Ample 3 = An Example to Dan's Talk

Wulf-Dieter Geyer (Erlangen)

GTEM Summer School
Geometry and Arithmetic around Galois Theory
Galatasaray University, Istanbul, June 8–19, 2009

Dan Haran gave in his talk (Ample 2) an axiomatic method, called **algebraic patching**, how to realize a group G[1] over a field K once one has realized certain subgroups G_i of G which generate G, more precisely, once there is given a patching datum

$$\mathcal{E} = (E, F_i, P_i, P; G_i, G)_{i\in I}$$

on which a group Γ operates, with certain properties.

This talk shall fill this abstract theorem with life presenting a crucial example, due to Haran, Völklein and Jarden, where the field E is a rational function field over a field K which is complete under a nonarchimedean absolute value.[2]

The talk splits into four parts: The first one is a warm up for the second part, where we construct the large fields P_i and P in $\mathcal{E}$. The third part constructs the fields F_i, galois with groups G_i over E. The last part gather all information to construct the patching datum $\mathcal{E}$ and verify all the necessary properties.

page

[1] or more generally to solve a split embedding problem $\Gamma \ltimes G \twoheadrightarrow \Gamma = \mathrm{Gal}(E|E_0)$

[2] and E_0 rational over a complete subfield K_0 of K.

1. Convergent Power Series

Let K be a field with a nontrivial complete ultrametric absolute value

$$| \ | : \ K \to \mathbb{R}_{\geq 0} \quad .$$

The unit circle $\mathfrak{E} = \{x \in K \, ; \ |x| \leq 1\}$ is the valuation ring of K and the open unit circle $\mathfrak{E}^\circ = \{x \in K \, ; \ |x| < 1\}$ is its maximal ideal. The residue field $\mathfrak{E}/\mathfrak{E}^\circ$ is denoted by $\overline{K}$, the residue map is $x \mapsto \overline{x}$.

Definition: A power series

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \in K[[z]]$$

is called **convergent** (on the unit circle $\mathfrak{E}$ in K), if

$$\lim_{n \to \infty} |a_n| = 0 \quad .$$

Then there is for each $c \in \mathfrak{E}$ a convergent **evaluation**

$$\varphi_c(f) := f(c) = \sum_{n=0}^{\infty} a_n c^n \in K \quad .$$

We call

$$|f| \ := \ \max_n |a_n|$$

the **norm** of f. For $c \in \mathfrak{E}$ we have

$$|f(c)| \leq |f| \quad .$$

The **Weierstrass degree** of a convergent power series f is the nonnegative integer

$$\deg^+(f) \ := \ \max\{n \in \mathbb{N}_0 \, ; \ |f| = |a_n|\} \quad .$$

If $|f| = 1$, then $\overline{f}$, the coefficientwise reduction of the convergent power series f, is a polynomial in $\overline{K}[z]$ of degree $\deg^+(f)$.

Proposition 1.1: *The convergent power series in $K[[z]]$ form a subring $K\{z\}$. The norm on $K\{z\}$ is an absolute value which continues the absolute value of K such that the residue $\overline{z}$ of z is transcendental over $\overline{K}$. The ring $K\{z\}$ is complete under* *this norm, it is the completion of the polynomial ring $K[z]$, provided with the functional extension of the absolute value of K. The Weierstrass degree is additive:*

$$\deg^+(f \cdot g) = \deg^+(f) + \deg^+(g) \qquad \textit{for } f, g \in K\{z\} \setminus \{0\}.$$

The units of $K\{z\}$ are exactly the power series of Weierstrass degree zero. ∎

The euclidean algorithm extends from $K[z]$ to $K\{z\}$:

Division with Remainder (Weierstrass): *Let $f, g \in K\{z\}$ with $g \neq 0$ and $\deg^+ g = d$. Then there are unique elements $q \in K\{z\}$ and $r \in K[z]$ with*

$$f = q \cdot g + r \quad , \quad \deg r < d \quad .$$

These elements satisfy the inequalities

$$|q| \cdot |g| \leq |f| \qquad |r| \leq |f| \quad .$$ ∎

This shows that $K\{z\}$ is a principal ideal domain. Moreover an important consequence of the division is the

Weierstrass' Preparation Theorem: *Let $0 \neq f \in K\{z\}$ with $\deg^+ f = d$. Then there is a unit $u \in K\{z\}^\times$ and a monic polynomial $g \in K[z]$ of degree d with*

$$f = u \cdot g \quad , \quad |g| = 1 \quad .$$

Proof: Divide z^d by f to get

$$z^d = q \cdot f + r \quad , \quad \deg r < d \ , \ |r| \leq 1 \quad .$$

Then $g = z^d - r$ is the wanted polynomial and $u = q$ is a unit because of $\deg^+ q = 0$. ∎

Definition: A power series $f = \sum_n a_n z^n \in K[[z]]$ is called **$\star$-convergent** (convergent somewhere in the stars), if it satisfies one of the following equivalent conditions:

1. There is a $c \in K^\times$ such that

$$f(c) = \sum_n a_n c^n \qquad \text{converges in } K \ .$$

2. There is an $\alpha \in K^\times$ such that

$$f(\alpha z) \in K\{z\} \quad .$$

3. There is $N \in \mathbb{N}$ such that

$$|a_n| \leq N^n \qquad \text{for all } \ n \geq 1\,.$$

The condition 3. gives the definition of a $\star$-convergent series in $K((z))$.

Proposition 1.2 (Cauchy): *The $\star$-convergent power series in $K[[z]]$ resp. $K((z))$ form a ring $K[[z]]_\star$ resp. a field $K((z))_\star$.*

The field $K((z))_\star$ is algebraically closed in $K((z))$.

Addendum (Kuhlmann-Roquette): *The field extension $K((z))|K((z))_\star$ is regular.* ∎

2. Convergent Mittag-Leffler Series

Preliminary remark: Recall the following special case of a **theorem of Mittag-Leffler**: Let $c_1, \ldots, c_e \in \mathbb{C}$. If $f : \mathbb{P}_1(\mathbb{C}) \setminus \{c_1, \ldots, c_e\} \to \mathbb{C}$ is a holomorphic function, then f can be written in a unique way as

$$f(z) = a_0 + \sum_{i=1}^{e} f_i(z) \quad , \quad f_i(z) = \sum_{j=1}^{\infty} \frac{a_{ij}}{(z-c_i)^j}$$

with $a_0, a_{ij} \in \mathbb{C}$, where the **principal parts** f_i of f at the singularities c_i converge in $\mathbb{P}_1(\mathbb{C}) \setminus \{c_i\}$.

We will now introduce a nonarchimedean analogue of this result. Let K be as above, let $E = K(z)$ be the rational function field, let $I = \{1, \ldots, e\}$ be a finite nonempty index set and $(c_i)_{i \in I}$ be a finite set of elements in $\mathfrak{C}$ and assume

$$|c_i - c_j| = 1 \qquad (i \neq j).$$

We put

$$w_i = \frac{1}{z - c_i} \in E \qquad (i \in I).$$

Remark: In the application to patching the situation $|c_i - c_j| < 1$ can occur. There are two solutions in this case:

1. Reduce to the case $|c_i - c_j| = 1$. This is the solution in this talk.
2. Consider the case $|c_i - c_j| < 1$ seriously. Then the function in (1)

$$\|f\| := \max\{|a_0|,\, |a_{in}|\,;\ i \in I,\ n \in \mathbb{N}\}$$

is not an absolute value but only a K-norm. To get the submultiplicativity $\|fg\| \leq \|f\| \cdot \|g\|$, we have to choose an $r \in K^{\times}$ with $|r| \leq |c_i - c_j|$ and put

$$w_i = \frac{r}{z - c_i} \qquad (i \in I).$$

Then all assertions go through with similar reasoning.

Let $R_I^{\circ} \subseteq E$ be the ring of rational functions over K with poles at most in $c_1, \ldots, c_e$. Then $R_I^{\circ} = R[w_i \, ; \; i \in I]$, by the decomposition into fractional parts each $f \in R_I^{\circ}$ has a unique representation

$$f = a_0 + \sum_{i \in I} \sum_{n \geq 1} a_{in} w_i^n \qquad (a_{in} \in K, \; = 0 \;\text{ if }\; n \gg 0).$$

Proposition 2.1: *The elements w_i/w_j are units in R_I°. If $f \in K[w_i]$ is a polynomial of degree d in w_i, then $(\frac{w_j}{w_i})^d f \in K[w_j]$ is a polynomial of degree $\leq d$ in w_j. The functional extension of the absolute value of K to E satisfies*

$$(1) \qquad f = a_0 + \sum_{i \in I} \sum_{n \geq 1} a_{in} w_i^n \quad \Longrightarrow \quad |f| = \max_{i,n}(|a_0|, |a_{in}|) \quad . \qquad ∎$$

Definition-Proposition 2.2: The completion of the ring R_I° with respect to the absolute value is a subring R_I of $\widehat{E}$, which we call the **ring of convergent Mittag-Leffler series**, convergent on the complement

$$C_I \;:=\; \mathbb{P}_1 \setminus \bigcup_{i \in I} (c_i + \mathfrak{C}^{\circ})$$

of e open disjoint discs. Each element $f \in R_I$ has a unique representation

$$f = a_0 + \sum_{i \in I} \sum_{n \geq 1} a_{in} w_i^n$$

with

$$a_0, a_{in} \in K \quad \text{ and } \quad \lim_{n \to \infty} |a_{in}| = 0 \;\text{ for }\; i \in I$$

and the evaluation $f(c)$ converges for $c \in C_I$. The norm on R_I is again given by (1). ∎

The Weierstrass Preparation Theorem for convergent power series in one variable has in our situation the following consequence:

Weierstrass Preparation Theorem for Mittag-Leffler Series: *Let* $0 \neq f \in R_I$ *and* $i \in I$. *Then there are representations*

$$f = p_i \cdot u_i \qquad \textit{with} \quad u_i \in R_I^\times\ , \quad p_i \in K[w_i]$$

where p_i *is monic and* $|p_i| = 1$.

So R_I is again a principal ideal domain and

$$Q_I = \mathrm{Quot}(R_I) = (K[w_i] \setminus \{0\})^{-1} \cdot R_I \quad .$$

Basic idea of proof for the Preparation Theorem: Start with $f = a_0 + \sum_i f_i(w_i) \in R_I$ and assume $|I| > 1$. By the Preparation theorem from chapter 1 transform $f_e(w_e)$ into a polynomial in $K[w_e]$ and by the shift in proposition 2.1 eliminate w_e. This do, until only one variable is left. ∎

Remark: In contrast to chapter 1 here the decomposition need not be unique, even if we fix $i \in I$. E.g.

$$w_i + \frac{1}{c_i - c_j} = \frac{1}{c_i - c_j} \cdot \frac{w_i}{w_j}$$

is a monic polynomial of norm 1 in $K[w_i]$ and a unit in R_I.

Proposition 2.3: *For each* $J \subseteq I$ *we can form in the same way rings* R_J *and fields* Q_J. *For* $J = \varnothing$ *we have* $R_\varnothing = K$ *and we put* $Q_\varnothing = E$. *Then for* $J, J' \subseteq I$

$$R_J \cap R_{J'} = R_{J \cap J'} \qquad , \qquad Q_J \cap Q_{J'} = Q_{J \cap J'} \quad .$$

The first equation is obvious, the second one can be reduced to it with some work, distinguishing the cases $J \cap J' \neq \varnothing$ resp. $= \varnothing$. ∎

At the end of this chapter we study Cartan's lemma which says that in special cases for a field $K = K_1 K_2 \neq K_1, K_2$ the equality

$$\mathrm{GL}_n(K) = \mathrm{GL}_n(K_1) \cdot \mathrm{GL}_n(K_2)$$

holds. Taking determinants (or $n = 1$) this means especially

$$K^\times = K_1^\times \cdot K_2^\times$$

which is impossible for many fields like number fields or function fields.

A situation where this is possible is given by fields which are quotient fields of completely normed rings of a special type.

Definition: A (nontrivial ultrametric) **norm** on a ring A is a function

$$\| \ \| : \ A \to \mathbb{R}_{\geq 0} \quad ,$$

which has at least one value ε with $0 < \varepsilon < 1$, such that for all $a, b \in A$:

$$\begin{aligned} \|a\| = 0 \quad &\Longrightarrow \quad a = 0 \\ \|a + b\| &\leq \max(\|a\|, \|b\|) \\ \|a \cdot b\| &\leq \|a\| \cdot \|b\| \\ \|1\| &= 1 \quad . \end{aligned}$$

Cartan's Lemma: *Let A be a completely normed ring which can be decomposed*

$$A = A^+ + A^-$$

into a sum of two completely normed subrings, such that each $a \in A$ has a representation

$$a = a^+ + a^- \qquad \text{with} \quad a^+ \in A^+ \, , \ a^- \in A^-$$

and

$$\|a^+\| \leq \|a\| \quad , \quad \|a^-\| \leq \|a\| \quad .$$

Then every 1-unit $b \in A^\times$, i.e. $\|b - 1\| < 1$, has a decomposition

$$b = b_+ \cdot b_- \qquad \text{with} \ \ b_\pm \in A^\pm \ , \quad \|1 - b_\pm\| < 1 \quad .$$

Proof: Put $a_1 = b - 1$. Define recursively a sequence (a_j) in A by

$$1 + a_{j+1} = (1 - a_j^+)(1 + a_j)(1 - a_j^-)$$

Then the products

$$(1 - a_1^-) \cdots (1 - a_j^-) \ \in (A^-)^\times$$

resp.

$$(1 - a_j^+) \cdots (1 - a_1^+) \ \in (A^+)^\times$$

converge against p_- resp. p_+ in A^- resp. A^+ with $|1 - p_\pm| < 1$. Therefore $b_\pm = p_\pm^{-1}$ gives the decomposition $b = b_+ \cdot b_-$. ∎

Corollary: *Let $A = A_+ + A_-$ be as in the lemma and let A_0 be a dense subring with quotient field E_0. Then*

$$\mathrm{GL}_n(A) \subseteq \mathrm{GL}_n(A^+) \cdot \mathrm{GL}_n(A^-) \cdot \mathrm{GL}_n(E_0) \quad .$$

Proof: The norm on A induces a complete norm on $\mathrm{M}_n(A)$ by

$$\|(a_{ij})\| = \max_{i,j} \|a_{ij}\|$$

and $\mathrm{M}_n(A) = \mathrm{M}_n(A_+) + \mathrm{M}_n(A_-)$ satisfies with A the requisites of Cartan's lemma. Let $b \in \mathrm{GL}_n(A)$. Since A_0 is dense in A, there is $a \in \mathrm{M}_n(A_0)$ with $\|b^{-1} - a\| < \|b\|^{-1}$. Then

$$\|1 - ba\| \leq \|b\| \cdot \|b^{-1} - a\| < 1 \quad ,$$

so ba is a 1-unit in $\mathrm{GL}_n(A)$. By Cartan's Lemma we have a decomposition

$$ba = b_+ b_- \qquad \text{with} \qquad b_+ \in \mathrm{GL}_n(A^+),\ b_- \in \mathrm{GL}_n(A^-) \quad .$$

From $\det a \neq 0$ follows $a \in \mathrm{GL}_n(E_0)$. This gives the claimed decomposition

$$b = b_+ \cdot b_- \cdot a^{-1} \ \in\ \mathrm{GL}_n(A^+)\,\mathrm{GL}_n(A^-)\,\mathrm{GL}_n(E_0) \quad . \qquad ∎$$

Proposition 2.4: *We use the notations of the last proposition, so R_I is a ring of convergent Mittag-Leffler series. Let $I = J \uplus J'$ be a decomposition of I into nonempty subsets J and J'. Let $b \in \mathrm{GL}_n(R_I)$. Then there is a decomposition*

$$b = b_1 \cdot b_2$$

with

$$b_1 \in \mathrm{GL}_n(R_J) \quad , \quad b_2 \in \mathrm{GL}_n(Q_{J'}) \quad . \qquad ∎$$

Remark: The stronger equation

$$\mathrm{GL}_n(R_J) \cdot \mathrm{GL}_n(R_{J'}) = \mathrm{GL}_n(R_I)$$

does not hold, because $R_J^\times \cdot R_{J'}^\times \neq R_I^\times$: The unit w_i/w_j is not a product of units from $K\{w_i\}$ and $K\{w_j\}$.

3. Realize Cyclic Groups over Rational Function Fields

The realization of cyclic groups is one of the first exercises in Inverse Galois Theory. Since Inverse Galois Theory is one main topic of this conference and since we have not only experts here, I will treat this basic exercise in detail in the case that the base field is a rational function field $K(x)$ over an arbitrary field K. Indeed there are many solutions as can be seen by keeping track of the ramification. Our examples are of minimal full ramification; remark that there is no unramified proper extension of $K(x)$.

Situation: Let K be a field of characteristic $p \geq 0$ with an absolute value, let $E = K(x)$ be the rational function field over K and let $n \in \mathbb{N}$ be a number, the order of the cyclic group we are going to realize. If $p \nmid n$ let $\zeta = \zeta_n$ be a primitive n^{th} root of unity. Let $\pi \in K^\times$ be with $|\pi| < 1$. Moreover let Q be the quotient field of the ring $K\{z\}$ of convergent power series with coefficients in K.

Lemma 3.1: *If $\zeta \in K$ and $a \neq b$ in $K^\times$, then there is a cyclic extension $F|E$ inside Q of degree n which ramifies only at $x = a\pi^{-m}$ and $x = b\pi^{-m}$ for some $m \in \mathbb{N}$, the ramification index being n.*

Proof: Let $y \in K[[z]]$ be such that $y^n = (1-a^{-1}x)/(1-b^{-1}x)$. Then $E(y)|E$ is a cyclic extension of degree n with full ramification at $x = a$ and $x = b$. Since y is algebraic over E it converges somewhere by Cauchy, so with $x = \pi^m z$ we get $y \in K\{z\}$ with ramification at $z = \pi^{-m}a$ and $z = \pi^{-m}b$. ∎

Remark: There is no cyclic extension of degree $n > 1$ with $p \nmid n$ of $K(x)$ which is ramified only in one rational place.

Lemma 3.2: *Let $p \nmid n$ but $\zeta \notin K$, and $a \in K^\times$. Let $L = K(\zeta)$ and $G = \mathrm{Gal}(L|K)$. Then there is a cyclic extension $F|E$ inside Q of degree n which ramifies only at $x = a\zeta^\gamma\pi^{-m}$ for $\gamma \in G$ and some $m \in \mathbb{N}$, and the ramification index is again n.*

Proof: For $\sigma \in G$ let $\chi(\sigma) \in \mathbb{N}$ with $\zeta^\sigma = \zeta^{\chi(\sigma)}$ be the cyclotomic character lifted to $\mathbb{N}$. As in the last lemma let $y \in L[[x]]$ be with

$$y^n = \frac{1 - a^{-1}\zeta^{-1}x}{1 - b^{-1}x} \quad .$$

This cyclic extension $E'(y)$ of $E' := L(x)$ does not come from a cyclic extension of E. We have to modify y in a clever way to

$$z = \prod_{\sigma \in G} (y^\sigma)^{\chi(\sigma^{-1})} \ \in L[[x]] \quad .$$

Then we have

$$z^n = \prod_{\sigma\in G} \Big(\frac{1 - a^{-1}\zeta^{-\sigma}x}{1 - b^{-1}x}\Big)^{\chi(\sigma^{-1})} \quad \in L(x) = E'$$

and $F' = E'(z)$ is a cyclic extension of E' of degree n, fully ramified for $x = a\zeta^\sigma$, $\sigma \in G$, and unramified elsewhere, since $\sum_\sigma \chi(\sigma) \equiv 0 \mod n$. A straightforward calculation, using $\chi(\sigma\tau) \equiv \chi(\sigma) + \chi(\tau) \mod n$, shows

$$z^\sigma = z^{\chi(\sigma)} \cdot f_\sigma(x) \qquad \text{with } \ f_\sigma \in E' \quad .$$

So the field F' is left invariant by G, let $F = (F')^G$ be the fixed field.

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash, "G"] & E' = L(x) \arrow[r, dash, "\varGamma"'] \arrow[d, dash] & F' \arrow[r, dash] \arrow[d, dash, "G"] & L((x)) \arrow[d, dash, "G"] \\
K \arrow[r, dash] & E = K(x) \arrow[r, dash, "\varGamma"'] & F \arrow[r, dash] & K((x))
\end{tikzcd}$$

The cyclic group $\varGamma = \mathrm{Gal}(F'|E')$ is generated by the element ω with $z^\omega = \zeta^{-1}z$. The straightforward identity $z^{\omega\sigma} = z^{\sigma\omega}$ shows that $F'|E$ is abelian with

$$\mathrm{Gal}(F'|E) = \mathrm{Gal}(F'|F) \times \mathrm{Gal}(F'|E') = \varGamma \times G \quad .$$

So $F \subseteq K((x))$ is a cyclic extension of E of degree n with ramification at $x = a\zeta^\sigma$, $\sigma \in G$. The embedding into Q follows as in the last lemma. ∎

Remark: Let $F|K(x)$ be a cyclic extension of degree n as in Lemma 3.2 with $m = [K(\zeta_n) : K] = |G|$, let $\tilde{K}$ be the algebraic closure of K. If $x = a$ with $a \in \tilde{K}$ is a fully ramified place in $L\tilde{K}|\tilde{K}(x)$ then $[K(a) : K] \geq m$ and there are at least m fully ramified, over K conjugate places in $F\tilde{K}|\tilde{K}(x)$.

Lemma 3.3 (Witt): *Let $p > 0$ and $F|E$ be a cyclic extension of degree $q = p^n$ inside $K((x))$, which is unramified over $K[x]$. Then there is a cyclic extension $F'|E$ of degree p^{n+1}, unramified over $K[x]$, with $F \subseteq F' \subseteq K((x))$ which can be embedded into Q.*

Proof: Let $O \subseteq K[[x]]$ be the integral closure of $K[x]$ in F, let Tr be the trace of $F|K(x)$ and σ a generator of $\mathrm{Gal}(F|K(x))$. From the unramifiedness follows $\mathrm{Tr}(O) = K[x]$, let $b \in O$ with $\mathrm{Tr}(b) = 1$. For $c = b - b^p$ we have $\mathrm{Tr}(c) = 0$. Again because of the unramifiedness we have (additive Hilbert 90)

$$H^{-1}(F|K(x), O) = 0$$

und therefore there is $a_1 \in O$ with

$$a_1 - a_1^\sigma = c \quad .$$

Let v be the complete valuation of $K((x))$. With $a = a_1 - a_1(0)$ one has $v(a) > 0$ and a satisfies

$$a - a^\sigma = c = b - b^p \quad . \tag{2}$$

Then the zeroes of the polynomial

$$Z^p - Z - a \;\equiv\; \prod_{\nu \in \mathbb{F}_p} (Z - \nu) \mod (x)$$

are by Hensel's lemma in $K[[x]]$, let z be one. So $F' = F(z)$ is a cyclic, over O unramified extension of F of degree 1 or p. From $z^p - z = a$ we get with (2), that $z + b$ is a zero of $Z^p - Z - a^\sigma$. Therefore $F'|K(x)$ is galois and $z^\sigma = z + b$ is a continuation of σ on F'. It remains to determine the order of σ in $\mathrm{Gal}(F'|K(x))$. Inductively we see

$$z^{\sigma^j} = z + b + b^\sigma + \ldots + b^{\sigma^{j-1}} \qquad (j \in \mathbb{N}),$$

especially

$$z^{\sigma^q} = z + \mathrm{Tr}(b) = z + 1 \quad .$$

This shows that $z \notin F$, so $[F' : F] = p$, and the order of σ is larger than $q = p^n$, so p^{n+1}. Therefore $F'|K(x)$ is a cyclic extension of degree p^{n+1}, unramified outside ∞ with $F \subseteq F' \subseteq K((x))$. The embedding of F' into Q runs as in Lemma 3.1 by a homothety $x := cx$. ∎

Corollary: *Let* $\mathrm{char}\, K = p > 0$, *let* $a \in K^\times$ *and* $n \in \mathbb{N}$. *Then* $K(x)$ *has a cyclic extension* F *in* $K((x))$ *of degree* p^n *which is ramified exactly at the place* $x = a$, *and there with full exponent* p^n. *We may inject* F *into* Q *with ramification at* $x = a\pi^{-m}$ *for some* $m \in \mathbb{N}$.

Proof: By replacing K by the algebraic closure of $\mathbb{F}_p$ in K we may assume K to be perfect. Then the extension in Witt's lemma has ramification index p^n at $x = \infty$ since there is no unramified proper extension of $K(x)$. By the Möbius transformation

$$x = \frac{z}{z - a}$$

the place $x = \infty$ will be transformed into $z = a$, and the corollary follows from $K((z)) = K((x))$. The embedding into Q follows as before. ∎

4. Solution of Constant Split Embedding Problems

Situation: Let K_0 be a field, complete under a nontrivial nonarchimedean absolute value, let $K|K_0$ be a finite galois extension with group Γ. Let $E_0 = K_0(x)$ resp. $E = K(x)$ be the rational function field over K_0 resp. K. Let G be a finite group, on which Γ operates, such that we can form the semidirect product $\Gamma \ltimes G$.

Problem: A **constant finite split embedding problem over** K_0 has the goal to realize the projection

$$\mathrm{pr}:\ \Gamma \ltimes G \longrightarrow \Gamma = \mathrm{Gal}(E|E_0) = \mathrm{Gal}(K|K_0)$$

of the semidirect product as the restriction

$$\mathrm{res}:\ \mathrm{Gal}(F|E_0) \longrightarrow \mathrm{Gal}(E|E_0)$$

with a **solution field** F which is galois over E_0 and contains E. Looking at the kernel we have an isomorphism $\mathrm{Gal}(F|R) \simeq G$.

$$\begin{tikzcd}
\bullet \arrow[r, dotted, no head] \arrow[d, dotted, no head] & F \arrow[d, no head, "G"] \\
E_0 \arrow[r, no head, "\Gamma"'] \arrow[d, no head] & E \arrow[d, no head] \\
K_0 \arrow[r, no head, "\Gamma"'] & K
\end{tikzcd}$$

Theorem: *The posed embedding problem is solvable by an extension $F|E$, which has a K-rational, over E_0 unramified place $\mathfrak{P}$ with decomposition group Γ. Especially $F|K$ is regular.*

Proof: We construct a patching datum

$$\mathcal{E} = (E, F_i, P_i, P; G_i, G)_{i\in I}$$

(from the start we only have E and G) like in the talk of Dan, on which the group Γ operates properly. Then we apply the main theorem of algebraic patching from Dan's talk and see that the compound F of $\mathcal{E}$ is the solution field of the embedding problem. At the end we have to prove the existence of the place with the wanted properties.

Altogether we need 7 steps for this purpose.

1. Construction of the index set I and the groups G_i:

   Let $G \neq 1$, let G_{pp} be the set of $g \in G$ of prime power order > 1, let G_0 be a Γ-transversal of G_{pp}. Put

   $$I = G_0 \times \Gamma \qquad \text{und} \qquad J = G_0 \times \{1\} \quad .$$

   On I we have a fixpoint free operation of Γ via

   $$(g_0, \gamma)^{\gamma'} = (g_0, \gamma\gamma') \quad .$$

   Then J is a Γ-transversal of I. To $i = (g_0, \gamma)$ associate the cyclic group

   $$G_i := \langle g_0^{\gamma} \rangle \quad .$$

   Then $G_i^{\gamma} = G_{i^{\gamma}}$ and the groups G_i generate G.

2. Choice of a subset $\{c_i\,;\ i \in I\}$ in K with

   $$c_i^{\gamma} = c_{i^{\gamma}} \quad \text{for} \ \ \gamma \in \Gamma \ , \qquad c_i \neq c_j \ \text{for} \ \ i \neq j \quad .$$

   For $j \in J$ choose primitive elements c_j of $K|K_0$, which are not conjugate over K. Then put $c_{j^{\gamma}} := c_j^{\gamma}$.

   To get $|c_i - c_j| = 1$ we have to assume that $K|K_0$ is unramified and $\overline{K}$ is infinite (Moshe's talk showed how to reduce to this case). Then take the c_i's as lifts from primitive elements $\overline{c}_i$'s of the residue field extension $\overline{K}|\overline{K}_0$.

3. Construction of the big fields $P_i \subseteq P$ for $i \in I$:

   With the rational functions

   $$w_i = \frac{1}{x - c_i} \qquad (i \in I),$$

   build the ring $R = K\{w_i\,;\ i \in I\}$ of the corresponding convergent Mittag-Leffler series and put $P = \mathrm{Quot}(R)$, and inside it

   $$P_i = \mathrm{Quot}(K\{w_j\,;\ j \neq i\}) \qquad , \qquad P_i' = \mathrm{Quot}(K\{w_i\})$$

   For $\gamma \in \Gamma$ holds

   $$w_i^{\gamma} = \frac{1}{x - c_i^{\gamma}} = \frac{1}{x - c_{i^{\gamma}}} = w_{i^{\gamma}} \qquad (i \in I).$$

   So γ induces an automorphism of the ring $R^{\circ} = K[w_i\,;\ i \in I]$, and from

   $$f = a_0 + \sum_{i \in I} \sum_{n \geq 1} a_{in} w_i^n \quad \Longrightarrow \quad f^{\gamma} = a_o^{\gamma} + \sum_{i \in I} \sum_{n \geq 1} a_{in}^{\gamma} (w_i^{\gamma})^n$$

we see that the $\mathit{\Gamma}$-operation is compatible with the norm:

$$|f^\gamma| = \max_{i,n}\left(|a_0^\gamma|, |a_{in}^\gamma|\right) = \max_{i,n}\left(|a_0|, |a_{in}|\right) = |f| \quad .$$

Therefore γ extends to an automorphism of the completion R, and $\mathit{\Gamma}$ becomes an automorphism group of the field P. Moreover we have $P_i^\gamma = P_{i^\gamma}$ and $(P_i')^\gamma = P_{i^\gamma}'$.

4. Construction of the extensions F_j of E in P_j' with

   $$\mathrm{Gal}(F_j|E) = G_j \qquad \text{for all} \;\; j \in J \quad .$$

   By chapter 3 we construct for each $j \in J$ inside P_j' a cyclic extension $F_j|E$ with galois group G_j.

   For $i = j^\gamma \in I$ we put $F_i = F_j^\gamma$ to get cyclic extensions of E with group $G_i = G_j^\gamma$ which satisfy the compatibility conditions of a patching datum with proper $\mathit{\Gamma}$-operation.

5. Solution of the embedding problem:

   The Cartan decomposition

   $$\mathrm{GL}_n(P) = \mathrm{GL}_n(P_i) \cdot \mathrm{GL}_n(P_i')$$

   holds by proposition 2.4. Therefore, including all previous steps, we conclude that

   $$\mathcal{E} = (E, F_i, P_i, P;\, G_i, G)_{i \in I}$$

   is a patching datum, on which the group $\mathit{\Gamma}$ operates properly. By the main theorem of algebraic patching the compound of $\mathcal{E}$ is a solution of the constant split embedding problem.

6. Construction of the K-rational place $\mathfrak{P}$:

   Choose $b \in K_0$ such that $|b| > 1$. Then we have an evaluation $\varphi_b : R \to K$. Since R is a principal ideal domain, this gives a place $\varphi_b : P \to \mathbb{P}_1 K$ which induces a K-rational place $\mathfrak{P}$ of F. For nearly all choices of b this place is unramified over E_0.

7. $\mathit{\Gamma}$ is the decomposition group of $\mathfrak{P}$.

   $\mathit{\Gamma}$ operates on K faithfully with fixed field K_0, so the fixed field in F is a function field F_0 with constant field K_0. Since $\mathfrak{P}$ is unramified this shows that F_0 is the decomposition field of $\mathfrak{P}$. ∎