(3) Division algorithm 知在field上 有用,因为只有field上对对division 有well-definedness.

Bitt' Ged of polynomiab)

(1)
$$2\chi^{2} - 10\chi + 12 = 2(\chi - 3) (\chi - 2)$$

 $\chi^{1} - 3\chi^{6} = \chi^{6}(\chi - 3)$ $)$ gcd = ($\chi - 3$)

(1) Pf of Remainder Thm; VLEF, f/(x-N \$ remainder \$ for

Pt - ièd division algo:

(2) If of factor Thm: (x-x) divides f (x-x) f(x)=0 By r >0 by (1) H f(x)=0 (x-x) f(x) -> f=a(x-x)+0 12f=e(x-x)+f(x)=0 12f=e(x-x)+f(x)=0

- (3) 1,2,3,4 \$12 Zs[N] + xt-1 60 wts.
 (plug in \$t to)
- (4) 使用 foctor thm 分解 Zs以中的 xs-x
- 米 Novt的概念: 一大 polynomial falls novt 就是当XERH / 如果fax = D, 双有哪些位 这个概念中不能限定在 R 中.

因为 Zs 一类只有5个元素 因而我们到以一个一个帮进去,发现;

217 $7^{5}-x = x(x^{4}-1)$, $4t\lambda x=0,1,2,3,4$ \Rightarrow By factor 7hm, $y^{5}-x = x(x-1)(x-1)(x-3)(x-4)$

(D) (D Thm 4.13) 如果一个poly fe FTX]

des =2基3, 则(f is irreducible)
(讲f.没有root.)

所以我们只需要证明如果 f没有rout,那么fireducible. (deg=2 or3)

可以证明其 contrapostive, 知果f reducible,那么一定在 not.

Let f = gh where gh ≠f, ≠ const. 那么这件事就很明显了: g, h 不是 const.那h degree 至少到1.因为 deg f 是土是3 所从 g,h 不能都 deg=2, 肯在有一个deg=1.

第3: 图为f是field → domain → depifi = depifi + depih). ア是gih 中有一ヶ是axtb ,那x x - 在一 注記一ケルセt. (2) 我们(V的pf只对 depf=2 or 3 成立 这显然的、我们够代码之 iff F=gh,其中从须有力del=1 which is ensured by depf=2/3 也蜱 dept 2% depg, degh 可以 both >27 所以破了 (3) H(x3-x) # Br (x) & bs factorization. 这处不多举、 我们发现一个事情:平方意公式对任何 rinp都成立 (a2-b2) = (a+b) (a-b) BB它只用了抖素的 t, X, distribution, ensued by def of ring 因而我们确认: x5-x= x(x4-1)=x(x2-1)(x2+1) = x(x-1)(x+1)(x+1) 所以我们确定 7-10,1,6 为 not. R需chak 7+1 25 irreducible By Thm 4.19, x2+1 irreducible BAFrout.

(1) modulo congruent f

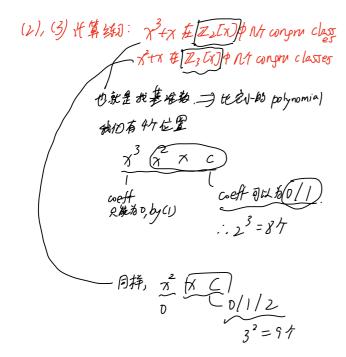
是大Cquiv relation on FCN

(2) 从ELGIF] [G] = [h] + (且然的)

(3) 所有equiv classes 要人的joint 要么identical

(套溢的)

F. BEFETIN, dest->0 (Uff: 146) augment class [5], #4 A [unique how exca), # deg < deg f Existence: A division algo fait. Un \$18 0,1,..., n-1 | dep g = degf =) anst congruent class by the deg g > deg f = remainder poly Denote & x Uniqueness: Bb Une Coly, my + kf 只需确定 K 二土(1987 GF) (1995 如果 K)是 越的 polynomial, 带物,就更远了) k=(=) deg m = max(degr, deg t) = def f > degr k=-1=) m=r-kf, 仍是degf(注3) 因为不可能在其他同degree的 polynomial A [3] + 93 Ex remainder poly 是deg最十的且唯一



G. f is congrue class this ring structure

(1) Bit f, deg > 0. $R = \{ [g]_f | g \in F(\pi) \}$ (At f is congrue class) $2 \times [g]_f + [h]_f = [g + h]_f$ $[g]_f = [g]_f = [g]_f = [g]_f$ $[g]_f = [g]_f = [g]_f = [g]_f$ (2) f =