ACTA ARITHMETICA
175.1 (2016)

On cyclotomic elements and cyclotomic subgroups in K_2 of a field

by

Kejian Xu (Qingdao) and Chaochao Sun (Linyi)

Dedicated to the memory of Jerzy Browkin

1. Introduction. For a field F, $K_2(F)$ denotes the Milnor K_2-group of F. It follows from Matsumoto's theorem [10] that $K_2(F)$ is generated by the symbols $\{a,b\}$, $a,b \in F^*$. In general, an element of $K_2(F)$ is a product of symbols. Therefore, expressing an element of $K_2(F)$ in a simple and more explicit form is much desired.

For a global field, Lenstra [7] proved a surprising fact that every element of $K_2(F)$ is not just a product of symbols, but actually a symbol. More precisely, if G is a finite subgroup of $K_2(F)$, then $G \subseteq \{a, F^*\}$ for some $a \in F^*$.

Moreover, for a global field F containing ζ_n, the nth primitive root of unity, Tate [19] investigated the n-torsion of $K_2(F)$. For an abelian group A, we use A_n to denote the n-torsion of A, i.e., $A_n = \{a \in A \mid a^n = 1\}$. Tate proved that

$$(K_2(F))_n = \{\zeta_n, F^*\}, \tag{1.1}$$

which implies that every element in $(K_2(F))_n$ can be written as $\{\zeta_n, a\}$, where $a \in F^*$. At the same time, Tate conjectured that (1.1) is true for any field containing ζ_n. Tate's conjecture was proved by Merkurjev and Suslin [9], [18].

Unfortunately, the condition $\zeta_n \in F$ is too restrictive. For example, as is well known, $K_2(\mathbb{Q})$ is a torsion group and it contains elements of any

2010 *Mathematics Subject Classification*: 11R70, 11R58, 19F15.
Key words and phrases: Milnor K_2-group, cyclotomic element, cyclotomic subgroup, essentially distinct, rational function field, number field.
Received 17 February 2015; revised 13 April 2016.
Published online 15 September 2016.

DOI: 10.4064/aa8084-4-2016

order by Dirichlet's theorem. But, according to Tate's result, only elements of order 2 in $K_2(\mathbb{Q})$ can be expressed explicitly.

For a given n, Browkin [1] considered *cyclotomic elements* of $K_2(F)$, i.e., elements of the form

$$c_n(a) := \{a, \Phi_n(a)\}, \quad a, \Phi_n(a) \in F^*,$$

where $\Phi_n(x)$ denotes the nth cyclotomic polynomial. The advantage of cyclotomic elements is that one can dispense with the condition $\zeta_n \in F$.

Let

$$G_n(F) = \{c_n(a) \in K_2(F) \mid a, \Phi_n(a) \in F^*\}.$$

Browkin [1] proved that $G_n(F) \subseteq (K_2(F))_n$, i.e., all the elements of $G_n(F)$ are n-torsion elements of $K_2(F)$. In particular, he proved that for any field $F \neq \mathbb{F}_2$, if $n = 1, 2, 3, 4, 6$ and $\zeta_n \in F$, then every element $\{\zeta_n, x\} \in K_2(F)$ can be written in the form $c_n(a)$. Moreover, it is also proved in [1] that $G_n(F) = (K_2(F))_n$ for $n = 3$ and $F = \mathbb{Q}$ (for any field F by Urbanowicz [20]). For $n = 4$, it follows from [1] for $F = \mathbb{Q}$ and from Qin [12] for any field F with $\mathrm{ch}(F) \neq 2$ that every element of order 4 in $K_2(F)$ can be written in the form $c_4(a) \cdot v$, where $v \in K_2(F)$ with $v^2 = 1$. But, in general, as conjectured in [1], $G_n(F)$ is not a group.

Browkin's Conjecture 1.1 ([1]). *For any integer $n \neq 1, 2, 3, 4$ or 6 and any field F, $G_n(F)$ is not a subgroup of $K_2(F)$, in particular, $G_5(\mathbb{Q})$ is not a subgroup of $K_2(\mathbb{Q})$.*

Qin [12], [13] proved that neither $G_5(\mathbb{Q})$ nor $G_7(\mathbb{Q})$ is a subgroup of $K_2(\mathbb{Q})$ and that $G_{2^n}(\mathbb{Q})$ is a group if and only if $n \leq 2$. Xu and Qin [25] proved that $G_{2^n3^m}(\mathbb{Q})$ is a group if and only if $n = 2$ and $m = 0$ (see [27] for more results). The first author of the present paper proved that for any number field F, if $n \neq 4, 8, 12$ has a square factor, then $G_n(F)$ is not a subgroup of $K_2(F)$ (see [22], [24]). A similar result can be established for function fields [24].

However, when n is a prime, $G_n(F)$ seems difficult to deal with, in particular when F is a number field or, in general, a global field. Xu, Sun and Chi [29] investigated the l-torsion of $K_2(F(x))$, where $F(x)$ is the rational function field over F and l is a prime with $l \neq \mathrm{ch}(F)$, and proved that if $l \geq 5$ and $\Phi_l(x)$ is irreducible in $F[x]$, then Browkin's conjecture is true for $F(x)$. But we still do not know whether it is true for every number field.

Browkin's conjecture implies that corresponding to Tate's result, we could only expect results on the "outer structure" of $G_n(F)$, that is, that $(K_2(F))_n$ is generated by something like $G_n(F)$. In fact, Lenstra [8] proved that $(K_2(\mathbb{Q}))_5$ is generated by $G_5(\mathbb{Q})$; alternative proofs are given in [23] and [2]. Du and Qin [2] also proved that $(K_2(\mathbb{Q}))_8$ is generated by $G_8(\mathbb{Q}) \cup G_4(\mathbb{Q}) \cup G_2(\mathbb{Q})$. In general, Qin proposed the following problem:

Qin's Problem 1.2 ([14]). *For which n, $(K_2(F))_n = \langle G_m(F) \mid all\ m \mid n\rangle$?*

Xu and Liu [24] even conjectured that if $n = p_1^{e_1} \cdots p_t^{e_t}$, then $(K_2(F))_n$ is generated by all $G_{p_i^{m_i}}(F)$, i.e.,

$$(K_2(F))_n = \langle G_{p_i^{m_i}}(F) \mid 1 \leq m_i \leq e_i,\ 1 \leq i \leq t\rangle.$$

Moreover, Qin proposed the following more general problem:

Qin's Problem 1.3 ([2]). *For a given field, what is the value of*

$$[(K_2(F))_n : \langle G_m(F) \mid all\ m \mid n\rangle]\ ?$$

In the present paper, we turn to the "inner structure" of $G_n(F)$, in particular, we are interested in the "inner" subgroup structure of $G_n(F)$. As a result, we modify Browkin's conjecture into more precise forms.

A subgroup of $K_2(F)$ is called *cyclotomic* if it is contained in $G_n(F)$. Our problems are formulated as follows.

Problem 1.4. *How many nontrivial cyclotomic elements are there in a subgroup of $K_2(F)$ generated by finitely many essentially distinct* (*see Section* 4) *cyclotomic elements in $G_n(F)$?*

Problem 1.5. *When does $K_2(F)$ contain a nontrivial cyclotomic subgroup?*

Problem 1.6. *How many cyclotomic subgroups are there in a subgroup of $K_2(F)$ generated by finitely many essentially distinct cyclotomic elements in $G_n(F)$?*

It follows from [1] that for $F \neq \mathbb{F}_2$ and $n = 1, 2, 3, 4$ or 6, $G_n(F)$ itself is a cyclotomic subgroup of $K_2(F)$. Qin and Xu [26, 28] proved that for a local field F, $G_n(F)$ is a cyclotomic subgroup in most cases (see also [4]). Moreover, we have the following conjecture.

Qin–Xu's Conjecture 1.7 ([28]). *For any local field F, the set $G_n(F)$ is a cyclotomic subgroup of $K_2(F)$.*

For a number field, the picture seems different. From [29], we only know that a subgroup of $K_2(F(x))$ generated by a cyclotomic element contains at least two noncyclotomic elements.

In this paper, we give a systematic study of the above three problems. For the rational function field $F(x)$, we will determine the exact number of nontrivial cyclotomic elements and of nontrivial cyclotomic subgroups in a subgroup generated by some kind of cyclotomic elements in $G_l(F(x)) \subseteq K_2(F(x))$, where l is a prime with $l \neq \mathrm{ch}(F)$.

More precisely, let $\mathfrak{G}_l(n; F)$ denote a subgroup of $K_2(F(x))$ generated by n essentially distinct (see Section 4) cyclotomic elements of some kind in

$G_l(F(x))$, and let $c(\mathfrak{G}_l(n;F))$ and $cs(\mathfrak{G}_l(n;F))$ denote respectively the numbers of nontrivial cyclotomic elements and nontrivial cyclotomic subgroups contained in $\mathfrak{G}_l(n;F)$. We prove the following result (see Theorem 5.17).

Theorem 1.8. *Assume that $l \geq 5$ is a prime number and F is a field such that $\Phi_l(x)$ is irreducible in $F[x]$. Let n be a positive integer satisfying*

$$n \leq (l-3)/2.$$

(i) *If* $\mathrm{ch}(F) = 0$, *then* $c(\mathfrak{G}_l(n;F)) = 2n$, *and so* $cs(\mathfrak{G}_l(n;F)) = 0$.

(ii) *If* $\mathrm{ch}(F) = p \neq 0$, *then* $c(\mathfrak{G}_l(n;F)) = n(2 + |\mathfrak{Z}(l,p)|)$, *where*

$$\mathfrak{Z}(l,p) := \{t \mid 2 \leq t \leq l-2,\ t \equiv p^{2m} \text{ or } -p^{2m} \pmod{l} \text{ for some } m \in \mathbb{N}\}.$$

(iii) *If* $\mathrm{ch}(F) = p \neq 0$, *then*

$$cs(\mathfrak{G}_l(n;F)) > 0 \ \Leftrightarrow\ l \equiv 3 \pmod 4 \text{ and } p \text{ is a primitive root of } l.$$

In this case, $cs(\mathfrak{G}_l(n;F)) = n$, i.e., $\mathfrak{G}_l(n;F)$ contains exactly n nontrivial cyclotomic subgroups.

(iv) *Every nontrivial cyclotomic subgroup of $\mathfrak{G}_l(n;F)$ is a cyclic subgroup of order l, i.e., every nontrivial cyclotomic subgroup has the form $\mathfrak{G}_l(1;F)$.*

We do not know how to remove the condition $n \leq (l-3)/2$ in Theorem 1.8. We present some computations for the cases $n > (l-3)/2$, in particular for $n = 2, 3$. The results of computations agree with the above theorem. So it seems that the condition $n \leq (l-3)/2$ is removable.

As for the number field cases, the situation seems quite different. In the proof of Theorem 1.8, essential use is made of the fact that $F(x)$ has a nontrivial derivation. Thus the proof does not carry over to number fields.

However, we find that $G_n(F)$ really has some "inner structure". In fact, it seems curious that we can construct number fields F for which the cube of some cyclotomic element in $K_2(F)$ is also cyclotomic (we can do the same for squares).

More precisely, let

$$\begin{aligned} f_{n,1}(x) &= x^n + x + 1 && \text{if } n \equiv 1 \pmod 3, \\ f_{n,2}(x) &= (x^n + x + 1)/(x^2 + x + 1) && \text{if } n \equiv 2 \pmod 3. \end{aligned}$$

Selmer proved that $f_{n,1}, f_{n,2}$ are both irreducible (see Lemma 9.1). Then we have (see Theorem 9.5):

Theorem 1.9.

(i) *Assume that $p > 3$ is a prime. Let α be a zero of $f_{p,i}(x)$, where $i = 1$ or 2, and $F = \mathbb{Q}(\alpha)$. Then*

$$1 \neq c_p(\alpha)^3 = c_p(\alpha^3) \in G_p(F).$$

(ii) *Assume that $p \geq 3$ is a prime. Let α be a zero of the irreducible polynomial $x^p + x^{p-1} + 2$ and $F = \mathbb{Q}(\alpha)$. Then*

$$1 \neq c_p(\alpha)^2 = c_p(\alpha^2) \in G_p(F).$$

As a consequence, we can construct a number field F such that $K_2(F)$ contains a cyclotomic subgroup of order five. Moreover, we have (see Examples 9.9 and 9.10):

Corollary 1.10.

(i) *Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f_{5,2}(x) = x^3 - x^2 + 1$ and $\widetilde{F} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Then $\langle c_5(\alpha_1)\rangle, \langle c_5(\alpha_2)\rangle, \langle c_5(\alpha_3)\rangle$ are three cyclotomic subgroups of order five of $K_2(\widetilde{F})$.*

(ii) *Let $\alpha_1, \ldots, \alpha_5$ be the roots of $x^5 + x^4 + 2$ and $\widetilde{F} = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$. Then $\langle c_5(\alpha_1)\rangle, \ldots, \langle c_5(\alpha_5)\rangle$ are five cyclotomic subgroups of order five of $K_2(\widetilde{F})$.*

We can also construct a quadratic field F such that $K_2(F)$ contains a cyclotomic subgroup of order five. In fact, let $F = \mathbb{Q}(\sqrt{5})$ and $\beta = (3 + \sqrt{5})/2$. Then we can prove that $\langle c_5(\beta)\rangle$ is a cyclotomic subgroup of $K_2(F)$ of order five (see Example 9.11).

A natural problem arises:

Problem 1.11. *For a number field F, is there always a cyclotomic subgroup of order five in $K_2(F)$? How many cyclotomic subgroups of order five are there in $K_2(F)$?*

We do not know how to attack this problem for general number fields. But based on numerical computations, we make the following conjecture:

Conjecture 1.12. *There does not exist a cyclotomic subgroup of order five in $K_2(\mathbb{Q})$.*

As for subgroups of other orders, it seems that the answer is negative if five is replaced by a prime greater than five:

Conjecture 1.13. *Let F be a number field. If $p > 5$ is a prime, then $K_2(F)$ contains no cyclotomic subgroups of order p.*

Corresponding to this conjecture, we have the following theorem which reflects deeper nonclosedness of the cyclotomic elements in $K_2(F)$ (see Theorem 10.4).

Theorem 1.14. *Assume that F is a number field and $n \neq 1, 4, 8, 12$ is a positive integer. If there is a prime p such that $p^2 \mid n$, then there exist infinitely many nontrivial cyclotomic elements $\alpha_1, \alpha_2, \ldots\ldots \in G_n(F)$ such that*

$$\langle \alpha_1^p \rangle \subsetneq \langle \alpha_1^p, \alpha_2^p \rangle \subsetneq \cdots \quad \textit{and} \quad \langle \alpha_1^p, \alpha_2^p, \ldots \rangle \cap G_n(F) = \{1\}.$$

This implies that in $K_2(F)$ there exists a subgroup generated by cyclotomic elements to the power of some prime, which contains no nontrivial cyclotomic elements. Clearly, this result is more precise than Browkin's conjecture. In particular, it implies that Browkin's conjecture is true for any number field if $n \neq 1, 4, 8, 12$ and n has a prime square factor, which was proved in [24].

It seems that the above results explain why Browkin's conjecture is difficult. The reason is that there exists an "inner structure" in $G_n(F)$, i.e., a partial mutiplication structure or a subgroup structure.

This paper is organized as follows. The first part, Sections 2–8, focuses on the case of function fields. In Section 2, we discuss some basic properties related to cyclotomic polynomials; in Section 3, the definition of a tame homomorphism and its computation are given; in Section 4, to remove superfluous generators in a finitely generated subgroup of $K_2(F(x))$, we introduce the concept of 'essentially distinct elements'; and in Section 5, our aim is to prove Theorem 1.8. In Section 6, some computations are presented for $n > (l-3)/2$, in particular, for $n = 2$ or 3; in Section 7, as a preparation for the next section, two diophantine equations are discussed; and in Section 8, a further example is given. Then, in the second part of this paper, we consider the number field cases. More precisely, in Section 9, Theorem 1.9 and Corollary 1.10 are proved. Finally in Section 10, Theorem 1.14 is proved, for which Faltings' theorem on the Mordell conjecture is used.

2. Cyclotomic polynomials. Let $l \geq 5$ be a prime number and F a field of characteristic $\neq l$. Throughout we assume that the cyclotomic polynomial $\Phi_l(x)$ is irreducible in $F[x]$. We denote by ζ any root of $\Phi_l(x)$.

Let $\Phi_l(x, y) := y^{l-1}\Phi_l(x/y)$. The irreducibility of $\Phi_l(x)$ in $F[x]$ implies the irreducibility of $\Phi_l(x, y)$ in $F[x, y]$.

Theorem 2.1. *For any nonzero $f(x), g(x) \in F[x]$ we have*

$$\deg \Phi_l(f(x), g(x)) = (l-1) \cdot \max(\deg f(x), \deg g(x)).$$

Proof. We have

$$\Phi_l(f(x), g(x)) = f(x)^{l-1} + f(x)^{l-2}g(x) + \cdots + g(x)^{l-1}. \tag{2.1}$$

Let a_0x^r and b_0x^s be the respective leading terms of $f(x)$ and $g(x)$.

If $r \neq s$, say $r > s$, then by (2.1) the leading term of $\Phi_l(f(x), g(x))$ is $(a_0x^r)^{l-1} = a_0^{l-1}x^{(l-1)r}$.

If $r = s$, then all summands in (2.1) are of the same degree, and the sum of their leading terms is

$$(a_0x^r)^{l-1} + (a_0x^r)^{l-2}b_0x^r + \cdots + (b_0x^r)^{l-1} = \Phi_l(a_0, b_0)x^{r(l-1)}.$$

Moreover, $\Phi_l(a_0,b_0) = b_0^{l-1}\Phi_l(a_0/b_0) \neq 0$, since the irreducibility of $\Phi_l(x)$ in $F[x]$ implies that it cannot have a zero in F.

Thus in both cases the leading term of $\Phi_l(f(x),g(x))$ is of degree $(l-1)r = (l-1)\cdot\max(\deg f(x), \deg g(x))$. ■

THEOREM 2.2. *If $f(x), g(x) \in F[x]$ are relatively prime, then the degree of every factor of $\Phi_l(f(x),g(x))$ is divisible by $l-1$.*

Proof. It is sufficient to prove that the degree of every irreducible factor of $\Phi_l(f(x),g(x))$ is divisible by $l-1$.

In $F(\zeta)[x]$ we have

$$\Phi_l(f(x),g(x)) = \prod_{j=1}^{l-1}(f(x)-\zeta^j g(x)). \tag{2.2}$$

Let α be a root of an irreducible factor $h(x)$ of $\Phi_l(f(x),g(x))$. Then it is a root of $\Phi_l(f(x),g(x))$, hence, by (2.2), $f(\alpha)-\zeta^j g(\alpha) = 0$ for some $1 \le j \le l-1$.

Therefore $f(\alpha) = 0$ if and only if $g(\alpha) = 0$. But $f(x)$ and $g(x)$ are coprime, so $f(x)$ and $g(x)$ cannot have a common root. Hence $f(\alpha)g(\alpha) \neq 0$.

Consequently, $\zeta^j = f(\alpha)/g(\alpha) \in F(\alpha)$. Hence $F(\zeta) \subseteq F(\alpha)$. Therefore

$$\deg h(x) = (F(\alpha):F) = (F(\alpha):F(\zeta))(F(\zeta):F) = (F(\alpha):F(\zeta))(l-1),$$

since α and ζ are roots of the polynomials $h(x)$ and $\Phi_l(x)$, respectively, which are irreducible. ■

COROLLARY 2.3. *If $\max(\deg f(x), \deg g(x)) = 1$, then $\Phi_l(f(x),g(x))$ is irreducible.*

Proof. By Theorem 2.1, $\deg\Phi_l(f(x),g(x)) = l-1$, and by Theorem 2.2, every factor of $\Phi_l(f(x),g(x))$ has degree divisible by $l-1$. It follows that $\Phi_l(f(x),g(x))$ has only one factor, so it is irreducible. ■

THEOREM 2.4. *Let $f(x), g(x) \in F[x]$, $(f(x),g(x)) = 1$ and $\deg f(x) \ge 1$. Let $\mathfrak{p}$ be the ideal of $F[x]$ generated by an irreducible factor of $\Phi_l(f(x),g(x))$. Then for $r \in \mathbb{Z}$,*

$$(f(x)/g(x))^r \equiv 1 \pmod{\mathfrak{p}} \quad \textit{if and only if} \quad l \mid r.$$

Proof. Since $\mathfrak{p}$ is generated by an irreducible polynomial, it is a prime ideal of $F[x]$. From $\Phi_l(f(x),g(x)) \mid f(x)^l - g(x)^l$, it follows that $f(x)^l \equiv g(x)^l \pmod{\mathfrak{p}}$, and $g(x) \not\equiv 0 \pmod{\mathfrak{p}}$, because $f(x)$ and $g(x)$ are relatively prime. Hence $(f(x)/g(x))^l \equiv 1 \pmod{\mathfrak{p}}$.

If $l \nmid r$ and $(f(x)/g(x))^r \equiv 1 \pmod{\mathfrak{p}}$, then from the last two congruences it follows that $f(x)/g(x) \equiv 1 \pmod{\mathfrak{p}}$, i.e., $f(x) \equiv g(x) \pmod{\mathfrak{p}}$. Hence

$$\Phi_l(f(x),g(x)) = \sum_{j=0}^{l-1} f(x)^j g(x)^{(l-1)-j} \equiv l g(x)^{l-1} \pmod{\mathfrak{p}},$$

so $g(x) \equiv 0 \pmod{\mathfrak{p}}$, which is impossible. This contradiction shows that $l \mid r$.

Conversely, if $l \mid r$, then from the congruence $(f(x)/g(x))^l \equiv 1 \pmod{\mathfrak{p}}$, it follows that $(f(x)/g(x))^r \equiv 1 \pmod{\mathfrak{p}}$. ■

Let $W(F)$ be the group of roots of unity in F.

We say that matrices $A, B \in \mathrm{GL}(2, F)$ are *essentially distinct* if

$$B \neq \alpha \begin{pmatrix} \mu & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{\epsilon} A$$

for every $\alpha \in F^*$, $\mu \in W(F)$, and $\epsilon = 0$ or 1.

Thus if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, F)$ then all matrices which are not essentially distinct from A are

$$\alpha \begin{pmatrix} \mu a & \mu b \\ c & d \end{pmatrix} \quad \text{and} \quad \alpha \begin{pmatrix} \mu c & \mu d \\ a & b \end{pmatrix}, \quad \text{for all } \alpha \in F^*,\ \mu \in W(F).$$

Theorem 2.5. *If*

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{GL}(2, F)$$

are essentially distinct, then the polynomials

$$\Phi_l(a_1x + b_1, c_1x + d_1) \quad \textit{and} \quad \Phi_l(a_2x + b_2, c_2x + d_2)$$

are relatively prime.

Proof. If matrices A_1 and A_2 are essentially distinct, then so are A_1B and A_2B for every $B \in \mathrm{GL}(2, F)$. Therefore, taking $B = A_1^{-1}$ we can assume that $A_1 = I$ is the identity matrix, and $A_2 = \left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right)$.

Assume that the corresponding polynomials $\Phi_l(x)$ and $\Phi_l(ax+b, cx+d)$ are not relatively prime. Since they are irreducible and of the same degree, they differ by a constant factor:

$$\Phi_l(x) = \alpha\Phi_l(ax + b, cx + d) \qquad \text{for some } \alpha \in F^*.$$

Hence the corresponding linear factors differ by a constant factor, in particular

$$x - \zeta = \alpha_1\big((ax + b) - \zeta^r(cx + d)\big) \qquad \text{for some } \alpha_1 \in F(\zeta)^* \text{ and } 1 \leq r \leq l - 1.$$

Comparing coefficients we get

$$1 = \alpha_1(a - \zeta^r c), \qquad -\zeta = \alpha_1(b - \zeta^r d).$$

Eliminating α_1 we obtain

$$-\zeta(a - \zeta^r c) = b - \zeta^r d.$$

If $r \neq 1, l-1$, then $1, \zeta, \zeta^r, \zeta^{r+1}$ are linearly independent over F, hence $a = b = c = d = 0$, which is impossible.

If $r = 1$, then $-\zeta a + \zeta^2 c = b - \zeta d$ implies that $b = c = 0$ and $a = d$. Consequently, $A_2 = a\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is not essentially distinct from $A_1 = I$.

If $r = l - 1$, then $-\zeta a + c = b - \zeta^{l-1} d$ implies that $a = d = 0$, $b = c$. Consequently, $A_2 = b\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is not essentially distinct from $A_1 = I$ either.

In every case we get a contradiction. Therefore the polynomials $\Phi_l(x)$ and $\Phi_l(ax + b, cx + d)$ are relatively prime. ∎

3. Tame homomorphisms. For a nonzero prime ideal $\mathfrak{p}$ of $F[x]$, the *tame homomorphism*

$$\tau_{\mathfrak{p}}:\ K_2(F(x)) \to (F[x]/\mathfrak{p})^*$$

is defined by

$$\tau_{\mathfrak{p}}(\{u, v\}) \equiv (-1)^{v_{\mathfrak{p}}(u)v_{\mathfrak{p}}(v)} \frac{u^{v_{\mathfrak{p}}(v)}}{v^{v_{\mathfrak{p}}(u)}} \pmod{\mathfrak{p}}, \tag{3.1}$$

where $u, v \in F(x)^*$.

Lemma 3.1. *Let* $f(x), g(x) \in F[x]$ *satisfy* $(f(x), g(x)) = 1$ *and* $\deg f(x)g(x) > 0$. *For a nonzero prime ideal* $\mathfrak{p}$ *of* $F[x]$ *denote* $r_{\mathfrak{p}} := v_{\mathfrak{p}}(\Phi_l(f(x), g(x)))$.

(i) *We have*

$$\tau_{\mathfrak{p}}(c_l(f/g)) \equiv \begin{cases} (f/g)^{r_{\mathfrak{p}}} \not\equiv 1 \pmod{\mathfrak{p}} & \textit{if } l \nmid r_{\mathfrak{p}}, \\ 1 \pmod{\mathfrak{p}} & \textit{if } l \mid r_{\mathfrak{p}}. \end{cases}$$

(ii) *In particular, if* $\max(\deg f(x), \deg g(x)) = 1$, *then*

$$\tau_{\mathfrak{p}}(c_l(f/g)) \equiv \begin{cases} f/g \not\equiv 1 \pmod{\mathfrak{p}} & \textit{if } \mathfrak{p} = (\Phi_l(f(x), g(x))), \\ 1 \pmod{\mathfrak{p}} & \textit{otherwise.} \end{cases}$$

Proof. (i) From $(f(x), g(x)) = 1$ it follows that $(f(x)g(x), \Phi_l(f(x), g(x))) = 1$. Therefore for every prime ideal $\mathfrak{p}$ of $F[x]$ at most one of the numbers $v_{\mathfrak{p}}(f(x)), v_{\mathfrak{p}}(g(x))$, $v_{\mathfrak{p}}(\Phi_l(f(x), g(x))$ does not vanish.

Clearly,

$$\begin{aligned} c_l\left(\frac{f(x)}{g(x)}\right) &= \left\{\frac{f(x)}{g(x)}, \Phi_l\left(\frac{f(x)}{g(x)}\right)\right\} \\ &= \left\{\frac{f(x)}{g(x)}, \Phi_l(f(x), g(x))\right\}\{f(x), g(x)\}^{-(l-1)}, \end{aligned} \tag{3.2}$$

because $\{g(x), g(x)^2\} = 1$ and $l - 1$ is even.

If $v_{\mathfrak{p}}(f(x)) > 0$ and $r_{\mathfrak{p}} = 0$, then $\Phi_l(f(x), g(x)) \equiv g(x)^{l-1} \pmod{\mathfrak{p}}$. Hence, by (3.1) and (3.2),

$$\tau_{\mathfrak{p}}(c_l(f/g)) \equiv \Phi_l(f(x), g(x))^{-v_{\mathfrak{p}}(f(x))} g(x)^{(l-1)v_{\mathfrak{p}}(f(x))} \equiv 1 \pmod{\mathfrak{p}}.$$

If $v_{\mathfrak{p}}(g(x)) > 0$ and $r_{\mathfrak{p}} = 0$, then we prove similarly that $\tau_{\mathfrak{p}}(c_l(f(x)/g(x))) \equiv 1 \pmod{\mathfrak{p}}$.

If $v_{\mathfrak{p}}(f(x))=v_{\mathfrak{p}}(g(x))=0$ and $r_{\mathfrak{p}}=0$, then (3.2) implies $\tau_{\mathfrak{p}}(c_l(f(x)/g(x))) \equiv 1 \pmod{\mathfrak{p}}$.

If $r_{\mathfrak{p}}>0$, then, by (3.1) and (3.2), we obtain $\tau_{\mathfrak{p}}(c_l(f(x)/g(x))) \equiv (f(x)/g(x))^{r_{\mathfrak{p}}} \pmod{\mathfrak{p}}$.

Moreover, by Theorem 2.4, $(f(x)/g(x))^{r_{\mathfrak{p}}} \not\equiv 1 \pmod{\mathfrak{p}}$ if and only if $l \nmid r_{\mathfrak{p}}$.

(ii) By Corollary 2.3, the polynomial $\Phi_l(f(x),g(x))$ is irreducible. Therefore $r_{\mathfrak{p}}=v_{\mathfrak{p}}(\Phi_l(f(x),g(x)))=1$. It is sufficient to apply the first part of the theorem with $r_{\mathfrak{p}}=1$. ∎

4. Essentially distinct elements.

Recall that

$$\mathrm{PGL}(2,F) := \mathrm{GL}(2,F)/Z,$$

where Z is the center of $\mathrm{GL}(2,F)$, that is, $Z = F^* \cdot \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Similarly,

$$\mathrm{PSL}(2,F) := \mathrm{SL}(2,F)/Z \subset \mathrm{PGL}(2,F).$$

In the following, we will use $\overline{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)}$ to denote the image of $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ in $\mathrm{PGL}(2,F)$. Clearly, the element $c_l\big(\frac{ax+b}{cx+d}\big)$ depends only on the coset $\overline{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)}$.

We will focus on the following subsets of $G_l(F(x))$:

$$GG_l(F(x)) := \left\{c_l\left(\frac{ax+b}{cx+d}\right) \in G_l(F(x)) \;\middle|\; \overline{\begin{pmatrix}a&b\\c&d\end{pmatrix}} \in \mathrm{PGL}(2,F)\right\},$$

$$SG_l(F(x)) := \left\{c_l\left(\frac{ax+b}{cx+d}\right) \in GG_l(F(x)) \;\middle|\; \begin{pmatrix}a&b\\c&d\end{pmatrix} \in \mathrm{SL}(2,F)\right\},$$

$$TG_l(F(x)) := \{c_l(x+b) \in GG_l(F(x)) \mid b \in F\}.$$

Definition 4.1. Let

$$\alpha = c_l\left(\frac{a_1x+b_1}{c_1x+d_1}\right),\ \beta = c_l\left(\frac{a_2x+b_2}{c_2x+d_2}\right) \in GG_l(F(x)).$$

We say that α,β are *essentially distinct* if the matrices $\left(\begin{smallmatrix}a_1&b_1\\c_1&d_1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}a_2&b_2\\c_2&d_2\end{smallmatrix}\right)$ are essentially distinct.

Lemma 4.2. *Assume that $\Phi_l(x)$ is irreducible in $F[x]$. Let*

$$\alpha = c_l\left(\frac{a_1x+b_1}{c_1x+d_1}\right),\ \beta = c_l\left(\frac{a_2x+b_2}{c_2x+d_2}\right) \in GG_l(F(x)).$$

If $\alpha=\beta$, then

$$\frac{a_1x+b_1}{c_1x+d_1} = \frac{a_2x+b_2}{c_2x+d_2}.$$

Proof. Since $\Phi_l(x)$ is irreducible in $F[x]$, so are $\Phi_l(a_ix+b_i,\ c_ix+d_i))$ $(i=1,2)$ by Corollary 2.3. From Lemma 3.1 we have

$$\tau_{\mathfrak{p}}(\alpha)\equiv\begin{cases}\frac{a_1x+b_1}{c_1x+d_1}\not\equiv 1 \pmod{\mathfrak{p}} & \text{if } \mathfrak{p}=(\Phi_l(a_1x+b_1,\ c_1x+d_1)),\\ 1 \pmod{\mathfrak{p}} & \text{otherwise;}\end{cases}$$

$$\tau_{\mathfrak{p}}(\beta)\equiv\begin{cases}\frac{a_2x+b_2}{c_2x+d_2}\not\equiv 1 \pmod{\mathfrak{p}} & \text{if } \mathfrak{p}=(\Phi_l(a_2x+b_2,\ c_2x+d_2)),\\ 1 \pmod{\mathfrak{p}} & \text{otherwise.}\end{cases}$$

If $\alpha=\beta$, then $\tau_{\mathfrak{p}}(\alpha)=\tau_{\mathfrak{p}}(\beta)$, so we must have $(\Phi_l(a_1x+b_1,\ c_1x+d_1))=(\Phi_l(a_2x+b_2,\ c_2x+d_2))$ as primes. Hence for $\mathfrak{p}=(\Phi_l(a_1x+b_1,\ c_1x+d_1))$ we have

$$\frac{a_1x+b_1}{c_1x+d_1}\equiv\frac{a_2x+b_2}{c_2x+d_2} \pmod{\mathfrak{p}}.$$

So

$$(a_1x+b_1)(c_2x+d_2)=(a_2x+b_2)(c_1x+d_1). \ ■$$

Lemma 4.3. *Assume that $\Phi_l(x)$ is irreducible in $F[x]$. Let*

$$\alpha=c_l\left(\frac{a_1x+b_1}{c_1x+d_1}\right),\ \beta=c_l\left(\frac{a_2x+b_2}{c_2x+d_2}\right)\in GG_l(F(x)).$$

Then

$$\alpha=\beta\ \Leftrightarrow\ \overline{\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}}=\overline{\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}}\in \mathrm{PGL}(2,F).$$

In particular, if $\alpha,\beta\in GG_l(F(x))$ are essentially distinct, then $\alpha\neq\beta$.

Proof. $\Leftarrow$: Clear.

$\Rightarrow$: If $\alpha=\beta$, then from Lemma 4.2 we have

$$\frac{a_1x+b_1}{c_1x+d_1}=\frac{a_2x+b_2}{c_2x+d_2}.$$

So

$$a_1c_2=a_2c_1,\qquad b_1d_2=b_2d_1,\qquad a_1d_2+b_1c_2=a_2d_1+b_2c_1.$$

Assume that $a_1c_2=a_2c_1=0$. If $a_1=0$, then $b_1c_1\neq 0$ since $a_1d_1-b_1c_1\neq 0$, so $a_2=0$, therefore $b_2c_2\neq 0$ since $a_2d_2-b_2c_2\neq 0$. So, we can let $d_1/d_2=b_1/b_2=c_1/c_2=u\neq 0$. Then

$$\begin{pmatrix}0 & b_1\\ c_1 & d_1\end{pmatrix}=u\begin{pmatrix}0 & b_2\\ c_2 & d_2\end{pmatrix},\quad\text{so}\quad \overline{\begin{pmatrix}0 & b_1\\ c_1 & d_1\end{pmatrix}}=\overline{\begin{pmatrix}0 & b_2\\ c_2 & d_2\end{pmatrix}}.$$

If $c_2=0$, the result is the same. Therefore $a_1c_2=a_2c_1\neq 0$. Similarly, $b_1d_2=b_2d_1\neq 0$.

Let $a_1/a_2=c_1/c_2=u\neq 0$ and $b_1/b_2=d_1/d_2=v\neq 0$. Then from $a_1d_2+b_1c_2=a_2d_1+b_2c_1$, we have $(a_2d_2-b_2c_2)(u-v)=0$, which leads to

$u = v$ since $a_2d_2 - b_2c_2 \neq 0$. Hence

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = u\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \quad \text{so} \quad \overline{\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}} = \overline{\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}}.$$

The last statement of the lemma is obvious. ∎

Corollary 4.4. *Let $\alpha = c_l(x + b_1)$ and $\beta = c_l(x + b_2)$. Then the following statements are equivalent:*

(i) *α and β are essentially distinct.*
(ii) *$\alpha \neq \beta$.*
(iii) *$b_1 \neq b_2$.*

Proof. (i)⇒(ii). This follows from Lemma 4.3.

(ii)⇒(iii). Clear.

(iii)⇒(i). It is easy to check directly that $\left(\begin{smallmatrix} 1 & b_1 \\ 0 & 1 \end{smallmatrix}\right)$ is essentially distinct from $\left(\begin{smallmatrix} 1 & b_2 \\ 0 & 1 \end{smallmatrix}\right)$ if and only if $b_1 \neq b_2$. ∎

In the following, we will use $\mathfrak{G}_l(n; F)$, $\mathfrak{S}_l(n; F)$ and $\mathfrak{T}_l(n; F)$ to denote the subgroups of $K_2(F(x))$ generated by (any) n essentially distinct nontrivial elements in $GG_l(F(x))$, $SG_l(F(x))$ and $TG_l(F(x))$, respectively.

From Corollary 4.4, we have

Lemma 4.5. *There exist mutually different $b_1, \dots, b_n \in F$ such that*

$$\mathfrak{T}_l(n; F) = \langle c_l(x + b_1), \dots, c_l(x + b_n) \rangle. \ \blacksquare$$

In general, for a field E, a subgroup of $K_2(E)$ is called *cyclotomic* if it is contained in $G_n(E)$. For a subgroup H of $K_2(F(x))$, we write $c(H)$ (resp. $cs(H)$) for the number of cyclotomic elements (resp. cyclotomic subgroups) of H.

5. The rational function field case. Assume that $l \geq 5$ is a prime. Let

$$\beta = \prod_{i=1}^{n} c_l\left(\frac{a_ix + b_i}{c_ix + d_i}\right)^{l_i}, \tag{5.1}$$

where $1 \leq l_i \leq l - 1$ and $n \geq 1$. If $n \geq 2$, we assume that

$$\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \mathrm{GL}(2, F), \qquad 1 \leq i \leq n,$$

are essentially distinct.

It is well known that

$$\mathrm{Gal}(F(x)/F) \cong \mathrm{PGL}(2, F)$$

and $\mathrm{PGL}(2,F)$ acts as automorphisms on $K_2(F(x))$ through

$$\sigma\cdot\{f(x),g(x)\}:=\{f(x),g(x)\}^{\sigma}=\{f(\sigma(x)),g(\sigma(x))\}$$
$$=\left\{f\left(\frac{ax+b}{cx+d}\right),g\left(\frac{ax+b}{cx+d}\right)\right\},$$

where $\sigma=\overline{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)}\in\mathrm{PGL}(2,F)$ with $\sigma(x)=\frac{ax+b}{cx+d}$.

Applying an automorphism of the field $F(x)$, we may assume that the first factor on the right hand side of (5.1) is $c_l(x)^{l_1}$.

The polynomials $\Phi_l(a_ix+b_i,c_ix+d_i)$ are irreducible and by Theorem 2.5, pairwise relatively prime, hence the ideals $\mathfrak{p}_i:=(\Phi_l(a_ix+b_i,c_ix+d_i))$ in $F[x]$ for $i=1,\dots,n$ are prime and distinct.

We will prove some necessary conditions for β to be cyclotomic. First we investigate the factorization of $\Phi_l(f(x),g(x))$.

THEOREM 5.1. *Assume that the element β given by* (5.1) *is cyclotomic:*

$$\beta=c_l(f(x)/g(x)),\tag{5.2}$$

where $f(x),g(x)\in F[x],(f(x),g(x))=1,\deg(f(x)g(x))\geq 1$. Then

(i)

$$\Phi_l(f(x),g(x))=\alpha\Psi^l\prod_{i=1}^{n}\Phi_l(a_ix+b_i,c_ix+d_i)^{r_i},\tag{5.3}$$

where $\alpha\in F^*$, $\Psi\in F[x]$, and $r_i:=v_{\mathfrak{p}_i}(\Phi_l(f(x),g(x)))$ satisfies $l\nmid r_i$. We have $l-1\mid\deg\Psi$.

(ii) *Moreover,*

$$\left(\frac{f(x)}{g(x)}\right)^{r_i}\equiv\left(\frac{a_ix+b_i}{c_ix+d_i}\right)^{l_i}\not\equiv 1 \pmod{\mathfrak{p}_i}\quad \textit{for } i=1,\dots,n.\tag{5.4}$$

Proof. By Lemma 3.1(i), for every prime ideal $\mathfrak{p}$ of $F[x]$ we have

$$\tau_{\mathfrak{p}}(c_l(f(x)/g(x)))\equiv\begin{cases}(f(x)/g(x))^{r_{\mathfrak{p}}}\not\equiv 1 \pmod{\mathfrak{p}} & \text{if } l\nmid r_{\mathfrak{p}},\\ 1 \pmod{\mathfrak{p}} & \text{if } l\mid r_{\mathfrak{p}},\end{cases}\tag{5.5}$$

and by Lemma 3.1(ii),

$$\tau_{\mathfrak{p}}\left(c_l\left(\frac{a_ix+b_i}{c_ix+d_i}\right)\right)\equiv\begin{cases}\frac{a_ix+b_i}{c_ix+d_i}\not\equiv 1 \pmod{\mathfrak{p}} & \text{if } \mathfrak{p}=\mathfrak{p}_i,\\ 1 \pmod{\mathfrak{p}} & \text{otherwise.}\end{cases}\tag{5.6}$$

From (5.1) and (5.2) we get

$$c_l\left(\frac{f(x)}{g(x)}\right)=\prod_{i=1}^{n}c_l\left(\frac{a_ix+b_i}{c_ix+d_i}\right)^{l_i},\tag{5.7}$$

where $1\leq l_i\leq l-1$.

Applying the tame homomorphism $\tau_{\mathfrak{p}}$, where $\mathfrak{p}$ is any prime ideal of $F[x]$, to both sides of (5.7), in view of (5.5) and (5.6) we obtain

$$\tag{5.8} \begin{aligned} \tau_{\mathfrak{p}}\biggl(c_l\biggl(\frac{f(x)}{g(x)}\biggr)\biggr) \not\equiv 1 \pmod{\mathfrak{p}} \ &\Leftrightarrow\ l \nmid v_{\mathfrak{p}}(\varPhi_l(f(x),g(x)))\\ &\Leftrightarrow\ \mathfrak{p} \in \{\mathfrak{p}_1,\dots,\mathfrak{p}_n\}. \end{aligned}$$

Hence in the representation of $\varPhi_l(f(x),g(x))$ as the product of powers of relatively prime polynomials, the irreducible factors $\varPhi_l(a_ix+b_i, c_ix+d_i)$ appear with exponents r_i not divisible by l, and other factors appear with exponents divisible by l. This proves (5.3).

The divisibility $l-1 \mid \deg\varPsi$ follows from Theorem 2.2, since $\varPsi$ is a factor of $\varPhi_l(f(x),g(x))$. Thus we have proved (i).

By (5.8), $\tau_{\mathfrak{p}_i}(c_l(f(x)/g(x))) \equiv (f(x)/g(x))^{r_i} \not\equiv 1 \pmod{\mathfrak{p}_i}$ and, by (5.6),

$$\tau_{\mathfrak{p}_i}\biggl(c_l\biggl(\frac{a_jx+b_j}{c_jx+d_j}\biggr)\biggr) \equiv \begin{cases} \frac{a_ix+b_i}{c_ix+d_i} \not\equiv 1 \pmod{\mathfrak{p}_i} & \text{if } j=i,\\ 1 \pmod{\mathfrak{p}_i} & \text{if } j\neq i. \end{cases}$$

Consequently, (5.7) implies that

$$\biggl(\frac{f(x)}{g(x)}\biggr)^{r_i} \equiv \biggl(\frac{a_ix+b_i}{c_ix+d_i}\biggr)^{l_i} \not\equiv 1 \pmod{\mathfrak{p}_i},$$

which proves (ii). ∎

Denote

$$\theta := \max(\deg f(x), \deg g(x)).$$

THEOREM 5.2. *Let $n \geq 2$. Under the assumption of Theorem 5.1 we have*

$$l \leq 2\theta + 1.$$

Proof. By Theorem 2.4, we have

$$\biggl(\frac{f(x)}{g(x)}\biggr)^{l} \equiv \biggl(\frac{a_ix+b_i}{c_ix+d_i}\biggr)^{l} \equiv 1 \pmod{\mathfrak{p}_i}.$$

Therefore raising both sides of (5.4) to the power r_i' such that $r_ir_i' \equiv 1 \pmod{l}$, we get

$$\frac{f(x)}{g(x)} \equiv \biggl(\frac{a_ix+b_i}{c_ix+d_i}\biggr)^{m_i} \pmod{\mathfrak{p}_i},$$

where $1 \leq m_i \leq l-1$, $m_i \equiv l_ir_i' \pmod{l}$. Hence

$$\frac{f(x)}{g(x)} \equiv \biggl(\frac{c_ix+d_i}{a_ix+b_i}\biggr)^{l-m_i} \pmod{\mathfrak{p}_i}.$$

From $\mathfrak{p}_i = (\varPhi_l(a_ix+b_i, c_ix+d_i))$ we deduce that

$$\tag{5.9} \begin{aligned} &\varPhi_l(a_ix+b_i, c_ix+d_i) \mid f(x)(c_ix+d_i)^{m_i} - g(x)(a_ix+b_i)^{m_i},\\ &\varPhi_l(a_ix+b_i, c_ix+d_i) \mid f(x)(a_ix+b_i)^{l-m_i} - g(x)(c_ix+d_i)^{l-m_i}. \end{aligned}$$

Assume that for some i_0 both polynomials on the r.h.s. of (5.9) are nonzero. Since $\deg \Phi_l(a_{i_0}x + b_{i_0}, c_{i_0}x + d_{i_0}) = l - 1$, the divisibilities (5.9) imply that

$$l - 1 \le \theta + m_{i_0}, \qquad l - 1 \le \theta + l - m_{i_0}.$$

Adding these inequalities we get $2(l-1) \le 2\theta + l$, hence $l \le 2\theta + 2$, and $l \le 2\theta + 1$, since l is an odd prime.

To finish the proof we have to exclude the possibility that for every $i = 1, \ldots, n$ at least one of the polynomials on the r.h.s. of (5.9) vanishes. Since $n \ge 2$, there is $j \ne i, 1 \le j \le n$. Thus it is sufficient to prove that at most one of the polynomials

$$\begin{aligned}
F_1 &= f(x)(c_ix + d_i)^{m_i} - g(x)(a_ix + b_i)^{m_i},\\
F_2 &= f(x)(a_ix + b_i)^{l-m_i} - g(x)(c_ix + d_i)^{l-m_i},\\
F_3 &= f(x)(c_jx + d_j)^{m_j} - g(x)(a_jx + b_j)^{m_j},\\
F_4 &= f(x)(a_jx + b_j)^{l-m_j} - g(x)(c_jx + d_j)^{l-m_j}
\end{aligned}$$

vanishes. Assume that at least two of them vanish. We consider several cases.

1) $F_1 = F_2 = 0$. (For $F_3 = F_4 = 0$ we proceed similarly, replacing i by j.) From $f(x)(c_ix+d_i)^{m_i} = g(x)(a_ix+b_i)^{m_i}$ and $(f(x), g(x)) = (a_ix+b_i, c_ix+d_i) = 1$ it follows that

$$(5.10) \qquad f(x) = \alpha(a_ix + b_i)^{m_i}, \quad g(x) = \alpha(c_ix + d_i)^{m_i} \quad \text{for some } \alpha \in F^*.$$

Analogously $f(x)(a_ix + b_i)^{l-m_i} = g(x)(c_ix + d_i)^{l-m_i}$ implies that

$$(5.11) \qquad f(x) = \alpha'(c_ix+d_i)^{l-m_i},\ g(x) = \alpha'(a_ix+b_i)^{l-m_i} \quad \text{for some } \alpha' \in F^*.$$

From (5.10) we get $\max(\deg f(x), \deg g(x)) = m_i$, and (5.11) implies that $\max(\deg f(x), \deg g(x)) = l - m_i$. Hence $m_i = l - m_i$, so $l = 2m_i$; this is impossible, since l is an odd prime.

2) $F_1 = F_3 = 0$. (For $F_2 = F_4 = 0$ we proceed analogously.) As above we get

$$\begin{aligned}
f(x) &= \alpha(a_ix + b_i)^{m_i}, & g(x) &= \alpha(c_ix + d_i)^{m_i},\\
f(x) &= \alpha'(a_jx + b_j)^{m_j}, & g(x) &= \alpha'(c_jx + d_j)^{m_j},
\end{aligned}$$

where $\alpha, \alpha' \in F^*$. Hence $\max(\deg f(x), \deg g(x)) = m_i = m_j =: m$. Therefore

$$\frac{f(x)}{g(x)} = \left(\frac{a_ix + b_i}{c_ix + d_i}\right)^m = \left(\frac{a_jx + b_j}{c_jx + d_j}\right)^m,$$

hence

$$\frac{a_ix + b_i}{c_ix + d_i} = \eta \cdot \frac{a_jx + b_j}{c_jx + d_j},$$

where $\eta^m = 1$, $\eta \in F$, thus $\eta \in W(F)$.

It follows that

$$\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} = \eta \begin{pmatrix} \eta a_j & \eta b_j \\ c_j & d_j \end{pmatrix},$$

where $\eta \in F^*$. This means that the matrices $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a_j & b_j \\ c_j & d_j \end{smallmatrix}\right)$ are not essentially distinct. We get a contradiction, since $i \neq j$.

3) $F_1 = F_4 = 0$. (The case $F_2 = F_4 = 0$ is quite analogous.) As above we get

$$f(x) = \alpha(a_i x + b_i)^{m_i}, \qquad g(x) = \alpha(c_i x + d_i)^{m_i},$$
$$f(x) = \alpha'(c_j x + d_j)^{l-m_j}, \quad g(x) = \alpha'(a_j x + b_j)^{l-m_j},$$

where $\alpha, \alpha' \in F^*$. Hence $\max(\deg f(x), \deg g(x)) = m_i = l - m_j =: m$. Therefore

$$\frac{f(x)}{g(x)} = \left(\frac{a_i x + b_i}{c_i x + d_i}\right)^m = \left(\frac{c_j x + d_j}{a_j x + b_j}\right)^m,$$

hence

$$\frac{a_i x + b_i}{c_i x + d_i} = \eta \cdot \frac{c_j x + d_j}{a_j x + b_j},$$

where $\eta^m = 1, \eta \in F$, thus $\eta \in W(F)$.

It follows that

$$\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} = \lambda \begin{pmatrix} \eta c_j & \eta d_j \\ a_j & b_j \end{pmatrix} = \lambda \begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix},$$

where $\lambda \in F^*$. This means that $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a_j & b_j \\ c_j & d_j \end{smallmatrix}\right)$ are not essentially distinct. We get a contradiction, since $i \neq j$. ■

LEMMA 5.3. *Let* $\mathrm{ch}(F) = p > 0$ *and* $f, g \in F[x]$. *Then:*

(i) *If* $f \notin F[x^p]$ *and* $f^r \in F[x^p]$, *then* $p \mid r$.
(ii) *If* $(f, g) = 1$ *and* $fg \in F[x^p]$, *then* $f, g \in F[x^p]$.
(iii) $F(x^p) \cap F[x] = F[x^p]$.

Proof. (i) By assumption, $(f^r)' = 0$ and $f' \neq 0$. On the other hand, $(f^r)' = rf'f^{r-1}$. Hence $r = 0$ in F, so $p \mid r$.

(ii) We have $(fg)' = 0$, hence $fg' + f'g = 0$. From $(f, g) = 1$ it follows that $f \mid f'$ and $g \mid g'$; then $f' = g' = 0$, that is, $f, g \in F[x^p]$.

(iii) This is obvious. ■

LEMMA 5.4. *Assume that* $\mathrm{ch}(F) = p > 0$. *If the polynomials* f, g *in* (5.3) *belong to* $F[x^p]$, *then* $\Psi \in F[x^p]$ *and* $p \mid r_i$ *for every* i. *Therefore* (5.3) *implies an analogous formula with* x^p *replaced by* x.

Proof. Let $f(x) = f_0(x^p)$ and $g(x) = g_0(x^p)$, where $f_0, g_0 \in F[x]$. Then

$$\Phi_l(f(x), g(x)) = \Phi_l(f_0(x^p), g_0(x^p)) \in F[x^p].$$

By Lemma 5.3(ii) and (5.3), the polynomials $\Psi(x)$ and $\Phi_l(a_ix+b_i, c_ix+d_i)^{r_i}$ belong to $F[x^p]$. Thus $\Psi(x) = \Psi_0(x^p)$, where $\Psi_0 \in F[x]$.

Since $\Phi_l(a_ix+b_i, c_ix+d_i) \notin F[x^p]$, Lemma 5.3(i) yields $p \mid r_i$. So $r_i = pr_{i0}$. We have $\Phi_l(a_ix+b_i, c_ix+d_i)^p = \Phi_l((a_ix+b_i)^p, (c_ix+d_i)^p)$, because $\Phi_l(x,y)$ has coefficients in $\mathbb{Z}/p$.

Obviously, $(a_ix+b_i)^p = a_{i0}x^p + b_{i0}$, and $(c_ix+d_i)^p = c_{i0}x^p + d_{i0}$, where $a_{i0}, b_{i0}, c_{i0}, d_{i0} \in F$. Therefore $\Phi_l(a_ix+b_i, c_ix+d_i)^p = \Phi_l((a_ix+b_i)^p = \Phi_l(a_{i0}x^p + b_{i0}, c_{i0}x^p + d_{i0})$. Thus (5.3) can be written in the form

$$\Phi_l(f_0(x^p), g_0(x^p)) = \alpha\Psi_0(x^p)^l \prod_{i=1}^{n} \Phi_l(a_{i0}x^p + b_{i0}, c_{i0}x^p + d_{i0})^{r_{i0}}.$$

Replacing x^p by x we get the formula analogous to (5.3). ■

Theorem 5.5. *Assume that* $\operatorname{ch}(F) = p$ *and* $f(x), g(x) \in F[x^p]$. *Then* (5.3) *can be written in the form*

$$\Phi_l(\widetilde{f}(x^{p^r}), \widetilde{g}(x^{p^r})) = \widetilde{\alpha}\widetilde{\Psi}(x^{p^r})^l \prod_{i=1}^{n} \Phi_l(\widetilde{a}_ix^{p^r} + \widetilde{b}_i, \widetilde{c}_ix^{p^r} + \widetilde{d}_i)^{\widetilde{r}_i},$$

where $f(x) = \widetilde{f}(x^{p^r})$, $g(x) = \widetilde{g}(x^{p^r})$ *and* $\Psi(x) = \widetilde{\Psi}(x^{p^r})$ *with* $\widetilde{f}'(x) \neq 0$ *or* $\widetilde{g}'(x) \neq 0$, *and* $\widetilde{r}_i = r_i/p^r \in \mathbb{N}$, $\widetilde{\alpha}, \widetilde{a}_i, \widetilde{b}_i, \widetilde{c}_i, \widetilde{d}_i \in F$.

Proof. If $f(x), g(x) \in F[x^{p^r}]$, but at least one of them does not belong to $F[x^{p^{r+1}}]$, then Lemma 5.4 applied r times yields a formula analogous to (5.3) with the r.h.s. of the form $\Phi_l(\widetilde{f}(x), \widetilde{g}(x))$, where $f(x) = \widetilde{f}(x^{p^r})$ and $g(x) = \widetilde{g}(x^{p^r})$. Moreover, $\widetilde{f}(x)$ or $\widetilde{g}(x)$ does not belong to $F[x^p]$, so $\widetilde{f}'(x) \neq 0$ or $\widetilde{g}'(x) \neq 0$. ■

Let $\widetilde{f}(x), \widetilde{g}(x), \widetilde{\Psi}(x)$ be as in Theorem 5.5, and let $\widetilde{\theta} := \max(\deg \widetilde{f}(x), \deg \widetilde{g}(x))$ and $\widetilde{\lambda} := \deg \widetilde{\Psi}(x)$. Then $\theta = p^r \cdot \widetilde{\theta}$ and $\lambda = p^r \cdot \widetilde{\lambda}$. Note that $r_i = \widetilde{r}_i \cdot p^r$.

Theorem 5.6. *Let* $n \geq 1$. *In the above notation, we have:*

(i) *If* $f'(x) \neq 0$ *or* $g'(x) \neq 0$, *then*

$$n \leq \theta \leq \frac{(l-1)^2 n - 2l}{(l-1)^2 - 2l}.$$

(ii) *If* $f'(x) = g'(x) = 0$, *then*

$$n \leq \widetilde{\theta} \leq \frac{(l-1)^2 n - 2l}{(l-1)^2 - 2l}.$$

(iii) *If* $n \leq \frac{1}{2}(l^2 - 4l + 1)$, *then* $\deg \Psi(x) = 0$, *i.e.*, $\Psi(x) \in F^*$.

Proof. (i) Assume that $f'(x) \neq 0$ or $g'(x) \neq 0$. Denote $\lambda := \deg \varPsi(x)$ and $\theta := \deg f(x) \geq \deg g(x)$. Then (5.3) implies

$$(l-1)\theta = l\lambda + (l-1)\sum_{i=1}^{n} r_i. \tag{5.12}$$

Multiplying (5.3) by $f(x) - g(x)$ we get

$$f(x)^l - g(x)^l = \alpha(f(x) - g(x))\varPsi(x)^l \prod_{i=1}^{n} \varPhi_l(a_i x + b_i, c_i x + d_i)^{r_i}. \tag{5.13}$$

By the well known property of differentiation, we have:

$$\text{If } a, b \in F[x] \text{ satisfy } a^r \mid b, r \geq 1, \text{ then } a^{r-1} \mid b'.$$

Consequently, setting $\varTheta(x) := \varPsi(x)^{l-1} \prod_{i=1}^{n} \varPhi_l(a_i x + b_i, c_i x + d_i)^{r_i - 1}$, from (5.13) we get

$$\varTheta(x) \mid (f(x)^l - g(x)^l)' = l(f'(x)f(x)^{l-1} - g'(x)g(x)^{l-1}). \tag{5.14}$$

By (5.13),

$$\varTheta(x) \mid f(x)^l - g(x)^l. \tag{5.15}$$

Hence $(\varTheta(x), f(x)) = (\varTheta(x), g(x)) = 1$, because $(f(x), g(x)) = 1$.

From

$$\begin{aligned} g'(x)(f(x)^l - g(x)^l) - g(x)\cdot(f'(x)f(x)^{l-1} - g'(x)g(x)^{l-1}) \\ = f(x)^{l-1}(f(x)g'(x) - g(x)f'(x)) \end{aligned}$$

and $(\varTheta(x), f(x)) = 1$, by (5.14) and (5.15), we conclude that

$$\varTheta(x) \mid f(x)g'(x) - g(x)f'(x). \tag{5.16}$$

Since $f'(x) \neq 0$ or $g'(x) \neq 0$, we get $f(x)g'(x) - g(x)f'(x) \neq 0$. Therefore from (5.14) and (5.16) it follows that

$$\begin{aligned} \deg \varTheta(x) &= (l-1)\lambda + (l-1)\sum_{i=1}^{n}(r_i - 1) \\ &\leq \deg(f(x)g'(x) - g(x)f'(x)) \leq 2\theta - 2. \end{aligned} \tag{5.17}$$

Indeed, it is an easy exercise to prove that for any $f(x), g(x) \in F[x]$ satisfying $\theta = \deg f(x) \geq \deg g(x)$ and $f(x)g'(x) - g(x)f'(x) \neq 0$ we have $\deg(f(x)g'(x) - g(x)f'(x)) \leq 2\theta - 2$. It is sufficient to consider the leading terms of $f(x)$ and $g(x)$.

Thus we have proved the two formulas (5.12) and (5.17) relating l, λ and θ. From (5.12) it follows that $l - 1 \mid \lambda$, so $\lambda = (l-1)\lambda_1$, where $\lambda_1 \geq 0$.

Dividing (5.12) and (5.17) by $l-1$ we get

$$\theta = l\lambda_1 + \sum_{i=1}^{n} r_i, \tag{5.18}$$

$$(l-1)\lambda_1 + \sum_{i=1}^{n} r_i - n \le \frac{2}{l-1}(\theta - 1). \tag{5.19}$$

Since $r_i \ge 1$ and $1 \le i \le n$, we get $\sum_{i=1}^{n} r_i \ge n$. Consequently, (5.18) and (5.19) imply

$$\theta \ge l\lambda_1 + n, \tag{5.20}$$

$$(l-1)\lambda_1 \le \frac{2}{l-1}(\theta - 1). \tag{5.21}$$

From (5.20) we get $\theta \ge n$, which gives the first inequality in (i).

By (5.18), (5.19) and (5.21), we have

$$\begin{aligned}\theta &= \sum_{i=1}^{n} r_i + (l-1)\lambda_1 + \lambda_1 \\ &\le n + \frac{2}{l-1}(\theta-1) + \frac{2}{(l-1)^2}(\theta-1) = n + \frac{2l}{(l-1)^2}(\theta-1).\end{aligned}$$

Hence

$$\theta \le \frac{(l-1)^2 n - 2l}{(l-1)^2 - 2l}.$$

This gives the second inequality in (i).

(ii) Assume that $f'(x) = 0$ and $g'(x) = 0$. Clearly we must have $\mathrm{ch}(F) = p > 0$ and $f(x), g(x) \in F[x^p]$. By Theorem 5.5,

$$\Phi_l(\widetilde{f}(X), \widetilde{g}(X)) = \widetilde{\alpha}\widetilde{\Psi}^l \prod_{i=1}^{n} \Phi_l(\widetilde{a}_i X + \widetilde{b}_i, \widetilde{c}_i X + \widetilde{d}_i)^{\widetilde{r}_i},$$

where $f(x) = \widetilde{f}(X)$, $g(x) = \widetilde{g}(X)$, $X = x^{p^r}$ with $\widetilde{f}'(X) \ne 0$ or $\widetilde{g}'(X) \ne 0$.

Let $\widetilde{\lambda} = (l-1)\widetilde{\lambda}_1$. Then similarly we have

$$\widetilde{\theta} = l\widetilde{\lambda}_1 + \sum_{i=1}^{n} \widetilde{r}_i, \tag{5.22}$$

$$(l-1)\widetilde{\lambda}_1 + \sum_{i=1}^{n} \widetilde{r}_i - n \le \frac{2}{l-1}(\widetilde{\theta} - 1). \tag{5.23}$$

Since $\sum_{i=1}^{n} \widetilde{r}_i \ge n$, (5.22) and (5.23) imply

$$\widetilde{\theta} \ge l\widetilde{\lambda}_1 + n, \tag{5.24}$$

$$(l-1)\widetilde{\lambda}_1 \le \frac{2}{l-1}(\widetilde{\theta} - 1). \tag{5.25}$$

From (5.24) we get $\widetilde{\theta} \ge n$, which gives the first inequality in (ii).

By (5.22), (5.23) and (5.25), we have

$$\widetilde{\theta} \leq \frac{(l-1)^2 n - 2l}{(l-1)^2 - 2l}.$$

This gives the second inequality in (ii).

(iii) If $f'(x) \neq 0$ or $g'(x) \neq 0$, from (5.21) and (i) we obtain

$$\lambda_1 \leq \frac{2}{(l-1)^2}(\theta - 1) \leq \frac{2(n-1)}{l^2 - 4l + 1}.$$

It follows that $\lambda_1 < 1$ if $n - 1 < \frac{1}{2}(l^2 - 4l + 1)$. Since $\frac{1}{2}(l^2 - 4l + 1)$ is an integer, the last inequality is equivalent to $n \leq \frac{1}{2}(l^2 - 4l + 1)$. This proves $\lambda_1 = 0$, so $\deg \Psi(x) = \lambda = (l-1)\lambda_1 = 0$.

If $f'(x) = g'(x) = 0$, from (5.25) and (ii) we obtain

$$\widetilde{\lambda}_1 \leq \frac{2}{(l-1)^2}(\widetilde{\theta} - 1) \leq \frac{2(n-1)}{l^2 - 4l + 1}.$$

Similarly $n \leq \frac{1}{2}(l^2 - 4l + 1)$ implies that $\widetilde{\lambda}_1 = 0$, that is, $\deg \Psi(x) = (l-1)\widetilde{\lambda}_1 p^r = 0$. ■

Remarks 5.7. (i) The argument above is analogous to the proof of the *abc*-conjecture for polynomials.

Theorem *abc* (W. W. Stothers). *Let $a, b, c \in F[x]$, where $\operatorname{ch}(F) = 0$ and not all polynomials a, b, c are constant. For a nonzero polynomial $h \in F[x]$ denote by $\operatorname{rad}(h)$ the number of distinct roots of h in the algebraic closure of F. Assume that a, b, c are relatively prime and $a + b = c$. Then*

$$\max(\deg a, \deg b, \deg c) \leq \operatorname{rad}(abc) - 1.$$

We can apply Theorem *abc* as follows. In the notation of (5.13) set $a := f^l$, $b := -g^l$, and $c :=$ the r.h.s. of (5.13). Then $\max(\deg a, \deg b, \deg c) = \deg(f^l) = l\theta, \operatorname{rad}(a) \leq \deg f = \theta, \operatorname{rad}(b) \leq \deg g \leq \theta$, and

$$\operatorname{rad}(c) \leq \deg(f - g) + \deg \Psi + \sum_{i=1}^{n} \deg \Phi_l(f_i, g_i) \leq \theta + \lambda + n(l-1).$$

Consequently, Theorem *abc* gives

$$l\theta \leq 3\theta + (l-1)\lambda_1 + (l-1)n - 1.$$

Considering all terms of this inequality modulo 2, we see that the last term -1 can be replaced by -2.

Hence

$$\theta\left(1 - \frac{2}{l-1}\right) \leq \lambda_1 + n - \frac{2}{l-1}.$$

Now, applying the estimate $\lambda_1 \le \frac{2}{(l-1)^2}(\theta - 1)$ following from (5.21), we get

$$\theta \le \frac{(l-1)^2 n - 2l}{(l-1)^2 - 2l}.$$

Thus we obtain the second inequality in Theorem 5.6(i).

(ii) When $n = 1$, (5.3) is trivial. In fact, we can prove the following statement:

Assume that $f' \ne 0$ or $g' \ne 0$. For $n = 1$ formula (5.3) *takes the form $\Phi_l(x) = \Phi_l(x)$.*

Proof. By Theorem 5.6(i), $n = 1$ implies $\theta = 1$, that is, $\deg f = 1 \ge \deg g$. Hence $f(x) = ax + b, g(x) = cx + d$, where $a = 1$, since we always assume that f is monic.

Therefore (5.3) takes the form

$$\Phi_l(f, g) = \alpha \Phi_l(x)^{r_1} \quad \text{for some } \alpha \in F^*, \tag{5.26}$$

since $\deg \Psi = 0$, by Theorem 5.6(iii).

Comparing the degrees of both sides of (5.26) we get $r_1 = 1$. From (5.26) it follows that the polynomials $\Phi_l(f, g) = \Phi_l(ax + b, cx + d)$ and $\alpha\Phi_l(x)$ are not relatively prime.

Then, by Theorem 2.5, the corresponding matrices

$$\begin{pmatrix} 1 & b \\ c & d \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

are not essentially distinct. Therefore $a = 1$ implies that $b = c = 0$ and $d = \mu$ is a root of unity. Hence

$$\Phi_l(f, g) = \Phi_l(x, \mu) = \alpha\Phi_l(x).$$

Comparing the leading terms we get $\alpha = 1$, so the coefficients of x^{l-2} in both polynomials are 1 and μ. Hence $\mu = 1$, so $f(x) = x, g(x) = 1$, and (5.26) takes the form $\Phi_l(x) = \Phi_l(x)$. ■

Theorem 5.8. *In the above notation, assume that $2 \le n \le \frac{1}{2}(l^2 - 4l + 1)$. Then*

$$l \le 2n + 1.$$

Proof. Assume that $f'(x) \ne 0$ or $g'(x) \ne 0$. Then if $\theta = n$, Theorem 5.2 shows that $l \le 2\theta + 1 = 2n + 1$.

If $\theta > n$, from Theorem 5.6(iii) we get $\lambda_1 = 0$, and then (5.18) and (5.19) give $1 \le \theta - n \le \frac{2}{l-1}(\theta - 1)$. Hence

$$l \le 1 + 2 \cdot \frac{\theta - 1}{\theta - n} = 3 + 2 \cdot \frac{n-1}{\theta - n} \le 3 + 2(n-1) = 2n + 1.$$

Assume that $f'(x) = g'(x) = 0$. Then $\widetilde{f}'(x) \neq 0$ or $\widetilde{g}'(x) \neq 0$. If $\widetilde{\theta} = n$, Theorem 5.2 yields $l \leq 2\widetilde{\theta} + 1 = 2n + 1$.

If $\widetilde{\theta} > n$, from Theorem 5.6(iii) we get $\widetilde{\lambda}_1 = 0$; then (5.22) and (5.23) give $1 \leq \widetilde{\theta} - n \leq \frac{2}{l-1}(\widetilde{\theta} - 1)$. So

$$l - 1 \leq \frac{2(\widetilde{\theta} - 1)}{\widetilde{\theta} - n} \leq 2n.$$

Hence $l \leq 2n + 1$. ■

Corollary 5.9. *Assume that $l \geq 5$ is a prime number and F is a field such that $\Phi_l(x)$ is irreducible in $F[x]$. Let n be an integer satisfying*

$$2 \leq n \leq (l-3)/2,$$

and let $\gamma_1, \ldots, \gamma_n \in GG_l(F(x))$ be essentially distinct. Then

$$\prod_{i=1}^{n} \gamma_i^{l_i} \notin G_l(F(x)),$$

where $1 \leq l_i \leq l - 1$, $i = 1, \ldots, n$.

Proof. This follows from Theorems 5.5 and 5.8. ■

Corollary 5.10. *Assume that $l \geq 5$ is a prime number and F is a field such that $\Phi_l(x)$ is irreducible in $F[x]$. Let n be an integer satisfying $2 \leq n \leq (l-3)/2$. Then every cyclotomic subgroup of $\mathfrak{G}_l(n; F)$ is cyclic of order l.* ■

The following result gives relations between n and θ (or $\widetilde{\theta}$).

Theorem 5.11. *Assume that $n \leq \frac{1}{2}(l^2 - 4l + 1)$. Then:*

(i) *If $f'(x) \neq 0$ or $g'(x) \neq 0$, then $\theta \leq 2n - 1$.*
(ii) *If $f'(x) = g'(x) = 0$, then $\widetilde{\theta} \leq 2n - 1$.*

Proof. If $\theta > 2n - 1$, then from Theorem 5.6(iii), (5.18) and (5.19),

$$l \leq 3 + 2 \cdot \frac{n-1}{\theta - n} < 3 + 2 \cdot \frac{n-1}{(2n-1) - n} = 5,$$

which contradicts the assumption that $l \geq 5$. Hence $\theta \leq 2n - 1$. The proof of $\widetilde{\theta} \leq 2n - 1$ is similar. ■

Remarks 5.12. (a) More precisely, in the case $f'(x) \neq 0$ or $g'(x) \neq 0$, from the proof of Theorem 5.11 it follows that

(i) if $\theta = n$, then $l \leq 2n + 1$;
(ii) if $n < \theta \leq 2n - 1$, then $l \leq 3 + 2 \cdot \frac{n-1}{\theta - n}$.

In particular,

$$\begin{aligned} &\text{if } \theta = n+1, && \text{then} \quad l \le 2n+1;\\ &\text{if } \theta = n+2, && \text{then} \quad l \le n+2;\\ &\text{if } \theta = 2n-1, && \text{then} \quad l \le 5. \end{aligned}$$

(b) From Theorem 5.2, we get a relation between l and θ, namely $l \le 2\theta + 1$. Furthermore, if $\mathrm{ch}(F) = 0$ and $\theta > n$, then from (5.18) and (5.19) we have $l \le 2\theta - 1$. As suggested to the first author by Browkin, the last inequality is actually a necessary condition for $\Phi_l(f, g)$ to have a multiple root. In fact, the following statement is true:

Theorem (Browkin). *Assume that $l \ge 5$ is a prime and $\Phi_l(x)$ is irreducible in $F[x]$. If $\mathrm{ch}(F) = 0$ and $\Phi_l(f, g)$ has a multiple root, where $\gcd(f, g) = 1$, then $l \le 2\theta - 1$.*

In particular, in the cases $l = 5$, $\theta = 2$ and $l = 7$, $\theta = 2$ or 3, the polynomials $\Phi_5(f, g)$ and $\Phi_7(f, g)$ have no multiple root, respectively.

Proof. Assume that α is a multiple root of $\Phi_l(f, g)$; then it must be a multiple root of $f(x) - \zeta g(x)$, where $\zeta = \zeta_l$. Then

$$f(\alpha) - \zeta g(\alpha) = 0, \qquad f'(\alpha) - \zeta g'(\alpha) = 0,$$

so

$$f(\alpha)g'(\alpha) - f'(\alpha)g(\alpha) = 0.$$

It follows that α is a root of $t(x) := f(x)g'(x) - f'(x)g(x)$. From $(f, g) = 1$ and $\mathrm{ch}(F) = 0$ it follows that $t(x)$ is a nonzero polynomial of degree at most $2\theta - 1$.

From $f(\alpha) - \zeta g(\alpha) = 0$ we conclude that $F \subseteq F(\zeta) \subseteq F(\alpha)$. As $[F(\alpha) : F]$ is the degree of the minimal polynomial of α over F, and $[F(\alpha) : F]$ is divisible by $[F(\zeta) : F] = l - 1$, we conclude that $l - 1 \le 2\theta - 1$, i.e., $l \le 2\theta$, so $l \le 2\theta - 1$ since l is odd, as claimed. ∎

Now, we turn to the case of $n = 1$. Let l, p be different prime numbers. Define

$$\mathfrak{Z}(l, p) := \{t \mid 2 \le t \le l - 2,\ t \equiv p^{2m} \text{ or } -p^{2m} \pmod{l} \text{ for some } m \in \mathbb{N}\}.$$

Lemma 5.13. *Assume that $l \ge 5$ is a prime number and F is a field such that $\Phi_l(x)$ is irreducible in $F[x]$. Let $\gamma \in GG_l(F(x))$.*

- (i) *If $\mathrm{ch}(F) = 0$, then none of the elements γ^t, $2 \le t \le l - 2$, is cyclotomic. So, the only cyclotomic elements contained in $\langle\gamma\rangle$ are γ, γ^{-1}. Hence, $\langle\gamma\rangle$ is not a cyclotomic subgroup.*
- (ii) *If $\mathrm{ch}(F) = p \ne 0$, then*

$$1 \ne \gamma^t \in G_l(F(x)) \ \Leftrightarrow\ t \in \{1, l - 1\} \cup \mathfrak{Z}(l, p).$$

So $\langle\gamma\rangle$ contains exactly $2 + |\mathfrak{Z}(l, p)|$ nontrivial cyclotomic elements.

Proof. Clearly, it suffices to consider $\gamma = c_l(x)$. Fix an integer t with $2 \le t \le l-2$. If γ^t is cyclotomic, then there exist nontrivial $f_t, g_t \in F[x]$ such that

$$\gamma^t = c_l(f_t/g_t).$$

By Theorem 5.1(i),

$$\varPhi_l(f_t, g_t) = \alpha_t \varPsi_t^l \varPhi_l(x)^{r_t}. \tag{5.27}$$

Let $\theta_t := \max(\deg f_t, \deg g_t)$ and $\lambda_t := \deg \varPsi_t$.

(i) Assume that $\mathrm{ch}(F) = 0$. Then $f_t'(x) \ne 0$ or $g_t'(x) \ne 0$. From Theorem 5.6(i) we have $\theta_t = 1$, hence $\lambda_t = 0$ and $r_t = 1$.

Now, let

$$f_t(x) = a_t x + b_t, \quad g_t(x) = c_t x + d_t.$$

Then (5.27) becomes

$$\varPhi_l(a_t x + b_t, c_t x + d_t) = \alpha_t \varPhi_l(x).$$

Let $x = \zeta$. Then there exists an i satisfying $1 \le i \le l-1$ such that

$$\frac{a_t\zeta + b_t}{c_t\zeta + d_t} = \zeta^i, \quad \text{so} \quad c_t\zeta^{i+1} + d_t\zeta^i - a_t\zeta - b_t = 0.$$

Easy computations show that the possible cases are only either $a_t = d_t \ne 0$, $b_t = c_t = 0$ or $b_t = c_t \ne 0$, $a_t = d_t = 0$. So either

$$\begin{aligned} f_t(x) &= a_t x, & g_t(x) &= a_t, \quad \text{or} \\ f_t(x) &= c_t, & g_t(x) &= c_t x. \end{aligned}$$

If $f_t(x) = a_t x$, $g_t(x) = a_t$ we get

$$c_l(x)^t = \beta = c_l(f_t/g_t) = c_l(x),$$

which implies $c_l(x) = 1$, a contradiction; if $f_t(x) = c_t$, $g_t(x) = c_t x$, we get

$$c_l(x)^t = c_l(x^{-1}) = c_l(x)^{-1},$$

so $c_l(x)^{t+1} = 1$, therefore $c_l(x) = 1$ since $2 \le t \le l-2$, also a contradiction.

In summary, the equality (5.27) does not hold. So none of $\gamma^t, 2 \le t \le l-2$, is cyclotomic.

(ii) Assume that $\mathrm{ch}(F) = p > 0$. If there exists some t satisfying $2 \le t \le l-2$ such that $f_t' \ne 0$ or $g_t' \ne 0$, then a discussion similar to that in (i) shows that $c_l(x)^t$ is not cyclotomic. Hence, if $\{x, \varPhi_l(x)\}^t$ is cyclotomic for some $2 \le t \le l-2$, we must have $f_t' = 0$ and $g_t' = 0$.

Similarly to (i), we have

$$\varPhi_l(a_t x^{p^{m_t}} + b_t, c_t x^{p^{m_t}} + d_t) = \alpha_t \varPhi_l(x^{p^{m_t}}).$$

Let $x^{p^{m_t}} = \zeta$. Then $\frac{a_t\zeta + b_t}{c_t\zeta + d_t} = \zeta^i$ for some i satisfying $1 \le i \le l-1$. A computation leads to either $a_t = d_t, b_t = c_t = 0$ or $a_t = d_t = 0, b_t = c_t$. So we have either

$$f_t(x) = a_t x^{p^{m_t}}, \quad g_t(x) = a_t, \quad \text{or} \quad f_t(x) = a_t, \quad g_t(x) = a_t x^{p^{m_t}}.$$

If $f_t(x) = a_t x^{p^{m_t}}$, $g_t(x) = a_t$, we have

$$c_l(x)^t = \beta = c_l(x^{p^{m_t}}) = c_l(x)^{p^{2m_t}}.$$

Hence $l \mid p^{2m_t} - t$, that is, $t \in \mathfrak{Z}(l,p)$. If $f_t(x) = a_t$, $g_t(x) = a_t x^{p^{m_t}}$, then $l \mid p^{2m_t} + t$, so also $t \in \mathfrak{Z}(l,p)$. Hence, for $2 \le t \le l-2$, if $c_l(x)^t$ is cyclotomic, then $t \in \mathfrak{Z}(l,p)$.

On the other hand, if $t \in \mathfrak{Z}(l,p)$, then either

$$\begin{aligned} t &= p^{2m_t} + lm' && \text{for some integer } m', \quad \text{or} \\ t &= -p^{2m_t} + lm'' && \text{for some integer } m''. \end{aligned}$$

So either

$$c_l(x)^t = c_l(x)^{p^{2m_t}+lm'} = c_l(x^{p^{m_t}}), \quad \text{or}$$
$$-2ptc_l(t)^t = c_l(x)^{-p^{2m_t}+lm''} = c_l(x)^{-p^{2m_t}} = c_l(x^{-p^{m_t}}).$$

This implies that if $t \in \mathfrak{Z}(l,p)$, then $c_l(x)^t \in G_l(F(x))$.

Note that $c_l(x)$, $c_l(x)^{-1} \in G_l(F(x))$. This proves the lemma. ∎

Lemma 5.13(i) can also be proved by using Remark 5.7(ii).

Lemma 5.14. *The following statements are equivalent:*

(i) $|\mathfrak{Z}(l,p)| = l-3$.

(ii) $l \equiv 3 \pmod 4$ *and* p *is a primitive root of* l.

Proof. Clearly, if p is not a primitive root of l, then the order of $p^2 \pmod l$ is less than $(l-3)/2$. So $|\mathfrak{Z}(l,p)| < l-3$.

When p is a primitive root of l, the set of all quadratic residues modulo l is

$$1, p^2, p^4, \ldots, p^{2(\frac{l-3}{2})}.$$

Consider the map $p^{2m} \mapsto -p^{2m}$. It is a bijection. If $l \equiv 3 \pmod 4$, then

$$\left(\frac{-p^{2m}}{l}\right) = \left(\frac{-1}{l}\right) = (-1)^{(l-1)/2} = -1,$$

where $\left(\frac{\cdot}{l}\right)$ is the Legendre symbol. Hence, if $t \equiv -p^{2m} \pmod l$, then t is a quadratic nonresidue $\pmod l$. So $|\mathfrak{Z}(l,p)| = l-3$.

Conversely, if $l \equiv 1 \pmod 4$, then

$$\left(\frac{-p^{2m}}{l}\right) = \left(\frac{-1}{l}\right) = 1.$$

This implies that the integers in $\mathfrak{Z}(l,p)$ are all quadratic residues modulo l. But the number of quadratic residues is $(l-1)/2$. So

$$|\mathfrak{Z}(l,p)| \le (l-1)/2 < l-3,$$

a contradiction. Hence $l \equiv 3 \pmod 4$. ∎

Corollary 5.15. *Assume that $l \geq 5$ is a prime number and F is a field with* $\mathrm{ch}(F) = p$ *such that $\Phi_l(x)$ is irreducible in $F[x]$. For any $\gamma \in GG_l(F(x))$, the subgroup of $K_2(F(x))$ generated by γ is cyclotomic if and only if* $l \equiv 3 \pmod 4$ *and p is a primitive root of l, i.e.,*

$$\langle\gamma\rangle \subset G_l(F(x)),\ \forall\gamma \in GG_l(F(x)) \\ \Leftrightarrow\ l \equiv 3 \pmod 4 \text{ and } p \text{ is a primitive root of } l.$$

Proof. Clearly,

$$\{\gamma, \gamma^{-1}\} \cup \{\gamma^t \mid t \in \mathfrak{Z}(l,p)\} \subseteq \langle\gamma\rangle,$$

which implies that

$$2 + |\mathfrak{Z}(l,p)| = |\{\gamma, \gamma^{-1}\} \cup \{\gamma^t \mid t \in \mathfrak{Z}(l,p)\}| < |\langle\gamma\rangle| = l.$$

If $l \equiv 3 \pmod 4$, then from Lemma 5.14 we have $2 + |\mathfrak{Z}(l,p)| = l - 1$, so from Lemma 5.13(ii) we get

$$\langle\gamma\rangle = \{1, \gamma, \gamma^{-1}\} \cup \{\gamma^t \mid t \in \mathfrak{Z}(l,p)\} \subseteq G_l(F(x)).$$

Conversely, from Lemma 5.13(ii) we have

$$\langle\gamma\rangle \subseteq \{1, \gamma, \gamma^{-1}\} \cup \{\gamma^t \mid t \in \mathfrak{Z}(l,p)\} \subseteq \langle\gamma\rangle.$$

So $l = 3 + |\mathfrak{Z}(l,p)|$, that is, $|\mathfrak{Z}(l,p)| = l - 3$. From Lemma 5.14 we deduce that $l \equiv 3 \pmod 4$. ∎

Example 5.16. It is easy to show that $\Phi_7(x)$ is irreducible in $\mathbb{F}_3[x]$ and 3 is a primitive root of 7.

Now we arrive at the main result of this section.

Theorem 5.17. *Assume that $l \geq 5$ is a prime number and F is a field such that $\Phi_l(x)$ is irreducible in $F[x]$. Let n be an integer satisfying*

$$n \leq (l-3)/2.$$

(i) *If* $\mathrm{ch}(F) = 0$, *then* $c(\mathfrak{G}_l(n;F)) = 2n$, *and so* $cs(\mathfrak{G}_l(n;F)) = 0$.
(ii) *If* $\mathrm{ch}(F) = p \neq 0$, *then* $c(\mathfrak{G}_l(n;F)) = n(2 + |\mathfrak{Z}(l,p)|)$.
(iii) *If* $\mathrm{ch}(F) = p \neq 0$, *then*

$$cs(\mathfrak{G}_l(n;F)) > 0\ \Leftrightarrow\ l \equiv 3 \pmod 4 \text{ and } p \text{ is a primitive root of } l.$$

In this case, $cs(\mathfrak{G}_l(n;F)) = n$, i.e., $\mathfrak{G}_l(n;F)$ contains exactly n nontrivial cyclotomic subgroups.

(iv) *Every nontrivial cyclotomic subgroup of $\mathfrak{G}_l(n;F)$ is cyclic of order l, i.e., every nontrivial cyclotomic subgroup has the form $\mathfrak{G}_l(1;F)$.*

Proof. (i) follows from Corollary 5.9 and Lemma 5.13(i); (ii) follows from Corollary 5.9 and Lemma 5.13 (ii); (iii) follows from Corollary 5.15; and (iv) follows from (iii) and Corollary 5.10. ∎

Corollary 5.18. *Assume that* $l \geq 5$ *is a prime number with* $l \equiv 3 \pmod 4$ *and* F *is a field with* $\mathrm{ch}(F) = p$ *such that* $\Phi_l(x)$ *is irreducible in* $F[x]$. *If* p *is a primitive root of* l, *then* $\mathfrak{G}_l(1; F)$ *is a cyclotomic subgroup.* ∎

Remark 5.19. From Theorem 5.17, we conclude immediately that $G_l(F(x))$ is not a group, as conjectured by Browkin [1].

Corollary 5.20. *Assume that* $l \geq 5$ *is a prime number. If* n *is a positive integer satisfying* $n \leq (l-3)/2$, *then* $c(\mathfrak{G}_l(n; \mathbb{Q})) = 2n$, *so* $cs(\mathfrak{G}_l(n; \mathbb{Q})) = 0$. ∎

Corollary 5.21. *Assume that* l *is a prime number,* F *is a field with* $\mathrm{ch}(F) \neq l$ *and* $\Phi_l(x)$ *is irreducible in* $F[x]$.

(i) *If* $\mathrm{ch}(F) = 0$ *and* $l \geq 5$ (*resp.* $l \geq 7$ *or* $l \geq 11$), *then* $c(\mathfrak{G}_l(1; F)) = 2$ (*resp.* $c(\mathfrak{G}_l(2; F)) = 4$ *or* $c(\mathfrak{G}_l(3; F)) = 6$ *and* $c(\mathfrak{G}_l(4; F)) = 8$).

(ii) *If* $\mathrm{ch}(F) = p \neq 0$ *and* $l \geq 5$ (*resp.* $l \geq 7$ *or* $l \geq 11$), *then* $c(\mathfrak{G}_l(1; F)) = 2 + |\mathfrak{Z}(l, p)|$ (*resp.* $c(\mathfrak{G}_l(2; F)) = 2(2 + |\mathfrak{Z}(l, p)|)$ *or* $c(\mathfrak{G}_l(3; F)) = 3(2 + |\mathfrak{Z}(l, p)|)$ *and* $c(\mathfrak{G}_l(4; F)) = 4(2 + |\mathfrak{Z}(l, p)|)$). ∎

Corollary 5.22. *Assume that* $l \geq 5$ *is a prime number,* F *is a field with* $\mathrm{ch}(F) \neq l$, *and* $\Phi_l(x)$ *is irreducible in* $F[x]$. *Let* n *be a positive integer satisfying* $n \leq (l-3)/2$.

(i) *If* $\mathrm{ch}(F) = 0$, *then* $c(\mathfrak{S}(n; F)) = c(\mathfrak{T}_l(n; F) = 2n$.

(ii) *If* $\mathrm{ch}(F) = p \neq 0$, *then*

$$c(\mathfrak{S}_l(n; F)) = c(\mathfrak{T}_l(n; F)) = n(2 + |\mathfrak{Z}(l, p)|).$$

In particular, when p *is a primitive root of* l *and* $l \equiv 3 \pmod 4$, *then*

$$cs(\mathfrak{S}_l(n; F)) = cs(\mathfrak{T}_l(n; F)) = n. \ ∎$$

Remark 5.23. The equality (5.3) is actually a diophantine equation for X, Y, Z over the polynomial ring $F[x]$, i.e., it can be rewritten as

$$\frac{X^l - Y^l}{X - Y} = \alpha \prod_{i=1}^{n} \Phi_l(a_i x + b_i, c_i x + d_i)^{e_i} \cdot Z^l,$$

where $1 \leq e_i \leq l-1, \alpha \in F^*$ and $a_i d_i - b_i c_i \neq 0$ with $1 \leq i \leq n$. If $l \geq 5$ is a prime number and $\Phi_l(x)$ is irreducible in $F[x]$, then from the proof of Theorem 5.17 we know that the above diophantine equation has no solution in $F[x]$ if $n \leq (l-3)/2$.

Let $\mathbb{F}_q$ be a finite field of q elements, where q is a power of the prime $p > 2$, and for an integer $m > 0$, denote

$$GG_l(\mathbb{F}_q(x))^m := \{c^m : c \in GG_l(\mathbb{F}_q(x))\}.$$

Corollary 5.24. *Assume that $l \geq 5$ is a prime with $l \equiv 3 \pmod 4$ and $l \neq p$, $\Phi_l(x)$ is irreducible in $\mathbb{F}_p[x]$, and*

$$n := p(p+1) \leq l-3.$$

If p is a primitive root of l, then the set $\bigcup_{m=0}^{l-1} GG_l(\mathbb{F}_p(x))^m$ of cyclotomic elements contains at least n distinct nontrivial cyclotomic subgroups, i.e., there are n essentially distinct elements $c_l\big(\frac{a_ix+b_i}{c_ix+d_i}\big), 1 \leq i \leq n$, such that

$$G_l(\mathbb{F}_p(x)) \supseteq \bigcup_{m=1}^{l-1} GG_l(\mathbb{F}_p(x))^m \supseteq \bigcup_{i=1}^{n} \left\langle c_l\left(\frac{a_ix+b_i}{c_ix+d_i}\right)\right\rangle.$$

Proof. First, since $l \equiv 3 \pmod 4$ and p is a primitive root of l, we have

$$\bigcup_{m=1}^{l-1} GG_l(\mathbb{F}_p(x))^m = \bigcup_{t\in\{1,\,l-1\}\cup\mathfrak{Z}(l,p)} GG_l(\mathbb{F}_p(x))^t \subseteq G_l(\mathbb{F}_p(x)).$$

It is well known that $|\mathrm{PGL}(2,\mathbb{F}_p)| = p(p^2-1)$. Hence from Lemma 4.3,

$$|GG_l(\mathbb{F}_p(x))| = |\mathrm{PGL}(2,\mathbb{F}_p)| = p(p^2-1).$$

According to the definition, if $A = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{F}_p)$ then all matrices which are not essentially distinct from A are

$$\alpha\begin{pmatrix} \mu a & \mu b \\ c & d\end{pmatrix} \quad\text{and}\quad \alpha\begin{pmatrix} \mu c & \mu d \\ a & b\end{pmatrix}, \qquad \text{for all } \alpha,\mu \in \mathbb{F}_p^*. \tag{5.28}$$

Since $p > 2$, it is easy to show that the matrices of (5.28) are different from each other, so the number of elements in each class of non-essentially distinct elements is $2(p-1)^2$. Therefore the number of classes of essentially distinct elements is

$$\frac{|\mathrm{GL}(2,\mathbb{F}_p)|}{2(p-1)^2} = \frac{(p^2-1)(p^2-p)}{2(p-1)^2} = \frac{p(p+1)}{2}.$$

Let $n := p(p+1)/2$. From the assumption, we have $n \leq (l-3)/2$. So by Theorem 5.17(iii), we can choose n essentially distinct elements $c_l\big(\frac{a_ix+b_i}{c_ix+d_i}\big)$, $1 \leq i \leq n$, such that the cyclic subgroups $\big\langle c_l\big(\frac{a_ix+b_i}{c_ix+d_i}\big)\big\rangle$ are different, and

$$\bigcup_{t\in\{1,\,l-1\}\cup\mathfrak{Z}(l,p)} GG_l(\mathbb{F}_p(x))^t \supseteq \bigcup_{i=1}^{n} \left\langle c_l\left(\frac{a_ix+b_i}{c_ix+d_i}\right)\right\rangle.$$

Hence

$$\bigcup_{m=1}^{l-1} GG_l(\mathbb{F}_p(x))^m = \bigcup_{t\in\{1,\,l-1\}\cup\mathfrak{Z}(l,p)} GG_l(\mathbb{F}_p(x))^t \supseteq \bigcup_{i=1}^{n} \left\langle c_l\left(\frac{a_ix+b_i}{c_ix+d_i}\right)\right\rangle. \blacksquare$$

6. The cases $5 \le l \le 2n+1$. Now, we consider the cases of $n > (l-3)/2$, i.e., $l \le 2n+1$, which seem difficult. For $n = 2$ and $l = 5$, we have:

Theorem 6.1. *Assume that F is a field and $\Phi_5(x)$ is irreducible in $F[x]$.*

(i) *If* $\mathrm{ch}(F) = 0$, *then* $c(\mathfrak{T}_5(2;F)) = 4$, *so* $cs(\mathfrak{T}_5(2;F)) = 0$.
(ii) *If* $\mathrm{ch}(F) = p \neq 0, 2$, *then* $c(\mathfrak{T}_5(2;F)) = 2(2 + |\mathfrak{Z}(5,p)|)$.

Proof. It suffices to prove

$$\beta = c_5(x)^{l_1} \cdot c_5(x+b)^{l_2} \notin G_5(F(x)),$$

where $b \neq 0$ and $1 \le l_1, l_2 \le 4$.

Indeed, if $\beta \in G_5(F(x))$, then in the proof of Theorem 5.17, letting $n = 2$, we find that there exist coprime polynomials $f(x), g(x) \in F[x]$, with $f(x)$ monic, such that

$$\Phi_5(f,g) = \alpha \Phi_5(x)^{e_1} \Phi_5(x+b)^{e_2} \quad \text{for some } \alpha \in F, \tag{6.1}$$

and either $\deg f = 2$ or $\deg f = 3$.

We consider the case $\deg f = 2$ (the case $\deg f = 3$ is completely similar). In this case, $e_1 = e_2 = 1$, so (6.1) becomes

$$\Phi_5(f,g) = \alpha \Phi_5(x) \Phi_5(x+b). \tag{6.2}$$

Let $x = \zeta := \zeta_5$. Then $f(\zeta)/g(\zeta) = \zeta^i$, $1 \le i \le 4$, so $f(\zeta) - \zeta^i g(\zeta) = 0$ and $\zeta^{5-i} f(\zeta) - g(\zeta) = 0$. Hence

$$\Phi_5(x) \mid x^2 f(x) - g(x) \quad \text{or} \quad \Phi_5(x) \mid f(x) - x^2 g(x).$$

Similarly, letting $x = \zeta - b$, we get

$$\Phi_5(x) \mid x^2 f(x-b) - g(x-b) \quad \text{or} \quad \Phi_5(x) \mid f(x-b) - x^2 g(x-b).$$

Since $f(x)$ is monic, comparing the degrees we obtain
(6.3)

$$\begin{gathered} \Phi_5(x) = x^2 f(x) - g(x) \quad \text{or} \quad -k_2 \Phi_5(x) = f(x) - x^2 g(x), \\ \Phi_5(x) = x^2 f(x-b) - g(x-b) \quad \text{or} \quad -k_2 \Phi_5(x) = f(x-b) - x^2 g(x-b), \end{gathered}$$

where k_2 is the leading coefficient of $g(x)$.

We claim that $k_2 \neq 0$. Indeed, if $k_2 = 0$, then we have either

$$f(x) = x^2 g(x) \quad \text{or} \quad f(x-b) = x^2 g(x-b).$$

Let

$$f(x) = x^2 + l_1 x + l_0, \qquad g(x) = k_2 x^2 + k_1 x + k_0.$$

If $f(x) = x^2 g(x)$, then $f(x) = x^2, g(x) = 1$, so $\Phi_5(x^2) = \Phi_5(x)\Phi_5(x+b)$. From $\Phi_5(x^2) = \Phi_5(x)\Phi_5(-x)$ we get $\Phi_5(-x) = \Phi_5(x+b)$. Substituting $x = -\zeta$ we get $\Phi_5(b-\zeta) = 0$. Consequently, $b - \zeta = \zeta^k$ for some $k = 1,2,3,4$. This is impossible, since $1, \zeta$ and $1, \zeta, \zeta^k$ $(k > 1)$ are linearly independent over F, because the minimal polynomial of ζ is of degree 4.

If $f(x-b)=x^2g(x-b)$, then $f(x)=(x+b)^2g(x)$, so $f(x)=(x+b)^2$, $g(x)=1$, therefore $\Phi_5((x+b)^2)=\Phi_5(x)\Phi_5(x+b)$. Similarly, a contradiction arises.

Now, formulas (6.3) lead to the following four cases:

(i) $\Phi_5(x)=x^2f(x)-g(x)=x^2f(x-b)-g(x-b)$. Hence $0\neq x^2(f(x)-f(x-b))=g(x)-g(x-b)$. This is impossible, since $\deg(g(x)-g(x-b))<\deg g(x)\le 2$.

(ii) $-k_2\Phi_5(x)=f(x)-x^2g(x)=f(x-b)-x^2g(x-b)$. Then $0\neq f(x)-f(x-b)=x^2(g(x)-g(x-b))$. This leads to a contradiction, since $\deg f(x)=\deg g(x)=2$ implies that we have $f(x)\neq f(x-b)$, $g(x)\neq g(x-b)$ and $\deg(f(x)-f(x-b))<2$.

(iii) $\Phi_5(x)=x^2f(x)-g(x)$ and $-k_2\Phi_5(x)=f(x-b)-x^2g(x-b)$. From the first equality it follows that $f(x)=x^2+x+l_0$ and $g(x)=(l_0-1)x^2-x-1$. Hence the second equality gives $-k_2=1-l_0=1-2b=2b(l_0-1)+1$, so $1-2b=-k_2=2b(l_0-1)+1=2b(2b-1)+1$. Since $\mathrm{ch}(F)\neq 2$, we get $b=0$, a contradiction.

(iv) $\Phi_5(x)=x^2f(x-b)-g(x-b)$ and $-k_2\Phi_5(x)=f(x)-x^2g(x)$. From the second equality it follows that $f(x)=x^2-k_2x-k_2$, $g(x)=k_2x^2+k_2x+k_2+1$. Then the first equality implies $2b+k_2=-1$, $2bk_2-k_2=1$. So $2b+2bk_2=0$, therefore $k_2=-1$. But this implies $b=0$, a contradiction.

Thus, in all the four cases we get a contradiction, so (6.2) does not hold. ■

Remark 6.2. The main result in [29] is a special case of Theorem 6.1. The assumption $\mathrm{ch}(k)\neq 2$ is needed in the proof of Theorem 6.1 because for $\mathrm{ch}(F)=2$ we have

$$\Phi_5(x^2+x,x^2+x+1)=\Phi_5(x)\Phi_5(x+1).$$

For $n=3$ and $l=5$ or 7, we have:

Theorem 6.3. *Assume that F is a field with $\mathrm{ch}(F)\neq 2$, $\Phi_l(x)$ is irreducible in $F[x]$, and $l=5$ or 7.*

(i) *If $\mathrm{ch}(F)=0$, then $c(\mathfrak{T}_l(3;F))=6$, so $cs(\mathfrak{T}_l(3;F))=0$.*
(ii) *If $\mathrm{ch}(F)=p\neq 0$, then $c(\mathfrak{T}_l(3;F))=3(2+|\mathfrak{Z}(l,p)|)$.*

Proof. Similar to the proof of Theorem 6.1, through a rather long computation. ■

7. Diophantine equations. To give a further example, we need the following two lemmas.

Lemma 7.1. *The integer solutions of the diophantine equation*

$$x^4+x^3y+x^2(y^2-1)+xy(y^2-1)+(y^2-1)^2=0$$

are only

$$(0,1),\ (-1,1),\ (0,-1),\ (1,-1).$$

In particular, if $y^2-1\neq 0$, then the equation has no integer solutions.

Proof. Let $(x,y)=(a,b)$ be an integer solution.

If $b^2=1$, then $b=\pm 1$ and $a^4+a^3b=0$. It is easy to see that in these cases the solutions are only

$$(0,1),\ (-1,1),\ (0,-1),\ (1,-1).$$

If $b^2\neq 1$, then rewrite the equation as

$$a^4=[(-ab)-(b^2-1)][a^2+b^2-1].$$

If $a=0$, then $b^2-1=0$, a contradiction; if $b=0$, then $a^4-a^2+1=0$, impossible. Hence $ab\neq 0$. Thus we should have $-ab>b^2-1>0$, so $-ab\geq b^2$. If $b>0$, then $b\leq -a$; if $b<0$, then $-b\leq a$. So, in either case,

$$a^4=[(-ab)-(b^2-1)][a^2+b^2-1]\leq[a^2-(b^2-1)][a^2+b^2-1]=a^4-(b^2-1)^2.$$

This is impossible since $b^2-1\neq 0$. ■

Lemma 7.2. *The equation*

$$x^4+x^3y+x^2(y^2+1)+xy(y^2+1)+(y^2+1)^2=0$$

has no real solutions.

Proof. The polynomial can be written in the form

$$(x^4+x^3y+x^2y^2+xy^3+y^4)+(x^2+xy+y^2)+(y^2+1).$$

The first two summands in brackets are nonnegative and the third is ≥ 1. Hence the value of the polynomial for $x,y\in\mathbb{R}$ is ≥ 1. ■

8. A further example. We continue to consider the cases of $l\leq 2n+1$.

We use $\mathfrak{S}_l^*(2;\mathbb{Z})$ to denote the subgroup of $K_2(\mathbb{Q}(x))$ generated by two essentially distinct nontrivial elements of the form

$$c_l\left(\frac{a_1x+b_1}{c_1x+d_1}\right),\quad c_l\left(\frac{a_2x+b_2}{c_2x+d_2}\right),$$

where

$$\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix},\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}\in\mathrm{SL}(2,\mathbb{Z})$$

satisfying the extra condition

$$\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}^{-1}\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}\neq\pm\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix},\ \pm\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}.$$

Theorem 8.1. *We have $c(\mathfrak{S}_5^*(2;\mathbb{Z}))=4$, hence $cs(\mathfrak{S}_5^*(2;\mathbb{Z}))=0$, i.e., $\mathfrak{S}_5^*(2;\mathbb{Z})$ contains no nontrivial cyclotomic subgroups.*

Proof. Let

$$\beta = c_5\left(\frac{a_1x+b_1}{c_1x+d_1}\right)^{l_1}\cdot c_5\left(\frac{a_2x+b_2}{c_2x+d_2}\right)^{l_2},$$

where

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

We can assume $1 \le l_1, l_2 \le 4$.

We claim that $\beta \notin G_5(\mathbb{Q}(x))$. Indeed, if $\beta \in G_5(\mathbb{Q}(x))$, then as in the discussions of Section 5, there exist coprime $f(x), g(x) \in \mathbb{Q}[x]$ such that

$$\varPhi_5(f,g) = \alpha\varPhi_5(a_1x+b_1, c_1x+d_1)^{e_1}\varPhi_5(a_2x+b_2, c_2x+d_2)^{e_2}, \tag{8.1}$$

where $\alpha \in \mathbb{Q}$, and either $\deg f = 2$ or $\deg f = 3$.

Case 1: $\deg f = 2$. In this case, $e_1 = e_2 = 1$, so (8.1) becomes

$$\varPhi_5(f,g) = \alpha\varPhi_5(a_1x+b_1, c_1x+d_1)\varPhi_5(a_2x+b_2, c_2x+d_2).$$

Let $X = \frac{a_1x+b_1}{c_1x+d_1}$. Then

$$\begin{aligned}\varPhi_5\bigg((a_1-c_1X)^2 f\bigg(\frac{d_1X-b_1}{a_1-c_1X}\bigg), (a_1-c_1X)^2 g\bigg(\frac{d_1X-b_1}{a_1-c_1X}\bigg)\bigg) \\ = \alpha\varPhi_5(X)\varPhi_5(a_2(d_1X-b_1)+b_2(a_1-c_1X), c_2(d_1X-b_1)+d_2(a_1-c_1X)).\end{aligned}$$

So, it suffices to consider

$$\varPhi_5(f,g) = \alpha\varPhi_5(x)\varPhi_5(ax+b, cx+d), \tag{8.2}$$

where $ad - bc = 1$ and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \ne \pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \pm\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Noting that $\zeta \notin \mathbb{Q}$, by the action of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ we have

$$f(x) - \zeta g(x) = \alpha_1(x-\zeta^i)(ax+b-\zeta^j(cx+d)) \quad \text{with } \alpha_1 \in \mathbb{Q}(\zeta). \tag{8.3}$$

Let

$$f(x) = x^2 + l_1x + l_0, \qquad g(x) = k_2x^2 + k_1x + k_0,$$

with $l_0, l_1, k_0, k_1, k_2 \in \mathbb{Q}$.

Inserting these expressions into (8.3) and comparing the coefficients, we get

$$\begin{aligned} ck_2\zeta^{i+j+1} - c\zeta^{i+j} + (ck_1 - dk_2)\zeta^{j+1} - ak_2\zeta^{i+1} \\ + (d - cl_1)\zeta^j + a\zeta^i + (bk_2 - ak_1)\zeta + al_1 - b = 0,\end{aligned} \tag{8.4}$$

$$dk_2\zeta^{i+j+1} - d\zeta^{i+j} + ck_0\zeta^{j+1} - bk_2\zeta^{i+1} - cl_0\zeta^j + b\zeta^i - ak_0\zeta + al_0 = 0. \tag{8.5}$$

We only consider the following cases; the other cases are similar and easy.

1) If $i=1$, $j=2$, from (8.4) and (8.5) we have

$$d-cl_1-ak_2=ck_2, \quad al_1-b=ck_2, \tag{8.6}$$

$$ck_1-dk_2-c=ck_2, \quad a-ak_1+bk_2=ck_2, \tag{8.7}$$

$$ck_0-d=dk_2, \quad b-ak_0=dk_2, \tag{8.8}$$

$$cl_0+bk_2=-dk_2, \quad al_0=dk_2. \tag{8.9}$$

From (8.6), we obtain $(a^2+c^2+ac)k_2=1$, so $k_2\neq 0$; from (8.7), we get $ac+c^2=-1$; so from this equality and (8.8), we have $(a+c)d=1-a^2$; therefore (8.9) yields

$$1-a^2+ab=0.$$

Hence $c^8+2c^6+4c^4+3c^2+1=0$, impossible.

2) If $i=1$, $j=3$, then

$$ck_1-dk_2-c=-ak_2, \quad a-ak_1+bk_2=-ak_2,$$
$$d-cl_1=-ak_2, \quad ck_2+al_1-b=-ak_2,$$
$$d-ck_0=bk_2, \quad ak_0-b=bk_2,$$
$$cl_0=bk_2, \quad dk_2+al_0=-bk_2.$$

From these equalities, we have $k_2\neq 0$ and

$$-1=(a^2+ac+c^2)k_2, \quad a^2+ac-1=0,$$
$$(ab+bc)k_2=1, \quad c(b+d)=-ab.$$

Cancelling k_2, b, c, we obtain $a^8-2a^6+4a^4-3a^2+1=0$, impossible.

3) If $i=1, j=4$, then

$$d-cl_1=ak_2=ck_2+a-ak_1+bk_2=al_1-b-c+ck_1-dk_2=0,$$
$$cl_0=bk_2=dk_2+b-ak_0=ck_0+al_0-d=0.$$

Hence

$$a^2=a^2k_1, \quad c^2k_1-cdk_2=c^2-1, \quad c^2k_0-cd=0, \quad b^2-abk_0=0.$$

Clearly $c\neq 0$, and $a\neq 0$ since $b^2-abk_0=0$. So $k_1=1$, therefore from $c^2k_1-cdk_2=c^2-1$, we obtain $cdk_2=1$; so from $ck_2+a-ak_1+bk_2=0$, we have $b=-c$. Hence from $b^2-abk_0=0, c^2k_0-cd=0$, we get $b/a=k_0=d/c$, that is, $ad-bc=0$, a contradiction.

4) If $i=2$, $j=3$, then

$$ck_1-dk_2=a, \quad ck_2-ak_1+bk_2=a, \quad d-ak_2-cl_1=a, \tag{8.10}$$

$$al_1-b-c=a, \quad ck_2=b, \quad bk_2+cl_0=-b, \quad dk_2-ak_0=b, \quad al_0=b. \tag{8.11}$$

From (8.10) and (8.11), we get respectively

$$(c^2-1)k_2=a^2+ac, \quad a^2k_2=1-a^2-ac-c^2.$$

So

$$a^4 + ca^3 + (c^2 - 1)a^2 + (c^3 - c)a + (c^2 - 1)^2 = 0.$$

From Lemma 7.1, we have $c^2 = 1$. So $a(a + c) = 0$.

If $a = 0$, then $b = 0$ from (8.11), a contradiction. So $a = -c$, hence $a^2 = 1$. From (8.10) and (8.11), we get

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ -a & a \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

This contradicts the assumption.

5) If $i = j = 2$, we have

$$ck_1 - dk_2 - ak_2 = -c, \quad ak_1 - bk_2 = c, \tag{8.12}$$

$$a - cl_1 + d = -c, \quad al_1 - b + ck_2 = -c, \tag{8.13}$$

From (8.12) and (8.13), we get respectively

$$(a^2 + 1)k_2 = c^2 + ac, \qquad c^2 k_2 = -1 - ac - a^2 - c^2.$$

So $c^4 + ac^3 = -(a^2 + 1)(1 + ac + a^2 + c^2)$, i.e.,

$$c^4 + ac^3 + c^2(a^2 + 1) + ac(a^2 + 1) + (a^2 + 1)^2 = 0.$$

This contradicts Lemma 7.2.

6) If $i = j = 3$, then

$$ck_1 - dk_2 - ak_2 = ck_2, \quad bk_2 - ak_1 - c = ck_2, \tag{8.14}$$

$$a - cl_1 + d = ck_2, \quad al_1 - b = ck_2, \tag{8.15}$$

$$ck_0 - bk_2 = dk_2, \quad ak_0 + d = -dk_2, \tag{8.16}$$

We claim that $k_2 \neq 0$. In fact, if $k_2 = 0$, then clearly $c = 0$ (otherwise from (8.14)–(8.16) we will have $k_0 = k_1 = k_2 = 0$), but from (8.15) this will imply $a = -d$, impossible.

From (8.14) and (8.15), we have respectively

$$(c^2 + ac)k_2 = a^2 + 1, \quad (1 + a^2)k_2 = -(a^2 + c^2 + 1).$$

So

$$c^4 + ac^3 + c^2(a^2 + 1) + ac(a^2 + 1) + (a^2 + 1)^2 = 0.$$

A contradiction now arises from Lemma 7.2.

7) If $i = 3$, $j = 2$, we have

$$\begin{aligned} &ck_1 - dk_2 + a = -ak_2, && d - cl_1 = -ak_2, \\ &ck_2 - ak_1 + bk_2 = -ak_2, && al_1 - b - c = -ak_2, \\ &b + ck_0 = -bk_2, && cl_0 = bk_2, \\ &dk_2 - ak_0 = -bk_2, && al_0 - d = -bk_2. \end{aligned}$$

From $cl_0 = bk_2$, $al_0 - d = -bk_2$, we have $cd = b(a+c)k_2$; from $d - cl_1 = -ak_2$, $al_1 - b - c = -ak_2$, we get $c^2 - 1 = a(a+c)k_2$. Hence $b = -c$. Clearly $c \neq 0$, since if $c = b = 0$, then $ad = 1$, hence $a^2 = 1$, so from $ck_1 - dk_2 + a = -ak_2$, we get $-k_2 + a^2 = -a^2k_2$, that is, $1 = 0$, a contradiction.

On the other hand, from $ck_1 - dk_2 + a = -ak_2, ck_2 - ak_1 + bk_2 = -ak_2$, we have

$$a^2 = (1 - a^2 - ac - c^2)k_2.$$

In view of $c^2 - 1 = a(a+c)k_2$, we get

$$a^3(a+c) = (c^2 - 1)(1 - a^2 - ac - c^2).$$

So we obtain

$$a^4 + a^3c + a^2(c^2 - 1) + ac(c^2 - 1) + (c^2 - 1)^2 = 0.$$

From Lemma 7.1, we get $c^2 - 1 = 0$. Hence $ad = 1 - c^2 = 0$.

If $a \neq 0$, then $d = 0$. So we have

$$k_0 = 1 + k_2, \quad l_0 = -k_2, \quad -ak_0 = ck_2, \quad al_0 = ck_2.$$

Hence $k_0 = -l_0 = k_2 = k_0 - 1$, a contradiction.

Therefore $a = 0$. If $d = 0$, then clearly $c(x)$ and $c\left(\frac{-c}{cx}\right)$ are not essentially distinct, which contradicts the assumption.

Hence we get $a = 0$, $d \neq 0$. So

$$ck_1 = dk_2, \quad d = cl_1, \quad k_0 = 1 + k_2, \quad -l_0 = k_2, \quad dk_2 = ck_2, \quad -d = ck_2.$$

Therefore $k_1 = k_2 \neq 0$ since $d \neq 0$, so $d = c$. Hence

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -c \\ c & c \end{pmatrix} = \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

This contradicts the assumption.

Case 2: $\deg f = 3$. In this case, $e_1 + e_2 = 3$, so by symmetry, it suffices to consider the case $e_1 = 2$, $e_2 = 1$, hence (8.1) becomes

$$\Phi_5(f,g) = \alpha\Phi_5(a_1x + b_1, c_1x + d_1)^2\Phi_5(a_2x + b_2, c_2x + d_2).$$

Similarly to (8.2), it suffices to consider

$$\Phi_5(f,g) = \alpha\Phi_5(x)^2\Phi_5(ax + b, cx + d),$$

where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. Similarly, we have

(8.17) $f(x) - \zeta g(x) = \alpha_2(x - \zeta^i)^2(ax + b - \zeta^j(cx + d))$ with $\alpha_2 \in \mathbb{Q}(\zeta)$.

Let

$$f(x) = x^3 + l_2x^2 + l_1x + l_0, \qquad g(x) = k_3x^3 + k_2x^2 + k_1x + k_0.$$

Putting these expression into (8.17) and comparing the coefficients, we get

$$\begin{aligned}&2ck_3\zeta^{i+j+1}-2c\zeta^{i+j}-2ak_3\zeta^{i+1}+(ck_2-dk_3)\zeta^{j+1}+2a\zeta^{i}+(d-cl_2)\zeta^{j}\\&\qquad\qquad\qquad\qquad\qquad\qquad+(bk_3-ak_2)\zeta+(al_2-b)=0,\\&ck_3\zeta^{2i+j+1}-2dk_3\zeta^{i+j+1}-c\zeta^{2i+j}-ak_3\zeta^{2i+1}+2d\zeta^{i+j}+2bk_3\zeta^{i+1}-ck_1\zeta^{j+1}\\&\qquad\qquad\qquad\qquad\qquad\qquad+a\zeta^{2i}-2b\zeta^{i}+cl_1\zeta^{j}+ak_1\zeta-al_1=0,\\&dk_3\zeta^{2i+j+1}-d\zeta^{2i+j}-bk_3\zeta^{2i+1}+b\zeta^{2i}-ck_0\zeta^{j+1}+cl_0\zeta^{j}+ak_0\zeta-al_0=0.\end{aligned}$$

Similarly to the proof of the case $\deg f=2$, we can prove that these equalities do not hold. We omit the details.

In summary, the equality (8.1) does not hold. So $\beta\notin G_5(\mathbb{Q}(x))$, as claimed.

This example implies that the cases of $l\le 2n+1$ are more complicated than one might expect.

QUESTION 8.2. *How to remove the condition $n\le(l-3)/2$ in Theorem 5.17?*

9. Cubes and squares.

From this section on, we turn to the number field cases. In this section we focus on the problem: When is the cube or square of a cyclotomic element still cyclotomic? As a result, we will construct some cyclotomic subgroups of order 5.

First, we need some lemmas on irreducibility of polynomials.

Let

$$\begin{aligned}f_{n,1}(x)&=x^n+x+1 &&\text{if } n\equiv 1 \pmod 3,\\ f_{n,2}(x)&=x^n+x+1/x^2+x+1 &&\text{if } n\equiv 2 \pmod 3).\end{aligned}$$

LEMMA 9.1 (Selmer [16]).

(i) *If $n\not\equiv 2 \pmod 3$, then the polynomial $f_{n,1}(x)$ is irreducible in $\mathbb{Q}[x]$.*

(ii) *If $n\equiv 2 \pmod 3$, then the polynomial x^n+x+1 has a factor x^2+x+1, but $f_{n,2}(x)$ is still irreducible in $\mathbb{Q}[x]$.* ∎

LEMMA 9.2. *For any integer $n\ge 1$ and any prime p, the polynomial $f(x)=x^n+x^{n-1}+p$ is irreducible over $\mathbb{Q}$.*

Proof. Clearly we can assume that $n\ge 2$. The Newton polygon of $f(x)$ for the prime p has vertices $(0,1),(n-1,0),(n,0)$. Therefore it has two sides with slopes $1/(n-1)$ and 0, respectively.

It follows that in $\mathbb{Q}_p[x]$, $f(x)=f_1(x)f_2(x)$, where $\deg f_1=n-1$, $\deg f_2=1$. Any root of $f_1(x)$ generates an extension of $\mathbb{Q}_p$ of degree $n-1$, from the value of the corresponding slope. Consequently, $f_1(x)$ is irreducible in $\mathbb{Q}_p[x]$.

Thus, if $f(x)$ were reducible in $\mathbb{Q}[x]$, it would have factors of degrees 1 and $n-1$. This is impossible since $f(x)$ does not vanish at $\pm 1, \pm 2$, so it does not have a root in $\mathbb{Q}$.

Thus $f(x)$ is irreducible in $\mathbb{Q}[x]$. ■

REMARK 9.3. (i) We can also give a more computational proof of Lemma 9.2 as follows (see [11]). Assume that we have a decomposition

$$x^n + x^{n-1} + p = f(x)g(x) \qquad \text{with } \deg f(x), \deg g(x) \geq 1.$$

Since p is a prime, we can assume that the constant term of, say, $f(x)$ is ± 1.

If $f(x)$ has a root α of modulus 1, that is, $\alpha^n + \alpha^{n-1} + p = 0$ with $|\alpha| = 1$, then

$$p = |\alpha^n + \alpha^{n-1}| = |\alpha^{n-1}|\,|\alpha + 1| = |\alpha + 1|.$$

Clearly $|\alpha + 1| < 2$ if $\alpha \neq 1$. So $\alpha = 1$. But 1 is not a root of $x^n + x^{n-1} + p$, a contradiction.

Hence $f(x)$ has no roots of unit modulus. This implies $\deg f(x) \geq 2$ and $f(x)$ must have a root α with $|\alpha| < 1$. So

$$p = |\alpha^n + \alpha^{n-1}| \leq |\alpha^n| + |\alpha^{n-1}| < 2,$$

a contradiction again. These contradictions prove the irreducibility of the polynomial $x^n + x^{n-1} + p$.

(ii) Similarly, we can prove that $x^n + x^{n-1} - p$ is also irreducible if $n \geq 1$ and $p \geq 3$ is a prime.

The following lemma is crucial in our discussions.

LEMMA 9.4 (Zsigmondy [30]). *If $a > b > 0$, $\gcd(a, b) = 1$ and $n > 1$ are positive integers, then $a^n + b^n$ has a prime factor that divides $a^k + b^k$ for no positive integers $k < n$, with exception $2^3 + 1^3$.* ■

We can construct the cube or square of a cyclotomic element which is also cyclotomic as follows.

THEOREM 9.5.

(i) *Assume that $p > 3$ is a prime. Let α be a zero of $f_{p,i}(x)$, where $i = 1$ or 2, and $F = \mathbb{Q}(\alpha)$. Then*

$$1 \neq c_p(\alpha)^3 = c_p(\alpha^3) \in G_p(F).$$

(ii) *Assume that $p \geq 3$ be a prime. Let α be a zero of $x^p + x^{p-1} + 2$ and $F = \mathbb{Q}(\alpha)$. Then*

$$1 \neq c_p(\alpha)^2 = c_p(\alpha^2) \in G_p(F).$$

Proof. (i) Clearly $\alpha^{p-1} \neq 0, 1$. From $\alpha^p + \alpha + 1 = 0$, we have

$$\alpha^{p-1}(\alpha^p + \alpha + 1) = 0,$$

therefore $\alpha^{2p-1}+\alpha^{p-1}=\alpha+1$, so $\alpha^{2p}+\alpha^{p}+1=\alpha^2+\alpha+1$, that is,

$$\frac{\alpha^{3p}-1}{\alpha^p-1}=\frac{\alpha^3-1}{\alpha-1},\quad \text{so}\quad \frac{\alpha^p-1}{\alpha-1}=\frac{\alpha^{3p}-1}{\alpha^3-1}.$$

Hence $\Phi_p(\alpha)=\Phi_p(\alpha^3)$, and therefore

$$c_p(\alpha)^3=\{\alpha^3,\Phi_p(\alpha)\}=\{\alpha^3,\Phi_p(\alpha^3)\}=c_p(\alpha^3)\in G_p(F).$$

Now, we prove that $c_p(\alpha)^3\neq 1$. Since $p>3$ is a prime, it suffices to prove $c_p(\alpha)\neq 1$.

First, we simplify the formula for $c_p(\alpha)$. Namely,

$$\Phi_p(\alpha)=\frac{1-\alpha^p}{1-\alpha}=\frac{1+(\alpha+1)}{1-\alpha}=\frac{\alpha+2}{1-\alpha}.$$

Hence

$$c_p(\alpha)=\{\alpha,\Phi_p(\alpha)\}=\left\{\alpha,\frac{\alpha+2}{1-\alpha}\right\}=\{\alpha,\alpha+2\},$$

since $\{\alpha,1-\alpha\}=1$. But

$$\begin{aligned}\{\alpha,\alpha+2\}&=\left\{-2\left(\frac{-\alpha}{2}\right),2\left(1+\frac{\alpha}{2}\right)\right\}=\left\{-2,1+\frac{\alpha}{2}\right\}\left\{\frac{-\alpha}{2},2\right\}\\&=\{-2,2+\alpha\}\{\alpha,2\}.\end{aligned}$$

So

$$c_p(\alpha)=\{-2,2+\alpha\}\{\alpha,2\}.$$

Clearly, α is a unit. Hence $v_{\mathfrak p}(\alpha)=0$ for every prime ideal $\mathfrak p$. Therefore, for every prime ideal $\mathfrak p\nmid 2$, we get

$$\tau_{\mathfrak p}(c_p(\alpha))=\tau_{\mathfrak p}(\{-2,\alpha+2\}\{\alpha,2\})\equiv(-2)^{v_{\mathfrak p}(\alpha+2)}\pmod{\mathfrak p}. \tag{9.1}$$

When $p\equiv 1\pmod 3$, from Lemma 9.1, $f_{p,1}(x)$ is irreducible in $\mathbb{Q}[x]$. So the minimal polynomial of $\alpha+2$ is

$$f_{p,1}(x-2)=(x-2)^p+(x-2)+1=x^p-2px^{p-1}+\cdots+2^{p-1}px+x-(2^p+1).$$

Hence $N_{F/\mathbb{Q}}(\alpha+2)=2^p+1$.

When $p\equiv 2\pmod 3$, from Lemma 9.1, $f_{p,2}(x)$ is also irreducible in $\mathbb{Q}[x]$. So the minimal polynomial of $\alpha+2$ is $f_{p,2}(x-2)$. From

$$(x-2)^p+(x-2)+1=[(x-2)^2+(x-2)+1]f_{p,2}(x-2),$$

we find that $N_{F/\mathbb{Q}}(\alpha+2)=\frac{1}{3}(2^p+1)$.

Now we assume that $p\equiv 1\pmod 3$; the case of $p\equiv 2\pmod 3$ can be treated in a similar way.

Suppose that we have a decomposition into prime ideals

$$(\alpha+2)\mathcal{O}_F=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}.$$

In view of $N_{F/\mathbb{Q}}(\alpha+2) = 2^p+1$, we can assume that $e_i \geq 1$ and $m \geq 1$. Let p_i be primes (not necessarily different) such that $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$. Then

$$N_{F/\mathbb{Q}}((\alpha+2)\mathcal{O}_F) = N_{F/\mathbb{Q}}(\mathfrak{p}_1)^{e_1} \cdots N_{F/\mathbb{Q}}(\mathfrak{p}_m)^{e_m} = p_1^{e_1 f_1} \cdots p_m^{e_m f_m}\mathbb{Z},$$

where $f_i = f(\mathfrak{p}_i|p_i)$ are the residue class degrees.

From Lemma 9.4, the number 2^p+1 has a primitive prime divisor, say q, i.e., $q \,|\, 2^p+1$ but $q \nmid 2^d+1$ for any integer $1 \leq d < p$.

Assume that $v_q(2^p+1) = l$. Then

$$N_{F/\mathbb{Q}}((\alpha+2)\mathcal{O}_F) = N_{F/\mathbb{Q}}(\alpha+2)\mathbb{Z} = (2^p+1)\mathbb{Z} = q^l a\mathbb{Z}$$

for some $q \nmid a$. Therefore

$$q^l a\mathbb{Z} = p_1^{e_1 f_1} \cdots p_m^{e_m f_m}\mathbb{Z}.$$

This implies that q must be one of the primes $p_1, \ldots, p_m$, say $q = p_1$. Note that the primes p_i may not be distinct. So we have

$$l = e_1 f_1 + \cdots \geq e_1.$$

On the other hand, clearly $q \neq 3$, i.e., $q \geq 5$, so

$$5^l \leq q^l < 2^p+1,$$

therefore $l < p$, hence $e_1 \leq l < p$, that is, $v_{\mathfrak{p}_1}(\alpha+2) = e_1 < p$. This implies

$$p_1 = q \nmid 2^{v_{\mathfrak{p}_1}(\alpha+2)} + 1.$$

Note that also

$$p_1 \nmid 2^{v_{\mathfrak{p}_1}(\alpha+2)} - 1.$$

In fact, if $p_1 \,|\, 2^{v_{\mathfrak{p}_1}(\alpha+2)} - 1$, then from $p_1 \,|\, 2^p+1$ we get

$$p_1 \,|\, (2^p+1) + (2^{v_{\mathfrak{p}_1}(\alpha+2)} - 1) = 2^p + 2^{v_{\mathfrak{p}_1}(\alpha+2)} = 2^{v_{\mathfrak{p}_1}(\alpha+2)}(2^{p-v_{\mathfrak{p}_1}(\alpha+2)} + 1).$$

Since $p_1 = q \neq 2$, we obtain $p_1 \,|\, 2^{p-v_{\mathfrak{p}_1}(\alpha+2)} + 1$. This contradicts the choice of $q = p_1$ since $v_{\mathfrak{p}_1}(\alpha+2) \neq 0$.

Hence from (9.1), we get

$$\tau_{\mathfrak{p}_1}(c_p(\alpha)) \equiv (-2)^{v_{\mathfrak{p}_1}(\alpha+2)} \not\equiv 1 \pmod{\mathfrak{p}_1}.$$

Therefore $c_p(\alpha) \neq 1$.

(ii) From $\alpha^p + \alpha^{p-1} + 2 = 0$, we have

$$(1+\alpha)^2\Phi_p(-\alpha) = (1+\alpha)(\alpha^p+1) = \alpha(\alpha^p+\alpha^{p-1}) + 1 + \alpha = 1 - \alpha.$$

Then $\{\alpha, (1+\alpha)^2\} = \{-1, 1+\alpha\}^2\{-\alpha, 1+\alpha\}^2 = \{1, 1+\alpha\} = 1$ yields

$$\begin{aligned} c_p(\alpha) &= \{\alpha, \Phi_p(\alpha)\} = \{\alpha, (1-\alpha)\Phi_p(\alpha)\} = \{\alpha, (1+\alpha)^2\Phi_p(-\alpha)\Phi_p(\alpha)\} \\ &= \{\alpha, \Phi_p(\alpha^2)\}. \end{aligned}$$

So

$$c_p(\alpha)^2 = \{\alpha^2, \Phi_p(\alpha^2)\} = c_p(\alpha^2) \in G_p(F).$$

Now, we prove $c_p(\alpha) \neq 1$. From $\alpha^p + \alpha^{p-1} + 2 = 0$ and $(1+\alpha)^2 \Phi_p(-\alpha) = 1 - \alpha$, we have

$$\begin{aligned} \Phi_p(\alpha) &= \frac{\alpha^p - 1}{\alpha - 1} = \frac{\alpha^p + 1}{\alpha + 1} \cdot \frac{\alpha + 1}{\alpha - 1} + \frac{2}{1 - \alpha} \\ &= \frac{1 - \alpha}{(1+\alpha)^2} \cdot \frac{1 + \alpha}{\alpha - 1} + \frac{2}{1 - \alpha} = \frac{1 + 3\alpha}{1 - \alpha^2}. \end{aligned}$$

So

$$c_p(\alpha) = \{\alpha, \Phi_p(\alpha)\} = \left\{\alpha, \frac{1+3\alpha}{1-\alpha^2}\right\} = \{-3, 1+3\alpha\}^{-1}\{-1, 1+\alpha\}.$$

Clearly, α is a unit. Hence $v_{\mathfrak{p}}(\alpha) = 0$ for every prime ideal $\mathfrak{p}$. Therefore, for every prime ideal $\mathfrak{p} \nmid 2$, we get

$$\begin{aligned} \tau_{\mathfrak{p}}(c_p(\alpha)) &= \tau_{\mathfrak{p}}(\{-3, 1+3\alpha\}^{-1}\{-1, 1+\alpha\}) \\ &\equiv (-3)^{-v_{\mathfrak{p}}(1+3\alpha)}(-1)^{v_{\mathfrak{p}}(1+\alpha)} \pmod{\mathfrak{p}}. \end{aligned} \tag{9.2}$$

From Lemma 9.2, $x^p + x^{p-1} + 2$ is irreducible over $\mathbb{Q}$. So

$$N_{F/\mathbb{Q}}(1+3\alpha) = 2(3^p + 1).$$

Suppose that we have a decomposition into prime ideals

$$(1+3\alpha)\mathcal{O}_F = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}.$$

In view of $N_{F/\mathbb{Q}}(1+3\alpha) = 2(3^p+1)$, we can assume that $e_i \geq 1$ and $m \geq 1$. Let p_i be primes (not necessarily different) such that $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$. Then

$$N_{F/\mathbb{Q}}((1+3\alpha)\mathcal{O}_F) = N_{F/\mathbb{Q}}(\mathfrak{p}_1)^{e_1} \cdots N_{F/\mathbb{Q}}(\mathfrak{p}_m)^{e_m} = p_1^{e_1 f_1} \cdots p_m^{e_m f_m}\mathbb{Z},$$

where $f_i = f(\mathfrak{p}_i | p_i)$ are the residue class degrees.

From Lemma 9.4, the number $3^p + 1$ has a primitive prime divisor, say q, i.e., $q \mid 3^p + 1$ but $q \nmid 3^d + 1$ for any integer $1 \leq d < p$. Clearly $q \neq 2, 3$.

Assume that $v_q(3^p + 1) = l$. Then

$$N_{F/\mathbb{Q}}((1+3\alpha)\mathcal{O}_F) = N_{F/\mathbb{Q}}(1+3\alpha)\mathbb{Z} = 2(3^p+1)\mathbb{Z} = q^l a\mathbb{Z}$$

for some $q \nmid a$. Therefore

$$q^l a\mathbb{Z} = p_1^{e_1 f_1} \cdots p_m^{e_m f_m}\mathbb{Z}.$$

This implies that q must be one of the primes $p_1, \ldots, p_m$, say $q = p_1$. Note that the primes p_i may not be distinct. Thus

$$l = e_1 f_1 + \cdots \geq e_1.$$

Let $\mathfrak{p}_1$ be a prime lying above q. Then

$$1 \leq v_{\mathfrak{p}_1}(1+3\alpha) \leq v_q(3^p+1) < p.$$

This implies that

$$p_1 = q \nmid 3^{v_{\mathfrak{p}_1}(1+3\alpha)} + 1,$$

Note that also

$$p_1 \nmid 3^{v_{\mathfrak{p}_1}(1+3\alpha)} - 1.$$

In fact, if $p_1 \mid 3^{v_{\mathfrak{p}_1}(1+3\alpha)} - 1$, then from $p_1 \mid 3^p + 1$ we get

$$p_1 \mid (3^p+1) + (3^{v_{\mathfrak{p}_1}(1+3\alpha)} - 1) = 3^p + 3^{v_{\mathfrak{p}_1}(1+3\alpha)} = 3^{v_{\mathfrak{p}_1}(1+3\alpha)}(3^{p-v_{\mathfrak{p}_1}(1+3\alpha)} + 1).$$

Since $p_1 = q \neq 3$, we get $p_1 \mid 3^{p-v_{\mathfrak{p}_1}(1+3\alpha)} + 1$. This contradicts the choice of $q = p_1$ since $v_{\mathfrak{p}_1}(1+3\alpha) \neq 0$.

From $\mathfrak{p}_1 \mid 1 + 3\alpha = (1+\alpha) + 2\alpha$ and $\mathfrak{p}_1 \mid q \neq 2$, we know that $\mathfrak{p}_1 \nmid 1 + \alpha$, i.e., $v_{\mathfrak{p}_1}(1+\alpha) = 0$. So

$$\tau_{\mathfrak{p}_1}(c_p(\alpha)) = (-3)^{v_{\mathfrak{p}_1}(1+3\alpha)}(-1)^{v_{\mathfrak{p}_1}(1+\alpha)} \equiv (-3)^{-v_{\mathfrak{p}_1}(1+3\alpha)} \not\equiv 1 \pmod{\mathfrak{p}_1}.$$

Therefore $c_p(\alpha) \neq 1$. ∎

Let S_n denote the symmetric group of degree n.

Lemma 9.6.

(i) *The Galois group of* $x^p + x + 1$ *is isomorphic to* S_p.
(ii) *The Galois group of* $x^3 - x^2 + 1$ *is isomorphic to* S_3.
(iii) *The Galois group of* $x^5 + x^4 + 2$ *is isomorphic to* S_5.

Proof. (i) follows from Lemma 9.1 and [11, Theorem 1]; (ii) follows from Lemma 9.1 and [11, Theorem 2]; (iii) can be proved using GP-Pari. ∎

Lemma 9.7 ([19]). *Let* L/F *be a Galois extension of finite degree* n *with* $G := \mathrm{Gal}(L/F)$. *Then the kernel of the canonical homomorphism* $K_2(F) \to K_2(L)^G$ *is killed by* n.

Corollary 9.8.

(i) *Let* α *be a zero of* $f_{p,1}(x) = x^p + x + 1$ *or* $f_{5,2}(x) = x^3 - x^2 + 1$, *let* $F = \mathbb{Q}(\alpha)$ *and let* $\widetilde{F}$ *be the normal closure of* F. *Then for any* $\sigma \in \mathrm{Gal}(\widetilde{F}/\mathbb{Q})$,

$$c_p(\sigma(\alpha))^{\pm 3} \neq 1.$$

Moreover, in $K_2(\widetilde{F})$ *we have*

$$\prod_{\sigma\in G} c_p(\sigma(\alpha)) = c_p(-2),$$

i.e., the element $\prod_{\sigma\in G} c_p(\sigma(\alpha))$ *is also cyclotomic.*

(ii) *Let* α *be a zero of* $x^p + x^{p-1} + 2$, *let* $F = \mathbb{Q}(\alpha)$ *and let* $\widetilde{F}$ *be the normal closure of* F. *Then for any* $\sigma \in \mathrm{Gal}(\widetilde{F}/\mathbb{Q})$,

$$c_p(\sigma(\alpha))^{\pm 3} \neq 1.$$

Moreover, in $K_2(\widetilde{F})$ *we have*

$$\prod_{\sigma\in G} c_p(\sigma(\alpha)) = c_p(-1/3).$$

Proof. (i) From Lemma 9.6(i), we have $[\widetilde{F} : F] = [\widetilde{F} : \mathbb{Q}]/[F : \mathbb{Q}] = |S_p|/p = (p-1)!$, and from Lemma 9.7, the kernel of $K_2(F) \to K_2(\widetilde{F})^G \subseteq K_2(\widetilde{F})$ is killed by $[\widetilde{F} : F]$. As $([\widetilde{F} : F], p) = 1$, we get the injection

$$G_p(F) \hookrightarrow G_p(\widetilde{F}),$$

since $G_p(F)$ is contained in the p-torsion of $K_2(F)$ (see [1]).

A similar discussion works for $f_{5,2}(x)$, since from Lemma 9.6(ii), we have $\mathrm{Gal}(\widetilde{F}/\mathbb{Q}) \cong S_3$, and so $[\widetilde{F} : F] = |S_3|/[F : \mathbb{Q}] = 2$.

Thus the first statement follows from Theorem 9.5(i) and the facts that $\sigma(c_p(\alpha)) = c_p(\sigma(\alpha))$ and $c_p(\alpha)^{-1} = c_p(\alpha^{-1})$.

From the proof of Theorem 9.5(i), in $K_2(\widetilde{F})$ we have

$$\begin{aligned}\prod_{\sigma\in G} c_p(\sigma(\alpha)) &= \prod_{\sigma\in G}\{-2, 2+\sigma(\alpha)\}\{\sigma(\alpha), 2\}\\ &= \{-2, -f_{p,1}(-2)\}\{N_{F/\mathbb{Q}}(\alpha), 2\}\\ &= \{-2, 2^p+1\} = \left\{-2, \frac{2^p+1}{3}\right\}\\ &= \{-2, \Phi_p(-2)\} = c_p(-2).\end{aligned}$$

A similar reasoning works for $f_{5,2}(x)$.

(ii) The proof of the first statement is similar to that of (i); one uses Lemmas 9.5(ii), 9.6(iii) and 9.7.

As for the second statement, from the proof of Theorem 9.5(i) we have

$$\begin{aligned}\prod_{\sigma\in G} c_p(\sigma(\alpha)) &= \prod_{\sigma\in G}\{-3, 1+3\sigma(\alpha)\}\{-1, 1+\sigma(\alpha)\}\\ &= \{-3, N_{F/\mathbb{Q}}(1+3\alpha)\}^{-1}\cdot\{-1, N_{F/\mathbb{Q}}(1+\alpha)\}\\ &= \{-3, 2(3^p+1)\}^{-1}\{-1,-1\}\\ &= \{-3, \Phi_p(-3)\}^{-1}\cdot\{-3,-8\}^{-1}\{-1,-1\}\\ &= c_p(-3)^{-1} = c_p(-1/3). \ \blacksquare\end{aligned}$$

In the case of $f_{p,2}(x)$, Browkin informed the first author that $\langle c_p(\alpha)\rangle$ is a cyclotomic subgroup when $p = 5$. Moreover, in the following examples, we can construct more nontrivial cyclotomic subgroups.

Example 9.9. Let $p = 5$. Then it is easy to show that

$$f_{5,2}(x) = x^3 - x^2 + 1.$$

Let α be a zero of $f_{5,2}(x)$ and $F = \mathbb{Q}(\alpha)$. Then from Theorem 9.5(i), we get

$$1 \neq c_5(\alpha)^3 = c_5(\alpha^3) \in G_5(F).$$

On the other hand,

$$c_5(\alpha)^2 = c_5(\alpha)^{-3} = c_5(\alpha^{-3}), \qquad c_5(\alpha)^4 = c_5(\alpha)^{-1} = c_5(\alpha^{-1}).$$

Hence $\langle c_5(\alpha)\rangle \subset G_5(F)$, i.e., $\langle c_5(\alpha)\rangle$ is a cyclotomic subgroup.

Now, let $\widetilde{F}$ be the normal closure of $F = \mathbb{Q}(\alpha)$. Then from Lemma 9.8(i), for any $\sigma \in G := \mathrm{Gal}(\widetilde{F}/\mathbb{Q})$, we have $1 \neq c_5(\sigma(\alpha))^{\pm 3} \in G_5(\widetilde{F})$, and therefore

$$\bigcup_{\sigma\in G} \langle c_5(\sigma(\alpha))\rangle \subseteq G_5(\widetilde{F}). \tag{9.3}$$

Let $\alpha := \alpha_1, \alpha_2$ and α_3 be the three roots of $f_{5,2}(x) = x^3 - x^2 + 1$. Then (9.3) becomes

$$\langle c_5(\alpha_1)\rangle \cup \langle c_5(\alpha_2)\rangle \cup \langle c_5(\alpha_3)\rangle \subseteq G_5(\widetilde{F}).$$

Claim. *The cyclotomic subgroups $\langle c_5(\alpha_1)\rangle, \langle c_5(\alpha_2)\rangle, \langle c_5(\alpha_3)\rangle$ are different from each other. Hence $G_5(\widetilde{F})$ contains at least three nontrivial cyclotomic subgroups.*

In fact, from the proof of Theorem 9.5(i), we have

$$c_5(\alpha_1) = \{-2, 2 + \alpha_1\}\{\alpha_1, 2\},$$

and $N_{F/\mathbb{Q}}(2 + \alpha_1) = 11$.

To compute the tame symbol of $c_5(\alpha_1)$, we need to know the prime decomposition of the integer 11 in $\mathcal{O}_{\widetilde{F}}$.

First, we determine the prime decomposition of 11 in $\mathcal{O}_F$. It is easy to show that the discriminant of $f_{5,2}(x)$ is -23, i.e.,

$$d_F(1, \alpha_1, \alpha_1^2) = d(f_{5,2}) = -23,$$

which is square-free. So $1, \alpha_1, \alpha_1^2$ is an integral base of $\mathcal{O}_F$, that is, $\mathcal{O}_F = \mathbb{Z}[\alpha_1]$. By the well known Kummer criterion, we have

$$11\mathcal{O}_F = \mathfrak{p}_1\mathfrak{p}_2, \tag{9.4}$$

where $\mathfrak{p}_1 := (2 + \alpha_1), \mathfrak{p}_2 := (\alpha_1^2 - 3\alpha_1 + 6)$ are different prime ideals in $\mathcal{O}_F$. Moreover $f(\mathfrak{p}_2|11) = 2$. Hence $f(\mathfrak{p}_1|11) = 1$.

Now, suppose that in $\mathcal{O}_{\widetilde{F}}$ we have prime decompositions

$$\mathfrak{p}_1\mathcal{O}_{\widetilde{F}} = \mathfrak{P}_1^{e_1}(\mathfrak{P}_1')^{e_1'}, \qquad \mathfrak{p}_2\mathcal{O}_{\widetilde{F}} = \mathfrak{B}_2^{e_2}\mathfrak{B}_3^{e_3}.$$

From $[\widetilde{F} : F] = 2$, we have

$$2 = e_1 f(\mathfrak{P}_1|\mathfrak{p}_1) + e_1' f(\mathfrak{P}_1'|\mathfrak{p}_1), \qquad 2 = e_2 f(\mathfrak{P}_2|\mathfrak{p}_2) + e_3 f(\mathfrak{P}_3|\mathfrak{p}_2).$$

Since $\widetilde{F}/F$ is a Galois extension, from $f(\mathfrak{p}_1|11) = 1, f(\mathfrak{p}_2|11) = 2$ we know that

$$f(\mathfrak{P}_1|\mathfrak{p}_1) = f(\mathfrak{P}_1'|\mathfrak{p}_1) = 2, \qquad f(\mathfrak{P}_2|\mathfrak{p}_2) = f(\mathfrak{P}_3|\mathfrak{p}_2) = 1.$$

So $e_1 = 1$, $e_1' = 0$ and $e_2 = e_3 = 1$, which implies that

$$\mathfrak{p}_1\mathcal{O}_{\widetilde{F}} = \mathfrak{P}_1, \quad \mathfrak{p}_2\mathcal{O}_{\widetilde{F}} = \mathfrak{B}_2\mathfrak{B}_3.$$

As in $\mathcal{O}_{\widetilde{F}}$ we have the decomposition $\alpha_1^2 - 3\alpha_1 + 6 = (2+\alpha_2)(2+\alpha_3)$, from (9.4) we get

$$11\mathcal{O}_{\widetilde{F}} = \mathfrak{P}_1\mathfrak{B}_2\mathfrak{B}_3, \tag{9.5}$$

where $\mathfrak{P}_i = (2+\alpha_i)\mathcal{O}_{\widetilde{F}}, i = 1,2,3$, are different prime ideals. Therefore (9.5) is just the prime decomposition of 11 in $\mathcal{O}_{\widetilde{F}}$, as required.

Note that α_i, $i = 1,2,3$, are units. Then

$$\tau_{\mathfrak{P}_i}(c_5(\alpha_j)) \equiv \begin{cases} -2 \pmod{\mathfrak{P}_i} & \text{if } 1 \le i = j \le 3, \\ 1 \pmod{\mathfrak{P}_i} & \text{if } 1 \le i \ne j \le 3. \end{cases} \tag{9.6}$$

Hence, if $\langle c_5(\alpha_i)\rangle = \langle c_5(\alpha_j)\rangle$, then

$$c_5(\alpha_1) = c_5(\alpha_2)^t \quad \text{for some } 1 \le t \le 4.$$

From (9.6) we have $-2 \equiv 1 \pmod{\mathfrak{P}_i}$. But $\mathfrak{P}_i$ is over 11, so we get $-2 \equiv 1 \pmod{11}$. This is impossible. Hence we must have $\langle c_5(\alpha_i)\rangle \ne \langle c_5(\alpha_j)\rangle$ for $1 \le i \ne j \le 3$. The claim is proved.

Question. *How many cyclotomic subgroups are there in $G_5(\widetilde{F})$?*

Furthermore, from Corollary 9.8(i), we have

$$c_5(\alpha_1)c_5(\alpha_2)c_5(\alpha_3) = \{-2, 11\} = \{-2, \Phi_5(-2)\}.$$

By Lemma 9.7, we have the injection $(K_2(\mathbb{Q}))_5 \hookrightarrow (K_2(\widetilde{F}))_5$. As in $K_2(\mathbb{Q})$ the tame symbol of $\{-2, 11\}$ is

$$\tau_{11}(\{-2, 11\}) \equiv -2 \not\equiv 1 \pmod{11},$$

we get

$$c_5(\alpha_1)c_5(\alpha_2)c_5(\alpha_3) = c_5(-2) \ne 1.$$

Moreover, let $F_n = F(\sqrt[5^{n-1}]{\alpha})$. As $\Phi_{5^n}(x) = \Phi_5(x^{5^{n-1}})$, we get

$$c_{5^n}(\sqrt[5^{n-1}]{\alpha})^{5^{n-1}} = \{\sqrt[5^{n-1}]{\alpha}, \Phi_{5^n}(\sqrt[5^{n-1}]{\alpha})\}^{5^{n-1}} = \{\alpha, \Phi_5(\alpha)\} = c_5(\alpha).$$

So $G_{5^n}(F_n)$ also contains the cyclotomic subgroup $\langle c_{5^n}(\sqrt[5^{n-1}]{\alpha})^{5^{n-1}}\rangle = \langle c_5(\alpha)\rangle$. ∎

Example 9.10. When $p = 5$, let α be a zero of $x^5 + x^4 + 2$, $F = \mathbb{Q}(\alpha)$ and $\widetilde{F}$ the normal closure of F.

As in Example 9.9, we conclude that $\langle c_5(\alpha)\rangle$ is a cyclotomic subgroup of order 5.

Let $\alpha := \alpha_1, \alpha_2, \ldots, \alpha_5$ be the five roots of $f(x) = x^5 + x^4 + 2$. From Lemma 9.4(iii), much as in Example 9.9, we have

$$\langle c_5(\alpha_1)\rangle \cup \cdots \cup \langle c_5(\alpha_5)\rangle \subseteq G_5(\widetilde{F}).$$

Claim. *The cyclotomic subgroups $\langle c_5(\alpha_1)\rangle, \ldots, \langle c_5(\alpha_5)\rangle$ are different from each other. Hence $G_5(\widetilde{F})$ contains at least five nontrivial cyclotomic subgroups.*

From the proof of Theorem 9.5(ii), we have

$$(1+3\alpha_i)\mathcal{O}_F = \mathfrak{p}_i \cdot \mathfrak{a}_i, \quad 1 \le i \le 5,$$

where $\mathfrak{p}_i$ is over 61 and $\mathfrak{a}_i$ is over 2.

Now it is easy to see that the discriminant of $f(x) = x^5 + x^4 + 2$ is

$$d(f) = N_{\widetilde{F}/\mathbb{Q}}(5\alpha_1^4 + 4\alpha_1^3) = 2^4 \cdot 3253.$$

The integer 3253 is a prime. Hence $61 \nmid d(f)$.

We claim that $\mathfrak{p}_i\mathcal{O}_{\widetilde{F}}$, $\mathfrak{p}_j\mathcal{O}_{\widetilde{F}}$ are relatively prime for $i \neq j$. In fact, otherwise there will exist a prime $\mathfrak{P}$ such that $\mathfrak{P} \mid (1+3\alpha_i), \mathfrak{P} \mid (1+3\alpha_j)$. So $\mathfrak{P} \mid (\alpha_i - \alpha_j)$ since $\mathfrak{P} \nmid 3$. Hence $\mathfrak{P} \mid d(f)$. Therefore $61 \mid d(f) = 2^4 \cdot 3253$, impossible.

Hence we conclude that for different i the primes in $\mathcal{O}_{\widetilde{F}}$ over $(1+3\alpha_i)$ but not over 2 are relatively prime.

Note that for any $\mathfrak{P}_i \mid (1+3\alpha_i)$ such that $\mathfrak{P}_i \nmid 2$, i.e., $\mathfrak{P}_i \mid \mathfrak{p}_i$, we have $\mathfrak{P}_i \nmid (1+\alpha_i)$. Thus from (9.2) we have

$$(9.7) \qquad \tau_{\mathfrak{P}_i}(c_5(\alpha_j)) \equiv \begin{cases} (-3)^{-v_{\mathfrak{P}_i}(1+3\alpha_j)} \pmod{\mathfrak{P}_i} & \text{if } 1 \le i = j \le 5, \\ 1 \pmod{\mathfrak{P}_i} & \text{if } 1 \le i \neq j \le 5. \end{cases}$$

Hence, if $\langle c_5(\alpha_i)\rangle = \langle c_5(\alpha_j)\rangle$ for some i, j, where $1 \le i \neq j \le 5$, then

$$c_5(\alpha_i) = c_5(\alpha_j)^t \quad \text{for some } 1 \le t \le 4.$$

Therefore from (9.7) we get $(-3)^{-v_{\mathfrak{P}_i}(1+3\alpha_i)} \equiv 1 \pmod{\mathfrak{P}_i}$, which implies

$$(-3)^{v_{\mathfrak{P}_i}(1+3\alpha_i)} \equiv 1 \pmod{61}.$$

It is easy to see that the order of $-3 \pmod{61}$ is 5, so $5 \mid v_{\mathfrak{P}_i}(1+3\alpha_j)$. On the other hand, $\widetilde{F}/F$ is a Galois extension with $[\widetilde{F} : F] = 24$, so 5 does not divide $e(\mathfrak{P}_i|\mathfrak{p}_i)$, the ramification number of $\mathfrak{P}_i$ over $\mathfrak{p}_i$. Hence for any $\mathfrak{P}_i \mid (1+3\alpha_i)$ with $\mathfrak{P}_i \nmid 2$, we have

$$5 \nmid v_{\mathfrak{P}_i}(1+3\alpha_i), \quad 1 \le i \le 5.$$

This is a contradiction.

Thus, $\langle c_5(\alpha_1)\rangle, \ldots, \langle c_5(\alpha_5)\rangle$ are different nontrivial cyclotomic subgroups of order five in $K_2(\widetilde{F})$.

A similar reasoning also works for Example 9.9.

Moreover, as in Example 9.9, from Corollary 9.8 we have

$$c_5(\alpha_1) \cdots c_5(\alpha_5) = \{-1/3, \Phi_5(-1/3)\}.$$

It is easy to see that $\{-1/3, \Phi_5(-1/3)\} = \{-1, 61\}\{3, 61\}^{-1} \neq 1 \in K_2(\widetilde{F})$.

We can also construct a quadratic field F such that $K_2(F)$ contains a cyclotomic subgroup of order 5. This was suggested to the first author by Browkin.

Example 9.11. The roots of the polynomial $x^2-3x+1=0$ are $(3\pm\sqrt{5})/2$. Let $\beta=(3+\sqrt{5})/2$, and $F=\mathbb{Q}(\beta)=\mathbb{Q}(\sqrt{5})$. Then

$$\Phi_5(-\beta)=(1-\beta^2)^2.$$

In view of $\{\beta,(1-\beta^2)^2\}=\{\beta^2,1-\beta^2\}=1$, we get

$$c_5(\beta)=\{\beta,(1-\beta^2)^2\Phi_5(\beta)\}=\{\beta,\Phi_5(-\beta)\Phi_5(\beta)\}=\{\beta,\Phi_5(\beta^2)\}.$$

So

$$c_5(\beta)^2=\{\beta^2,\Phi_5(\beta^2)\}=c_5(\beta^2)\in G_5(F).$$

As in Example 9.9, we find that $\langle c_5(\beta)\rangle$ is a nontrivial cyclotomic subgroup. But we need to prove that $c_5(\beta)\neq 1$.

In fact, note that $\beta^2+1=3\beta$. Thus

$$\Phi_5(\beta)=(1+\beta^2)^2-\beta^2+\beta(1+\beta^2)=9\beta^2-\beta^2+3\beta^2=11\beta^2.$$

Consequently, $c_5(\beta)=\{\beta,11\beta^2\}=\{\beta,11\}$.

In $\mathcal{O}_F=\mathbb{Z}[(1+\sqrt{5})/2]$, we have $11=(4+\sqrt{5})(4-\sqrt{5})$. Therefore $4+\sqrt{5}$ generates a prime $\mathfrak{p}$. From $\beta^2-3\beta+1=0$, we get $\beta(3-\beta)=1$ and $(\beta-1)^2=\beta$, so $(3-\beta)(\beta-1)^2=1$. These imply that $\beta,\beta-1$ are both units. So $v_{\mathfrak{p}}(11)=1$ and $v_{\mathfrak{p}}(\beta)=0$, and therefore

$$\tau_{\mathfrak{p}}(c_5(\beta))=\tau_{\mathfrak{p}}(\{\beta,11\})\equiv\beta\not\equiv 1 \pmod{\mathfrak{p}}.$$

Now, let $\overline{\beta}=(3-\sqrt{5})/2$. Then similarly $c_5(\overline{\beta})=\{\overline{\beta},11\}$, and it is easy to see that $c_5(\beta)c_5(\overline{\beta})=1$. So we get $\langle c_5(\beta)\rangle=\langle c_5(\overline{\beta})\rangle$. ■

Question. *Are there any nontrivial cyclotomic subgroups of order five other than $\langle c_5(\beta)\rangle$ in $K_2(\mathbb{Q}(\sqrt{5}))$?*

We do not know how to construct other cyclotomic subgroups. In particular, we do not know how to construct a cyclotomic subgroup of order seven.

10. Nonclosedness.

In this section, for any number field F, we will construct a subgroup generated by an infinite number of cyclotomic elements to the power of some prime, which contains no nontrivial cyclotomic elements. This is more clear than what Browkin's conjecture implies.

We need the following celebrated result.

Theorem 10.1 (Faltings [3]). *Any smooth, projective curve over a number field F that has genus greater than 1 can have only finitely many F-rational points.* ■

In the following, we will use $g(C)$ and $g(F(C))$ to denote respectively the genus of a curve C and of its function field $F(C)$. We also need a genus formula for Kummer extensions of function fields.

Let K/k be an algebraic function field where k is the field of constants which contains a primitive mth root of unity (with $m > 1$ and m relatively prime to the characteristic of k). Suppose that $u \in K$ satisfies

$$u \neq w^d \quad \text{for all } w \in K \quad \text{and} \quad d \,|\, m, d > 1.$$

Let

$$K' = K(y) \quad \text{with} \quad y^m = u.$$

Such an extension K'/K is said to be a *Kummer extension* of K. We have the following genus formula.

LEMMA 10.2 ([17]). *Let K'/K be the Kummer extension of a function field K with $y^m = u$ as above. If k' denotes the constant field of K', then*

$$g(K') = 1 + \frac{m}{[k' : k]}\left(g(K) - 1 + \frac{1}{2}\sum_{P \in S_K}\left(1 - \frac{r_P}{m}\right)\deg P\right)$$

where $r_P := \gcd(m, v_P(u))$ and S_K is the set of places of K/k. ■

LEMMA 10.3. *Let F be a number field. Assume that $n \geq 3$ and p is a prime. If either $p \geq 5$, or $p = 2$ but $n \neq 3, 4, 5, 6, 8, 10, 12$, or $p = 3$ but $n \neq 3, 4, 6$, then there are only finitely many F-rational points on the curve $C : \Phi_n(x) = cy^p$, where $c \in F^*$.*

Proof. Let $\overline{C}$ be the projective closure of C over F, i.e.,

$$\overline{C} : \Phi_n(x, z) - cy^p z^{\varphi(n)-p} = 0.$$

Note that $\overline{C}$ is a singular curve with singular point $(0 : 1 : 0)$. So we need to consider the normalization of $\overline{C}$, i.e.,

$$\pi : \overline{C}' \to \overline{C}.$$

As we know [5], $\overline{C}'$ is a projective smooth curve over F. It is also well known that the genus of a projective smooth curve is equal to the genus of its function field [6]. So

$$g(\overline{C}') = g(F(\overline{C}')).$$

Since π is a birational morphism, we have $F(\overline{C}') \simeq F(\overline{C}) \simeq F(C)$, so $g(F(\overline{C}')) = g(F(C))$, therefore

$$g(\overline{C}') = g(F(C)).$$

Now, we calculate the genus $g(F(C))$.

First, since F is a perfect field, the genus is unchanged under the algebraic extension of F. So $g(F(C)) = g(\overline{F}(C))$, where $\overline{F}$ is the algebraic closure of F.

Clearly,

$$\overline{F}(C) = \overline{F}(x, y) = \overline{F}(x)(y) \quad \text{with} \quad y^p = \Phi_n(x).$$

It is easy to see that $\overline{F}(x)(y)/\overline{F}(x)$ is a Kummer extension. As is well known, $g(\overline{F}(x))=0$.

For the Kummer extension $\overline{F}(x)(y)/\overline{F}(x)$ with

$$y^p=u:=\Phi_n(x)=\prod_{1\le i\le n,\,(n,i)=1}(x-\zeta^i),$$

where ζ is the nth primitive root of unity, it is easy to show that for any $P\in S_{\overline{F}(x)}$, we have:

(i) if $P=(x-\zeta^i), 1\le i\le n$, $\gcd(n,i)=1$, then $v_P(u)=1$, so $r_P=\gcd(p,v_P(u))=1$;
(ii) if $P=(x-a)$, $a\neq\zeta^i$, $\gcd(n,i)=1$, then $v_P(u)=0$, so $r_P=p$;
(iii) if $P=\infty=(\frac{1}{x})$, then $v_\infty(u)=-\varphi(n)$, so $r_\infty=\gcd(p,\varphi(n))$.

We apply Lemma 10.2 to the extension $\overline{F}(x)(y)/\overline{F}(x)$. Note that $\overline{F}$ is an algebraically closed field, so the constant field of $\overline{F}(x)(y)$ is also $\overline{F}$ and so $\deg P=1$ for any place $P\in S_{\overline{F}(x)}$. Therefore

$$g(\overline{F}(C))=1+p\biggl[-1+\frac{1}{2}\varphi(n)\Bigl(1-\frac{1}{p}\Bigr)+\frac{1}{2}\Bigl(1-\frac{\gcd(p,\varphi(n))}{p}\Bigr)\biggr].$$

Thus, to prove $g(\overline{F}(C))\ge 2$, it suffices to prove

$$\varphi(n)(p-1)>p+\gcd(p,\varphi(n)). \tag{10.1}$$

Note that $\varphi(n)\ge 2$ since $n\ge 3$.

For $p\ge 5$, if $\varphi(n)\ge 3$, then $\varphi(n)(p-1)\ge 3(p-1)>2p\ge p+\gcd(p,\varphi(n))$; if $\varphi(n)=2$, then $\varphi(n)(p-1)=2(p-1)>p+1=p+\gcd(p,\varphi(n))$.

For $p=2$, the inequality (10.1) becomes

$$\varphi(n)>2+\gcd(2,\varphi(n)).$$

It is easy to see that this holds if and only if $\varphi(n)>4$. So $n\neq 3,4,5,6,8,10,12$.

For $p=3$, the inequality (10.1) becomes

$$2\varphi(n)>3+\gcd(3,\varphi(n)).$$

Obviously, this holds if and only if $\varphi(n)>3$. So $n\neq 3,4,6$.

Summarizing, we have $g(F(C))\ge 2$ under the given assumptions on n and p. So $g(\overline{C}')\ge 2$. Hence, $\overline{C}'$ is a projective smooth curve of genus ≥ 2. Therefore, from Theorem 10.1, there are only finitely many F-rational points on $\overline{C}'$; as π is an F-birational morphism, there are also finitely many F-rational points on $\overline{C}$ and therefore on C, as required. ∎

Theorem 10.4. *Assume that F is a number field and $n\neq 1,4,8,12$. If there is a prime p such that $p^2\mid n$, then there exist infinitely many nontrivial* *cyclotomic elements* $\alpha_1, \alpha_2, \ldots \in G_n(F)$ *such that*

$$\langle \alpha_1^p \rangle \subsetneq \langle \alpha_1^p, \alpha_2^p \rangle \subsetneq \cdots \quad \textit{and} \quad \langle \alpha_1^p, \alpha_2^p, \ldots, \rangle \cap G_n(F) = \{1\}.$$

Proof. Let S be a finite set of places of F containing all archimedean ones, and all places above p and above the primes ramified in F. Moreover, assume that S is sufficiently large, so that the ring $\mathcal{O}_{F,S}$ of S-integers is a unique factorization domain. Let P_S denote the set of all the rational primes which the finite primes in S lie above.

Let $\mathbb{J} = \{1, \ldots, n/p - 1\}$, and let N be a positive integer which is greater than p, the rational primes ramified in F and all the rational primes in P_S.

Note that the polynomials $\Phi_n(x)$ and $\Phi_n'(x)$ are coprime, so there exist $g(x), h(x) \in \mathbb{Z}[x]$ and an integer m_0 such that

$$g(x)\Phi_n(x) + h(x)\Phi_n'(x) = m_0. \tag{10.2}$$

Let $M_1 = m_0 \prod_{1<q\le N} q$ with q running over the rational primes. We can choose a sufficiently large integer k_1 and a rational prime p_1 such that $p_1 \mid \Phi_n(k_1M_1)$ (so $p_1 \nmid k_1M_1$).

Let

$$A_1 := \begin{cases} k_1M_1 & \text{if } v_{p_1}(\Phi_n(k_1M_1)) = 1, \\ k_1M_1 + p_1 & \text{if } v_{p_1}(\Phi_n(k_1M_1)) > 1. \end{cases}$$

Then it is easy to show that $v_{p_1}(\Phi_n(A_1)) = 1$, i.e., $p_1 \parallel \Phi_n(A_1)$. In fact, if $v_{p_1}(\Phi_n(k_1M_1)) > 1$, then from the Taylor formula,

$$\Phi_n(k_1M_1 + p_1) = \Phi_n(k_1M_1) + \Phi_n'(k_1M_1)p_1 + \tfrac{1}{2}\Phi_n''(k_1M_1)p_1^2 + \cdots .$$

We must have $p_1 \nmid \Phi_n'(k_1M_1)$. Indeed, if $p_1 \mid \Phi_n'(k_1M_1)$, then from (10.2), we have $p_1 \mid m_0$. But according to the choice of M_1, we have $m_0 \mid M_1$, so $p_1 \mid k_1M_1$, a contradiction. Therefore $v_{p_1}(\Phi_n(A_1)) = v_{p_1}(\Phi_n(k_1M_1 + p_1) = 1$, as claimed.

Let

$$M_2 = \prod_{q_1 \mid k_1M_1} q_1 \prod_{q_1' \mid k_1M_1+p_1} q_1' \prod_{q_2 \mid \Phi_n(k_1M_1)} q_2 \prod_{q_2' \mid \Phi_n(k_1M_1+p_1)} q_2',$$

where q_1, q_2 run over rational primes. Then we can choose a sufficiently large integer k_2 and a rational prime p_2 such that $p_2 \mid \Phi_n(k_2M_2)$, and similarly we get A_2 with $p_2 \parallel \Phi_n(A_2)$.

Repeating this procedure, we get the following sequences of elements of $K_2(F)$:

$$\{c_n(A_i)^{pj} \mid i = 1, 2, \ldots\}, \qquad j \in \mathbb{J}, \tag{10.3}$$

where

$$A_i = \begin{cases} k_iM_i & \text{if } v_{p_i}(\Phi_n(k_iM_i)) = 1, \\ k_iM_i + p_i & \text{if } v_{p_i}(\Phi_n(k_iM_i)) > 1, \end{cases}$$

in which p_i is a rational prime satisfying $p_i \mid \Phi_n(k_iM_i)$ (therefore $p_i \nmid k_iM_i$) and

$$M_i = \prod_{q_1 \mid k_iM_{i-1}} q_1 \prod_{q_1 \mid k_iM_{i-1}+p_{i-1}} q_1' \prod_{q_2 \mid \Phi_n(k_iM_{i-1})} q_2 \prod_{q_2 \mid \Phi_n(k_iM_{i-1}+p_{i-1})} q_2'.$$

Hence $p_i \parallel \Phi_n(A_i)$. Note that $p_i \notin P_S$ for any i.

Claim 1. *For each $j \in \mathbb{J}$, the elements of* (10.3) *are all nontrivial and different from each other.*

In fact, for each p_i, we can choose a prime $\mathfrak{p}_i \subset \mathcal{O}_{F,S}$ with $\mathfrak{p}_i \mid p_i$ since $p_i \notin P_S$. According to the above construction, p_i is unramified in F, so from $p_i \parallel \Phi_n(A_i)$ and $\mathfrak{p}_i \mid p_i$, we have $\mathfrak{p}_i \parallel \Phi_n(A_i)$, i.e., $v_{\mathfrak{p}_i}(\Phi_n(A_i)) = 1$. So

$$\tau_{\mathfrak{p}_i}(c_n(A_i)^{pj}) \equiv A_i^{pj} \pmod{\mathfrak{p}_i}.$$

It suffices to prove $A_i^{pj} \not\equiv 1 \pmod{\mathfrak{p}_i}$. In fact, assume $A_i^{pj} \equiv 1 \pmod{\mathfrak{p}_i}$. Let

$$j = p^m j_1, \quad \text{where} \quad 0 \le m \le v_p(n) - 2 \text{ and } (j_1, p) = 1.$$

Then

$$\gcd(n, pj) = p^{m+1} \cdot \gcd(n/p^{m+1}, j_1) = p^{m+1} \cdot \gcd(n/p^{v_p(n)}, j_1)$$

since $p \nmid j_1$.

So from $A_i^n \equiv 1 \pmod{\mathfrak{p}_i}$ and $A_i^{pj} \equiv 1 \pmod{\mathfrak{p}_i}$, we have

$$A_i^{p^{m+1} \cdot gcd(np^{-v_p(n)}, j_1)} \equiv 1 \pmod{\mathfrak{p}_i}.$$

Therefore $A_i^{n/p} \equiv 1 \pmod{\mathfrak{p}_i}$.

It is easy to prove that there exists $\Psi_{n,p}(x) \in \mathbb{Z}[x]$ such that

$$\Phi_n(x)\Psi_{n,p}(x) = \Phi_p(x^{n/p}).$$

Hence

$$0 \equiv \Phi_n(A_i)\Psi_{n,p}(A_i) = \Phi_p(A_i^{n/p}) \equiv p \pmod{\mathfrak{p}_i},$$

that is, $\mathfrak{p}_i \mid p$. This is impossible since $p_i \neq p$ (note that $p \in P_S$).

So we get

$$\tau_{\mathfrak{p}_i}(c_n(A_i)^{pj}) \equiv A_i^{pj} \not\equiv 1 \pmod{\mathfrak{p}_i},$$

which implies that $c_n(A_i)^{pj}$ is nontrivial.

Next, we have $p_{i+1} \nmid M_{i+1}$, so $\mathfrak{p}_{i+1} \nmid M_{i+1}$. Therefore, according to the construction, $\mathfrak{p}_{i+1} \nmid A_l$, $\mathfrak{p}_{i+1} \nmid \Phi_n(A_l)$, $l \le i$, hence

$$\tau_{\mathfrak{p}_{i+1}}(c_n(A_l)^{pj}) \equiv 1 \pmod{\mathfrak{p}_{i+1}}, \qquad \forall l \le i.$$

But from the above discussion, we know that

$$\tau_{\mathfrak{p}_{i+1}}(c_n(A_{i+1})^{pj}) \not\equiv 1 \pmod{\mathfrak{p}_{i+1}}.$$

Hence

$$c_n(A_l)^{pj} \neq c_n(A_{i+1})^{pj}, \qquad \forall l \le i.$$

The claim is proved.

Claim 2. *There exists i_1 such that $c_n(A_{i_1})^{pj} \notin G_n(F)$ for each $j \in \mathbb{J}$.*

First, if there are only finitely many i such that $c_n(A_i)^p \in G_n(F)$, choose a large integer N_1 such that when $i > N_1$, $c_n(A_i)^p \notin G_n(F)$; otherwise, choose an infinite subset $I_1 \subseteq \mathbb{N}$ such that for any $i \in I_1$, we have $c_n(A_i)^p \in G_n(F)$.

Next, if there are only finitely many $i \in I_1$ such that $c_n(A_i)^{2p} \in G_n(F)$, choose a large integer $N_2 > N_1$ (if N_1 exists) such that when $i \in I_1$ and $i > N_2$, we have $c_n(A_i)^{2p} \notin G_n(F)$; otherwise, choose an infinite subset $I_2 \subseteq I_1$ such that for any $i \in I_2$, we have $c_n(A_i)^{2p} \in G_n(F)$.

Repeating this procedure, we will finally get an infinite set $I \subseteq \mathbb{N}$ and a set of integers

$$J := \{j_1, \dots, j_s\} \quad \text{with} \quad 1 \le j_1 < \cdots < j_s \le n/p - 1,$$

which satisfy

$$\begin{aligned} c_n(A_i)^{pj} &\in G_n(F), \quad && i \in I,\, j \in J, \\ c_n(A_i)^{pj} &\notin G_n(F), \quad && i \in I,\, j \in \mathbb{J} - J. \end{aligned}$$

In the above construction, if $J = \emptyset$, i.e., if for each $j \in \mathbb{J}$, the first case holds, in other words, there are only finitely many i such that $c_n(A_i)^{pj} \in G_n(F)$, then the claim is proved. Otherwise, $J \neq \emptyset$. We will prove that this is impossible.

In fact, since $c_n(A_i)^{pj} \in G_n(F)$ for $i \in I$, $j \in J$, we can assume that

$$c_n(A_i)^{pj} = c_n(B_{ij}), \qquad \text{where } i \in I,\, j \in J,\, B_{ij} \in F^*.$$

By the Dirichlet–Hasse–Chevalley theorem (see [21]), the group of S-units in $\mathcal{O}_{F,S}$ is finitely generated: there are fundamental S-units $\varepsilon_1, \dots, \varepsilon_t$ such that every S-unit can be written in the form

$$\zeta^r \varepsilon_1^{k_1} \cdots \varepsilon_t^{k_t}, \qquad \text{where } r, k_1, \dots, k_t \in \mathbb{Z}.$$

Here ζ is a generator of the group of roots of unity in F and $0 \le r < \operatorname{ord} \zeta$.

By Lemma 10.3, the equation $\varPhi_n(x) = cy^p$ has only finitely many solutions with $x, y \in F$. Hence, there are only finitely many $x \in F$ such that $\varPhi_n(x)$ can be written in the form cy^p with c of the form

$$\zeta^r \varepsilon_1^{k_1} \cdots \varepsilon_t^{k_t}, \qquad 0 \le r < p,\, 0 \le k_j < p,\, 1 \le j < t. \tag{10.4}$$

Hence, we can find an integer $\widetilde{N} \in I$ such that when $i \in I$ and $i > \widetilde{N}$, $\varPhi_n(B_{ij})$ cannot be written in the form cy^p with c of the form (10.4). This implies that we must have

$$\varPhi_n(B_{ij}) = c_{ij} a_{ij} y_{ij}^p,$$

where c_{ij} has the form (10.4), and $a_{ij} \in F^* \backslash \mathcal{O}_{F,S}^* \cdot (F^*)^p$ and $y_{ij} \in F^*$.

Assume that

$$a_{ij} \mathcal{O}_{F,S} = \mathfrak{q}_{ij1}^{e_{ij1}} \cdots \mathfrak{q}_{ijs}^{e_{ijs}}.$$

Claim 3. *There exists k_0 with $1 \le k_0 \le s$ such that $p \nmid e_{ijk_0}$, that is, $p \nmid v_{\mathfrak{q}_{ijk_0}}(a_{ij})$.*

In fact, if $p \mid e_{ijk}$ for $1 \le k \le s$, letting $e_{ijk} = pe'_{ijk}, 1 \le k \le s$, we have

$$a_{ij}\mathcal{O}_{F,S} = (\mathfrak{q}_{ij1}^{e'_{ij1}} \cdots \mathfrak{q}_{ijs}^{e'_{ijs}})^p = (a'_{ij}\mathcal{O}_{F,S})^p \quad \text{for some } a'_{ij} \in F^*,$$

since, according to the choice of S, $\mathcal{O}_{F,S}$ is a PID, so a UFD. Therefore

$$a_{ij} = u_{ij}(a''_{ij})^p \quad \text{for some } u_{ij} \in \mathcal{O}^*_{F,S} \text{ and } a''_{ij} \in F^*,$$

that is, $a_{ij} \in \mathcal{O}^*_{F,S} \cdot (F^*)^p$, a contradiction. So Claim 3 is true.

For convenience, we denote $\mathfrak{q}_{ij} := \mathfrak{q}_{ijk_0}$.

From Claim 3, we conclude that if $i > \widetilde{N}$, then for each $j \in J$ there exists a prime $\mathfrak{q}_{ij}$ such that

$$p \nmid v_{\mathfrak{q}_{ij}}(\Phi_n(B_{ij})).$$

Since $p \in P_S$, we have $\mathfrak{q}_{ij} \nmid p$.

Now, we prove that this leads to a contradiction.

On the one hand, we have

$$c_n(B_{ij})^{n/p} = c_n(A_i)^{nj} = 1.$$

On the other hand, if $v_{\mathfrak{q}_{ij}}(B_{ij}) > 0$, then $v_{\mathfrak{q}_{ij}}(\Phi_n(B_{ij})) = 0$, a contradiction; if $v_{\mathfrak{q}_{ij}}(B_{ij}) < 0$, then from $v_{\mathfrak{q}_{ij}}(\Phi_n(B_{ij})) = v_{\mathfrak{q}_{ij}}(B_{ij}) \cdot \deg \Phi_n(x)$ and $p \mid \deg \Phi_n(x)$, we have

$$p \mid v_{\mathfrak{q}_{ij}}(\Phi_n(B_{ij})),$$

a contradiction again. Hence, $v_{\mathfrak{q}_{ij}}(B_{ij}) = 0$.

Note that $v_{\mathfrak{q}_{ij}}(\Phi_n(B_{ij})) > 0$, i.e., $\mathfrak{q}_{ij} \mid \Phi_n(B_{ij})$. Computing the tame symbol, we get

$$\tau_{\mathfrak{q}_{ij}}(c_n(B_{ij})^{n/p}) \equiv B_{ij}^{v_{\mathfrak{q}_{ij}}(\Phi_n(B_{ij}))n/p} \pmod{\mathfrak{q}_{ij}}.$$

Since $c_n(B_{ij})^{n/p} = 1$, we have

$$B_{ij}^{v_{\mathfrak{q}_{ij}}(\Phi_n(B_{ij}))n/p} \equiv 1 \pmod{\mathfrak{q}_{ij}}.$$

From $\mathfrak{q}_{ij} \mid \Phi_n(B_{ij}) \mid (B_{ij}^n - 1)$, we obtain $B_{ij}^n \equiv 1 \pmod{\mathfrak{q}_{ij}}$. Hence

$$B_{ij}^{n/p} \equiv 1 \pmod{\mathfrak{q}_{ij}},$$

since $\gcd(n, v_{\mathfrak{q}_{ij}}(\Phi_n(B_{ij}))n/p) = n/p$. Therefore

$$0 \equiv \Phi_n(B_{ij})\Psi_{n,p}(B_{ij}) = \Phi_p(B_{ij}^{n/p}) \equiv \Phi_p(1) \equiv p \pmod{\mathfrak{q}_{ij}},$$

i.e., $\mathfrak{q}_{ij} \mid p$, a contradiction. Thus, Claim 2 is proved.

Now, let $\alpha_1 = c_n(A_{i_1})$. Then Claim 2 implies

$$\langle \alpha_1^p \rangle \cap G_n(F) = \{1\},$$

as required.

Next, we construct α_2.

First, from Claim 1, we can choose a sufficiently large integer N_1 such that when $i > N_1 + i_1$, we have $c_n(A_i)^{pj} \notin \langle \alpha_1 \rangle$ for any $j \in \mathbb{J}$.

Let

$$M_i' := M_{N_1+i_1+i}, \qquad A_i' := A_{N_1+i_1+i}, \qquad p_i' := p_{N_1+i_1+i}.$$

The notation is as above.

As in (10.3), we construct sequences of elements:

$$\{c_n(A_{i_1})^{pj} \cdot c_n(A_i')^{pj'} \mid i = 1, 2, \ldots\}, \qquad j, j' \in \mathbb{J}, \tag{10.5}$$

with $p_i' \parallel \Phi_n(A_i')$.

As in Claim 1, we can prove that for each fixed pair $(j, j') \in \mathbb{J} \times \mathbb{J}$, the elements of (10.5) are all nontrivial and different from each other.

Assume that for each i, there exists a couple $(j, j') \in \mathbb{J} \times \mathbb{J}$ such that

$$c_n(A_{i_1})^{pj} \cdot c_n(A_i')^{pj'} \in G_n(F).$$

Similar to the above discussion, there exists an infinite subset $I' \subseteq \mathbb{N}$ and $J' \subseteq \mathbb{J} \times \mathbb{J}$ such that

$$c_n(A_{i_1})^{pj} \cdot c_n(A_i')^{pj'} \in G_n(F), \quad i \in I',\ (j, j') \in J',$$
$$c_n(A_{i_1})^{pj} \cdot c_n(A_i')^{pj'} \notin G_n(F), \quad i \in I',\ (j, j') \in \mathbb{J} \times \mathbb{J} - J'.$$

Now, assume that

$$c_n(A_{i_1})^{pj} \cdot c_n(A_i')^{pj'} = c_n(B_{ij}'), \qquad i \in I',\ (j, j') \in J',$$

with $B_{ij}' \in F^*$. As above, we can prove that $J' = \emptyset$.

Hence, there exists i_2 such that

$$c_n(A_{i_1})^{pj} \cdot c_n(A_{i_2})^{pj'} \notin G_n(F) \quad \text{for any } (j, j') \in \mathbb{J} \times \mathbb{J}.$$

Let $\alpha_2 = c_n(A_{i_2})$. Since $i_2 > N_1 + i_1$, we have $\alpha_2 \notin \langle \alpha_1 \rangle$. So we get

$$\langle \alpha_1^p \rangle \subsetneq \langle \alpha_1^p, \alpha_2^p \rangle, \qquad \langle \alpha_1^p, \alpha_2^p \rangle \cap G_n(F) = \{1\}.$$

Repeating the procedure, we can find $\alpha_1, \alpha_2, \ldots \in G_n(F)$ such that

$$\langle \alpha_1^p \rangle \subsetneq \langle \alpha_1^p, \alpha_2^p \rangle \subsetneq \ldots \quad \text{and} \quad \langle \alpha_1^p, \alpha_2^p, \ldots \rangle \cap G_n(F) = \{1\}.$$

The proof is complete. ∎

Acknowledgements. We are grateful to Professor Jerzy Browkin for his many helpful suggestions which made the proofs of the results in this paper more transparent.

This research is supported by National Natural Science Foundation of China (No. 10871106).

References

[1] J. Browkin, *Elements of small order in K_2F*, in: Algebraic K-Theory, Lecture Notes in Math. 966, Springer, Berlin, 1982, 1–6.

[2] B. Du and H. R. Qin, *An expression for primes and its application to $K_2\mathbb{Q}$*, J. Pure Appl. Algebra 216 (2012), 1637–1645.

[3] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[4] X. J. Guo, *The torsion elements in K_2 of some local fields*, Acta Arith. 127 (2007), 97–102.

[5] R. Hartshorne, *Algebraic Geometry*, Springer, New York, 1977.

[6] E. Kunz, *Introduction to Plane Algebraic Curves*, Birkhäuser Boston, Boston, MA, 2005.

[7] H. W. Lenstra, Jr., *K_2 of a global field consists of symbols*, in: Algebraic K-Theory (Evanston 1976), M. R. Stein (ed.), Lecture Notes in Math. 551, Springer, Berlin, 1976, 69–73.

[8] H. W. Lenstra, *A letter from Lenstra to Browkin*, 19 May 1981.

[9] A. S. Merkurjev and A. A. Suslin, *$\mathcal{K}$-cohomology of Severi–Brauer varieties and norm residue homomorphism*, Math. USSR-Izv. 21 (1983), 307–340.

[10] J. Milnor, *Introduction to Algebraic K-Theory*, Ann. of Math. Stud. 72, Princeton Univ. Press, Princeton, NJ, 1971.

[11] H. Osada, *The Galois groups of the polynomial $X^n + aX^l + b$*, J. Number Theory 25 (1987), 230–238.

[12] H. R. Qin, *Elements of finite order in $K_2(F)$*, Chin. Sci. Bull. 38 (1994), 2227–2229.

[13] H. R. Qin, *The subgroups of finite orders in $K_2\mathbb{Q}$,* in: Algebraic K-Theory and Its Applications, H. Bass et al. (eds.), World Sci., Singapore, 1999, 600–607.

[14] H. R. Qin, *Lectures on K-Theory*, in: Cohomology of Groups and Algebraic K-Theory, Adv. Lect. Math. 12, Int. Press, Somerville, MA, 2010, 387–411.

[15] M. Rosen, *Number Theory in Function Fields*, Springer, New-York, 2002.

[16] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. 4 (1956), 287–302.

[17] H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer, New York, 1993.

[18] A. A. Suslin, *Torsion in K_2 of fields*, K-Theory 1 (1987), 5–29.

[19] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. 36 (1976), 257–274.

[20] J. Urbanowicz, *On elements of given order in K_2F*, J. Pure Appl. Algebra 50 (1988), 295–307.

[21] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

[22] K. J. Xu, *On the elements of prime power order in K_2 of a number field*, Acta Arith. 127 (2007), 199–203.

[23] K. J. Xu, *On Browkin's conjecture about the elements of order five in $K_2(\mathbb{Q})$*, Sci. China Ser. A 50 (2007), 116–120.

[24] K. J. Xu and M. Liu, *On the torsion in K_2 of a field*, Sci. China Ser. A 51 (2008), 1187–1195.

[25] K. J. Xu and H. R. Qin, *Some elements of finite order in $K_2(\mathbb{Q})$*, Chin. Ann. Math. Ser. A 22 (2001), 563–570.

[26] K. J. Xu and H. R. Qin, *A conjecture on a class of elements of finite order in* $K_2(F_\wp)$, Sci. China Ser. A 44 (2001), 484–490.

[27] K. J. Xu and H. R. Qin, *Some diophantine equations over $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ with applications to K_2 of a field*, Comm. Algebra 30 (2002), 353–367.

[28] K. J. Xu and H. R. Qin, *A class of torsion elements in K_2 of a local field*, Sci. China Ser. A 46 (2003), 24–32.

[29] K. J. Xu, C. C. Sun and S. J. Chi, *On the cyclotomic elements in K_2 of a rational function field*, Acta Arith. 164 (2014), 209–219.

[30] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), 265–284.

Kejian Xu
School of Mathematics and Statistics
Qingdao University
Qingdao 266071, China
and
Institute of Applied Mathematics of Shandong
Qingdao University
Qingdao 266071, China
E-mail: kejianxu@amss.ac.cn

Chaochao Sun
Department of Mathematics
Linyi University
Linyi 276005, China
and
School of Mathematics
Jilin University
Changchun 130012, China
E-mail: sunuso@163.com