Seminar Computer Assisted Mathematics
Project: PID

Veliyan Taslev, Philipp Sivov

July 2025

We wanted to look at this handout as a part of the project, not just the presentation, that's why we decided to make it such that anyone reading has all the information needed to understand it in the handout itself.

Our main goal is to show that $R[X]$ is a PID iff R is a field. To do this we need the following definitions:

1 Defintions

Informally a (unitary) ring is just any bunch of elements that we can add, subtract and multiply, that has a 0 and a 1. The formal definition is the following:

A **Ring** R is a tuple $R = (R, 0, 1, +, \times)$, where R is a set, $0, 1 \in R$ and

$$*, + : R \times R \to R$$

are the multiplication and addition operations, such that the following hold for all $a, b, c \in R$:

1. $a + 0 = 0 + a = a$
2. $(a + b) + c = a + (b + c)$
3. $\forall a \in R\ \exists b \in R : a + b = 0$ (we usually write $-a$ for this specific b, as one can show it is unique)
4. $a + b = b + a$
5. $1 * a = a * 1 = a$
6. $a * (b * c) = (a * b) * c$
7. $(a + b) * c = a * b + a * c$
8. $c * (a + b) = c * a + c * b$

We call the ring **commutative** if $a * b = b * a$. We call a ring a **domain** if it is commutative, has more then one element and for all $a, b \in R$ we have $ab = 0 \iff a = 0$ or $b = 0$.

We call a commutative ring a **field** if for all nonzero $a \in R$ there exists some $b \in R$ such that $a * b = 1$. We can show that this b is unique and we denote it by a^{-1} or $\frac{1}{a}$. Such an a is called a **unit**.

An element $c \in R$ is called **irreducible** if it is not a unit and for all $a, b \in R$ such that $a * b = c$ either a or b is a unit (If you've never seen this defintion you can think of irreducible elements as the "prime numbers" in our ring).

An **Ideal** $I \subset R$ is a subset of R such that for all $a, b \in I$ and $r \in R$ we have $a + b \in I$ and $ra \in I$.

An ideal is called **maximal** if the only other ideal that properly contains it is R itself. Note: we don't count R itself as a maximal ideal.

The most common ideals we look at are the ones generated by some elements, so for any $a \in R$ we define the ideals $(a) := \{ra \mid r \in R\}$ and $(a_1, a_2, ..., a_n) := \{r_1a_1 + r_2a_2... + r_na_n \mid r_1, ..., r_n \in R\}$. An ideal is called **principal** if it's of the form (a). A domain R is called a **principal ideal domain** (PID for short) if all its ideals are principal. We like PID's because they behave very well. PID's are your friend.

We can generalize the idea of counting modulo something for all rings: For a Ring R and an ideal I we can define the **quotient ring** R/I, which has elements $\overline{r} := \{r + i \mid i \in I\}$. The addition and multiplication are defined as $\overline{r} + \overline{s} := \overline{r + s}$ and $\overline{r} * \overline{s} := \overline{r * s}$. We can for example see that that looking at the numbers modulo 3 is the same as looking at the elements of $\mathbb{Z}/(3)$.

2 Propositions we're going to use

Proposition 1
Let $I \subset R$ be an Ideal. If $1 \in I$ then $I = R$

Proof: We have $1 \in I$ therefore for each $r \in R$ we get $r = 1 * r \in I$ □

Proposition 2
X is irreducible in $R[X]$

Proof: Let $f, g \in R[X] - \{0\}$ such that $X = fg$. We have $1 = deg(X) = deg(fg) = deg(f) + deg(g)$, therefore WLOG $deg(f) = 0$. Therefore we can think of f as an element in R. If a polynomial of degree 0 divides another, then it must divide all of its coefficents (in R), therefore we have f divides 1, therefore f must be a unit □

Propoistion 3
In PID's irreducible elements generate maximal ideals.

Proof: Let $a \in R$ irreducible, where R is a PID. If (a) is not maximal, then there must exist some other nontivial ideal (b) such that $(a) \subsetneq (b)$. It follows that b divides a, but that would be a contradiction since b is not a unit (since $(b) \neq R$) and from a irreducible it would follow that $a \simeq b$, which would contradict $(b) \neq (a)$. □

Proposition 4
Let $I \subset R$ be a maximal ideal. Then ${}^{R}/_{I}$ is a field.

Proof: We know a domain is a field whenever the only ideals are (0) and (1) (Prop 7). According to the correspondence theorem we know that each ideal $\overline{J}$ in ${}^{R}/_{I}$ corresponds to a uniqe ideal J such that $I \subset J \subset R$. Since I is maximal there are only two possible ideals that contain I (namely R and I itself), therefore there are at most two ideals in ${}^{R}/_{I}$ and since in domains (0) and (1) are always different (R domain) ideals, it follows that ${}^{R}/_{I}$ must be a field □

Proposition 5
For all R we have ${}^{R[X]}/_{(X)} \simeq R$

Proof: Observe the morphism $ev_0 : R[X] \to R,\ p(X) \mapsto p(0)$. It is obviously surjective, so we just need to show its kernel is (X) and then we're done by the homoomorphism theorem. We can write every polynomial $p \in R[X]$ as $p = Xf + a$ for some unique $f \in R[X]$ and $a \in R$. We then get $ev_0(p) = ev_0(Xf) + ev_0(a) = a$. Therefore $p \in ker(ev_0) \iff a = 0 \iff p \in (X)$. □

Proposition 6
A domain R is a field $\iff$ there are only two ideals in R (namely (0) and R).

Proof: Note that since R is a domain $1 \neq 0$, therefore (0) and (1) are always different ideals.

If R is a field, than for each nonzero ideal $(0) \subsetneq I \subset R$, we have some $a \in I - \{0\}$. But since R is a field we know a^{-1} exists and we get $1 = a * a^{-1} \in I$.

Conversely, if the only nonzero ideal is (1), then for each nonzero $a \in R$ we have $(a) = (1)$, therefore $1 \in (a)$, therefore there must exist some b such that $1 = ab$. □

3 Our statements

The first thing we want to show is that $\mathbb{Z}$ is a PID.

Theorem 1
$\mathbb{Z}$ is a PID.

Proof: Let $I \subset \mathbb{Z}$ and let $a \in I$ be the smallest nonegative integer in I. We're going to show that $I = (a)$. The $(a) \subset I$ part is obvious, since $a \in I$. Suppose there existed some $b \in I - (a)$, this would mean that b is not divisible by b. Therefore the (nonnegative) $g := gcd(a, b)$ must be strictly smaller than a. But by the Bezout lemma g can be represented as $g = ra + sb$ for some $r, s \in \mathbb{Z}$. However this would imply that $g \in I$, but since $g < a$ this contradicts the minimality of a. □

Our next theorem is that a field will always be a PID. We've given two different proofs in lean, here's the mathematical version:

Theorem 2
If R is a field then R is a PID.

Proof: According to Prop 6 there are only two ideals in R: (0) and (1) and they're both principal.

□

Now we let's move on to the main theorem:

Theorem 3
If R is not a field then $R[X]$ is not a PID.

Proof: We'll show the negation, namely that if $R[X]$ is a PID then R is a field. We know that $X \in R[X]$ is irreducible by Prop 2, therefore the ideal (X) is a maximal ideal in $R[X]$ by prop 3. It follows that the ring $R[X]/(X)$ is a field by Prop 4. Since by Prop 5 we have $R[X]/(X) \simeq R$ it follows that R must also be a field. □

We obtain the following results:

Example 1:
$\mathbb{Z}[X]$ is not a PID. This follows directely from Theroem 2, since $\mathbb{Z}$ is not a field.

Example 2:
$R[X, Y]$ is not a PID. This follows directely from Theroem 2 since $R[X]$ is not a field for any domain R and $R[X, Y] \simeq (R[X])[Y]$.

Let's give a specific example of a non-principal Ideal in $\mathbb{Z}$:

Example 3: $(2, X) \subset \mathbb{Z}[X]$ is not a principal ideal.

Proof: Supose $(2, X) = (f)$ for some $f \in \mathbb{Z}[X]$. Because of the equality of the two ideals we must have that f divides X and since X is irreducible we get that f is either a unit itself or $fu = X$ for some unit u.

If f is a unit, then we can easily follow that $1 \in (f) = (2, X)$. Therefore we can write 1 as $1 = 2a + bX$ for some $a, b \in \mathbb{Z}[X]$. However this cannot be true since plugging in 0 on both sides of the equation gives us $1 = 2a(0) + b(0) * 0 = 2a(0)$, but this would mean that 2 divides 1 in the integers which is false.

If $fu = X$ where u is a unit, we get $f = Xu^{-1}$. But since $(2, X) = (f)$ we know that f divides 2, more precisely $2 = fa = Xu^{-1}a$ for some $a \in \mathbb{Z}[X]$. However this cannot be true, since plugging in 0 in the equation gives us $0 = 2$, which is obviously false. $\square$