22 May 2023
MAT 2250

Polynomial ring:
Let K be a field (like $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$), then $K[x]$ is the set of polynomials with coefficient in K.
We add & multiply 2 polynomials like usual.

Example: $\mathbb{Z}_3[x]$
$P_1(x) = x^2 + 2x$, $P_2(x) = x + 1$

$P_1(x) + P_2(x) = (x^2 + 2x) + (x+1)$
$= x^2 + 3x + 1$
$= x^2 + 1$

$P_1(x) + 0 = 0$

$P_1(x) \cdot 1 = 1$

$P_1(x) \cdot P_2(x) = (x^2+2x)(x+1)$
$= x^3 + x^2 + 2x^2 + 2x$
$= x^3 + 3x^2 + 2x = x^3 + 2x$

Rmk: It is not true that every polynomial in $K[x]$ has a root in K.
Ex: $f(x) = x^2 + 1$ in $\mathbb{R}[x]$ has no root in $\mathbb{R}$.

Finding roots of polynomials (or systems) is & still is an important question in mathematics & applications. (Has connections to optimization.)

Galois theory: For e

Def Algebraically closed: A field K is algebraically closed if every polynomial in $K[x]$ has a root in K.

Example: $\mathbb{C}$ is algebraically closed

Galois theory: For every field K, there is a field $\overline{K}$ which is algebraically closed & which contains K. $\overline{K}$ is unique upto isomorphism & is called the algebraic closure of K.

Ex: $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

$\overline{\mathbb{Q}}$ = the field of algebraic numbers
(algebraic number is a number in $\mathbb{C}$ which is a root of a polynomial in $\mathbb{Z}[x]$)
= algebraic closure of $\mathbb{Q}$.

$\overline{\mathbb{Q}}$ is countable. $\overline{\mathbb{Q}} \subseteq \mathbb{C}$

$\overline{\mathbb{Z}_p}$ = algebraic closure of $\mathbb{Z}_p$.

Then $\overline{\mathbb{Z}_p}$ is countable. $\overline{\mathbb{Z}_p} \not\subset \mathbb{C}$.

Why? For every $x \in \overline{\mathbb{Z}_p}$ then $p \cdot x = 0$

The polynomial ring $\overline{\mathbb{Z}_p}[x]$: ($p$: prime number)

Claim 1: $(x+y)^p = x^p + y^p \quad \forall x, y \in \overline{\mathbb{Z}_p}$

By binomial coefficient theorem: $(x+y)^p = x^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j} + y^p$.

For $1 \le j \le p-1$:

$\binom{p}{j}$ is divisible by p

so it is 0 in $\mathbb{Z}_p$.

Claim 2: Let $p(x)$ be a polynomial of degree n in $\mathbb{Z}_p[x]$. Assume that $p(x)$ has no root in $\overline{\mathbb{Z}_p}$ $\Rightarrow$ $p(x)$ and $p'(x)$ have no common divisor $\Rightarrow$ $p(x)$ has n distinct roots in $\overline{\mathbb{Z}_p}$.

Now, we will construct a field with p^n elements

Lagrange theorem: Let G be a finite group, G has m elements. Let x be $a \in G$. Then $\exists$ m_1, which is a divisor of m, so that

$x^{m_1} = 1$ (neutral element in the group.)

In particular, $\forall x \in G$: $x^m = 1$. □

Apply to a field K:

$(K \setminus 0, \times)$ ($\times$: multiplication) is a group

If K has n elements, then $\forall x \in K \setminus 0$:

$x^{n-1} = 1$.

Now let

$\mathbb{F}_{p^n} = \{ x \in \overline{\mathbb{Z}_p} : x^{p^n} = x \} \subset \overline{\mathbb{Z}_p}$.

Prop: $\mathbb{F}_{p^n}$ is a field with p^n elements.

Proof:

We need to show:

- $\mathbb{F}_{p^n}$ has p^n elements
- $\mathbb{F}_{p^n}$ is a subring of $\overline{\mathbb{Z}_p}$.
- $x \in \mathbb{F}_{p^n} \setminus 0 \Rightarrow \frac{1}{x}$ is also in $\mathbb{F}_{p^n}$.

Let's look at $Q(x) = x^{p^n} - x$.

has degree p^n.

We also need to show that all roots of $Q(x)$ are simple. (no multiple roots).

just need to check that $Q(x)$ & $Q'(x)$ have no common roots.

$$Q'(x) = \left(x^{p^n} - x\right)'$$
$$= p^n \cdot x^{p^n - 1} - 1$$
$$= -1 \text{ in } \overline{\mathbb{Z}_p}[x]$$

$\Rightarrow \mathbb{F}_{p^n}$ has p^n elements.

$x \in \mathbb{F}_{p^n} \setminus 0$: $x^{p^n} = x$

$\Rightarrow \frac{1}{x^{p^n}} = \frac{1}{x}$

$$\left(\frac{1}{x}\right)^{p^n} = \frac{1}{x}$$

$\Rightarrow \frac{1}{x} \in \mathbb{F}_{p^n}$.

$\mathbb{F}_{p^n}$ is a ring:

$0 \in \mathbb{F}_{p^n}$: $x = 0 \Rightarrow 0^{p^n} = 0$

$1 \in \mathbb{F}_{p^n}$: $x = 1 \Rightarrow 1^{p^n} = 1$

$x, y \in \mathbb{F}_{p^n}$: WTS:

$x + y \in \mathbb{F}_{p^n}$

$x \cdot y \in \mathbb{F}_{p^n}$

$x^{p^n} = x$

$y^{p^n} = y$

$\Rightarrow xy = x^{p^n} \cdot y^{p^n} = (xy)^{p^n}$

$\Rightarrow xy \in \mathbb{F}_{p^n}$.

$(x+y)^{p^n} = x^{p^n} + y^{p^n} = x + y$

$(x+y)^{p^2} = \left((x+y)^p\right)^p = \left(x^p + y^p\right)^p$

$= (x^p)^p + (y^p)^p = x^{p^2} + y^{p^2}$

$\Rightarrow x + y \in \mathbb{F}_{p^n}$.

$x \in \mathbb{F}_{p^n}$: WTS $-x \in \mathbb{F}_{p^n}$.

$x^{p^n} = x$

$\Rightarrow (-x)^{p^n} = (-1)^{p^n} x^{p^n} = (-1)^{p^n} x$

$\forall$ p prime number then $(-1)^{p^n} = -1$ in $\mathbb{Z}_p$.

If p is odd then it is OK.

If p is even $\Rightarrow p = 2 \Rightarrow -1 = 1$ in $\mathbb{Z}_2$.

(Q.E.D.)

Claim: Up to isomorphism, there is only one field with p^n elements.

Proof:

If $F \leq \overline{\mathbb{Z}}_p$ has p^n elements then by Lagrange's theorem $\forall x \in F$ we must have: $x^{p^n} = x$.

$\Rightarrow F = \mathbb{F}_{p^n}$.

Now it is known every field with p^n elements must be in $\overline{\mathbb{Z}}_p \Rightarrow F$ is unique. (Q.E.D.)

Prop: If F is a finite field, then $\exists$ a prime p so that

$p \cdot x = 0 \quad \forall x \in F$.

p is called the characteristic of F.

Proof: Apply Lagrange theorem from $(F, +)$. Then show that for one prime divisor p of $n = \#F$, then $p \cdot 1 = 0$ in F. $\square$ $(\#F \geq 2)$

Quotient rings of $\mathbb{Z}_p[t]$: (Can replace $\mathbb{Z}_p$ by any field)

Recall:

$\mathbb{Z}_p = \mathbb{Z} / \equiv_p$ ($x, y \in \mathbb{Z}$: $x \equiv_p y$ if $x - y$ is divisible by p)

Now we replace $\mathbb{Z}$ by $\mathbb{Z}_p[t]$, m by a polynomial $Q(t)$, & define $\mathbb{Z}_p[t]/Q(t)$ as the quotient of the equivalent relation:

$Q_1(t) \equiv Q_2(t) \Leftrightarrow Q_1(t) - Q_2(t)$ is divisible by $Q(t)$.

Claim 1: $\mathbb{Z}_p[t]/Q(t)$ is a finite ring.

Proof: That it is a ring is easy. Now we show that it has a finite number of elements.

Let $\deg(Q(t)) = n$.

Claim $\mathbb{Z}_p[t]/Q(t)$

$= \{ a_0 + a_1 t + \dots + a_{n-1} t^{n-1} : a_0, \dots, a_{n-1} \in \mathbb{Z}_p \}$

By Euclidean division algorithm, $\forall f(t) \in \mathbb{Z}_p[t]$, $\exists$ $p(t)$ & $r(t)$, $\deg r(t) \le n-1$ so that:

$f(t) = p(t) Q(t) + r(t)$.

$\Rightarrow [f(t)] = [r(t)]$ in $\mathbb{Z}_p[t]/Q(t)$ (Q.E.D.)

Corollary: $\#\, \mathbb{Z}_p[t]/Q(t) = p^n$, where $n = \deg(Q(t))$.

□

Irreducible polynomial: $\in \mathbb{Z}_p[t]$

A polynomial $Q(t)$ is irreducible, if there are no $Q_1(t), Q_2(t) \in \mathbb{Z}_p[t]$ with $\deg Q_1, Q_2 \ge 1$ & $Q(t) = Q_1(t) Q_2(t)$.

Ex: $Q(t) = t^2 + 1$ is not irreducible in $\mathbb{Z}_2[t]$.

$Q(t) := \underbrace{(t+1)}_{Q_1(t)} \underbrace{(t+1)}_{Q_2(t)}$ in $\mathbb{Z}_2[t]$.

Ex: $Q(t) = t^2 + 1$ is irreducible in $\mathbb{Z}_3[t]$. Proof: if not then $\exists$ would exist $Q_1(t) = t + \alpha$, $Q_2(t) = t + \beta$ so that:

$t^2 + 1 = (t+\alpha)(t+\beta)$ in $\mathbb{Z}_3[t]$

$\Leftrightarrow t^2 + 1 = t^2 + (\alpha+\beta)t + \alpha\beta$ in $\mathbb{Z}_3[t]$

$\Leftrightarrow \begin{cases} \alpha + \beta = 0 \text{ in } \mathbb{Z}_3 \\ \alpha\beta = 1 \text{ in } \mathbb{Z}_3 \end{cases}$

$\Leftrightarrow \begin{cases} \alpha = -\beta \text{ in } \mathbb{Z}_3 \\ -\alpha^2 = 1 \text{ in } \mathbb{Z}_3 \end{cases}$

$\alpha = 0 \Rightarrow -\alpha^2 = 0 \neq 1$ in $\mathbb{Z}_3$

$\alpha = 1 \Rightarrow -\alpha^2 = -1 \neq 1$ in $\mathbb{Z}_3$ $\Rightarrow$ no solution

$\alpha = 2 \Rightarrow -\alpha^2 = -1 \neq 1$ in $\mathbb{Z}_3$.

Thm: ~~if $Q(x)$ is irreducible~~
$\mathbb{Z}_p[t]/Q(t)$ is a field
$\Leftrightarrow$ $Q(t)$ is ~~not~~ irreducible.

Proof:
($\Leftarrow$) if $Q(t)$ is not irreducible then $\mathbb{Z}_p[t]/Q(t)$ is not a field.

$Q(t) = Q_1(t)\,Q_2(t)$, $Q_1(t)$, $Q_2(t) \in \mathbb{Z}_p[t]$, $\deg Q_1(t), \deg Q_2(t) \geq 1$,
So $[Q_1(t)] \neq 0$, $[Q_2(t)] \neq 0$ in $\mathbb{Z}_p[t]/Q(t)$

but
$[Q_1(t)] \cdot [Q_2(t)]$
$= [Q_1(t)Q_2(t)] = [Q(t)]$
$= 0$ in $\mathbb{Z}_p[t]/Q(t)$.

($\Rightarrow$) if $Q(t)$ is irreducible $\Rightarrow$ $\mathbb{Z}_p[t]/Q(t)$ is a field.

If $\mathbb{Z}_p[t]/Q(t)$ were not a field, there would be $[Q_1(t)], [Q_2(t)]$, $\deg Q_1, \deg Q_2 \leq n-1$, $\notin [Q_1], [Q_2] \neq 0$ in $\mathbb{Z}_p[t]/Q(t)$

but $Q_1(t)Q_2(t) = 0$ in $\mathbb{Z}_p[t]/Q(t)$

$\Rightarrow$ $Q_1(t)Q_2(t)$ is divisible by $Q(t)$.

But $Q(t)$ is irreducible $\Rightarrow$ impossible. □

Corollary: To find a field F with p^n elements, it suffices to find an irreducible polynomial $Q(t)$ in $\mathbb{Z}_p[t]$ with degree n. Then $F = \mathbb{Z}_p[t]/Q(t)$.

Rmk: if we can find an irreducible polynomial $Q(t)$, then $\mathbb{Z}_p[t]/Q(t)$ is explicitly constructed (than the one given through the zero set of $x^{p^n} = x$ in $\mathbb{Z}_p$). However, it may be not easy to construct irreducible polynomials in $\mathbb{Z}_p[x]$.

Ex: $Q(t) = t^2 + 1$ is irreducible in $\mathbb{Z}_3[t]$. $\deg Q = 2 \Rightarrow$ we have a field F with $3^2 = 9$ elements, whose elements are as follows:

$a_0 = 0,\ a_1 = 1,\ a_2 = t,\ a_3 = 0+t,\ a_4 = 1+t,\ a_5 = 2+t,$
$0+2t,\ 1+2t,\ a_7 = 2t,\ a_8 = 2+2t.$

$a_6 =$

$(2+2t)(1+t) = 2 + 4t + 2t^2$

$= 2(1+t^2) + 4t$

$= t$ in $\mathbb{Z}_3[t]/\overbrace{(t^2+1)}^{Q(t)}$

$\Rightarrow a_8 \cdot a_4 = a_3.$

What is the inverse of a_8? (Use Euclidean division algorithm)

$\underbrace{t^2+1}_{Q(t)} = \underbrace{(2t+2)}_{t^2+t}(2t + \underline{1} - t$

$= (2t+2)2t + (2t+2) - 1$

$= (2t+2)(2t+1) - 1$

$\Rightarrow (2t+2)(2t+1) = \underline{1}$ in $\mathbb{Z}_3[t]/Q(t)$

$\Rightarrow 2t+1$ is inverse to $2t+2$.

For to do division in many variables look at Gröbner basis.

Projective plane over $\mathbb{Z}_p$ (or in general over a field K): ($K = \mathbb{Z}_p$ for example)

Let consider

$K^3 = \{(a,b,c) : a,b,c \in K\}$

This is a vector space. origin ↓

A line in K^3 going through $(0,0,0)$ is given by:

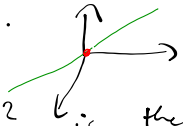
$L_{a,b,c} = \{t(a,b,c) : t \in K\}$

where $(a,b,c) \neq (0,0,0)$.

Q: How many such lines we have in K^3 $\mathbb{Z}_p^3$?

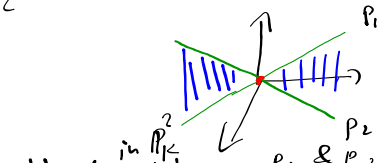
Def: (Projective plane over K)

A "point" in the projective plane over K, $\mathbb{P}^2_K$, is a line in K^3 going through the origin.



Nhận: A "line" in $\mathbb{P}^2_K$ is the plane in K^3 generated by the 2 lines representing the "points".

Let P_1 be a "point" in $\mathbb{P}^2_K$
$\hookrightarrow$ L_1 a line in K^3 going through $(0,0,0)$
P_2 .... "point" in $\mathbb{P}^2_K$
$\hookrightarrow$ L_2 ... line in K^3 ....



The line between P_1 & P_2 in $\mathbb{P}^2_K$ $\hookrightarrow$ the plane in K^3 containing L_1 & L_2.

Thm: If M_1 & M_2 are 2 distinct "lines" in $\mathbb{P}^2_K$ then $M_1 \cap M_2$ = a "point" in $\mathbb{P}^2_K$.

Proof: 2 distinct planes in K^3 going through $(0,0,0)$ intersect along a line in K^3 going through $(0,0,0)$. ☐

Rmk: $K^2 \subseteq \mathbb{P}^2_K$ ← "compact" space

On $\mathbb{P}^2_K$ we have Bezout's theorem

$\mathbb{P}^2_K$ is an object in algebraic geometry, number theory, cryptography (elliptic curves in $\mathbb{P}^2_K$)