ON NOETHER’S RATIONALITY PROBLEM
FOR CYCLIC GROUPS OVER \( \mathbb{Q} \)

BERNAT PLANS

Abstract. Let \( p \) be a prime number. Let \( C_p \), the cyclic group of order \( p \), permute transitively a set of indeterminates \( \{ x_1, \ldots, x_p \} \). We prove that the invariant field \( \mathbb{Q}(x_1, \ldots, x_p)^{C_p} \) is rational over \( \mathbb{Q} \) if and only if the \((p - 1)\)-th cyclotomic field \( \mathbb{Q}(\zeta_{p-1}) \) has class number one.

1. Introduction

Let a finite group \( G \) act regularly on a set of indeterminates \( \{ x_1, \ldots, x_n \} \) and let \( k \) be a field. Noether’s problem for \( G \) over \( k \) asks whether the field extension \( k(x_1, \ldots, x_n)^G/k \) is rational, i.e. purely transcendental.

The present note deals with Noether’s problem for finite cyclic groups over the field of rational numbers. The reader is referred to [3] for a brief survey of Noether’s problem for abelian groups, including the most relevant references to work of Masuda, Swan, Endo, Miyata, Voskresenski, Lenstra and others.

Let \( P_Q \) denote the set of prime numbers \( p \) for which \( \mathbb{Q}(x_1, \ldots, x_p)^{C_p}/\mathbb{Q} \) is rational, where \( C_p \) denotes the cyclic group of order \( p \).

Lenstra proved in [4, Cor. 7.6] that \( P_Q \) has Dirichlet density 0 inside the set of all prime numbers. Moreover, he suggested in [5, p. 8] that \( P_Q \) could be finite and that perhaps coincides with the set

\[ R := \{ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71 \}. \]

It is known that \( R \subseteq P_Q \). This is a consequence of the fact that, by the main result in [6], \( R \) is nothing but the set of prime numbers \( p \) such that the \((p - 1)\)-th cyclotomic field \( \mathbb{Q}(\zeta_{p-1}) \) has class number one.

For prime numbers \( p < 20000 \), some computational evidence in favour of the equality \( P_Q = R \) is given by Hoshi in [3].

Our goal is to check the validity of Lenstra’s suggestion. We prove:

Theorem 1.1. \( P_Q = R \).

From [5] Cor. 3] and [5] Prop. 4], we get:

Corollary 1.2. Let \( n \) be a positive integer and let \( C_n \) denote the cyclic group of order \( n \). Then \( \mathbb{Q}(x_1, \ldots, x_n)^{C_n}/\mathbb{Q} \) is rational if and only if \( n \) divides

\[ 2^2 \cdot 3^m \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 67 \cdot 71, \]

for some \( m \in \mathbb{Z}_{\geq 0} \).

1991 Mathematics Subject Classification. 12F10, 12F20, 12A35, 12A50.

Key words and phrases. Noether’s problem, rational field extension, cyclic group, cyclotomic field.

Research partially supported by grant 2014 SGR-634 and grant MTM2015-66180-R.
2. Proof

Proof of Thm. 1.1. As has already been mentioned, the inclusion \( R \subseteq P \) is known. See \([2, \text{Prop. 3.4}]\).

Let \( p \in P \). This implies (actually, it is equivalent to) the existence of an element \( \alpha \in \mathbb{Z}[\zeta_{p-1}] \) with norm \( N_{\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}}(\alpha) = \pm p \). See \([2, \text{Thm. 3.1}]\).

Thus, \( p = (\alpha) \) is a principal prime ideal in \( \mathbb{Z}[\zeta_{p-1}] \) above \( (p) \).

If \( \text{Gal}(\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_m\} \), then we have the prime ideal decomposition

\[
(p)_{\mathbb{Z}[\zeta_{p-1}]} = \sigma_1(p) \cdots \sigma_m(p).
\]

Here \( m = [\mathbb{Q}(\zeta_{p-1}) : \mathbb{Q}] = \phi(p-1) \), where \( \phi \) denotes Euler’s totient function. Note that \( (p) \) splits completely in \( \mathbb{Q}(\zeta_{p-1}) \), hence \( \sigma_i(p) \neq \sigma_j(p) \) for \( i \neq j \).

Now, a result of Amoroso and Dvornicich \([1, \text{Cor. 2}]\) ensures that

\[
\log(p)
\]

\[
\phi(p-1)
\]

\[
\geq \begin{cases} \log(5)/12, & \text{for every } p, \\ \log(7/2)/8, & \text{for every } p \equiv 1 \pmod{7}. \end{cases}
\]

It may be worth mentioning here that we are not assuming that \( \mathbb{Q}(\zeta_{p-1}) \) contains an imaginary quadratic subfield, even though this hypothesis is apparently used in the proof of \([1, \text{Cor. 2}]\); in fact, if \( \overline{\alpha} \) denotes the complex conjugate of \( \alpha \), then the argument in \([1, \text{Cor. 2}]\) works whenever \( (\alpha) \neq (\overline{\alpha}) \), and this holds because \( (p) \) splits completely in \( \mathbb{Q}(\zeta_{p-1}) \).

On the other hand, from a result of Rosser and Schoenfeld \([7, \text{Thm. 15}]\), we also know that

\[
\frac{\log(p)}{\phi(p-1)} < \frac{\log(p)}{p-1} \left( e^C \log(p-1) + \frac{5}{2\log(p-1)} \right),
\]

where \( C \approx 0.57721 \) denotes Euler’s constant.

If \( f(p) \) denotes the right hand side of the above inequality, it is easily checked that \( f(x) \) defines a decreasing function for, say, \( x > 43 \). Since \( f(173) < \frac{\log(5)}{12} \), we conclude that \( p < 173 \).

Once we restrict ourselves to prime numbers \( p < 173 \), Hoshi’s computations \([8]\) show that the only possible counterexamples to the inclusion \( P \subseteq R \) are 59, 83, 107 and 163.

Finally, each \( p \in \{59, 83, 107, 163\} \) satisfies

\[
p \not\equiv 1 \pmod{7} \quad \text{and} \quad \frac{\log(p)}{\phi(p-1)} < \frac{\log(7/2)/8}{8},
\]

hence \( p \not\in P \).

\[ \square \]

Remark 2.1. Let \( n = p^r \) for some prime number \( p \geq 5 \).

Lenstra proved \([5, \text{Lemma 5}]\) that \( \mathbb{Z}[\zeta_{\phi(n)}] \) contains no element of norm \( \pm p \) in the following cases:

(i) \( p \geq 11 \) and \( r \geq 2 \).

(ii) \( p \geq 5 \) and \( r \geq 3 \).

Then, by \([2, \text{Thm. 3.1}]\), \( \mathbb{Q}(x_1, \ldots, x_n)^{C_n}/\mathbb{Q} \) cannot be rational in these cases \([8, \text{Prop. 4}]\).
Arguing as in the proof of Theorem 1.1, one can easily prove Lenstra’s Lemma as follows.

If $\alpha \in \mathbb{Z}[\zeta_{p(n)}]$ has norm $\pm p$, then $p = (\alpha)$ is a principal prime ideal above $(p)$ whose inertia degree over $(p)$ is 1. Since $(p)$ splits completely in $\mathbb{Z}[\zeta_{p-1}]$, it must be $p \neq \mathfrak{p}$. It follows that Amoroso and Dvornicich’s result [1] Cor. 2] applies and it ensures that

$$\frac{\log(p)}{\phi(p(n))} \geq \frac{\log(5)}{12}.$$  

But it is readily seen that this inequality does not hold in cases (i) and (ii), just checking that:

1) In case (i), $\frac{\log(p)}{\phi(p(n))} \leq \frac{\log(p)}{2(p-1)} \leq \frac{\log(11)}{2 \cdot 10} < \frac{\log(5)}{12}.$

2) In case (ii), $\frac{\log(p)}{\phi(p(n))} \leq \frac{\log(p)}{p(p-1)} \leq \frac{\log(5)}{5 \cdot 4} < \frac{\log(5)}{12}.$

References

[1] F. Amoroso and R. Dvornicich, A lower bound for the height in abelian extensions, J. Number theory 80(2) (2000), 260–272.

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

[3] A. Hoshi, On Noether’s problem for cyclic groups of prime order, Proc. Japan Acad. Ser. A 91 (2015), 39–44.

[4] H. W. Lenstra Jr., Rational functions invariant under a finite abelian group, Invent. Math. 25 (1974), 299–325.

[5] H. W. Lenstra Jr., Rational functions invariant under a cyclic group, in: Proc. of the Queen’s Number Theory Conference, 1979 (Kingston, Ont., 1979), Queen’s Papers in Pure and Appl. Math. 54, pp. 91–99. Queen’s Univ., Kingston, Ont., 1980.

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

[7] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962), 64–94.

Departament de Matemàtiques, Universitat Politècnica de Catalunya, Av. Diagonal, 647, 08028 Barcelona

E-mail address: bernat.plans@upc.edu