Math 332 Winter 2023, Lecture 15: Rings

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

1. Rings and ideals (cont'd)

1.12. The Chinese Remainder Theorem (cont'd)

1.12.8. A few words about noncommutative rings

Recall the main theorem from Lecture 14:

Theorem 1.12.7 (The Chinese Remainder Theorem for k ideals)**.** Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a commutative ring R. Then:

(a) We have

$$I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k.$$

(b) We have

$$R/\left(I_1 I_2 \cdots I_k\right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

(c) More concretely, there is a ring isomorphism

$$R/\left(I_1 I_2 \cdots I_k\right) \to R/I_1 \times R/I_2 \times \cdots \times R/I_k,$$
$$\overline{r} \mapsto \left(\overline{r}, \overline{r}, \ldots, \overline{r}\right).$$

We sketched the proof of this and applied it to the case of $R = \mathbb{Z}$.

Abstract algebra is called "abstract" because it is about generalizing, not about applying to particular cases. Commutative rings are legion, but arbitrary rings are an even broader universe. Thus, for good or bad, we might wonder: Can Theorem 1.12.7 be generalized to arbitrary rings (not just commutative ones)?

The proof used the commutativity of R in a crucial point. Indeed, we used it back in the proof of Theorem 1.12.3 **(a)** in Lecture 13, when we rewrote ai as ia. If R is not commutative, then we cannot do this, so (for two comaximal ideals I and J of R) we obtain $I \cap J = IJ + JI$ instead of $I \cap J = IJ$. As Exercise 2 on homework set #4 shows, this is the best we can get.

As a consequence, Theorem 1.12.7 also wouldn't hold without the commutativity of R. However, can we tweak it in such a way that it would for noncommutative R as well?

For parts **(b)** and **(c)**, this turns out to be surprisingly easy: Just replace $I_1 I_2 \cdots I_k$ by $I_1 \cap I_2 \cap \cdots \cap I_k$! This way, the claim remains the same for commutative R, because Theorem 1.12.7 **(a)** shows that $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$ in this case, but for general R it remains true even without commutativity. That is, we have the following:

Theorem 1.12.10 (The Chinese Remainder Theorem for k ideals: quotient part)**.** Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a ring R. Then:

(a) We have

$$R/\left(I_1 \cap I_2 \cap \cdots \cap I_k\right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

(b) More concretely, there is a ring isomorphism

$$R/\left(I_1 \cap I_2 \cap \cdots \cap I_k\right) \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$$

that sends each residue class $r + \left(I_1 \cap I_2 \cap \cdots \cap I_k\right)$ to the k-tuple $(r + I_1,\ r + I_2,\ \ldots,\ r + I_k)$.

The proof is not much harder than the proof of the respective parts of Theorem 1.12.7 (see §2.12.5 in the text for details).

Now what about Theorem 1.12.7 **(a)** – do we have to say goodbye to it if R is not commutative?

As we know, the case $k = 2$ can be fixed by replacing IJ by $IJ + JI$ (where $I = I_1$ and $J = I_2$). The same applies to an arbitrary k:

Theorem 1.12.11. Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a ring R. Then, $I_1 \cap I_2 \cap \cdots \cap I_k$ is the sum of all $k!$ possible products of $I_1, I_2, \ldots, I_k$ in some order.

For instance, for $k = 3$, Theorem 1.12.11 claims that

$$I_1 \cap I_2 \cap I_3 = I_1 I_2 I_3 + I_1 I_3 I_2 + I_2 I_1 I_3 + I_2 I_3 I_1 + I_3 I_1 I_2 + I_3 I_2 I_1$$

whenever I_1, I_2, I_3 are three mutually comaximal ideals of a ring R.

Theorem 1.12.11 can be proved by an easy adaptation of our proof of Theorem 1.12.10 **(a)**.

But it turns out that this theorem can be improved. Surprisingly, no one seems to have observed this until Birgit van Dalen in her 2005 bachelor's thesis [vanDal05] (see [vanDal06] for a summary in English). It is possible to replace the sum of all $k!$ possible products by certain smaller sums so that Theorem 1.12.11 still remains true. Van Dalen has characterized precisely which smaller sums work (i.e., what subsets of the $k!$ possible products can be discarded so that the remaining products still add up to $I_1 \cap I_2 \cap \cdots \cap I_k$), and in particular found two choices that work for every k:

Theorem 1.12.12. Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a ring R. Then:

(a) We have

$$I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k + I_k I_{k-1} \cdots I_1.$$

(b) We have

$$I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k + I_2 I_3 \cdots I_k I_1 + I_3 I_4 \cdots I_k I_1 I_2 + \cdots + I_k I_1 I_2 \cdots I_{k-1}.$$

(The right hand side here is the sum of all cyclically rotated versions of the product $I_1 I_2 \cdots I_k$.)

We refer to [vanDal05, Stellingen 4.7 and 4.8] for the proof of this theorem.

See also §2.12.7 in the text for some more identities for comaximal ideals. (I think there are some things left unexplored in this field, both in terms of finding identities and in terms of finding applications/examples for them.)

1.13. Euclidean rings and Euclidean domains

1.13.1. All ideals of $\mathbb{Z}$ are principal

We have been talking about ideals of $\mathbb{Z}$ for quite a while now, but so far they have all been principal. Coincidence? Not really:

Proposition 1.13.1. Any ideal of $\mathbb{Z}$ is principal.

Proof. Let I be an ideal of $\mathbb{Z}$. We must prove that I is principal.

If I contains only 0, then $I = \{0\} = 0\mathbb{Z}$, which is principal.

Thus, we WLOG assume that I contains not only 0. Hence, I contains a nonzero element. Therefore, I contains a positive element (since you can otherwise take a negative element of I and multiply it by -1). Let b be the **smallest** positive element of I. Then, $b \in I$, and thus every multiple of b belongs to I (by the second ideal axiom). In other words, $b\mathbb{Z} \subseteq I$.

Now we shall show that $b\mathbb{Z} = I$.

To prove this, pick any $a \in I$. As you know from elementary number theory, we can divide a by b with remainder (since b is a positive integer). That is, there exist some $q \in \mathbb{Z}$ and some $r \in \{0, 1, \ldots, b-1\}$ such that $a = qb + r$.

Consider these q and r. From $r \in \{0, 1, \ldots, b-1\}$, we obtain $r \geq 0$ and $r \leq b - 1 < b$.

From $a = qb + r$, we obtain $r = a - qb = a + (-q)\, b \in I$ (since $a, b \in I$, and since I is an ideal). Therefore, r is an element of I that is smaller than b (since $r < b$).

However, b is the **smallest** positive element of I. Thus, no positive element of I can be smaller than b. If r was positive, this would contradict the result of the preceding paragraph. Hence, r cannot be positive. Since $r \geq 0$, we thus obtain $r = 0$. Hence, $a = qb + \underbrace{r}_{=0} = qb = bq \in b\mathbb{Z}$.

So we have shown that $a \in b\mathbb{Z}$ for each $a \in I$. In other words, $I \subseteq b\mathbb{Z}$. Combined with $b\mathbb{Z} \subseteq I$, this yields $I = b\mathbb{Z}$, which shows that $b\mathbb{Z}$ is principal. Thus, Proposition 1.13.1 is proved. □

Note that this proof is non-constructive as stated, as it is not clear how to find the smallest positive element of a given ideal of $\mathbb{Z}$ (or to even figure out whether this ideal has a nonzero element to begin with). However, at the level of generality at which Proposition 1.13.1 is stated, nothing can be done about this, since the ideal I could be given in an arbitrarily abstract way, and in that case it might be algorithmically impossible to find an integer b that satisfies $I = b\mathbb{Z}$ [1].

For certain ways of defining an ideal I, however, there exist algorithms for finding a generator of I (that is, an integer b satisfying $I = b\mathbb{Z}$). Most famously, if a and b are two integers, then the ideal $a\mathbb{Z} + b\mathbb{Z}$ equals the ideal $c\mathbb{Z}$ for $c = \gcd(a, b)$ (we will prove this in Lecture 16), and the latter number c can be computed by the Euclidean algorithm. The extended Euclidean algorithm furthermore computes two integers x and y satisfying $xa + yb = c$, thus making the ideal equality $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ explicit.

Both the Euclidean algorithm and the proof of Proposition 1.13.1 rely on one important feature of the integers: division with remainder. Not every ring has this feature. However, many rings do, and we can give them a name:

1.13.2. Euclidean rings

Definition 1.13.2. Let R be a commutative ring.

(a) A **norm** on R means a function $N : R \to \mathbb{N}$ with $N(0) = 0$.

(b) A norm N on R is said to be **Euclidean** if for any $a \in R$ and any nonzero $b \in R$, there exist elements $q, r \in R$ with

$$a = qb + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(b)).$$

(c) We say that R is a **Euclidean ring** if R has a Euclidean norm.

(d) We say that R is a **Euclidean domain** if R is a Euclidean ring and an integral domain.

You can think of the norm as a measure of "how big" an element of R is, similar to the absolute value of an integer or to the degree of a polynomial[2]. Note that we are **not** requiring that the norm N be multiplicative (i.e., satisfy $N(ab) = N(a) \cdot N(b)$). We also are not requiring the q and the r in Definition 1.13.2 **(b)** to be unique.

Some examples:

[1] For example, let I be the set of all integers that are 0 or multiples of an odd perfect number (where a **perfect number** means a positive integer that equals the sum of all its proper positive divisors). This is clearly an ideal of $\mathbb{Z}$, but does it have a nonzero element? This question requires knowing whether an odd perfect number exists, but this is a well-known open problem. Finding an integer b satisfying $I = b\mathbb{Z}$ is at least as hard as solving this problem.

[2] As we will soon see, these two examples actually are Euclidean norms on their respective rings.

- Any field F is a Euclidean domain. To wit, any map $N : F \to \mathbb{N}$ with $N(0) = 0$ is a Euclidean norm on F. (Indeed, for any $a \in F$ and any nonzero $b \in F$, the condition in Definition 1.13.2 **(b)** is satisfied for $q = \frac{a}{b}$ and $r = 0$.)

- The ring $\mathbb{Z}$ is a Euclidean domain. Indeed, the map

$$\begin{aligned} N : \mathbb{Z} &\to \mathbb{N}, \\ a &\mapsto |a| \end{aligned}$$

is a Euclidean norm on $\mathbb{Z}$. The fact that it is Euclidean follows from division with remainder[3]. Note that our condition in Definition 1.13.2 **(b)** does not require that $r \geq 0$, so it is more liberal than the notion of remainder that you know from high school. And indeed, the q and the r in Definition 1.13.2 **(b)** are usually not unique: For $a = 7$ and $b = 5$, there are **two** pairs $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ with

$$a = qb + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(b)).$$

These pairs are $(1, 2)$ and $(2, -3)$. The second pair has negative r, which disqualifies it as a remainder in the high-school sense, but is perfectly fine for Definition 1.13.2 **(b)**.

- If F is a field, then the ring $F[x]$ of polynomials (in a single indeterminate x) with coefficients in F is a Euclidean domain. A Euclidean norm for it is the map

$$\begin{aligned} p &\mapsto \deg p \qquad (\text{for } p \neq 0), \\ 0 &\mapsto 0. \end{aligned}$$

We will see this in more details once we have properly defined polynomials.

However, polynomial rings in more than 1 variable are not Euclidean; neither are polynomial rings over non-fields.

- The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain.

Indeed, we claim that the map

$$\begin{aligned} N : \mathbb{Z}[i] &\to \mathbb{N}, \\ a + bi &\mapsto a^2 + b^2 \qquad (\text{for } a, b \in \mathbb{Z}) \end{aligned}$$

is a Euclidean norm.

[3] You may need to think for a few moments about the $b < 0$ case in Definition 1.13.2 **(b)**, but it is not significantly harder than the (classical) $b > 0$ case (and can be reduced to the latter quite easily).

To prove this, we must show that for any $\alpha \in \mathbb{Z}[i]$ and any nonzero $\beta \in \mathbb{Z}[i]$, there exist elements $q, r \in \mathbb{Z}[i]$ such that

$$\alpha = q\beta + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(\beta)).$$

So let us fix an $\alpha \in \mathbb{Z}[i]$ and a nonzero $\beta \in \mathbb{Z}[i]$. We are looking for elements $q, r \in \mathbb{Z}[i]$ such that

$$\alpha = q\beta + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(\beta)).$$

Actually, we don't need the $r = 0$ option; I claim that we can find elements $q, r \in \mathbb{Z}[i]$ such that

$$\alpha = q\beta + r \qquad \text{and} \qquad N(r) < N(\beta).$$

To find such elements q and r, we make the following observation: Any $z \in \mathbb{Z}[i]$ satisfies $N(z) = |z|^2$. Hence, we have the following chain of equivalences:

$$\begin{aligned}(N(r) < N(\beta)) &\iff \left(|r|^2 < |\beta|^2\right) \iff (|r| < |\beta|) \\ &\iff \left(\frac{|r|}{|\beta|} < 1\right) \iff \left(\left|\frac{r}{\beta}\right| < 1\right)\end{aligned}$$

(since $\dfrac{|z|}{|w|} = \left|\dfrac{z}{w}\right|$ for any complex numbers z and $w \neq 0$). Moreover, we have the equivalence

$$(\alpha = q\beta + r) \iff \left(\frac{\alpha}{\beta} = q + \frac{r}{\beta}\right) \iff \left(\frac{\alpha}{\beta} - q = \frac{r}{\beta}\right).$$

Thus, we need to find elements $q, r \in \mathbb{Z}[i]$ such that

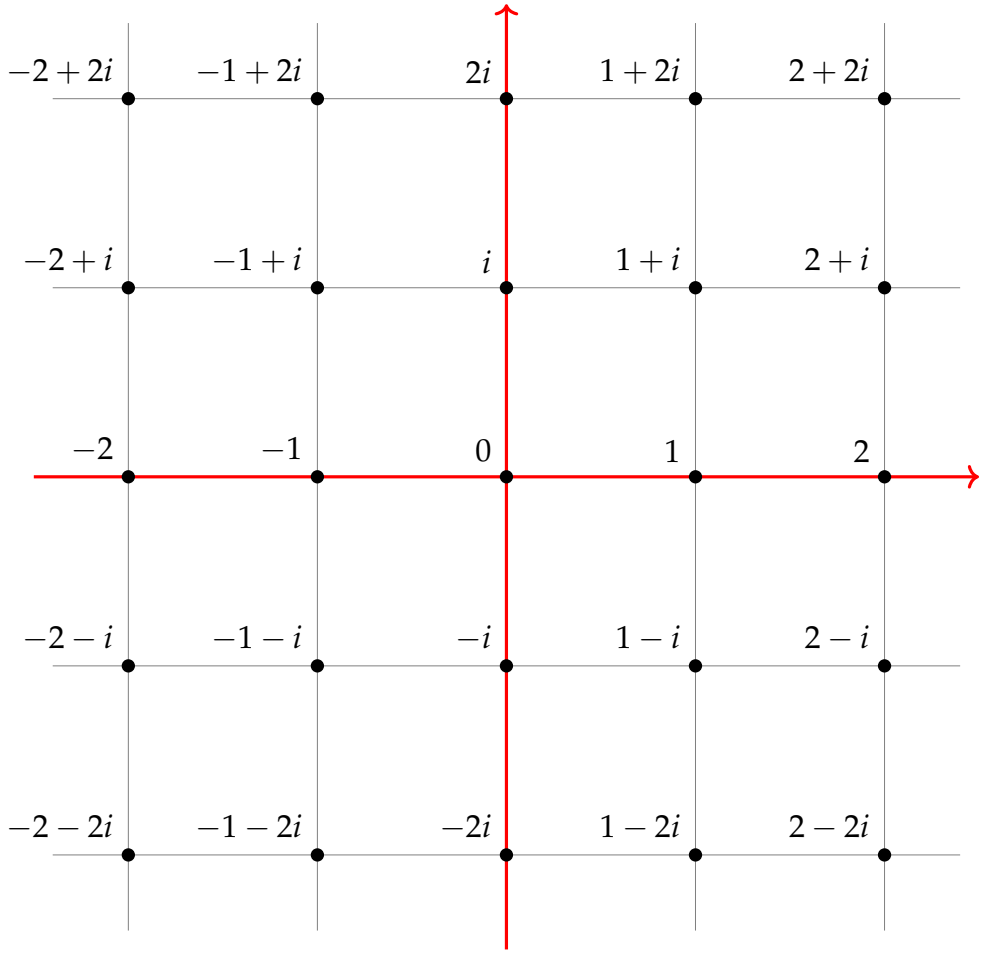
$$\frac{\alpha}{\beta} - q = \frac{r}{\beta} \qquad \text{and} \qquad \left|\frac{r}{\beta}\right| < 1.$$

In other words, we need to find an element $q \in \mathbb{Z}[i]$ such that

$$\left|\frac{\alpha}{\beta} - q\right| < 1$$

(because if we have found such a q, then the corresponding r can be obtained by setting $r = \alpha - q\beta$). This becomes a lot more intuitive if we recall the geometric meaning of Gaussian integers: The Gaussian integers

are the lattice points of a square lattice in the plane:

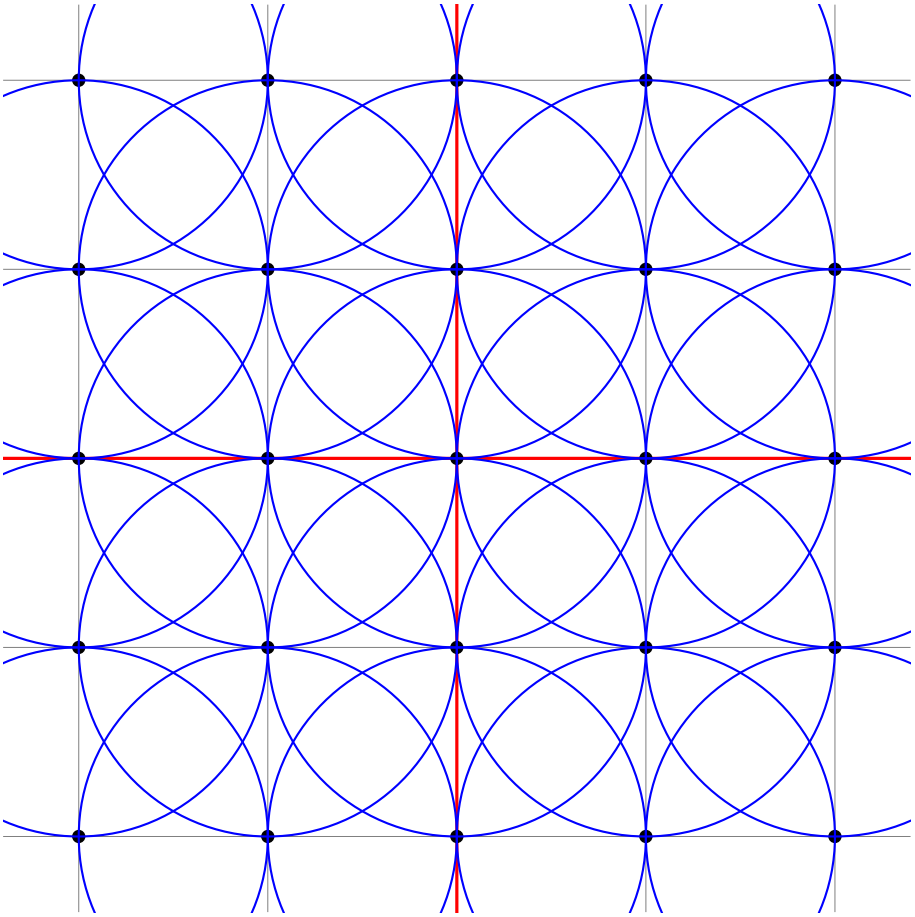


So a Gaussian integer $q \in \mathbb{Z}[i]$ satisfying $\left|\frac{\alpha}{\beta} - q\right| < 1$ simply means a lattice point at a distance less than 1 from the point $\frac{\alpha}{\beta}$.

I claim that such a point exists. Visually, this follows from the fact that if we draw a circle with radius 1 around each lattice point (i.e., each Gaussian integer), then these circles cover the entire plane[4], as shown in the

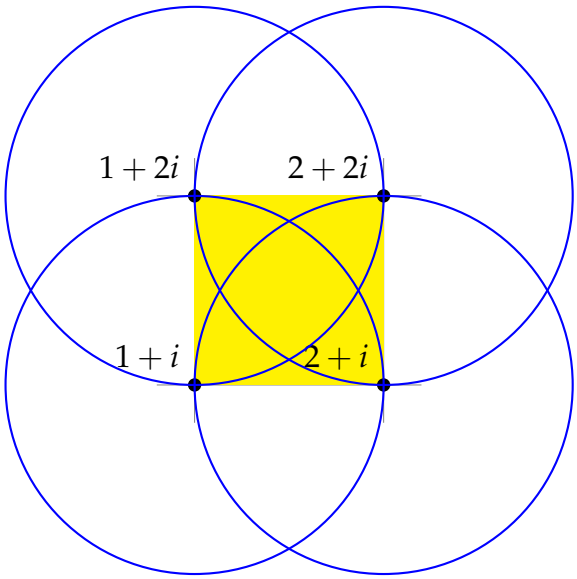
[4] I want the circles to be open (i.e., the boundary of such a circle does not count as part of the circle).

following picture:



.

The easiest way to see this geometrically is to show that the four circles around the vertices of a unit square cover the entire square:



(where we understand the circles to be open, i.e., the circumference of a circle is not included in the circle).

This geometric argument is not hard to translate into algebra: You write the complex number $\frac{\alpha}{\beta}$ as $(u+x)+(v+y)\,i$, where u and v are integers and $x, y \in [0,1]$ (since every real number can be written in the form $u+x$ for some integer u and some $x \in [0,1]$). Then, the required point q will be

- the point $u+vi$ if $x \leq \frac{1}{2}$ and $y \leq \frac{1}{2}$;
- the point $(u+1)+vi$ if $x > \frac{1}{2}$ and $y \leq \frac{1}{2}$;
- the point $u+(v+1)\,i$ if $x \leq \frac{1}{2}$ and $y > \frac{1}{2}$;
- the point $(u+1)+(v+1)\,i$ if $x > \frac{1}{2}$ and $y > \frac{1}{2}$.

In either case, this point q really has a distance less than 1 from the point $\frac{\alpha}{\beta}$ (this is easy to check[5]).

Thus, we have found our q, and consequently the r as well (since $r = \alpha - q\beta$). This completes the proof that the norm N is Euclidean. Hence, $\mathbb{Z}[i]$ is a Euclidean ring, thus a Euclidean domain.

- The ring
$$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a+b\sqrt{-3} \mid a,b \in \mathbb{Z}\right\}$$
(this is another subring of $\mathbb{C}$, since $\sqrt{-3} = \sqrt{3}i$) is **not** Euclidean. This is not obvious, but it can be proved.

- The ring
$$\mathbb{Z}\left[\sqrt{2}\right] = \left\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\right\}$$

[5] In fact,

- the real parts of q and $\frac{\alpha}{\beta}$ differ by at most $\frac{1}{2}$;
- the imaginary parts of q and $\frac{\alpha}{\beta}$ differ by at most $\frac{1}{2}$;

and thus (by the Pythagorean theorem) the distance between q and $\frac{\alpha}{\beta}$ is at most $\sqrt{\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2} = \frac{\sqrt{2}}{2} < 1$.

(a subring of $\mathbb{R}$) is Euclidean. A Euclidean norm for it is the map

$$\begin{aligned} \mathbb{Z}\left[\sqrt{2}\right] &\to \mathbb{N}, \\ a + b\sqrt{2} &\mapsto \left|a^2 - 2b^2\right| \qquad (\text{for } a, b \in \mathbb{Z}). \end{aligned}$$

(This is not obvious, but can be proved.)

- The ring
$$\mathbb{Z}\left[\sqrt{14}\right] = \left\{a + b\sqrt{14} \mid a, b \in \mathbb{Z}\right\}$$
is Euclidean, but the map $a + b\sqrt{14} \to \left|a^2 - 14b^2\right|$ is **not** a Euclidean norm. An actual Euclidean norm for this ring is notoriously hard to construct.
- The ring $\mathbb{Z}\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$ is **not** Euclidean.
- For each $n \in \mathbb{Z}$, the quotient ring $\mathbb{Z}/n$ is Euclidean. More generally, if R is a Euclidean ring, then any quotient ring R/I of R is Euclidean.

We can now generalize Proposition 1.13.1:

Proposition 1.13.3. Let R be a Euclidean ring. Then, any ideal of R is principal.

Proof. The proof of Proposition 1.13.1 can be easily adapted. Most importantly, instead of taking the smallest positive element of I, we take a nonzero element b of I that has the smallest possible $N(b)$ (where N is a Euclidean norm on R). □

Again, this is not a constructive proof. However, there is an analogue of the Euclidean algorithm in any Euclidean ring. Thus, if a and b are two elements of a Euclidean ring R, then you can algorithmically find an element $c \in R$ such that $aR + bR = cR$ (and you can even find elements $x, y \in R$ such that $xa + yb = c$). See §2.13.3 in the text for the algorithm that finds this c (and these x and y). This c is a generalization of the greatest common divisor of two integers. More on that next time.

References

[vanDal05] Birgit van Dalen, *Lenstra's wonderlijke kaartspel: Een generalisatie van de Chinese Reststelling voor niet-commutatieve ringen*, bachelor thesis, 9 May 2005.
`https://www.universiteitleiden.nl/binaries/content/assets/science/mi/scripties/dalenbachelor.pdf`

[vanDal06] Birgit van Dalen, *Card games with ideals*, Nieuw Archief voor Wiskunde **5/7** (2006), pp. 52–56.