Part 1

A

(2) $x^2+1 \;\big)\; x^5+x^3+x^2+1$

x^5+x^3

x^2+1

x^2+1

0

$\Rightarrow q = x^3+1$

$r = 0$.

(3) Division algorithm 只在 field 上有用，因为只有 field 上才对 division 有 well-definedness.

这是显然的，但可以 prove 一下：

Assume $\exists q, r \in \mathbb{Z}[x]$ s.t. $\deg r < \deg g$ 且 $f = qg + r$

By uniqueness of r, through division algorithm $\Rightarrow$ $q(x) = \frac{1}{5}x + \frac{1}{5}$, 非 $\mathbb{Z}[x]$ 的元

B. (找 Gcd of polynomials)

(1) $2x^2 - 10x + 12 = 2(x-3)(x-2)$

$x^7 - 3x^6 = x^6(x-3)$ $\Rightarrow \gcd = (x-3)$

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

$x^5(x+1)^2 = x^5(x^2+2x+1)$ $\rightarrow = [0]_2 x = 0_T$

$= x^5(x^2+1)$ 因为在 $\mathbb{Z}_2[x]$ 上.

official def: 一定有更大的 ring T 使 R 为 T 的 subring，且 r 和 t 上元 基本的 multip 是 well-defined 的

$0_R = [0]_2 = 0_T$, $\Rightarrow 0_T \cdot x = 0_T = [0]_2$

$\Rightarrow \gcd = x^2(x^2+1)$

(3) (不必 Bezout): 一定有 $f, g \in \mathbb{Q}[x]$

使 $f(2x^2-10x+12) + g(x^7-3x^6) = \gcd(f,g)$

$= x-3$

C. Fix $f \in F[x]$

(1) Pf of Remainder Thm:

$\forall \lambda \in F$, $f(x)$ 除 $(x-\lambda)$ 的 remainder 为 $f(\lambda)$

Pf. 通过 division algo:

$f(x) = q(x)(x-\lambda) + r(x)$

关键：$\deg r < \deg (x-\lambda) = 1$

$\Rightarrow \deg r = 0$

因而 $r(x)$ 其实是个 const，将其当作 r.

$\Rightarrow$ 不论 x 取多少，r 的值都相同.

不妨令 $x = \lambda \Rightarrow f(\lambda) = 0 + r = r$

因而 $r = f(\lambda)$

(2) Pf of Factor Thm: $(x-\lambda)$ divides f iff $f(\lambda) = 0$

自然: ① $f(\lambda) = 0$ 即 $r = 0$ 由 (1)

$\Rightarrow (x-\lambda) \mid f(x)$

② $(x-\lambda) \mid f(x) \rightarrow f = q(x-\lambda) + 0$

i.e. $f = q(x-\lambda) + f(\lambda) \Rightarrow f(\lambda) = 0$

(3) 1, 2, 3, 4 都是 $\mathbb{Z}_5[x]$ 中 $x^4 - 1$ 的 roots.

(plug in 就好)

(4) 使用 factor thm 分解 $\mathbb{Z}_5[x]$ 中的 $x^5 - x$

* root 的概念：一个 polynomial $f(x)$ 的 root 就是当 $x \in R$ 时，如果 $f(x) = 0$，x 有哪些值

这个概念中 x 的限定在 R 中.

因为 $\mathbb{Z}_5$ 一共只有 5 个元素，因而我们可以一个一个带进去，发现：

对于 $x^5 - x = x(x^4-1)$，代入 $x = 0, 1, 2, 3, 4$ 结果都为 0.

$\Rightarrow$ By factor Thm,

$x^5 - x = x(x-1)(x-2)(x-3)(x-4)$ in $\mathbb{Z}_5[x]$.

(D) (1) Thm 4.15 如果一个 poly $f \in F[x]$ deg = 2 或 3，则 (f is irreducible iff f 没有 root.)

首先 by factor thm, 如果 f irreducible

$\Rightarrow$ f 不能被任何 $(x-a)$ divide

$\Rightarrow$ 没有 $a \in F$ 使得 $f(a)=0$

$\Rightarrow$ 没有 root.

所以我们只需要证明如果

f 没有 root, 那么 f irreducible.

(deg = 2 or 3)

可以证明其 contrapositive: 如果 f reducible,

那么一定有 root.

Let $f = gh$ where $g, h \neq f, \neq \text{const}$.

那么这件事就很明显了: g, h 不是 const, 那么

degree 至少为 1. 因为 deg f 最大是 3 所以

g, h 不能都 deg = 2, 肯定有一个 deg = 1.

(需要:

因为 f 是 field $\to$ domain $\to$ $\deg(f) = \deg(g) + \deg(h)$.)

于是 g, h 中有一个是 $ax+b$, 那么 $x = -\frac{b}{a}$ ($a \neq 0$ 因为 deg = 1)

一定是一个 root. □

(2) 我们 (1) 的 pf 只对 deg f = 2 or 3 成立

这显然的. 我们的条件成立 iff

$f = gh$, 其中必须有一个 deg = 1

which is ensured by deg f = 2/3

但如果 deg f 大于 3,

deg g, deg h 可以 both ≥ 2 了所以破了

(3) 找 $(x^5 - x)$ 在 $\mathbb{Z}_7[x]$ 中的 factorization.

这边不容易.

我们发现一个事情: 平方差公式对任何 ring 都成立

$(a^2 - b^2) = (a+b)(a-b)$

因为它只用了括号的 +, ×, distribution, ensured by def of ring

因而我们确认:

$x^5 - x = x(x^4 - 1) = x(x^2-1)(x^2+1)$

$= x(x-1)(x+1)(x^2+1)$

所以我们确定 $x = 0, 1, 6$ 为 root. 只需 check x^2+1 是否 irreducible

By Thm 4.19, x^2+1 irreducible 因为无 root.

Part 3.

Def: $g, h \in F[x]$ congment modulo f

或者 $g \equiv h \pmod f$

指 $f \mid g-h$.

$[g]_f$ 指所有 congment to g modulo f polynomial, 即所有和 g 相差任何 polynomial 个 f 的 polynomial

$\Rightarrow [g]_f = \{g + tf \mid t \in F[x]\}$

$(g(x) + t(x) f(x))$

这里不证其它了. 我们易证:

(1) modulo congment f 是个 equiv relation on F[x]

(2) $h \in [g]_f \Rightarrow [g]_f = [h]_f$ (显然的)

(3) 所有 equiv classes 要么 disjoint 要么 identical

(普遍的)

F. 固定 $f \in F[x]$, $\deg f > 0$

(1) Pf: 任何 congment class $[g]_f$, 其中一定存在 unique $h(x) \in F[x]$, 其 deg < deg f

这就像 $\mathbb{Z}_n$ 里的 0, 1, ..., n-1 congruent class 的基准

Existence: 由 division algo 保证.

($\deg s < \deg f \Rightarrow$ s 本身; $\deg g = \deg f \Rightarrow$ const; $\deg g > \deg f \Rightarrow$ remainder poly)

Denote 它为 r

Uniqueness: 因为 $\forall m \in [g]_f$, $m = r + kf$

只需确定 k = 1 时不行 (因为如果 k 是其他的 polynomial, 带入的, 就更远了)

$k = 1 \Rightarrow \deg m = \max(\deg r, \deg f)$

$= \deg f > \deg r$

$k = -1 \Rightarrow m = r - kf$, 仍是 $\deg f$ (主导) $> \deg r$

因为不可能有其他同 degree 的 polynomial 在 $[g]_f$ 中了. 这个 remainder poly 是 deg 最小的且唯一.

(2), (3) 此算练习: x^3+x 在 $\mathbb{Z}_2[x]$ 中有 congru classes

x^3+x 在 $\mathbb{Z}_3[x]$ 中有 congru classes

也就是找基准数 ⇒ 比它小的 polynomial

我们有4个位置

x^3 | x^2 x c

x^3: coeff 只能为0, by (1)

x^2 x c: coeff 可以为 0/1

$\therefore 2^3 = 8$ 个

同样, x^2 | x c

x^2: 0

x c: 0/1/2

$3^2 = 9$ 个

6. f 的 congru class 上的 ring structure

(1) 固定 f, ($\in F[x]$) $\deg > 0$.

$R = \{[g]_f \mid g \in F[x]\}$

(所有 f 的 congru classes)

定义: $[g]_f + [h]_f = [g+h]_f$

$[g]_f \cdot [h]_f = [gh]_f$ ⇒ well-def

$0_R = [0]_f$ 这是个 ring

$1_R = [1]_f$

(2) $R = \{[g]_{x^2} \mid \pi \in \mathbb{Z}_2[x]\}$ 有一个4个元素的 ring

isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ ⊗

$(0,0) \longleftrightarrow 0$ $(1,0) \longleftrightarrow 1+x$

$(1,1) \longleftrightarrow 1$ $(0,1) \longleftrightarrow x$.