MA542 Lecture

Timothy Kohl

Boston University

March 3, 2025

Euclidean Domains

We next wish to consider a class of domains that are in-between Fields and PIDs.

In particular, we are considering rings where a form of the division algorthim holds, as this has strong implications for the ideal structure of the ring.

Definition

An integral domain D is called a Euclidean Domain if there is a function d (called the measure or degree) from D^*, the non-zero elements of D, to the non-negative integers such that:
(1) $d(a) \leq d(ab)$ for all $a, b \in D^*$
(2) if $a, b \in D$ $b \neq 0$ then there exists $q, r \in D$ such that $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

We have two immediate examples.

In $\mathbb{Z}$ let $d(a) = |a|$, and we note that for each non-zero $b \in \mathbb{Z}$ we have $|b| \geq 1$ and so $d(ab) = |ab| = |a||b| \geq |a| = d(a)$ and so (1) holds, and the well ordering principle, applied to the set

$$\{a - kb \mid a - kb \geq 0\}$$

gives us (2).

In $F[x]$ let $d(f(x)) = deg(f(x))$ and note that $deg(f(x)g(x)) = deg(f(x)) + deg(g(x)) \geq deg(f(x))$ and so (1) holds, and (2) is (basically) the well ordering principle again.

So are there other examples besides the two classical ones $\mathbb{Z}$ and $F[x]$?

Yes. For $\mathbb{Z}[i]$, define $d(x+yi) = x^2 + y^2$ and note that $d(x+yi) > 0$ as long as $x + yi \neq 0$.

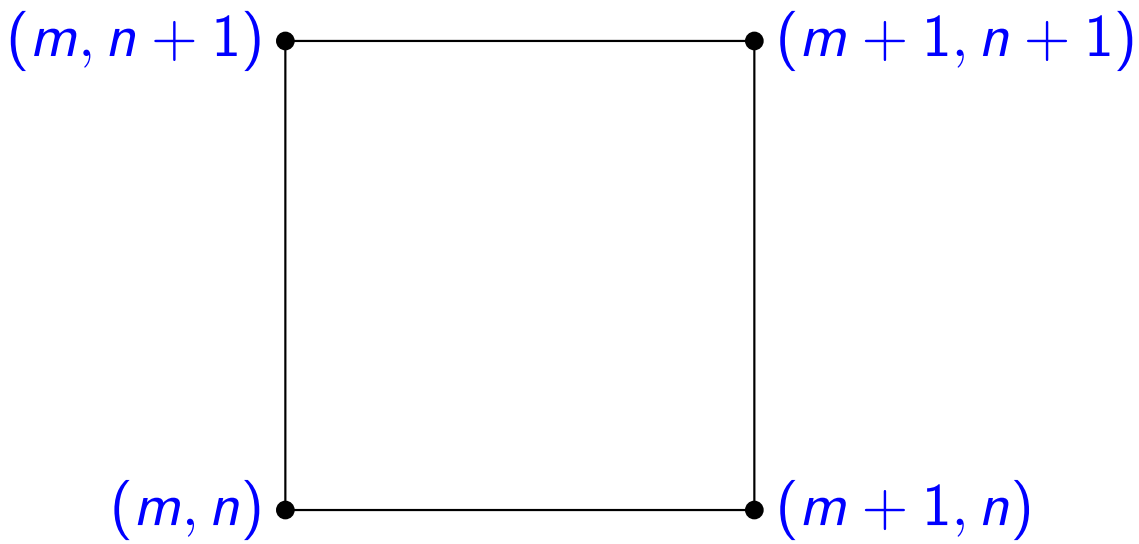
Moreover, it's an easy exercise to show that $d((x_1 + y_1 i)(x_2 + y_2 i)) = d(x_1 + y_1 i)d(x_2 + y_2 i)$ and since $x, y \in \mathbb{Z}$ we have $d(x+yi) \geq 1$ if $x + yi \neq 0$, so $d(ab) = d(a)d(b) \geq d(a)$.

In fact, the value $d(x+yi)$ is related to the 'distance' of the point (x, y) from the origin which is $\|x + yi\| = \sqrt{x^2 + y^2}$, in that $d(x+yi) = \|x + yi\|^2$.

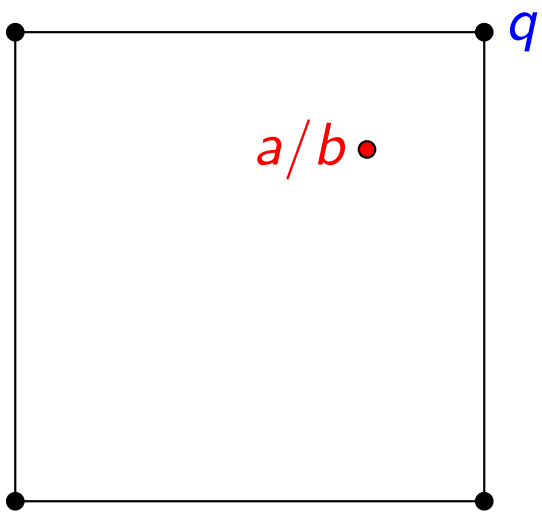
How do we show part (2), namely the existence of a quotient and remainder when dividing one Gaussian integer by another?

First, the Gaussian integers correspond to those points (m, n) in the xy-plane (i.e. complex plane) with integer coordinates.

These divide up the plane into 'cells' of unit width and height.



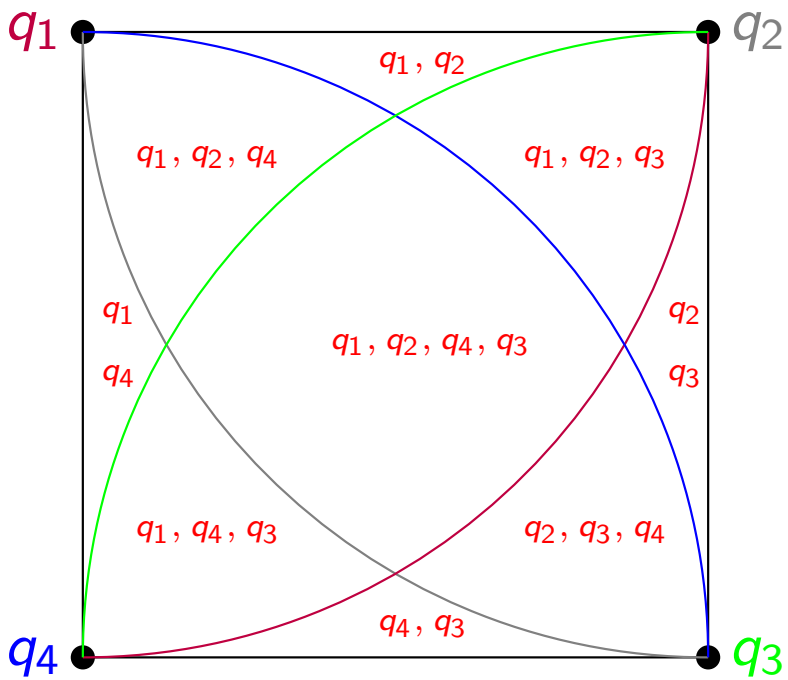
Now, if $a = x_1 + y_1 i$ and $b = x_2 + y_2 i$ then consider a/b which is going to be a complex number with rational components, which will therefore lie in one of these 'cells' and as such, we can pick 'q' to be a 'corner' of the cell *that is closest* to a/b, so in particular the distance from q to a/b is less than one unit away in the plane.



This means that $d(a/b - q) < 1$ which means $d(b(a/b - q)) < d(b)$, that is $d(a - qb) < d(b)$ so if we let $r = a - qb$ then $d(r) < d(b)$ as required.

This leads to an interesting question, is there a unique choice of q? That is, is there only one 'corner' which is less than one unit away from a/b?

No. This can be seen by drawing arcs of unit radius from each corner and realizing that anything within a given arc is one unit away, but that for some q, there are more than one corners that are less than one unit away.

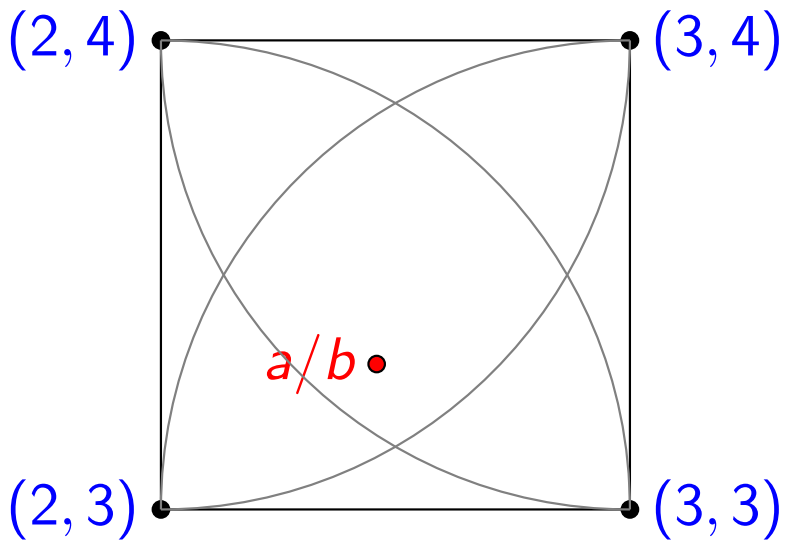


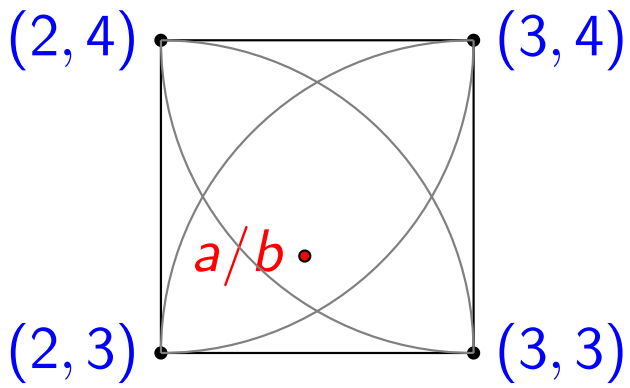
What this implies, is that there may be more than one possible quotient!

This is a bit different than the case of $\mathbb{Z}$ and $F[x]$ where the quotient and remainder are unique, but the uniqueness is actually not so critical when one is proving the ring is a PID.

The only thing which truly matters is that the remainder is 'smaller' than the divisor.

Let's consider an example. Let $a = 14 + 5i$ and $b = 3 - 2i$ which implies that $a/b = \frac{32}{13} + \frac{43}{13}i \approx 2.46 + 3.31i$ which puts a/b in this 'cell' of the $\mathbb{C}$-plane.





So we see that a/b is within 1 one unit of all four possible q and so have four possible quotient/remainder combinations.

For $a = 14 + 5i$ and $b = 3 - 2i$ we have $d(b) = 13$.

- $a = (2 + 4i)b + (0 - 3i)$ where $d(0 - 3i) = 9$
- $a = (3 + 4i)b + (-3 - i)$ where $d(-3 - i) = 10$
- $a = (2 + 3i)b + (2 + 0i)$ where $d(2 + 0i) = 4$
- $a = (3 + 3i)b + (-1 + 2i)$ where $d(-1 + 2i) = 5$

This may seem a bit jarring given what we know about $\mathbb{Z}$ and $F[x]$.

However, if one looks closely at the way the division algorithm for $\mathbb{Z}$ is usually phrased:

If a is an integer, and b is a *positive* integer, then there exists unique integers q and r such that $a = qb + r$ where $0 \leq r \leq b$.

but if we drop the word 'positive' then we have the possibility that r could be negative, which means $a = qb + r$ where $d(r) = |r| < d(b) = |b|$ but uniqueness is no longer true.

Say $a = 7$ and $b = -3$ then $d(b) = |-3| = 3$ and we have

$7 = (-2)(-3) + 1$ $[q = -2,\ r = 1$ so $d(r) = 1$ and $d(r) < d(b)]$

$7 = (-3)(-3) - 2$ $[q = -3,\ r = -2$ so $d(r) = 2$ but still $d(r) < d(b)]$

As it turns out, for $F[x]$ the quotient and remainder *are* unique.

Finally, we come back to unique factorization with the following.

Theorem

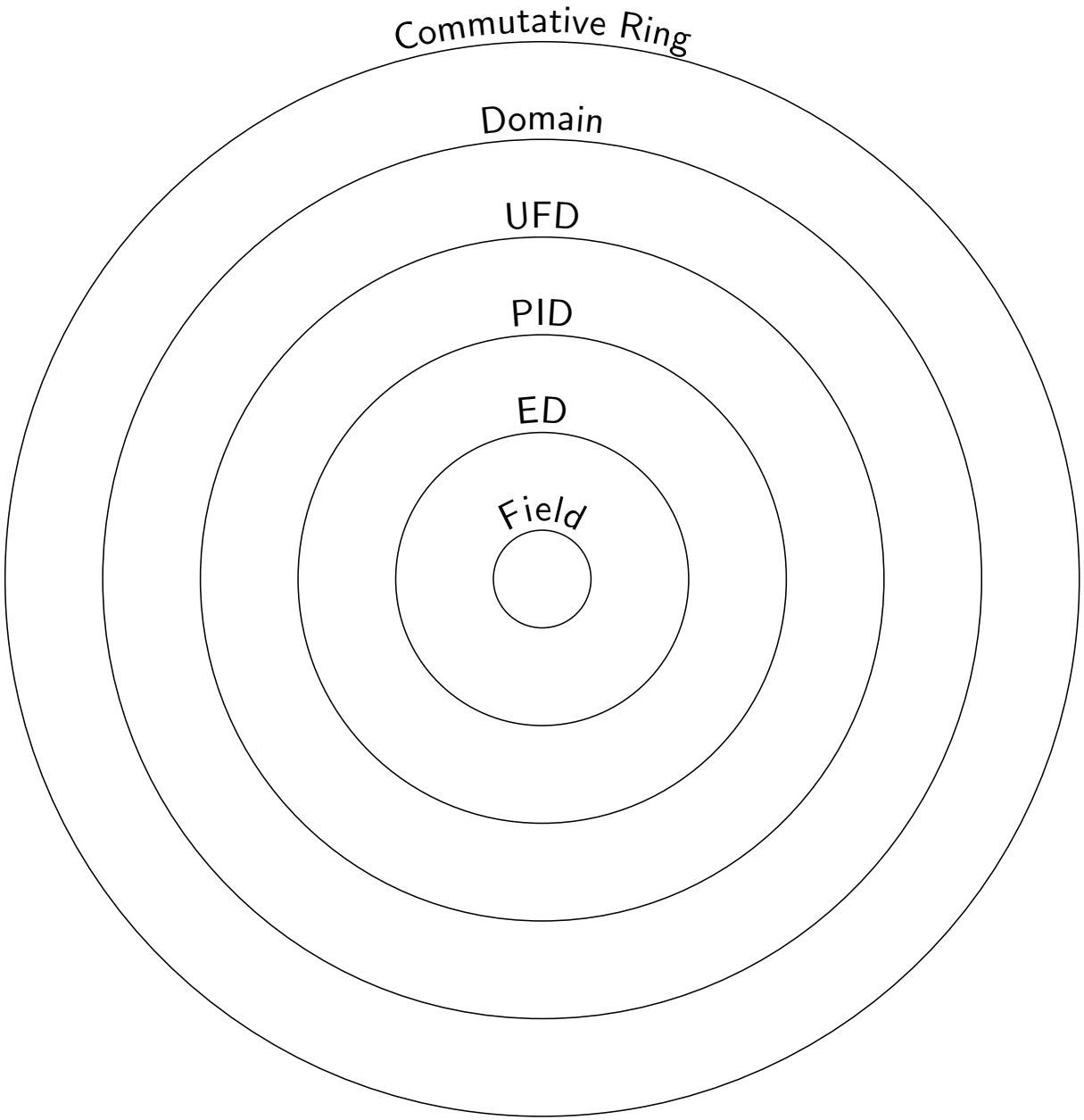
Every Euclidean domain is a PID.

As we've seen with the proof of $F[x]$ being a PID, the division algorithm allows one to prove all ideals in a ED are principal.

Corollary

Every Euclidean domain is Unique Factorization Domain.

Lastly, we can fit Euclidean Domains into the hierarchy of commutative rings.



The very last point to consider is whether PIDs are EDs?

As it turns out, the answer is no.

There is a famous example that was proven to be a PID but not a ED, let

$$\theta = \frac{1 + \sqrt{-19}}{2}$$

then

$$R = \{a + b\theta \mid a, b \in \mathbb{Z}\}$$

is PID but not a ED.

Note by the way that $\mathbb{Z}[\sqrt{-19}]$ is a proper subring of $R = \mathbb{Z}[\theta]$ because $\theta = \frac{1+\sqrt{-19}}{2} \notin \mathbb{Z}[\sqrt{-19}]$.

One proof that $\mathbb{Z}[\theta]$ is a PID but not ED can be found in:

A Principal Ideal Domain That Is Not a Euclidean Domain
Oscar A. Cámpoli
The American Mathematical Monthly
Vol. 95, No. 9 (Nov., 1988), pp. 868-871 (4 pages)

Before we leave this discussion, we can ask, is $\mathbb{Z}[\sqrt{-19}]$ a PID?

The answer is yes, actually, and indeed, what is kind of amazing is that there are only a finite number of these objects which are PIDs.

Specifically, $\mathbb{Z}[\sqrt{-d}]$ is a PID iff

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

and that's it.

These were discovered by Gauss, but the proof that there are no others is due to Stark and Heegner.