One final thing about PIDs:

- For any nonzero polynomial $f(x) \in \mathbb{F}[x]$, the quotient ring $\mathbb{F}[x]/f(x)\mathbb{F}[x]$ is a vector space over $\mathbb{F}$. If $\deg(f) = d$, then $\underline{1}, \underline{x}, \underline{x}^2, \ldots, \underline{x}^{d-1}$ (images of $1, x, \ldots, x^{d-1}$) is a basis, hence $\dim = \deg(d)$.

Proof: Existence and uniqueness of remainder mod $f(x)$. ///

Let $R := \mathbb{F}[x]/f(x)\mathbb{F}[x]$.

If $f(x)$ is irreducible/prime then R is a field. If $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ then $\# R = p^d$. Thus existence of finite fields is equivalent to existence of irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$:

$$\begin{array}{l} f(x) \in \mathbb{Z}/p\mathbb{Z}[x] \\ \text{irred. of deg } d \end{array} \rightsquigarrow \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(f)} \quad \begin{array}{l} \text{field of} \\ \text{size } p^d. \end{array}$$

Theorem (Gauss): Irred polys exist of every degree in $\mathbb{Z}/p\mathbb{Z}[x]$. ///

Theorem (Galois): The imaginary roots of $x^{(p^d-1)} - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ form a field of size p^d.

Back to geometry.

Homogeneous polynomials.

R ring.

$\vec{x} = \{x_1, x_2, \ldots, x_n\}$ "independent variables."

$\vec{x} \subseteq E \supseteq R$ some ring E,

x_i transcendental $/ R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$.

Say $R[\vec{x}] \subseteq E$ are called "polynomials in $\vec{x}$."

If $\vec{x}$ & $\vec{y}$ are mutually independent variables then

$$R[\vec{x}][\vec{y}] = R[\vec{y}][\vec{x}] = R[\vec{x},\vec{y}].$$

For any vector $I \in \mathbb{N}^n$ we define

$$\vec{x}^I = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

and observe $\vec{x}^I \vec{x}^J = \vec{x}^{I+J}$.

Monomials give an R-linear basis of polynomials $R[\vec{x}]$. That is:

$$f(\vec{x}) = \sum_{I \in \mathbb{N}^n} a_I \vec{x}^I$$

(unique expression)

where $a_I \in R$ are almost all zero.

By collecting terms with common "total degree" $\Sigma I = i_1 + i_2 + \cdots + i_n$. we get filtration into <u>homogeneous components</u>:

$$f(\vec{x}) = f^{(0)}(\vec{x}) + f^{(1)}(\vec{x}) + \cdots$$

where $f^{(k)}(\vec{x}) = \sum_{\Sigma I = k} a_I \vec{x}^I$.

[Terminology: $R[\vec{x}] = \bigoplus_{k \geq 0} R_k[\vec{x}]$

where $f^{(k)} \in R_k[\vec{x}]$, $g^{(l)} \in R_l[\vec{x}]$,

then $f^{(k)} g^{(l)} \in R_{k+l}[\vec{x}]$, is called

a <u>grading</u>. Filtration if $\oplus$ is $+$.]

If $f(\vec{x}) \neq 0$ then $\deg(f) = d \in \mathbb{N}$

where $f^{(d)}(\vec{x}) \neq 0$, $f^{(k)}(\vec{x}) = 0 \ \forall k > d$.

Then $f^{(d)}(\vec{x})$ is the <u>leading form</u> of $f(\vec{x})$.

Problem 1.4: If R is a domain,

$$\deg(fg) = \deg(f) + \deg(g).$$

Hence $R[\vec{x}]$ are a domain.

Problem 1.5 : Let $f(\vec{x}) \in R[\vec{x}]$ and consider two conditions:

(H1) $f(\vec{x}) = f^{(d)}(\vec{x})$

(H2) $f(\vec{x}) \neq 0$ and $f(\lambda \vec{x}) = \lambda^d f(\vec{x}) \quad \forall \lambda \in R \setminus 0$

forgot to say this before

Claim: (H1) $\Rightarrow$ (H2) always

(H2) $\Rightarrow$ (H1) if R is infinite domain

(e.g. $R = \mathbb{Z}$, $R = \mathbb{Z}/p\mathbb{Z}[x]$)

<u>Proof</u>: (H1) $\Rightarrow$ (H2)

For any $\vec{x}^I$ we have

$$(\lambda \vec{x})^I = (\lambda x_1)^{i_1} (\lambda x_2)^{i_2} \cdots (\lambda x_n)^{i_n}$$

$$= \lambda^{\Sigma I} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

$$= \lambda^{\Sigma I} \vec{x}^I .$$

Hence $f^{(k)}(\lambda \vec{x}) = \lambda^k f^{(k)}(\vec{x})$.

(H2) $\Rightarrow$ (H1).

Let R be infinite domain & define

$$g(\vec{x}, y) := y^d f(\vec{x}) \in R[\vec{x}, y]$$

$$h(\vec{x}, y) := f(y\vec{x})$$

$$= \sum_{k \geq 0} y^k f^{(k)}(\vec{x}) \in R[\vec{x}, y]$$

By assumption:

$$g(\vec{x}, \lambda) = h(\vec{x}, \lambda) \quad \forall \lambda \in R \setminus 0.$$

$$g(\vec{x}, \lambda) - h(\vec{x}, \lambda) = 0 \in R[\vec{x}].$$

Since $g(\vec{x}, y) - h(\vec{x}, y) \in R[\vec{x}][y]$

has infinitely many roots in the domain $R[\vec{x}]$, we conclude that

$$g(\vec{x}, y) - h(\vec{x}, y) = 0(\vec{x}, y)$$

i.e. y-coeffs of $g(\vec{x}, y)$ & $h(\vec{x}, y)$

are the same:

$$y^d f(\vec{x}) = \sum_{k \geq 0} y^k f^{(k)}(\vec{x})$$

$$\Longrightarrow \quad f^{(d)}(\vec{x}) = f(\vec{x})$$
$$f^{(k)}(\vec{x}) = 0 \text{ for } k \neq d.$$

///

This criterion can be quite useful.

Application (Problem 1.6):

Let R be infinite domain &
$A \in GL_n(R)$ be invertible $n \times n$ matrix.
If $F(\vec{x}) \in R[\vec{x}]$ is homogeneous
of degree d, then

$$G(\vec{x}) := F(A\vec{x}) \in R[\vec{x}]$$

is also homogeneous of degree d.

[Thus projective transformation sends degree d curves to degree d curves. More generally, hypersurfaces.]

<u>Proof</u>: First we observe that $G(\vec{x}) \neq 0(\vec{x})$. Indeed, if

$F(A\vec{x}) = G(\vec{x}) = 0(\vec{x})$ then

$0(\vec{x}) \neq F(\vec{x}) = 0(A^{-1}\vec{x}) = 0(\vec{x})$,

contradiction.

Then since matrix multiplication is linear, we have

$$
\begin{aligned}
G(\lambda\vec{x}) &= F(A\lambda\vec{x}) \\
&= F(\lambda A\vec{x}) \\
&= \lambda^d F(A\vec{x}) = \lambda^d G(\vec{x})
\end{aligned}
$$

for all $\lambda \neq 0$. ///

Next time: Multivariable Taylor series expansions

&

relationship to local behavior near a point.