Universiteit
Leiden
The Netherlands

Enumerative arithmetic

Pagano, C.

Citation
Pagano, C. (2018, December 5). *Enumerative arithmetic*. Retrieved from https://hdl.handle.net/1887/67539

Version:	Not Applicable (or Unknown)
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/67539

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/67539 holds various files of this Leiden University dissertation.

Author: Pagano, C.
Title: Enumerative arithmetic
Issue Date: 2018-12-05

Enumerative arithmetic

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 5 december 2018
klokke 16:15 uur

door

Carlo Pagano

geboren te Napoli, Italië in 1990

Promotor: Prof. dr. Hendrik Lenstra

Samenstelling van de promotiecommissie:

Prof. dr. Aad van der Vaart (Universiteit Leiden)

Prof. dr. Bart de Smit (Universiteit Leiden)

Prof. dr. Tim Dokchitser (University of Bristol)

Prof. dr. Felipe Voloch (University of Canterbury, New Zealand)

Prof. dr. Melanie Matchett Wood (University of Wisconsin, USA)

Table of content

CHAPTER

1

On the equation $X_1 + X_2 = 1$ in finitely generated groups in positive characteristic

Peter Koymans, Carlo Pagano

On the equation $x_1 + x_2 = 1$ in finitely generated groups in positive characteristic

Peter Koymans, Carlo Pagano

1 Introduction

Let G be a subgroup of $\mathbb{C}^* \times \mathbb{C}^*$ with coordinatewise multiplication. Assume that the rank $\dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q} = r$ is finite. Beukers and Schlickewei [1] proved that the equation

$$x_1 + x_2 = 1$$

in $(x_1, x_2) \in G$ has at most 2^{8r+8} solutions. A key feature of their upper bound is that it depends only on r.

In this paper we will analyze the characteristic p case. To be more precise, let $p > 0$ be a prime number and let K be a field of characteristic p. Let G be a subgroup of $K^* \times K^*$ with $\dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q} = r$ finite. Then Voloch proved in [5] that an equation

$$ax_1 + bx_2 = 1 \text{ in } (x_1, x_2) \in G$$

for given $a, b \in K^*$ has at most $p^r(p^r + p - 2)/(p-1)$ solutions $(x_1, x_2) \in G$, unless $(a, b)^n \in G$ for some $n \geq 1$.

Voloch also conjectured that this upper bound can be replaced by one depending only on r. Our main theorem answers this conjecture positively.

Theorem 1.1. *Let K, G, r, a and b be as above. Suppose that there is no positive integer n with $\gcd(n, p) = 1$ such that $(a, b)^n \in G$. Then the equation*

$$ax_1 + bx_2 = 1 \text{ in } (x_1, x_2) \in G \tag{1}$$

has at most $31 \cdot 19^{r+1}$ solutions.

Our main theorem will be a consequence of the following theorem.

Theorem 1.2. *Let K be a field of characteristic $p > 0$ and let G be a finitely generated subgroup of $K^* \times K^*$ of rank r. Then the equation*

$$x_1 + x_2 = 1 \text{ in } (x_1, x_2) \in G \tag{2}$$

has at most $31 \cdot 19^r$ solutions (x_1, x_2) satisfying $(x_1, x_2) \notin G^p$.

Clearly, the last condition is necessary to guarantee finiteness. Indeed if we have any solution to $x_1 + x_2 = 1$, then we get infinitely many solutions $x_1^{p^k} + x_2^{p^k} = 1$ for $k \in \mathbb{Z}_{\geq 0}$ due to the Frobenius operator.

The set-up of the paper is as follows. We start by introducing the basic theory about valuations that is needed for our proofs. Then we derive Theorem 1.2 by

generalizing the proof of Beukers and Schlickewei [1] to positive characteristic. We remark that their proof heavily relies on techniques from diophantine approximation. Most of the methods from diophantine approximation can not be transferred to positive characteristic, so that this is possible with the method of Beukers and Schlickewei is a surprising feat on its own. It was more convenient for us to follow [2], which is directly based on the proof of Beukers and Schlickewei. Theorem 1.1 is a simple consequence of Theorem 1.2.

2 Valuations and heights

Our goal in this section is to recall the basic theory about valuations and heights without proofs. To prove Theorem 1.2 we may assume without loss of generality that $K = \mathbb{F}_p(G)$. Thus, K is finitely generated over $\mathbb{F}_p$. Note that Theorem 1.2 is trivial if K is algebraic over $\mathbb{F}_p$, so from now on we further assume that K has positive transcendence degree over $\mathbb{F}_p$. The algebraic closure of $\mathbb{F}_p$ in K is a finite field, which we denote by $\mathbb{F}_q$. Then there is an absolutely irreducible, normal projective variety V defined over $\mathbb{F}_q$ such that its function field $\mathbb{F}_q(V)$ is isomorphic to K.

Fix a projective embedding of V such that $V \subseteq \mathbb{P}^M_{\mathbb{F}_q}$ for some positive integer M. A prime divisor $\mathfrak{p}$ of V over $\mathbb{F}_q$ is by definition an irreducible subvariety of V of codimension one. Recall that for a prime divisor $\mathfrak{p}$ the local ring $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring, since V is non-singular in codimension one. Following [3] we will define heights on V. To do this, we start by defining a set of normalized discrete valuations

$$M_K := \{\mathrm{ord}_\mathfrak{p} : \mathfrak{p} \text{ prime divisor of } V\},$$

where $\mathrm{ord}_\mathfrak{p}$ is the normalized discrete valuation of K corresponding to $\mathcal{O}_\mathfrak{p}$. If $v = \mathrm{ord}_\mathfrak{p} \in M_K$, we define for convenience $\deg v := \deg \mathfrak{p}$ with $\deg \mathfrak{p}$ being the projective degree in $\mathbb{P}^M_{\mathbb{F}_q}$. Then the set M_K satisfies the sum formula

$$\sum_{v \in M_K} v(x) \deg v = 0$$

for $x \in K^*$. This is indeed a well-defined sum, since for $x \in K^*$ there are only finitely many valuations v satisfying $v(x) \neq 0$. Furthermore, we have $v(x) = 0$ for all $v \in M_K$ if and only if $x \in \mathbb{F}_q^*$. If P is a point in $\mathbb{A}^{n+1}(K) \setminus \{0\}$ with coordinates $(y_0, \dots, y_n)$ in K, then its homogeneous height is

$$H_K^{\mathrm{hom}}(P) = -\sum_{v \in M_K} \min_i\{v(y_i)\} \deg v$$

and its height

$$H_K(P) = H_K^{\mathrm{hom}}(1, y_0, \dots, y_n).$$

We will need the following properties of the height.

Lemma 2.1. *Let $P \in \mathbb{A}^{n+1}(K) \setminus \{0\}$. The height defined above has the following properties:*
1) $H_K^{hom}(\lambda P) = H_K^{hom}(P)$ for $\lambda \in K^*$.
2) $H_K^{hom}(P) \geq 0$ with equality if and only if $P \in \mathbb{P}^n(\mathbb{F}_q)$.

3 Proof of Theorem 1.1.2

This section is devoted to the proof of Theorem 1.2. We will follow the proof in [2], see Section 6.4, with some crucial modifications to take care of the presence of the Frobenius map. The general strategy of the proof in characteristic 0, and how we adapt it to characteristic p, will be explained after Lemma 3.9. Let us start with a simple lemma.

Lemma 3.1. *The equation*

$$x_1 + x_2 = 1 \text{ in } (x_1, x_2) \in G \tag{3}$$

has at most p^r solutions (x_1, x_2) satisfying $x_1 \notin K^p$ and $x_2 \notin K^p$.

Proof. Let $x = (x_1, x_2)$ and $y = (y_1, y_2)$ be two solutions of (3). We claim that $x \equiv y \mod G^p$ implies $x = y$. Indeed, if $x \equiv y \mod G^p$, we can write $y_1 = x_1\gamma^p$ and $y_2 = x_2\delta^p$ with $(\gamma, \delta) \in G$. In matrix form this means that

$$\begin{pmatrix} 1 & 1 \\ \gamma^p & \delta^p \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

For convenience we define

$$A := \begin{pmatrix} 1 & 1 \\ \gamma^p & \delta^p \end{pmatrix}.$$

If A is invertible, we find that $x_1, x_2 \in K^p$ contrary to our assumptions. So A is not invertible, which implies that $\gamma = \delta = 1$. This proves the claim.

The claim implies that the number of solutions is at most $|G/G^p|$. Let $\mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_p$ in K. It is a finite extension of $\mathbb{F}_p$, since K is finitely generated over $\mathbb{F}_p$. It follows that $G^{\text{tors}} \subseteq \mathbb{F}_q^* \times \mathbb{F}_q^*$. Hence $|G^{\text{tors}}| \mid (q-1)^2$, which is co-prime to p. We conclude that $|G/G^p| = p^r$ as desired. □

Lemma 3.1 gives the following corollary.

Corollary 3.2. *The equation*

$$x_1 + x_2 = 1 \text{ in } (x_1, x_2) \in G \tag{4}$$

has at most p^r solutions (x_1, x_2) satisfying $(x_1, x_2) \notin G^p$.

Proof. Define

$$G' := \{(x_1, x_2) \in K \times K : (x_1^N, x_2^N) \in G \text{ for some } N \in \mathbb{Z}_{>0}\}.$$

It is a well known fact that G' is finitely generated if G and K are. It follows that G' is a finitely generated group of rank r. Our goal is to give an injective map from the solutions $(x_1, x_2) \in G$ of (4) satisfying $(x_1, x_2) \notin G^p$ to the solutions $(x_1', x_2') \in G'$ of (3) satisfying $(x_1', x_2') \notin K^p$ and then apply Lemma 3.1.

So let $(x_1, x_2) \in G$ be a solution of (4) satisfying $(x_1, x_2) \notin G^p$. We start by remarking that $x_1, x_2 \notin \mathbb{F}_q$. Hence we can repeatedly take p-th roots until we get $x_1', x_2' \notin K^p$. Using heights one can prove that this indeed stops after finitely many steps. Then it is easily verified that $(x_1', x_2') \in G'$ is a solution of (3) and that the map thus defined is injective. Now apply Lemma 3.1. □

By Corollary 3.2 we may assume that p is sufficiently large throughout, say $p > 7$. Both the proof in [2] and our proof rely on very special properties of the family of binary forms $\{W_N(X,Y)\}_{N\in\mathbb{Z}_{>0}}$ defined by the formula

$$W_N(X,Y) = \sum_{m=0}^{N} \binom{2N-m}{N-m}\binom{N+m}{m} X^{N-m}(-Y)^m.$$

We have for all positive integers N that $W_N(X,Y) \in \mathbb{Z}[X,Y]$. Furthermore, setting $Z = -X - Y$, the following statements hold in $\mathbb{Z}[X,Y]$.

Lemma 3.3. *1)* $W_N(Y,X) = (-1)^N W_N(X,Y)$.
2) $X^{2N+1}W_N(Y,Z) + Y^{2N+1}W_N(Z,X) + Z^{2N+1}W_N(X,Y) = 0$.
3) There exist a non-zero integer c_N *such that*

$$det\begin{pmatrix} Z^{2N+1}W_N(X,Y) & Y^{2N+1}W_N(Z,X) \\ Z^{2N+3}W_{N+1}(X,Y) & Y^{2N+3}W_{N+1}(Z,X)\end{pmatrix} = c_N(XYZ)^{2N+1}(X^2+XY+Y^2).$$

Proof. This is Lemma 6.4.2 in [2], which is a variant of Lemma 2.3 in [1]. □

Since the formulas in the previous lemma hold in $\mathbb{Z}[X,Y]$ they hold in every field K. But if $\mathrm{char}(K) = p > 0$ and $p \mid c_N$, then part 3) of Lemma 3.3 tells us that

$$det\begin{pmatrix} Z^{2N+1}W_N(X,Y) & Y^{2N+1}W_N(Z,X) \\ Z^{2N+3}W_{N+1}(X,Y) & Y^{2N+3}W_{N+1}(Z,X)\end{pmatrix} = 0$$

in $K[X,Y]$. The following remarkable identity will be handy later on, when we need that c_N does not vanish modulo p.

Lemma 3.4. *For every positive integer* N*, one has* $W_N(2,-1) = 4^N\binom{\frac{3}{2}N}{N}$.

Proof. It is enough to evaluate $\sum_{i=0}^{N}\binom{2N-i}{N}\binom{N+i}{N}2^{-i}$. We have

$$\sum_{i=0}^{N}\binom{2N-i}{N}\binom{N+i}{N}2^{-i} = \binom{2N}{N}F\left(-N, N+1, -2N, \frac{1}{2}\right),$$

where $F(a,b,c,z)$ is the hypergeometric function defined by the power series $F(a,b,c,z) := \sum_{i=0}^{\infty}\frac{(a)_i(b)_i}{i!(c)_i}z^n$. Here we define for a real t and a non-negative integer i $(t)_i = 1$ if $i = 0$ and for i positive $(t)_i = t(t+1)\cdot\ldots\cdot(t+i-1)$. Now the desired result follows from Bailey's formulas where special values of the function F are expressed in terms of values of the Γ-function, see [4] page 297. □

We obtain the following corollary.

Corollary 3.5. *Let* p *be an odd prime number and let* N *be a positive integer with* $N < \frac{p}{3} - 2$*. Then* $c_N \not\equiv 0$ *mod* p.

Proof. Indeed one has that

$$det\begin{pmatrix} Z^{2N+1}W_N(X,Y) & Y^{2N+1}W_N(Z,X) \\ Z^{2N+3}W_{N+1}(X,Y) & Y^{2N+3}W_{N+1}(Z,X)\end{pmatrix}$$

evaluated at $(X,Y,Z) = (2,-1,-1)$ gives up to sign $2W_N(2,-1)W_{N+1}(2,-1)$. By the previous proposition, this is a power of 2 times the product of two binomial coefficients whose top terms are less than p, hence it can not be divisible by p. □

We now state and prove the analogues of Lemmata 6.4.3-6.4.5 from [2] for function fields of positive characteristic. These are variants of respectively Lemma 2.1, Corollary 2.2 and Lemma 2.3 from [1].

Lemma 3.6. *Let a, b, c be non-zero elements of K, and let $(\alpha_i, \beta_i, \gamma_i)$ for $i = 1, 2$ be two K-linearly independent vectors from K^3 such that $a\alpha_i + b\beta_i + c\gamma_i = 0$ for $i = 1, 2$. Then*

$$H_K^{hom}(a, b, c) \leq H_K^{hom}(\alpha_1, \beta_1, \gamma_1) + H_K^{hom}(\alpha_2, \beta_2, \gamma_2).$$

Proof. The vector (a, b, c) is K-proportional to the vector $(\beta_1\gamma_2 - \gamma_1\beta_2, \gamma_1\alpha_2 - \alpha_1\gamma_2, \alpha_1\beta_2 - \beta_1\alpha_2)$. So we have

$$\begin{aligned} H_K^{\hom}(a, b, c) &= H_K^{\hom}(\beta_1\gamma_2 - \gamma_1\beta_2, \gamma_1\alpha_2 - \alpha_1\gamma_2, \alpha_1\beta_2 - \beta_1\alpha_2) \\ &= \sum_{v \in M_K} -\min(v(\beta_1\gamma_2 - \gamma_1\beta_2), v(\gamma_1\alpha_2 - \alpha_1\gamma_2), v(\alpha_1\beta_2 - \beta_1\alpha_2)) \deg v \\ &\leq \sum_{v \in M_K} -\min(v(\beta_1), v(\gamma_1), v(\alpha_1)) \deg v + \sum_{v \in M_K} -\min(v(\gamma_2), v(\alpha_2), v(\beta_2)) \deg v \\ &= H_K^{\hom}(\alpha_1, \beta_1, \gamma_1) + H_K^{\hom}(\alpha_2, \beta_2, \gamma_2), \end{aligned}$$

which was the claimed inequality. □

We apply Lemma 3.6 to the equation $x_1 + x_2 = 1$.

Lemma 3.7. *Suppose $x = (x_1, x_2) \in G$ and $y = (y_1, y_2) \in G$ satisfy $x_1 + x_2 = 1$ and $y_1 + y_2 = 1$. Then we have $H_K(x) \leq H_K(yx^{-1})$.*

Proof. Apply Lemma 3.6 with $(a, b, c) = (x_1, x_2, -1)$, $(\alpha_1, \beta_1, \gamma_1) = (1, 1, 1)$, $(\alpha_2, \beta_2, \gamma_2) = (y_1x_1^{-1}, y_2x_2^{-1}, 1)$ and use the fact that $H_K^{\hom}(1, 1, 1) = 0$. □

The next Lemma takes advantage of the properties of $W_N(X, Y)$ listed in Lemma 3.3 and the non-vanishing of c_N modulo p obtained in Corollary 3.5.

Lemma 3.8. *Let x, y be as in Lemma 3.7. Let $N < \frac{p}{3} - 2$. Then there exists $M \in \{N, N + 1\}$ such that $H_K(x) \leq \frac{1}{M+1} H_K(yx^{-2M-1})$.*

Proof. The proof is almost the same as in Lemma 6.4.5 in [2], with only few necessary modifications. For completeness we give the full proof.

If x_1, and thus both x_1 and x_2 are roots of unity, we have that $H_K(x) = 0$ so the lemma is trivially true. By Lemma 3.3 part 2) we get that

$$x_1^{2M+1} W_M(x_2, -1) + x_2^{2M+1} W_M(-1, x_1) - W_M(x_1, x_2) = 0$$

for $M \in \{N, N + 1\}$ as well as

$$x_1^{2M+1}(y_1x_1^{-2M-1}) + x_2^{2M+1}(y_2x_2^{-2M-1}) - 1 = 0.$$

Now we claim that there is $M \in \{N, N + 1\}$ such that the vectors

$$(y_1, y_2, -1) \text{ and } ({x_1}^{2M+1} W_M(x_2, -1), {x_2}^{2M+1} W_M(-1, x_1), -W_M(x_1, x_2)) \qquad (5)$$

are linearly independent. Clearly, to prove the claim it is enough to prove that the two vectors

$$(x_1^{2M+1}W_M(x_2,-1), x_2^{2M+1}W_M(-1,x_1), -W_M(x_1,x_2)) \quad (M \in \{N, N+1\}) \quad (6)$$

are linearly independent. But we know that for $M \in \{N, N+1\}$ we have that $c_M \not\equiv 0 \bmod p$ by Corollary 3.5 and the assumption that $N < \frac{p}{3} - 2$. Furthermore, x_1 and x_2 are not algebraic over $\mathbb{F}_p$. Thus the identity Lemma 3.3 part 3) gives us the non-vanishing of the first 2×2 minor of the vectors in 6, which proves the claimed independence. So by applying to (5) the diagonal transformation that divides the first coordinate by x_1^{2M+1} and the second by x_2^{2M+1}, we deduce that the two vectors

$$(y_1 x_1^{-2M-1}, y_2 x_2^{-2M-1}, -1)$$

and

$$(W_M(x_2,-1), W_M(-1,x_1), -W_M(x_1,x_2)) =: (w_1, w_2, w_3)$$

are linearly independent. So by Lemma 3.6 we get that

$$(2M+1)H_K(x) \leq H_K(yx^{-2M-1}) + H_K^{\hom}(w_1, w_2, w_3)$$

But now the inequality

$$H_K^{\hom}(w_1, w_2, w_3) \leq M \cdot H_K(x)$$

follows immediately from the non-archimedean triangle inequality. So we indeed get

$$(M+1)H_K(x) \leq H_K(yx^{-2M-1}),$$

completing the proof. □

Define

$$\mathrm{Sol}(G) := \{(x_1, x_2) \in G \setminus G^{\mathrm{tors}} : x_1 + x_2 = 1\}$$

and

$$\text{Prim-Sol}(G) := \{(x_1, x_2) \in G \setminus G^p : x_1 + x_2 = 1\}.$$

It is easily seen that $\text{Prim-Sol}(G) \subseteq \mathrm{Sol}(G)$. Finally define

$$S := \{v \in M_K : \text{ there is } (x_1, x_2) \in G \text{ with } v(x_1) \neq 0 \text{ or } v(x_2) \neq 0\}.$$

The set S is clearly finite. Write $s := |S|$, $S = \{v_1, \ldots, v_s\}$. Then we have a homomorphism $\varphi : G \to \mathbb{Z}^s \times \mathbb{Z}^s \subseteq \mathbb{R}^s \times \mathbb{R}^s$ defined by sending $(g_1, g_2) \in G$ to

$$(v_1(g_1)\deg v_1, \ldots, v_s(g_1)\deg v_s, v_1(g_2)\deg v_1, \ldots, v_s(g_2)\deg v_s).$$

Note that $\varphi(G)$ is a subgroup of $\mathbb{Z}^s \times \mathbb{Z}^s$ of rank r.

Let $u, v \in \mathrm{Sol}(G)$ be such that $\varphi(u) = \varphi(v)$. Suppose that $u \neq v$. Then Lemma 3.7 implies that $H_K(u) \leq 0$. Hence by Lemma 2.1 part 2) it follows that u and thus v are in G^{tors}. This implies that the restriction of φ to $\mathrm{Sol}(G)$ is injective. In particular the restriction of φ to $\text{Prim-Sol}(G)$ is injective. We now call $\mathcal{S} := \varphi(\mathrm{Sol}(G))$ and $\mathcal{PS} := \varphi(\text{Prim-Sol}(G))$. To prove Theorem 1.2 it suffices to bound the cardinality of $\mathcal{PS}$.

Let $||\cdot||$ be the norm on $\mathbb{R}^s \times \mathbb{R}^s$ that is the average of the $||\cdot||_1$ norms on $\mathbb{R}^s$. More precisely, we define for $u = (u_1, u_2) \in \mathbb{R}^s \times \mathbb{R}^s$

$$||u|| = \frac{1}{2}(||u_1|| + ||u_2||).$$

We now state the most important properties of $\mathcal{S}$.

Lemma 3.9. *The set $\mathcal{S} \subseteq \mathbb{Z}^s \times \mathbb{Z}^s$ has the following properties:*
1) For any two distinct $u, v \in \mathcal{S}$, we have that $||u|| \leq 2||v - u||$.
2) For any two distinct $u, v \in \mathcal{S}$ and any positive integer N such that $N < \frac{p}{3} - 2$, there is $M \in \{N, N+1\}$ such that $||u|| \leq \frac{2}{M+1}||v - (2M+1)u||$.
3) $p\mathcal{S} \subseteq \mathcal{S}$.

Proof. Let $x = (x_1, x_2) \in G$. By construction we have

$$||\varphi(x)|| = H_K^{\mathrm{hom}}(1, x_1) + H_K^{\mathrm{hom}}(1, x_2).$$

Note the basic inequalities

$$H_K^{\mathrm{hom}}(x_1, x_2) \leq H_K^{\mathrm{hom}}(1, x_1) + H_K^{\mathrm{hom}}(1, x_2) \leq 2H_K^{\mathrm{hom}}(x_1, x_2).$$

It is now clear that Lemma 3.7 implies part 1) and Lemma 3.8 implies part 2). Finally, part 3) is due to the action of the Frobenius operator. □

Denote by V the real span of $\varphi(G)$. Then V is an r-dimensional vector space over $\mathbb{R}$. We will keep writing $||\cdot||$ for the restriction of $||\cdot||$ to V.

Recall that our goal is to bound $|\mathcal{PS}|$. We sketch the ideas behind our strategy here. Let us first describe the strategy in characteristic 0 as used in [1] and [2]. In their work the set $\mathcal{S}$ satisfies part 1) of Lemma 3.9 and part 2) of Lemma 3.9 without the condition $N < \frac{p}{3} - 2$.

To finish the proof, they subdivide the vector space V in B^r cones for some absolute constant B. In each cone one can use part 1) of Lemma 3.9 to show that two distinct points $u, v \in \mathcal{S}$ are not too close. But part 2) of Lemma 3.9 shows that inside the same cone two points $u, v \in \mathcal{S}$ can not be too far apart. Together with a lower bound for the height of $u, v \in \mathcal{S}$, this proves that there are at most finitely many points $u \in \mathcal{S}$, say A, in each cone. Hence we get an upper bound of the shape $A \cdot B^r$.

Now we describe how to modify this to characteristic p. Again we subdivide V in B^r cones for some absolute constant B. From now on we only consider points $u \in \mathcal{PS}$ inside a fixed cone C. Our goal is to show that there are at most A points $u \in \mathcal{PS} \cap C$, where A is an absolute constant. It follows that then all points $v \in \mathcal{S} \cap C$ are of the shape $v = p^k u$ for $u \in \mathcal{PS}$ and $k \in \mathbb{Z}_{\geq 0}$.

Part 1) of Lemma 3.9 tells us that two distinct points $u, v \in \mathcal{PS}$ are not too close. Using part 3) of Lemma 3.9 we can multiply two points $u, v \in \mathcal{PS}$ with a power of p in such a way that the then obtained $u', v' \in \mathcal{S}$ satisfy $1 \leq \frac{||u'||}{||v'||} \leq \sqrt{p}$. Then we are in the position to apply part 2) of Lemma 3.9, which shows that $||u'||$ and $||v'||$ are not too far apart. This allows us to deduce that $\mathcal{PS} \cap C$ contains at most A points.

The following lemma subdivides the vector space V in B^r cones for some absolute constant B.

Lemma 3.10. *Given a positive real number θ, one can find a set $\mathcal{E} \subseteq \{u \in V : ||u|| = 1\}$ satisfying*
1) $|\mathcal{E}| \leq (1 + \frac{2}{\theta})^r$,
2) for all $0 \neq u \in V$ there exists $e \in \mathcal{E}$ satisfying $||\frac{u}{||u||} - e|| \leq \theta$.

Proof. See Lemma 6.3.4 in [2], which is an improvement of Corollary 3.8 in [1]. □

Let $\theta \in (0, \frac{1}{9})$ be a parameter and fix a corresponding choice of a set $\mathcal{E}$ satisfying the above properties. Given $e \in \mathcal{E}$, we define the cone

$$\mathcal{S}_e := \left\{ u \in \mathcal{S} : \left|\left| \frac{u}{||u||} - e \right|\right| \leq \theta \right\}, \ \mathcal{PS}_e := \mathcal{S}_e \cap \mathcal{PS}.$$

Fix $e \in \mathcal{E}$. We proceed to bound $|\mathcal{PS}_e|$. We start by deducing a so-called gap principle from part 1) of Lemma 3.9.

Lemma 3.11. *Let u_1, u_2 be distinct elements of $\mathcal{S}_e$, with $||u_2|| \geq ||u_1||$. Then $||u_2|| \geq \frac{3-\theta}{2+\theta}||u_1||$.*

Proof. Write $\lambda_i := ||u_i||$ for $i = 1, 2$. Then we have $u_i = \lambda_i e + u_i'$ where $||u_i'|| \leq \theta\lambda_i$, by definition of $\mathcal{S}_e$. Part 1) of Lemma 3.9 gives

$$\lambda_1 \leq 2||(\lambda_2 - \lambda_1)e + (u_2' - u_1')|| \leq 2(\lambda_2 - \lambda_1) + \theta(\lambda_2 + \lambda_1),$$

and after dividing by λ_1 we get that

$$1 \leq 2\left(\frac{\lambda_2}{\lambda_1} - 1\right) + \theta\left(\frac{\lambda_2}{\lambda_1} + 1\right).$$

This can be rewritten as $\frac{3-\theta}{2+\theta} \leq \frac{\lambda_2}{\lambda_1}$. □

From part 2) of Lemma 3.9 we can deduce the following crucial Lemma.

Lemma 3.12. *Let u_1, u_2 be distinct elements of $\mathcal{S}_e$. Suppose that $\frac{||u_2||}{||u_1||} < \frac{2}{3}p - 3$. Then $\frac{||u_2||}{||u_1||} \leq \frac{10}{\theta}$.*

Proof. We follow the proof of Lemma 6.4.9 of [2] part (ii) with a few modifications. For completeness we write out the full proof.

Again define $\lambda_i = ||u_i||$ and $u_i' = u_i - \lambda_i e$, for $i = 1, 2$. Assume that $\lambda_2 \geq \frac{10}{\theta}\lambda_1$. Let N be the positive integer with $2N+1 \leq \frac{\lambda_2}{\lambda_1} < 2N+3$. Then $2N+1 < \frac{2}{3}p-3$ and hence $N < \frac{p}{3} - 2$. Applying part 2) of Lemma 3.9 gives an integer $M \in \{N, N+1\}$ satisfying

$$\lambda_1 \leq \frac{2}{M+1}||(\lambda_2 - (2M+1)\lambda_1)e + u_2' - (2M+1)u_1'||.$$

Furthermore, we have that

$$|\lambda_2 - (2M+1)\lambda_1| \leq 2\lambda_1$$

and $M > \frac{4}{\theta}$ from the assumption $\lambda_2 \geq \frac{10}{\theta}\lambda_1$. Hence

$$\lambda_1 \leq \frac{2}{M+1}||(\lambda_2 - (2M+1)\lambda_1)e + u_2' - (2M+1)u_1'|| \leq \frac{2}{M+1}(2\lambda_1 + \lambda_2\theta + (2M+1)\lambda_1\theta)$$
$$\leq \frac{2}{M+1}(2 + (4M+4)\theta)\lambda_1 = \left(\frac{4}{M+1} + 8\theta\right)\lambda_1 < 9\theta\lambda_1.$$

It follows that $\lambda_1 < \frac{1}{1-9\theta}$. Now observe that for any non-negative integer h the elements $p^h u_1, p^h u_2$ of $\mathcal{S}_e$ satisfy all the assumptions made so far. We conclude that also $p^h \lambda_1 < \frac{1}{1-9\theta}$ for every non-negative integer h, which implies that $||u_1|| = 0$. This contradicts the fact that $u_1 \in \mathcal{S}_e$, completing the proof. □

Remark 3.13. In characteristic 0, the analogue of Lemma 3.12 holds only when both u_1, u_2 have norms at least $\frac{1}{1-9\theta}$. Then one deals with the remaining points in $\mathcal{S}_e$ by using the analogue of part 1) of Lemma 3.9, together with a separate argument to deal with the "very small" solutions. In characteristic p, it is because of the additional tool given by the action of Frobenius that the condition that u_1, u_2 have norm at least $\frac{1}{1-9\theta}$ has disappeared.

Assume without loss of generality that $\mathcal{PS}_e$ is not empty, and fix a choice of $u_0 \in \mathcal{PS}_e$ with $||u_0||$ minimal. For any $u \in \mathcal{PS}_e$, denote by $k(u)$ the smallest non-negative integer such that $\frac{||u||}{p^{k(u)}||u_0||} < p$ and denote $\lambda(u) := \frac{||u||}{p^{k(u)}||u_0||}$.

We define $\mathcal{PS}_e(1) := \{u \in \mathcal{PS}_e : \lambda(u) \leq \sqrt{p}\}$ and $\mathcal{PS}_e(2) := \{u \in \mathcal{PS}_e : \lambda(u) > \sqrt{p}\}$. Since we may assume $p > 7$ by Corollary 3.2, we have $\frac{2p}{3} - 3 > \sqrt{p}$.

Lemma 3.14. *1) Let $i \in \{1, 2\}$ and let u_1, u_2 be distinct elements of $\mathcal{PS}_e(i)$ with $\lambda(u_2) \geq \lambda(u_1)$. Then $\lambda(u_2) \geq \frac{3-\theta}{2+\theta}\lambda(u_1)$ and $\lambda(u_2) \leq \frac{10}{\theta}\lambda(u_1)$.*
2) $\lambda(\mathcal{PS}_e(2)) \subseteq [\frac{\theta p}{10}, p)$.
3) λ is an injective map on $\mathcal{PS}_e$.

Proof. 1) Let $u_1' := p^{k(u_2)-k(u_1)}u_1$, $u_2' := u_2$ if $k(u_2) \geq k(u_1)$ and $u_1' := u_1$, $u_2' := p^{k(u_1)-k(u_2)}u_2$ if $k(u_2) < k(u_1)$. Now apply Lemma 14 and Lemma 15 to u_1', u_2' instead of u_1, u_2. We stress that u_1', u_2' are distinct elements of $\mathcal{S}_e$, since u_1, u_2 are distinct elements of $\mathcal{PS}_e(i)$.
2) This follows from Lemma 3.12 applied to the pair $(u_1, p^{k(u_1)+1}u_0)$ for each u_1 in $\mathcal{PS}_e(2)$.
3) Use part 1) and the fact that $\frac{3-\theta}{2+\theta} > 1$ for $\theta \in (0, \frac{1}{9})$. □

Proof of Theorem 1.2. By part 3) of Lemma 3.14 it suffices to bound $|\lambda(\mathcal{PS}_e)|$. By part 1) and 2) of Lemma 3.14 it will follow that we can bound $|\lambda(\mathcal{PS}_e)|$ purely in terms of θ: thus collecting all the bounds for e varying in $\mathcal{E}$ we obtain a bound depending only on r. We now give all the details.

For any $\theta \in (0, \frac{1}{9})$ we have

$$\frac{3-\theta}{2+\theta} > \frac{26}{19}.$$

Then we find that $|\lambda(\mathcal{PS}_e(1))|$ is at most the biggest n such that

$$\left(\frac{26}{19}\right)^{n-1} \leq \frac{10}{\theta}$$

and similarly for $|\lambda(\mathcal{PS}_e(2))|$. We conclude that

$$|\mathcal{PS}_e| \leq 2 + 2\frac{\log(\frac{10}{\theta})}{\log(\frac{26}{19})}.$$

Multiplying by $|\mathcal{E}|$ gives that for every $\theta \in (0, \frac{1}{9})$

$$|\mathcal{PS}| \leq 2\left(1 + \frac{\log(\frac{10}{\theta})}{\log(\frac{26}{19})}\right)\left(1 + \frac{2}{\theta}\right)^r.$$

So letting θ increase to $\frac{1}{9}$ we obtain

$$|\mathcal{PS}| \leq 2\left(1 + \frac{\log(90)}{\log(\frac{26}{19})}\right) 19^r < 31 \cdot 19^r.$$

This completes the proof of Theorem 1.2. □

4 Proof of Theorem 1.1.1

First suppose that G and K are finitely generated. Before we can start with the proof of Theorem 1.1, we will rephrase Theorem 1.2. Recall that we write $\mathbb{F}_q$ for the algebraic closure of $\mathbb{F}_p$ in K.

Then Theorem 1.2 implies that there is a finite subset T of G with $|T| \leq 31 \cdot 19^r$ such that any solution of

$$x_1 + x_2 = 1, (x_1, x_2) \in G$$

with $x_1 \notin \mathbb{F}_q$ and $x_2 \notin \mathbb{F}_q$ satisfies $(x_1, x_2) = (\gamma, \delta)^{p^t}$ for some $t \in \mathbb{Z}_{\geq 0}$ and $(\gamma, \delta) \in T$.

Now let $(x_1, x_2) \in G$ be a solution to

$$ax_1 + bx_2 = 1.$$

If $ax_1 \in \mathbb{F}_q$ or $bx_2 \in \mathbb{F}_q$, it follows that both $ax_1 \in \mathbb{F}_q$ and $bx_2 \in \mathbb{F}_q$, which implies that $(a, b)^{q-1} \in G$. This contradicts the condition on (a, b) in Theorem 1.1.

Hence $ax_1 \notin \mathbb{F}_q$ and $bx_2 \notin \mathbb{F}_q$. Define G' to be the group generated by G and the tuple (a, b). Then the rank of G' is at most $r + 1$. Let $T \subseteq G'$ be as above, so $|T| \leq 31 \cdot 19^{r+1}$. We can write

$$(ax_1, bx_2) = (\gamma, \delta)^{p^t}$$

with $t \in \mathbb{Z}_{\geq 0}$ and $(\gamma, \delta) \in T$. Since $T \subseteq G'$, we can write

$$(\gamma, \delta) = (a^k y_1, b^k y_2)$$

with $k \in \mathbb{Z}$ and $(y_1, y_2) \in G$. This means that

$$(ax_1, bx_2) = (a^k y_1, b^k y_2)^{p^t},$$

which implies $(a, b)^{kp^t - 1} \in G$. If $kp^t - 1$ is co-prime to p, we have a contradiction with the condition on (a, b) in Theorem 1.1. But p can only divide $kp^t - 1$ if $t = 0$. Then we find immediately that there are at most $|T| \leq 31 \cdot 19^{r+1}$ solutions as desired.

We still need to deal with the case that K is an arbitrary field of characteristic p and G is a subgroup of $K^* \times K^*$ with $\dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q} = r$ finite. Suppose that $ax_1 + bx_2 = 1$ has more than $31 \cdot 19^{r+1}$ solutions $(x_1, x_2) \in G$. Then we can replace G by a finitely generated subgroup of G with the same property. We can also replace K by a subfield, finitely generated over its prime field, containing the coordinates of the new G and a, b. This gives the desired contradiction.

5 Acknowledgements

We are grateful to Julian Lyczak for explaining us how identities as in Lemma 3.4 follow from basic properties of hypergeometric functions. Many thanks go to Jan-Hendrik Evertse for providing us with this nice problem, his help throughout and the proofreading.

References

[1] F. Beukers, H.P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups,* Acta Arith. 78, 189-199 (1996).

[2] J.-H. Evertse, K. GyHory, *Unit Equations in Diophantine Number Theory,* Cambridge University Press, 2015.

[3] S. Lang, *Fundamentals of Diophantine Geometry,* Springer, Berlin, 1983.

[4] J.L. Lavoie, F. Grondin, A.K. Rathie, *Generalizations of Whipple's theorem on the sum of a ${}_3F_2$,* Journal of Computational and Applied Mathematics 72, 293-300 (1996).

[5] J.F. Voloch, *The equation $ax + by = 1$ in characteristic p,* J. Number Theory 73, 195-200 (1998).

Addendum to chapter 1

On the equation $X_1 + X_2 = 1$ in finitely generated multiplicative groups in positive characteristic

Peter Koymans, Carlo Pagano

Addendum to "On the equation $X_1 + X_2 = 1$ in finitely generated multiplicative groups in positive characteristic"

Peter Koymans, Carlo Pagano

On the 22nd October of 2018 Professor Felipe Voloch brought to our attention the unpublished master thesis of Yi-Chih Chiu, written under the supervision of Professor Ki-Seng Tan. In this work, Chiu establishes a special case of our main theorems [4, Theorem 1.1, Theorem 1.2]. We shall begin by explaining his result, and we will next compare it to our result.

Let p be a prime number. For a field extension K of $\mathbb{F}_p$ with transcendence degree equal to 1, we let k be the algebraic closure of $\mathbb{F}_p$ in K. Denote by Ω_K the set of valuations of K. Let S be a finite subset of Ω_K and fix $\alpha, \beta \in K^*$. The following theorem is proven in Chiu's master thesis.

Theorem 1. *The S-unit equation to be solved in $x, y \in \mathcal{O}_S^*$*

$$\alpha x + \beta y = 1,$$

has at most $3 \cdot 7^{2|S|-2}$ pairwise inequivalent non-trivial solutions if $\alpha, \beta \in \mathcal{O}_S^*$. If instead α, β are not both in $\mathcal{O}_S^*$, then it has at most $39 \cdot 7^{2|S|-2}$ non-trivial solutions.

Here a solution (x, y) is called trivial if $\frac{\alpha x}{\beta y} \in k$. Two solutions $(x_1, y_1), (x_2, y_2)$ are said to be equivalent if there exists $n \in \mathbb{Z}_{\geq 0}$ with

$$(\alpha x_1)^{p^n} = \alpha x_2, (\beta y_1)^{p^n} = \beta y_2 \quad \text{or} \quad (\alpha x_2)^{p^n} = \alpha x_1, (\beta y_2)^{p^n} = \beta y_1.$$

This result is a special case with slightly better constants of our theorems that we state now for the reader's convenience, see [4, Theorem 1.1, Theorem 1.2].

Theorem 2. *Let K be a field of characteristic $p > 0$. Take $\alpha, \beta \in K^*$ and let G be a finitely generated subgroup of $K^* \times K^*$ of rank $r := \dim_{\mathbb{Q}} G \otimes \mathbb{Q}$. Then the equation*

$$\alpha x + \beta y = 1,$$

to be solved in $(x, y) \in G$, has at most $31 \cdot 19^r$ pairwise inequivalent non-trivial solutions if $(\alpha, \beta)^n \in G$ for some $n > 0$. If instead $(\alpha, \beta)^n \notin G$ for all $n > 0$, then it has at most $31 \cdot 19^{r+1}$ non-trivial solutions.

Note that Theorem 2 applies to *any* finitely generated subgroup in *any* field of characteristic p. In contrast, Chiu's theorem applies only to the case of S-units of fields of transcendence degree 1 (with some care Chiu's theorem can be extended to S-units of function fields of projective varieties).

The reason for this difference in generality comes from the fact that Chiu's work is an adaptation of Evertse's work [3] to characteristic p. Our work is instead an adaptation of the work of Beukers and Schlickewei [1] to characteristic p. In both works [1, 3], there is a key use of a certain set of identities coming from hypergeometric functions, see [4, Lemma 3.3, Lemma 3.4]. In characteristic p these identities can be used only in a limited range, see [2, Proposition 2] and [4, Corollary 3.5] respectively.

Correspondingly, the solutions to the unit equations need to be counted only up to equivalence. One of the most important steps is to use this equivalence relation in such a way that one is inside this limited range. It is this step that allows one to obtain an upper bound that is independent of p. The reader can find this step in the two papers respectively at [2, Lemma 4] and at [4, Lemma 3.9].

References

[1] F. Beukers and H.P. Schlickewei. *The equation $x + y = 1$ in finitely generated groups*. Acta Arith., 78, 1996, $189 - 199$.

[2] Y.-C. Chiu. *S-unit equation over algebraic function fields of characteristic $p > 0$*. Master Thesis, 2002, National Taiwan University.

[3] J.-H. Evertse. *On equations in S-units and the Thue–Mahler equation*. Invent. Math., 75, 1984, $561 - 584$.

[4] P. Koymans and C. Pagano. *On the equation $X_1 + X_2 = 1$ in finitely generated multiplicative groups in positive characteristic*. Q. J. Math., 68, 2017, $923-934$.

CHAPTER

2

4-Ranks and the general model for statistics of ray class groups of imaginary quadratic number fields

C. Pagano and E. Sofos

4-RANKS AND THE GENERAL MODEL FOR STATISTICS OF RAY CLASS GROUPS OF IMAGINARY QUADRATIC NUMBER FIELDS

C. PAGANO AND E. SOFOS

ABSTRACT. We use homological algebra to extend the Cohen–Lenstra heuristics to the setting of ray class groups of imaginary quadratic number fields, viewed as exact sequences of Galois modules. By asymptotically estimating the mixed moments governing the distribution of a cohomology map, we prove these conjectures in the case of 4-ranks.

CONTENTS

1. INTRODUCTION

Let c be a positive odd square-free integer. Partition the set of its prime divisors, S, into $S_1 \cup S_3$, where if $l \in S_i$ then $l \equiv i \,(\mathrm{mod}\ 4)$. For an imaginary quadratic number field K, denote by $\mathrm{Cl}(K, c)$ the ray class group of K of conductor c, and by $\mathrm{D}(K)$ the discriminant of K. Let j_1 and j_2 be two non-negative integers. The following theorem will be shown to be a special case of the present work.

Theorem 1.1. *Consider all imaginary quadratic number fields K such that $\mathrm{D}(K) \equiv 1 \,(\mathrm{mod}\ 4)$ and $\mathscr{O}_K/c \cong_{\mathrm{ring}} \prod_{l\in S} \mathbb{F}_{l^2}$. When such K are ordered by the size of their discriminants the fraction of them that satisfy*

$$\mathrm{rk}_4(\mathrm{Cl}(K)) = j_1,\ \mathrm{rk}_4(\mathrm{Cl}(K, c)) = j_2$$

approaches

$$\frac{\eta_\infty(2)}{\eta_{j_1}(2)2^{j_1^2}} \frac{\#\{\varphi \in \mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, \mathbb{F}_2^{\#S_3}) : \mathrm{rk}(\varphi) = \#S - (j_2 - j_1)\}}{\#\,\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1}, \mathbb{F}_2^{\#S_3})}.$$

For $M \in \mathbb{Z}_{\geqslant 1}$ and $s \in \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$, $\eta_s(M)$ denotes $\prod_{i=1}^{s}(1 - M^{-i})$. For the statement in full generality see Theorem 5.4.

Date: November 7, 2018.
2010 *Mathematics Subject Classification.* 11R65, 11R29, 11R11, 11R45.

The special case $c = 1$ of Theorem 1.1 recovers a result of Fouvry and Klüners [7, Cor. 1] (in the subfamily of imaginary quadratic number fields above). The theorem of Fouvry and Klüners on 4-ranks is one of the strongest pieces of evidence for the heuristic of Cohen–Lenstra and Gerth about the distribution of the p-Sylow subgroup of the class group of an imaginary quadratic number field.

Indeed, for odd primes p, Cohen and Lenstra [4] constructed a heuristic model to predict the outcome of any statistic on the p-Sylow of the class group of imaginary quadratic number fields. For every prime p they equipped the set of isomorphism classes of abelian p-groups, $\mathscr{G}_p$, with the only probability measure that gives to each abelian p-group G a weight inversely proportional to $\#\operatorname{Aut}(G)$. This measure is now often called the Cohen–Lenstra measure on $\mathscr{G}_p$, and denoted by μ_{CL}. Their heuristic model, for odd primes p, consisted in predicting the equidistribution of $\mathrm{Cl}(K)[p^\infty]$ in $\mathscr{G}_p$, as K ranges through natural families of imaginary quadratic number fields. Later, Gerth [9] adapted this heuristic model for $p = 2$. His idea was that the only obstruction for $\mathrm{Cl}(K)[2^\infty]$ to behave like a random abelian 2-group in the sense of Cohen–Lenstra comes from $\mathrm{Cl}(K)[2]$; therefore his heuristic model is that $2\,\mathrm{Cl}(K)[2^\infty]$ behaves like a random abelian 2-group. The result of Fouvry and Klüners can then be formulated by saying that, consistently with Gerth's conjecture, the 2-torsion of $2\,\mathrm{Cl}(K)$ behaves like the 2-torsion of a random abelian 2-group in the sense of Cohen–Lenstra.

Before the present paper, no analogue of any of these heuristics has been proposed for ray class groups. Our second main achievement, aside from the proof of Theorem 1.1, is to provide an extension of the Cohen–Lenstra and Gerth heuristics for ray class groups. We obtain this by means of two innovations, one of a rather conceptual nature and one of a technical nature. Namely we first introduce the novel viewpoint of using homological algebra to weight the possible occurrences of ray class groups, as explained in §2. Secondly, to overcome the difficulties imposed by $p = 2$, we introduce in §3 the new notion of *embeddable extensions* (see Definition 3.2). This notion allows us to take care of the additional structure of this case, furnishing a natural way to define the adjusted weights for the 2-part of ray class groups. Theorem 1.1 will then be a strong evidence supporting our new heuristic for ray class groups and precisely in the case where our heuristic has the most demanding algebraic shape. The agreement of Theorem 1.1 and our heuristic at $p = 2$ is established in Proposition 3.5.

With our model we can provide the conjectural analogue of Theorem 1.1 for all odd primes p. Partition S into $S_1 \cup \ldots \cup S_{p-1}$, where $l \in S_i$ if $l \equiv i \pmod p$.

Conjecture 1.2. *Let p be an odd prime. Consider all imaginary quadratic number fields K having the property $\mathscr{O}_K/c \cong_{\mathrm{ring}} \prod_{l\in S} \mathbb{F}_{l^2}$. When such K are ordered by the size of their discriminants the fraction of them that satisfy*

$$\mathrm{rk}_p(\mathrm{Cl}(K)) = j_1,\ \mathrm{rk}_p(\mathrm{Cl}(K,c)) = j_2$$

approaches

$$\frac{\eta_\infty(p)}{\eta_{j_1}(p)^2 p^{j_1^p}} \frac{\#\{\varphi \in \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^{j_1}, \mathbb{F}_p^{\#S_{p-1}}) : \mathrm{rk}(\varphi) = \#S_1 + \#S_{p-1} - (j_2 - j_1)\}}{\#\,\mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^{j_1}, \mathbb{F}_p^{\#S_{p-1}})}.$$

For the statement in the general case see Conjecture 2.10, in particular, in the main body of the paper, we shall allow any admissible ring structure for $\mathscr{O}_K/c$. From our model in its full generality we shall derive conjectural formulas for the average size of the p-torsion of ray class groups of imaginary quadratic number fields.

Conjecture 1.3. *Let p be an odd prime. The average value of $\#\operatorname{Cl}(K,c)[p]$ as K ranges over imaginary quadratic number fields with $\gcd(\mathrm{D}(K),c)=1$ and ordered by their discriminant is:*
(1)

$$p^{\#\{l \text{ prime: } l\mid c, l\equiv 1 (\mathrm{mod}\ p)\}}\Big(1+\Big(\frac{p+1}{2}\Big)^{\#\{l \text{ prime: } l\mid c, l\equiv 1 \text{ or } -1 (\mathrm{mod}\ p)\}}\Big)$$

if p^2 does not divide c,
(2)

$$p^{\#\{l \text{ prime: } l\mid c, l\equiv 1 (\mathrm{mod}\ p)\}+1}\Big(1+p\Big(\frac{p+1}{2}\Big)^{\#\{l \text{ prime: } l\mid c, l\equiv 1 \text{ or } -1 (\mathrm{mod}\ p)\}}\Big)$$

if p^2 divides c.

For $p=3$ this conjecture was recently proved by Varma [18] using geometry of numbers. In [18, §1] she asked whether one can formulate an extension of the Cohen–Lenstra heuristic that explains her result. Our model for ray class groups settles this for imaginary quadratic number fields (for the full comparison with Varma's result see §2.2).

Our main theorems and conjectures are not merely about the group $\operatorname{Cl}(K,c)$ but also about the entire exact sequence naturally attached to it:

$$1\to\frac{(\mathscr{O}_K/c)^*}{\mathscr{O}_K^*}\to\operatorname{Cl}(K,c)\to\operatorname{Cl}(K)\to 1.$$

For simplicity, in this section we will continue to assume that all the primes in S are inert in K. Then one can show that there is a long exact sequence whose first terms are

$$1\to\Big(\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle}\Big)^2[2]\to(2\operatorname{Cl}(K,c))[2]\to(2\operatorname{Cl}(K))[2]\xrightarrow{\delta_2(K)}\prod_{l\in S_3}\frac{\mathbb{F}_{l^2}^{*2}}{\mathbb{F}_{l^2}^{*4}}.$$

To obtain the last map one chooses any identification between $\frac{\left(\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle}\right)^2}{\left(\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle}\right)^4}$ and $\prod_{l\in S}\frac{\mathbb{F}_{l^2}^{*2}}{\mathbb{F}_{l^2}^{*4}}$ via an identification of the rings $\mathscr{O}_K/c$ and $\prod_{l\in S}\mathbb{F}_{l^2}$. The resulting set of maps is an orbit under $\operatorname{Aut}_{\mathrm{ring}}(\prod_{l\in S}\mathbb{F}_{l^2})$, acting by post-composition. But $\operatorname{Aut}_{\mathrm{ring}}(\prod_{l\in S}\mathbb{F}_{l^2})$ acts trivially on $\prod_{l\in S_3}\frac{\mathbb{F}_{l^2}^{*2}}{\mathbb{F}_{l^2}^{*4}}$, so one has a canonical identification.

Let Y be a subspace of $\prod_{l\in S_3}\frac{\mathbb{F}_{l^2}^{*2}}{\mathbb{F}_{l^2}^{*4}}$ and j a non-negative integer. In this setting we manage to control the statistical distribution of $(\#2\operatorname{Cl}(K))[2],\operatorname{Im}(\delta_2(K))$, thus providing a considerable refinement of Theorem 1.1. Our result is as follows.

Theorem 1.4. *Consider all imaginary quadratic number fields K such that $\mathrm{D}(K)\equiv 1\,(\mathrm{mod}\ 4)$ and $\mathscr{O}_K/c\cong_{\mathrm{ring}}\prod_{l\in S}\mathbb{F}_{l^2}$. When such K are ordered by the size of their discriminants the fraction of them that satisfy*

$$(2\operatorname{Cl}(K))[2]\cong\mathbb{F}_2^j,\ \operatorname{Im}(\delta_2(K))=Y$$

approaches

$$\frac{\eta_\infty(2)}{\eta_{j_1}(2)2^{2j_1}}\frac{\#\operatorname{Epi}_{\mathbb{F}_2}(\mathbb{F}_2^j,Y)}{\#\operatorname{Hom}_{\mathbb{F}_2}\left(\mathbb{F}_2^j,\prod_{l\in S_3}\frac{\mathbb{F}_{l^2}^{*2}}{\mathbb{F}_{l^2}^{*4}}\right)}.$$

This means that $(\#(2\,\mathrm{Cl}(K))[2], \mathrm{Im}(\delta_2(K)))$ behaves like $(\#G[2], \mathrm{Im}(\delta))$, where G is a random abelian 2-group in the Cohen–Lenstra sense, and $\delta : G[2] \to \mathbb{F}_2^{\#S_3}$ is a random map. For the statement in full generality see Theorem 5.2. We show in §3 that this result is also predicted by our heuristic model. Our model enables us to provide a conjectural analogue of Theorem 1.4 for all odd p. Its formulation is in Conjecture 2.8.

Theorem 1.4 determines the joint distribution of the pair $(\#(2\,\mathrm{Cl}(K))[2], \mathrm{Im}(\delta_2(K)))$. Theorem [7, Cor.1] of Fouvry and Klüners determines the distribution of the first component, $\#(2\,\mathrm{Cl}(K))[2]$ via the use of another result of the two authors, [8, Theorem 3], where they obtained asymptotics for all moments of $\#(2\,\mathrm{Cl}(K))[2]$. A surprising feature of our work is that we establish the joint distribution of the pair $(\#(2\,\mathrm{Cl}(K))[2], \mathrm{Im}(\delta_2(K)))$ by means of the moment-method, despite the fact that $\mathrm{Im}(\delta_2(K))$ is not a number. *Although the general philosophy of using moments to study distributions is standard in the literature related to the Cohen–Lenstra heuristics* (*see, for example,* [22]), *we stress that no object like the image of the δ-map has been treated in the subject.* It is instructive to see how we incorporate the image-data into the Fouvry–Klüners method. We do this by introducing for every real character $\chi : \prod_{l\in S_3} \mathbb{F}_{l^2}^{*2} \to \mathbb{R}^*$, the random variable

$$m_\chi(\delta_2(K)) := \#\ker(\chi(\delta_2(K))).$$

To know the pair $(\#(2\,\mathrm{Cl}(K))[2], \mathrm{Im}(\delta_2(K)))$ is equivalent to knowing $(m_\chi(\delta_2(K)))_\chi$. However, the advantage is that the latter is a *numerical* vector and therefore one can hope to apply the method of moments to control its distribution. This is precisely what we achieve in Theorem 5.6. The expressions that appear during the proof of Theorem 5.6 are of the shape

$$\sum_{D<X} \prod_{\chi} m_\chi(\delta_2(\mathbb{Q}(\sqrt{-D})))^{k_\chi},$$

where D ranges over all positive square-free integers with $D \equiv 3 \pmod 4$ and χ ranges over all real characters $\chi : \prod_{l\in S_3} \mathbb{F}_{l^2}^* \to \mathbb{R}^*$. As explained in §6.1, the additional complexity of these expressions compared to the classical case settled by Fouvry and Klüners, is tempered by the fact that, with our heuristic model for ray class groups, we already have a candidate main term. In particular, the shape of its expression suggests a way to subdivide the sum, with the benefit of hindsight, in many smaller sub-sums. For each of these sub-sums it turns out that the techniques of Fouvry and Klüners are applicable with only minor modifications. After proving Theorem 5.6 we turn our attention to the distribution of $(\#(2\,\mathrm{Cl}(K))[2], \mathrm{Im}(\delta_2(K)))$, which we reconstruct from the mixed moments by following an argument of Heath-Brown [10].

We stress that Theorem 1.4 is stronger than Theorem 1.1. Here the finer information (which is the *image* of the δ-map), is obtained precisely owing to the fact that we use ring identifications rather than merely group identifications[1]. Using the latter we could have studied only the *size* of $\mathrm{Im}(\delta_2(K))$, which is precisely what occurs in Theorem 1.1. On the other hand, it is important to note that the techniques employed in the proof of Theorem 1.4 are not applicable in studying directly the moments of the isolated quantity $\#(2\,\mathrm{Cl}(K, c))[2]$: we can access the distribution of the quantity $\#(2\,\mathrm{Cl}(K, c))[2]$ only by the moments of a finer object, the δ-map. This contrast reflects the fact that the natural algebraic structure attached to the ray class group is the entire exact sequence naturally attached to it, rather than just the isolated group $\mathrm{Cl}(K, c)$. It is precisely this phenomenon that leads us to

[1]We thank Hendrik Lenstra for having suggested this.

formulate a general heuristic for ray class *sequences* of conductor c. In this framework, Theorem 1.4 gives compelling evidence that our heuristic model predicts correct answers also when it is challenged to produce the outcome of statistics about the *ray class sequence*, and not only when, less directly, one isolates the group $\mathrm{Cl}(K, c)$.

Encouraged by this corroboration, we formulate our heuristic to predict the outcome of *any* statistical question about the p-part of the ray class sequence, viewed as an exact sequence of Galois modules. A positive side effect of this enhanced generality is the consequent logical simplification of our conjectural framework: our heuristic is based on a simple unifying principle, which, if true, implies at once all our conjectures. This heuristic principle is stated in §2 for an odd prime p, and in §3 for $p = 2$.

Let p be an odd prime and G a finite abelian p-group. The following is an attractive and easy example of the conjectural conclusions that are available in this new model:

Conjecture 1.5. *Consider all imaginary quadratic number fields K having the property that $\mathscr{O}_K/c \cong_{\mathrm{ring}} \prod_{l\in S} \mathbb{F}_{l^2}$. When such K are ordered by the size of their discriminants, the fraction of them having the properties that the p-part of the ray class sequence of modulus c splits and*

$$\mathrm{Cl}(K)[p^\infty] \cong_{\mathrm{ab.gr.}} G,$$

approaches

$$\frac{\eta_\infty(p)}{\#\,\mathrm{Aut}_{\mathrm{ab.gr.}}(G)} \frac{1}{\#\,\mathrm{Hom}_{\mathrm{ab.gr.}}(G, \prod_{l\in S_{p-1}} \mathbb{F}_{l^2}^*)}.$$

1.1. **Comparison with the literature.** The present work sits in an active area of research focused on extending the classical Cohen–Lenstra heuristics to other interesting arithmetical objects and on establishing the correctness of these statistical models in cases where an 'analytically-friendly' description of the problem is available. Developments along this line of research can be found in the very recent work by Wood [21], which provides a heuristic for the average number of unramified G-extensions of a quadratic number field for any finite group G: the Cohen–Lenstra heuristics are recovered by taking G to be an abelian group. It would be interesting to reach the generality of both the present paper and [21], by considering G-extensions with prescribed ramification data. The evidence provided in [21] is over function fields, by means of the approach of Ellenberg, Venkatesh and Westerland [6]. In a recent preprint, Alberts and Klys [1] offered evidence for the heuristics in Wood's work [21] over number fields using the approach of Fouvry and Klüners. It is interesting to note that in a previous work Klys [14] extended the work of Fouvry and Klüners to the p-torsion of cyclic degree p extensions. These last two examples, together with the present work, show the remarkable versatility of the method used in [8] and pioneered (in the context of Selmer groups) by Heath-Brown [10].

The case of narrow class groups was investigated by Bhargava and Varma [3] and by Dummit and Voight [5]. The latter work provides, among other things, a conjectural formula for the average size of the 2-torsion of narrow class groups among the family of S_n-number fields, for odd n. For $n = 3$, this was a theorem of Bhargava and Varma [3].

Very recently, Jordan, Klagsbrun, Poonen, Skinner and Zaytman [13] made a conjecture for the distribution of the p-torsion of K-groups of real and imaginary quadratic number fields. Building on the recent improvement of the work of Bhargava, Shankar and Tsimerman [2], they established their conjecture for the average size of the 3-torsion. Incidentally, the

work [2] is also employed by Varma [18] on the average 3-torsion of ray class groups, which is placed in a general conjectural framework by the present paper.

Despite this rich context of developments, the present paper is, to the best of our knowledge, the first one to propose a heuristic model for the ray class sequence of imaginary quadratic number fields and to prove its correctness for the pair $(\#(2\,\mathrm{Cl}(K))[2], \mathrm{Im}(\delta_2(K)))$, establishing, as a corollary, the joint distribution of the 4-ranks of $\mathrm{Cl}(K)$ and $\mathrm{Cl}(K, c)$.

1.2. **Organization of the material.** The remainder of this paper is organized as follows: In §2 we explain our heuristic model for the distribution of the p-part of ray class sequences of imaginary quadratic number fields, for odd primes p. We draw several conjectures from this heuristic principle and verify its consistency with the theorems of Varma [18] in the imaginary quadratic case.

In §3 we examine the case $p = 2$. This case requires some additional work to isolate the 'random' part of the 2-Sylow of the ray class sequences of imaginary quadratic number fields. This additional difficulty arises already for the ordinary class group as can be seen in the work of Gerth [9]. However, for ray class sequences overcoming such difficulties is much more intricate due to the more articulate underlying algebraic structures. This will allow us to formulate a number of predictions that will be proved in §§5-7. A key step in these proofs is the reformulation of the problem about 4-ranks into a purely analytic problem about mixed moments. For this we introduce the notion of special divisors in §4 and certain related statistical questions that will be subsequently answered. This statistic is a special case of a ray class group statistic, as subsequently established in §5. Therefore the material of §3 would implicitly provide a heuristic for it. Nevertheless, in §4 we present the problem and the heuristic in a direct way using the language of special divisors. This has the advantage that §4, Theorems 5.6-5.7, §6 and §7 are mostly analytic in nature and can be read independently of the algebraic considerations in §2 and §3.

In §5 we state the main theorems about the 2-part of the ray class sequences and reduce their proof so as to establish the predictions in §4. The section ends with the statement of the corresponding main theorems on special divisors. In §6 we prove the main theorem on mixed moments attached to the maps on special divisors introduced in §4. Finally, in §7 we reconstruct the distribution from the mixed moments, concluding the proof of all theorems stated in §5.

Notation. The symbol $\mathrm{D}(K)$ will always refer to the discriminant of a number field K. Let us furthermore denote

$$\mathscr{F} := \{K \text{ imaginary quadratic number field}\}.$$

Acknowledgements. We are very grateful to Hendrik Lenstra for several insightful discussions and for useful feedback during the course of this project. In particular, we thank him for suggesting to consider the first terms of the ray class sequences only up to *ring* automorphisms, which turned out to be a natural level of greater generality where we could prove our main theorems on 4-ranks. We thank Alex Bartel for many stimulating discussions about our work, as well as organizing an inspiring conference on the Cohen–Lenstra heuristics in Warwick in July 2016, where this project started. We also wish to thank Djordjo Milovic and Peter Koymans for useful discussions and Ila Varma and Peter Stevenhagen for profitable feedback. Furthermore, we thank Alex Bartel, Joseph Gunther and Peter Koymans for helpful remarks on earlier versions of this paper.

2. Heuristics and conjectures for p odd

Let p be an odd prime number and c a positive integer. Denote by C_2 a group with 2 elements and denote by τ its generator. In this section we provide a heuristic model that predicts the statistical behavior of the exact sequence of $\mathbb{Z}_p[C_2]$-modules attached to the ray class group of conductor c of an imaginary quadratic number field K. Denote it by

$$S_p(K) := \Big(1 \to \frac{(\mathscr{O}_K/c)^*}{\mathscr{O}_K^*}[p^\infty] \to \mathrm{Cl}(K,c)[p^\infty] \to \mathrm{Cl}(K)[p^\infty] \to 1\Big), \tag{2.1}$$

where the C_2-action comes from the natural action of $\mathrm{Gal}(K/\mathbb{Q})$ on each term of the sequence. The reader is referred to [15, §IV] for related background material. We shall call $S_p(K)$ the p-part of the *ray class sequence* of conductor c. We shall henceforth ignore the fields $K = \mathbb{Q}(\mathrm{i})$ and $K = \mathbb{Q}(\sqrt{-3})$, to ensure that $\mathscr{O}_K^* = \langle -1\rangle$. Owing to $p \neq 2$ we furthermore have $((\mathscr{O}_K/c)^*/\langle -1\rangle)[p^\infty] = (\mathscr{O}_K/c)^*[p^\infty]$, thus allowing us to write

$$S_p(K) := (1 \to (\mathscr{O}_K/c)^*[p^\infty] \to \mathrm{Cl}(K,c)[p^\infty] \to \mathrm{Cl}(K)[p^\infty] \to 1).$$

Denote by $\mathscr{G}_p$ a set of representatives of isomorphism classes of finite abelian p-groups, viewed as C_2-modules under the action of $-\mathrm{Id}$ and call $G_p(K)$ the unique representative of $\mathrm{Cl}(K)[p^\infty]$ in $\mathscr{G}_p$. Any family of imaginary quadratic fields can be partitioned in finitely many subfamilies where the isomorphism class of the ring $\mathscr{O}_K/c$ is fixed, by imposing finitely many congruence conditions on the discriminants. Therefore we can always assume that $(\mathscr{O}_K/c)^*$ has been fixed as the unit group of some ring that is independent of K.

Definition 2.1. Let K, c be as above and R a finite commutative ring. We shall say that K is of type R if $\mathscr{O}_K/\mathrm{char}(R) \cong R$ as rings. With this definition in mind let us denote

$$\mathscr{F}(R) := \{K \text{ imaginary quadratic number field of type } R\}.$$

From now on we will assume that R is of the form $R := \mathscr{O}_{\mathscr{A}}/c$, where $\mathscr{O}_{\mathscr{A}}$ is the integral closure of $\prod_{l|c}\mathbb{Z}_l$ in $\mathscr{A} := \prod_{l|c} E_l$, with E_l being an etale $\mathbb{Q}_l$-algebra of degree 2. Under this assumption, a positive fraction of all discriminants lies in $\mathscr{F}(R)$.

Suppose K is of type R. Then $(\mathscr{O}_K/c)^*$ can be identified with R^* via any restriction of a ring isomorphism, that is via any element of $\mathrm{Isom}_{\mathrm{ring}}(\mathscr{O}_K/c, R)$. Furthermore, we can identify $\mathrm{Cl}(K)[p^\infty]$ and $G_p(K)$ via any element of $\mathrm{Isom}_{\mathrm{ab.gr.}}(\mathrm{Cl}(K)[p^\infty], G_p(K))$. Therefore applying $\mathrm{Isom}_{\mathrm{ring}}(\mathscr{O}_K/c, R) \times \mathrm{Isom}_{\mathrm{ab.gr.}}(\mathrm{Cl}(K)[p^\infty], G_p(K))$ to $S_p(K)$, we obtain a unique orbit

$$O_{c,p}(K) \in \mathrm{Ext}_{\mathbb{Z}_p[C_2]}(G_p(K), R^*[p^\infty])/(\mathrm{Aut}_{\mathrm{ring}}(R) \times \mathrm{Aut}_{\mathrm{ab.gr.}}(G_p(K))).$$

We refer the reader to [19, §3] for definition and properties of $\mathrm{Ext}_S(A,B)$, where S is a ring and A, B are S-modules. For the remainder of the paper, given S-modules A, B, C, A', B' and C', we call a *commutative diagram* of S-modules, a diagram of maps of S-modules

$$\begin{array}{ccccccc} 0 & \to & B_1 & \xrightarrow[f_1]{} & C_1 & \xrightarrow[g_1]{} & A_1 \to 0 \\ & & \downarrow \psi_1 & & \downarrow \psi_2 & & \downarrow \psi_3 \\ 0 & \to & B_2 & \xrightarrow[f_2]{} & C_2 & \xrightarrow[g_2]{} & A_2 \to 0, \end{array}$$

with $\psi_2 \circ f_1 = f_2 \circ \psi_1$ and $\psi_3 \circ g_1 = g_2 \circ \psi_2$. Note that $\mathrm{Cl}(K_1)[p^\infty] \cong_{\mathrm{ab.gr}} \mathrm{Cl}(K_2)[p^\infty]$ and $O_{c,p}(K_1) = O_{c,p}(K_2)$ if and only if there is a commutative diagram of $\mathbb{Z}_p[C_2]$ modules

$$\begin{array}{ccccccc} 0 & \to & (\mathscr{O}_{K_1}/c)^*[p^\infty] & \to & \mathrm{Cl}(K_1,c)[p^\infty] & \to & \mathrm{Cl}(K_1)[p^\infty] \to 0 \\ & & \downarrow \varphi_1 & & \downarrow \varphi_2 & & \downarrow \varphi_3 \\ 0 & \to & (\mathscr{O}_{K_2}/c)^*[p^\infty] & \to & \mathrm{Cl}(K_2,c)[p^\infty] & \to & \mathrm{Cl}(K_2)[p^\infty] \to 0, \end{array}$$

with φ_1 being the restriction of a ring isomorphism and φ_3 being an isomorphism of abelian groups.

Definition 2.2. Define $\mathscr{S}_p(R)$ as the set of equivalence classes of pairs (G, θ), where

$$G \in \mathscr{G}_p,\ \theta \in \mathrm{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty])$$

under the following equivalence relation: two pairs $(G_1, \theta_1), (G_2, \theta_2)$ are identified if $G_1 = G_2$ and θ_1 and θ_2 are in the same $\mathrm{Aut}_{\mathrm{ring}}(R) \times \mathrm{Aut}_{\mathrm{ab.gr.}}(G_1)$-orbit.

Let us denote by $\widetilde{\mathscr{S}_p}(R)$ the set of pairs (G, θ) where $G \in \mathscr{G}_p$ and $\theta \in \mathrm{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty])$, thus bringing into play the quotient map $\pi : \widetilde{\mathscr{S}_p}(R) \to \mathscr{S}_p(R)$. We are interested in studying the distribution of $S'_p(K)$ given by the pair

$$K \mapsto S'_p(K) := (G_p(K), O_{c,p}(K)) \in \mathscr{S}_p(R).$$

Definition 2.3. Let μ_{CL} be the unique probability measure on $\mathscr{G}_p$ which gives to each abelian p-group G a weight inversely proportional to the size of the automorphism group of G.

This measure was introduced by Cohen and Lenstra in [4] to predict the distribution of $G_p(K)$, the first component of $S'_p(K)$. We shall introduce a measure on $\mathscr{S}_p(R)$ that enables us to predict the joint distribution of the vector $S'_p(K)$. Consider the discrete σ-algebra on both $\widetilde{\mathscr{S}_p}(R), \mathscr{S}_p(R)$ and equip $\widetilde{\mathscr{S}_p}(R)$ with the following measure,

$$\widetilde{\mu}_{\mathrm{seq}}((G, \theta)) := \frac{\mu_{\mathrm{CL}}(G)}{\#\,\mathrm{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty])}.$$

Let $\mu_{\mathrm{seq}} := \pi_*(\widetilde{\mu}_{\mathrm{seq}})$ be the pushforward measure of $\widetilde{\mu}_{\mathrm{seq}}$ on $\mathscr{S}_p(R)$ via π. It is evident that $\widetilde{\mu}_{\mathrm{seq}}$ and μ_{seq} are probability measures. We now formulate a heuristic which roughly states that ray class sequences equidistribute within the set of isomorphism classes of exact sequences with respect to the measure μ_{seq}.

Heuristic assumption 2.4. *For any 'reasonable' function $f : \mathscr{S}_p(R) \to \mathbb{R}$ we have*

$$\lim_{X \to \infty} \#\{K \in \mathscr{F}(R) : |\,\mathrm{D}(K)| \leqslant X\}^{-1} \sum_{\substack{K \in \mathscr{F}(R) \\ |\,\mathrm{D}(K)| \leqslant X}} f(S'_p(K)) = \sum_{S \in \mathscr{S}_p(R)} f(S)\mu_{\mathrm{seq}}(S).$$

Letting f be the indicator function of a singleton yields the following statement.

Conjecture 2.5. *For any $S \in \mathscr{S}_p(R)$ we have*

$$\lim_{X \to \infty} \frac{\#\{K \in \mathscr{F}(R) : |\,\mathrm{D}(K)| \leqslant X, S'_p(K) = S\}}{\#\{K \in \mathscr{F}(R) : |\,\mathrm{D}(K)| \leqslant X\}} = \mu_{\mathrm{seq}}(S).$$

A special concrete example is the case of split sequences.

Conjecture 2.6. *The fraction of $K \in \mathscr{F}(R)$, ordered by the size of their discriminant, for which $\mathrm{Cl}(K)[p^\infty] \cong_{\mathrm{ab.gr.}} G$ and the p-part of the ray class sequence of modulus c splits, approaches*

$$\frac{\mu_{\mathrm{CL}}(G)}{\#\,\mathrm{Hom}_{\mathrm{ab.gr.}}(G, R^*[p^\infty]^-)},$$

where $(R^*[p^\infty])^-$ denotes the minus part of $R^*[p^\infty]$ under the action of C_2.

Indeed, $\mathrm{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty]) = \mathrm{Ext}_{\mathbb{Z}_p}(G, (R^*[p^\infty])^-)$ holds, hence Conjecture 2.6 is derived from Conjecture 2.5 by recalling that for two finite abelian p-groups A, B, there is a non-canonical isomorphism $\mathrm{Ext}_{\mathbb{Z}_p}(A, B) \cong_{\mathrm{ab.gr.}} \mathrm{Hom}_{\mathbb{Z}_p}(A, B)$.

2.1. **Conjectures on the p-torsion.** We next state certain consequences of Heuristic assumption 2.4 regarding the p-torsion of the ray class sequences. Taking p-torsion in (2.1) provides us with a long exact sequence whose first four terms are given by

$$S(K)[p] := \left(1 \to (\mathscr{O}_K/c)^*[p] \to \mathrm{Cl}(K,c)[p] \to \mathrm{Cl}(K)[p] \xrightarrow{\delta_p(K)} \frac{(\mathscr{O}_K/c)^*}{((\mathscr{O}_K/c)^*)^p}\right),$$

where the map $\delta_p(K)$ is defined as follows: given a class $x \in \mathrm{Cl}(K)[p]$ pick a representative ideal $\mathscr{I}$ of x which is coprime to c, take a generator of $\mathscr{I}^p$ and reduce it modulo c. The choice of another representative does not change it modulo p-th powers. More generally, taking p-torsion in any short exact sequence of $\mathbb{Z}_p[C_2]$-modules

$$S := (0 \to A \to B \to C \to 0)$$

provides us with a long exact sequence whose first terms are

$$S[p] := \left(1 \to A[p] \to B[p] \to C[p] \xrightarrow{\delta_p(S)} \frac{A}{pA}\right),$$

where $\delta_p(S)$ is defined in the same way as explained above (in particular we have $\delta_p(S_p(K)) = \delta_p(K)$). Thus this provides a map sending an element θ of $\mathrm{Ext}_{\mathbb{Z}_p[C_2]}(C, A)$ to a map $\delta_p(\theta) : C[p] \to A/pA$. We will make repeatedly use of the following fact.

Proposition 2.7. *The map sending θ to $\delta_p(\theta)$, from $\mathrm{Ext}_{\mathbb{Z}_p[C_2]}(C, A)$ to $\mathrm{Hom}_{\mathbb{Z}_p[C_2]}(C[p], A/pA)$, is a surjective group homomorphism.*

The reader interested in a proof of Proposition 2.7, can look at the proof of the analogous, but more complicated, Proposition 3.5: all the ingredients for the proof of Proposition 2.7 are contained in the proof of Proposition 3.5.

Next we shall define $j := \dim_{\mathbb{F}_p}(\mathrm{Cl}(K)[p])$ and apply any pair of identifications from $\mathrm{Isom}_{\mathbb{F}_p}(\mathrm{Cl}(K)[p], \mathbb{F}_p^j) \times \mathrm{Isom}_{\mathrm{ring}}(\mathscr{O}_K/c, R)$. Therefore, we obtain a unique orbit of maps $\varphi \in \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^j, (\frac{R^*}{R^{*p}})^-)$ under the action of $\mathrm{GL}_j(\mathbb{F}_p) \times \mathrm{Aut}_{\mathrm{ring}}(R)$. This is tantamount to having a $\mathrm{Aut}_{\mathrm{ring}}(R)$-orbit of images in $(\frac{R^*}{R^{*p}})^-$ of $\delta_p(K)$ via any of the previous identifications. We denote this orbit by $[\mathrm{Im}(\delta_p(K))]$. The assignment $K \mapsto [\mathrm{Im}(\delta_p(K))]$ attaches to each imaginary quadratic field $K \in \mathscr{F}_c(R)$ a well-defined $\mathrm{Aut}_{\mathrm{ring}}(R)$-orbit of vector sub-spaces of $(\frac{R^*}{R^{*p}})^-$.

By Proposition 2.7, the map

$$\mathrm{Ext}_{\mathbb{Z}_p}(G, R^*[p^\infty]^-) \to \mathrm{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)$$

induces, by pushforward, the counting probability measure from $\mathrm{Ext}_{\mathbb{Z}_p}(G,(R^*[p^\infty])^-)$ to $\mathrm{Hom}_{\mathbb{Z}_p}(G[p],(R^*/R^{*p})^-)$. Therefore, fixing a sub-$\mathbb{F}_p$-space Y of $(\frac{R^*}{R^{*p}})^-$ and a non-negative integer j, Heuristic assumption 2.4 supplies us with the following.

Conjecture 2.8. *The proportion of $K\in\mathscr{F}(R)$ ordered by the size of their discriminant, for which $\dim_{\mathbb{F}_p}(\mathrm{Cl}(K)[p])=j$ and $[\mathrm{Im}(\delta_p(K))]$ is $O(Y)$, the $\mathrm{Aut}_{\mathrm{ring}}(R)$-orbit of Y, approaches*

$$\mu_{\mathrm{CL}}(G\in\mathscr{G}_p:\dim_{\mathbb{F}_p}(G[p])=j)\ \frac{\#\operatorname{Epi}_{\mathbb{F}_p}(\mathbb{F}_p^j,Y)\cdot\#O(Y)}{\#\operatorname{Hom}_{\mathbb{F}_p}\left(\mathbb{F}_p^j,(R^*/R^{*p})^-\right)}.$$

We will prove the analogous statement of this Conjecture 2.8 for $p=2$ in Theorem 5.2. A concrete special case is given by the following

Conjecture 2.9. *The proportion of $K\in\mathscr{F}(R)$ ordered by the size of their discriminant, for which $\dim_{\mathbb{F}_p}(\mathrm{Cl}(K)[p])=j$ and $\mathrm{Cl}(K,c)[p]$ splits as the direct sum of $\mathrm{Cl}(K)[p]$ and $(\mathscr{O}_K/c)^*[p]$, approaches*

$$\frac{\mu_{\mathrm{CL}}(G\in\mathscr{G}_p:\dim_{\mathbb{F}_p}(G[p])=j)}{\#\operatorname{Hom}_{\mathbb{F}_p}\left(\mathbb{F}_p^j,(R^*/R^{*p})^-\right)}.$$

More generally, as a cruder result, one derives a conjectural formula for the joint distribution of the p-rank of $\mathrm{Cl}(K)$ and of $\mathrm{Cl}(K,c)$, as follows. Fix j_1,j_2 two non-negative integers.

Conjecture 2.10. *As K varies among imaginary quadratic number fields of type R, the proportion of them for which $\dim_{\mathbb{F}_p}(\mathrm{Cl}(K)[p])=j_1$ and $\dim_{\mathbb{F}_p}(\mathrm{Cl}(K,c)[p])=j_2$ approaches*

$$\mu_{\mathrm{CL}}(G\in\mathscr{G}_p:\dim_{\mathbb{F}_p}(G[p])=j_1)\frac{\#\{\varphi:\mathbb{F}_p^{j_1}\to(R^*/R^{*p})^-:\mathrm{rk}(\varphi)=\mathrm{rk}_p(R^*)-(j_2-j_1))\}}{\#\operatorname{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^{j_1},(R^*/R^{*p})^-)}.$$

The statements analogous to Conjectures 2.8 and 2.10 for $p=2$ will be proved in Theorem 5.3, with a more explicit version provided by Theorem 5.4.

2.2. **Agreement with Varma's results.** In this section we make a certain choice for f in Heuristic assumption 2.4 with the aim of stating conjectures for the average of p-torsion of ray class groups. These statements were previously proved for $p=3$ by Varma [18]. In fact, the present paper partly began as an effort to fit her results into a general heuristic framework.

For an element $S\in\mathscr{S}_p(R)$, denote by $M(S)$ the isomorphism class of the middle term of the sequence corresponding to S. Similarly, for $\theta\in\mathrm{Ext}_{\mathbb{Z}_p[C_2]}$ we denote by $M(\theta)$ the isomorphism class of the middle term of the equivalence class of sequences corresponding to θ. We will adopt the standard notation $\widehat{A}$ for the dual of a finite abelian group A.

Proposition 2.11. *We have*

$$\sum_{S\in\mathscr{S}_p(R)}\#M(S)[p]\mu_{\mathrm{seq}}(S)=\#\left(\frac{R^*}{R^{*p}}\right)^+\left(1+\#\left(\frac{R^*}{R^{*p}}\right)^-\right).$$

Proof. By the definition of μ_{seq} we obtain equality of the sum in our proposition with

$$\sum_{G\in\mathscr{G}_p}\frac{\mu_{\mathrm{CL}}(G)}{\#\mathrm{Ext}_{\mathbb{Z}_\iota[C_2]}(G,R^*[p^\infty])}\sum_{\theta\in\mathrm{Ext}_{\mathbb{Z}_p[C_2]}(G,R^*[p^\infty])}\#M(\theta)[p].$$

Again by Proposition 2.7 we know that the map $\theta \to \delta_p(\theta)$ is a surjective homomorphism

$$\mathrm{Ext}_{\mathbb{Z}_p[C_2]}(G, R^*[p^\infty]) \to \mathrm{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)$$

Thus we can rewrite the last sum as

$$\sum_{G\in\mathscr{G}_p} \frac{\mu_{\mathrm{CL}}(G)}{\#\,\mathrm{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)} \sum_{\delta}{}^{*} \#R^*[p] \frac{\#G[p]}{\#\mathrm{Im}(\delta)}, \tag{2.2}$$

where the sum $\sum^*$ is taken over δ in $\mathrm{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)$. For each χ in the dual of $(R^*/R^{*p})^-$ denote by $\mathbf{1}_\chi$ the indicator function of those δ for which χ vanishes on the image of δ. This allows us to recast (2.2) in the following manner,

$$\sum_{G\in\mathscr{G}_p} \frac{\mu_{\mathrm{CL}}(G)}{\#\,\mathrm{Hom}_{\mathbb{Z}_p}(G[p], (R^*/R^{*p})^-)} \sum_{\delta}{}^{*} \#(R^*/R^{*p})^+ \#G[p] \sum_{\chi\in\widehat{(R^*/R^{*p})^-}} \mathbf{1}_\chi(\delta),$$

where δ varies over all elements in $\mathrm{Hom}_{\mathbb{Z}_p}(G[p], (\frac{R^*}{R^{*p}})^-)$. Exchanging the order of summation yields

$$\sum_{G\in\mathscr{G}_p} \#(R^*/R^{*p})^+ \#G[p]\mu_{\mathrm{CL}}(G) \sum_{\chi\in\widehat{(\frac{R^*}{R^{*p}})^-}} \frac{\sum_{\delta\in\mathrm{Hom}_{\mathbb{Z}_p}(G[p],(\frac{R^*}{R^{*p}})^-)} \mathbf{1}_\chi(\delta)}{\#\,\mathrm{Hom}_{\mathbb{Z}_p}(G[p], (\frac{R^*}{R^{*p}})^-)}.$$

The χ-th summand in the last expression equals 1 if χ is the trivial character and equals $\frac{1}{\#G[p]}$ otherwise, thus obtaining

$$\sum_{G\in\mathscr{G}_p} \#(R^*/R^{*p})^+ \#G[p]\Big(1 + \frac{\#(R^*/R^{*p})^- - 1}{\#G[p]}\Big)\mu_{\mathrm{CL}}(G).$$

Recalling the classical equality $\sum_{G\in\mathscr{G}_p} \#G[p]\mu_{\mathrm{CL}}(G) = 2$ provides us with

$$\#(R^*/(R^{*p}))^+\big(2 + \#(R^*/R^{*p})^- - 1\big) = \#(R^*/R^{*p})^+\Big(1 + \#\Big(\frac{R^*}{R^{*p}}\Big)^-\Big),$$

which concludes our proof. □

Combining Proposition 2.11 and Heuristic Assumption 2.4 offers the following.

Conjecture 2.12. *The average value of $\#\,\mathrm{Cl}(K, c)[p]$, as K ranges among imaginary quadratic number fields of type R ordered by their discriminant, is given by*

$$\#\Big(\frac{R^*}{R^{*p}}\Big)^+\Big(1 + \#\Big(\frac{R^*}{R^{*p}}\Big)^-\Big).$$

In particular we can now derive conjectural formulas for the average size of $\mathrm{Cl}(K, c)[p]$ with K varying in larger families.

We next consider here two cases: in §2.2.1 the case when all the primes dividing c are required to be unramified in K, and in §2.2.2 the case where K ranges through all discriminants. The letter l will refer to a prime until the end of §2.

2.2.1. *Collecting unramified discriminants.* Observe that if R correspond to a splitting type where all the primes dividing c are unramified in K, and if p^2 does not divide c (so there is no contribution to the p-part from p itself in case it divides c) then we have that

$$\#\Big(\frac{R^*}{R^{*p}}\Big)^+\Big(1+\#\Big(\frac{R^*}{R^{*p}}\Big)^-\Big)=p^{\#\{l \text{ prime: } l|c,\ l\equiv 1 (\mathrm{mod}\ p)\}}(1+p^{\omega_R(c)}),$$

where $\omega_R(c)$ is defined by

$$\#\{l \text{ prime} : l|c, (l\equiv 1 \pmod p \text{ and } l \text{ is split in } R) \text{ or } (l\equiv -1 \pmod p \text{ and } l \text{ is inert in } R)\}.$$

Therefore when we average over all $2^{\omega(c)}$ choices of R, using the binomial formula we get

$$p^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ p)\}}\Big(1+\Big(\frac{p+1}{2}\Big)^{\#\{l \text{ prime: } l|c, l\equiv 1 \text{ or } -1 (\mathrm{mod}\ p)\}}\Big)$$

as average value of the size of $\mathrm{Cl}(K,c)[p]$ when K ranges over imaginary quadratic number fields unramified at all primes dividing c, as long as $p^2\nmid c$. Instead, if $p^2\mid c$ there is an additional contribution from the principal units modulo p^2 to $\#(\frac{R^*}{R^{*p}})^+(1+\#(\frac{R^*}{R^{*p}})^-)$, which gives

$$p^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ p)\}+1}\Big(1+p\Big(\frac{p+1}{2}\Big)^{\#\{l \text{ prime: } l|c, l\equiv 1 \text{ or } -1 (\mathrm{mod}\ p)\}}\Big).$$

This leads to the Conjecture 1.3 that we stated in the introduction. The special case $p=3$ of Conjecture 1.3 was recently proved by Varma [18, Th.2.(b)].

Theorem 2.13 (Varma)**.** *The average value of* $\#\,\mathrm{Cl}(K,c)[3]$ *as* K *ranges over imaginary quadratic number fields with* $\gcd(\mathrm{D}(K),c)=1$ *is:*
(1)

$$3^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ 3)\}}(1+2^{\#\{l \text{ prime: } l|c,\ l\neq 3\}})$$

if 9 *does not divide* c*.*
(2)

$$3^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ 3)\}+1}(1+3\cdot 2^{\#\{l \text{ prime: } l|c,\ l\neq 3\}})$$

if 9 *divides* c*.*

2.2.2. *Collecting all discriminants.* We now consider the case where K is allowed to ramify at the primes dividing c. Now we have to evaluate

$$\sum_R \#\Big(\frac{R^*}{R^{*p}}\Big)^+\Big(1+\#\Big(\frac{R^*}{R^{*p}}\Big)^-\Big)w(R),$$

where R varies between all the possible types of ring at c, and

$$w(R):=\lim_{X\to+\infty}\frac{\#\{K\in\mathscr{F}_c(R):|\mathrm{D}(K)|\leqslant X\}}{\#\{K\in\mathscr{F}:|\mathrm{D}(K)|\leqslant X\}}.$$

First observe that if $p^2\nmid c$ then

$$\#\Big(\frac{R^*}{R^{*p}}\Big)^+=p^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ p)\}},$$

while if $p^2|c$ then

$$\#\Big(\frac{R^*}{R^{*p}}\Big)^+=p^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ p)\}+1}.$$

Therefore we are left with computing the average of $\#\Big(\frac{R^*}{R^{*p}}\Big)^-$, over all R. But this, as a function of c, is multiplicative, thus we only have to deal with prime powers, i.e. $c=l^n$ for

some prime l and some positive integer n. Clearly, the value of this average is 1 if l is such that $\gcd(p, l^3 - l) = 1$. Instead, if $p|l^2 - 1$ the value of the average is

$$\frac{1}{l+1} + \frac{(\frac{p+1}{2})l}{l+1} = 1 + \Big(\frac{p-1}{2}\Big)\frac{l}{l+1},$$

where the first contribution comes from the R ramified at l, and the second from the R unramified at l. [2] Meanwhile, the value of the average for $p = c$ is

$$\frac{p}{p+1} + \frac{p}{p+1},$$

where the first contribution comes from R ramified at p and the second from R unramified at p. Lastly, we consider the case $p^2|c$. Remarkably enough, one observes that the case $p = 3$ acquires a special status in the computation of this average: indeed $\frac{1}{8}$ of the imaginary quadratics locally at 3 give the extension $\mathbb{Q}_3(\zeta_3)/\mathbb{Q}_3$, and the result for them will be different than for the $\frac{1}{8}$ totally ramified that locally at 3 become $\mathbb{Q}_3(\sqrt{3})$. Clearly for all $p > 3$ there is no p-th root of unity in a quadratic extension of $\mathbb{Q}_p$, so, as we will see, in that case the contribution from the two R ramified at p will be the same.

Assume $p = 3$. The contribution from powers of 3 starting from 9 is

$$\frac{9}{8} + \frac{3}{8} + \frac{9}{4} = \frac{15}{4},$$

where the first contribution is from $\mathbb{Q}_3(\zeta_3)$, the second from $\mathbb{Q}_3(\sqrt{3})$ and the third from unramified R. This gives a prediction that was previously verified by Varma [18, Th.1.(b)].

Theorem 2.14 (Varma)**.** *The average value of* $\#\operatorname{Cl}(K, c)[3]$ *as* K *ranges through imaginary quadratic number fields ordered by their discriminant is:*
(1)

$$3^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ 3)\}}\Big(1 + \prod_{l|c}\Big(1 + \frac{l}{l+1}\Big)\Big)$$

if 3 *does not divide* c*,*
(2)

$$3^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ 3)\}}\Big(1 + \frac{6}{7}\prod_{l|c}\Big(1 + \frac{l}{l+1}\Big)\Big)$$

if 3 *divides* c *but* 9 *does not divide* c*,*
(3)

$$3^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ 3)\}+1}\Big(1 + \frac{15}{7}\prod_{l|c}\Big(1 + \frac{l}{l+1}\Big)\Big)$$

if 9 *divides* c*.*

Now assume that $p > 3$. Then we get

$$\frac{p}{p+1} + \frac{p^2}{p+1},$$

where the first contribution is from the R ramified at p and the second from R unramified at p. Collecting everything together we get the following prediction.

[2] R is said unramified at l if R/lR does not contain non-zero nilpotents. Otherwise R is said ramified at l.

Conjecture 2.15. *Suppose $p > 3$. Then the average value of $\#\operatorname{Cl}(K,c)[p]$ as K ranges over imaginary quadratic number fields ordered by their discriminant is:*
(1)

$$p^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ p)\}}\Big(1+\prod_{l|c, p|l^2-1}\Big(1+\frac{p-1}{2}\frac{l}{l+1}\Big)\Big)$$

if p does not divide c,
(2)

$$p^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ p)\}}\Big(1+\Big(\frac{2p}{p+1}\Big)\prod_{l|c, p|l^2-1}\Big(1+\frac{p-1}{2}\frac{l}{l+1}\Big)\Big)$$

if p divides c but p^2 does not divide c,
(3)

$$p^{\#\{l \text{ prime: } l|c, l\equiv 1 (\mathrm{mod}\ p)\}}\Big(1+\Big(\frac{p+p^2}{p+1}\Big)\prod_{l|c, p|l^2-1}\Big(1+\frac{p-1}{2}\frac{l}{l+1}\Big)\Big)$$

if p^2 divides c.

It would be desirable to extend Varma's arguments to prove Conjecture 2.12 for $p = 3$. In particular, it would be informative to see how the proof distinguishes between the cases $R/3^m = \mathscr{O}_{\mathbb{Q}_3(\zeta_3)}/3^m$ and $R/3^m = \mathscr{O}_{\mathbb{Q}_3(\sqrt{3})}/3^m$, for $m \geqslant 2$.

3. Heuristic and conjectures for $p = 2$

Let c be an odd positive integer. In this section we explain a heuristic model for the 2-part of ray class sequences of conductor c, in the case that no primes dividing c ramify in the fields. The additional difficulty with respect to the case of p odd, is that $\operatorname{Cl}(K)[2^\infty]$ does not behave like a random 2-group (in the sense of Cohen and Lenstra), but instead (as conjectured by Gerth [9]), $2\operatorname{Cl}(K)[2^\infty]$ is believed to behave like a random 2-group: the behavior of $\operatorname{Cl}(K)[2]$ is governed instead by genus theory which trivially excludes any Cohen–Lenstra behavior for $\operatorname{Cl}(K)[2^\infty]$, when K varies among usual families of imaginary quadratic number fields.

Our approach will be as follows: we will see that for 'most' discriminants of type R, $2\operatorname{Cl}(K,c)$ is an extension of $2\operatorname{Cl}(K)$ with a certain subgroup of $\frac{R^*}{\langle -1\rangle}$, which we will call W_R. Nevertheless, one cannot completely ignore the presence of the class group, since it leaves an additional restriction on such extensions. Namely it forces them to belong to a certain subgroup of the Ext, that we will call $\widetilde{\operatorname{Ext}}$. From there we will proceed in analogy with the previous section replacing Ext with $\widetilde{\operatorname{Ext}}$. Using this heuristic we will offer several predictions which are proved in the subsequent sections.

Since we will only consider the case that no primes dividing c ramify in the imaginary number fields K, and since we assume that c is odd, we do not lose generality in assuming that c is also square-free: indeed, in our setting, the 2-part of $(\mathscr{O}_K/c)^*/\langle -1\rangle$ is no different from the one of $(\mathscr{O}_K/c')^*/\langle -1\rangle$, where c' is the square-free part of c. Therefore the choice of a ring type at c amounts to the choice of a partition of the set $S_c := \{l \text{ prime}: \ l|c\}$ in the disjoint union of two sets $S_c(\text{inert})$ and $S_c(\text{split})$. Then one takes $R := (\prod_{l\in S_c(\text{inert})}\mathbb{F}_{l^2})\times(\prod_{l'\in S_c(\text{split})}(\mathbb{F}_{l'})^2)$. For such an R, the C_2-action is given by l-Frobenius on the non-split components, and by swapping on the split components. We will call such R, unramified at c. By a small abuse of notation, we denote by $\mathbb{Z}/c\mathbb{Z}$ the natural image of $\mathbb{Z}/c\mathbb{Z}$ in R.

For R unramified at c, we define

$$W_R := \frac{(\mathbb{Z}/c\mathbb{Z})^*}{\langle -1\rangle}\left(\frac{R^*}{\langle -1\rangle}\right)^2 \subseteq \frac{R^*}{\langle -1\rangle}. \tag{3.1}$$

Now fix some R unramified at c. For the remainder of this section we will assume, for simplicity, the imaginary quadratic number field K to have an odd discriminant. We shall prove that one has an exact sequence

$$2S(K) := (0 \to W_R \to 2\,\mathrm{Cl}(K,c) \to 2\,\mathrm{Cl}(K) \to 0),$$

for all imaginary quadratic number fields of type R with the exception of $O(x(\log x)^{-1/\varphi(c)})$ discriminants up to x. Indeed, by the theory of ambiguous ideals, one has that

$$\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle} \cap 2\,\mathrm{Cl}(K,c) = \langle\{q \text{ prime and } q|\,\mathrm{D}(K)\}\rangle\Big(\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle}\Big)^2.$$

Therefore it is enough to show that the set of positive square-free $D \leqslant x$ such that

$$\{q \pmod c : q \text{ prime and } q|D\} \neq (\mathbb{Z}/c\mathbb{Z})^*$$

is $O(x(\log x)^{-1/\varphi(c)})$. This cardinality is

$$\leqslant \sum_{a\in(\mathbb{Z}/c\mathbb{Z})^*} \sum_{\substack{1\leqslant D\leqslant X\\ p|D\Rightarrow p\neq a(\mathrm{mod}\ c)}} \mu(D)^2 \ll \frac{x}{(\log x)^{1/\varphi(c)}},$$

where the last bound is easily derived by using [12, Eq.(1.85)] with f being the characteristic function of integers all of whose prime divisors are not $a \pmod c$. Identifying $\mathscr{O}_K/c$ with R via a ring isomorphism gives an identification between W_R and

$$\frac{(\mathbb{Z}/c\mathbb{Z})^*}{\langle -1\rangle}\Big(\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle}\Big)^2.$$

Definition 3.1. Among the imaginary quadratic number fields of type R, we call *strongly* of type R, those satisfying

$$\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle} \cap 2\,\mathrm{Cl}(K,c) = \frac{(\mathbb{Z}/c\mathbb{Z})^*}{\langle -1\rangle}\Big(\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle}\Big)^2.$$

Let $E(x)$ denote the cardinality of negative discriminants $1 \pmod 4$ of absolute value at most x and which are of type R but not strongly of type R. The analysis above can be summarised by the bound

$$E(x) \ll \frac{x}{(\log x)^{1/\varphi(c)}}. \tag{3.2}$$

One could be tempted to think of the sequence $S_2(K) := 2S(K)[2^\infty]$ as a 'random' sequence, just as in the previous section. This would be incorrect, since the way the sequences $S_2(K)$ are produced naturally puts on them an additional restriction. Namely one has a commutative diagram of $\mathbb{Z}[C_2]$-modules:

$$\begin{array}{ccccccccc}
0 & \to & \frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle} & \to & \mathrm{Cl}(K,c) & \xrightarrow{\pi} & \mathrm{Cl}(K) \to 0\\
 & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3\\
0 & \to & \frac{(\mathbb{Z}/c\mathbb{Z})^*}{\langle -1\rangle}(\frac{(\mathscr{O}_K/c)^*}{\langle -1\rangle})^2 & \to & 2\,\mathrm{Cl}(K,c) & \to & 2\,\mathrm{Cl}(K) \to 0
\end{array}$$

where i_1, i_2, i_3 are the natural inclusion maps, so i_2 and i_3 consist of isomorphisms between the source groups and the double of the target groups. The top sequence has two obvious properties that are automatically satisfied:

$$\pi(\mathrm{Cl}(K,c)[2^\infty]^-) = \mathrm{Cl}(K)[2^\infty] \text{ and } \pi(\mathrm{Cl}(K,c)[2^\infty]^+) = \mathrm{Cl}(K)[2].$$

The first property is equivalent to the sequence remaining exact after taking $(1+\tau)$-torsion, where τ is the generator of C_2. Indeed, this is equivalent to the natural map

$$\mathrm{Cl}(K)[2^\infty] \to \frac{\frac{R^*}{\langle -1\rangle}}{(\tau+1)\frac{R^*}{\langle -1\rangle}}$$

being the 0-map, which holds since the norm of an integral ideal is always an integer. The second property follows from the fact that we are looking at families of discriminants coprime to c. Therefore we are allowed to lift a prime ideal $\mathfrak{q}$ lying above a prime q dividing $\mathrm{D}(K)$, using the class of the ideal $\mathfrak{q}$ in $\mathrm{Cl}(K,c)$: this class will still be a fixed point, since it is the class of a τ-invariant *ideal*. This motivates the following:

Definition 3.2. Let G be a finite abelian 2-group, viewed as a C_2 module with the $-$id-action. We say that an element θ of $\mathrm{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$:

$$\theta : 1 \to W_R[2^\infty] \to B \to G \to 1$$

is *embeddable* if there is an exact sequence of $\mathbb{Z}_2[C_2]$-modules

$$1 \to \frac{R^*}{\langle -1\rangle}[2^\infty] \to \tilde{B} \to \tilde{G} \to 1$$

and a commutative diagram of $\mathbb{Z}_2[C_2]$-modules

$$\begin{array}{ccccccccc} 0 & \to & \frac{(R)^*}{\langle -1\rangle}[2^\infty] & \to & \tilde{B} & \xrightarrow{\pi} & \tilde{G} & \to & 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 & & \\ 0 & \to & W_R[2^\infty] & \to & B & \to & G & \to & 0 \end{array}$$

where:

• The map $\pi : \tilde{B} \to \tilde{G} \to 1$ satisfies

$$\pi(\tilde{B}^-) = \tilde{G} \text{ and } \pi(\tilde{B}^+) = \tilde{G}[2].$$

• The maps i_2 and i_3 are isomorphisms between the source groups and the double of the target groups. The map i_1 is the natural inclusion.

We denote the set of embeddable extensions by $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$. It will be clear by Proposition 3.5, that the two following sets do not always coincide:

$$\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty]), \mathrm{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty]).$$

On the other hand, the set of embeddable extensions has the algebraic structure that allows us to proceed in perfect parallel with the previous section.

Proposition 3.3. *One has that* $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ *is a subgroup of* $\mathrm{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ *stable under the action of* $\mathrm{Aut}_{\mathrm{ring}}(R) \times \mathrm{Aut}_{\mathrm{ab.gr.}}(G)$.

Proof. Let

$$\begin{array}{ccccccc} 0 & \to & \frac{(R)^*}{\langle -1\rangle}[2^\infty] & \to & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \to 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \to & W_R[2^\infty] & \to & B & \underset{f}{\to} & G \to 0 \end{array}$$

and

$$\begin{array}{ccccccc} 0 & \to & \frac{(R)^*}{\langle -1\rangle}[2^\infty] & \to & \tilde{B}' & \xrightarrow{\pi'} & \tilde{G}' \to 0 \\ & & \uparrow i_1 & & \uparrow i'_2 & & \uparrow i'_3 \\ 0 & \to & W_R[2^\infty] & \to & B' & \underset{f'}{\to} & G \to 0 \end{array}$$

be two embeddable extensions equipped with their respective diagrams. We now consider the following commutative diagram of $\mathbb{Z}_2[C_2]$-modules,

$$\begin{array}{ccccccc} 0 & \to & \frac{(R)^*}{\langle -1\rangle}[2^\infty] & \to & (\tilde{B} \times_G \tilde{B}')/Y' & \xrightarrow{\pi\times\pi'} & \tilde{G} \times_G \tilde{G}' \to 0 \\ & & \uparrow i_1 & & \uparrow i_2 \times i'_2 & & \uparrow i_3 \times i'_3 \\ 0 & \to & W_R[2^\infty] & \to & (B \times_G B')/Y & \underset{f\times f'}{\to} & G \to 0 \end{array}$$

where $\tilde{B} \times_G \tilde{B}' := \{(b_1, b_2) \in \tilde{B} \times \tilde{B}' : 2\pi(b_1) = 2\pi'(b_2)\}$, while Y' denotes the antidiagonal embedding of $\frac{(R)^*}{\langle -1\rangle}[2^\infty]$ in $\tilde{B} \times_G \tilde{B}'$. Similarly $B \times_G B' := \{(b_1, b_2) \in B \times B' : f(g_1) = f'(g_2)\}$, with Y denoting the anti-diagonal embedding of $W_R[2^\infty]$, and

$$\tilde{G} \times_G \tilde{G}' := \{(g_1, g_2) \in \tilde{G} \times \tilde{G}' : 2g_1 = 2g_2\}.$$

There is an obviously induced compatible C_2 action on each terms and one can deduce that

$$(\pi \times \pi')(((\tilde{B} \times_G \tilde{B}')/Y')^-) = \tilde{G} \times_G \tilde{G}' \text{ and } (\pi \times \pi')(((\tilde{B} \times_G \tilde{B}')/Y')^+) = (\tilde{G} \times_G \tilde{G}')[2]$$

using the fact that individually π and π' satisfy the respective property.

On the other hand, by construction one has that $i_2 \times i'_2$ and $i_3 \times i'_3$ are isomorphisms between the source groups and the double of the targets. This shows that $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is closed under addition because the sequence $0 \to W_R[2^\infty] \to (B \times_G B')/Y \to G \to 0$ represents the class of the Baer sum of the two embeddable sequences in $\mathrm{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$. Since $\mathrm{Ext}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is finite, in order to conclude that $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is a subgroup, one is only left to show that $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is non-empty. To this end we refer the reader to Proposition 3.5, which in particular implies that $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is non-empty (alternatively one could also directly prove that the split sequence is embeddable, which one can indeed show using the same steps of the proof of Proposition 3.5). Finally, given an embeddable sequence

$$\begin{array}{ccccccc} 0 & \to & \frac{(R)^*}{\langle -1\rangle}[2^\infty] & \xrightarrow{g} & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \to 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \to & W_R[2^\infty] & \xrightarrow{h} & B & \underset{f}{\to} & G \to 0 \end{array}$$

and a pair $(\varphi_1, \varphi_2) \in \mathrm{Aut}_{\mathrm{ring}}(R) \times \mathrm{Aut}_{\mathrm{ab.gr.}}(G)$, we can consider

$$\begin{array}{ccccccc} 0 & \to & \frac{(R)^*}{\langle -1\rangle}[2^\infty] & \xrightarrow{g\varphi_1} & \tilde{B} & \xrightarrow{\pi} & \tilde{G} \to 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3\varphi_2^{-1} \\ 0 & \to & W_R[2^\infty] & \xrightarrow{h\varphi_1} & B & \underset{\varphi_2 f}{\to} & G \to 0 \end{array}$$

which gives an embeddability diagram for the sequence

$$(\varphi_1, \varphi_2)(0 \to W_R[2^\infty] \to B \to G \to 0)$$

showing that $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ is stable under the action of $\mathrm{Aut}_{\mathrm{ring}}(R) \times \mathrm{Aut}_{\mathrm{ab.gr.}}(G)$. □

Denote by $\mathscr{G}_2$ a set of representatives of isomorphism classes of finite abelian 2-groups, viewed as C_2-modules under the action of $-\mathrm{Id}$. For an imaginary quadratic number field K, denote by $G_2(K)$ the unique representative of $2\,\mathrm{Cl}(K)[2^\infty]$ in $\mathscr{G}_2$. Suppose K is strongly of type R. Then $(\mathscr{O}_K/c)^*/\langle -1\rangle$ can be identified with $R^*/\langle -1\rangle$ via any restriction of a ring isomorphism, that is via any element of $\mathrm{Isom}_{\mathrm{ring}}(\mathscr{O}_K/c, R)$. Furthemore, we can identify $2\,\mathrm{Cl}(K)[2^\infty]$ and $G_2(K)$ via any element of $\mathrm{Isom}_{\mathrm{ab.gr.}}(\mathrm{Cl}(K)[2^\infty], G)$. Therefore applying $\mathrm{Isom}_{\mathrm{ring}}(\mathscr{O}_K/c, R) \times \mathrm{Isom}_{\mathrm{ab.gr.}}(2\,\mathrm{Cl}(K)[2^\infty], G_2(K))$ to $S_2(K)$, we obtain a unique orbit

$$O_{c,2}(K) \in \widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G_2(K), W_R[2^\infty])/(\mathrm{Aut}_{\mathrm{ring}}(R) \times \mathrm{Aut}_{\mathrm{ab.gr.}}(G)).$$

For K strongly of type R we use the notation

$$S_2'(K) := (G_2(K), O_{c,2}(K)).$$

If K is not strongly of type R, we set $S_2'(K)$ to be the symbol $\bullet$. We now proceed by offering a heuristic model for $S_2'(K)$ as K varies among imaginary quadratic number fields of type R. Let R be an unramified ring at c and denote by $\mathscr{G}_2$ a set of representatives of isomorphism classes of finite abelian 2-groups, viewed as C_2-modules under the action of $-\mathrm{Id}$. Denote by $\mathscr{S}_2(R)$ the union of the singleton $\{\bullet\}$ and of the set of equivalence classes of pairs (G, θ), where $G \in \mathscr{G}_2$, $\theta \in \widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$ and the equivalence is defined as follows: two pairs $(G_1, \theta_1), (G_2, \theta_2)$ are identified if $G_1 = G_2$ and θ_1, θ_2 are in the same $\mathrm{Aut}_{\mathrm{ring}}(R) \times \mathrm{Aut}_{\mathrm{ab.gr.}}(G)$-orbit. Denote by $\widetilde{\mathscr{S}_2}(R)$ the union of the singleton $\{\bullet\}$ and the set of pairs (G, θ), where $G \in \mathscr{G}_2$ and $\theta \in \widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])$, thus bringing into play the quotient map

$$\pi : \widetilde{\mathscr{S}_2}(R) \to \mathscr{S}_2(R).$$

Consider the sigma algebra generated by all subsets on $\widetilde{\mathscr{S}_2}(R)$, as well as on $\mathscr{S}_2(R)$, and equip $\widetilde{\mathscr{S}_2}(R)$ with the measure

$$\widetilde{\mu}_{\mathrm{seq}}((G, \theta)) := \frac{\mu_{\mathrm{CL}}(G)}{\#\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R[2^\infty])}, \widetilde{\mu}_{\mathrm{seq}}(\{\bullet\}) = 0,$$

where μ_{CL} denotes, as usual, the Cohen–Lenstra probability measure on $\mathscr{G}_2$ that gives to each abelian 2-group G weight inversely proportional to the size of the automorphism group of G. Push forward, via π, the measure $\widetilde{\mu}_{\mathrm{seq}}$ to a measure μ_{seq} on $\mathscr{S}_2(R)$. It is clear by construction that $\widetilde{\mu}_{\mathrm{seq}}$ and μ_{seq} are probability measures.

The heuristic assumption that we propose for the 2-part of ray class sequences of conductor c of imaginary quadratic fields of type R is as follows.

Heuristic assumption 3.4. *For any 'reasonable' function $f : \mathscr{S}_2(R) \to \mathbb{R}$ one has that, as K varies among imaginary quadratic number fields of type R, the following equality of averages takes place*

$$\lim_{X \to \infty} \frac{\sum_{-\mathrm{D}(K) \leqslant X} f(S_2'(K))}{\#\{-\mathrm{D}(K) \leqslant X\}} = \sum_{S \in \mathscr{S}_2(R)} f(S)\mu_{\mathrm{seq}}(S).$$

As a consistency check, observe that the above identity of average takes place if one chooses as f the indicator function of $\{\bullet\}$: indeed, since the number of K with $\mathrm{D}(K) \leqslant X$ that are not strongly of type R is at most $\ll_c X(\log X)^{-1/\varphi(c)}$, we see that we obtain 0 in the left side, while in the right side we obtain 0 by definition. Clearly one can readily formulate the analogues of Conjectures 2.5 and 2.6. We shall instead opt to devote the rest of the section to the analogues of Conjectures 2.8-2.10.

If $\alpha \in R^*/\langle -1\rangle$ then $\alpha^2 N(\alpha) \in W_R$, where $N(\cdot)$ is the norm-function with respect to the C_2-action prescribed to $R^*/\langle -1\rangle$: indeed both α^2 and $N(\alpha)$ are in W_R. We define the map $g_R : R^*/\langle -1\rangle \to W_R$ given by $\alpha \mapsto \alpha^2 N(\alpha)$. With a small abuse of notation, we use the same notation for the induced map $g_R : \frac{R^*/\langle -1\rangle}{(R^*/\langle -1\rangle)^2} \to W_R/2W_R$ and we denote by $\mathrm{Im}(g_R)$ the image of g_R in $W_R/2W_R$.

Proposition 3.5. *The image of the natural map*

$$\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G, W_R) \to \mathrm{Hom}_{\mathbb{F}_2[C_2]}(G[2], W_R/2W_R)$$

is

$$\mathrm{Hom}_{\mathbb{F}_2[C_2]}(G[2], \mathrm{Im}(g_R)) \quad (= \mathrm{Hom}_{\mathbb{F}_2}(G[2], \mathrm{Im}(g_R))).$$

Proof. Consider θ an embeddable sequence

$$\begin{array}{ccccccccc} 0 & \to & \frac{(R)^*}{\langle -1\rangle}[2^\infty] & \to & \tilde{B} & \stackrel{\pi}{\to} & \tilde{G} & \to & 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 & & \\ 0 & \to & W_R[2^\infty] & \to & B & \underset{f}{\to} & G & \to & 0 \end{array}$$

and pick $b \in G[2]$. By definition of embeddability there exist $\mathfrak{b}$ in $\tilde{B}^+$ such that $\pi(\mathfrak{b}) = i_3(b)$. On the other hand we can find $x \in \tilde{B}$ such that $\pi(2x) = i_3(b)$. Therefore there exists an element $\alpha \in \frac{(R)^*}{\langle -1\rangle}[2^\infty]$ such that $\mathfrak{b}\alpha^{-1} = x^2$, which implies that $\mathfrak{b}^2 N(\alpha)^{-1} = N(x)^2$. Furthermore, $2x$ is in B, hence we have that $\delta_2(\theta)(b) = \mathfrak{b}^2\alpha^{-2}$ as an element of $W_R/2W_R$. However note that $N(x)^2 \in 2W_R$: indeed, by definition of embeddability, we can always write $x = x^- \beta$ with x^- an anti-fixed point and $\beta \in \frac{R^*}{\langle -1\rangle}$, so that $N(x)^2 = N(\beta)^2 \in W_R$. Therefore we find that $\delta_2(\theta)(b) = N(\alpha)\alpha^2$, i.e. $\delta_2(\theta)(b) \in \mathrm{Im}(g_R)$.

Conversely, we prove that given a C_2-map $\delta_0 : G[2] \to \mathrm{Im}(g_R)$, there exists a $\theta \in \widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}$ such that $\delta_2(\theta) = \delta_0$. Firstly observe that $\mathrm{Hom}_{\mathbb{F}_2[C_2]}(G[2], \mathrm{Im}(g_R)) = \mathrm{Hom}_{\mathbb{F}_2}(G[2], \mathrm{Im}(g_R)))$, since τ clearly fixes $N(\alpha)$ for any α in R and $\alpha^2\tau(\alpha^2) = N(\alpha)^2 \in 2W_R$, therefore τ acts trivially on $\mathrm{Im}(g_R)$ (see Lemma 3.6 for a more general fact). Thus pick $\delta_0 \in \mathrm{Hom}_{\mathbb{F}_2}(G[2], \mathrm{Im}(g_R)))$. We divide the construction of θ and its embedding in four steps:
Step 1: Observe that $\alpha^2 N(\alpha) = \frac{\alpha^2}{N(\alpha)} N(\alpha)^2 = \frac{\alpha}{\tau(\alpha)} N(\alpha)^2$. Since $N(\alpha)^2 \in 2W_R[2^\infty]$, we conclude that any element of $\mathrm{Im}(g_R)$ can be represented as $\frac{\alpha}{\tau(\alpha)}$ for some $\alpha \in \frac{R^*}{\langle -1\rangle}[2^\infty]$.
Step 2: Write $G = \langle e_1\rangle \oplus \ldots \oplus \langle e_j\rangle$, with the order of e_i being 2^{m_i} for a positive integer m_i, for each $i \in \{1, \ldots, j\}$. Therefore $G[2] = \langle 2^{m_1-1}e_1\rangle \oplus \ldots \oplus \langle 2^{m_j-1}e_j\rangle$ and now, use Step 1 for each $i \in \{1, \ldots, j\}$ to construct $\alpha_i \in \frac{R^*}{\langle -1\rangle}[2^\infty]$ such that $\delta_0(2^{m_i-1}e_i) = \frac{\alpha_i}{\tau(\alpha_i)}$.
Step 3: Embed G in a group $\tilde{G} = \langle \tilde{e}_1\rangle \oplus \ldots \oplus \langle \tilde{e}_j\rangle \oplus \langle d_1\rangle \oplus \ldots \oplus \langle d_h\rangle$, with the rules $2\tilde{e}_i = e_i$ for every i in $\{1, \ldots, j\}$, $2d_s = 0$ for every $s \in \{1, \ldots, h\}$ and $h \geqslant \mathrm{rk}_2((\mathbb{Z}/c\mathbb{Z}^*)) - 1$. Take an extension $\theta \in \mathrm{Ext}_{\mathbb{Z}_2}(\tilde{G}, \frac{R^*}{\langle -1\rangle})$ such that for every $i \in \{1, \ldots, j\}$ one has that $\delta_{2^{m_i+1}}(\theta)(\tilde{e}_i) = \frac{\alpha_i}{\tau(\alpha_i)}$ and such that $\langle \{\delta_2(\theta)(d_1), \ldots, \delta_2(\theta)(d_h)\}\rangle = \mathrm{Im}((\mathbb{Z}/c\mathbb{Z})^* \to W_R/2W_R)$. Call $\tilde{B}$ the middle term of this extension. Pick $\tilde{e}'_1, \ldots, \tilde{e}'_j$ liftings of $e_1, \ldots, e_j$ with the property that $2^{m_i+1}\tilde{e}'_i = \frac{\alpha_i}{\tau(\alpha_i)}$

for all i in $\{1,\dots,j\}$. Choose also $d'_1,\dots,d'_h$ liftings of $d_1,\dots,d_h$ in $\tilde{B}$ and put $2\tilde{B}=B$. Observe that by construction the kernel of $B\to G$ is $W_R[2^\infty]$. This gives a commutative diagram of $\mathbb{Z}_2$-modules,

$$\begin{array}{ccccccc} 0 & \to & \frac{(R)^*}{\langle -1\rangle}[2^\infty] & \to & \tilde{B} & \stackrel{\pi}{\to} & \tilde{G}\to 0 \\ & & \uparrow i_1 & & \uparrow i_2 & & \uparrow i_3 \\ 0 & \to & W_R[2^\infty] & \to & B & \underset{f}{\to} & G\to 0. \end{array}$$

By construction i_2 and i_3 are isomorphisms between the source groups and the double of the target groups.

Step 4: Define $A_1:=\langle\{\tilde{e}'_1,\dots,\tilde{e}'_j\}\rangle$, $A_2:=\langle\{d'_1,\dots,d'_h\}\rangle$ and $A:=\langle A_1,A_2\rangle$. Consider A_1 as a C_2-module with the $-$Id-action and A_2 with the Id-action. Observe that, by construction, the C_2-action on A_1 and A_2 restrict to the same C_2-action on $A_1\cap A_2$. Therefore the C_2-action extend to an action on A. Observe that, by construction, the C_2-action on A and $\frac{R^*}{\langle -1\rangle}[2^\infty]$ restricts to the same C_2-action on $A\cap\frac{R^*}{\langle -1\rangle}[2^\infty]$. It is also clear that $\langle A,\frac{R^*}{\langle -1\rangle}[2^\infty]\rangle=\tilde{B}$. Therefore one can put on $\tilde{B}$ a C_2-action which restricted to A is $-$Id and restricted to $\frac{R^*}{\langle -1\rangle}$ is the usual action. This turns the above diagram into a diagram of C_2-modules, and we want to prove that the top sequence remains exact when we take $(1+\tau)$-torsion and when we take $(1-\tau)$-torsion. But by construction

$$\begin{aligned}(1+\tau)(\tilde{B}) &= (1+\tau)\Big(\langle A_1,A_2,R^*/\langle -1\rangle\rangle\Big)=(1+\tau)\Big(\langle A_2,R^*/\langle -1\rangle\rangle\Big)\\ &=\langle 2A_2,(1+\tau)(R^*/\langle -1\rangle)\rangle\subseteq\langle(1+\tau)(R^*/\langle -1\rangle)\rangle\end{aligned}$$

and

$$\begin{aligned}(1-\tau)(\pi^{-1}(\tilde{G}[2]) &= (1-\tau)(\langle A_1\cap\ker(2\pi),R^*/\langle -1\rangle\rangle)\\ &=\langle 2(A_1\cap\ker(2\pi)),(1-\tau)(R^*/\langle -1\rangle)\rangle\\ &\subseteq(1-\tau)(R^*/\langle -1\rangle),\end{aligned}$$

where the last two inclusions follow from Step 3. This shows that δ_0 can be realized as $\delta_2(\theta)$ for some θ in $\widetilde{\mathrm{Ext}}_{\mathbb{Z}_2[C_2]}(G,W_R[2^\infty])$ (i.e. $0\to W_R[2^\infty]\to B\stackrel{f}{\to}G\to 0$). □

If K is strongly of type R, we denote by $\delta_2(K)$ the map $\delta_2(S_2(K))$. By choosing any ring identification in $\mathrm{Isom}_{\mathrm{ring}}(\mathscr{O}_K/c,R)$ and any identification in $\mathrm{Isom}_{\mathrm{ab.gr.}}(2\,\mathrm{Cl}(K),G_2(K))$ we obtain an $\mathrm{Aut}_{\mathrm{ring}}(R)$-orbit of subspaces of $W_R/2W_R$. On the other hand this orbit is composed of a single element due to the following fact:

Lemma 3.6. *The action of* $\mathrm{Aut}_{\mathrm{ring}}(R)$ *on* $\mathrm{Im}(g_R)$ *is trivial.*

Proof. Consider the ring decomposition $R=\prod_{l|c}R/lR$. It is clear that the following holds, $\mathrm{Aut}_{\mathrm{ring}}(R)=\prod_{l|c}\mathrm{Aut}_{\mathrm{ring}}(R/lR)$. On the other hand, this decomposition is compatible with g_R, i.e. $g_R=\prod_{l|c}g_{R/lR}$, where $\prod$ of maps is to be thought of as the map obtained by applying the maps coordinatewise. This reduces the claim to $c=l$ a prime number. In that case one has that $\alpha^2\tau(\alpha)^2=N(\alpha)^2$, but $N(\alpha)^2$ is in $2W_R$, therefore, modulo $2W_R$, one has that $\alpha^2N(\alpha)$ is fixed by τ. □

Hence we see that $\mathrm{Im}(\delta_2(K))$ can be identified with a well-defined subgroup of $\mathrm{Im}(g_R)$. We will keep denoting this subgroup as $\mathrm{Im}(\delta_2(K))$. Moreover, thanks to Proposition 3.5 and the fact that the pushforward, via an epimorphism, of the counting probability measure induces

the counting probability measure on the target group, we readily obtain the prediction of the distribution of the pair $(\#(2\,\mathrm{Cl}(K))[2], \mathrm{Im}(\delta_2(K)))$.

Fix a subspace $Y \subseteq \mathrm{Im}(g_R)$ and a non-negative integer j.

Prediction 3.7. *As K varies among imaginary quadratic number fields of type R, we have the following equality*

$$\lim_{X\to\infty} \frac{\#\{K : -\mathrm{D}(K) \leqslant X, \#(2\,\mathrm{Cl}(K))[2] = 2^j \text{ and } \mathrm{Im}(\delta_2(K)) = Y\}}{\#\{K : -\mathrm{D}(K) \leqslant X\}}$$
$$= \mu_{\mathrm{CL}}(G \in \mathscr{G}_2 : \#G[2] = 2^j) \frac{\#\,\mathrm{Epi}_{\mathbb{F}_2}(\mathbb{F}_2^j, Y)}{\#\,\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^j, \mathrm{Im}(g_R))}.$$

This will be proved in Theorem 5.2, but see also Theorem 5.4 for a more explicit statement. A crucial step is to deduce it from a statement about *mixed moments*. Indeed, observe that to know the pair

$$(\#G[2], \mathrm{Im}(\delta : G[2] \to \mathrm{Im}(g_R)))$$

is equivalent to knowing for each χ in the dual group $\widehat{\mathrm{Im}(g_R)}$, the value of

$$m_\chi(\delta) := \#\ker(\chi(\delta)).$$

For each $\chi \in \widehat{\mathrm{Im}(g_R)}$, fix a non-negative integer k_χ.

Notation. For any function $\widehat{\mathrm{Im}(g_R)} \to \mathbb{Z}_{\geqslant 0}$, $\chi \mapsto k_\chi$, we will use the notation

$$|\mathbf{k}|_1 := \sum_{\chi \in \widehat{\mathrm{Im}(g_R)}} k_\chi.$$

Pick a random subset of $\widehat{\mathrm{Im}(g_R)}$ by choosing each character χ independently at random with the rule that χ is not in the set with probability $\frac{1}{2^{k_\chi}}$ and that χ is in the set with probability $\frac{2^{k_\chi}-1}{2^{k_\chi}}$. For a subspace $Y \subseteq \widehat{\mathrm{Im}(g_R)}$ denote by $\mathbb{P}_{(k_\chi)}(Y)$ the probability that such a random subset generates Y. Observe that if $\dim(Y) > |\mathbf{k}|_1$ then $\mathbb{P}_{(k_\chi)}(Y) = 0$: indeed, in that case we select with probability 1 less characters than $\dim_{\mathbb{F}_2}(Y)$, so they they generate Y with zero probability. Denote by $\mathscr{N}_2(j)$ the number of vector subspaces of $\mathbb{F}_2^j$. If $j < 0$, we shall make sense of the expression $0 \cdot \mathscr{N}_2(j)$ by setting it equal to 0.

The following proposition reveals the value predicted by the heuristic model for the $(k_\chi)_{\chi \in \widehat{\mathrm{Im}(g_R)}}$-mixed moment. In what follows we use the convention $m_\chi(\delta_S) = 0$ if we have $S = \bullet \in \mathscr{S}_2(R)$.

Proposition 3.8. *One has that*

$$\sum_{S \in \mathscr{S}_2(R)} \mu_{\mathrm{seq}}(S) \prod_{\chi \in \widehat{\mathrm{Im}(g_R)}} m_\chi(\delta_S)^{k_\chi} = \sum_{Y \subseteq \widehat{\mathrm{Im}(g_R)}} \mathbb{P}_{(k_\chi)}(Y) \mathscr{N}_2(|\mathbf{k}|_1 - \dim(Y)).$$

We do not spell out the proof of Proposition 3.8 because it is identical to the proof of Proposition 4.8 which we will provide in §4.

Proposition 3.8 leads to the following prediction.

Prediction 3.9. *As K varies among imaginary quadratic number fields of type R, the following equality of averages takes place*

$$\lim_{X\to\infty}\frac{\sum_{-\mathrm{D}(K)\leqslant X}\prod m_\chi(\delta_2(K))^{k_\chi}}{\#\{K:-\mathrm{D}(K)\leqslant X\}}=\sum_{V\subseteq\widehat{Im(g_R)}}\mathbb{P}_{(k_\chi)}(V)\mathscr{M}_2(|\mathbf{k}|_1-\dim(V)).$$

A stronger statement will be proved in Theorem 5.1.

As a cruder result, one derives a prediction for the joint-distribution of the 4-ranks of the class group and the ray class group. Let j_1, j_2 be two non-negative integers. Then we have the following prediction.

Prediction 3.10. *As K varies among imaginary quadratic number fields of type R, we have the following equality*

$$\lim_{X\to\infty}\frac{\#\{K:-\mathrm{D}(K)\leqslant X,\mathrm{rk}_4(\mathrm{Cl}(K))=j_1,\mathrm{rk}_4(\mathrm{Cl}(K,c))=j_2\}}{\#\{K:-\mathrm{D}(K)\leqslant X\}}$$
$$=\mu_{\mathrm{CL}}(G\in\mathscr{G}_2:\dim_{\mathbb{F}_2}(G[2])=j_1)\frac{\#\{\varphi\in\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1},\mathrm{Im}(g_R)):\mathrm{rk}(\varphi)=\mathrm{rk}_2(W_R)-(j_2-j_1)\}}{\#\,\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1},\mathrm{Im}(g_R))}.$$

This will be proved in Theorem 5.3, but see also Theorem 5.4 for a more explicit law. Similarly, the heuristic of the present section can be used to conjecturally predict the distribution of the pair $(\mathrm{rk}_{2^m}(\mathrm{Cl}(K)),\mathrm{rk}_{2^m}(\mathrm{Cl}(K,c)))$ among imaginary quadratic number fields K with $\gcd(\mathrm{D}(K),c)=1$. For reasons of space we do not explicitly state such a conjecture but it is implicitly given in the present section; such a conjecture might be within reach given the recent work of Smith [16].

4. Special divisors and 4-rank

Let D be a square-free odd positive integer. In this section we introduce the notion of *special divisors* of D, which will be instrumental in our proof of Theorems 5.1, 5.2, 5.3, and 5.4. We call a positive divisor d of D *special* if d is a square modulo D/d and D/d is a square modulo d. We denote by $S(D)$ the set of special divisors of D, and by $T(D)$ the set of all divisors of D. The set $T(D)$ has naturally the structure of a vector space over $\mathbb{F}_2$ under the operation

$$d_1\odot d_2:=\frac{d_1d_2}{\gcd(d_1,d_2)^2}.$$

Lemma 4.1. *The set $S(D)$ is a subspace of $T(D)$ over $\mathbb{F}_2$.*

Proof. We need to show that if d_1, d_2 are special then $d_1\odot d_2$ is special as well. This amount to showing firstly that if a prime q divides D but $q\nmid d_1\odot d_2$ then $d_1\odot d_2$ is a square (mod q) and secondly that if a prime q divides $d_1\odot d_2$ then $D/d_1\odot d_2$ is a square (mod q).

For the proof of the first claim, suppose that $q|D$ but $q\nmid d_1\odot d_2$. Then either $\gcd(d_1d_2,q)=1$ or $q|\gcd(d_1,d_2)$. In the first case we know that, since both d_1 and d_2 are special, d_1 and d_2 are both squares (mod q), thus showing that $d_1\odot d_2$ is a square (mod q). In the second case we know that, since both d_1 and d_2 are special, D/d_1 and D/d_2 are both squares (mod q). This shows that

$$\frac{D}{d_1}\frac{D}{d_2}=(d_1\odot d_2)\left(\frac{D}{\frac{d_1d_2}{\gcd(d_1,d_2)}}\right)^2$$

is a square (mod q), hence $d_1 \odot d_2$ is a square (mod q).

Next, suppose that $q \mid d_1 \odot d_2$. Then, either $q \mid d_1$ and $q \nmid d_2$, or $q \mid d_2$ and $q \nmid d_1$: by symmetry we are allowed to focus on the former case. Then, since both d_1 and d_2 are special, we have that both D/d_1 and d_2 are squares (mod q). Therefore

$$\frac{D}{d_1}\frac{1}{d_2}\gcd(d_1,d_2)^2 = \frac{D}{(d_1 \odot d_2)}$$

is a square (mod q), thus concluding our proof. □

Let n be another square-free odd positive integer with $\gcd(n, D) = 1$ and consider the group $G_n := (\mathbb{Z}/n\mathbb{Z})^*/(\mathbb{Z}/n\mathbb{Z})^{*2}$. One has a natural map $\varphi_{n,D} : S(D) \to G_n$ by reducing (mod n) and then modulo squares.

Lemma 4.2. *The map $\varphi_{n,D}$ is a homomorphism of $\mathbb{F}_2$-vector spaces.*

Proof. By definition we have $d_1 \odot d_2 = \frac{d_1 d_2}{\gcd(d_1,d_2)^2}$ and reducing this equality (mod n) and then modulo squares, the right side yields $d_1 d_2$. Thus $\varphi_{n,D}(d_1 \odot d_2) = \varphi_{n,D}(d_1)\varphi_{n,D}(d_2)$. □

Observe that $S(D)$ always contains the subgroup $\{1, D\}$. It is then a consequence of the work of Fouvry and Klüners [8] that $S(D)/\{1, D\}$ behaves like the 2-torsion of a random abelian 2-group, in the sense of Cohen and Lenstra. In other words, for every positive integer j we have

$$\lim_{X\to\infty} \frac{\#\{1 \leqslant D \leqslant X, D \text{ square-free} : S(D)/\{1,D\} \cong \mathbb{F}_2^j\}}{\#\{1 \leqslant D \leqslant X, D \text{ square-free}\}} = \mu_{\mathrm{CL}}(A \in \mathscr{G}_2 : A[2] \cong \mathbb{F}_2^j),$$

where $\mathscr{G}_2$ is a set of representatives of isomorphism classes of finite abelian 2-groups. The present section in addition to Theorems 5.6-5.7, §6 and §7 are devoted to the determination of the distribution of the pair

$$(\#S(D), \mathrm{Im}(\varphi_{n,D})).$$

The general heuristic constructed in §3 specializes to a heuristic model for this pair, thanks to the commutative diagram after Lemma 5.5. However, we choose to give here a direct presentation of this heuristic avoiding ray class groups. Therefore the present section, Theorems 5.6-5.7, §6 and §7 are completely self-contained.

Before proceeding we introduce a modification of $\varphi_{n,D}$ which will be required in the ray class group applications in §5. Denote by L_n the subgroup of G_n generated by an integer which is a quadratic non-residue modulo every prime dividing n and write $\widetilde{G}_n := G_n/L_n$. Now let n_1, n_2 be two integers such that $2Dn_1n_2$ is square-free and assume that D is a square modulo n_1 and generates L_{n_2} (mod n_2). Denote by $\varphi_{n_1,n_2,D}$ the natural map

$$\varphi_{n_1,n_2,D} : S(D)/\{1, D\} \to G_{n_1} \times \widetilde{G}_{n_2}.$$

Our goal is to understand the statistical behavior of the pair

$$(\#S(D), \mathrm{Im}(\varphi_{n_1,n_2,D})),$$

as D varies through positive square-free integers coprime to n_1n_2, which are squares (mod n_1) and non-squares modulo every prime dividing n_2. There is an obvious guess: namely that, once $\dim_{\mathbb{F}_2}(S(D)/\{1, D\}) = j$ is fixed, then $\mathrm{Im}(\varphi_{n_1,n_2,D})$ should distribute as the image of a random map $\varphi : \mathbb{F}_2^j \to G_{n_1} \times \widetilde{G}_{n_2}$. We formalize this guess in a more general heuristic principle.

Definition 4.3. Consider the set $\mathscr{M}_{n_1,n_2}$ consisting of equivalence classes of pairs (A,V), where A is a vector space over $\mathbb{F}_2$ and V is a vector subspace of $G_{n_1}\times\widetilde{G}_{n_2}$: declare $(A_1,V_1),(A_2,V_2)$ identified, if A_1 and A_2 have the same $\mathbb{F}_2$-dimension and $V_1=V_2$. Denote this equivalence relation by $\sim$. Each representative pair $(\mathbb{F}_2^j,V)$ is equipped with the following mass,

$$\mu((\mathbb{F}_2^j,V)):=\mu_{\mathrm{CL}}(A\in\mathscr{G}_2:A[2]\cong\mathbb{F}_2^j)\frac{\#\operatorname{Epi}_{\mathbb{F}_2}(\mathbb{F}_2^j,V)}{\#\operatorname{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^j,G_{n_1}\times\widetilde{G}_{n_2})}.$$

By construction, this is a probability measure on $\mathscr{M}_{n_1,n_2}$.

Now we formulate the following.

Heuristic assumption 4.4. *For any 'reasonable' function $f:\mathscr{M}_{n_1,n_2}\to\mathbb{R}$ one has*

$$\lim_{X\to\infty}\frac{\sum_{D\leqslant X}f((S(D)/\{1,D\},\operatorname{Im}(\varphi_{n_1,n_2,D})))}{\sum_{D\leqslant X}1}=\sum_{T\in\mathscr{M}_{n_1,n_2}}f(T)\mu(T),$$

where in both sums D varies among square-free positive integers which are squares (mod n_1) *and non-squares modulo any prime divisor of n_2. Furthermore, for any positive integers a,r with* $\gcd(r,an_1n_2)=1$ *the same holds if we have the additional restriction $D\equiv a\,(\mathrm{mod}\ r)$.*

The simple case where f is the indicator function of an element $(\mathbb{F}_2^j,V)\in\mathscr{M}_{n_1,n_2}$ yields the following prediction.

Prediction 4.5. *We have*

$$\lim_{X\to\infty}\frac{\#\{D\leqslant X,(S(D)/\{1,D\},\varphi_{n_1,n_2,D})\sim T\}}{\#\{D\leqslant X\}}=\mu(T),$$

where D varies among square-free positive integers which are squares (mod n_1) *and non-squares modulo every prime divisor of n_2.*

This prediction will be confirmed in Theorem 5.7.

Despite the fact that the 'random variable' $(S(D),\operatorname{Im}(\varphi_{n_1,n_2,D}))$ does not consist of two *numbers*, we achieve its distribution by means of the moment-method. For this we shall replace the pair $(S(D),\operatorname{Im}(\varphi_{n_1,n_2,D}))$ by a *higher-dimensional numerical* 'random variable', which we proceed to define. For each character χ in the dual of $G_{n_1}\times\widetilde{G}_{n_2}$ define

$$m_\chi(D):=\#\{d\in S(D):\chi(\varphi_{n_1,n_2,D}(d))=1\}\tag{4.1}$$

and recall that $\operatorname{Im}(\varphi_{n_1,n_2,D})^\perp$ is the set of all character χ with $\chi\circ\varphi_{n_1,n_2,D}$ being trivial. Clearly for each $\chi\in\operatorname{Im}(\varphi_{n_1,n_2,D})^\perp$ we have $m_\chi(D)=m_1(D)=\#S(D)$, while for the remaining characters we have $m_\chi(D)=\#S(D)/2$. Therefore the knowledge of the pair

$$(\#S(D),\operatorname{Im}(\varphi_{n_1,n_2,D}))$$

is equivalent to the knowledge of

$$(m_\chi(D))_{\chi\in\widehat{G}_{n_1}\times\widehat{\widetilde{G}}_{n_2}}.$$

It will transpire that this shift in focus will be advantageous since it will allow us to study the asymptotic behaviour of the latter vector by the method of moments.

We conclude this section by providing a prediction regarding the mixed moments of $(m_\chi(D))$. This will be later used in the proof of Theorem 5.6.

Notation 4.6. For any function $\widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2} \to \mathbb{Z}_{\geqslant 0}$, $\chi \mapsto k_\chi$, we will use the notation

$$\mathbf{k} := (k_\chi)_{\chi \in \widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}} \quad \text{and} \quad |\mathbf{k}|_1 := \sum_{\chi \in \widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}} k_\chi.$$

Definition 4.7. For any subspace $Y \subseteq \widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}$, denote by $\mathbb{P}_{(k_\chi)}(Y)$ the probability that a random subset of $\widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}$ generates Y, where the characters χ are chosen independently and with probability $1 - 2^{-k_\chi}$.

For any pair $(\mathbb{F}_2^j, Y)$ in $\mathscr{M}_{n_1,n_2}$, define $m_\chi((\mathbb{F}_2^j, Y))$ to be 2^j if $\chi(Y) = 1$, and 2^{j-1} otherwise. Observe that if $\dim(Y) > |\mathbf{k}|_1$ then $\mathbb{P}_{(k_\chi)}(Y) = 0$. Denote by $\mathscr{N}_2(j)$ the number of vector subspaces of $\mathbb{F}_2^j$. If $j < 0$ we define $\mathscr{N}_2(j) := 1$. It is important to note that every time $\mathscr{N}_2(j)$ appears for some negative j then it will always appear multiplied by zero.

Proposition 4.8. *One has that*

$$\sum_{T \in \mathscr{M}_{n_1,n_2}} \Big(\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}} m_\chi(T)^{k_\chi} \Big) \mu(T) = \sum_{W \subseteq \widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}} \mathbb{P}_{(k_\chi)}(W) \mathscr{N}_2(|\mathbf{k}|_1 - \dim(W)).$$

Proof. We want to compute

$$\sum_{(\mathbb{F}_2^j, \delta)} \Big(\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}} m_\chi((\mathbb{F}_2^j, \delta))^{k_\chi}) \Big) \mu((\mathbb{F}_2^j, \delta)),$$

where j ranges over non-negative integers, δ ranges over $\mathrm{Hom}(\mathbb{F}_2^j, G_{n_1} \times \widetilde{G}_{n_2})$ and

$$\mu((\mathbb{F}_2^j, \delta)) = \frac{\mu_{\mathrm{CL}}(A \in \mathscr{G}_2 : \#A[2] = 2^j)}{\#\,\mathrm{Hom}(\mathbb{F}_2^j, G_{n_1} \times \widetilde{G}_{n_2})}.$$

Therefore the sum becomes

$$\sum_{V \subseteq \widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}} \sum_{j \geqslant 0} \frac{2^{j|\mathbf{k}|_1}}{2^{\sum_{\chi \notin V} k_\chi}} \frac{\#\,\mathrm{Epi}(\mathbb{F}_2^j, V^\perp)}{\#\,\mathrm{Hom}(\mathbb{F}_2^j, G_{n_1} \times \widetilde{G}_{n_2})} \mu_{\mathrm{CL}}(A \in \mathscr{G}_2 : \#A[2] = 2^j).$$

We assume familiarity of the reader with Möbius inversion in posets, see [17, Chapter 3], for example. Writing $\mathrm{Epi}(\mathbb{F}_2^j, V^\perp)$ via inclusion-exclusion on the poset of vector subspaces of $G_{n_1} \times \widetilde{G}_{n_2}$ and exchanging the order of summation we obtain

$$\sum_{W \subset \widehat{G}_{n_1} \times \widehat{\widetilde{G}}_{n_2}} \Big(\sum_{V \subset W} \frac{\mu(V, W)}{2^{\sum_{\chi \notin V} k_\chi}} \Big) \Big(\sum_{G \in \mathscr{G}_2} \#G[2]^{|\mathbf{k}|_1 - \dim(W)} \mu_{\mathrm{CL}}(G) \Big).$$

By applying Möbius inversion with respect to the poset of vector subspaces, to the obvious relation

$$2^{-\sum_{\chi \notin W} k_\chi} = \mathbb{P}_{(k_\chi)}(V \subseteq W) = \sum_{V \subset W} \mathbb{P}_{(k_\chi)}(V)$$

we obtain

$$\mathbb{P}_{(k_\chi)}(W) = \sum_{V \subset W} \frac{\mu(V, W)}{2^{\sum_{\chi \notin V} k_\chi}}.$$

On the other hand, one has that whenever $|\mathbf{k}|_1 - \dim(W) \geqslant 0$, then

$$\sum_{G \in \mathscr{G}_2} \#G[2]^{|\mathbf{k}|_1 - \dim(W)} \mu_{\mathrm{CL}}(G) = \mathscr{N}_2(|\mathbf{k}|_1 - \dim(W)).$$

Instead, when $|\mathbf{k}|_1 - \dim(W) < 0$, we have that $\mathbb{P}_{(k_\chi)}(W) = 0$. In conclusion we get that the total sum equals

$$\sum_{W \subseteq \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}} \mathbb{P}_{(k_\chi)}(W) \mathscr{N}_2(|\mathbf{k}|_1 - \dim(W)). \qquad \square$$

Choosing $f(T) = \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}} m_\chi(T)^{k_\chi}$ in Heuristic assumption 4.4 suggests the following prediction by means of Proposition 4.8.

Prediction 4.9. *We have*

$$\lim_{X \to \infty} \frac{\sum_{D \leqslant X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}} m_\chi(D)^{k_\chi}}{\sum_{D \leqslant X} 1} = 2^{|\mathbf{k}|_1} \sum_{W \subseteq \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}} \mathbb{P}_{(k_\chi)}(W) \mathscr{N}_2(|\mathbf{k}|_1 - \dim(W)),$$

where in both sums D varies among square-free positive integers which are squares $(\mathrm{mod}\ n_1)$ *and non-squares modulo every prime divisors of n_2.*

A version of Prediction 4.9 with an explicit error term is proved in Theorem 5.6. This prediction has a noteworthy feature: it realizes the (k_χ)-mixed moments of $(m_\chi(D))$ as an average over all subspaces of $\widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}$ of ordinary moments of $\#S(D)$ and in doing so, it suggests the first step of the proof of Theorem 5.6, see (6.2).

5. Main theorems on the 2-part of ray class sequences

Throughout the section we keep the notation used in §3. We begin by stating Theorems 5.1,5.2 and 5.3 that corroborate Predictions 3.7,3.9 and 3.10 when $\mathrm{D}(K) \equiv 1 \,(\mathrm{mod}\ 4)$. We restrict our attention to the cases with $\mathrm{D}(K) \equiv 1 \,(\mathrm{mod}\ 4)$ only for the sake of brevity, the remaining case being amenable to a similar analysis. Our main task in this section will then be to reduce Theorems 5.1, 5.2, 5.3 and 5.4 that are about ray class groups to Theorems 5.6 and 5.7 which regard only special divisors.

Theorem 5.1. *For any $\beta \in \mathbb{R}$ satisfying $0 < \beta < \min\{2^{-|\mathbf{k}|_1}, \varphi(c)^{-1}\}$ we have*

$$\frac{\sum_{-\mathrm{D}(K) \leqslant X} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}} m_\chi(\delta_2(K))^{k_\chi}}{\sum_{-\mathrm{D}(K) \leqslant X} 1} = \sum_{V \subseteq \widehat{Im(g_R)}} \mathbb{P}_{(k_\chi)}(V) \mathscr{N}_2(|\mathbf{k}|_1 - \dim(V)) + O((\log X)^{-\beta}),$$

where in both sums K varies among imaginary quadratic number fields of type R, having $\mathrm{D}(K) \equiv 1 \,(\mathrm{mod}\ 4)$ *and the implied constant depends at most on c and $(k_\chi)_\chi$.*

Theorem 5.2. *We have*

$$\lim_{X \to \infty} \frac{\#\{K : -\mathrm{D}(K) \leqslant X, \#(2\,\mathrm{Cl}(K))[2] = 2^j \text{ and } \mathrm{Im}(\delta_2(K)) = Y\}}{\#\{K : -\mathrm{D}(K) \leqslant X\}}$$

$$= \mu_{\mathrm{CL}}(G \in \mathscr{G}_2 : \#G[2] = 2^j) \frac{\#\,\mathrm{Epi}_{\mathbb{F}_2}(\mathbb{F}_2^j, Y)}{\#\,\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^j, \mathrm{Im}(g_R))},$$

where K varies among imaginary quadratic number fields with $\mathrm{D}(K) \equiv 1 \,(\mathrm{mod}\ 4)$ *and of type R.*

Recall the definition of W_R in (3.1) and the definition of the map g_R before the statement of Proposition 3.5.

Theorem 5.3. *We have*

$$\lim_{X\to\infty}\frac{\#\{K:-\mathrm{D}(K)\leqslant X,\mathrm{rk}_4(\mathrm{Cl}(K))=j_1,\mathrm{rk}_4(\mathrm{Cl}(K,c))=j_2\}}{\#\{K:-\mathrm{D}(K)\leqslant X\}}$$
$$=\mu_{\mathrm{CL}}(G\in\mathscr{G}_2:\dim_{\mathbb{F}_2}(G[2])=j_1)\frac{\#\{\varphi\in\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1},\mathrm{Im}(g_R)):\mathrm{rk}(\varphi)=\mathrm{rk}_2(W_R)-(j_2-j_1)\}}{\#\,\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1},\mathrm{Im}(g_R))},$$

where K varies among imaginary quadratic number fields with $\mathrm{D}(K)\equiv 1\,(\mathrm{mod}\ 4)$ and of type R.

We will prove a stronger version of Theorems 5.1, 5.2 and 5.3. Namely, the fact that we deal with progressions $a\,(\mathrm{mod}\ q)$ in Theorems 5.6 and 5.7 yields results analogous to the ones in Theorems 5.1, 5.2 and 5.3 when one imposes finitely many unramified local conditions at primes independent of c on the discriminants $D(K)$. This supports the point of view in Wood's recent work [20] that local conditions on the quadratic field do not affect the distribution of class groups, with the obvious modification that for ray class groups such conditions must be taken independently of the primes dividing c.

We proceed to restate Theorem 5.3 in a more explicit way. Recalling that c is square-free we let $n_1(R)$ be the product of the prime divisors of c which are either $3\,(\mathrm{mod}\ 4)$ and inert in R, or $1\,(\mathrm{mod}\ 4)$ and split. Furthermore, let $n_2(R)$ be the product of the prime divisors of c that are $3\,(\mathrm{mod}\ 4)$ and split in R. Recall that

$$\frac{\eta_\infty(2)}{\eta_{j_1}(2)^2 2^{j_1^2}}=\mu_{CL}(G\in\mathscr{G}_2:\dim_{\mathbb{F}_2}(G[2])=j_1).$$

Theorem 5.4. *We have*

$$\lim_{X\to\infty}\frac{\#\{K:-\mathrm{D}(K)\leqslant X,\mathrm{rk}_4(\mathrm{Cl}(K))=j_1,\mathrm{rk}_4(\mathrm{Cl}(K,c))=j_2\}}{\#\{K:-\mathrm{D}(K)\leqslant X\}}$$
$$=\frac{\eta_\infty(2)}{\eta_{j_1}(2)^2 2^{j_1^2}}\frac{\#\{\varphi\in\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1},G_{n_1(R)}\times\widetilde{G}_{n_2(R)}):\mathrm{rk}(\varphi)=\mathrm{rk}_2(W_R)-(j_2-j_1)\}}{\#\,\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^{j_1},G_{n_1(R)}\times G_{n_2(R)})},$$

where K varies among imaginary quadratic number fields with $\mathrm{D}(K)\equiv 1\,(\mathrm{mod}\ 4)$ and of type R.

The congruence conditions (mod 4) related to the definition of $n_1(R)$ and $n_2(R)$ in Theorem 5.4 are analogous to the congruences (mod 3) for the primes l appearing in the first part of Varma's Theorem 2.13.

Our next goal is to realise the δ_2-map

$$\delta_2(\mathbb{Q}(\sqrt{-D})):(2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-D})))[2]\to\mathrm{Im}(g_R)$$

with the map on special divisors introduced in §4,

$$\varphi_{n_1(R),n_2(R),D}:\frac{S(D)}{\{1,D\}}\to G_{n_1(R)}\times\widetilde{G}_{n_2(R)}.$$

5.1. **Realizing $\delta_2(\mathbb{Q}(\sqrt{-D}))$ as $\varphi_{n_1(R),n_2(R),D}$.** Let D be a square-free positive integer with $D \equiv 3 \pmod 4$. and denote its its prime factorization by $D = p_1 \cdots p_j$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_j$ be the corresponding prime ideals in $\mathbb{Q}(\sqrt{-D})$, i.e. $\mathfrak{p}_i^2 = (p_i)$). Recall that $\mathrm{Cl}(\mathbb{Q}(\sqrt{-D}))[2]$ is generated by $\mathfrak{p}_1, \dots, \mathfrak{p}_j$ subject only to the relation $\mathfrak{p}_1 \cdots \mathfrak{p}_j = (\sqrt{-D})$. For any b positive divisor of D, denote by $\mathfrak{b}$ the ideal of $\mathbb{Q}(\sqrt{-D})$ with $\mathfrak{b}^2 = (b)$. Let us now recall from [8, Lem.16] that given a positive divisor b of D, we have $\mathfrak{b} \in 2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-D}))$ if and only if $b \in S(D)$. The assignment $\mathfrak{b} \mapsto b$ gives an isomorphism

$$(2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-D})))[2] \cong S(D)/\{1, D\}.$$

Indeed, from the proof of [8, Lem.16], we know that $b \in S(D)$ if and only if there exists a primitive element (i.e. not divisible by any $m \in \mathbb{Z}_{\geqslant 2}$) $\alpha \in \mathscr{O}_{\mathbb{Q}(\sqrt{-D})}$ and $w \in \mathbb{Z}_{\neq 0}$ such that

$$bw^2 = \mathrm{N}_{\mathbb{Q}(\sqrt{-D})/\mathbb{Q}}(\alpha). \tag{5.1}$$

In that case the factorization of (α) gives an integral ideal $h(\mathfrak{b})$ such that $(\alpha) = h(\mathfrak{b})^2\mathfrak{b}$. We rewrite this as $\mathfrak{b}(\alpha/b) = h(\mathfrak{b})^2$ and observe that this shows in particular that $\mathfrak{b} \in 2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-D}))$.

By weak approximation for conics, one has that such an α can be found with $(\alpha, c) = 1$, i.e. a primitive point on (5.1) such that $\gcd(w, c) = 1$. Therefore both $(\alpha), h(\mathfrak{b})$ are coprime to (c). Therefore the fractional ideal $\mathfrak{b}(\frac{\alpha}{b})$ can be employed as a lifting of $\mathfrak{b}$ to $2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-D}), c)$. Therefore the definition of the δ_2-map gives us that

$$\delta_2(\mathbb{Q}(\sqrt{-D}))(\mathfrak{b}) = b\frac{\alpha^2}{b^2}.$$

However squares of integers in $W_R/2W_R$ give rise to the trivial element, therefore by (5.1) we obtain that $\delta(\mathfrak{b}) = g_R(\alpha)$ Recalling that $N(\cdot)$ is the norm-function with respect to the C_2-action prescribed to $R^*/\langle -1\rangle$ we see that $g_R(\alpha) = \alpha^2 N(\alpha)$. Next, we provide a more concrete description of $\mathrm{Im}(g_R)$. The proof of the following result is straightforward and therefore omitted.

Lemma 5.5. *There is an isomorphism $\varphi_R : \mathrm{Im}(g_R) \to G_{n_1(R)} \times G_{n_2(R)}$ such that*

$$\varphi_R(g_R(x)) = N(x)$$

for every $x \in \frac{R^*}{\langle -1\rangle}[2^\infty]$.

Since $N(\alpha) = bw^2$ and w^2 is trivial in $W_R/2W_R$, we get a commutative diagram

$$\begin{array}{ccc} (2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-D})))[2] & \xrightarrow{\delta} & \mathrm{Im}(g_R) \\ \downarrow & & \downarrow \varphi_R \\ \frac{S(D)}{\{1,D\}} & \underset{\varphi_{n_1,n_2,D}}{\to} & G_{n_1(R)} \times \widetilde{G}_{n_2(R)} \end{array}$$

where the vertical rows are isomorphisms. This gives us precisely the realization of the δ_2-map in terms of special divisors that we were looking for.

5.2. **Reduction to special divisors.** Our next result holds for integers a, q, n_1, n_2 satisfying

$$4n_1n_2 \text{ divides } q, a \equiv 3 \pmod 4, \gcd(a, q) = 1, \tag{5.2}$$

$$a \text{ is a square} \pmod{n_1} \tag{5.3}$$

and

$$p \text{ prime}, p \mid n_2 \Rightarrow a \text{ is a non-square} \pmod p. \tag{5.4}$$

Theorem 5.6. *Let a, q, n_1, n_2 be positive integers satisfying* (5.2), (5.3) *and* (5.4). *Then for every $\delta \in (0, 2^{-|\mathbf{k}|_1})$ we have*

$$\frac{\sum_{D\leqslant X}\prod_{\chi\in\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}} m_\chi(D)^{k_\chi}}{\sum_{D\leqslant X}1} - 2^{|\mathbf{k}|_1}\Big(\sum_{W\subseteq\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}}\mathbb{P}_{(k_\chi)}(W)\mathscr{N}_2(|\mathbf{k}|_1-\dim(W))\Big) \ll (\log X)^{-\delta},$$

where in both sums D varies among square-free positive integers which are congruent to $a \pmod q$ and the implied constant depends at most on a, q, n_1, n_2, δ and $(k_\chi)_\chi$.

This proves Prediction 4.9 with an explicit error term.

Recall Definition 4.3. We shall use Theorem 5.6 in §7 to deduce the following.

Theorem 5.7. *Let a, q, n_1, n_2 be positive integers satisfying* (5.2), (5.3) *and* (5.4). *Then*

$$\lim_{X\to\infty}\frac{\#\{D\leqslant X, (S(D)/\{1,D\}, \varphi_{n_1,n_2,D})\sim T\}}{\#\{D\leqslant X\}} = \mu(T),$$

where D varies among positive square-free integers satisfying $D\equiv a \pmod q$.

This confirms the Prediction 4.5.

We are finally in place to explain why Theorems 5.6 and 5.7 imply Theorems 5.1, 5.2, 5.3 and 5.4. Owing to the final diagram of the previous subsection, we have the following implications. Theorems 5.2, 5.3 and 5.4 follow immediately from Theorem 5.7 because the family of fields K that are strongly of type R has zero proportion.

To deduce Theorem 5.1 from Theorem 5.6 recall the definition of $E(X)$ given prior to (3.2) and that $m_\chi(\delta_2(K))$ coincides with $m_\chi(-\mathrm{D}(K))$ if $\mathrm{D}(K)\notin E(X)$ and that it vanishes otherwise. We thus obtain

$$\sum_{-\mathrm{D}(K)\leqslant X}\prod_{\chi\in\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}} m_\chi(\delta_2(K))^{k_\chi} - \sum_{D\leqslant X}\prod_{\chi\in\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}} m_\chi(D)^{k_\chi} = -\sum_{D\in E(X)}\prod_{\chi\in\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}} m_\chi(D)^{k_\chi}. \tag{5.5}$$

Fixing any $\gamma\in(0,1/\varphi(c))$ we can pick a positive integer p' which satisfies $\gamma\varphi(c)<1-1/p'<1$ and define q' via $1/p'+1/q'=1$. Using Hölder's inequality we see that the quantity in (5.5) has modulus

$$\begin{aligned}\sum_{D\in E(X)}\prod_{\chi\in\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}} m_\chi(D)^{k_\chi} &= \sum_{D\leqslant X}\mathbf{1}_{E(X)}(D)\Big(\prod_{\chi\in\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}} m_\chi(D)^{k_\chi}\Big)\\ &\leqslant \Big(\sum_{D\leqslant X}\mathbf{1}_{E(X)}(D)^{q'}\Big)^{1/q'}\Big(\sum_{D\leqslant X}\prod_{\chi\in\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}} m_\chi(D)^{p'k_\chi}\Big)^{1/p'}\\ &= E(X)^{1/q'}\Big(\sum_{D\leqslant X}\prod_{\chi\in\widehat{G}_{n_1}\times\widehat{\widehat{G}}_{n_2}} m_\chi(D)^{p'k_\chi}\Big)^{1/p'}.\end{aligned}$$

Observe that the obvious bound $m_\chi(D)\leqslant \#S(D)$ shows that the second sum is

$$\leqslant \sum_{D\leqslant X}\#S(D)^{p'|\mathbf{k}|_1}$$

hence by [8, Th.9] it is $O_{p',\mathbf{k}}(X)$. Using (3.2) we conclude that the quantity in (5.5) is

$$\ll \Big(\frac{X}{(\log X)^{1/\varphi(c)}}\Big)^{1/q'} X^{1/p'} = \frac{X}{(\log X)^{1/(q'\varphi(c))}} \ll \frac{X}{(\log X)^{\gamma}},$$

This concludes our argument that shows that Theorem 5.6 implies Theorem 5.1.

6. Main theorems on special divisors

This section is devoted to the proof of Theorem 5.6.

6.1. **Pre-indexing trick.** In the present subsection we reduce Theorem 5.6 into a statement that can be proved with the method of Fouvry and Klüners. Recall the definition of the set of special divisors $S(D)$ given in the beginning of §4. For a character $\chi \in \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}$ we bring into play the sum

$$A_\chi(D) := \sum_{a'b'=D} \chi(a') \Big(\sum_{c'|b'} \Big(\frac{a'}{c'}\Big)\Big) \Big(\sum_{d'|a'} \Big(\frac{b'}{d'}\Big)\Big) \tag{6.1}$$

and let $A(D) := A_1(D)$. By definition (4.1) we see that $m_\chi(D)$ is the cardinality of elements $a' \in S(D)$ such that $\chi(a') = 1$. Detecting the latter condition via $(1+\chi(a'))/2$ we obtain

$$m_\chi(D) = 2^{-\omega(D)} \frac{(A(D) + A_\chi(D))}{2}.$$

Recalling Notation 4.6 we obtain

$$\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}} m_\chi(D)^{k_\chi} = 2^{-|\mathbf{k}|_1 \omega(D)} \frac{\prod_{\chi \in \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}} (A(D) + A_\chi(D))^{k_\chi}}{2^{|\mathbf{k}|_1}}. \tag{6.2}$$

Letting $|(i_\chi)|_1$ be the ℓ^1-norm of the vector $(i_\chi)_\chi$ we see that the right side equals

$$2^{-|\mathbf{k}|_1\omega(D)} \sum_{\substack{(i_\chi)_\chi \\ 0 \leqslant i_\chi \leqslant k_\chi}} \frac{\lambda_{(i_\chi)}}{2^{|\mathbf{k}|_1}} A(D)^{|\mathbf{k}|_1 - |(i_\chi)|_1} \prod_{\chi \in \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}} A_\chi(D)^{i_\chi}$$

for some integers $\lambda_{(i_\chi)}$. To each vector (i_χ) we attach the space

$$Y_{(i_\chi)} := \langle \{\chi : i_\chi \neq 0\} \rangle \subseteq \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}$$

and recalling Definition 4.7 we see that for a fixed subspace $Y \subseteq \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2}$ we have

$$\sum_{\substack{(i_\chi): Y_{(i_\chi)} = Y \\ 0 \leqslant i_\chi \leqslant k_\chi}} \frac{\lambda_{(i_\chi)}}{2^{|\mathbf{k}|_1}} = \mathbb{P}_{(k_\chi)}(Y).$$

Hence Theorem 5.6 would follow from proving that for any $\varepsilon > 0$, any integers a, q, n_1, n_2 satisfying (5.2), (5.3) and (5.4), any $B \subseteq \widehat{G}_{n_1} \times \widehat{\widehat{G}}_{n_2} - \{1\}$ and any choice of a function $i : B \to \mathbb{Z}_{>0}$ with $i_\chi \leqslant k_\chi$, one has that

$$\begin{aligned} &\sum_{D \leqslant X} 2^{-|\mathbf{k}|_1 \omega(D)} A(D)^{|\mathbf{k}|_1 - \sum_{\chi \in B} i_\chi} \prod_{\chi \in B} A_\chi(D)^{i_\chi} \\ =& 2^{|\mathbf{k}|_1} \mathscr{N}_2(|\mathbf{k}|_1 - \dim(Y_{(i_\chi)})) \Big(\sum_{D \leqslant X} 1 \Big) + O(X(\log X)^{\varepsilon - 2^{-|\mathbf{k}|_1}}), \end{aligned} \tag{6.3}$$

where in both sums D varies among positive square-free integers which are congruent to $a \pmod q$. Here $\mathscr{N}_2(h)$ denotes as usual the number of vector subspaces of $\mathbb{F}_2^h$. To prove (6.3) we will use the approach in the proof of [8, Th.6]. In the present notation their result corresponds to the case $B = \varnothing$ in (6.3).

6.2. **Indexing trick.** We begin by performing the following change of variables in (6.1),

$$a' = D_{10}D_{11}, b' = D_{00}D_{01}, c' = D_{00}, d' = D_{11}.$$

Letting $\Phi_1(\mathbf{u},\mathbf{v}) := (\mathbf{u}_1+\mathbf{v}_1)(\mathbf{u}_1+\mathbf{v}_2)$ and $\Psi(\mathbf{u}) := \mathbf{u}_1$ we can thus conclude that

$$A_\chi(D) = \sum_{D=D_{10}D_{11}D_{00}D_{01}} \prod_{(\mathbf{u},\mathbf{v})\in(\mathbb{F}_2^2)^2} \Big(\frac{D_\mathbf{u}}{D_\mathbf{v}}\Big)^{\Phi_1(\mathbf{u},\mathbf{v})} \prod_{\mathbf{u}\in\mathbb{F}_2^2} \chi(D_\mathbf{u})^{\Psi(\mathbf{u})}.$$

Next, if $\langle B\rangle$ is not the zero subspace we choose a basis $T \subset B$ of $\langle B\rangle$. Now suppose we choose in each factor of

$$A(D)^{|\mathbf{k}|_1-\sum_{\chi\in B} i_\chi} \prod_{\chi\in B} A_\chi(D)^{i_\chi}$$

a decomposition of D as follows,

$$D = \prod_{\mathbf{u}^{(1)}\in\mathbb{F}_2^2} D^{(1)}_{\mathbf{u}^{(1)}} = \ldots = \prod_{\mathbf{u}^{(|\mathbf{k}|_1)}\in\mathbb{F}_2^2} D^{(|\mathbf{k}|_1)}_{\mathbf{u}^{|\mathbf{k}|_1}}.$$

We change variables and write $D_{\mathbf{u}^{(1)},\ldots,\mathbf{u}^{(|\mathbf{k}|_1)}} := \gcd(D^{(1)}_{\mathbf{u}^{(1)}},\ldots,D^{(|\mathbf{k}|_1)}_{\mathbf{u}^{(|\mathbf{k}|_1)}})$, where one can reconstruct the old variables with the help of

$$D^{(\ell)}_{\mathbf{u}^{(\ell)}} = \prod_{\substack{1\leqslant n\leqslant|\mathbf{k}|_1\\ n\neq\ell}} \prod_{\mathbf{u}^{(n)}\in\mathbb{F}_2^2} D_{\mathbf{u}^{(1)},\ldots,\mathbf{u}^{(\ell)},\ldots,\mathbf{u}^{(|\mathbf{k}|_1)}}$$

as in [8, Eq.(23)]. Thus we can write

$$A(D)^{|\mathbf{k}|_1-\sum_{\chi\in B} i_\chi} \prod_{\chi\in B} A_\chi(D)^{i_\chi} = \sum_{\prod_{\mathbf{u}\in\mathbb{F}_2^{2|\mathbf{k}|_1}} D_\mathbf{u}=D} \Big(\prod_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^{2|\mathbf{k}|_1}} \Big(\frac{D_\mathbf{u}}{D_\mathbf{v}}\Big)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})}\Big)\Big(\prod_{\mathbf{u}\in\mathbb{F}_2^{2|\mathbf{k}|_1}} \prod_{\chi\in T} \chi(D_\mathbf{u})^{\Psi_\chi(\mathbf{u})}\Big),$$

where

$$\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v}) := \sum_{j=1}^{|\mathbf{k}|_1} \Phi_1(\mathbf{u}^{(j)},\mathbf{v}^{(j)})$$

and Ψ_χ are linear maps from $\mathbb{F}_2^{2|\mathbf{k}|_1}$ to $\mathbb{F}_2$, which we next describe. Decompose

$$\mathbb{F}_2^{2|\mathbf{k}|_1} = \mathbb{F}_2^{2|\mathbf{k}|_1-2\sum_{\chi\in B} i_\chi} \times \prod_{\chi\in B} \mathbb{F}_2^{2i_\chi}$$

and we denote a vector in this space as $\mathbf{u} := (\mathbf{u}_0, (\mathbf{u}^{(\chi)})_{\chi\in B})$, where $\mathbf{u}^{(\chi)} := (\mathbf{u}_1^{(\chi)},\ldots,\mathbf{u}_{i_\chi}^{(\chi)})$ and for every j we have $\mathbf{u}_j^{(\chi)} \in \mathbb{F}_2^2$. Next, write

$$\Psi'_\chi(\mathbf{u}) = \sum_{j=1}^{i_\chi} \Psi(\mathbf{u}_j^{(\chi)})$$

and note that we have

$$\Psi_\chi(\mathbf{u}) = \sum_{\chi'\in B_\chi} \Psi'_{\chi'}(\mathbf{u}), \tag{6.4}$$

where B_χ denotes the set of characters $\chi' \in B$, such that χ is used in writing χ' in the basis T. In particular, this implies that $\chi \in B_\chi$. The construction of Ψ_χ depends on T and (i_χ), but we suppress this dependency to simplify the notation.

Let us observe that there are $\#T = \dim(\langle B\rangle)$ many linear maps Ψ_χ and that they are independent. Indeed, given $\chi \in T$, all maps $\Psi_{\chi'}$ with $\chi' \in T - \{\chi\}$ vanish on the vectors $\mathbf{u}$ with $\mathbf{u}^{(\widetilde{\chi})} = \mathbf{0}$ for each $\widetilde{\chi} \neq \chi$, while Ψ_χ evaluated in such $\mathbf{u}$ equals $\Psi'_\chi(\mathbf{u}^{(\chi)})$, which does not vanish identically.

We can therefore rewrite the first sum over D in (6.3) as

$$\begin{aligned}&\sum_{D\leqslant X} 2^{-|\mathbf{k}|_1\omega(D)} A(D)^{|\mathbf{k}|_1-\sum_{\chi\in B} i_\chi} \prod_{\chi\in B} A_\chi(D)^{i_\chi}\\ &= \sum_{(D_{\mathbf{u}})} \Big(\prod_{\mathbf{u}\in\mathbb{F}_2^{2|\mathbf{k}|_1}} 2^{-|\mathbf{k}|_1\omega(D_{\mathbf{u}})}\Big)\Big(\prod_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^{2|\mathbf{k}|_1}} \Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})}\Big)\Big(\prod_{\mathbf{u}\in\mathbb{F}_2^{2|\mathbf{k}|_1}} \prod_{\chi\in T} \chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})}\Big),\end{aligned} \tag{6.5}$$

where the second sum is over positive integers $D_{\mathbf{u}}$ such that $\prod_{\mathbf{u}\in\mathbb{F}_2^{2|\mathbf{k}|_1}} D_{\mathbf{u}}$ varies among positive square-free integers which are congruent to $a \pmod q$ and at most X.

Our goal in §§6.3-6.5 is to prove an asymptotic for the sum over $D_{\mathbf{u}}$ in (6.5) under the assumptions on the integers a, q, n_1, n_2 in Theorem 5.6. For a real number $X > 1$ we bring into play the following subset of $\mathbb{N}^{4^{|\mathbf{k}|_1}}$,

$$\mathscr{D}(X,|\mathbf{k}|_1;q,a):=\left\{ (D_{\mathbf{u}})_{\mathbf{u}} \in \mathbb{N}^{4^{|\mathbf{k}|_1}}, \mathbf{u}=(\mathbf{u}^{(1)},\dots,\mathbf{u}^{(|\mathbf{k}|_1)}) \in (\mathbb{F}_2^2)^{|\mathbf{k}|_1} : \begin{array}{l}\prod_{\mathbf{u}} D_{\mathbf{u}} \text{ is square-free,}\\ \text{bounded by } X \text{ and}\\ \text{congruent to } a \pmod q\end{array} \right\}.$$

We are interested in asymptotically evaluating the succeeding average,

$$S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a):=\sum_{(D_{\mathbf{u}})\in\mathscr{D}(X,|\mathbf{k}|_1;q,a)} 2^{-|\mathbf{k}|_1\omega(D)} \Bigg(\prod_{\mathbf{u},\mathbf{v}\in(\mathbb{F}_2^2)^{|\mathbf{k}|_1}} \Big(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\Big)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})}\Bigg)\Bigg(\prod_{\mathbf{u}\in(\mathbb{F}_2^2)^{|\mathbf{k}|_1}} \prod_{\chi\in T} \chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})}\Bigg)$$

and in doing so we shall not keep track of the dependence of the implied constants on $T, (i_\chi), \mathbf{k}, \boldsymbol{\chi}, a, q, n_1, n_2$. The sum $S_{\boldsymbol{\chi}}$ also depends on (i_χ) and the choice of T but we suppress this in the notation. The function $S_{\boldsymbol{\chi}}$ should be compared with [8, Eq.(26)]; we will verify in §6.3 that the presence of the characters $\boldsymbol{\chi}$ does not affect the analysis of Fouvry–Klüners [8] in the error term and we shall see in §§6.4-6.5 how their presence influences the main term.

6.3. **The four families of sums of Fouvry and Klüners.** We begin by restricting the summation in $S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a)$ to variables having a suitably small number of prime factors as in [8,§5.3]. Letting $\Omega := 2^{|\mathbf{k}|_1+1}|\mathbf{k}|_1^{-1}\log\log X$ we shall study the contribution, say Σ_1, towards $S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a)$ of elements not fulfilling

$$\omega(D_{\mathbf{u}}) \leqslant \Omega, \text{ for all } \mathbf{u} \in \mathbb{F}_2^{2|\mathbf{k}|_1}.$$

Writing $m = \prod_{\mathbf{u}} D_{\mathbf{u}}$ and bounding each character by 1 provides us with

$$\Sigma_1 \ll \sum_{m\leqslant X} \frac{\mu(m)^2}{\tau(m)^{|\mathbf{k}|_1}} \sum_{\substack{m_1\cdots m_{4^{|\mathbf{k}|_1}}=m\\ \omega(m_1)>\Omega}} 1 \leqslant 4^{-|\mathbf{k}|_1\Omega} \sum_{m\leqslant X} \frac{\mu(m)^2}{\tau(m)^{|\mathbf{k}|_1}} \sum_{m_1\cdots m_{4^{|\mathbf{k}|_1}}=m} 4^{|\mathbf{k}|_1\omega(m_1)}.$$

Invoking [12, Eq.(1.82)] to bound the sum over m makes the following estimate available,

$$\Sigma_1 \ll X(\log X)^{-1-2^{|\mathbf{k}|_1+1}\log(4/\mathrm{e})-2^{|\mathbf{k}|_1}}. \tag{6.6}$$

We continue in the footsteps laid out in [8, §5.4], where four families of elements in $\mathbb{N}^{4^{|\mathbf{k}|_1}}$ are shown to make a negligible contribution towards a quantity that resembles $S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a)$. Using the trivial bound

$$\left|\prod_{\mathbf{u}\in(\mathbb{F}_2^2)^{|\mathbf{k}|_1}}\prod_{\chi\in T}\chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})}\right|\leqslant 1 \tag{6.7}$$

allows us to adopt in a straightforward manner the arguments leading to [8, Eq.(34),(39)] and we proceed to briefly explain how. Let

$$\Delta := 1+(\log X)^{-2^{|\mathbf{k}|_1}}$$

and let $A_{\mathbf{u}}$ denote numbers of the form Δ^m where $m\in\mathbb{Z}_{\geqslant 0}$. For $\mathbf{A}=(A_{\mathbf{u}})_{\mathbf{u}\in(\mathbb{F}_2^2)^{|\mathbf{k}|_1}}$ we let

$$S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a;\mathbf{A}) := \sum_{\substack{(D_{\mathbf{u}})\in\mathscr{D}(X,|\mathbf{k}|_1;q,a)\\ \forall\mathbf{u}(A_{\mathbf{u}}\leqslant D_{\mathbf{u}}<\Delta A_{\mathbf{u}})\\ \forall\mathbf{u}(\omega(D_{\mathbf{u}})\leqslant\Omega)}} 2^{-|\mathbf{k}|_1\omega(D)}\left(\prod_{\mathbf{u},\mathbf{v}\in(\mathbb{F}_2^2)^{|\mathbf{k}|_1}}\left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\right)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})}\right)\prod_{\mathbf{u}\in(\mathbb{F}_2^2)^{|\mathbf{k}|_1}}\prod_{\chi\in T}\chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})}$$

and note that, in light of (6.6), we can deduce as in [8, Eq.(32)] that

$$S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a) = \sum_{\mathbf{A}:\prod_{\mathbf{u}}A_{\mathbf{u}}\leqslant X} S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a;\mathbf{A}) + O(X(\log X)^{-1}). \tag{6.8}$$

The contribution towards (6.8) of the first family, defined through

$$\prod_{\mathbf{u}} A_{\mathbf{u}} \geqslant \Delta^{-4^{|\mathbf{k}|_1}}X,$$

can be proved to be $\ll X(\log X)^{-1}$ with a similar argument as the one leading to [8, Eq.(34)]. We now let

$$X^{\ddagger} := \min\left\{\Delta^{\ell}\geqslant\exp\left((\log X)^{\varepsilon 2^{-|\mathbf{k}|_1}}\right)\right\}.$$

The contribution towards (6.8) of those $\mathbf{A}$ fulfilling that

$$\text{at most } 2^{|\mathbf{k}|_1}-1 \text{ of the } A_{\mathbf{u}} \text{ are larger than } X^{\ddagger} \tag{6.9}$$

can be shown to be $\ll X(\log X)^{\varepsilon-2^{-|\mathbf{k}|_1}}$ as in [8, Eq.(39)].

We next pass to arguments related to cancellation due to oscillation of characters, in this case (6.7) is not enough. The exponents $\Phi_k(\mathbf{u},\mathbf{v})$ will now play a rôle. Following Fouvry and Klüners we call two indices $\mathbf{u},\mathbf{v}$ *linked* if $\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})+\Phi_{|\mathbf{k}|_1}(\mathbf{v},\mathbf{u})=1$. We next define

$$X^{\dagger} := (\log X)^{3[1+4^{|\mathbf{k}|_1}(1+2^{|\mathbf{k}|_1})]}$$

and consider the contribution of $\mathbf{A}$ with

$$\prod_{\mathbf{u}} A_{\mathbf{u}} < \Delta^{-4^{|\mathbf{k}|_1}}X \text{ and for two linked } \mathbf{u} \text{ and } \mathbf{v} \text{ we have } \min\{A_{\mathbf{u}},A_{\mathbf{v}}\}\geqslant X^{\dagger}. \tag{6.10}$$

Fouvry and Klüners treat this case by drawing upon the important work of Heath-Brown [11] in the form stated in [8, Lem.12]. Specifically for $\mathbf{A}$ as in (6.10) we have

$$|S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a;\mathbf{A})| \leqslant \sum_{(D_{\mathbf{w}})_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}}} \Big(\prod_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}} 2^{-|\mathbf{k}|_1\omega(D_{\mathbf{w}})}\Big) \sum_{\substack{a_1,a_2\in(\mathbb{Z}\cap(0,q])^2\\ a_1a_2\prod_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}} D_{\mathbf{w}}\equiv a(\mathrm{mod}\ q)}} \Big|M((D_{\mathbf{w}}))\Big|,$$

where

$$M((D_{\mathbf{w}})) := \sum_{D_{\mathbf{u}},D_{\mathbf{v}}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\right) g(D_{\mathbf{u}},(D_{\mathbf{w}})_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}}) g(D_{\mathbf{v}},(D_{\mathbf{w}})_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}}),$$

$$g(D_{\mathbf{u}},(D_{\mathbf{w}})_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}}) := \frac{\mathbf{1}_{a_1,q}(D_{\mathbf{u}})}{2^{|\mathbf{k}|_1\omega(D_{\mathbf{u}})}} \prod_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{w}}}\right)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{w})} \prod_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}} \left(\frac{D_{\mathbf{w}}}{D_{\mathbf{u}}}\right)^{\Phi_{|\mathbf{k}|_1}(\mathbf{w},\mathbf{u})} \prod_{\chi\in T} \chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})},$$

$\mathbf{1}_{\alpha,\beta}$ denotes the indicator function of the set $\{m\in\mathbb{Z} : m\equiv\alpha\,(\mathrm{mod}\ \beta)\}$ and similarly for $g(D_{\mathbf{v}},(D_{\mathbf{w}})_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}})$. Since $|g(D_{\mathbf{u}},(D_{\mathbf{w}})_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}})|, |g(D_{\mathbf{v}},(D_{\mathbf{w}})_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}})| \leqslant 1$ the argument in [8, p.476] that validates [8, Eq.(42)] can be adopted in the obvious way to yield

$$\sum_{\mathbf{A}\ \text{fulfils (6.10)}} |S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a;\mathbf{A})| \ll X(\log X)^{-1}.$$

Note that we have used [8, Lem.15] for sequences satisfying $|a_m|,|b_n|\leqslant 1$ rather than $|a_m|,|b_n|<1$, however using [8, Lem.15] for $a_m/2, b_n/2$ in place of a_m, b_n proves a version of [8, Lem.15] under the more general assumption $|a_m|,|b_n|<2$ and with the same conclusion.

The fourth family consists of $\mathbf{A}$ fulfilling $\prod_{\mathbf{u}} A_{\mathbf{u}} < \Delta^{-4^{|\mathbf{k}|_1}} X$, any linked $\mathbf{u},\mathbf{v}$ satisfy the inequality $\min\{A_{\mathbf{u}},A_{\mathbf{v}}\} < X^\dagger$ and there exist linked $\mathbf{u},\mathbf{v}$ with $2\leqslant A_{\mathbf{v}}$ and $A_{\mathbf{u}}\geqslant X^\ddagger$. Their contribution towards $S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a;\mathbf{A})$ is

$$\ll \max_{\substack{\sigma(\mathrm{mod}\ q)\\ \gcd(\sigma,q)=1}} \sum_{\substack{(D_{\mathbf{w}})_{\mathbf{w}\notin\{\mathbf{u},\mathbf{v}\}}\\ A_{\mathbf{w}}\leqslant D_{\mathbf{w}}<\Delta A_{\mathbf{w}}}} \sum_{\substack{D_{\mathbf{v}}\\ A_{\mathbf{v}}\leqslant D_{\mathbf{v}}<\Delta A_{\mathbf{v}}}} |M_\sigma|, \tag{6.11}$$

where M_σ is defined through

$$\sum_{\substack{D_{\mathbf{u}}\equiv\sigma(\mathrm{mod}\ q)\\ A_{\mathbf{u}}\leqslant D_{\mathbf{u}}<\Delta A_{\mathbf{u}}}} 2^{-|\mathbf{k}|_1\omega(D_{\mathbf{u}})} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\right) \prod_{\chi\in T}\chi(D_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})} = \left(\prod_{\chi\in T}\chi(\sigma)^{\Psi_\chi(\mathbf{u})}\right) \sum_{\substack{D_{\mathbf{u}}\equiv\sigma(\mathrm{mod}\ q)\\ A_{\mathbf{u}}\leqslant D_{\mathbf{u}}<\Delta A_{\mathbf{u}}}} 2^{-|\mathbf{k}|_1\omega(D_{\mathbf{u}})} \left(\frac{D_{\mathbf{u}}}{D_{\mathbf{v}}}\right).$$

Letting $P^+(m)$ denote the largest prime factor of a positive integer $m>1$ and setting $P^+(1):=1, m:=D_{\mathbf{u}}/P^+(D_{\mathbf{u}})$ we obtain

$$M_\sigma \ll \sum_{\substack{mP^+(m)<\Delta A_{\mathbf{u}}\\ (m,q)=1}} \frac{\mu(m)^2}{2^{|\mathbf{k}|_1\omega(m)}} \Big| \sum_{mp\equiv\sigma(\mathrm{mod}\ q)} \mu\big(pm\prod_{\mathbf{w}\neq\mathbf{u}} D_{\mathbf{w}}\big)^2 \left(\frac{p}{D_{\mathbf{v}}}\right)\Big|,$$

where the inner sum is over primes p with $\max\{A_{\mathbf{u}}/m, P^+(m)\}\leqslant p<\Delta A_{\mathbf{u}}/m$. We may now use Dirichlet characters to modulus q to detect the congruence condition on p. We will subsequently be faced with $\varphi(q)$ new sums over p, each one of which can be bounded via [8, Lem.13]. This furnishes

$$\sum_{mp\equiv\sigma(\mathrm{mod}\ q)} \mu\big(pm\prod_{\mathbf{w}\neq\mathbf{u}} D_{\mathbf{w}}\big)^2 \left(\frac{p}{D_{\mathbf{v}}}\right) \ll \frac{A_{\mathbf{v}}^{1/2}A_{\mathbf{u}}}{m}(\log X)^{-N\varepsilon 2^{-|\mathbf{k}|_1+1}} + \Omega,$$

valid for each large enough positive N that is independent of $\mathbf{A}$ and m. The term Ω accounts for the presence of the μ^2-terms. Indeed, by (6.6) the number of distinct prime divisors of m and each $D_{\mathbf{w}}$ is at most Ω. A moment's thought now reveals that once the last bound is injected into (6.11) and N is suitably increased in comparison to $|\mathbf{k}|_1$, the contribution of $\mathbf{A}$ in the fourth case is $\ll X(\log X)^{-1}$, as in [8, Eq.(47)].

Let us now introduce the conditions

$$\begin{cases} \prod_{\mathbf{u}\in(\mathbb{F}_2^2)^k} A_{\mathbf{u}} < \Delta^{-4^{|\mathbf{k}|_1}} X, \\ \text{at least } 2^{|\mathbf{k}|_1} \text{ indices satisfy } A_{\mathbf{u}} > X^{\ddagger}, \\ \text{two indices } \mathbf{u} \text{ and } \mathbf{v} \text{ with } A_{\mathbf{u}}, A_{\mathbf{v}} > X^{\dagger} \text{ are always linked}, \\ \text{if } A_{\mathbf{u}} \text{ and } A_{\mathbf{v}} \text{ with } A_{\mathbf{v}} \leqslant A_{\mathbf{u}} \text{ are linked, then either} \\ A_{\mathbf{v}} = 1 \text{ or } (2 \leqslant A_{\mathbf{v}} < X^{\dagger} \text{ and } A_{\mathbf{v}} \leqslant A_{\mathbf{u}} < X^{\ddagger}). \end{cases} \tag{6.12}$$

Increasing the value of A in comparison to $|\mathbf{k}|_1$ and assorting all estimates so far yields

$$S_{\boldsymbol{\chi}}(X, |\mathbf{k}|_1; q, a) = \sum_{\mathbf{A} \text{ satisfies (6.12)}} S_{\boldsymbol{\chi}}(X, |\mathbf{k}|_1; q, a; \mathbf{A}) + O(X(\log X)^{\varepsilon - 2^{-|\mathbf{k}|_1}}), \tag{6.13}$$

which is in analogy with [8, Prop.2].

6.4. **The main term.** We can now obtain the following as in [8, Prop.3],

$$S_{\boldsymbol{\chi}}(X, |\mathbf{k}|_1; q, a) = \sum_{\mathbf{A} \text{ satisfies (6.15)}} S_{\boldsymbol{\chi}}(X, |\mathbf{k}|_1; q, a; \mathbf{A}) + O(X(\log X)^{\varepsilon - 2^{-|\mathbf{k}|_1}}), \tag{6.14}$$

where

$$\begin{cases} \mathscr{U} := \{\mathbf{u} : A_{\mathbf{u}} > X^{\ddagger}\} \text{ is a maximal subset of unlinked indices}, \\ \prod_{\mathbf{u}\in(\mathbb{F}_2^2)^{|\mathbf{k}|_1}} A_{\mathbf{u}} \leqslant \Delta^{-4^{|\mathbf{k}|_1}} X \text{ and } A_{\mathbf{u}} = 1 \text{ for } \mathbf{u} \notin \mathscr{U}. \end{cases} \tag{6.15}$$

Similarly to [8, Eq.(50)] we will say that $\mathbf{A}$ is *admissible* for $\mathscr{U}$ if $A_{\mathbf{u}} > X^{\ddagger} \Leftrightarrow \mathbf{u} \in \mathscr{U}$, $A_{\mathbf{u}} = 1 \Leftrightarrow \mathbf{u} \notin \mathscr{U}$ and $\prod_{\mathbf{u}\in(\mathbb{F}_2^2)^{|\mathbf{k}|_1}} A_{\mathbf{u}} \leqslant \Delta^{-4^{|\mathbf{k}|_1}} X$. Assume that $\mathbf{A}$ is admissible for $\mathscr{U}$ and note that $\#\mathscr{U} = 2^{|\mathbf{k}|_1}$. By quadratic reciprocity we obtain that $S_{\boldsymbol{\chi}}(X, |\mathbf{k}|_1; q, a; \mathbf{A})$ equals

$$\sum_{(h_{\mathbf{u}})\in(\mathbb{Z}/4\mathbb{Z})^{2^{|\mathbf{k}|_1}}, \prod_{\mathbf{u}\in\mathscr{U}} h_{\mathbf{u}} \equiv 3 (\mathrm{mod}\ 4)} \left(\prod_{\mathbf{u},\mathbf{v}\in\mathscr{U}} (-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v}) \frac{h_{\mathbf{u}}-1}{2} \frac{h_{\mathbf{v}}-1}{2}} \right) \times$$

$$\sum_{\substack{(g_{\mathbf{u}})\in(\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}}, \prod_{\mathbf{u}\in\mathscr{U}} g_{\mathbf{u}} \equiv a (\mathrm{mod}\ q) \\ \forall \mathbf{u}\in\mathscr{U} (h_{\mathbf{u}} \equiv g_{\mathbf{u}} (\mathrm{mod}\ 4))}} \left(\prod_{\mathbf{u}\in\mathscr{U}} \prod_{\chi\in T} \chi(g_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})} \right) \times$$

$$\sum_{\substack{(D_{\mathbf{u}})\in\mathbb{N}^{2^{|\mathbf{k}|_1}}, \forall \mathbf{u}\ (\omega(D_{\mathbf{u}}) \leqslant \Omega) \\ \forall \mathbf{u}\ (D_{\mathbf{u}} \equiv g_{\mathbf{u}} (\mathrm{mod}\ q), A_{\mathbf{u}} \leqslant D_{\mathbf{u}} < \Delta A_{\mathbf{u}})}} \left(\prod_{\mathbf{u}\in\mathscr{U}} 2^{-|\mathbf{k}|_1 \omega(D_{\mathbf{u}})} \right) \mu^2 \left(\prod_{\mathbf{u}\in\mathscr{U}} D_{\mathbf{u}} \right).$$

We can evaluate the sum over $D_{\mathbf{u}}$ via the estimate,

$$\sum_{\substack{m\in\mathbb{N}\cap[y,Y] \\ \omega(m)=\ell \\ m\equiv g (\mathrm{mod}\ q)}} \mu(n_0 m)^2 = \frac{1}{\varphi(q)} \sum_{\substack{m\in\mathbb{N}\cap[y,Y] \\ \omega(m)=\ell \\ \gcd(m,q)=1}} \mu(n_0 m)^2 + O_A\left(\frac{(\ell+1)^A}{Y^{-1}(\log 2Y)^A} + \frac{\omega(n_0)}{Y^{-1+\frac{1}{7}}} \right), \tag{6.16}$$

valid for each square-free integer n_0 that is coprime to q, $A > 0, Y \geqslant y \geqslant 1, \ell \in \mathbb{Z}_{\geqslant 0}$, where the implied constant depends at most on A. This can be proved in a similar way as [8,

Lem.19] by replacing the congruence condition to modulus 4 on p_ℓ in [8, Eq.(53)] by one to modulus q. Applying (6.16) repeatedly as in [8, p.g.481-482] to estimate the sums over $D_{\mathbf{u}}$ leads us to

$$\sum_{\substack{(D_{\mathbf{u}})\in\mathbb{N}^{2^{|\mathbf{k}|_1}},\forall \mathbf{u}(\omega(D_{\mathbf{u}})\leqslant\Omega)\\ \forall \mathbf{u}(D_{\mathbf{u}}\equiv g_{\mathbf{u}}(\mathrm{mod}\ q),A_{\mathbf{u}}\leqslant D_{\mathbf{u}}<\Delta A_{\mathbf{u}})}}\left(\prod_{\mathbf{u}\in\mathscr{U}}2^{-|\mathbf{k}|_1\omega(D_{\mathbf{u}})}\right)\mu^2\left(\prod_{\mathbf{u}\in\mathscr{U}}D_{\mathbf{u}}\right)$$

$$=\varphi(q)^{-2^{|\mathbf{k}|_1}}\sum_{\substack{(D_{\mathbf{u}})\in\mathbb{N}^{2^{|\mathbf{k}|_1}},\forall \mathbf{u}(\omega(D_{\mathbf{u}})\leqslant\Omega)\\ \forall \mathbf{u}(A_{\mathbf{u}}\leqslant D_{\mathbf{u}}<\Delta A_{\mathbf{u}})}}\left(\prod_{\mathbf{u}\in\mathscr{U}}2^{-|\mathbf{k}|_1\omega(D_{\mathbf{u}})}\right)\mu^2\left(q\prod_{\mathbf{u}\in\mathscr{U}}D_{\mathbf{u}}\right)+O(X(\log X)^{-1-4^{|\mathbf{k}|_1}(1+2^{|\mathbf{k}|_1})}).$$

Using this we obtain as in [8, Eq.(55)] that for any fixed admissible $\mathscr{U}$ we have

$$\sum_{\mathbf{A}\text{ admissible for }\mathscr{U}}S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a;\mathbf{A})=2^{-|\mathbf{k}|_1}\varphi(q)^{-2^{|\mathbf{k}|_1}}\sum_{\substack{(h_{\mathbf{u}})\in(\mathbb{Z}/4\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}}h_{\mathbf{u}}\equiv 3(\mathrm{mod}\ 4)}}\left(\prod_{\mathbf{u},\mathbf{v}\in\mathscr{U}}(-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})\frac{h_{\mathbf{u}}-1}{2}\frac{h_{\mathbf{v}}-1}{2}}\right)\times$$

$$\sum_{\substack{(g_{\mathbf{u}})\in(\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}},\prod_{\mathbf{u}\in\mathscr{U}}g_{\mathbf{u}}\equiv a(\mathrm{mod}\ q)\\ \forall \mathbf{u}\in\mathscr{U}(h_{\mathbf{u}}\equiv g_{\mathbf{u}}(\mathrm{mod}\ 4))}}\left(\prod_{\mathbf{u}\in\mathscr{U}}\prod_{\chi\in T}\chi(g_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})}\right)\times$$

$$\sum_{\substack{(D_{\mathbf{u}})\in\mathbb{N}^{2^{|\mathbf{k}|_1}},\forall \mathbf{u}\ (\omega(D_{\mathbf{u}})\leqslant\Omega)\\ \forall \mathbf{u}\ (A_{\mathbf{u}}\leqslant D_{\mathbf{u}}<\Delta A_{\mathbf{u}})}}\left(\prod_{\mathbf{u}\in\mathscr{U}}2^{-|\mathbf{k}|_1\omega(D_{\mathbf{u}})}\right)\mu^2\left(\mathrm{rad}(q)\prod_{\mathbf{u}\in\mathscr{U}}D_{\mathbf{u}}\right)+O\left(\frac{X}{\log X}\right),$$

where the radical $\mathrm{rad}(m)$ stands for the product of the distinct prime divisors of an integer $m>1$. We can now see that the condition $\omega(D_{\mathbf{u}})\leqslant\Omega$ can be ignored at the cost of an error term of size $\ll X(\log X)^{-1}$ as in the beginning of §6.3. We can furthermore show as in [8, p.g.482] that

$$\sum_{\substack{(D_{\mathbf{u}})\in\mathbb{N}^{2^{|\mathbf{k}|_1}}\\ \forall \mathbf{u}(A_{\mathbf{u}}\leqslant D_{\mathbf{u}}<\Delta A_{\mathbf{u}})}}\left(\prod_{\mathbf{u}\in\mathscr{U}}2^{-|\mathbf{k}|_1\omega(D_{\mathbf{u}})}\right)\mu^2\left(\mathrm{rad}(q)\prod_{\mathbf{u}\in\mathscr{U}}D_{\mathbf{u}}\right)=\sum_{m\leqslant X}\mu(\mathrm{rad}(q)m)^2+O\Big(X(\log X)^{\varepsilon-2^{-|\mathbf{k}|_1}}\Big).$$

It is easily proved via Möbius inversion that for fixed $a,q>0$ with $\gcd(a,q)=1$ we have

$$\sum_{m\leqslant X}\mu(\mathrm{rad}(q)m)^2=\frac{\varphi(q)}{q}\Big(\prod_{p\mid q}(1-p^{-2})\Big)X+O\left(\sqrt{X}\right)$$

and

$$\sum_{\substack{m\leqslant X\\ m\equiv a(\mathrm{mod}\ q)}}\mu(m)^2=\frac{1}{q}\Big(\prod_{p\mid q}(1-p^{-2})\Big)X+O\left(\sqrt{X}\right).$$

Combining these yields

$$\sum_{m\leqslant X}\mu(\mathrm{rad}(q)m)^2=\varphi(q)\sum_{\substack{m\leqslant X\\ m\equiv a(\mathrm{mod}\ q)}}\mu(m)^2+O\left(\sqrt{X}\right).$$

We thus obtain the following for every maximal unlinked subset $\mathscr{U}$,

$$\sum_{\mathbf{A}\text{ admissible for }\mathscr{U}} S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a;\mathbf{A}) = \frac{\gamma_{\boldsymbol{\psi}}(\mathscr{U})}{2^{|\mathbf{k}|_1}\varphi(q)^{2^{|\mathbf{k}|_1}-1}}\left(\sum_{\substack{m\leqslant X\\ m\equiv a(\mathrm{mod}\ q)}}\mu(m)^2\right)+O\Big(X(\log X)^{\varepsilon-2^{-|\mathbf{k}|_1}}\Big),$$

where

$$\gamma_{\boldsymbol{\psi}}(\mathscr{U}) := \sum_{\substack{(h_{\mathbf{u}})\in(\mathbb{Z}/4\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} h_{\mathbf{u}}\equiv 3(\mathrm{mod}\ 4)}}\left(\prod_{\mathbf{u},\mathbf{v}\in\mathscr{U}}(-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})\frac{h_{\mathbf{u}}-1}{2}\frac{h_{\mathbf{v}}-1}{2}}\right)\sum_{\substack{(g_{\mathbf{u}})\in(\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} g_{\mathbf{u}}\equiv a(\mathrm{mod}\ q)\\ \forall\mathbf{u}\in\mathscr{U}(h_{\mathbf{u}}\equiv g_{\mathbf{u}}(\mathrm{mod}\ 4))}}\left(\prod_{\mathbf{u}\in\mathscr{U}}\prod_{\chi\in T}\chi(g_{\mathbf{u}})^{\Psi_\chi(\mathbf{u})}\right).$$

We can now infer via (6.14) that the last equation proves

$$\frac{S_{\boldsymbol{\chi}}(X,|\mathbf{k}|_1;q,a)}{\#\big\{m\in[1,X]:q\mid m-a,\mu(m)^2=1\big\}} = \left(\sum_{\mathscr{U}}\gamma_{\boldsymbol{\psi}}(\mathscr{U})\right)\frac{\varphi(q)^{1-2^{|\mathbf{k}|_1}}}{2^{|\mathbf{k}|_1}}+O((\log X)^{\varepsilon-2^{-|\mathbf{k}|_1}}),$$

where $\mathscr{U}$ ranges over maximal unlinked subsets of $\mathbb{F}_2^{2|\mathbf{k}|_1}$.

6.5. **Simplifying $\gamma_\psi(\mathscr{U})$.** Introduce the following Dirichlet character (mod n_1n_2),

$$\rho_{\mathbf{u}} := \prod_{\chi\in T}\chi^{\Psi_\chi(\mathbf{u})}.$$

We will call a maximal set of unlinked indices $\mathscr{U}$ *stable* if

$$\forall\chi\in T,\forall\mathbf{u}\in\mathscr{U}(\Psi_\chi(\mathbf{u})=0)\text{ or }\forall\chi\in T,\forall\mathbf{u}\in\mathscr{U}(\Psi_\chi(\mathbf{u})=1).$$

Let us now prove that

$$\sum_{\substack{(g_{\mathbf{u}})\in(\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} g_{\mathbf{u}}\equiv a(\mathrm{mod}\ q)\\ \forall\mathbf{u}\in\mathscr{U}(h_{\mathbf{u}}\equiv g_{\mathbf{u}}(\mathrm{mod}\ 4))}}\prod_{\mathbf{u}\in\mathscr{U}}\rho_{\mathbf{u}}(g_{\mathbf{u}}) = \mathbf{1}_{\mathscr{U}\text{ stable}}(\mathscr{U})\left(\frac{\varphi(q)}{2}\right)^{2^{|\mathbf{k}|_1}-1}.$$

Write $q=2^bn_0m$, where $b:=\nu_2(q)$, $\gcd(n_0,n_1n_2)=1$ and n_0 has radical equal to n_1n_2. Define

$$U_1(n_0):=\{u\in\mathbb{Z}/n_0\mathbb{Z}:u\equiv 1\,(\mathrm{mod}\ n_1n_2)\}\text{ and }U_1(2^b):=\{u\in\mathbb{Z}/2^b\mathbb{Z}:u\equiv 1\,(\mathrm{mod}\ 4)\}.$$

Recalling the identification of groups $(\mathbb{Z}/q\mathbb{Z})^*=U_1(2^b)\times(\mathbb{Z}/4\mathbb{Z})^*\times U_1(n_0)\times(\mathbb{Z}/n_1n_2\mathbb{Z})^*$, we see that

$$\sum_{\substack{(g_{\mathbf{u}})\in(\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} g_{\mathbf{u}}\equiv a(\mathrm{mod}\ q)\\ \forall\mathbf{u}\in\mathscr{U}(h_{\mathbf{u}}\equiv g_{\mathbf{u}}(\mathrm{mod}\ 4))}}\prod_{\mathbf{u}\in\mathscr{U}}\rho_{\mathbf{u}}(g_{\mathbf{u}}) = (\#U_1(2^b)\#U_1(n_0)\varphi(m))^{2^{|\mathbf{k}|_1}-1}\sum_{\substack{(m_{\mathbf{u}})\in(\mathbb{Z}/n_1n_2\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} m_{\mathbf{u}}\equiv a(\mathrm{mod}\ n_1n_2)}}\prod_{\mathbf{u}\in\mathscr{U}}\rho_{\mathbf{u}}(m_{\mathbf{u}}).$$

Note that we have $\prod_{\mathbf{u}\in\mathscr{U}}\rho_{\mathbf{u}}(m_{\mathbf{u}})=\rho_{\mathbf{u}_0}(a)=1$ owing to (5.2)-(5.4). Therefore, fixing $\mathbf{u}_0\in\mathscr{U}$, we have the following equality for any choice of $m_{\mathbf{u}}$ in the above sum

$$\prod_{\mathbf{u}\in\mathscr{U}}\rho_{\mathbf{u}}(m_{\mathbf{u}}) = \rho_{\mathbf{u}_0}(\mathbf{u}_0)\prod_{\mathbf{u}\in\mathscr{U}-\{\mathbf{u}_0\}}\rho_{\mathbf{u}}(\mathbf{u}) = \prod_{\mathbf{u}\in\mathscr{U}-\{\mathbf{u}_0\}}\Big(\frac{\rho_{\mathbf{u}}(m_{\mathbf{u}})}{\rho_{\mathbf{u}_0}(m_{\mathbf{u}})}\Big).$$

Therefore

$$\sum_{\substack{(m_{\mathbf{u}})\in(\mathbb{Z}/n_1n_2\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} m_{\mathbf{u}}\equiv a(\mathrm{mod}\ n_1n_2)}}\prod_{\mathbf{u}\in\mathscr{U}}\rho_{\mathbf{u}}(m_{\mathbf{u}}) = \sum_{(m_{\mathbf{u}})\in((\mathbb{Z}/n_1n_2\mathbb{Z})^*)^{2^{|\mathbf{k}|_1-1}}}\prod_{\mathbf{u}\in\mathscr{U}-\{\mathbf{u}_0\}}\frac{\rho_{\mathbf{u}}(m_{\mathbf{u}})}{\rho_{\mathbf{u}_0}(m_{\mathbf{u}})}.$$

But the last clearly splits as

$$\prod_{\mathbf{u}\in\mathscr{U}-\{\mathbf{u}_0\}}\Big(\sum_{(m_{\mathbf{u}})\in(\mathbb{Z}/n_1n_2\mathbb{Z})^*}\frac{\rho_{\mathbf{u}}(m_{\mathbf{u}})}{\rho_{\mathbf{u}_0}(m_{\mathbf{u}})}\Big) = \prod_{\mathbf{u}\in\mathscr{U}-\{\mathbf{u}_0\}}\Big(\sum_{(m_{\mathbf{u}})\in(\mathbb{Z}/n_1n_2\mathbb{Z})^*}\prod_{\chi\in T}\chi^{\psi_\chi(\mathbf{u})-\psi_\chi(\mathbf{u}_0)}(m_{\mathbf{u}})\Big).$$

Using that the set of χ in T consists of a set of linearly independent characters, we obtain that each factor of the last product vanishes if and only if ψ_χ is not constant on $\mathscr{U}$, i.e. if and only if $\mathscr{U}$ is not stable. In the stable case its value is $\varphi(n_1n_2)^{2^{|\mathbf{k}|_1-1}}$. Therefore we have proved that

$$\sum_{\substack{(g_{\mathbf{u}})\in(\mathbb{Z}/q\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} g_{\mathbf{u}}\equiv a(\mathrm{mod}\ q)\\ \forall\mathbf{u}\in\mathscr{U}(h_{\mathbf{u}}\equiv g_{\mathbf{u}}(\mathrm{mod}\ 4))}}\prod_{\mathbf{u}\in\mathscr{U}}\rho_{\mathbf{u}}(g_{\mathbf{u}}) = (\#U_1(2^b)\#U_1(n_0)\varphi(m)\varphi(n_1n_2))^{2^{|\mathbf{k}|_1-1}}\mathbf{1}_{\mathscr{U}\text{ stable}}(\mathscr{U})$$

$$= \Big(\frac{\varphi(q)}{2}\Big)^{2^{|\mathbf{k}|_1-1}}\mathbf{1}_{\mathscr{U}\text{ stable}}(\mathscr{U}),$$

from which we deduce that

$$\sum_{\mathscr{U}}\gamma_\psi(\mathscr{U}) = \Big(\frac{\varphi(q)}{2}\Big)^{2^{|\mathbf{k}|_1-1}}\sum_{\mathscr{U}\text{stable}}\sum_{\substack{(h_{\mathbf{u}})_{\mathbf{u}\in\mathscr{U}}\in(\mathbb{Z}/4\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} h_{\mathbf{u}}\equiv 3(\mathrm{mod}\ 4)}}\Big(\prod_{\mathbf{u},\mathbf{v}\in\mathscr{U}}(-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})\frac{h_{\mathbf{u}}-1}{2}\frac{h_{\mathbf{v}}-1}{2}}\Big),$$

where the pairs $\mathbf{u},\mathbf{v}$ are unordered. The inner sum is identical to the one appearing in the work of Fouvry and Klüners, however the outer sum does not appear in their work. Define

$$\gamma(\mathscr{U}) := \sum_{\substack{(h_{\mathbf{u}})_{\mathbf{u}\in\mathscr{U}}\in(\mathbb{Z}/4\mathbb{Z})^{2^{|\mathbf{k}|_1}}\\ \prod_{\mathbf{u}\in\mathscr{U}} h_{\mathbf{u}}\equiv 3(\mathrm{mod}\ 4)}}\Big(\prod_{\mathbf{u},\mathbf{v}\in\mathscr{U}}(-1)^{\Phi_{|\mathbf{k}|_1}(\mathbf{u},\mathbf{v})\frac{h_{\mathbf{u}}-1}{2}\frac{h_{\mathbf{v}}-1}{2}}\Big).$$

We are left with proving

$$\sum_{\mathscr{U}\text{ stable}}\gamma(\mathscr{U}) = 2^{2^{|\mathbf{k}|_1}+|\mathbf{k}|_1-1}\mathscr{N}_2(|\mathbf{k}|_1-\#T) \tag{6.17}$$

and this will be our aim in §6.6.

6.6. **Combinatorics.** From [8, Lem.18] we know that the maximal unlinked sets of indices $\mathscr{U}$ consist precisely of cosets of $|\mathbf{k}|_1$-dimensional subspaces of $\mathbb{F}_2^{2|\mathbf{k}|_1}$. Therefore stable $\mathscr{U}$ are cosets of $|\mathbf{k}|_1$-dimensional subspace of $\mathbb{F}_2^{2|\mathbf{k}|_1}$, where all the Ψ_χ vanish.

Next, introduce the bilinear form on $\mathbb{F}_2^{2|\mathbf{k}|_1}$ via

$$L(\mathbf{u},\mathbf{v}) := \sum_{j=0}^{|\mathbf{k}|_1}\mathbf{u}_{2j+1}(\mathbf{v}_{2j+1}+\mathbf{v}_{2j+2}).$$

Using the the terminology from [8], we say that a $|\mathbf{k}|_1$-dimensional subspace, $\mathscr{U}_0$, of $\mathbb{F}_2^{2|\mathbf{k}|_1}$ is *good* if

$$L_{|\mathscr{U}_0\times\mathscr{U}_0}\equiv\ 0.$$

Recall that the upshot of [8, Lem.22-25] is that γ vanishes on all cosets of non-good subspaces, meanwhile the total contribution from the set of cosets of a fixed good subspace is $2^{2^{|\mathbf{k}|_1}+|\mathbf{k}|_1-1}$. This provides us with

$$\sum_{\mathscr{U}\ \text{stable}}\gamma(\mathscr{U})=2^{2^{|\mathbf{k}|_1}+|\mathbf{k}|_1-1}\#\{\mathscr{U}_0\ \text{good}:\Psi_\chi(\mathscr{U}_0)=0\ \text{for each}\ \chi\in T\}.$$

Now, following the proof of [8, Lem.26], if $\{e_1,\cdots,e_{2|\mathbf{k}|_1}\}$ denotes the standard basis of $\mathbb{F}_2^{2|\mathbf{k}|_1}$, choose a new basis via

$$\{b_1,\cdots,b_{2|\mathbf{k}|_1}\}=\{e_1+e_2,e_2,\cdots,e_{2j-1}+e_{2j},e_{2j},\cdots,e_{2|\mathbf{k}|_1-1}+e_{2|\mathbf{k}|_1},e_{2|\mathbf{k}|_1}\}.$$

Then, with respect to the new basis, L assumes the form

$$L(\mathbf{x},\mathbf{y})=\sum_{j=0}^{j-1}\mathbf{x}_{2j+1}\mathbf{y}_{2j+2}.$$

In the proof of part (i) of [8, Lem.25] it is verified that, if X consists of the subspace generated by $\{b_i:i\ \text{odd}\}$ and Y consists of the subspace generated by $\{b_i:i\ \text{even}\}$, the map sending $\mathscr{U}_0\mapsto\pi_X(\mathscr{U}_0)$ where π_X is the projection map $\mathbb{F}_2^{2|\mathbf{k}|_1}=X\oplus Y\to X$ gives a bijection between good subspaces of $\mathbb{F}_2^{2|\mathbf{k}|_1}$ and vector subspaces of $\mathbb{F}_2^{|\mathbf{k}|_1}$. On the other hand, we are counting only good subspaces where Ψ_χ vanishes for each $\chi\in T$. Observe that owing to (6.4) we have that Ψ_χ are all constantly 0 on Y, hence they define $\#T$ linearly independent linear functions from X to $\mathbb{F}_2$ which we will denote by the same letters. Therefore $\mathscr{U}_0\to\pi_X(\mathscr{U}_0)$ provides a bijection between good subspaces where all Ψ_χ vanish and subspaces of X where all Ψ_χ vanish. Given that $\Psi_\chi:X\to\mathbb{F}_2$ are independent we find that the cardinality of such subspaces is precisely $\mathscr{N}_2(|\mathbf{k}|_1-\#T)$. This substantiates (6.17), which concludes the proof of Theorem 5.6.

7. From the mixed moments to the distribution

This section is devoted to deduce Theorem 5.7 from Theorem 5.6. We will follow an adaptation of a method used by Heath-Brown in [10].
As explained in §4, Theorem 5.7 can be equivalently rephrased as a theorem about the distribution of the vector

$$D\mapsto(m_\chi(D))_{\widehat{G}_{n_1}\times\widetilde{\widehat{G}}_{n_2}}.$$

Namely consider for any positive integer j and subspace $Y\subseteq\widehat{G}_{n_1}\times\widetilde{\widehat{G}}_{n_2}$, the vector

$$\mathbf{v}^{(j,Y)}\in\mathbb{Z}_{\geqslant0}^{\widehat{G}_{n_1}\times\widetilde{\widehat{G}}_{n_2}},$$

defined as $\mathbf{v}_\chi^{(j,Y)}=j$ if $\chi\in Y$ and $\mathbf{v}_\chi^{(j,Y)}=j-1$ if $\chi\notin Y$. Assign to $\mathbf{v}^{(j,Y)}$ *mass*

$$\mu(\mathbf{v}^{(j,Y)})=\mu_{\mathrm{CL}}(A\in\mathscr{G}_2:\#A[2]=2^{j-1})\frac{\#\operatorname{Epi}(\mathbb{F}_2^{j-1},Y)}{\#\operatorname{Hom}(\mathbb{F}_2^{j-1},\widehat{G}_{n_1}\times\widetilde{\widehat{G}}_{n_2})}.$$

On the other hand, assign to all other vectors $\mathbf{v} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}$ mass equal to 0. In Proposition 4.8 it is shown that this equips $\mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}$ with a probability measure satisfying the following *moment equations*:

$$\sum_{\mathbf{v} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}} 2^{\mathbf{v} \cdot \mathbf{k}} \mu(\mathbf{v}) = C_{\mathbf{k}},$$

where for any $\mathbf{k} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}$ we define

$$C_{\mathbf{k}} := 2^{|\mathbf{k}|_1} \sum_{Y \subseteq \widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}} \mathbb{P}_{(\mathbf{k})}(Y) \mathscr{N}_2(|\mathbf{k}|_1 - \dim(Y))$$

and where $\mathbf{v} \cdot \mathbf{k}$ denotes the inner product.

We begin the proof of Theorem 5.7 by showing that the distribution μ is characterized by the moment equations given above. Indeed we show more, namely assume x is a map $\mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}} \to [0,1]$ satisfying for any $\mathbf{k} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}$ the moment relations

$$\sum_{\mathbf{v} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}} 2^{\mathbf{v} \cdot \mathbf{k}} x(\mathbf{v}) = C_{\mathbf{k}}. \tag{7.1}$$

Observe that one has the trivial bound $C_{\mathbf{k}} \ll 2^{|\mathbf{k}|_1} \mathscr{N}_2(|\mathbf{k}|_1)$, which leads to $C_{\mathbf{k}} \ll 2^{\frac{|\mathbf{k}|_1^2 + 4|\mathbf{k}|_1}{4}}$. Letting $F(t) := \prod_{n=0}^{\infty}(1 - t2^{-n})$, we therefore see that for any $\mathbf{k} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}$, the following series is absolutely convergent,

$$\sum_{\mathbf{n} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}} a_{\mathbf{n}} C_{\mathbf{n}} 2^{-\mathbf{n} \cdot \mathbf{k}}, \tag{7.2}$$

where $a_{\mathbf{n}}$ is the $\mathbf{n}$-coefficient of the Taylor expansion of

$$\widetilde{F}(\mathbf{z}) := \prod_{\chi \in \widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}} F(z_\chi).$$

Injecting (7.1) into (7.2), expanding in terms of x and exchanging the order of summation, we obtain

$$\sum_{\mathbf{n} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}} a_{\mathbf{n}} C_{\mathbf{n}} 2^{-\mathbf{n} \cdot \mathbf{k}} = \sum_{\mathbf{m} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}} \widetilde{F}((2^{\mathbf{m}_\chi - \mathbf{k}_\chi})) x(\mathbf{m}).$$

If for all χ we have $\mathbf{m}_\chi < \mathbf{k}_\chi$ then $\widetilde{F}((2^{\mathbf{m}_\chi - \mathbf{k}_\chi})) \neq 0$, otherwise we have $\widetilde{F}((2^{\mathbf{m}_\chi - \mathbf{k}_\chi})) = 0$. Therefore, the right side is a finite sum supported in the region $\mathbf{m}_\chi < \mathbf{k}_\chi$ for every χ. Hence, using the triangular system of relations above one can successively reconstruct the function $x(\mathbf{m})$ from the moments $C_{\mathbf{k}}$. Therefore, we necessarily have $x(\mathbf{m}) = \mu(\mathbf{m})$ described above.

Let a, q be integers as in Theorem 5.7 and for any $\mathbf{j} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}$ and $X \in \mathbb{R}_{\geqslant 1}$, define the quantity $d_{\mathbf{j}}(X)$ as the proportion of all positive square-free integers $D \leqslant X$ satisfying $D \equiv a \pmod q$ and $\mathbf{m}_\chi(D) = 2^{\mathbf{j}_\chi}$ for all χ. Therefore, Theorem 5.6 shows that for any $\mathbf{k} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widehat{G}}_{n_2}}$ we have $\sum_{\mathbf{r}} d_{\mathbf{r}}(X) 2^{\mathbf{r} \cdot \mathbf{k}} = C_{\mathbf{k}} + o(1)$, as $X \to +\infty$, where the sum is taken

over $\mathbf{r} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widetilde{G}}_{n_2}}$. The argument concludes as follows: fix any vector $\mathbf{v} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widetilde{G}}_{n_2}}$; by compactness of the interval $[0,1]$ and a standard diagonal argument, one can choose a sequence $\{Y_n\}_{n\in\mathbb{N}}$ tending to infinity, such that $d_{\mathbf{v}}(Y_n)$ converges to any of the limit points of $\{d_{\mathbf{v}}(X) : X \in \mathbb{R}_{\geqslant 1}\}$, call it $d'_{\mathbf{v}}$, while for every other $\mathbf{w}$ the sequence $d_{\mathbf{w}}(Y_n)$ is also converging to some limit point $d'_{\mathbf{w}}$. Next, we fix $\mathbf{h} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widetilde{G}}_{n_2}}$, and we use the previous moment relation for $\mathbf{k} = 2\mathbf{h}$, trivially bounding each terms with the total sum, providing $d_{\mathbf{r}}(Y_n) \ll_{\mathbf{h}} 2^{-\mathbf{r}\cdot\mathbf{h}}$. This enables us to apply the dominated convergence theorem to exchange the sum and the limit in the expression of the $\mathbf{h}$-th moment, from which we deduce that $d'_{\mathbf{w}}$ satisfies the following moment equations as well:

$$\sum_{\mathbf{w}\in\mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widetilde{G}}_{n_2}}} 2^{\mathbf{w}\cdot\mathbf{h}} d'_{\mathbf{w}} = C_{\mathbf{h}}.$$

We must therefore have $d'_{\mathbf{w}} = \mu(\mathbf{w})$ for all $\mathbf{w} \in \mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widetilde{G}}_{n_2}}$. Note that $d'_{\mathbf{v}}$ was an arbitrary limit point of $d_{\mathbf{v}}(X)$, hence we deduce that

$$\lim_{X\to\infty} d_{\mathbf{v}}(X) = \mu(\mathbf{v}).$$

Since $\mathbf{v}$ was chosen arbitrarily in $\mathbb{Z}_{\geqslant 0}^{\widehat{G}_{n_1} \times \widetilde{\widetilde{G}}_{n_2}}$ we have thus shown that Theorem 5.7 holds, thereby concluding the proof of Theorem 5.7.

References

[1] B. Alberts and J. Klys, The distribution of H_8-extensions of quadratic fields. `arXiv:1611.05595`, (2017).
[2] M. Bhargava, A. Shankar and J. Tsimerman, On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.* **193** (2013), 439–499.
[3] M. Bhargava and I. Varma, On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields. *Duke Math. J.* **164** (2015), 1911–1933.
[4] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields. *Number theory, Noordwijkerhout 1983*, Lecture Notes in Math., Springer, Berlin, (1984), 33–62.
[5] D. Dummit and J. Voight (with appendix of R. Foote), The 2-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units. `arXiv:1702.00092`, (2017).
[6] J. Ellenberg, A. Venkatesh and C. Westerland, Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. *Ann. of Math.* **183** (2016), 729–786.
[7] É. Fouvry and J. Klüners, Cohen-Lenstra heuristics of quadratic number fields. *Algorithmic number theory*, Lecture Notes in Comput. Sci., Springer, Berlin, (2006), 40–55.
[8] ———, On the 4-rank of class groups of quadratic number fields. *Invent. Math.* **167** (2007), 455–513.
[9] F. Gerth, Extension of conjectures of Cohen and Lenstra. *Exposition. Math.* **5** (1987), 181–184.
[10] R. Heath-Brown, The size of Selmer groups for the congruent number problem. II. *Invent. Math.* **118** (1994), 331–370.
[11] ———, A mean value estimate for real character sums. *Acta Arith.* **72** (1995), 235–275.
[12] H. Iwaniec and E. Kowalski, *Analytic number theory*. American Math. Soc. Providence, RI, (2004).
[13] B. W. Jordan, Z. Klagsbrun, B. Poonen, C. Skinner and Y. Zaytman, Statistics of K-groups modulo p for the ring of integers of a varying quadratic number field. `arXiv:1703.00108`, (2017).
[14] J. Klys, The distribution of p-torsion in degree p cyclic fields. `arXiv:1610.00226`, (2016).
[15] J. Neukirch, *Algebraic number theory*. Springer-Verlag, Berlin, (1999).
[16] A. Smith, 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. `arXiv:1702.02325v2`, (2017).
[17] R. P. Stanley, *Enumerative combinatorics. Volume 1.* Cambridge University Press, Cambridge, (2012)
[18] I. Varma, The mean number of 3-torsion elements in ray class groups of quadratic fields. `arXiv:1609.02292`, (2016).

[19] C. A. Weibel, *An introduction to homological algebra*. Cambridge University Press, Cambridge, (1994).
[20] M. M. Wood, Cohen–Lenstra and local conditions. *Preprint*, (2017).
[21] ———, Non-abelian Cohen–Lenstra moments. `arXiv:1702.04644`, (2017).
[22] ———, Random integral matrices and the Cohen–Lenstra Heuristics. `arxiv.org/abs/1504.04391`, (2015).

Mathematisch Instituut, Universiteit Leiden, Leiden, 2333 CA, Netherlands
E-mail address: `c.pagano@math.leidenuniv.nl`

Max Planck Institute for Mathematics, Vivatsgasse 7, Bonn, 53111, Germany
E-mail address: `sofos@mpim-bonn.mpg.de`

CHAPTER

3

Jump sets in local fields

C. Pagano

JUMP SETS IN LOCAL FIELDS

C. PAGANO

Abstract. We show how to use the combinatorial notion of jump sets to parametrize the possible structures of the group of principal units of local fields, viewed as filtered modules. We establish a natural bijection between the set of jump sets and the orbit space of a p-adic group of filtered automorphisms acting on a free filtered module. This, together with a Markov process on Eisenstein polynomials, culminates into a *mass-formula* for unit filtrations. As a bonus the proof leads in many cases to explicit invariants of Eisenstein polynomials, yielding a link between the filtered structure of the unit group and ramification theory. Finally, with the basic theory of filtered modules developed here, we recover, with a more conceptual proof, a classification, due to Miki, of the possible sets of upper jumps of a wild character: these are all jump sets, with a set of exceptions explicitly prescribed by the jump set of the local field and the size of its residue field.

Contents

1. Introduction

In this paper we introduce *jump sets*, elementary combinatorial objects, and use them to establish several fundamental results concerning two natural filtrations in the theory of local fields. These are the unit filtration and the ramification filtration. We subdivide our main results into three themes and introduce each of the themes with a basic question. We use the answer to each question as a starting point to explain our main results.

1.1. **Three questions.**

Date: November 7, 2018.
2010 *Mathematics Subject Classification.* 11F85.

1.1.1. *Principal units.* Let p be a prime number. A non-archimedean local field is a field K, equipped with a non-archimedean absolute value $|\cdot|$, such that K is a non-discrete locally compact space with respect to the topology induced by $|\cdot|$. Write $O := \{x \in K : |x| \leqslant 1\}$ for the ring of integers and $m := \{x \in K : |x| < 1\}$ for its unique maximal ideal. We assume that p is the residue characteristic of K, i.e. the characteristic of the finite field O/m. Denote by f_K the positive integer satisfying $p^{f_K} = \#O/m$. Recall that O is a discrete valuation ring, and denote by $\mathrm{v}_K : K^* \to \mathbb{Z}$ the valuation that maps any generator of the ideal m to 1.

The inclusions $K^* \supseteq O^* \supseteq U_1(K) = 1 + m = \{\text{principal units}\}$ split in the category of topological groups. So, as topological groups, we have $K^* \simeq_{\text{top.gr.}} \mathbb{Z} \times O^*$, $O^* = (O/m)^* \times U_1(K)$, where $\mathbb{Z}$ is taken with the discrete topology. This paper focuses on $U_1(K)$. The profinite group $U_1(K)$ is a pro-p group, thus, being abelian, it has a natural structure of $\mathbb{Z}_p$-module. As a topological $\mathbb{Z}_p$-module $U_1(K)$ is very well understood. If $\mathrm{char}(K) = 0$ then $U_1(K) \simeq \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times \mu_{p^\infty}(K)$, while if $\mathrm{char}(K) = p$ then $U_1(K) \simeq \mathbb{Z}_p^\omega$. Here ω denotes the first infinite ordinal number and $\mu_{p^\infty}(K)$ denotes the p-part of the group of roots of unity of K. In both cases the isomorphism is meant in the category of topological $\mathbb{Z}_p$-modules. For a reference see [3, Chapter 1, Section 6]

The $\mathbb{Z}_p$-module $U_1(K)$ comes naturally with some additional structure, namely the filtration $U_1(K) \supseteq U_2(K) \supseteq \ldots \supseteq U_i(K) \supseteq \ldots$, where $U_i(K) = 1 + m^i$. In order to take into account this additional structure we make the following definition. A *filtered $\mathbb{Z}_p$-module* is a sequence of $\mathbb{Z}_p$-modules, $M_1 \supseteq M_2 \supseteq \ldots \supseteq M_i \supseteq \ldots$, with $\bigcap_{i \in \mathbb{Z}_{\geqslant 1}} M_i = \{0\}$. We will use the symbol $M_\bullet$ to denote a filtered $\mathbb{Z}_p$-module. A morphism of filtered $\mathbb{Z}_p$-modules is a morphism of $\mathbb{Z}_p$-modules $\varphi : M_1 \to N_1$ such that $\varphi(M_i) \subseteq N_i$ for each positive integer i. A filtered module can be also described in terms of its *weight* map $w : M_1 \to \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$ attaching to each x the sup of the set of integers i such that $x \in M_i$.

Question (**1**) What does $U_1(K)$ look like as a filtered $\mathbb{Z}_p$-module?

In other words, we ask what is, as a function of K, the isomorphism class of $U_1(K)$ in the category of filtered $\mathbb{Z}_p$-modules. We will sometimes use the symbol $U_\bullet(K)$ to stress the presence of the additional structure present in $U_1(K)$, coming from the filtration. Denote by G_K the absolute Galois group of K. Thanks to local class field theory, the above question is essentially asking to describe G_K^{ab} as a filtered group, where the filtration is given by the upper numbering on G_K^{ab}. Equipping any quotient of G_K with the upper numbering filtration and studying it in the category of filtered groups is a natural thing to do. Indeed it is a fact that the local field K can be uniquely determined from the filtered group G_K, see [7].

1.1.2. *Galois sets.* Fix K^{sep} a separable closure of K. Denote by $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ the absolute Galois group. Denote by $|\cdot|$ the unique extension of $|\cdot|$ to K^{sep}. Take L/K finite separable. Thus L naturally comes with a *Galois set*: $\Gamma_L = \{K\text{-embeddings } L \to K^{\mathrm{sep}}\}$. Recall by Galois theory that this is a transitive G_K-set with $|\Gamma_L| = [L : K]$. This holds for any field K. But, if K is a local field, there is an additional piece of structure, namely a G_K-invariant metric on Γ_L, defined as follows: $d(\sigma, \tau) = \max_{x \in O_L} |\sigma(x) - \tau(x)|$ $(\sigma, \tau \in \Gamma_L)$. Here O_L denotes the ring of integers of L. Observe that the maximum is attained since O_L is compact and the function in consideration is continuous. If L/K is unramified then the metric space Γ_L is a simple one: $d(\sigma, \tau) = 1$ whenever $\sigma \neq \tau$. Since every finite separable extension of local fields splits canonically as an unramified one and a totally ramified one,

we go to the other extreme of the spectrum and consider L/K totally ramified: in other words we put $L = K(\pi)$, with $g(\pi) = 0$, where $g \in K[x]$ is *Eisenstein*. We can now phrase the second question.

Question (**2**) Which invariants does the metric space impose on the coefficients of g?

As we shall see, the answer to our second question comes often with a surprising link to the answer to our first question.

1.1.3. *Jumps of characters.* A *character* of $U_1(K)$ is a continuous group homomorphism $\chi : U_1(K) \to \mathbb{Q}_p/\mathbb{Z}_p \simeq \mu_{p^\infty}(\mathbb{C})$. Define $J_\chi = \{i \in \mathbb{Z}_{\geqslant 1} : \chi(U_i(K)) \neq \chi(U_{i+1}(K))\} = \{\text{jumps for } \chi\}$. Since $U_1(K)$ is a profinite group, a character χ has always finite image. Moreover it is easy to check that at each jump the size of the image gets divided exactly by p. So one has that $\text{order}(\chi) = p^{|J_\chi|} < \infty$. In particular J_χ is always a finite subset of $\mathbb{Z}_{\geqslant 1}$. We can now phrase our third question.

Question (**3**) Given a local field K, which subsets of $\mathbb{Z}_{\geqslant 1}$ occur as J_χ for a character of $U_1(K)$?

Thanks to local class field theory this question is essentially asking to determine which sets $A \subseteq \mathbb{Z}_{\geqslant 1}$ occur as the set of jumps in the upper filtration of $\text{Gal}(L/K)$, for some L, a finite cyclic totally ramified extension of K, with $[L : K]$ a power of p. This connection is articulated in Section 6.

1.2. **Shifts and jump sets.** The goal of this subsection is to explain the notion of a *jump set*. Jump sets are defined using *shifts*. A *shift* is a strictly increasing function $\rho : \mathbb{Z}_{\geqslant 1} \to \mathbb{Z}_{\geqslant 1}$, with $\rho(1) > 1$. If $T_\rho = \mathbb{Z}_{\geqslant 1} - \rho(\mathbb{Z}_{\geqslant 1})$ is finite, put $e^* = \max(T_\rho) + 1$. The example of shift relevant for local fields is the following:

$$\rho_{e,p}(i) = \min\{i + e, pi\} \text{ for } p \text{ prime}, e \in \mathbb{Z}_{>0} \cup \{\infty\}.$$

In this example one has that if $e \neq \infty$, then $e^* = \lceil \frac{pe}{p-1} \rceil$. The case $e \neq \infty$ will be used for local fields of characteristic 0, and the case $e = \infty$ will be used for local fields of characteristic p.

The following property explains how this shift can be used to express how p-powering in U_1 changes the weights in the filtration.

Crucial property: If K is local field, $e = \text{v}_K(p)$, then

$$U_i^p \subset U_{\rho(i)} \text{ for } \rho = \rho_{e,p}.$$

This follows at once inspecting valuations in the binomial expansion $(1+x)^p = 1+px+\ldots+x^p$. For a local field K we denote by ρ_K the shift $\rho_{e,p}$.

We can now provide the notion of a jump set for a shift ρ and respectively, in case T_ρ is finite, of an extended jump set for ρ. A *jump set* for ρ (resp. an *extended jump set* for ρ) is a finite subset $A \subseteq \mathbb{Z}_{\geqslant 1}$, satisfying the following two conditions:

(C.1) if $a, b \in A$, and $a < b$ then $\rho(a) \leqslant b$,
(C.2) one has that $A - \rho(A) \subseteq T_\rho$ (resp. $A - \rho(A) \subseteq T_\rho^* = T_\rho \cup \{e^*\}$).

Write $\text{Jump}_\rho = \{\text{jump sets for } \rho\}$ (resp. $\text{Jump}_\rho^* = \{\text{extended jump sets for } \rho\}$). The jump set A can be reconstructed from the following data.

(*a*) $I_A = A - \rho(A)$.
(*b*) The function $\beta_A : A - \rho(A) \to \mathbb{Z}_{\geqslant 1}$, $i \to |[i, \infty) \cap A|$.

The pair (I_A, β_A) satisfies the following three conditions.

$(C.1)'$ One has that $I_A \subseteq T_\rho$ (resp. $I_A \subseteq T_\rho^*$),
$(C.2)'$ the map β_A is a strictly decreasing map $\beta : I_A \to \mathbb{Z}_{\geqslant 1}$,
$(C.3)'$ the map $i \mapsto \rho^{\beta(i)}(i)$ from I_A to $\mathbb{Z}_{\geqslant 1}$ is strictly increasing.

Conversely, given any pair (I, β) satisfying properties $(C.1)', (C.2)'$ and $(C.3)'$, we can attach to it a jump set for ρ denoted by $A_{(I,\beta)}$ (resp. an extended jump set for ρ). The assignments $A \mapsto (I_A, \beta_A)$ and $(I, \beta) \mapsto A_{(I,\beta)}$ are inverses to each other. Namely we have

$$A_{(I_A, \beta_A)} = A,$$

and

$$(I_{A_{(I,\beta)}}, \beta_{A_{(I,\beta)}}) = (I, \beta).$$

We will refer also to the pair (I, β) as a jump set.

1.2.1. *Answer to question* (1). We will answer question (1) exploiting the following analogy with usual $\mathbb{Z}_p$-modules. We denote by $\mu_p(K) := \{\alpha \in K : \alpha^p = 1\}$. It is not difficult to show that $\mu_p(K) = \{1\}$ if and only if

$$U_1(K) \simeq_{\mathbb{Z}_p\text{-mod}} \prod_{i \in T_{\rho_K}} \mathbb{Z}_p^{f_K}.$$

Suppose that $\mu_p(K) \neq \{1\}$. Then $U_1(K)$ has a presentation:

$$0 \to \mathbb{Z}_p \to \mathbb{Z}_p^{[K:\mathbb{Q}_p]+1} \to U_1(K) \to 0.$$

Denote by v_0 the image of 1 in the inclusion of $\mathbb{Z}_p$ into $\mathbb{Z}_p^{[K:\mathbb{Q}_p]+1}$. One can obtain a different presentation using the natural action of $\mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{Z}_p^{[K:\mathbb{Q}_p]+1})$ on $\mathrm{Epi}_{\mathbb{Z}_p}(\mathbb{Z}_p^{[K:\mathbb{Q}_p]+1}, U_1(K))$, which denotes the set of surjective morphisms of $\mathbb{Z}_p$-modules from $\mathbb{Z}_p^{[K:\mathbb{Q}_p]+1}$ to $U_1(K)$. In this way all presentations are obtained. That is, $\mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{Z}_p^{[K:\mathbb{Q}_p]+1})$ acts transitively on $\mathrm{Epi}_{\mathbb{Z}_p}(\mathbb{Z}_p^{[K:\mathbb{Q}_p]+1}, U_1(K))$. Thus knowing $U_1(K)$ as a $\mathbb{Z}_p$-module is tantamount to knowing the orbit of the vector v_0 under the action of $\mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{Z}_p^{[K:\mathbb{Q}_p]+1})$. But recall that for all $v_1, v_2 \in \mathbb{Z}_p^{[K:\mathbb{Q}_p]+1}$ one has that

$$v_1 \sim_{\mathrm{Aut}_{\mathbb{Z}_p}} v_2 \leftrightarrow \mathrm{ord}(v_1) = \mathrm{ord}(v_2).$$

Here ord of a vector $v \in \mathbb{Z}_p^{[K:\mathbb{Q}_p]+1}$ denotes the minimum of $\mathrm{v}_{\mathbb{Q}_p}(a)$ as a varies among the coordinates of v with respect to the standard basis of $\mathbb{Z}_p^{[K:\mathbb{Q}_p]+1}$. Therefore we have that

$$\{v : \mathbb{Z}_p^{[K:\mathbb{Q}_p]+1}/\mathbb{Z}_p v \simeq U_1(K)\} = \{v : |\mu_{p^\infty}(K)| = p^{\mathrm{ord}(v)}\}.$$

We will see that in the finer category of filtered $\mathbb{Z}_p$-modules the story is very similar. To reach an analogous picture we need to introduce the analogues of the actors appearing above. Namely we need a notion of a "*free-filtered-module*".

As we shall explain in section 3.2.1, with filtered modules one can do the usual operations of direct sums, direct product, and when the modules are finitely generated of taking quotients. Having this in mind, one defines what may be thought of as the building blocks for "free-filtered-modules", namely the analogue of rank 1 modules over $\mathbb{Z}_p$ (but now there will be many different rank 1 filtered modules), as follows. Let ρ be a shift, and let i be a positive integer.

Definition 1.1. The i-th standard filtered module, S_i, for ρ, is given by setting $S_i = \mathbb{Z}_p$, with weight map

$$w(x) = \rho^{\mathrm{ord}_p(x)}(i).$$

The analogues of a "free-filtered-module" used to describe $U_1(K)$ will be

$$M_\rho = \prod_{i \in T_\rho} S_i,$$

$$M_\rho^* = \prod_{i \in T_\rho^*} S_i.$$

We have the following theorem.

Theorem 1.2. *Let K be a local field, with $|O/m| = p^{f_K}$. Then $U_1 \simeq M_{\rho_K}^{f_K}$ as filtered $\mathbb{Z}_p$-modules if and only if $\mu_p(K) = \{1\}$.*

So we are left with the case $\mu_p(K) \neq \{1\}$. In particular we have that $\mathrm{char}(K) = 0$. We proceed in analogy with the case of $\mathbb{Z}_p$-modules described above.

To describe $U_\bullet$ as a *filtered* $\mathbb{Z}_p$-module one *constructs* a filtered presentation:

$$M_{\rho_K}^{f_K - 1} \oplus M_{\rho_K}^* \twoheadrightarrow U_\bullet(K).$$

Just as with $\mathbb{Z}_p$-modules, one can obtain a different presentation using the natural action of $\mathrm{Aut}_{\mathrm{filt}}(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*)$ on $\mathrm{Epi}_{\mathrm{filt}}(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*, U_\bullet(K))$. As established in Proposition 3.32 we obtain a statement in perfect analogy with the case of $\mathbb{Z}_p$-modules explained above. Namely we have the following crucial proposition.

Proposition 1.3. *Let K be a local field with $\mu_p(K) \neq \{1\}$. Then the action of* $\mathrm{Aut}_{\mathrm{filt}}(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*)$ *upon the set* $\mathrm{Epi}_{\mathrm{filt}}(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*, U_\bullet(K))$ *is transitive.*

For a local field K as in Proposition 1.3 knowing the filtered module $U_\bullet(K)$ is tantamount to knowing the set of vectors $v \in M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*$ such that

$$(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*)/\mathbb{Z}_p v \simeq_{\mathrm{filt}} U_\bullet(K).$$

Thanks to Proposition 1.3 the set of such vectors v consists of a single orbit under the action of the group $\mathrm{Aut}_{\mathrm{filt}}(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*)$. Thus we are led to study the orbits of $\mathrm{Aut}_{\mathrm{filt}}(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*)$ acting on $M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*$, just as we did above in the case of $\mathbb{Z}_p$-modules. In particular we are led to find the filtered analogue of the function ord. It is in this context that jump sets come into play. For two vectors $v_1, v_2 \in M_\rho^{f-1} \oplus M_\rho^*$ we will use the notation

$$v_1 \sim_{\mathrm{Aut}_{\mathrm{filt}}} v_2$$

to say that v_1 and v_2 are in the same orbit under the action of $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M_\rho^*)$. Observe that if $\varphi \in \mathrm{Epi}_{\mathrm{filt}}(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*, U_\bullet(K))$, then in particular $\ker(\varphi) \subseteq p \cdot (M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*)$. Therefore we proceed to describe only orbits of $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M_\rho^*)$ acting upon $p \cdot (M_\rho^{f-1} \oplus$

M_ρ^*). However there is no loss of generality in doing so. Indeed it is clear that given v_1, v_2 in $M_\rho^{f-1} \oplus M_\rho^*$ one has that $v_1 \sim_{\mathrm{Aut_{filt}}} v_2$ if and only if $p \cdot v_1 \sim_{\mathrm{Aut_{filt}}} p \cdot v_2$. We attach to each extended jump set (I, β) a vector in $p \cdot (M_\rho^{f-1} \oplus M_\rho^*)$ defined as follows:

$$v_{(I,\beta)} = (x_j)_{j \in T_\rho^*} \in p \cdot M_\rho^* = \prod_{j \in T_\rho^*} p \cdot S_j$$

$$\text{by } x_j = 0 \text{ if } j \notin I, \ x_j = p^{\beta(j)} \text{ if } j \in I.$$

Theorem 1.4. *(*Jump sets parametrize orbits*) Let ρ be any shift with $\#T_\rho < \infty$ and f be a positive integer. Then there exists a unique map*

$$\text{filt-ord} : p \cdot (M_\rho^{f-1} \oplus M_\rho^*) \to \mathrm{Jump}_\rho^*$$

having the following two properties.
(1) *For all $v_1, v_2 \in p \cdot (M_\rho^{f-1} \oplus M_\rho^*)$ one has*

$$v_1 \sim_{\mathrm{Aut_{filt}}} v_2 \leftrightarrow \text{filt-ord}(v_1) = \text{filt-ord}(v_2).$$

(2) *For each $(I, \beta) \in \mathrm{Jump}_\rho^*$, we have that*

$$\text{filt-ord}(v_{(I,\beta)}) = (I, \beta).$$

In fact the proof of Theorem 1.4, as given in Section 3, provides us with an effective way to *compute* the map filt-ord. This goes as follows. Let v be in $p \cdot (M_\rho^{f-1} \oplus M_\rho^*)$. Firstly define the following subset of $\mathbb{Z}^2_{\geqslant 1}$

$$S_v := \{(i, \mathrm{ord}(v_i))\}_{i \in T_\rho^* : v_i \neq 0},$$

where v_i is the projection of v on the factor S_i^f if $i < e_\rho^*$ and on $S_{e_\rho^*}$ in case $i = e_\rho^*$. Next, for any shift ρ consider the following partial order $\leqslant_\rho$ defined on $\mathbb{Z}^2_{\geqslant 1}$. We let $(a_1, b_1) \leqslant_\rho (a_2, b_2)$ if and only if

$$b_2 \geqslant b_1 \text{ and } \rho^{b_2}(a_2) \geqslant \rho^{b_1}(a_1).$$

Finally define S_v^- to be the set of minimal points of S_v with respect to $\leqslant_\rho$. One can easily show that there is a unique extended jump set $(I_v, \beta_v) \in \mathrm{Jump}_\rho^*$ such that

$$S_v^- = \mathrm{Graph}(\beta_v).$$

It is shown in Section 3 that $\text{filt-ord}(v) = (I_v, \beta_v)$. This phenomenon of a jump set arising as the set of minimal or maximal elements of some finite subset of $\mathbb{Z}^2_{\geqslant 1}$ is a leitmotif of this paper. Another instance of this phenomenon will emerge at the end of this sub-section in Theorem 1.13, in the context of Eisenstein polynomials. We mention that this way of computing filt-ord is used in [1] where, among other things, algorithmic problems of this subject are explored.

From Theorem 1.4 one concludes the following.

Theorem 1.5. *Let K be a local field, with $\mu_p(K) \neq \{1\}$ and $|O/m| = p^{f_K}$. Then there is a* unique $(I_K, \beta_K) \in \mathrm{Jump}_{\rho_K}^*$ *such that*

$$U_1(K) \simeq M_{\rho_K}^{f_K - 1} \oplus (M_{\rho_K}^* / \mathbb{Z}_p v_{(I_K, \beta_K)})$$

as filtered $\mathbb{Z}_p$-modules.

So when $\mu_p(K) \neq \{1\}$, knowing $U_1(K)$ as a filtered module is tantamount to knowing the extended ρ_K-jump set (I_K, β_K).

The next theorem tells us, for given e, f, which orbits of the action of $\mathrm{Aut}_{\mathrm{filt}}(M_{\rho_{e,p}}^{f-1} \oplus M_{\rho_{e,p}}^*)$ on $M_{\rho_{e,p}}^{f-1} \oplus M_{\rho_{e,p}}^*$ are realized by a local field K with $\mu_p(K) \neq \{1\}$, $e_K = e$ and $f_K = f$. In other words, together with Theorem 1.2 this provides a complete classification of the filtered $\mathbb{Z}_p$-modules $M_\bullet$ such that

$$U_\bullet(K) \simeq_{\mathrm{filt}} M_\bullet,$$

for some local field K, therefore answering Question (1).

Theorem 1.6. *Let p be a prime number, let $e, f \in \mathbb{Z}_{>0}$, and let (I, β) be an extended $\rho_{e,p}$-jump set. Then the following are equivalent.*
(1) There exists a local field K with residue characteristic p and

$$\mu_p(K) \neq \{1\},\ f_K = f,\ e = \mathrm{v}_K(p),\ (I_K, \beta_K) = (I, \beta).$$

(2) We have that $p-1|e$, $I \neq \varnothing$ and

$$\rho_{e,p}^{\beta(\min(I))}(\min(I)) = \frac{pe}{p-1}\ (= e^*).$$

For a shift ρ such that T_ρ is finite, the extended jump sets $(I, \beta) \in \mathrm{Jump}_\rho^*$ such that $I \neq \varnothing$ and $\rho^{\beta(\min(I))}(\min(I)) = e^*$ are said to be *admissible*. The implication (2) $\to$ (1), in the above theorem, is proved in Section 5 in Theorem 5.4. The implication (1) $\to$ (2) follows from Proposition 5.1 and Theorem 3.38 combined.

Our next main result provides a quantitative strengthening of Theorem 1.6. Once we fix $e \in (p-1)\mathbb{Z}_{\geqslant 1}$ and a positive integer f, then, thanks to Theorem 1.6, we know precisely which $(I, \beta) \in \mathrm{Jump}_{\rho_{e,p}}^*$ occur as (I_K, β_K) for some local field K with $\mu_p(K) \neq \{1\}, e_K = e, f_K = f$. But Theorem 1.6 doesn't tell us "*how often*" each (I, β) occurs. To make this point precise we should firstly agree in which manner we *weight* local fields. A very natural way to do this is provided by Serre's Mass formula [10]. We briefly recall how this works.

Let E be a local field. Write $q = |O_E/m_E|$. Let e be a positive integer. Let $S(e, E)$ be the set of isomorphism classes of separable totally ramified degree e extensions K/E. To $K \in S(e, E)$ one gives mass $\mu_{e,E}(K) := \frac{1}{q^{c(K/E)}|\mathrm{Aut}_E(K)|}$, where $c(K/E) = \mathrm{v}_K(\delta_{K/E}) - e + 1$, and $\delta_{K/E}$ denotes the different of the extension K/E. Serre's Mass formula [10] states that $\mu_{e,E}$ is a probability measure on $S(e, E)$, i.e.

$$\sum_{K \in S(e,E)} \mu_{e,E}(K) = 1.$$

Now we can make the "*how often*" written above precise. Namely given $e \in (p-1)\mathbb{Z}_{\geqslant 1}, f \in \mathbb{Z}_{\geqslant 1}$ and $(I, \beta) \in \mathrm{Jump}_\rho^*$, write $E_f := \mathbb{Q}_{p^f}(\zeta_p)$. Here $\mathbb{Q}_{p^f}$ denotes the degree f unramified extension of $\mathbb{Q}_p$. We can ask to evaluate

$$\sum_{K \in S(\frac{e}{p-1}, E_f) : (I_K, \beta_K) = (I, \beta)} \mu_{\frac{e}{p-1}, E_f}(K),$$

in words we are asking to evaluate the probability that a random K, totally ramified degree $\frac{e}{p-1}$ extension of E_f, has $(I_K, \beta_K) = (I, \beta)$.

Observe that, thanks to Proposition 1.3 and Theorems 1.4 and 1.5 combined, we know that for $K \in S(\frac{e}{p-1}, E_f)$ the set of vectors $O := \{v \in M_{\rho_K}^{f_K - 1} \oplus M_{\rho_K}^* : U_\bullet(K) \simeq_{\mathrm{filt}} (M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*)/\mathbb{Z}_p v\}$ is precisely equal to the orbit of the vector $v_{(I_K, \beta_K)}$ under $\mathrm{Aut}_{\mathrm{filt}}(M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*)$.

Moreover $M_{\rho_K}^{f_K-1} \oplus M_{\rho_K}^*$ viewed as a topological group is compact, and hence has a Haar measure. It is then natural to think that, for a given admissible extended $\rho_{e,p}$-jump set (I,β), a randomly chosen totally ramified degree $\frac{e}{p-1}$ extension K of E_f, satisfies

$$(I_K,\beta_K)=(I,\beta)$$

with probability *proportional* to the Haar measure of the orbit of $v_{(I,\beta)}$. Our next theorem shows that this turns out to be exactly right.

For $(I,\beta)\in \mathrm{Jump}^*_{\rho_{e,p}}$, with $I\neq\varnothing$, it is easy to see that the set filt-ord$^{-1}((I,\beta))$ is an open subset of $M_{\rho_{e,p}}^{f-1}\oplus M_{\rho_{e,p}}^*$. Normalize μ_{Haar}, imposing that

$$\mu_{\mathrm{Haar}}\Big(\bigcup_{(I,\beta)\ \text{admissible}} \text{filt-ord}^{-1}(I,\beta)\Big)=1.$$

In other words, choose the unique normalization of the Haar measure that induces a probability measure on the union of the orbits of the vectors $v_{(I,\beta)}$ as (I,β) runs among admissible extended jump sets for $\rho_{e,p}$. We call admissible those orbits of $M_{\rho_{e,p}}^{f-1}\oplus M_{\rho_{e,p}}^*$, under the action of $\mathrm{Aut}_{\mathrm{filt}}(M_{\rho_{e,p}}^{f-1}\oplus M_{\rho_{e,p}}^*)$, that contain a vector $v_{(I,\beta)}$ with (I,β) admissible. Let E_f be $\mathbb{Q}_{p^f}(\zeta_p)$, the unramified extension of $\mathbb{Q}_p(\zeta_p)$ of degree f.

Theorem 1.7. *Let $e\in(p-1)\mathbb{Z}_{\geqslant 1}$, $f\in\mathbb{Z}_{\geqslant 1}$ and $(I,\beta)\in\mathrm{Jump}^*_{\rho_{e,p}}$ be an admissible jump set. Then the probability that a random totally ramified degree $\frac{e}{p-1}$ extension K of E_f satisfies $(I_K,\beta_K)=(I,\beta)$, is equal to the probability that a vector $v\in M_{\rho_{e,p}}^{f-1}\oplus M_{\rho_{e,p}}^*$, randomly chosen among admissible orbits, is in the orbit of $v_{(I,\beta)}$. In other words*

$$\sum_{K\in S(\frac{e}{p-1},E_f):(I_K,\beta_K)=(I,\beta)} \mu_{\frac{e}{p-1},E_f}(K)=\mu_{\mathrm{Haar}}(\text{filt-ord}^{-1}(I,\beta)).$$

From the first proof given by Serre [10], Theorem 1.7 can be equivalently expressed as a volume computation in a space of Eisenstein polynomials. Namely for $e\in(p-1)\mathbb{Z}_{\geqslant 1}$ and $f\in\mathbb{Z}_{\geqslant 1}$, denote by $\mathrm{Eis}(\frac{e}{p-1},\mathbb{Q}_{p^f}(\zeta_p))$ the set of degree $\frac{e}{p-1}$-Eisenstein polynomials over $\mathbb{Q}_{p^f}(\zeta_p)$. This can be viewed as a topological space equipped with a natural probability measure, simply by using the Haar measure on the coefficients. For a $g(x)\in\mathrm{Eis}(\frac{e}{p-1},\mathbb{Q}_{p^f}(\zeta_p))$, denote by $F_{g(x)}:=\mathbb{Q}_{p^f}(\zeta_p)[x]/(g(x))$. We can reformulate Theorem 1.7 in the following manner.

Theorem 1.8. *Let $e\in(p-1)\mathbb{Z}_{\geqslant 1}$, $f\in\mathbb{Z}_{\geqslant 1}$ and $(I,\beta)\in\mathrm{Jump}^*_{\rho_{e,p}}$ be an admissible jump set. Then the volume of the set of $g(x)\in\mathrm{Eis}(\frac{e}{p-1},\mathbb{Q}_{p^f}(\zeta_p))$ satisfying $(I_{F_{g(x)}},\beta_{F_{g(x)}})=(I,\beta)$, equals*

$$\mu_{\mathrm{Haar}}(\text{filt-ord}^{-1}(I,\beta)).$$

The above two Theorems are implied by Theorem 9.1. As a bonus, the method of the proof of Theorem 9.1 allows us to *explicitly compute* the jump set $(I_{F_{g(x)}},\beta_{F_{g(x)}})$ out of the valuation of the coefficients of $g(x)$, for a large class of Eisenstein polynomials $g(x)$. This will be the class of *strongly separable Eisenstein polynomials*, which are defined right after Proposition 1.10. To state our next Theorem, we begin attaching to any $g(x)\in\mathrm{Eis}(\frac{e}{p-1},\mathbb{Q}_{p^f}(\zeta_p))$, an element $(I_{g(x)},\beta_{g(x)})\in\mathrm{Jump}_{\rho_{\infty,p}}$. Under certain conditions, given below, we have that actually $(I_{g(x)},\beta_{g(x)})\in\mathrm{Jump}^*_{\rho_{e,p}}$ and $(I_{F_{g(x)}},\beta_{F_{g(x)}})=(I_{g(x)},\beta_{g(x)})$. We shall begin by explaining the

construction of $(I_{g(x)}, \beta_{g(x)})$. Write

$$g(x) := \sum_{i=0}^{\frac{e}{p-1}} a_i x^i.$$

Firstly consider the following subset of $\mathbb{Z}^2$

$$S_{g(x)} := \{\big(\frac{\mathrm{v}_{E_f}(a_i)\frac{e}{p-1} + i}{p^{\mathrm{v}_{\mathbb{Q}_p}(i)}}, \mathrm{v}_{\mathbb{Q}_p}(i) + 1\big)\}_{1 \leqslant i \leqslant \frac{e}{p-1} : \mathrm{v}_{\mathbb{Q}_p}(i) \leqslant \mathrm{v}_{\mathbb{Q}_p}(e) \text{ and } a_i \neq 0}.$$

Recall the definition of the partial order $\leqslant_\rho$ attached to a shift ρ given right after Theorem 1.4. We denote by $S^-_{g(x)}$ the set of *minimal* elements of $S_{g(x)}$ with respect to the order $\leqslant_{\rho_{\infty,p}}$. One can prove that there is a unique pair

$$(I_{g(x)}, \beta_{g(x)}) \in \mathrm{Jump}_{\rho_{\infty,p}},$$

such that $S^-_{g(x)} = \mathrm{Graph}(\beta_{g(x)})$. It turns out that if $g(x)$ is strongly separable, a notion that we are going to provide right after Proposition 1.10, then the pair $(I_{g(x)}, \beta_{g(x)})$ is also in $\mathrm{Jump}_{\rho_{e,p}}$.

We next make a definition that will have the effect of sub-dividing the characteristic 0 local field extensions into two sub-categories. Loosely speaking, when the ramification of E/F will not be "too big" compared to $\mathrm{v}_E(p)$, then the arithmetic of this extension will be, for our purposes, indistinguishable from the arithmetic of a characteristic p extension. We make this notion precise in the following definition, while the relation with characteristic p fields will only become visible in Theorem 1.14. For an extension of local fields F/E we denote by $\delta_{F/E}$ the different of the extension.

Definition 1.9. Let F/E be any extension of local fields of residue characteristic p. We say that F/E is *strongly separable* if

$$\mathrm{v}_F(\delta_{F/E}) < \mathrm{v}_F(p).$$

Observe that in characteristic p the notions of strongly separable and separable coincide. One can easily show the following general fact.

Proposition 1.10. *Let n be a positive integer. Consider F/E a monogenic degree n extension given by an Eisenstein polynomial $g(x) := \sum_{i=0}^n a_i x^i$. Then F/E is strongly separable if and only if there exists $i \in \{1, \ldots, n\}$ such that $(i, p) = 1$ and $\mathrm{v}_E(a_i) < \mathrm{v}_E(p)$.*

An Eisenstein polynomial $g(x) \in \mathrm{Eis}(n, E)$ giving rise to a strongly separable extension is itself called strongly separable. So Proposition 1.10 says that $g(x)$ is strongly separable if and only if it has a coefficient a_i with $(i, p) = 1$ and $\mathrm{v}_E(a_i) < \mathrm{v}_E(p)$. We can now state our next result. For a positive integer f, recall that E_f denotes $\mathbb{Q}_{p^f}(\zeta_p)$, the unramified extension of $\mathbb{Q}_p(\zeta_p)$ of degree f.

Theorem 1.11. *Let $e \in (p-1)\mathbb{Z}_{\geqslant 1}$, $f \in \mathbb{Z}_{\geqslant 1}$ and $g(x) \in \mathrm{Eis}(\frac{e}{p-1}, E_f)$ be strongly separable. Then*

$$(I_{g(x)}, \beta_{g(x)}) = (I_{E_f[x]/g(x)}, \beta_{E_f[x]/g(x)}).$$

As explained at the end of Section 10, the assumption of being strongly separable cannot be omitted. Theorem 1.11 is deduced in Section 10 from a slightly finer result. Moreover in that Section we provide a *procedure* that allows one to compute $(I_{g(x)}, \beta_{g(x)})$ very quickly, even by hand. See [1] for an actual implementation of this as well.

The moral of Theorem 1.11 is that in a portion of the space of Eisenstein polynomials, the assignment $K \mapsto (I_K, \beta_K)$ can be read off very explicitly from the valuations of the coefficients of an Eisenstein polynomial giving the field K. In general this is not the case, but nevertheless one is able to establish the exact counting formula as in Theorem 1.7 by means of a genuinely probabilistic argument.

1.2.2. *Answer to question* (2). Let n be a positive integer and let L/K be a degree n totally ramified separable extension of local fields with residue characteristic p. Suppose L/K is given by $g(x) \in \mathrm{Eis}(n, K)$, i.e. $L = K[x]/g(x)$. Denote by Γ_L the metric space introduced in 1.1.2. One can find invariants of $g(x)$ from the structure of the metric space Γ_L as follows. Fix $\pi \in K^{\mathrm{sep}}$ a root of $g(x)$. Denote by $\sigma_\pi \in \Gamma_L$ the corresponding embedding

$$\sigma_\pi(x) = \pi.$$

Consider the polynomial

$$g_{\mathrm{twist}}(t) = g(\pi \cdot t + \pi) \in K[\pi][t].$$

The knowledge of the Newton polygon of $g_{\mathrm{twist}}(t)$ tells us precisely how the distances are disposed around σ_π in Γ_L. But recall that Γ_L is a transitive G_K-set, and every element of G_K acts as an isometry on Γ_L. Hence the Newton polygon of $g_{\mathrm{twist}}(\pi \cdot x + \pi)$ is an invariant of the metric space Γ_L independent of the choice of π and of g. Denote this polygon by

$$\mathrm{Newt}(L/K).$$

Observe that in case L/K is Galois, then the knowledge of $\mathrm{Newt}(L/K)$ amounts to the knowledge of the map $\mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$

$$u \mapsto |\mathrm{Gal}(L/K)_u|, \ (u \in \mathbb{Z}_{>0})$$

where $\mathrm{Gal}(L/K)_u$ denotes the lower u-th ramification group as defined in [9]. But $\mathrm{Newt}(L/K)$ makes sense also for non-Galois extensions.

This Newton polygon is called the *ramification polygon* in the literature, and, among other things, a complete survey on this subject can be found in [13]. In that paper the polynomial in consideration is instead $\frac{g(\pi t + \pi)}{\pi^n}$. Of course this has simply the effect of shifting the polygon vertically by $-n$. As it will become clear to the reader in a moment, we have chosen our normalization since the form of our results is slightly more pleasant with our convention.

The following fact, certainly folklore, can be shown by direct inspection. We refer the reader to Section 10 for how to calculate in practice $(I_{g(x)}, \beta_{g(x)})$: this together with the basic properties of $\mathrm{Newt}(L/K)$, which can be found in [13], gives the following fact quite rapidly.

Theorem 1.12. *Let n be a positive integer and let K be a local field with residue characteristic p. Let $g(x) \in \mathrm{Eis}(n, K)$ be a strongly separable polynomial. Then*

$$\text{Lower-Convex-Hull}(\{(p^{\beta_{g(x)}(i)-1}, p^{\beta_{g(x)}(i)-1} i) : i \in I_{g(x)}\} \cup \{(n, n)\}) = \mathrm{Newt}(K[x]/g(x)/K).$$

In other words Theorem 1.12 gives us a way to read off $\mathrm{Newt}(K[x]/g(x)/K)$ from $(I_{g(x)}, \beta_{g(x)})$, in case $g(x)$ is strongly separable. Hence combined with Theorem 1.11 we obtain the following surprising result.

Theorem 1.13. *Let $L/\mathbb{Q}_{p^f}(\zeta_p)$ be a strongly separable totally ramified extension. Then*

$$\text{Lower-Convex-Hull}(\{(p^{\beta_L(i)-1}, p^{\beta_L(i)-1} i) : i \in I_L\} \cup \{(n, n)\}) = \mathrm{Newt}(L/\mathbb{Q}_{p^f}(\zeta_p)).$$

Hence for a strongly separable extension $L/\mathbb{Q}_{p^f}(\zeta_p)$ the knowledge of the filtered $\mathbb{Z}_p$-module $U_\bullet(L)$ implies the knowledge of the ramification polygon $\mathrm{Newt}(L/\mathbb{Q}_{p^f}(\zeta_p))$. Moreover we see something else going on: for such an extension the full object $(I_{g(x)}, \beta_{g(x)})$ is an invariant of the extension. This indeed follows from Theorem 1.11: that Theorem is telling us that the object $(I_{g(x)}, \beta_{g(x)})$ encodes the structure of $U_\bullet(\mathbb{Q}_{p^f}(\zeta_p)[x]/g(x))$ as a filtered $\mathbb{Z}_p$-module. But in the more general case of Theorem 1.12 we see a priori only a way to *deduce* an invariant from $(I_{g(x)}, \beta_{g(x)})$, without any structural information provided for $(I_{g(x)}, \beta_{g(x)})$ itself. In particular it gives us no a priori guarantees that $(I_{g(x)}, \beta_{g(x)})$ is the same as $g(x)$ varies among polynomials representing the same field. In Section 11 we pinpoint this additional structural information. Namely to *any* strongly separable extension L/K of local fields, we will attach $(I_{L/K}, \beta_{L/K})$, a $\rho_{\infty,p}$-jump set that encodes structural information about the filtered inclusion

$$U_\bullet(K) \subseteq U_\bullet(L).$$

In particular, if $\mu_p(L) = \{1\}$ then $(I_{L/K}, \beta_{L/K})$ has the following simple interpretation. In this case one can attach, essentially by means of Theorem 1.4, to any element u of $U_1(K) - U_2(K)$ a $\rho_{e_L,p}$-jump set $(I_{L/K}(u), \beta_{L/K}(u))$. The jump set $(I_{L/K}(u), \beta_{L/K}(u))$ tells us the orbit of u under the action of $\mathrm{Aut}_{\mathrm{filt}}(U_\bullet(L))$. Let u be any element of $U_1(K) - U_2(K)$ and let $g(x)$ be any Eisenstein polynomial giving L/K^{nr}, where K^{nr} is the maximal unramified extension of K in L. It turns out that $(I_{L/K}(u), \beta_{L/K}(u)) = (I_{g(x)}, \beta_{g(x)})$. In particular all the elements of $U_1(K) - U_2(K)$ are in the same orbit for the action of $\mathrm{Aut}_{\mathrm{filt}}(U_\bullet(L))$. This orbits correspond to a single jump set $(I_{L/K}, \beta_{L/K})$.

For general strongly separable extensions of local fields we have the following joint generalization of Theorem 1.11 and Theorem 1.13.

Theorem 1.14. *Let L/K be a strongly separable totally ramified extension of local fields of residue characteristic p. Then*

$$\text{Lower-Convex-Hull}(\{(p^{\beta_{L/K}(i)-1}, p^{\beta_{L/K}(i)-1} i) : i \in I_{L/K}\} \cup \{(n,n)\}) = \mathrm{Newt}(L/K).$$

Moreover if L/K is given by an Eisenstein polynomial $g(x)$, then

$$(I_{L/K}, \beta_{L/K}) = (I_{g(x)}, \beta_{g(x)}).$$

Therefore Theorem 1.14 provides an intrinsic description of $(I_{g(x)}, \beta_{g(x)})$ as a filtered invariant of the corresponding inclusion of groups of principal units. In particular this says that $(I_{g(x)}, \beta_{g(x)})$ is an invariant of the Eisenstein polynomial $g(x)$ as long as $g(x)$ is strongly separable.

1.2.3. *Answer to question (3).* Denote by $\mathscr{J}_K$ the set of possible sets of jump for a character of $U_1(K)$. Clearly $\mathscr{J}_K$ is determined by the structure of $U_1(K)$ as a filtered $\mathbb{Z}_p$-module. So one can use the answer to question (1) in order to answer question (3). The first step is answering the same problem for free filtered modules. The main idea for doing this is again to exploit the action of the group of filtered automorphisms. Denote by $\widehat{M_\rho^f}$ the group of characters of M_ρ^f. There is a natural action of $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^f)$ on $\widehat{M_\rho^f}$. The action clearly preserves the set of jumps of each character. It turns out that conversely one can reconstruct the orbit of the character from the set of jumps: two characters in $\widehat{M_\rho^f}$ are in the same orbit under the action of $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^f)$ if and only if they have the same set of jumps. Moreover the possible sets of jumps are exactly the ρ-jump sets. This fact is expressed in the following theorem.

Theorem 1.15. *(*Jump sets parametrize orbits of characters*) Let ρ be a shift, and f be a positive integer. Then the set of possible sets of jumps of characters of the free-filtered $\mathbb{Z}_p$-module M_ρ^f is exactly* Jump_ρ*. Moreover two characters have the same set of jumps if and only if they are in the same orbit under the group* $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^f)$.

So in particular we have the following result.

Theorem 1.16. *Let K be a local field with $\mu_p(K) = \{1\}$, then $\mathscr{J}_K = \mathrm{Jump}_{\rho_K}$.*

We now consider the case $\mu_p(K) \neq \{1\}$. By Theorem 1.5, we first look at the possible sets of jumps of characters of $M_\rho^{f-1} \oplus M_\rho^*$. These are precisely the extended jump sets, as we next explain.

Theorem 1.17. *(*Jump sets parametrize orbits of characters—part 2*) Let ρ be a shift with $\#T_\rho < \infty$. Let f be a positive integer. Then the set of possible sets of jumps of characters of the free-filtered $\mathbb{Z}_p$-module $M_\rho^{f-1} \oplus M_\rho^*$ is exactly* Jump_ρ^**. Moreover two characters have the same set of jumps if and only if they are in the same orbit under the group* $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M_\rho^*)$.

We then show that this, essentially thanks to Proposition 3.11, implies that $\mathscr{J}_K \subseteq \mathrm{Jump}_{\rho_K}^*$ always, i.e. a set of jumps for a character is always an extended ρ_K-jump set. The remaining task is to classify which orbits of characters of $M_\rho^{f-1} \oplus M_\rho^*$ admit a representative killing a given element of $M_\rho^{f-1} \oplus M_\rho^*$. In this way we obtain the final classification, which is Theorem 6.2. This Theorem says that $\mathscr{J}_K$ consists of the elements of $\mathrm{Jump}_{\rho_K}^*$ that are (I_K, β_K, f_K, p)-*compatible*. Compatibility is an explicit combinatorial criterion that consists in a comparison between a jump set (I, β) and the jump set of the field (I_K, β_K): in the comparison an important role is played by the case distinction of whether $f_K \geqslant 2$ or not and whether $p = 2$ or not. For a precise definition see Definition 6.1. In the rest of Section 6 we establish several explicit applications of this criterion, stressing especially the first dichotomy. As an example we give here the following result.

Theorem 1.18. *Let K_1, K_2 be two totally ramified extensions of $\mathbb{Q}_p(\zeta_p)$. Then $\mathscr{J}_{K_1} = \mathscr{J}_{K_2}$ if and only if $U_\bullet(K_1) \simeq_{\mathbb{Z}_p\text{-filt}} U_\bullet(K_2)$.*

In other words, for totally ramified extensions $K/\mathbb{Q}_p(\zeta_p)$, not only do we have an explicit criterion to compute $\mathscr{J}_K$ from the filtered $\mathbb{Z}_p$-module $U_\bullet(K)$, but we can conversely reconstruct the filtered $\mathbb{Z}_p$-module $U_\bullet(K)$ from $\mathscr{J}_K$.

Finally we remark that, by the reciprocity map, this criterion gives an explicit classification of the possible sets of jumps in the upper numbering of a cyclic wild extension of a local field. We explain this in further detail in Section 6.

1.3. **Further results and questions.** We hope to have shed some light on the role that the jump set (I_K, β_K) plays in the arithmetic of the local field K. This makes some basic questions about this invariant worth investigating. A very basic one is the following. Let K be a local field with $\mu_p(K) \neq \{1\}$. Let e be in $e_K\mathbb{Z}_{\geqslant 1}$ and let f be in $f_K\mathbb{Z}_{\geqslant 1}$.

Question: For which $(I, \beta) \in \mathrm{Jump}_{\rho_{e,p}}^*$ does there exist an extension L of K such that $e_L = e, f_L = f$ and $(I_L, \beta_L) = (I, \beta)$?

We have made some progress on this question, see Section 12. In that Section we establish some peculiarly specific rules that constraint the possible changes of a jump set under a

totally ramified extension. As the reader will learn in that section, the interesting case, among totally ramified extensions, is only that of wild extensions. In the present paper we leave open a complete characterization of which jump sets occur under such extensions, providing only necessary conditions. From further calculations, not included in the present paper, we believe that a full classification might be within reach, but the final result might look quite intricate.

In a different direction, we would like to mention that most of the results of the present paper can be viewed as an investigation of the filtered $\mathbb{Z}_p$-modules arising from taking points of one of the simplest formal groups, namely $\mathbb{G}_m$. The theory in Section 3 should be general enough to cover the case of other Lubin-Tate formal groups giving rise to filtered O_K-modules with cyclic torsion sub-module, where K is any other local field, and O_K its ring of integers. It would be an interesting investigation to see which of the results of the present paper extend to this context. For instance, it should be possible to provide a theorem on the lines of Theorem 5.4.

Finally we would like to conclude with yet another potentially worthwhile direction of investigation. Our mass formula, contained in Theorem 1.7, follows the first interpretation of Serre's weight for local fields, namely using volumes of Eisenstein polynomials. But Serre [10] established also a different interpretation of these weights, by means of division algebras. This suggests the possibility of studying the filtered pro-p group $U_\bullet(D)$ of principal units of a central division algebra over a local field, and to study the action of the group $\mathrm{Aut}_{\mathrm{filt}}(U_\bullet(D))$ on the set of maximal abelian filtered $\mathbb{Z}_p$-sub-modules. It would be very elegant to reach in this manner a different proof of Theorem 1.7.

1.4. **Comparison with the literature.** An explicit classification of the possible upper jumps of wild characters of a local field K, i.e. of the set $\mathscr{J}_K$, was given in a series of papers, by respectively Maus, Miki and Sueyoshi [5], [6], [11]. The first author has given the criterion for characteristic p local fields. The full classification was given by Miki, and some of Miki's arguments in [6] were simplified by Suyeoshi in [11], where the reader can find also a neat statement for Miki's criterion. Two points come here in order. The first point is that in [6] and [11] the invariant (I_K, β_K) was already introduced. This is buried in [6, Lemma 17]. In the language of this paper, we can say that (I_K, β_K) was understood as the unique element of $\mathrm{Jump}^*_{\rho_K}$ such that there is an equation of the form $\zeta_p = \prod_{i\in I_K} u_i^{p^{\beta_K(i)-1}}$, where $\mathrm{v}_K(u_i - 1) = i$, and in case $\frac{pe_K}{p-1} \in I_K$, then $u_{\frac{pe_K}{p-1}} \notin K^{*p}$. The uniqueness was proved in an ad hoc manner in the above mentioned [6, Lemma 17]. The present work is the first place in the literature where the *structural meaning* of the invariant (I_K, β_K) is established: it gives, together with f_K and $p := \mathrm{char}(O_K/m_K)$, the structure of $U_\bullet(K)$ as a filtered module. Apart from being conceptually more satisfying, this slightly more abstract approach has two practical advantages. Firstly it leads naturally to all the above mentioned additional results: the interpretation of jump sets in terms of *filtered orbits* of vectors, see Theorem 1.4, leads to the mass formula for unit filtrations, Theorem 1.7, which in turns leads naturally to Theorem 1.13, which links the filtered structure of $U_\bullet(K)$ with ramification theory. To the best of our knowledge all these results are new. Secondly the interpretation of jump sets as parametrizing filtered orbits of characters, see 1.15, makes it an easy job to deduce, from first principles, our classification of the possible sets of jumps for a character, contained in Theorem 6.2. This brings us to the second point. Namely the combinatorial criterion of [6] is not tautologically equal to the one contained in Theorem 6.2. We check, by direct

combinatorial inspection, that they coincide in Proposition 6.7, showing in this way that the tools of this paper give, among other things, a simple unified approach to deduce all the results in [5], [6] and [11], by means of a general theory of filtered modules.

Coming to more recent literature, in 2014, I. del Corso and L. Capuano [2] have obtained a classification of all possible upper jumps in an exponent p extensions of a local field K. It would be interesting to push this further obtaining a classification, for *any* finite abelian p-group A, of the possible structures $A_\bullet$ as *filtered group* on A such that $\mathrm{Epi}_{\mathrm{filt}}(U_\bullet(K), A_\bullet) \neq \varnothing$. For instance, this might be useful in counting the average number of extensions with prescribed ramification data at p, in families of number fields containing ζ_p. For a first work in the direction of such counting with "prescribed ramification", see [12].

Finally we would like to mention that the ramification polygon of an Eisenstein polynomial has been the object of study of several papers [4], [8], [13], especially in relation to the problem of calculating Galois groups of Eisenstein polynomials. In his Ph.D. thesis, D. Romano [8] provided a characterization of *strongly Eisenstein* polynomials in terms of their Galois group. In a sense these are the polynomials with the simplest possible ramification polygon. It is then interesting that strongly Eisenstein polynomials $g(x)$ over $\mathbb{Q}_{p^f}(\zeta_{p^j})$ with $(p,j) \neq (2,1)$ and $\mathrm{v}_{\mathbb{Q}_p}(\deg(g(x))) > j$, can be also characterized in terms of filtered modules, see Theorem 10.3. Under the assumption $(p,j) \neq (2,1)$ and $\mathrm{v}_{\mathbb{Q}_p}(\deg(g(x))) > j$, these polynomials are the ones giving the simplest possible filtered module, which is also the most frequent one, in the sense of Theorem 1.7: it occurs $\frac{p^f-1}{p^f}$ of the times, just as the probability for an Eisenstein polynomial over $\mathbb{Q}_{p^f}(\zeta_{p^j})$ to be strongly Eisenstein. The work of Romano has been substantially refined by S. Pauli and C. Greve [4].

Acknowledgements. This project is part of my Ph.D. work. I would like to warmly thank my Ph.D. advisor, Hendrik Lenstra, for suggesting that I could think about this subject. In particular I would like to thank him for suggesting several of the starting ideas of the project and for frequent insightful feedback on my progress. I would also like to thank him for relevant pointers to the literature on local fields: this considerably enriched the scope of the results of this paper.

Many thanks go to Ted Chinburg and Sebastian Moore, for showing interest in this research, for following its development and for providing several useful suggestions. In particular I would like to thank them for suggesting to seek for an *explicit* relation between the jump set (I_K, β_K) and the set of sets of jumps $\mathscr{J}_K$.

I am thankful to Ilya Nekrasov and Sergey Vostokov for showing interest in these results, asking me for a talk on this subject, where they provided useful feedback.

I would like to thank Tim Dokchitser for suggesting to contact Maurizio Monge.

Many thanks to Maurizio Monge for pointing out the papers [5], [6] and [11], when I announced to him Theorem 6.2. Also I would like to thank him for providing me with some of his notes on these papers.

2. Jump sets

The goal of this section is to define and explain the notion of a jump set, which is the key object of this paper. Jump sets are defined in terms of shifts. A *shift* is a strictly increasing function $\rho : \mathbb{Z}_{\geqslant 1} \to \mathbb{Z}_{\geqslant 1}$, with $\rho(1) > 1$. For a shift ρ, we denote by T_ρ the set $\mathbb{Z}_{\geqslant 1} - \rho(\mathbb{Z}_{\geqslant 1})$. If T_ρ is finite, we denote by e^* the positive integer $\max(T_\rho) + 1$. We denote by e'_ρ the positive

integer $\rho^{-1}(e^*)$. The shifts that will be relevant for local fields are the ones explained in the following.

Example 2.1. For p a prime, and $e \in \mathbb{Z}_{>0} \cup \{\infty\}$ denote $\rho_{e,p}(i) = \min\{i + e, pi\}$. It is a shift. Clearly $T_{\rho_{e,p}}$ is finite iff e is finite. Indeed one has always $e = |T_{\rho_{e,p}}|$. If $e \neq \infty$, then $e^* = \lceil \frac{pe}{p-1} \rceil$. The reason why these shifts will play a role is due to the following property.

Crucial property: let K local field, of residue characteristic p, let $e = \mathrm{v}_K(p)$, then we have that

$$U_i^p \subset U_{\rho(i)},$$

for $\rho = \rho_{e,p}$ $(= \rho_K)$. One can see this by inspection of the valuations in the expansion $(1 + x)^p = 1 + px + \ldots + x^p$.

We now define ρ-jump sets (resp. extended ρ-jump sets).

Definition 2.2. A *jump set* for ρ (resp. an *extended jump* set for ρ) is a finite subset $A \subseteq \mathbb{Z}_{\geqslant 1}$ such that:

- if $a, b \in A$, and $a < b$ then $\rho(a) \leqslant b$,
- $A - \rho(A) \subseteq T_\rho$ (resp. $A - \rho(A) \subseteq T_\rho^* = T_\rho \cup \{e^*\}$).

Write $\mathrm{Jump}_\rho = \{\text{jump sets for } \rho\}$ (resp. $\mathrm{Jump}_\rho^* = \{\text{extended jump sets for } \rho\}$).

A jump set for ρ will also be called ρ-jump set (resp. an extended jump set for ρ will also be called an extended ρ-jump set).

If A is a ρ-jump set (resp. an extended jump set) then we denote by I_A the set $A - \rho(A)$, and by β_A the map $\beta_A : I_A \to \mathbb{Z}_{\geqslant 1}$, $i \to |[i, \infty) \cap A|$. This allows us to express the notion of jump sets in different, but equivalent, terms. Namely the pair (I_A, β_A) evidently has the following three properties.

(1) $I_A \subseteq T_\rho = \mathbb{Z}_{>0} - \rho(\mathbb{Z}_{>0})$ (resp. $I_A \subseteq T_\rho^* = T_\rho \cup \{e^*\}$),
(2) β_A is a strictly decreasing map $\beta : I_A \to \mathbb{Z}_{\geqslant 1}$,
(3) the map $i \mapsto \rho^{\beta(i)}(i)$ from I_A to $\mathbb{Z}_{\geqslant 1}$ is strictly increasing.

Suppose now we have a pair (I, β) with the three above properties $(1), (2), (3)$. We can attach to such an (I, β) an element $A_{(I,\beta)}$ of Jump_ρ (resp. of Jump_ρ^*) defined as follows. If $I = \varnothing$ then $A_{(I,\beta)} = \varnothing$. Suppose now that I is not empty. Then put

$$A_{(I,\beta)} := \{\rho^n(i)\}_{i \in I - \{\max(I)\}, 0 \leqslant n < \beta(i) - \beta(s(i))} \cup \{\rho^n(\max(I))\}_{0 \leqslant n < \beta(\max(I))},$$

where, for $i \in I - \{\max(I)\}$, the element $s(i)$ denotes the successor of i in I. The following proposition follows in a straightforward manner from the definitions.

Proposition 2.3. *The assignments $A \mapsto (I_A, \beta_A)$ and $(I, \beta) \mapsto A_{(I,\beta)}$ are inverse to each other yielding a bijection between* Jump_ρ *(resp.* Jump_ρ^**) and the set of pairs (I, β) having the following properties:*

- *$I \subseteq T_\rho = \mathbb{Z}_{>0} - \rho(\mathbb{Z}_{>0})$ (resp. $I \subseteq T_\rho^* = T_\rho \cup \{e^*\}$),*
- *β is a strictly decreasing map $\beta : I \to \mathbb{Z}_{\geqslant 1}$,*
- *the map $i \mapsto \rho^{\beta(i)}(i)$ from I to $\mathbb{Z}_{\geqslant 1}$ is strictly increasing.*

From now on, we shall often write (I, β) to denote a jump set (resp. an extended jump set), meaning implicitly that we are identifying it with an actual jump set via the above mentioned bijection.

Example 2.4. • There is a unique jump set having $|I| = 0$, namely the empty set $A = \varnothing \in \mathrm{Jump}_\rho$.
• A ρ-jump set (resp. extended ρ-jump set) (I, β) with $|I| = 1$ is given by the choice of an element, a, of T_ρ (resp. T_ρ^*), and of a positive integer $m = \beta(a)$. The actual jump set will then be $\{a, \rho(a), \dots, \rho^{m-1}(a)\}$.
• A ρ-jump set (resp. extended ρ-jump set) (I, β) with $|I| = 2$ is given by the choice of two elements, $a < b$, of T_ρ (resp. T_ρ^*)), and of two positive integers $m_1 = \beta(a) > \beta(b) = m_2$, such that $\rho^{m_1 - m_2}(a) < b$ (or equivalently $\rho^{m_1}(a) < \rho^{m_2}(b)$). The actual jump set will then be $\{a, \rho(a), \dots, \rho^{m_1 - m_2 - 1}(a)\} \cup \{b, \rho(b), \dots, \rho^{m_2 - 1}(b)\}$.

Example 2.5. We now explain a general procedure to inductively construct any jump set A for ρ (resp. extended jump set). As a first step one decides whether $A = \varnothing$ or not. In case $A = \varnothing$ one has obtained a jump set and stops. Suppose instead that one wants to construct a jump set $A \neq \varnothing$. Then pick an $i_1 \in T_\rho$ (resp. in T_ρ^*) and a positive integer n_1. Consider the set

$$A_1 := \{\rho^j(i_1)\}_{0 \leqslant j < n_1}.$$

Now you can stop and have obtained a jump set $A := A_1$. In this case $I = \{i_1\}$ and $\beta(i_1) = n_1$. If you want instead a jump set with $|I| > 1$, then you check whether there is a $y \in T_\rho$ (resp. in T_ρ^*) such that $\rho^{n_1}(i_1) < y$. If such a y doesn't exist, then we set $A := A_1$ and we stop having obtained a jump set (resp. an extended jump set). Otherwise you pick any such y and put $y := i_2$ and pick a positive integer n_2. Then write

$$A_2 := A_1 \cup \{\rho^j(i_2)\}_{0 \leqslant j < n_2}.$$

Now you can stop and have obtained a jump set $A := A_2$. In this case $I = \{i_1, i_2\}$ and $\beta(i_1) = n_1 + n_2, \beta(i_2) = n_1$. If you want instead a jump set with $|I| > 2$, then you check whether there is a $y \in T_\rho$ (resp. T_ρ^*) such that $\rho^{n_2}(i_2) < y$. If such a y doesn't exist, then we set $A := A_2$ and we stop having obtained a jump set (resp. an extended jump set). Otherwise you pick any such y and put $y := i_3$ and pick a positive integer n_3. Then write

$$A_3 := A_2 \cup \{\rho^j(i_3)\}_{0 \leqslant j < n_3}.$$

In this case we have $I = \{i_1, i_2, i_3\}$ and $\beta(i_1) = n_1 + n_2 + n_3, \beta(i_2) = n_2 + n_3, \beta(i_3) = n_3$.

One continues inductively as follows. Having arrived at A_k, together with i_k, n_k, for $k \in \mathbb{Z}_{\geqslant 3}$, either we set $A := A_k$ and we have obtained a jump set, or we verify whether there exists a $y \in T_\rho$ (resp. in T_ρ^*) such that $\rho^{n_k}(i_k) < y$. If such a y doesn't exist then we set $A := A_k$ and we stop having obtained a jump set (resp. an extended jump set). Otherwise we pick any such y and set $y := i_{k+1}$, we choose a positive integer n_{k+1} and write

$$A_{k+1} = A_k \cup \{\rho^j(i_{k+1})\}_{0 \leqslant j < n_k}.$$

The set A_{k+1} is a jump set for ρ (resp. an extended jump set). In this case we have $I = \{i_1, \dots, i_{k+1}\}$ with $\beta(i_1) = n_1 + \ldots + n_{k+1}, \beta(i_2) = n_2 + \ldots + n_{k+1}, \dots, \beta(i_k) = n_k + n_{k+1}, \beta(i_{k+1}) = n_{k+1}$.

Jump sets will often arise as the set of *maximal* or *minimal* of certain sets, with respect to the following partial order. This partial order will also play an important role in the classification of the possible sets of jumps of a character.

Definition 2.6. Let $(a_1, b_1), (a_2, b_2)$ be in $(\mathbb{Z}_{\geqslant 1})^2$. We let $(a_1, b_1) \leqslant_\rho (a_2, b_2)$ if and only if

$$b_2 \geqslant b_2 \text{ and } \rho^{b_2}(a_2) \geqslant \rho^{b_1}(a_1).$$

Let now A be a subset of T_ρ (resp. of T_ρ^*), and let $b : A \to \mathbb{Z}_{\geqslant 1}$. Let $\mathrm{Max}(A, b)$ and $\mathrm{Min}(A, b)$ be the subsets of $\mathrm{Graph}(b)$ consisting of, respectively, the maximal and the minimal elements with respect to $\leqslant_\rho$. Then the following fact follows from the definition of a jump set.

Proposition 2.7. *There are unique jump sets* $(I^+_{(A,b)}, \beta^+_{(A,b)})$ *and* $(I^-_{(A,b)}, \beta^-_{(A,b)})$ *(resp. extended jump sets) such that* $\mathrm{Graph}(\beta^+_{(A,b)}) = \mathrm{Max}(A, b)$ *and* $\mathrm{Graph}(\beta^-_{(A,b)}) = \mathrm{Min}(A, b)$.

Proposition 2.7 is repeatedly used throughout this paper. Moreover it occurs always in the same manner, namely to recover an intrinsic description of an object presented in a non-canonical fashion. This will firstly apply in the context of filtered modules in Proposition 3.34, to reconstruct from a coordinate representation, with respect to a filtered basis (see 3.24) the orbit of a vector of a free filtered module (see 3.26) acted upon by the group of filtered automorphisms. Another example is given by Proposition 4.3, where Proposition 2.7 is used to determine the set of jumps of a character. Finally it is used in the context of Eisenstein polynomials in Theorem 1.13 and Theorem 1.14.

3. Filtered modules

3.1. **Overview.** The goal of this section is to use jump sets to parametrize quasi-free filtered modules (see definition 3.27). As stated in Proposition 5.1, principal units give rise to a free or quasi-free filtered module. So the material of this section will provide exactly the amount of general (elementary) theory of filtered modules sufficient to classify, in terms of jump sets, the possible structures of U_1, as a filtered module.

The rest of the section is organized as follows:

In 3.2 we will collect very general facts about filtered modules that will be applied in the other sections.

In 3.3 we will specialize to the case where the base ring, R, is a complete DVR.

In 3.3.1 we explain how one can attach to a filtered module M a non-decreasing function ρ_M, by looking at the action of π_R, a uniformizer in R, on the filtration.

In 3.3.2 we introduce the notion of free filtered modules: in a precise sense they stand as universal modules among those having a fixed ρ-map (see 3.22 for the precise universal property). Next we will introduce the notion of quasi-free filtered modules, which in a precise sense are just one step more complicated than the free ones. The goal of the rest of the section is classifying quasi-free modules.

In 3.3.4 we will provide presentations of a quasi-free filtered module via a free filtered module and exploit the action of the filtered automorphism group of the free filtered module on the set of presentations of a given quasi-free filtered module.

In 3.3.5 we will parametrize the set of orbits of lines in a free filtered module, under the filtered automorphism group, via jump sets.

In 3.3.6 we will use 3.3.4 and 3.3.5 to explain how jump sets parametrize the set of quasi-free filtered modules.

In 3.3.7 we explain an internal procedure to reconstruct the jump set of a quasi-free filtered module. This will suggest a generalization which will be exploited in later sections. This will be used to detect a more general connection between phenomena in the filtration and ramification theory. See also Theorem 1.14.

3.2. **General facts about filtered modules.** Let R be a commutative ring with unity.

Definition 3.1. *A filtered R-module* is a sequence of R-modules, $M_1 \supseteq M_2 \supseteq \ldots \supseteq M_i \supseteq \ldots$ with $\bigcap_{i\in\mathbb{Z}_{\geqslant 1}} M_i = \{0\}$.

We will usually denote by $M_\bullet$ a filtered R-module $M_1 \supseteq M_2 \supseteq \ldots \supseteq M_i \supseteq \ldots$. A filtered module comes with a weight map $w : M_1 \to \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$, defined as $w(x) := \sup\{i \in \mathbb{Z}_{\geqslant 1} : x \in M_i\}$. The weight map w enjoys the following conditions: $w^{-1}(\{\infty\}) = \{0\}$ and if $x, y \in M_1, a \in R$, then $w(x + y) \geqslant \min\{w(x), w(y)\}$ and $w(ax) \geqslant w(x)$. Clearly one can recover the filtration from the knowledge of w, and conversely given an R-module M, together with a map $w : M \to \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$ enjoying the above conditions, one can define the filtration $M_i := \{x \in M : w(x) \geqslant i\}$. It follows that one can equivalently speak of a filtered R-module as a pair (M, w), where M is an R-module and w is a map with the above properties. We will interchangeably denote a filtered module as $M_\bullet$ and as a pair (M, w).

Definition 3.2. Given $M_\bullet, N_\bullet$ two filtered R-modules, a morphism of filtered R-modules $\varphi : M_\bullet \to N_\bullet$ is a morphism of R-modules $\varphi : M_1 \to N_1$, such that, for each positive integer i, $\varphi(M_i) \subseteq N_i$.

With definitions 3.1 and 3.2, filtered R-modules form a category, which we will denote as Filt-R-mod. We next explain basic constructions in this category which we will use later in this section.

3.2.1. *Direct products and direct sums.* Let $\{M_{h\bullet}\}_{h\in\mathscr{H}}$ be a collection of filtered R-modules. The filtration $\prod_{h\in\mathscr{H}} M_{h,1} \supseteq \prod_{h\in\mathscr{H}} M_{h,2} \supseteq \ldots \supseteq \prod_{h\in\mathscr{H}} M_{h,n} \supseteq \ldots$ gives to $\prod_{h\in\mathscr{H}} M_{h,1}$ the structure of a filtered R-module. This filtered module behaves as a categorical direct product. The filtration $\bigoplus_{h\in\mathscr{H}} M_{h,1} \supseteq \bigoplus_{h\in\mathscr{H}} M_{h,2} \supseteq \ldots \supseteq \bigoplus_{h\in\mathscr{H}} M_{h,n} \supseteq \ldots$ gives to $\bigoplus_{h\in\mathscr{H}} M_{h,1}$ the structure of a filtered R-module. This filtered module behaves as a categorical direct sum.

3.2.2. *Metric structure.* Let (M, w) be a filtered module. Fix a real number $c \in (0, 1)$. Then we have a distance on M, defined as $d(x, y) = c^{w(x-y)}$, which gives to M the structure of a metric space and of a Hausdorff topological group. In the notation $M_\bullet$, the topology can be alternatively described by saying that the $\{M_i\}_{i\in\mathbb{Z}_{\geqslant 1}}$ form a fundamental system of neighborhoods of 0_{M_1}.

It is with respect to this metric that we will perform, in the rest of this paper, any metric or topological operation on a filtered R-module. For instance a filtered module $M_\bullet$ will be said to be complete, if M_1, with the above metric, is a complete metric space. There is a completion functor from R-filt-mod to the full subcategory whose objects are complete filtered modules, Compl-R-filt-mod, which consists simply of completing the underlying metric space. We denote this functor by $\widehat{\ }$. It is left adjoint to the inclusion functor Compl-R-filt-mod $\subseteq$ R-filt-mod which is the identity on both objects and morphisms. Thus one has a natural transformation of the identity, which we denote by compl : $\mathrm{id}_{R\text{-filt-mod}} \to \widehat{\ }$. This natural transformation consists of the natural inclusion of a filtered module $M_\bullet$ in its completion, which we denote by $\widehat{M}_\bullet$.

3.2.3. *Sub-modules.* If (M, w) is a filtered R-module, and $N \subseteq M$ an R-sub-module of M, then $(N, w_{|N})$ is a filtered R-module. If the filtration for M is $M_1 \supseteq M_2 \supseteq \ldots \supseteq M_i \supseteq \ldots$, the one for N is $N \cap M_1 \supseteq N \cap M_2 \supseteq \ldots \supseteq N \cap M_i \supseteq \ldots$. It is in this sense that we will speak of a filtered R-sub-module.

3.2.4. *Quotients.* Let $M_\bullet$ be a filtered R-module and $N \subseteq M_1$ an R-sub-module of M. Then the filtration $M_1/N = (M_1+N)/N \supseteq (M_2+N)/N \supseteq \ldots \supseteq (M_i+N)/N \supseteq \ldots$, gives to M_1/N the structure of a filtered R-module if and only if N is closed. Indeed this filtration defines a fundamental system of neighbours of $0_{M_1/N}$ corresponding to the quotient topology coming from M_1: the requirement of being a filtered module is equivalent to the requirement that this topology is Hausdorff, and the quotient of a topological group by a normal subgroup is Hausdorff iff the normal subgroup is closed, since a topological group is Hausdorff iff the origin is closed.

We now introduce the functors which will play an important role in the rest of the section.

Definition 3.3. (a) Let $M_\bullet, N_\bullet$ be two filtered R-modules, and i, j two positive integers with $i \leqslant j$. Denote by $F_{i,j}(M_\bullet) := M_i/M_j$. Given a morphism of filtered R-modules $\varphi : M_\bullet \to N_\bullet$, denote by $F_{i,j}(\varphi)$, the induced morphism $F_{i,j}(\varphi) : M_i/M_j \to N_i/N_j$. Denote by $F_{i,j}$ the functor, $F_{i,j}$: Filt-R-mod $\to$ R-mod, obtained in this way. Denote by F_i the functor $F_{i,i+1}$.

The rest of this section describes the relations between a morphism $\varphi : M_\bullet \to N_\bullet$ of filtered R-modules and the sequence of morphisms $\{F_j(\varphi) : F_j(M_\bullet) \to F_j(N_\bullet)\}_{j\in\mathbb{Z}_{\geqslant 1}}$ of R-modules. We begin by describing the effect of F_j on the completion morphism:

Remark 3.4. For every positive integer i, the natural transformation compl induces an isomorphism of functors $F_i \circ \widehat{\ } \simeq_{\text{functors}} F_i$.

Next we determine basic properties when applying F_j to the inclusion of the direct sum in the direct product.

3.2.5. *More on direct sum and direct product.*

Remark 3.5. For each positive integer j and $\{(M_i, w_i)\}_{i\in I}$ any collection of filtered R-modules, we have that

- $F_j(\prod_{i\in I} M_i) = \prod_{i\in I} F_j(M_i)$
- $F_j(\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I} F_j(M_i)$
- $F_j(\bigoplus_{i\in I} M_i \subseteq \prod_{i\in I} M_i) = (\bigoplus_{i\in I} F_j(M_i) \subseteq \prod_{i\in I} F_j(M_i))$, where in both cases we mean the natural inclusion of the direct sum in the direct product.

Proposition 3.6. *Given $\{M_{i,\bullet}\}_{i\in I}$ any collection of R-filtered modules, the following are equivalent:*
(a) *The inclusion of filtered modules $\bigoplus_{i\in I} M_{i,\bullet} \subseteq \prod_{i\in I} M_{i,\bullet}$ induces a dense inclusion of metric spaces.*
(b) *For each $m \in \mathbb{Z}_{\geqslant 1}$ there are only finitely many $i \in I$ such that $\min(w_{M_{i,\bullet}}(M_{i,1})) \leqslant m$.*
(c) *We have that $F_m(\bigoplus_{i\in I} M_{i,\bullet} \subseteq \prod_{i\in I} M_{i,\bullet})$ is an isomorphism for all $m \in \mathbb{Z}_{\geqslant 1}$.*

Proof. (a) $\to$ (b) Fix $m \in \mathbb{Z}_{\geqslant 1}$. Pick a vector $v = (v_i)_{i\in I} \in \prod_{i\in I} M_{i,1}$ such that, for all $i \in I$, $v_i = 0$ or $w_{M_{i,\bullet}}(v_i) \leqslant m$ holds. By assumption we can find a finite subset, J, of I, and a vector $(y_i)_{i\in I} \in \prod_{i\in I} M_{i,1}$, such that $y_i = 0$ if $i \notin J$ and $(w_{\prod_{i\in I} M_{i,\bullet}})(v_i - y_i)_{i\in I} > m$. It follows that for all $i \notin J$, $w_{M_{i,\bullet}}(v_i) > m$. Thus for every $v = (v_i)_{i\in I} \in \prod_{i\in I} M_i$, $w_{M_{i,\bullet}}(v_i) \leqslant m$ holds for only finitely many $i \in I$, that is $\min(w_{M_{i,\bullet}}(M_i)) \leqslant m$ holds for only finitely many $i \in I$.

(b) → (a) Observe that assumption (b) implies that $M_i = 0$ holds for all but countably many $i \in I$: indeed, by assumption, the function $M_{i,\bullet} \to \min(w(M_{i,1}))$ has finite fiber over every positive integer, so, except for a countable set of indices, $w_{M_{i,\bullet}}(M_{i,1}) = \{\infty\}$ holds, which is equivalent (by definition of filtered module) to $M_{i,1} = 0$ for all but countably many indices. So we can assume that $I = \mathbb{Z}_{\geqslant 1}$. Thus fix $v := (v_n)_{n\in\mathbb{Z}_{\geqslant 1}} \in \prod_{i\in\mathbb{Z}_{\geqslant 1}} M_{i,1}$. Consider the sequence $\{h_l\}_{l\in\mathbb{Z}_{\geqslant 1}} := \{(w_{l,i})_{i\in\mathbb{Z}_{\geqslant 1}}\}_{l\in\mathbb{Z}_{\geqslant 1}}$, where $w_{l,i} = v_i$ if $i \leqslant l$, 0 otherwise. One has that for all $m \in \mathbb{Z}_{\geqslant 1}$, $(w_{\prod_{i\in\mathbb{Z}_{\geqslant 1}} M_i})(v - w_l) > m$, holds for all but finitely many values of l. This means exactly that $h_l \to v$ as $l \to \infty$. Thus the inclusion of filtered modules $(\bigoplus_{i\in I} M_i, d_{\oplus_{i\in I} M_{i,\bullet}}) \subseteq (\prod_{i\in I} M_i, d_{\prod_{i\in I} M_{i,\bullet}})$ induces a dense inclusion of metric spaces. For the equivalence between (b) and (c) see Remark 3.16. □

Finally we look at the relation between injectivity/surjectivity of φ and the pointwise injectivity/surjectivity of the sequence $\{F_j(\varphi)\}_{j\in\mathbb{Z}_{\geqslant 1}}$:

3.2.6. *Surjectivity and injectivity.*

Proposition 3.7. *Let $M_\bullet, N_\bullet$ be two filtered modules, and $\varphi \in \mathrm{Hom}_{\mathrm{filt}}(M_\bullet, N_\bullet)$. Then the following holds:*
(a) *Assume $M_\bullet$ complete. If for all $i \in \mathbb{Z}_{\geqslant 1}$ we have that $\mathrm{coker}(F_i(\varphi)) = 0$, then $\mathrm{coker}(\varphi) = 0$.*
(b) *We have that for all $i \in \mathbb{Z}_{\geqslant 1}$ the module $\ker(F_i(\varphi))$ is 0 if and only if for all $x \in M_1$ the weights $w_{M_\bullet}(x)$ and $w_{N_\bullet}(\varphi(x))$ coincide.*
(c) *If for all $i \in \mathbb{Z}_{\geqslant 1}$ we have that $\ker(F_i(\varphi)) = 0$, then $\ker(\varphi) = 0$.*
(d) *If φ is an isomorphism then for all $i \in \mathbb{Z}_{\geqslant 1}$ the map $F_i(\varphi)$ is an isomorphism. If $M_\bullet$ is complete, the converse holds as well.*

Proof. (a) Let $x \in N_1$. We construct inductively sequences $\{x_n\}_{n\in\mathbb{Z}_{\geqslant 0}}, \{y_n\}_{n\in\mathbb{Z}_{\geqslant 0}}$ respectively N_1, M_1-valued, which will do for us the following: $\{\sum_{i=0}^n y_i\}_{n\in\mathbb{Z}_{\geqslant 1}}$ will be a convergent sequence, with $\varphi(\sum_{i=0}^n y_i) - x = x_{n+1}$, with $\lim_{n\to\infty} x_n = 0$. Since φ is a filtered morphism and in particular continuous, and $M_\bullet$ is complete, we can conclude then that $\varphi(\sum_{i=0}^\infty y_i) = x$. The construction of $\{x_n\}_{n\in\mathbb{Z}_{\geqslant 0}}, \{y_n\}_{n\in\mathbb{Z}_{\geqslant 0}}$ goes as follows. Put $x_0 = x, y_0 = 0$; construct x_{n+1}, y_{n+1} from x_n in the following way. If $x_n = 0$ put $x_{n+1} = y_{n+1} = 0$. Otherwise $w_{N_\bullet}(x_n) \in \mathbb{Z}_{\geqslant 1}$ holds. Since the map $F_{w_{N_\bullet}(x_n)}(\varphi)$ is surjective, pick $y \in M_{w_{N_\bullet}(x_n)}$ such that $(\varphi)(y) \equiv x_n \bmod N_{w_{N_\bullet}(x_n)+1}$, and denote $y_{n+1} = y$ and $x_{n+1} = -\varphi(y) + x_n$. By construction, the sequences $\{x_n\}_{n\in\mathbb{Z}_{\geqslant 0}}, \{y_n\}_{n\in\mathbb{Z}_{\geqslant 0}}$ both converge to 0. So by the ultrametric inequality and completeness of $M_\bullet$ the series $\sum_{n\in\mathbb{Z}_{\geqslant 0}} y_n$ converges to an element of M_1, which we denote by $\overline{y}$. By construction $\varphi(\sum_{1\leqslant j\leqslant n} y_j) - x = x_{n+1} \to 0$, so, since φ is continuous, $\varphi(\overline{y}) = x$. So $\mathrm{coker}(\varphi) = 0$.

(b) By definition $M_i - M_{i+1} = \{x \in M_i, w_{M_\bullet}(x) = i\}$, on the other hand $\ker(\varphi)_i = 0$ iff $\varphi(M_i - M_{i+1}) \subseteq N_i - N_{i+1} = \{y \in N_i, w_{M_\bullet}(y) = i\}$, thus $\ker(\varphi)_i = 0$ for all $i \in \mathbb{Z}_{\geqslant 1}$ iff $w_{M_\bullet}(x) = w_{N_\bullet}(\varphi(x))$ for all $x \in M_1$.

(c) Thanks to (b) the hypothesis in (c) is equivalent to $\varphi(M_i - M_{i+1}) \subseteq N_i - N_{i+1}$, which implies that $\ker(\varphi) \subseteq \bigcap_{i\in\mathbb{Z}_{\geqslant 1}} M_i = \{0\}$.

(d) The first implication follows from the general fact that a functor preserves isomorphisms, applied to the functors F_i. For the second implication: assume $M_\bullet$ complete, then (a) implies that φ is surjective. On the other hand (c) implies that φ is also injective. Thus φ is a filtered isomorphism. □

Remark 3.8. Suppose $\varphi : M_\bullet \to N_\bullet$ is a filtered epimorphism. Then $F_1(\varphi)$ is surjective. Indeed by definition of filtered epimorphism, and the fact that 1 is minimal in $\mathbb{Z}_{\geqslant 1}$ we have $\varphi^{-1}(N_1 - N_2) \subseteq M_1 - M_2$: since φ is surjective, applying φ to both sizes of this relation one gets $N_1 - N_2 \subseteq \varphi(M_1 - M_2)$, which proves that $F_1(\varphi)$ is surjective.

Definition 3.9. Let i be a positive integer and let $M_\bullet$ be a filtered R-module. We define $M_{\bullet+i}$ to be the filtered R-module

$$M_{i+1} \supseteq M_{i+2} \supseteq \dots$$

Proposition 3.10. *Let $M_\bullet, N_\bullet$ be two filtered modules. Let $\varphi : M_\bullet \to N_\bullet$ be a filtered epimorphism. Let i be a positive integer such that $F_j(\varphi)$ is an isomorphism for every j such that $1 \leqslant j \leqslant i$. Then $\varphi_{|M_{\bullet+i}} : M_{\bullet+i} \to N_{\bullet+i}$ is a filtered epimorphism and $F_{i+1}(\varphi)$ is surjective.*

Proof. Indeed, by Proposition 3.7, the hypothesis is equivalent to $F_{1,i+1}(\varphi)$ being a filtered isomorphism. Thus $\varphi(M_1 - M_{i+1}) \subseteq N_1 - N_{i+1}$. Thus, since φ is an epimorphism, it follows that $\varphi(M_{i+1}) = N_{i+1}$, in particular by remark 3.8 we have that $F_{i+1}(\varphi) = F_1(\varphi_{|M_{\bullet+i}})$ is surjective, proving the statement. □

Proposition 3.11. *Let $M_\bullet, N_\bullet$ be two filtered modules with $M_\bullet$ complete. Let φ be an element of* $\mathrm{Hom}_{\mathrm{filt}}(M_\bullet, N_\bullet)$. *The following are equivalent:*
(a) *For every positive integer i, we have that* $\mathrm{coker}(F_i(\varphi)) = 0$.
(b) *For every positive integer i, we have that* $\mathrm{coker}(\varphi_{|M_i} : M_i \to N_i) = 0$.

Proof. (a) → (b) Let i be a positive integer. For a positive integer $j > i$, the equality $F_j(\varphi_{|M_{\bullet+i}}) = F_{i+j-1}(\varphi)$ trivially holds. Thus assumption (a) is preserved by restriction of φ to the filtered submodule $M_{\bullet+i}$. So Proposition 3.7 implies that $\mathrm{coker}(\varphi_{|M_i} : M_i \to N_i) = 0$.

(b) → (a) The statement trivially follows applying remark 3.8 to every filtered morphism $\varphi_{|M_i} : M_{\bullet+i} \to N_{\bullet+i}$ since they are all assumed to be epimorphisms. □

Proposition 3.12. *Let $M_\bullet, N_\bullet$ be two filtered modules, $M_\bullet$ complete, and $\varphi \in \mathrm{Hom}_{\mathrm{filt}}(M_\bullet, N_\bullet)$. Assume $i \in \mathbb{Z}_{\geqslant 1}$ is such that $\ker(F_j(\varphi)) = \mathrm{coker}(F_j(\varphi)) = 0$ for all $j > i$. Then $\ker(\varphi) \cap w_{M_\bullet}^{-1}\{i, \infty\}$ is an R-submodule, and the inclusion in M_i induces an isomorphism $\ker(\varphi) \cap w_{M.}^{-1}\{i, \infty\} \simeq \ker(F_i(\varphi))$.*

Proof. Since $\ker(F_j(\varphi)) = 0$ for all $j > i$, it follows that $\ker(\varphi) \cap M_i = \ker(\varphi) \cap w_{M.}^{-1}\{i, \infty\}$ proving thus that is an R-submodule, and that the inclusion in $F_i(M_\bullet)$ is injective. Suppose $x \in M_i - M_{i+1}$, $\varphi(x) \in N_{i+1}$ holds. Thanks to the assumption $\ker(F_j(\varphi)) = \mathrm{coker}(F_j(\varphi)) = 0$ for all $j > i$, and to Proposition 3.7, we see that $\varphi_{|M_{\bullet+i+1}}$ is an isomorphism and thus it follows that there is exactly one $y \in M_{i+1}$ such that $\varphi(x) = \varphi(y)$. Thus, since $x \equiv x - y \bmod M_{i+1}$, and $x - y \in \ker(\varphi)$ we obtain that the natural map from $\ker(\varphi) \cap w_{M_\bullet}^{-1}\{i, \infty\}$ to $F_i(M_\bullet)$ is also surjective. □

Corollary 3.13. *Let $M_\bullet, N_\bullet$ be two filtered modules, $M_\bullet$ complete, and $\varphi \in \mathrm{Hom}_{\mathrm{filt}}(M_\bullet, N_\bullet)$. Assume $i \in \mathbb{Z}_{\geqslant 1}$ is such that $\mathrm{coker}(F_j(\varphi)) = 0$ for all $j > i$ and $\ker(F_j(\varphi)) = 0$ for all $j \neq i$. Then $\ker(\varphi) \subseteq w_{M.}^{-1}\{i, \infty\}$, and this inclusion induces an isomorphism $\ker(\varphi) \simeq_{R\text{-mod}} \ker(F_i(\varphi))$.*

Proof. Clearly the assumption that $\ker(F_j(\varphi)) = 0$ for all $j \neq i$ implies that $\ker(\varphi) \subseteq w_{M_\bullet}^{-1}\{i, \infty\}$. Thus lemma 3.12 implies that this inclusion induces an isomorphism

$$\ker(\varphi) = \ker(\varphi) \cap w_{M_\bullet}^{-1}\{i, \infty\} \simeq_{R\text{-mod}} \ker(F_i(\varphi)).$$

□

Remark 3.14. Part (a),(c) of Proposition 3.7 do not hold without the assumption of completeness. An example is given as follows: take a collection of filtered modules $\{(M_i, w_{M_i})\}_{i\in\mathbb{Z}_{\geqslant 1}}$ such that for all $m \in \mathbb{Z}_{\geqslant 1}$ there are only finitely many $i \in I$ such that $\min(w_i(M_i)) \leqslant m$. Now consider $\bigoplus_{i\in I}(M_i, w_i) \subseteq \prod_{i\in I}(M_i, w_i)$. Then $F_m(M_i) = 0$ for all but finitely many i. Thus, by remark 3.5, we have that the inclusion of the direct sum of the direct product is preserved by F_m, but since it is over a finite set of indices (the ones where F_m does not vanish) it is also an isomorphism. But if $M_i \neq 0$ for infinitely many $i \in \mathbb{Z}_{\geqslant 1}$ the inclusion of the direct sum in the direct product is not an isomorphism. This suggests the following proposition.

Proposition 3.15. *Let $M_\bullet, N_\bullet$ be two filtered modules, and $\varphi \in \mathrm{Hom}_{\mathrm{filt}}(M_\bullet, N_\bullet)$, denote by $\hat{\varphi} : \hat{M} \to \hat{N}$ the map induced on the completions. Then the following hold:*
(a) *If $\mathrm{coker}(F_i(\varphi)) = 0$ for all $i \in \mathbb{Z}_{\geqslant 1}$, then $\mathrm{coker}(\hat{\varphi}) = 0$.*
(b) *If $\ker(F_i(\varphi)) = 0$ for all $i \in \mathbb{Z}_{\geqslant 1}$, then $\ker(\hat{\varphi}) = 0$.*
(c) *$F_i(\varphi)$ is an isomorphism for every $i \in \mathbb{Z}_{\geqslant 1}$ iff $\hat{\varphi}$ is an isomorphism.*

Proof. From remark 3.4, we know that F_i and $F_i(\mathrm{compl})$ are isomorphic functors. Thus $\mathrm{coker}F_i(\varphi) = 0$ for all $i \in \mathbb{Z}_{\geqslant 1}$ is equivalent to $\mathrm{coker}F_i(\hat{\varphi}) = 0$ for all $i \in \mathbb{Z}_{\geqslant 1}$, and $\ker(F_i(\varphi)) = 0$ for all $i \in \mathbb{Z}_{\geqslant 1}$, is equivalent to $\ker(F_i(\hat{\varphi})) = 0$ for all $i \in \mathbb{Z}_{\geqslant 1}$. Thus the proposition follows from Proposition 3.7. □

Remark 3.16. Proposition 3.15 implies the equivalence between (b) and (c) in Proposition 3.6. Indeed if we have (c) of Proposition 3.6 then we conclude that the completion of $\prod_{i\in I} M_i$ is also the completion of $\bigoplus_{i\in I} M_i$. Hence in particular $\bigoplus_{i\in I} M_i$ is dense in $\prod_{i\in I} M_i$. This gives that (c) implies (a). But we have shown in Proposition 3.6 that (a) is equivalent to (b), hence (c) implies (b). Conversely it is an immediate verification that (b) implies (c).

3.3. **Filtered modules over a complete DVR.** Now we specialize to the case where R is a complete DVR: we ask completeness because in what follows, we want to apply Propositions 3.7, 3.11, 3.13, and moreover it will be handy when taking filtered quotients of finitely generated modules (see 3.2.4). We fix a uniformizer of R, and we denote it by π_R.

3.3.1. *The ρ-map.* Let $M_\bullet$ a filtered R-module, denote by w its weight map. Define $\rho_{M_\bullet} : \mathbb{Z}_{\geqslant 1} \to \mathbb{Z}_{\geqslant 1} \cup \{\infty\}$ as follows: $\rho_{M_\bullet}(i) := \sup\{j \in \mathbb{Z}_{\geqslant 1}, \pi_R M_i \subseteq M_j\}$. In terms of the weight map we have that $\rho_{M_\bullet}(i) = \min_{x\in M_i}\{w(\pi_R x)\}$.

Remark 3.17. The condition that $\rho_{M_\bullet}$ is a shift map is equivalent to the conjunction of the following two conditions:
(a) For all positive integers i, one has that M_i/M_{i+1} is an $R/(\pi_R)$-vector space. Moreover $\pi_R M_i \neq 0$.
(b) For all positive integers i the R-linear map $\pi_{R|M_i} : M_i \to M_{\rho_{M_\bullet}(i)}$, given by multiplication by π_R, is a filtered morphism.

Definition 3.18. We call a filtered R-module *linear* if it satisfies (a) of remark 3.17. We call a filtered R-module *strictly linear* if it satisfies both part (a) and part (b) of remark 3.17.

Let $M_\bullet$ be a linear filtered R-module. Multiplication by π_R induces a map $F_i(M_\bullet) \to F_{\rho_{M_\bullet}(i)}(M_\bullet)$, which we denote by $[\pi_R]_i$. One has by definition that $[\pi_R]_i = F_1(\pi_{R|M_i})$.

Observe that the right hand side is well defined thanks to part (b) of the definition of a linear filtered R-module.

Definition 3.19. Let $M_\bullet$ be a linear R-filtered module and let i be a positive integer.
(a) We denote by $f_i(M_\bullet) = \dim_{R/(\pi_R)}(F_i(M_\bullet))$.
(b) We denote by $\text{defect}_{M_\bullet}(i) := \dim_{R/(\pi_R)}(\ker([\pi_R]_i))$.
(c) We denote by $\text{codefect}_{M_\bullet}(i) := \dim_{R/(\pi_R)}(\text{coker}([\pi_R]_i))$.

3.3.2. *Free filtered modules.* Fix ρ a shift map. Here we introduce the class of free filtered R-modules with respect to ρ. Free filtered modules play a role in the category of filtered modules similar to the one played by free R-modules in the category of R-modules. We thus recall the role of the latter to clarify the introduction of the former.

Free R-modules. Recall that if X is a set, then we have a covariant functor $H_X : R\text{-mod} \to \text{Set}$, defined on an object $M \in R\text{-mod}$ as $H_X(M) := \text{Hom}_{\text{Set}}(X, M)$, and defined on a morphism $\varphi : M \to N$ as $H_X(\varphi)(f) := \varphi \circ f$ for each $f \in \text{Hom}_{\text{Set}}(X, M)$. In other words H_X is the restriction of the functor $\text{Hom}_{\text{Set}}(X, -)$ to the image of R-mod in Set via the forgetful functor. This functor is representable in R-mod: up to isomorphism there is a unique R module, N_X, such that $H_X \simeq_{\text{functor}} \text{Hom}_{R\text{-mod}}(N_X, -)$. This module is called the free module over X, and concretely it is the module of finite formal R-linear combinations of elements of X. By Yoneda's Lemma the different choices of an isomorphism $\Phi : \text{Hom}_{R\text{-mod}}(N_X, -) \to H_X$, correspond to the different choices of $\Phi_{N_X}(\text{id}_{N_X}) : X \to N_X$, which are the different choices of a basis $\mathscr{B}$ for N_X together with a bijection between $\mathscr{B}$ and X. Again, by Yoneda's Lemma, the set $\text{Isom}_{\text{functors}}(H_X, N_X)$ is a torsor under $\text{Aut}_{R\text{-mod}}(N_X)$.

Free R-modules are the easiest R-modules, and once we trivialize $\text{Isom}_{\text{functors}}(H_X, N_X)$, by the choice of a basis Φ, then, by construction, for any R-module M, the set $\text{Hom}_{R\text{-mod}}(N_X, M)$ is in natural bijection with $\text{Hom}_{\text{Set}}(X, M)$, via Φ. Thus we can easily use suitable free R-modules to present other modules. The ease in defining presentations $N_X \twoheadrightarrow M$, once a trivialization Φ is chosen, has the price of obscuring structural information about M. Thus one is led to look for properties of the presentation which are invariant under $\text{Aut}_{R\text{-mod}}(N_X)$. This is exactly the path we will follow in attaching jump sets to special filtered modules. So, first, we need to define the analogue of a free filtered module, which we do next.

Free filtered R-modules. First we introduce the analogue of the functors H_X of the previous paragraph. Consider pairs (X, g), where X is a set and g is a map $g : X \to \mathbb{Z}_{\geqslant 1}$. Denote by ρ-Filt-R-mod the full sub-category of Compl-Filt-R-mod, having as objects complete linear R-filtered modules $M_\bullet$ such that $\rho_{M_\bullet} \geqslant \rho$. Consider the functor $H_{(X,g)} : \rho\text{-Filt-}R\text{-mod} \to \text{Set}$, defined on an object $M_\bullet \in \rho\text{-Filt-}R\text{-mod}$ as $H_{(X,g)}(M_\bullet) := \{f \in \text{Hom}_{\text{Set}}(X, M_1) : \text{for all } x \text{ in } X,\ w(f(x)) \geqslant g(x)\}$, and defined on morphisms by left composition. The goal of this paragraph is show that this functor is representable. We start with the simplest possible case of a pair (X, g) with $X = \{x\}$ being a point. Put $n := g(x)$. Clearly the functor depends only on n, so, for simplicity, we will denote it by H_n.

Definition 3.20. The n-th standard filtered module, S_n, for ρ, is given by: $S_n = R$, with weight map defined as $w(x) = \rho^{\text{ord}_R(x)}(n)$, for all x in R.

Observe that S_n is an object of ρ-Filt-R-mod (recall that R is assumed complete). It turns out that it represents H_n.

Proposition 3.21. *The functor H_n is represented by S_n.*

Proof. Observe that by definition H_n is simply the functor sending $M_\bullet$ to the set M_n, and sending a morphism $\varphi : M_\bullet \to N_\bullet$ to the restriction $\varphi_{|M_n} : M_n \to N_n$. So it suffices to prove that given $M_\bullet \in \rho$-Filt-R-mod, and given $v \in M_n$, the unique R-linear morphism from R to M_1 sending $1 \mapsto v$, is a filtered morphism from S_n to $M_\bullet$, and that these are all the possible filtered morphism from S_n to $M_\bullet$. But this follows directly from the definition of S_n and the fact that $M_\bullet$ is an object of ρ-Filt-R-mod. □

Now we can prove that $H_{(X,g)}$ is representable for any set X and any map $g : X \to \mathbb{Z}_{\geqslant 1}$. For a positive integer i denote by $c_{(X,g)}(i) := |g^{-1}(i)|$. Given c a cardinal number and $N_\bullet$ a filtered module, denote by $N_\bullet^{(c)}$ the direct sum of c copies of $N_\bullet$.

Proposition 3.22. *The functor $H_{(X,g)}$ is represented by the filtered R-module $\prod_{i\in\mathbb{Z}_{\geqslant 1}} \widehat{S_i^{(c_{(X,g)}(i))}}$.*

Proof. The functor $H_{(X,g)}$ is isomorphic to the direct product of the functors $H_{g(x)}$ as x varies in X. So it follows from Proposition 3.6, Claim 3.21 and the universal property of the completion, that $H_{(X,g)}$ is isomorphic to the functor $\mathrm{Hom}_{\mathrm{filt}}(\widehat{\prod_{i\in\mathbb{Z}_{\geqslant 1}} S_i^{(c_{(X,g)}(i))}}, -)$. □

Remark 3.23. Let i be a positive integer. If $c_{(X,g)}(i)$ *finite*, then we can omit the completion of the factor $S_i^{(c_{(X,g)}(i))}$, since it is already a complete filtered module. In our application $c_{(X,g)}(i)$ will always be finite.

An object $M_\bullet$ in ρ-Filt-R-mod, representing $H_{(X,g)}$ (so by Yoneda's Lemma and by Proposition 3.22, isomorphic to $\widehat{\prod_{i\in\mathbb{Z}_{\geqslant 1}} S_i^{(c_{(X,g)}(i))}}$), is said to be free on (X, g). Motivated by the discussion in the above paragraph on free modules, we introduce the following notion.

Definition 3.24. Let $M_\bullet$ be in ρ-Filt-R-mod a free module on (X, g). A *filtered* basis for $M_\bullet$ is an element of $\mathrm{Isom}_{\mathrm{functor}}(\mathrm{Hom}_{\mathrm{filt}}(M_\bullet, -), H_{(X,g)})$.

Given Φ a filtered basis for $M_\bullet$, one recovers a more concrete version of the notion of a filtered basis, by means of Yoneda's Lemma, taking $\Phi_{M_\bullet}(\mathrm{id}_{M_\bullet}) : X \to M_1$. The image of this map generates a free R-module that is dense in M_1 (coinciding with M_1 if and only if X is finite, observe that for X infinite the resulting module is never free as an R-module).

Clearly, the functor $H_{(X,g)}$ depends only on the map $c_{(X,g)}$. So from now on we will directly speak of the functors H_{f^*}, where f^* is a map from $\mathbb{Z}_{\geqslant 1}$ to the cardinal numbers.

We next give an internal criterion for a filtered module to be representing the functor H_{f^*}, under the assumption that f^* is supported in T_ρ, that is, we assume that $f^*(\mathrm{Im}(\rho)) = \{0\}$.

Proposition 3.25. *Let $M_\bullet$ be an object of ρ-Filt-R-mod, and f^* as above. Then the following are equivalent:*
(a) *For every positive integer i one has* $\mathrm{defect}_{M_\bullet}(i) = \mathrm{codefect}_{M_\bullet}(i) = 0$. *Moreover if i is in T_ρ, one has $f_i(M_\bullet) = f^*(i)$.*
(b) *One has an isomorphism of functors $H_{f^*} \simeq_{\mathrm{functor}} \mathrm{Hom}_{\mathrm{filt}}(M_\bullet, -)$.*
(c) *One has an isomorphism of filtered modules $M_\bullet \simeq_{\mathrm{filt}} \widehat{\prod_{i\in\mathbb{Z}_{\geqslant 1}} S_i^{f^*(i)}}$.*

Proof. The equivalence between (b) and (c) is an immediate consequence of Proposition 3.22 and Yoneda's Lemma. It is a straightforward verification that (c) implies (a). We prove that (a) implies (c).

For every positive integer i in T_ρ, lift a basis of M_i/M_{i+1} to M_i and denote it by $\mathscr{B}_i$. The inclusion $\bigcup_{i\in T_\rho} \mathscr{B}_i \subseteq M_1$ consists of an element of $H_{\tilde{f}}(M_\bullet)$, which thus gives, thanks

to Proposition 3.22, a filtered morphism $\varphi : \prod_{i\in\mathbb{Z}_{\geqslant 1}} \widehat{S_i^{f^*(i)}} \to M_\bullet$. We claim that φ is an isomorphism.

Indeed by construction $F_i(\varphi)$ is an isomorphism for every i in T_ρ. But together with the fact that for every positive integer i one has $\mathrm{defect}_{M_\bullet}(i) = \mathrm{codefect}_{M_\bullet}(i) = 0$, this easily implies that for every positive integer i, the map $F_i(\varphi)$ is an isomorphism. So, since $M_\bullet$ is complete, we conclude by part (d) of Proposition 3.7. □

Definition 3.26. Let $M_\bullet$ be an object of ρ-Filt-R-mod, and f a positive integer. Then we call $M_\bullet$ a (f,ρ)-*free filtered module* if it satisfies any of the equivalent conditions of Proposition 3.25, with respect to the constant map $T_\rho \to \mathbb{Z}_{\geqslant 1}$, $i \mapsto f$.

We denote by $M_\rho := \prod_{i\in T_\rho} S_i$, i.e. the $(1,\rho)$-free filtered module. So M_ρ^f is the (f,ρ)-free filtered module.

We next introduce the class of filtered modules that, together with those described in this paragraph, will suffice to classify the possible filtered structures of U_1.

3.3.3. *Quasi-free filtered R-modules.* Recall that in case ρ is a shift with $\#T_\rho < \infty$, then we denote by $e_\rho^* = \max(T_\rho) + 1$. Moreover we define $e_\rho^{'}$ to be the unique positive integer such that $\rho(e_\rho') = e_\rho^*$.

Definition 3.27. Let $M_\bullet$ be an object of ρ-Filt-R-mod. Then we call it (f,ρ)-quasi-free if it satisfies the following three conditions:
(a) For every positive integer i, we have that $f_i(M_\bullet) = f$.
(b) If T_ρ is finite (resp. if T_ρ is not finite), for every positive integer i different from $e_\rho^{'}$ (resp. for every positive integer i), one has $\mathrm{defect}_{M_\bullet}(i) = \mathrm{codefect}_{M_\bullet}(i) = 0$.
(c) If T_ρ is finite one has that $\mathrm{defect}_{M_\bullet}(e_\rho') \leqslant 1$.

So we see that if T_ρ is not finite the notion of a (f,ρ)-quasi-free module coincides with the notion of a (f,ρ)-free module. We characterize this distinction with a module-theoretic property:

Proposition 3.28. *Let $M_\bullet$ be a (f,ρ)-quasi-free filtered module. Then the following are equivalent:*
(a) *T_ρ is finite,*
(b) *M_1 is finitely generated.*

Proof. (a) → (b) Since all the $F_i(M_\bullet)$ are finite dimensional, (b) is equivalent to the statement that for some positive integer n, the R-module M_n is finitely generated. But for $n > e_\rho'$, the filtered R-module $M_{\bullet+n}$ is a $(f, \tau_{|T_\rho|})$-free-module, where for a positive integer m, the symbol τ_m denotes the shift sending any positive integer x to $x+m$. So one concludes by Proposition 3.25.

(b) → (a) Since M_1 is finitely generated, so is M_n. But for $n > e_\rho'$, one has that $M_{\bullet+n}$ is a $(f, \rho\circ\tau_{n-1})$-free module. So by Proposition 3.25 one has that $T_{\rho\circ\tau_{n-1}}$ is finite, which is equivalent to say that T_ρ is finite. □

Until the end of the next paragraph, we will restrict to the case that T_ρ is finite or equivalently that M_1 is finitely generated. We will work again in greater generality only from Section 3.3.4 onward.

We now recover the distinction between (f,ρ)-quasi-free and (f,ρ)-free with a module-theoretic property.

Proposition 3.29. *Let $M_\bullet$ be a ρ-Filt-R-Mod such that $f_i(M_\bullet) = f$ for every positive integer i, and $\mathrm{defect}_{M_\bullet}(j) = \mathrm{codefect}_{M_\bullet}(j) = 0$ for every positive integer $j \neq e'_\rho$. Then the following are equivalent:*
(a) *$M_\bullet$ is (f,ρ)-quasi-free.*
(b) *$M_1[\pi_R]$ is a cyclic R-module.*

Proof. Given the hypothesis we have to prove that $\mathrm{defect}_{M_\bullet}(e'_\rho) \leqslant 1$ is equivalent to $M[\pi_R]$ cyclic. One has that multiplication by π_R is a filtered morphism $\pi_R : M_{\bullet+e'_\rho-1} \to M_{\bullet+e^*_\rho-1}$. Thus the conclusion follows immediately from Corollary 3.13. □

In particular we have the following.

Corollary 3.30. *Let $M_\bullet$ be a (f,ρ)-quasi-free module which is not (f,ρ)-free. Then we have an isomorphism $M[\pi_R] \simeq_{R\text{-mod}} R/\pi_R$ and $w_{M_\bullet}(M[\pi_R]) = \{e'_\rho, \infty\}$.*

3.3.4. *Presentations of a quasi-free modules are conjugate.* We keep assuming that T_ρ is finite. Let f be a positive integer. We will proceed classifying (f,ρ)-quasi-free modules with the help of the additional free module $M^*_\rho := M_\rho \oplus S_{e^*_\rho}$: we will use the module $M_\rho^{f-1} \oplus M^*_\rho$. This module is the free module over the map $f^* : \mathbb{Z}_{\geqslant 1} \to \mathbb{Z}_{\geqslant 1}$ defined as $f^*(i) = f$ for $i \in T_\rho$, $f^*(e^*_\rho) = 1$ and $f^*(i) = 0$ for all the other i. So we fix an isomorphism between $M_\rho^{f-1} \oplus M^*_\rho$ and H_{f^*}, that is we fix a filtered basis for $M_\rho^{f-1} \oplus M^*_\rho$. Let now $M_\bullet$ be a (f,ρ)-quasi-free module that is not (f,ρ)-free. We call a subset $\mathscr{B} \subseteq M_1$ a quasi-basis if it consists of the union of the lifting of a basis of M_i/M_{i+1} for each $i \in T_\rho$ together with the lifting of a generator of $\mathrm{coker}[\pi_R]_{e'_\rho}$ (this cokernel is 1-dimensional because the kernel is 1-dimensional and we assume that $f_i(M_\bullet)$ is constantly f). By the universal property proved in Proposition 3.22, each inclusion of a quasi-basis $\mathscr{B} \subseteq M_1$ gives uniquely (via the above choice of a filtered basis for $M_\rho^{f-1} \oplus M^*_\rho$) a morphism $\varphi_{\mathscr{B}} : M_\rho^{f-1} \oplus M^*_\rho \to M_\bullet$.

Proposition 3.31. *For each quasi-basis $\mathscr{B}$, one has that $\varphi_{\mathscr{B}}$ is a filtered epimorphism.*

Proof. By construction for each $i \in T^*_\rho$, one has that $F_i(\varphi_{\mathscr{B}})$ is surjective. But since for both modules one has that $[\pi_R]_i$ is surjective for i different from e'_ρ, and at e^*_ρ a generator of the co-kernel has been added, one clearly concludes that $F_i(\varphi_{\mathscr{B}})$ is surjective for all i, by repeatedly using the above conditions and the multiplication by π_R. Since $M_\bullet$ is complete, we conclude with Proposition 3.7. □

We have found for $M_\bullet$ presentations with the easiest possible type of filtered module with the given constraints (namely those on the ρ-map) and in a minimal way: $M_\bullet$ and $M_\rho^{f-1} \oplus M^*_\rho$ have the same minimal number of generators as R-modules. This presentation is obtained via the choice of a quasi-basis. To read off the intrinsic structure of $M_\bullet$ via these presentations we proceed looking at the action of $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M^*_\rho)$ on $\mathrm{Epi}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M^*_\rho, M_\bullet)$, in search of invariants. The next proposition is then quite relevant for us.

Proposition 3.32. *The action of $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M^*_\rho)$ on $\mathrm{Epi}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M^*_\rho, M_\bullet)$ is transitive.*

Proof. Recall from definition 3.3 that for a positive integer i we denote by $F_{1,i}$ the functor $F_{1,i} : \text{Filt-}R\text{-mod} \to \text{Filt-}R\text{-mod}$, defined as $F_{1,i}(N_\bullet) := N_1/N_i$, with the quotient filtration, on the objects, and on a morphism $\varphi : M_\bullet \to N_\bullet$, one has that $F_{1,i}(\varphi)$ is defined as the morphism induced by φ, from $F_{1,i}(M_\bullet)$ to $F_{1,i}(N_\bullet)$. Fix $\mathscr{B}$ a quasi-basis of $M_\bullet$. Take $\varphi \in \mathrm{Epi}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M^*_\rho, M_\bullet)$. We claim that we can find a filtered basis $\mathscr{B}'$ of $M_\rho^{f-1} \oplus M^*_\rho$ such that $\varphi(\mathscr{B}') = \mathscr{B}$. We prove this in 2 steps.

1) Firstly we observe that $F_{1,e_\rho^*}(\varphi)$ is an isomorphism. Indeed by construction $F_i(\varphi) = F_i(F_{1,e_\rho^*})(\varphi)$ is an isomorphism for each $i \in T_\rho$, and on both sides the $[\pi]_i$-maps are isomorphisms for each $i < e'_\rho$ since they are (f,ρ)-quasi-free. So it follows that they are isomorphisms for all $i < e_\rho^*$. So the observation is proved by Proposition 3.7. This provides us with the piece of the filtered basis corresponding to the elements $x \in \mathscr{B}$ with $w(x) \in T_\rho$.

2) Take the unique $x \in \mathscr{B}$ with $w(x) = e_\rho^*$. By Proposition 3.10, together with Step 1), we can find $y \in \varphi^{-1}(x)$ with $w(y) = e_\rho^*$. Now we claim that y must generate $\operatorname{coker}[\pi]_{e'_\rho}$. Since this is a 1-dimensional $R/(\pi_R)$-vector space this is equivalent to claiming that y is not the 0-class in that cokernel. But if it were the 0-class, then it there would exist z with $w(z) = e'_\rho$, such that $\pi_R z = y \bmod (M_\rho^{f-1} \oplus M_\rho^*)_{e_\rho^*+1}$. But, from Step 1), it follows that $w(\varphi(z)) = e'_\rho$, but then, since $x = \pi_R\varphi(z) \bmod (M_\rho^{f-1} \oplus M_\rho^*)_{e_\rho^*+1}$, we see that x is in the 0-class in $\operatorname{coker}[\pi]_{e'_\rho}$, which is a contradiction.

So given $\varphi_1, \varphi_2 \in \operatorname{Epi}_{\text{filt}}(M_\rho^{f-1} \oplus M_\rho^*, M_\bullet)$, there are two filtered basis $\mathscr{B}_1, \mathscr{B}_2$ of $M_\rho^{f-1} \oplus M_\rho^*$ mapping to $\mathscr{B}$ via respectively φ_1, φ_2 as explained above. It follows that there exists a suitable bijection, θ, between $\mathscr{B}_1$ and $\mathscr{B}_2$ that respects the weights and such that $\varphi_2 \circ \theta = \varphi_1$ on $\mathscr{B}_1$. But then, by Proposition 3.22, we have that θ extends to a filtered automorphism of $M_\rho^{f-1} \oplus M_\rho^*$ and $\varphi_2 \circ \theta = \varphi_1$ holds on all $M_\rho^{f-1} \oplus M_\rho^*$ and we are done. □

Proposition 3.32 and Proposition 3.31 tell us that to classify-(f,ρ)-quasi-free filtered modules we have to accomplish two tasks:
(a) Classify the orbits of vectors in $M_\rho^{f-1} \oplus M_\rho^*$ under $\operatorname{Aut}_{\text{filt}}(M_\rho^{f-1} \oplus M_\rho^*)$.
(b) Recover which orbits of task (a) arise from (f,ρ)-quasi-free filtered modules.
This is what we do next.

3.3.5. *Jump sets parametrize orbits.* We keep denoting by ρ a shift map, and by f a positive integer. Whenever a star is added, and we refer to an extended jump set in the following statements, we will be implicitly assuming that, in that case, T_ρ is finite. On the other hand, in the parts of the statements where there is no star and we refer to regular jump sets, we only require ρ to be a shift. We begin by attaching to each jump set a vector.

Definition 3.33. Let (I,β) be a ρ-jump set (resp. an extended ρ-jump set). We denote by $v_{(I,\beta)}$ the following vector of $\pi_R M_\rho^f$ (resp. $\pi_R(M_\rho^{f-1} \oplus M_\rho^*)$): for each $i \in T_\rho$ (resp. in T_ρ^*) with $i \notin I$, the projection of $v_{(I,\beta)}$ on S_i^f (resp. the same and on $S_{e_\rho^*}$) is 0. For each $i \in I$, the projection of $v_{(I,\beta)}$ on S_i^f (resp. the same and on $S_{e_\rho^*}$) is the vector $(\pi_R^{\beta(i)}, 0, \dots, 0)$, having $\pi_R^{\beta(i)}$ on the first coordinate and 0 on all the others (resp. $(\pi_R^{\beta(e_\rho^*)})$).

We now prove that with the map $(I,\beta) \mapsto v_{(I,\beta)}$ we catch each orbit at least once. For a vector $v \in \pi_R M_\rho^f$ (resp. $\pi_R M_\rho^{f-1} \oplus \pi_R M_\rho^*$), denote by A_v the set of elements of T_ρ (resp. T_ρ^*), such that $\operatorname{proj}_i(v) \neq 0$, where proj_i denotes the projection on the factor S_i^f (resp. the same if $i \in T_\rho$ and we look at $\operatorname{proj}_{S_{e_\rho^*}}$ for $i = e_\rho^*$). For $a \in A_v$ define $b_v(a) = \operatorname{ord}_R(\operatorname{proj}_i(v))$, the valuation of the a-th projection. Recall the definition of $(I^-_{(A_v,b_v)}, \beta^-_{(A_v,b_v)})$ from Proposition 2.7.

Proposition 3.34. *For each $v \in \pi_R M_\rho^f$ (resp. $\pi_R M_\rho^{f-1} \oplus \pi_R M_\rho^*$) there exists an automorphism $\theta \in \operatorname{Aut}_{\text{filt}}(M_\rho^f)$ (resp. $\theta \in \operatorname{Aut}_{\text{filt}}(M_\rho^{f-1} \oplus M_\rho^*)$) such that $\theta(v) = v_{(I,\beta)}$, where $(I,\beta) := (I^-_{(A_v,b_v)}, \beta^-_{(A_v,b_v)})$.*

Proof. Clearly we can find a filtered automorphism θ_0 such that $\theta_0(v) = v_{(A_v,b_v)}$, where $v_{(A_v,b_v)}$ denotes the following vector of $\pi_R M_\rho^f$ (resp. $\pi_R(M_\rho^{f-1} \oplus M_\rho^*)$): for each $i \in T_\rho$ (resp. T_ρ^*) with $i \notin A_v$, the projection of $v_{(A_v,b_v)}$ on S_i^f (resp. the same and to $S_{e_\rho^*}$) is 0, while for each $i \in A_v$, the projection of $v_{(A_v,b_v)}$ on S_i^f is $(\pi_R^{b_v(i)}, 0, \dots, 0)$ (resp. the same and for $i = e_\rho^*$ is $(\pi_R^{b_v(e_\rho^*)})$). So without loss of generality, we can assume that v has this special form.

Next, let $(i, b_v(i)) <_\rho (j, b_v(j))$. That means that either $i < j$ and $b_v(i) < b_v(j)$, or that $i > j$ and $\rho^{b_v(i)}(i) < \rho^{b_v(j)}(j)$. Observe that in either case we have $b_v(i) < b_v(j)$ and the R-linear automorphism $\theta_{i,j}$ on M_ρ (resp. M_ρ^*), defined as $\theta_{i,j}((x_h)_{h\in T_\rho}) = (x_h - \pi_R^{b_v(j)-b_v(i)}\delta_{i,h}x_j)_{i\in T_\rho}$ (resp. as $\theta_{i,j}((x_h)_{h\in T_\rho^*}) = (x_h - \pi_R^{b_v(j)-b_v(i)}\delta_{i,h}x_j)_{i\in T_\rho^*}$) is *filtered*, precisely due to the above inequalities. Clearly we can extend $\theta_{i,j}$ to a filtered automorphism of M_ρ^f (resp. $M_\rho^{f-1} \oplus M_\rho^*$) by simply letting it act as the identity on the complementary factor M_ρ^{f-1}. The obtained filtered automorphism $\theta_{i,j}$ satisfies the identity

$$A_{\theta_{i,j}(v)} = A_v - \{j\}, b_{\theta_{i,j}(v)} = b_{v|A_v-\{j\}}.$$

If T_ρ is finite, by repeatedly applying transformations $\theta_{i,j}$ we end up precisely having constructed a θ as claimed in this Proposition. If T_ρ is infinite, one can repeatedly apply such elementary transformations $\theta_{i,j}$ in a a sequence that *converges* to a filtered automorphism θ as we wanted to prove this Proposition. □

For a vector $v \in \pi_R M_\rho^f$ (resp. in $\pi_R M_\rho^{f-1} \oplus \pi_R M_\rho^*$), denote by g_v the map $g_v : \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \cup \{\infty\}$ defined as $g_v(i) := w_{M_\rho^f/\pi_R^i M_\rho^f}(v)$ (resp. $g_v(i) := w_{M_\rho^{f-1}\oplus M_\rho^*/\pi_R^i(M_\rho^{f-1}\oplus M_\rho^*)}(v)$). Here $w_{M_\rho^f/\pi_R^i M_\rho^f}(v)$ (resp. $w_{M_\rho^{f-1}\oplus M_\rho^*/\pi_R^i(M_\rho^{f-1}\oplus M_\rho^*)}(v)$) denotes the weight of v in the R-module $M_\rho^f/\pi_R^i M_\rho^f$ (resp. $M_\rho^{f-1} \oplus M_\rho^*/\pi_R^i(M_\rho^{f-1} \oplus M_\rho^*)$) viewed as a filtered R-module with the quotient filtration (see Section 3.2.4). Say that g_v *breaks* at i if $g_v(i) \neq g_v(i+1)$.

Proposition 3.35. *Let (I, β) be a ρ-jump set (resp. an extended ρ-jump set). Let $v_{(I,\beta)} \in \pi_R M_\rho^f$ (resp. $v_{(I,\beta)} \in \pi_R M_\rho^{f-1} \oplus \pi_R M_\rho^*$). Then g_v breaks at i if and only if $i \in \beta(I)$. Moreover if $i \in I$, then we have that $g_v(\beta(i)+1) = \rho^{\beta(i)}(i)$.*

Proof. Let n be a positive integer such that there exists an $i \in I$ with $\beta(i) < n$. Denote by i_0 the smallest such i. Fix the standard basis for M_ρ^f (resp. for $M_\rho^{f-1} \oplus M_\rho^*$) and denote it by $\{b_{ij} : i \in T_\rho,\ j \in \{1, \dots, f\}\}$ (resp. denote it by $\{b_{ij} : i \in T_\rho,\ j \in \{1, \dots, f\}\} \cup \{b_{e_\rho^*,1}\}$). In this notation we have that $v_{(I,\beta)} = \sum_{i\in I} \pi_R^{\beta(i)} e_{i,1}$. It is clear that

$$v_{(I,\beta)} \equiv \sum_{i\in I:\beta(i)<n} \pi_R^{\beta(i)} e_{i,1} \bmod \pi_R^n M_\rho^f.$$

(resp. $v_{(I,\beta)} \equiv \sum_{i\in I:\beta(i)<n} \pi_R^{\beta(i)} e_{i,1} \bmod \pi_R^n \cdot (M_\rho^{f-1} \oplus M_\rho^*)$). Observe that, thanks to the definition of a jump set, we have that

$$w_{M_\rho^f}(\sum_{i\in I:\beta(i)<n} \pi_R^{\beta(i)} e_{i,1}) = \rho^{\beta(i_0)}(i_0).$$

(resp. $w_{M_\rho^{f-1}\oplus M_\rho^*}(\sum_{i\in I:\beta(i)<n} \pi_R^{\beta(i)} e_{i,1}) = \rho^{\beta(i_0)}(i_0)$). Therefore we conclude that

$$w_{M_\rho^f/\pi_R^n M_\rho^f}(\sum_{i\in I:\beta(i)<n} \pi_R^{\beta(i)} e_{i,1}) \geqslant \rho^{\beta(i_0)}(i_0).$$

(resp. $w_{(M_\rho^{f-1}\oplus M_\rho^*)/\pi_R^n\cdot(M_\rho^{f-1}\oplus M_\rho^*)}(\sum_{i\in I:\beta(i)<n}\pi_R^{\beta(i)}e_{i,1}) \geqslant \rho^{\beta(i_0)}(i_0)$). We next prove that this inequality is actually an equality which clearly gives the desired result.

Let $x \in M_\rho^f$ (resp. in $M_\rho^{f-1}\oplus M_\rho^*$). We claim that

$$w_{M_\rho^f}(\pi_R^n x + \sum_{i\in I:\beta(i)<n}\pi_R^{\beta(i)}e_{i,1}) \leqslant \rho^{\beta(i_0)}(i_0).$$

(resp. $w_{M_\rho^{f-1}\oplus M_\rho^*}(\pi_R^n x+\sum_{i\in I:\beta(i)<n}\pi_R^{\beta(i)}e_{i,1}) \leqslant \rho^{\beta(i_0)}(i_0)$). Indeed if this claim would not hold we must conclude that

$$w_{M_\rho^f}(\pi_R^n x) = \rho^{\beta(i_0)}(i_0).$$

(resp. $w_{M_\rho^{f-1}\oplus M_\rho^*}(\pi_R^n x) = \rho^{\beta(i_0)}(i_0)$). But, by construction of the free filtered modules, we have that $w_{M_\rho^f}(\pi_R^n x) = \rho^n(w_{M_\rho^f}(x))$ (resp. $w_{M_\rho^{f-1}\oplus M_\rho^*}(\pi_R^n x) = \rho^n(w_{M_\rho^{f-1}\oplus M_\rho^*}(x))$). This implies that $\rho^{n-\beta(i_0)}(w_{M_\rho^f}(x)) = i_0$, contradicting that $i_0 \in T_\rho$, since $n > \beta(i_0)$ by construction (resp. it implies that $\rho^{n-\beta(i_0)}(w_{M_\rho^{f-1}\oplus M_\rho^*}(x)) = i_0$. In case $i_0 < e_\rho^*$, it again contradicts that $i_0 \in T_\rho$. If $i_0 = e_\rho^*$ we would conclude that $b_{e_\rho^*,1} \in \pi_R\cdot(M_\rho^{f-1}\oplus M_\rho^*)$, which is not possible). This ends the proof. □

This allows us to conclude the following important corollary.

Corollary 3.36. *In each orbit $\mathscr{O}$ of $\pi_R M_\rho^f$ under $\mathrm{Aut}_{filt}(M_\rho^f)$ (resp. $M_\rho^{f-1}\oplus M_\rho^*$ under $\mathrm{Aut}_{filt}(M_\rho^{f-1}\oplus M_\rho^*)$), there exist at most one ρ-jump set (resp. extended ρ-jump set) such that $v_{(I,\beta)}$ belongs to $\mathscr{O}$.*

Proof. Clearly the function g_v is preserved by applying a filtered automorphism. But by Proposition 3.35 it follows that from the function $g_{v_{(I,\beta)}}$ one can reconstruct (I,β). The conclusion follows. □

So, putting together Proposition 3.34 and 3.36, we see that with the map $(I,\beta)\mapsto v_{(I,\beta)}$ we catch each orbit exactly once:

Theorem 3.37. *The map $(I,\beta)\to v_{(I,\beta)}$ induces a bijection between the set of ρ-jump sets (resp. extended ρ-jump sets) and the set of orbits of $\pi_R M_\rho^f$ under the action of $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^f)$ (resp. orbits of $\pi_R M_\rho^{f-1}\oplus\pi_R M_\rho^*$ under the action of $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^{f-1}\oplus M_\rho^*)$).*

Given a vector $v\in\pi_R M_\rho^f$ (resp. in $\pi_R M_\rho^{f-1}\oplus\pi_R M_\rho^*$) we define filt-ord$(v)$ to be the jump set corresponding to the orbit of v under the above bijection. As the terminology suggests, the map filt-ord can be considered as the filtered analogue of the map ord, which gives the valuation of the vector v. Indeed in the latter case knowing ord(v) gives exactly the orbit, under R-linear automorphisms, of v, likewise in the former case knowing filt-ord(v) gives exactly the orbit, under filtered R-linear automorphisms, of v. Moreover as ord(v) is computed by taking the minimum valuation of the coordinates of v, with respect to an R-linear basis, so filt-ord(v) is computed by taking the set of minimal points with respect to $\leqslant_\rho$ for the graph of valuations of the coordinates of v, with respect to a filtered basis (see definition 3.24).

3.3.6. *Jump sets parametrize quasi-free filtered module.* Now we fix ρ a shift with T_ρ finite and f a positive integer. Let $M_\bullet$ be a (f,ρ)-quasi-free filtered module that is not free. By Proposition 3.31 and 3.32 we see that $M_\bullet$ correspond to a unique orbit of vectors in $M_\rho^{f-1}\oplus M_\rho^*$ under $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^{f-1}\oplus M_\rho^*)$. So, together with Theorem 3.37, we obtain a unique

extended ρ-jump set $(I_{M_\bullet}, \beta_{M_\bullet})$ that determines $M_\bullet$ as a filtered module. Thus the map $M_\bullet \mapsto (I_{M_\bullet}, \beta_{M_\bullet})$ gives an injection of the set of isomorphism classes of (f,ρ)-quasi-free module that are not (f,ρ)-free to the set of extended ρ-jump sets. We now want to describe the image. By Proposition 3.35, together with Corollary 3.30, we find that $\rho^{\beta(\min(I_{M_\bullet}))}(\min(I_{M_\bullet})) = e^*_\rho$. Conversely one checks immediately that for an extended ρ-jump set (I,β) such that $\rho^{\beta(\min(I))}(\min(I)) = e^*_\rho$, the filtered R-module $(M_\rho^{f-1} \oplus M_\rho^*)/Rv_{(I,\beta)}$ is a (f,ρ)-quasi-free module. We call these jump sets *admissible*. We have thus proved the following theorem.

Theorem 3.38. *The map sending an admissible extended ρ-jump set (I,β) to $(M_\rho^{f-1} \oplus M_\rho^*)/Rv_{(I,\beta)}$ induces a bijection from the set of admissible extended ρ-jump sets to the set of (f,ρ)-quasi-free filtered modules that are not (f,ρ)-free.*

3.3.7. *Reading the jump set inside the module.* We have classified (f,ρ)-quasi-free modules (which are not free) via admissible extended ρ-jump sets. We have proceeded by introducing an external module, $M_\rho^{f-1} \oplus M_\rho^*$, presenting each of them, and proving that the invariant of each presentation is an admissible extended (f,ρ)-jump set.

We now provide a description of the jump set $(I_{M_\bullet}, \beta_{M_\bullet})$, internally from $M_\bullet$, without any further reference to an external module $M_\rho^{f-1} \oplus M_\rho^*$. In other words we face the task of providing the inverse of the bijection in Theorem 3.38, without reference to $M_\rho^{f-1} \oplus M_\rho^*$. We will proceed by imitating the way we reconstructed the jump set belonging to each orbit in Proposition 3.35. For $v \in M_\bullet$ denote by $g_{v,M_\bullet}$ the map $g_{v,M_\bullet} : \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \cup \{\infty\}$ defined as $g_{v,M_\bullet}(i) := w_{M_\bullet/\pi_R{}^i M_\bullet}(v)$. Say that g_v breaks at i if $g_{v,M_\bullet}(i) \neq g_{v,M_\bullet}(i+1)$. Fix $\tilde{m}$ a generator of $(M_1)_{\mathrm{tors}}$, denote by N the exponent of the torsion, that is $N := \min\{i \in \mathbb{Z}_{\geqslant 1} : \pi_R^i \tilde{m} = 0\}$. The following proposition can be proved by a straightforward imitation of the proof of Proposition 3.35.

Proposition 3.39. *The function $g_{\tilde{m},M_\bullet}$ breaks exactly at the elements of $\beta_{M_\bullet}(I_{M_\bullet}) - N$, moreover if $i \in I_{M_\bullet}$ then $g_{\tilde{m},M_\bullet}(i+1) = \rho^{\beta_{M_\bullet}(i)-N}(i)$.*

So we deduce the following corollary.

Corollary 3.40. *Let $M_\bullet$ be a (f,ρ)-quasi-free filtered module that is not free. Let $\tilde{m} \in M_1$ be a generator of $(M_1)_{\mathrm{tors}}$, then the map $g_{\tilde{m},M_\bullet}$ determines $M_\bullet$ as a filtered module.*

The following simple corollary of Theorem 3.38 will be often useful. Recall the notation $(I^-_{(A,b)}, \beta^-_{(A,b)})$ introduced in Proposition 2.7.

Corollary 3.41. *Let $M_\bullet$ be a (f,ρ)-quasi-free filtered module that is not free. Let I be a subset of T^*_ρ and b a map from I to $\mathbb{Z}_{\geqslant 1}$. Suppose that for each $i \in I$ we have $m_i \in M_i$ satisfying the following three conditions.*
(1) *For each $i \in I$ we have that $w_{M_\bullet}(m_i) = i$.*
(2) *We have that*
$$\sum_{i \in I} \pi_R^{b(i)} m_i = 0.$$
(3) *If $e^*_\rho \in I$ then $m_{e^*_\rho} \notin \pi_R M_1$.*
Then it must be that
$$(I^-_{(A,b)}, \beta^-_{(A,b)}) = (I_{M_\bullet}, \beta_{M_\bullet}).$$

The following proposition shall be often used to recover the structure of the R-module $M_1[\pi_R^\infty] := (M_1)_{\mathrm{tors}}$ from $(I_{M_\bullet}, \beta_{M_\bullet})$. This goes as follows.

Proposition 3.42. *Let $M_\bullet$ be a (f,ρ)-quasi-free filtered R-module. Then we have that*

$$M_1[\pi_R^\infty] \simeq R/\pi_R^{\beta(\max(I_{M_\bullet}))}R,$$

as R-modules.

Proof. Using Theorem 3.38 we deduce that

$$M_1[\pi_R^\infty] \simeq R/\pi_R^{\min(\beta(I_{M_\bullet}))}R.$$

Since $(I_{M_\bullet}, \beta_{M_\bullet})$ is a jump set, the map $\beta_{M_\bullet}$ is in particular decreasing. Hence $\min(\beta(I_{M_\bullet})) = \beta(\max(I_{M_\bullet}))$, which gives precisely the desired conclusion. □

4. Jumps of characters of a quasi-free module

4.1. **Motivation and main results.** In section 5 we will see that U_1 as a filtered module is quasi-free. So, as we will see in detail in 6, via the local reciprocity map the question of determining the possible upper jumps of a cyclic p-power totally ramified extension of a given local field is a special case of the question of determining the jumps of a cyclic character of a given (f,ρ)-quasi-free filtered module, which is the goal of the present section.

Let R be a complete DVR. We denote by $Q(R)$ the fraction field of R. We equip $Q(R)/R$ with the discrete topology.

Definition 4.1. (a) Let $M_\bullet$ be a filtered R-module. A *character* of $M_\bullet$ is a continuous R-linear homomorphism $\chi : M_1 \to Q(R)/R$, where the implicit topology on M_1 is the one coming from the filtration, see 3.2.2.

(b) Let χ be a character of $M_\bullet$. A positive integer i is said to be a *jump* of χ, if $\chi(M_i) \neq \chi(M_{i+1})$. We denote the collection of jumps of χ by J_χ. Finally we denote by $\mathscr{J}_{M_\bullet}$ the collection of all J_χ as χ varies among characters of $M_\bullet$.

One can easily show that if $M_\bullet$ is linear (see definition 3.18), then for each character χ of $M_\bullet$ the set J_χ is finite. We fix a shift map ρ, and a positive integer f. Recall that (f,ρ)-quasi-free modules are in particular linear. The goal of this section is to understand exactly which are the possible sets of jumps:

Goal. *Let $M_\bullet$ be a (f,ρ)-quasi-free module. Characterize the sets $A \subseteq \mathbb{Z}_{\geqslant 1}$ such that $A = J_\chi$ for some character χ of $M_\bullet$.*

We will proceed as follows: in 4.2 we prove that $\mathscr{J}_{M_\rho^f} = \mathrm{Jump}_\rho$ and $\mathscr{J}_{M_\rho^{f-1}\oplus M_\rho^*} = \mathrm{Jump}_\rho^*$. Next in 4.3 we examine the case of (f,ρ)-quasi-free modules that are not free. Given such a module $M_\bullet$, we know from Theorem 3.38 that all we need to know to understand $M_\bullet$ as a filtered module is the extended jump set $(I_{M_\bullet}, \beta_{M_\bullet})$. So it must be possible to predict $\mathscr{J}_{M_\bullet}$ from $(I_{M_\bullet}, \beta_{M_\bullet})$. We achieve this in Theorem 4.8, where it is shown that $\mathscr{J}_{M_\bullet} \subseteq \mathrm{Jump}_\rho^*$, and the missing jump sets are characterized by a combinatorial criterion involving $(I_{M_\bullet}, \beta_{M_\bullet})$.

4.2. **Set of jumps are jump set for a free module.** We proceed in the same way as we did for orbits of vectors in 3.3.5. Clearly the set of jumps of a character does not change if we apply to it a filtered automorphism of $M_\bullet$. Therefore we shall take advantage of this symmetry. It turns out that, for free filtered modules, knowing the set of jumps of a character χ is *equivalent* to knowing to which orbit χ belongs (under the action of the group of filtered automorphisms).

Definition 4.2. (a) Let χ be a character of M_ρ^f (resp. of $M_\rho^{f-1} \oplus M_\rho^*$). Denote by A_χ the set of i in T_ρ (resp. T_ρ^*), such that $\chi(\mathrm{proj}_i) \neq \{0\}$, where proj_i denotes the projection on S_i^f (resp. the same if $i \in T_\rho^*$, where the projection is on $S_{e_\rho^*}$ for the last coordinate).

(b) For a in A_χ, denote by $b_\chi(a) = \min\{r \in \mathbb{Z}_{\geqslant 1} : \pi_R^r \chi(\mathrm{proj}_a) = \{0\}\}$.

We next show that, after applying a suitable filtered automorphism, one can make the pair (A_χ, b_χ) a jump set (resp. an extended jump set). Recall the notation (A_χ^+, b_χ^+) introduced in Proposition 2.7.

Proposition 4.3. *Let χ be a character of M_ρ^f (resp. of $M_\rho^{f-1} \oplus M_\rho^*$). Then there exists $\theta \in \mathrm{Aut}_{\mathrm{filt}}(M_\rho^f)$ (resp. $\mathrm{Aut}_{\mathrm{filt}}(M_\rho^{f-1} \oplus M_\rho^*)$) such that $(A_{\chi\circ\theta}, b_{\chi\circ\theta}) = (A_\chi^+, b_\chi^+)$. In particular $(A_{\chi\circ\theta}, b_{\chi\circ\theta})$ is a ρ-jump set (resp. an extended ρ-jump set).*

Proof. The structure of the proof is the same as the one given for Proposition 3.34, we just mention some differences. Just as in that proof, as a first step we can assume χ is a character vanishing on the factor $M_\rho^{f-1} \oplus 0$ and, as a character of the factor M_ρ (resp. M_ρ^*), it is defined as follows. If $i \notin A_\chi$, then we have $\chi_{|S_i} = 0$. If $i \in A_\chi$, we have $\chi_{|S_i}(1) = \pi_R^{-b_\chi(i)}$. Next if for two points $(i, b_\chi(i), (j, b_\chi(j))$ in $\mathrm{Graph}(b_\chi)$ we have $(i, b_\chi(i) <_\rho (j, b_\chi(j))$, it follows that the transformation $\theta_{i,j}$, introduced in the proof of Proposition 3.34, is filtered. Now, the only difference with that proof, is that the effect of applying $\theta_{i,j}$ is to erase the smaller point, namely $(i, b_\chi(i))$. Indeed the character $\chi \circ \theta_{i,j}$ will send to 0 all the factors S_a with $a \notin A_\chi$, and it will be 0, additionally also on S_i. On the other hand, on all the other factors S_a, with $a \in A_\chi - \{i\}$ it coincides with χ. Thus by repeatedly applying this type of transformation the sequence of filtered automorphism so produced converges to a filtered automorphism θ with $(A_{\chi\circ\theta}, b_{\chi\circ\theta}) = (A_\chi^+, b_\chi^+)$, concluding the proof. □

We now show that if (A_χ, b_χ) is a ρ-jump set (resp. an extended ρ-jump set), then, if viewed as a subset of $\mathbb{Z}_{\geqslant 1}$, it is the set of jumps of χ.

Proposition 4.4. *Let χ be a character of M_ρ^f (resp. of $M_\rho^{f-1} \oplus M_\rho^*$), such that (A_χ, b_χ) is a jump set (resp. an extended jump set). Then $J_\chi = J_{(A_\chi, b_\chi)}$.*

Proof. For a general χ we have the following formula

$$\mathrm{ord}(\chi(M_\rho^f)_i) = \max(\{b_\chi(j) - v_\rho(j,i)\}_{j \in T_\rho}),$$

where for $i \in \mathbb{Z}_{\geqslant 1}$ and $j \in T_\rho$ (resp. T_ρ^*) we have that $v_\rho(j,i) = \min(\{s \in \mathbb{Z}_{\geqslant 0} : \rho^s(j) \geqslant i\})$ (respectively we have the formula

$$\mathrm{ord}(\chi(M_\rho^f)_i) = \max(\{b_\chi(j) - v_\rho(j,i)\}_{j \in T_\rho^*})).$$

Since (A_χ, b_χ) is a jump set (resp. an extended jump set), it is visible from the definition that the right hand side, as a function of i, changes value precisely in the set $J_{(A_\chi, b_\chi)}$, which is precisely giving the desired identity $J_{(A_\chi, b_\chi)} = J_\chi$. □

So for two characters of M_ρ^f or $M_\rho^{f-1} \oplus M_\rho^*$ the equivalence relation "having the same set of jumps" and "being in the same filtered orbit" are precisely the same relation and one obtains the following fact.

Theorem 4.5. *Let ρ be a shift map, and let f be a positive integer. We have that $\mathscr{J}_{M_\rho^f} = \mathrm{Jump}_\rho$, and if T_ρ is finite, then $\mathscr{J}_{M_\rho^{f-1} \oplus M_\rho^*} = \mathrm{Jump}_\rho^*$.*

The similarity with Theorem 1.4 is noteworthy: in both cases jump sets parametrize orbits.

4.3. **Sets of jumps for a quasi-free module.** Let ρ be a shift map with T_ρ finite. Let f be a positive integer. Let $M_\bullet$ be a (f,ρ)-quasi-free module that is not free. Then from Theorem 3.38 we know that the knowledge of $M_\bullet$ as a filtered module is equivalent to the knowledge of the extended ρ-jump set $(I_{M_\bullet}, \beta_{M_\bullet})$. So the invariant $\mathscr{J}_{M_\bullet}$ is completely determined once we know $(I_{M_\bullet}, \beta_{M_\bullet})$. Here we explain how. We know from Proposition 3.31 that $M_\bullet$ admits a presentation $\varphi : M_\rho^{f-1} \oplus M_\rho^* \to M_\bullet$, with $\operatorname{coker}(F_i(\varphi)) = 0$ for every positive integer i, so from Proposition 3.11 we know that $\varphi_{|(M_\rho^{f-1}\oplus M_\rho^*)_i}$ is a map onto M_i for each positive integer i. It follows that given a character χ of $M_\bullet$, the induced character on $M_\rho^{f-1} \oplus M_\rho^*$ obtained by post-composition to φ, has the same set of jumps of χ. So together with Theorem 4.5 we obtain:

Proposition 4.6. *Let $M_\bullet$ be a (f,ρ)-quasi-free module. Then $\mathscr{J}_{M_\bullet} \subseteq \mathrm{Jump}_\rho^*$.*

Thus we see that to characterize which elements of Jump_ρ^* belongs to $\mathscr{J}_{M_\bullet}$ we need to see which jump sets are ruled out when on a character χ of $M_\rho^{f-1} \oplus M_\rho^*$ we impose the condition $\chi(v_{(I_{M_\bullet},\beta_{M_\bullet})}) = 0$. The following simple lemma will be relevant to this end. For $x \in Q(R)/R$ we denote by $\operatorname{ord}(x)$ the smallest non-negative integer n such that $\pi_R^n x = 0$. Equivalently we can say that $\operatorname{ord}(x)$ is the unique non-negative integer such that Rx is isomorphic to $R/\pi_R^n R$ as R-modules.

Lemma 4.7. *Let n be a positive integer and $(v_1,\dots,v_n) \in (Q(R)/R)^n$. Write $Y := \{i \in \{1,\dots,n\} : 0 < \operatorname{ord}(v_i), \operatorname{ord}(v_i) = \max\{\operatorname{ord}(v_j),\ j \in \{1,\dots,n\}\}\}$. Then the following hold:*
(a) *Assume $|R/m_R| \neq 2$. Then there exists a vector $(a_1,\dots,a_n) \in (R^*)^n$ such that $\sum_{i=1}^n a_i v_i = 0$ if and only if $|Y| \neq 1$.*
(b) *Assume $|R/m_R| = 2$. Then there exists a vector $(a_1,\dots,a_n) \in (R^*)^n$ such that $\sum_{i=1}^n a_i v_i = 0$ if and only if $|Y| \equiv 0$ mod 2.*

Proof. (a) Assume $|Y| \neq 1$. We can assume $|Y| \neq 0$ because otherwise $(v_1,\dots,v_n)$ is the zero vector and any $(a_1,\dots,a_n) \in (R^*)^n$ would prove the conclusion. Since $|R/m_R| \neq 2$ we can find $\lambda \in R^*$ such that $\lambda \not\equiv 1 \bmod m_R$. Now pick i,j distinct elements of Y, and observe that at least one of the following two hold:
1) $\operatorname{ord}(v_i) = \operatorname{ord}(v_j + \sum_{h\notin\{i,j\}} v_h)$.
2) $\operatorname{ord}(v_i) = \operatorname{ord}(\lambda v_j + \sum_{h\notin\{i,j\}} v_h)$.
In each case, 1) and 2), we can find $\mu \in R^*$ such that, respectively $\mu v_i = v_j + \sum_{h\notin\{i,j\}} v_h$, or $\mu v_i = \lambda v_j + \sum_{h\notin\{i,j\}} v_h$. In each of the two cases we obtain the desired conclusion. Conversely assume that there exists a vector $(a_1,\dots,a_n) \in (R^*)^n$ such that $\sum_{i=1}^n a_i v_i = 0$. Suppose that $|Y| = 1$, call k its unique element: then we have $\operatorname{ord}(v_k) = \operatorname{ord}(\sum_{i=1}^n a_i v_i) = 0$, contradicting the definition of Y.

(b) Assume $|Y| \equiv 0 \bmod 2$. We can assume $|Y| \neq 0$ because otherwise $(v_1,\dots,v_n)$ is the zero vector and any $(a_1,\dots,a_n) \in (R^*)^n$ would prove the conclusion. So pick $i \in Y$. Then observe that, since $|Y - \{i\}| \equiv 1 \bmod 2$ and $|R/m_R| = 2$, we have that $\operatorname{ord}(v_i) = \operatorname{ord}(\sum_{h\neq i} v_h)$. Thus, it follows that there exists $\mu \in R^*$ such that $\mu v_i = \sum_{h\neq i} v_h$, which is the desired conclusion. Conversely assume there exists a vector $(a_1,\dots,a_n) \in (R^*)^n$ such that $\sum_{i=1}^n a_i v_i = 0$. Suppose that $|Y| \equiv 1 \bmod 2$. Then pick $k \in Y$ and observe that, since $|R/m_R| = 2$, we have $\operatorname{ord}(v_k) = \operatorname{ord}(\sum_{i=1}^n a_i v_i) = 0$ contradicting the definition of Y. □

We can now give a criterion to decide if an extended jump set (I,β) is realizable as a set of jumps of a character of $M_\bullet$. Such a criterion consists in a combinatorial comparison

between (I,β) and $(I_{M_\bullet},\beta_{M_\bullet})$. The precise condition for (I,β) to be ruled out are conditions 2.1) and 2.2) of the following theorem (in case (a) and (b) respectively).

Theorem 4.8. *Let f be a positive integer and let ρ be a shift. Let $M_\bullet$ be a (f,ρ)-quasi-free filtered R-module that is not free. Let $(I,\beta)\in Jump^*_\rho$. Define* $\mathrm{Max}((I,\beta),(I_{M_\bullet},\beta_{M_\bullet})) := \{i\in I\cap I_{M_\bullet} : \beta(i)-\beta_{M_\bullet}(i)>0 \wedge \forall j\in I\cap I_{M_\bullet},\ \beta(i)-\beta_{M_\bullet}(i)\geqslant \beta(j)-\beta_{M_\bullet}(j)\}$. *In what follows we denote by* $\mathrm{Max} := \mathrm{Max}((I,\beta),(I_{M_\bullet},\beta_{M_\bullet}))$.

(a) *Suppose $|R/m_R|\neq 2$. Then one has that $(I,\beta)\notin \mathscr{J}_{M_\bullet}$ if and only if the following two conditions are satisfied:*
(a.1) $|\mathrm{Max}|=1$ *and if $f>1$ then* $\mathrm{Max}=\{e^*_\rho\}$.
(a.2) *Let j be the unique element of* $\mathrm{Max}_{M_\bullet}((I,\beta))$. *For every $i\in I_{M_\bullet}-I$, the point $(i,\beta(j)-\beta_{M_\bullet}(j)+\beta_{M_\bullet}(i))$ is maximal in* $\mathrm{Graph}(\beta)\cup\{(i,\beta(j)-\beta_{M_\bullet}(j)+\beta_{M_\bullet}(i))\}$, *with respect to the ordering $\leqslant_\rho$.*

(b) *Suppose $|R/m_R|=2$. Then $(I,\beta)\notin\mathscr{J}_{M_\bullet}$ if and only if the following two conditions are satisfied:*
(b.1) $|\mathrm{Max}|\equiv 1 \bmod 2$ *and if $f>1$ then* $\mathrm{Max}=\{e^*_\rho\}$.
(b.2) *Let j be any element of* Max. *For every $i\in I_{M_\bullet}-I$, the point $(i,\beta(j)-\beta_{M_\bullet}(j)+\beta(i))$ is maximal in* $\mathrm{Graph}(\beta)\cup\{(i,\beta(j)-\beta_{M_\bullet}(j)+\beta_{M_\bullet}(i))\}$, *with respect to the ordering $\leqslant_\rho$.*

Proof. (a) Denote by $\{b_{i,j} : i\in T_\rho,\ j\in\{1,\dots,f\}\}\cup\{b_{e^*_\rho,1}\}$ the standard filtered basis for $M_\rho^{f-1}\oplus M_\rho^*$). With this notation we have that

$$v_{(I_{M_\bullet},\beta_{M_\bullet})}=\sum_{i\in I}\pi_R^{\beta_{M_\bullet}(i)}b_{i,1}.$$

We divide the proof in 9 elementary steps.

1) We fix a presentation $\varphi : M_\rho^{f-1}\oplus M_\rho^*\to M_\bullet$ as in Proposition 3.31, with $\ker(\varphi)=Rv_{(I_{M_\bullet},\beta_{M_\bullet})}$ as in Theorem 3.38.

2) The task of realizing (I,β) from a character is equivalent to the task of finding a $\chi : M_\rho^{f-1}\oplus M_\rho^*\to Q(R)/R$ such that $(I_\chi,\beta_\chi)=(I,\beta)$, and $\sum_{i\in I_{M_\bullet}}\pi_R^{\beta_{M_\bullet}(i)}\chi(b_{i,1})=0$.

3) Suppose that $I\cap I_{M_\bullet}$ is either empty or that $\beta-\beta_{M_\bullet}$ does not assume a strictly positive maximum on $I\cap I_{M_\bullet}$. We claim that then task 2) is realizable. Indeed thanks to Lemma 4.7 part (a), we can find for each $i\in I\cap I_{M_\bullet}$ a unit $\varepsilon_i\in R^*$ with the property that

$$\sum_{i\in I\cap I_{M_\bullet}}\frac{\varepsilon_i}{\pi_R^{\beta(i)-\beta_{M_\bullet}(i)}}=0.$$

Therefore we can realize task 2) with the following character χ. For $i\in I\cap I_{M_\bullet}$ we put $\chi(b_{1,i}):=\frac{\varepsilon_i}{\pi_R^{\beta(i)}}$. For $i\in I-I_{M_\bullet}$ we put $\chi(b_{1,i}):=\frac{1}{\pi_R^{\beta(i)}}$. For any $(i,h)\in T_\rho\times\{1,\dots,f\}\cup\{e^*_\rho\}\times\{1\}$ with $i\notin I$ or $h>1$ we put $\chi(b_{i,h})=0$. With Proposition 4.4 we conclude immediately that $J_\chi=(I,\beta)$ and we are done. So we can assume that $I\cap I_{M_\bullet}$ is non-empty and that $\beta-\beta_{M_\bullet}$ assumes a positive maximum at a unique point of $I\cap I_{M_\bullet}$, which we shall call j.

4) Assume that $j\neq e^*_\rho$ and $f>1$. Then we proceed by distinguishing two cases.
4.1) There is no other $k\in I\cap I_{M_\bullet}$ different from j such that $\beta(k)-\beta_{M_\bullet}(k)>0$. Then we consider the following character χ. For each i in $I-\{e^*_\rho\}$ we put $\chi(b_{i,2})=\frac{1}{\pi_R^{\beta(i)}}$. If $e^*_\rho\in I$ we put $\chi(b_{e^*_\rho,1})=\frac{1}{\pi_R^{\beta(e^*_\rho)}}$. For all the other (i',h) in $T^*_\rho\times\{1,\dots,f\}$ we put $\chi(b_{i',h})=0$. We see

that since $f > 1$ and $j \neq e_\rho^*$ we trivially obtain

$$\sum_{i \in I_{M_\bullet}} \pi_R^{\beta_{M_\bullet}(i)} \chi(b_{i,1}) = 0.$$

Hence task 2) is accomplished thanks to Proposition 4.4. So we can assume that such a k exists.

4.2) Suppose that there exists $k' \in I \cap I_{M_\bullet}$ different from j such that $\beta(k') - \beta_{M_\bullet}(k') > 0$. Choose a k such that $\beta(k) - \beta_{M_\bullet}(k) \geqslant \beta(k') - \beta_{M_\bullet}(k')$ for each $k' \in I \cap I_{M_\bullet}$ with k' different from j. Next observe that thanks to Proposition 4.7 part (a), we can find for each $i \in I \cap I_{M_\bullet}$ a unit $\varepsilon_i \in R^*$ in such a way that

$$\sum_{i \in (I \cap I_{M_\bullet}) - \{j\}} \frac{\varepsilon_i}{\pi_R^{\beta(i) - \beta_{M_\bullet}(i)}} + \frac{\varepsilon_j}{\pi_R^{\beta(k) - \beta_{M_\bullet}(k)}} = 0.$$

Now we proceed constructing a character χ. We put $\chi(b_{j,1}) = \frac{\varepsilon_j}{\pi_R^{\beta(k) - \beta_{M_\bullet}(k) + \beta_{M_\bullet}(j)}}$ and $\chi(b_{j,2}) = \frac{1}{\pi_R^{\beta(j)}}$. For all $i \in (I \cap I_{M_\bullet}) - \{j\}$ we put $\chi(b_{i,1}) = \frac{\varepsilon_i}{\pi_R^{\beta(i)}}$. For all $i \in I - I_{M_\bullet}$ we put $\chi(b_{i,1}) = \frac{1}{\pi_R^{\beta(i)}}$. For all remaining vectors b of the basis we put $\chi(b) = 0$. Since $\beta(k) - \beta_{M_\bullet}(k) + \beta_{M_\bullet}(j) < \beta(j)$ we conclude by Proposition 4.3 and Proposition 4.4 that $J_\chi = (I, \beta)$. Moreover, by construction,

$$\sum_{i \in I_{M_\bullet}} \pi_R^{\beta_{M_\bullet}(i)} \chi(b_{i,1}) = 0.$$

Hence we have realized task 2) in this case as well.

5) Thanks to Step 1)–4) we can assume that $|\mathrm{Max}| = 1$, and that either $f = 1$ or $\mathrm{Max} = \{e_\rho^*\}$. Otherwise we have shown, in the previous steps, that we can accomplish task 2). Keep denoting by j the unique point of Max.

6) Assume there is $i' \in I_{M_\bullet} - I$ such that the point $(i', \beta(j) - \beta_{M_\bullet}(j) + \beta_{M_\bullet}(i'))$ is not maximal in $\mathrm{Graph}(\beta) \cup \{(i', \beta(j) - \beta_{M_\bullet}(j) + \beta_{M_\bullet}(i')\}$, with respect to the ordering $\leqslant_\rho$. Then we can accomplish task 2) constructing a character χ in the following manner. Observe that, thanks to Proposition 4.7 part (a), we can attach to each $i \in (I \cap I_{M_\bullet}) \cup \{i'\}$ a unit $\varepsilon_i \in R^*$ in such a way that

$$\sum_{i \in I \cap I_{M_\bullet}} \frac{\varepsilon_i}{\pi_R^{\beta(i) - \beta_{M_\bullet}}} + \frac{\varepsilon_{i'}}{\pi_R^{\beta(j) - \beta_{M_\bullet}(j)}} = 0.$$

For each $i \in I \cap I_{M_\bullet}$ put $\chi(b_{i,1}) = \frac{\varepsilon_i}{\pi_R^{\beta(i)}}$. Moreover put $\chi(b_{i',1}) = \frac{1}{\pi_R^{\beta(j) - \beta_{M_\bullet}(j) + \beta_{M_\bullet}(i')}}$ and $\chi(b_{i,1}) = \frac{1}{\pi_R^{\beta(i)}}$ for each $i \in I - I_{M_\bullet}$. By construction we obtain

$$\sum_{i \in I_{M_\bullet}} \pi_R^{\beta_{M_\bullet}(i)} \chi(b_{i,1}) = 0.$$

Finally the hypothesis that the point $(i', \beta(j) - \beta_{M_\bullet}(j) + \beta_{M_\bullet}(i'))$ is not larger, with respect to $\leqslant_\rho$, than some point in $\mathrm{Graph}(\beta)$, tells us, through Proposition 4.3 and Proposition 4.4, that $J_\chi = (I, \beta)$.

7) Steps 1)–6) prove that if (a.1) and (a.2) are not both satisfied then $(I, \beta) \in \mathscr{J}_{M_\bullet}$. We next proceed proving the converse implication.

8) Observe that if a set $A \subseteq \mathbb{Z}^2$ is given, together with a point $(x, y) \in A$ that is maximal in A with respect to $\leqslant_\rho$, then any point of the form $(x, \tilde{y})$ with $\tilde{y} \geqslant y$ is maximal in A, with respect to $\leqslant_\rho$.

9) Suppose (a.1) and (a.2) both hold. Denote by j the unique element of Max. Let χ be a character of $M_\rho^{f-1} \oplus M_\rho^*$ with $J_\chi = (I, \beta)$. We shall prove that

$$\sum_{i \in I} \pi_R^{\beta_{M_\bullet}(i)} \chi(b_{i,1}) \neq 0.$$

We proceed by contradiction. Suppose that $\sum_{i \in I} \pi_R^{\beta_{M_\bullet}(i)} \chi(b_{i,1}) = 0$. By Proposition 4.3 and Proposition 4.4 we have that $\mathrm{ord}(\chi(b_{j,1})) = \beta(j)$: this is clear for $f = 1$ and if $f \geqslant 2$ we are using that in this case j must be e_ρ^*. Next using Lemma 4.7 part (a), we see that at least one $i \in I_{M_\bullet} - \{j\}$ must satisfy $\mathrm{ord}(\chi(b_{i,1})) \geqslant \beta_{M_\bullet}(i) + \beta(j) - \beta_{M_\bullet}(j)$. Such an i cannot be in I. Indeed in that case we would conclude by Proposition 4.3 and Proposition 4.4 that $J_\chi \neq (I, \beta)$ since we would have $\beta(i) \geqslant \beta_{M_\bullet}(i) + \beta(j) - \beta_{M_\bullet}(j)$, which would contradict the defining property of Max. Hence it must be that $i \in I_{M_\bullet} - I$. But then Step 8) together with assumption (a.2) and Proposition 4.3 and Proposition 4.4 imply again that χ does not belong to the orbit of characters χ' having $J_{\chi'} = (I, \beta)$. This ends the proof.

Statement (b) can be proved by the same 9 steps of part (a) of this proof, replacing each time, part (a) of Lemma 4.7 with part (b) of Lemma 4.7. □

5. U_1 as a filtered module

In this section we apply the results of Section 3 to classify the possible structures of $U_\bullet$ as a filtered $\mathbb{Z}_p$-module. Let p be a prime number and let e be in $(p-1)\mathbb{Z}_{\geqslant 1} \cup \{\infty\}$. Recall the definition of $\rho_{e,p}$ from Example 2.1.

Let K be a local field with residue characteristic p. Denote by f_K the residue degree, $f_K = [O_K/m_K : \mathbb{F}_p]$. Denote by $\rho_K := \rho_{e_K,p}$. Recall that $e^*_{\rho_K} = \frac{pe_K}{p-1}$ and $e'_{\rho_K} = \frac{e_K}{p-1}$.

Proposition 5.1. *One has that $U_\bullet(K)$ is a (f_K, ρ_K)-quasi-free filtered $\mathbb{Z}_p$-module.*

Proof. Firstly one has that $U_i/U_{i+1} \simeq_{\mathrm{ab.gr.}} O/m$, which gives for every positive integer i that $f_i(U_\bullet(K)) = f_K$ (for a definition of $f_i(U_\bullet(K))$ see 3.19). Observe that the formula $(1+x)^p = 1 + px + \ldots + x^p$ implies that given $u \in U_i(K)$ then $u^p \in U_{\rho_K(i)}$. Moreover if $u \in U_i(K) - U_{i+1}(K)$ and $u^p \in U_{\rho_K(i)+1}$, then $pi = i + e_K$, which implies that $i = e'_{\rho_K}$. So we have firstly that $\rho_{U_\bullet(K)} \geqslant \rho_K$ (for a definition of $\rho_{U_\bullet(K)}$ see subsection 3.3.1), which means that $U_\bullet(K)$ is a ρ_K-filtered-$\mathbb{Z}_p$-module (see subsection 3.3.2), and secondly that $\mathrm{defect}_{U_\bullet(K)}(i) = \mathrm{codefect}_{U_\bullet(K)}(i) = 0$ for every positive integer $i \neq e'_{\rho_K}$ (for a definition of $\mathrm{defect}_{U_\bullet(K)}(i)$ and $\mathrm{codefect}_{U_\bullet(K)}(i)$, see 3.19). On the other hand we know that $\mu_p(U_1(K))$ is a cyclic group. Thus we conclude by Proposition 3.29. □

Therefore we deduce the following.

Theorem 5.2. *One has that $U_\bullet(K)$ is a free (f_K, ρ_K)-filtered module if and only if $\mu_p(K) = \{1\}$. In other words, $U_\bullet(K) \simeq_{\mathrm{filt}} M_{\rho_K}^{f_K}$ if and only if $\mu_p(K) = \{1\}$.*

Proof. This follows immediately from Proposition 3.25, Proposition 3.29 and Corollary 3.30 combined. □

If instead $\mu_p(K) \neq \{1\}$ the following holds.

Theorem 5.3. *Let K be a local field with $\mu_p(K) \neq \{1\}$. Then there is a* unique *$(I_K, \beta_K) \in \mathrm{Jump}^*_{\rho_K}$ such that*

$$U_1 \simeq M_{\rho_K}^{f_K - 1} \oplus (M^*_{\rho_K}/\mathbb{Z}_p v_{(I_K,\beta_K)})$$

as filtered $\mathbb{Z}_p$-module.

Proof. This follows immediately from Proposition 5.1 and Theorem 3.38 combined. □

We now fix $e_K = e$, and therefore we have $\rho_K = \rho_{e,p}$. Fix as well $f_K = f$. Our next goal is to show that every $(\rho_{e,p}, f)$-quasi-free filtered module can be realized as $U_\bullet(K)$ for some K, a totally ramified degree $\frac{e}{p-1}$ extension of $\mathbb{Q}_{p^f}(\zeta_p)$. In view of Theorem 3.38, this is tantamount to prove that every jump set realizable from a filtered module can be realized by a local field. Recall from Theorem 3.38 that the latter are precisely the admissible extended $\rho_{e,p}$-jump sets. For a definition of these jump sets see the discussion immediately before Theorem 3.38.

Theorem 5.4. *Let (I, β) be an extended admissible $\rho_{e,p}$-jump set. Then there is a totally ramified extension $K/\mathbb{Q}_{p^f}(\zeta_p)$ with $e_K = e$ and with*

$$(I_K, \beta_K) = (I, \beta).$$

During the proof we will make use of the two propositions that follow below. Recall that if $\zeta_p \in K$, then the extension $L/K := K(\sqrt[p]{U_{\frac{pe_K}{p-1}}/U_{\frac{pe_K}{p-1}+1}})/K$ is the unique unramified extension of degree p of K. Indeed $[L : K] = p$, so if $e_{L/K} > 1$ then $e_{L/K} = p$. Observe that the inclusion $U_{pe_K}(K) \subseteq U_{pe_L}(L)$ would, in case that $e_{L/K} = p$, induce an isomorphism $U_{\frac{pe_K}{p-1}}(K)/U_{\frac{pe_K}{p-1}+1}(K) \to U_{\frac{pe_L}{p-1}}(L)/U_{\frac{pe_L}{p-1}+1}(L)$, which, by construction would imply that $\mathrm{codefect}_{U_\bullet(L)}(e'_L) = 0$, which is impossible since $\zeta_p \in L$. So it must be that $e_{L/K} = 1$ and $f_{L/K} = [L : K]$.

Proposition 5.5. *Let K be a finite extension of $\mathbb{Q}_p(\zeta_p)$. Then $e^*_K \in I_K$ if and only if $K(\sqrt[p]{\mu_{p^\infty}(K)})/K$ is unramified.*

Proof. Let ζ_{p^j} be a generator of $U_1(K)_{\mathrm{tors}}$. Thanks to Proposition 3.39, we have that $e^*_K \in I_K$ if and only if $w_{U_1(K)/U_1(K)^p}(\zeta_{p^j}) = \frac{pe_K}{p-1}$. On the other hand this is equivalent to $K(\zeta_{p^{j+1}}) = K(\sqrt[p]{U_{\frac{pe_K}{p-1}}/U_{\frac{pe_K}{p-1}+1}})$, which, as explained just above this proposition, is the unique unramified degree p extension of K. □

Let j be a positive integer. The following notation will be helpful. Consider the compositum extension $\mathbb{Q}_{p^{pf}}(\zeta_{p^j}) \cdot \mathbb{Q}_{p^f}(\zeta_{p^{j+1}})/\mathbb{Q}_{p^f}(\zeta_{p^j})$, which is a Galois extension with Galois group $C_p \times C_p$. So one is provided with $p + 1$ degree p sub-extensions. We denote the unique unramified one as $\mathbb{Q}_{p^f}(\zeta_{p^j})(0)$ (which of course is just $\mathbb{Q}_{p^{pf}}(\zeta_{p^j})$). Further we list the $p - 1$ totally ramified ones without an element of order p^{j+1} as $\mathbb{Q}_{p^f}(\zeta_{p^j})(i)$ with i running through $\{1, \ldots, p-1\}$. And we will sometimes make use of an extended notation for $i = p$, by letting $\mathbb{Q}_{p^f}(\zeta_{p^j})(p) := \mathbb{Q}_{p^f}(\zeta_{p^{j+1}})$.

Proposition 5.6. *Let j be a positive integer. Let K be a totally ramified extension of $\mathbb{Q}_{p^f}(\zeta_p)$ with $e_K =: e$. Then the following are equivalent:*
(1) *$e^* \in I_K$ and $\beta_K(e^*) = j$.*
(2) *There is exactly one $i \in \{1, \ldots, p-1\}$ such that K contains $\mathbb{Q}_{p^f}(\zeta_{p^j})(i)$.*

Proof. (1) → (2) Thanks to Proposition 5.5, we have that (1) implies that $K(\zeta_{p^{j+1}})/K$ is unramified, thus we have that $K(\zeta_{p^{j+1}})/\mathbb{Q}_{p^f}(\zeta_{p^j})$ contains $\mathbb{Q}_{p^f}(\zeta_{p^{j+1}}) \cdot \mathbb{Q}_{p^{pf}}(\zeta_{p^j})$. But this last one must then intersect K non-trivially, otherwise one would have $[K(\zeta_{p^{j+1}}) : K] = p^2$, which is impossible. At the same time the intersection cannot be $\mathbb{Q}_{p^{pf}}(\zeta_{p^j})$ because $f_K = f$, and it cannot be $\mathbb{Q}_{p^f}(\zeta_{p^{j+1}})$. Indeed we have $\beta_K(e^*) = j$ and Proposition 3.42 implies that $p^j = \#\mu_{p^\infty}(K)$. So there must be an $i \in \{1, \ldots, p-1\}$ such that K contains $\mathbb{Q}_{p^f}(\zeta_{p^j})(i)$. But

there must be exactly one since otherwise the whole extension $\mathbb{Q}_{p^f}(\zeta_{p^{j+1}}) \cdot \mathbb{Q}_{p^{pf}}(\zeta_{p^j})$ would be in K, which has been already explained to be not possible.

(2) $\to$ (1) We have that $K(\sqrt[p]{U_1(K)_{\mathrm{tors}}})/K$ contains $\mathbb{Q}_{p^f}(\zeta_{p^j})(i)(\zeta_{p^{j+1}}) \supset \mathbb{Q}_{p^{pf}}$, thus one concludes that $K(\sqrt[p]{U_1(K)_{\mathrm{tors}}})/K$ is unramified and by Proposition 5.5 one concludes that $e^* \in I_K$. Moreover we must have that $\beta_K(e^*) = j$. Indeed K contains in particular ζ_{p^j}, which, by Proposition 3.42, implies that $\beta_K(e^*) \geqslant j$. If we would have $\beta_K(e^*) > j$ then, still by Proposition 3.42, the field K would contain also $\mathbb{Q}_{p^f}(\zeta_{p^{j+1}})$. Hence K would contain the compositum of $\mathbb{Q}_{p^f}(\zeta_{p^{j+1}})$ and $\mathbb{Q}_{p^f}(\zeta_{p^j})(i)$. Therefore K would contain the field $\mathbb{Q}_{p^{pf}}$ providing a contradiction with $f_K = f$. Hence, since $\beta_K(e^*) \geqslant j$ and $\beta_K(e^*) < j+1$, it must be that $\beta_K(e^*) = j$. □

In particular we derive the following:

Corollary 5.7. *Let j, f be positive integers, and $i \in \{1, \dots, p-1\}$. Then*

$$I_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)} = \{1, p^{j+1}\},\ \beta_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}(1) = j+1 \text{ and } \beta_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}(p^{j+1}) = j.$$

Proof. Since the jump set must be admissible, we know that $1 \in I_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}$ with $\beta_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}(1) = j+1$. By Proposition 5.5, we know that $p^{j+1} \in I_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}$ with $\beta_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}(p^{j+1}) = j$. Moreover we certainly have that $1 = \min(I_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)})$ and $p^{j+1} = \max(I_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)})$ since 1 and p^{j+1} are respectively the smallest and the largest elements of T^*_ρ, for $\rho := \rho_{e,p}$ with $e := p^j(p-1)$. Moreover the very beginning of this proof gives us in particular that $\beta_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}(1) - \beta_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}(p^{j+1}) = 1$. Therefore, recalling that the map β is strictly decreasing (by definition of a jump set), we must conclude that between 1 and p^{j+1} no other value of $I_{\mathbb{Q}_{p^f}(\zeta_{p^j})(i)}$ can be found. This gives us the desired conclusion. □

Now we can proceed proving Theorem 5.4. Take (I, β) an extended admissible $\rho_{e,p}$-jump set. We distinguish two cases, depending on whether $e^* \in I$. First assume that $e^* \notin I$. Next define the polynomial

$$G(x) := \prod_{i \in I} (1 + x^i)^{p^{\beta(i)-1}} - \zeta_p \in \mathbb{Q}_{p^f}(\zeta_p)[x].$$

Using the fact that (I, β) is admissible (for a definition see immediately before the statement of Theorem 3.38) one finds that the Newton polygon of $G(x)$ consists of the segment connecting $(0,1)$ and $(\frac{e}{p-1}, 0)$ continued with a horizontal segment starting from $(\frac{e}{p-1}, 0)$. Therefore there exists a degree $\frac{e}{p-1}$ Eisenstein polynomial $g(x) \in \mathbb{Q}_{p^f}(\zeta_p)$, such that $g(x)$ divides $G(x)$. Define

$$K := \mathbb{Q}_{p^f}(\zeta_p)[x]/g(x).$$

Clearly $\pi := x$ is a uniformizer in K. Moreover we have that

$$\prod_{i \in I} (1 + \pi^i)^{p^{\beta(i)}} = 1$$

with $\mathrm{v}_K((1+\pi^i) - 1) = i$, thus giving

$$(I_K, \beta_K) = (I, \beta),$$

thanks to Corollary 3.41. Now suppose that $e^* \in I$ and write $j := \beta(e^*)$. We prove that $p^j(p-1) | e$. Indeed we have that $\min(I) < e^*$ giving that $\beta(\min(I)) \geqslant j+1$. Thus, since

we have that $\rho^{\beta(\min(I))}(\min(I)) = p^{\beta(\min(I))}(\min(I)) = \frac{pe}{p-1}$, we obtain that $p^j(p-1)|e$. Next, pick $u_1, u_2 \in \mathbb{Q}_{p^f}(\zeta_{p^j})(1)$ such that

$$\mathrm{v}_{\mathbb{Q}_{p^f}(\zeta_{p^j})(1)}(u_1 - 1) = 1,\ \mathrm{v}_{\mathbb{Q}_{p^f}(\zeta_{p^j})(1)}(u_2 - 1) = p^{j+1},\ u_2 \notin (\mathbb{Q}_{p^f}(\zeta_{p^j})(1))^{*p}$$

and

$$u_1^{p^{j+1}} u_2^{p^j} = 1$$

as guaranteed by Corollary 5.7. Now define

$$G^*(x) := \prod_{i \in I, i < e^*} (1 + x^i)^{p^{\beta(i)-j-1}} - u_1 \in \mathbb{Q}_{p^f}(\zeta_{p^j})(1)[x].$$

Using the fact that (I, β) is admissible one finds that the Newton polygon of $G^*(x)$ consists of the segment connecting $(0, 1)$ and $(\frac{e}{p^j(p-1)}, 0)$ continued with a horizontal segment starting from $(\frac{e}{p^j(p-1)}, 0)$. Therefore there exists a degree $\frac{e}{p^j(p-1)}$ Eisenstein polynomial $g^*(x) \in \mathbb{Q}_{p^f}(\zeta_{p^j})(1)[x]$ such that $g^*(x)$ divides $G^*(x)$. Define

$$\tilde{K} := \mathbb{Q}_{p^f}(\zeta_{p^j})(1)[x]/g^*(x).$$

Clearly $\pi := x$ is a uniformizer in $\tilde{K}$. Moreover we have that

$$(\prod_{i \in I, i < e^*} (1 + \pi^i)^{p^{\beta(i)}}) u_2^{p^j} = 1$$

with $\mathrm{v}_{\tilde{K}}((1 + \pi^i) - 1) = i$ for each $i \in I$, with $i < e^*$ and with $\mathrm{v}_{\tilde{K}}(u_2 - 1) = e^*$. Thus, in order to apply Corollary 3.41, we are only left with checking that $u_2 \notin \tilde{K}^{*p}$. But this follows at once from the fact that $\mathbb{Q}_{p^{pf}} \subseteq \mathbb{Q}_{p^f}(\zeta_{p^j})(1)(\sqrt[p]{u_2})$ and the fact that $g^*(x)$ is an Eisenstein polynomial and thus $\tilde{K}/\mathbb{Q}_{p^f}(\zeta_{p^j})(1)$ is totally ramified. This ends the proof of Theorem 5.4 and therefore of Theorem 1.6 in the Introduction.

6. Upper jumps of cyclic extensions

In this section we use Theorem 4.8, together with Theorem 5.1, to establish Theorem 6.2, a classification in terms of jump sets for the possible sets of upper jumps of a cyclic wild extension of a local field K. We next prove combinatorially that the classification obtained is equivalent to that obtained by Miki [6], Maus [5] and Sueyoshi [11]: in this way those results are *deduced* from Theorem 6.2. Finally we give a sense of how in practice the classification of Theorem 6.2 may look, by examining it for several possible values of the triple $((I, \beta), f, p)$, and in particular we do so for the most typical occurrences of (I, β) in the sense of Theorem 1.7. We also show that for $K/\mathbb{Q}_p(\zeta_p)$ totally ramified, the knowledge of the filtered $\mathbb{Z}_p$-module $U_\bullet(K)$ is equivalent to the knowledge of all possible sets of upper jumps of cyclic wild totally ramified extensions of K (see Corollary 6.12).

6.1. **Classification of possible sets of jumps.** In the rest of the section K will denote as usual a local field of residue characteristic a prime number denoted by p. We fix K^{sep} a separable closure of K and we denote by $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ the absolute Galois group of K. Let H be a normal closed subgroup of G_K. Recall that for every $\alpha \in \mathbb{R}_{\geqslant 0}$ the Galois group G_K/H is provided with a subgroup $(G_K/H)^\alpha$ via the so-called upper ramification filtration (see [9]). Let L/K be a finite cyclic totally ramified extension of K, with degree a power of p. Denote by G the Galois group $\mathrm{Gal}(L/K)$. A number $\alpha \in \mathbb{R}_{\geqslant 0}$ is said to be an *upper jump* for L/K if $G^\alpha \supsetneq G^{\alpha+\varepsilon}$ for each $\varepsilon > 0$. We denote by $J(L/K)$ the set of upper

jumps for L/K. From the Hasse–Arf Theorem (see [9]) we have that $J(L/K) \subset \mathbb{Z}_{\geqslant 1}$. We denote by $\mathscr{J}_K$ the collection of all such subsets of $\mathbb{Z}_{\geqslant 1}$ as L varies among all cyclic, p-power, totally ramified extensions of K. The set $\mathscr{J}_K$ can be also described as follows. We consider all totally ramified continuous homomorphisms

$$\chi : G_K \to \mathbb{Q}_p/\mathbb{Z}_p,$$

where χ is said to be totally ramified if the corresponding field extension is totally ramified. The set of upper jumps for χ are the $\alpha \in \mathbb{R}_{\geqslant 0}$ such that $\chi(G_K^{\alpha}) \neq \chi(G_K^{\alpha+\varepsilon})$ for all $\varepsilon > 0$. This set is denoted by J_χ. One has that $J_\chi = J((K^{\mathrm{sep}})^{\ker(\chi)}/K)$, so that $\mathscr{J}_K$ consists of the collection of all J_χ as χ varies among continuous totally ramified characters $\chi : G_K \to \mathbb{Q}_p/\mathbb{Z}_p$. Of course the set of such continuous totally characters $\chi : G_K \to \mathbb{Q}_p/\mathbb{Z}_p$ can be equivalently described as the set of all $\chi : G_K^{\mathrm{ab}} \to \mathbb{Q}_p/\mathbb{Z}_p$ continuous totally ramified. Finally it is not difficult to see that $\mathscr{J}_K$ is also the collection of all J_χ for all continuous homomorphisms $\chi : (G_K^{\mathrm{ab}})^1 \to \mathbb{Q}_p/\mathbb{Z}_p$. On the other hand $(G_K^{\mathrm{ab}})^1 \simeq_{\mathbb{Z}_p\text{-filt}} U_\bullet(K)$ via the Artin local reciprocity law. Therefore we see that the definition of $\mathscr{J}_K$ given in this section is equivalent to the one given in the introduction: we have $\mathscr{J}_K = \mathscr{J}_{U_\bullet(K)}$, where the right hand side is defined at the beginning of Section 4. Therefore we are in a position to apply the results of Section 4, notably Theorem 4.8. To make the statements simpler we first make a definition. Let ρ denote a general shift with T_ρ finite, f a positive integer, and p a prime number. Let moreover (I, β), (I', β') be in Jump_ρ^*.

Definition 6.1. We say that (I, β) is $((I', \beta'), f, p)$-incompatible if the following conditions hold.

(1) The set $I \cap I'$ is non-empty. Moreover the subset $\mathrm{Max}((I, \beta), (I', \beta'))$ of $I \cap I'$ consisting of those i in $I \cap I'$ where $\beta(i) - \beta'(i)$ is strictly positive and assumes the maximal possible value, which we denote by c, has precisely one element if $p > 2$ and an odd number of elements if $p = 2$.

(2) If $f > 1$ then $\mathrm{Max}((I, \beta), (I', \beta')) = \{e_\rho^*\}$.

(3) Given any $i \in I' - I$, there is no $j \in I$ such that $(j, \beta'(j)) \geqslant_\rho (i, c + \beta'(i))$.

We say that (I, β) is $((I', \beta'), f, p)$-compatible if it is not $((I', \beta'), f, p)$-incompatible.

Combining Theorem 4.5 and Theorem 4.8 together with Theorem 5.1 we obtain the following.

Theorem 6.2. *Suppose that $\mu_p(K) = \{1\}$. Then $\mathscr{J}_K = \mathrm{Jump}_{\rho_K}$. Suppose that $\mu_p(K) \neq \{1\}$. Then $\mathscr{J}_K$ consists precisely of the elements of $\mathrm{Jump}_{\rho_K}^*$ that are $((I_K, \beta_K), f_K, p)$-compatible.*

We conclude this subsection by proving that the notion of $((I', \beta'), f, p)$-incompatibility is equivalent to a slightly simpler criterion. This is given by the next proposition, which will be repeatedly applied in the next subsection. We make first the following definition.

Definition 6.3. Let a be a positive integer and let (I, β) be an extended ρ-jump set with $I \neq \varnothing$. Suppose that $a \geqslant \min(I)$, then we denote by $\lfloor a \rfloor_I$ the largest element i of I such that $i \leqslant a$. Suppose that $a \leqslant \max(I)$, then we denote by $\lceil a \rceil_I$ the smallest element i of I such that $a \leqslant i$.

Let now (I, β) and (I', β') be two extended ρ-jump sets.

Proposition 6.4. *The jump set (I, β) is $((I', \beta'), f, p)$-incompatible if and only if the following holds.*

(a) *Conditions* (1) *and* (2) *from definition 6.1 hold. If that is the case, let* $c(I, I') := \beta(i_0) - \beta'(i_0)$ *for any* $i_0 \in \mathrm{Max}((I, \beta), (I', \beta'))$.

(b) *For every point* $i \in I' - \mathrm{Max}((I, \beta), (I', \beta'))$*, we have that*

$$\beta'(i) + c(I, I') > \beta(\lceil i \rceil_I),$$

whenever $i \geqslant \min(I)$ *and*

$$\rho^{\beta'(i)+c(I,I')}(i) > \rho^{\beta(\lfloor i \rfloor_I)}(\lfloor i \rfloor_I),$$

whenever $i \leqslant \max(I)$.

Proof. This follows immediately by noticing that condition (3) of definition 6.1, requires only the comparisons with $\lfloor i \rfloor_I$ and $\lceil i \rceil_I$, as soon as they are defined, since the two inequalities in part (b) of the present statement must certainly hold, but they trivially imply all the others since $j \mapsto \beta(j)$ is strictly decreasing and $j \mapsto \rho^{\beta(j)}(j)$ is strictly increasing, by definition of a jump set. □

6.2. **Comparison with Miki-Maus-Sueyoshi.** In this subsection we give a direct combinatorial verification that Theorem 6.2 and the main Theorem of [5] are indeed classifying precisely the same sets. Of course this follows also from applying both theorems, but both criteria being of a purely combinatorial form, it is natural to provide a combinatorial proof of their equivalence, not relying on local fields. As an upshot we can *deduce* Miki's classification from Theorem 6.2 and the bit extra of combinatorial work of this subsection. Moreover the combinatorial nature of the equivalence between the two classification is highlighted from the fact that it follows from a statement about a general shift, see Proposition 6.7. Recall indeed that the case discussed in the present section is only a very special case of the classification we provide Theorem 4.8, which is about a general (f, ρ)-quasi-free R-module (see Definition 3.27), where R is any complete DVR, f is any positive integer and ρ is a general shift. In the case $\mu_p(K) = \{1\}$ the two descriptions are literally equal. So we pass to examine the case $\mu_p(K) \neq \{1\}$, where both Theorems say that $\mathscr{J}_K \subseteq \mathrm{Jump}^*_{\rho_K}$ and they both provide a criterion for an element of $\mathrm{Jump}^*_{\rho_K}$ to be realizable as the set of jumps of a character. In the case of Theorem 6.2, this is precisely the notion of being $((I_K, \beta_K), f_K, p)$-compatible. For the convenience of the reader we recap the formulation of Miki's criterion as stated in [11] in terms of a general definition, valid for any shift ρ with T_ρ finite. As usual, let p denote a prime number and f a positive integer. Let moreover (I, β) and (I', β') be in Jump^*_ρ, with both I, I' being non-empty.

Definition 6.5. We say that (I, β) is $((I', \beta'), f, p)$-inadequate if the following holds. Write $J_{(I,\beta)} = \{t_1, \ldots, t_m\}$ and $J_{(I',\beta')} = \{\lambda_1, \ldots, \lambda_l\}$ (see immediately above Proposition 2.3 for the notation $J_{(I',\beta')}$) with $\{t_i\}_{1 \leqslant i \leqslant m}$ and $\{\lambda_i\}_{1 \leqslant i \leqslant l}$ written in increasing order. Write $s = \beta'(\max(I'))$. Then there is a positive integer L with $L < m - (s-1)$ such that the sequences $\{x_i\}_{0 \leqslant i < l-(s-1)}, \{y_i\}_{0 \leqslant i < l-(s-1)}$ defined as $x_i := t_{L-i}, y_i := \lambda_{l-i-(s-1)}$, with $x_i = 0$ when $L \leqslant i$, satisfy the following condition. Whenever $y_i \in I'$, then $x_i \leqslant y_i$, with equality occurring, among these inequalities, precisely once if $p > 2$, and an odd number of times if $p = 2$. Moreover, in case $f > 2$, equality occurs precisely once, for all p, and it occurs for $i = 0$ with $x_0 = y_0 = e^*_\rho \in I \cap I'$ (i.e. $x_1, y_1 < e'_\rho$). Recall that $e^*_\rho = \max(T_\rho) + 1$ and that e'_ρ is the unique positive integer such that $\rho(e'_\rho) = e^*_\rho$.

We say that (I, β) is $((I', \beta'), f, p)$-adequate if it is not $((I', \beta'), f, p)$-inadequate.

Remark 6.6. In [11], the final condition requires only that $x_1 < e_\rho^{'}$ (i.e. that $e_\rho^* \in I$) because in that case (I', β') is admissible (since it is the jump set of a local field, see definition right after Theorem 1.6), so the condition $y_0 = e_\rho^*$, which is equivalent to $e_\rho^* \in J_{(I',\beta')}$, is actually equivalent to $e_\rho^* \in I'$.

We next furnish a direct combinatorial proof that incompatibility and inadequacy are the same notion.

Proposition 6.7. *Let ρ be a shift with finite T_ρ, let p be a prime number and f a positive integer. Let (I, β) and (I', β') be in Jump_ρ^*. Then (I, β) is $((I', \beta'), f, p)$-inadequate if and only if it is $((I', \beta'), f, p)$-incompatible.*

Proof. Suppose that (I, β) is $((I', \beta'), f, p)$-inadequate. Let $L < m - (s-1)$ and the two sequences $\{x_i\}_{0 \leqslant i \leqslant l-(s-1)}, \{y_i\}_{0 \leqslant i \leqslant l-(s-1)}$ be as in definition 6.5. Let M be the set of non-negative integers i_0, with $i_0 \leqslant l - (s-1)$, $y_{i_0} \in I'$ and $x_{i_0} = y_{i_0}$: the size of M must be, by definition, equal to 1 if $p > 2$, and odd if $p = 2$. We claim that $\{y_i\}_{i \in M} = \mathrm{Max}((I, \beta), (I', \beta'))$ (for a definition of $\mathrm{Max}((I, \beta), (I', \beta'))$ see Theorem 4.8). We know that, in either case, M is non-empty. Let i_0 be one of its elements. Firstly, from the fact that $L < m - (s-1)$ we deduce precisely that the set $J_{(I,\beta)} \cap \lceil y_{i_0}, \infty)$ has strictly more elements than $J_{(I',\beta')} \cap \lceil y_{i_0}, \infty)$. In other words $y_{i_0} \in I \cap I'$ with $\beta(y_{i_0}) - \beta'(y_{i_0}) > 0$. Next let $0 \leqslant i \leqslant l - (s-1)$ be any other index such that $y_i \in I \cap I'$. Assume $y_i > y_{i_0}$, i.e. that $i < i_0$. From the fact that $x_i \leqslant y_i$, we conclude that in the interval $[y_{i_0}, y_i]$ there are at least as many points of $J_{(I,\beta)}$ as there are points of $J_{(I',\beta')}$, which amounts to $\beta(y_{i_0}) - \beta(y_i) \geqslant \beta'(y_{i_0}) - \beta'(y_i)$, which can be rewritten as $\beta(y_{i_0}) - \beta'(y_{i_0}) \geqslant \beta(y_i) - \beta'(y_i)$, with equality iff $i \in M$. A completely analogous reasoning in the case $i > i_0$ brings us to the same conclusion. In other words we have just shown that $y_{i_0} \in \mathrm{Max}((I, \beta), (I', \beta'))$ and all other $i \in M$ are precisely the i such that $y_i \in \mathrm{Max}((I, \beta), (I', \beta'))$. Therefore we conclude by the very definition of inadequacy that conditions $(1) - (2)$ of definition 6.1 hold. We are left with proving condition (3). Let i_1 be an index such that $y_{i_1} \in I' - I$. Take $i_0 \in M$, and suppose $i_1 < i_0$. Since $|J_{(I,\beta)} \cap [y_{i_0}, x_{i_1}]| = |J_{(I',\beta')} \cap [y_{i_0}, y_{i_1}]|$, we have that $\beta(y_{i_0}) - \beta(\lceil y_{i_1} \rfloor_I) > \beta'(y_{i_0}) - \beta'(y_{i_1})$, which can be rewritten as $c + \beta'(y_{i_1}) > \beta(\lceil y_{i_1} \rfloor_I)$. This last inequality is precisely the first of the two inequalities in Proposition 6.4. Next, always assuming $i_1 < i_0$, consider the two possible cases: $x_{i_1} < \lfloor y_{i_1} \rfloor_I$ or $\lfloor y_{i_1} \rfloor_I \leqslant x_{i_1} < \lceil y_{i_1} \rfloor_I$. In the first case observe that $\beta(y_{i_0}) - \beta(\lfloor y_{i_1} \rfloor_I) > \beta'(y_{i_0}) - \beta'(y_{i_1})$, which can be recast as $c + \beta'(y_{i_1}) > \beta(\lfloor y_{i_1} \rfloor_I)$. This last inequality trivially implies that $\rho^{c+\beta'(y_{i_1})}(y_{i_1}) > \rho^{\beta(\lfloor y_{i_1} \rfloor_I)}(\lfloor y_{i_1} \rfloor_I)$, since ρ is strictly increasing. So in the first case one, trivially, obtains the second inequality of Proposition 6.4. In the second case observe that $(\beta'(y_{i_0}) - \beta'(y_{i_1})) - (\beta(x_{i_0}) - \beta(\lfloor y_{i_1} \rfloor_I)) = v_\rho(x_{i_0})$, i.e. $\rho^{\beta'(y_{i_0}) - \beta'(y_{i_1})) - (\beta(y_{i_0}) - \beta(\lfloor y_{i_1} \rfloor_I)}(\lfloor y_{i_1} \rfloor_I) = x_{i_1} < y_{i_1}$, which can be rewritten as $\rho^{\beta(\lfloor y_{i_1} \rfloor_I)}(\lfloor y_{i_1} \rfloor_I) < \rho^{c+\beta'(y_{i_1})}(y_{i_1})$. This last inequality is precisely the second inequality in Proposition 6.4. The case $i_1 > i_0$ can be treated in the same way. Altogether this proves that (I, β) is $((I', \beta'), f, p)$-incompatible.

The proof of the converse implication proceeds analogously, and basically it can be obtained by inverting the above arguments. □

From Proposition 6.7 we can infer the main Theorem in [11].

Theorem 6.8. *(Miki's Theorem) Suppose that $\mu_p(K) \neq \{1\}$. Then $\mathscr{J}_K$ consists precisely of the elements of $\mathrm{Jump}_{\rho_K}^*$ that are $((I_K, \beta_K), f_K, p)$-adequate.*

Proof. This follows immediately from Theorem 6.2 and Proposition 6.7 together. □

6.3. **Examples and special cases.** We begin by providing several cases where Theorem 6.2 specializes to something much simpler, the interesting case being clearly that $\mu_p(K) \neq \{1\}$, which we will assume in the rest of this subsection.

Corollary 6.9. *Let $(I,\beta) \in \mathrm{Jump}^*_\rho$, with $I \cap I_K = \varnothing$. Then $(I,\beta) \in \mathscr{J}_K$.*

Proof. Indeed, in this case condition (1) of definition 6.1 cannot possibly hold if $(I',\beta') := (I_K,\beta_K), f := f_K, p := \mathrm{char}(O_K/m_K)$. Therefore (I,β) is $((I_K,\beta_K),f,p)$-compatible and the conclusion follows from Theorem 6.2. □

As soon as $f_K \geqslant 2$ we can say the following.

Corollary 6.10. *Suppose that $f_K \geqslant 2$. Then the following facts holds.*
(a) *Suppose that $e^*_{\rho_K} \notin I_K$. Then $\mathscr{J}_K = \mathrm{Jump}^*_{\rho_K}$.*
(b) *Suppose that $e^*_{\rho_K} \in I_K$. Then $\mathrm{Jump}_{\rho_K} \subseteq \mathscr{J}_K \subsetneq \mathrm{Jump}^*_{\rho_K}$.*
(c) *Suppose that $e^*_{\rho_K} \in I_K$. Then each $(I,\beta) \in \mathrm{Jump}^*_{\rho_K}$ with $e^*_{\rho_K} \in I$ and $\beta(e^*_{\rho_K}) \leqslant \beta_K(e^*_{\rho_K})$ is in $\mathscr{J}_K$.*

Proof. Let (I,β) be in $\mathrm{Jump}^*_{\rho_K}$. Then condition (2) of definition 6.1 cannot possibly hold if $(I',\beta') := (I_K,\beta_K), f := f_K, p := \mathrm{char}(O_K/m_K)$, therefore by Theorem 6.2, we obtain that $(I,\beta) \in \mathscr{J}_K$, thus giving (a). Similarly if $e^*_{\rho_K} \notin I$, which amounts to saying that $(I,\beta) \in \mathrm{Jump}_{\rho_K}$, then condition (2) from definition 6.1 cannot possibly hold, giving $\mathrm{Jump}_{\rho_K} \subseteq \mathscr{J}_K$ from (b). The inclusion $\mathscr{J}_K \subseteq \mathrm{Jump}^*_{\rho_K}$ always holds, thanks to Theorem 6.2, so, to conclude the proof of (b), we only need to prove the strict inclusion, i.e. to provide, under the conditions of (b), an element of $\mathrm{Jump}^*_{\rho_K}$ that is not in $\mathscr{J}_K$. Consider $(\{e^*_{\rho_K}\},(e^*_{\rho_K} \mapsto n))$ with $n > \beta_K(e^*_{\rho_K})$: it trivially satisfies condition (a) from Proposition 6.4. Condition (b) amounts to saying that for any $i \in I_K - \{e^*_{\rho_K}\}$ we need to have $n - \beta_K(e^*_{\rho_K}) + \beta_K(i) > n$. This last inequality is equivalent to the inequality $\beta_K(i) - \beta_K(e^*_{\rho_K}) > 0$ and this inequality holds by definition of jump set. Hence we conclude by Theorem 6.2 and Proposition 6.4 that $(\{e^*_{\rho_K}\},(e^*_{\rho_K} \mapsto n)) \notin \mathscr{J}_K$. This concludes the proof of (b).

For (c), notice that the assumption $\beta(e^*_{\rho_K}) < \beta_K(e^*_{\rho_K})$ together with $f_K \geqslant 2$ makes condition (2) of 6.1 impossible to hold for (I,β), giving by Theorem 6.2 that $(I,\beta) \in \mathscr{J}_K$. □

If instead $f_K = 1$, then there are always exceptions.

Corollary 6.11. *If $f_K = 1$, then $\mathscr{J}_K \subsetneq \mathrm{Jump}^*_{\rho_K}$.*

Proof. We proceed as in (b) of the previous corollary. For any $i \in I_K$ we consider the jump set $(\{i\},(i \mapsto n))$ with $n > \beta_K(i)$. We proceed to show that this jump set is $((I_K,\beta_K),1,p)$-incompatible. Condition (a) of Proposition 6.4 is clearly satisfied, so we proceed to verify condition (b) of that Proposition. Taking $j \in I_K$ with $j < i$, we need to check that $\beta_K(j) + n - \beta_K(i) > n$, or equivalently that $\beta_K(j) > \beta_K(i)$. This last inequality follows from the definition of a jump set. Take now $j \in I_K$ with $j > i$, we need to check that $\rho_K^{\beta_K(j)+n-\beta_K(i)}(j) > \rho_K^n(i)$, which, ρ_K being strictly increasing, reduces to $\rho_K^{\beta_K(i)-\beta_K(j)}(i) < j$, which follows from the definition of a jump set. Therefore we conclude from Theorem 6.2 and Proposition 6.4 that $(\{i\},(i \mapsto n)) \notin \mathscr{J}_K$. □

We remark that if we would have put $n \leqslant \beta_K(i)$ during the proof of Corollary 6.11 we would have found, thanks to Theorem 6.2, that $(\{i\},(i \mapsto n)) \in \mathscr{J}_K$, since condition (1) of 6.1 is not satisfied. This will be helpful in the next corollary. It turns out that in the

case $f_K = 1$ there are even enough exceptions to reconstruct the full structure of the filtered $\mathbb{Z}_p$-module $U_\bullet(K)$ out of $\mathscr{J}_K$. Namely we have the following.

Corollary 6.12. *Let K_1, K_2 be two totally ramified extensions of $\mathbb{Q}_p(\zeta_p)$. Then $\mathscr{J}_{K_1} = \mathscr{J}_{K_2}$ if and only if $U_\bullet(K_1) \simeq_{\mathbb{Z}_p\text{-filt}} U_\bullet(K_2)$.*

Proof. Firstly observe that $T^*_{\rho_K}$ consists precisely of the positive integers $i \in \mathbb{Z}_{\geqslant 1}$ such that $(\{i\}, (i \mapsto n)) \in \mathscr{J}_K$ for some positive integer n. Indeed if $i \notin I_K$, then by Corollary 6.9 any $n \in \mathbb{Z}_{\geqslant 1}$ is allowed. If instead $i \in I_K$ then any $n \leqslant \beta(i)$ will be allowed, since in that way $\mathrm{Max}((\{i\}, (i \mapsto n)), (I_K, \beta_K)) = \varnothing$ (for the definition of $\mathrm{Max}((\{i\}, (i \mapsto n)), (I_K, \beta_K)) = \varnothing$ see Theorem 4.8). Conversely, by definition of a jump set, it is clear that for any $i \in \mathbb{Z}_{\geqslant 1}$ such that $(\{i\}, (i \mapsto n)) \in \mathscr{J}_K$ for some positive integer n, one has $i \in T^*_{\rho_K}$. Hence $T^*_{\rho_K}$ can be reconstructed from $\mathscr{J}_K$, and, since $e_K = |T^*_{\rho_K}| - 1$, we can reconstruct e_K from $\mathscr{J}_K$.

Next, from the proof of the previous corollary, it is clear that under the assumption $f_K = 1$, the set I_K can be reconstructed from $\mathscr{J}_K$ as the set of $i \in T^*_{\rho_K}$ for which there exists a positive integer n such that the extended ρ_K-jump set $(\{i\}, (i \mapsto n))$ is not in $\mathscr{J}_K$. Moreover in that proof we saw that, for $i \in I_K$, the set of such integers consists precisely of the left interval $[\beta_K(i) + 1, \infty) \cap \mathbb{Z}_{\geqslant 1}$, hence also β_K can be reconstructed from $\mathscr{J}_K$. Hence we can reconstruct (I_K, β_K).

So given K_1 and K_2 as in the statement we have that $1 = f_{K_1} = f_{K_2}$, and we have shown above that we have $e_{K_1} = e_{K_2}$ and so $\rho_{K_1} = \rho_{K_2}$. Moreover by the reasoning just made, from $\mathscr{J}_{K_1} = \mathscr{J}_{K_2}$ we conclude that $(I_{K_1}, \beta_{K_1}) = (I_{K_2}, \beta_{K_2})$. Hence we conclude by Theorem 5.3 that $U_\bullet(K_1) \simeq_{\mathbb{Z}_p\text{-filt}} U_\bullet(K_2)$. The converse is a triviality. □

In other words, for K_1, K_2, totally ramified extension of $\mathbb{Q}_p(\zeta_p)$, one has $\mathscr{J}_{K_1} = \mathscr{J}_{K_2}$ if and only if $e_{K_1} = e_{K_2}$ and $(I_{K_1}, \beta_{K_1}) = (I_{K_2}, \beta_{K_2})$.

We conclude this subsection providing a more explicit description of $\mathscr{J}_K$ in a family of simple cases, namely when $|I_K| \leqslant 2$. Observe that thanks to Theorem 1.7, the equality $|I_K| = 2$ is the most typical phenomenon. If $\mathrm{v}_{\mathbb{Q}_p}(e) \geqslant 2$, the probability that $|I_K| > 2$ is at most $(\frac{1}{q})^{p-1} \cdot \frac{q-1}{q}$ and at least $(\frac{1}{q})^{p-1} \cdot (\frac{q-1}{q})^2$, while if $\mathrm{v}_{\mathbb{Q}_p}(e) \leqslant 1$, then $|I_K| \leqslant 2$ always. Observe also that $|I_K| = 1$ if and only if K is a tame extension of $\mathbb{Q}_{p^{f_K}}(\zeta_{p^n})$ where n is the unique element of $\beta_K(I_K)$. The classification for $|I_K| = 1$ takes a very simple form. Denoting by $e_0(K)$ the part of $\frac{e_K}{p-1}$ coprime to p, recall that, from the definition of admissible jump sets, one has that $|I_K| = 1$ if and only if $I_K = \{e_0(K)\}$. Recall by admissibility that $\beta_K(e_0(K)) = \mathrm{v}_{\mathbb{Q}_p}(e_K) + 1$.

Corollary 6.13. (a) *Suppose $|I_K| = 1, f_K = 1$. An extended ρ_K-jump set (I, β) belongs to $\mathscr{J}_K$ if and only if either $e_0(K) \notin I$ or both $e_0(K) \in I$ and $\beta(e_0(K)) \leqslant \mathrm{v}_{\mathbb{Q}_p}(e_K) + 1$.*
(b) *Suppose $|I_K| = 1, f_K \geqslant 2$. Then $\mathscr{J}_K = \mathrm{Jump}^*_{\rho_K}$.*

Proof. (a) If $e_0(K) \notin I$ we conclude by Corollary 6.9. If $e_0(K) \in I$ and $\beta(e_0(K)) \leqslant \beta_K(e_0(K))$, then condition (1) of definition 6.1 cannot possibly hold, hence we conclude by Theorem 6.2. Suppose instead that $\beta(e_0(K)) > \beta_K(e_0(K))$. Then all three conditions of definition 6.1 are trivially satisfied and we conclude by Theorem 6.2, finishing the proof.

(b) This follows immediately from Corollary 6.10, given the fact that $e^*_{\rho_K} \neq e_0(K) \in I_K$. □

We next proceed providing an explicit classification in the case $|I_K| = 2, f_K = 1$.

Corollary 6.14. *Suppose* $|I_K| = 2, f_K = 1$. *Write* $I_K = \{e_0(K), i\}$. *Let* $(I, \beta) \in \mathrm{Jump}^*_{\rho_K}$. *Then* $(I, \beta) \in \mathscr{J}_K$ *if and only if one of the following two conditions holds.*
(1) *One has that* $I_K \cap I = \varnothing$.
(2) *One has that* $I_K \subseteq I$, *with* $\mathrm{Max}((I, \beta), (I_K, \beta_K)) = I_K$ *or* $\mathrm{Max}((I, \beta), (I_K, \beta_K)) = \varnothing$.

Proof. From Corollary 6.9 we see that condition (1) indeed implies that $(I, \beta) \in \mathscr{J}_K$. On the other hand condition (2) implies that $|\mathrm{Max}((I, \beta), (I_K, \beta_K))|$ is even, which makes the condition (1) of definition 6.1 impossible to hold. Hence we see that condition (2) also implies that $(I, \beta) \in \mathscr{J}_K$. Conversely, assume that $|\mathrm{Max}((I, \beta), (I_K, \beta_K))| = 1$ but $I_K \subseteq I$. Then conditions (1) − (2) − (3) of definition 6.1 are clearly satisfied, since $I_K - I = \varnothing$. So are left with the case $\mathrm{Max}((I, \beta), (I_K, \beta_K)) = I \cap I_K$. Suppose $I \cap I_K = \{e_0(K)\}$. Then we have to check that $\rho_K^{\beta_K(i)+\beta(e_0(K))-\beta_K(e_0(K))}(i) > \rho_K^{\beta(e_0(K))}(e_0(K))$ which is equivalent to $\rho_K^{\beta_K(e_0(K))-\beta_K(i)}(e_0(K)) < i$: this follows from the definition of a jump set. Suppose that $I \cap I_K = \{i\}$. Then we have to check that $\beta_K(e_0(K)) + \beta(i) - \beta_K(i) > \beta(i)$ which is saying that $\beta_K(e_0(K)) > \beta_K(i)$: this follows from the definition of a jump set. □

Remark 6.15. The reason why for $|I_K| = 2$ one gets such a simple criterion can be learned from the proof of the previous corollary. Namely the inequality in condition (3) in definition 6.1 will always hold when tested against elements of $\mathrm{Max}((I, \beta), (I', \beta'))$, but if I_K has two elements and $I \cap I_K$ has only one, then that is the only possible test to do. So one is left with either $I_K \subseteq I$ or $I \cap I_K = \varnothing$, where in both cases it is very easy to say what Theorem 6.2 prescribes. Indeed the ease of the latter case was formalized in Corollary 6.9. For convenience we formalize also the ease of the case $I_K \subseteq I$ in the following last corollary.

Corollary 6.16. *Suppose that* $f_K = 1$. *Suppose that* $(I, \beta) \in \mathrm{Jump}^*_{\rho_K}$, *with* $I_K \subseteq I$. *Then* $(I, \beta) \in \mathscr{J}_K$ *if and only if* $|\mathrm{Max}((I, \beta), (I_K, \beta_K))| \neq 1$ *when* $\mathrm{char}(O_K/m_K) > 2$ *and* $|\mathrm{Max}((I, \beta), (I_K, \beta_K))| \not\equiv 1 \bmod 2$ *when* $\mathrm{char}(O_K/m_K) = 2$.

Proof. The third condition of definition 6.1 becomes trivially satisfied, and the first two conditions are precisely translated in the statement. □

7. The shooting game

The goal of this section is to explain the rules of a certain Markov process, which we called the *shooting game*, and some of its variants. This process is the bridge between the two sides of the equality in Theorem 1.7. This will be explained in detail in the next two sections. We shall begin with an informal description.

Let ρ be a shift, and let r be a positive integer. Let p be a prime, f a positive integer and let $q := p^f$. We will use the following notation: given $m \in \mathbb{Z}_{\geqslant 1}$, denote by $v_\rho(m) := \max(i \in \mathbb{Z}_{\geqslant 0} : m \in \mathrm{im}(\rho^i))$. Denote by $n := v_\rho(r)$. Imagine there are $n + 1$ shooters $S_0, S_1, \ldots, S_n$, and a rabbit R placed in initial position r. The activity of the shooters is to shoot at the rabbit in turns. If the rabbit sits in position x the shooter will always shoot from the $y \in T_\rho$ such that $\rho^{v_\rho(x)}(y) = x$. We shall call such a y the *shooting position* of the shot. The value $v_\rho(x)$ is called the *length* of the shot. The rules describing how the shooters take turns and what the outcome of each turn is are the following.

(1) The shooter S_i cannot perform any shot of length strictly smaller than i.

(2) Whenever it turns out (with the above rules) that a shot of length strictly smaller than i must be performed, then S_i leaves the game forever.

(3) A shooter S_i can start shooting only when all the other shooters S_j with $j > i$ had to leave the game by rule (2). In this case he will actually shoot.

(4) The rabbit R moves only when someone shoots. At each shot the rabbit moves somewhere forward on $\mathbb{Z}_{\geqslant 1}$. If h is a positive integer, then R moves exactly h steps forward with probability $\frac{q-1}{q^h}$.

(5) The rabbit R starts in position r.

We next explain a natural way to attach to a shooting game G a ρ-jump set (I_G, β_G). Suppose that during the game G we keep track of the shooting positions where a new shooter came in. Let's call this set I_G. To each element of I_G we attach the length of the corresponding shot plus one, and call β_G the resulting map from I_G to $\mathbb{Z}_{\geqslant 1}$. Observe that, thanks to the rules, it is clear that β_G gives also exactly one plus the number of shooters still participating in that round. Indeed this is true for n by the assumption that the first round must be played with length n (and so must be played necessarily by S_n otherwise rule (3) would be contradicted). For $b < n$, the shooter S_b cannot enter the game playing a shot of length smaller than b by virtue of rule (1), moreover, by virtue of rule (3), it must be that S_{b+1} has left the game if S_b is playing so the length of the shot cannot be more than b, otherwise S_{b+1} is still allowed to play and, still by rule (3), he will do so. Thus the length must be b. So the map β_G is strictly decreasing. Moreover, by rule (4), the rabbit moves forward, which means that the map $i \to \rho^{\beta_G(i)}(i)$ is strictly increasing on I_G. In other words we have shown the following fact.

Proposition 7.1. *For each game G, the pair (I_G, β_G) is a ρ-jump set.*

Shooting games can be conveniently formalized in the language of discrete-time Markov processes. We recall the basic definition in the generality that will be relevant for us.

A discrete-time Markov process consists of a set S, called the *state space*, equipped with a *transition function*

$$P : S \times S \to [0, 1],$$

and with a point $x_0 \in S$, called the *initial state* of the process. Moreover we require that for each x in S the function $y \mapsto P(x, y)$ is a probability measure on S, with respect to the discrete sigma-algebra on S. In other words we require that $\sum_{y \in S} P(x, y) = 1$. We shall refer to $P(x, y)$ as the probability to *transition* from x to y. The data (S, P, x_0) with the above properties, suffice to construct a probability space that models the behavior of a discrete random walk in S starting at x_0 and proceeding at each stage from x to y with probability $P(x, y)$. To do so we consider the *space of paths*

$$\Omega := S^{\mathbb{Z}_{\geqslant 1}},$$

as a topological space with the product topology, where S is viewed as a topological space with the discrete topology. On $\mathscr{B}(\Omega)$, the sigma-algebra of Borel sets of Ω, a unique probability measure μ_{P,x_0} is defined with the following property. Take m a positive integer. Let $y_1, \ldots, y_m$ be elements of S. For convenience put $y_0 := x_0$. Let Y be the *cylinder* set $Y := \{y_0\} \times \ldots \times \{y_m\} \times S^{\mathbb{Z}_{\geqslant m+1}}$. We have that

$$\mu_{P,x_0}(Y) = \prod_{i=0}^{m-1} P(y_i, y_{i+1}).$$

Moreover we ask that $\mu_{P,x_0}(\{x_0\} \times S^{\mathbb{Z}_{\geqslant 2}}) = 1$. The existence of such a measure is a simple consequence of the Kolmogorov extension theorem [14, Theorem 2.4.3].

For the shooting game the triple (S, P, x_0) is as follows. We take as state space

$$S := \{(x_1, x_2) \in \mathbb{Z}_{\geqslant 1} \times \mathbb{Z}_{\geqslant 0} : v_\rho(x_1) = x_2\}.$$

In the informal description being in state $(x_1, x_2) \in S$, means that the rabbit R is in position x_1 and that the next shot will be of length $x_2 = v_\rho(x_1)$. The initial point is

$$x_0 := (r, n).$$

The transition function is defined as follows. Let $x := (x_1, x_2)$ and $y := (y_1, y_2)$ be in S with $y_1 > x_1$. Then we put

$$P(x, y) := \frac{q-1}{q^{y_1 - x_1}}.$$

For all other choices of $x, y \in S$ we put $P(x, y) = 0$. We shall denote by $(\mathscr{S}(\rho, r, q), \mu_{q,r})$ the pair (Ω, μ_{P,x_0}) defined in the above paragraph. This is the space of shooting games. Sometimes we shall also use the notation $\mathscr{S}(\rho, r)$ to denote merely the topological space $\Omega = S^{\mathbb{Z}_{\geqslant 1}}$. Observe that

$$\mu_{q,r}(\{(\omega_1, \omega_2) \in \mathscr{S}(\rho, r) : \omega_1 \text{ is strictly increasing}\}) = 1.$$

The informal description, at the beginning of this section, gives us a map

$$\mathscr{S}(\rho, r) \to \mathrm{Jump}_\rho,$$

which can be described as follows. Let (ω_1, ω_2) be in $\mathscr{S}(\rho, r)$ with ω_1 strictly increasing. Define

$$I_{(\omega_1,\omega_2)} := \{i \in \mathbb{Z}_{\geqslant 1} : \text{ for all positive integers } j \text{ smaller than } i \text{ we have } \omega_2(i) < \omega_2(j)\}.$$

We put $\beta_{(\omega_1,\omega_2)}$ to be the restriction of $\omega_2 + 1$ to $I_{(\omega_1,\omega_2)}$. One readily sees that if G is the shooting game corresponding to (ω_1, ω_2), then the jump set $(I_{(\omega_1,\omega_2)}, \beta_{(\omega_1,\omega_2)})$ coincides with (I_G, β_G). In the subspace, having measure 0, of (ω_1, ω_2) such that ω_1 is not an increasing map, we let $I_{(\omega_1,\omega_2)} = \varnothing$. Extended jump sets arise from a natural modification of the shooting game, called the extended shooting game. From now on we assume that T_ρ is finite. Moreover from now on we shall restrict the variable r to be smaller than $e^*_\rho = \max(T_\rho) + 1$. The key difference with a shooting game is that in an extended shooting game the shooters can shoot from T^*_ρ and not only from T_ρ. We shall directly introduce the extended shooting game in terms of Markov processes.

For the extended shooting game we consider the following triple (S^*, P^*, x_0). For any two positive integers k_1, k_2 define $v_\rho(e^*_\rho, k_1, k_2) := \#\{m \in \mathbb{Z}_{\geqslant 0} : k_1 < \rho^m(e^*_\rho) \leqslant k_2\}$. We take as state space the set S^* of points $(x_1, x_2) \in \mathbb{Z}_{\geqslant 1} \times \mathbb{Z}_{\geqslant 0}$ such that one of the following two holds. Either we have $v_\rho(x_1) = x_2$: in this case (x_1, x_2) is said to be of the *first kind*. Or we have that $\rho^{x_2}(e^*_\rho) = x_1$: in this case (x_1, x_2) is said to be of the *second kind*. The initial point is

$$x_0 := (r, v_\rho(r)).$$

The definition of the transition function is slightly more involved. However, right after the definition, we will give an intuitive perspective on such functions. Let $x := (x_1, x_2)$ and $y := (y_1, y_2)$ be in S with $y_1 > x_1$. If y is of the first kind we put

$$P^*(x, y) := \frac{q-1}{q^{y_1 - x_1} p^{v_\rho(e^*_\rho, x_1, y_1)}}.$$

If y is of the second kind we put

$$P^*(x,y) := \frac{p-1}{q^{y_1-x_1-1}p^{v_\rho(e^*_\rho,x_1,y_1)}}.$$

In all the other cases we put $P^*(x,y)=0$. A straightforward calculation shows that this function P^* satisfies the equations of a transition functions. We shall instead explain this in a different way, which offers a more intuitive perspective on the formula for P^*. This can be done by considering an auxiliary family of Markov processes: informally these can be imagined as the Markov processes modeling the behavior of a repeated coin toss that is stopped at the first win. Fix $x_1 \in \mathbb{Z}_{\geqslant 0}$. Let the state space be $S_{x_1} := \{0,1\} \times \mathbb{Z}_{\geqslant x_1}$. Let the initial point be $x_0 := (1,x_1)$. Let y be an integer larger than x_1. We put $P_{x_1}((1,y),(1,y)) := 1$, and $P_{x_1}((1,y),z)=0$ for all the other values of z in S_{x_1}. Moreover we put $P_{x_1}((0,y),(0,y+1)) = \frac{1}{q}$ and $P_{x_1}((0,y),(1,y+1)) = \frac{q-1}{q}$. Finally we put $P_{x_1}((1,x_1),(0,x_1+1)) = \frac{1}{q}$ and $P_{x_1}((1,x_1),(1,x_1+1)) = \frac{q-1}{q}$. For all the other values of z_1, z_2 in S_{x_1} we put $P_{x_1}(z_1,z_2)=0$. In this manner one obtains a Markov process where with probability 1 a path is eventually constant, with second coordinate strictly greater than x_1. In this manner a probability measure on $\mathbb{Z}_{>x_1}$ is induced, with respect to the discrete sigma-algebra. This measure is precisely the one used in the shooting games: it gives to each $x \in \mathbb{Z}_{>x_1}$ weight equal to $\frac{q-1}{q^{x-x_1}}$. We can imagine a path in S_{x_1} as given by the following scenario. A walker is equipped with a coin C giving 1 with probability $\frac{q-1}{q}$ and 0 with probability $\frac{1}{q}$. He starts his walk at x_1 and moves at x_1+1 to see if he will stop there forever. He tosses C and if the result is 1 he will stop there forever, otherwise he has to move at x_1+2 and repeat the operation. On the other hand, to obtain the formula for P^* we are in the following scenario. Our walker has also a second special coin C^*, this coin takes 1 with probability $\frac{p-1}{p}$ and 0 with probability $\frac{1}{p}$. The rule is that he can use C^* only when he arrives at a position x such that there is a nonnegative integer m with $\rho^m(e^*_\rho)=x$. In this case before using C he uses C^*. In case C^* gives 1 he will remain in x forever and he is also provided with a cash prize. If C^* gives 0 he will use C that will still follow the rules as before, telling him if he will stay forever at x (though without cash prize) or if he has to move to $x+1$ to try again his luck. In this manner we obtain a natural probability measure on $\{0,1\} \times \mathbb{Z}_{>x_1}$, which we denote by $\mathbb{P}^*_{x_1}$, where the first coordinate is 1 precisely when the walker has obtained also a cash prize. One has that if (y_1,y_2) is of the first type, then

$$\mathbb{P}^*_{x_1}((0,y_1)) = P^*((x_1,x_2),(y_1,y_2)),$$

and if (y_1,y_2) is of the second type, then

$$\mathbb{P}^*_{x_1}((1,y_1)) = P^*((x_1,x_2),(y_1,y_2)).$$

The triple (S^*,P^*,r) gives rise to the probability space of extended shooting games. This is the pair $(\mathscr{S}^*(\rho,r,q),\mu^*_{q,r}) := (\Omega^*,\mu_{P^*,r})$, where $\Omega^* = (S^*)^{\mathbb{Z}_{\geqslant 1}}$ is the space of paths and $\mu^*_{q,r}$ is the natural probability measure on it, as explained above. Sometimes we shall use the notation $\mathscr{S}^*(\rho,r)$ to denote merely the topological space $\Omega^* = (S^*)^{\mathbb{Z}_{\geqslant 1}}$.

Imitating what we have done in the case of shooting games, we obtain a map

$$\mathscr{S}^*(\rho,r) \to \mathrm{Jump}^*_\rho.$$

Equip Jump^*_ρ with the discrete sigma algebra. Pushing forward $\mu^*_{q,r}$ via the map $\mathscr{S}^*(\rho,r,q) \to \mathrm{Jump}^*_\rho$, we obtain a probability measure on Jump^*_ρ, which we will denote also by $\mu^*_{q,r}$. Let

(I,β) be in Jump^*_ρ. Observe that for $r = e'_\rho$ the measure $\mu^*_{q,r}$ gives positive probability to (I,β) if and only if (I,β) is admissible (for a definition see immediately before Theorem 3.38).

We devote the next subsection to describe a number of subspaces and quotients of $\mathscr{S}^*(\rho,r)$ that will play an important role in the proof of Theorem 1.7.

7.1. **Subspaces and quotients of extended shooting games.** For any positive integer j we define $\mathscr{S}^*_{\geqslant j}(\rho,r)$ to be the set of $G \in \mathscr{S}^*(\rho,r)$ such that $I_G \neq \varnothing$ and $\min(\beta_G) \geqslant j$. We denote by $\mathscr{S}^*_{\geqslant j}(\rho,r,q)$ the above set viewed as a measure space with the restriction of $\mu^*_{q,r}$. If we normalize the measure in the unique way to get a probability space, we will denote the resulting probability space as $\mathscr{S}^*_{\geqslant j}(\rho,r|q)$: this is the probability space of games G *conditioned* to never invoke a shooter of lower index then S_j.

Next we define $\mathscr{S}^*_{=j}(\rho,r)$ to be the set of $G \in \mathscr{S}^*(\rho,r)$ such that $I_G \neq \varnothing$ and $\min(\beta_G) = j$ and $e^*_\rho \notin I_G$. We denote by $\mathscr{S}^*_{=j}(\rho,r,q)$ the above set viewed as a measure space with the restriction of $\mu^*_{q,r}$. If we normalize the measure in the unique way to get a probability space, we will denote the resulting probability space as $\mathscr{S}^*_{=j}(\rho,r|q)$: this is the probability space of games G *conditioned* to invoke as a last shooter S_j, with his first shot being not from e^*_ρ.

We define $\mathscr{S}^*_{=j,*}(\rho,r)$ to be the set of $G \in \mathscr{S}^*(\rho,r)$ such that $\min(\beta_G) = j$ and $e^*_\rho \in I_G$. We denote by $\mathscr{S}^*_{=j,*}(\rho,r,q)$ the above set viewed as a measure space with the restriction of $\mu^*_{q,r}$. If we normalize the measure in the unique way to get a probability space, we will denote the resulting probability space as $\mathscr{S}^*_{=j,*}(\rho,r|q)$: this is the probability space of games G *conditioned* to invoke as a last shooter S_j, and by letting him shoot for the first time from e^*_ρ.

Finally for any positive integers x we define $\mathscr{S}_{x,\mathrm{stop}}(\rho,r,q)$ as the quotient probability space of $\mathscr{S}^*(\rho,r,q)$, where two games are identified precisely when the trajectories of the rabbit are identical as long as the rabbit stays below x.

For all the following remarks m will denote $v_\rho(e^*_\rho)$. We will assume that ρ is such that $m \geqslant 2$. Equivalently we are assuming that in $\mathscr{S}^*(\rho,e'_\rho,q)$ the subspace $\mathscr{S}^*_{=1}(\rho,e'_\rho,q)$ has probability strictly smaller than 1: in case the subspace $\mathscr{S}^*_{=1}(\rho,e'_\rho,q)$ has probability equal to 1, then the shooting game gives constantly the jump set $(\{e'_\rho\}, e'_\rho \mapsto 1)$.

For a positive integer x and a nonnegative integer m', such that $x \in \mathrm{Im}(\rho^{m'})$ we denote by $\rho^{-m'}(x)$ the unique positive integer y such that $\rho^{m'}(y) = x$.

Remark 7.2. Let $j \in \{1,\dots,m\}$. Given G an element of $\mathscr{S}^*(\rho,\rho^{-(j-1)}(e'_\rho))$, by applying ρ^{j-1} to it, we obtain an element of $\mathscr{S}^*_{\geqslant j}(\rho,e'_\rho)$, this map is a bijection. Moreover the map ρ^{j-1} induces an isomorphism of measure spaces $\mathscr{S}^*_{\geqslant j}(\rho,e'_\rho|q) \simeq_{\text{meas. space}} \mathscr{S}^*(\rho,\rho^{-(j-1)}(e'_\rho),q)$. The map induced on jump sets consists simply of shifting β by $j-1$. We call ψ_j the inverse of the isomorphism given by ρ^{j-1}.

Remark 7.3. The map described in Remark 7.2 induces an isomorphism of measure spaces $\mathscr{S}^*_{=j}(\rho,e'_\rho,q) \simeq_{\text{meas. space}} \mathscr{S}^*_{=1}(\rho,\rho^{-(j-1)}(e'_\rho),q)$.

Remark 7.4. For all elements G of a given equivalence class C in $\mathscr{S}_{x,\mathrm{stop}}(\rho,r,q)$ the set $\{i \in I_G : \rho^{\beta_G(i)}(i) \leqslant x\}$ will be the same, and similarly the restriction of β_G to this set will be the same. The resulting pair (I_C,β_C) is also an extended ρ-jump set. In particular the set $\mathscr{S}^*_{=1}(\rho,e'_\rho)$ consists of a union of equivalence classes for the projection to $\mathscr{S}_{e^*_\rho,\mathrm{stop}}(\rho,e'_\rho)$.

Moreover in each such equivalence class C, the jump set (I_C, β_C) coincides with the jump set (I_G, β_G) for any G belonging to C.

Remark 7.5. Let j be in $\{1, \dots, m-1\}$. Observe that the projection of $\mathscr{S}^*_{=j,*}(\rho, e'_\rho|q)$ to $\mathscr{S}_{\rho^j(e^*_\rho),\mathrm{stop}}(\rho, e'_\rho, q)$ lands in the image of $\mathscr{S}^*_{\geqslant j+1}(\rho, e'_\rho, q)$. Thus we can apply to it ψ_{j+1}, landing in $\mathscr{S}^*_{e'_\rho,\mathrm{stop}}(\rho, \rho^{-j}(e'_\rho), q)$. We denote by $\psi^*_j : \mathscr{S}^*_{=j,*}(\rho, e'_\rho|q) \to \mathscr{S}_{\rho^{-j+1}(e'_\rho),\mathrm{stop}}(\rho, \rho^{-j}(e'_\rho), q)$ the resulting map. If $C = \psi^*_j(G)$ then $I_G = I_C \cup \{e^*\}$ with $\beta_{G|I_C} = \beta_C + j - 1$ and $\beta_G(e^*) = j$. This provides a reconstruction of (I_G, β_G) from $(I_{\psi(G)}, \beta_{\psi(G)})$.

Remark 7.6. Given $j \in \{1, \dots, n\}$, it can be easily shown that one has always that

$$(p-1)\mu^*_{q,e'_\rho}(\mathscr{S}^*_{\geqslant j+1}(\rho, e'_\rho, q)) = \mu^*_{q,e'_\rho}(\mathscr{S}^*_{=j,*}(\rho, e'_\rho, q)).$$

In the setting of local fields this fact is mirrored by Proposition 5.6.

8. Shooting game and filtered orbits

Fix p a prime number. Using the notation of Section 3, we take $R = \mathbb{Z}_p$, and we fix f a positive integer and ρ a shift. Let $q := p^f$, and we recall that the module $M^{f-1}_\rho \oplus M^*_\rho$ was defined on top of subsection 3.3.4. On the other hand recall from Theorem 3.37 that the set of extended jump sets is in bijection with the set of $\mathrm{Aut}_{\mathrm{filt}}(M^{f-1}_\rho \oplus M^*_\rho)$-orbits of vectors in $\pi_R(M^{f-1}_\rho \oplus M^*_\rho)$. Thus, by using the Haar measure, this induces naturally a probability measure on the set of extended admissible ρ-jump sets. We call this measure $\mu_{q,\mathrm{Haar}}$: given (I, β) an admissible extended ρ-jump set, we have that $\mu_{q,\mathrm{Haar}}(I, \beta) := \mu_{\mathrm{Haar}}(\text{filt-ord}^{-1}(I, \beta))$, where the Haar measure is normalized giving total mass 1 to the set of orbits corresponding to admissible jump sets (for a definition of admissible see right before Theorem 3.38).

On the other hand Section 7 provides us with another measure on admissible extended jump sets, namely the probability that a shooting game in $\mathscr{S}(\rho, e'_\rho, q)$ gives the jump set (I, β). We denoted by μ^*_{q,e'_ρ} this probability measure on Jump^*_ρ.

Proposition 8.1. *For any extended admissible ρ-jump set (I, β) one has that*

$$\mu_{q,\mathrm{Haar}}(I, \beta) = \mu^*_{q,e'_\rho}(I, \beta).$$

Proof. We prove slightly more. Namely we construct a map $G(-)$ sending an admissible vector v into a shooting game $G(v) \in \mathscr{S}^*(\rho, e'_\rho, q)$, in such a way that $G^*(\mu_{\mathrm{Haar}}) = \mu^*_{q,e'_\rho}$ and that $(I_v, \beta_v) = (I_{G(v)}, \beta_{G(v)})$.

To construct such a map fix a filtered basis $\mathscr{B}$ for $M^{f-1}_\rho \oplus M^*_\rho$, in the sense of Definition 3.24. This provides us for each $i \in T_\rho$ with elements $b_{i,1}, \dots, b_{i,f}$ of $M^{f-1}_\rho \oplus M^*_\rho$ with weights obeying $w(b_{i,j}) = i$, and for e^*_ρ we are provided with an element $b_{e^*_\rho}$ with $w(b_{e^*_\rho}) = e^*_\rho$ and $b_{e^*_\rho} \notin \pi_R \cdot (M^{f-1}_\rho \oplus M^*_\rho)$. Next fix $\mathscr{A} := \{\alpha_1, \dots, \alpha_{|R/m_R|-1}\}$ a set of representatives in R of $(R/m_R)^*$. For every $i \in T_\rho$, denote by $\mathscr{F}_i := \mathscr{A} \cdot \mathscr{B}_i$ the set of ab with $a \in \mathscr{A}$ and $b \in \mathscr{B}$. Denote by i^* the unique element of T_ρ such that there exists a positive integer m with $e^*_\rho = \rho^m(i^*)$. Furthermore denote by $\mathscr{F}_{e^*_\rho} := \pi_R^{v_\rho(e^*_\rho)}\mathscr{F}_{i^*} + \mathscr{A}\{b_{e^*_\rho}\}$. The sets $\mathscr{F}_i$ as i runs in T^*_ρ are pairwise disjoint. For any vector $z \in M^{f-1}_\rho \oplus M^*_\rho$, there exists a unique $i \in T^*_\rho$, which we denote by i_z, such that there exist $b_z \in \mathscr{F}_{i_z}$ and $v(z) \in \mathbb{Z}_{\geqslant 0}$ with $w(-\pi_R^{v(z)}b_z + z) > w(z)$, where $\rho^{v(z)}(i_z) = w(z)$ and $b_z \in \mathscr{F}_{i_z}$. The elements $b_z, v(z)$ are unique.

Now let $v \in \pi_R(M_\rho^{f-1} \oplus M_\rho^*)$ be a vector in an admissible orbit. Let x be the vector in $M_\rho^{f-1} \oplus M_\rho^*$ such that $\pi_R x = v$. We inductively construct a sequence of vectors by letting $x_1 = x$ and setting $x_{j+1} = x_j - \pi_R^{v(x_j)} b_{x_j}$ the unique expression explained above. We use this sequence of vectors to attach to v a shooting game $G(v)$ as follows: we consider the map $(f_1, f_2) : \mathbb{Z}_{\geqslant 1} \to \mathbb{Z}_{\geqslant 1} \times \mathbb{Z}_{\geqslant 1}$, given by the relation $f_1(i) = w(x_i)$ and $f_2(i) = v(x_i)$. One can easily verify that the pushforward with $G(-)$ of the Haar measure is μ^*_{q,e'_ρ} and that the map $G(-)$ preserves jump sets. □

9. A mass-formula for U_1

Let p be a prime number, f be a positive integer, denote by $q = p^f$, let $e \in (p-1)\mathbb{Z}_{\geqslant 1}$ and let (I, β) be an extended admissible $\rho_{e,p}$-jump set. The goal of this section is to provide a proof of Theorem 1.7. In virtue of Proposition 8.1, this task is equivalent to proving the following Theorem.

Theorem 9.1.

$$\mu_{\frac{e}{p-1},\mathbb{Q}_{p^f}(\zeta_p)}(\{K \in S(\frac{e}{p-1}, \mathbb{Q}_{p^f}(\zeta_p)) : (I_K, \beta_K) = (I, \beta)\}) = \mu^*_{q,e'_\rho}(I, \beta).$$

If F is a local field and h is a positive integer, then $\mathrm{Eis}(h, F)$ denotes the set of degree h Eisenstein polynomials in $F[x]$. These are monic polynomials $f(x)$ with coefficients in O_F, that reduced modulo m_F, the maximal ideal of O_F, become x^h and such that $f(0) \notin m_F^2$.

9.1. **Proof outline.** Since our proof of Theorem 9.1 is quite long, we shall first explain its basic idea. In subsection 9.1.1 we give an overview of the main ideas of the proof. In subsection 9.1.2 we explain how the proof reduces to the construction of certain maps from certain spaces of Eisenstein polynomials to shooting games. Finally we spend the rest of the section to construct such maps and to show that they meet all the requirements explained in subsection 9.1.2.

9.1.1. *The idea of the proof.* In this subsection the discussion is *informal*. Our priority here is to provide some intuition about how the proof of Theorem 9.1 goes. For a formal proof see from subsection 9.1.2 on.

The starting idea is to proceed as in the proof of Proposition 8.1. One has immediately a difference between the set-up of Proposition 8.1 and the one of Theorem 9.1. In Proposition 8.1 one has a *fixed* free-filtered module where it is possible to successively "shoot at elements of $M_\rho^{f-1} \oplus M_\rho^{*}$" as done in that proof, using a fixed filtered basis. In this manner a measure-preserving map is obtained sending each vector of $M_\rho^{f-1} \oplus M_\rho^*$ to an extended shooting game. By measure-preserving here we mean that the push-forward of the measure on the source is equal to the measure on the target. In Theorem 9.1 we have a *varying* quasi-free filtered module, namely $U_\bullet(K)$, so we need firstly to find a common manner to successively "shoot at the units" in order to proceed as in the proof of Proposition 8.1. This step can be done by fixing the set of polynomials $\mathscr{B} := \{(1 + \gamma x^i) : i \in T_{\rho_{e,p}}, \gamma \in \mathrm{Teich}(\mathbb{Q}_{p^f}) - \{0\}\} \cup \{1 + \varepsilon' x^{\frac{pe}{p-1}}\}$, where $\mathrm{Teich}(\mathbb{Q}_{p^f})$ denotes the set of Teichmüller representatives of $\mathbb{F}_{p^f}$ in $\mathbb{Q}_{p^f}$. Here ε' is a Teichmüller representative of a fixed element $\varepsilon' \in \mathbb{F}_{p^f}$ with $\mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(\varepsilon) \neq 0$. To keep a stricter analogy with the proof of Theorem 8.1, we should only allow a set of Teichmüller representatives that, once it is reduced modulo $p\mathbb{Z}_{p^f}$, it becomes a basis of $\mathbb{F}_{p^f}$. Since this restriction would make the description of the next steps heavier and is irrelevant

for the present discussion, we shall disregard it. One can attempt to proceed precisely as in the proof of Theorem 8.1 in order to construct a measure-preserving function from the set of Eisenstein polynomials to the set of shooting games. As we will see, we will use only a part of this idea, one that is still good enough to obtain a proof of Theorem 9.1 and that combined with a different set of observations (explained at the end of this subsection) leads to more informative results. More concretely one starts with an Eisenstein polynomial $g(x) = x^{\frac{e}{p-1}} + \sum_{i=0}^{\frac{e}{p-1}-1} a_i x^i$. Next one finds a unit u in $\mathbb{Z}_{p^f}[\zeta_p]^*$ in such a way that $ug(x) = ux^{\frac{e}{p-1}} + \sum_{i=1}^{\frac{e}{p-1}-1} ua_i x^i + 1 - \zeta_p$. Hence in the field $\mathbb{Q}_{p^f}(\zeta_p)[x]/g(x)$ one can write $\zeta_p = 1 + \sum_{i=1}^{\frac{e}{p-1}-1} ua_i x^i + ux^{\frac{e}{p-1}} =: g_1(x)$. At this point one multiplies $g_1(x)$ by $(1+\gamma x^{e_0})^{p^{\mathrm{v}_{\mathbb{Q}_p}(e)}}$ for a suitable $\gamma \in \mathrm{Teich}(\mathbb{Q}_{p^f})$, where e_0 denotes the largest divisor of $\frac{e}{p-1}$ coprime to p. *After* expanding the product, we replace all the powers of x having degree larger than $\frac{e}{p-1}$ with their remainder upon division by $g(x)$. In this way a second expression $g_2(x) = 1 + \sum_{i=1}^{\frac{pe}{p-1}-1} a_i(2)x^i$ is obtained. Now we would like to iterate this. We do so as long as this unit has weight less than $\frac{pe}{p-1}$. In this case we have precisely one way to choose an element of $\mathscr{B}$ that does the same job $1+\gamma x^{e_0}$ did for $g_1(x)$: in particular we do not use the element $1+\varepsilon' x^{\frac{pe}{p-1}}$. If we iterate this procedure as long as the weight stays below $\frac{pe}{p-1}$, we obtain a sequence of polynomials $g_1(x), \dots, g_k(x)$ where $g_{s+1}(x)$ is obtained by "shooting" $g_s(x)$ with an element of $\mathscr{B}$ in the way hinted above. Moreover it is relatively easy to determine that the change of weight from $g_s(x)$ to $g_{s+1}(x)$ obeys the same rule as the change of positions of the rabbit during the shooting game. Indeed, as we shall see in the proof, although the expressions for $g_{s+1}(x)$ can become increasingly complicated, there is a simple way to get the *probability* that the weight of $g_{s+1}(x)$ will be larger than a given y, with $y < \frac{pe}{p-1}$. The reason for this is that we can divide in two pieces the expressions that decide whether the weight of $g_{s+1}(x)$ will be larger than y. One piece comes from "lower order terms" and it behaves in the proof, from the probabilistic point of view, as a *constant*. The other piece comes in a very simple manner from the Eisenstein polynomial $g(x)$ and one sees, directly from the definition of Haar measure on Eisenstein polynomials, that it is a uniform random variable in $\mathrm{Teich}(\mathbb{Q}_{p^f})$. In this way we can prove Theorem 9.1 for all (I,β) with $\min(\beta) = 1$ and $\frac{pe}{p-1} \notin I$. To proceed further we need to deal with the case that, in the above "shooting process", the unit has reached a weight at least $\frac{pe}{p-1}$ and we have not yet used a shot of length 0. That means that either $\frac{pe}{p-1} \in I_K$ with $\beta(\frac{pe}{p-1}) = 1$ or $\zeta_{p^2} \in K$. The last remark in Section 7.1 tells us that the former possibility should occur precisely $p-1$ times as often as the latter. On the other hand Proposition 5.6 tells us that the same happens for local fields. Indeed the fields $\{\mathbb{Q}_{p^f}(\zeta_p)(s) : s \in \{1,\dots,p\}$ have all the same mass, therefore by Proposition 5.6 we conclude that they partition the set of local fields K, having either $\frac{pe}{p-1} \in K$ or $\zeta_{p^2} \in K$, into p disjoint sets $X_1, \dots, X_p$ having all the same mass, with $K \in X_s$ if and only if $\mathbb{Q}_{p^f}(\zeta_p)(s) \subseteq K$. For $s \in \{1,\dots,p-1\}$ we have that the total mass of X_s equals $\frac{1}{p-1}$ of the total mass of the fields K with $\frac{pe}{p-1} \in I_K$ and $\beta_K(\frac{pe}{p-1}) = 1$. On the other hand X_p consists of those fields K with $\zeta_{p^2} \in K$. So we deal with the set $X_1, \dots, X_{p-1}$ working with Eisenstein polynomials over $\mathbb{Q}_{p^f}(\zeta_p)(1), \dots, \mathbb{Q}_{p^f}(\zeta_p)(p-1)$ and we deal with X_p using $\mathbb{Q}_{p^f}(\zeta_{p^2})$. Thanks to Proposition 5.6, by repeating the above "shooting argument" for the sets $X_1, \dots, X_{p-1}$, Theorem 9.1 is proved also in the case that $\frac{pe}{p-1} \in I$ with $\beta(\frac{pe}{p-1}) = 1$. The idea is to repeat this whole proof structure over $\mathbb{Q}_{p^f}(\zeta_{p^2})$.

9.1.2. *Proof strategy.* The plan of the proof is the following. Let $n := \mathrm{v}_{\mathbb{Q}_p}(e)$. We will use the notation from Section 7 and in particular from Section 7.1. For each $j \in \{0, 1, \dots, n\}$ we construct maps

$$\sigma_j : \mathrm{Eis}(\frac{e}{p^j(p-1)}, \mathbb{Q}_q(\zeta_{p^{j+1}})) \to \mathscr{S}_{\frac{pe}{p-1},\mathrm{stop}}(\rho_{e,p}, \frac{e}{p^j(p-1)}, q)$$

and for each $j_1 \in \{0, \dots, n-1\}$ and $j_2 \in \{1, .., p-1\}$ we construct maps

$$\sigma_{j_1,j_2} : \mathrm{Eis}(\frac{e}{p^{j_1+1}(p-1)}, \mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)) \to \mathscr{S}_{\frac{e}{p-1},\mathrm{stop}}(\rho_{e,p}, \frac{e}{p^{j_1+1}(p-1)}, q),$$

having the following two properties.

(P.1) For any $j \in \{0, 1, \dots, n\}$ and $f(x) \in \mathrm{Eis}(\frac{e}{p^j(p-1)}, \mathbb{Q}_q(\zeta_{p^{j+1}}))$, denoting by $K_{f(x)} := \mathbb{Q}_q(\zeta_{p^{j+1}})[x]/f(x)$, we have that

$$\{i \in I_{K_{f(x)}} : \rho_{e,p}^{\beta_{K_{f(x)}}-(j+1)}(i) < \frac{pe}{p-1}\} = I_{\sigma_j(f(x))}$$

and for each $i \in I_{\sigma_j(f(x))}$ we have that

$$\beta_{K_{f(x)}}(i) = \beta_{\sigma_j(f(x))}(i) + j.$$

For any $j_1 \in \{0, \dots, n-1\}$, $j_2 \in \{1, \dots, p-1\}$ and $f(x) \in \mathrm{Eis}(\frac{e}{p^{j+1}(p-1)}, \mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2))$, we have that

$$I_{K_{f(x)}} = I_{\sigma_{j_1,j_2}(f(x))} \cup \{\frac{pe}{p-1}\}.$$

For $i \in I_{\sigma_{j_1,j_2}(f(x))}$ we have

$$\beta_{K_{f(x)}}(i) = \beta_{\sigma_{j_1,j_2}(f(x))}(i) + j_1 + 1.$$

Finally we have

$$\beta_{K_{f(x)}}(\frac{pe}{p-1}) = j_1 + 1.$$

(P.2) For any $j \in \{0, 1, \dots, n\}$ pushing forward μ_{Haar}, the natural probability measure on $\mathrm{Eis}(\frac{e}{p^j(p-1)}, \mathbb{Q}_q(\zeta_{p^{j+1}}))$ coming from the Haar measure on the coefficients, with σ_j one obtains $\mu^*_{q,\frac{e}{p^j(p-1)},\rho_{e,p}}$, the probability measure on $\mathscr{S}_{\frac{pe}{p-1},\mathrm{stop}}(\rho_{e,p}, \frac{e}{p^j(p-1)}, q)$ introduced in Section 7.

For any $j_1 \in \{0, 1, \dots, n-1\}$ and $j_2 \in \{1, \dots, p-1\}$, pushing forward μ_{Haar} with σ_{j_1,j_2} from $\mathrm{Eis}(\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2))$ to $\mathscr{S}_{\frac{e}{p^{j_1}(p-1)}}(\rho_{e,p}, \frac{e}{p^{j_1+1}(p-1)}, q)$, one obtains $\mu^*_{q,\frac{e}{p^{j_1+1}(p-1)},\rho_{e,p}}$.

The construction of such maps σ_j and σ_{j_1,j_2} satisfying (P.1) and (P.2) as above, is sufficient to prove Theorem 9.1 and thus Theorem 1.7. Indeed, thanks to Remark 7.4, we can conclude with σ_0 that Theorem 9.1 holds for all (I, β) with $\min(\beta) = 1$ and $\frac{pe}{p-1} \notin I$. At that point we know that the probability of the event $\{\min(\beta) > 1$ or $\frac{pe}{p-1} \in I\}$ has equal probability on both sides (Eisenstein polynomials and shooting games). We remark that this conclusion can be reached alternatively also by a direct computation. By Remark 7.6 we know that, at the level of shooting games, the probability of the event $\{\frac{pe}{p-1} \in I, \beta(\frac{pe}{p-1}) = 1\}$ is $p-1$ times as large as the event $\{\min(\beta) > 1\}$. On the other hand this is clearly true also at the level of Eisenstein polynomials: the fields $\mathbb{Q}_q(\zeta_p)(j)$ have the same mass as j runs through $\{1, \dots, p\}$, and by Proposition 5.6, precisely the first $p-1$ of them give the event $\{\frac{pe}{p-1} \in I, \beta(\frac{pe}{p-1}) = 1\}$, while the last (which is $\mathbb{Q}_q(\zeta_{p^2})$) gives the event $\{\min(\beta) > 1\}$. Thus we can go on in the proof of Theorem 9.1 by conditioning on both sides with either the event $\{\frac{pe}{p-1} \in I, \beta(\frac{pe}{p-1}) = 1\}$ or the event $\{\min(\beta) > 1\}$. Thus by Remark 7.5, and with the σ_{0,j_2} we conclude the validity

of Theorem 9.1 for (I,β) with $\frac{pe}{p-1} \in I$ and $\beta(\frac{pe}{p-1}) = 1$. Here we are using that if F/K is a totally ramified Galois extension of local fields, then, for an extension F/E and a positive integer $d \in [F:E]\mathbb{Z}_{\geqslant 1}$, the conditional probability measure $\mu_{d,E}(-|\{F \text{ is a subfield}\})$ equals the probability measure $\mu_{\frac{d}{[F:E]},F}$[1]. That justifies the passage to Eisenstein polynomials over the extensions $\mathbb{Q}_q(\zeta_p(j))$.

Now we continue working over $\mathbb{Q}_q(\zeta_{p^2})$ and we proceed precisely as above. Namely we first use the map σ_1 to show that Theorem 9.1 holds for (I,β) with $\min(\beta) = 2$ and $\frac{pe}{p-1} \notin I$. If $n = 1$ we are done. Otherwise we again obtain that the measure of the event $\{\min(\beta) > 2 \text{ or } \frac{pe}{p-1} \in I\}$ coincides on both sides of Theorem 9.1. Finally Remark 7.6 gives that, at the level of shooting games, the event $\{\frac{pe}{p-1} \in I, \beta(\frac{pe}{p-1}) = 2\}$ is $p-1$ times as frequent as the event $\{\min(\beta) > 2\}$. This holds also for Eisenstein polynomials thanks to the fact that the extensions $\mathbb{Q}_q(\zeta_{p^2})(j)$ of $\mathbb{Q}_q(\zeta_{p^2})$ for $j \in \{1,\dots,p\}$ have all the same mass, and by Proposition 5.6 we have that the first $p-1$ give the event $\{\frac{pe}{p-1} \in I, \beta(\frac{pe}{p-1}) = 2\}$ while the last (which is $\mathbb{Q}_q(\zeta_{p^3})$) gives the event $\{\min(\beta) > 2\}$. Thus we use the maps $\sigma_{1,j}$ to prove Theorem 9.1, with the same considerations made above, and we go on working over $\mathbb{Q}_q(\zeta_{p^3})$. Iterating this argument we prove Theorem 9.1 for every (I,β), an extended admissible jump set. Therefore to finish the proof, we are left with constructing the maps $\sigma_j, \sigma_{j_1,j_2}$ and showing that they have properties $(P.1)$ and $(P.2)$. This done in the next two subsections.

9.2. **Construction of the maps $\sigma_j, \sigma_{j_1,j_2}$.** Let $j \in \{0,\dots,n\}$, we begin with the construction of σ_j. To lighten the notation, denote $e_j := \frac{e}{p^j(p-1)}$. An element

$$f(x) := x^{e_j} + \sum_{i=0}^{e_j-1} a_i x^i$$

in $\mathrm{Eis}(e_j, \mathbb{Q}_q(\zeta_{p^{j+1}}))$ can be equivalently represented as

$$\tilde{f}(x) := 1 + \sum_{i=1}^{e_j} \tilde{a}_i x^i$$

where $\tilde{f}(x) := \frac{1-\zeta_{p^{j+1}}}{a_0} f(x) + \zeta_{p^{j+1}}$. This gives us an embedding of $\mathrm{Eis}(e_j, \mathbb{Q}_q(\zeta_{p^{j+1}}))$ into $H_{e_j}(\mathbb{Q}_q(\zeta_{p^{j+1}})) := \{g \in \mathbb{Z}_q[\zeta_{p^{j+1}}] : \deg(g) \leqslant e_j, g(0) = 1, g(x) \equiv 1 \text{ or } g(x) \equiv 1 + ax^{e_j} \bmod (1-\zeta_{p^{j+1}}) \text{ for some } a \in \mathbb{Z}_q[\zeta_{p^{j+1}}]^*\}$. Starting with $f_0(x) := \tilde{f}(x)$, we define inductively a sequence $\{f_n(x)\}_{n\in\mathbb{Z}_{\geqslant 0}}$ with $f_n(x) \in H_{e_j}(\mathbb{Q}_q(\zeta_{p^{j+1}}))$ for every $n \in \mathbb{Z}_{\geqslant 0}$. To do so we first define a weight map on $H_{e_j}(\mathbb{Q}_q(\zeta_{p^{j+1}}))$ by

$$w(1 + \sum_{i=1}^{e_j} b_i x^i) = \min_{1\leqslant i\leqslant e_j : b_i \neq 0} (e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(b_i) + i).$$

Now, suppose that $w(f_n(x)) \geqslant \frac{pe}{p-1}$, then declare

$$f_{n+1}(x) = f_n(x).$$

So, suppose that $w(f_n(x)) < \frac{pe}{p-1}$. Observe that

$$f_n(x) \in U_{w(f_n(x))}(\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/f(x)) - U_{w(f_n(x))+1}(\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/f(x)),$$

[1]Here we are using the following standard notation. If (X,μ) is a probability space and $A \subseteq X$ is a measurable subset with $\mu(A) > 0$, then $\mu(-|A)$ denotes the probability measure on A, defined by the formula $\mu(-|A)(B) := \frac{\mu(B)}{\mu(A)}$ for each $B \subseteq A$ measurable.

thus there exist unique $i_n \in T_{\rho_{e,p}}, \beta_n \in \mathbb{Z}_{\geqslant 0}$ and unique ε_n, a Teichmüller representative in $\mathbb{Q}_q$, such that

$$(1+\varepsilon_n x^{i_n})^{p^{\beta_n}} f_n(x) \in U_{w(f_n(x))+1}(\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/f(x)).$$

It is not difficult to show that there exists a unique element of $H_{e_j}(\mathbb{Q}_q(\zeta_{p^{j+1}}))$ congruent to $(1+\varepsilon_n x^{i_n})^{p^{\beta_n}} f_n(x)$ modulo $f(x)$ and of degree at most e_j. We put $f_{n+1}(x)$ to be this element. It follows by construction that $w(f_{n+1}(x)) \geqslant w(f_n(x))$ with equality occurring iff $w(f_n(x)) \geqslant \frac{pe}{p-1}$. Moreover in the case of equality we have $f_{n+1}(x) = f_n(x)$. Thus we define

$$\sigma_j(f(x)) := \{n \mapsto (w(f_{n-1}(x)), \beta_{n-1})\}_{n\in\mathbb{Z}_{\geqslant 1}} \in \mathscr{S}_{\frac{pe}{p-1},\mathrm{stop}}(\rho_{e,p}, \frac{e}{p^j(p-1)}, q).$$

Let now $j_1 \in \{0,\dots,n-1\}$ and $j_2 \in \{1,\dots,p-1\}$. The map σ_{j_1,j_2} is defined similarly to how the maps σ_j were defined. We briefly explain the modifications. Fix units $u_1, u_2 \in \mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)$ with

$$u_1^p u_2 = \zeta_{p^{j_1+1}},\ \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)}(u_1-1) = 1,\ \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)}(u_2-1) = \frac{pe}{p-1}$$

and $u_2 \notin (\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2))^{*p}$, as guaranteed by Proposition 5.7 and Corollary 3.41 together. Next, given $f(x) := x^{e_{j_1+1}} + \sum_{i=0}^{e_{j_1}} a_i x^i \in \mathrm{Eis}(e_{j_1+1}, \mathbb{Q}_q(\zeta_{p^{j_1+1}}))$, define this time

$$\tilde{f}(x) := \frac{1-u_1}{a_0} f(x) + u_1.$$

Also change $H_{e_{j_1+1}}(\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2))$ to be the set

$$\{g \in \mathbb{Z}_q[\zeta_{p^{j_1+1}}, u_1] : \deg(g) \leqslant e_{j_1+1}, g(0) = 1, g(x) \equiv 1 \text{ or } g(x) \equiv 1 + x^{e_j} \bmod (1-u_1)\},$$

and set the cut-off for concluding $f_{n+1}(x) = f_n(x)$ to be $w(f_n(x)) \geqslant e_j$. Following the above procedure, with these modifications, we get the construction of

$$\sigma_{j_1,j_2}(f(x)) \in \mathscr{S}_{\frac{e}{p-1},\mathrm{stop}}(\rho_{e,p}, \frac{e}{p^{j_1+1}(p-1)}, q).$$

9.3. **The maps $\sigma_j, \sigma_{j_1,j_2}$ satisfy properties $(P.1), (P.2)$.** Let us begin showing that, for $j \in \{0,\dots,n\}$, the map σ_j obeys the property $(P.1)$. By construction, we know that for $f(x) \in \mathrm{Eis}(e_j, \mathbb{Q}_q(\zeta_{p^{j+1}}))$, we have that

$$\zeta_{p^{j+1}} \cdot \prod_{n : w(f_n(x)) < \frac{pe}{p-1}} (1+\alpha_n x^{i_n})^{p^{\beta_n}} \in U_{\frac{pe}{p-1}}(\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/f(x)),$$

with $p^{\beta_n} i_n = w(f_n(x))$, so the sequence $n \mapsto p^{\beta_n} i_n$ is strictly increasing as n runs with the constraint $w(f_n(x)) < \frac{pe}{p-1}$. Of course, the weight of $1+\alpha_n x^{i_n}$ in $U_\bullet(\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/f(x))$ is precisely i_n. Therefore one sees that the values of n such that $i_n \in I_{\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/f(x)}$ are precisely those where β_n reaches a new minimum. This is precisely the same rule that implies $i_n \in I_{\sigma_j(f(x))}$. For such an i_n it easily follows from Corollary 3.41 that

$$\beta_n + j + 1 = \beta_{\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/f(x)}.$$

This shows that σ_j enjoys the property $(P.1)$ for each $j \in \{0,\dots,n\}$.

We next show that for $j_1 \in \{0, \dots, n-1\}$ and $j_2 \in \{1, \dots, p-1\}$, the map σ_{j_1,j_2} satisfies $(P.1)$. Recall the definition of the units u_1, u_2 introduced during the construction of the map σ_{j_1,j_2}. By construction, we know that for $f(x) \in \mathrm{Eis}(e_{j_1+1}, \mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2))$, we have that

$$u_1 \cdot \prod_{n:w(f_n(x))<e_{j_1}} (1+\alpha_n x^{i_n})^{p^{\beta_n}} \in U_{\frac{e}{p-1}}(\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)[x]/f(x)).$$

This implies that

$$u_2^{-p^{j_1}} \cdot \prod_{n:w(f_n(x))<e_{j_1}} (1+\alpha_n x^{i_n})^{p^{\beta_n+j_1+1}} \in U_{\frac{p^{j_1+1}e}{p-1}}(\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)[x]/f(x)).$$

Therefore all the other units that will be employed in order to write the full relation, cannot give a contribution to $(I_{\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)[x]/f(x)}, \beta_{\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)[x]/f(x)})$, due to the presence of $\frac{pe}{p-1}$ in $I_{\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)[x]/f(x)}$, with $\beta_{\mathbb{Q}_q(\zeta_{p^{j_1+1}})(j_2)[x]/f(x)}(\frac{pe}{p-1}) = j_1$ as guaranteed by Proposition 5.6. Thus one concludes using the same argument employed for σ_j.

We next prove that the maps $\sigma_j, \sigma_{j_1,j_2}$ satisfy $(P.2)$. We will do so for σ_j, the argument for σ_{j_1,j_2} being basically the same with different notation.

Given $f \in \mathrm{Eis}(e_j, \mathbb{Q}_q(\zeta_{p^{j+1}}))$, let us begin expanding each of the coefficients of

$$\tilde{f}(x) := 1 + \sum_{i=1}^{e_j} \tilde{a}_j x^j$$

as

$$\tilde{a}_i = \sum_{k=1}^{\infty} \varepsilon_{k,i}(1-\zeta_{p^{j+1}})^k,$$

for $1 \leqslant i < e_j$ and for $i = e_j$ we write

$$\tilde{a}_{e_j} = \sum_{k=0}^{\infty} \varepsilon_{k,e_j}(1-\zeta_{p^{j+1}})^k,$$

where all $\varepsilon_{k,i}$ are Teichmüller representatives of $\mathbb{Z}_q$. We can consider any finite subset of the $\varepsilon_{k,i}$ as independent random variables taking values in all possible Teichmüller representatives with the uniform distribution if $(k,i) \neq (0,e_j)$ and uniformly in the non-zero Teichmüller representatives of $\mathbb{Z}_q$ for ε_{0,e_j}.

Next, for each $n \in \mathbb{Z}_{\geqslant 1}$, we set

$$f_n(x) = 1 + \sum_{i=1}^{e_j} a_i(n) x^i,$$

and we let

$$a_i(n) := \sum_{k=1}^{\infty} \varepsilon_{k,i}(n)(1-\zeta_{p^{j+1}})^k.$$

the corresponding Teichmüller expansion with respect to $(1-\zeta_{p^{j+1}})$. The fact that the second sum started with $k=1$ is a consequence of the fact that the weights of $f_n(x)$ are strictly increasing as n increases together with the definition of $H_{e_j}(\mathbb{Q}_q(\zeta_{p^{j+1}}))$.

For any fixed $n \in \mathbb{Z}_{\geqslant 0}$ the monomials $\varepsilon_{k,i}(n)(1-\zeta_{p^{j+1}})^k x^i$ can be given the weight $ke_j + i$ if $\varepsilon_{k,i}(n) \neq 0$ and ∞ otherwise. This induces a total order on the various non-zero monomials, and the weight $w(f_n(x))$ of $f_n(x)$ as defined before, equals the minimum weight of the

various monomials as long as there is a monomial with weight less than $\frac{pe}{p-1}$, otherwise we have already arrived at the point where the sequence $f_n(x)$ is eventually constant.

From the rule to obtain $f_{m+1}(x)$ out of $f_m(x)$ we see that for any $n \in \mathbb{Z}_{\geqslant 1}$, and any positive integer $\frac{pe}{p-1} > w_0 > w(f_{n-1}(x))$, there exists a function $F_{w_0,n}$ taking as input the sequence of $(\varepsilon_{k,i})_{e_jk+i<w_0}$ and giving as output a Teichmüller representative of $\mathbb{Z}_q$, in such a way that if we write $w_0 = e_jq' + h$, the division with remainder of w_0 by e_j, we have that

$$\varepsilon_{q',h}(n) = [F_{w_0,n}((\varepsilon_{k,i})_{e_jk+i<w_0}) + \varepsilon_{q',h}]_{\mathrm{Teich}},$$

where for $a \in \mathbb{Z}_q$, the symbol $[a]_{\mathrm{Teich}}$ denotes the unique Teichmüller representative ε in $\mathbb{Z}_q$ such that $\varepsilon \equiv a \bmod p$. It thus follows at once that for the collection of (q', h) with $\frac{pe}{p-1} > e_jq' + h > w(f_{n-1}(x))$, the variables $\varepsilon_{q',h}(n)$ are independent random variables taking values in the Teichmüller representatives of $\mathbb{Z}_q$ with the uniform distribution. Therefore the change of weights from $w(f_{n-1}(x))$ to $w(f_n(x))$ is governed precisely by the rules of the shooting game. This ends the proof.

10. Finding jump sets inside an Eisenstein polynomial

The primary goal of this Section is to establish Theorem 10.1, which is a generalization of Theorem 1.11 from the Introduction. We will next specialize Theorem 10.1 to obtain several consequences that aim to give a sense to the reader on how efficiently one can establish the value of (I, β) in the range of the Theorem. Most notably we will see that for q odd or for $j \geqslant 1$, the set of *strongly* Eisenstein polynomials (see Definition 10.2) over $\mathbb{Q}_q(\zeta_{p^{j+1}})$ is precisely the set of polynomials giving the jump set that has the highest probability. Also we will see the relation between Theorem 10.1 and Theorem 9.1. Indeed we shall prove Theorem 10.1, by establishing the equality between the jump set of a shooting game coming from the valuation of the coefficients of an Eisenstein polynomial (denoted as $\tilde{\sigma}_j$ below) and (part of the) jump set of the shooting game constructed using the maps introduced during the proof of Theorem 9.1 (denoted as σ_j). Also we observe that Theorem 9.1 partially *follows* as a direct counting from Theorem 10.1, namely it does so for the jump sets coming from the region of Eisenstein polynomials where Theorem 1.11 applies (which for instance for $p = 2$ and $j = 0$ (i.e. over $\mathbb{Q}_2$) is empty, and for general p it misses an open set of Eisenstein polynomials). Finally we shall give examples, showing that without the main assumption on the different, the conclusion of Theorem 10.1 is not anymore valid in general.

Let $j \in \mathbb{Z}_{\geqslant 0}$, p a prime number, $f \in \mathbb{Z}_{\geqslant 1}$ and $q := p^f$. Let $e \in p^j(p-1)\mathbb{Z}_{\geqslant 1}$. Recall the notation $e_j := \frac{e}{p^j(p-1)}$, used during the proof of Theorem 9.1. Let $g(x) \in \mathrm{Eis}(e_j, \mathbb{Q}_q(\zeta_{p^{j+1}}))$ (see notation from the proof of Theorem 9.1). We proceed to define a stopping shooting game attached to g, which will be denoted as

$$\tilde{\sigma}_j(g(x)) \in \mathscr{S}_{e,\mathrm{stop}}(\rho_{e,p}, e_j, q).$$

It is defined with the following simple rule. Write $g(x) = x^{e_j} + \sum_{i=0}^{e_j-1} a_i x^i$ and give to each monomial $a_i x^i$ weight $w(a_i x^i) := e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(a_i) + i$. Arrange $w(a_i x^i)$ as an increasing sequence $n \mapsto w(a_{i_n} x^{i_n})$. Then the sequence

$$\tilde{\sigma}_j(g(x)) := \{(w(a_{i_n} x^{i_n}), v_p(i_n))\}_{n : w(a_{i_n} x^{i_n}) \leqslant e}$$

is an element of

$$\mathscr{S}_{e,\mathrm{stop}}(\rho_{e,p}, e_j, q).$$

One can now see that the pair $(I_{g(x)}, \beta_{g(x)})$ defined in the Introduction right before Theorem 1.11 is simply the jump set of the shooting game $\tilde{\sigma}_j(g(x))$. We now explain more closely how one calculates this pair. It is clear that the smallest weight is precisely $e_j = w(x^{e_j})$, consistently with the fact that in $\tilde{\sigma}_j(g(x))$ the rabbit is supposed to start from e_j. So we start with $\alpha_0 = e_j$. Next, given α_h (thus the rabbit being at $\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_{\alpha_h})e_j + \alpha_h$), to obtain a larger weight, either we find other weights that are contained in the interval $[\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_{\alpha_h})e_j, (\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_{\alpha_h}) + 1)e_j]$ or there are no such other weights. In the first case the contribution comes only from the weights α that are larger than α_h (otherwise the weight is smaller). Among these, in order to have a change of shooters and thus a contribution to the jump set, we are only interested in those requiring a smaller shot-length, i.e. with smaller $\mathrm{v}_{\mathbb{Q}_p}(\alpha_h)$, in good harmony with rule (3) of the shooting game. Thus the first such weight with smaller $\mathrm{v}_{\mathbb{Q}_p}$ is precisely where the shooter is changed. In the second case, the weight will be larger anyway, thus (as long as larger weight matters) we are now interested in examining all α with $\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_\alpha) > \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_{\alpha_h})$. Again, among these we are only interested in those where $\mathrm{v}_{\mathbb{Q}_p}(\alpha)$ becomes smaller. The smallest such weight, again, is the first place where the shot length became smaller and a new shooter came in giving the next contribution to the jump set of the shooting game. We formalize this explanation in the following procedure.

Procedure. Let $g(x) := x^{e_j} + \sum_{i=0}^{e_j-1} a_i x^i \in \mathrm{Eis}(e_j, \mathbb{Q}_q(\zeta_{p^{j+1}}))$. Set $\alpha_0 = e_j$. Given α_h, construct α_{h+1} as follows. Search if there is α such that $\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_\alpha) = \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_{\alpha_h})$ and $\alpha \geqslant \alpha_h$. If such an α exists, search if there is among them one with $\mathrm{v}_{\mathbb{Q}_p}(\alpha) < \mathrm{v}_{\mathbb{Q}_p}(\alpha_h)$. If there is such α, pick the smallest such α and declare $\alpha_{h+1} = \alpha$. If no such α exists, then look if there is an α such that $\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_\alpha) > \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_{\alpha_h})$ and $e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_\alpha) < e$. If no such α exists then set $\alpha_{h+1} = \alpha_h$. Otherwise let d be the next valuation that attains the above constraints. Look if there is α with $\mathrm{v}_{\mathbb{Q}_p}(\alpha) < \mathrm{v}_{\mathbb{Q}_p}(\alpha_h)$ and $\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_\alpha) = d$, in that case take the smallest such α as α_{h+1}. If there is none, go to the next valuation with the above constraints and do the same search, iterating until you either have to set $\alpha_{h+1} = \alpha_h$, or you have found an $\alpha_{h+1} \neq \alpha_h$. In this way the sequence $\{\alpha_i\}$ is produced. With this notation, writing $I_{\tilde{\sigma}_j(g(x))} = \{i_1 < \ldots < i_s\}$, we have that $\beta_{\tilde{\sigma}_j}(i_k) = v_p(\alpha_k)$ and $p^{\beta_{\tilde{\sigma}_j}(i_k)} i_k = e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^j+1})}(a_{\alpha_k}) + \alpha_k$.

Let j be a positive integer. Recall that for an integer e in $p^j(p-1)\mathbb{Z}_{\geqslant 1}$ we define $e_j := \frac{e}{p^j(p-1)}$.

Theorem 10.1. *Let j be a positive integer and let $e \in p^j(p-1)\mathbb{Z}_{\geqslant 1}$. For any $g(x) \in \mathrm{Eis}(e_j, \mathbb{Q}_q(\zeta_{p^{j+1}}))$, we have that the set*

$$i_1 < \ldots < i_s,$$

described in the above procedure, is equal to the set

$$\{i \in I_{\mathbb{Q}_q(\zeta_{p^j+1})[x]/g(x)} : p^{\beta_{\mathbb{Q}_q(\zeta_{p^j+1})[x]/g(x)}(i) - j - 1} i < e\}$$

and for each $k \in \{1, .., s\}$ we have that

$$\beta_{\mathbb{Q}_q(\zeta_{p^j+1})[x]/g(x)}(i_k) = \mathrm{v}_{\mathbb{Q}_p}(\alpha_k) + j + 1.$$

Proof. We proceed by looking more closely at the construction of the maps σ_j in the proof of Theorem 9.1. One first crucial ingredient is that, thanks to the shape of the conclusion, we can disregard, in the setting of the proof of Theorem 9.1, monomials with weights larger than e, so that we can perform p-th powering as if we were in a characteristic p field. Keeping

this in mind one sees from the construction of the sequence $g_n(x)$ in the proof of Theorem 9.1, that given an α_k as above, then as long as n satisfies $w(g_n(x)) < e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(a_{\alpha_k}) + \alpha_k$, then for each positive integer w_0 with

$$w(g_n(x)) < w_0 \leqslant e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(a_{\alpha_k}) + \alpha_k,$$

and

$$\mathrm{v}_{\mathbb{Q}_p}(w_0) \leqslant \mathrm{v}_{\mathbb{Q}_p}(\alpha_k),$$

one sees that

$$F_{w_0,n}((\varepsilon_{k,i})_{e_j k+i<e_j a_{\alpha_k}}) = 0.$$

This is seen by induction on n and direct inspection. The key observation is that, once we can disregard the multiples of p in p-powering, when we perform a shot, as in the proof of Theorem 9.1, it sends all the monomials having weight *smaller* than $e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(a_{\alpha_k}) + \alpha_k$ only to monomials having an index with *larger* p-adic valuation. With this, the formula appearing at the end of the proof of Theorem 9.1 gives

$$\varepsilon_{w_0,h}(n) = [F_{w_0,n}((\varepsilon_{k,i})_{e_j k+i<w_0}) + \varepsilon_{q',h}]_{\mathrm{Teich}} = [\varepsilon_{q',h}]_{\mathrm{Teich}},$$

where $w_0 = e_j q' + h$. In terms of the shooting game $\sigma_j(g(x))$, this means precisely that the rabbit will visit the position $e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(a_{\alpha_k}) + \alpha_k$, and that all the shots used before that event are of length strictly larger than $\mathrm{v}_{\mathbb{Q}_p}(\alpha_k)$. Indeed the rabbit doesn't visit any of the positions $w_0 < e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(a_{\alpha_k}) + \alpha_k$ with $\mathrm{v}_{\mathbb{Q}_p}(w_0) \leqslant \mathrm{v}_{\mathbb{Q}_p}(\alpha_k)$. But these are precisely the positions where a stop of the rabbit would have given a shot of length at most $\mathrm{v}_{\mathbb{Q}_p}(\alpha_k)$ before the position $e_j \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(a_{\alpha_k}) + \alpha_k$ was reached.

□

Observe that from the *Procedure* it is clear that the set of Eisenstein polynomials $g(x)$ such that the full jump sets of the field $\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/g(x)$ can be reconstructed from Theorem 10.1, consists precisely of those polynomials $g(x)$ having a coefficient a_i, with $(i,p) = 1$, such that $\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(a_i) < \mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(p) = p^j(p-1)$. This condition is precisely equivalent to the condition on the different

$$\mathrm{v}_{\mathbb{Q}_q(\zeta_{p^{j+1}})}(\delta(\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/g)/\mathbb{Q}_q(\zeta_{p^{j+1}})) < p^j(p-1).$$

For $j = 0$, this shows Theorem 1.11 from the Introduction. The only case where this is an empty set of Eisenstein polynomials is if $p = 2$, $j = 0$ and $2|e$: one would get a non extremal coefficient of an Eisenstein polynomial being a unit, which is impossible by definition. For all other values of p and j one obtains, with Theorem 10.1, a positive proportion of the Eisenstein polynomials where the jump set can be read off completely from the valuation of the coefficients of the polynomial, also in a fairly easy way. For p or j getting large the volume of this region gets quickly pretty large. In particular, if $(p,j) \neq (2,0)$, we next see that one can identify the set of Eisenstein polynomials giving the *most likely* jump set.

Definition 10.2. If K is a local field, $d \geqslant 2$ an integer, and $g(x) := x^d + \sum_{i=0}^{d-1} a_i x^i \in \mathrm{Eis}(d,K)$, we say that $g(x)$ is strongly Eisenstein if $\mathrm{v}_K(a_1) = 1$.

The following is a very special case of Theorem 10.1. Recall that if $e \in p^j(p-1)\mathbb{Z}_{\geqslant 1}$ we have the notation $e_j := \frac{e}{p^j(p-1)}$.

Theorem 10.3. *Let p, j, such that $(p,j) \neq (2,0)$. Let $e \in p^{j+1}(p-1)\mathbb{Z}_{\geqslant 1}$, f a positive integer and set $q := p^f$. Then $g(x) \in \mathrm{Eis}(e_j, \mathbb{Q}_q(\zeta_{p^{j+1}}))$ is strongly Eisenstein if and only if*

$$I_{\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/g(x)} = \{\frac{e}{p^{\mathrm{v}_{\mathbb{Q}_p}(e)}(p-1)}, e_j + 1\}$$

with

$$\beta_{\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/g(x)}(\frac{e}{p^{\mathrm{v}_{\mathbb{Q}_p}(e)}(p-1)}) = \mathrm{v}_{\mathbb{Q}_p}(e) + 1,\ \beta_{\mathbb{Q}_q(\zeta_{p^{j+1}})[x]/g(x)}(e_j + 1) = j + 1.$$

Observe that this gives, explicitly, the counting that the above jump set, $\{\frac{e}{p^{\mathrm{v}_{\mathbb{Q}_p}(e)}(p-1)}, e_j+1\}$ with $\frac{e}{p^{\mathrm{v}_{\mathbb{Q}_p}(e)}(p-1)} \mapsto \mathrm{v}_{\mathbb{Q}_p}(e) + 1$ and $e_j + 1 \mapsto j + 1$, occurs with probability $\frac{q-1}{q}$ among all totally ramified degree e_j-extensions of $\mathbb{Q}_q(\zeta_{p^{j+1}})$: this is the jump set occurring with highest probability. We know that this jump set occurs with probability $\frac{q-1}{q}$ also from Theorem 9.1. So in particular this fact is true also for $(2,0)$. To see that explicitly for $e = 2$, observe that among the 6 totally ramified quadratic extension of $\mathbb{Q}_2$, the only ones not giving the above jump set are $\mathbb{Q}_2(\zeta_4)$ and $\mathbb{Q}_2(\zeta_4)(1) = \mathbb{Q}_2(\sqrt{3})$; they have same mass (as we saw in general) and it equals $\frac{1}{4}$, hence the remaining mass equals $\frac{1}{2}$. But we can immediately see that in this case the same conclusion of Theorem 10.3 does not hold. Consider for instance $x^2 + 2x + 2 \in \mathrm{Eis}(2, \mathbb{Q}_2)$: it is a strongly Eisenstein polynomial. But $\mathbb{Q}_2[x]/g(x)$ is isomorphic to the extension $\mathbb{Q}_2(\zeta_4)$, whose jump set is merely $\{1\}$, with $1 \mapsto 2$, in contrast to the conclusion of Theorem 10.3. Thus in Theorem 10.3 the requirement $(p,j) \neq (2,0)$ cannot be dropped, and so in particular the assumption in Theorem 1.11 of being strongly separable cannot be avoided.

11. Filtered inclusions of principal units

In this section we explain how to attach to any strongly separable extension of local fields, L/K, a $\rho_{\infty,p}$-jump set $(I_{L/K}, \beta_{L/K})$, which is an invariant of the filtered inclusion

$$U_\bullet(K) \subseteq U_\bullet(L).$$

Moreover for $K = \mathbb{Q}_q(\zeta_p)$, we will have that

$$(I_{L/K}, \beta_{L/K}) = (I_L, \beta_L).$$

As we shall see, the fact that the extension is strongly separable will force $(I_{L/K}, \beta_{L/K})$ to be a $\rho_{e_L,p}$-jump set as well for $e_L = v_L(p)$.

We will begin to attach to any $u \in U_1(K) - U_2(K)$ a $\rho_{e_L,p}$-jump set $(I_{L/K}(u), \beta_{L/K}(u))$. We will immediately see that it is also a $\rho_{\infty,p}$-jump set, thanks to strong separability. Finally we will see the big effect of assuming strong separability: the jump set $(I_{L/K}(u), \beta_{L/K}(u))$ is independent on the choice of $u \in U_1(K) - U_2(K)$ and can be computed, by means of an immediate generalization of Theorem 1.11, from an Eisenstein polynomial giving the extension $L/\tilde{K}$, where $\tilde{K}$ is the largest unramified extension of K in L.

Let $u \in U_1(K) - U_2(K)$. Recall from Section 3.3.7 that we can attach to u the function $g_{u,U_\bullet(L)}$. We have the following. The proof is along the same lines seen in Proposition 3.35 and is therefore omitted.

Proposition 11.1. *There exists a unique jump set $(I_{L/K}(u), \beta_{L/K}(u))$ such that $g_{u,U_\bullet(L)}$ breaks at the elements of $\mathrm{Im}(\beta_{L/K}(u)) - 1$. Moreover if $i \in I_{L/K}(u)$, then*

$$g_{u,U_\bullet(L)}(i+1) = \rho_{e_L,p}^{\beta_{L/K}(u)(i)-1}(i).$$

In the torsion-free case, the jump set $(I_{L/K}(u), \beta_{L/K}(u))$ has a more familiar interpretation. In what follows the function filt-ord (as introduced in Proposition 3.37) will always be with respect to the filtered module (denoted as) $U_\bullet(L)$.

Proposition 11.2. *Let u, L, K as above and suppose moreover that $\mu_p(L) = \{1\}$. Then*

$$\text{filt-ord}(u^p) = (I_{L/K}(u), \beta_{L/K}(u)).$$

Moreover for $u_1, u_2 \in U_1(K) - U_2(K)$ we have that

$$(I_{L/K}(u_1), \beta_{L/K}(u_1)) = (I_{L/K}(u_2), \beta_{L/K}(u_2)),$$

if and only if u_1, u_2 are in the same orbit under $\text{Aut}_{\text{filt}}(U_\bullet(L))$.

Proof. This is a simple consequence of Theorem 5.2 and Proposition 3.37 combined. □

We now show that the jump set of Proposition 11.1 is independent of the choice of $u \in U_1(K) - U_2(K)$ for all strongly separable extensions L/K. Recall the way we attached to any strongly separable Eisenstein polynomial $g(x)$ a jump set $(I_{g(x)}, \beta_{g(x)})$ right after Theorem 1.7 in the Introduction.

Theorem 11.3. *Let L/K be any strongly separable extension of local fields. Let $u_1, u_2 \in U_1(K) - U_2(K)$. Then*

$$(I_{L/K}(u_1), \beta_{L/K}(u_1)) = (I_{L/K}(u_2), \beta_{L/K}(u_2)).$$

Denote by $(I_{L/K}, \beta_{L/K}) := (I_{L/K}(u), \beta_{L/K}(u))$ for any $u \in U_1(K) - U_2(K)$. Denote by $\tilde{K}$ the maximal unramified extension of K in L, and let $g(x)$ be any Eisenstein polynomial in $\tilde{K}[x]$ giving the extension $L/\tilde{K}$. We have that

$$(I_{L/K}, \beta_{L/K}) = (I_{g(x)}, \beta_{g(x)}).$$

Proof. This can be shown by precisely the same argument used in the proof of Theorem 10.1. □

In particular we find the following corollary.

Corollary 11.4. *Let L/K be a strongly separable extension of local fields, with $\mu_p(L) = \{1\}$. Then $U_1(K) - U_2(K)$ is contained in one orbit under $\text{Aut}_{\text{filt}}(U_\bullet(L))$. Call this orbit $\mathscr{O}_{L/K}$. The set $\mathscr{O}_{L/K}$ can be also characterized as follows*

$$\mathscr{O}_{L/K} = \{u \in U_\bullet(L) : u^p \in \text{filt-ord}^{-1}((I_{L/K}, \beta_{L/K}))\}.$$

In positive characteristic the statement further simplifies.

Corollary 11.5. *Let L/K be a separable extension of local fields with $char(K) = p$. Then $U_1(K) - U_2(K)$ is contained in one orbit under $\text{Aut}_{\text{filt}}(U_\bullet(L))$. Call this orbit $\mathscr{O}_{L/K}$. The set $\mathscr{O}_{L/K}$ can be also characterized as follows*

$$\mathscr{O}_{L/K} = \{u \in U_\bullet(L) : u^p \in \text{filt-ord}^{-1}((I_{L/K}, \beta_{L/K}))\}.$$

12. Jump sets under field extensions

Let $K_1/\mathbb{Q}_p(\zeta_p)$ be a finite extension. Fix a positive integer d. Consider the following natural question.

Question: Which extended admissible $\rho_{de_{K_1},p}$-jump sets are realizable as (I_{K_2},β_{K_2}) for some totally ramified extension K_2/K_1 of degree d?

In case $(d,p)=1$ the answer is very easy.

Proposition 12.1. *Let K_2/K_1 be totally ramified degree d extension, with $(d,p)=1$. Then*

$$I_{K_2}=dI_{K_1}$$

with

$$\beta_{K_2}(di)=\beta_{K_1}(i),$$

for each $i\in I_{K_1}$.

Proof. First notice that, since $(d,p)=1$, we have $dT^*_{\rho_{e,p}}\subseteq T^*_{\rho_{de,p}}$. Moreover we notice that the assignment (I_{K_2},β_{K_2}) given in the statement is clearly an extended $\rho_{de_{K_1},p}$-jump set. Next we write

$$\prod_{i\in I_{K_1}} u_i^{p^{\beta_{K_1}(i)-1}}=\zeta_p,$$

with $u_i\in U_i(K_1)-U_{i+1}(K_1)$ for each $i\in I_{K_1}$, and $\frac{pe_{K_1}}{p-1}\in I_{K_1}$ implies $u_{\frac{pe_{K_1}}{p-1}}\notin K_1^{*p}$. We thus conclude with Corollary 3.41 by noticing that $u_i\in U_{di}(K_2)-U_{di+1}(K_2)$ for each $i\in I_{K_1}$, and that if $\frac{pe_{K_1}}{p-1}\in I_{K_1}$ then we must have that $u_{\frac{pe_{K_1}}{p-1}}\notin K_2^{*p}$. Indeed taking a p-th root of $u_{\frac{pe_{K_1}}{p-1}}$ gives an unramified degree p extension of K_1 which would contradict both that $(d,p)=1$ and that K_2/K_1 is totally ramified. □

The previous proof teaches us also what is the difficulty when $(d,p)\neq 1$ in answering Question. In this case the relation

$$\prod_{i\in I_{K_1}} u_i^{p^{\beta_{K_1}(i)-1}}=\zeta_p,$$

cannot be directly used to calculate (I_{K_2},β_{K_2}), because $\mathrm{v}_{K_2}(u_i-1)\notin T_{\rho_{de_{K_1},p}}$ for each $i<\frac{pe_{K_1}}{p-1}$. Nevertheless, a more careful inspection shows that this relation can sometimes be used to extrapolate properties of (I_{K_2},β_{K_2}). This is the content of the next theorem, which, together with Theorem 12.3, contains as a very special case Proposition 12.1.

Theorem 12.2. *Let d be a positive integer and K_2/K_1 a degree d totally ramified extension. Let $i\in I_{K_1}$ with $i\neq\frac{pe_K}{p-1}$. Suppose that if the set $J:=\{j\in I_{K_1}: j<i\}$ is not empty, then*

$$\beta_{K_1}(\max(J))-\beta_{K_1}(i)>\mathrm{v}_{\mathbb{Q}_p}(d).$$

Then

$$\frac{d}{p^{\mathrm{v}_{\mathbb{Q}_p}(d)}}i\in I_{K_2}$$

with

$$\beta_{K_2}\left(\frac{d}{p^{\mathrm{v}_{\mathbb{Q}_p}(d)}}i\right)=\beta_{K_1}(i)+\mathrm{v}_{\mathbb{Q}_p}(d).$$

Proof. Take $i \neq \frac{pe_{K_1}}{p-1}$ as in the assumptions of this theorem. Write

$$\prod_{i' \in I_{K_1}} u_{i'}^{p^{\beta_{K_1}(i')-1}} = \zeta_p,$$

with $u_{i'} \in U_{i'}(K_1) - U_{i'+1}(K_1)$ for each $i' \in I_{K_1}$, and $\frac{pe_{K_1}}{p-1} \in I_{K_1}$ implies $u_{\frac{pe_{K_1}}{p-1}} \notin K_1^{*p}$. Next, for each $i' \in I_{K_1}$, write

$$\prod_{j \in A(i')} u_{i',j}^{p^{\beta(i',j)}},$$

with $A(i') \subseteq T^*_{\rho_{K_2}}$, $\mathrm{v}_{K_2}(u_{i',j} - 1) = j$ for each $j \in A(i')$ and $\frac{d}{p^{\mathrm{v}_{\mathbb{Q}_p}(d)}} i' \in A(i')$ with $\beta(i',j) = \mathrm{v}_{\mathbb{Q}_p}(d)$ and $\mathrm{v}_{K_2}(u_{i',i'}^{p^{\beta(i',i')}} - 1) < \mathrm{v}_{K_2}(u_{i',j}^{p^{\beta(i',j)}} - 1)$ for each $j \in A(i') - \{i'\}$. We now proceed to expand the above expression for ζ_p. Attach to each term $u_{i',j}$ the pair $(\mathrm{v}_{K_2}(u_{i',j}-1), \beta_{K_1}(i') + \beta(i,j))$. We see that the point attached to $u_{i,i}$, which is $(\frac{d}{p^{\mathrm{v}_{\mathbb{Q}_p}(d)}} i, \beta_{K_1}(i) + \mathrm{v}_{\mathbb{Q}_p}(d))$, is strictly smaller, with respect to $\leqslant_{\rho_{K_2}}$, than all the other points (and hence occurs precisely once). Indeed, using that (I_{K_1}, β_{K_1}) is a jump set, we see that it must be smaller than any term coming from some $u_{i'}$ with $i' > i$. On the other hand for each $i' < i$, we use the fact that $\beta_{K_2}(i') > \beta_{K_2}(i) + \mathrm{v}_{\mathbb{Q}_p}(d)$ to conclude that the point attached to $u_{i,i}$ must be smaller than any term attached to $u_{i',j}$ with $i' < i$. This is enough to conclude with Corollary 3.41. □

The case of $e^*_{K_1}$ requires no special assumptions and can be treated more easily in a different way.

Theorem 12.3. *Let d be a positive integer and K_2/K_1 a degree d totally ramified extension. Suppose $\frac{pe_K}{p-1} \in I_{K_1}$. Then $di \in I_{K_2}$ and $\beta_{K_2}(di) = \beta_{K_1}(i)$.*

Proof. This follows immediately from Proposition 5.6 and Proposition 5.5. □

Remark 12.4. In the very special case $K_1 = \mathbb{Q}_q(\zeta_p)$ one recovers the restriction that (I_{K_2}, β_{K_2}) must be an *admissible* extended $\rho_{d,p}$-jump set as a very special case of Theorem 12.2, see Theorem 1.6.

In particular Theorem 12.2 implies the following fact.[2]

Corollary 12.5. *Let d be a positive integer and K_2/K_1 a degree d totally ramified extension. Suppose that for any two consecutive elements i, j in I_{K_1} (that is $(i,j) \cap I_{K_1} = \varnothing$) we have that*

$$\beta_{K_1}(i) - \beta_{K_1}(j) > \mathrm{v}_{\mathbb{Q}_p}(d).$$

Then

$$\frac{d}{p^{\mathrm{v}_{\mathbb{Q}_p}(d)}}(I_{K_1} - \{e^*_{K_1}\}) \subseteq I_{K_2},$$

[2]We take the opportunity here to signal a typo in the way this result was mentioned in [1], where the assumption of Theorem 12.2 and the conclusion of Corollary 12.5 were accidentally merged in transcribing the statement. It was stated only with the assumption of Theorem 12.2, but the conclusion mentioned there is about *both* consecutive indexes, which we can guarantee, instead, only under the assumption of Corollary 12.5.

with

$$\beta_{K_2}(\frac{d}{p^{\mathrm{v}_{\mathbb{Q}_p}(d)}}i) = \beta_{K_1}(i) + \mathrm{v}_{\mathbb{Q}_p}(d)$$

for each $i \in I_{K_1} - \{e^*_{K_1}\}$.

References

[1] K. de Boer, C. Pagano, Calculating the power residue symbol and Ibeta, *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, **68** (2017), 923–934.

[2] L. Capuano, I. del Corso, Upper ramification jumps in abelian extensions of exponent p, *Rivista di Matematica della Universita' di Parma*, (2014), 317–329.

[3] I. Fesenko, S. Vostokov, Local fields and their extensions, *Second edition*, (2002).

[4] S. Pauli, C. Greve, Galois groups of Eisenstein polynomials whose Ramification Polygon has one side.

[5] E. Maus, Die gruppentheoretische Struktur der Verzweigungsgruppenreihen, *Journal für die reine und angewandte Mathematik* **230** (1968), 1–28.

[6] H. Miki, On the ramification numbers of cyclic p-extensions over local fields, *Journal für die reine und angewandte Mathematik* **328** (1981), 99–115.

[7] S. Mochizuki, A Version of the Grothendieck Conjecture for p-adic Local Fields, *The International Journal of Math.* **8** (1997), 499–506.

[8] D. S. Romano, Galois groups of strongly Eisenstein polynomials, Dissertation, UC Berkeley, 2007.

[9] J.P. Serre, *Local fields,* Springer-Verlag, (1995).

[10] J.P. Serre, Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, *C.R. Acad. Sc. Paris Série A* **286** (1978), 1031–1036.

[11] Y. Sueyoshi, Ramification numbers in cyclic p-extensions over p-adic number fields, *Memoirs of the Faculty of Science, Kyushu University. Series A, Mathematics* **38** (1984), 163–168.

[12] C. Pagano, E. Sofos, 4-ranks and the general model for statistics of ray class groups of imaginary quadratic number fields. `arXiv:1710.07587`, (2017).

[13] S. Pauli, B. Sinclair, Enumerating extensions of (π)-adic fields with given invariants. `arXiv:1504.06671`, (2015).

[14] Terence Tao, *An introduction to measure theory*, Graduate Studies in Mathematics, volume 126, (2017).

Mathematisch Instituut, Universiteit Leiden, 2333 CA, Leiden, Netherlands
E-mail address: `carlein90@gmail.com`

Summary

Summary

This thesis consists of three chapters. Each chapter is on a different subject. However, all chapters address issues that arise in counting arithmetically interesting objects.

Chapter 1 is a joint paper with Peter Koymans about unit equations in positive characteristic. In this paper we establish the first upper bound that is uniform in the characteristic for the number of "solutions" to the unit equation. With this tool we settle a conjecture of F. Voloch. If p is a prime number, r a positive integer, K is a field with $\mathrm{char}(K) = p$ and $\Gamma \subseteq K^* \times K^*$ a finitely generated subgroup of rank r, the unit equation is the equation

$$x + y = 1,$$

to be solved in $(x, y) \in \Gamma$ but $(x, y) \notin \Gamma^p$. Denote by $S(\Gamma)$ the set of solutions to the unit equation for Γ. Our main theorem establishes that

$$\#S(\Gamma) \leq 31 \cdot 19^r.$$

Chapter 2 is a joint paper with Efthymios Sofos about statistical properties of ray class groups of fixed integral conductor of imaginary quadratic number fields. If c is a positive integer and K is a finite extension of $\mathbb{Q}$, the *ray class group* of conductor c of K is the group

$$\mathrm{Cl}(K, c) := \frac{I(K, c)}{\mathrm{Pr}(K, c)},$$

where $I(K, c)$ is the subgroup of $I_K := \{\text{fractional ideals in } K\}$ that is generated by ideals of O_K that are coprime to c and $\mathrm{Pr}(K, c)$ is the subgroup of I_K that is generated by principal ideals (α) with $\alpha \in O_K - \{0\}$ and α congruent to 1 modulo c. When K varies among imaginary quadratic number fields whose discriminant is coprime to c and congruent to 1 modulo 4, we establish the asymptotic behavior of the natural map

$$(2\mathrm{Cl}(K, c))[2] \to (2\mathrm{Cl}(K))[2],$$

obtaining as a corollary the joint distribution of

$$(\#2(\mathrm{Cl}(K, c))[2], \#(2\mathrm{Cl}(K))[2]).$$

Even though there is a surjective natural map $2\mathrm{Cl}(K, c) \twoheadrightarrow 2\mathrm{Cl}(K)$, the surjectivity of the induced map $(2\mathrm{Cl}(K, c))[2] \to (2\mathrm{Cl}(K))[2]$ encounters a cohomological obstruction. In a refined version of our main theorem, we show the equidistribution of this obstruction in the full obstruction group (viewed as a probability space with the counting measure).

These results extend the only previously known case, which is $c = 1$, where there is only the ordinary class group. This was due E. Fouvry and J. Klüners.

Next, we extend the Cohen–Lenstra and the Gerth heuristics from class groups to general ray class groups. The Cohen–Lenstra heuristic is a probabilistic model designed by H. Cohen and H. Lenstra, which predicts conjecturally the exact asymptotic outcome of most statistical questions about the $\mathbb{Z}[\frac{1}{2}]$-module $\mathrm{Cl}(K) \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{2}]$ as K varies among imaginary quadratic number fields. Later F. Gerth formulated a heuristic about $\mathrm{Cl}(K)[2^\infty]$. We formulate a more general probabilistic model aimed at predicting the exact asymptotic outcome of most statistical questions about ray class groups, viewed as exact sequences of Galois modules. This statistical model agrees with our result on 4-ranks, yielding a heuristic interpretation of the equidistribution of the above mentioned cohomological obstructions. Moreover, our model explains the precise constants given by a theorem of I. Varma about the average 3-torsion of ray class groups. With this statistical model for ray class groups, both our results on 4-ranks and Varma's result on the 3-torsion obtain a precise heuristical explanation and are placed within a broad conjectural framework.

Chapter 3 is about the arithmetic of local fields and it mostly focuses on the sub-class of p-adic fields for some prime number p. If p is a prime number, a p-adic field is a finite field extension $K/\mathbb{Q}_p$. The multiplicative group K^* carries a natural filtration

$$K^* \supseteq O_K^* \supseteq 1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...,$$

where O_K denotes the ring of integers of K and m_K is its unique maximal ideal. One can show that the sequence

$$1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...$$

is a filtration of $\mathbb{Z}_p$-modules. In this work I give a parametrization of the set of sequences of $\mathbb{Z}_p$-modules

$$M_1 \supseteq ... \supseteq M_i \supseteq ...$$

that are *isomorphic* to $1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...$ for some local field K. This means that there exists an isomorphism of $\mathbb{Z}_p$-modules

$$\varphi : 1 + m_K \to M_1$$

such that $\varphi(1 + m_K^i) = M_i$. In case such a K exists, we say that the sequence $M_1 \supseteq ... \supseteq M_i \supseteq ...$ is *admissible*. I parametrize admissible sequences in terms of certain combinatorial objects called *jump sets*. One of the main theorems in this study is the remarkable property that this parametrization is *weight preserving*, in the following sense. It turns out that there is a natural way to attach to each jump set a weight. One can give the weight of a jump set also a natural interpretation in terms of the Haar measure. On the other hand, Serre introduced a natural probability measure on the set of totally ramified extensions of given degree of a given local field. In this chapter I show that the total mass of the set of local fields whose filtration of subgroups is isomorphic to a given admissible sequence equals the combinatorial weight of the corresponding jump set. Finally I use my identification between the set of jump sets and the set of admissible sequences to give a simpler and more conceptual proof of a classification, due to H. Miki, of the possible sets of *upper jumps* of a cyclic totally ramified p-power degree extension of a fixed p-adic field K.

Samenvatting

Samenvatting

Dit proefschrift bestaat uit drie hoofdstukken, waarbij ieder hoofdstuk een ander onderwerp behandelt. De hoofdstukken hebben echter gemeen dat zij problemen aanpakken die zich voordoen bij het tellen van aritmetisch interessante objecten.

Hoofdstuk 1 is een artikel dat geschreven is samen met Peter Koymans over eenheidsvergelijkingen in positieve karakteristiek. In dit artikel bewijzen wij de eerste bovengrens voor het aantal "oplossingen" van de eenheidsvergelijking die uniform is in de karakteristiek. Hiermee bewijzen wij een vermoeden van F. Voloch. Zij p een priemgetal, r een positief geheel getal, K een lichaam met $\mathrm{char}(K) = p$ en $\Gamma \subseteq K^* \times K^*$ een eindig voortgebrachte ondergroep van rang r. Dan is de eenheidsvergelijking de vergelijking

$$x + y = 1,$$

met $(x, y) \in \Gamma \setminus \Gamma^p$. Zij $S(\Gamma)$ de verzameling oplossingen voor de eenheidsvergelijking voor Γ. Dan zegt onze hoofdstelling dat

$$\#S(\Gamma) \leq 31 \cdot 19^r.$$

Hoofdstuk 2 is een artikel dat geschreven is samen met Efthymios Sofos omtrent statistische eigenschappen van straalklassengroepen met een gegeven gehele conductor. Zij c een positief geheel getal en K een eindige uitbreiding van $\mathbb{Q}$. Dan is de *straalklassengroep* van conductor c van K de groep

$$\mathrm{Cl}(K, c) := \frac{I(K, c)}{\mathrm{Pr}(K, c)},$$

waar $I(K, c)$ de ondergroep van $I_K := \{\text{gebroken idealen in } K\}$ is die wordt voortgebracht door idealen van O_K die copriem zijn met c, en $\mathrm{Pr}(K, c)$ de ondergroep van I_K is die wordt voortgebracht door hoofdidealen (α) met $\alpha \in O_K - \{0\}$ en α congruent met 1 modulo c. Als we K laten lopen over de imaginair-kwadratische getallenlichamen met discriminant copriem met c en congruent met 1 modulo 4, bepalen wij het asymptotische gedrag van de natuurlijke afbeelding

$$(2\mathrm{Cl}(K, c))[2] \to (2\mathrm{Cl}(K))[2].$$

Als gevolg hiervan vinden wij de gezamenlijke verdeling van

$$(\#(2\mathrm{Cl}(K, c))[2], \#(2\mathrm{Cl}(K))[2]).$$

Hoewel er een surjectieve natuurlijke afbeelding $2\mathrm{Cl}(K, c) \twoheadrightarrow 2\mathrm{Cl}(K)$ is, bestaat er een cohomologische obstructie voor de surjectiviteit van de geïnduceerde afbeelding $(2\mathrm{Cl}(K, c))[2] \to (2\mathrm{Cl}(K))[2]$. In een verfijnde versie van onze hoofdstelling

bewijzen we de gelijkverdeling van deze obstructie in de volledige obstructiegroep (gezien als een kansruimte onder de telmaat).

Deze resultaten generaliseren het enige eerder bekende geval $c = 1$, dat bewezen was door E. Fouvry and J. Klüners.

Vervolgens breiden wij de heuristieken van Cohen–Lenstra en Gerth uit van klassengroepen naar algemene straalklassengroepen. De Cohen–Lenstra-heuristiek is een onbewezen probabilistisch model van H. Cohen en H. Lenstra dat voorspelt wat de exacte asymptotische uitkomst is van de meeste statistische vragen over het $\mathbb{Z}[\frac{1}{2}]$-moduul $\mathrm{Cl}(K) \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{2}]$ als K loopt over alle imaginair-kwadratische getallenlichamen. Nadien formuleerde F. Gerth een heuristiek voor $\mathrm{Cl}(K)[2^\infty]$. Wij formuleren een algemener probabilistisch model gericht op het voorspellen van de exacte asymptotische uitkomst van de meeste statistische vragen over straalklassengroepen, gezien als exacte rijen van Galois-modulen. Dit statistische model komt overeen met ons resultaat voor 4-rangen, hetgeen een heuristische interpretatie van de gelijkverdeling van de bovengenoemde cohomologische obstructies oplevert. Bovendien verklaart ons model de precieze constanten die worden verkregen uit een stelling van I. Varma over de gemiddelde 3-torsie van straalklassengroepen. Met dit statistische model voor straalklassengroepen verkrijgen onze resultaten over de 4-rangen en Varma's resultaat over de 3-torsie een precieze heuristische verklaring en worden zij tevens geplaatst binnen een breed kader.

Hoofdstuk 3 betreft de aritmetiek van lokale lichamen, en richt zich voornamelijk op de deelklasse van p-adische lichamen, waar p een priemgetal is. Zij p een priemgetal. Dan is een *p-adisch lichaam* een eindige lichaamsuitbreiding K van $\mathbb{Q}_p$. De multiplicatieve groep K^* van K heeft een natuurlijke filtratie

$$K^* \supseteq O_K^* \supseteq 1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...,$$

waar O_K de ring van gehelen is van K en m_K het unieke maximale ideaal van O_K is. De rij

$$1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...$$

is een filtratie van $\mathbb{Z}_p$-modulen. In dit hoofdstuk geef ik een parametrisering van de verzameling van rijen van $\mathbb{Z}_p$-modulen

$$M_1 \supseteq ... \supseteq M_i \supseteq ...$$

die *isomorf* zijn met $1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...$ voor een zeker lokaal lichaam K. Dit betekent dat er een isomorfisme

$$\varphi : 1 + m_K \to M_1$$

van $\mathbb{Z}_p$-modulen met $\varphi(1 + m_K^i) = M_i$ bestaat. In het geval dat zo'n K bestaat, zeggen we dat de rij $M_1 \supseteq ... \supseteq M_i \supseteq ...$ *toelaatbaar* is. Ik parametriseer toelaatbare rijen in termen van zekere combinatorische objecten genaamd *sprongverzamelingen*. Een van de hoofdstellingen in dit proefschrift is de opmerkelijke eigenschap dat deze parametrisatie *gewichtbehoudend* is. Er blijkt namelijk een natuurlijke combinatorische manier te zijn om aan iedere sprongverzameling een gewicht toe te kennen. Deze toekenning heeft een natuurlijke interpretatie in termen van de Haar-maat. Anderzijds introduceerde Serre een natuurlijke kansmaat op de verzameling van volledig vertakte uitbreidingen van gegeven graad over een gegeven

lokaal lichaam. In dit hoofdstuk laat ik zien dat het totale gewicht van de verzameling van lokale lichamen waarvoor de filtratie van ondergroepen isomorf is met een gegeven toelaatbare rij, gelijk is aan het combinatorische gewicht van de bijbehorende sprongverzameling. Tot slot gebruik ik mijn identificatie tussen de verzameling van sprongverzamelingen en de verzameling van toelaatbare rijen om een eenvoudiger en conceptueler bewijs te geven van een classificatie van H. Miki van de mogelijke verzamelingen van *bovenste sprongen* van een cyclische totaal vertakte uitbreiding van p-macht graad over een gegeven p-adisch lichaam K.

Stellingen

Stellingen

1

Let p be a prime number and let K be a field with $\mathrm{char}(K) = p$. Let $\Gamma \subseteq K^* \times K^*$ be a finitely generated subgroup. Denote by $r := \dim_{\mathbb{Q}}(\Gamma \otimes_{\mathbb{Z}} \mathbb{Q})$. Then

$$\#\{(x, y) \in \Gamma - \Gamma^p : x + y = 1\} \leq 31 \cdot 19^r.$$

2

Let p be an odd prime number and denote by ζ_p an element of $\mathbb{Q}_p^{\mathrm{sep}}$ having multiplicative order equal to p. Let d be in $p\mathbb{Z}_{\geq 1}$. For each $h \in \{1, ..., d-1\}$ we say that a polynomial $g(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$ in $\mathbb{Q}_p(\zeta_p)[x]$ is *h-Eisenstein* if $a_i \in (1-\zeta_p)\mathbb{Z}_p[\zeta_p]$ for each $i \in \{0, ..., d-1\}$ and $a_i \in (1-\zeta_p)\mathbb{Z}_p[\zeta_p] - (1-\zeta_p)^2\mathbb{Z}_p[\zeta_p]$ if and only if $i \in \{0, h\}$.

Let k, j be in $\{1, ..., d-1\}$ with $\gcd(p, kj) = 1$, and let $r_1(x), r_2(x)$ be respectively k- and j-Eisenstein polynomials of degree d. Then one has $k = j$ if and only if there is a group isomorphism $\varphi : (\frac{\mathbb{Z}_p[\zeta_p][x_1]}{r_1(x_1)})^* \to (\frac{\mathbb{Z}_p[\zeta_p][x_2]}{r_2(x_2)})^*$ such that

$$\varphi(1 + x_1^n \frac{\mathbb{Z}_p[\zeta_p][x_1]}{r_1(x_1)}) = 1 + x_2^n \frac{\mathbb{Z}_p[\zeta_p][x_2]}{r_2(x_2)},$$

for every positive integer n.

3

For a number field K and a positive integer c, we denote by $\mathrm{Cl}(K)$ the class group of K and by $\mathrm{Cl}(K, c)$ the ray class group of conductor c of K.

Let l be a prime number congruent to 3 modulo 8. Let $\mathcal{P}$ be the set of imaginary quadratic number fields K such that $\mathrm{disc}(K)$ is congruent to 1 modulo 4, $2\mathrm{Cl}(K)[2^\infty]$ is a cyclic non-trivial group and l is inert in K. Let $\mathcal{P}_0$ be the set of $K \in \mathcal{P}$ such that $\mathrm{Cl}(K, l)[2^\infty] \simeq_{\mathrm{ab.gr.}} \mathbb{Z}/4\mathbb{Z} \oplus \mathrm{Cl}(K)[2^\infty]$. We have that

$$\lim_{X \to \infty} \frac{\#\{K \in \mathcal{P}_0 : |\mathrm{disc}(K)| < X\}}{\#\{K \in \mathcal{P} : |\mathrm{disc}(K)| < X\}} = \frac{1}{2}.$$

Moreover, if $K \in \mathcal{P} - \mathcal{P}_0$ then $2\mathrm{Cl}(K, l)[2^\infty]$ is also cyclic with $\#2\mathrm{Cl}(K, l)[2^\infty] = 2 \cdot \#2\mathrm{Cl}(K)[2^\infty]$.

4

Let G be a topological group and H a normal subgroup of G. A *set of topological normal generators* of H in G is a subset X of H such that $\{gxg^{-1} : x \in X, g \in G\}$ is a set of topological generators of H.

Let p be a prime number and suppose that G is a pro-p group. Let moreover r be a positive integer. Then the group G is isomorphic to $\mathbb{Z}_p^r$ if and only if for every open normal subgroup N of G, a set of topological normal generators of N in G of smallest possible size has cardinality r.

5

Let L/K be a finite Galois extension of fields, with $\mathrm{Gal}(L/K)$ being an elementary abelian 2-group and with $\mathrm{char}(K) \neq 2$. Denote by $\mathbb{F}_2[\mathrm{Gal}(L/K)]$ the group ring of $\mathrm{Gal}(L/K)$ with coefficients in $\mathbb{F}_2$; this is a local Gorenstein $\mathbb{F}_2$-algebra. For an element $\alpha \in L^*$ denote by $\tilde{L}_{\sqrt{\alpha}}$ the normal closure of $L(\sqrt{\alpha})$ over K. Then the element $N_{L/K}(\alpha)$ is not in L^{*2} if and only if

$$\mathrm{Gal}(\tilde{L}_{\sqrt{\alpha}}/K) \simeq_{\mathrm{grp.}} \mathbb{F}_2[\mathrm{Gal}(L/K)] \rtimes \mathrm{Gal}(L/K),$$

where the implicit action in the semidirect product is given by the regular representation.

6

Let r be a positive integer and p a prime number. Let A be a free module over the ring $\mathbb{Z}/p^{r+1}\mathbb{Z}$ and G be a subgroup of $\mathrm{Aut}_{\mathrm{gr}}(A)$. Suppose that $p-1 > \mathrm{rk}_{\mathbb{Z}/p^{r+1}\mathbb{Z}}(A)$ and that A^G admits a cyclic direct summand of size p^r. Then there exists a cyclic subgroup H_0 of G such that A^{H_0} admits a cyclic direct summand of size p^r.

7

Let p be a prime number. Let $G := (\mathbb{Z}/p\mathbb{Z})^2$. Then there is a $\mathbb{Z}/p^2\mathbb{Z}[G]$-module A, free of rank $p(p+1)$ as a $\mathbb{Z}/p^2\mathbb{Z}$-module, such that A^G admits a cyclic direct summand of size p, but A^H doesn't for any proper subgroup H of G.

For a commutative ring R and for an R-module N, the *annihilator* of N is the set $\mathrm{Ann}_R(N) := \{x \in R : \forall n \in N, xn = 0\}$; it is an ideal of R. An R-module N is said to be *faithful* if $\mathrm{Ann}_R(N) = 0$.

8

Let R be a commutative ring, M a faithful R-module and J an ideal of R. Then $M/\mathrm{Ann}_R(J)M$ is a faithful $R/\mathrm{Ann}_R(J)$-module.

9

Let k be a field and A a commutative k-algebra such that $\dim_k(A) < \infty$. Suppose A has a unique maximal ideal m_A, and that $\dim_k(A/m_A) = 1$. Let M be a faithful A-module. Then

$$\dim_k(M) \geq 2\sqrt{\dim_k(A) - 1}.$$

Acknowledgments

Acknowledgments

I want to express my deepest gratitude to Hendrik Lenstra for the mathematics that I have learned out of our frequent meetings, during the past 4 years. I am especially grateful for all the insightful conversations that were *not* directly related to the present dissertation or to my own research. Yet, all these meetings have had a tremendous impact on this thesis and on my contributions elsewhere, as they shaped my way of organizing mathematical knowledge and of thinking about mathematical problems. I would also like to thank him for extraordinary patience and perseverance in trying to improve my unsatisfactory communication skills.

I am very grateful to Jan-Hendrik Evertse for suggesting interesting projects about the unit equation to Peter Koymans and me, and for providing important feedback on our progress and helpful remarks on earlier versions of our articles.

Many thanks to Peter Stevenhagen and Ronald Van Luijk, for several helpful conversations about mathematics, and also for investing a substantial amount of time and energies in providing constructive criticism of my deficiencies in communicating mathematics.

I am indebted to René Schoof for educating me in algebra and number theory during my bachelor and master courses in Rome and for helping me to find a Ph.D. position in Leiden.

Many results of this thesis were stimulated by the presence of the Kloosterman seminar that has taken place in Leiden from the Summer of 2016 until the Spring of 2017. All the participants are warmly thanked for contributing to such an inspiring atmosphere. Two of them deserve special gratitude. I am grateful to Efthymios Sofos for our fruitful collaborations, for teaching me some analytic number theory and for constructive criticism of my defective communication skills. Many thanks go to Peter Koymans for all the energy and open minded collaboration that he invested in the past 2 years of weekly meetings on challenging mathematical problems.

It is a pleasure to thank Mima Stajnokovski, Djordjo Milovic and Raymond Van Bommel for frequent mathematical discussions and for their precious friendship.

The University of Warwick, the Max Planck Institute and the University of Glasgow are gratefully acknowledged for their kind hospitality.

For all sorts of practical help I thank Carla Musella, Bianca Magliano, Paola, Guido, Marco and Paolo Pagano and Guido Lido. I thank all of them also for encouraging me to focus on the present dissertation, as well as for occasionally distracting me from it with refreshing conversations.

Curriculum Vitae

Curriculum Vitae

Carlo Pagano was born on March 17, 1990, Naples (Italy), where he received his pre-university education, with a focus on classical studies and music. He received his high school diploma from Liceo Classico A. Genovesi, Napoli.

After high school, Carlo enrolled in a B.A. in mathematics at the University of Rome Tor Vergata. During this period he participated in several mathematical competitions for university students and in 2012 he obtained a silver medal at the IMC. He graduated in 2013 with a thesis on structural and combinatorial aspects of finite Coxeter groups: the thesis was titled *Gruppi di riflessione finiti* and was supervised by Ilaria Damiani. In 2013 he enrolled in a Master program in Mathematics in the same university, where he was awarded a scholarship funded by INDAM (Istituto Nazionale di Alta Matematica), upon obtaining second placement at the corresponding national exam. He received his Master degree from the University of Rome Tor Vergata in September 2014. His master thesis, entitled *Il teorema di Fontaine*, was supervised by René Schoof.

In September 2014 he enrolled in the Ph.D. in mathematics of Leiden University, under the supervision of Hendrik Lenstra. Upon completing his doctoral studies Carlo will join the Max Planck Institute in Bonn as a post-doc from September 2018 to August 2020, and then the University of Glasgow from September 2020 to September 2022.