def: ring: set naturally endowed with 2 binary operations "+", "×"; "closed"
加法: commutative, associative; zero, inverse
乘法: associate, distributive
field: commutative ring, 且存在 unity, $\forall$ 非零元素有 muliplicative inverse
= division ring

def: $E \supset F$, E, F 为域, E 为 extension of F

例: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q}$ proper subfield of $\mathbb{R}$

若有, 设为 E, $1 \in E$, $0 \in E$

E 为 first a ring, $1 \in E$, then $|1| \in E$, $|1|+\cdots|1| \in E$; inverse also

$\therefore E \supseteq \mathbb{Z}$ … step1

满足乘法群 $x \in E$, $\frac{1}{x} \in E$, $\therefore E \supseteq \{\frac{1}{z} : z \in \mathbb{Z}\backslash\{0\}\}$ … step2

$\forall m \in \mathbb{Q}$, $m = \frac{p}{q}$, $p, q \in \mathbb{Z}$,

$\frac{1}{q} \in E$, $p \in E$ by step1,2 $\Rightarrow m \in E$ $\therefore \mathbb{Q} \subseteq E$, E 为 not proper

例: $\mathbb{Q}(\sqrt{n}) = \{a+b\sqrt{n} : a, b \in \mathbb{Q}\}$ n not square integer, $\mathbb{Q}(\sqrt{n})$ is a field

$\mathbb{Q}(\sqrt{n})$ is a commu- ring with unity 1

即证 $\forall a+b\sqrt{n} \neq 0$ $\exists$ inverse $c+d\sqrt{n}$; $b=0$ 易知, 考虑 $b \neq 0$ 时

$(c+d\sqrt{n})(a+b\sqrt{n}) = ac+bdn+(bc+ad)\sqrt{n} = 1$ $\therefore bc+ad=0$, $d \neq 0$ since $b \neq 0$

设 $d=1$ $a=-bc$, $bdn-b^2c=1$

$b = \frac{dn \pm \sqrt{d^2n^2-4c}}{2}$ 即 want $d^2n^2 = 4c+m^2$ $m \in \mathbb{Q}$

Obv: $\forall n$: $\exists d, c$ s.t. $\sqrt{4c+m^2} \in \mathbb{Q}$, thus $d \in \mathbb{Q}$, $b \in \mathbb{Q}$, 找到 inverse

例: $S = \mathbb{Q}(2^{\frac{1}{3}})$ smallest subfield of $\mathbb{R}$ containing $\mathbb{Q}$, $2^{\frac{1}{3}}$; $S = \{a+b\cdot 2^{\frac{1}{3}}+c\cdot 2^{\frac{2}{3}} \cdots \in \mathbb{Q}\}$

$\mathbb{Q} \subseteq S$, $a+\cdots$

$2^{\frac{1}{3}} \subseteq S$, $b\times 2^{\frac{1}{3}} + c\times 2^{\frac{2}{3}} + \cdots$ 封闭性, 不可写成非常数多项式的积

任意 F?

Thm: let $F = \mathbb{Q}$ or $\mathbb{F}_p$, $R = F[x]$; take $p(x) \in R$ s.t. p irreducible, $I = (p(x))$;
= irreducible

then $S = R/I = \{r+I : r \in F[x]\}$ is a field

更准确的写法是 "p(x) irreducible polynomial

$\Leftrightarrow$ "$I = (p(x))$ 为 $F[x]$ 的最大理想环 $\overset{(3)}{\Leftrightarrow} F[x]/(p(x))$ is field

在反面证明了 (1) $\Leftrightarrow$ (3) 和 (1) $\Leftrightarrow$ (2), 也可推出 (2) $\Leftrightarrow$ (3)

principle ideal domain (PID):

- integral Domain: commutative, 无 zero factors
- ∀ principle ideas: 每个理想环均可由单元素生成, ∀ I∈PID, I=(a) some a∈I
- unique factorization: (0外) ∀ element can be factored uniquely into irreducible elements
- Noetherian: PID本质是一个诺特环, 每个理想环的升链稳定

(1)⇒(3): $F[x]/(p(x)) = \{f(x)+(p(x)) : f(x)\in F[x]\}$

满足加法定律, ∃ zero = $(p(x))$, inverse

满足乘法定律, ∃ unity, $1+(p(x))$ ⇒ 各 inverse

证: $(f(x)+(p(x)))(g(x)+(p(x))) = 1+(p(x))$; $f\notin(p(x))$ 若 $f\in(p(x))$ 证毕

then: $f(x)\cdot g(x) = 1+q(x)$, $q(x)\in(p(x)) = \{\sum p(x)r_1(x) + r_2(x)p(x) + r_3(x)p(x)r_4(x) + \dots p(x)\}$

∃ $f\cdot g - p\cdot t = 1$ since $\gcd(f,p)=1$

⇕

p irreducible, $f\notin(p(x))$ ∴ $\gcd(f,p)=1$ → 广义因式(不只是数) $\{r(x)p(x)\}$

∴ Bezout: ∃ $g,q\in F[x]$ $f\cdot g + pq = 1$

⇒ $(f(x)+(p(x)))^{-1} = (g(x)+(p(x)))$

(3)⇒(1) 类似于 $\mathbb{Z}/n\mathbb{Z}$ is field ⇌ n prime

设 $p = qr$

need $q(x)\cdot g = 1+s(x)p(x)$ Some s, g 注意一下多项式乘法 commutative

q|LHS, q∤RHS ∴ 找不到

即: $p(x)$ 为 $F[x]$ 中的 irreducible polynomial ⇌ $F[x]/(p(x))$ is a field

(2)⇒(1) 若 $p(x) = q(x)s(x)$

$(p(x)) = \{\sum p(x)r_1(x) + r_2(x)p(x) + r_3(x)p(x)r_4(x) + \dots p(x)\} = \{r(x)p(x) : r\in F[x]\}$

$(q(x)) = \{r(x)q(x) : r\in F[x]\}$

$(p(x)) \subsetneq (q(x))$ since $q\in(q(x))$, $q\notin(p(x))$ ∴ $(p(x))$ 不为最大

∴ $(p(x))$ 是最大 ideal, p 不可约

(1)⇒(2) $p(x)$ irreducible $(p(x)) = \{r(x)\cdot p(x) : r\in F(x)\}$

加了个条件也一样的

$F[x] \supset A \supsetneq (p(x))$, $q\in A$, $A = \{r_1(x)p + r_2(x)q : r_1 r_2 \in F\}$ ∴ $p\nmid q$ 则 $p\nmid q$ $\gcd(p,q)=1$

∴ ∃ $m(x)p + n(x)q = 1$

∴ ∀ $h(x)\in F[x]$ $r_1 = hm$ $r_2 = hn$ ⇒ 说明 $h\in A$ ∴ $A = F[x]$

即 (1)⇌(2) 多项式不可约⇌最大理想

Thm: F is a finite field, then $|F| = s^d$ $d \in \mathbb{Z}^+$, s prime

pf1: $F_n \subseteq \{0, 1, 2, \cdots n\}$, $n = pq$

$pr = 1$, $pr = 1 + pq \times z$ contradict $\Rightarrow$ p, q 均不存在 inverse

pf2: 对 finite field 是 finite Abel group, for both "+", "×"

若 F_n $p|k$, $q|k$

F_n is finite Abel with "+" $\therefore \exists |x| = p$, $|y| = q$ by Cachy 前面证过

$\therefore \underbrace{x+x+x+\cdots x}_{p \text{ times}} = 0$, $\underbrace{y+y+\cdots y}_{q\text{-times}} = 0$

$(F^\times)$ is a group, $\therefore \exists y^{-1}, x^{-1}$ $yx^{-1}, xy^{-1} \in F$

$yx^{-1}(x+x+\cdots x) = \underbrace{y+y+\cdots y}_{p\text{-times}} = 0$, 同理 $\underbrace{x+x+\cdots x}_{q\text{-times}} = 0$

$\therefore p|q$, $q|p \Rightarrow p = q$

说明 $|F|$ 不存在两个不同的因数 $\Rightarrow |F| = s^d$ for prime numbers s

例: $F_3 = \{0, 1, 2\}$, $p(x) = x^2 + 1$ 在 F_3 上 irreducible, 由此由 Thm 知 $F_3[x]/(p(x))$ is field,

$F_3[x]/(p(x)) = \{a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n + (p(x)) : a_i \in F_3\}$

$\Rightarrow a_n(x^n + x^{n-2}) + (a_{n-2} - a_n)(x^{n-2} + x^{n-4}) + \cdots + (a_2 - a_4)(x^2 + x^0) + (a_0 - a_2 + a_4)$

$+ a_{n-1}(x^{n-1} + x^{n-3}) + \cdots + (a_3 - a_5)(x^3 + x^1) + (a_1 - a_3 + a_5)x^1 + (p(x))$

$= (\cdots) + (\cdots)x + (p(x))$

$\therefore$ 基为 1, x. field 由 $1 + (p(x))$, $x + (p(x))$ 生成.

Def: F is a field, n: 最小正整数 s.t. $n \cdot 1 = 0$, n: characteristic of F

若 n 不为正整数, characteristic = 0 / ring 也是的

Thm: char(F) = 0 或 prime number p $\Rightarrow$ F 可以改成 integral domain {commutative, 无 zero factors}

(1) CAAP241 对于含 unity 的 ring: if 1 has infinite order, under addition, $\text{char}(R) = 0$; if 1 has order n under addition, $\text{char}(R) = n$

若 1 在加法下无限 order $1+1+1+\cdots \neq 0$, 对 $m \cdot 1 = 0$ $\therefore$ char = 0

若 $o(1) = n$ $n \times 1 = 0$ $\underbrace{\quad}_{\forall m\text{-times}}$

(2) 在 field 中以上结论仍适用

F is infinite, $1+1+\cdots \neq 0$ $\therefore$ char = 0

☆F is finite; ~~此时将 field 看成 +, × 上的 finite Abel group~~ 没用

~~$|F|=p^n$ for prime p~~ (下面用)

F中写0要说明"+"或"×"

设 $o(1)=n=xy$ 0:表示additive order

$(xy)\cdot 1=0$ ∴ $(xy)\cdot 1\cdot 1=0$

$(x\cdot 1)(y\cdot 1)=0$ ⇒ commutative } integral

∴ $x\cdot 1=0$ 或 $y\cdot 1=0$ since 有 zero factors

由于char取最小,所同样方商对x或y ⇒最后总是系数

对于 $|F|=p^r$, $\mathrm{char}(F)=p$

Thm: ∀ fields contains subfield iso to $\mathbb{Q}$ or $\mathbb{F}_p$ prime field

设E为 smallest subfield of F. $0,1\in E$

$$\Rightarrow \begin{cases} 1+1+\cdots+1\cdots=n\cdot 1\in E\ \forall n\in\mathbb{Z}^+ & n<o(1) \\ \frac{m}{n}\in E\ \forall m,n\in\mathbb{Z}^+,\ m,n<o(1) \end{cases}$$

"⇌"

o为加法order

① 若 $\mathrm{char}(F)=0$, $o(1)=+\infty$

$\forall z\in\mathbb{Z}^*$ 或 $z\in E$ $\forall m,n\in\mathbb{Z}^+$ $\frac{m}{n}\in E$ ⇒ $E\cong\mathbb{Q}$

② $\mathrm{char}(F)=p$ $\underbrace{1+1+\cdots 1}_{p}=0$; $F\cong\mathbb{F}_p\cong\mathbb{Z}_p$

(∵为field⇒p prime)

Rmk: $|F|=p^r$ 作为 Finite Abel group

F中阶数最高的元素为 a_1 $F=\langle a_1\rangle\times K$ 内直积 $F=\langle a_1\rangle K$, $\langle a_1\rangle\cap K=e$

K中 ··· 为 a_2, $F=\langle a_1\rangle\times\langle a_2\rangle\times K$ ···

$|\langle a_1\rangle|\geq|\langle a_2\rangle|\geq\cdots$, 记阶数为 $n_1,n_2\cdots$

在"+"和"×"上: $\langle a_1\rangle\cong\mathbb{Z}_{n_1}$, $\langle a_2\rangle\cong\mathbb{Z}_{n_2}$ ··· cyclic group性质

即此时是作为F的iso,而不只是单一运算的group iso