§3. Picard–Vessiot extensions

Recall.

· algebra

K field, $f \in K[x]$ with $\deg(f) = n$

$\rightsquigarrow \#\{\alpha \in K \mid f(\alpha) = 0\} \leq n$

· ∂-algebra

F ∂-field, $A \in F^{n \times n}$ system of ∂-equations

$\rightsquigarrow \dim_{K_F} \mathrm{Sol}_F(A) \leq n$

In algebra, if f irreducible and separable, then we can construct a splitting field L/K which is minimal such that

$$\#\{\alpha \in L \mid f(\alpha) = 0\} = n.$$

We will now introduce the ∂-analog of splitting fields:

Definition 3.1. Let F ∂-field and let $A \in F^{n\times n}$.
A ∂-field extension E/F is a **Picard–Vessiot (PV) extension for A** if

(1) $\exists \quad Y \in GL(n,E) \ : \ \partial(Y) = A\cdot Y$

(2) $E = F(Y_{ij} \mid 1 \le i,j \le n)$

(3) $K_E = K_F$.

Example 3.2. To motivate (3) consider the ∂-field $F = K(t,x)$ with $\partial(t)=1$, $\partial(x)=x$, and consider the extension $E = F(y)$ with $\partial(y)=y$.
Then there is already a fundametal matrix for $A=(1)$ in F, namely (x). But still E/F satisfies (1) and (2) of Definition 3.1.
However, $K_E \supsetneq K_F$: indeed, $\partial(x^{-1}y) = 0$.
This phenomenon is a general one: superfluous solutions lead to new constants, so that condition (3) excludes such superfluous solutions.

We formalize the observation of Example 3.2 as follows:

Proposition 3.3. Let F ∂-field and let E/F PV extension for $A \in F^{n\times n}$. Suppose $F \subseteq M \subseteq E$ is an intermediate ∂-field such that there exists $Z \in GL(n, M)$ with $\partial(Z) = AZ$. Then $M = E$.

Proof. We differentiate the equation $Z \cdot Z^{-1} = I$ to obtain

$$\partial(Z) \cdot Z^{-1} + Z\,\partial(Z^{-1}) = 0$$

$$\Rightarrow \partial(Z^{-1}) = -Z^{-1}A.$$

Then, we compute (with $Y \in GL(n, E)$ fund. sol.)

$$\partial(Z^{-1}Y) = \partial(Z^{-1})\,Y + Z^{-1}\partial(Y)$$

$$= -Z^{-1}AY + Z^{-1}AY = 0$$

Thus, we have $C := Z^{-1}Y \in GL(n, K_E)$ and since $K_E = K_F$, further $C \in GL(n, F)$ and

$$Y = Z \cdot C$$

so that, by 3.1(2), we have $M = E$. $\square$

We will now address the existence and uniqueness of PV extensions. To this end, we need some preparation:

A ∂-ring R is called <u>∂-simple</u> if the only ∂-ideals in R are (0) and R.

Proposition 3.4. Let R be a ∂-simple ∂-ring with $\mathbb{Q} \subseteq R$. Then R is an integral domain.

<u>Proof</u>. Suppose there are nonzero $x, y \in R$ with $xy = 0$.

Then consider the ideal

$$I := \{ z \in R \mid \exists n \geq 1 : x^n z = 0 \}$$

For $z \in I$, with $x^n z = 0$, we have

$$0 = \partial(x^n z) = n x^{n-1} \partial(x) z + x^n \partial(z) \qquad | \cdot x$$

$$\rightsquigarrow x^{n+1} \partial(z) = 0 \qquad \Rightarrow \partial(z) \in I$$

$$\Rightarrow I \ \partial\text{-ideal}. \qquad 0 \neq y \in I \overset{\partial\text{-simple}}{\Longrightarrow} I = R$$

Thus $1 \in I$ and thus $\exists n \geq 1 : x^n = 0$, in other words, x is nilpotent.

Now let

$$\sqrt{0} := \{ z \in R \mid \exists n \geq 1 : z^n = 0 \} \trianglelefteq R$$

the ideal of nilpotents. Claim: $\sqrt{0}$ is ∂-ideal.

For $z \in \sqrt{0}$, we have $z^n = 0$.

$$\rightsquigarrow 0 = n z^{n-1} \partial(z) \overset{n \in R^\times}{\rightsquigarrow} z^{n-1} \partial(z) = 0 .$$

$$\overset{\partial(-)}{\rightsquigarrow} (n-1) z^{n-2} \partial(z)^2 + z^{n-1} \partial^2(z) = 0 \qquad \mid \cdot \partial(z)$$

$$\rightsquigarrow z^{n-2} \partial(z)^3 = 0$$

$$\left.\begin{matrix} \vdots \end{matrix}\right\} \text{ induction}$$

$$\rightsquigarrow \partial(z)^{2n-1} = 0 \qquad \Rightarrow \partial(z) \in \sqrt{0} .$$

Thus, the ideal $\sqrt{0}$ is ∂-ideal. But $1 \notin \sqrt{0}$ and thus, by ∂-simplicity: $\sqrt{0} = (0)$ ↯ $x \neq 0$.

$\Rightarrow$ R integral domain $\square$

Lemma 3.5. Let F ∂-field and R ∂-simple ∂-ring with $F \subseteq R$. We assume further

- $\mathrm{char}(F) = 0$
- K_F is algebraically closed.
- R is finitely generated as an F-algebra.

Then

$$K_{\mathrm{Quot}(R)} = K_F.$$

Proof. First note that, by Prop 3.4, R is an integral domain so that we may indeed form the field of fractions $\mathrm{Quot}(R) =: E$.

Let $x \in K_E$. Consider the ideal

$$I := \{ r \in R \mid xr \in R \} \trianglelefteq R$$

We have, for $r \in R$, $\partial(xr) = x\,\partial(r)$ so that $r \in I \Rightarrow \partial(r) \in I$. So I ∂-ideal $\Rightarrow I = R$.

$\Rightarrow K_E \subseteq R$.

Now suppose $x \notin K_F$. We will lead this to a contradiction.

Then, for every $c \in K_F$, consider the ideal

$$R(x-c) \trianglelefteq R.$$

Since $x-c$ is constant, this is a ∂-ideal so that $R(x-c) = R \Rightarrow \boxed{x - c \in R^\times}$.

Since $x \notin K_F$ and K_F is algebraically closed, we further have that x is not algebraic $/ K_F$.
Then by HW2.2, x can also not be algebraic $/ F$.
Therefore x is transcendental $/ F$.

<u>Notation</u> For elements $r_1, r_2, \ldots \in R$, we will denote by $F\langle r_1, r_2, \ldots\rangle \subseteq R$ the smallest subring of R containing F and $r_1, r_2, \ldots$.

Since R is finitely generated as an F-algebra, there exist elements $x_1 = x, x_2, \ldots, x_m \in R$ with

$$F\langle x_1, x_2, \ldots, x_m\rangle = R$$

and

1. $x_1, \dots, x_r$ algebraically independet / F
2. $x_{r+1}, \dots, x_m$ algebraic / $F(x_1, \dots, x_r)$.

So in particular, we have $E / F(x_1, \dots, x_r)$ is algebraic. Choose a primitive element $y \in R$ of $E/F(x_1, \dots, x_r)$. Multiplying by the denominators of the coefficients of the minimal polynomial of y over $F(x_1, \dots, x_r)$ we obtain

$$\sum_{i=0}^{n} h_i(x_1, \dots, x_r)\, y^i = 0 \qquad (*)$$

with $h_i(x_1, \dots, x_r) \in F[x_1, \dots, x_r]$.

We then choose $h \in F[x_1, \dots, x_r]$ such that

1. $h_n(x_1, \dots, x_r) \mid h$
2. $\forall r+1 \le j \le n : x_j \in F\langle x_1, \dots, x_r, y, h^{-1}\rangle$

(to achieve 2. we multiply, if necessary, h by the denominators of the coefficients in the expressions

$$x_j = \sum_{i=0}^{n-1} \underbrace{r_{i,j}(x_1, \dots, x_r)}_{\in F(x_1, \dots, x_r)} y^i$$

We thus have

$$R \subseteq F\langle x_1, \dots, x_r, y, h^{-1}\rangle \subseteq E.$$

Now, since $h \in F[x_1, \dots, x_n]$ is a nonzero polynomial, we may (!) find $c_1, \dots, c_r \in K_F$ such that

$$h(c_1, \dots, c_r) \neq 0$$

(To show this, we use that a polynomial in a single variable only has finitely many zeros, that K_F has infinitely many elements, and proceed by induction on r).

We further denote the splitting field of the polynomial

$$g(T) := \sum_{i=0}^{n} h_i(c_1, \dots, c_r)\, T^i \in F[T]$$

by L/F and let $\alpha \in L$ be a root of $g(T)$.

In this context, we may (!) define a "specialization homomorphism":

$$
\begin{aligned}
\varphi : F\langle x_1, x_2, \dots, x_r, y, h^{-1}\rangle &\longrightarrow L \\
x_i &\longmapsto c_i \\
y &\longmapsto \alpha \\
h^{-1} &\longmapsto h^{-1}(c_1, \dots, c_r) \quad (\neq 0)
\end{aligned}
$$

ring homomorphism with $\varphi \neq 0$, and

$$x_1 - c_1 \in \mathrm{Ker}(\varphi).$$

But this contradicts that $\lightning$

$$x_1 - c_1 \in R^\times \subseteq F\langle x_1, \dots, x_r, y, h^{-1}\rangle \quad \square$$

We will now use the above key insights on ∂-simplicity to construct PV extension via an intermediate construction of PV rings.

Definition 3.6 Let F ∂-field with K_F alg. closed and of char. 0, and $A \in F^{n\times n}$. A ∂-ring R with $F \subseteq R$ is called a Picard-Vessiot (PV) ring for A if

(1) R is ∂-simple.

(2) $\exists\ Y \in GL(n, R) : \partial(Y) = AY$

(3) $R = F\langle Y_{ij}, \det(Y)^{-1} \mid 1 \leq i,j \leq n \rangle$.

Remark 3.7 It is immediate from Prop 3.4 and Lemma 3.5 that the field of fractions of a PV ring for $A \in F^{n\times n}$ is a PV extension for A.