# RATIONAL FUNCTIONS INVARIANT UNDER A CYCLIC GROUP

H.W. Lenstra, Jr.

## 1. Introduction

Let $k$ be a field, $n$ a positive integer, and $k(x_1,x_2,\ldots,x_n)$ a purely transcendental field extension of $k$ of transcendence degree $n$. Let the field automorphism $\sigma$ of $k(x_1,x_2,\ldots,x_n)$ be defined by

$$\sigma(c) = c \quad \text{for} \quad c \in k, \quad \sigma(x_i) = x_{i+1} \quad \text{(indices mod } n),$$

and denote the field of invariants of $\sigma$ by $k_n$:

$$k_n = k(x_1,x_2,\ldots,x_n)^{\sigma} = \{f \in k(x_1,x_2,\ldots,x_n) : \sigma(f) = f\}.$$

The question is, whether $k_n$ is a purely transcendental field extension of $k$.

By $\zeta_m$ we denote a primitive $m$-th root of unity in a fixed algebraic closure of $k$ or of $\mathbb{Q}$; which, will be clear from the context.

*Theorem 1.* *Let* $k, n$ *be as above, and put*

$$V = \{ k(\zeta_{p^s}) : p \text{ is a prime number distinct from the characteristic of } k, \ s \text{ is a positive integer, and } p^s \text{ divides } n\}.$$

*Then* $k_n$ *is purely transcendental over* $k$ *if and only if every* $K \in V$ *satisfies the following condition:*

> $K$ *is cyclic over* $k$, *and if* $\sigma_K$ *generates the Galois group* $\mathrm{Gal}(K/k)$, *then the following ideal of* $\mathbb{Z}[\zeta_{[K:k]}]$ *is principal:*
>
> (*) $$\prod (p, \zeta_{[K:k]} - t_p);$$
>
> *here the ideal product ranges over all pairs* $(p,s)$ *as in the definition of* $V$ *for which* $K = k(\zeta_{p^s})$, *the integer* $t_p$ *is defined* (mod $p$) *by* $\sigma_K(\zeta_p) = \zeta_p^{t_p}$, *and* $[K:k]$ *is the degree of* $K$ *over* $k$.

Proof. This is a restatement, for the cyclic case, of the main theorem

of [6], which deals with arbitrary finite abelian groups. □

We note some consequences of the main theorem. If $k = \mathbb{Q}$ and 8 divides $n$, then $K = \mathbb{Q}(\zeta_8)$ belongs to $V$ and is not cyclic over $\mathbb{Q}$, so $\mathbb{Q}_n$ is not purely transcendental over $\mathbb{Q}$. We remark that the condition that every $K \in V$ is cyclic over $k$ is satisfied if the characteristic of $k$ is non-zero or $n$ is not divisible by 8.

If $k = \mathbb{R}$ or $\mathbb{C}$, then $[K:k] \leq 2$ so the ring $\mathbb{Z}[\zeta_{[K:k]}] = \mathbb{Z}$ is a principal ideal domain, and then certainly the ideal (*) is principal. Hence for all $n$ the field extensions $\mathbb{R}_n/\mathbb{R}$ and $\mathbb{C}_n/\mathbb{C}$ are purely transcendental. A direct proof of this will be given in section 2. The set of $n$ for which $\mathbb{Q}_n/\mathbb{Q}$ is purely transcendental will be discussed in section 3.

Exercise. Let $k_0$ be the prime field of $k$, and $k' = k \cap k_0(\zeta_n)$. Then $k'_n/k'$ is purely transcendental if and only if $k_n/k$ is.

Exercise. Let $q$ be a prime power. Then $(\mathbb{F}_q)_n/\mathbb{F}_q$ is purely transcendental if there exists a positive integer $m$ such that $n = \Phi_m(q)$ and $\gcd(n,m) = 1$; here $\Phi_m$ denotes the $m$-th cyclotomic polynomial. In particular, the field extensions $(\mathbb{F}_2)_{2^{p-1}}/\mathbb{F}_2$, for $p$ prime, and $(\mathbb{F}_2)_{2^{2^k+1}}/\mathbb{F}_2$, for $k$ a non-negative integer, are purely transcendental.

## 2. The complex numbers and the real numbers.

Let first $k = \mathbb{C}$, and $n \in \mathbb{Z}$, $n \geq 1$. We prove that $\mathbb{C}_n/\mathbb{C}$ is purely transcendental. Put

$$L = \mathbb{C}(x_1, x_2, \ldots, x_n)$$

and let $\sigma$ be as before. Define

$$e_i = \sum_{j \bmod n} \zeta_n^{-ij} x_j \qquad (i \bmod n),$$

then by Vandermonde the $x_j$ can be expressed in the $e_i$, so

$$L = \mathbb{C}(e_1, e_2, \ldots, e_n)$$

and a short computation shows that

$$(\dagger) \qquad \sigma(e_i) = \zeta_n^{\,i} \cdot e_i \,.$$

Let $E = \langle e_1, e_2, \ldots, e_n \rangle \subset L^*$ be the multiplicative group generated by the $e_i$. Then $E \cong \mathbb{Z}^n$, and by $(\dagger)$ there is a surjective group homomorphism

$$\phi : E \longrightarrow \langle \zeta_n \rangle$$
$$\phi(e) = \sigma(e)/e.$$

Let $I \subset E$ be the kernel of $\phi$. Then $\sigma(e) = e$ for all $e \in I$, so $\mathbb{C}(I) \subset L^{\sigma} = \mathbb{C}_n$. The group $I$ has index $n$ in $E$, and from $E = \langle I, e_1 \rangle$, $e_1^{\,n} \in I$, we see that

$$[\mathbb{C}(E) : \mathbb{C}(I)] \leq n.$$

But $\mathbb{C}(E) = L$ and $\mathbb{C}(I) \subset \mathbb{C}_n$, while we know from Galois theory that

$$[L : \mathbb{C}_n] = n.$$

We conclude that $\mathbb{C}(I) = \mathbb{C}_n$. Since $I$ is of finite index in $E$, it is generated by $n$ elements, and it follows that $\mathbb{C}_n$ is purely transcendental over $\mathbb{C}$. Explicitly, we have

$$\mathbb{C}_n = \mathbb{C}(e_0,\ e_1^{\,n},\ e_2 e_1^{\,-2},\ e_3 e_1^{\,-3},\ \ldots,\ e_{n-1} e_1^{\,1-n}) \,.$$

This elegant proof is due to Fischer [3] (1915).

Next we treat the case $k = \mathbb{R}$ by extending the base field from $\mathbb{R}$ to $\mathbb{C}$, applying the above argument and descending from $\mathbb{C}$ to $\mathbb{R}$ by means of complex conjugation. More explicitly, define the field automorphism $\tau$ of $L = \mathbb{C}(x_1, x_2, \ldots, x_n)$ by

$$\tau(c) = \bar{c} \quad (c \in \mathbb{C}), \qquad \tau(x_i) = x_i \quad (i \bmod n).$$

Then $\tau$ and $\sigma$ commute, and

$$\mathbb{R}(x_1, x_2, \ldots, x_n) = L^{\tau} = \{f \in L : \tau(f) = f\},$$
$$\mathbb{R}_n = (L^{\tau})^{\sigma} = (L^{\sigma})^{\tau} = (\mathbb{C}_n)^{\tau} = \mathbb{C}(I)^{\tau} \,.$$

We have $\tau(e_i) = e_{-i}$ $(i \bmod n)$, so $E$ is a module over the group ring $\mathbb{Z}[\tau]$. Further $\tau(\zeta_n) = \zeta_n^{-1}$, and the map $\phi$ is a $\mathbb{Z}[\tau]$-homomorphism. It follows that $I$ is a $\mathbb{Z}[\tau]$-submodule of $E$.

From a general theorem on finitely generated, $\mathbb{Z}$-free $\mathbb{Z}[\tau]$-modules [1, th. (74.3)] we know that $I$ has a $\mathbb{Z}$-basis

$$a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_r, c_1, c_2, \ldots, c_s, d_1, d_2, \ldots, d_t$$

satisfying $2r + s + t = n$ and

$$\tau(a_j) = b_j, \quad \tau(b_j) = a_j, \quad \tau(c_j) = c_j, \quad \tau(d_j) = d_j^{-1}.$$

Then we have, with $i = \zeta_4$:

$$\begin{aligned} \mathbb{C}(I) &= \mathbb{C}(a_1, \ldots, d_t) = \\ &= \mathbb{C}(a_j + b_j, \quad ia_j - ib_j && (1 \le j \le r), \\ &\qquad c_j && (1 \le j \le s), \\ &\qquad (1 + d_j)/(i - id_j) && (1 \le j \le t)), \end{aligned}$$

where the last $2r + s + t$ expressions are algebraically independent over $\mathbb{C}$ and invariant under $\tau$. Hence

$$\mathbb{R}_n = \mathbb{C}(I)^{\tau} = \mathbb{C}\,(\text{these expressions})^{\tau} = \mathbb{R}\,(\text{these expressions}),$$

which proves that $\mathbb{R}_n/\mathbb{R}$ is purely transcendental.

If we do explicit calculations to avoid application of the theorem on $\mathbb{Z}[\tau]$-modules, then we find that $t = 0$, and that the following $n$ expressions form a transcendence basis of $\mathbb{R}_n$ over $\mathbb{R}$:

if $n = 2k$:

$$e_j \cdot e_1^{-j} + e_{-j} \cdot e_{-1}^{-j}, \quad i \cdot e_j \cdot e_1^{-j} - i \cdot e_{-j} \cdot e_{-1}^{-j} \qquad (2 \le j \le k),$$

$$e_0, \; e_1 e_{-1};$$

if $n = 2k + 1$:

$$e_1^{k+1} \cdot e_{-1}^{-k} + e_{-1}^{k+1} \cdot e_1^{-k}, \quad i \cdot e_1^{k+1} \cdot e_{-1}^{-k} - i \cdot e_{-1}^{k+1} \cdot e_1^{-k},$$

$$e_j \cdot e_1^{-j} + e_{-j} \cdot e_{-1}^{-j}, \quad i \cdot e_j \cdot e_1^{-j} - i \cdot e_{-j} \cdot e_{-1}^{-j} \qquad (2 \le j \le k),$$

$$e_0.$$

The arguments of this section generalize without difficulty

to the case of a finite abelian group acting $\mathbb{R}$-linearly on $\mathbb{R}x_1 + \ldots + \mathbb{R}x_n$.

For general $k$ the proof of theorem 1 runs along similar lines. First one proves that without loss of generality it may be assumed that $n$ is not divisible by the characteristic of $k$. Next, one solves the problem over the extension field $k(\zeta_n)$, as above. Descending, finally, from $k(\zeta_n)$ to $k$ one encounters the $\mathbb{Z}$-free module $I$ over the group ring $\mathbb{Z}[\mathrm{Gal}(k(\zeta_n)/k)]$. It turns out that the solution of the problem depends on how this module looks like under the change of rings

$$\mathbb{Z}[\mathrm{Gal}(k(\zeta_n)/k)] \longrightarrow\!\!\!\!\rightarrow \mathbb{Z}[\mathrm{Gal}(K/k)] \longrightarrow\!\!\!\!\rightarrow \mathbb{Z}[\zeta_{[K:k]}]$$

$$\text{canonical} \qquad \sigma_K \longmapsto \zeta_{[K:k]}$$

for $K \in V$, $\mathrm{Gal}(K/k) = \langle \sigma_K \rangle$. This very short indication may at least explain how the condition stated in theorem 1 arises in the proof. For further details one should consult [6].

## 3. The rational numbers.

In this section we derive some consequences of theorem 1.

*Proposition 2.* *Let $n$ be a positive integer. Then the following three assertions are equivalent:*

*a)* $\mathbb{Q}_n$ *is purely transcendental over* $\mathbb{Q}$;

*b)* $k_n$ *is purely transcendental over* $k$, *for every field* $k$;

*c)* $n$ *is not divisible by* 8, *and for every prime number* $p$ *and every integer* $s \geq 1$ *for which* $n$ *is divisible by* $p^s$ *but not by* $p^{s+1}$, *the ring* $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ *contains an element of norm* $p$.

Proof: b) $\Rightarrow$ a) is obvious, and a) $\Rightarrow$ c) follows by applying theorem 1 to $k = \mathbb{Q}$, using that in that case there is only one factor in the product (*). To prove c) $\Rightarrow$ b), let $K = k(\zeta_{p^r}) \in V$, with $r \leq s$. Then $[K:k]$ divides $(p-1)p^{s-1}$ so taking the relative norm from $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ to $\mathbb{Z}[\zeta_{[K:k]}]$ one discovers that $\mathbb{Z}[\zeta_{[K:k]}]$ has an element of norm $p$ if c) is satisfied. Then every ideal of norm $p$ in $\mathbb{Z}[\zeta_{[K:k]}]$ is principal, and (*) is a product of principal ideals. Application of theorem 1 concludes the proof of proposition 2. □

*Corollary 3.* *Let* $n = \prod_p p^{s(p)}$ *be a positive integer,* $p$ *running over the set of primes and* $s(p)$ *being a non-negative integer which is zero for almost all* $p$. *Then* $\mathbb{Q}_n/\mathbb{Q}$ *is purely transcendental if and only if* $\mathbb{Q}_{p^{s(p)}}/\mathbb{Q}$ *is purely transcendental for every prime number* $p$.

Proof: Clear. □

Thus we see that the question whether $\mathbb{Q}_n/\mathbb{Q}$ is purely transcendental is reduced to the case that $n$ is a prime power. Prime powers which are no primes can be completely dealt with, as proposition 4 shows.

*Proposition 4.* *Let* $p$ *be a prime number and* $s$ *an integer,* $s \geq 2$. *Then* $\mathbb{Q}_{p^s}/\mathbb{Q}$ *is purely transcendental if and only if* $p^s \in \{2^2, 3^m, 5^2, 7^2 : m \in \mathbb{Z}, m \geq 2\}$.

This proposition confirms a conjecture of Endo and Miyata [2, prop. 3.7].

Proof. If. For $p^s = 3^m$, the number $1 - \zeta_{3m-1} \in \mathbb{Z}[\zeta_{3m-1}] = \mathbb{Z}[\zeta_{(p-1)p^{s-1}}]$ has norm 3, and we can apply proposition 2. For $p^s = 2^2, 5^2$ or $7^2$, the ring $\mathbb{Z}[\zeta_{(p-1)p^{s-1}}] = \mathbb{Z}[\zeta_2]$, $\mathbb{Z}[\zeta_{20}]$ or $\mathbb{Z}[\zeta_{42}]$ has class number one [7] and an ideal of norm $p$, so again proposition 2 c) is satisfied.

The only if part follows immediately from proposition 2 and the following lemma.

*Lemma 5.* *a) Let* $p \geq 5$ *be prime. Then* $\mathbb{Z}[\zeta_{(p-1)p^2}]$ *contains no element of norm* $p$.

*b) Let* $p \geq 11$ *be prime. Then* $\mathbb{Z}[\zeta_{(p-1)p}]$ *contains no element of norm* $p$.

Proof. a) Suppose $\alpha \in \mathbb{Z}[\zeta_{(p-1)p^2}]$ has norm $p$, and let $L$ be the subfield of $\mathbb{Q}(\zeta_{(p-1)p^2})$ containing $\mathbb{Q}(\zeta_{p-1})$ for which $[L:\mathbb{Q}(\zeta_{p-1})] = p$. Taking the norm to $L$, one finds an algebraic integer $\beta$ in $L$ of norm $p$, so $(\beta) = q$ where $q$ is a prime of $L$ lying above $p$. Let $p = q \cap \mathbb{Z}[\zeta_{p-1}]$. Since $p$ splits completely in $\mathbb{Q}(\zeta_{p-1})$, and $\mathbb{Q} \neq \mathbb{Q}(\zeta_{p-1})$ (here we use that $p \geq 5$), the ideal $p$ is different from $\bar{p}$, where $\bar{}$ denotes complex conjugation. It follows that $q \neq \bar{q}$.

Put $\gamma = \beta/\bar{\beta}$ and $\eta = \gamma/\rho(\gamma)$, where $\rho$ generates $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{p-1}))$. Since $q/p$ and $\bar{q}/\bar{p}$ are totally ramified, we have $\rho(q) = q$ and $\rho(\bar{q}) = \bar{q}$. Hence $(\gamma) = q/\bar{q}$ is mapped to itself by $\rho$ and therefore $\eta = \gamma/\rho(\gamma)$ is a unit. Moreover, from $\gamma\bar{\gamma} = 1$ it follows that $\eta\bar{\eta} = 1$, so $\eta$ has absolute value one under any embedding of $L$ in $\mathbb{C}$. It now follows from Kronecker's theorem that $\eta$ is a root of unity. But all roots of unity in $L$ lie in $\mathbb{Q}(\zeta_{p-1})$, so we have

$$\eta \in \mathbb{Q}(\zeta_{p-1}), \qquad \eta^{p-1} = 1,$$

$$\eta^p = \mathrm{norm}_{L/\mathbb{Q}(\zeta_{p-1})}(\eta) = \mathrm{norm}_{L/\mathbb{Q}(\zeta_{p-1})}(\gamma)/\mathrm{norm}_{L/\mathbb{Q}(\zeta_{p-1})}(\rho(\gamma))$$

$$= 1$$

and therefore $\eta = 1$ and $\gamma = \rho(\gamma)$. It follows that $\gamma \in \mathbb{Q}(\zeta_{p-1})$, which contradicts its prime ideal decomposition $(\gamma) = q.\bar{q}^{-1} \neq (1)$ and the fact that $q, \bar{q}$ are totally ramified over $p, \bar{p}$. This proves a).

b) Suppose $\beta \in \mathbb{Z}[\zeta_{(p-1)p}]$ has norm $p$, and let now $\rho$ generate the group $\mathrm{Gal}(\mathbb{Q}(\zeta_{(p-1)p})/\mathbb{Q}(\zeta_{p-1}))$, which is cyclic of order $p-1$. As before one finds, with $\gamma = \beta/\bar{\beta}$, that $\eta = \gamma/\rho(\gamma)$ is a root of unity. Changing $\beta$ by a suitable $p$-th root of unity we can achieve that $\eta^{p-1} = 1$.

Again, $(\beta) = q$ is totally ramified over $p = q \cap \mathbb{Z}[\zeta_{p-1}]$, and $q \neq \bar{q}$. The number of prime ideals of $\mathbb{Z}[\zeta_{(p-1)p}]$ lying above $p$ equals $\phi(p-1) > 2$ (here we use that $p \geq 11$); hence there is one, say $q_1$, different from both $q$ and $\bar{q}$. The ideal $q_1$ is generated by some conjugate (over $\mathbb{Q}$) $\beta_1$ of $\beta$, and with $\gamma_1 = \beta_1/\bar{\beta}_1$, $\eta_1 = \gamma_1/\rho(\gamma_1)$ we again have $\eta_1^{p-1} = 1$.

Since the map $(\mathbb{Z}/(p-1)\mathbb{Z}) \times (\mathbb{Z}/(p-1)\mathbb{Z}) \longrightarrow \langle \zeta_{p-1} \rangle$, $(a,b) \longmapsto \eta^a \eta_1^b$, is clearly non-injective, there are integers $a,b \in \{0,1,\ldots,p-2\}$, not both zero, such that $\eta^a \eta_1^b = 1$. Then $\gamma^a \gamma_1^b \in \mathbb{Q}(\zeta_{p-1})$, which contradicts the prime ideal decomposition $(\gamma^a \gamma_1^b) = q^a.\bar{q}^{-a}.q_1^b.\bar{q}_1^{-b}$ as in the proof of a). This proves the lemma.

The proof of the lemma leads to divisibility statements for the class number of cyclotomic fields which seem to be related to results of Ribet [9].

We are left with the question for which prime numbers $p$ the field $\mathbb{Q}_p$ (not the p-adic numbers!) is purely transcendental over $\mathbb{Q}$. Evidently this happens if $\mathbb{Z}[\zeta_{p-1}]$ has class number one, which by [7] is the case if and only if

(#) $\qquad p \leq 43$ or $p = 61, 67$ or $71$ (seventeen values).

For $p = 47, 79, 113, 137$ and many more values (see proposition 6 below) $\mathbb{Q}_p/\mathbb{Q}$ is not purely transcendental. The cases $p = 53, 59, 73$ are undecided, but the tables of Reuschle [8] suggest that in these cases $\mathbb{Q}_p/\mathbb{Q}$ is not purely transcendental either.

It may well be that for only finitely many prime numbers $p$ the extension $\mathbb{Q}_p/\mathbb{Q}$ is purely transcendental, and that perhaps (#) are the only such $p$, but this seems difficult to prove. All we know is the following proposition.

*Proposition 6.* *For a real number $x$, let $\pi(x)$ denote the number of prime numbers $\leq x$, and let $\pi^*(x)$ denote the number of prime numbers $p \leq x$ for which $\mathbb{Q}_p$ is purely transcendental over $\mathbb{Q}$. Then we have*

$$\lim_{x\to\infty} \frac{\pi^*(x)}{\pi(x)} = 0.$$

*More precisely, we have*

$$\frac{\pi^*(x)}{\pi(x)} = O\big((\log\log\log x)^{-\frac{1}{2}}\big) \qquad \text{for } x \to \infty,$$

*and if certain generalized Riemann hypotheses are satisfied then*

$$\frac{\pi^*(x)}{\pi(x)} = O\big((\log\log x)^{-\frac{1}{2}}\big) \qquad \text{for } x \to \infty.$$

Proof (sketch; cf. [6, cor. (7.6)]). Let $q$ be a prime which is $3 \bmod 4$, and $p$ a prime for which $\mathbb{Q}_p/\mathbb{Q}$ is purely transcendental. Using proposition 2 and basic properties of the Hilbert class field one proves that if $p$ splits completely in $\mathbb{Q}(\zeta_q)$, then it also splits completely in the Hilbert class field of $\mathbb{Q}(\sqrt{-q})$. By Tchebotarev's density theorem this implies that

$$\limsup_{x\to\infty} \frac{\pi^*(x)}{\pi(x)} \leq \prod_{q \leq y \text{ prime},\ q \equiv 3 \bmod 4} \left(1 - \frac{h(q)-1}{(q-1)\cdot h(q)}\right)$$

for every $y$, where $h(q)$ denotes the class number of $\mathbb{Q}(\sqrt{-q})$. Letting

y tend to infinity one now finds that $\lim_{x\to\infty} \frac{\pi^*(x)}{\pi(x)} = 0$. The more precise assertions are obtained by choosing y as a function of x and applying the effective versions of Tchebotarev's density theorem proved in [4,5]. This proves proposition 6.

References.


1. C.W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience 1962.

2. S. Endo and T. Miyata, Invariants of finite abelian groups, J. Math. Soc. Japan 25 (1973), 7-26.

3. E. Fischer, Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen, Nachr. Königl. Ges. Wiss. Göttingen (1915), 77-80.

4. J.C. Lagarias, H.L. Montgomery and A.M. Odlyzko, A bound for the least prime ideal in the Chebotarev density theorem, Inventiones math., to appear.

5. J.C. Lagarias and A.M. Odlyzko, Effective versions of the Chebotarev density theorem, pp. 409-464 in: A. Fröhlich (ed.), Algebraic number fields, Academic Press, 1977.

6. H.W. Lenstra, Jr., Rational functions invariant under a finite abelian group, Inventiones math. 25 (1974), 299-325.

7. J.M. Masley and H.L. Montgomery, Cyclotomic fields with unique factorization, J. Reine Angew. Math. 286/287 (1976), 248-256.

8. C.G. Reuschle, Tafeln complexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind, Kön. Akad. der Wiss., Berlin 1875.

9. K.A. Ribet, p-adic L-functions attached to characters of p-power order, Sém. Delange-Pisot-Poitou 19 (1977/78), exp. 9.


Acknowledgements are due to Macquarie University (New South Wales), where this paper was typed. Author's address:
Mathematisch Instituut, Roetersstraat 15, 1018 WB Amsterdam, The Netherlands.