MA542 Lecture

Timothy Kohl

Boston University

February 28, 2025

Chains of Ideals

We need to discuss 'chains' of ideals

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq \ldots$$

namely each ideal is contained in the next one after it, although the containments may, or may not be proper.

For such a chain, we can ask if it terminates.

Definition

In a commutative ring R, we say the ascending chain condition (ACC) holds if for any chain of ideals

$$I_1 \subseteq I_2 \subseteq \dots$$

there is an index r such that $I_{r-1} \subseteq I_r = I_{r+1} = I_{r+2} = \dots$, that is the chain 'stabilizes'.

This is crucial for proving certain rings are UFDs.

Lemma

Every PID satisfies the ACC.

Proof.

Let $I_1 \subseteq I_2 \subseteq \dots$ be any chain in the PID we will call D. Consider the set $J = I_1 \cup I_2 \cup \cdots$, namely the union of all the ideal in the chain.We can show that J is an ideal. If $x, y \in J$ then $x \in I_m$ and $y \in I_n$ for some m, n. We can assume that $m \leq n$ which means $x, y \in I_n$ so $x - y \in I_n$ and if $d \in D$ then any $x \in J$ is in some I_m so $dx \in I_m$ so $dx \in J$ since J is the union of all the I's.
Since J is an ideal, then $J = \langle z \rangle$ for some $z \in D$, but this means $z \in I_r$ for some r so $\langle z \rangle \subseteq I_r \subseteq J = \langle z \rangle$, but this means $I_r = \langle z \rangle$ and that $I_t = \langle z \rangle$ for any $t \geq r$ as well. □

What this means is that in a PID D, a chain of ideals, where each containment can only have a finite number of ideals.

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq I_r$$

and therefore any ideal that properly contains I_r must actually be D.

What this means is that $I_r = \langle p \rangle$ and if p is *not* irreducible then $p = xy$ where x and y are non-units and so $I_r = \langle p \rangle \subsetneq \langle x \rangle$ which would imply that $\langle x \rangle = D$ meaning that x is actually a unit, which is a contradiction.

The bottom line is that p must actually be irreducible.

Now, we can prove one of the main results about unique factorization.

Theorem

If D is a PID then it is a UFD.

PROOF: The proof is in three parts,

(1) show that every non-zero non-unit is divisible by at least one irreducible

(2) deduce that every non-zero non-unit is a product of irreducibles

(3) this factorization is unique up to order and associates.

So we begin by proving that a non-zero, non-unit has an irreducible factor.

Let $a \in D$ be a non-zero non-unit, we wish to first show that a is divisible by at least one irreducible.

If a is irreducible, then we're done, otherwise $a = x_1 y_1$ where x_1,y are non-zero, non-units so

$$\langle a \rangle \subsetneq \langle x_1 \rangle$$

and if x_1 is not irreducible, it's a product $x_2 y_2$ where x_2 and y_2 are non-zero, non-units and so

$$\langle a \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_2 \rangle$$

and we continue checking to see if x_i is irreducible, and if not, it has a factor x_{i+1} which leads to in (increasing) chain of principal ideals $I_i = \langle x_i \rangle$

$$\langle a \rangle \subsetneq I_1 \subsetneq I_2 \cdots \subsetneq I_i \subsetneq I_{i+1} \ldots$$

PROOF (continued)
But now, because D is a PID, this chain must terminate

$$\langle a \rangle \subsetneq I_1 \subsetneq I_2 \cdots \subsetneq I_i \subsetneq I_{i+1} \cdots \subsetneq I_r$$

where $I_r = \langle p \rangle$ so any larger ideal containing I_r would have to be all of D. This means that p must be irreducible, otherwise it would have a factor giving us a *larger* ideal containing I_r which we saw earlier is impossible.

So now, we have that a has an irreducible factor p_1, and if a is not already irreducible, then $a = p_1 b$ where b is a non-zero, non-unit, so either b is irreducible, or b has an irreducible factor p_2 in which case, either $a = p_1 p_2 c$ for some non-zero, non-unit c which in turn...

So every non-zero, non-unit $a \in D$ is a product of irreducibles $a = p_1 p_2 \cdots p_n$.

So what if $a = q_1 q_2 \cdots q_m$ is another such factorization?

Well since p_1 is a factor of a that means $p \mid q_1 q_2 \cdots q_m$ but in a PID irreducibles are prime so p_1 divides one of the q_j, so assume that $p_1 \mid q_1$, so that $q_1 = u_1 p_1$.

So this means $p_1 p_2 \cdots p_n = u_1 p_1 q_2 \cdots q_m$ and since D is a domain we can cancel p_1 from both sides to get $p_2 p_3 \cdots p_n = (u_1 q_2) q_3 \cdots q_m$ and we can continue to divide both sides by p_2, p_3 and so on, and so $n \leq m$ but if $n < m$ then we get

$$1 = (u_1 u_2 \ldots u_n) q_{n+1} \cdots q_m$$

which is impossible since the left side is the unit 1, and the right has irreducible factors (i.e. isn't a unit.)

So we must have $n = m$ and so $a = p_1 \cdots p_m$ where if $a = q_1 q_2 \ldots q_m$ is another factorization then we may assume that each $q_i = u_i p_i$ for u_i a prime.

Moreover,

$$\begin{aligned} p_1 \cdots p_m &= q_1 q_2 \ldots q_m \\ &= (u_1 p_1)(u_2 p_2) \ldots (u_m p_m) \\ &\downarrow \\ 1 &= u_1 u_2 \cdots u_m \end{aligned}$$

More on UFDs

We just proved that every PID is a UFD.

Corollary

For every field F, the ring $F[x]$ is a UFD.

Of course, we outlined a proof of this a few lectures earlier, but the full statement follows easily from knowing that $F[x]$ is a PID.

So, for example, $\mathbb{Q}[x]$ is a UFD, and it begs the question, is $\mathbb{Z}[x]$ a UFD?

We saw that $\mathbb{Z}[x]$ is *not* a PID so we can't use the $PID \rightarrow UFD$ argument.

The proof that $\mathbb{Z}[x]$ is a UFD follows from a much more general and powerful fact.

Theorem

If R is a UFD, then $R[x]$ is a UFD.

The proof is basically built on some of the ideas we used in proving that a polynomial in $\mathbb{Z}[x]$ being factorable in $\mathbb{Q}[x]$ implies that it's actually factorable in $\mathbb{Z}[x]$. (e.g. Gauss' Lemma)

The full argument is developed in the text.

We mentioned earlier that the Gaussian integers $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ are a PID and therefore a UFD.

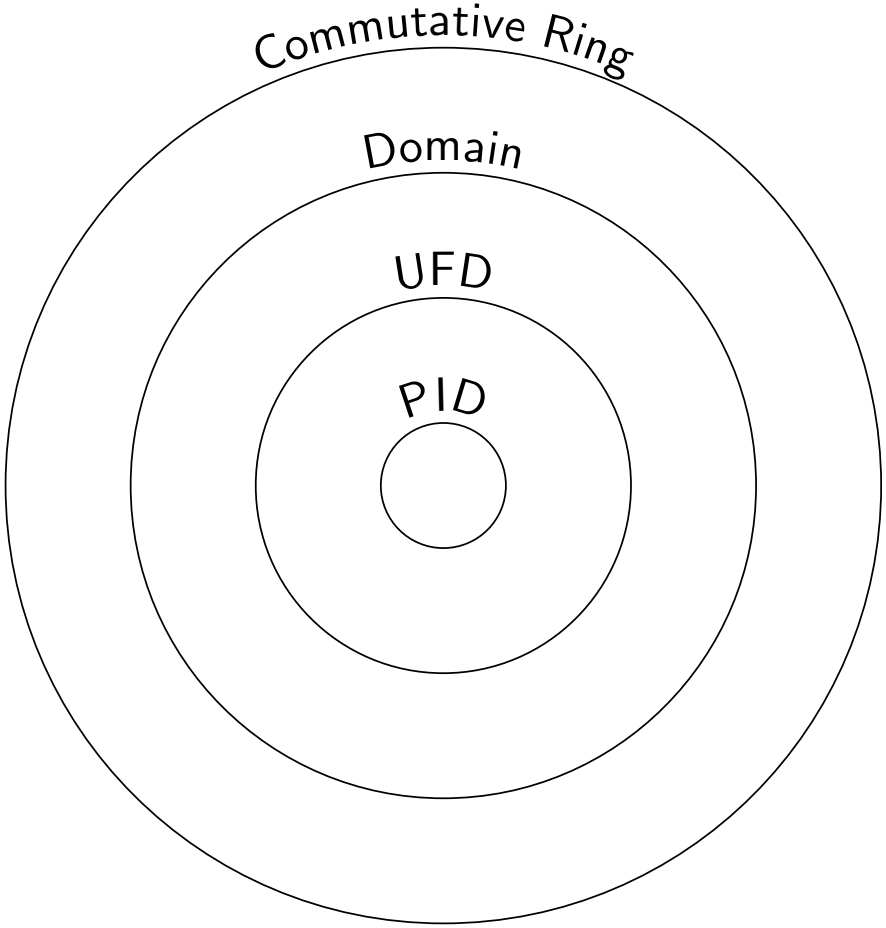
We also saw that in $\mathbb{Z}[\sqrt{-3}]$ one has an irreducible element, which is not a prime, specifically $1 + \sqrt{-3}$, and what's interesting is that the demonstration of this was by using the fact that

$$4 = (1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$$

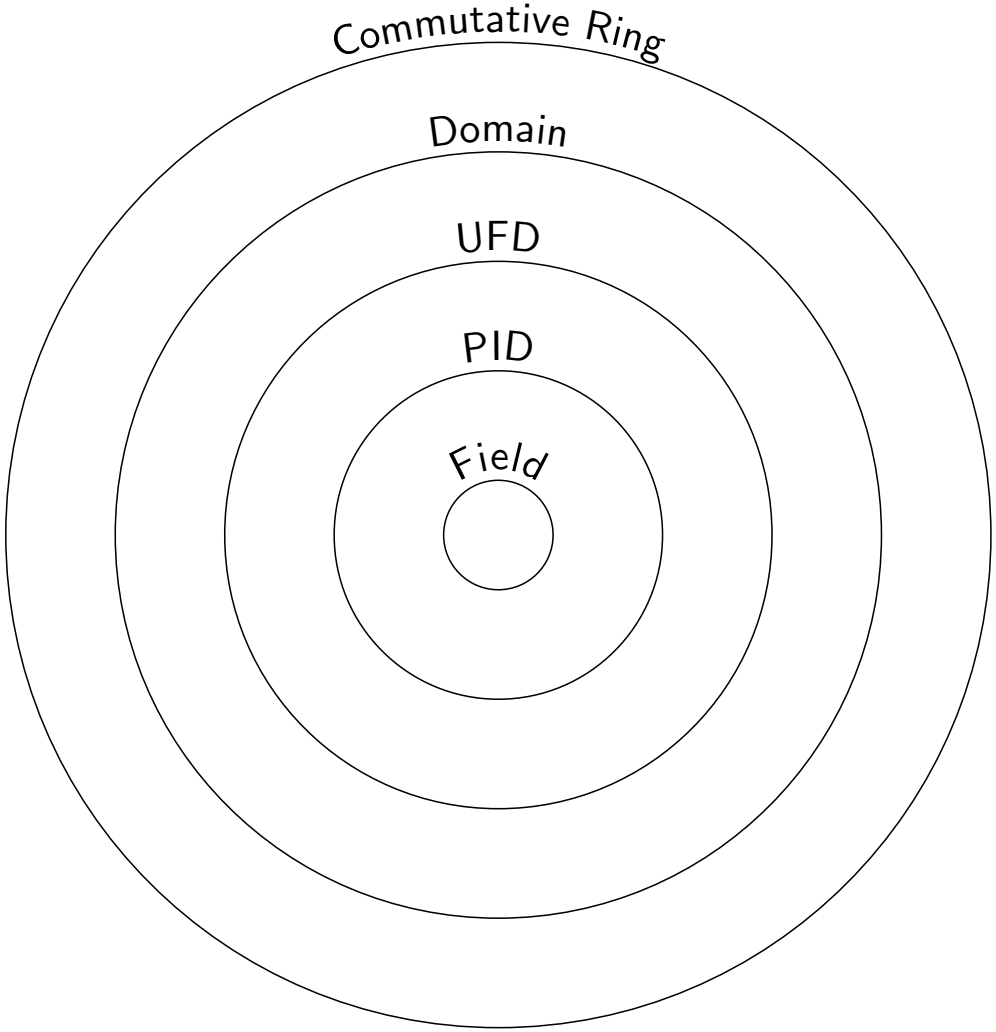
where we also observe that 2 is an irreducible.

This also shows that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD since we have two distinct factorizations of 4 into irreducibles where $(1 \pm \sqrt{-3}) \nmid 2$. (i.e. they are not associates of each other)

So we have the following basic containments of ring categories.



Actually we could also fit in one more category, namely fields, but where would fields go in this picture?



Why? Well, there are two questions, what are the ideals of a field, and what are the irreducibles?

Well, since every non-zero element of a field F is a unit, then any ideal, except $\{0\}$ contains at least one unit, and is therefore all of F!

And since every non-zero element of F is a unit, then there *are no* irreducibles.

We have seen that in rings like $\mathbb{Z}$ and $F[x]$ (for F a field) there is a division algorithm, which allowed us to deduce that these rings are PIDs and therefore UFDs.

This prompts one to ask if there are other rings where some version of a division algorithm holds?

It turns out that this is indeed the case, and the key is a function which one my apply to all elements of the ring, (e.g. the degree function in $F[x]$) and the value of this function when applied to the 'remainder' that distinguishes it from the divisor.