

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 $\underline{1}, \underline{x}, \underline{x^2}, \dots, \underline{x^{d-1}}$ (images of $1, x, \dots, x^{d-1}$) is a basis, hence $\dim = \deg(f)$.

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

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

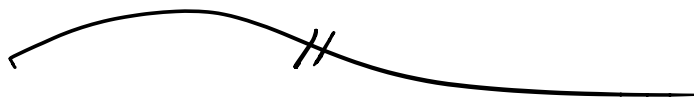
If $f(x)$ is irreducible/prime then R is a field. If $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ then

$\# R = p^d$. Thus existence of finite fields is equivalent to existence of irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$:

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

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.

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

$\vec{x} \in E \cong R$ some ring E ,

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

Say $R[\vec{x}] \subseteq E$ are called

"polynomials in \vec{x} ."

[Thus projective transformation sends degree d curves to degree d curves. More generally, hyper-surfaces.]

Proof : 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.