Primitive finite nilpotent linear groups over number fields

Tobias Rossmann

Fakultät für Mathematik, Universität Bielefeld, D-33501 Bielefeld, Germany

Building upon the author's previous work on primitivity testing of finite nilpotent linear groups over fields of characteristic zero, we describe precisely those finite nilpotent groups which arise as primitive linear groups over a given number field. Our description is based on arithmetic conditions involving invariants of the field.

The definitive version of this article has been published:
J. Algebra 451 (2016), 248–267.
DOI: 10.1016/j.jalgebra.2015.11.044

1 Introduction

Let V be a finite-dimensional vector space over a field K and let $G \leqslant \mathrm{GL}(V)$ be an irreducible linear group over K. If there exists a decomposition $V = U_1 \oplus \cdots \oplus U_r$ into a direct sum of proper subspaces permuted by G, then G is imprimitive; otherwise, G is **primitive**. Irreducibility and primitivity of linear groups play a similarly fundamental role in the theory of linear groups as transitivity and primitivity do for permutation groups; for basic results on primitivity, we refer to [21, §15].

Related work: primitive nilpotent linear groups over finite fields. Detinko and Flannery [5] investigated primitive nilpotent linear groups over finite fields. Their work culminated in a classification [4] of these groups in the sense that they constructed explicit representatives for the conjugacy classes of primitive nilpotent subgroups of $\mathrm{GL}_d(\mathbf{F}_q)$. Building on their classification, they devised an algorithm [6, Alg. 7] which simultaneously tests irreducibility and primitivity of nilpotent linear groups over finite fields.

2010 Mathematics Subject Classification. 20D15, 20H20.

Keywords. Nilpotent groups, linear groups, primitivity, cyclotomic fields.

This work was supported by the Research Frontiers Programme of Science Foundation Ireland, grant 08/RFP/MTH1331 and the DFG Priority Programme "Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory" (SPP 1489).

Previous work: primitivity testing. Inspired by [6], the author developed methods for irreducibility [17] and primitivity [18] testing of finite nilpotent linear groups over many fields of characteristic zero, including number fields. At the heart of primitivity testing in [6, 18] lies a distinguished class of nilpotent groups: as in [17, 18], by an **ANC group**, we mean a finite nilpotent group whose **a**belian **n**ormal subgroups are all **c**yclic. These groups are severely restricted in their structure, see Theorem 3.1. It follows from Clifford's theorem that every primitive finite nilpotent linear group is an ANC group.

Results I: primitivity of $G(K)$. Given our ability from [18] to test primitivity of linear ANC groups, it is natural to ask for a description of those ANC groups which arise as primitive linear groups over a given number field. Among other things, the present article provides such a description. First, for an ANC group G and a number field K, in §3, we construct an irreducible K-linear group $G(K)$ (Definition 3.8) with $G \cong G(K)$. Based on our previous work on primitivity testing, in §4, we then characterise primitivity of $G(K)$ in terms of field-theoretic conditions (Lemma 4.2, Proposition 4.4). As we will see in §5, we can express these conditions in terms of numerical invariants, $\varkappa_K$ and $\varkappa_K^{\pm}$, of K which we introduce in Definition 5.1. We will further see that these invariants can be determined using a finite computation (Remark 5.6). In §6, we then derive our first main result and the technical heart of the present article, Theorem 6.4, which provides a concise description of those non-abelian ANC groups G such that $G(K)$ is primitive.

Results II: uniqueness of $G(K)$ and further properties of linear ANC groups. Theorem 7.1 shows that an irreducible K-linear ANC group G is necessarily similar to $G(K)$. It follows that the necessary and sufficient conditions for primitivity of $G(K)$ from §3 in fact characterise all primitive finite nilpotent linear groups over K (up to similarity). Based on our detailed knowledge of the groups $G(K)$, we then derive an asymptotic bound for the number of similarity classes of primitive finite nilpotent linear groups of given degree over K (Proposition 7.4). Finally, we show that for every ANC group G, the group $G(K)$ is primitive for some number field K (Proposition 7.5).

Results III: primitive nilpotent linear groups over cyclotomic and quadratic fields. As a demonstration of the explicit nature of the results in §6, in §8, we list those ANC groups G such that $G(K)$ is primitive for two infinite families of number fields, namely cyclotomic (Theorem 8.1) and quadratic (Theorem 8.5) fields. We proceed by computing the invariants $\varkappa_K$ and $\varkappa_K^{\pm}$ for such fields and by invoking Theorem 6.4.

Related work: Sylow subgroups of general linear groups. For arbitrary fields K, the primitive Sylow p-subgroups of $\mathrm{GL}_d(K)$ have been classified in terms of arithmetic properties of K, see [12, 14, 22]. (The historically first account, [22], contained a mistake which was corrected in the other two articles mentioned.) We note that in the particular case of ANC p-groups, there is an unavoidable overlap between the techniques used in the present article and those in [12, 14], see Remark 6.6.

Most of the results in the present article are contained in [19, Ch. 12–14]. Remark 4.5 corrects a minor mistake in the author's article [18].

Notation

We write $A \subset B$ to indicate that A is a not necessarily proper subset of B. We write $\mathbf{N} = \{1, 2, \dots\}$ and $2\mathbf{N} - 1 = \{1, 3, 5, \dots\}$. We often write $(a, b) = \gcd(a, b)$ for the non-negative greatest common divisor of $a, b \in \mathbf{Z}$. For a prime p, we let $\nu_p(a) \in \mathbf{Z} \cup \{\infty\}$ be the usual p-adic valuation of $a \in \mathbf{Q}$. For coprime $a, m \in \mathbf{Z}$, we let $\mathrm{ord}(a \bmod m)$ denote the multiplicative order of $a + m\mathbf{Z}$ in $(\mathbf{Z}/m\mathbf{Z})^\times$.

2 Background

Linear groups. Apart from some of our terminology, the following is folklore; see [21, Ch. IV]. By the **degree** of a linear group $G \leqslant \mathrm{GL}(V)$ over K, we mean the K-dimension $|V : K|$ of V. Given $G \leqslant \mathrm{GL}(V)$, we let $K[G]$ denote the subalgebra of $\mathrm{End}(V)$ spanned by G. We say that G is **homogeneous** if $K[G]$ is simple. Since the centre of a simple algebra is a field, if G is homogeneous, then so is its centre $\mathrm{Z}(G)$. If G is irreducible, then it is homogeneous. An abelian group $A \leqslant \mathrm{GL}(V)$ is homogeneous if and only if $K[A]$ is a field. Two linear groups $G \leqslant \mathrm{GL}(V)$ and $H \leqslant \mathrm{GL}(W)$, both over K, are **similar** if there exists a K-isomorphism $\theta\colon V \to W$ with $\theta^{-1}G\theta = H$. Similar K-linear groups of a given degree, d say, correspond exactly to conjugacy classes of subgroups of $\mathrm{GL}_d(K)$.

Schur indices. For details on the following, see [3, §70], [9, §38], and [10, §10]. Let K be a field of characteristic zero and let $\bar{K}$ be an algebraic closure of K. Let G be a finite group and let $\mathrm{Irr}_K(G)$ denote the set of irreducible K-characters of G. For $\chi \in \mathrm{Irr}_{\bar{K}}(G)$, there exists a finite extension $L/K(\chi)$ such that χ is afforded by an LG-module. The **Schur index** $\mathrm{m}_K(\chi)$ of χ over K is the smallest possible degree $|L : K(\chi)|$.

Let $\psi \in \mathrm{Irr}_K(G)$. By [3, Thm 70.15], there exists $\chi \in \mathrm{Irr}_{\bar{K}}(G)$ such that $\psi = \mathrm{m}_K(\chi) \left(\sum_{\sigma \in \Gamma} \chi^\sigma\right)$, where $\Gamma = \mathrm{Gal}(K(\chi)/K)$ and the conjugates $\chi^\sigma \in \mathrm{Irr}_{\bar{K}}(G)$ are distinct. If the KG-module V affords ψ, then the above decomposition of ψ can be found by splitting the EG-module $V \otimes_K E$, where $E \supset K$ is a splitting field for G which is Galois over K. Conversely, let $\chi \in \mathrm{Irr}_{\bar{K}}(G)$. Choose $L \supset K(\chi)$ with $|L : K(\chi)| = \mathrm{m}_K(\chi)$ such that χ is afforded by an LG-module W. By [9, Ex. 1.6(e)], the character of W as a KG-module is $\mathrm{m}_K(\chi) \left(\sum_{\sigma \in \Gamma} \chi^\sigma\right)$, where again $\Gamma = \mathrm{Gal}(K(\chi)/K)$. The characters χ^σ are distinct by [10, Lem. 9.17(c)]. It follows from [10, Cor. 10.2(b)] that $\mathrm{m}_K(\chi) \left(\sum_{\sigma \in \Gamma} \chi^\sigma\right)$ is the character of an irreducible KG-module and we conclude from [15, 8.3.7] that W is irreducible as a KG-module.

Cyclotomic fields. Throughout this article, $\bar{\mathbf{Q}}$ denotes the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. Let $\zeta_n \in \bar{\mathbf{Q}}$ be a fixed but arbitrary primitive nth root of unity and let $\mathbf{E}_n = \mathbf{Q}(\zeta_n)$ denote the nth cyclotomic field. For $n = 2^j m$ where m is odd, let $\mathbf{E}_n^\pm = \mathbf{Q}(\zeta_{2^j} \pm \zeta_{2^j}^{-1})\mathbf{E}_m \subset \mathbf{E}_n$ if $j \geqslant 3$ and $\mathbf{E}_n^\pm = \mathbf{E}_m$ for $0 \leqslant j \leqslant 2$. It is easy to see that $\mathbf{E}_n^\pm = \mathbf{Q}(\zeta_{2^j}^k \pm \zeta_{2^j}^{-k}, \zeta_m^\ell)$ for any odd $k \in \mathbf{Z}$ and $\ell \in \mathbf{Z}$ with $(\ell, m) = 1$. We often let $\mathbf{E}_n^\circ$ denote one of the fields $\mathbf{E}_n$, $\mathbf{E}_n^+$, and $\mathbf{E}_n^-$. Note that if $n, m \in \mathbf{N}$ with $(n, m) = 1$ and $\circ \in \{+, -, \ \}$, then $\mathbf{E}_n^\circ \mathbf{E}_m^\circ = \mathbf{E}_{nm}^\circ$. We often use the identities $\mathbf{E}_n \cap \mathbf{E}_m = \mathbf{E}_{(n,m)}$ and $\mathbf{E}_n\mathbf{E}_m = \mathbf{E}_{\mathrm{lcm}(n,m)}$, see [20, §11].

3 The construction of $G(K)$

Let K be a field of characteristic zero with algebraic closure $\bar{K}$. In this section, given an ANC group G, we construct an irreducible linear group $G(K)$ (Definition 3.8) over K with $G(K) \cong G$.

Abstract ANC groups. Let G_p denote the Sylow p-subgroup of a finite nilpotent group G and let $G_{p'} = \prod_{\ell \neq p} G_\ell$ be its Hall p'-subgroup. Let D_{2^j}, SD_{2^j}, and Q_{2^j} denote the dihedral, semidihedral, and generalised quaternion group of order 2^j, respectively; see [15, §5.3].

Theorem 3.1 ([16, Lem. 3])**.** *A non-cyclic finite nilpotent group G is an ANC group if and only if $G_{2'}$ is cyclic and G_2 is isomorphic to Q_8 or to D_{2^j}, SD_{2^j}, or Q_{2^j} for $j \geqslant 4$.*

Note the absence of D_8 which contains a non-cyclic abelian maximal subgroup.

Irreducible $\bar{K}$-representations of ANC 2-groups. We henceforth identify $\bar{\mathbf{Q}} \subset \bar{K}$ which allows us to consider composite fields of the form $\mathbf{E}_{2^j}^\circ K$, where $\mathbf{E}_{2^j}^\circ$ is defined as in §2.

Definition 3.2 ([18, §7])**.** For a non-abelian ANC group G, let $\vartheta(G) = 1$ if G_2 is (semi)dihedral and $\vartheta(G) = -1$ if G_2 is generalised quaternion. Further let $\delta(G) = 1$ if G_2 is dihedral or generalised quaternion and $\delta(G) = -1$ if G_2 is semidihedral.

Proposition 3.3 (Cf. [13, Prop. 10.1.16])**.** *Let $G = \langle a, g\rangle$ be a non-abelian ANC 2-group (or $G \cong \mathrm{D}_8$), where $\langle a\rangle$ is cyclic of order 2^j and index 2 in G and $g^2 = 1$ if $\vartheta(G) = 1$ and $g^4 = 1$ if $\vartheta(G) = -1$. Up to equivalence, the faithful irreducible $\bar{K}$-representations of G, written over the splitting field $\mathbf{E}_{2^j}K$ of G, are precisely given by*

$$\varrho_k^{G,K} \colon G \to \mathrm{GL}_2(\mathbf{E}_{2^j}K), \;\; a \mapsto \begin{bmatrix} \zeta_{2^j}^k & 0 \\ 0 & \delta(G)\zeta_{2^j}^{-k} \end{bmatrix}, \;\; g \mapsto \begin{bmatrix} 0 & 1 \\ \vartheta(G) & 0 \end{bmatrix},$$

where $0 < k < 2^{j-1}$ and k is odd.

Let $\chi_k^{G,K}$ be the character of $\varrho_k^{G,K}$ with character field $K(\chi_k^{G,K}) = K(\zeta_{2^j}^k + \delta(G) \cdot \zeta_{2^j}^{-k})$ over K (see [13, Prop. 10.1.17]); note that $K(\chi_k^{G,K}) = \mathbf{E}_{2^j}^\pm K$ does not depend on k. We now consider the Schur indices (see §2) of these characters.

Lemma 3.4 ([13, Prop. 10.1.17(i)])**.** $\mathrm{m}_K(\chi_k^{G,K}) = 1$ *if G is (semi)dihedral.*

For generalised quaternion groups, we compute Schur indices using a variation of [13, Prop. 10.1.17(ii)–(iii)]. The case $G \cong \mathrm{Q}_8$ of the following is well-known, cf. [3, p. 470]; the first part can also be deduced from [10, Prb. 10.5].

Lemma 3.5. *Let $G \cong \mathrm{Q}_{2^{j+1}}$. If $x^2+y^2=-1$ is soluble in $K(\chi_k^{G,K})$, then $\mathrm{m}_K(\chi_k^{G,K})=1$; otherwise, $\mathrm{m}_K(\chi_k^{G,K})=2$.*

Proof. Since ζ_{2^j} is chosen arbitrarily among the primitive 2^jth roots of unity, we may assume that $k=1$. Write $\theta_i = \zeta_{2^i}+\zeta_{2^i}^{-1}$. The corresponding statements for the equation $x^2+\theta_j xy+y^2=-1$ over $K(\chi_k^{G,K}) = K(\theta_j)$ follow from [13, Prop. 10.1.17(ii)–(iii)]. It suffices to show that $a_i = \left[\begin{smallmatrix} 1 & \theta_i/2 \\ \theta_i/2 & 1\end{smallmatrix}\right]$ is congruent to the 2×2 identity matrix over $\mathbf{Q}(\theta_i)$ for $i \geqslant 2$. We may assume that $\zeta_{2^{i+1}}^2 = \zeta_{2^i}$ for $i \geqslant 0$ so that $\theta_i^2 = 2+\theta_{i-1}$ for $i \geqslant 1$. Hence, $(2+\theta_i)(2-\theta_i) = 4-\theta_i^2 = 2-\theta_{i-1}$. Let $\lambda_3=\theta_3$ and $\lambda_i = \lambda_{i-1}/\theta_i \in \mathbf{Q}(\theta_i)$ $(i \geqslant 4)$. By induction, $\lambda_i^2 = 2-\theta_{i-1}$ for $i \geqslant 3$; indeed $\lambda_i^2 = \lambda_{i-1}^2/\theta_i^2 = (2-\theta_{i-2})/(2+\theta_{i-1}) = 2-\theta_{i-1}$ for $i\geqslant 4$. We obtain $x_i a_i x_i^T = 1$, where $x_2=1$ and $x_i = \left[\begin{smallmatrix} 1 & 0 \\ \theta_i/\lambda_i & -2/\lambda_i\end{smallmatrix}\right]$ $(i \geqslant 3)$. ♦

Irreducible K-representations of ANC 2-groups: constructing $\sigma_k^{G,K}$. Let $G=\langle a,g\rangle$ and k be as in Proposition 3.3. Let $\chi_k := \chi_k^{G,K}$, $\varrho_k := \varrho_k^{G,K}$, and $Z := K(\chi_k) = \mathbf{E}_{2^j}^{\pm}K$. In the following, we will construct an irreducible faithful K-representation $\sigma_k^{G,K}$ of G. Define $L = \mathbf{E}_{2^j}K$ and $\Delta = \mathrm{Gal}(L/Z)$.

Case 1: $\zeta_4 \in Z$.
Since $\mathbf{E}_{2^j}^{\pm}(\zeta_4) = \mathbf{E}_{2^j}$, we have $L=Z$ (so that $\mathrm{m}_K(\chi_k)=1$). We define $\sigma_k^{G,K}$ to be the irreducible K-representation obtained from ϱ_k by restriction of scalars (cf. §2).

Case 2: $\zeta_4 \notin Z$.
In this case, $L=Z(\zeta_4)$ is a quadratic extension of Z and

$$\psi\colon L \to \mathrm{M}_2(Z),\ \ \alpha+\zeta_4\cdot\beta \mapsto \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha\end{bmatrix} \qquad\qquad (\alpha,\beta\in Z)$$

is equivalent to the regular representation of L as a Z-algebra. Hence, $\mathrm{trace}_Z(u\psi) = \mathrm{trace}_{L/Z}(u)$ for $u \in L$. Our use of ψ in the following is similar to and inspired by arguments in [12]. Note that the space of matrices of the form $\left[\begin{smallmatrix} \alpha & \beta \\ \beta & -\alpha\end{smallmatrix}\right]$ $(\alpha,\beta\in Z)$ is the orthogonal complement of $L\psi$ with respect to the trace bilinear form $(s,t)\mapsto \mathrm{trace}_Z(st)$ on $\mathrm{M}_2(Z)$. We distinguish the following three subcases.

Case 2a: $\vartheta(G)=1$.
The Z-representation $\tau_k\colon G\to \mathrm{GL}_2(Z)$ given by $a\mapsto \zeta_{2^j}^k\psi$ and $g\mapsto \mathrm{diag}(1,-1)$ affords χ_k. We define $\sigma_k^{G,K}$ to be the (irreducible) restriction of scalars of τ_k to K.

Case 2b: $\vartheta(G)=-1$ and $\mathrm{m}_K(\chi_k)=1$.
By Lemma 3.5, $\mathrm{m}_K(\chi_k)=1$ is equivalent to the existence of $x,y\in Z$ with $x^2+y^2=-1$; we assume that (x,y) has been chosen independently of k. Let $t = \left[\begin{smallmatrix} x & y \\ y & -x\end{smallmatrix}\right]$ and let $\gamma\in\Delta$

be defined by $(\alpha + \zeta_4 \cdot \beta)^\gamma = \alpha - \zeta_4 \cdot \beta$ for $\alpha, \beta \in Z$. Then $(a^\gamma)\psi = t^{-1}(a\psi)t$ for all $a \in L$ and $t^2 = -1$. We conclude that $\upsilon_k \colon G \to \mathrm{GL}_2(Z)$ defined by $a \mapsto (\zeta_{2^j}^k)\psi$ and $g \mapsto t$ affords χ_k. We define $\sigma_k^{G,K}$ to be the (irreducible) restriction of scalars of υ_k to K.
Case 2c: $\vartheta(G) = -1$ and $\mathrm{m}_K(\chi_k) = 2$.
We define $\sigma_k^{G,K}$ to be the restriction of scalars of ϱ_k to K; since $\sigma_k^{G,K}$ affords the K-character $2\sum_{\sigma\in\Gamma}\chi_k^\sigma$ (where $\Gamma = \mathrm{Gal}(K(\chi_k)/K)$), it is irreducible.

Using Proposition 3.3 and the description of the irreducible K-representations of a finite group in terms of Galois orbits of its irreducible $\bar{K}$-representations in §2, we deduce the following.

Proposition 3.6. *Let G be a non-abelian* ANC *2-group. Then every faithful irreducible K-representation of G is equivalent to $\sigma_k^{G,K}$ for some odd k.* ♦

We record the following consequence of our construction of $\sigma_k^{G,K}$ for later use in §7.

Lemma 3.7. *Let G be a non-abelian* ANC *2-group of order 2^{j+1} and let $0 < k < 2^{j-1}$ be odd. Then $\mathrm{Im}(\sigma_1^{G,K}) = \mathrm{Im}(\sigma_k^{G,K})$.* ♦

Definition 3.8. Let G be an ANC group and let K be a field of characteristic zero.

(i) Let G be cyclic of order n. Define $G(K) := \langle\zeta_n\rangle \leqslant \mathrm{GL}_1(\mathbf{E}_n K)$, regarded as an irreducible K-linear group of degree $|\mathbf{E}_n K : K|$.

(ii) Let G be non-abelian. Write $m = |G_{2'}|$. Let W denote the $\mathbf{E}_m K$-space on which G_2 acts via $\sigma_1^{G_2,\mathbf{E}_m K}$. Define

$$G(K) := \left\langle \mathrm{Im}\left(\sigma_1^{G_2,\mathbf{E}_m K}\right), \zeta_m \cdot 1_W \right\rangle \leqslant \mathrm{GL}(W),$$

regarded as an irreducible K-linear group of degree $|W : K|$.

Note that $G \cong G(K)$.

4 A first characterisation of primitivity of $G(K)$

Let $K \subset \bar{\mathbf{Q}}$ be a subfield.

Lemma 4.1. *$\mathrm{C}_n(K)$ is primitive if and only if $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \neq p$ for each prime $p \mid n$.*

Proof. Let $G = \mathrm{C}_n(K)$. By [18, Cor. 4.5, Prop. 5.1], G is primitive if and only if $|K[G] : K[H]| \neq p$ for every maximal subgroup $H < G$ of prime index p. The claim follows since the towers $K[G]/K[H]/K$ and $\mathbf{E}_n K/\mathbf{E}_{n/p} K/K$ are isomorphic. ♦

It is well-known (see [18, Lem. 4.3]) that for a linear group to be primitive it is necessary that every subgroup of index 2 is irreducible. As a first step towards characterising primitivity of a non-abelian group $G(K)$, we now consider irreducibility of its cyclic maximal subgroups.

Lemma 4.2. *Let G be a non-abelian ANC group of order $2n$. Let $A \lhd G(K)$ be a cyclic subgroup of index 2. Let $\circ = +$ if G_2 is dihedral or generalised quaternion and let $\circ = -$ if G_2 is semidihedral.*

(i) A is homogeneous if and only if $\sqrt{-1} \notin \mathbf{E}_n^\circ K$.

(ii) Let A be homogeneous. Then A is irreducible if and only if $\vartheta(G) = 1$ or $x^2 + y^2 = -1$ is soluble in $\mathbf{E}_n^+ K$.

Proof. Write $n = 2^j m$ for odd m. It follows from the construction of $G(K)$ in §3 that $K[A] \cong_K K[a, b]$, where $a = \operatorname{diag}(\zeta_{2^j}, \delta(G)\zeta_{2^j}^{-1}) \in \mathrm{GL}_2(\mathbf{E}_n K)$ and $b = \operatorname{diag}(\zeta_m, \zeta_m) \in \mathrm{GL}_2(\mathbf{E}_n K)$; note that the K-isomorphism type of $K[a, b]$ does not depend on whether the faithful irreducible $\mathbf{E}_n K$-representation $\varrho_1^{G_2, \mathbf{E}_m K}$ of G_2 used in the construction of $\sigma_1^{G_2, \mathbf{E}_m K}$ is rewritten over $\mathbf{E}_n^\circ K$ (which amounts to conjugation by a suitable element of $\mathrm{GL}_2(\mathbf{E}_n K)$). In particular, $K[A] \cong_K (\mathbf{E}_n^\circ K)[a]$. The minimal polynomial of a over $\mathbf{E}_n^\circ K$ is $X^2 - (\zeta_{2^j} + \delta(G)\zeta_{2^j}^{-1})X + \delta(G)$. Thus, $K[A]$ is a field if and only if $\zeta_{2^j} \notin \mathbf{E}_n^\circ K$ or, equivalently, $\mathbf{E}_n K \neq \mathbf{E}_n^\circ K$. As $\mathbf{E}_n = \mathbf{E}_n^\circ(\sqrt{-1})$, this is equivalent to $\sqrt{-1} \notin \mathbf{E}_n^\circ K$ which proves (i). Let A be homogeneous. The degree of $G(K)$ is then $2^{\ell-1}|\mathbf{E}_n K : K|$, where ℓ is the Schur index of $\varrho_1^{G_2, \mathbf{E}_m K}$ over $\mathbf{E}_m K$. Thus, A is irreducible if and only if $\ell = 1$ which happens precisely under the given conditions by Lemmas 3.4–3.5. ♦

Remark 4.3. Note that A in Lemma 4.2 is uniquely determined unless $G_2 \cong \mathrm{Q}_8$ in which case irreducibility of A implies that of the other two cyclic subgroups of index 2 of G (see also [18, Lem. 8.1]).

By a **prime** of a number field K, we mean a non-zero prime ideal of its ring of integers. Let $\mathfrak{p}$ be a prime of K and let p be the underlying rational prime. Then we let $K_\mathfrak{p}$ denote the $\mathfrak{p}$-adic completion of K; it is a finite extension of the field $\mathbf{Q}_p$ of p-adic numbers. The following variation of a result from [18] characterises primitivity of $G(K)$.

Proposition 4.4. *Let G be a non-abelian ANC group of order $2n$, where $n = 2^j m$ and m is odd. Let $K \subset \bar{\mathbf{Q}}$ be a subfield. Suppose that a cyclic subgroup of index 2 of $G(K)$ is irreducible.*

(i) Let G_2 be dihedral or semidihedral or let $|G_2| > 16$. Then $G(K)$ is primitive if and only if $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \neq p$ for all primes $p \mid n$.

(ii) Let $G_2 \cong \mathrm{Q}_8$. Then $G(K)$ is primitive if and only if $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \neq p$ for all odd primes $p \mid n$ (that is, for all primes $p \mid m$).

(iii) Let $G_2 \cong \mathrm{Q}_{16}$ and let K be a number field. Then $G(K)$ is primitive if and only if the following two conditions are satisfied: (a) $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \neq p$ for all odd primes $p \mid n$. (b) If $\operatorname{ord}(2 \bmod m) \cdot |K_\mathfrak{p} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p} \mid 2$ of K, then $|\mathbf{E}_n K : \mathbf{E}_{n/2} K| \neq 2$.

Proof. If A denotes a cyclic subgroup of index 2 of G as in [18] and $p \mid n$, then $|K[A] : K[A^p]| = |\mathbf{E}_n K : \mathbf{E}_{n/p} K|$. All claims now follow from [18, §8.4] and [18, Cor. 7.4, Lem. 8.3–8.4] or, equivalently, by using [18, Alg. 9.1] to test primitivity of $G(K)$. ♦

Remark 4.5. It is claimed in [18, §8] that a maximal subgroup H of a non-abelian ANC group G is itself an ANC group. This is not correct: since D_8 is a maximal subgroup of D_{16} and SD_{16}, the group H might also be of the form $\mathrm{D}_8 \times \mathrm{C}_m$ for odd $m \in \mathbf{N}$. Subsequent arguments in [18, §8] then apply results from [18, §7] which are stated for non-abelian ANC groups only. Apart from the incorrect assertion that H is necessarily an ANC group, this reasoning is sound since all results in [18, §7] remain valid verbatim if, in addition to non-abelian ANC groups, we also allow groups of the form $G = \mathrm{D}_8 \times \mathrm{C}_m$ for odd $m \in \mathbf{N}$ and if we also define $\vartheta(G) = \delta(G) = 1$, extending Definition 3.2.

For fixed G and K, Lemma 4.2 and Proposition 4.4 together allow us to decide primitivity of $G(K)$. In the following, let K be fixed. Then, if we test conditions such as "$\sqrt{-1} \in \mathbf{E}_n^{\pm}K$" or "$|\mathbf{E}_nK : \mathbf{E}_{n/p}K| = p$" on a case-by-case basis, it remains unclear precisely for which ANC groups G, the linear group $G(K)$ is primitive. In particular, we cannot yet answer questions of the following type: is $(\mathrm{D}_{16} \times \mathrm{C}_m)(K)$ primitive for any odd $m \in \mathbf{N}$? A global picture of all the primitive groups $G(K)$ for fixed K which allows us to answer such questions will be provided by Theorem 6.4.

5 Relative cyclotomic extensions: the invariants $\varkappa_K$ and $\varkappa_K^{\pm}$

Throughout, let $K \subset \bar{\mathbf{Q}}$ be a subfield. Recall the notation for cyclotomic fields from §2.

Definition 5.1. Let $\circ \in \{+,-,\;\}$. Let $\mathfrak{D}_K^{\circ}(n) = \left\{d \in \mathbf{N} : K \cap \mathbf{E}_n \subset \mathbf{E}_d^{\circ}\right\}$ and define

$$\varkappa_K^{\circ} \colon \mathbf{N} \to \mathbf{N} \cup \{0\}, \quad n \mapsto \gcd(\mathfrak{D}_K^{\circ}(n)),$$

where we set $\gcd(\emptyset) = 0$.

Note that $n \in \mathfrak{D}_K(n)$ so that $\varkappa_K(n) \mid n$; in contrast, $\varkappa_K^{\pm}(n) = 0$ is possible. This section is devoted to the study of the numerical invariants $\varkappa_K^{\circ}$ of K. These invariants are related to primitivity of the groups $G(K)$ in Definition 3.8 via §4 and the following two lemmas, to be proved in §5.2 below.

Lemma 5.2. *Let $n \in \mathbf{N}$ and let $p \mid n$ be prime. Then $|\mathbf{E}_nK : \mathbf{E}_{n/p}K| = p$ if and only if $p^2 \mid n$ and $p \mid \frac{n}{\varkappa_K(n)}$.*

Note that for $K = \mathbf{Q}$, Lemma 5.2 simply asserts that $p = \frac{\varphi(n)}{\varphi(n/p)}$ if and only if $p^2 \mid n$.

Lemma 5.3. *Let $n \in \mathbf{N}$ with $4 \mid n$. Then:*

(i) $\sqrt{-1} \notin \mathbf{E}_n^{+}K$ if and only if $\varkappa_K^{+}(n) \neq 0$.

(ii) $\sqrt{-1} \notin \mathbf{E}_n^{-}K$ if and only if (a) $2\,\varkappa_K^{+}(n) \mid n$ or (b) $\varkappa_K^{-}(n) \mid n$ and $2\,\varkappa_K^{-}(n) \nmid n$.

If K is a number field, then $K \cap \mathbf{E}_n$ is contained in the maximal abelian subfield K_{ab} of K. By the Kronecker-Weber theorem [11, Thm 5.10], there exists $c \in \mathbf{N}$ with $K_{\mathrm{ab}} \subset \mathbf{E}_c$; the smallest possible value of c is precisely the (finite part of the) **conductor** of K_{ab}.

Proposition 5.4. *Let K be a number field and let $\circ \in \{+,-,\;\}$. Let $\mathfrak{f}$ be the conductor of K_{ab}. Then $\varkappa_K^{\circ}(n) = \varkappa_K^{\circ}(\gcd(n,\mathfrak{f}))$ for all $n \in \mathbf{N}$.*

Proof. $K \cap \mathbf{E}_n = K \cap \mathbf{E}_n \cap \mathbf{E}_{\mathfrak{f}} = K \cap \mathbf{E}_{(n,\mathfrak{f})}$. ♦

5.1 The sets $\mathfrak{D}_K^{\circ}(n)$

In preparation for proving Lemmas 5.2–5.3, we now study the sets $\mathfrak{D}_K^{\circ}(n)$ and their relationships with the $\varkappa_K^{\circ}(n)$. Let $\mathfrak{D}_K^{\circ}(n;i) = \{d \in \mathfrak{D}_K^{\circ}(n) : d \equiv i \bmod 2\}$. The following will be proved at the end of this subsection.

Proposition 5.5. *Let $K \subset \bar{\mathbf{Q}}$ be a subfield and let $n \in \mathbf{N}$.*

- *(i) Let $\circ \in \{+,-,\ \}$ and $\mathfrak{D}_K^{\circ}(n) \neq \emptyset$. Then $\mathfrak{D}_K^{\circ}(n) \subset \varkappa_K^{\circ}(n)\cdot\mathbf{N}$ and $\varkappa_K^{\circ}(n)$ is the least element of $\mathfrak{D}_K^{\circ}(n)$. If $\circ \neq -$, then $\mathfrak{D}_K^{\circ}(n) = \varkappa_K^{\circ}(n)\cdot\mathbf{N}$ and $\varkappa_K^{\circ}(n) \mid n$.*
- *(ii) If $d \in \mathfrak{D}_K^{-}(n)$, then $(d,n) \in \mathfrak{D}_K^{-}(n)$ or $2(d,n) \in \mathfrak{D}_K^{-}(n)$.*
- *(iii) $\mathfrak{D}_K(n;1) = \mathfrak{D}_K^{\pm}(n;1)$.*
- *(iv) Let $\mathfrak{D}_K^{+}(n) = \emptyset$ but $\mathfrak{D}_K^{-}(n) \neq \emptyset$. Then $8 \,|\, \varkappa_K^{-}(n)$ and $\mathfrak{D}_K^{-}(n) = \varkappa_K^{-}(n)\cdot(2\mathbf{N}-1)$. Furthermore, $\varkappa_K^{-}(n) = \gcd\big(d \in \mathfrak{D}_K^{-}(n) : d \mid n\big)$.*
- *(v) Let $\mathfrak{D}_K^{+}(n) \neq \emptyset$. Then $\mathfrak{D}_K^{-}(n;0) = 2\cdot\mathfrak{D}_K^{+}(n) \subset \mathfrak{D}_K^{+}(n;0)$. If $\varkappa_K^{+}(n)$ is even, then $\varkappa_K^{-}(n) = 2\,\varkappa_K^{+}(n)$; otherwise, $\mathfrak{D}_K^{-}(n) = \mathfrak{D}_K^{+}(n)$ and therefore $\varkappa_K^{-}(n) = \varkappa_K^{+}(n)$.*

Remark 5.6. Let K be a number field and $\circ \in \{+,-,\ \}$. Using Proposition 5.5(i)–(ii), in order to test if $\mathfrak{D}_K^{\circ}(n)$ is empty, it suffices to test if some divisor of $2n$ belongs to it. If $\mathfrak{D}_K^{\circ}(n) \neq \emptyset$, then the precise value of $\varkappa_K^{\circ}(n)$ can be computed using Proposition 5.5(i),(iv),(v). By Proposition 5.4, it suffices to compute $\varkappa_K^{\circ}(n)$ for the divisors of the conductor of K_{ab}. It follows that a finite computation suffices to determine $\varkappa_K^{\circ}$.

In order to derive Proposition 5.5, we consider intersections involving the fields $\mathbf{E}_n^{\pm}$ from §2. Let $j \geqslant 3$. The three involutions in $\mathrm{Gal}(\mathbf{E}_{2^j}/\mathbf{Q}) \cong (\mathbf{Z}/2^j)^{\times}$ are $\zeta_{2^j} \mapsto -\zeta_{2^j}$, $\zeta_{2^j} \mapsto \zeta_{2^j}^{-1}$, and $\zeta_{2^j} \mapsto -\zeta_{2^j}^{-1}$ with corresponding fixed fields $\mathbf{E}_{2^{j-1}}$, $\mathbf{E}_{2^j}^{+} = \mathbf{E}_{2^j} \cap \mathbf{R}$, and $\mathbf{E}_{2^j}^{-}$, respectively. By considering the subgroup lattice of $(\mathbf{Z}/2^j)^{\times}$, the subfields are seen to be arranged as in Figure 1. Using $\mathrm{Gal}(\mathbf{E}_{rs}/\mathbf{Q}) \cong \mathrm{Gal}(\mathbf{E}_r/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{E}_s/\mathbf{Q})$ for $(r,s)=1$, we can then read off the following.

Lemma 5.7. *Let $n, m \in \mathbf{N}$. Then:*

(i) $\mathbf{E}_n^{+} \cap \mathbf{E}_m^{+} = \mathbf{E}_n^{+} \cap \mathbf{E}_m = \mathbf{E}_{(n,m)}^{+}$.

(ii) $$\mathbf{E}_n^{+} \cap \mathbf{E}_m^{-} = \begin{cases} \mathbf{E}_{(n,m)/2}^{+}, & 0 < \nu_2(m) \leqslant \nu_2(n) \\ \mathbf{E}_{(n,m)}^{+}, & \textit{otherwise.} \end{cases}$$

(iii) $$\mathbf{E}_n^{-} \cap \mathbf{E}_m^{-} = \begin{cases} \mathbf{E}_{(n,m)/2}^{+}, & 0 \neq \nu_2(n) \neq \nu_2(m) \neq 0 \\ \mathbf{E}_{(n,m)}^{-}, & \textit{otherwise.} \end{cases}$$

(iv) $$\mathbf{E}_n \cap \mathbf{E}_m^{-} = \begin{cases} \mathbf{E}_{(n,m)}^{-}, & \nu_2(n) \geqslant \nu_2(m) \\ \mathbf{E}_{(n,m)}^{+}, & \textit{otherwise.} \end{cases}$$ ♦

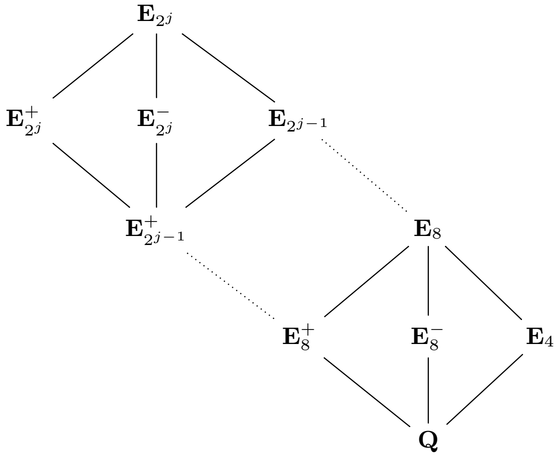

Figure 1: The subfield lattice of $\mathbf{E}_{2^j}$ for $j \geqslant 3$

Proof of Proposition 5.5. We freely use Lemma 5.7.

(i) Let $\circ \in \{+,-,\ \}$ and $d,e \in \mathfrak{D}_K^\circ(n)$. Then $K \cap \mathbf{E}_n \subset \mathbf{E}_d^\circ \cap \mathbf{E}_e^\circ \subset \mathbf{E}_{(d,e)}^\circ$ and therefore $(d,e) \in \mathfrak{D}_K^\circ(n)$. Since $\varkappa_K^\circ(n) = \gcd(F)$ for some finite $F \subset \mathfrak{D}_K^\circ(n)$, we conclude that $\varkappa_K^\circ(n) \in \mathfrak{D}_K^\circ(n)$ whence the first two claims follow immediately. Let $\circ \neq -$. Then $\mathbf{E}_d^\circ \subset \mathbf{E}_e^\circ$ for $d \mid e$ so that $\varkappa_K^\circ(n) \cdot \mathbf{N} \subset \mathfrak{D}_K^\circ(n)$. Finally, if $d \in \mathfrak{D}_K^\circ(n)$, then $K \cap \mathbf{E}_n \subset \mathbf{E}_d^\circ \cap \mathbf{E}_n = \mathbf{E}_{(d,n)}^\circ$ whence $(d,n) \in \mathfrak{D}_K^\circ(n)$ and the final claim follows.

(ii) $K \cap \mathbf{E}_n \subset \mathbf{E}_d^- \cap \mathbf{E}_n$ which is either equal to $\mathbf{E}_{(d,n)}^-$ or to $\mathbf{E}_{(d,n)}^+ \subset \mathbf{E}_{2(d,n)}^-$.

(iii) $\mathbf{E}_d\ = \mathbf{E}_d^\pm$ for odd $d \in \mathbf{N}$.

(iv) Let $d,e \in \mathfrak{D}_K^-(n)$. Then $K \cap \mathbf{E}_n \subset \mathbf{E}_d^- \cap \mathbf{E}_e^-$ and $\mathbf{E}_d^- \cap \mathbf{E}_e^- \neq \mathbf{E}_f^+$ for any $f \in \mathbf{N}$ whence $\nu_2(d) = \nu_2(e) \geqslant 3$. Thus, $(d,e) \in \mathfrak{D}_K^-(n)$ and we conclude that $\varkappa_K^-(n) \in \mathfrak{D}_K^-(n)$ (by (i)) is divisible by 8 and $\mathfrak{D}_K^-(n) = \varkappa_K^-(n) \cdot (2\mathbf{N}-1)$. Finally, if $d \in \mathfrak{D}_K^-(n)$, then $K \cap \mathbf{E}_n \subset \mathbf{E}_n \cap \mathbf{E}_d^- = \mathbf{E}_{(n,d)}^-$ since $\mathfrak{D}_K^+(n) = \emptyset$. Hence, $(d,n) \in \mathfrak{D}_K^-(n)$.

(v) Write $e = \varkappa_K^+(n)$ and let $d \in \mathfrak{D}_K^-(n;0)$. Then $K \cap \mathbf{E}_n \subset \mathbf{E}_d^- \cap \mathbf{E}_e^+ = \mathbf{E}_f^+$, where $f = (d,e)/2$ if $\nu_2(e) \geqslant \nu_2(d)$ and $f = (d,e)$ otherwise. By (i) and since d is even, $f = e \mid d$ and $\nu_2(d) > \nu_2(e)$. Therefore, $2e \mid d$ and hence $\mathfrak{D}_K^-(n;0) \subset 2\,\varkappa_K^+(n) \cdot \mathbf{N} = 2\,\mathfrak{D}_K^+(n)$ by (i). Conversely, let $d \in \mathbf{N}$ with $2e \mid d$. Then $K \cap \mathbf{E}_n \subset \mathbf{E}_e^+ \subset \mathbf{E}_{d/2}^+ \subset \mathbf{E}_d^-$ whence $2\,\mathfrak{D}_K^+(n) \subset \mathfrak{D}_K^-(n;0)$. The final claims now follow using (i) and (iii). ⧫

5.2 Proofs of Lemmas 5.2–5.3

Lemma 5.8. *Let $d,n \in \mathbf{N}$, $d \mid n$, and let $L \subset \mathbf{E}_d$ be a subfield. Then the restriction map* $\operatorname{Gal}(\mathbf{E}_n K/LK) \xrightarrow{\varrho} \operatorname{Gal}(\mathbf{E}_n/L)$ *is injective. It is surjective if and only if $K \cap \mathbf{E}_n \subset L$.*

Proof. Let $G = \operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, $U = \operatorname{Gal}(\bar{\mathbf{Q}}/K) \leqslant G$, $N = \operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{E}_n) \triangleleft G$, and $M = \operatorname{Gal}(\bar{\mathbf{Q}}/L) \triangleleft G$. By Galois theory, we obtain a commutative diagram

$$\begin{tikzcd}
(U \cap M)/(U \cap N) \arrow[r] \arrow[d, "\cong"] & M/N \arrow[d, "\cong"] \\
\operatorname{Gal}(\mathbf{E}_n K/LK) \arrow[r, "\varrho"] & \operatorname{Gal}(\mathbf{E}_n/L)
\end{tikzcd}$$

where all maps are the natural ones. The top map factors as

$$(U \cap M)/(U \cap N) \xrightarrow{\cong} (U \cap M)N/N \hookrightarrow M/N$$

whence ϱ is injective. By Dedekind's modular law [15, 1.3.14], we have $(U \cap M)N = UN \cap M$. Hence, ϱ is surjective if and only if $M \leqslant UN$ or, equivalently, $K \cap \mathbf{E}_n \subset L$. ♦

Corollary 5.9. *Let $d, n \in \mathbf{N}$ with $d \mid n$, let $\circ \in \{+, -,\ \}$, and let $\operatorname{Gal}(\mathbf{E}_n K/\mathbf{E}_d^\circ K) \xrightarrow{\varrho} \operatorname{Gal}(\mathbf{E}_n/\mathbf{E}_d^\circ)$ be the (necessarily injective) restriction map.*

(i) If $\circ \in \{+,\ \}$, then ϱ is surjective if and only if $\varkappa_K^\circ(n) \mid d$.

(ii) If $\circ = -$, then ϱ is surjective if and only if one of the following conditions is satisfied:

(a) $2\,\varkappa_K^+(n) \mid d$ if d is even or $\varkappa_K^+(n) \mid d$ if d is odd.

(b) $\varkappa_K^+(n) = 0$, $\varkappa_K^-(n) \mid d$, and $2\,\varkappa_K^-(n) \nmid d$.

Proof. Using Lemma 5.8 with $L = \mathbf{E}_d^\circ$, the map ϱ is surjective if and only if $d \in \mathfrak{D}_K^\circ(n)$. Part (i) thus follows from Proposition 5.5(i). For (ii), let $\circ = -$ and note that (a) and (b) are mutually exclusive. Let $\varkappa_K^+(n) \neq 0$. By Proposition 5.5(v), $\mathfrak{D}_K^-(n)$ consists of those multiples of $\varkappa_K^+(n)$ which are odd (if any) and arbitrary multiples of $2\,\varkappa_K^+(n)$. Hence, $d \in \mathfrak{D}_K^-(n)$ is equivalent to (a). If $\varkappa_K^+(n) = \varkappa_K^-(n) = 0$, then neither (a) nor (b) can be satisfied and ϱ is not surjective since $\mathfrak{D}_K^-(n) = \emptyset$. Finally, let $\varkappa_K^+(n) = 0 \neq \varkappa_K^-(n)$ so that Proposition 5.5(iv) applies. In particular, $8 \mid \varkappa_K^-(n)$ and $d \in \mathfrak{D}_K^-(n)$ if and only if $\varkappa_K^-(n) \mid d$ and $d/\varkappa_K^-(n)$ is odd. The latter condition can be replaced by $2\,\varkappa_K^-(n) \nmid d$. ♦

Proof of Lemma 5.2. If $p^2 \nmid n$, then $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \leqslant |\mathbf{E}_n : \mathbf{E}_{n/p}| = p - 1$ so let $p^2 \mid n$. As $\varkappa_K(n) \mid n$ by Proposition 5.5(i), the claim follows from Corollary 5.9(i) with $d = n/p$. ♦

Proof of Lemma 5.3. First, $\mathbf{E}_n = \mathbf{E}_n^\pm(\sqrt{-1}) \neq \mathbf{E}_n^\pm$ since $4 \mid n$. Thus, $\sqrt{-1} \notin \mathbf{E}_n^\pm K$ if and only if $|\mathbf{E}_n K : \mathbf{E}_n^\pm K| = 2$ or, equivalently, restriction $\operatorname{Gal}(\mathbf{E}_n K/\mathbf{E}_n^\pm K) \to \operatorname{Gal}(\mathbf{E}_n/\mathbf{E}_n^\pm)$ is surjective. By Proposition 5.5(i), if $\varkappa_K^+(n) \neq 0$, then $\varkappa_K^+(n) \mid n$. Now apply Corollary 5.9 with $d = n$. This proves (i) and also (ii) if we add the condition "$\varkappa_K^+(n) = 0$" to (b) in Lemma 5.3. To complete the proof, we show that in Lemma 5.3, if (b) is satisfied and $\varkappa_K^+(n) \neq 0$, then (a) is satisfied too. By Proposition 5.5(v), $\varkappa_K^-(n) = 2\,\varkappa_K^+(n)$ if $\varkappa_K^+(n)$ is even and $\varkappa_K^-(n) = \varkappa_K^+(n)$ otherwise. If $\varkappa_K^+(n)$ were odd, then, since $\varkappa_K^-(n) \mid n$, we would have $2\,\varkappa_K^-(n) \mid n$, contradicting (b). Thus, $\varkappa_K^+(n)$ is even and $\varkappa_K^-(n) = 2\,\varkappa_K^+(n) \mid n$ which establishes (a). ♦

6 Characterising primitivity of $G(K)$ using $\varkappa_K$ and $\varkappa_K^{\pm}$

In this section, given a number field K, we derive arithmetic conditions which characterise those ANC groups G such that $G(K)$ (Definition 3.8) is primitive. Our description depends on G and invariants of K, in particular the $\varkappa_K^{\circ}$ introduced and studied in §5.

Recall that a **supernatural number** is a formal product $a = \prod_p p^{n_p}$ indexed by primes with $n_p \in \mathbf{N} \cup \{0, \infty\}$, see e.g. [23, §2.1]; we write $\nu_p(a) = n_p$. Every natural number is a supernatural number and divisibility of natural numbers naturally extends to the supernatural case.

Definition 6.1. For a supernatural number a, let

$$\widehat{a} = a \cdot \prod\{p \text{ prime} : \nu_p(a) = 0\} = \operatorname{lcm}(a, 2, 3, 5, 7, 11, \dots).$$

We will use supernatural numbers to concisely encode notions of generalised "square-freeness". For instance, note that $d \in \mathbf{N}$ is square-free if and only if $d \mid \widehat{1}$.

Lemma 6.2. *Let $n \in \mathbf{N}$. Then $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \neq p$ for every prime p with $p \mid n$ if and only if $n \mid \widehat{\varkappa_K(n)}$.*

Proof. For $d \in \mathbf{N}$ with $d \mid n$, it is easy to see that $n \mid \widehat{d}$ if and only if $p \nmid \frac{n}{d}$ for every prime p with $p^2 \mid n$. Setting $d = \varkappa_K(n)$, the claim follows from Lemma 5.2. ♦

Corollary 6.3. *For a number field K, $\mathrm{C}_n(K)$ is primitive if and only if $n \mid \widehat{\varkappa_K(n)}$.*

Proof. Combine Lemmas 4.1 and 6.2. ♦

The following is one of the main results of the present article.

Theorem 6.4. *Let G be a non-abelian ANC group of order $2n$, where $n = 2^j m$ ($j \geqslant 2$) and m is odd. Let K be a number field. Let $\varkappa_K, \varkappa_K^{\pm} \colon \mathbf{N} \to \mathbf{N} \cup \{0\}$ be as in Definition 5.1. Define $\widehat{a}$ as in Definition 6.1.*

(i) If G_2 is dihedral, then $G(K)$ is primitive if and only if $\varkappa_K^{+}(n) \neq 0$ and $n \mid \widehat{\varkappa_K(n)}$.

(ii) Let G_2 be semidihedral. Then $G(K)$ is primitive if and only if $\varkappa_K^{-}(n) \mid n$ and $n \mid \widehat{\varkappa_K(n)}$.

(iii) Let G_2 be generalised quaternion with $|G_2| > 16$. Then $G(K)$ is primitive if and only if $\varkappa_K^{+}(n) \neq 0$, $n \mid \widehat{\varkappa_K(n)}$, and, in addition, K is totally imaginary or $m > 1$.

(iv) If $G_2 \cong \mathrm{Q}_8$, then $G(K)$ is primitive if and only if $\varkappa_K^{+}(n) \neq 0$, $m \mid \widehat{\varkappa_K(m)}$, $\operatorname{ord}(2 \bmod m) \cdot |K_{\mathfrak{p}} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p} \mid 2$ of K and, finally, K is totally imaginary or $m > 1$.

(v) Let $G_2 \cong \mathrm{Q}_{16}$. Then $G(K)$ is primitive if and only if the following conditions are satisfied:

- $\varkappa_K^+(n) \neq 0$.
- $m \mid \widehat{\varkappa_K(m)}$.
- *K is totally imaginary or $m > 1$.*
- *If $\operatorname{ord}(2 \bmod m) \cdot |K_{\mathfrak{p}} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p} \mid 2$ of K, then $n/\varkappa_K(n)$ is odd.*

Our proof of Theorem 6.4, given below, relies on the following.

Lemma 6.5. *Let $n \in \mathbf{N}$. Write $n = 2^j m$, where m is odd.*

(i) $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \neq p$ for all prime divisors $p \mid m$ if and only if $m \mid \widehat{\varkappa_K(m)}$.

(ii) Let $4 \mid n$. Then $|\mathbf{E}_n K : \mathbf{E}_{n/2} K| \neq 2$ if and only if $n/\varkappa_K(n)$ is odd.

(iii) ([17, §8.1].) *$x^2 + y^2 = -1$ is soluble in $\mathbf{E}_m K$ if and only if $\operatorname{ord}(2 \bmod m) \cdot |K_{\mathfrak{p}} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p} \mid 2$ of K and, in addition, K is totally imaginary or $m > 1$.*

(iv) If $8 \mid n$, then $x^2 + y^2 = -1$ is soluble in $\mathbf{E}_n^+ K$ if and only if K is totally imaginary or $m > 1$.

Proof.

(i) By Lemmas 5.2 and 6.2, it suffices to show that if p is a prime divisor of m, then $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| = p$ if and only if $|\mathbf{E}_m K : \mathbf{E}_{m/p} K| = p$. To that end, by Galois theory, $r = |\mathbf{E}_n K : \mathbf{E}_{n/p} K|$ divides $s = |\mathbf{E}_m K : \mathbf{E}_{m/p} K|$ which in turn divides $|\mathbf{E}_{p^a} : \mathbf{E}_{p^{a-1}}| \leqslant p$, where $a = \nu_p(m)$. Hence, if $r = p$, then $s = p$. Conversely, let $s = p$. Then $a \geqslant 2$ (otherwise, $s \leqslant p - 1$) and $r \in \{1, p\}$. Suppose, for the sake of contradiction, that $r = 1$. Then $\mathbf{E}_m K \subset \mathbf{E}_n K = \mathbf{E}_{n/p} K = (\mathbf{E}_{m/p} K)\mathbf{E}_{2^j}$, whence s divides $t = |(\mathbf{E}_{m/p} K)\mathbf{E}_{2^j} : \mathbf{E}_{m/p} K|$. However, t divides $|\mathbf{E}_{2^j} : \mathbf{Q}|$, which is a power of 2. This contradicts $s = p$ and proves that $r = p$.

(ii) Immediate from Lemma 5.2.

(iv) $\sqrt{2} \in \mathbf{E}_n^+ K$ so the local degrees in (iii) (with $\mathbf{E}_{2^j}^+ K$ in place of K) are even. Also, since $\mathbf{E}_{2^j}^+$ is totally real, $\mathbf{E}_n^+ K$ is totally imaginary if and only if $\mathbf{E}_m K$ is. ♦

Proof of Theorem 6.4. Lemma 4.2, Remark 4.3, and Lemma 5.3 together characterise irreducibility of the cyclic maximal subgroups of $G(K)$ in terms of $\varkappa_K^{\pm}(n)$. In order to derive the conditions stated in Theorem 6.4, combine Proposition 4.4, Lemma 6.2, and Lemma 6.5. For instance, in (i), the group $G(K)$ is primitive if and only if $\sqrt{-1} \notin \mathbf{E}_n^+ K$ (Lemma 4.2) and $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \neq p$ for all primes $p \mid n$ (Proposition 4.4(i)); these two conditions are equivalent to $\varkappa_K^+(n) \neq 0$ (Lemma 5.3) and $n \mid \widehat{\varkappa_K(n)}$ (Lemma 6.2), respectively. The other cases (ii)–(v) are obtained similarly. For (ii), we also need need the following two observations which allow us to replace the conditions in Lemma 5.3(ii) by "$\varkappa_K^-(n) \mid n$". First, if $n \mid \widehat{\varkappa_K(n)}$, then $2\,\varkappa_K^+(n) \nmid n$. Indeed, suppose that $2\,\varkappa_K^+(n) \mid n$. Then $2\,\varkappa_K(n) \mid n$ and thus $\nu_2(\varkappa_K(n)) \leqslant \nu_2(n/2)$. As $8 \mid n$, we obtain $\nu_2(\widehat{\varkappa_K(n)}) \leqslant$

$\nu_2(n/2) < \nu_2(n)$ and so $n \nmid \widehat{\varkappa_K(n)}$, a contradiction. Secondly, if $n \mid \widehat{\varkappa_K(n)}$ and $\varkappa_K^-(n) \mid n$, then $n/\varkappa_K^-(n)$ is necessarily odd. To that end, $8 \mid n$ implies that $\nu_2(n) \leqslant \nu_2(\widehat{\varkappa_K(n)}) = \nu_2(\varkappa_K(n)) \leqslant \nu_2(n)$ whence $n/\varkappa_K(n)$ is odd. As $\varkappa_K(n) \mid \varkappa_K^-(n) \mid n$, we conclude that $n/\varkappa_K^-(n)$ is odd. ♦

Remark 6.6. A description of the primitive p-subgroups of $\mathrm{GL}_d(K)$ can also be deduced from the maximal case in [12, 14]. The field invariants α, β, γ used in [14] are concerned with the inclusions of the fields $\mathbf{E}_{p^i}$ and $\mathbf{E}_{2^i}^{\pm}$ in the ground field. In our approach, these fields enter (in a different way) via the functions $\varkappa_K$ and $\varkappa_K^{\pm}$. The latter invariants were initially considered by the author in an attempt to describe the behaviour of α, β, and γ under cyclotomic extensions.

7 Irreducible and primitive linear ANC groups

In this section, we put our results from §§3–6 on the particular linear groups $G(K)$ into the context of general irreducible and primitive linear ANC groups.

7.1 Uniqueness of irreducible realisations of ANC groups

In this subsection, let K be an arbitrary field of characteristic zero.

Theorem 7.1. *Let $G \leqslant \mathrm{GL}(V)$ and $H \leqslant \mathrm{GL}(W)$ be irreducible linear ANC groups over K. Suppose that $G \cong H$ as abstract groups. Then G and H are similar. In particular, G and $G(K)$ are similar.*

Prior to giving a proof of Theorem 7.1, we record the following characteristic zero analogue of [5, Thm 5.11].

Corollary 7.2. *Abstractly isomorphic primitive finite nilpotent linear groups over a field of characteristic zero are similar.* ♦

The following is elementary.

Lemma 7.3. *Let $G = \langle g \rangle$ and H be homogeneous finite linear groups over K. If $G \cong H$, then there exists a generator $h \in H$ of H such that $K[G] \cong K[H]$ via $g \mapsto h$.*

Proof. Write $m = |G| = |H|$. The mth cyclotomic polynomial ϕ_m splits completely both over $K[G]$ and over $K[H]$. Let f be the minimal polynomial of g over K. Then $f \mid \phi_m$ whence $f(h) = 0$ for some $h \in K[H]$. As $K[H]$ is a field, the roots of $X^m - 1$ in $K[H]$ are precisely the elements of H. Since h is a primitive mth root of unity, we conclude that $H = \langle h \rangle$. The map $g \mapsto h$ now induces isomorphisms $G \to H$ and $K[G] \to K[H]$. ♦

Proof of Theorem 7.1. First, if G is cyclic, then the claim follows from Lemma 7.3. Next, suppose that G is a non-abelian ANC 2-group. Let $\theta\colon G \to H$ be an isomorphism. By Proposition 3.6, the natural representation of G is equivalent to $\sigma_k^{G,K}$ for some odd k. For the same reason, the composite $G \xrightarrow{\theta} H \hookrightarrow \mathrm{GL}(W)$ is equivalent to $\sigma_{k'}^{G,K}$ for some odd k'. Thus, it follows from Lemma 3.7 that G and H are both similar to $G(K) = \mathrm{Im}(\sigma_1^{G,K})$.

Finally, let G and H be non-abelian but not necessarily 2-groups. Using Lemma 7.3, we find $a \in G_{2'} \leqslant \mathrm{Z}(G)$ and $b \in H_{2'} \leqslant \mathrm{Z}(H)$ of order $m := |G_{2'}| = |H_{2'}|$ such that $a \mapsto b$ induces a K-isomorphism $K[a] \xrightarrow{\phi} K[b]$. We may then regard both G and H as Z-linear groups, where $Z := K[a]$ acts on W via ϕ. We see that G_2 and H_2 are isomorphic irreducible Z-linear ANC 2-groups. By using what we have proved above with Z in place of K, we see that there exists a Z-isomorphism $V \xrightarrow{t} W$ with $t^{-1}G_2t = H_2$. In particular, $|V : K[a]| = |W : K[b]|$. Since a and b have the same (irreducible) minimal polynomial over K, we obtain $s^{-1}as = b$ for some K-isomorphism $V \xrightarrow{s} W$. Now replace G by $s^{-1}Gs$. Repeating the above steps with $V = W$, $G_{2'} = H_{2'}$, $a = b$, and $\phi = 1$, we obtain $t^{-1}G_2t = H_2$. Since $t^{-1}at = b = a$ by Z-linearity of t, we conclude that $t^{-1}Gt = H$. ♦

7.2 The number of primitive ANC groups of a given degree

Proposition 7.4. *Let $K/\mathbf{Q}$ be a finitely generated field extension and let $\varepsilon > 0$. The number of conjugacy classes of primitive finite nilpotent subgroups of $\mathrm{GL}_d(K)$ is $\mathcal{O}(d^{1+\varepsilon})$.*

Proof. Let $\psi(n) = |\mathbf{E}_nK : K|$. As shown in the proof of [17, Lem. 5.4], there exists $C > 0$ such that $\psi(n) \leqslant n \leqslant C \cdot \psi(n)^{1+\varepsilon}$ for all $n \in \mathbf{N}$. The conjugacy classes of irreducible finite cyclic subgroups of $\mathrm{GL}_d(K)$ correspond precisely (via $n \mapsto \mathrm{C}_n(K)$) to the solutions $n \in \mathbf{N}$ of $\psi(n) = d$ and for such a solution, $n \leqslant Cd^{1+\varepsilon}$. Let $G \leqslant \mathrm{GL}_d(K)$ be a non-abelian irreducible ANC group of order $2n$. Given n, there are at most 3 different isomorphism classes of such groups and therefore at most that many conjugacy classes of irreducible realisations of these groups in $\mathrm{GL}_d(K)$. Given G and n, the construction of $G(K)$ in §3 and Theorem 7.1 show that either $d = \psi(n)$ or $d = 2\psi(n)$. By the above estimate, the number of solutions $n \in \mathbf{N}$ of either equation is $\mathcal{O}(d^{1+\varepsilon})$. ♦

It is natural to ask for the precise number of conjugacy classes of primitive finite nilpotent subgroups of $\mathrm{GL}_d(K)$. Even for $K = \mathbf{Q}$, this problem is related to challenging number-theoretic questions. Indeed, denoting Euler's totient function by φ, Theorem 8.1(i) below provides us with a bijection between square-free numbers $n \in \mathbf{N}$ with $\varphi(n) = d$ and conjugacy classes of primitive finite cyclic subgroups of $\mathrm{GL}_d(\mathbf{Q})$; for the problem of enumerating solutions n of $\varphi(n) = d$, see e.g. [2,8].

7.3 Primitive realisations of arbitrary abstract ANC groups

Corollary 6.3 and Theorem 6.4 characterise primitivity of $G(K)$ for fixed K and varying G in terms of the $\varkappa_K^\circ$. Regarding the case of a fixed G, we observe the following.

Proposition 7.5. *Let G be an ANC group. Then there exists an abelian number field K such that $G(K)$ is primitive.*

Proof. This is largely a consequence of Lemma 4.2 and Proposition 4.4 which we both use freely. First, $\mathrm{C}_n(\mathbf{E}_n)$ is trivially primitive. Let $n = 2^jm$ for $j \geqslant 2$ and odd $m \in \mathbf{N}$.

Then $\sqrt{-1} \notin \mathbf{E}_n^{\pm}$. If p is a prime divisor of n, then $\mathbf{E}_n = \mathbf{E}_{n/p}\mathbf{E}_n^{\pm}$, unless $p = j = 2$. It follows that $(\mathrm{D}_{2^{j+1}} \times \mathrm{C}_m)(\mathbf{E}_n^{+})$ and $(\mathrm{SD}_{2^{j+1}} \times \mathrm{C}_m)(\mathbf{E}_n^{-})$ are primitive for $j \geqslant 3$. By Lemma 6.5(iv), if $j \geqslant 2$, then $(\mathrm{Q}_{2^{j+1}} \times \mathrm{C}_m)(\mathbf{E}_{n\ell}^{+})$ is primitive for any odd $\ell > 1$ such that $\operatorname{ord}(2 \bmod \ell)$ is even; there are infinitely many such ℓ, cf. Remark 8.4 below. ♦

8 Applications

8.1 Cyclotomic fields

We apply the results from §6 to give a precise description of those ANC groups G such that $G(\mathbf{E}_r)$ is primitive. Since $\mathbf{E}_r = \mathbf{E}_{2r}$ for odd r, we may assume that $r \not\equiv 2 \bmod 4$.

Theorem 8.1. *Let $r \not\equiv 2 \bmod 4$. Recall that $\mathbf{E}_r$ denotes the rth cyclotomic field. Define $\widehat{a}$ as in Definition 6.1. A complete list (up to isomorphism) of those ANC groups G such that $G(\mathbf{E}_r)$ is primitive is given by the following.*

(i) C_n*, where* $n \mid \widehat{r}$.

(ii) $\mathrm{Q}_8 \times \mathrm{C}_m$*, where m and r are odd, $m \mid \widehat{r}$, $rm > 1$, and* $\operatorname{ord}(2 \bmod rm)$ *is even.*

(iii) $\mathrm{Q}_{16} \times \mathrm{C}_m$*, where m and r are odd, $m \mid \widehat{r}$, $rm > 1$, and* $\operatorname{ord}(2 \bmod rm)$ *is odd.*

The following will be used in the proof of Theorem 8.1.

Lemma 8.2 (Cf. [7, Thm 3])**.** *Let $m \in \mathbf{N}$ be odd. Then* $\operatorname{ord}(2 \bmod m)$ *is even if and only if* $\operatorname{ord}(2 \bmod p)$ *is even for some prime $p \mid m$.*

Corollary 8.3. *Let $m_1, m_2 \in \mathbf{N}$ both be odd. Then* $\operatorname{ord}(2 \bmod m_1m_2) \equiv \operatorname{ord}(2 \bmod m_1) \cdot \operatorname{ord}(2 \bmod m_2) \bmod 2$. ♦

Proof of Theorem 8.1. For $n \in \mathbf{N}$, we have $\varkappa_{\mathbf{E}_r}(n) = (r,n)$ if $(r,n) \equiv 0,1,3 \bmod 4$ and $\varkappa_{\mathbf{E}_r}(n) = (r,n)/2$ if $(r,n) \equiv 2 \bmod 4$; in particular, $\widehat{\varkappa_{\mathbf{E}_r}(n)} = \widehat{(r,n)}$. Also,

$$\varkappa^{\pm}_{\mathbf{E}_r}(n) = \begin{cases} (r,n), & (r,n) \equiv 1,3 \bmod 4, \\ (r,n)/2, & (r,n) \equiv 2 \bmod 4, \\ 0, & (r,n) \equiv 0 \bmod 4. \end{cases}$$

Given $a, b \in \mathbf{N}$, it is easy to see that $a \mid \widehat{(a,b)}$ if and only if $a \mid \widehat{b}$. The cyclic case (i) now follows from Corollary 6.3. Since $4 \mid n$ in Theorem 6.4, $\varkappa^{\pm}_{\mathbf{E}_r}(n) \neq 0$ (which is equivalent to $4 \nmid r$) and $n \mid \widehat{\varkappa_{\mathbf{E}_r}(n)}$ (which is equivalent to $n \mid \widehat{r}$) cannot both be satisfied. This rules out primitivity of the groups in Theorem 6.4(i)–(iii). Let $G_2 \cong \mathrm{Q}_8$. By Theorem 6.4(iv) in order for $G(\mathbf{E}_r)$ to be primitive it is necessary that r is odd (recall that $r \not\equiv 2 \bmod 4$), $m \mid \widehat{r}$, and $rm > 1$. The degree of the rth cyclotomic field over $\mathbf{Q}_2$ is $\operatorname{ord}(2 \bmod r)$, see e.g. [1, Prop. 3.5.18]. Together with Corollary 8.3, this yields the conditions in (ii). Finally, let $G_2 \cong \mathrm{Q}_{16}$. Again, by Theorem 6.4, for $G(K)$ to be primitive, it is necessary that r is odd, $rm > 1$, and $r \mid \widehat{m}$. In particular, $\varkappa_{\mathbf{E}_r}(n) = (n,r)$ whence $n/\varkappa_{\mathbf{E}_r}(n)$ is even and $\operatorname{ord}(2 \bmod rm)$ has to be odd, leading to the given conditions. ♦

Remark 8.4. It is shown in [7, Thm 5] that the set of odd primes p such that $\operatorname{ord}(2 \bmod p)$ is even has Dirichlet density 17/24. In view of Corollary 8.3, even if $\operatorname{ord}(2 \bmod r)$ is odd, the case (iii) in Theorem 8.1 is thus still rare.

8.2 Quadratic fields

Theorem 8.5. *Let $d \in \mathbf{Z}$ be square-free with $d \neq 1$. Let $\mathfrak{f}$ be the conductor of $\mathbf{Q}(\sqrt{d})$ or, equivalently, the absolute value of the discriminant of $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$. Define $\widehat{a}$ as in Definition 6.1. A complete list (up to isomorphism) of those ANC groups G such that $G(\mathbf{Q}(\sqrt{d}))$ is primitive is as follows.*

(i) C_n, *where $n \in \mathbf{N}$ is square-free or $\mathfrak{f} \mid n \mid \widehat{\mathfrak{f}}$.*

(ii) $\mathrm{D}_{16} \times \mathrm{C}_m$, *where $d \equiv 2 \bmod 8$ and $m \in \mathbf{N}$ is odd and square-free with $d \mid 2m$.*

(iii) $\mathrm{SD}_{16} \times \mathrm{C}_m$, *where $d \equiv 6 \bmod 8$ and $m \in \mathbf{N}$ is odd and square-free with $d \mid 2m$.*

(iv) $\mathrm{Q}_8 \times \mathrm{C}_m$ *for odd and square-free $m \in \mathbf{N}$ subject to the following conditions:*

- *If $d > 0$, then $m > 1$.*
- *If $d \equiv 1 \bmod 8$, then $\operatorname{ord}(2 \bmod m)$ is even.*
- *If $d \equiv 3 \bmod 4$, then $d \nmid m$.*

(v) $\mathrm{Q}_{16} \times \mathrm{C}_m$ *for odd and square-free $m \in \mathbf{N}$ such that $m > 1$ if $d > 0$ and one of the following (mutually exclusive) conditions is satisfied:*

- *$d \equiv 1 \bmod 8$ and $\operatorname{ord}(2 \bmod m)$ is odd.*
- *$d \equiv 2 \bmod 8$ and $d \mid 2m$.*

In preparation for our proof of Theorem 8.5, we first determine the invariants $\varkappa_K^{\circ}$ for these fields. By Proposition 5.4, it suffices to evaluate these functions at divisors of the conductor of the field in question.

Lemma 8.6. *Let $d \in \mathbf{Z}$ be square-free with $d \neq 1$. Let $\mathfrak{f} \in \mathbf{N}$ be the conductor of $\mathbf{Q}(\sqrt{d})$. Then:*

(i) If $n \in \mathbf{N}$ is a proper divisor of $\mathfrak{f}$, then $\varkappa_{\mathbf{Q}(\sqrt{d})}(n) = \varkappa^{\pm}_{\mathbf{Q}(\sqrt{d})}(n) = 1$.

(ii) $\varkappa_{\mathbf{Q}(\sqrt{d})}(\mathfrak{f}) = \mathfrak{f}$.

(iii) $\varkappa^{\pm}_{\mathbf{Q}(\sqrt{d})}(\mathfrak{f}) \in \{0, \mathfrak{f}, 2\mathfrak{f}\}$ *as indicated in the following table:*

$d \bmod 8$	$\mathfrak{f}$	$\varkappa^{+}_{\mathbf{Q}(\sqrt{d})}(\mathfrak{f})$	$\varkappa^{-}_{\mathbf{Q}(\sqrt{d})}(\mathfrak{f})$
$1, 5$	$\lvert d\rvert$	$\mathfrak{f}$	$\mathfrak{f}$
$3, 7$	$4\lvert d\rvert$	0	0
2	$4\lvert d\rvert$	$\mathfrak{f}$	$2\mathfrak{f}$
6	$4\lvert d\rvert$	0	$\mathfrak{f}$

Proof. Let $K = \mathbf{Q}(\sqrt{d})$. Let D be the discriminant of K. It is well-known [1, Prop. 3.4.1] that $D = d$ if $d \equiv 1 \bmod 4$ and $D = 4d$ otherwise. Moreover, $\mathfrak{f} = |D|$, see [11, Cor. VI.1.3]. Parts (i)–(ii) follow since $K \subset \mathbf{E}_n$ if and only if $\mathfrak{f} \mid n$; otherwise, $K \cap \mathbf{E}_n = \mathbf{Q}$.

Let $d \equiv 1 \bmod 4$. Then $\mathfrak{f} = |d|$ and $K \subset \mathbf{E}_{\mathfrak{f}} = \mathbf{E}_{\mathfrak{f}}^{\pm}$. For $r \in \mathbf{N}$, if $K \subset \mathbf{E}_r^{\pm}$, then $K \subset \mathbf{E}_r$ and thus $\mathfrak{f} \mid r$. We conclude that $\varkappa_K^{\pm}(\mathfrak{f}) = \mathfrak{f}$.

Let $d \equiv 3 \bmod 4$. Suppose that $K \subset \mathbf{E}_r^{\pm}$ for $r \in \mathbf{N}$. Then $K \subset \mathbf{E}_r^{\pm} \cap \mathbf{E}_{\mathfrak{f}} = \mathbf{E}_{(r,d)}$ which contradicts the fact that $\mathfrak{f} = 4|d|$ is minimal subject to $K \subset \mathbf{E}_{\mathfrak{f}}$. Hence, $\varkappa_K^{\pm}(\mathfrak{f}) = 0$.

Let $d = 2a$ for $a \equiv 1 \bmod 4$. As $\mathbf{E}_8^+ = \mathbf{Q}(\sqrt{2})$ and $\sqrt{a} \in \mathbf{E}_{|a|}$, we have $K \subset \mathbf{E}_{\mathfrak{f}}^+ \subset \mathbf{E}_{2\mathfrak{f}}^-$. If $r \in \mathbf{N}$ with $K \subset \mathbf{E}_r^+$, then $K \subset \mathbf{E}_r^+ \cap \mathbf{E}_{\mathfrak{f}}^+ \subset \mathbf{E}_{(r,\mathfrak{f})}$ whence $\mathfrak{f} \mid r$. Thus, $\varkappa_K^+(\mathfrak{f}) = \mathfrak{f}$. Next, if $K \subset \mathbf{E}_r^-$ for $r \in \mathbf{N}$, then $\nu_2(r) > \nu_2(\mathfrak{f})$ and $K \subset \mathbf{E}_{\mathfrak{f}}^+ \cap \mathbf{E}_r^- = \mathbf{E}_{(r,\mathfrak{f})}^-$ for otherwise $K \subset \mathbf{E}_{(r,\mathfrak{f})/2}^+$ (see Lemma 5.7), contradicting $\varkappa_K^+(\mathfrak{f}) = \mathfrak{f}$. Since $K \subset \mathbf{E}_{(r,\mathfrak{f})}^- \subset \mathbf{E}_{(r,\mathfrak{f})}$, we conclude that $\mathfrak{f} \mid r$ and thus even $2\mathfrak{f} \mid r$. It thus follows that $\varkappa_K^-(\mathfrak{f}) = 2\mathfrak{f}$.

Finally, let $d = 2a$ and $a \equiv 3 \bmod 4$. Then $\pm\sqrt{d} = \sqrt{-2}\sqrt{-a} \in \mathbf{E}_8^- \mathbf{E}_{|a|} = \mathbf{E}_{\mathfrak{f}}^-$. If $r \in \mathbf{N}$ with $K \subset \mathbf{E}_r^-$, then $\nu_2(r) = \nu_2(\mathfrak{f})$ and $K \subset \mathbf{E}_r^- \cap \mathbf{E}_{\mathfrak{f}}^- = \mathbf{E}_{(r,\mathfrak{f})}^-$ since all other cases in Lemma 5.7(iii) would contradict the minimality of $\mathfrak{f}$. Hence, $\mathfrak{f} \mid r$ and we conclude that $\varkappa_K^-(\mathfrak{f}) = \mathfrak{f}$. Suppose that $r \in \mathbf{N}$ with $K \subset \mathbf{E}_r^+$. Then $K \subset \mathbf{E}_r^+ \cap \mathbf{E}_{\mathfrak{f}}^- \subset \mathbf{E}_{\mathfrak{f}}^+$ and thus $K \subset \mathbf{E}_{\mathfrak{f}}^+ \cap \mathbf{E}_{\mathfrak{f}}^- = \mathbf{E}_{|a|}$ which contradicts the minimality of $\mathfrak{f}$. Therefore, $\varkappa_K^+(\mathfrak{f}) = 0$. ♦

The local degrees related to quaternion groups in Theorem 6.4 are easily determined.

Lemma 8.7 (Cf. [7, Thm 7]). *Let $d \in \mathbf{Z}$ be square-free with $d \neq 1$. Let $\mathfrak{p}$ be a prime of $K = \mathbf{Q}(\sqrt{d})$ lying above 2. Then $K_{\mathfrak{p}} = \mathbf{Q}_2$ if and only if $d \equiv 1 \bmod 8$.*

Proof. If $d \not\equiv 1 \bmod 4$, then K has even discriminant whence 2 ramifies. If, on the other hand, $d \equiv 1 \bmod 4$, then 2 splits if and only if $d \equiv 1 \bmod 8$, see e.g. [1, Prop. 3.4.3]. ♦

Proof of Theorem 8.5. For $n \in \mathbf{N}$, Lemma 8.6(i) implies that $n \mid \widehat{\varkappa_K(n)}$ if and only if n is square-free or $\mathfrak{f} \mid n \mid \widehat{\mathfrak{f}}$ whence (i) follows from Corollary 6.3. Let G be a non-abelian ANC group of order $2n$, where $n = 2^j m$ for odd m and $j \geqslant 2$. Write $d = 2^{\varepsilon} a$ for odd $a \in \mathbf{Z}$ and $\varepsilon \in \{0, 1\}$. Let $K = \mathbf{Q}(\sqrt{d})$. We freely use Theorem 6.4.

Since n is not square-free (indeed, $4 \mid n$), the condition $n \mid \widehat{\varkappa_K(n)}$ is equivalent to $\mathfrak{f} \mid n \mid \widehat{\mathfrak{f}}$. A necessary condition for that is $4 \mid \mathfrak{f}$ or, equivalently, $d \not\equiv 1 \bmod 4$. Next, if $\mathfrak{f} \mid n$, then $\varkappa_K^+(n) \neq 0$ is equivalent to $d \equiv 1, 2, 5 \bmod 8$. We conclude that both $n \mid \widehat{\varkappa_K(n)}$ and also $\varkappa_K^+(n) \neq 0$ if and only if $\mathfrak{f} \mid n \mid \widehat{\mathfrak{f}}$ and $d \equiv 2 \bmod 8$. In that case, $\mathfrak{f} = 8|a|$ whence $\nu_2(n) = 3$ is necessary. This proves (ii) and also shows that $G(K)$ is never primitive if G_2 is generalised quaternion with $|G_2| > 16$.

Suppose that G_2 is semidihedral. We can assume that $\mathfrak{f} \mid n \mid \widehat{\mathfrak{f}}$ and rule out the case $d \equiv 1 \bmod 4$ as above. If $d \equiv 2 \bmod 8$, then, analogously to the dihedral case, $G_2 \cong \mathrm{SD}_{16}$ is necessary for $G(K)$ to be primitive. However, in that case $\varkappa_K^-(n) = 2\mathfrak{f} = 8d$ cannot divide $n = 8m$. This leaves the case $d \equiv 6 \bmod 8$ and the conditions stated in (ii).

In order to deal with the remaining cases $G_2 \cong \mathrm{Q}_8$ and $G_2 \cong \mathrm{Q}_{16}$, first note that for odd $m \in \mathbf{N}$, the condition $m \mid \widehat{\varkappa_K(m)}$ is equivalent to m being square-free. Indeed, if

$d \equiv 1 \bmod 4$, then $\mathfrak{f} = |d|$ is itself square-free whence $\widehat{\varkappa_K(n)} = \widehat{1}$ for all $n \in \mathbf{N}$. If, on the other hand, $d \not\equiv 1 \bmod 4$, then $4 \mid \mathfrak{f}$ and $\varkappa_K(m) = 1$ for odd $m \in \mathbf{N}$.

Now let $G_2 \cong \mathrm{Q}_8$. Then $G(K)$ is primitive if and only if m is square-free, the conditions in the first two bullet points are satisfied (for the second one, use Lemma 8.7), and $\varkappa_K^+(4m) \neq 0$. By Lemma 8.6(iii), the latter condition is certainly satisfied whenever $d \equiv 1 \bmod 4$ or $d \equiv 2 \bmod 8$. If $d \equiv 3 \bmod 4$, then $\varkappa_K^+(n) = 0$ if and only if $d \mid m$ which gives the third bullet point. If $d \equiv 6 \bmod 8$, then $\varkappa_K^+(n) = 1$ since $\mathfrak{f} = 8|a| \nmid 4m = n$.

Finally, let $G_2 \cong \mathrm{Q}_{16}$. As in the preceding case, we may assume that m is square-free and that $m > 1$ if $d > 0$. By the second paragraph of this proof and Lemma 6.5(i)–(ii), if $\mathrm{ord}(2 \bmod m)$ or the local degrees $|K_{\mathfrak{p}} : \mathbf{Q}_2|$ in Theorem 6.4(v) are even, then $G(K)$ is primitive if and only if $\mathfrak{f} \mid n \mid \widehat{\mathfrak{f}}$ and $d \equiv 2 \bmod 8$; by Lemma 8.7, the aforementioned local degrees are necessarily even for $d \equiv 2 \bmod 8$. Since $n = 8m$, if $d \equiv 2 \bmod 8$, the second bullet point thus characterises primitivity of $G(K)$. Finally, it remains to consider the situation that $\mathrm{ord}(2 \bmod m)$ and the local degrees from above are all odd, in which case no further conditions need to be imposed. This case happens precisely when $d \equiv 1 \bmod 8$ and $\mathrm{ord}(2 \bmod m)$ is odd and thus leads to the first bullet point. ♦

References

[1] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, New York, 2007.

[2] S. Contini, E. Croot, and I. E. Shparlinski, *Complexity of inverting the Euler function*, Math. Comp. **75** (2006), no. 254, 983–996.

[3] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[4] A. S. Detinko and D. L. Flannery, *Classification of nilpotent primitive linear groups over finite fields*, Glasg. Math. J. **46** (2004), no. 3, 585–594.

[5] ———, *Nilpotent primitive linear groups over finite fields*, Comm. Algebra **33** (2005), no. 2, 497–505.

[6] ———, *Computing in nilpotent matrix groups*, LMS J. Comput. Math. **9** (2006), 104–134 (electronic).

[7] B. Fein, B. Gordon, and J. H. Smith, *On the representation of* -1 *as a sum of two squares in an algebraic number field*, J. Number Theory **3** (1971), 310–315.

[8] K. Ford, *The number of solutions of* $\phi(x) = m$, Ann. of Math. (2) **150** (1999), no. 1, 283–311.

[9] B. Huppert, *Character theory of finite groups*, de Gruyter Expositions in Mathematics, vol. 25, Walter de Gruyter & Co., Berlin, 1998.

[10] I. M. Isaacs, *Character theory of finite groups*, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. Pure and Applied Mathematics, No. 69.

[11] G. J. Janusz, *Algebraic number fields*, Second, Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[12] V. S. Konyukh, *On linear p-groups (Russian)*, Vestsī Akad. Navuk BSSR Ser. Fīz.-Mat. Navuk **1** (1987), 3–8, 124.

[13] C. R. Leedham-Green and S. McKay, *The structure of groups of prime power order*, London Mathematical Society Monographs. New Series, vol. 27, Oxford University Press, Oxford, 2002. Oxford Science Publications.

[14] C. R. Leedham-Green and W. Plesken, *Some remarks on Sylow subgroups of general linear groups*, Math. Z. **191** (1986), no. 4, 529–535.

[15] D. J. S. Robinson, *A course in the theory of groups*, Second, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996.

[16] P. Roquette, *Realisierung von Darstellungen endlicher nilpotenter Gruppen*, Arch. Math. (Basel) **9** (1958), 241–250.

[17] T. Rossmann, *Irreducibility testing of finite nilpotent linear groups*, J. Algebra **324** (2010), no. 5, 1114–1124.

[18] ______, *Primitivity testing of finite nilpotent linear groups*, LMS J. Comput. Math. **14** (2011), 87–98.

[19] ______, *Algorithms for nilpotent linear groups*,. PhD Thesis, National University of Ireland, Galway, 2011. See `http://hdl.handle.net/10379/2145`.

[20] G. Stroth, *Algebra. Einführung in die Galoistheorie.*, Walter de Gruyter & Co., Berlin, 1998.

[21] D. A. Suprunenko, *Matrix groups*, American Mathematical Society, Providence, R.I., 1976. Translations of Mathematical Monographs, Vol. 45.

[22] R. T. Vol′vačev, *Sylow p-subgroups of the full linear group*, AMS Translations (2) **64** (1967), 216–243.

[23] J. S. Wilson, *Profinite groups*, London Mathematical Society Monographs. New Series, vol. 19, The Clarendon Press Oxford University Press, New York, 1998.