THE GALOIS GROUP OF RANDOM ELEMENTS OF LINEAR GROUPS

ALEXANDER LUBOTZKY, LIOR ROSENZWEIG

Abstract. Let $\mathbb{F}$ be a finitely generated field of characteristic zero and $\Gamma \leq \mathrm{GL_n}(\mathbb{F})$ a finitely generated subgroup. For $\gamma \in \Gamma$, let $\mathrm{Gal}(\mathbb{F}(\gamma)/\mathbb{F})$ be the Galois group of the splitting field of the characteristic polynomial of γ over $\mathbb{F}$. We show that the structure of $\mathrm{Gal}(\mathbb{F}(\gamma)/\mathbb{F})$ has a typical behaviour depending on $\mathbb{F}$, and on the geometry of the Zariski closure of Γ (but not on Γ).

1. Introduction

Let F be a field of characteristic zero, and Γ a finitely generated subgroup of $GL_n(F)$. For an element $\gamma \in \mathrm{GL_n}(F)$, we denote by $\chi_\gamma(T)$ the characteristic polynomial of γ, $F(\gamma)$ is the splitting field of χ_γ over F, and $\mathrm{Gal}(F(\gamma)/F)$ the Galois group of $F(\gamma)$ above F.

The goal of the paper is to describe the structure of $\mathrm{Gal}(F(\gamma)/F)$ for the generic element of Γ. Our work was inspired by the work of Jouve, Kowalski, and Zywina [9], where a similar problem is treated when Γ is an arithmetic subgroup of a connected algebraic group G defined over a number field k. The main result of [9] (which in turn is related to [5, 6] and generalizes some special cases in [18, 11, 8, 10]) is that for a typical element γ of such a group Γ, $\mathrm{Gal}(k(\gamma)/k)$ is isomorphic to an explicitly described finite group $\Pi(G)$, depending only on G. If G splits over k, $\Pi(G)$ is the Weyl group $W(G)$ of (the reductive part of) G.

Our goal is to generalize this result to general F and Γ. As we will see, the situation can be quite different, especially in the cases where the Zariski closure $H = \overline{\Gamma}$ is not connected. In this case, there is *no typical* behaviour, but rather it decomposes into finitely many typical behaviours according to the connected components, but even this description does not give the full picture. To give the precise result, let us introduce some notations.

Let Σ be a finite admissible generating set (c.f. [13] or §4) of Γ. A random walk on Γ is a map $w : \mathbb{N} \to S$ where the k-step is $w_k = w(1)\cdots w(k)$ (so $w_0 = e$ is the identity element). For a subset $Z \subset \Gamma$ we write $\mathbb{P}(w_k \in Z)$ for the probability of w_k to be in Z.

Let H be the Zariski closure of Γ, and H^o its connected component, so H^o is a normal subgroup of finite index, say m, in H. We can now state our main theorem.

The authors are supported by ERC, ISF and NSF.

Theorem 1.1. *Let $\Gamma = \langle \Sigma \rangle \leq \mathrm{GL_n}(F)$, where F is a finitely generated field of characteristic zero, $\overline{\Gamma} = H$, and $m = (H : H^o)$ as above. Assume H^o has no central tori (e.g. H^o is semisimple). Then there exist $0 < c, \beta \in \mathbb{R}$, and a function $\Pi : H/H^o \to$Finite Groups, such that*

$$\mathbb{P}(\mathrm{Gal}(F(w_k)/F) \not\simeq \Pi(H^o w_k)) \leq ce^{-\beta k}$$

i.e. for any coset H_i of H^o in H, there exists a finite group $\Pi_i = \Pi(H_i)$ such that given w_k is in the coset H_i, the probability that its associated Galois group is isomorphic to Π_i is approaching 1 at an exponential rate in k.

The theorem is best possible. In §6 we will show that the result is not necessarily true if either F is not finitely generated or if H^o has a central torus. As we will show there, the theorem can fail in different ways, but also in the general case one can describe how $\mathrm{Gal}(F(w_k)/F)$ behaves, though the description is not that enlightening. As mentioned above, Theorem 1.1 generalizes the main theorem of [9] in several ways: general finitely generated field F, and general finitely generated group Γ. But the most interesting aspect is the fact that when $m > 1$, the typical behaviour is not uniform. This can happen even for arithmetic groups. Let us illustrate this by an example:

Example: Let $\Lambda = SL_n(\mathbb{Z})$ and $\Gamma = SL_n(\mathbb{Z}) \rtimes C_2$ where the cyclic group $C_2 = \langle \tau \rangle$ acting on Λ by: $\tau(A) = ({}^tA)^{-1}$. The group Γ can be embedded $\rho : \Gamma \to GL_{2n}(\mathbb{Z})$ by: For $A \in SL_n(\mathbb{Z})$

$$\rho(A) = \begin{pmatrix} A & 0 \\ 0 & ({}^tA)^{-1} \end{pmatrix}$$

and

$$\rho(\tau) = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$$

Now for $\gamma \in \Gamma \leq GL_{2n}(\mathbb{Z})$ we will see the following behaviour:

(i) If γ is in the index two subgroup Λ, then typically $\mathrm{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q}) \simeq S_n$ the symmetric group of n elements (This follows from [11], and in fact from [18])

(ii) If $\gamma \in \Gamma \setminus \Lambda$ then typically $\mathrm{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z}) wr_\Omega W_r$, where $r = \lfloor \frac{n}{2} \rfloor$, $\Omega = \{a_1, b_1, \ldots, a_r, b_r\}$, and $W_r = (\mathbb{Z}/2\mathbb{Z}) wr S_r$, the group of signed permutations of r pairs of elements, acting on Ω in the natural way.

The fact that we get in (ii) an extension of a finite abelian group by the Weyl group of a smaller semisimple group is not accidental. In fact, what comes into the game is the "Weyl group of the coset" $SL_n \cdot \tau$ (see [14]) which is an extension of an abelian group by the Weyl group of the group of fixed points of τ in SL_n.

Let us say a few words about the proof: By some field theoretic argument, one can reduce the problem to the case when $F = k$ a number field. Then Γ is a subgroup of an arithmetic group (or more precisely of an $S-$ arithmetic group). If H is semisimple, we will apply the recent developed sieve method for linear groups (as in [9], but we will follow [13] and in particular we will use [19] which gives property τ for fairly general subgroups of arithmetic groups). As said, the main novelty of the current paper is the treatment of the non-connected case. Here we show that the "Weyl group of a coset" (as in [14]) indeed replaces the "Weyl group of the connected component".

There is another aspect of our work which seems worth to be mentioned here: In [9], the Galois group of an element γ of an arithmetic group Γ is studied over the field of definition for Γ. We study the same problem over general fields $\mathbb{F}$. For an individual element $\gamma \in \Gamma$, the Galois group $\mathrm{Gal}(\mathbb{F}(\gamma)/\mathbb{F})$ depends very much on the field $\mathbb{F}$, e.g. it is the trivial group if $\mathbb{F}$ happens to contain the eigenvalues of γ. The proof of Theorem 1.1 shows, however that for a generic $\gamma \in \Gamma$, $\mathbb{F}(\gamma)$ contains a fixed finite extension $\mathbb{F}'$ of $\mathbb{F}$. Then $\mathrm{Gal}(\mathbb{F}(\gamma)/\mathbb{F}') = \mathrm{Gal}(\mathbb{F}'(\gamma)/\mathbb{F}')$ depends only on $H = \overline{\Gamma}$ and neither on $\mathbb{F}$ or Γ, as long as $\mathbb{F}$ is finitely generated .The next result shows that the finite generation of $\mathbb{F}$ is crucial for generic behaviour:

Theorem 6.1. *Let $H := SL_n$, $n \geq 5$, $\Gamma := H(\mathbb{Z})$. Let Σ be a finite generating set of Γ, and let X_k be the corresponding random walk. Then for any pair of subgroups $\underline{\mathcal{G}} = (G_1, G_2)$ of the alternating group $Alt(n)$ there exists an algebraic extension $\mathbb{F}_{\mathcal{G}}$ of $\mathbb{Q}$, and sequences $\{n_i(\mathcal{G})\}, \{k_i(\mathcal{G})\}$, such that*

$$\mathbb{P}(\mathrm{Gal}(\mathbb{F}_{\mathcal{G}}(X_{n_i(\mathcal{G})})/\mathbb{F}_{\mathcal{G}}) = G_1) \geq 1 - \frac{1}{2^i}$$
$$\mathbb{P}(\mathrm{Gal}(\mathbb{F}_{\mathcal{G}}(X_{k_i(\mathcal{G})})/\mathbb{F}_{\mathcal{G}}) = G_2) \geq 1 - \frac{1}{2^i}$$

The paper is organized as follows: We will start in Section 2, by defining the groups $\Pi_1, \ldots, \Pi_m$ associated with the various cosets $H_1, \ldots, H_m$. We further show that when $\gamma \in H_i$, there is a map from $\mathrm{Gal}(F(\gamma)/F)$ to $\Pi_i = \Pi(H_i)$. In Section 3 we assume $\mathbb{F}$ is a finite field, and prove some properties of Cartan subgroups and Weyl group, that lay the background for §4, where we assume that $F = k$ is a number field and H^o is semisimple and prove Theorem 1.1 in this case using the sieve method (leaving the reduction of the general case to §5). In Section 5, we will prove the reduction from general groups and general fields to number fields. In Section 6, we will give various examples illustrating the various possibilities of $\Pi(H_i)$. In the last two subsections we will explain how Theorem 1.1 can fail if either F is not finitely generated or if H^o has a central tori. We also include two appendices developing further over [14, 16] some results we need on "Weyl groups of cosets" and on k-quasi-irreducibility.

1.1. **Notations.** Throughout the paper we will use the following notations. For a set X ,we denote by $|X|$ the cardinality of the set. We write $A = O(B)$ or $A \ll B$ if there exists an absolute constant $C \geq 0$ such that $A \leq CB$. For a group G, we denote by $G^\sharp$ the set of conjugacy classes, and for an element $g \in G$, $[g] \in G^\sharp$ is the conjugacy class containing it. For an element $g \in G$ and a subgroup $H < G$, denote $Z_H(g)$, the centralizer of g inside H, that is the subgroup of elements in H commuting with g. We use $\mathbb{F}$ for an ambient field, $\overline{\mathbb{F}}$ its algebraic closure and k for a number field. For an algebraic group G, G^o denotes the connected component of G.

1.2. **Acknowledgments.** We would like to thank A. Rapinchuk, M. Larsen, M. Jarden and L. Bary-Soroker for their helpful comments and discussions. We also would like to thank E. Kowalski and F. Jouve for discussions about their work.

2. Splitting fields of elements in algebraic groups

Let $\mathbb{F}$ be a perfect field, $\Sigma \subset \mathrm{GL_n}(\mathbb{F})$ a finite set. Denote by $\Gamma := \langle \Sigma \rangle$, and $H := \overline{\Gamma}$ its Zariski closure. In the following section we will construct for any coset H_i of H^o in H a finite group $\Pi(H_i)$, such that for any element $h \in H_i \cap \Gamma$ the Galois group of the splitting field of its characteristic polynomial, denoted by $\mathrm{Gal}(\mathbb{F}(h)/\mathbb{F})$, is a quotient of a subgroup of $\Pi(H_i)$. To do so we recall some properties of diagonalizable groups over perfect fields.

2.1. **Diagonalizable groups.** A linear algebraic group D defined over a perfect field $\mathbb{F}$ is called *diagonalizable* if there exists a faithful rational representation $\rho : D \to GL_n$ such that $\rho(D(\overline{\mathbb{F}}))$ is contained in the group of diagonal matrices. For such a group D, denote by $X(D)$ the group of characters $\chi : D \to G_m$, where G_m is the one dimensional torus. The group $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ acts on D, and on $X(D)$ by $\chi^\sigma(d) = \sigma(\chi(\sigma^{-1}(d)))$, for $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}), \chi \in X(D), d \in D$. Let $\phi_D : \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \to Aut(X(D))$ be the homomorphism such that $\phi_D(\sigma)(\chi) = \chi^\sigma$, and denote by $\mathbb{F}_D$ the fixed field of $\ker(\phi_D)$. We call this field the *splitting field* of D. It is a finite Galois extension of $\mathbb{F}$. The group D is said to be *split* over $\mathbb{F}$ is its splitting field is $\mathbb{F}$. In fact the following conditions are equivalent

(i) The action of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ on $X(D)$ is trivial.
(ii) There exists a faithful $\mathbb{F}$-rational representation $\rho : D(\overline{\mathbb{F}}) \to \mathbb{D}_n(\overline{\mathbb{F}})$ where $\mathbb{D} < \mathrm{GL_n}$ is the group of diagonal matrices.

A connected diagonalizable group is called a *torus*. In fact every diagonalizable group D is of the form $D^o \times F$, where D^o is a torus, and F is a finite group.

2.2. **Cartan subgroups.** In the theory of connected algebraic groups, the notion of a maximal torus plays a central role. But, for non-connected groups this notion is not enough. We therefore recall the following definition of Cartan subgroup (cf. [14]). Let H be a linear algebraic group.

Definition 2.1. *A Zariski closed subgroup $C < H$ is called a* <u>*Cartan subgroup*</u> *if the following conditions hold*

(i) *C is diagonalizable*
(ii) *C/C^o is cyclic.*

(iii) *C has finite index in $N_H(C)$.*

The group $W(C) = N_{H^o}(C)/C^o$ is called the outer Weyl group of C.

Let H_i be a fixed coset of H^o, and denote by

$$\mathcal{C}_i := \{C < H : C \text{ is a Cartan subgroup s.t. } C/C^o \text{ is generated by } C^o g \text{ with } g \in H_i\} \tag{1}$$

We call the elements of $\mathcal{C}_i$ the *Cartan subgroups associated to H_i*. In [14] some properties of Cartan subgroup are proved. We list in the proposition below some of them that are needed in this paper

Proposition 2.2. *Let H be a linear algebraic group such that H^o is reductive, and let H_i be a coset of H^o in H.*

(i) *Every semisimple element $g \in H_i$ is contained in a Cartan subgroup associated to H_i. In fact if T is a maximal torus in $(Z_{H^o}(g))^o$, then the group $\langle T, g\rangle$ is a Cartan subgroup.*
(ii) *If $C \in \mathcal{C}_i$ is a Cartan subgroup associated to H_i, such that C/C^o is generated by $C^o g$, with $g \in H_i$, then C^o is a maximal torus of $(Z_{H^o}(g))^o$.*
(iii) *Any two Cartan subgroups $C_1, C_2 \in \mathcal{C}_i$, are conjugate by an element of H^o.*
(iv) *Let C be a Cartan subgroup and $h_1, h_2 \in H_i \cap C$. Then h_1 and h_2 are H^o conjugate if and only if they are $N_{H^o}(C)$ conjugate.*
(v) *If H^o is semisimple and simply connected, then $Z_{H^o}(C) = C^o$, and hence, the outer Weyl group $W(H_i, C) = N_{H^o}(C)/C^o$ acts faithfully on C. In general C^o is of finite index inside $Z_{H^o}(C)$.*

2.3. **$\mathbb{F}$-Cartan subgroups.** Since in this paper the base field plays an important role, the notion of $\mathbb{F}$-Cartan subgroup is in order. As above, let H be a linear algebraic group, defined over a field $\mathbb{F}$ (in general not algebraically closed), and let H_i be a coset of the connected component H^o. Denote by

$$\mathcal{C}_i(\mathbb{F}) = \{C < H : C \text{ is a Cartan subgroup defined over } \mathbb{F} \text{ such that } C/C^o \text{ is generated by } C^o g,\ g \in H_i(\mathbb{F})\}$$

We say that the coset H_i *splits over* $\mathbb{F}$ if there exists an $\mathbb{F}$-Cartan subgroup associated to H_i, (i.e. a member of $\mathcal{C}_i(\mathbb{F})$) that splits over $\mathbb{F}$ (note that this notion agrees with the case of connected groups, where a group is said to split over $\mathbb{F}$ if it contains an $\mathbb{F}$- split maximal torus). Recall that for a Cartan subgroup $C \in \mathcal{C}_i(\mathbb{F})$ the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ acts on $X(C)$. Denote by $\mathbb{F}_C$ the splitting field of C. Let $C \in \mathcal{C}_i(\mathbb{F})$ be a fixed $\mathbb{F}$-Cartan subgroup. The outer Weyl group $W(H_i, C)$ acts on C, and therefore also on $X(C)$, and can be mapped into $Aut(X(C))$. We denote its image by $\widetilde{W}(H_i, C)$, and denote this action by $w \cdot \chi = \chi(w(c))$ for $\chi \in X(C)$, and $c \in C$. Since C is defined over $\mathbb{F}$, then its normalizer and centralizer in H^o, $N_{H^o}(C), Z_{H^o}(C)$, are also defined over $\mathbb{F}$, and hence the Galois group

$\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ acts on the outer Weyl group $W(H_i, C)$, and on $\widetilde{W}(H_i, C)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$, $w \in \widetilde{W}(H_i, C)$ and $\chi \in X(C)$. Then

$$\sigma(w) \cdot \chi = \left(w \cdot \chi^{\sigma^{-1}}\right)^{\sigma}. \tag{2}$$

In particular, if C splits over $\mathbb{F}$, and so the action of the Galois group is trivial on $X(C)$, it is also trivial on $\widetilde{W}(H_i, C)$.

We can now define the group $\Pi(H_i)$ that will contain as a subquotient the Galois group of the splitting field of the characteristic polynomial of every element in H_i. Let $C \in \mathcal{C}_i(\mathbb{F})$ be an $\mathbb{F}$-Cartan subgroup of H associated to H_i. Denote by $\Pi(H_i, C, \mathbb{F})$ the subgroup of $Aut(X(C))$ generated by the image of $\widetilde{W}(H_i, C)$ and $\phi_C(\mathrm{Gal}(\mathbb{F}_C/\mathbb{F}))$. Let C_1 be another $\mathbb{F}$-Cartan subgroup of H associated to H_i. Then C_1 and C are H^o-conjugate, that is there exists an element $h \in H^o$ such that $C = h^{-1}C_1h$. Notice that since both Cartan subgroups are defined over $\mathbb{F}$, we have that for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ the element $h^{-1}\sigma(h)$ normalizes C, and therefore it defines an element of $W(H_i, C)$, and therefore an element of $\widetilde{W}(H_i, C^o)$. Denote this element by w_σ. Denote by $f : C_1 \to C$ the isomorphism sending $x \mapsto h^{-1}xh$, and by $F : X(C) \to X(C_1)$ the one sending $\chi \mapsto \chi \circ f$.

Proposition 2.3. *Under the above notations, we have:*

(i) *$\widetilde{W}(H_i, C)$ is a normal subgroup of $\Pi(H_i, C, \mathbb{F})$.*

(ii) *The isomorphism of $Aut(X(C)) \to Aut(X(C_1))$ sending $\gamma \mapsto F \circ \gamma \circ F^{-1}$ induces an isomorphism of $\Pi(H_i, C, \mathbb{F})$ onto $\Pi(H_i, C_1, \mathbb{F})$, and of $\widetilde{W}(H_i, C)$ onto $\widetilde{W}(H_i, C_1)$.*

(iii) *Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$. Denote by $w_\sigma \in \widetilde{W}(H_i, C)$ the element represented by $h^{-1}\sigma(h)$. Then*

$$F^{-1} \circ \phi_{C_1}(\sigma) \circ F = w_\sigma \circ \phi_C(\sigma)$$

(iv) *Let $K \subset \overline{\mathbb{F}}$ be an extension of $\mathbb{F}$ over which H_i splits. Then $\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/K)) \subset \widetilde{W}(H_i, C)$.*

Proof. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ and $w \in \widetilde{W}(H_i, C)$ we need to show that $\phi_C(\sigma) \circ w \circ \phi_C(\sigma^{-1})$ lies in $\widetilde{W}(H_i, C)$. Now,

$$\left(\phi_C(\sigma) \circ w \circ \phi_C(\sigma^{-1})\right)(\chi) = \left(w \cdot \chi^{\sigma^{-1}}\right)^{\sigma} = \sigma(w) \cdot \chi \tag{3}$$

We therefore get that $\phi_C(\sigma) \circ w \circ \phi_C(\sigma^{-1}) = \sigma(w) \in \widetilde{W}(H_i, C)$. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ we will show that $F^{-1} \circ \phi_{C_1}(\sigma) \circ F$ lies in $\Pi(H_i, C, \mathbb{F})$.

$$\left(F^{-1} \circ \phi_{C_1}(\sigma) \circ F\right)(\chi) = (\chi \circ f)^{\sigma} \circ f^{-1} = \chi^{\sigma} \circ (f^{\sigma} \circ f^{-1}) = \chi^{\sigma} \circ (f \circ (f^{\sigma})^{-1})^{-1} \tag{4}$$

where the isomorphism $f \circ (f^\sigma)^{-1}$ of C maps $x \mapsto h^{-1}\sigma(h)x(h^{-1}\sigma(h))^{-1}$, which equals the isomorphism of C given by w_σ. This proves that

$$F^{-1} \circ \phi_{C_1}(\sigma) \circ F = w_\sigma \circ \phi_C(\sigma) \tag{5}$$

and is therefore an element of $\Pi(H_i, C, \mathbb{F})$, and we also proved (3). To finalize the proof of part (2) we need to see the isomorphism of the Weyl groups: we note that if $w \in W(H_i, C_1)$ is represented by $n \in N_{H^o}(C)$ then $h^{-1}nh \in N_{H^o}(C_1)$. The isomorphism of $\widetilde{W}(H_i, C), \widetilde{W}(H_i, C_1)$ then follows immediately.

For the last part, if H_i splits over K, we may then take C as a split Cartan group. We therefore get by (5) that

$$\phi_{C_1}(\sigma) = F \circ w_\sigma \circ F^{-1}$$

which is an element of $\widetilde{W}(H_i, C_1)$ by part (ii) of the proposition. □

For a fixed field $\mathbb{F}$, the group $\Pi(H_i, C, \mathbb{F})$ is unique up to isomorphism, and the isomorphisms $\Pi(H_i, C, \mathbb{F}) \widetilde{\to} \Pi(H_i, C', \mathbb{F})$ are unique up to inner automorphisms of H^o. We can therefore denote it by $\Pi(H_i, \mathbb{F})$, and the set of conjugacy classes $\Pi(H_i, C, \mathbb{F})^\sharp$ are unambiguous and we will denote it by $\Pi(H_i, \mathbb{F})^\sharp$. Notice that by the last part of Proposition 2.3 we have that if H_i splits over $\mathbb{F}$, then $\Pi(H_i, C, \mathbb{F}) = \widetilde{W}(H_i, C)$. In the case that two or more fields of different types take place we denote the set of conjugacy classes by $\widetilde{W}(H_{i,\overline{\mathbb{F}}})^\sharp$.

For a coset H_i, define the *splitting field of H_i* to be $\mathbb{F}_i := \cap_{C \in \mathcal{C}_i(\mathbb{F})} \mathbb{F}_C$, and $\mathbb{F}_i^W = \phi_C^{-1}(\widetilde{W}(H_i, C))$ for an $\mathbb{F}$-Cartan subgroup C associated to H_i (notice that the definition of $\mathbb{F}_i^W$ is independent of C by Proposition 2.3(ii)). Although H_i does not necessarily split over $\mathbb{F}_i$, the following lemma shows that some connection with the splitting property still holds.

Lemma 2.4. *Let $\mathbb{F}$, H, and H_i be as above. Then*

(i) *For any $\mathbb{F}$-Cartan subgroup C associated to H_i, $\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_i)) \subseteq \widetilde{W}(H_i, C)$. i.e. $\mathbb{F}_i^W \subset \mathbb{F}_i$, and in particular $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_i) \leq \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_i^W)$*

(ii) *For any $\mathbb{F}$-Cartan subgroup C associated to H_i, the following holds:*
   (a) *$\mathrm{Gal}(\mathbb{F}_C/\mathbb{F}_i^W)$ is isomorphic to a subgroup of $\widetilde{W}(H_i, C)$.*
   (b) *There is an exact sequence:*

$$1 \to \widetilde{W}(H_i, C) \cap \phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})) \to \phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})) \to \mathrm{Gal}(\mathbb{F}_i^W/\mathbb{F}) \to 1. \tag{6}$$

Furthermore, the group $\Pi(H_i, C, \mathbb{F})$ satisfies the following exact sequence

$$1 \to \widetilde{W}(H_i, C) \to \Pi(H_i, C, \mathbb{F}) \to \mathrm{Gal}(\mathbb{F}_i^W/\mathbb{F}) \to 1 \tag{7}$$

(iii) **Functoriality of Π***: For any finite field extension $E/\mathbb{F}$, $\Pi(H_i, C, E) \leq \Pi(H_i, C, \mathbb{F})$.*

(iv) *Let C be an $\mathbb{F}$-Cartan subgroup associated to H_i. Then if there exists a finite extension E such that $\phi_C : \mathrm{Gal}(\overline{\mathbb{F}}/E) \to \Pi(H_i, C, E)$ is surjective, then $\phi_C : \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \to \Pi(H_i, C, \mathbb{F})$ is also surjective*

Remark 2.5. (i) *We do not know if $\mathbb{F}_i^W = \mathbb{F}_i$. In [17], Prasad and Rapinchuk show that if H is connected, then $\mathbb{F}_i^W$ is the smallest field L such that H is an inner form over L.*

(ii) *Part (iv) will allow us, in the proof of Theorem 1.1, to assume that H_i splits over $\mathbb{F}$*

Proof.

(i) Since $\widetilde{W}(H_i, C)$ is a normal subgroup of $\Pi(H_i, C, \mathbb{F})$, then so is its inverse image $W_\phi := \phi^{-1}(\widetilde{W}(H_i, C))$. Furthermore, as mentioned above, by Proposition 2.3(ii), it is independent of C. $\mathbb{F}_i \subset \overline{\mathbb{F}}$ is the fixed field of W_ϕ, which is the finite extension of $\mathbb{F}$ satisfying that it is the minimal extension of $\mathbb{F}$ such that $\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/L)) \subset \widetilde{W}(H_i, C)$. For a Cartan subgroup C_1, by Proposition 2.3(iv) we have that $\mathbb{F}_i^W \subset \mathbb{F}_{C_1}$. Since C_1 is arbitrary, we get that $\mathbb{F}_i^W \subset \mathbb{F}_i$.

(ii) (a) As $\ker(\phi_C) = \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_C)$, we get by the first part that $\mathrm{Gal}(\mathbb{F}_C/\mathbb{F}_i)$ is isomorphic to a subgroup of $\widetilde{W}(H_i, C)$.

(b) By (i), $\mathbb{F}_i^W \subset \mathbb{F}_C$, and therefore $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_C) \leq \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_i^W)$. Also by the definition of $\mathbb{F}_i^W$, and the fact that $\ker(\phi_C) = \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_C)$, we get that

$$\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}))/\left(\widetilde{W}(H_i, C) \cap \phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}))\right) \simeq \left(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})/\,\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_C)\right) / \left(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_i^W)/\,\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}_C)\right) \simeq \mathrm{Gal}(\mathbb{F}_i^W/\mathbb{F}) \tag{8}$$

By definition, $\Pi(H_i, C, \mathbb{F})$ is generated by $\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}))$ and $\widetilde{W}(H_i, C)$. Since $\widetilde{W}(H_i, C)$ is a normal subgroup of $\Pi(H_i, \mathbb{F}, C)$, it is in fact equal to $\widetilde{W}(H_i, C)\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}))$. Therefore, by the computation above, we have that

$$\Pi(H_i, \mathbb{F}, C)/\widetilde{W}(H_i, C) = \widetilde{W}(H_i, C)\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}))/\widetilde{W}(H_i, C) \simeq \phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}))/\left(\widetilde{W}(H_i, C) \cap \phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}))\right) \simeq \mathrm{Gal}(\mathbb{F}_i^W/\mathbb{F}) \tag{9}$$

(iii) Since $\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/E))$ is a subgroup of $\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}))$, and by the definition of the groups, we get that $\Pi(H_i, C, \mathbb{F}) \leq \Pi(H_i, C, E)$.

(iv) By (6),(7), we get that for any field K, $\phi_C : \mathrm{Gal}(\overline{\mathbb{F}}/K) \to \Pi(H_i, C, K)$ is surjective if and only if the image contains $\widetilde{W}(H_i, C)$. Therefore, if there exists a field E such that $\phi_C : \mathrm{Gal}(\overline{\mathbb{F}}/E) \to \Pi(H_i, C, E)$ is surjective, then the image $\phi_C(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ contains $\widetilde{W}(H_i, C)$, and therefore, $\phi_C : \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \to \Pi(H_i, C, \mathbb{F})$ is surjective.

□

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$. We define a function $\theta_\sigma : \mathcal{C}_i(\mathbb{F}) \to \Pi(H_i, \mathbb{F})^\sharp$ given by $\theta_\sigma(C) = [\phi_C(\sigma)]$. Notice that if H_i splits over $\mathbb{F}$, then the image is in fact inside $\widetilde{W}(H_i)^\sharp$. In section A.2 we define the notion of regular semisimple elements. A semisimple element is called *regular* if the connected component of its centralizer in H^o is a torus. From Proposition A.1 (2) it follows that such an element $g \in H_i$ is contained in a unique Cartan subgroup associated to H_i that we denote C_g. Note that when $g \in H_i(\mathbb{F})$, then C_g

is defined over $\mathbb{F}$. Using this we can extend θ_σ, defined above for Cartan subgroups, to the set of regular semisimple elements in $H_i(\mathbb{F})$, which we denote $(H_i(\mathbb{F}))_{sr}$. We do this by defining for an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}})$ the map $\theta_\sigma : (H_i(\mathbb{F}))_{sr} \to \Pi(H_i, \mathbb{F})^\sharp$ with $\theta_\sigma(g) = \left[\phi_{C_g}(\sigma)\right]$.

The following proposition shows that in the case where $\mathrm{char}(\mathbb{F}) = 0$, for any element $h \in H_i(\mathbb{F})$, the Galois group of the splitting field over $\mathbb{F}$ of the characteristic polynomial of h is a subquotient of $\Pi(H_i, \mathbb{F})$.

Proposition 2.6. *Let $H, H_i, \mathbb{F}_i$ be as above, and assume $\mathrm{char}(\mathbb{F}) = 0$. For any $h \in H_i(\mathbb{F})$, let $\mathrm{Gal}(\mathbb{F}(h)/\mathbb{F})$ be the Galois group of the splitting field of $\det(T - h)$. Then $\mathrm{Gal}(\mathbb{F}(h)/\mathbb{F})$ is isomorphic to a quotient of a subgroup of $\Pi(H_i, \mathbb{F})$, and $\mathrm{Gal}(\mathbb{F}(h)/(\mathbb{F}(h) \cap \mathbb{F}_i))$ is isomorphic to a quotient of a subgroup of $\widetilde{W}(H_i)$.*

Proof. Let $h \in H_i(\mathbb{F})$. By Jordan decomposition there exists a unique pair $h_s, h_u \in H(\mathbb{F})$ with h_s semisimple, and h_u unipotent, such that $h = h_s h_u = h_u h_s$. Furthermore, since h_u is unipotent, the group generated by it is connected and therefore $h_u \in H^o$, and so $h_s \in H_i(\mathbb{F})$. Let $D_h := D_{h_s}$ be the Zariski closed subgroup generated by h_s. Then D_h is contained in any Cartan subgroup C of G containing h_s. Let C_h be a Cartan subgroup containing h_s, such that C_h/C_h^o is generated by $C_h^o h_s$, so $C_h \in \mathcal{C}_i(\mathbb{F})$. The splitting field of $\det(T - h) = det(T - h_s)$ is the splitting field of D_h. Since $D_h \subset C_h$, we have that the splitting field of D_h is contained in the splitting field of C_h. By the construction of $\Pi(H_i, C_h, \mathbb{F})$ we have that $\mathrm{Gal}(\mathbb{F}_{C_h}/\mathbb{F})$ is a subgroup of $\Pi(H_i, C_h, \mathbb{F})$, and since $\mathrm{Gal}(\mathbb{F}_{D_h}/\mathbb{F})$ is a quotient of $\mathrm{Gal}(\mathbb{F}_{C_h}/\mathbb{F})$ the result follows. Since $\mathbb{F}_i \subset \mathbb{F}_{C_h}$, and $\mathrm{Gal}(\mathbb{F}_{C_h}/\mathbb{F}_i) \subset \widetilde{W}(H_i, C_h)$ (by lemma 2.4) the second part follows in a similar way. □

2.4. **Outer Weyl groups and reduction modulo primes.** In this section we apply the above construction in the following setting: Let $\mathbb{F} = k$ be a number field, $\Sigma \subset \mathrm{GL_n}(k)$ a finite set, $\Gamma = \langle\Sigma\rangle$, $H = \overline{\Gamma}$. Let $\mathcal{O}_k$ be the ring of integers of k. There exists a finite set of places S, such that $\Gamma \subset \mathrm{GL_n}(\mathcal{O}_{k,S}) \cap H =: H(\mathcal{O}_{k,S})$. A significant role in this paper is played by the Frobenius conjugacy class. We give here a reminder for that. Let $\mathfrak{p} \triangleleft \mathcal{O}_k$ be an unramified prime ideal, and let $k_\mathfrak{p}, \mathcal{O}_\mathfrak{p}$ be the corresponding field completion, and valuation ring, respectively. Let $\mathbb{F}_\mathfrak{p}$ be the residue field, and $\pi_\mathfrak{p} : \mathcal{O}_\mathfrak{p} \to \mathbb{F}_\mathfrak{p}$ be the residue map. Denote by $k_\mathfrak{p}^{nr} \subset \overline{k}_\mathfrak{p}$ the maximal unramified extension, and the algebraic closure of $k_\mathfrak{p}$ of $k_\mathfrak{p}$, respectively. It is a well known fact (c.f. chapter V in [3]) that $\mathrm{Gal}(k_\mathfrak{p}^{nr}/k) \simeq \mathrm{Gal}(\overline{\mathbb{F}_\mathfrak{p}}/\mathbb{F}_\mathfrak{p})$ are isomorphic, and thus there exists a unique element denoted $\mathrm{Frob}_\mathfrak{p}$ that corresponds to the generator of $\mathrm{Gal}(\overline{\mathbb{F}_\mathfrak{p}}/\mathbb{F}_\mathfrak{p})$ (denoted also by $\mathrm{Frob}_\mathfrak{p}$ sending $x \mapsto x^{N(\mathfrak{p})}$, where $N(\mathfrak{p})$ is the cardinality of $\mathbb{F}_\mathfrak{p}$). For an embedding $\overline{k} \to \overline{k}_\mathfrak{p}$ corresponds an inclusion $\mathrm{Gal}(\overline{k}_\mathfrak{p}/k_\mathfrak{p}) \to \mathrm{Gal}(\overline{k}/k)$, which defines an element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(\overline{k}/k)$. This element is defined up to a conjugation, and thus defines a conjugacy class of $\mathrm{Gal}(\overline{k}/k)$, and, as in §2.3, defines a map from the regular semisimple elements of $H_i(k)$ to conjugacy classes of $\Pi(H_i,k)$. That is, the following map

$$\theta_{\mathrm{Frob}_{\mathfrak{p}}} : (H_i(k))_{sr} \to \Pi(H_i,k)^\sharp$$

is well defined.

Let us now consider the reduction modulo prime ideals. Note that since H is defined over k, by a finite number of polynomials, H and therefore also H^o, and any coset of it, are defined over $\mathbb{F}_{\mathfrak{p}}$ for almost all prime ideals $\mathfrak{p}$ (depending only on H), by using the same polynomials defining H, regraded as polynomials over $\mathbb{F}_{\mathfrak{p}}$. Notice also, that given a coset H_i, the Weyl group $W(H_i)$, seen as $N_{H^o}(C)/C^o$ for a k-Cartan subgroup C is also defined over $\mathbb{F}_{\mathfrak{p}}$ for all large enough $\mathfrak{p}$, and in fact as it is finite, it is isomorphic to the Weyl group defined over k. The goal of this subsection is to prove the following proposition:

Proposition 2.7. *Let $k, \mathcal{O}_k, S, H, H^o, H_i$ be as above, and assume that H_i splits over k. Then there exists a finite set of primes S' containing S such that*

(i) *There exists a non-empty open subset $V \subset \left(H_i(\overline{k})\right)_{rs}$ defined over k, such that for any $\mathfrak{p} \notin S'$, if $h \in H_i(\mathcal{O}_{k,S})$ satisfying $\pi_{\mathfrak{p}}(h) \in V(\mathbb{F}_{\mathfrak{p}})$, then $h \in V(\mathcal{O}_{k,S}) \subset (H_i(\mathcal{O}_{k,S}))_{rs}$, that is*

$$\{h \in H_i(\mathcal{O}_{k,S}) : h \notin V(\mathcal{O}_{k,S})\} \subset \left\{h \in H_i(\mathcal{O}_{k,S}) : \pi_{\mathfrak{p}}(h) \notin V(\mathbb{F}_{\mathfrak{p}}) \forall \mathfrak{p} \notin S'\right\}$$

(ii) *For any $\mathfrak{p} \notin S'$ there exists a bijection $\alpha : \widetilde{W}(H_{i,\overline{k}})^\sharp \to \widetilde{W}(H_{i,\overline{\mathbb{F}_{\mathfrak{p}}}})^\sharp$, such that for any $h \in H_i(\mathcal{O}_{k,S})$ if $\pi_{\mathfrak{p}}(h) \in (H_i(\mathbb{F}_{\mathfrak{p}}))_{sr}$, then $\alpha(\theta_{\mathrm{Frob}_{\mathfrak{p}}}(h)) = \theta_{\mathrm{Frob}_{\mathfrak{p}}}(\pi_{\mathfrak{p}}(h))$. In particular, we have that the following diagram commutes:*

$$\begin{array}{ccc} H_i(\mathcal{O}_{k,S})_{rs} \supset V(\mathcal{O}_{k,S}) & \xrightarrow{\theta_{\mathrm{Frob}_{\mathfrak{p}}}} & \widetilde{W}(H_i,\overline{k}) \\ \downarrow{\scriptstyle \pi_{\mathfrak{p}}} & & \downarrow{\scriptstyle \alpha} \\ H_i(\mathbb{F}_{\mathfrak{p}})_{rs} \supset V(\mathbb{F}_{\mathfrak{p}}) & \xrightarrow[\theta_{\mathrm{Frob}_{\mathfrak{p}}}]{} & \widetilde{W}(H_i,\overline{\mathbb{F}_{\mathfrak{p}}}) \end{array}$$

and for any $U \in \widetilde{W}(H_i)^\sharp$

$$\left\{h \in H_i(\mathcal{O}_{k,S}) : h \in (H_i(\mathcal{O}_{k,S}))_{sr} \text{ and } \theta_{\mathrm{Frob}_{\mathfrak{p}}}(h) \neq U \ \forall \mathfrak{p} \notin S'\right\} \subset \left\{h \in H_i(\mathcal{O}_{k,S}) : \pi_{\mathfrak{p}}(h) \in (H_i(\mathbb{F}_{\mathfrak{p}}))_{sr} \wedge \theta_{\mathrm{Frob}_{\mathfrak{p}}}(\pi_{\mathfrak{p}}(h)) \neq \alpha(U) \ \forall \mathfrak{p} \notin S'\right\}$$

Remark 2.8. *Notice that since H_i is assumed to be split, there exists a Cartan subgroup C associated to H_i that splits, and therefore for all but finitely many primes, H_i splits also over $\mathbb{F}_{\mathfrak{p}}$. In particular $\theta_{\mathrm{Frob}_{\mathfrak{p}}} \in \widetilde{W}(H_i)^\sharp$. Throughout the proof we will assume that the set S' contains the finite set of exceptional primes.*

Proof. Let $V \subset H_i$ be the open subset given by Proposition A.9. Let C be a fixed split Cartan subgroup, and S' be such that C splits for all $\mathfrak{p} \notin S'$. Furthermore, let $A(C^o)$ be the set of roots of C^o. Since C splits, also C^o does, and choose S' such that for all $\mathfrak{p} \notin S'$ the elements of $A(C^o)$ are defined over $\mathbb{F}_\mathfrak{p}$, and are all different. Notice also that if an element h is inside the kernel of a root of C^o, then its reduction modulo any prime will also be inside the kernel. Therefore, by the proof of Proposition A.9 this shows that if $\pi_\mathfrak{p}(h) \in V(\overline{\mathbb{F}_\mathfrak{p}})$ then $\pi_\mathfrak{p}(h)$ is regular semisimple, and part (1) is proved. For the second part, we follow Lemma 3.2 in [9]. We first construct the bijection $\alpha : \widetilde{W}(H_{i,\overline{k}})^\sharp \to \widetilde{W}(H_{i,\overline{\mathbb{F}_\mathfrak{p}}})^\sharp$. Let $C_0 < H$ be a fixed split k-Cartan subgroup associated to H_i. Let $\mathfrak{p} \notin S$ be an unramified prime. The following maps

$$(N_{H^o}(C_0)/Z_{H^o}(C_0^o))\left((\mathcal{O}_{k,S})_\mathfrak{p}\right) \hookrightarrow (N_{H^o}(C_0)/Z_{H^o}(C_0^o))\,(k_\mathfrak{p}) = \widetilde{W}(H_{i,\overline{k}}, C_0)$$

$$(N_{H^o}(C_0)/Z_{H^o}(C_0^o))\left((\mathcal{O}_{k,S})_\mathfrak{p}\right) \twoheadrightarrow (N_{H^o}(C_0)/Z_{H^o}(C_0^o))\,(\mathbb{F}_\mathfrak{p}) = \widetilde{W}(H_{i,\mathbb{F}_\mathfrak{p}}, C_0)$$

are indeed injective and surjective (notice that the latter is surjective by Hensel's Lemma, and the fact that C_0 splits), and since $\widetilde{W}(H_{i,\overline{k}}, C_0) \simeq \widetilde{W}(H_{i,\overline{\mathbb{F}_\mathfrak{p}}}, C_0)$ are isomorphic (recall that these groups are isomorphic for $\mathfrak{p}$ outside a finite set by the discussion before the Proposition). Therefore, they are both isomorphisms, and as such define a bijection between conjugacy classes. Let $h \in H_i(\mathcal{O}_{k,S})$ be a regular semisimple element such that $\pi_\mathfrak{p}(h) \in H_i(\mathbb{F}_\mathfrak{p})$ is regular semisimple, $C_h = \langle (Z_{H^o}(h))^o, h\rangle$ be the unique Cartan containing it, and $C_{h,\mathfrak{p}}$ be the unique Cartan containing $\pi_\mathfrak{p}(h)$. Let $x \in H^o(\overline{\mathbb{F}})$ be such that $C_0 = xC_{h,\mathfrak{p}}x^{-1}$. Then by Proposition 2.3(iv) $\theta_{\mathrm{Frob}_\mathfrak{p}}(\pi_\mathfrak{p}(h)) = [x^{-1}Frob_\mathfrak{p}(x)]$. By Hensel's Lemma applied to $(\mathcal{O}_{k,S})_\mathfrak{p}^{nr} \to \overline{\mathbb{F}_\mathfrak{p}}$, there exists $\overline{x} \in N_{H^o}(H)((\mathcal{O}_{k,S})_\mathfrak{p}^{nr})$ that lifts x, and thus satisfy $\overline{x}^{-1}C_0\overline{x} = C$, and thus $\theta_{\mathrm{Frob}_\mathfrak{p}}(h) = [\overline{x}^{-1}Frob_\mathfrak{p}(\overline{x})]$. By the definition of the bijection of conjugacy classes, the result is proved. □

3. Outer Weyl groups over finite fields

In this section we prove some properties of outer Weyl groups for groups defined over finite fields. Here H is a linear algebraic group defined and split over a finite field $k = \mathbb{F}_q$ of q elements, H^o, its unit component, is semisimple, and we fix a connected component H_i. We recall first the definition of the function θ defined in the preceding section. For a Cartan subgroup C, we have defined in Section 2 a homomorphism

$$\phi_C : \mathrm{Gal}(\overline{k}/k) \to \widetilde{W}(H_i, C)$$

(note that the image is indeed inside $\widetilde{W}(H_i)$ since we assume that H splits over k). Let $h \in H_i$ be a semisimple regular element, and let C_h be the unique Cartan subgroup containing it. Denote by Frob the Frobenius element in $\mathrm{Gal}(\overline{k}/k)$. We defined in Section 2 the following functions

$$\theta_{\mathrm{Frob}} : \mathcal{C}_i(k) \to \widetilde{W}(H_i)^\sharp \qquad (10)$$
$$C \mapsto [\phi_C(\mathrm{Frob})]$$

and

$$\theta_{\mathrm{Frob}} : H_i(k)_{sr} \to \widetilde{W}(H_i)^\sharp \qquad (11)$$
$$h \mapsto [\phi_{C_h}(\mathrm{Frob})]$$

We abbreviate $\theta := \theta_{\mathrm{Frob}}$. Our goal in this section is to prove that for a fixed connected component H_i, and for a fixed conjugacy class $U \in \widetilde{W}(H_i)^\sharp$, the density of elements $h \in H_i(k)$ such that $\theta(h) = U$ is positive as the size of the field k grows. For a connected component H_i, let $\mathcal{C}_i$ and $\mathcal{C}_i(k)$ be as before. The following theorem, known as the Lang-Steinberg Theorem (c.f. [20] Theorem 10.1), plays a crucial role in the sequel, and we therefore state it.

Theorem 3.1 (Lang-Steinberg Theorem)**.** *Let G be a connected reductive linear algebraic group, and let F be an endomorphism of G. Suppose that F has only finitely many fixed points. Then the map $x \mapsto x^{-1}F(x)$ is surjective.*

Throughout this section, denote for any Cartan subgroup C, $\pi : N_{H^o}(C) \to W(H_i, C)$, and $\widetilde{\pi} : N_{H^o}(C) \to \widetilde{W}(H_i, C)$.

Lemma 3.2. *Let H and H_i be as above. Let $\widetilde{C}$ be a split k-Cartan subgroup associated to H_i, and denote by $W^F = W^F(H_i, \widetilde{C}) := \{w \in W(H_i, \widetilde{C}) : \mathrm{Frob}(w) = w\}$. Then*

(i) *Every $C \in \mathcal{C}_i(k)$ defines a $\widetilde{W}(H_i, \widetilde{C})$ conjugacy class, given by $\theta(C)$.*
(ii) *For every $\widetilde{W}(H_i, \widetilde{C})$-conjugacy class U there exists a Cartan subgroup $C \in \mathcal{C}_i(k)$ such that $\theta(C) = U$.*
(iii) *Let $C_1, C_2 \in \mathcal{C}_i(k)$, and let $x_i, i = 1, 2$ be such that $C_i = \widetilde{C}^{x_i}, i = 1, 2$. Assume that $\pi(x_1^{-1}\mathrm{Frob}(x_1))$ is W^F-conjugate to $\pi(x_2^{-1}\mathrm{Frob}(x_2))$ then C_1 is conjugate to C_2 by an element of $H^o(k)$. Conversely, if C_1 and C_2 are conjugated by an element of $H^o(k)$ then $\theta(C_1) = \theta(C_2)$*

Remark 3.3. *Note that as H_i splits, $\widetilde{W}(H_i, \widetilde{C}) = \widetilde{W}(H_i, \widetilde{C})^F$, but we do not know if also $W(H_i, \widetilde{C}) = W(H_i, \widetilde{C})^F$.*

Proof. For $C \in \mathcal{C}_i(k)$, there exists $x \in H^o(\overline{k})$ such that $C^x = \widetilde{C}$, and $\theta(C) = [x^{-1}\mathrm{Frob}(x)] \in W(H_i, \widetilde{C})^\sharp$. If $\widetilde{C} = C^y$ for $y \in H^o(\overline{k})$, we have that $x^{-1}y = n \in N_{H^\circ}(\widetilde{C})$, and

$$y^{-1}\mathrm{Frob}(y) = n^{-1}x^{-1}\mathrm{Frob}(x)\,\mathrm{Frob}(n) = n^{-1}x^{-1}\mathrm{Frob}(x)n \pmod{Z_{H^\circ}(\widetilde{C})}$$

because $n = \mathrm{Frob}(n) \pmod{Z_{H^\circ}(\widetilde{C})}$ since $\widetilde{C}$ splits. Therefore we get a corresponding equality in $\widetilde{W}(H_i, \widetilde{C})$. Let $U \subset \widetilde{W}(H_i, \widetilde{C})$ be a conjugacy class, and let $n \in N_{H^\circ}(C)$ a corresponding element. Then by Lang-Steinberg

Theorem there exists $g \in H^o(\overline{k})$ such that $g^{-1}\operatorname{Frob}(g) = n$. Then $\widetilde{C}^{g^{-1}}$ is a k-Cartan subgroup such that $\theta(\widetilde{C}^{g^{-1}}) = U$.

Assume now that $C_1, C_2 \in \mathcal{C}_i(k)$ are such that $C_1^{x_1} = \widetilde{C} = C_2^{x_2}$, and $\pi(x_1^{-1}\operatorname{Frob}(x_1))$ and $\pi(x_2^{-1}\operatorname{Frob}(x_2))$ are conjugated by an element W^F. Let $n \in N_{H^o}(\widetilde{C})$ be a conjugating element, that is

$$n^{-1}x_1^{-1}\operatorname{Frob}(x_1)n = x_2^{-1}\operatorname{Frob}(x_2) \pmod{\widetilde{C}^o} \tag{12}$$

Since $w \in W^F$, we get that $n = \operatorname{Frob}(n) \pmod{\widetilde{C}^o}$, and so from (12) we get that

$$x_2 n^{-1} x_1^{-1}\operatorname{Frob}(x_1 n x_2^{-1}) \in (\widetilde{C}^o)^{x_2^{-1}} = C_2^o$$

Applying the Lang-Steinberg theorem for C_2^o, k and Frob, we find that there exists $g \in C_2^o$ such that

$$x_2 n^{-1} x_1^{-1}\operatorname{Frob}(x_1 n x_2^{-1}) = g^{-1}\operatorname{Frob}(g) \tag{13}$$

$$g x_2 n^{-1} x_1^{-1} = \operatorname{Frob}(g x_2 n^{-1} x_1^{-1}) \tag{14}$$

hence $y = g x_2 n^{-1} x_1^{-1} \in H^o(k)$, and it satisfies $C_1^y = C_2$. The converse direction is clear. □

Lemma 3.4. *Let H, H^o and H_i be as above. Let $\widetilde{C} \in \mathcal{C}_i(k)$ be a split Cartan subgroup, and let $C \in \mathcal{C}_i(k)$. Let $g \in H^o(\overline{k})$ be such that $C = \widetilde{C}^g$, and denote by $w = \widetilde{\pi}(g^{-1}\operatorname{Frob}(g)) \in \widetilde{W}(H_i, \widetilde{C})$. Let $N(k) = N_{H^o}(C)(k), C^o(k)$ be the k-points of $N_{H^o}(C), C^o$ respectively. Then*

(i) *Let $\pi_W : W(H_i, \widetilde{C}) \twoheadrightarrow \widetilde{W}(H_i, \widetilde{C})$, then for any $x \in W^F(H_i, C)$*

$$\pi(gxg^{-1}) \in Z_{\widetilde{W}(H_i,\widetilde{C})}(w)$$

(ii) *Let $A = |\ker(\pi_W)|$. Then*

$$\frac{|N(k)|}{|C^o(k)|} \leq A|Z_{\widetilde{W}(H_i,\widetilde{C})}(w)|$$

In particular, there exists a constant $c >$ independent of k, such that $\frac{|N(k)|}{|C^o(k)|} < c$.

Proof. We first note that conjugation by g sends $N_{H^o}(\widetilde{C})$ to $N_{H^o}(C)$, and $\widetilde{C}^o$ to C^o. Let $x \in N_{H^o}(\widetilde{C})$, and let Frob be the Frobenius automorphism of k. Then $gxg^{-1} \in W(H_i, \widetilde{C})$. Notice that

$$\operatorname{Frob}(gxg^{-1}) = gg^{-1}\operatorname{Frob}(g)\operatorname{Frob}(x)\operatorname{Frob}(g)^{-1}gg^{-1} = gw^{-1}\operatorname{Frob}(x)wg^{-1}$$

where all equalities are as elements of $W(H_i, \widetilde{C})$. Therefore, if $gxg^{-1} \in W^F(H_i, \widetilde{C})$, then

$$gxg^{-1} = gw^{-1}\operatorname{Frob}(x)wg^{-1} \Rightarrow x = w^{-1}\operatorname{Frob}(x)w$$

since $\widetilde{C}$ splits which implies that $\pi_W(x) = \pi_W(\operatorname{Frob}(x))$. We get that $w^{-1}\pi_W(x)w = \pi_W(x)$.

By [2] §1.17 we have that $N(k)/C^o(k)$ is isomorphic to $(N/C^o)(k)$, the subgroup of $W(H_i, C)$ consisting of Frobenius fixed points, that is $W^F(H_i, C)$, which concludes the proof of the second part. □

Proposition 3.5. *Let H, H^o and H_i be as above, and let $U \in W(H_i)^\sharp$ a fixed conjugacy class. Then there exists a constant $c > 0$ (independent of k), such that*

$$\frac{|\{g \in (H_i(k))_{sr} : \theta(g) \in U\}|}{|H_i(k)|} \geq c > 0 \quad \textit{as } |k| \to \infty \tag{15}$$

Proof. Denote by $\mathcal{C}_i(k, U)$ the set of Cartan subgroups $C \in \mathcal{C}_i(k)$ such that $\theta(C) = U$. This is a nonempty set by Lemma 3.2. Let $C_1 \in \mathcal{C}_i(k, U)$ be a fixed Cartan subgroup. Then

$$\frac{\{g \in (H_i(k))_{sr} : \theta(g) \in U\}}{|H_i(k)|} = \frac{|\{g \in H_i(k)_{sr} : \exists C \in \mathcal{C}_i(k,U) \text{ s.t } g \in C\}|}{|H_i(k)|} \geq$$
$$\frac{|\{g \in H_i(k)_{sr} : \exists x \in H^o(k) \text{ s.t } g \in C_1^x\}|}{|H_i(k)|} = \frac{1}{|H_i(k)|} \sum_{\substack{C = C_1^x \\ x \in H^o(k)}} |C \cap H_i(k)| + o(1)$$

Where in the last line we use the fact that most elements are semisimple regular, and the fact that if C, C' are $H^o(k)$-conjugate then $\theta(C) = \theta(C')$. We now get that

$$\frac{1}{|H_i(k)|} \sum_{\substack{C = C_1^x \\ x \in H^o(k)}} |C \cap H_i(k)| = \frac{1}{|H_i(k)|} \sum_{g \in H^o(k)/N_{H^o}(C_1)(k)} |g^{-1}Cg \cap H_i(k)| =$$
$$\frac{1}{|H_i(k)|} \sum_{g \in H^o(k)/N_{H^o}(C_1)(k)} |g^{-1}(C_1 \cap H_i(k))g| = \frac{|C_1 \cap H_i(k)|}{|N_{H^o}(C_1)(k)|}$$

Let $h \in C_1 \cap H_i(k)$ be a fixed element, and write $H_i(k) = H^o(k)h$. Therefore

$$|C_1 \cap H_i(k)| = |C_1 \cap H^o(k)h| = |C_1 \cap H^o(k)| \geq |C_1^o(k)|$$

since $C_1^o \subset (C_1 \cap H^o)$. Therefore,

$$\frac{|C_1 \cap H_i(k)|}{|N_{H^o}(C_1)(k)|} \geq \frac{|C_1^o(k)|}{|N_{H^o}(C_1)(k)|} \geq$$
$$\frac{A}{|Z_{W(H_i,C_1)}(w)|} = A\frac{|U|}{|\widetilde{W}(H_i)|} > 0$$

where in the first equality we use $|H^o(k)| = |H_i(k)|$, and in the last line we use Lemma 3.4 and that the size of a conjugacy class U in $\widetilde{W}(H_i, C_1)$ is $|U| = \frac{|\widetilde{W}(H_i,C_1)|}{|Z_{\widetilde{W}(H_i,C_1)}(w)|}$, for any $w \in U$. □

4. Proof of theorem 1.1 for number fields

In this section we prove the following theorem which is the special case of Theorem 1.1 under the assumption that $\mathbb{F} = k$ is a number fields. We recall that a subset Σ in a group Γ is called admissible if $\Sigma = \Sigma^{-1}$ and satisfying that $Cay(\Gamma, \Sigma)$ is not bipartite. This can be achieved if the elements of Σ satisfy an odd relation. In general this is true if Σ is not contained in the complement of a subgroup of index 2.

Theorem 4.1. *Let k be a number field, $n \in \mathbb{N}$, and $\Sigma \subset \mathrm{GL_n}(k)$ a finite admissible subset. Let $\Gamma := \langle \Sigma \rangle$, and $H := \overline{\Gamma}$ with H^o semisimple. For $\gamma \in \Gamma$ let $\Pi(\gamma H^o)$ be the group $\Pi(\gamma H^o, k)$ defined in §2.3. Let $w : \mathbb{N} \to \Sigma$ be a random walk of Γ. Then there exists $c > 0$, such that for all $k \in \mathbb{N}$*

$$\mathbb{P}(w_k \in \{\gamma \in \Gamma : \mathrm{Gal}(k(\gamma)/k) \neq \Pi(\gamma H^o)\}) \ll e^{-ck}$$

We first recall the basic setting from the previous sections. Let H be an algebraic group with H^o semisimple. Let H_i be a coset of H^o. For a semisimple regular element $h \in H_i$, let C_h be the unique Cartan subgroup associated to H_i that contains h. We have constructed a homomorphism $\phi_h : \mathrm{Gal}(\overline{k}/k) \to \Pi(H_i, C_h)$, with $\ker(\phi_h)$ satisfying $\mathrm{Gal}(k_{C_h}/k) \simeq \mathrm{Gal}(\overline{k}/k)/\ker(\phi_h)$. Furthermore, if H_i splits over k, then $\Pi(H_i, C_h, k) = W(H_i, C_h)$ the outer Weyl group associated to H_i, and in general $\Pi(H_i, C_h, k) = \langle \phi_h(\mathrm{Gal}(k_{C_h}/k)), W(H_i, C_h) \rangle$. In order to justify our focus on Cartan subgroups instead of elements we need the following definition generalizing similar notions from [16].

Definition 4.2. *Let H, H^o, H_i and k be as above. Let $H^o = H^1 \cdots H^l$ be the decomposition of H^o as an almost produck of k-simple subgroups, and $H^o = H^{(1,i)} \cdots H^{(r,i)}$ be the minimal decomposition of H^o into normal subgroups of H^o invariant under conjugation by H_i (see Appendix B). We say that*

- (i) *A k-Cartan subgroup C associated to H_i is $H_i - k$ quasi irreducible if C^o has no k-subtori other than $C^o \cap H^{(j,i)}, j = 1, \dots, r$.*
- (ii) *An element $x \in H^o$ is without H_i-components of finite order if for some (equivalently, any) decomposition $x = x_1 \cdots x_r$ with $x_i \in H^{(s,i)}, s = 1, \dots, r$, all the x_i's have infinite order.*

In Appendix B we prove (see Lemma B.3 and Corollary B.4) the following generalization of a result in [16]:

Lemma 4.3. *Let H be a linear algebraic group defined over a number field k, such that H^o is semisimple. Fix a coset H_i of H^o, and let $H = H^{(1,i)} \cdots H^{(r,i)}$ as above. Let C be a k-Cartan subgroup associated to H_i such that $\mathrm{Gal}(k_C/k)$ contains the Weyl group $W(H_i, C)$, then C^o is $H_i - k$ quasi irreducible. Furthermore, if $x \in C \cap H_i(k)$ is such that $x^{\mathrm{ord}(H_i)}$ is without H_i-components of finite order (where $\mathrm{ord}(H_i)$ is the order of H_i in H/H^o), then $\mathrm{Gal}(k(x)/k) = \mathrm{Gal}(k_C/k)$.*

Theorem 4.1 follows from the following two lemmas

Lemma 4.4. *Let $\Sigma, \Gamma, H, H^o, H_i, w : \mathbb{N} \to \Sigma$ be as above, and assume H^o is semisimple. Then there exists $c_1 > 0$ such that for all $k \in \mathbb{N}$*

$$\mathbb{P}(w_k \in \{\gamma \in \Gamma : \gamma \text{ is not regular semisimple }\}) \ll e^{-c_1 k} \tag{16}$$

and

$$\mathbb{P}(w_k \in \{\gamma \in \Gamma \cap H_i : \gamma \text{ has an } H_i\text{-component of finite order}\}) \ll e^{-c_1 k} \tag{17}$$

Lemma 4.5. *Let $\Sigma, \Gamma, H, H^o, H_i, w : \mathbb{N} \to \Sigma$ be as above, and assume H^o is semisimple, and H_i splits over k. For $U \in W(H_i)^\sharp$ denote*

$$Z_1 = \left\{\gamma \in \Gamma : \gamma \text{ is semisimple regular, and } \phi_\gamma(\mathrm{Gal}(\overline{k}/k)) \cap U = \emptyset\right\}.$$

There exists $c_2 > 0$ such that for all $n \in \mathbb{N}$

$$\mathbb{P}(w_k \in Z_1) \ll e^{-c_2 n} \tag{18}$$

We first conclude the proof of the Theorem 4.1 assuming the above Lemmas, by showing that the complement of the set

$$\{\gamma \in \Gamma : \mathrm{Gal}(k(\gamma)/k) = \Pi(\gamma H^o)\}$$

is contained in a finite union of exponentially small sets. By Lemma 4.4, we may assume that if $\gamma \in H_i$ then γ is regular semisimple without H_i-components of finite order. In particular, for such $\gamma \in \Gamma \cap H_i$, $C_\gamma := \langle (Z_{H^o}(\gamma))^o, \gamma\rangle$ is the unique k-Cartan subgroup associated to H_i containing γ, and by Lemma 4.3, that $\mathrm{Gal}(k_{C_\gamma}/k) = \mathrm{Gal}(k(\gamma)/k)$. We therefore concentrate our attention from now on to elements in Cartan subgroups, and Galois groups of splitting fields of them. We want to show that for any coset H_i, most elements C of $\mathcal{C}_i(k)$ satisfy $\mathrm{Gal}(k_C/k) = \Pi(H_i, k)$. By Lemma 2.4(iv) $\mathrm{Gal}(k_C/k) = \Pi(H_i, k)$ if there exists a finite extension K of k, such that $\mathrm{Gal}(K_C/K) = \Pi(H_i, K)$. We may therefore assume, by replacing the field k with a finite extension, that all cosets of H^o split over k. In particular, we have that $\Pi(H_i, k) = \widetilde{W}(H_i)$. Using a well known theorem of Jordan, stating that for any finite group, a proper subgroup must have an empty intersection with at least one conjugacy class, we have that if $C \in \mathcal{C}_i(k)$ satisfies that the image of $\mathrm{Gal}(k_C/k) \neq \widetilde{W}(H_i, C)$, then there exists a conjugacy class $U \in \widetilde{W}(H_i)^\sharp$, such that for any $\sigma \in \mathrm{Gal}(\overline{k}/k)$, $\theta_\sigma(C) \neq U$. We therefore have the following inclusion:

$$\{\gamma \in \Gamma : \mathrm{Gal}(k(\gamma)/k) \ncong \Pi(\gamma H^o)\} \subset \tag{19}$$
$$\bigcup_{i=1}^{m} \{\gamma \in \Gamma \cap H_i : \gamma \notin (H_i(k))_{rs} \text{ or has an } H_i\text{-component of finite order}\} \bigcup$$
$$\bigcup_{U \in W(H_i)^\sharp} \left\{\gamma \in \Gamma \cap (H_i(k))_{rs} : {}^{\gamma \text{ is without } H_i\text{-components of finite order,}}_{\phi_\gamma(\mathrm{Gal}(\overline{k}/k)) \cap U = \emptyset}\right\}$$

and since this is a finite union, it suffice to show that each set is exponentially small, which is the content of Lemma 4.5 and Lemma 4.4, and thus the Theorem is proved.

4.1. **Sieve method.** For both Lemmas the following theorem of Salehi Golsefidi-Varju [19] is essential.

Theorem 4.6. *Let $\Gamma \subset \mathrm{GL_n}(\mathbb{Z}[\frac{1}{q_0}])$ be the group generated by a symmetric set S. Then $\mathcal{G}(\pi_q(\Gamma), \pi_q(S))$ form a family of expanders when q ranges over square free integers coprime to q_0 if and only if the connected component of the Zariski closure of Γ is perfect.*

4.1.1. *Proof of Lemma 4.4.* Assume, without loss of generality, that $H = \langle H^o, H_i \rangle$, and let $\pi_{(j,i)} : H \to H/\widehat{H^o_{i,j}}$, where

$$\widehat{H^o_{i,j}} := H^{(1,i)} \cdots H^{(j-1,i)} H^{(j+1,i)} \cdots H^{(r,i)},$$

(that is the product with $H^{(j,i)}$ dropped) be the reduction map from H onto the adjoint representation of $H^{(j,i)}$. Notice that if $x = x_1 \cdots x_r \in H^o$ is such that x_j is of finite order, then $\pi_{(j,i)}(x)$ has finite order. The proof will follow from Proposition 2.7 and the following Proposition 2.7 from [13]:

Proposition 4.7. *Let Γ be a finitely generated subgroup of $\mathrm{GL_n}(\mathbb{Q})$, such that the identity component of the Zariski closure of $H = \overline{\Gamma}$ is perfect. Let V be a proper subvariety of H, defined over $\mathbb{Q}$. Then the set $V(\mathbb{C}) \cap \Gamma$ is exponentially small.*

By Proposition A.9, the set of regular semisimple elements in H_i contain an open dense subset, defined over k, and therefore (16) is a consequence of Proposition 4.7. Notice, also, that for a fixed field k, there exists $m \in \mathbb{N}$, such that if $h \in H(k)$ with eigenvalue that is a root of unity, then the order of the root divides m. Therefore all regular semisimple elements of finite order in H_i are inside the variety defined by $x^{mn} = 1$, where n is the order of H_i in H/H^o, and thus (17) also follows from Proposition 4.7.

4.1.2. *Proof of Lemma 4.5.* Lemma 4.5 is a consequence of the sieve method for groups, and in particular the following Theorem:

Theorem 4.8 ([13] Corollary 3.3)**.** *Fix $s \geq 2$. Let Γ be a finitely generated group, and let $\Sigma \subset \Gamma$ an admissible subset of it. Let $\Lambda < \Gamma$ be a subgroup of Γ of finite index, and let $(N_i)_{i \geq s}$ be a sequence normal subgroups of Γ of finite index which are contained in Λ. Let $Z \subset \Gamma$ and assume the following*

(i) *Γ has property-τ w.r.t the series of normal subgroup $(N_i \cap N_j)_{i,j \geq s}$.*
(ii) *There exists d such that $|\Gamma/N_j| \leq j^d$ for every $j \geq s$.*
(iii) *$|\Lambda/ (N_i \cap N_j)| = |\Lambda/N_i||\Lambda/N_j|$ for every $i \neq j \geq s$*
(iv) *There is $c > 0$ such that for every coset $\kappa \in \Gamma/\Lambda$ and every $j \geq s$*

$$|(Z \cap \kappa) N_j/N_j| \leq (1-c)|\Lambda/N_j|. \tag{20}$$

Then there exist $\alpha, t > 0$ such that

$$\mathbb{P}\left(\{w_k \in \Gamma : w_k \in Z\}\right) \leq e^{-\alpha k} \quad \forall k \geq t \log s$$

By Proposition 2.7 there exists an open non-empty subset V defined over k and a finite set of primes S, such that the following set

$$Z = \left\{h \in \Gamma : h \in V(k) \subset (H_i(k))_{rs}\,,\ \theta_{\mathrm{Frob}_{\mathfrak{p}}}(h) \neq U, \forall \mathfrak{p} \notin S\right\}.$$

is contained in the following

$$Z_1 := \left\{h \in \Gamma : \pi_{\mathfrak{p}}(h) \in V(\mathbb{F}_{\mathfrak{p}}) \subset (\pi_{\mathfrak{p}}(\Gamma))_{rs}\,, \theta_{\mathrm{Frob}_{\mathfrak{p}}}(\pi_{\mathfrak{p}}(h)) \neq U, \forall \mathfrak{p} \notin S\right\}$$

and thus it suffice to show that the latter is exponentially small. For this goal we will use Theorem 4.8. In order to define the sequence of normal subgroups $\{N_i\}_{i \geq s}$, and the subgroup $\Lambda < \Gamma$ we use the following Proposition

Proposition 4.9. *Let k be a number field, $\Delta = \langle g_1, \ldots, g_r\rangle, g_i \in \mathrm{GL_n}(k)$ a finitely generated group, such that $G := \overline{\Delta}$ is connected and semisimple. Let $\psi : \widetilde{G} \to G$ be the simply connected cover of G. Then there exists a finite set S of primes of $\mathcal{O}_k$, the ring of integers of k, and a set $\mathcal{P}$ of primes of positive density such that for any $\mathfrak{p} \in \mathcal{P}$*

$$\pi_{\mathfrak{p}}(\Delta) \subset \psi(\widetilde{G}(\mathbb{F}_{\mathfrak{p}}))$$

Proof. Let $\widetilde{\Delta} := \psi^{-1}(\Delta)$. This is a subgroup of $\psi^{-1}(G(k)) \subset \widetilde{G}(K)$ where K is a finite extension of k. Since $\widetilde{\Delta}$ is finitely generated the entries of its elements are S-arithmetic for a finite set of primes of K. By Chebotarev's density Theorem (c.f. p. 143 in [7]), there exists a set of positive density of primes $\mathcal{P}$ of $\mathcal{O}_k$, that totally splits in K, that is for any prime ideal $\mathfrak{P} \lhd \mathcal{O}_{K,S}$ such that $\mathfrak{P}|\mathfrak{p}$, $\mathcal{O}_{K,S}/\mathfrak{P} \simeq \mathcal{O}_k/\mathfrak{p} \simeq \mathbb{F}_{\mathfrak{p}}$ and thus when reducing Δ mod $\mathfrak{p}$ we have

$$\pi_{\mathfrak{p}}(\Delta) \subset \psi(\widetilde{G}(\mathbb{F}_{\mathfrak{p}}))$$

□

We apply Proposition 4.9 with $G = H^o$, $\Delta = \Gamma \cap H^o$. For the set $\mathcal{P}$ given by Proposition 4.9, set $\{N_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{P}}$, and $\Lambda := \psi(\psi^{-1}(\Delta) \cap \widetilde{H^o})$. It is therefore left to show that all conditions of Theorem 4.8 hold:

(i) Condition i holds by Theorem 4.6.
(ii) Condition ii holds since $\mathcal{P}$ has positive density inside primes.
(iii) Condition iii holds since by the Strong Approximation Theorem (see e.g. [21] Theorem 9.1.1,[15] Theorem 5.1, and Proposition 5.2 in [9] and the references therein) $\Lambda/N_{\mathfrak{p}} \simeq \widetilde{H}(\mathbb{F}_p)$ and by the Chinese Remainder Theorem, $\Lambda/(N_{\mathfrak{p}} \cap N_{\mathfrak{q}}) = \Lambda/N_{\mathfrak{p}} \times \Lambda/N_{\mathfrak{q}} \simeq \widetilde{H}(\mathbb{F}_{\mathfrak{p}}) \times \widetilde{H}(\mathbb{F}_{\mathfrak{q}})$
(iv) For Condition iv, let $\kappa \in \Gamma/\Lambda$, and let H_i be the coset of H^o such that $\kappa \in H_i$. Let $\mathfrak{p} \in \mathcal{P}$, and write $\kappa = \Lambda\gamma$, where $\gamma \in \kappa$. For a regular semisimple element $h \in \kappa$ such that $\pi_{\mathfrak{p}}(h)$ is also regular semisimple,

denote $C_{h,\mathfrak{p}}$ the unique Cartan subgroup containing $\pi_{\mathfrak{p}}(h)$. Then

$$(21)\quad |\pi_{\mathfrak{p}}(Z_1 \cap \kappa)| \leq \left| \left\{ h \in \pi_{\mathfrak{p}}(\Gamma)_{rs} : \theta_{\mathrm{Frob}_{\mathfrak{p}}}(h) \neq U \right\} \right| \leq \left| \bigcup_{\substack{h:\pi_{\mathfrak{p}}(h)\in (H_i(\mathbb{F}_{\mathfrak{p}}))_{rs} \\ \theta_{Frob_{\mathfrak{p}}}(\pi_{\mathfrak{p}}(h))\neq U}} (C_{h,\mathfrak{p}})^o \, \pi_{\mathfrak{p}}(h) \cap \pi_{\mathfrak{p}}(\Lambda\gamma) \right| = \left| \bigcup_{\substack{h:\pi_{\mathfrak{p}}(h)\in (H_i(\mathbb{F}_{\mathfrak{p}}))_{rs} \\ \theta_{Frob_{\mathfrak{p}}}(\pi_{\mathfrak{p}}(h))\neq U}} (C_{h,\mathfrak{p}})^o \cap \pi_{\mathfrak{p}}(\Lambda) \right|$$

Where the last equality is since $\pi_{\mathfrak{p}}(\gamma h^{-1}) \in \pi_{\mathfrak{p}}(\Lambda)$ by Proposition 4.9. Let $C_1 \in \mathcal{C}_i(\mathbb{F})$ be a fixed Cartan subgroup (provided by Lemma 3.2) satisfying $\theta(C_1) = U$. Since $H_i(\mathbb{F}_{\mathfrak{p}})$ splits, and by Lemma 3.2 the complement set of the latter set contains the following union of sets

$$\left| \bigcup_{C\in\mathcal{C}_i(\mathbb{F}_{\mathfrak{p}}):\theta_{\mathrm{Frob}_{\mathfrak{p}}}(C)\in U} \left(C^o \cap \widetilde{H}(\mathbb{F}_{\mathfrak{p}}) \right) \right| \geq \left| \bigcup_{g\in H^o(\mathbb{F}_{\mathfrak{p}})/N_{H^o}(C_1)(\mathbb{F}_{\mathfrak{p}})} C_1^o \cap \widetilde{H}(\mathbb{F}_{\mathfrak{p}}) \right| \geq \frac{|C_1^o \cap \psi\left(\widetilde{H}(\mathbb{F}_{\mathfrak{p}})\right)||H^o(\mathbb{F}_{\mathfrak{p}})|}{|N_{H^o}(C_1)(\mathbb{F}_{\mathfrak{p}})|} \geq \frac{|C_1^o||\widetilde{H}(\mathbb{F}_{\mathfrak{p}})||H(\mathbb{F}_{\mathfrak{p}})|}{|N_{H^o}(C_1)(\mathbb{F}_{\mathfrak{p}})|}.$$

In the last inequality we used the fact that $\psi\left(\widetilde{H}(\mathbb{F}_{\mathfrak{p}})\right)$ is a normal subgroup of $H^o(\mathbb{F}_{\mathfrak{p}})$, and that

$$|C_1^o \cap \psi\left(\widetilde{H}(\mathbb{F}_{\mathfrak{p}})\right)| \geq \frac{|C_1^o(\mathbb{F}_{\mathfrak{p}})||\psi\left(\widetilde{H}(\mathbb{F}_{\mathfrak{p}})\right)}{|H(\mathbb{F}_{\mathfrak{p}})|}.$$

By Lemma 3.4 and as $\widetilde{H}(\mathbb{F}_{\mathfrak{p}})$ is a normal subgroup of bounded index in $H^o(\mathbb{F}_{\mathfrak{p}})$ we get that there exists a constant $c > 0$ such that the last expression is bounded below by $c|\psi\left(\widetilde{H}(\mathbb{F}_{\mathfrak{p}})\right)|$. We thus find that $1 - |\pi_{\mathfrak{p}}(Z)|/|\pi_{\mathfrak{p}}(\Lambda)| \geq c > 0$, which shows that condition iv holds.

Since all conditions of Theorem 4.8 hold, this concludes the proof of Lemma 4.5.

4.2. **Arbitrary groups.** We conclude this section by proving Theorem 1.1 over number fields, for any group H such that H^o does not contain a central torus. The following lemma was proved in [9] (Lemma 2.3)

Lemma 4.10. *Let k be a field of characteristic 0, and $\Gamma < \mathrm{GL_n}(k)$ a subgroup. Let $G = \overline{\Gamma}$ be the Zariski closure of Γ, $R_u(G)$ the unipotent radical* *of G^o, and $\pi_u : G \to G/R_u(G)$ the reduction map. Then for any $g \in G(k)$, $k(g) = k(\pi_u(g))$.*

Let $\Gamma' = \pi_u(\Gamma) = \langle \pi_u(\Sigma) \rangle$ where $\pi_u : H \to H/R_u(H^o)$. Then by the assumption that H^o does not contain a central torus we get that $\pi_u(H^o)$ is semisimple. By Lemma 4.10, $k(\gamma) = k(\pi_u(\gamma))$. For a coset H_i of H^o, let $\Pi(H_i, k) = \Pi(\pi_u(H_i), k)$. Then we get that

$$\mathbb{P}(w_k \in \{\gamma \in \Gamma : \mathrm{Gal}(k(\gamma)/k) \neq \Pi(\gamma H^o)\}) \leq$$
$$\mathbb{P}(w_k \in \left\{\pi_u(\gamma) \in \Gamma' : \mathrm{Gal}(k(\pi_u(\gamma))/k) \neq \Pi(\pi_u(\gamma H^o))\right\})$$

which by Theorem 4.1 is exponentially small.

5. From number fields to finitely generated fields

In the previous section we proved Theorem 1.1 for the case when $\mathbb{F} = k$ is a number field. The goal of this section is to prove the same result for the general case of finitely generated field $\mathbb{F}$. This will be done using the procedure of specialization.

Let us recall the notations of §2: Let $\mathbb{F}$ be any characteristic zero field, H an algebraic subgroup of GL_n defined over $\mathbb{F}$, H^o its connected component and $\{H_i\}_{i=1}^m$ the cosets of H^o in H. For every $1 \leq i \leq m$ we defined a group $\Pi(H_i, \mathbb{F})$ and we showed (Proposition 2.6) that for every $h \in H_i(\mathbb{F})$, $\mathrm{Gal}(\mathbb{F}(h)/\mathbb{F})$ is isomorphic to a quotient of a subgroup of $\Pi(H_i, \mathbb{F})$. By Lemma 4.10, we can assume that the connected component of the Zariski closure of Γ is semisimple. In §4 we proved Theorem 1.1 for the case where $\mathbb{F} = k$ is a number field and H^o is a semisimple group, namely we showed that if $\Gamma = \langle \Sigma \rangle$ is a finitely generated subgroup of $H(k)$, then outside an exponentially small subset of Γ, $\mathrm{Gal}(k(\gamma)/k)$ is isomorphic to $\Pi(H^o\gamma, k)$.

Now, if we turn to the general case of finitely generated field $\mathbb{F}$, and $\Gamma = \langle \Sigma \rangle$ is a Zariski dense subgroup of $H(\mathbb{F}) \subset GL_n(\mathbb{F})$, then $\Gamma \subset GL_n(A)$ where A is some finitely generated $\mathbb{Q}$-algebra of $\mathbb{F}$, with $\mathbb{F}$ being its field of quotients. If $\varphi : A \to k$ is a ring homomorphism (in fact $\mathbb{Q}$-algebra homomorphism) onto a number field (such φ is called a *specialization*), then φ induces a group homomorphism $\varphi : GL_n(A) \to GL_n(k)$,and for every $h \in GL_n(A)$, $\mathrm{Gal}(k(\varphi(h))/k)$ is a quotient of $\mathrm{Gal}(\mathbb{F}(h)/\mathbb{F})$. Let $\widetilde{\Gamma}$ be the image of Γ, so it is generated by $\widetilde{\Sigma} = \varphi(\Sigma)$, and $\widetilde{H}$ be the Zariski closure of $\widetilde{\Gamma}$. In Proposition 5.1 below, we will show that for any coset H_i there exists such a specialization φ_i with $\widetilde{\langle H^o, H_i \rangle}$ isomorphic to $\langle H^o, H_i \rangle$, and such that $\Pi(\widetilde{H_i}, k) = \Pi(H_i, \mathbb{F})$. Once Proposition 5.1 is proved, Theorem 1.1 holds for any finitely generated $\mathbb{F}$ and H^o semisimple. Indeed, we know on one hand that for $h \in H_i$, $\mathrm{Gal}(\mathbb{F}(h)/\mathbb{F})$ is a subquotient of $\Pi(H_i, \mathbb{F})$. On the other hand $\mathrm{Gal}(k(\varphi_i(h))/k)$ which is a quotient of $\mathrm{Gal}(\mathbb{F}(h)/\mathbb{F})$ is isomorphic , for *almost all* h, to $\Pi(\widetilde{H_i}, k) \simeq \Pi(H_i, \mathbb{F})$. This implies that $\mathrm{Gal}(\mathbb{F}(h)/\mathbb{F})$ is isomorphic to $\Pi(H_i, \mathbb{F})$ for *almost all* $h \in H$, i.e., outside an exponentially small subset.

We are left to prove:

Proposition 5.1. *Let $\mathbb{F} = \mathbb{Q}(y_1, \dots, y_r)$ be a finitely generated field, $\Gamma \leq GL_n(\mathbb{F})$ a finitely generated with semisimple Zariski closure H. For a connected component H_i denote $\Gamma_i := \Gamma \cap \langle H^o, H_i \rangle$. Then for any connected component H_i, there exist a finitely generated $\mathbb{Q}$-algebra $A_i = \mathbb{Q}[x_1, \dots, x_r]$ and a $\mathbb{Q}$-algebra homomorphism φ_i from A_i to a number field k_i, inducing a group homomorphism $\tilde{\varphi}_i : GL_n(A_i) \to GL_n(k_i)$ such that:*

- (i) $\Gamma_i \leq GL_n(A_i)$
- (ii) $\mathbb{F}$ *is the field of quotients of* A_i.
- (iii) *If $\widetilde{H}$ denotes the Zariski closure of $\tilde{\varphi}_i(\Gamma_i)$, then $\tilde{\varphi}_i$ induces an isomorphism between $\Gamma_i / H^o \cap \Gamma$ and $\tilde{\varphi}_i(\Gamma_i)/\widetilde{H^o} \cap \tilde{\varphi}_i(\Gamma_i)$ and (as Γ_i is Zariski dense in $\langle H^o, H_i \rangle$ and $\tilde{\varphi}_i(\Gamma_i)$ in $\widetilde{H}$) also between $\langle H^o, H_i \rangle / H^o$ and $\widetilde{H}/\widetilde{H^o}$ which we also denote by $\tilde{\varphi}_i$.*
- (iv) $\Pi(H_i, \mathbb{F}) \simeq \Pi(\widetilde{H_i}, k)$

The proof of Proposition 5.1 is a consequence of the following lemmas

Lemma 5.2. *Let K be a number field, $R = K[x_1, \dots, x_l]$ a finitely generated integral domain over K, $F = Quot(R)$ the field of quotients of R, E a finite Galois extension of F and S the integral closure of R in E. Then there exists a K-epimorphism φ from S onto a finite extension $\overline{E}$ of K, such that if we denote $\overline{F} = \varphi(R)$, then $\overline{E}$ is a Galois extension of $\overline{F}$ and* $\mathrm{Gal}(\overline{E}/\overline{F}) = \mathrm{Gal}(E/F)$.

Proof. By Noether's normalization Lemma, let $t_1, \dots, t_r \in R$ be algebraically independent over K, such that R is integral over $R_0 = K[t_1, \dots, t_r]$ (cf. [4] Proposition 5.2.1). Denote $F_0 = Quot(R_0)$. Let $z \in S$ be a primitive element for E/F_0, and let $f = f(t_1, \dots, t_r, Z) \in R_0[Z]$ be the irreducible polynomial of z over F_0. Since K is a Hilbertian field, there exists $a = (a_1, \dots, a_r) \in K^r$ such that $f(a, Z)$ is separable and irreducible over K, and $\deg(f(a, Z)) = \deg(f(t, Z))$. Since S is integral over R_0, we can extend the specialization $t \mapsto a$ to a K-homomorphism φ from S onto a finite extension $\overline{E}$ of K. Denote by $\overline{F} = \varphi(R)$, and get that

$$[E : F_0] \geq [\overline{E} : K] \geq \deg(f(a, Z)) = \deg(f(t, Z)) = [E : F_0] \tag{22}$$

and therefore $[E : F_0] = [\overline{E} : K]$. Notice that $[\overline{F} : K] \leq [F : F_0]$ and $[\overline{E} : \overline{F}] \leq [E : F]$. Now, since $[\overline{E} : K] = [\overline{E} : \overline{F}][\overline{F} : K]$, and $[E : F_0] = [E : F][F : F_0]$ we get from (22) that $[\overline{E} : \overline{F}] = [E : F]$, and by Lemma 6.1 in [4] $[\overline{E} : \overline{F}]$ is a Galois extension, and φ induces an isomorphism $\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(\overline{E}/\overline{F})$. ☐

Lemma 5.3. *Let A be a finitely generated integral domain over $\mathbb{Q}$, $\Gamma \leq GL_n(A)$ a finitely generated group with Zariski closure H satisfying H^o is semisimple and H/H^o is cyclic. Then there is a number field k and a $\mathbb{Q}$-homomorphism $\varphi : A \to k$, such that the Zariski closure of $\varphi(\Gamma)$ is isomorphic to H.*

Proof. This is proved in [12] Theorem 4.1 for the case where H is a connected simple group. The proof works word by word if H is semisimple and connected , as long as we are in the characteristic zero. (The remark there before Theorem 4.1 warns that the proof is more complicated for semisimple groups, but this is because of the positive characteristic cases. In these cases H has many finite subgroups, which in characteristic zero all of them lie in a proper subvariety, while in positive characteristic they do not). In fact the proof in [12] shows that the result holds for an open subset of $Spec(A)$.

Now, to get the non-connected case, we use Proposition A.3, to get that if H/H^o is cyclic, then there exists a finite cyclic group J such that $H = H^o \rtimes J$. We can assume J is inside $GL_n(K)$ where K is some number field, and we can replace A by KA, and use [12] Theorem 4.1 when this time we take a K-homomorphism from KA to k, a number field containing K. It is easy to see that different connected components give different cosets of $\varphi(\Gamma)^o$, as these cosets are represented by elements of J on which φ acts trivially. □

We are now ready to prove Proposition 5.1: Fix a connected component H_i, and assume $H = \langle H^o, H_i\rangle$. We can clearly choose $A_i \subset \mathbb{F}$ satisfying i and ii since Γ and $\mathbb{F}$ are finitely generated. Lemma 5.3 shows that we can arrange for φ_i for which $\tilde{\varphi}_i$ satisfies also iii. Moreover, this is so for an open subset of $Spec(KA)$ where K is the number field defined in the proof. Finally we recall that for every connected component H_i, $\Pi(H_i, \mathbb{F})$ is satisfies the following exact sequence:

$$1 \to \widetilde{W}(H_i, C) \to \Pi(H_i, C, \mathbb{F}) \to \mathrm{Gal}(\mathbb{F}_i^W/\mathbb{F}) \to 1,$$

where $\mathbb{F}_i^W$ is the fixed field of the inverse image of $\widetilde{W}(H_i, C)$, under the map $\phi_C : \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \to \Pi(H_i, C, \mathbb{F})$. Since $H = H^o \rtimes J$ for a finite cyclic group defined over K, we get that the action of every connected component on H^o is K-rational, and therefore it is the same on $\widetilde{H^o}, \widetilde{W}(\widetilde{H}^o)$, and in particular $\widetilde{W}(H_i) = \widetilde{W}(\widetilde{H_i})$. It is therefore left to show that there exists a specialization φ such that $\mathrm{Gal}(\mathbb{F}_i/\mathbb{F}) \simeq \mathrm{Gal}(k_i^W/k)$, where k_i is the fixed field of the inverse image of $\widetilde{W}(\widetilde{H}_i, \widetilde{\varphi}(C))$. We first notice that since φ is onto, any Cartan subgroup $\widetilde{C} < \widetilde{H}$ is the image of a Cartan subgroup $C < H$. Also, if $\mathbb{F}_C$ is the splitting of C which is the splitting field of a polynomial $f_C(T) \in \mathbb{F}[T]$, then the splitting field of $\varphi(f_C)(T) \in k[T]$ is the splitting field of $\widetilde{C}$, and if $\sigma \in \mathrm{Gal}(k_C/k)$ satisfies that $\phi_{\widetilde{C}}(\sigma) \in \widetilde{W}(H_i, \widetilde{C})$, then $\phi_C(\sigma) \in \widetilde{W}(H_i, C)$. In particular, if we denote by $f_i(T) \in \mathbb{F}[T]$ to be a polynomial such that its splitting field is $\mathbb{F}_i^W$, then the splitting field of $\varphi(f_i)(T) \in k[T]$ is k_i^W. Now, let S_i be the integral closure of A_i in F_i^W. By Lemma 5.2, there is a specialization of S_i onto a number field k, such that $\mathrm{Gal}(\mathbb{F}_i^W/\mathbb{F}) = \mathrm{Gal}(\varphi(S_i)/\varphi(A))$. Moreover, the set of such specializations is an Hilbertian set (cf. [4], ch. 12) and so Zariski dense, hence has a non trivial intersection with the set of specializations given by Lemma 5.3 which ensures that the Zariski closure of $\tilde{\varphi}(\Gamma)$ is isomorphic to H. Now for any fixed connected component H_i,

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \widetilde{W}(H_i, C) & \longrightarrow & \Pi(H_i, C, \mathbb{F}) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_i^W/\mathbb{F}) & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & \widetilde{W}(H_i, \widetilde{C}) & \longrightarrow & \Pi(H_i, \widetilde{C}, k) & \longrightarrow & \mathrm{Gal}(k_i^W/k) & \longrightarrow & 1
\end{array}$$

where all arrows from the bottom sequence above are induced by φ. By construction we get that all arrows are isomorphisms, and thus $\Pi(H_i, C, \mathbb{F}), \Pi(\widetilde{H}_i, \widetilde{C}, k)$ are isomorphic, and Proposition 5.1 is proven.

6. Examples and counter examples

In order to give a better understanding for the types of Galois groups constructed by Theorem 1.1, we give, in this section, some examples. We end this section with some counter examples to Theorem 1.1 for different types of groups and fields for which one of the conditions of Theorem 1.1 fails.

6.1. **Connected groups with Π larger than the Weyl group.** As a first example, we show how it can happen that the group H is connected, but $\Pi(H, \mathbb{F}) \neq W(H)$. Let $\mathbb{F} = \mathbb{Q}$, k a number field, and L its Galois closure. Let $\Gamma = Res^k_{\mathbb{Q}}(SL_n)(\mathbb{Z})$. Note that Γ is isomorphic to $SL_n(\mathcal{O}_k)$, where $\mathcal{O}_k$ is the ring of integers of k, but we take it as a subgroup of $SL_{nd}(\mathbb{Q})$. It is finitely generated, and its Zariski closure is H which over $\overline{\mathbb{Q}}$ is isomorphic to SL_n^d, where d is the degree of k over $\mathbb{Q}$. The splitting field of H is L, since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts transitively on the absolutely simple components of H, which are the SL_n components, and clearly H splits over L. We therefore get that $\Pi(H, \mathbb{Q}) = \langle S_n^d, \mathrm{Gal}(L/\mathbb{Q})\rangle \simeq S_n wr\, \mathrm{Gal}(L/\mathbb{Q})$. This example can be generalized by replacing SL_n with any other semisimple group G. In that case, $H = Res^k_{\mathbb{Q}}(G), \Gamma = H(\mathbb{Z})$, and we get that $\Pi(H, \mathbb{Q}) \simeq W(G) wr\, \mathrm{Gal}(L/\mathbb{Q})$.

6.2. **Non connected groups.**

6.2.1. *Groups with irreducible Dynkin diagram.* Let $H := SL_n \rtimes \langle\tau\rangle$, where τ is the automorphism of SL_n sending $A \mapsto (A^t)^{-1}$, and $\Gamma := H(\mathbb{Z})$. A representation $\rho : H \to GL_{2n}$ is given by

$$\rho(A) = \begin{pmatrix} A & 0 \\ 0 & (A^t)^{-1} \end{pmatrix}, \quad \rho(\tau) = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$$

In order to have a better understanding of $W(H^o\tau)$, we first give examples of two Cartan subgroups associated to $H^o\tau$. Since τ is of finite order, then it is contained in a Cartan subgroup. Let C_τ be such a group. Then C_τ^o is a maximal torus of $Z_{SL_n}(\tau) = SO(n)$. Notice that if $n = 2k+1$, then $W^\tau = W(SO(n)) \simeq (\mathbb{Z}/2\mathbb{Z})^k \rtimes S_k$, however if $n = 2k$, then W^τ is still isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k \rtimes S_k$, but $W(SO(n)) = (\mathbb{Z}/2\mathbb{Z})_0^k \rtimes S_k$, where the subscript stands for vectors with sum zero. For the second example, assume $n = 2k$ is even, and denote

$$J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

Again $J\tau$ is of finite order, and therefore contained in a Cartan subgroup. Denote $C_{J\tau}$ such a group. Again $C^o_{J\tau}$ is a maximal torus in $Z_{SL_n}(J\tau) = Sp_n$. Notice that the centralizers of $\tau, J\tau$ are of different types, however they are of the same rank, k, and $W^{J\tau} = W(Sp_n) = (\mathbb{Z}/2\mathbb{Z})^k \rtimes S_k$. By Lemma A.6, for the connected component $H^o\tau$, the Weyl group is $W(H^o\tau) = (T_C/(T^\tau))^\tau \rtimes W^\tau$ (notice that since H^o is simply connected $W(H^o\tau) = \widetilde{W}(H^o\tau)$). As mentioned, W^τ in this case is $W_k = (\mathbb{Z}/2\mathbb{Z})^k \rtimes S_k \simeq W(B_k) \simeq W(C_k)$, where $n = 2k$ if n is even or $n = 2k+1$ if n is odd, and $(T_C/(T^\tau))^\tau = (\mathbb{Z}/2\mathbb{Z})^r$, where $r = n-1-k$ is the difference between the ranks of the A_{n-1} type group and B_k type. We therefore get that for both cases ,n even or odd, $W(H^o\tau) = (\mathbb{Z}/2\mathbb{Z}) wr_\Omega W_k$, where Ω is a set of k signed pairs, and W_k acts on Ω in the standard way.

6.2.2. *Groups with reducible Dynkin diagram.* Let $H := SL_n^d \rtimes \langle\tau\rangle$, where τ is the automorphism that cyclicly permutes the SL_n factors, and $\Gamma := H(\mathbb{Z})$. A representation of $\rho : H \to GL_{nd}$ is given in a similar way to the previous example. Notice that this representation is in fact into $GL(\underbrace{V \oplus \cdots \oplus V}_{d \text{ times}})$ permuting the V factors, where V is n-dimensional. In particular, since $\rho(\tau)$ permutes the factors isomorphic to V cyclicly, we find that if λ is an eigenvalue of an element $\rho(A\tau)$, then $\lambda\zeta_d$ is also an eigenvalue for every ζ_d an d-th root of unity. In particular $\mathbb{Q}(\zeta_d)$ is contained in the splitting field of $H^o\tau$. The Weyl group in this case by a similar computation is $W(H^o\tau) = (\mathbb{Z}/d\mathbb{Z})^{n-1} \rtimes S_n$, and $\Pi(H^o\tau, \mathbb{Q}) = \langle W(H^o\tau), \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})\rangle$.

The situation can be described by the following diagram of tower of fields extensions:

$$\begin{array}{rc} & \mathbb{Q}(\gamma) \\ {\scriptstyle \mathrm{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q}(\gamma^d))\simeq(\mathbb{Z}/d\mathbb{Z})^{n-1}} & \Big| \\ & \mathbb{Q}(\gamma^d) \\ {\scriptstyle \mathrm{Gal}(\mathbb{Q}(\gamma^d)/\mathbb{Q}(\zeta_d))\simeq S_n} & \Big| \\ & \mathbb{Q}(\zeta_d) \\ {\scriptstyle \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})\simeq(\mathbb{Z}/d\mathbb{Z})^\times} & \Big| \\ & \mathbb{Q} \end{array}$$

6.3. **Counter examples.**

6.3.1. *Non semisimple groups.* Let $\Gamma := \langle A^{\pm 1}, J\rangle$, where

$$A = \begin{pmatrix} 2 & \\ & 3 \end{pmatrix}, \quad J = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$

Then $H = \overline{\Gamma} = \begin{pmatrix} * & \\ & * \end{pmatrix} \bigcup \begin{pmatrix} & * \\ * & \end{pmatrix}$. Let $\Sigma := \{A, A^{-1}, J, I_2\}$ be an admissible generating set, where I_2 is the identity element, and let X_k be the k-th step of the random walk generated by Σ. Notice that if $X_k = \begin{pmatrix} & a \\ b & \end{pmatrix} \notin H^o$, then $\mathbb{Q}(X_k) = \mathbb{Q}(\sqrt{ab})$. Also, if $X_k \notin H^o$, then if $X_k = A^{n_1} J A^{n_2} J \cdots = s_1 s_2 \cdots s_k \quad, s_i \in \Sigma$, then J must appear an odd number of times, and therefore, if k is even, ab is a square if and only if $N_I := |\{i : s_i = I\}|$ is odd, which occurs with probability $1/2 - (1/2)^n$. On the other hand, if k is odd, then ab is a square if and only if N_I is even which occurs with probability $1/2 - (1/2)^n$. In particular we get that

$$\lim_{k\to\infty} \mathbb{P}(\mathrm{Gal}(\mathbb{Q}(X_k)/\mathbb{Q}) = \Pi_1(H^o X_k)) = \frac{1}{2}$$
$$\lim_{k\to\infty} \mathbb{P}(\mathrm{Gal}(\mathbb{Q}(X_k)/\mathbb{Q}) = \Pi_2(H^o X_k)) = \frac{1}{2}$$

where

$$\Pi_1(H^o\gamma) = \begin{cases} \{1\} & H^o\gamma = H^o \\ \mathbb{Z}/2\mathbb{Z} & H^o\gamma \neq H^o \end{cases}, \quad \Pi_2(H^o\gamma) = \{e\}$$

That is, there is no typical behaviour for the non connected component.

6.3.2. *Not finitely generated fields.* In this example, we show that if the field $\mathbb{F}$ is not finitely generated, then again it is possible that there is no typical behaviour for the Galois groups. We prove the following:

Theorem 6.1. *Let $H := SL_n$, $n \geq 5$, $\Gamma := H(\mathbb{Z})$. Let Σ be a finite generating set of Γ, and let X_k be the corresponding random walk. Then for any pair of subgroups $\mathcal{G} = (G_1, G_2)$ of the alternating group $Alt(n)$ there exists an algebraic extension $\mathbb{F}_{\mathcal{G}}$ of $\mathbb{Q}$, and sequences $\{n_i(\mathcal{G})\}, \{k_i(\mathcal{G})\}$, such that*

$$\mathbb{P}(\mathrm{Gal}(\mathbb{F}_{\mathcal{G}}(X_{n_i(\mathcal{G})})/\mathbb{F}_{\mathcal{G}}) = G_1) \geq 1 - \frac{1}{2^i}$$
$$\mathbb{P}(\mathrm{Gal}(\mathbb{F}_{\mathcal{G}}(X_{k_i(\mathcal{G})})/\mathbb{F}_{\mathcal{G}}) = G_2) \geq 1 - \frac{1}{2^i}$$

In particular, this theorem shows that in this case, when the base field is not finitely generated, there is no generic behaviour.

Proof. Let $R_i = \{\sigma_{1,1}, \ldots, \sigma_{r_i,i}\}, i = 1, 2$ be a generating set of G_i. Without loss of generality we may assume $r_1 = r_2$, and therefore denote $|R_i| = r$. We will construct the field $\mathbb{F}_{\mathcal{G}}$ as a fixed field of Galois automorphisms $\sigma_1^{\mathcal{G}}, \ldots, \sigma_r^{\mathcal{G}} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $Q_{(2)}$ be the maximal pro-2 extension of $\mathbb{Q}$. Then for any $\gamma \in \Gamma$ such that $\mathrm{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q}) = S_n$, we have $\mathrm{Gal}(\mathbb{Q}_{(2)}(\gamma)/\mathbb{Q}_{(2)}) =$

A_n. Since A_n is simple, we get that $\mathbb{Q}_{(2)}(\gamma_1), \mathbb{Q}_{(2)}(\gamma_2)$ are linearly disjoint if and only if they are different.

Let $n_1 \in \mathbb{N}$ be chosen, by applying Theorem 1.1 such that

$$\mathbb{P}(\omega_{k_1} \in \{\gamma \in \Gamma : \mathrm{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q}) = S_n\}) > 1 - \frac{1}{2}$$

Let $F_{1,1}, \ldots, F_{1,N_1}$ be the finite set of fields occurring as splitting fields over $\mathbb{Q}$ of all possible $n_1 - th$ steps of the random walk with Galois group over isomorphic to S_n, and set F_1 to be their composite.

Let $k_1 \in \mathbb{N}$ be chosen by applying Theorem 1.1 such that

$$\mathbb{P}(\omega_{k_1} \in \{\gamma \in \Gamma : \mathrm{Gal}(F_1(\gamma)/F_1) = S_n\}) > 1 - \frac{1}{2}$$

Denote $E_{1,1}, \ldots, E_{1,M_1}$ the set of fields over $\mathbb{Q}$ occurring as splitting fields of all possible $k_1 - th$ step of the random walk (notice that the random walk itself did not change, only the base field) with Galois group over F_1 isomorphic to S_n, and set E_1 to be the composite of F_1 with these fields. Notice that these fields are linearly disjoint from $F_{1,1}, \ldots, F_{1,N_1}$ over $\mathbb{Q}$, and $\mathbb{Q}_{(2)}E_{1,1}, \ldots, \mathbb{Q}_{(2)}E_{1,M_1}$ are linearly disjoint from $\mathbb{Q}_{(2)}F_{1,1}, \ldots, \mathbb{Q}_{(2)}F_{1,N_1}$ over $\mathbb{Q}_{(2)}$.

We continue by induction: Let n_{i+1} be such that

$$\mathbb{P}(\omega_{k_1} \in \{\gamma \in \Gamma : \mathrm{Gal}(E_i(\gamma)/E_i) = S_n\}) > 1 - \frac{1}{2^{i+1}}$$

Let $F_{i+1,1}, \ldots, F_{i+1,N_{i+1}}$ be the set of fields which are splitting fields over $\mathbb{Q}$ of all $n_{i+1} - th$ step of the random walk with Galois group isomorphic to S_n. Let F_{i+1} be the composite of these fields with E_i. Continue as before to define k_{i+1}, $E_{i+1,1}, \ldots, E_{i+1,M_{i+1}}$, and E_{i+1}. Notice that at any step we add fields $F_{i,j}$ or $E_{i,j}$ that are linearly disjoint fields from the previous fields over $\mathbb{Q}$, since their Galois groups over F_i or E_i are isomorphic to S_n. Furthermore, when taking the composite of all fields with $\mathbb{Q}_{(2)}$, we get fields that are linearly disjoint over $\mathbb{Q}_{(2)}$. So all fields $\mathbb{Q}_{(2)}F_{i,j}$ and $\mathbb{Q}_{(2)}E_{i,j}$ are linearly disjoint over $\mathbb{Q}_{(2)}$. Also, by the construction of these fields, we have that

$$\mathbb{P}(\omega_{n_i} \in \{\gamma \in \Gamma : \exists 1 \le j \le N_i, \mathbb{Q}(\gamma) = F_{i,j}\}) > 1 - \frac{1}{2^i} \tag{23}$$

$$\mathbb{P}(\omega_{k_i} \in \{\gamma \in \Gamma : \exists 1 \le j \le M_i, \mathbb{Q}(\gamma) = E_{i,j}\}) > 1 - \frac{1}{2^i} \tag{24}$$

Define $\sigma_1^{\mathcal{G}}, \ldots, \sigma_r^{\mathcal{G}} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{(2)})$ in the following way: By construction we know that $\mathrm{Gal}(\mathbb{Q}_{(2)}F_{i,j}/\mathbb{Q}_{(2)}) \simeq \mathrm{Gal}(\mathbb{Q}_{(2)}E_{i,j}/\mathbb{Q}_{(2)}) \simeq Alt(n)$. We may therefore fix for any such field an isomorphism to $Alt(n)$, and consider $\sigma_{d,i} \in \mathrm{Gal}(\mathbb{Q}_{(2)}F_{i,j}/\mathbb{Q}_{(2)})$ (or $\mathrm{Gal}(\mathbb{Q}_{(2)}E_{i,j}/\mathbb{Q}_{(2)})$) for $d = 1, \ldots, r,\ i = 1, 2$. Since furthermore the fields $\mathbb{Q}_{(2)}F_{i,j}, \mathbb{Q}_{(2)}E_{i,j}$ are linearly disjoint over $\mathbb{Q}_{(2)}$ we can find $\sigma_d^{\mathcal{G}} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{(2)})$ such that $\sigma_d^{\mathcal{G}}|_{F_{i,j}} = \sigma_{d,1}, \forall i \in \mathbb{N}, j = 1, \ldots, N_i$, and $\sigma_d^{\mathcal{G}}|_{E_{i,j}} = \sigma_{d,2}, \forall i \in \mathbb{N}, j = 1, \ldots, M_i$. Set $F = \{x \in \overline{\mathbb{Q}} : \sigma_d^{\mathcal{G}}(x) = x\ \forall d = 1, \ldots, r\}$.

We claim now that for all $i \in \mathbb{N}, j = 1, \dots, N_i$, $\mathrm{Gal}(FF_{i,j}/F) \simeq G_1$, and similarly $\mathrm{Gal}(FE_{i,j}/F) \simeq G_2$. To see this notice that by the fundamental theorem of Galois theory, $\mathrm{Gal}(\overline{\mathbb{Q}}/F) = \langle \sigma_1^{\mathcal{G}}, \dots, \sigma_r^{\mathcal{G}} \rangle$, that is the closure of the group generated by $\sigma_1^{\mathcal{G}}, \dots, \sigma_r^{\mathcal{G}}$ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{(2)})$. Furthermore, $\mathrm{Gal}(FK/F) \simeq \langle \sigma_1^{\mathcal{G}}|_K, \dots, \sigma_r^{\mathcal{G}}|_K \rangle$ for any Galois field K. Since by definition of F, $\sigma_d^{\mathcal{G}}, d = 1, \dots, r$ acts trivially on F, the action of $\sigma_d^{\mathcal{G}}$ on $FF_{i,j}$ is determined by its action on $\mathbb{Q}_{(2)}F_{i,j}$, which was defined to be $\sigma_d^{\mathcal{G}}|_{\mathbb{Q}_{(2)}F_{i,j}} = \sigma_{d,1}$. We therefore get that $\mathrm{Gal}(FF_{i,j}/F) \simeq G_1$, and by the analogous computation, $\mathrm{Gal}(FE_{i,j}/F) \simeq G_2$. By (23),(24) the theorem is now proved. □

Appendix A. Cartan subgroups

In this appendix we list and prove some of the basic properties of Cartan subgroups, following the work of Mohrdieck in [14]. Throughout this section, the ground field is assumed to be algebraically closed. We recall the definition of a Cartan subgroup. Let G be a linear algebraic group with G^o reductive. A *Cartan subgroup* of G is a subgroup $C < G$ satisfying the following properties

(i) C is diagonalizable.
(ii) C/C^o is cyclic.
(iii) The index $[N_G(C) : C]$ is finite.

A.1. Basic properties.

In [14] §3, the following is proved

Proposition A.1. *Let G be as above.*

(i) *Let $h \in G$ be semisimple element. Then h is contained in a Cartan subgroup. In fact, the subgroup generated by S and h, where S is a maximal torus in $Z_{G^o}(h)^o$ is a Cartan subgroup.*
(ii) *Let $C < G$ be a Cartan subgroup, and let $h \in G$ be such that hC^o generates C/C^o. Then C^o is a maximal torus of $Z_{G^o}(h)^o$.*
(iii) *Let $C < G$ be a Cartan subgroup. Then C^o is a regular torus in G^o, that is $Z_{G^o}(C^o)$ is a maximal torus in G^o.*

Remark A.2. *Since $Z_{G^o}(C^o)$ is a maximal torus, T_C, of G^o, we get that the the intersection of C^o with the set of regular semisimple elements of G^o contains an open dense subset of C^o. To see this, let $A(T_C)$ be the finite set of roots of T_C. For $\alpha \in A(T_C)$, let $u_\alpha : \mathbb{G}_a \to G^o$ be a homomorphism satisfying*

$$tu_\alpha(x)t^{-1} = u_\alpha(\alpha(t)x), \quad t \in T_C, x \in \mathbb{G}_a$$

This shows that if $t \in \ker(\alpha)$, then there exists a unipotent element that commutes with it. Since C^o is irreducible, we find that if

$$C^o \subset \cup_{\alpha \in A(T_C)} \ker(\alpha)$$

then there exists $\alpha \in A(T_C)$ such that $C^o \in \ker(\alpha)$, in which case $Z_{G^o}(C^o)$ will contain a unipotent, and therefore can not be a torus. Since the set

$\cap_\alpha\{t \in T_C : \alpha(t) \neq 1\}$ is open, contains only semisimple regular elements, and has a non empty intersection with C^o, we get the result.

In the following we prove some properties of Cartan subgroups, generalizing the one proved in [14]. We first prove a structure result on non-connected algebraic groups.

Proposition A.3. *Let G be a linear algebraic group defined over a field $\mathbb{F}$, such that G/G^o is cyclic of order m. Assume $\mathrm{char}(\mathbb{F}) = 0$ or $(\mathrm{char}(\mathbb{F}), m) = 1$. Then for any coset G_i of G^o that generates G/G^o, there exists $x \in G_i$ such that $G = G^o \rtimes \langle x \rangle$.*

Proof. Let $y \in G_i$ be any elements in G_i. By definition $y^m \in G^o$, and so let $t \in G^o$ be an elements such that $t^m = y^m$ (to find such t write $y^m = y_u y_s$ according to the Jordan decomposition of y^m, and find t_u in the one parameter unipotent subgroup generated by y_u and t_s in a maximal torus containing y_s such that $t_u^m = y_u, t_s^m = y_s$. Notice that this is all possible by the assumption on $\mathrm{char}(\mathbb{F})$). Then t commutes with y, and $yt^{-1} \in G_i$ satisfies $\left(yt^{-1}\right)^m = e$, and the result follows. □

Proposition A.4. *Let G be a linear algebraic group, with G^o reductive. Let $C < G$ be a Cartan subgroup, and $h \in C$ semisimple such that hC^o generates C/C^o.*

(i) *There exist a maximal torus $T_h < G^o$ containing C^o, and a Borel subgroup $B_h < G^o$ containing T_h, both invariant under conjugation by h.*
(ii) *Let T be a maximal torus containing C^o, invariant under conjugation by h. Then for any $t \in T$, there exists $t' \in T$ such that $t'tht'^{-1} \in C^o h$*
(iii) *Let $g \in G^o h$ be a semisimple element. Then there exists $x \in G^o$ such that $x^{-1}gx \in C^o h$.*

Proof. For the first part, we consider T_h to be the maximal torus $Z_{G^o}(C^o)$, containing C^o, provided by Proposition A.1(iii). Let B' be a Borel subgroup of $Z_{G^o}(h)$ containing C^o. By corollary 7.4 in [20], it is contained in a Borel subgroup B of G^o, invariant under conjugation by h. Since $Z_B(C^o)$ is a maximal torus of G^o, it must coincide with T_h, and therefore we get the required result. For the second part, notice that since t and t' commute, it is equivalent to showing that $[t', h] \in t^{-1}C^o$. Consider the automorphism c_h of T/C^o via conjugation by h. Then $[t', h] = t'c_h(t'^{-1})$. By definition of C, C^o and h, we have that this automorphism has only finitely many fixed points (since any fixed point is a C^o -coset inside $N_G(C)$, and $[N_{G^o}(C) : C^o] < \infty$). Since T/C^o is connected, we can apply the Lang-Steinberg Theorem (Theorem 3.1 above), to get that the map $t' \mapsto t'c_h(t'^{-1})$ as a map from T/C^o to itself is onto, and therefore $t^{-1}C^o$ is in the image. For the last part: by Corollary 7.5 in [20] there exist a Borel subgroup B_g of G^o and a maximal torus $T_g < B_g$ of G^o both invariant under conjugation by

g. After conjugation by an element of G^o, we may have that $T_g = T_h$, and $B_g = B_h$. We therefore get that $gh^{-1} \in G^o$, preserving T_h and B_h and therefore $gh^{-1} \in T_h$ (since it preserves T_h, it is inside the normalizer of T_h and since it preserves a Borel subgroup B_h, it is a trivial element of the (classical) Weyl group $W(G^o, T_h)$). The last part is now a consequence of the second part of the proposition. □

With this proposition, we can now show that Cartan subgroups are conjugated by elements of G^o.

Corollary A.5. *Let G be as in Proposition A.1. Let $h, g \in G$, be semisimple elements such that $hg^{-1} \in G^o$, and let C_h, C_g be Cartan subgroups containing h, g respectively, such that $C_h^o h, C_g^o g$ generate $C_h/C_h^o, C_g/C_g^o$ respectively. Then there exist an element $x \in G^o$ such that $C_h = (C_g)^x$.*

Proof. By Proposition A.4 (iii), we get that there exists $x \in G^o$, such that $g^x \in C_h^o h$. Therefore, since C_h is a Cartan subgroup containing g^x, and C_h/C_h^o is generated by $C_h^o g^x$, by Proposition A.1, C_h^o is a maximal torus of $Z_{G^o}(g^x) = (Z_{G^o}(g))^x$, and therefore there exists $y \in Z_{G^o}(g)$ such that $\left(C_g^o\right)^{yx} = C_h^o$. We therefore have

$$C_h = \langle C_h^o, h\rangle = \langle C_h^o, g^x\rangle = \langle \left(C_g^o\right)^{yx}, g^{yx}\rangle = \langle C_g^o, g\rangle^{yx} = C_g^{yx}$$

which concludes the proof. □

Another property that we will exploit in this paper is the structure of the Weyl group $W(G_i, C)$ of a given Cartan subgroup. For this we need some notations. Let G be a semisimple linear algebraic group, G_i a fixed coset of G^o, and C a Cartan subgroup associated to G_i (see §2.2). Let $g \in G_i \cap C$ be a fixed element, and denote by c_g the automorphism of G^o of conjugation with g. As mentioned above, $T_C := Z_{G^o}(C^o)$ is a maximal torus of G^o. Denote $W := W(G^o, T_C)$ the Weyl group of G^o with respect to T_C, and denote by $W_C := \{w \in W : w^g = w\}$, where $\bullet^g$ denotes the action of g on W.

Lemma A.6. *Under the above notations we have the following split exact sequence*

$$1 \to (T_C/C^o)^g \to W(G_i, C) \to W_C \to 1 \tag{25}$$

where $(T_C/C^o)^g$ is the set of fixed points of the automorphism $c_g : T_C/C^o \to T_C/C^o$.

Proof. For every $n \in N_{G^o}(C)$ we have that $n \in N_{G^o}(T_C)$, and therefore we can define the maps

$$\phi : W(G_i, C) \to W(G^o, T_C) \quad \phi(nC^o) = nT_C$$

Assume $nC^o \in \ker\phi$, then $nT_C = T_C$, that is $n \in T_C$. Furthermore, $n \in N_{G^o}(C)$, and so $ngn^{-1} \in gC^o$, and therefore $c_g(nC^o) = nC^o$ showing that the sequence is left exact. For right exactness, let $n \in N_{G^o}(T_C)$ such that $gng^{-1} = nt$, for some $t \in T_C$, and hence $ngn^{-1} = nt$. By Proposition A.4

ii we may assume that $t \in C^o$. We therefore get that nT_C preserves $C^o g$. Furthermore, since $C^o = (Z_{T_C}(g))^o$, we find that $g^{-1}n^{-1}C^o ng = C^o$ and so nT_C preserves C, and thus the map $nC^o \mapsto nT_C$ is surjective onto W_C. To get that the map splits, we notice that if the map $nC^o \mapsto nT_C$ satisfies the splitting. To see this, notice that since $C^o = (Z_{T_C}(g))^o$, if $w \in W_C$ then w sends $C^o \mapsto C^o$, and $C^o g \mapsto C^o g$, and therefore $C \mapsto C$. In particular we get that the map $nT_C \mapsto nC^o$ is well defined, injective, and we get that the exact sequence splits. □

Corollary A.7. *Under the above notations, we have that* $W(G_i, C) = (T/C^o)^g \rtimes W_C$. *Furthermore,* $W_C < \widetilde{W}(G_i, C) = N_{G^o}(C)/Z_{G^o}(C)$.

This is an immediate corollary of Lemma A.6, and the fact that $Z_{G^o}(C) < T_C$.

A.2. **Regular semisimple elements in cosets.** For a connected linear reductive algebraic group G^o, an element $g \in G^o$ is called regular semisimple if its centralizer is a maximal torus, and henceforth it is contained in a unique maximal torus. It is known that the set of regular semisimple elements contains an open dense subset. In the following we show a similar result for non connected groups.

Definition A.8. *Let G be a linear algebraic group, with G^o reductive. We say that a semisimple element $g \in G$ is regular, if $(Z_{G^o}(g))^o$ is a torus.*

Notice that this definition generalizes the definition in the connected case, and that if $g \in G_i$, for some coset G_i, is regular, then by proposition A.1 (2), g is contained in a unique Cartan subgroup associated to G_i. We show now that most elements are regular semisimple.

Proposition A.9. *Let G be as above, G_i a coset of G^o, and $C < G$ a Cartan subgroup associated to G_i (as in* (1) *in Section 2.2).*

(i) *The set of regular semisimple elements in $C \cap G_i$ contains an open dense subset.*
(ii) *The set of regular semisimple elements in G_i contains an open dense subset.*

Proof. Recall that a diagonalizable linear algebraic group D, can be decomposed as $D \simeq D^o \times F$, where $F \simeq D/D^o$. Therefore there exists $\mu \in C \cap G_i$ such that $C \simeq C^o \times \langle\mu\rangle$. Furthermore, any element of $C \cap G_i$ is of the form $t\mu$, for $t \in C^o$. Denote by $n = \mathrm{ord}(\mu)$, and let

$$U_1 := \{t \in C^o : \ t^n \text{ is regular}\}$$

Then, $Z_{G^o}(t) = Z_{G^o}(t^n)$ for all $t \in U_1$. Notice also that by Remark A.2, U_1 contains an open dense subset of C^o. Let $t\mu \in U_1\mu$. Then

$$Z_{G^o}(t\mu) \subset Z_{G^o}(t^n\mu^n) = Z_{G^o}(t)$$

and therefore if $g \in (Z_{G^o}(t\mu))^o$, then $g \in (Z_{G^o}(t))^o$, and therefore $g \in (Z_{G^o}(\mu))^o$. Since $t \in U_1$ is regular semisimple, its centralizer is a maximal torus, and therefore $Z_{G^o}(t\mu)$ is diagonalizable, and its connected component is a torus, which proves part (1). To prove (2), we use the following morphism

$$\Phi : G^o/C^o \times C^o \to G_i \quad \Phi(gC^o, h) = gh\mu g^{-1}$$

Notice that the dimension of both sides is the same. Moreover, since by the definition of a Cartan subgroup it has a finite index in $N_{G^o}(C)$, this map is finite to one, and so the image of $G^o/C^o \times U$, where $U\mu$ is the set of regular semisimple in $C \cap G_i$, contains an open dense subset of G_i. □

Appendix B. k-Cartan subgroups and k-quasi irreducibility

Let k be a number field, and let G be an algebraic group defined over k. We say, as in Section 2.3, that a Cartan subgroup is a k-Cartan subgroup if C is defined over k, and that C/C^o is generated by $C^o g$, where $g \in C(k)$. As in Section 2.1, set k_C to be the splitting field of C. In [16] Prasad and Rapinchuk introduced the following definitions:

Definition B.1. *Let G^o be a connected semisimple linear algebraic group defined over a number field k, and let $G^o = G^{(1)} \cdots G^{(r)}$ be its decomposition into an almost direct product of connected normal k-almost simple groups.*

(i) *We say that an element is without component of finite order if for some (equivalently, any) decomposition $x = x_1 \cdots x_r$ with $x_i \in G^{(i)}$, all the x_i's have infinite order.*
(ii) *We say that a maximal torus $T < G$ is k-quasi-irreducible if whenever $T' < T$ is a k-subtorus of T, then T' is an almost direct product of a subset of $T^{(i)} := T \cap G^{(i)}, i = 1, \ldots, r$.*

In [16] Prasad and Rapinchuk proved that for a semisimple group, if T is a k-quasi-irreducible anisotropic maximal torus, then any element $x \in T$ without any component of finite order, generates a dense subgroup of T. Furthermore, they show that if the image of $\mathrm{Gal}(k_T/k)$ in the group $Aut(X(T))$, as defined in §2.1, contains the image of the Weyl group $W(G,T)$, then T is k-quasi irreducible anisotropic. In the following Lemma we generalize this result for non connected groups. Let G be a linear algebraic group defined over k, such that G^o is semisimple. Fix a coset G_i and denote by $G^o = G^1 \cdots G^l = G^{(1,i)} \cdots G^{(r,i)}$ where the product of $G^j, j = 1, \ldots, l$ is the minimal decomposition of G^o into k-simple normal subgroups and the product of $G^{(j,i)}, j = 1, \ldots, r$ is the decomposition of G^o into an almost direct product of k-normal subgroups invariant under conjugation by G_i.

Definition B.2. *Let G, G^o, G_i and k be as above. Denote $G^o = G^1 \cdots G^l = G^{(1,i)} \cdots G^{(r,i)}$ be the minimal decomposition as above. We say that*

(i) *A k-Cartan subgroup C associated to G_i is $G_i - k$ quasi irreducible if C^o has no k-subtori other than products of a subsets of $C^o \cap G^{(j,i)}, j = 1, \ldots, r$.*

(ii) *An element $x \in G^o$ is without G_i-component of finite order if for some (equivalently, any) decomposition $x = x_1 \cdots x_r$ with $x_i \in G^{(s,i)}, s = 1, \dots, r$, all the x_i's have infinite order.*

Following this definition we have the following generalization of the result in [16]:

Lemma B.3. *Let G be a linear algebraic group defined over a number field k, such that G^o is semisimple. Fix a coset G_i of G^o, and let $G^o = G^{(1,i)} \cdots G^{(r,i)}$ as above. Let C be a k-Cartan subgroup associated to G_i such that the image of $\mathrm{Gal}(k_C/k)$ in $Aut(X(C^o))$ contains the image of the Weyl group $W(G_i, C)$. Then C^o is $G_i - k$ quasi irreducible.*

Proof. Let $T_C = Z_{G^o}(C^o)$ be the unique maximal torus of G^o containing C^o, and let $R = R(G^o, T_C)$ be the root system of G^o with respect to T_C. For a k-simple normal subgroup G^j, let $G^j = G^j_1 \cdots G^j_{m_j}$ be its decomposition into absolutely almost simple subgroups, and let $R^j_s = R(G^j_s, T_C \cap G^j_s)$ be the corresponding root systems. Denote by $Y_T = X(T_C) \otimes_{\mathbb{Z}} \mathbb{Q}$, and $Y_C = X(C^o) \otimes_{\mathbb{Z}} \mathbb{Q}$. Let $g \in C \cap G_i(k)$ be an element such that gC^o generates C/C^o. Then $C^o = \left(T_C^g\right)^o$, the connected component of the fixed points of T_C under conjugation by g. The element g defines an automorphism of Y_T induced by the conjugation automorphism on T_C, which we denote also by g. Let V^j_s be the subspace of Y_T spanned by R^j_s, and $V^{(a,i)}$ the direct sum of V^j_s for $G^j < G^{(a,i)}, s = 1, \dots, m_j$. We claim that any subspace of Y_T which is invariant under $\mathrm{Gal}(k_C/k)$ and g is a sum of some $V^{(a,i)}$. Since C^o is a maximal torus in $(Z_{G^o}(g))^o$, we find that Y_C is the fixed points of Y_T under the g-action. Furthermore, notice that $\mathrm{Gal}(\overline{k}/k)$ acts on Y_C, and since C^o splits over k_C, the action factors through $\mathrm{Gal}(k_C/k)$. Let Δ be the Dynkin diagram of R, and let $\tau \in Aut(\Delta)$ be an automorphism such the action of g on T coincides with τ, and let $v \mapsto p(v) = \frac{1}{\mathrm{ord}(\tau)} \sum_{n=1}^{\mathrm{ord}(\tau)} \tau(v)$ be the projection from Y_T to Y_C. Then $p(R)$ is a root system of Y_C with Weyl group $W^\tau = \{w \in W(R) : w\tau = \tau w\}$ (cf. [1] Proposition 13.2.2). We can now finish the proof as in [16]: Since W^τ acts irreducibly on the irreducible components of $p(R)$, we get the same for $\mathrm{Gal}(k_C/k)$ which we assume contains $W(H_i, C) \supset W^\tau$. Furthermore, since for a fixed j, $\mathrm{Gal}(k_C/k)$ acts transitively on $G^{(j,i)}$, we find that any g-invariant subspace which is invariant under $\mathrm{Gal}(k_C/k)$ must be the sum of some of the $V^{(a,i)}$. Now if $C' \subset C$ is a k-subtorus of C^o, then it is in particular g-invariant, and therefore $\ker\left(res : X(C^o) \to X(C')\right) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a subspace of Y_T which is invariant under $\mathrm{Gal}(k_C/k)$ and g, and thus is of the form $\oplus_{a \in A} V^{(a,i)}, A \subset \{1, \dots, r\}$, and hence C' is an almost direct product of $C^o \cap G^{(a,i)}, a \notin A$. □

The following immediate corollary of this Lemma will allow us to reduce the question of splitting fields of elements into splitting fields of $G_i - k$ quasi irreducible Cartan subgroups.

Corollary B.4. *Let G, G_i and K be as in Lemma B.3, and assume C is a Cartan subgroup such that $W(G_i, C) \subset \mathrm{Gal}(k_C/K)$. Then for any regular semisimple $g \in G_i(k) \cap C(k)$ such that $g^{\mathrm{ord}(\tau)}$ has no G_i-components of finite order, the group generated by g is Zariski dense in C and, in particular, $\mathrm{Gal}(k(g)/k) = \mathrm{Gal}(k_C/k)$.*

References

[1] Roger W. Carter. *Simple groups of Lie type*. John Wiley & Sons, London-New York-Sydney, 1972. Pure and Applied Mathematics, Vol. 28. B

[2] Roger W. Carter. *Finite groups of Lie type*. Wiley Classics Library. John Wiley & Sons Ltd., Chichester, 1993. Conjugacy classes and complex characters, Reprint of the 1985 original, A Wiley-Interscience Publication. 3

[3] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original. 2.4

[4] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden. 5, 5, 5

[5] P. X. Gallagher. The large sieve and probabilistic Galois theory. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 91–101. Amer. Math. Soc., Providence, R.I., 1973. 1

[6] Alexander Gorodnik and Amos Nevo. Splitting fields of elements in arithmetic groups. *Math. Res. Lett.*, 18(06):1281–1288, 2011. 1

[7] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004. 4.1.2

[8] Florent Jouve. The large sieve and random walks on left cosets of arithmetic groups. *Comment. Math. Helv.*, 85(3):647–704, 2010. 1

[9] Florent Jouve, Emmanuel Kowalski, and David Zywina. Splitting fields of characteristic polynomials of random elements in arithmetic groups. To appear in Israel Journal of Mathematics, arxiv:1008.3662v2 [math.NT]. 1, 1, 1, 2.7, iii, 4.2

[10] Florent Jouve, Emmanuel Kowalski, and David Zywina. An explicit integral polynomial whose splitting field has Galois group $W(E_8)$. *J. Théor. Nombres Bordeaux*, 20(3):761–782, 2008. 1

[11] E. Kowalski. *The large sieve and its applications*, volume 175 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2008. 1, i

[12] Michael Larsen and Alexander Lubotzky. Normal subgroup growth of linear groups: the (G_2, F_4, E_8)-theorem. In *Algebraic groups and arithmetic*, pages 441–468. Tata Inst. Fund. Res., Mumbai, 2004. 5

[13] Alexander Lubotzky and Meiri Chen. Sieve methods in group I: powers in linear groups. J. Amer. Math. Soc., posted on April 11, 2012, PII S 0894-0347(2012)00736-X (to appear in print). 1, 1, 4.1.1, 4.8

[14] S. Mohrdieck. Conjugacy classes of non-connected semisimple algebraic groups. *Transform. Groups*, 8(4):377–395, 2003. 1, 1, 2.2, 2.2, A, A.1, A.1

[15] Madhav V. Nori. On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$. *Invent. Math.*, 88(2):257–275, 1987. iii

[16] Gopal Prasad and Andrei S. Rapinchuk. Existence of irreducible $\mathbb{R}$-regular elements in Zariski-dense subgroups. *Math. Res. Lett.*, 10(1):21–32, 2003. 1, 4, 4, B, B, B, B

[17] Gopal Prasad and Andrei S. Rapinchuk. Weakly commensurable arithmetic groups and isospectral locally symmetric spaces. *Publ. Math. Inst. Hautes Études Sci.*, (109):113–184, 2009. i

[18] Igor Rivin. Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms. *Duke Math. J.*, 142(2):353–379, 2008. 1, i

[19] Alireza Salehi Golsefidy and Péter P. Varjú. Expansion in perfect groups. arXiv:1108.4900. 1, 4.1

[20] Robert Steinberg. *Endomorphisms of linear algebraic groups.* Memoirs of the American Mathematical Society, No. 80. American Mathematical Society, Providence, R.I., 1968. 3, A.1

[21] Boris Weisfeiler. Strong approximation for Zariski-dense subgroups of semisimple algebraic groups. *Ann. of Math. (2)*, 120(2):271–315, 1984. iii

E-mail address: alexlub@math.huji.ac.il,rosenzwe@math.huji.ac.il