Further results for complete rings

Prop. A = complete ring wrt. ideal I.

$A[\![x]\!]$ = power series ring over A

$F(x) \in A[\![x]\!]$, $F(x) = \sum_{i \geq 0} f_i x^i$ s.t. $f_0 \in I$.

Then $\exists$ unique A-algebra homomorphism $\varphi : A[\![x]\!] \to A[\![x]\!]$ s.t. $\varphi(x) = F$.

If $f_0 = 0$, $f_1 \in A$ is a unit, then φ is an isomorphism, and $\varphi^{-1}(x)$ has no constant term.

pf Let $\alpha = \sum_{i \geq 0} a_i x^i \in A[\![x]\!]$.

Since $f_0 \in I$, coeff. of x^n in $F(x)^{n+i}$ for $i \geq 0$ belongs to I^i.

$\Rightarrow$ coeff. of x^n in $\sum_{i \geq 0} a_i F(x)^i$ is well-defined in A

Set $\varphi(\alpha) = \sum_{i \geq 0} a_i F(x)^i$ $\Rightarrow$ φ is A-algebra homomorphism

---

Now suppose $f_0 = 0$, $f_1 \in A$ is a unit, let $g_1 = \frac{1}{f_1}$.

Define coefficients $g_1, g_2, \ldots$ by induction.

Given $g_1, \ldots, g_{n-1}$, define

$$g_n = -\frac{1}{f_1} \sum_{i=2}^{n} f_i \, [x^n] \left(g_1 x + g_2 x^2 + \cdots + g_{n-1} x^{n-1}\right)^i$$

(take coeff. of x^n)

Define $G(x) = \sum_{n \geq 1} g_n x^n$ (note $g_0 = 0$)

The coeff. of x^n in $F(G(x))$ is

$$f_1 g_n + \sum_{i=2}^{n} f_i [x^n] G(x)^i$$

If $n=1$, get $f_1 g_1 = 1$

If $n>1$, then $[x^n] G(x)^i = [x^n](g_1 x + g_2 x^2 + \cdots + g_{n-1} x^{n-1})^i$

for $i \geq 2 \Rightarrow$ get 0 for $[x^n] f(G(x))$.

$\Rightarrow \varphi(G(x)) = x$.

By first part, $\exists$ unique $\Psi: A[[x]] \to A[[x]]$ s.t.

$\Psi(x) = G(x)$. $\Rightarrow \varphi(\Psi(x)) = \varphi(G(x)) = x$

$\Rightarrow \varphi \circ \Psi = id$

By work for second part, $\exists H(x)$ s.t. $\Psi(H(x)) = x$

$\Rightarrow \exists$ unique $\theta: A[[x]] \to A[[x]]$ s.t. $\theta(x) = H(x)$

$\Rightarrow \Psi(\theta(x)) = x \Rightarrow \Psi \circ \theta = id$

$\Rightarrow \Psi$ is isomorphism $\Rightarrow \varphi$ is isomorphism & $\varphi^{-1} = \Psi$. $\square$

Thm. (Hensel's lemma) Let A = complete ring w.r.t. ideal I.

Let $f(x) \in A[x]$ be polynomial, $f'(x)$ = derivative

Pick $a \in A$, set $e = f'(a)$, suppose that

$$f(a) \in e^2 I$$

Then $\exists b \in A$ s.t. $f(b) = 0$ and $b \equiv a \bmod eI$.

Pf. $\exists$ polynomial $h(x)$ s.t.

$$f(a+x) = f(a) + ex + h(x) x^2$$

$\exists$ A-algebra homomorphism $\varphi: A[\![x]\!] \to A[\![x]\!]$ s.t.

$\varphi(x) = x + x^2 h(ex)$ & φ is invertible.

By assumption, $\exists c \in I$ s.t. $f(a) = e^2 c$.

$\exists$ A-algebra homomorphism $\psi: A[\![x]\!] \to A[\![x]\!]$ s.t.

$\psi(x) = -c$

Define $b = a + e\psi(\varphi^{-1}(x))$ $\left[b \equiv a \pmod{eI} \right]$

$$
\begin{aligned}
f(b) &= f(a + e\psi(\varphi^{-1}(x))) \\
&= \psi(f(a + e\varphi^{-1}(x))) \\
&= \psi(f(a) + e^2\varphi^{-1}(x) + h(e\varphi^{-1}(x))(e\varphi^{-1}(x))^2) \\
&= f(a) + e^2\psi(\varphi^{-1}(x) + \varphi^{-1}(x)^2 h(e\varphi^{-1}(x))) \\
&= f(a) + e^2\psi(\varphi^{-1}(x + x^2 h(ex))) \\
&= f(a) + e^2\psi(x) \\
&= f(a) - e^2 c \\
&= 0.
\end{aligned}
$$

□

Squares in $\mathbb{Z}_p$ (p prime)

Case 1: $p \neq 2$.

Claim: Every square is of form $p^{2n}c$ where $c \notin (p)$ and $\bar{c} \in \mathbb{Z}_p/p \cong \mathbb{Z}/p$ is a square.

Sufficiency: let $\bar{a} \in \mathbb{Z}/p$ be s.t. $\bar{a}^2 = \bar{c}^2$.

Let $a \in \mathbb{Z}_p$ be preimage of $\bar{a}$.

Apply Hensel's lemma w/ $A = \mathbb{Z}_p$, $I = (p)$ and

$f(x) = x^2 - c$.

Note: $a \notin (p)$, so a is unit, and $f'(a) = 2a$ also unit.

$\Rightarrow f'(a)^2 I = (p)$

$f(a) = a^2 - c \equiv 0 \bmod p$, so $f(a) \in f'(a)^2 I$

Hensel $\Rightarrow \exists\, b$ s.t. $f(b) = 0$ ✓

Case 2: $p = 2$

Claim: Every square is of the form $4^n c$ where $c \equiv 1 \pmod 8$.

Suffiency: Use Hensel's lemma w/ $A = \mathbb{Z}_2$, $I = (2)$

$f(x) = x^2 - c$, $a = 1$.

$\Rightarrow f'(a) = 2 \Rightarrow f'(a)^2 I = (8)$

$f(1) = 1^2 - c \equiv 0 \pmod 8$

$\Rightarrow f(a) \in f'(a)^2 I \Rightarrow \exists\, b \in \mathbb{Z}_2$ s.t. $f(b) = 0$.

Squares in $k[[x]]$, k field.

Case 1: char $k \neq 2$

Claim: $\alpha = \sum_{n \geq 0} a_n x^n \neq 0$ is square $\iff \alpha = x^{2n} \beta$

where constant term of β is nonzero square in k

(similar to above)

Case 2: char $k = 2$

Note: $\left(\sum_{n \geq 0} c_n x^n\right)^2 = \sum_{n \geq 0} c_n^2 x^{2n}$

$\Rightarrow \quad \alpha = \sum_{n\geq 0} a_n x^n$ is a square

$\Leftrightarrow a_n = 0$ for n odd

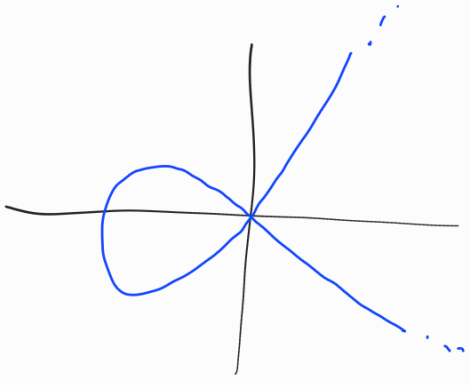
& a_n is a square in k for n even.

Ex. $A = \mathbb{C}[x,y]/(y^2 - x^2(x+1))$ domain.

By nullstellensatz, maximal ideals of A

$\leftrightarrow \{(a,b) \in \mathbb{C}^2 \mid b^2 = a^2(a+1)\}$

Real points:



In $\mathbb{C}[[x]]$, $x^2(x+1)$ is a square

$\Rightarrow y^2 - x^2(x+1)$ factors, so

$\mathbb{C}[[x,y]]/(y^2 - x^2(x+1))$ is not a domain.

[Completion need not preserve property of being a domain]

Thm. (Cohen structure theorem)

A = noeth. local ring, complete w.r.t maximal ideal m, let $k = A/m$.

(1) A is a quotient of a regular local ring.

(2) If A contains a field, then A is quotient of $k[[x_1, \dots x_n]]$ for some n.

(3) If A contains field, and A is a regular local ring, Then $A \cong k[[x_1, \ldots, x_n]]$ $(n = \dim A)$

Def. A (local) is equicharacteristic if it contains a field

(note: if $L \subset A$ is a field, $k = A/m$

then $L \to A \to k$ is injective

so $\operatorname{char} L = \operatorname{char} A = \operatorname{char} k$)

Def. A (local) is mixed characteristic if does not contain a field.

$\Rightarrow$ $\operatorname{char} A = 0$, $\operatorname{char} k > 0$.

[example: $A = \mathbb{Z}_p$]