

Lazard's Lemma. A : ring. F, G : formal gp / A

$$F \equiv G \pmod{\text{deg } n} \Rightarrow F \equiv G + T_n \pmod{\text{deg } n+1}$$

homog. pol. of deg n .

$$T_n = x_n X^n + x_{n-1} X^{n-1} Y + \dots + x_1 X Y^{n-1} + x_0 Y^n$$

$$F(x, y) = F(y, x) \Rightarrow x_i = x_{n-i}$$

$$F(x, 0) = x \Rightarrow x_0 = x_n = 0$$

$$F(x, y) = x + y + \square xy + \begin{cases} \square x^2 y \\ \square x y^2 \end{cases} + \begin{cases} \square x^3 y \\ \square x^2 y^2 \\ \square x y^3 \end{cases} + \begin{cases} \square x^4 y \\ \square x^3 y^2 \\ \square x^2 y^3 \\ \square x y^4 \end{cases} + \dots$$

Def: $B_n(x, y) := (x+y)^n - (x^n + y^n)$

Lemma 1 $B_n(x^p, y^p) \equiv B_{pn}(x, y) \pmod{\begin{cases} p & (\forall n \geq 1) \\ p^r & (n = p^r, r \geq 1) \end{cases}}$
 $\forall p$: prime.

$$\begin{aligned} \therefore B_n(x^p, y^p) &= (x^p + y^p)^n - (x^{pn} + y^{pn}) \\ &= [(x+y)^p - B_p(x, y)]^n - (x^{pn} + y^{pn}) \\ &= B_{pn}(x, y) - \sum_{i=1}^n \underbrace{\binom{n}{i}}_{\equiv 0 \pmod{p}} \underbrace{(-B_p(x, y))^i}_{\equiv 0 \pmod{p}} (x+y)^{p(n-i)} \end{aligned}$$

(always)

Def: $A_n(x, y) := \begin{cases} \frac{1}{p} B_n(x, y) & (n = p^r \text{ for } \exists p \text{ prime}) \\ B_n(x, y) & (\text{otherwise}) \end{cases}$
 $\in \mathbb{Z}[x, y]$

Lemma 2 $A_n \not\equiv 0 \pmod{p}$. ($\forall p$: prime).

$\therefore B_p \not\equiv 0 \pmod{p^2}$ (coeff. of $x^{p-1}y = p$) $\stackrel{\text{lem.}}{\Rightarrow} B_{p^r} \not\equiv 0 \pmod{p^2}$ ($\forall r \geq 1$) by lemma.

$B_m \not\equiv 0 \pmod{p}$ (coeff. of $x^{m-1}y = m$) $\stackrel{\text{lem.}}{\Rightarrow} B_{m \cdot p^r} \not\equiv 0 \pmod{p}$ ($\forall r \geq 1$). $A_{m \cdot p^r} = \frac{1}{m} B_{m \cdot p^r}$
 $m \pmod{p} \in \mathbb{F}_p^\times$

Lazard's Lemma. A : ring. F, G : formal gp / A .

\parallel $F \equiv G \pmod{\text{deg } n} \Rightarrow F \equiv G + \square \cdot A_n \pmod{\text{deg } n+1}$. ($\square \in A$)

pf. $F \equiv G + T_n \Rightarrow \begin{cases} T_n(x, y) = T_n(y, x) \\ \textcircled{*} \dots \{ T_n(x, y) + T_n(x+y, z) = T_n(x, y+z) + T_n(y, z) \end{cases}$

$\therefore F(F(x, y), z) \equiv G(G(x, y) + T_n(x, y), z) + T_n(F(x, y), z)$

\parallel $\equiv_{\text{mod deg } n+1} G(G(x, y), z) + T_n(x, y) + T_n(x+y, z)$

$F(x, F(y, z)) \equiv G(x, G(y, z)) + T_n(x, y+z) + T_n(y, z)$

Solve \otimes . $T_n(x, y) = \sum_{\substack{i, j > 0 \\ i+j=n}} x_{ij} x^i y^j$. ($x_{ij} = x_{ji}$).

LHS = $\sum_{i+j=n} x_{ij} x^i y^j + \sum x_{n-k, k} (x+y)^{n-k} z^k$
 $= \sum_{i+j=n} x_{ij} x^i y^j + \sum_{i+k=n} x_{ik} x^i z^k + \sum_{j+k=n} x_{jk} y^j z^k + \sum_{i+j+k=n} x_{(i+j), k} x^i y^j z^k$

RHS = $\dots + \sum_{i+j+k=n} x_{i, j+k} x^i y^j z^k$
 $\Rightarrow x_{(i+j), k} \binom{i+j}{i} = x_{i, j+k} \binom{j+k}{j}$

Set $x_i := x_{ij} \otimes \dots$ $\begin{cases} x_i = x_{n-i} \\ x_{i+j} \binom{i+j}{i} = x_i \binom{n-i}{j} \dots (1) \end{cases}$ ($1 \leq i \leq n-1$).
 homog. lin. eq. on x_1, \dots, x_{n-1} . $\Lambda_n := \mathbb{Z} \langle x_1, \dots, x_{n-1} \rangle$ free \mathbb{Z} -mod gen. by x_1, \dots, x_{n-1} .
 $\{ T_n \text{ satisfying } \otimes \} \cong \Lambda_n / (\text{homog. eq. } \otimes)$

$\{ \text{Solutions of } \otimes \text{ w/ } x_i \in A \} \cong \text{Hom}_{\mathbb{Z}\text{-mod}}(\Lambda_n, A)$.

$\bullet A = \mathbb{Q}$. set $i=1$. $(j+1)x_{j+1} = \binom{n-1}{j} x_1 \dots (2)$
 $\mathbb{Q} \xrightarrow{\sim} \text{Hom}(\Lambda_n, \mathbb{Q})$
 defining B_n : $x_{j+1} = \binom{n}{j+1} x_1 = \frac{1}{j+1} \cdot \binom{n-1}{j} \cdot n$

$T_n := A_n$ gives a solution in \mathbb{Z}
 $A_n : \Lambda_n \rightarrow \mathbb{Z}$
 $x_i \mapsto a_i$
 $A_n = \sum a_i x^i y^{n-i}$ (Lemma shows $A_n : \Lambda_n \rightarrow \mathbb{Z}$)
 $\Rightarrow \forall A. A \in \text{Hom}(\Lambda_n, A)$

$\bullet A = \mathbb{F}_p$. set $j=1$. $(i+1)x_{i+1} = (n-i)x_i \dots (3)$

$\bullet \phi \nmid n$ or $\phi = n \Rightarrow$ either $(i, \phi) = 1$ or $(n-i, \phi) = 1$
 $\downarrow (2)$ $x_i = \frac{1}{i} \binom{n-1}{i-1} x_1$ $\downarrow (3)$ $x_i = \frac{i+1}{n-i} x_{i+1} \stackrel{(2)}{=} \frac{1}{n-i} \binom{n-1}{i} x_1$

$\bullet n = \phi m, m > 1 \Rightarrow$ induction on n .

$(3) \Rightarrow \left[\begin{array}{l} \phi \nmid i \Rightarrow x_{i+1} = 0 \\ \phi \nmid i+1 \\ x_i = 0 \end{array} \right] \Rightarrow x_i = 0$ whenever $\phi \nmid i, i > \phi$
 $\Rightarrow x_i = 0 (\forall \phi \nmid i) (\because x_i = x_{n-i})$ ($n \geq 2\phi$)

$\therefore T_n(x, y) = T_m^0(x^\phi, y^\phi) = x \cdot A_m(x^\phi, y^\phi)$ by ind. hyp.
 (some T_m^0 satisfying \otimes) $= x u A_m$ by Lemma 1.
 ($u \in \mathbb{F}_p^*$)

$\mathbb{F}_p \xrightarrow{\sim} \text{Hom}(\Lambda_n, \mathbb{F}_p)$.

$\Lambda_n \cong \mathbb{Z}^m \oplus \bigoplus_i \mathbb{Z}/\phi_i^{m_i} \Rightarrow \Lambda_n \cong \mathbb{Z} \Rightarrow A_n : \Lambda_n \xrightarrow{\sim} \mathbb{Z}$
 $(\Rightarrow A \ni c \xrightarrow{\sim} c \cdot A_n \in \text{Hom}(\Lambda_n, A) \forall A.)$

O-Lazard's Lemma. $A : \mathcal{O}$ -alg. $\Sigma_1, \Sigma_2 : \text{formal } \mathcal{O}\text{-mod.} / A$
 $(\exists \delta \in \mathcal{O} \subset K. \mathcal{O} \neq \mathbb{F}_q).$ $(F_1, [\cdot]_1), (F_2, [\cdot]_2)$

$$\Sigma_1 \equiv \Sigma_2 \pmod{\text{deg } n} \Rightarrow \exists c \in A. \begin{cases} F_1 \equiv F_2 + c \cdot A_n^{\mathcal{O}} \\ [a]_1 \equiv [a]_2 + c \cdot a_n \cdot X^n \end{cases} \pmod{\text{deg } n+1}$$

(i.e. $F_1 \equiv F_2$
 $[a]_1 \equiv [a]_2 \quad \forall a \in \mathcal{O}$) $(\forall a \in \mathcal{O})$

$$A_n^{\mathcal{O}}(x, y) := \begin{cases} \frac{1}{\delta} B_n(x, y) & (n = q^r) \\ B_n(x, y) & (\text{otherwise}) \end{cases} \quad a_n := \begin{cases} \frac{1}{\delta} (a^n - a) & (n = q^r) \\ a^n - a & (\text{otherwise}) \end{cases}$$

$\mathcal{O}[x, y]$

$\phi^f. F_1 \equiv F_2 + T_n. [a]_1 \equiv [a]_2 + \gamma_a X^n \quad (\forall a \in \mathcal{O}).$

$$\begin{aligned} [a]_1 \circ F_1 &\equiv ([a]_2 + \gamma_a X^n) \circ (F_2 + T_n) \\ &\equiv [a]_2 \circ F_2 + a T_n + \gamma_a (x+y)^n \\ F_1 \circ [a]_1 &\equiv (F_2 + T_n) \circ ([a]_2 + \gamma_a X^n) \\ &\equiv F_2 \circ [a]_2 + (\gamma_a X^n + \gamma_a Y^n) + \underline{T_n(aX \cdot aY)} = a^n T_n. \end{aligned}$$

$\therefore \gamma_a \cdot B_n = (a^n - a) \cdot T_n$

$$\begin{aligned} [a+b]_1 &\equiv [a+b]_2 + \gamma_{a+b} X^n \\ [a]_1 +_{F_1} [b]_1 &\equiv ([a]_2 + \gamma_a X^n) +_{F_2} ([b]_2 + \gamma_b X^n) + T_n([a]_2 + \gamma_a X^n, [b]_2 + \gamma_b X^n) \\ &\equiv [a]_2 +_{F_2} [b]_2 + \gamma_a X^n + \gamma_b X^n + \underline{T_n(aX \cdot bX)} = T_n(a \cdot b) \cdot X^n \end{aligned}$$

$\therefore \gamma_{a+b} = \gamma_a + \gamma_b + T_n(a \cdot b)$

$$\begin{aligned} [ab]_1 &\equiv [ab]_2 + \gamma_{ab} X^n \\ [a]_1 \circ [b]_1 &\equiv ([a]_2 + \gamma_a X^n) \circ ([b]_2 + \gamma_b X^n) \\ &\equiv [a]_2 \circ [b]_2 + a \gamma_b X^n + \gamma_a (bX)^n \end{aligned}$$

$\therefore \gamma_{ab} = a \gamma_b + \gamma_a b^n. \quad [\text{in particular } \gamma_1 = 0].$

$(*)_{\mathcal{O}} : \begin{cases} \cdot T_n \text{ satisfies } (*) \\ \cdot \gamma_a B_n = (a^n - a) T_n \\ \cdot \gamma_{a+b} = \gamma_a + \gamma_b + T_n(a \cdot b) \\ \cdot \gamma_{ab} = a \gamma_b + b^n \gamma_a. \end{cases} \xrightarrow{\text{Lazard's Lemma}} \boxed{T_n = c \cdot A_n}$

$\begin{cases} (1) (a^n - a) \cdot c = \begin{cases} p \cdot \gamma_a & (n = p^r) \\ \gamma_a & (\text{otherwise}) \end{cases} \\ (2) \gamma_{a+b} = \gamma_a + \gamma_b + A_n(a \cdot b) \cdot c \\ (3) \gamma_{ab} = a \cdot \gamma_b + b^n \cdot \gamma_a. \end{cases}$

$\dots (*)_{\mathcal{O}} \quad (c \cdot \gamma_a \in A)$

$\boxed{\mathcal{O}\text{-linear homog. eqn on } c \cdot \gamma_a.}$

$A_n^{\mathcal{O}} := \mathcal{O} \langle c \cdot \gamma_a \rangle / (\text{homog. eq. } (*)_{\mathcal{O}})$ Solutions = $\text{Hom}_{\mathcal{O}\text{-mod}}(A_n^{\mathcal{O}}, A)$ in A

Need to show: $\mathcal{O} \cong A_n^{\mathcal{O}}$ and $A_n^{\mathcal{O}} = (A_n^{\mathcal{O}}, a_n) \xrightarrow{\cong} A \xrightarrow{\sim} \text{Hom}_{\mathcal{O}}(A_n^{\mathcal{O}}, A)$ for $\forall A$
 is isom. $\text{Hom}_{\mathcal{O}}(A_n^{\mathcal{O}}, \mathcal{O})$

Solution $A_n^{\mathcal{O}} := (A_n^{\mathcal{O}}; a_n) \in \text{Hom}_{\mathcal{O}}(\Lambda_n^{\mathcal{O}}, \mathcal{O})$

stated in the lemma :

- i) $n \neq p^r$ $B_n = u \cdot A_n$ ii) $n = p^r \neq q^s$ iii) $n = q^s$
- $\left\{ \begin{array}{l} c \mapsto u \in \mathcal{O}^{\times} \\ \gamma_a \mapsto (a^n - a) \cdot u \end{array} \right.$
 $\left\{ \begin{array}{l} c \mapsto p \\ \gamma_a \mapsto a^n - a \end{array} \right.$
 $\left\{ \begin{array}{l} c \mapsto p/\varpi \\ \gamma_a \mapsto (a^n - a)/\varpi \end{array} \right.$

It's easily checked that they are indeed solutions of $(*)_{\mathcal{O}}$. i.e. gives $A_n^{\mathcal{O}} \in \text{Hom}_{\mathcal{O}}(\Lambda_n^{\mathcal{O}}, \mathcal{O})$.

They are surjections $A_n^{\mathcal{O}} : \Lambda_n^{\mathcal{O}} \rightarrow \mathcal{O}$

because

- i) : $c \mapsto u \in \mathcal{O}^{\times}$
- ii) : $\gamma_a \mapsto a^n - a \in \mathcal{O}^{\times}$ for $\exists a \in \mathcal{O}$.
- iii) : $\gamma_{\bar{a}} \mapsto \bar{a}^n - \bar{a} \in \mathcal{O}^{\times}$

$\left[\begin{array}{l} \because \bar{a} := a \pmod{p} \in \mathbb{F}_q \\ \exists \bar{a} \in \mathbb{F}_q \text{ s.t.} \\ \bar{a} \neq \bar{a}' \Rightarrow a^n - a \notin p \\ (\because n \neq q^s) \end{array} \right]$

To show that $A_n^{\mathcal{O}}$ are isom. it's enough to show :

i) : $\Lambda_n^{\mathcal{O}} = \mathcal{O} \cdot c$ $\because \gamma_a = (a^n - a) \cdot c \quad (\forall a \in \mathcal{O})$. by ①. \lrcorner

ii) : $\Lambda_n^{\mathcal{O}} = \mathcal{O} \cdot \gamma_a$ $\because c = (a^n - a)^{-1} \cdot p \cdot \gamma_a$. by ①
 if $a^n - a \in \mathcal{O}^{\times}$. $\gamma_b = \frac{b^n - b}{a^n - a} \cdot \gamma_a \quad (\forall b \in \mathcal{O})$. \lrcorner

$\left[\begin{array}{l} \gamma_{ab} = a\gamma_b + b^n\gamma_a \\ = b\gamma_a + a^n\gamma_b \end{array} \right]$ by ③ \Rightarrow

iii) : $\Lambda_n^{\mathcal{O}} = \mathcal{O} \cdot \gamma_{\bar{a}}$. write $\bar{x} := x \pmod{\varpi}$ for $x \in \Lambda_n^{\mathcal{O}}$.

$\overline{\gamma_{\bar{a}a}} = \overline{a\gamma_{\bar{a}} + \bar{a}^n\gamma_a} = \bar{a}^n \cdot \bar{\gamma}_a \Rightarrow (\bar{a}^{n-1} - 1) \bar{a} \bar{\gamma}_a = 0$
 $= \overline{\bar{a}\gamma_a + a^n\gamma_{\bar{a}}} = \bar{a} \cdot \bar{\gamma}_a \Rightarrow \bar{a} \bar{\gamma}_a = \overline{\gamma_{\bar{a}a}} = 0 \quad (\forall a \in \mathcal{O})$

$\bar{\gamma}_p = 0$. but $\gamma_p = (p^n - 1) \cdot c$ by ②. $\Rightarrow \bar{c} = 0 \Rightarrow \overline{\gamma_{a+b}} = \bar{\gamma}_a + \bar{\gamma}_b$

$\Lambda_n^{\mathcal{O}} / \mathcal{O} \cdot \gamma_{\bar{a}} : k$ -vect. sp. gen. by $\bar{\gamma}_a \Rightarrow \bar{\gamma}_a$ depends only on $\bar{a} := a \pmod{p} \in k$

$\gamma_{ab} = \bar{a}\bar{\gamma}_b + \bar{b}^n\bar{\gamma}_a$

$= \bar{a}\bar{\gamma}_b + \bar{b}\bar{\gamma}_a \Rightarrow \bar{\gamma}_{a^m} = m \cdot \bar{a}^{m-1} \bar{\gamma}_a$

but $\bar{\gamma}_{a^m} = \bar{\gamma}_1 = 0$ for $m = q - 1$. $(\forall a \in k)$

$\Rightarrow \bar{\gamma}_a = 0 \quad (\forall a \in k)$. \parallel

In other words.

$k \ni \bar{a} \mapsto \bar{\gamma}_a \in \Lambda_n^{\mathcal{O}} / \mathcal{O} \cdot \gamma_{\bar{a}}$
 $\dots \mathbb{F}_p$ -derivation of k . but k/\mathbb{F}_p separable!!

Rem. F, G : formal gp. $F \equiv G \pmod{\text{deg } n}$. $\forall a \in \mathbb{N}$
 \Rightarrow by Lazard's lemma. $[a]_F \equiv [a]_G + c \cdot a_n X^n \pmod{\text{deg } n+1}$. $(F \equiv G + c \cdot A_n)$

$a_n := \begin{cases} p(a^n - a) & (n = p^r) \\ a^n - a & \text{otherwise} \end{cases}$
some p .