Existence of a Picard-Vessiot extension

Jerald Kovacic
The City College of CUNY
jkovacic@verizon.net
http:/mysite.verizon.net/jkovacic

November 3, 2006

Throughout, K is an ordinary Δ-field of characteristic 0. We let $C = K^{\Delta}$.

We could start with a finite dimensional Δ-K-vector space V. Then we want a Δ-extension field L such that $L \otimes_K V$ has a basis of horizontal vectors. If B is the defining matrix of V relative to some basis, then we want a Δ-field L and $\alpha \in \mathrm{GL}(n, L)$ with

$$\alpha' + B\alpha = 0.$$

Or we could start with

$$L(y) = y^{(n)} - a_{n-1}y^{(n-1)} - \cdots - a_0 y = 0.$$

Then we want a fundamental system $\eta_1, \ldots, \eta_n$ of solutions in some Δ-extension field L of K. In this case, the Wronskian matrix

$$W = W(\eta_1, \ldots, \eta_n) = \begin{pmatrix} \eta_1 & \cdots & \eta_n \\ \eta_1' & \cdots & \eta_n' \\ \vdots & & \vdots \\ \eta_1^{(n-1)} & \cdots & \eta_n^{(n-1)} \end{pmatrix}$$

is invertible and satisfies

$$W' = AW$$

where

$$A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ a_0 & \cdots\cdots & & a_{n-1} \end{pmatrix}$$

is a companion matrix.

In both cases we have a first-order matrix Δ-equation

$$Y' = AY, \qquad A \in \mathrm{Mat}(n, K),$$

and we look for a Δ-extension field L of K and $\alpha \in \mathrm{GL}(n, L)$ with

$$\alpha' = A\alpha.$$

Choose a matrix of n^2 Δ-indeterminates over K

$$Y = (y_{ij}).$$

We denote by Y' the result of differentiating each entry of Y,

$$Y' = (y'_{ij}).$$

Consider the Δ-ideal

$$\mathfrak{a} = [Y' - AY]$$

i.e.

$$\mathfrak{a} = \left[y'_{ij} - \sum_{k=1}^{n} A_{ik} y_{kj}\right].$$

If $\mathfrak{p} \subset K\{Y\}$ is a prime Δ-ideal and $\mathfrak{a} \subset \mathfrak{p}$ then we have

$$\pi \colon K\{Y\} \to K\{Y\}/\mathfrak{p} \subset \mathrm{qf}(K\{Y\}/\mathfrak{p}) = L.$$

Let $\alpha = \pi(Y)$, then $\alpha' = A\alpha$.

Of course we want to do this so that α is invertible, i.e. $\det Y \notin \mathfrak{p}$. And, for Picard-Vessiot theory, we want $L^\Delta = K^\Delta = C$.

Lemma 1. *Let $\mathfrak{a} \subset K\{Y\}$ be the Δ-ideal generated by the entries of $Y' - AY$. Then no power of $\det Y$ is in $\mathfrak{a}$.*

Proof. Suppose, on the contrary, that $(\det Y)^e \in \mathfrak{a}$. Then

$$(\det Y)^e = \sum_{i,j=1}^{n} \sum_{k=0}^{d} P_{ijk} \Big(y'_{ij} - \sum_{l=1}^{n} A_{il} y_{lj} \Big)^{(k)},$$

where $P_{ijk} \in K\{Y\}$. We write this symbolically as

$$(\det Y)^e = \sum_{k=0}^{d} P_k \cdot (Y' - AY)^{(k)}.$$

Choose d minimal, so that there is a d-th derivative of some entry of $Y' - AY$ that appears with a non-zero coefficient on the right hand side. Think of this as an equation in the indeterminates $Y, Y', Y'', \ldots$, *not* as a Δ-polynomial.

Observe that

$$(Y' - AY)^{(d)} = Y^{(d+1)} - M$$

where M is a polynomial in the y_{ij} and their derivatives of order no higher than d. Substitute

$$Y^{(d+1)} \mapsto M.$$

The left hand side does not change, since it has order 0 and the right hand side gets shorter; i.e. d decreases. But this is a contradiction since we had chosen d minimal. $\square$

Using Zorn's Lemma we can find a radical Δ-ideal that contains $\mathfrak{a}$ and is maximal with respect to the condition that it not contain $\det Y$. (See the Δ-ring theory notes on the web, Corollary 1.10.7, p. 23.) But it is easier to pass to the ring of fractions

$$S = K\{Y, \tfrac{1}{\det Y}\}.$$

Proposition 2. *Let $A \in \mathrm{Mat}(n, K)$. Then there is a Δ-extension field L of K and $\alpha \in \mathrm{GL}(n, L)$ such that $\alpha' = A\alpha$.*

Proof. The ideal $\mathfrak{b} = S\mathfrak{a}$ is proper and therefore (by Zorn's Lemma) is contained in a maximal Δ-ideal $\mathfrak{p}$, which is prime (Adam proved this). Let

$$\pi\colon S \to S/\mathfrak{p} \subset \mathrm{qf}(S) = L, \qquad \alpha = \pi(Y).$$

Then

$$\alpha' = A\alpha.$$

Also $\det Y \notin \mathfrak{p}$ so $\det \alpha \neq 0$. □

We do not have uniqueness. In fact any prime Δ-ideal that contains $\mathfrak{b}$ will work in the above proof. We might want to choose $\mathfrak{p}$ minimal, but that is not a good choice.

Example 3. Consider the ordinary Δ-field

$$K = \mathbb{C}(e^x).$$

and the linear homogeneous Δ-equation

$$L(y) = y' - y = 0.$$

The matrix equation is

$$Y' = Y$$

(1 by 1 matrices). Then

$$\mathfrak{a} = [y' - y]$$

is prime and so is

$$\mathfrak{p} = \mathfrak{b} = [y' - y] \subset K\{y, \tfrac{1}{y}\}.$$

Note that $\alpha \notin K$ since every element of $\mathfrak{a}$ has order at least 1. Also

$$\alpha' = \alpha$$

so $\alpha = ke^x$ where k is a constant *not* in $\mathbb{C}$.

Another possibility is to choose $\mathfrak{p}$ as large as possible, i.e. maximal.

Proposition 4. *The following conditions are equivalent.*

1. $\mathfrak{p}$ *is a maximal* Δ*-ideal.*
2. $R = K[\alpha, \frac{1}{\det \alpha}] = K[\alpha, \alpha^{-1}]$ *is* Δ*-simple.*
3. L^{Δ} *is algebraic over* C*.*

Proof. $1 \iff 2$ is immediate. $2 \implies 3$ is Proposition 6 and $3 \implies 2$ is Proposition 8, both of which will be proved shortly. □

Later, to simplify the theory, we shall assume that C is algebraically closed. In that case the third condition becomes

3' L has no new constants, i.e. $L^{\Delta} = C$.

Lemma 5. *Let L be a Δ-extension field of K. If $c \in L^{\Delta}$ is algebraic over K, then it is algebraic over C.*

Proof. Let $c \in L^{\Delta}$ be algebraic over K with

$$P = X^d + P_{d-1}X^{d-1} + \cdots + P_0 \in K[X]$$

being the minimal monic polynomial for c. Then, because c is a constant,

$$0 = (P(c))' = P'_{d-1}c^{d-1} + \cdots + P'_0.$$

The minimality of d implies that $P'_i = 0$, i.e. c is algebraic over C. $\square$

Proposition 6. *Suppose that R is a finitely generated (not finitely Δ-generated) K-algebra that Δ-simple. Then R is a domain and $\mathrm{qf}(R)^\Delta$ is algebraic over K^Δ.*

Proof. Since (0) is a maximal Δ-ideal, it is prime, hence R is a domain. Let $c \in \mathrm{qf}(R)^\Delta$ and define the "set of denominators"

$$\mathfrak{a} = \{b \in R \mid bc \in R\}.$$

Then $\mathfrak{a}$ is a non-zero ideal and a Δ-ideal since c is a constant. Because R is Δ-simple, $1 \in \mathfrak{a}$ and $c \in R^\Delta$.

We have shown that

$$\mathrm{qf}(R)^\Delta \subset R^\Delta \subset \mathrm{qf}(R)^\Delta,$$

and therefore $\mathrm{qf}(R)^\Delta = R^\Delta$. Because the left hand side is a field, so is the right.

By the lemma, it suffices to prove that $c \in R^\Delta$ is algebraic over K. Suppose not. We use (a weak form of) the Chevalley Extension Theorem (Bourbaki, Commutative Algebra, Chapter V, Section 3.2, Corrollary 3, page 348). Let K_a be an algebraic closure of K. Since R is finitely generated over K, there exists a polynomial $P \in K[c]$ such that any homomorphism

$$\phi\colon K[c] \to K_a,$$

with $\phi(P) \neq 0$, extends to a homomorphism of R into K_a. Choose $d \in C$ with $P(d) \neq 0$. Let

$$\phi\colon K[c] \to K_a, \qquad c \mapsto d$$

be the substitution homomorphism. Now, $c-d \in R^\Delta$ and therefore is either 0 or else invertible in R^Δ. But it cannot be invertible since $\phi(c-d) = 0$. Therefore $c = d \in K^\Delta$, which contradicts the assumption that c is transcendental over K. □

This proposition proves $2 \Longrightarrow 3$ of Proposition 4.

Next we prove $3 \Longrightarrow 2$ of Proposition 4. But first we need some notation and a lemma from commutative algebra. If A is any K-algebra that is a domain, we denote the transcendence degree of $\mathrm{qf}(A)$ over K by

$$\mathrm{tr.\,deg.}\, A/K = \mathrm{tr.\,deg.}\, \mathrm{qf}(A)/K.$$

Lemma 7. *Suppose that A is a K-algebra which is a domain, and B is a K-homomorphic image of A. Then*

$$\text{tr. deg. } B/K \leq \text{tr. deg. } A/K.$$

Assume that $\text{tr. deg. } A/K$ *is finite. Then*

$$\text{tr. deg. } B/K = \text{tr. deg. } A/K$$

if and only if A is isomorphic to B.

Proof. Zariski-Samuel, Commutative Algebra, Vol. 1, Theorems 28 and 29, p. 101. □

Be careful. This proposition requires that the mapping

$$\phi\colon A \to B$$

be surjective. For example

$$\phi\colon \mathbb{C}[x] \mapsto \mathbb{C}[x], \qquad x \mapsto x^2$$

is not an isomorphism even though the transcendence degrees are the same.

Proposition 8. *Let* $R = K[\alpha, \alpha^{-1}]$*, where*

$$\alpha' = A\alpha.$$

If $\mathrm{qf}(R)^\Delta$ *is algebraic over* C *then* R *is* Δ*-simple.*

Proof. We let $L = \mathrm{qf}(R) = K(\alpha)$ and $C = K^\Delta$. By hypothesis L^Δ is algebraic over C.

Let $\mathfrak{a} \subset R$ be a proper Δ-ideal. We need to show that $\mathfrak{a} = (0)$. Choose a maximal Δ-ideal $\mathfrak{m}$ of $L \otimes_K R/\mathfrak{a}$ and set

$$S = (L \otimes_K R/\mathfrak{a})/\mathfrak{m}.$$

We have Δ-homomorphisms of rings

$$\begin{aligned} &\phi\colon L \to L \otimes_K R \to L \otimes_K R/\mathfrak{a} \to S, \qquad \text{and} \\ &\psi\colon R \to L \otimes_K R \to L \otimes_K R/\mathfrak{a} \to S. \end{aligned}$$

We identify K with its image, so that $K \subset S$. Since L is a field, ϕ is injective. We identify L with its image, so that $\phi = \mathrm{id}$.

Note that α (really $\phi(\alpha)$) and $\psi(\alpha)$ are both solutions of

$$Y' = AY.$$

Therefore there is a constant matrix $c \in \mathrm{GL}(n, \mathrm{qf}(S)^\Delta)$ with

$$\alpha = \psi(\alpha)c.$$

Because $\mathfrak{m}$ is a maximal Δ-ideal, S is Δ-simple. It is also finitely generated over L. So $\mathrm{qf}(S)^\Delta$ is algebraic over L^Δ and therefore over C. Hence c is a matrix whose entries are algebraic over C.

We have

$$L = K(\alpha) \subset K(\psi(\alpha), c),$$

Hence

$$\begin{aligned} \mathrm{tr.deg.}\, R/K &= \mathrm{tr.deg.}\, L/K \le \mathrm{tr.deg.}\, K(\psi(\alpha), c)/K \\ &= \mathrm{tr.deg.}\, K(\psi(\alpha))/K = \mathrm{tr.deg.}\, \psi(R)/K. \end{aligned}$$

By the lemma, ψ is injective. But $\mathfrak{a} \subset \ker \psi$ hence $\mathfrak{a} = (0)$. □

Definition 9. (Standard definition.) Let $A \in \mathrm{Mat}(n, K)$. Then L is a Picard-Vessiot extension of K for A if

1. $L^{\Delta} = C$,
2. there exists $\alpha \in \mathrm{GL}(n, L)$ such that $\alpha' = A\alpha$,
3. $L = K(\alpha)$.

Theorem 10. *Suppose that C is algebraically closed and let $A \in \mathrm{Mat}(n, K)$. The there exists a Δ-extension field L over K which is a Picard-Vessiot extension of K for A.*

We will see later, by example, that a Picard-Vessiot extension need not exist in the case that C is not algebraically closed.

Definition 11. (Churchill definition.) Let V be a finite dimensional Δ-K-vector space. Then L is a Picard-Vessiot extension of K for V if

1. $L^{\Delta} = C$,
2. $L \otimes_K V$ has a basis of horizontal vectors.
3. If M is a Δ-extension field of K that satisfies conditions (1) and (2) then there is a Δ-embedding

$$\phi \colon L \to M.$$

If B is the defining matrix of V relative to some basis, then the second condition is equivalent to the second condition of the standard definition (where $A = -B$). Churchill proved this as Proposition 9.2.

Proposition 12. *Suppose that C is algebraically closed. Then the Churchill definition is equivalent to the standard definition.*

Proof. Assume that L satisfies the conditions of the Churchill definition. Churchill has proved (Proposition 9.3) that $L = K(\alpha)$, which is the condition of the standard definition.

Now assume that L satisfies the standard definition. We set

$$R = K[\alpha, \alpha^{-1}]$$

and

$$S = (M \otimes_K R)/\mathfrak{m}$$

where $\mathfrak{m} \subset M \otimes_K R$ is a maximal Δ-ideal. Because S is finitely generated over (the image of) M, S is Δ-simple and $\mathrm{qf}(S)^\Delta = M^\Delta = C$. (Here is where we used the assumption that C is algebraically closed.)

Let

$$\phi\colon M \to S, \qquad \psi\colon R \to S$$

be the canonical mappings of Δ-rings. ϕ is injective since M is a field and ψ is injective since R is Δ-simple. We extend ψ to a Δ-embedding

$$\chi\colon L \to \mathrm{qf}(S)$$

By assumption, there exists $\beta \in \mathrm{GL}(n, M)$ with

$$\beta' = A\beta.$$

Then there exists $c \in \mathrm{GL}(n, C)$ such that

$$\psi(\alpha) = \phi(\beta)c.$$

Therefore

$$\phi(M) = K(\phi(\beta)) = K(\psi(\alpha)) = \chi(L),$$

and

$$\phi^{-1} \circ \chi\colon L \to M$$

is a Δ-embedding. □

Proposition 13. *Suppose that C is algebraically closed. Then any two Picard-Vessiot extensions of K for A are Δ-isomorphic.*

Proof. If L and M are Picard-Vessiot extensions then the previous proposition shows that there are Δ-embeddings $\phi\colon L \to M$ and $\psi\colon M \to L$. The composition

$$\psi \circ \phi\colon L \to L$$

is an automorphism of L (Churchill's Proposition 9.3. Hence ϕ and ψ are isomorphisms. $\square$

Example 14. (A. Seidenberg, Contribution to the Picard-Vessiot theory of homogeneous linear differential equations, Amer. J. Math, **78** (1956), 808–817.) Let

$$K = \mathbb{R}\langle i \sin 2x \rangle.$$

Using Seidenberg's notation, we set

$$a = \frac{i}{2} \sin 2x.$$

Then

1. $a' = i \cos 2x$,
2. $a'' = -4a$,
3. $a'^2 = -4a^2 - 1$.

Thus

$$K = \mathbb{R}(a)[a'],$$

where a is transcendental over $\mathbb{R}$ and a' is algebraic of degree 2 over $\mathbb{R}(a)$.

We first claim that $C = K^\Delta = \mathbb{R}$. Suppose that

$$c = A + Ba' \in C,$$

where $A, B \in k(a)$. Then

$$\begin{aligned} 0 = c' &= \frac{dA}{da}\, a' + \frac{dB}{da}\, a'^2 + B\, a'' \\ &= \frac{dA}{da}\, a' - (4a^2 + 1)\frac{dB}{da} - 4aB. \end{aligned}$$

Therefore $dA/da = 0$ so $A \in \mathbb{R}$, and

$$(4a^2 + 1)\frac{dB}{da} + aB = 0.$$

Assume that $B \neq 0$ and write

$$B = (4a^2 + 1)^r \frac{C}{D}$$

where $r \in \mathbb{Z}$ and $C, D \in \mathbb{R}[a]$ are not divisible by (the irreducible polynomial) $4a^2+1$. From the equation above we have

$$(4a^2+1)\left(r(4a^2+1)^{r-1}8a\frac{C}{D}+(4a^2+1)^r\frac{D\frac{dC}{da}-C\frac{dD}{da}}{D^2}\right)+$$
$$a(4a^2+1)^r\frac{C}{D}=0,$$

or

$$(4a^2+1)\left(D\frac{dC}{da}-C\frac{dD}{da}\right)+a(1+8r)CD=0.$$

But this contradicts the condition that a^2+1 does not divide C or D. Therefore $B=0$ and $c=A\in\mathbb{R}$.

We next claim that any solution η of the differential equation

$$y''+y=0$$

introduces new constants. In fact, we claim more. If

$$u=\frac{\eta'}{\eta},$$

then we claim that

$$K\langle u\rangle^{\Delta}\neq\mathbb{R}.$$

It is easy to see that

$$u'=-1-u^2.$$

If $1+u^2=0$ then $u=\pm i$ which is a new constant. So we may assume that $1+u^2\neq 0$. Let

$$c=\frac{a+a'u-au^2}{1+u^2}.$$

Then

$$\begin{aligned}c'&=\frac{(1+u^2)\big(a'+a''u+a'u'-a'u^2-2auu'\big)-(a+a'u-au^2)2uu'}{(1+u^2)^2}\\&=\frac{a'-4au-a'(1+u^2)-a'^2u+2au(1+u^2)+2u(a+a'u-au^2)}{1+u^2}\\&=0.\end{aligned}$$

If $c \notin \mathbb{R}$ then c is a new constant, so we assume that $c \in \mathbb{R}$. The formula

$$c = \frac{a + a'u - au^2}{1 + u^2}$$

implies that

$$(c + a)u^2 - a'u + (c - a) = 0.$$

Using the quadratic formula we get

$$u = \frac{a' \pm \sqrt{a'^2 - 4(c + a)(c - a)}}{2(c + a)}.$$

This implies that

$$\sqrt{a'^2 - 4(c^2 - a^2)} = \sqrt{-1 - 4c^2} = i\sqrt{1 + 4c^2} \in k\langle u \rangle.$$

Since $\sqrt{1 + 4c^2} \in \mathbb{R}$, we have $i \in K\langle u \rangle$, which is a new constant.

In general we may find a Δ-extension field whose constants are algebraic over C, even a normal (Galois) extension. M. P. Epstein, On the theory of Picard-Vessiot extensions, Amer. J. Math. **62** (1955) 528–547, developed a Picard-Vessiot theory for this case however was unable to get a bijection between all intermediate Δ-fields and (certain) subgroups of the Galois group. His approach appears to have been dropped.

E. R. Kolchin, Differential algebra and algebraic groups, Chapter VII, also develops the theory without assuming that C is algebraically closed. He makes use of a universal Δ-field.

The "correct" way to do it is to define the Galois group as a representable functor from the category of C-algebras to groups.

Definition 15. The Galois group is

$$\mathrm{Gal} = \mathrm{Gal}(L/K) = \mathrm{Aut}^{\Delta}(L/K).$$

It is the group of all Δ-automorphisms of L over K.

If $\sigma \in \mathrm{Gal}$ then

$$(\sigma\alpha)' = \sigma(\alpha') = \sigma(A\alpha) = A\sigma(\alpha).$$

Churchill proved that there exists $c(\sigma) \in \mathrm{GL}(n, C)$ with

$$\sigma\alpha = \alpha c(\sigma).$$

Indeed

$$\begin{aligned} c(\sigma)' &= (\alpha^{-1}\sigma\alpha)' = -\alpha^{-1}\alpha'\alpha^{-1}\sigma\alpha + \alpha^{-1}(\sigma\alpha)' \\ &= -\alpha^{-1}A\sigma\alpha + \alpha^{-1}A\sigma\alpha \\ &= 0 \end{aligned}$$

Proposition 16. *The mapping*

$$c\colon\ \mathrm{Gal}(L/K) \to \mathrm{GL}(n, C), \qquad c(\sigma) = \alpha^{-1}\sigma\alpha,$$

is an injective homomorphism of groups (in the category of sets).

Proof. Let $\sigma, \tau \in \mathrm{Gal}(L/K)$. Then

$$\begin{aligned} c(\sigma\tau) &= \alpha^{-1}\sigma\tau\alpha \\ &= \alpha^{-1}\sigma\alpha \cdot \sigma\alpha^{-1}\sigma\tau\alpha \\ &= c(\sigma)\sigma(c(\tau) \\ &= c(\sigma)c(\tau) \end{aligned}$$

because $c(\tau) \in \mathrm{GL}(n, C)$ and $\sigma \,|\, C = \mathrm{id}$.

If $c(\sigma) = 1$ then $\sigma\alpha = \alpha$. Because $L = K(\alpha)$, $\sigma = \mathrm{id}$. □

Note that the mapping $c\colon\ \mathrm{Gal} \to \mathrm{GL}(n, C)$ depends on α. If A is fixed and also

$$L = K(\beta), \qquad \text{where } \beta' = A\beta,$$

then there exists $c \in \mathrm{GL}(n, C)$ with

$$\beta = \alpha c.$$

Therefore

$$c_\beta(\sigma) = \beta^{-1}\sigma\beta = c^{-1}\alpha^{-1}\sigma(\alpha c) = c^{-1}c_\alpha(\sigma)c,$$

i.e. $c_\beta(\mathrm{Gal})$ is conjugate to $c_\alpha(\mathrm{Gal})$.

Definition 17. The ring of constants of $L \otimes_K L$ is denoted by

$$D = D(L/K) = (L \otimes_K L)^{\Delta}.$$

D is not necessarily a domain, however it is reduced. It turns out that there is a canonical bijection

$$\mathrm{Gal} \approx \max \operatorname{spec} D.$$

Proposition 18. *Let $P = K[\alpha, \alpha^{-1}]$. Then*

$$D = (L \otimes_K P)^{\Delta} = (P \otimes_K P)^{\Delta}.$$

Proof. Let $d \in D$ and define the "set of denominators"

$$\mathfrak{a} = \{a \in P \mid (1 \otimes a)d \in L \otimes P\}.$$

$\mathfrak{a}$ is clearly an ideal and is a Δ-ideal since d is constant:

$$(1 \otimes a')d = \big((1 \otimes a)d\big)'.$$

But P is Δ-simple and $\mathfrak{a} \neq (0)$ so $1 \in \mathfrak{a}$ and

$$d \in (L \otimes_K P)^{\Delta}.$$

The second equality is similar. □

Suppose that $A, B \in \mathrm{Mat}(n, P)$. We define

$$A \otimes B \in \mathrm{Mat}(n, P \otimes_K P)$$

by the formula

$$(A \otimes B)_{ij} = \sum_{k=1}^{n} A_{ik} \otimes B_{kj}.$$

Another way of writing this is

$$A \otimes B = \begin{pmatrix} A_{11} \otimes 1 & \dots & A_{1n} \otimes 1 \\ \vdots & & \vdots \\ A_{n1} \otimes 1 & \dots & A_{nn} \otimes 1 \end{pmatrix} \begin{pmatrix} 1 \otimes B_{11} & \dots & 1 \otimes B_{1n} \\ \vdots & & \vdots \\ 1 \otimes B_{n1} & \dots & 1 \otimes B_{nn} \end{pmatrix}$$

We denote the identity matrix of $\mathrm{Mat}(n, P)$ by I.

Proposition 19. *Let $A, B \in \mathrm{Mat}(n, P)$. Then*

1. $(A \otimes I)(B \otimes I) = AB \otimes I$,
2. $(A \otimes I)(I \otimes B) = A \otimes B$,
3. $(A \otimes I)_{rs} = A_{rs} \otimes 1$,
4. $(A \otimes B)' = A' \otimes B + A \otimes B'$
5. $\det(A \otimes B) = \det A \otimes \det B$.

Proof. For the first formula we compute

$$\begin{aligned} ((A \otimes I)(B \otimes I))_{rs} &= \sum_i (A \otimes I)_{ri}(B \otimes I)_{is} = \sum_{ijk} (A_{rj} \otimes I_{ji})(B_{ik} \otimes I_{ks}) \\ &= \sum_{ijk} A_{rj}B_{ik} \otimes I_{ji}I_{ks} = \sum_i A_{ri}B_{is} \otimes 1 \\ &= (AB)_{rs} \otimes 1 = \sum_l (AB)_{ri} \otimes I_{is} \\ &= (AB \otimes I)_{rs}. \end{aligned}$$

The second and third formulas are proven similarly. The fourth follows immediately from the second and the last from the second and third. □

However

$$(I \otimes B)(A \otimes I) \neq A \otimes B.$$

The correct formula is

$$(1 \otimes B)(1 \otimes A) = (A^t \otimes B^t)^t.$$

Note that $A \otimes B$ is invertible if both A and B are, however

$$(A \otimes B)^{-1} \neq A^{-1} \otimes B^{-1}.$$

The correct formula is

$$(A \otimes B)^{-1} = \left((A^t)^{-1} \otimes (B^t)^{-1}\right)^t.$$

Definition 20. Define $\gamma = \alpha^{-1} \otimes \alpha \in P \otimes P$.

Proposition 21. *γ and γ^{-1} are constants, i.e. are elements of D.*

Proof. We compute

$$\begin{aligned}\gamma' &= -\alpha^{-1}\alpha'\alpha^{-1} \otimes \alpha + \alpha^{-1} \otimes \alpha' \\ &= -\alpha^{-1}A \otimes \alpha + \alpha^{-1} \otimes A\alpha \\ &= 0.\end{aligned}$$

It follows that $\det \gamma$ is a constant and so is $\frac{1}{\det \gamma} \in D$. □

Proposition 22. $P \otimes_K P = (P \otimes_K 1)[\gamma, \gamma^{-1}]$.

Proof. Note that

$$\begin{aligned} 1 \otimes \alpha &= (\alpha \otimes 1)(\alpha^{-1} \otimes 1)(1 \otimes \alpha) \\ &= (\alpha \otimes 1)(\alpha^{-1} \otimes \alpha) \\ &= (\alpha \otimes 1)\gamma. \end{aligned}$$

Also

$$1 = (1 \otimes \alpha)(1 \otimes \alpha^{-1}) = (\alpha \otimes 1)\gamma(1 \otimes \alpha^{-1}),$$

hence

$$1 \otimes \alpha^{-1} = \gamma^{-1}(\alpha^{-1} \otimes 1).$$

Therefore

$$1 \otimes_K P \subset (P \otimes_K 1)[\gamma, \gamma^{-1}],$$

and

$$P \otimes_K P \subset (P \otimes_K 1)[\gamma, \gamma^{-1}] \subset P \otimes_K P.$$

□

Proposition 23. *Let A be a Δ-ring containing a Δ-field M. Then M and A^Δ are linearly disjoint over M^Δ, i.e. if $a_1, \ldots, a_r \in M$ are linearly dependent over A^Δ then they are linearly dependent over M^Δ.*

Proof. We want to use the Wronskian condition however we need to be careful since A is not necessarily a domain.

Suppose that

$$\sum_{i=1}^{r} a_i d_i = 0, \qquad (a_i \in M, d_i \in A^\Delta),$$

where $d_r \neq 0$. Then, for each $k \geq 0$,

$$\sum_{i=1}^{r} a_i^{(k)} d_i = 0.$$

In the matrix

$$\begin{pmatrix} a_1 & \ldots & a_{r-1} & d_r a_r \\ \vdots & & \vdots & \vdots \\ a_1^{(r-1)} & \ldots & a_{r-1}^{(r-1)} & d_r a_r^{(r-1)} \end{pmatrix}$$

the last column is a linear combination of the preceding columns. Therefore the determinant is 0:

$$0 = d_r \det \begin{pmatrix} a_1 & \ldots & a_r \\ \vdots & & \vdots \\ a_1^{(r-1)} & \ldots & a_r^{(r-1)} \end{pmatrix} = d_r w,$$

where w is the Wronskian determinant of $a_1, \ldots, a_r$.

However $w \in M$, which is a field. If $w \neq 0$ then it is invertible so $d_r = 0$ which contradicts the hypotheses. Hence $w = 0$. Now we can use the Wronskian condition in the field M and conclude that $a_1, \ldots, a_r$ are linearly dependent over C, which contradicts the hypotheses. □

Corollary 24. *With the notation of the proposition, the mapping of Δ-C-algebras*

$$M \otimes_C A^\Delta \to A, \qquad a \otimes c \mapsto ac,$$

is injective.

Proof. Suppose that

$$x = \sum_{i=1}^{r} a_i \otimes d_i$$

is in the kernel. We may suppose that $a_1, \ldots, a_r$ are linearly independent over C. But $\sum_{i=1}^{r} a_i d_i = 0$ so $a_1, \ldots, a_r$ are linearly dependent over A^{Δ}. By the proposition they are linearly dependent over C, which contradicts the hypotheses. □

Proposition 25. $D = C[\gamma, \gamma^{-1}]$.

Proof. We know that $C[\gamma, \gamma^{-1}] \subset D$. And we also have, by Proposition 22,

$$P \otimes_K P = (P \otimes_K 1)[\gamma, \gamma^{-1}] \subset (P \otimes_K 1)[D] \subset P \otimes_K P,$$

so $D \subset (P \otimes_K 1)[\gamma, \gamma^{-1}] \subset (L \otimes_K 1)[\gamma, \gamma^{-1}]$.

If $d \in D$ we have

$$d = \sum_{i=1}^{r} (a_i \otimes 1)c_i,$$

where $a_i \in L$ and $c_i \in C[\gamma, \gamma^{-1}]$. We may assume that $c_1, \ldots, c_r$ are linearly independent over C and therefore, by Proposition 23, over $L \otimes_K 1$. But

$$0 = d' = \sum_{i=1}^{r} (a_i' \otimes 1)c_i$$

so $a_i' = 0$, $a_i \in C$, and

$$d = \sum_{i=1}^{r} a_i c_i \in C[\gamma, \gamma^{-1}].$$

□

Proposition 26. *The mapping of Δ-rings (actually Δ–P-algebras)*

$$P \otimes_C D \to P \otimes_K P, \qquad a \otimes_C d \mapsto (a \otimes_K 1)d$$

is bijective.

Proof. Evidently the image is $(P \otimes_K 1)[D]$ which equals $P \otimes_K P$ by the proposition. The mapping is injective by Corollary 24. □

Definition 27. Let $\sigma \in \mathrm{Gal}(L/K)$. Then we define

$$\overline{\sigma} \colon P \otimes_K P \to P$$

by

$$\overline{\sigma}(a \otimes b) = a\sigma b.$$

and

$$\mathfrak{p}_\sigma = \ker \overline{\sigma}.$$

Proposition 28. $\mathfrak{p}_\sigma$ *is a maximal* Δ*-ideal of* $P \otimes_K P$*.*

Proof. The image of $\mathfrak{o}\sigma$ is a Δ-simple ring. □

Proposition 29. *Let $\mathfrak{p} \subset P \otimes_K P$ be a maximal Δ-ideal. Then there is a unique $\sigma \in \mathrm{Gal}$ with $\mathfrak{p} = \mathfrak{p}_\sigma$.*

Proof. Let

$$S = (P \otimes_K P)/\mathfrak{p}.$$

As before define

$$\begin{aligned} j_1 &\colon P \to P \otimes_K P, \qquad j_1(a) = a \otimes 1 \\ j_2 &\colon P \to P \otimes_K P, \qquad j_1(a) = 1 \otimes a \\ \pi &\colon P \otimes_K P \to S \end{aligned}$$

As before the image of $\pi \circ j_1$ equals the image of $\pi \circ j_2$ so we define $\sigma \colon P \to P$ by

$$\sigma = (\pi \circ j_1)^{-1} \circ (\pi \circ j_2).$$

Since σ is injective it extends to an injective Δ-homomorphism $L \to L$ which must be surjective. I.e. $\sigma \in \mathrm{Gal}$. Also

$$(\pi \circ j_1)(\overline{\sigma}(a \otimes b)) = \pi(j_2(a\sigma b)) = \pi(j_2(a))\pi(j_1(b)) = \pi(a \otimes b).$$

Since $\pi \circ j_1$ is injective,

$$\mathfrak{p}_\sigma = \ker \overline{\sigma} = \ker \pi = \mathfrak{p}.$$

Suppose that $\mathfrak{p} = \mathfrak{p}_\sigma = \mathfrak{p}_\tau$. Let $a \in P$. Then

$$\sigma a \otimes 1 - 1 \otimes a \in \mathfrak{p}_\sigma$$

so

$$0 = \overline{\tau}(\sigma a \otimes 1 - 1 \otimes a) = \sigma a - \tau a.$$

Therefore $\sigma = \tau$. □

Proposition 30. $\mathrm{Gal}(L/K)$ *is canonically isomorphic (as a set) to* $\max \mathrm{diffspec}(P \otimes_K P)$.

If R is a Δ-ring we denote the set of all Δ-ideals of R by $\mathfrak{I}(R)$. Note that $\mathfrak{I}(D)$ is the set of all ideals of D since every ideal of D is a Δ-ideal.

Proposition 31. *The the mappings (of sets ordered by inclusion)*

$$\Phi\colon \mathfrak{I}(D) \to \mathfrak{I}(R \otimes_C D) \quad \textit{where} \quad \Phi(\mathfrak{a}) = R \otimes_C \mathfrak{a}$$

and

$$\Psi\colon \mathfrak{I}(R \otimes_C D) \to \mathfrak{I}(D) \quad \textit{where} \quad \Psi(\mathfrak{b}) = \{\, d \in D \mid 1 \otimes d \in \mathfrak{b} \,\}.$$

are bijective and inverse to each other.

Proof. Evidently $\mathfrak{a} \subset \Psi(\Phi(\mathfrak{a})) = \Psi(R \otimes_C \mathfrak{a})$. Choose a basis Λ of $\mathfrak{a}$ over C and extend it to a basis M of D over C. Then $R \otimes_C D$ is a free R-module with basis $1 \otimes_C \mathrm{M}$. Let $d \in \Psi(\Phi(\mathfrak{a}))$, so $1 \otimes d \in R \otimes_C \mathfrak{a}$. Therefore

$$1 \otimes d = \sum_{\lambda \in \Lambda} r_\lambda \otimes \lambda \qquad (r_\lambda \in R).$$

But $d \in D$, so

$$1 \otimes d = \sum_{\mu \in \mathrm{M}} 1 \otimes c_\mu \mu \qquad (c_\mu \in C).$$

Comparing coefficients, we see that $c_\mu = 0$ for $\mu \notin \Lambda$, and $r_\lambda = c_\lambda$; thus $d \in \mathfrak{a}$.

It is also clear that $\Phi(\Psi(\mathfrak{b})) = R \otimes_C \Psi(\mathfrak{b}) \subset \mathfrak{b}$. Suppose they are unequal. As above, choose a vector space basis Λ of $\Psi(\mathfrak{b})$ over C and extend it to a basis M of D over C. Among elements $a \in \mathfrak{b}$, $a \notin R \otimes_C \Psi(\mathfrak{b})$, choose one whose representation in the form

$$a = \sum_{\mu \in M} r_\mu \otimes \mu \qquad (r_\mu \in R)$$

has fewest non-zero terms. Say that $r_{\mu_0} \neq 0$. Then

$$(r_{\mu_0} \otimes 1)a' - (r'_{\mu_0} \otimes 1)a = \sum_{\mu \neq \mu_0} \left(r_{\mu_0} r'_\mu - r'_{\mu_0} r_\mu\right) \otimes \mu$$

has fewer terms, so

$$r_{\mu_0} r'_\mu - r'_{\mu_0} r_\mu = 0$$

for every $\mu \in \mathrm{M}$. This means that

$$\frac{r_\mu}{r_{\mu_0}}$$

is a constant in $\mathrm{qf}(R)$, and therefore, by hypothesis, in C. Let

$$c_\mu = \frac{r_\mu}{r_{\mu_0}} \in C\,.$$

If

$$b = \sum_{\mu \in \mathrm{M}} c_\mu \mu \in D$$

then

$$a = \sum_{\mu \in \mathrm{M}} c_\mu r_{\mu_0} \otimes \mu = r_{\mu_0} \otimes b.$$

Because R is Δ-simple, the radical Δ-ideal $\{r_{\mu_0}\}$ cannot be proper. Therefore

$$1 \otimes 1 \in \{r_{\mu_0} \otimes 1\} \subset R \otimes_C D\,.$$

But this implies (by, for example, Kaplansky, Lemma 1.6, page 12) that

$$1 \otimes b \in \{r_{\mu_0} \otimes 1\}\{1 \otimes b\} = \{(r_{\mu_0} \otimes 1)(1 \otimes b)\} = \{a\} \subset \mathfrak{b}\,.$$

This implies that $b \in \Psi(\mathfrak{b})$ and

$$a \in R \otimes_C \Psi(\mathfrak{b})\,,$$

which is a contradiction. □

Proposition 32. *The mappings Φ and Ψ of the proposition are bijective when restricted to maximal Δ-ideals.*

Putting Proposition 30 and Proposition 32 together we get

$$\mathrm{Gal} \approx \max \mathrm{diffspec}(\mathcal{P} \otimes_K P) \approx \max \mathrm{diffspec}(P \otimes_C D) \approx \max \mathrm{spec}\, D.$$