_2)$.
- But since p is prime and $N(s_1)$ and $N(s_2)$ are integers, the only possibility is to have one of $N(s_1)$ and $N(s_2)$ equal to ± 1.
- By our result earlier, this means that s_1 or s_2 is a unit.
- Then r is indeed irreducible, as claimed.

Quadratic Integer Rings, XII

We remark that the proposition is not an if-and-only-if, as there can exist irreducible elements of non-prime norm as well.

Examples:

3. The element $3 \in \mathbb{Z}[i]$ has $N(3) = 9$, but 3 is irreducible because any factorization $3 = z_1 z_2$ would require $9 = N(3) = N(z_1)N(z_2)$, but since there are no elements of norm 3 in $\mathbb{Z}[i]$, the only possible factorizations require $N(z_1)$ or $N(z_2)$ to equal 1.
4. The element $1 + \sqrt{-5} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ has $N(1 + \sqrt{-5}) = 6$, but $1 + \sqrt{-5}$ is irreducible because any factorization would have to be into a product of an element of norm 2 and an element of norm 3, but there are no such elements in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$.

Quadratic Integer Rings, XIII

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.

Euclidean Domains, I

Our next goal is to discuss what it means for an integral domain to possess a "division algorithm":

Definition

If R is an integral domain, any function $N : R \to \{0, 1, 2, \dots\}$ such that $N(0) = 0$ is called a norm on R.

The purpose of the norm function is to allow us to compare the size of the remainder to the size of the original element.

Definition

A Euclidean domain (or domain with a division algorithm) is an integral domain R that possesses a norm N with the property that, for every a and b in R with $b \neq 0$, there exist some q and r in R such that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$.

Euclidean Domains, II

A few comments:

- The norm property is fairly weak, and any given domain may possess many different norms. Also, the use of the word "norm" has very little to do with the field norm on $\mathbb{Q}(\sqrt{D})$.
- Also, note that the quotient and remainder are *not* required to be unique! There may be multiple pairs (q, r) with $a = qb + r$ and $N(r) < N(b)$.

Examples:

1. Any field is a Euclidean domain, because any norm will satisfy the defining condition. This follows because for every a and b with $b \neq 0$, we can write $a = qb + 0$ with $q = a \cdot b^{-1}$.
2. The integers $\mathbb{Z}$ are a Euclidean domain with $N(n) = |n|$.
3. If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain with norm given by $N(p) = \deg(p)$ for $p \neq 0$.

Euclidean Domains, III

The reason Euclidean domains have that name is that we can perform the Euclidean algorithm in such a ring:

Definition

If R is a Euclidean domain and $a, b \in R$ with $b \neq 0$, the Euclidean algorithm in R consists of repeatedly applying the division algorithm to a and b until a remainder of zero is obtained:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_k r_k + r_{k+1} \\ r_k &= q_{k+1} r_{k+1}. \end{aligned}$$

Since $N(r_1) > N(r_2) > \cdots \geq 0$, this sequence must eventually terminate with a zero remainder.

Euclidean Domains, IV

The Gaussian integers provide another important example of a Euclidean domain:

Proposition ($\mathbb{Z}[i]$ is Euclidean)

The Gaussian integers $\mathbb{Z}[i]$ are a Euclidean domain under the norm $N(a+bi) = a^2 + b^2$.

To prove this theorem we will explain how to compute the quotient and remainder and establish that they have the required property.

- Explicitly, given $a+bi$ and $c+di$ in $\mathbb{Z}[i]$, we will show how to produce $q, r \in \mathbb{Z}[i]$ such that $a+bi = q(c+di) + r$ and $N(r) \leq \frac{1}{2}N(c+di)$.
- This is even stronger than is needed (once we note that the only element of norm 0 is 0).

Euclidean Domains, IV

Proof:

- Suppose we are dividing $a + bi$ by $c + di$.
- If $c + di \neq 0$, then we can write $\dfrac{a + bi}{c + di} = x + iy$ for reals $x = (ac + bd)/(c^2 + d^2)$ and $y = (bc - ad)/(c^2 + d^2)$.
- Now we define $q = s + ti$ where s is the integer closest to x and t is the integer closest to y, and set $r = (a + bi) - q(c + di)$. Clearly, $(a + bi) = q(c + di) + r$.
- All we need to do now is show $N(r) \leq \frac{1}{2}N(c + di)$.
- First observe that $\frac{r}{c+di} = \frac{a+bi}{c+di} - q = (x - s) + (y - t)i$.
- Then because $|x - s| \leq \frac{1}{2}$ and $|y - t| \leq \frac{1}{2}$ by construction, we have $\left|\frac{r}{c+di}\right| \leq \left|\frac{1}{2} + \frac{1}{2}i\right| = \frac{\sqrt{2}}{2}$.
- Squaring and rearranging gives $N(r) \leq \frac{1}{2}N(c + di)$, as desired.

Euclidean Domains, V

It is reasonable to ask about other quadratic integer rings $\mathcal{O}_{\sqrt{D}}$.

- For such rings, the function $N(a + b\sqrt{D}) = \left|a^2 - Db^2\right|$ is always a norm, but it does not in general give a division algorithm.
- In our proof, we needed to know that the remainder had a smaller size than $c + di$, which required an estimate on the ratio $r/(c + di)$. For other values of D, the resulting estimate will end up being greater than 1, and so we don't get a Euclidean norm.
- The proof does, however, adapt fairly easily to show that $\mathcal{O}_{\sqrt{D}}$ is a Euclidean domain for a few other small values of D, such as $D = -7$, -3, -2, and 2.

Euclidean Domains, VI

The polynomial ring $F[x]$ is also a Euclidean domain:

Theorem ($F[x]$ is Euclidean)

If F is a field, the polynomial ring $F[x]$ is a Euclidean domain with norm given by the degree map $N(p) = \deg(p)$.

- We require F to be a field to be able to divide by arbitrary nonzero coefficients. (Over $\mathbb{Z}$, for instance, we cannot divide x^2 by $2x$ and get a remainder that is a constant polynomial.)
- The proof is just the usual long-division algorithm for polynomials.

Euclidean Domains, VII

Proof:

- We induct on the degree n of $a(x)$.
- The base case is trivial, as we may take $q = r = 0$ if $a = 0$.
- Now suppose the result holds for all polynomials $a(x)$ of degree $\leq n - 1$. If $\deg(b) > \deg(a)$ then we can simply take $q = 0$ and $r = a$, so now also assume $\deg(b) \leq \deg(a)$.
- Write $a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ and $b(x) = b_m x^m + \cdots + b_0$, where $b_m \neq 0$ since $b(x) \neq 0$.
- Observe that $a^\dagger(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$ has degree less than n, since we have cancelled the leading term of $a(x)$. (Here we are using the fact that F is a field, so that $\frac{a_n}{b_m}$ also lies in F.)
- By the induction hypothesis, $a^\dagger(x) = q^\dagger(x) b(x) + r^\dagger(x)$ for some $q^\dagger(x)$ and $r^\dagger(x)$ with $r^\dagger = 0$ or $\deg(r^\dagger) < \deg(b)$.
- Then $a(x) = [q^\dagger(x) + \frac{a_n}{b_m} x^{n-m}] b(x) + r^\dagger(x)$, so $q(x) = q^\dagger(x) + \frac{a_n}{b_m} x^{n-m}$ and $r(x) = r^\dagger(x)$ work as claimed.

Euclidean Domains, VIII

As in $\mathbb{Z}$, the main significance of the Euclidean algorithm in a Euclidean domain is that we can use it to compute gcds:

Theorem (Bézout's Theorem)

If R is a Euclidean domain and a and b are arbitrary elements with $b \neq 0$, then the last nonzero remainder d arising from the Euclidean Algorithm applied to a and b is a greatest common divisor of a and b. (In particular, any two elements in a Euclidean domain always possess at least one gcd.) Furthermore, there exist elements $x, y \in R$ such that $d = ax + by$.

The ideas in the proof are the same as for $\mathbb{Z}$.

Euclidean Domains, IX

Proof:

- By an easy induction (starting with $r_k = q_{k+1} r_{k+1}$), we see that $d = r_{k+1}$ divides r_i for each $1 \leq i \leq k$.
- Thus, $d|a$ and $d|b$, so the last nonzero remainder is a common divisor of a and b.
- Now suppose d' is some other common divisor of a and b.
- By another easy induction (starting with $d'|(a - q_1 b) = r_1$), it is easy to see that d' divides r_i for each $1 \leq i \leq k + 1$, and therefore $d'|d$. Hence d is a greatest common divisor.
- For the existence of x and y with $d = ax + by$, we simply observe (by yet another easy induction starting with $r_1 = a - q_1 b$) that each remainder can be written in the form $r_i = x_i a + y_i b$ for some $x_i, y_i \in R$.

Euclidean Domains, X

Example: Inside $\mathbb{Z}$, find a gcd of 1598 and 4879 using the Euclidean algorithm, and write it explicitly as a linear combination.

Euclidean Domains, X

Example: Inside $\mathbb{Z}$, find a gcd of 1598 and 4879 using the Euclidean algorithm, and write it explicitly as a linear combination.

- First, we use the Euclidean algorithm:

$$\begin{aligned} 4879 &= 3 \cdot 1598 + 85 \\ 1598 &= 18 \cdot 85 + 68 \\ 85 &= 1 \cdot 68 + 17 \\ 68 &= 4 \cdot 17 \end{aligned}$$

  and so the gcd is 17.

- For the linear combination, we solve for the remainders:

$$\begin{aligned} 85 &= && = && 1 \cdot 4879 - 3 \cdot 1598 \\ 68 &= 1598 - 18 \cdot 85 && = && -18 \cdot 4879 + 55 \cdot 1598 \\ 17 &= 85 - 1 \cdot 68 && = && 19 \cdot 4879 - 58 \cdot 1598 \end{aligned}$$

  so we obtain $17 = 19 \cdot 4879 - 58 \cdot 1598$.

Euclidean Domains, XI

Example: In $\mathbb{Z}[i]$, find a greatest common divisor of $50 - 50i$ and $43 - i$, and write it explicitly as a linear combination.

Euclidean Domains, XI

Example: In $\mathbb{Z}[i]$, find a greatest common divisor of $50 - 50i$ and $43 - i$, and write it explicitly as a linear combination.

- We use the Euclidean algorithm. Dividing $43 - i$ into $50 - 50i$ yields $\frac{50 - 50i}{43 - i} = \frac{44}{37} - \frac{42}{37}i$, so rounding to the nearest Gaussian integer yields the quotient $q = 1 - i$. The remainder is then $50 - 50i - (1 - i)(43 - i) = (8 - 6i)$.
- Next, dividing $8 - 6i$ into $43 - i$ yields $\frac{43 - i}{8 - 6i} = \frac{7}{2} + \frac{5}{2}i$, so rounding to the nearest Gaussian integer (there are four possibilities so we just choose one) yields the quotient $q = 3 + 2i$. The remainder is then $43 - i - (3 + 2i)(8 - 6i) = (7 + i)$.
- Finally, dividing $7 + i$ into $8 - 6i$ yields $\frac{8 - 6i}{7 + i} = 1 - i$, so the quotient is $1 - i$ and the remainder is 0.

Euclidean Domains, XI

Example: In $\mathbb{Z}[i]$, find a greatest common divisor of $50 - 50i$ and $43 - i$, and write it explicitly as a linear combination.

- We can summarize these calculations more compactly:

$$\begin{aligned} 50 - 50i &= (1 - i) \cdot (43 - i) + (8 - 6i) \\ 43 - i &= (3 + 2i) \cdot (8 - 6i) + (7 + i) \\ 8 - 6i &= (1 - i) \cdot (7 + i) \end{aligned}$$

- To find the linear combination, solve for the remainders:

$$\begin{aligned} 8 - 6i &= 1 \cdot (50 - 50i) - (1 - i) \cdot (43 - i) \\ 7 + i &= (43 - i) - (3 + 2i)(8 - 6i) \\ &= (43 - i) - (3 + 2i) \cdot (50 - 50i) + (3 + 2i)(1 - i) \cdot (43 - i) \\ &= (-3 - 2i) \cdot (50 - 50i) + (6 - i) \cdot (43 - i). \end{aligned}$$

Euclidean Domains, XII

Example: In $\mathbb{F}_3[x]$, find a greatest common divisor of $p = x^6 + 2$ and $q = x^8 + 2$, and write it explicitly as a linear combination.

Euclidean Domains, XII

Example: In $\mathbb{F}_3[x]$, find a greatest common divisor of $p = x^6 + 2$ and $q = x^8 + 2$, and write it explicitly as a linear combination.

- We apply the Euclidean algorithm: we have

$$\begin{aligned} x^8 + 2 &= x^2(x^6 + 2) + (x^2 + 2) \\ x^6 + 2 &= (x^4 + x^2 + 1)(x^2 + 2) \end{aligned}$$

  and so the last nonzero remainder is $x^2 + 2$.
- By back-solving, we see that $x^2 + 2 = 1 \cdot (x^8 + 2) - x^2(x^6 + 2)$.

Of course, most situations require more than one step, in which case we would solve the equations for the remainders from the top down.

Euclidean Domains, XIII

The ideals of Euclidean domains are particularly simple:

Theorem (Ideals of Euclidean Domains)

Every ideal of a Euclidean domain is principal.

Proof:

- Clearly (0) is principal, so suppose $I \neq (0)$ and let d be a nonzero element of I of smallest possible norm. (Such an element must exist by the well-ordering axiom of $\mathbb{Z}$.)
- Since $d \in I$ we have $(d) \subseteq I$. If $a \in I$ is any other element, by the division algorithm we can write $a = qd + r$ for some r where either $r = 0$ or $N(r) < N(d)$.
- However, since $r = a - qd \in I$ since both a and qd are in I, and $N(d)$ is minimal, we must have $r = 0$. Therefore, $a = qd$ and thus $a \in (d)$. Thus $I \subseteq (d)$ and so $I = (d)$ is principal.

Euclidean Domains, XIV

Corollary

Every ideal of $\mathbb{Z}$, $F[x]$, and $\mathbb{Z}[i]$ is principal, for any field F.

Proof:

- Each of these rings is a Euclidean domain.

From this result, we see that any ring containing a non-principal ideal is not Euclidean with respect to any norm.

Examples:

1. The ring $\mathbb{Z}[x]$ is not a Euclidean domain, since the ideal $(2, x)$ is not principal.
2. The ring $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean domain, since the ideal $(2, 1 + \sqrt{-5})$ is not principal.

Euclidean Domains, XV

Having a Euclidean algorithm in a domain R is very useful, as we have seen, since it allows us to compute greatest common divisors, and it also implies that every ideal in R is principal.

- However, most integral domains are not Euclidean. In some cases, however, we can still salvage a criterion that is close enough to being Euclidean to allow us to deduce most of the nice facts about divisibility and GCDs that we got for Euclidean domains.
- The condition we investigate next is that of having every ideal be principal, which leads to the class of principal ideal domains. We will discuss these rings, and their properties, next time.

Summary

We defined the quadratic integer rings and discussed some of their properties.

We introduced Euclidean domains and established some of their properties.

Next lecture: Principal ideal domains and unique factorization domains.