Field Theory

by

Wulf-Dieter Geyer, Universität Erlangen-Nürnberg

Winter School on Galois Theory

Luxembourg, 15–24 February 2012

Contents

1. Definition of a field and first properties of field extensions

DEFINITION 1: A **field** (German: **Körper**, French: **corps**) K, more precisely denoted by $(K, +, \cdot\,)$, is a set K, together with two operations

$$+ :\ K \times K \to K \qquad , \qquad \cdot :\ K \times K \to K$$

called **addition** and **multiplication** such that the following three laws hold:

(K1) $(K, +)$ is a (commutative) group whose neutral element is called 0 (zero).

(K2) If $K^\times = K \setminus \{0\}$ then $(K^\times, \cdot\,)$ is a commutative group whose neutral element is called 1 (one).

(K3) The two operations are connected by a distributive law

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad\qquad \text{for all } a, b, c \in K\ .$$

As consequence of these axioms there are two more operations

$$- \ :\ K \times K \to K \qquad , \qquad \div \ :\ K \times K^\times \to K \quad ,$$

called **subtraction** and **division**, where $b - a$ is defined as solution of $a + x = b$ and $\frac{b}{a}$ is the solution of $a \cdot x = b$.

EXAMPLES:

1. The field $\mathbb{Q}$ of rational numbers, the field $\mathbb{R}$ of real numbers, the field $\mathbb{C}$ of complex numbers.
2. To each integral domain R we have a smallest field containing R, the **quotient field**

$$\mathrm{Quot}(R) = \left\{ \frac{a}{b}\,;\ a, b \in R,\ b \neq 0 \right\} \quad .$$

   Especially to each field K we have the ring $K[x_1, \ldots, x_n]$ of polynomials in n variables and its quotient field

$$\mathrm{Quot}(K[x_1, \ldots, x_n]) = K(x_1, \ldots, x_n) \quad ,$$

   the field of rational functions in n variables. The polynomials induce functions on K^n. The rational functions induce functions on some „open“ subset in K^n (in the sense of Zariski topology), they are undefined where denominators vanish.

3. To each prime number p the residue classes of integers modulo p form a finite field

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \quad .$$

4. If X is a connected complex manifold or an irreducible algebraic variety then the set of all meromorphic functions on X is a field under the natural addition and multiplication of functions.

5. Especially let $f(x,y)$ be an irreducible polynomial in two variables over an algebraically closed field K. Then the solutions $(\xi,\eta) \in K^2$ of the equation $f(\xi,\eta) = 0$ form an affine curve C in the plane K^2. The polynomials $g \in K[x,y]$ induce on the curve C functions, which form an integral domain
$$K[C] \simeq K[x,y]/f \cdot K[x,y]$$
of *holomorphic* functions on C, and its quotient field
$$K(C) = \mathrm{Quot}(K[C]) = \Big\{\frac{g}{h}\,;\ f \nmid h\Big\}\Big/\Big\{\frac{fg}{h}\,;\ f \nmid h\Big\} \qquad (g,h \in K[x,y])$$
is the field of rational functions on C. Birational equivalent curves lead to isomorphic function fields.
6. If A is an affine space of at least 3 dimensions then A can be coordinatized with coefficients in a field, determined by A up to isomorphism, cf. [St1857] and [Hi1899].
7. Fields are the native soil of Linear Algebra, the natural environment where linear equations can be studied and solved. A central problem and driving force in the development of algebra is the study of polynomial equations of higher degree. This usually leads to extension of fields. For polynomials in one variable this leads to Galois Theory, for polynomials in several variables this leads to Algebraic Geometry.

First concepts and properties:

Definition 2: A subset $K_\circ$ of a field K is called a **subfield**, if $K_\circ$ is closed under the two base operations and satisfies the axioms (K1) and (K2), or equivalently, if $K_\circ$ contains 1 and is closed under subtraction and division. In this case $K|K_\circ$ is called a **field extension**. Examples are the extensions
$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \qquad \text{or} \qquad K \subset K(x_1) \subset K(x_1,x_2) \subset \dots \quad .$$
A **subfield** of an extension $K|K_\circ$ is a subfield of K containing $K_\circ$.

$K|K_\circ$ is called a **finite extension**, if $\dim_{K_\circ} K < \infty$. This dimension is then called the **degree** $[K : K_\circ]$ of the extension.

Maps between two fields $\varphi : K \to L$ which respect the operations $+$ and $\cdot$ and map 1 to 1 are injective, and traditionally called **isomorphisms**. They also respect the operations $-$ and $\div$, the image $\varphi(K)$ is a subfield of L, **isomorphic** to K. If $K_\circ$ is a common subfield of K and L and if $\varphi|_{K_\circ}$ is the identity on $K_\circ$, then the isomorphism φ is called a $K_\circ$-isomorphism.

Proposition 1: *Let K be a field.*

a) *If $M|L$ and $L|K$ are finite extensions, then $M|K$ is also finite with*
$$[M : K] = [M : L] \cdot [L : K] \quad .$$

b) *The intersection of any set of subfields of K is again a subfield.*

Corollaries to b):

c) *Any field contains a smallest subfield, its* **prime field**, *which is either $\mathbb{F}_p$ or $\mathbb{Q}$.* We call p resp. 0 in the latter case the **characteristic of** K.

d) *If $L|K$ is a field extension and $S \subseteq L$ a subset, then there is a smallest subfield of $L|K$ containing S, denoted by $K(S)$. The extension $K(S)$ of K is called* **generated by** S. *The elements of $K(S)$ are exactly the values $f(s_1, \ldots, s_n)$ of rational functions f in any number $n \leq |S|$ of variables with coefficients in K at n-tuples (s_ν) in S^n with different s_ν.*

If $S = \{a\}$ consists of only one element, the extension $K(a)|K$ is called **simple** *and a a* **primitive element** *of the extension.*

Definition 3: Let $L|K$ be a field extension. An element $a \in L$ is called **algebraic over** K, if there is a non vanishing polynomial $f \in K[x]$ with $f(a) = 0$. The monic polynomial of smallest degree with this property is called the **minimal polynomial** $\mathrm{MinPol}(a|K)$ of a over K, its degree is the **degree** $[a : K]$ of a over K. One has $[a : K] = [K(a) : K]$. If a is not algebraic over K it is called **transcendental over** K.

The extension $L|K$ is called **algebraic**, if all $a \in L$ are algebraic over K, otherwise **transcendental**. The field K is called **algebraically closed**, if K has no proper algebraic extension.

Proposition 2:

a) *Field extensions of finite degree are algebraic. Adjunction of a set of algebraic elements gives an algebraic extension. With $M|L$ and $L|K$ also the extension $M|K$ is algebraic. In any field extension $L|K$ there is a unique maximal algebraic subfield*

$$L_{\text{alg}} = \{\alpha \in L\,;\ \alpha \text{ is algebraic over } K\} \quad .$$

b) Theorem of Lüroth 1876 (cf. [St10]): *Let x be transcendental over K. Then any subfield $L_\circ \neq K$ of the simple transcendental extension $K(x)|K$ is again simple transcendental of the form $L_\circ = K(\varphi)$ with*

$$\varphi = \frac{f}{g} \qquad , \quad f, g \in K[x] \text{ with } \quad \gcd(f, g) = 1$$

and $\delta = \max(\deg f, \deg g) \geq 1$. Moreover we have

$$\delta = [K(x) : L_\circ] \quad .$$

So the primitive elements for $K(x)|K$ are exactly the rational functions

$$\varphi = \frac{ax + b}{cx + d} \qquad \text{with} \quad ad - bc \neq 0 \quad .$$

c) *If $L|K$ is an algebraic simple extension, every subfield is so too.*

DEFINITION 4: Let $\mathbf{P}$ be the set of prime numbers. A **supernatural number** n is a formal product

$$n = \prod_{p \in \mathbf{P}} p^{n(p)} \qquad \text{with } \ n(p) \in \mathbb{N}_0 \cup \{\infty\}$$

(Steinitz 1910 called them „G-Zahlen“, Prüfer 1928 called them „ideale Zahlen“. Serre 1964 called them „nombres surnaturels“). If almost all $n(p)$ are zero and none is infinite, then n is a natural number. There is a natural multiplication on the set $\mathcal{N}$ of supernatural numbers, making $\mathcal{N}$ into a commutative monoid with unit $n = 1$. From this we get a notion of divisibility on $\mathcal{N}$. This divisibility is a complete partial ordering on $\mathcal{N}$ with minimum 1 and maximum $\prod_p p^\infty$, such that each subset of $\mathcal{N}$ has an infimum and supremum. Every supernatural number is the supremum of a set (even a chain) of natural numbers.

PROPOSITION 3: *Let $L|K$ be an algebraic extension. We define the* **degree** *of $L|K$ as the supernatural number*

$$[L : K] = \sup_M \, [M : K] \quad ,$$

where M runs over all subfields of $L|K$, finite over K. Then the following holds:

a) *If $M|L$ is another algebraic extension, then*

$$[M : K] = [M : L] \cdot [L : K] \quad .$$

b) *If K is finite and $L|K$ is algebraic, then L is determined up to isomorphism by its degree $n = [L : K]$. For each divisor $m \mid n$ there is exactly one subfield L_m of $L|K$ with $[L_m : K] = m$.*

PROPOSITION 4: *Let K be a field.*

a) (Kronecker 1887): *Let $f \in K[x]$ be a polynomial. Then there is a smallest extension $L|K$ such that f splits completely in L, i.e. is a product of linear polynomials $x - \alpha_i$ and a constant. L is generated by the roots of f and is unique up to K-isomorphism.* It is called the **splitting field** of f over K.

b) (Steinitz 1910): *The same is true for any subset $S \subseteq K[x]$ of polynomials. Especially $S = K[x]$ gives an algebraic extension of K which is algebraically closed, called the* **algebraic closure** $\widetilde{K} = K^{\mathrm{alg}}$ *of K. It is unique up to K-isomorphism.*

DEFINITION 5: Let K be a field of characteristic $p \geq 0$.

a) A polynomial $f \in K[x]$ is called **separable**, if it has no double root in $\widetilde{K}$, i.e. if $\gcd(f, f') = 1$, otherwise **inseparable**.

b) If f is an irreducible inseparable polynomial, then $f' = 0$, so we have $p > 0$ and $f(x) = g(x^p)$ for some $g \in K[x]$. The maximal e such that $f \in K[x^{p^e}]$ is called the **exponent of inseparability** $e = \exp_{\mathrm{ins}} f$ of f and $p^e = \deg_{\mathrm{ins}} f$ is called the **degree of**

inseparability of f. Then we have $f = g(x^{p^e})$ with separable g and $\deg g = \deg_{\text{sep}} f$ is called the **degree of separability** of f. This $\deg_{\text{sep}} f$ is the number of different roots of f in $\widetilde{K}$. We have

$$\deg f = \deg_{\text{sep}} f \cdot p^{\exp_{\text{ins}} f} = \deg_{\text{sep}} f \cdot \deg_{\text{ins}} f \quad .$$

c) An algebraic element a over K is called **separable**, if $f = \mathrm{MinPol}(a|K)$ is separable, otherwise **inseparable**. The element a is called **purely inseparable** over K, if $\deg_{\text{sep}} f = 1$, i.e. if f has only one root. Remark that the elements in K are separable and purely inseparable over K.

d) An algebraic extension $L|K$ is called **separable**, if all $a \in L$ are separable over K, otherwise **inseparable**.

e) The algebraic extension $L|K$ is called **purely inseparable**, if all $a \in L$ are purely inseparable. If in case $p > 0$ there is an exponent e with $L^{p^e} \subseteq K$, we call the smallest such e to be the **exponent of inseparability** $\exp_{\text{ins}}(L|K)$ of $L|K$, otherwise it is $= \infty$. If $L = K(a)$ is purely inseparable with $f = \mathrm{MinPol}(a|K)$ then $\exp_{\text{ins}}(L|K) = \exp_{\text{ins}} f$.

PROPOSITION 5: *Let K be a field,* $\operatorname{char} K = p \geq 0$.

a) *If $p = 0$ then all algebraic extensions are separable.*

b) *If $p > 0$ and $K = K^p$ then all algebraic extensions are separable.*

c) *If $p > 0$ and $a \in K \setminus K^p$, then $X^{p^e} - a$ is an inseparable irreducible polynomial in $K[x]$ of degree p^e for any $e \in \mathbb{N}$.*

The fields satisfying a) or b), i.e. fields having only separable algebraic extensions, are called **perfect**, the other fields **imperfect**.

EXAMPLE 1: $\mathbb{F}_p$ is perfect, the rational function field $\mathbb{F}_p(x)$ not.

EXAMPLE 2: Every field K with $\operatorname{char} K = p > 0$ is contained in a smallest perfect field, the **perfect closure** of K, namely the union $K^{p^{-\infty}}$ of the ascending sequence of fields

$$K \subseteq K^{1/p} \subseteq K^{1/p^2} \subseteq \ldots\ldots \subseteq K^{1/p^e} \subseteq \ldots\ldots$$

d) *If the algebraic extensions $M|L$ and $L|K$ are separable, so is the extension $M|K$.*

e) *Every algebraic extension of a perfect field is perfect.*

PROPOSITION 6: *Let K be a field with* $\operatorname{char} K = p \geq 0$, *and $L|K$ be an algebraic extension.*

a) *There is a maximal subfield L_{sep} of $L|K$ such that $L_{\text{sep}}|K$ is separable, namely*

$$L_{\text{sep}} = \{a \in L\,;\ a \text{ is separable over } K\} \quad .$$

Then $L|L_{\text{sep}}$ is purely inseparable. We denote the **degree of separability** *and the* **degree of inseparability** *of the extension $L|K$ by*

$$[L:K]_{\text{sep}} = [L_{\text{sep}}:K] \qquad \text{and} \qquad [L:K]_{\text{ins}} = [L:L_{\text{sep}}] \quad .$$

The latter is always a power of p (resp. 1 it $p = 0$). If $L = K(a)$ and $f = \mathrm{MinPol}(a|K)$ then

$$[L : K]_{\mathrm{sep}} = \deg_{\mathrm{sep}} f \qquad , \qquad [L : K]_{\mathrm{ins}} = \deg_{\mathrm{ins}} f \quad .$$

b) THEOREM OF THE PRIMITIVE ELEMENT: *Let $L|K$ be a finite extension. Then the following statements are equivalent:*

(1) *The extension $L|K$ is simple, i.e. has a primitive element.*

(2) *The extension $L|K$ has only finitely many subfields.*

(3) *We have $p = 0$ or $p > 0$ and*

$$[L : K]_{\mathrm{ins}} = p^{\exp_{\mathrm{ins}}(L|K)} \quad .$$

c) COROLLARY: *Every separable finite extension is simple. All finite extensions of the field K are simple iff K is perfect or $[K : K^p] = p$.*

EXAMPLE: Let $K = \mathbb{F}_p(x, y)$ be the rational function field in 2 variables over $\mathbb{F}_p$. Then $K|K^p$ is not simple, and an infinite family of subfields is given by $K^p(y + x^n)$ with $p \nmid n$.

After this crash course in algebraic field extensions let us consider transcendental extensions.

DEFINITION 6: Let $L|K$ be a field extension. A subset $A \subseteq L$ is called **K-algebraically independent** if no finite subset $\{a_1, \ldots, a_n\}$ of A satisfies a polynomial relation, i.e. if

$$f \in K[x_1, \ldots, x_n] \ , \ f(a_1, \ldots, a_n) = 0 \implies f = 0 \qquad\qquad (a_\nu \in A \text{ different})$$

holds.

PROPOSITION 7: *Let $L|K$ be a field extension.*

a) *There are maximal K-algebraically independent sets A in L and all have the same cardinality.*

b) *This common cardinality is called the* **transcendence degree** *of $L|K$ and every such maximal A is called a* **transcendence base** *of $L|K$. For any such A the extension $L|K(A)$ is algebraic.* If $L = K(A)$ for one such an A, the extension $L|K$ is called **purely trancendental**.

c) *If $L|K$ is finitely generated, say $L = K(b_1, \ldots, b_m)$, then a transcendence base can be choosen among the b_μ.*

d) *Any subextension of a finitely generated field extension is again finitely generated.*

e) *An algebraically closed field is determined up to isomorphism by the transcendence degree over the prime field and its characteristic.*

All concepts and results up to now are at least 100 years old and contained in a paper of Steinitz (cf. 2.4). Let us now come to some newer concepts, developed in the first chapter of the *Foundations* of A. Weil. For proofs see also [FJ] or [La93].

Definition 7: Let F be a field with subfields L and M which contain a common subfield K.

a) L and M are called **linearly disjoint over** K if the canonical map $L \otimes_K M \to F$, given by $x \otimes y \mapsto x \cdot y$, is injective. We denote this by a rectangular diagram:

$$\begin{tikzcd}
L \arrow[r, dash] & LM \\
K \arrow[u, dash] \arrow[r, dash] & M \arrow[u, dash]
\end{tikzcd}$$

If $[L : K] < \infty$, this is equivalent to say that $[L : K] = [LM : M]$. If L or M is algebraic over K, the compositum LM of the two fields L and M is exactly the image of $L \otimes_K M$, otherwise the image is a subdomain of LM.

b) The extension $L|K$ is called **separable** if L is linearly disjoint from the perfect closure $K^{p^{-\infty}}|K$ of K. This is equivalent to say that L is linearly disjoint from $K^{1/p}$. For algebraic extensions this definition of separable coincides with the former definition.

c) The extension $L|K$ is called **regular** if L is linearly disjoint from the algebraic closure $\widetilde{K}|K$ of K.

Example: If $f \in K[x_1, \ldots, x_n]$ is an irreducible polynomial then the function field of the hypersurface $f = 0$ is regular over K iff f is **absolutely irreducible**, i.e. irreducible over $\widetilde{K}$.

More generally let X be a scheme of finite type over a field K. If X is reduced and irreducible, the rational functions on X form a finitely generated function field $K(X)|K$. This extension is regular iff X is absolutely reduced and absolutely irreducible, i.e. if $X \times_K \widetilde{K}$ is reduced and irreducible over $\widetilde{K}$. We call such schemes **varieties** over K.

Proposition 8: *Let F be a field with subfields K, L, M, N with inclusions*

$$K \subseteq L \qquad \textit{and} \qquad K \subseteq M \subseteq N \quad .$$

a) Tower property: *L and N are linearly disjoint over K iff L and M are linearly disjoint over K, and LM and N are linearly disjoint over M:*

$$\begin{tikzcd}
L \arrow[r, dash] & LM \arrow[r, dash] & LN \\
K \arrow[u, dash] \arrow[r, dash] & M \arrow[u, dash] \arrow[r, dash] & N \arrow[u, dash]
\end{tikzcd}$$

b) *If L and M are linearly disjoint over K then $L \cap M = K$.* (Therefore one could drop the term *over* K in the notion of linear disjointness).

EXAMPLE: Let α, β be different complex roots of the polynomial $x^3 + 2$. Then $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, but the fields are not linearly disjoint over $\mathbb{Q}$.

c) *If $L|K$ is Galois and $L \cap M = K$, then L and M are linearly disjoint over K.*

d) *Let $u_1, \ldots, u_n$ be L-algebraically independent elements of F, then L and $K(u_1, \ldots, u_n)$ are linearly disjoint over K.*

e) *If $L|K$ and $M|L$ are separable extensions, so is $M|K$.*

f) *The extension $L|K$ is separable iff every finitely generated subfield $L_\circ$ has a transcendence base $(a_1, \ldots, a_n)$ with $L_\circ|K(a_1, \ldots, a_n)$ is separable (a* **separating transcendence base***).*

g) *If K is algebraically closed in L and $M|K$ is a simple algebraic extension then L and M are linearly disjoint over K.*

EXAMPLE: Let $K = \mathbb{F}_p(a, b)$ be the field of rational functions in two variables a, b over $\mathbb{F}_p$. The equation $y^p = x^{2p} + ax^p + b$ is irreducible over K, so defines a purely inseparable field extension $L = K(x, y)|K(x)$ of degree p. K is algebraically closed in L, but L and $K^{1/p}$ are not linearly disjoint over K since $[K^{1/p} : K] = p^2$ but $[LK^{1/p} : L] = p$ since $b^{1/p} = y - x^2 - a^{1/p}x$.

h) *The extension $L|K$ is regular iff $L|K$ is separable and K is algebraically closed in L.*

2. Historical remarks about the concept of field

The operations of addition, multiplication, subtraction and division can be found in all cultures with written tradition, in Egypt, in Sumer, in Babylon, in China, in India, among the ancient Greeks and so on. But this does not mean that already the concept of field existed.

2.1. What Wikipedia says

If you open up the english Wikipedia and look for the subentry *History* in the article *Fields (mathematics)* you find at the moment of this talk the following statement:

> The concept of **field** was used implicitly by Niels Henrik Abel and Évariste Galois in their work on the solvability of polynomial equations with rational coefficients of degree five or higher.

What does that mean? Did they think about fields by preparing their papers but refused to write down this word? Did they have this concept but no name for it? If you look at their papers, you see: They are dealing with polynomials and with rational functions, not with individual ones but with generic ones and sometimes use them as variables. But they do not form the set of all of them. Moreover they do not specify the field of coefficients (rationals or complex numbers, but certainly of characteristic zero) because this is not important for their work. So the environment in which their mathematics live is not clearly specified. Especially they did not look for solvability of polynomial equations over the rationals (as Wikipedia claims) but they considered general polynomials

$$f = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

over some rational function field $K_\circ(a_1, \ldots, a_n)$ in n variables $a_1, \ldots, a_n$ (in modern language).

Abel and Galois, great mathematicians, worked without a general concept of field, just with polynomials and with rational functions — but used them also in the sense of generators (proposition 1.1.d) for subfields of rational functions, and here especially Galois emphasizes the importance of distinguishing between the different subfields. Indeed Galois in his papers of the years 1828-32 (published only in 1846 by Liouville) sees the importance of adjoining irrationalities for the study of polynomials in one variable and their roots. He constructs a Galois resolvent g for a separable polynomial f whose root generates the splitting field of f, he finds the Galois group of an equation and its importance for the nature of the roots . . . , but all this without the concept of field — in the same way as Gauß in 1801 inaugurated the theory of cyclotomic fields without having the concept of field.

Two things were missing at their time, to come up with a general concept of a field.

First the notion of "infinite sets" was absent. Aristotle, the highest authority in logic and science for 2000 years, denied that the unbounded sequence of natural numbers can be seen as one quantity, as something finished. It was ἄπειρον, unfinished, unlimited, something horrible for greek philosophers as the antimonies of Zenon and others showed. Still in the year 1831 (five year after Abel's first paper) Carl Friedrich Gauß agreed with Aristotle when he wrote to his friend Schumacher, astronomer in Altona:

> ... so protestire ich zuvörderst gegen den Gebrauch einer unendlichen Grösse als einer **Vollendeten**, welcher in der Mathematik niemals erlaubt ist. Das Unendliche ist nur eine façon de parler, indem man eigentlich von Grenzen spricht, denen gewisse Verhältnisse so nahe kommen als man will, während anderen ohne Einschränkung zu wachsen verstattet ist.

One interpretation of Gauß' words, clearer formulated by him in other letters, is the following: Infinite diverging series are in his mind not part of mathematics, contrary to the belief of Leonhard Euler, the most important mathematician of the 18th century. They are infinite objects without any limit attached to them, so of no use. Gauß (1812), Cauchy (1821) and Abel (1826) were the first mathematicians who did substantial and rigorous investigations about convergence of certain infinite series. For our question more important is another interpretation of Gauß' words: As you know, Gauß did invent the notion of congruences in 1801. We interprete congruences as a method to simplify the infinite set of integers into a finite set of residue classes. This Gauß never did; the congruence classes are infinite quantities, so not an object of mathematics; one has finitely many representatives, but not a finite structure of similar nature as the integers. His followers like Galois, Serret, Schönemann did the same, and so did Richard Dedekind 1857 in a paper on higher congruences, where he summarized the results and simplified the proofs of theorems which we interprete as theorems on finite fields like

> The multiplicative group of a finite field is cyclic, or
>
> If $\mathcal{F}$ is the family of all irreducible monic polynomials in $\mathbb{F}_p[x]$ of degree dividing n, then we have in $\mathbb{F}_p[x]$
>
> $$x^{p^n} - x = \prod_{f \in \mathcal{F}} f(x) \quad .$$

But for them, including Dedekind at that time, these theorems were theorems on congruences between numbers or polynomials with integral coefficients, not as equations in some new structure. They did not see finite fields.

Let me make two claims:

I. The general concept of field could not be born before the invention of set theory which was done by a single man, Georg Cantor, in papers between 1874 and 1897, against strong opposition, but with a few excellent supporters like Richard Dedekind and David Hilbert.

II. The driving motor of mathematics are good problems and good examples. Fruitful abstract concepts are usually an outgrow of interesting examples where the

> definitions, arguments and proofs start to be repeated in similar ways until a common structure behind them starts to come into existence.

The second claim gives another hint why the concept of a field could not be installed in the times of Abel and Galois: Good examples were missing.

Already the first example I gave, the field of rational numbers, was unknown at the time of Abel and Galois, at least in England. Augustus de Morgan, first professor for mathematics at the University College London and first president of the London Mathematical Society, still today known by *de Morgan's laws* in Boolean algebra, denied the existence of negative numbers still in the year 1837 (!). In that year 1837 he wrote a book for the *Society for the Diffusion of Useful Mathematics* which contained the following sentences:

> The teacher must recollect that the signs + and − are not quantities, but directions to add and subtract. Above all he must reject the definition still sometimes given of the quantity $-a$ that it is less than nothing.
> ...
> It is astonishing that the human intellect should ever have tolerated such an absurdity as the idea of a quantity less than nothing, above all, that the notion should have outlived the belief in judicial astronomy and the existence of witches, either of which is ten thousand times more probable.

If you do not know rational numbers, you do not have a single example of a field! —

I have to add that until the end of Middle Ages negative numbers were practically unknown in Europe and also among the Arabs, although Chinese and Indian mathematicians used them already in the middle of the first millennium. In the Renaissance this slowly changed: Prominent champions for negative numbers were e.g. Michael Stifel, an Augustinian monk and protestant parson at Martin Luther's time, Simon Stevin, founder of the engeneering school at the university of Leiden, and the Italian physician and polymath Geronimo Cardano. Later Newton accepted them, Leibniz had problems of understanding them. Vieta, Descartes and John Wallis denied their existence. In the 18th century the authority of Leonhard Euler and his famous textbooks made the negative numbers into acceptible mathematical objects, at least at the continent.

So despite de Morgan one can say that the example $\mathbb{Q}$, more precisely the concept of rational numbers, was essentially known and accepted at Abel's times, although not as visible as today. Also the example $\mathbb{R}$ of real numbers was more or less known in Europe through the efforts of Bombelli (1572) and Stevin. The 18th century used them permanently, although an exact definition was only given during the 19th century by Bolzano, Méray, Dedekind and Cantor. For the example $\mathbb{C}$, first invented by Cardano (1545), more precisely by Bombelli (1572), the situation is a little bit more complicate. At best they were told to be *imaginary*, i.e. only to exist in the imagination but not in reality. The question, what a complex number is, was not even answered reasonably by Leonhard Euler. Despite he was very familiar with complex numbers, the explanation of "what they are" in his textbook on algebra (1770) is not understandable and is caricatured in Robert Musil's first novel *Die Verwirrungen des Zöglings Törleß* (1906).

Even Cauchy, one of the heroes of complex function theory, did not allow in his famous *Cours d'Analyse* (1821) the complex numbers to be numbers. An equation between complex numbers is, as he says, only a symbolic abbrevation for two real equations; this does not give the complex numbers an independent existence. He even formulates (p.175) sentences like

> L'équation
>
> $$\cos(a+b) + \sqrt{-1}\sin(a+b) = (\cos a + \sqrt{-1}\sin a)(\cos b + \sqrt{-1}\sin b)$$
>
> elle-même, prise à la lettre, se trouve inexacte et n'a pas de sens.

Precise definitions of complex numbers were among others given by Gauß (1832: points in the plane), Hamilton (1837: pairs of real numbers), the most interesting algebraic definition was done 1847 by Cauchy: Complex numbers are residues of real polynomials modulo the irreducible polynomial x^2+1:

$$\mathbb{C} = \mathbb{R}[x]/(x^2+1)$$

(This was the starting point for Kronecker's construction of root and splitting fields for arbitrary polynomials in 1887).

So at the time of Abel and Galois at most two or three examples of fields of numbers were known, and besides them fields of rational functions, which were seen as quite a different object. This is a too narrow base of examples to create a new concept.

2.2. New Examples

A new class of examples came with the thesis of Bernhard Riemann in 1851 where he presented his ideas of complex function theory by introducing geometric ideas like Riemann surfaces. In modern terminology his ideas lead to the following facts: A compact Riemann surface X, in modern terms: a connected compact one-dimensional complex manifold, is the same as the desingularization of the projective closure of a plane affine curve $\mathcal{C}$ with an equation $f(x,y)=0$ over $\mathbb{C}$. The field of rational functions

$$\mathbb{C}(\mathcal{C}) = \mathrm{Quot}(\mathbb{C}[x,y]/(f))$$

on this curve is exactly the field of meromorphic functions on the complex manifold X:

$$\mathcal{M}(X) = \mathbb{C}(\mathcal{C}) \quad .$$

There is a bijection between compact Riemann surfaces (modulo conform equivalence), complex curves (modulo birational equivalence) and their functions fields (up to isomorphism). These function fields (Riemann calls them *Klasse von Functionen*) are exactly the finite extensions of the field rational function $\mathbb{C}(x)$, the field of meromorphic functions on Riemann's x-sphere. They were called algebraic function fields of one variable and studied thoroughly for the first time by Dedekind and Weber in 1880, in one of the many attempts by many people to lay solid foundations to the splendid visions of Riemann.

So Riemann's ideas not only led to a new family of fields, but combined these fields with important geometrical and analytical objects which stressed their importance. In our terminology of today we may say: These function fields form a second class of fields besides the fields of algebraic numbers, which were studied after Gauß especially by Kummer, cf. [Ku75]. Kummer was the most eminent pioneer of algebraic number theory in his time, working since 1844 in rings of algebraic integers without having the concept of an algebraic integer, not to speak of the concept of field.

Besides these examples, new types of fields occured 1891 in Veronese's construction of non archimedean geometries, using fields of formal power series $K(\!(z)\!) = \operatorname{Quot} K[[z]]$. These fields led Hensel to his creation of p-adic number fields like $\mathbb{Q}_p$ which he popularized 1908 in his book on algebraic numbers. Moreover no later than 1893 the finite fields appear as fields. Now enough examples existed and the need of a general concept of field was quite obvious.

2.3. The Birth of the Concept of Field and of its Notation

The birth of the concept of a field and its notation took several steps.

The name **Körper** was coined by Richard Dedekind in his famous Supplement XI (§159) to Dirichlet's lectures on number theory in 1871 ([Di1871]) after he used this term already in his lectures. To be precise, Dedekind defines by the term **Körper** or **Zahlkörper** subfields of the field of complex numbers. He explains this name in §160 of [Di1894] in the following way:

> Dieser Name soll, ähnlich wie in den Naturwissenschaften, in der Geometrie und im Leben der menschlichen Gesellschaft, auch hier ein System bezeichnen, das eine gewisse Vollständigkeit, Vollkommenheit, Abgeschlossenheit besitzt, wodurch es als ein organisches Ganzes, als eine natürliche Einheit erscheint. Anfangs, in meinen Göttinger Vorlesungen (1857 bis 1858) hatte ich denselben Begriff mit dem Namen eines **rationalen Gebietes** belegt, der aber weniger bequem ist.

Dedekind also gives fundamental properties of his fields. Firstly he defines basic concepts of Linear Algebra (only the theory of determinants did exist at his times) like linear dependence, basis, dimension. He has the first definitions and propositions of §1, gets the notion of norm and trace in a finite extension. He gets the notion of Galois hull of a finite field extension, defines the Galois group, shows the linear independence of automorphisms, gets part of the main theorem of (finite) Galois theory, gets the notion of the discriminant of a basis and could prove the existence of primitive elements. Only after these preliminaries on field theory he turns in his Supplement XI to arithmetic, to the notion of integral elements and to the arithmetic of the rings of algebraic integers in a finite extension of $\mathbb{Q}$. The notion of **Zahlkörper** as finite extensions of $\mathbb{Q}$ was made popular especially through Hilbert's papers on number theory.

In his already mentioned paper [DW1882] with Heinrich Weber, written in 1880, Dedekind introduced in analogy to his notion of **Zahlkörper** the notion of **Körper alge-**

braischer Funktionen for finite extensions of the field $\mathbb{C}(x)$. The most important result in this seminal paper is the discovery that the arithmetic of these function fields and of the finite number fields follow nearly the same rules, a fact which 1927 leads Emmy Noether to her axiomatic treatment of **Dedekind domains**. In 1901 Hensel and Landsberg enlarged this paper to a book, but substituted some of the algebraic arguments of Dedekind and Weber by analytic ones to come nearer to Riemann's point of view.

Another approach to a concept of field was done by Kronecker who considered finitely generated fields in characteristic zero — finite fields he only treated using congruences like Gauß and Galois before him. In a paper from 1879 he calls them **Rationalitätsbezirke**. In his famous paper in Kummer's Festschrift from 1882 (which Dieudonné called a first glimpse into Grothendieck's theory of schemes) he calls the finitely generated extensions of $\mathbb{Q}$ **Rationalitätsbereiche**. This notation, covering a somehow different class of fields than the fields of Dedekind, was frequently used in the following years, by Hilbert in his papers on algebra, by Felix Klein and others, even by Weber, until Weber in August 1893 sent a paper to the Mathematische Annalen, giving the first general definition of a **Körper** in the same way as we have done in §1: He first defines the notion of an abstract group (in the 19th century groups were usually permutation groups), then the notion of an abstract field with Dedekind's notation **Körper**. He explicitly said that the finite fields $\mathbb{Z}/p\mathbb{Z}$ fall under his definition.

In the same month E. H. Moore coined the english expression **field** for Weber's **Körper**. Indeed his paper, read in August 1893 at a congress in Chicago, is on finite fields $\mathbb{F}_q$ which he called **fields of order** q or **Galois-fields of order** q. The main result of his paper is that a finite field is determined, up to isomorphy, by the number q of its elements. Despite the results of Gauß, Galois, ... on congruences in my eyes this paper is the starting point of the theory of finite fields.

Astonishingly Weber seems to have forgotten his general definition rather soon, at least partially. In his famous textbook [We1895] which he wrote in 1894 he defines in §146 the notion of **Körper**, first **Zahlenkörper**, then **Funktionenkörper**, then the general notion of **Körper**. But then, in the same paragraph, he states (also in the 2. edition from 1898) that $\mathbb{Q}$ is contained in every field, because every field contains 1, so $1+1$ and so on, so all natural numbers, so all rational numbers. So Weber's textbook considered only fields of characteristic zero which simplified his theory of finite field extensions by avoiding inseparability.

If this happens in the most prominent textbook on algebra at the end of the 19th century it is not clear if one is allowed to say that the concept of field already was a known concept in the 19th century.

2.4. The paper of Steinitz

In my eyes the birth of the general notion of a field is a paper from the year 1910, written by Ernst Steinitz in Berlin, which was initiated as he said by the book of Hensel in 1908 with a new class of fields, the p-adic numbers. N. Bourbaki in the historical notes to the chapter V (*Corps commutatifs*) in his book *Algèbre* wrote:

> Ce travail fondamental de Steinitz peut être considéré comme ayant donné naissance à la conception de l'Algèbre. Développant systématiquement les conséquences des axiomes des corps commutatifs, il introduit ainsi les notions de corps premier, d'éléments (algébriques) séparables, de corps parfait, définit le degré de transcendance et démontre enfin l'existence des extensions algébriquement closes d'un corps quelconque.

Indeed the paper of Steinitz contains all what I said in §1 except the newer concepts of linear disjointness etc. The theory of fields was born in full generality. Steinitz had the right concepts, although partially his notations were changed afterwards, e.g.: The suggestive notion **separable** and **inseparable** for polynomials and field extensions was invented by van der Waerden in his textbook from 1930, Steinitz called them **erster Art** and **zweiter Art** (polynomials/extensions of first resp. second kind).

Although Steinitz had the right concepts and the basic results, his proofs could be improved. The reason for this is his dealing with infinite constructions. Of course set theory had been invented, otherwise he could not have done his general theory. But the first fundamental book about set theory by Hausdorff only appeared in 1914. So he had to build up his set theoretical tools by himself, and the reader of today is astonished seeing that Steinitz did not know the concept of an empty set which made some of his formulations not so smooth. His essential tool was the well ordering theorem of Zermelo from 1904. So he well ordered all his field extensions in clever ways and his proof of the existence of an algebraic closure took 20 (!) pages in Crelle's journal. He also saw very clear (much clearer then his later editors Baer and Hasse) that for several of his statements like existence and uniqueness of the algebraic closure he needed the use of the axiom of choice on which the theorem of Zermelo was based. He wrote in the introduction to his paper, that the negative approach of many of his collegues against the axiom of choice will soon dwindle, since there are natural questions in mathematics which cannot be handled without this axiom:

> Noch stehen viele Mathematiker dem Auswahlprinzip ablehnend gegenüber. Mit der zunehmenden Erkenntnis, daß es Fragen in der Mathematik gibt, die ohne dieses Prinzip nicht entschieden werden können, dürfte der Widerstand gegen dasselbe mehr und mehr schwinden. Dagegen erscheint es im Interesse der Reinheit der Methode zweckmäßig, das genannte Prinzip so weit zu vermeiden, als die Natur der Frage seine Anwendung nicht erfordert. Ich habe mich bemüht, diese Grenze scharf hervortreten zu lassen.

20 years later, after Steinitz' premature death, Baer and Hasse reedited this seminal paper as a book together with an appendix on Galois theory, since Galois theory was not completely covered by Steinitz, but belongs to the basic elements of the theory of fields. They tried to simplify some proofs of Steinitz and reduced the mentioned proof of 20 pages to 2 pages. They still did it using well orderings.

This I find a little strange since the right tool for algebra is Zorn's lemma which gives an even shorter and more natural proof and is the usual tool in all textbooks of today. Why Baer and Hasse did not use Zorn's lemma? One may answer that Zorn stated his lemma only in 1935. This is not a very good objection since Zorn's lemma (the name was coined 1939 by Bourbaki who called it *le théorème de Zorn*) appeared already in 1922 in a paper by Kuratowski. You may even say that Steinitz himself could have used Zorn's lemma in the form of Hausdorff's maximal chain principle which says that every ordered set contains a maximal chain (= totally ordered subset). This was stated by Hausdorff in a paper from 1909. There are more people like L. Brouwer (1910/11), S. Bochner (1928), R. L. Moore (1932) who used maximality principles of similar nature as Zorn's lemma before Zorn. But Zorn in 1935 was the first to apply it to algebra.

3. Galois theory

The interplay between the study of polynomials in $K[x]$, in modern language: the study of finite extensions of the field K, and the theory of finite groups was started by Lagrange and brought to a first culmination by Galois. But Galois's papers were not understood by his contemporaries, their publication started 14 years after his death. Many first rate mathematicians of the 19th century studied them and slowly a clear Galois theory was fixed. Dedekind gave lectures on Galois theory in Göttingen in the years 1858 to 1860, which later entered into his Supplement XI. The first presentation of Galois theory in a textbook was done 1866 by Serret.

Only in 1893 Weber defined the general notion of field to give the right frame to Galois theory, but he did not come to the problems with inseparable extensions. Steinitz saw them 1910 very clearly; but he developed Galois theory only to the extent he needed for the proofs of the statements given in §1; e.g. he proved Proposition 1.c. In the 1920's several textbooks (Hasse, Haupt, ...) developed Galois theory in the frame of separable field extensions; 1930 van der Waerden's lucid textbook appeared.

Definition 1: An algebraic field extension $L|K$ is called **normal**, if for every irreducible polynomial $f \in K[x]$ the following holds: If f has a zero in L then f splits completely in L.

An irreducible polynomial $f \in K[x]$ is called **normal** if it splits completely after you adjoin one root of f to K, i.e. if the **root field** $K[x]/(f)$ is already a splitting field.

An algebraic field extension resp. an irreducible polynomial is called **Galois**, if it is normal and separable.

Corollary: *If $L|K$ is normal (Galois), then L is normal (Galois) over each subfield of $L|K$.*

Proposition 1: *Let K be a field with algebraic closure $\widetilde{K}$, let L be a subfield of $\widetilde{K}|K$.*

a) *If $L|K$ is normal then L is the splitting field of a set of polynomials in $K[x]$.*

b) *Conversely a splitting field L' of a set of polynomials in $K[x]$ is normal over K. If all polynomials are separable then $L'|K$ is Galois.*

c) *Let $L|K$ be normal, $L_\circ$ be a subfield and $\varphi : L_\circ \to L$ be a K-isomorphism. Then φ can be extended to a K-automorphism of L. If $L|L_\circ$ is finite, the number of these extensions is just $[L : L_\circ]_{\text{sep}}$.*

d) *$L|K$ is normal iff any K-isomorphism $\varphi : L \to \widetilde{K}$ maps L into (and then onto) itself.*

e) *The intersection of normal extensions of K is again normal. Therefore each algebraic extension $L|K$ is contained in a smallest normal one $M|K$ which is called the* **normal hull** *of $L|K$. It can be constructed by taking the composite of all conjugate fields of*

L over K:

$$M = \prod_{\sigma \in \mathrm{Aut}(\widetilde{K}|K)} L^\sigma \quad = \prod_{\sigma\colon L \xrightarrow[K]{} \widetilde{K}} L^\sigma \quad .$$

If $L|K$ is separable, $M|K$ will be Galois.

f) *If $L|K$ is normal and $G = \mathrm{Aut}(L|K)$ is the group of automorphisms of this extension then the fixed field*

$$\mathrm{Fix}_G(L) = \{a \in L\,;\ \forall \sigma \in G:\ a^\sigma = a\}$$

is purely inseparable over K and $L|\,\mathrm{Fix}_G(L)$ is Galois.[1]

Definition 2: Let $L|K$ be a Galois extension. Its automorphism group is called the **Galois group**

$$\mathrm{Gal}(L|K) = \mathrm{Aut}(L|K) = \{\sigma : L \to L\,;\ \sigma \text{ is a } K\text{-isomorphism}\}$$

of $L|K$. The orbits of $G = \mathrm{Gal}(L|K)$ on L are finite and consist of **conjugate elements**. If G is abelian resp. (pro-)cyclic resp. (pro-)nilpotent resp. (pro-)solvable the Galois extension $L|K$ is called **abelian** resp. **cyclic** resp. **nilpotent** resp. **solvable**.

If L is the splitting field of the monic separable polynomial $f \in K[x]$ with the decomposition

$$f = \prod_{i=1}^{n} (x - a_i)$$

over L, then the group $\mathrm{Gal}(L|K)$ acts faithfully on the set of roots $\{a_1, \ldots, a_n\}$ of f, and this permutation group is called the **Galois group** $\mathrm{Gal}(f|K)$ of f over K. We say that the polynomial f whose roots generate L give rise to a faithful representation of the abstract group $G = \mathrm{Gal}(L|K)$ as permutation group. Conversely, if K is infinite, to every faithful permutation representation $\rho : G \hookrightarrow S_n$ of $G = \mathrm{Gal}(L|K)$ there is a separable polynomial $f \in K[x]$ of degree n with splitting field L such that G operates on the roots of f as it does through ρ.

The groups $\mathrm{Gal}(f|K)$ were the Galois groups of the 19th century, the groups $\mathrm{Gal}(L|K)$ are the Galois groups of newer type. The formulation of Galois theory had been much improved through the switch from $\mathrm{Gal}(f|K)$ to the more invariant objects $\mathrm{Gal}(L|K)$. But for concrete studies in Galois theory the permutation representations are indispensable and often used.

Fact: *The group $\mathrm{Gal}(f|K)$ is transitive iff f is irreducible. It is regular iff f is Galois.*

[1] In Proposition 1.6.a we got, without assuming normality of $L|K$, another splitting of $L|K$ into a tower of two extensions, the purely inseparable part $L|L_{\mathrm{sep}}$ at top, the separable part $L_{\mathrm{sep}}|K$ at bottom. In the normal case the properties can be switched: separable at top and purely inseparable at bottom. In general this cannot be done: Let $L = \mathbb{F}_2(x,y)$ be the rational function field in two variables over the field with two elements, and let $K = \mathbb{F}_2(u,y)$ the subfield with $u = x^4 + yx^2$. Here we have $L_{\mathrm{sep}} = \mathbb{F}_2(x^2,y)$, so $[L:K]_{\mathrm{sep}} = [L:K]_{\mathrm{ins}} = 2$, but no element in L is purely inseparable over K (Exercise!).

THEOREM 2: (E. Artin 1942) *Let K be a field and $G \leq \mathrm{Aut}(K)$ be a finite group of n automorphisms $\sigma : K \to K$. Let $K_\circ = \mathrm{Fix}_G(K)$ be the fixed field of G. Then $K|K_\circ$ is a Galois extension of degree n with $G = \mathrm{Gal}(K|K_\circ)$.*

The classical Galois theory did not use Artin's view which emancipated the theory completely from polynomials. It used the permutation groups $\mathrm{Gal}(f|K)$. But the terminology of the 20th century, switching to the abstract groups $\mathrm{Gal}(L|K)$, simplified the presentation of the basic results considerably. The main theorem can be summarized in detail as follows:

THEOREM 3: *Let $L|K$ be a finite Galois extension of degree n. Let $G = \mathrm{Gal}(L|K)$ be its Galois group. Then G has exactly n elements and there is a bijection between the set $\mathfrak{S}(L|K)$ of subfields of $L|K$ and the set $\mathfrak{S}(G)$ of subgroups of G by forming isotropy groups and fixed fields:*

$$\begin{aligned} \mathfrak{S}(L|K) \ni M &\longmapsto M^\circ = \{\sigma \in G\,;\ \sigma|_M = \mathrm{id}_M\} = \mathrm{Gal}(L|M) \ \in \mathfrak{S}(G) \\ \mathfrak{S}(G) \ni H &\longmapsto H^\circ = \{a \in L\,;\ a^H = a\} \qquad \in \mathfrak{S}(L|K) \end{aligned}$$

These maps have the following properties for subfields M and subgroups H, if $H^\sigma = \sigma^{-1}H\sigma$ denotes for $\sigma \in G$ a conjugate subgroup of H and MM' denotes the smallest subfield containing M and M':

$$\begin{array}{ll}
(0) & K^\circ = G\ ,\quad L^\circ = \{\,\mathrm{id}_L\}\ .\quad G^\circ = K\ ,\quad \{\,\mathrm{id}_L\}^\circ = L \\
(1) & M^{\circ\circ} = M \qquad , \qquad H^{\circ\circ} = H \\
(2) & M \subseteq M' \implies M'^\circ \subseteq M^\circ\ ,\quad [M' : M] = [M^\circ : M'^\circ] \\
(3) & H \subseteq H' \implies H'^\circ \subseteq H^\circ\ ,\quad [H' : H] = [H^\circ : H'^\circ] \\
(4) & (MM')^\circ = M^\circ \cap M'^\circ \quad , \quad (M \cap M')^\circ = \langle M^\circ, M'^\circ \rangle \\
(5) & \langle H, H' \rangle^\circ = H^\circ \cap H'^\circ \quad , \quad (H \cap H')^\circ = H^\circ H'^\circ \\
(6) & \sigma \in G \implies (M^\sigma)^\circ = (M^\circ)^\sigma\ ,\quad (H^\sigma)^\circ = (H^\circ)^\sigma \\
(7) & M'|M \ \text{normal} \iff M'^\circ \ \text{normal in}\ M^\circ \\
& \text{and in this case we have}\quad \mathrm{Gal}(M'|M) \simeq M^\circ/M'^\circ = \mathrm{Gal}(L|M)/\,\mathrm{Gal}(L|M')
\end{array}$$

If $L|K$ is an infinite Galois extension, then $G = \mathrm{Gal}(L|K)$ is not only a group but has a topology, as already Dedekind in 1901 remarked, the topology of pointwise convergence on L. This makes G into a compact, totally disconnected group, so a profinite group, which can also seen by representing G as a projective limit of finite groups:

$$G = \varprojlim \mathrm{Gal}(M|K) \quad ,$$

where M runs over the subfields of $L|K$ which are finite Galois over K. Then Theorem 3 (without the statement about the number of elements of G) remains true, as Krull 1928 showed, if one restricts $\mathfrak{S}(G)$ to be the set of closed subgroups of G and understands the operation $\langle H, H' \rangle$ as building the smallest closed subgroup of G containing H and H'. This, by the way, was overlooked by Baer and Hasse in their appendix in [St30].

Galois groups are no special projective groups:

PROPOSITION 4 (Leptin): *Every profinite group is isomorphic to* $\mathrm{Gal}(L|K)$ *for some Galois extension* $L|K$.

One main topic in Galois theory, started with Hilbert in 1892, is the so-called **inverse problem of Galois theory**. It asks which finite groups are Galois groups over a given field K, i.e. to find all finite factor groups (= quotient groups) of the **absolute Galois group**

$$\mathrm{Gal}(K) = \mathrm{Gal}(K^{\mathrm{sep}}|K)$$

of K where K^{sep} is the **separable closure** of K, i.e. the maximal separable subfield of $\widetilde{K}|K$. Originally this question was put for $K = \mathbb{Q}$. A famous deep theorem in this respect is

THEOREM 5 (Shafarevich 1954): *Every finite solvable group is a factor group of* $\mathrm{Gal}(\mathbb{Q})$.

But the "complimentary" question

Which finite simple (nonabelian) groups occur as Galois group over $\mathbb{Q}$ *?*

is only partially solved with large gaps and a completion of this task is not to be seen. The methods and results of the 20th century are gathered in a book by Matzat and Malle from 1999, several new results have since appeared, but we are far from a complete answer. One nice result is already more than 100 years old:

THEOREM 6 (Hilbert 1892): *For any n the symmetric group S_n and the alternating group A_n are Galois groups over* $\mathbb{Q}$.

I will come to Hilbert's ideas of proof in the next section; they are the best useful tool for solving the inverse problem we have.

A more general formulation of the inverse problem of Galois theory is the following:

What is the structure of Gal(K) ?

Another important and wide open question is:

Which groups appear as absolute Galois groups ?

EXAMPLES:

1. If $\mathrm{Gal}(K) = 1$, then K is separably closed.

2. (Artin-Schreier 1926) If $\mathrm{Gal}(K) \neq 1$ is finite, then $|\,\mathrm{Gal}(K)| = 2$ and K is a field of characteristic 0 with an ordering and the following properties:

   a. Every positive element is a square.

   b. Every polynomial in $K[x]$ of odd degree has a zero in K.

   Conversely such fields (they are called **real closed fields** because they have the same elementary properties as the real numbers) have a 2-element Galois group with $\widetilde{K} = K(\sqrt{-1})$.

3. (Geyer 1969) Every abelian subgroup of $\mathrm{Gal}(\mathbb{Q})$ is procyclic. (In general any abelian profinite group A can occur as absolute Galois group, if it does not contradict example 2, i.e. if the torsion part of A is 0 or $\mathbb{Z}/2$.)

4. If $K = \mathbb{F}_q$ is a finite field, then $\mathrm{Gal}(K)$ is a free profinite group with one generator, namely the **Frobenius automorphism**

$$F:\ x \mapsto x^q \quad .$$

5. If $K = \mathbb{C}((x))$ is the field of formal power series over $\mathbb{C}$, then $\widetilde{K} = \bigcup_n \mathbb{C}((x^{1/n}))$ and $\mathrm{Gal}(K)$ is again the free procyclic group, a generator is given by

$$\gamma:\ x^{1/n} \mapsto e^{2\pi i/n}\cdot x^{1/n} \qquad (n \in \mathbb{N}).$$

6. If $K = \mathbb{C}(x)$ then $\mathrm{Gal}(K)$ is a free profinite group with $|\mathbb{C}|$ generators (Riemann).
7. The same is true if $\mathbb{C}$ is replaced by any algebraically closed field K of characteristic zero (Grothendieck).
8. The same is true in any characteristic (Pop 1995, ...)
9. *Shafarevich conjecture*: The absolute Galois group of the maximal abelian extension of $\mathbb{Q}$, the cyclotomic field

$$\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(e^{2\pi i/n};\ n \in \mathbb{N}) \quad ,$$

   is a free profinite group of countable rank.

The question which finite groups are factors of $\mathrm{Gal}(K)$ can be refined to the following question, which gives more insight into the structure of $\mathrm{Gal}(K)$ then just the list of finite factors:

> Let $L|K$ be a finite Galois extension with group A, let B be a finite extension of A, i.e. a finite group with an epimorphism $\alpha:\ B \twoheadrightarrow A$. Does there exist an extension $M|L$ such that M is Galois over K with group B such that $\alpha:\ B \to A$ becomes the restriction map $\mathrm{res}_L:\ \mathrm{Gal}(M|K) \to \mathrm{Gal}(L|K)$?

We formulate this question usually in the following way: Is the **embedding problem**

$$\begin{tikzcd}
 & \mathrm{Gal}(K) \arrow[d] & \\
B \arrow[r, "\alpha"] & A = \mathrm{Gal}(L|K) \arrow[r] & 1
\end{tikzcd}$$

solvable? A **solution** is an epimorphism $\gamma : \mathrm{Gal}(K) \to B$ which makes the diagram commutative. A **weak solution** is a not neccessarily surjective homomorphism γ with the same property. Kern α is called the **kernel** of the embedding problem.

Example: The embedding problem

$$\begin{tikzcd}
 & \mathrm{Gal}(\mathbb{Q}) \arrow[d] & \\
\mathbb{Z}/4 \arrow[r, two heads] & \mathbb{Z}/2 = \mathrm{Gal}(\mathbb{Q}(i)|\mathbb{Q}) \arrow[r] & 0
\end{tikzcd}$$

is not even weakly solvable: Let $\sigma \in \mathrm{Gal}(\mathbb{Q})$ be a complex conjugation, so an element of order 2 whose restriction generates $\mathbb{Z}/2$. Then the restricted (local) embedding problem

$$\begin{tikzcd}
 & \mathbb{Z}/2 \arrow[d, "\simeq"] \\
\mathbb{Z}/4 \arrow[r, two heads] & \mathbb{Z}/2
\end{tikzcd}$$

has no weak solution, because any weak solution has to be a strong solution (only the full subgroup of $\mathbb{Z}/4$ maps onto $\mathbb{Z}/2$, we have a **Frattini cover**) — and there is no epimorphism $\mathbb{Z}/2 \twoheadrightarrow \mathbb{Z}/4$.

Solving embedding problems is, besides Hilbert's theorem of the next section, the most important tool to construct field extension with a given group. Shafarevich's proof of theorem 5 is a very, very long iteration of solving embedding problems with abelian kernels. One example of solving embedding problems with cyclic kernels of order p to get cyclic p-groups in characteristic p is given in the last section of this course.

4. Hilbertian fields

The polynomial $x^4 + 1 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, but all its reductions modulo p are reducible over $\mathbb{F}_p$ (because $\mathrm{Gal}(x^4 + 1|\mathbb{Q})$ is not cyclic).

Absolute irreducible polynomials behave differently, as the following rather elementary proposition shows, proved several times by different people and called theorem of Bertini-Noether in [FJ 9.4.3].

Proposition 1: *Let R be an integral domain and $f \in R[x_1, \dots, x_n]$ be an absolutely irreducible polynomial. Then for almost all (in the sense of Zariski topology) prime ideals $\mathfrak{p} \in \mathrm{Spec}(R)$ the following holds where $\kappa(\mathfrak{p}) = \mathrm{Quot}(R/\mathfrak{p})$ denotes the residue field of $\mathfrak{p}$:*

The polynomial $f \bmod \mathfrak{p}$ is absolutely irreducible in $\kappa(\mathfrak{p})[x_1, \dots, x_n]$.

Whereas the reduction of coefficients conserve absolute irreducibility this is in general no more true for substitution of variables by elements in the field: An absolutely irreducible polynomial $f \in \mathbb{C}[x, y]$, monic in y with $\deg_y(f) > 1$ obviously becomes a reducible polynomial $f(x, \eta) \in \mathbb{C}[x]$ for all $\eta \in \mathbb{C}$.

There are fields where this phenomenon does not appear, the Hilbertian fields which were named after Hilbert's results from 1892 (a modern approach can be found in chap.12, 13 and 15 of [FJ]).

Definition 1: A field K is called **Hilbertian**, if for any irreducible polynomial $f \in K[x, y]$, separable in y, there are infinitely many elements $\xi \in K$ such that $f(\xi, y)$ is irreducible in $K[y]$.

Remarks:

1. In the language of valuations (places) a field K is Hilbertian, iff vor every finite separable field extension $L|K(x)$ — the root field of f — there are infinitely many rational places v of $K(x)|K$ which are completely inert in L, i.e. they have a (unique) continuation w on L with $[\kappa(w) : \kappa(v)] = [L : K(x)]$, where $\kappa(w)$ denotes the residue field of w, so $\kappa(v) = K$. Since the ramification of $L|K(x)$ is finite, we may even assume that $\kappa(x)|\kappa(v)$ is separable.
2. In definition 1 one can assume f is monic, of degree ≥ 2 and Galois in y, i.e. $L|K(x)$ is a proper Galois extension.
3. In definition 1 one can moreover assume f is absolutely irreducible, i.e. $L|K$ is regular.
4. If K is Hilbertian and $f_1, \dots, f_r$ are finitely many irreducible, in y separable polynomials in $K[x, y]$, there are infinitely many $\xi \in K$ such that all polynomials $f_1(\xi, y)$, $\dots$, $f_r(\xi, y)$ are irreducible in $K[y]$.

Theorem 1 (**Hilbert's irreducibility theorem** 1892): *The field $\mathbb{Q}$ and all its finite extensions K are Hilbertian.* More precisely Hilbert showed: *Let $f \in K[x, y]$ be* *irreducible. The $\xi \in \mathbb{N}$ which give a reducible polynomial $f(\xi, y) \in K[y]$ form a subset of $\mathbb{N}$ of density zero:*

$$\lim_{n\to\infty} \frac{\#\{\xi \in \mathbb{N}\,;\ \xi \le n\,,\ f(\xi,y)\ \textit{ is reducible}\}}{n} = 0 \quad .$$

The example $f = x - y^2$ shows that there can be infinitely many exceptions, the square numbers. Later considerations showed that the exceptional set never can be more dense than the set of squares.

The following theorem gives other examples of Hilbertian fields, for more look at [FJ].

Theorem 2:

a) *For every field $K_\circ$ the rational function field $K = K_\circ(t)$ is Hilbertian. If $K_\circ$ is a finite field, one gets a density result as in theorem 2. If $K_\circ$ is infinite, one gets an even better result: If $f \in K[x,y]$ is irreducible then the set of $(a,b) \in K_\circ^2$ such that $f(a+bt, y)$ is irreducible in $K[y]$ form a Zariski dense subset of $K_\circ^2$.*

b) Corollary to a): *Let K be Hilbertian and $f \in K[x_1,\ldots,x_n,y]$ be irreducible and separable in y. Then the set*

$$\{(a_1,\ldots,a_n) \in K^n\,;\ f(a_1,\ldots,a_n,y)\ \textit{ is irreducible in }\ K[y]\}$$

is Zariski dense in K^n.

c) *If K is Hilbertian and $L|K$ is a finite extension, then for each irreducible $f \in L[X,Y]$, separable in Y there are infinitely many $\xi \in K$ such that $f(\xi, Y)$ is irreducible in $L[Y]$.*[2)]

d) *Every finite extension of a Hilbertian field is Hilbertian.*

e) *Every finitely generated infinite field is Hilbertian.*

f) *Let K be Hilbertian and $L|K$ be a Galois extension. Then every proper finite separable extension of L is Hilbertian (Weissauer 1982).*

g) *Let K be Hilbertian and $L|K$ be a Galois extension with group G. In the following cases L is again Hilbertian:*

   1. *G is small, i.e. for each n there are only finitely many subgroups of index n in G.*
   2. *G is Abelian (Kuyk 1970). Therefore no algebraic extension of a finite field is Hilbertian.*
   3. *G is pro-nilpotent, but not a pro-p-group.*

h) *If $K_\circ$ is an arbitrary field, then the power series field $K_\circ((t))$ is not Hilbertian, but for each $n > 1$ the field $K((t_1,\ldots,t_n))$ is Hilbertian (Weissauer 1982).*

[2)] Proof: Let $N|L(x)$ be a finite separable extension. Let L_{sep} resp. N_{sep} be the maximal separable subfield of $L|K$ resp. $N|L(x)$. Then L and N_{sep} are linearly disjoint over L_{sep} and $N = LN_{\text{sep}}$. Let v be a K-rational place with a separable totally inert continuation w_{sep} on N_{sep}. Then the unique extension w of w_{sep} to N is totally inert with purely inseparable residue field extension, and the restriction $w|_{L(x)}$ is L-rational and totally inert in N. ∎

The fact that a field is Hilbertian has strong consequences for the inverse Galois problem over the field K as already Hilbert stressed in 1892. The reason is the following

THEOREM 3: *Let K be an Hilbertian field and $L|K(t)$ be a finite Galois extension with group G. Then G is also a Galois group over K, i.e. a finite factor group of $\mathrm{Gal}(K)$. If $L|K$ is regular, then also all powers G^n with $n \in \mathbb{N} \cup \{\infty\}$ can be realized as Galois groups over K.*

Proof: Let $L = K(t,u)$ with an irreducible polynomial equation $f(t,u) = 0$ with $f \in K[T,U]$. Then f is a separable polynomial in the variable U so there are many $\tau \in K$ (*specializations*) such that $\overline{f} = f(\tau, U) \in K[U]$ is irreducible. For almost all τ the specialized polynomial $\overline{f}$ is again Galois over K as f was Galois over $K(t)$. In general a specialization $t \mapsto \tau$ gives an embedding $\mathrm{Gal}(\overline{f}|K) \hookrightarrow \mathrm{Gal}(f|K(T))$ of the specialized Galois group as decomposition group of the situation over $K(t)$. But here both Galois groups are regular permutation groups of the same degree, so $G = \mathrm{Gal}(\overline{f}|K)$ which gives the first claim: We get a Galois extension $L|K$ with group G. If $L|K$ is regular, i.e. f is absolutely irreducible, then f remains irreducible over L and by Hilbert's theorem 2.c we get a specialization $t \mapsto \tau_2$ which lead to a Galois polynomial $f(\tau_2, U) \in K[U]$ which is irreducible over L, so gives a linearly disjoint realization of the group G, so a realization of the group G^2. Continuing we get the result. ∎

EXERCISE: Simplify the above proof by using valuations!

CORLLARY (van der Waerden 1933): *Let $\mathcal{P}_n$ be the space of monic polynomials*

$$f = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \qquad (a_\nu \in \mathbb{Z})$$

of degree n with integral coefficients. Then the set of polynomials $f \in \mathcal{P}_n$ with $\mathrm{Gal}(f|\mathbb{Q}) = S_n$ has density 1.

Idea of proof: The generic polynomial f has Galois group S_n over $\mathbb{Q}(a_1, \ldots, a_n)$. Specialising the a_ν to integers gives usually the same Galois group. ∎

This corollary shows that it is not an easy task to produce other Galois groups than the symmetric groups just by trying random polynomials. But theorem 3 says how you can succeed to find a polynomial over $\mathbb{Q}$ with group G: You have to find such a polynomial over $\mathbb{Q}(t)$. Now $\mathbb{Q}(t)$ is the rational function field of the line C, and you can apply methods from geometry to produce coverings of C with Galois group G. In this way Hilbert got the alternating groups as Galois groups over $\mathbb{Q}$ by first contructing A_n-coverings over the Riemann sphere; then to see that they can be defined over $\mathbb{Q}$, so you get an A_n-covering of $\mathbb{Q}(t)$; and then applying the irreducibility theorem.

5. PAC fields

The examples 5 to 8 (and possibly 9) in §3 are fields whose absolute Galois group is a free profinite group. Therefore every embedding problem over such a field is weakly solvable. But these are not the only profinite groups with this property. The following proposition is taken from Serre (1964) and Gruenberg (1967):

Proposition 1: *For a profinite group G the following properties are equivalent:*

(i) *Every exact sequence*

$$1 \longrightarrow P \longrightarrow E \longrightarrow G \longrightarrow 1 \tag{$*$}$$

of profinite groups splits.

(ii) *Sequences of type $(*)$ split it P is a finite elementary abelian group.*

(iii) *For every exact sequence*

$$1 \longrightarrow P \longrightarrow E \longrightarrow W \longrightarrow 1 \tag{$\dagger$}$$

of profinite groups, any homomorphism $\alpha : G \to W$ can be lifted to a homomorphism $G \to E$.

(iv) *This lifting property holds for all sequences $(\dagger)$ for which E is finite, P is elementary abelian and α is surjective.*

(v) *For all primes p the p-Sylowgroups of G are free pro-p-groups.*

(vi) *For all primes p the cohomological p-dimension of G is at most 1,*

$$\mathrm{cd}_p(G) \leq 1 \quad ,$$

i.e. $H^n(G, A) = 0$ for all $n \geq 2$ where A is a discrete G-module and a p-primary abelian group.

(vii) *For all primes p we have $H^2(G, A) = 0$ for all simple G-modules A with $pA = 0$.*

Definition 1: A profinite group is called **projective**, if it satisfies the properties in theorem 1.

Definition 2: A field K is called a **PAC-field** or **pseudo algebraically closed** if every non-empty variety V over K has a rational point: $V(K) \neq \varnothing$. A direct consequence is: $V(K)$ is Zariki dense in V if K is PAC.[3)]

Theorem: (Ax 1968) If K is a PAC-field, then $\mathrm{Gal}(K)$ is projective.

Before we can prove this we need a

[3)] The concept was seen by James Ax in [Ax67]. He showed that infinite algebraic extensions and non trivial ultraproducts of finite fields are PAC. The name is from Moshe Jarden in [Fr73].

Lemma: *Let $L|K$ be a finite Galois extension with Galois group G. Let B be a finite group with m elements and α be an epimorphism*

$$\alpha : \ B \to G \quad .$$

Then there is a Galois extension $F|E$ with Galois group B, such that $E|K$ is a finitely generated regular extension and $F|L$ is a purely transcendental extension of transcendence degree m, and

$$\alpha = \mathrm{res}_{F|L} : \ \mathrm{Gal}(F|E) \to \mathrm{Gal}(L|K) \quad .$$

Proof:

$$\begin{tikzcd}
\widetilde{K} \arrow[dd, dotted, no head] & \\
 & F \arrow[d, no head] \\
L \arrow[r, no head] & LE \\
K \arrow[u, no head] \arrow[r, no head] & E \arrow[u, no head]
\end{tikzcd}$$

Let $X = \{x^{\beta} ; \ \beta \in B\}$ be a set of m indeterminates over K. Then B operates on X via $(x^{\beta})^{\beta'} = x^{\beta\beta'}$. Put $F = L(X)$. Then B operates on L via α, on X as above, so on F. Let

$$E = \mathrm{Fix}_B(F)$$

be the fixed field of this action. Then $F|E$ is Galois with group B by Artin, and $\mathrm{res}_{F|L}(\beta) = \alpha(\beta)$, so $L \cap E = K$, so L and E are linearly disjoint over K. The purely transcendental extension $F|L$ and $\widetilde{K} = \widetilde{L}$ are linearly disjoint over L, so especially LE and $\widetilde{L}$ are linearly disjoint over L. From the tower property follows that E and $\widetilde{L} = \widetilde{K}$ are linearly disjoint, so $E|K$ is regular. Moreover $E|K$ as subfield of the finitely generated extension $F|K$ is finitely generated. ∎

Proof of the Theorem (Haran): We have to solve weakly a finite embedding problem of the following type: Let A and B be finite groups and let

$$\rho : \ \mathrm{Gal}(K) \twoheadrightarrow A \qquad \text{and} \qquad \alpha : \ B \twoheadrightarrow A$$

be epimorphisms. Then there exists a homomorphism $\beta : \ \mathrm{Gal}(K) \to B$ such that $\rho = \alpha \circ \beta$.

Let L be the fixed field of Kern(ρ) in K^{sep}. Then $L|K$ is Galois and the Galois group can be identified with A such that $\rho : \ \mathrm{Gal}(K) \to A = \mathrm{Gal}(L|K)$ is the restriction map res_L. In the lemma we constructed a field extension $F|E$ with $E|K$ regular, $L \subseteq F$, $\mathrm{Gal}(F|E) = B$ and $\alpha = \mathrm{res}_L$. Now since $E|K$ is regular, E is the function field of a normal variety V over K. Then $V \times L$ is the normalization of V in LE. Let W

be the normalization of V in F. Shrinking V to an open subset we may assume that $W|V$ is unramified. Let $P \in V(K)$ be a rational point (K is PAC) and $Q \in W$ be a point above V with residue field $M = \kappa(Q)$. Then the extension $M|K$ is Galois, contains L and $\mathrm{Gal}(M|K) = \mathrm{Gal}(\kappa(Q)|\kappa(P))$ is isomorphic to the decomposition group $\{\sigma \in B\,;\ Q^\sigma = Q\}$, a subgroup of $B = \mathrm{Gal}(W|V)$. This gives a homomorphism

$$\beta:\ \mathrm{Gal}(K) \overset{\mathrm{res}_M}{\twoheadrightarrow} \mathrm{Gal}(M|K) \hookrightarrow B$$

such that $\alpha \circ \beta = \mathrm{res}_L$ as desired. ∎

Remark: The examples $K = \mathbb{F}_p$ or $K = \mathbb{C}((x))$ show that a field whose absolute Galois group is projective, need not be a PAC field.

Addendum (Lubotzky & v.d.Dries 1981): *Every projective profinite group G is the absolute Galois group of a PAC field.*

6. Construction of cyclic field extensions

The realization of cyclic groups is one of the first exercises in Inverse Galois Theory. I will treat this here in the case that the base field is a rational function field $K(x)$ over an arbitrary field K.

Theorem: *For any field K and any natural number n there are Galois extensions $L|K(x)$ with*

$$\mathrm{Gal}(L|K(x)) = \mathbb{Z}/n \quad .$$

Moreover one may choose L as a subfield of $K((x))$, so $L|K$ is regular.

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 $K(x)$.

Notation: Let $\mathrm{char}\, K = p \geq 0$. let $E = K(x)$ be the rational function field over K. Let $n > 1$. If $p \nmid n$ let $\zeta = \zeta_n$ be a primitive n^{th} root of unity in $\widetilde{K}$.

The proof of the theorem will done in three steps: First by a Kummer extension if $\zeta \in K$. Then by a twisted Kummer extension if $p \nmid n$ but $\zeta \notin K$. At last the case $p|n$ will be handled by an iteration of Artin-Schreier extensions $y^p - y = a$.

Lemma 1: *If $\zeta \in K$ and $a \neq b$ in $K^\times$, then there is*[4] *a cyclic extension $F|E$ of degree n with $F \subseteq K((x))$, which ramifies only at $x = a$ and $x = b$, the ramification index being n.*

Proof: Let $y \in K[[x]]$ be such that

$$y^n = \frac{1 - a^{-1}x}{1 - b^{-1}x} = \Big(1 - \frac{x}{a}\Big) \cdot \Big(1 + \frac{x}{b} + \frac{x^2}{b^2} + \ldots\ldots\Big) \quad .$$

Then $E(y)|E$ is a cyclic extension of degree n, contained in $K((x))$, with full ramification at $x = a$ and $x = b$. ∎

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 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 $F|E$ of degree n inside $K((x))$ which ramifies only at $x = a\zeta^\gamma$ for $\gamma \in G$, 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

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

[4] If you wonder where you get two non zero elements in $\mathbb{F}_2$ remark that $\zeta \notin \mathbb{F}_2$.

This cyclic extension $E'(y)$ of $E' := L(x)$ does not come from a cyclic extension of E, since it is not Galois over E (look at the ramification). 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

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

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 for $\tau \in G = \mathrm{Gal}(L(\!(x)\!)|K(\!(x)\!))$

$$z^\tau = z^{\chi(\tau)} \cdot f_\tau(x) \qquad \text{with } \ f_\tau \in L(x) \quad .$$

So the field F' is invariant under G. Let F be the fixed field of G in F'.

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

The cyclic group $\Gamma = \mathrm{Gal}(F'|E')$ is generated by the element ω with $z^\omega = \zeta z$. The straightforward identity

$$z^{\omega\tau} = (\zeta z)^\tau = \zeta^{\chi(\tau)} z^{\chi(\tau)} f_t(x) = \Big(z^{\chi(t)} f_\tau(x)\Big)^\omega = z^{\tau\omega}$$

for $\tau \in G$ shows that $F'|E$ is abelian with

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

So $F \subseteq K(\!(x)\!)$ is a cyclic extension of E of degree n with ramification at $x = a\zeta^\sigma$ for all $\sigma \in G$. ∎

Remark: Let $F|K(x)$ be a cyclic extension of degree n as in Lemma 2 with

$$m = [K(\zeta_n) : K] = |G| \quad .$$

let $\widetilde{K}$ be the algebraic closure of K. If $x = a$ with $a \in \widetilde{K}$ is a fully ramified place in $F\widetilde{K}|\widetilde{K}(x)$ then $[K(a) : K] \geq m$ and there are at least m fully ramified, over K conjugate places in $F\widetilde{K}|\widetilde{K}(x)$.

Lemma 3 (Witt 1936): *Let $p > 0$, $n \in \mathbb{N}_0$ 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 $F \subseteq F' \subseteq K(\!(x)\!)$.*

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

$$(*) \qquad a - a^{\sigma} = c = b - b^p \quad .$$

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 $(*)$, 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 $F \subseteq F' \subseteq K((x))$. ∎

Corollary: *Let* 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.

Proof: By replacing K by the algebraic closure of $\mathbb{F}_p$ in K we may assume K to be perfect. Iteration of Lemma 3 gives a cyclic extension of $K(x)$ in $K((x))$ of degree p^n which has, since K is perfect, ramification index p^n at $x = \infty$ — for there is no unramified proper extension of $K(x)$. By the Möbius transformation

$$x = \frac{z}{z-a} = -\sum_{\nu=1}^{\infty} \frac{z^{\nu}}{a^{\nu}}$$

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

8. References

[Ab1826] Niels Hendrick Abel: *Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen*, Journal für die reine und angewandte Mathematik **1** (1826), 65-84

[Ar42] Emil Artin: *Galois Theory*, University of Notre Dame Press 1942

[AS26] Emil Artin & Otto Schreier: *Algebraische Konstruktion reeller Körper*, Abhandlungen aus dem mathematischen Seminar der Universität Hamburg **5** (1926), 85–99 = E. Artin: Collected Papers (Reading 1965), 258–272

[Ax67] James Ax: *Solving diophantine problems modulo every prime*, Annals of Mathematics **85** (1967), 161–183

[Ax68] James Ax: *The elementary theory of finite fields*, Annals of Mathematics **88** (1968), 239-271

[Bo28] Salomon Bochner: *Fortsetzung Riemannscher Flächen*, Mathematische Annalen **98** (1928), 406–421

[Br11] Luitzen E. J. Brouwer: *On the structure of perfect sets of points*, Proceedings of the Section of Sciences, Koningklijke Akademie van Wetenschapen te Amsterdam **12** (1910), 785–794 & **14** (1911), 137–147

[Ca1545] Hieronymus Cardano: *Ars magna sive de regulis algebraicis ...*, Nürnberg 1545

[Bo1572] Rafael Bombelli: *L'Algebra ...*, Bologna 1572

[Bo39] Nicolas Bourbaki: *Éléments de mathématique. Théorie des Ensembles: Fascicule de Résultats*, Paris 1939

[Bo81] Nicolas Bourbaki: *Éléments de mathématique. Algèbre, Chapitres 4 à 7*, Paris 1981

[Ca1847] Augustin-Louis Cauchy: *Mémoire sur une nouvelle théorie des imaginaires, et sur les racines symboliques des équations et des équivalences*, Comptes Rendus hebdomadaires des séances de l'Académie des Sciences de Paris **24** (1847), 1120 = Œuvres complètes (1) **10**, 312–323

[De1857] Richard Dedekind: *Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus*, Journal für die reine und angewandte Mathematik **54** (1957), 1–26

[DW1882] Richard Dedekind & Heinrich Weber: *Theorie der algebraischen Funktionen einer Veränderlichen*, Journal für die reine und angewandte Mathematik **92** (1882), 181–290 = Dedekind: Gesammelte Werke I (Braunschweig 1930), 238–350

[Di1871] Peter Gustav Lejeune-Dirichlet: *Vorlesungen über Zahlentheorie*, herausgegeben und mit Zusätzen versehen von Richard Dedekind, 2. Auflage, Braunschweig 1871

[Di1894] Peter Gustav Lejeune-Dirichlet: *Vorlesungen über Zahlentheorie*, herausgegeben und mit Zusätzen versehen von Richard Dedekind, 4. Auflage, Braunschweig 1894

[De01] Richard Dedekind: *Über die Permutationen des Körpers aller algebraischen Zahlen*, Festschrift aus Anlaß des 150jährigen Bestehens der Göttinger Gesellschaft der Wissenschaften, 1901, Abhandlungen der mathematisch-physikalischen Klasse **1901**, 1–17 = Werke **2** (Braunschweig 1931), 272–292

[FJ] Michael D. Fried & Moshe Jarden: *Field Arithmetic*, 3rd Edition revised by Moshe Jarden, Ergebnisse der Mathematik (3) **11**, Berlin–Heidelberg 2008

[Fr73] Gerhard Frey: *Pseudo algebraically closed fields with non-archimedean real valuations*, Journal of Algebra **26** (1973), 202–207

[Ga1897] Évariste Galois: *Œuvres mathématiques*, Paris 1897

[Gau1801] Carl Friedrich Gauß: *Disquisitiones arithmeticae*, Leipzig 1801

[Gau1831] Carl Friedrich Gauß: *Brief an den Astronomen Schumacher in Altona*, Werke **8** (Leipzig 1900), 216

[Gau1832] Carl Friedrich Gauß: *Theoria Residuorum Biquadraticorum, Commentatio Secunda*, Comm. Soc. Reg. Sci. Göttingen **7** (1832), 1–34 = Werke **2**, 93–149

[Ge69] Wulf-Dieter Geyer: *Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist*, Journal of Number Theory **1** (1969), 346-374

[Gr67] Karl W. Gruenberg: *Projective profinite groups*, Journal of the London Mathematical Society **42** (1967), 155–165

[Ha1837] Sir William Rowan Hamilton: *Theory of Conjugate Functions, or Algebraic Couples; with a Preliminary and Elementary Essay on Algebra as the Science of Pure Time*, Transactions of the Royal Irish Academy **17** (1837), 293–422 = Mathematical Papers III, 3–96

[Ha09] Felix Hausdorff: *Die Graduierung nach dem Endverlauf*, Abhandlungen der Königlichen Sächsischen Gesellschaft der Wissenschaften zu Leipzig, Mathematisch-physikalische Klasse **31** (1909), 295–334

[Ha14] Felix Hausdorff: *Grundzüge der Mengenlehre*, Berlin 1914

[Ha27] Felix Hausdorff: *Grundzüge der Mengenlehre*, 2. Auflage, Berlin 1927

[He08] Kurt Hensel: *Theorie der algebraischen Zahlen*, Leipzig 1908

[HL02] Kurt Hensel & Georg Landsberg: *Theorie der algebraischen Funktionen*, Leipzig 1902

[Hi1892] David Hilbert: *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, Journal für die reine und angewandte Mathematik **110** (1892), 104–129 = Gesammelte Abhandlungen II (Berlin 1933), 264–286

[Hi1899] David Hilbert: *Grundlagen der Geometrie*, Leipzig 1899

[Kr1879] Leopold Kronecker: *Einige Entwicklungen aus der Theorie der algebraischen Gleichungen*, Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin **1879**, 205–229 = Werke **4** (Leipzig 1929), 75–96

[Kr1882] Leopold Kronecker: *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, Festschrift zu Kummer's 50jährigem Doctor-Jubiläum (10.9.1881), Berlin 1882 = Journal für die reine und angewandte Mathematik **92** (1881/82), 1–122 = Werke **2** (Leipzig 1897), 237–387

[Kr1887] Leopold Kronecker: *Ein Fundamentalsatz der allgemeinen Arithmetik*, Journal für die reine und angewandte Mathematik **100** (1887), 490–510 = Werke $\mathbf{3}_1$ (Leipzig 1899), 209–240

[Kr28] Wolfgang Krull: *Galoissche Theorie der unendlichen algebraischen Erweiterungen*, Mathematische Annalen **100** (1928), 687-698

[Ku22] Kazimierz Kuratowski: *Une méthode d'élimination des nombres transfinis des raisonnements mathématiques*, Fundamenta Mathematica **3** (1922), 76–108

[Ku70] Willem Kuyk: *Extensions de corps hilbertiens*, Journal of Algebra **14** (1970), 112–124

[Ku75] Ernst Eduard Kummer: *Collected Papers I*, Berlin 1975

[La93] Serge Lang: *Algebra*, 3rd edition, Addison Wesley 1993

[LD81] Alex Lubotzky & Lou van den Dries: *Subgroups of free profinite groups and large subfields of* $\tilde{\mathbb{Q}}$, Israel Journal of Mathematics **39** (1981), 25–45

[Lü1876] Jacob Lüroth: *Beweis eines Satzes über rationale Kurven*, Mathematische Annalen **9** (1876), 163–165

[MM] Gunter Malle & B. Heinrich Matzat: *Inverse Galois Theory*, Berlin 1999

[Mo1831] Augustus de Morgan: *On the Study and Difficulties of Mathematics*, London 1831

[Mo1893] Eliakim Hastings Moore: *Galois-field of order* $s = q^n$, Bulletin of the New York Mathematical Society **3** (November 1893), 75 = Papers read at the international mathematical congress, Chicago 1893 (1896), 208–226

[Mo32] Robert Lee Moore: *Foundations of Point Set Theory*, American Mathematical Society Colloquium Publications **13**, New York 1932

[No27] Emmy Noether: *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Mathematische Annalen **96** (1927), 26–61 = Gesammelte Abhandlungen (Berlin 1983), 493–528

[Po95] Florian Pop: *Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture*, Inventiones mathematicae **120** (1995), 555–578

[Pr28] Heinz Prüfer: *Neue Begründung der algebraischen Zahlentheorie*, Mathematische Annalen **94** (1928), p.198

[Ri1851] Bernhard Riemann: *Grundlagen für eine allgemeine Theorie der Functionen einer veränderlichen complexen Grösse*, Inauguraldissertation Göttingen 1851 = Werke (Leipzig 1876), 3–48

[Se64] Jean-Pierre Serre: *Cohomologie Galoisienne*, Springer LNM **5**, Berlin 1964

[1866] Joseph-Alfred Serret: *Cours d'Algèbre Supérieure*, Gauthier-Villars, Paris ^{3}1866

[Sh54] Igor R. Shafarevich: *Construction of fields of algebraic numbers with given solvable Galois group*, Izvestija Akad. Nauk SSSR Ser. Mat. **18**:6 (1954), 525–578

[St1857] Karl Georg Christian von Staudt: *Beiträge zur Geometrie der Lage. Zweites Heft*, Nürnberg 1857

[St10] Ernst Steinitz: *Algebraische Theorie der Körper*, Journal für die reine und angewandte Mathematik **137** (1910), 167-309

[St30] Ernst Steinitz: *Algebraische Theorie der Körper*, neu herausgegeben von Reinhold Baer und Helmut Hasse, de Gruyter, Berlin 1930

[Ve1891] Guiseppe Veronese: *Fondamenti di geometria*, Padova 1891; deutsch: *Grundzüge der Geometrie*, Leipzig 1894

[Wa30] Bartel Leendert van der Waerden: *Moderne Algebra I*, Berlin 1930

[Wa31] Bartel Leendert van der Waerden: *Moderne Algebra II*, Berlin 1931

[Wa33] Bartel Leendert van der Waerden: *Die Seltenheit der Gleichungen mit Affekt*, Mathematische Annalen **109** (1933), 13–16

[We1893] Heinrich Weber: *Untersuchungen über die allgemeinen Grundlagen der Galoisschen Gleichungstheorie*, Mathematische Annalen **43** (1893), 521

[We1895] Heinrich Weber: *Lehrbuch der Algebra I*, Braunschweig 1895

[We46] André Weil: *Foundations of Algebraic Geometry*, American Mathematical Society Colloquium Publications **29**, New York 1946

[We82] Rainer Weissauer: *Der Hilbertsche Irreduzibilitätssatz*, Journal für die reine und angewandte Mathematik **334** (1982), 203–220

[Wi36] Ernst Witt: *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, Journal für die reine und angewandte Mathematik **174** (1936), 237–245

[Ze04] Ernst Zermelo: *Beweis, daß jede Menge wohlgeordnet werden kann*, Mathematische Annalen **59** (1904), 514–516

[Zo35] Max Zorn: *A remark on method in transfinite algebra*, Bulletin of the American Mathematical Society **41** (1935), 667-670