MA542 Lecture

Timothy Kohl

Boston University

February 26, 2025

We have the following.

Theorem

In a PID, every irreducible element is prime.

Proof.

Let $a \in D$ (a PID) be irreducible and suppose $a \mid bc$ for $b, c \in D$. We wish to show that either $a \mid b$ or $a \mid c$.

Let $I = \{ax + by \mid x, y \in D\}$ which is an ideal of D, and so $I = \langle d \rangle$ for some $d \in D$.

Since $a \in I$ then $a = dr$ for some $r \in D$ but then either d or r is a unit since a is irreducible.

If d is a unit then $I = D$ and so $1 = ax + by$ for some x, y so $c = acx + bcy$ and since $a \mid bc$ and $a \mid ac$ then $a \mid c$.

If r is a unit then $\langle a \rangle = \langle d \rangle = I$ and since $b \in I$ then there is a $t \in D$ such that $at = b$ i.e. $a \mid b$. □

Corollary

If D is a PID, then $p \in D$ is a prime if and only if it is irreducible.

For example, in $\mathbb{Z}$ primes and irreducibles are indeed the same thing.

We also deduce this.

Corollary

If there exists an irreducible $a \in D$ (a domain) that is not prime, then D is not a PID.

So for example, $\mathbb{Z}[\sqrt{-3}]$ is not a PID, since $1 + \sqrt{-3}$ is irreducible, but not prime.

Indeed, it is precisely those $\mathbb{Z}[\sqrt{d}]$ which are PIDs for which prime and irreducible are the same.

For example, the Gaussian integers $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ is a PID.

We saw that $F[x]$ is PID, for example, $\mathbb{Q}[x]$, so it begs the question of whether $\mathbb{Z}[x]$ is a PID?

The answer is no, which can be demonstrated by the following counterexample

$$I = \{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even}\}$$

is an ideal of $\mathbb{Z}[x]$ which is *not* principal.

Why? Well if $I = \langle h(x) \rangle$ then since $2 \in I$ we would have to have $h(x) \mid 2$ which would mean that $h(x)$ is constant polynomial.

But if $h(x)$ is a constant polynomial then we would have to have $h(x) = 2$, but then $f(x) = x + 2$ is in I but *not* in $\langle 2 \rangle$ since $2 \nmid x + 2$.
Remember, the coefficients are *integers*.

We note one last thing, even though $\mathbb{Z}[x]$ is not a PID, it turns out that irreducibles are primes in this ring.

Unique Factorization

Definition

An integral domain D is a unique factorization domain (UFD) if
(1) every non-zero, non-unit of D can be written as a product of irreducibles in D
(2) this factorization is unique, up to the order of the irreducibles, and to associates.

So for $a \in D$ is a non-zero, non-unit, and $a = p_1 p_2 \cdots p_r$ and $a = q_1 q_2 \cdots q_s$ where the p_i and q_j are irreducibles, then $r = s$ and without loss of generality $q_i = u_i p_i$ where $u_i \in U(D)$.

We explored this earlier for the most fundamental example $\mathbb{Z}$.

Now in $\mathbb{Z}$ the only units are ± 1 so a given irreducible p, has only two associates p and $-p$.

So for example, 12 can be written in a few different (but equivalent) ways

$$\begin{aligned} 12 &= 2 \cdot 2 \cdot 3 \\ &= 2 \cdot (-2) \cdot (-3) \\ &= (-2) \cdot (-2) \cdot 3 \\ &= (-2) \cdot 2 \cdot (-3) \end{aligned}$$

The point is that if $a = p_1p_2\cdots p_r = (u_1p_1)(u_2p_2)\cdots(u_rp_r)$ then

$$\begin{aligned} p_1p_2\cdots p_r &= (u_1p_1)(u_2p_2)\cdots(u_rp_r) \\ &= (u_1u_2\cdots u_r)(p_1p_2\cdots p_r) \\ &= 1(p_1p_2\cdots p_r) \end{aligned}$$

namely $u_1u_2\cdots u_r = 1$.

The fundamental example of a UFD is the integers $\mathbb{Z}$ of course and the fact that $\mathbb{Z}$ *is* a UFD is a theorem called the Fundamental Theorem of Arithmetic where the irreducibles are prime numbers.

Moreover, if we ignore the associates p and $-p$ then every natural number is uniquely expressible as a product of primes.

So how would one actually prove that a given domain is a UFD?

As it turns out the answer to this, in part, depends on the ideals in the domain, in particular principal ideals.

Lemma

If D is a domain then for any unit $u \in U(D)$ we have $\langle u\rangle = D$.

We've seen something similar to this earlier, but we include this here as it is germane to the discussion of factoring.

Proof.

If $u \in U(D)$ then for $I = \langle u\rangle$ we have that $ru \in I$ for any $r \in D$, so in particular for $r = u^{-1}$ so that $1 \in I$, and so $d \cdot 1 = d \in I$ for all $d \in D$ so $D \subseteq I$ so $D = I$.

For the converse, if $D = \langle u\rangle$ then $1 = du$ for some $d \in D$ but this means that $d \in U(D)$ and that $u = d^{-1}$ which means $u \in U(D)$ too of course. □

Lemma

If D is a domain then $a = ub$ for $u \in U(D)$ iff $\langle a \rangle = \langle b \rangle$.

Proof.

If $a = ub$ and $x \in \langle a \rangle$ then $x = ac = ubc = b(uc) \in \langle b \rangle$ so $\langle a \rangle \subseteq \langle b \rangle$.
If $y \in \langle b \rangle$ then $y = bc$ but $a = ub$ implies $b = u^{-1}a$ so $y = u^{-1}ac = a(u^{-1}c)$ which means $y \in \langle a \rangle$, i.e. $\langle b \rangle \subseteq \langle a \rangle$ and thus $\langle a \rangle = \langle b \rangle$.
For the converse, if $\langle a \rangle = \langle b \rangle$ then $a \in \langle b \rangle$ so $a = bc$, and since $b \in \langle a \rangle$ then $b = ad$ so $a = adc$ and since D is a domain, we can cancel a from both sides to yield $1 = dc$ so that d, c are units. □

Now, for a 'proper' factorization, namely $a = bc$ where b and c are non-units of D, we have the following relationship between principal ideals.

Lemma

If D is a domain then $a = cb$ where b, c are not units iff $\langle a \rangle \subsetneq \langle b \rangle$

Proof.

Since $a = cb$ then any multiple of a is a multiple of b which means $x \in \langle a \rangle$ implies $x \in \langle b \rangle$ so $\langle a \rangle \subseteq \langle b \rangle$.

This inclusion is proper only if c is a non-unit by the previous lemma. □

Factorization centers around a basic question,what is the difference between reducible and irreducible?

Well, recall that a non-zero, non-unit is irreducible if it *cannot* be written as a product of other non-units.

And if it is reducible (factorable) then it can written as a product of at least two other non-units.

So start with a non-zero, non-unit $a \in D$ where D is a domain.

If a is irreducible then we're done.

Otherwise $a = x_1 y$ where x_1 and y are other non-units.

If x_1 and y are irreducible then we're done.

Otherwise we have that, for example, x_1 is reducible so we can write $x_1 = x_{11}x_{12}$ for non-units x_{11} and x_{12}.

Thus $a = x_{11}x_{12}y$ and if x_{11} is not irreducible we can write it as $x_{111}x_{112}$ for non-units x_{111} and x_{112}.

And so we have:

$$\begin{aligned} a &= x_1 y \\ &= x_{11}x_{12}y \\ &= x_{111}x_{112}x_{12}y \end{aligned}$$

and so we can keep 'drilling down' and see if x_{111} is irreducible or not, and if not, factor *it* as say $x_{1111}x_{1112}$ etc.

This can be viewed in the setting of ideals.

If $a = x_1 y$ where x_1,y are non-units, then we saw earlier that this implies $\langle a \rangle \subsetneq \langle x_1 \rangle$.

And if $x_1 = x_{11}x_{12}$ (where x_{11} and x_{12} are non-units) then $\langle x_1 \rangle \subsetneq \langle x_{11} \rangle$.

And if $x_{11} = x_{111}x_{112}$ (for non-units x_{111} and x_{112}) then $\langle x_{11} \rangle \subsetneq \langle x_{111} \rangle$.

Continuing this way, we have a chain of ideals:

$$\langle a \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_{11} \rangle \subsetneq \langle x_{111} \rangle$$

corresponding to each factorization

$$a = x_1 y = x_{11} x_{12} y = x_{111} x_{112} x_{12} y$$

and each time we factor one of the non-units into a product of two non-units, we add another ideal to this chain.

The question is, does this process stop after a finite number of steps?