Fields Institute Communications
Volume 00, 0000

About Merckel's lemma

Henri Lombardi
Laboratoire de Mathématiques, (UMR CNRS 6623), UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANÇON cedex, France.
lombardi@math.univ-fcomte.fr

Abstract. We give a simple constructive proof of Merckel's lemma (used in the theory of p-adic fields).

1 Introduction

Given an infinite field k and a rational function $\varphi(X) \in k(X)$ whose derivative is nonzero, Merckel's lemma says that X belongs to the field generated by k and all finite elements $\varphi(\psi(X))$ for $\psi(X) \in k(X)$. An easy consequence is that, if k is an infinite subfield of a field K, then $k(\varphi(K)) = K$.

This result is used in the theory of p-adic fields [2]. In section 6, the authors consider a p-valued field k, with π a prime element. If the residue field $\overline{k}$ has q elements, given two positive integers e and f, the π-adic Kochen operator over k of type (e, f) is defined by

$$\gamma(X) = \frac{1}{\pi}\ \left(\frac{X^q - X}{(X^q - X)^2 - 1}\right)^e .$$

Let S be the ring of integers in k. When K is an extension of k, the γ-Kochen ring R is defined as the ring of quotients of the form $\frac{b}{1+\pi\, c}$ where $b, c \in S[\gamma(K)]$ and $1 + \pi\, c \neq 0$. The quotient field of the Kochen ring is $k(\gamma(K))$ and it is important to be able to assert that this quotient field is in fact equal to K.

An abstract proof of Merckel's lemma is given in an appendix p. 153–158 of [2]. We give here a simple proof which allows to compute an explicit formula for any φ.

2 Some easy particular cases

We call Δ the operator on $k(X)$ defined by

$$\Delta(\psi(X)) = \psi(X + 1) - \psi(X)$$

and we define, for any natural integer i, Δ^i as $\Delta \circ \cdots \circ \Delta$ (i times).

It is clear that $\Delta^i(\psi)$ is a $\mathbb{Z}$-linear combination of the elements $\psi(X + j)$ for $j = 0, \ldots, i$.

1991 *Mathematics Subject Classification.* 12E05, 12J12.

The polynomial case in zero characteristic. When φ is a polynomial of degree d, and $d!$ is invertible in k, then Merckel's lemma is an immediate consequence of:

Lemma 2.1 *Let k be a commutative ring and $P \in k[X]$ be a polynomial of degree d with leading coefficient c_d. Assume that $d!\,c_d$ is invertible (e.g., k is a field with characteristic zero) then $X = \frac{1}{d!\,c_d}\,\Delta^{d-1}(P) + a$ for some constant $a \in k$.*

A very simple formula for Merckel's lemma in an interesting particular case. Here we consider a slight variant of the Kochen operator

$$\gamma(X) = \frac{1}{p}\ \frac{X^p - X}{(X^p - X)^2 - 1}$$

(this is the one given in the introduction when $q = p$ and $e = 1$). We can replace $X^p - X$ by $A_p(X) = X(X+1)\cdots(X+p-1)$. We get an operator $\tilde{\gamma}(X)$ playing the same role as the Kochen operator for the theory of p-adic fields.

We show how to express X as an explicit rational function of the $\tilde{\gamma}(X+j)$'s for $j = 0, 1, \ldots, p$.

We have

$$\lambda(X) := \frac{1}{p\tilde{\gamma}(X)} = A_p(X) - \frac{1}{A_p(X)}.$$

Then we remark that

$$\Delta(1/A_n(X)) = -n/A_{n+1}(X).$$

So we get

$$\Delta^p(\lambda(X)) = p! + \frac{(-1)^{p+1}p(p+1)\cdots(2p-1)}{A_{2p}(X)}$$

whence

$$\frac{1}{\Delta^p(\lambda(X)) - p!}$$

is a polynomial of degree $2p$ and it suffices to apply lemma 2.1.

3 Basic results on rational functions

We recall some well known results, with constructive proofs. See e.g., [1] chapter VI lemma 2.8 and theorem 2.9 or [3] theorem 12.14. Given a rational function

$$\varphi(X) = \frac{P(X)}{Q(X)}$$

with polynomials P and Q coprime, the degree of φ is by definition the integer $\max(\deg(P), \deg(Q))$. The following results are well known.

Theorem 3.1 *Let k be a field, $K = k(X)$, $\varphi(X) \in K$ with degree $d > 0$ and $L = k(\varphi)$. Then φ is transcendental over k, and K is an algebraic extension of degree d of L.*

Corollary 3.2 *If φ and ψ are rational functions of degrees d and d' then $\varphi(\psi)$ is a rational function of degree dd', i.e. the usual computation of $\varphi(\psi)$ from reduced fractions for φ and ψ gives a reduced fraction.*

Corollary 3.3 *Let k be a field. A k-automorphism of $k(X)$ is characterized by the image of X, and this may be any rational function $\sigma(X)$ of degree 1. So the group of k-automorphisms of $k(X)$ is isomorphic to the group of linear fractional transformations of the projective line over the field k.*

Corollary 3.4 *Let k be a field, $\varphi, \psi \in k(X)$ (non-constant). Then $k(\varphi) = k(\psi)$ iff there exists σ of degree 1 such that $\varphi = \sigma(\psi)$.*

We can give some explicit form for theorem 3.1.

Proposition 3.5 *Let k be a field, $K = k(X)$, $\varphi(X) \in K$ with degree $d > 0$, $L = k(\varphi)$, and $\psi \in K$. Then one can compute elements $(\alpha_i)_{i=0,\dots,d-1}$ of L such that*

$$\psi = \alpha_0 + \alpha_1 X + \cdots + \alpha_{d-1} X^{d-1}.$$

Proof Let $R(T) = P(T) - \varphi Q(T)$. Write $\psi(X) = A(X)/B(X)$ (an irreducible fraction). Then $B(T)$ and $R(T)$ are coprime in $k(\varphi)[T]$: otherwise, $B(T)$ would be a multiple of $R(T)$ in $k(\varphi)[T]$, hence also in $k[\varphi][T]$, but the degree of B in φ is 0. We choose $U(T)$ and $V(T)$ such that $U(T)B(T) + V(T)R(T) = 1$ in $L[T]$. So $\psi(X) = A(X)U(X)$ and it remains to divide $A(T)U(T)$ by $R(T)$ in $L[T]$. □

Finally we recall the constructive version of Lüroth's theorem.

Theorem 3.6 *Let k be a field, $K = k(X)$, $\varphi, \psi \in K$. Then one can compute $\theta \in K$ such that $k(\theta) = k(\varphi, \psi)$.*

Proof The meaning of "one can compute" is that we give an algorithm computing θ from the coefficients c_i of φ and ψ with only rational computations (i.e., we use only the knowledge of vanishing or nonvanishing of some $\mathbb{Z}$-polynomials in the c_i's arising in the algorithm.)

Let d be the degree of φ. We compute the minimum polynomial $S(T)$ of ψ over $L = k(\varphi)$ (inside the L-algebra K). From this, we know the structure of $L(\psi)$ as a finite extension of L. If $\deg(S) = d$ then we get $K = L(\psi) = L[\psi]$ and so $X \in L(\psi) = k(\varphi, \psi)$ in an explicit way ($\theta = X$). If $\deg(S) < d$, then it is a divisor of d, and we can compute explicitly the minimal polynomial $U(T)$ of X over $L(\psi)$. We get $X^{d'} = \beta_{d'-1} X^{d'-1} + \cdots + \beta_0$, with β_j's $\in L(\psi) = k(\varphi, \psi)$. At least one of the β_j's doesn't belong to k. Let θ be one such coefficient, then $k(\theta) = k(\varphi, \psi)$ (see [1] or [3] for a detailed proof of this last fact). □

4 The general case

Our next goal is to prove explicitly the following proposition.

Proposition 4.1 *Let k be an infinite field and $\varphi \in k(X)$ a rational function whose derivative is nonzero. Assume $\deg(\varphi) > 1$. Then one can find a polynomial $\mu \in k[X]$ of degree 1 such that $\varphi(\mu) \notin k(\varphi)$.*

First we remark that we can always put φ in some standard form without changing the generated field (the proof is immediate):

Lemma 4.2 *For any $\varphi \in k(X)$ of degree $d > 0$ there exists σ of degree 1 such that $\sigma(\varphi) = A(X)/B(X)$ with $\deg(B) < d = \deg(A)$.*

By corollary 3.4, $k(\varphi) = k(\sigma(\varphi))$.

Recall that if the characteristic is $p > 0$ the derivative of φ is nonzero if and only iff $\varphi \notin k(X^p)$.

The following lemma is a precise formulation of proposition 4.1.

Lemma 4.3 *Let k be an infinite field and $\varphi \in k(X)$ of degree $d > 1$. Then, either $\varphi(rX) \notin k(\varphi)$ for some $r \neq 0$ in k, or $k(\varphi) = k(X^d)$. If the latter holds and φ has nonzero derivative, then $\varphi(X+1) \notin k(\varphi)$ and $k(\varphi, \varphi(X+1)) = k(X)$.*

Proof Choose an element $r \in k$ that is not an n-th root of unity for any $n \leq d$. By lemma 4.2 we can assume $\varphi = A(X)/B(X)$ with $\deg(B) < d = \deg(A)$. If $\varphi(rX) \in k(\varphi)$ then $k(\varphi) = k(\varphi(rX))$ and $\varphi(rX) = \sigma(\varphi)$ with $\deg(\sigma) = 1$. So we get

$$\frac{A(rX)}{B(rX)} = \varphi(rX) = \sigma(\varphi) = \frac{aA(X) + bB(X)}{a'A(X) + b'B(X)}$$

(with $ab' - a'b \neq 0$). As $A(rX)/B(rX)$ is reduced and the degrees of the numerator and the denominator on the right hand side are $\leq d$, we see that $a' = 0$, so $B(rX) = c \times B(X)$ for some $c \in k$. From the choice of r, this is impossible except if $B(X)$ has only one nonzero coefficient. On the other hand $A(rX) = c' \times (aA(X) + bB(X))$ for some $c' \in k$. Since $B(X)$ is a monomial, this implies (with our choice of r) that $A(X)$ has at most two nonzero coefficients: the ones of degrees $\deg(B)$ and $\deg(A)$. Since the fraction A/B is reduced, this implies that $\deg(B) = 0$. Finally we get that $\varphi = uX^d + v$ and $k(\varphi) = k(X^d)$. If d is not a multiple of the characteristic, it is then clear that $\varphi(X+1) - \varphi$ is a polynomial of degree $d-1$ and $k(\varphi, \varphi(X+1)) = k(X)$. □

Summarizing the previous results we get:

Theorem 4.4 *Let k be an infinite field and $\varphi \in k(X)$ a rational function whose derivative is nonzero. Assume $\deg(\varphi) > 1$. Then we can compute polynomials σ_j ($j = 1, \ldots, n$) of degree 1 in $k(X)$ and $\lambda \in k(Y_0, Y_1, \ldots, Y_n)$ such that $X = \lambda(\varphi, \varphi(\sigma_1), \ldots, \varphi(\sigma_n))$. Moreover, $n \leq 2m - 1$ where m is the sum of the exponents when factoring d into primes.*

Proof Applying lemma 4.3 and Lüroth's theorem we see that either $k(\varphi, \varphi(rX)) = k(\varphi_1)$ where $d_1 = \deg(\varphi_1)$ strictly divides $d = \deg(\varphi)$, or $k(\varphi, \varphi(X+1)) = k(X)$. In the second case, we are done. In the first case, if $d_1 > 1$ and the characteristic is $p > 0$, we note that since $\varphi \notin k(X^p)$ and $k(\varphi) \subset k(\varphi_1)$ we have also $\varphi_1 \notin k(X^p)$. So we can repeat the process with φ_1. We remark that m is replaced by $m_1 \leq m - 1$. Either $k(\varphi_1, \varphi_1(rX)) = k(\varphi_2)$ where $d_2 = \deg(\varphi_2)$ strictly divides d_1, or $k(\varphi_1, \varphi_1(X+1)) = k(X)$. In the second case we note that $k(\varphi_1, \varphi_1(X+1)) = k(\varphi, \varphi(rX), \varphi(X+1), \varphi(rX+r))$. In the first case we note that $k(\varphi_2) = k(\varphi, \varphi(rX), \varphi(r^2X))$.

So the proof is easily finished by induction on the number m. □

Remarks 1) When k is a finite field with q elements, the previous proofs works if $q > d+1$: in lemma 4.3 we have to choose an element $r \in k$ that is not an n-th root of unity for any $n \leq d$.

2) The following result is also an easy consequence of corollary 3.3, lemma 4.3 and Lüroth's theorem : the fields containing k and setwise fixed by $\mathrm{Aut}_k(k(X))$ are exactly k, $k(X)$ and, in case of characteristic $p > 0$, the fields $k(X^{p^n})$.

Acknowledgments: Many thanks to Franz-Viktor Kuhlmann for carefull reading and usefull suggestions.

References

[1] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext (Springer-Verlag) 1988.
[2] Prestel A., Roquette P. *Formally p-adic fields.* LNM 1050 (Springer-Verlag) 1984.
[3] Spindler K. *Abstract algebra with applications. Vol 2.* (Marcel Dekker) 1994.