4.3.2024

42

Up to now we've seen that
if F is a field then
$F[x]$ is a ED, hence a PID (Thm 12.8).
Holbeisen

In fact the converse is also true.

$\boxed{\text{Thm 1.11 Let } R \text{ be a comm ring s.t } R[x] \text{ is a PID. Then } R \text{ is a field.}}$

Proof. $R[x]$ is a PID. R is a subring of $R[x]$ which is an I.D. Hence R is an I.D. The map
$$\varphi : R[x] \to R$$
$$f(x) \to f(0)$$
is a surjective hom with kernel (x)

Hence $R[x]/(x) \cong R$ is an I.D
which implies
(x) is a prime ideal
Since $R[x]$ is a PID, (x) is also maximal. Hence $R[x]/(x) \cong R$ is a field.

Rmk: Note if $R[x]$ is a ED (since it is also PID) then R is field

We have also seen that any PID is a UFD. Hence

Thm 1.12 If F is a field then $F[X]$ is a UFD

But it is not the case that

$$R[X] \text{ is a UFD} \not\Rightarrow R \text{ a field}$$

$\mathbb{Z}[X]$ is a UFD but $\mathbb{Z}$ is not a field. But,

Lemma 1.13. $R[X]$ is a UFD $\Rightarrow$ R is a UFD

Proof Since $R[X]$ a UFD imply in particular that the constant polynomials have to be factored uniquely.

If $r \in R \subset R[X]$ has a factorization in $R[X]$ because of degree considerations ($\deg fg = \deg f + \deg g$) the factorization of r in $R[X]$ is a factorization of r in R.

The converse statement of lemma 1.13 that R a UFD $\Rightarrow$ $R[X]$ a UFD is also true and uses the following idea: Since R is a ID we can form its field of fractions F. Then $F[X]$ is a UFD. Now we want to recover a factorization for $f \in R[X]$ from its factorization in $F[X]$.

For this we need to compare irreducibles in $F[x]$ to those of $R[x]$.

(This intuitive idea goes back to Gauss)

First we need some definitions.

Defn ① Let R be a UFD, $a_1, \ldots a_n \in R$ non-zero elements of R. An element $d \in R$ is a greatest common divisor of all a_i, $i = 1 \ldots n$ if

① $d | a_i \quad \forall i = 1, \ldots n$

② if $\tilde{d} \in R$ divides all a_i then it also divides d.

② Let R be a UFD. A nonconstant polynomial $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Then $c = \gcd(a_0, \ldots, a_n)$ is called the content of f

If the content of f is 1 then f is called primitive.

Rmk. In a ring we defined irreducible elements as non-zero, non-units which cannot be represented as a product of nonunits.

For an ID R, we call irreducible elements of $R[x]$ irreducible polynomials

If F is a field, since $(F[X])^\times = F^\times$
in this case an irreducible element
of $F[X]$ has degree ≥ 1 (constants are units)
and cannot be factored into polynomials
of lower degree.
A poly which is not irreducible is called
reducible.

- reducibility $f(x) \in R[X]$ depends
on R

x^2+1 is irred in $\mathbb{R}[X]$ but
reducible in $\mathbb{C}[X]$, $x^2+1 = (x+i)(x-i)$

Now if R is not a field but a UFD
eg $R = \mathbb{Z}$. Then the polynomial
$f = 2X + 4 = 2(X+2)$ is <u>not</u> irreducible
in $\mathbb{Z}[X]$.

In this case it is convinent to
factor $f = \underbrace{(\text{content}(f))}_{2}\, g$ where $g(x) = x+2$
is a primitive polynomial.

Note that every non-constant irreducible
polynomial in $\mathbb{Z}[x]$ must be primitive

Note $2x+4 = 2(x+2) \in \mathbb{R}[x]$ is irreducible
since 2 is a unit in this case.

The next lemma shows that for a UFD R we can always write a poly $f(x) \in R[x]$ the product of its content and a primitive polynomial.

Lemma 1.14. If R is a UFD, then every non-constant polynomial $f(x) \in R[X]$ can be written as $f(x) = c\,g(x)$ where $g(x) \in R[X]$ is primitive and c is unique up to a unit in R and is the content of f. g is also unique up to a unit factor; and $\deg g = \deg f$.

Proof. Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$

Let $c := \gcd(a_0 \dots a_n)$. Then

$a_i = c b_i$ for some $b_i \in R$

and

$$f(x) = c\,(b_0 + b_1 x + \dots + b_n x^n) = c\,g(x)$$

and $g(x) \in R[x]$

Note no irreducible $r \in R$ divides all of b_i's since otherwise cr would divide all a_i's but c is the $\gcd(a_0 \dots a_i)$

Hence $g(x)$ is primitive.

To see uniqueness, suppose $f(x) = d\,h(x)$ for $d \in R$, $h(x) \in R[x]$ primitive.

then $c\,g(x) = d\,h(x)$. Any irreducible factor of c must divide d and vice versa we get that $c = du$ for some unit $u \in R^\times$

and $u\,g(x) = h(x)$ as claimed ⊠.

The next Lemma is called Gauss's Lemma

Lemma 1.15 (Gauss Lemma) If R is a UFD then the product of 2 primitive polynomials is primitive. Hence (by induction) any finite product of primitive polys in $R[x]$ is primitive.

Proof let
$$f(x) = a_0 + a_1 x + \dots + a_n x^n \qquad a_n \neq 0$$
$$g(x) = b_0 + b_1 x + \dots + b_m x^m \qquad b_m \neq 0$$

be 2 primitive polys in $R[x]$.

let $h(x) = f(x)g(x) = c_0 + \dots + c_{m+n} x^{n+m}$

let $p \in R$ be an irreducible. Then p does not divide all of a_i and p does not divide all of b_j, since f, g are primitive.

let a_r be the first coef of f not divisible by p
ie $p \mid a_i$ for $i < r$. Similarly
let b_s " " " g " "
ie $p \mid b_j$ for $j < s$.

Now the coefs of x^{r+s} is given by

$$c_{r+s} = (a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r-1} b_{s+1})$$

$$+ a_r b_s$$

$$+ (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots + a_{r+s} b_0)$$

Now since $p \mid a_i$ for $i < r$, $p \mid (a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1})$

and since $p \mid b_j$ for $j < s$, $p \mid (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0)$

but $p \nmid a_r a_s$ since $p \nmid a_r$, $p \nmid a_s$

Hence $p \nmid c_{r+s}$. Hence there is no irreducible $p \in R$ s.t p divides all c_k's. Hence $h(x) = f(x) g(x)$ is primitive

∎.

Rmk. Note it follows similarly that for 2 polynomials $f, g \in R[X]$, $(\text{content}(f))(\text{content}(g)) = \text{content}(fg)$

Now let R be a UFD, $F = \text{Quot}(R)$ field of quotients of R. The next proposition relates non-constant irred. polys in $R[X]$ to those of $F[x]$.

Prop 1.16. Let R be a UFD, $F = \mathrm{Quot}(R)$ quotient field of R. Let $f(x) \in R[x]$ $\deg f > 0$.
If f is irreducible in $R[x]$ then f is irreducible in $F[x]$

Moreover if f is primitive in $R[x]$ and irreducible in $F[x]$, then f is irreducible in $R[x]$.
ie for primitive polynomials $f(x) \in R[x]$
f is irred in $R[x] \iff f$ is irred in $F[x]$

Proof: We'll prove the contrapositive.
Suppose $f(x) \in R[x] \subset F[x]$ is a product of lower degree polynomials in $F[x]$, ie

$$f(x) = r(x)s(x) \qquad r(x), s(x) \in F[x]$$

and $\deg r < \deg f$, $\deg s < \deg f$.

Since F is the quotient field of R each coef of $r(x)$ and $s(x)$ is of the form $\frac{a}{b}$ with $a, b \in R$

By clearing the denominators we can write

$$f(x) = \frac{r_1(x)s_1(x)}{d} \quad \text{with } d \in R.$$

so that $df(x) = r_1(x)s_1(x)$ with $r_1, s_1 \in R[x]$ and $\deg r_1 = \deg r$, $\deg s_1 = \deg s$.

By lemma 1.14 we can also factor out the contents of $r_1(x)$, $s_1(x)$ to write

$$r_1(x) = c_1 r_2(x) \quad , \quad s_1(x) = c_2 s_2(x)$$

with $c_1, c_2 \in R$, $r_2(x), s_2(x) \in R[x]$ and primitive

Similarly for f we write $f = cg(x)$ with $c \in R$ $g \in R[x]$, g primitive

Then we have $df(x) = dcg(x) = (c_1c_2)r_2(x)s_2(x)$

By Gauss lemma $r_2 s_2$ is also primitive.

Hence looking at contents on both sides we get $c_1c_2 = dcu$ for some unit u.

and $dcg(x) = dcur_2(x)s_2(x)$ gives

$$f(x) = cg(x) = cu\, r_2(x)s_2(x)$$

We've shown that if f factors non-trivially in $F[x]$ into polys of smaller degree, then f factors into polynomials of the same degrees in $R[x]$ and possibly an elt of R, thus f is reducible in $R[x]$.
Thus $f(x)$ irred in $R[x] \Rightarrow f$ is irred in $F[x]$.

A non constant poly which is primitive in $R[x]$

and irreducible in $F[x]$ is irreducible in $R[x]$. Because if $f(x)$ were reducible

then $f(x) = r(x)s(x) \subset R[x] \subset F[x]$.
with $\deg r < \deg f$ since f is primitive
$\deg s < \deg f$
and this would be a factorization of f in $F[x]$ which we assumed is irred in F.
☒.

Rmk. For non primitive $f \in R[x]$
$f(x)$ can be reducible in $R[x]$ and irreducible in $F[x]$

eg $5x = (5)(x) \in \mathbb{Z}[x]$ neither factor is a unit, hence reducible
since 5 is a unit in $\mathbb{Q}$, it is irreducible in $\mathbb{Q}[x]$

The Prop 1.16 says this is the only difference between the irreducible elts in $R[x]$ and those in $F[x]$.

Finally an application of Prop 1.16 gives

Thm 1.17. If R is a UFD, then so is $R[x]$

Proof. Let $f \in R[x]$, $f \neq 0$, and non-unit
If $\deg f = 0$ then we are done since R is a UFD. Suppose $\deg f > 0$
Viewing $f \in F[x]$, which is a UFD
$f(x) = p_1(x) \dots p_r(x)$, with $p_i(x) \in F[x]$