Technische Universität Kaiserslautern

On the distribution of eigenspaces in classical groups over finite rings and the Cohen-Lenstra heuristic

Michael Adam
AG Algebra, Geometrie und Computeralgebra
Fachbereich Mathematik
TU Kaiserslautern

Vom Fachbereich Mathematik der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades Doktor der Naturwissenschaften
(Doctor rerum naturalium, Dr. rer. nat.) genehmigte Dissertation

1. Gutachter: Prof. Dr. Gunter Malle
2. Gutachter: Prof. Dr. Jürgen Klüners

Datum der Disputation: 13.02.2014

D 386

The measure of our intellectual capacity is the capacity to feel less and less satisfied with our answers to better and better problems.

(Charles West Churchman(1913-2004))

Danksagung

An erster Stelle möchte ich mich bei Prof. Dr. Gunter Malle für das Bereitstellen eines sehr aktuellen und interessanten Themas und die exzellente Betreuung während der gesamten Dauer meiner Promotion bedanken. Viele Ideen und Anstöße sind während der zahlreichen Diskussionen mit Herrn Malle entstanden und haben so einen wesentlichen Beitrag zum Entstehen der vorliegenden Arbeit geleistet.

Als Nächstes möchte ich ganz herzlich Prof. Dr. Claus Fieker und Tommy Hofmann danken, die jederzeit ein offenes Ohr für meine Probleme hatten und in den meisten Fällen mir auch weiterhelfen konnten.

Außerdem möchte ich hier die Möglichkeit nutzen und mich bei einigen Menschen, die mich während meines Studiums und meiner Promotionszeit begleitet haben, für die schöne gemeinsame Zeit bedanken. Vielen Dank Dimitri Bräul, Sergej Shirajew, Benedikt Heinrich, Benedict Baur, Sebastian Geissel, Robert Voßhall, Birte Schmidtmann und Wladimir Emelin.

Ein ganz besonderer Dank geht an meine Eltern, Tatjana und Vladimir Adam, und meine Schwestern Evgenija und Kristina Adam, die für mich während der letzten Jahre immer da waren und eine wichtige Stütze bildeten.

Für die finanzielle Unterstützung bedanke ich mich bei der Deutschen Forschungsgesellschaft.

Diese Arbeit ist ein Teil des Projektes "Class groups and unramified extensions of number fields" im Schwerpunktprogramm 1489.

Abstract

In 2006 Jeffrey Achter proved that the distribution of divisor class groups of degree 0 of function fields with a fixed genus and the distribution of eigenspaces in symplectic similitude groups are closely related to each other. Gunter Malle proposed that there should be a similar correspondence between the distribution of class groups of number fields and the distribution of eigenspaces in certain matrix groups. Motivated by these results and suggestions we study the distribution of eigenspaces corresponding to the eigenvalue one in some special subgroups of the general linear group over finite factor rings of rings of integers of number fields and derive some conjectural statements about the distribution of p-parts of class groups of number fields over a base field K_0. Here, our main interest concerns the case that K_0 contains the pth roots of unity because in this situation the p-parts of class groups seem to behave in an other way than predicted by the well-known conjectures of Henri Cohen, Hendrik Lenstra and Jacques Martinet. In 2010, based on computational data Malle has succeeded in formulating a conjecture in the spirit of Cohen and Martinet for this case. Using our investigations about the distribution in matrix groups we generalize the conjecture of Malle to a more abstract level and establish a theoretical backup for these statements.

Contents

Chapter 1

Introduction

This thesis combines two sectors of pure mathematics, namely on the one hand we deal with topics in number theory and on the other hand we develop some combinatorial results in matrix theory. Certainly, our main interest affects the number theoretical aspects, particularly we would like to understand the behavior of class groups of number fields. Class groups are one of the most important invariants of number fields and can be used to answer questions about possible solutions of Diophantine equations and factorization of big numbers. Unfortunately, there is not much known about class groups in general, for instance it is still an open question if there are infinitely many number fields with trivial class group. Because of the fact that class groups are finite abelian groups it is sufficient to look at the Sylow p-subgroups of class groups with p a prime number and study these objects.

At this the celebrated paper of Henri Cohen and Hendrik Lenstra [11, 1983] plays the decisive role to push that issue forward. Basically they presented a heuristic saying that a given finite abelian p-group should occur in "nature" with probability inversely proportional to the order of its automorphism group. As an application of this universal principle Cohen and Lenstra stated some conjectural results about the distribution of p-parts of class groups of quadratic number fields. In 1990 Cohen and Jacques Martinet [12] extended these ideas to arbitrary number fields. This work still forms the basis for further investigations on this topic and finds a big acceptance by numerical data.

However, Gunter Malle [37, 38] discovered that in the situation where we consider the distribution of p-parts of class groups of number fields over a base field K_0 which contains p-th roots of unity the predicted distributions by Cohen and Martinet seem to be false, in particular always for $p = 2$. Malle attested his doubts with lots of computational support and worked out a conjectural statement in the spirit of Cohen-Lenstra-Martinet for this particular situation.

Due to the analogy of number fields and function fields it is not surprising that people are concerned with the respective problems in the function field case. Eduardo Friedman and Lawrence C. Washington [20, 1989] were the first ones who addressed the quadratic function field case and published some conjectural results for the distribution of divisor class groups of degree 0. It took a bit of time until the next essential step was done. Namely, in 2006 Jeffrey Achter [4] managed to prove some results about the distribution of divisor class groups of function fields by establishing a connection to the distribution of eigenspaces in symplectic similitude groups.

In this text we pick up the idea of Achter and transfer it to the number field case. Even though we can not present some proven theorems about a similar connection in our situation we use our computations of the distribution of eigenspaces corresponding to the eigenvalue one in certain matrix groups over finite factor rings of the rings of integers of number fields in order to derive some very general conjectural statements about the distribution of p-parts of class groups of number fields in the setting of Malle.

Studying matrix groups und trying to understand what a random element looks like is a very interesting task and has been treated by several authors (see for instance [8, 24, 25]). The listed works consider matrix groups over finite fields. Here we look at these over finite rings, precisely over factor rings of rings of integers of number fields and determine the proportion of elements with a fixed 1-eigenspace. Formulating it in a more detailed way: we calculate for a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module H, where $\mathcal{O}$ is the ring of integers of a number field and $\mathfrak{p}$ a non-zero prime ideal of $\mathcal{O}$ with $q = |\mathcal{O}/\mathfrak{p}|$, the limit

$$P_{G,\infty,q,f}(H) := \lim_{n\to\infty} P_{G,n,q,f}(H) := \lim_{n\to\infty} \frac{|\{g \in G_n(\mathcal{O}/\mathfrak{p}^f) \mid \ker(g - \mathbf{1}_n) \cong H\}|}{|G_n(\mathcal{O}/\mathfrak{p}^f)|}$$

for certain classical groups G of increasing dimension n. In the case where G is the general linear group we thus generalize the results of Jason Fulman in [22] and in the case of symplectic and orthogonal groups we extend his work [23].

As mentioned above our hope is to derive some evidence about the distribution of class groups of number fields from our calculations in matrix groups. We shall see that $P_{\mathrm{GL},\infty,p,f}$ agrees with the Cohen-Lenstra probability (see Rem. 4.10). Modelling the setting of Malle (presence of p-th roots of unity in the base field) we introduce the following subgroup of the general linear group

$$\mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^f) := \{g \in \mathrm{GL}_{2n}(\mathcal{O}/\mathfrak{p}^f) \mid g^t J_n g \equiv J_n \bmod \mathfrak{p}^m\}$$

where $n,\ f,\ m$ are natural numbers with $m \leq f$ and J_n denotes, as usual, the skew-symmetric matrix defining the symplectic form.

We shall observe that $P_{\mathrm{Sp}_{2n}^{(m)},\infty,p,f}$ should correspond to the distribution of p-parts of class groups of number fields over K_0 containing the p^mth but not the p^{m+1}st roots of unity (see Conj. 5.14). To be able to derive these consequences first of all we need to calculate $P_{G,\infty,q,f}(H)$. Here are the crucial results we obtained

$$(1)\qquad P_{\mathrm{GL},\infty,q,f}(H) = (q)_\infty \cdot \frac{1}{|\mathrm{Aut}_{\mathcal{O}}(H)|} \qquad \text{(see Thm. 4.8)},$$

$$(2)\quad P_{\mathrm{Sp}^{(1)},\infty,q,f}(H) = \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{(q)_r \cdot q^{\binom{r}{2}}}{|\mathrm{Aut}_{\mathcal{O}}(H)|} \qquad \text{(see Thm. 4.24)}$$

where r is the $\mathfrak{p}$-rank of H and $(q)_\infty$ is some well-defined constant. Using the latter statement and the notion of u-probabilities (see 5.1) of finite abelian groups we prove some statements (see 5.9, 5.10, 5.11) which give a theoretical backup for Malle's conjecture. At the end we present a very general conjecture which describes the behavior of p-parts of class groups in the presence of p^mth roots of unity.

This text is organized in the following way. In the second chapter we collect the basic and necessary notations, definitions and results from mathematical areas we need here. Chapter 3 summarizes the knowledge about the distribution of class groups starting with the Cohen-Lenstra heuristic and examines the situation where roots of unity come into play. At the end of Chapter 3 we give an overview about proven results on this topic and draw some parallels to similar problems. The next chapter studies the distribution of eigenspaces corresponding to the eigenvalue one in matrix groups[1]. In the last chapter we combine the results from the previous one with the ideas and concepts from the third chapter which allows us to formulate some statements about the distribution of class groups.

[1] Main parts of this chapter are published in [1].

Chapter 2

Preliminaries

In this chapter we introduce the basic notations of the following text and bring together the necessary tools for the upcoming chapters. In doing so we recall some properties of modules over Dedekind domains, present certain classical groups over finite rings and state some results about q-binomials. Moreover we collect the significant terms, together with their basic attributes, of the field of number theory and the theory of partitions and Hall polynomials. Also we review the crucial definitions and statements from a paper written by K. Dutta and A. Prasad [17] and derive some consequences for a special type of Hall numbers we are interested in later in this text.

2.1 Notations

The set of positive natural numbers (without zero) is denoted by $\mathbb{N}$. The greatest common divisor of two natural numbers a and b is expressed by $\gcd(a, b)$. For the set of positive primes we write $\mathbb{P}$. Given a finite group G we denote by $\mathrm{Aut}(G)$ the automorphism group of G and by G_p some Sylow p-subgroup of G for a prime p. For $g \in G$ we write $\mathrm{ord}(g)$ for the order of g in G. The identity element of a group G we denote by $\mathbf{1}_G = \mathbf{1}$. By a ring we always understand a commutative ring with identity and we write $R^\times$ for the unit group of R. For the set of prime ideals of a ring R we write $\mathrm{Spec}(R)$. The cyclic group of order p^α, for $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$, we denote by $\mathbb{Z}/p^\alpha\mathbb{Z}$ and also the corresponding quotient ring. The finite field with q elements where q is a prime power we denote by $\mathbb{F}_q$. For a ring R and $n \in \mathbb{N}$ we write $\mathrm{Mat}_n(R)$ for the set of all square matrices of dimension n with entries in R. The identity matrix in $\mathrm{Mat}_n(R)$ we label with $\mathbf{1}_n$. For an element $g \in \mathrm{Mat}_n(R)$ we denote by g^t its transpose and by $\det(g)$ its determinant.

For natural numbers n and k we set

$$(n)_k := \prod_{i=1}^{k} (1 - n^{-i})$$

and

$$(n)_\infty := \prod_{i=1}^{\infty}(1-n^{-i}).$$

Note that the latter product converges for all n.

Convention: If not otherwise specified we always mean by p a positive prime number.

2.2 q-Binomials

Here we define for a prime power q the notion of q-binomials and state some identities concerning them.

Definition 2.1. For natural numbers n and k with $k \leq n$ and a prime power q let

$$\binom{n}{k}_q := \frac{(q^n-1)\cdots(q^n-q^{k-1})}{(q^k-1)\cdots(q^k-q^{k-1})} \text{ if } k>0, \text{ and } \binom{n}{0}_q := 1.$$

Directly one sees the following identity.

Corollary 2.2. *For n, k and q as in the definition above we have*

$$\binom{n}{k}_q = \binom{n}{n-k}_q.$$

The next statement is a well-known result in combinatorics and will be used in Chapter 4 of this thesis.

Proposition 2.3. *Let $k \leq n$ be natural numbers. Then*

$$|\{U \leq (\mathbb{F}_q)^n \mid \dim(U)=k\}| = \binom{n}{k}_q.$$

Proof. See [29, Sect. 2]. □

2.3 Classical groups over finite rings

Here we introduce the classical matrix groups of interest and determine their orders.

Definition 2.4. Let $n,\ f$ be natural numbers. For a ring R and a non-zero prime ideal $\mathfrak{p} \trianglelefteq R$ of R we define

(a) the *general linear group* over the ring $R/\mathfrak{p}^f$ as

$$\mathrm{GL}_n(R/\mathfrak{p}^f) := \{g \in \mathrm{Mat}_n(R/\mathfrak{p}^f) \mid \det(g) \in (R/\mathfrak{p}^f)^\times\},$$

(b) the *symplectic group* over the ring $R/\mathfrak{p}^f$ as

$$\mathrm{Sp}_{2n}(R/\mathfrak{p}^f) := \{g \in \mathrm{GL}_{2n}(R/\mathfrak{p}^f) \mid g^t J_n g = J_n\},$$

where $J_n := \begin{pmatrix} 0 & \mathbf{1}_n \\ -\mathbf{1}_n & 0 \end{pmatrix} \in \mathrm{GL}_{2n}(R/\mathfrak{p}^f)$.

(c) the *m-th symplectic group* for $m \leq f$ over the ring $R/\mathfrak{p}^f$ as

$$\mathrm{Sp}_{2n}^{(m)}(R/\mathfrak{p}^f) := \{g \in \mathrm{GL}_{2n}(R/\mathfrak{p}^f) \mid g^t J_n g \equiv J_n \bmod \mathfrak{p}^m\},$$

(d) the *orthogonal group* over the ring $R/\mathfrak{p}^f$ as

$$\mathrm{O}_n(R/\mathfrak{p}^f) := \{g \in \mathrm{GL}_{2n}(R/\mathfrak{p}^f) \mid gg^t = \mathbf{1}_n\}.$$

Remark 2.5. In order to avoid a cluster of different cases we only consider orthogonal groups over rings of odd characteristic.

In the following we determine the order of the groups above for a specified class of rings R.

Proposition 2.6. *Let R be a Dedekind ring with finite quotients and let $\mathfrak{p} \trianglelefteq R$ be a prime ideal of R with $q = |R/\mathfrak{p}|$. Then for natural numbers $m,\ n$ and f with $m \leq f$ the following holds*

(a) $|\mathrm{GL}_n(R/\mathfrak{p}^f)| = q^{n^2(f-1)} \cdot |\mathrm{GL}_n(R/\mathfrak{p})|$,

(b) $|\mathrm{Sp}_{2n}(R/\mathfrak{p}^f)| = q^{(2n^2+n)(f-1)} \cdot |\mathrm{Sp}_{2n}(R/\mathfrak{p})|$,

(c) $|\mathrm{Sp}_{2n}^{(m)}(R/\mathfrak{p}^f)| = q^{4n^2(f-m)} \cdot |\mathrm{Sp}_{2n}(R/\mathfrak{p}^m)|$,

(d) $|\mathrm{O}_n(R/\mathfrak{p}^f)| = q^{\binom{n}{2}(f-1)}|\mathrm{O}_n(R/\mathfrak{p})|$.

Proof. For $f \in \mathbb{N}$ the ring $R/\mathfrak{p}^f$ is local with the maximal ideal $\mathfrak{p}/\mathfrak{p}^f$. According to the Theorem 2.7.(3) in [30] we get then

$$|\mathrm{GL}_n(R/\mathfrak{p}^f)| = |\mathfrak{p}/\mathfrak{p}^f|^{n^2} \cdot |\mathrm{GL}_n(R/\mathfrak{p})|$$

and with $q^{f-1} = |\mathfrak{p}/\mathfrak{p}^f|$ we obtain (a).
To show part (b) we pick up the idea of Juncheol Han from [30]. So we need to determine the order of the kernel of the following natural homomorphism

$$\theta : \mathrm{Sp}_{2n}(R/\mathfrak{p}^f) \to \mathrm{Sp}_{2n}(R/\mathfrak{p}).$$

We do this in an inductive way. For $f \geq 2$ the elements of the kernel of

$$\theta_f : \mathrm{Sp}_{2n}(R/\mathfrak{p}^f) \to \mathrm{Sp}_{2n}(R/\mathfrak{p}^{f-1})$$

are of the form $h := \mathbf{1}_{2n} + g$ for a matrix $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Mat}_{2n}(\mathfrak{p}^{f-1}/\mathfrak{p}^f)$. Furthermore h needs to be an element of the symplectic group $\mathrm{Sp}_{2n}(R/\mathfrak{p}^f)$, so h fulfills the condition $h^t J_n h = J_n$ in $\mathrm{GL}_{2n}(R/\mathfrak{p}^f)$. But this leads to the following criterion for g

$$B = B^t, \ C = C^t \text{ and } A^t + D = 0_n.$$

For this reason we obtain $|\ker(\theta_f)| = q^{\binom{n+1}{2}} q^{\binom{n+1}{2}} q^{n^2} = q^{2n^2+n}$. Inductively we get

$$|\mathrm{Sp}_{2n}(R/\mathfrak{p}^f)| = q^{(2n^2+n)(f-1)} |\mathrm{Sp}_{2n}(R/\mathfrak{p})|.$$

From the definition of $\mathrm{Sp}_{2n}^{(m)}(R/\mathfrak{p}^f)$ we immediately observe

$$|\mathrm{Sp}_{2n}^{(m)}(R/\mathfrak{p}^f)| = |\mathrm{Sp}_{2n}(R/\mathfrak{p}^m)| \cdot |\ker(\theta)|,$$

where θ is the natural epimorphism $\theta : \mathrm{GL}_{2n}(R/\mathfrak{p}^f) \to \mathrm{GL}_{2n}(R/\mathfrak{p}^m)$. By [30] we have

$$|\ker(\theta)| = q^{4n^2(f-m)}$$

and thereby the result follows.
To verify part (d) we repeat the proof of (b) replacing symplectic groups by orthogonal groups.

So let

$$\theta_f : \mathrm{O}_n(R/\mathfrak{p}^f) \to \mathrm{O}_n(R/\mathfrak{p}^{f-1})$$

be the natural epimorphism. Then $h \in \mathrm{O}_n(R/\mathfrak{p}^f)$ is in the kernel of θ_f if and only if $h = \mathbf{1}_n + g$ for $g \in \mathrm{Mat}_n(\mathfrak{p}^{f-1}/\mathfrak{p}^f)$. With that the condition $hh^t = \mathbf{1}_n$ implies $g = -g^t$ and therefore we obtain

$$|\ker(\theta_f)| = q^{\binom{n}{2}}.$$

Inductively we get the statement. □

Remark 2.7. The order of classical groups over finite fields is well-known. See for instance [3, Chap. IV, § 3] for the order of the general linear groups over $\mathbb{F}_q$. The order of $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ and of $\mathrm{O}_n(\mathbb{F}_q)$ is given in [3, Chap. III, § 6].

2.4 Partitions and Hall polynomials

In this part we give a description of finite abelian p-groups via partitions and introduce the notion of Hall polynomials and Hall numbers. For a good introduction to partitions and their applications consult the book of G. Andrews [2]. A basic work on Hall polynomials is the text of I. Macdonald [36].
We start by repeating the definition of a partition and its describing terms.

Definition 2.8. We call a sequence $\lambda = (\lambda_1, \dots, \lambda_r, \dots)$ of non-negative integers a *partition* where $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r \geq \dots$ and λ contains only finitely many non-zero terms. The non-zero λ_i are called the *parts* of λ. The number of parts is the *length* of λ, denoted by $l(\lambda)$, and the sum of parts is the *weight* of λ, denoted by $|\lambda|$. The number $m_i(\lambda) := |\{j \mid \lambda_j = i\}|$ is called the *multiplicity* of i in λ. If $|\lambda| = n$ we say that λ is a partition of n.

We now present an involution on the set of partitions which is a kind of reflection.

Definition 2.9. Given a partition $\lambda = (\lambda_1, \lambda_2, \dots)$ we define the *conjugate (partition)* $\lambda' = (\lambda'_1, \lambda'_2, \dots)$ of λ by $\lambda'_i := |\{j \mid \lambda_j \geq i\}|$ for $i \geq 1$.

Now we link the term of a partition with that of a finite abelian p-group.

Definition 2.10. Given a finite abelian p-group $G = \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{\lambda_t}\mathbb{Z}$ we say G is of *type* $\lambda = (\lambda_1, \dots, \lambda_t)$.

Remark 2.11. By the classification theorem for finite abelian p-groups one can write every finite abelian p-group in an unique way as product of cyclic groups of order p^k for some k. So we have a one to one correspondence between the set of all isomorphism classes of finite abelian p-groups and the set of all partitions of the natural numbers modulo the equivalence relation " $\sim$ ", where we write $\lambda \sim \mu$ for partitions $\lambda = (\lambda_1, \dots, \lambda_r, 0, 0, \dots)$ and $\mu = (\mu_1, \dots, \mu_s, 0, 0, \dots)$ with $\lambda_r \neq 0 \neq \mu_s$ if and only if $r = s$ and $\lambda_i = \mu_i$ for all $i \leq r$.

At this point we bring in the notion of Hall polynomials and in the next proposition we state elementary facts about these.

Definition 2.12. Let G be a finite abelian p-group of type λ. The *Hall polynomial* $g^{\lambda}_{\mu,\nu}$ is a function such that, for any prime p, $g^{\lambda}_{\mu,\nu}(p)$ is the number of subgroups H of G such that H has type μ and G/H has type ν. We call these numbers the *Hall numbers.*

Remark 2.13. In the situation of the above definition we also call ν the *cotype* of H.

Proposition 2.14. *Let $g^{\lambda}_{\mu,\nu}$ be a Hall polynomial. Then we have*

(a) $g^{\lambda}_{\mu,\nu}(x) \in \mathbb{Z}[x]$,

(b) $g^{\lambda}_{\mu,\nu}(p) = g^{\lambda}_{\nu,\mu}(p)$ for all $p \in \mathbb{P}$.

Proof. See [36, Chap. II, (4.1)-(4.3)]. □

Now we bring together the set up we need to characterize the type of Hall numbers we want to deal with later in this text.

Definition 2.15. Given two partitions λ and μ we write $\lambda \supset \mu$ if $\lambda_i \geq \mu_i$ for all $i \in \mathbb{N}$. For $\lambda \supset \mu$ we call the set-theoretic difference $\theta = \lambda - \mu$ a *skew diagram.* The *conjugate* of θ is defined by $\theta' := \lambda' - \mu'$ and the *weight* of θ is given by $|\theta| = |\lambda| - |\mu|$. We say θ is a *horizontal m-strip* if $|\theta| = m$ and $\theta'_i \leq 1$.

A direct consequence of the definition above is the following lemma.

Lemma 2.16. *A skew diagram $\lambda - \mu$ is a horizontal strip if and only if the condition $\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \mu_2 \geq \dots$ is satisfied.*

Proof. Let $\lambda - \mu$ be a horizontal strip. By definition we get $\lambda'_i - \mu'_i \leq 1$ for all i. This means that λ contains just as many or one more parts of a given size as μ. In other words we obtain $\mu_i \geq \lambda_{i+1}$ for all i and we are done. □

The coming result gives an important characterization of the type of Hall polynomials we are interested in.

Proposition 2.17. *For $r \in \mathbb{N}$ the Hall polynomials $g^{\lambda}_{(r),\mu}$ are zero unless $\lambda - \mu$ is a horizontal r-strip.*

Proof. See [36, Chap. II (4.12)]. □

2.5 Degenerations and orbits in finite abelian groups

In this section we present a way to compute the Hall numbers $g^{\lambda}_{(r),\mu}(p)$. The foundation for this is given by the paper [17] written by K. Dutta and A. Prasad and so we keep most of the definitions and notations from their work with the difference that we only consider finite abelian p-groups instead of arbitrary abelian groups. At the end of this section we profit of a discussion between Prasad and D. Speyer [44] which makes it possible to state a closed formula for $g^{\lambda}_{(r),\mu}(p)$. Throughout this section we always mean by a group a finite abelian p-group.
We begin with the fundamental definition of this section.

Definition 2.18. Let G and H be groups. For elements $g \in G$ and $h \in H$ we say that g *degenerates to* h (denoted by $g \to h$) if there exists a homomorphism $\phi : G \longrightarrow H$ such that $\phi(g) = h$.

The following lemma provides a criterion of degeneracy in cyclic groups.

Lemma 2.19. *Let $u,\ v,\ r,\ s,\ k$ and l be natural numbers such that u and v are not divisible by p, $r < k$ and $s < l$. Then $p^r u \in \mathbb{Z}/p^k\mathbb{Z}$ degenerates to $p^s v \in \mathbb{Z}/p^l\mathbb{Z}$ if and only if $r \leq s$ and $k - r \geq l - s$.*

Proof. See [17, Lem. 3.1]. □

Next we consider the action on a group G by its automorphism group and establish a connection to the notion of degeneracy.

Notation 2.20. For a group G we define the action

$$\omega : \mathrm{Aut}(G) \times G \longrightarrow G,\ \omega(\phi, g) := \phi(g).$$

For an element $g \in G$ we denote by $[g]$ its orbit under ω and by $G/\mathrm{Aut}(G)$ the set of $\mathrm{Aut}(G)$-orbits in G.

The following lemma allows us to talk about degeneracy on orbits.

Lemma 2.21. *Let G be a group and let $g,\ g',\ h,\ h'$ be elements of G with $[g] = [g']$ and $[h] = [h']$. Then $g \to h$ if and only if $g' \to h'$.*

Proof. Since $[g] = [g']$ and $[h] = [h']$ there exist $\phi_1,\ \phi_2 \in \mathrm{Aut}(G)$ with $\phi_1(g') = g$ and $\phi_2(h) = h'$. Assuming $g \to h$ we find a $\phi \in \mathrm{Aut}(G)$ such that $\phi(g) = h$. Hence we get $\phi_2(\phi(\phi_1(g'))) = h'$. The other direction follows similarly. □

This result allows us to provide $G/\mathrm{Aut}(G)$ with an ordering.

Definition 2.22. For $g,\ h \in G$ we set $[g] \geq [h]$ if $g \to h$.

Corollary 2.23. *$G/\mathrm{Aut}(G)$ is a partially ordered set with respect to "$\geq$".*

In the case of cyclic groups the situation looks as follows.

Example 2.24. The group $\mathbb{Z}/p^k\mathbb{Z}$ has k orbits of non-zero elements under the action of its automorphism group, represented by $1, p, \dots, p^{k-1}$, and ordered in the following way

$$[1] \geq [p] \geq \cdots \geq [p^{k-2}] \geq [p^{k-1}].$$

In the following we introduce some fundamental notations for the rest of this section.

Notation 2.25. We denote the orbit of g in $\mathbb{Z}/p^k\mathbb{Z}$ by (g, k) and write $P := \bigcup_{k\in\mathbb{N}}(g, k)$ for the partially ordered set of such orbits.

Now we repeat the notion of an ordered ideal and continue to work on our setting to determine the Hall numbers $g^{\lambda}_{(r),\mu}(p)$.

Definition 2.26. Given a partially ordered set $(S, \leq)$ we call a subset I of S an *(ordered) ideal*, denoted by $I \trianglelefteq S$, if

(a) for all $x \in I$ and $y \in S$, $y \leq x$ implies $y \in I$ and

(b) for every $x,\ y \in I$ there is some element $z \in I$ such that $x \leq z$ and $y \leq z$.

In the following definition we present a class of ideals in P which comes from group elements.

Definition 2.27. Given a group G of type $\lambda = (\lambda_1, \dots, \lambda_t)$ and an element $g = (g_1, \dots, g_t)$ of G we define the *ideal of* g, denoted by $I_\lambda(g)$, as the ideal in P generated by the set of orbits $\{(g_i, \lambda_i) \mid g_i \neq 0,\ i = 1, \dots, t\}$.

We illustrate the definition by an example.

Example 2.28. Consider a group G of type $\lambda = (4, 3, 1)$ and the element $g = (p^2, p, 1) \in G$ we get $I_\lambda(g) = \{(p^2, 4), (p^3, 4), (p, 3), (p^2, 3), (1, 1)\}$.

In the next step we adapt the partially ordered set we want to deal with to our setting. Since the set P is rather too big for our purpose it is enough to consider the following subset of it.

Definition 2.29. Given a partition $\lambda = (\lambda_1, \ldots, \lambda_t)$ we define the subset P_λ of P consisting of orbits of the form (g, k) with $k = \lambda_i$ for some $i = 1, \ldots, t$. Furthermore we denote by $J(P_\lambda)$ the lattice of all ideals in P_λ.

At this point we bring together the $\mathrm{Aut}(G)$-orbits of the group G and the ideals of P_λ, where λ is the type of G.

Proposition 2.30. *Let G be a group of type λ. Then the map*

$$\varphi : G/\mathrm{Aut}(G) \longrightarrow J(P_\lambda) \text{ given by } \varphi([g]) = I_\lambda(g)$$

is an isomorphism of partially ordered sets.

Proof. See [17, Thm. 5.4]. □

Next we define the orbit in G corresponding to an ideal I under the bijection given by the last proposition.

Definition 2.31. For a partition λ, a group G of type λ and an ideal I of P_λ we define the set $O_{p,I} := \{g \in G \mid I_\lambda(g) = I\}$.

To compute the cardinality of $O_{p,I}$ we need the following terms.

Definition 2.32. Let λ be a partition and I be an ideal in P_λ. For an element (g, k) of P_λ we define its *multiplicity* as the number $m((g, k)) := |\{i \mid k = \lambda_i\}|$ and by $[I] := \sum_{(g,k)\in I} m((g, k))$ we denote the number of points in I.

Proposition 2.33. *Given a partition λ for every ideal $I \subset P_\lambda$ we have*

$$|O_{p,I}| = p^{[I]} \cdot \prod_{x \in \max I} \left(1 - p^{-m(x)}\right),$$

where $\max I$ *is the set of maximal elements of I with respect to " $\geq$ ".*

Proof. See [17, Thm. 8.5]. □

The rest of this section is based on a discussion of Prasad and Speyer [44] and in particular the following proofs are inspired by them.
We start by a lemma which points out a straightforward calculation of the Hall numbers $g^\lambda_{(r),\mu}(p)$ using the notions defined above.

Lemma 2.34. *Given a group G of type λ we get the following formula*

$$g^{\lambda}_{(r),\mu}(p) = \sum_{I \subseteq P_\lambda} \frac{|O_{p,I}|}{p^r - p^{r-1}},$$

where the summation runs over all ideals I such that for all $g \in O_{p,I}$

(a) the order $\operatorname{ord}(g) = p^r$ *and*

(b) $G/\langle g \rangle$ is of type μ.

Proof. Given a group G of type λ the Hall number $g^{\lambda}_{(r),\mu}(p)$ is defined as the number of subgroups isomorphic to $\mathbb{Z}/p^r\mathbb{Z}$ where the quotient is of type μ. The ideals I in the lemma are chosen in such a way that $O_{p,I}$ only contains elements of G with the desired properties, i.e. $\operatorname{ord}(g) = p^r$ and $G/\langle g \rangle$ is of type μ for all $g \in O_{p,I}$. Since we are interested in the number of groups we need to divide $|O_{p,I}|$ by the number of generators of $\mathbb{Z}/p^r\mathbb{Z}$, so by $p^r - p^{r-1}$. □

In the following we will see that the sum only consists of one summand. To observe this we need to establish a connection between the possible types of the group $G/\langle g \rangle$ and $J(P_\lambda)$.

Lemma 2.35. *Given a group G of type λ there is a one to one correspondence between the set S of all possible cotypes of $\langle g \rangle$ for $g \in G$ and the set of orbits $G/\operatorname{Aut}(G)$. In particular there is a bijection between S and $J(P_\lambda)$.*

Proof. Given a group G of type $\lambda = (\lambda_1, \dots, \lambda_t)$ and an element $g \in G$ the possible types of $G/\langle g \rangle$ range through all partitions $\mu = (\mu_1, \dots, \mu_t)$ which can be obtained from λ by deleting a horizontal strip. By Lemma 2.16 we have $\lambda_i - \lambda_{i+1} + 1$ possibilities for μ_i, where $i = 1, \dots, t-1$ and $\lambda_t + 1$ possibilities for μ_t. So all in all we get

$$(\lambda_t + 1) \cdot \prod_{i=1}^{t} (\lambda_i - \lambda_{i+1} + 1)$$

for the order of S. But this coincides by [17, (1)] with the number of orbits in $G/\operatorname{Aut}(G)$. So there must be a bijection between these two sets. The one to one correspondence between S and $J(P_\lambda)$ follows by Proposition 2.30. □

So we have seen that $g^{\lambda}_{(r),\mu}(p) = |O_{p,I}|/(p^r - p^{r-1})$ for an ideal $I \trianglelefteq P_\lambda$ which is uniquely determined by λ and μ. Now we need to show how to construct I from λ and μ. For this step we need the following general result from computational group theory.

Lemma 2.36. *Given a group G of type $\lambda = (\lambda_1, \dots, \lambda_t)$ and an element $g = (p^{\nu_1}, \dots, p^{\nu_t}) \in G$ the type of the quotient $G/\langle g\rangle$ is given by $\mu = (\mu_1, \dots, \mu_t)$ where p^{μ_i} are the elementary divisors of the Smith normal form of the following matrix*

$$A := \begin{pmatrix} p^{\lambda_1} & & & \\ & p^{\lambda_2} & & \\ & & \ddots & \\ & & & p^{\lambda_t} \\ p^{\nu_1} & p^{\nu_2} & \cdots & p^{\nu_t} \end{pmatrix}.$$

Proof. See [10, Sect. 4.1.3]. □

Using this we obtain the following conclusion.

Lemma 2.37. *Let G be a group of type $\lambda = (\lambda_1, \dots, \lambda_t)$ and let $I \subseteq P_\lambda$ be an order ideal. Given an element $g = (p^{\nu_1}, \dots, p^{\nu_t}) \in O_{p,I}$ the type of $G/\langle g\rangle$ equals $\mu = (\mu_1, \dots, \mu_t)$, where*

$$\mu_t = \nu_t,\ \mu_i = \lambda_{i+1} + v_i - v_{i+1} \text{ for } i = 1, \dots, t-1.$$

Proof. By Lemma 2.36 we need to determine the elementary divisors of A, where A is like in 2.36. To do so we compute the greatest common divisor of the $i \times i$-minors of A, write a_i for this term. Since $g \in O_{p,I}$ we get the inequalities $\nu_i \leq \nu_{i-1} \leq \nu_i + (\lambda_{i-1} - \lambda_i)$ for all $i = 2, \dots, t$ (see [17, Sect. 6, Eq. (3)][1]). Using this we obtain the following values for the a_i

$$\begin{aligned} a_1 &= p^{\nu_t} \\ a_2 &= p^{\nu_{t-1}} \cdot p^{\lambda_t} \\ &\vdots \\ a_{t-1} &= p^{\nu_2} \cdot p^{\lambda_3} \cdots p^{\lambda_t} \\ a_t &= p^{\nu_1} \cdot p^{\lambda_2} \cdots p^{\lambda_t} \end{aligned}$$

and so we get

$$\mu_t = \nu_t,\ \mu_{t-i+1} + \cdots + \mu_t = \nu_{t-i+1} + \lambda_{t-i+2} + \cdots + \lambda_t, \text{ for } 2 \leq i \leq t.$$

From this we obtain the stated identities. □

Fitting all together we get a closed formula for the Hall numbers $g^{\lambda}_{(r),\mu}(p)$.

[1] Here the result is shown for $i < t$, but using the same arguments one verifies the inequality for $i = t$.

Corollary 2.38. *Given a group G of type λ and a partition $\lambda \supset \mu$ such that $|\lambda - \mu|$ is a horizontal r-strip the Hall number $g^{\lambda}_{(r),\mu}(p)$ is equal to $\dfrac{|O_{p,I}|}{p^r - p^{r-1}}$ with $I = I_\lambda(\nu)$ and $\nu = (p^{\nu_1}, \dots, p^{\nu_t})$, where*

$$\nu_t = \mu_t,\ \nu_i = \mu_i - \left(\sum_{j=i+1}^{t} \lambda_j - \mu_j \right) \text{ for } i = 1, \dots, t-1.$$

Proof. By Lemma 2.35 the ideal I is uniquely determined by λ and μ. Lemma 2.37 shows how to get I from λ and μ. □

2.6 Modules over Dedekind domains

Definition 2.39. An integral domain R is called *Dedekind*, if R is noetherian, integrally closed and every non-zero prime ideal is already maximal.

An important class of examples for Dedekind domains is given by the rings of integers of number fields (see [45, Ex. 11.88]). In the next step we characterize the finitely generated modules over Dedekind domains. Before doing this we need a further definition.

Definition 2.40. Let R be a ring. We say that an R-module M is *torsion* if, for each $m \in M$, there exists a non-zero $r \in R$ such that $rm = 0$.

In the following we collect some classification results on finitely generated torsion modules.

Theorem 2.41. *Let M be a finitely generated torsion module over a Dedekind domain R. Then there exist prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ of R so that*

$$M \cong R/\mathfrak{p}_1^{\alpha_1} \oplus \cdots \oplus R/\mathfrak{p}_t^{\alpha_t}$$

for some $t \in \mathbb{N}$ and $\alpha_1, \dots, \alpha_t \in \mathbb{N}$.

Proof. See [45, Thm. 11.113]. □

Remark 2.42. By [45, Thm. 11.114], there exists

$$M_{\mathfrak{p}} := (R/\mathfrak{p}^{\beta_1})^{k_1} \oplus \cdots \oplus (R/\mathfrak{p}^{\beta_s})^{k_s}$$

for all non-zero $\mathfrak{p} \in \operatorname{Spec}(R)$ where $\beta_1, \ldots, \beta_s,\ k_1, \ldots, k_s \in \mathbb{N}$ are chosen in such a way that

$$M \cong \bigoplus_{\mathfrak{p} \in \operatorname{Spec}(R)} M_{\mathfrak{p}}.$$

Definition 2.43. For an R-module M we define the set of R-automorphisms of M by

$$\operatorname{Aut}_R(M) := \{f : M \to M \mid f \text{ is } R\text{-linear and bijective}\}.$$

Theorem 2.44. *With the notations as above assuming the finiteness of $R/\mathfrak{p}$ for all non-zero $\mathfrak{p} \in \operatorname{Spec}(R)$ we have*

(a) $\operatorname{Aut}_R(M) \cong \bigoplus_{\mathfrak{p} \in \operatorname{Spec}(R)} \operatorname{Aut}_R(M_{\mathfrak{p}})$,

(b) $|\operatorname{Aut}_R(M_{\mathfrak{p}})| = q^{\sum_{1 \leq i,j \leq t} \min\{\alpha_i, \alpha_j\} k_i k_j} \cdot \prod_{i=1}^{t} (q)_{k_i}$ *for* $q = |R/\mathfrak{p}|$.

Proof. See [12, Thm. 2.11]. □

2.7 Number fields

In this section we recall some basic definitions and properties concerning number fields. For general background on number fields, see e.g. the books of G. Janusz [31] and J. Neukirch [43].

Notation 2.45. Let K_0 be a number field. We write $D(K_0)$ for the *(absolute) discriminant* and $\operatorname{Cl}(K_0)$ for the *class group* of K_0. Given a finite field extension K/K_0 we denote by $D(K/K_0)$ the *relative discriminant* of K/K_0 and by $\operatorname{Cl}(K/K_0)$ the *relative class group* of K/K_0, defined as the kernel of the norm map $N_{K/K_0} : \operatorname{Cl}(K) \to \operatorname{Cl}(K_0)$. For the *ring of integers* of K_0 we write $\mathcal{O}_{K_0}$.

In the following proposition we outline the fundamental properties of the above invariants of a number field and show the connection between the absolute and the relative notions.

Proposition 2.46. *With the terminology from the last notation the following is true.*

(a) $\operatorname{Cl}(K_0)$ *and* $\operatorname{Cl}(K/K_0)$ *are finite groups.*

(b) If $p \nmid |\operatorname{Cl}(K_0)|$ *then* $\operatorname{Cl}(K)_p \cong \operatorname{Cl}(K/K_0)_p$.

(c) Given a natural number n there are only finitely many number fields K_0 with $|D(K_0)| < n$.

(d) $D(K/K_0)$ *is an ideal in* $\mathcal{O}_{K_0}$ *and in the case* $K_0 = \mathbb{Q}$ *we have* $(D(K))_{\mathbb{Z}} = D(K/\mathbb{Q})$*.*

Proof. By [43, Chap. I, (6.3)] the class group is finite and with this we have the finiteness of the relative class group. The second statement is a direct consequence of [32, Prop. 1]. Part (c) is shown in [43, Chap. III, (2.16)] and (d) is given by definition. □

Next we focus on ideals and their behavior in an extension. In particular we ask the question what happens when a prime ideal $\mathfrak{p} \lhd \mathcal{O}_{K_0}$ is lifted to $\mathcal{O}_K$. To deal with this we need some more vocabulary.

Definition 2.47. Given a number field extension K/K_0 of degree n and a prime ideal $\mathfrak{p} \lhd \mathcal{O}_{K_0}$ with its prime ideal decomposition

$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{t} \mathfrak{P}_i^{e_{\mathfrak{P}_i/\mathfrak{p}}}$$

in $\mathcal{O}_K$ we call the exponent $e_{\mathfrak{P}_i/\mathfrak{p}}$ the *ramification index* of $\mathfrak{P}_i$ and $f_{\mathfrak{P}_i/\mathfrak{p}} := [\mathcal{O}_K/\mathfrak{P}_i : \mathcal{O}_{K_0}/\mathfrak{p}]$ the *inertia degree* of $\mathfrak{P}_i$. Furthermore we say that $\mathfrak{P} \lhd \mathcal{O}_K$ *lies above* $\mathfrak{p} \lhd \mathcal{O}_{K_0}$ if $\mathfrak{P}$ divides $\mathfrak{p}\mathcal{O}_K$ in $\mathcal{O}_K$.

Proposition 2.48. *We keep the notation of the above definition and assume that* K/K_0 *is separable. Then*

$$[K : K_0] = n = \sum_{i=1}^{t} e_{\mathfrak{P}_i/\mathfrak{p}} f_{\mathfrak{P}_i/\mathfrak{p}}.$$

Proof. See [43, Chap. I, (8.2)]. □

Definition 2.49. Let K/K_0 be a degree n extension of number fields. Given a prime ideal $\mathfrak{p} \lhd \mathcal{O}_{K_0}$ such that there is (at least) one prime ideal $\mathfrak{P} \lhd \mathcal{O}_K$ above $\mathfrak{p}$ satisfying $e_{\mathfrak{P}/\mathfrak{p}} > 1$, then $\mathfrak{p}$ is called *ramified* in the extension K/K_0. If there is only one such ideal $\mathfrak{P} \lhd \mathcal{O}_K$ which also satisfies $e_{\mathfrak{P}/\mathfrak{p}} = n$, then $\mathfrak{p}$ is called *totally ramified* in the extension K/K_0. In the situation where $e_{\mathfrak{P}/\mathfrak{p}} = 1$ for all prime ideals $\mathfrak{P}$ lying above $\mathfrak{p}$ we say $\mathfrak{p}$ is *unramified.* If $\mathfrak{p}\mathcal{O}_K$ is a product of n distinct primes, then we say that $\mathfrak{p}$ *splits completely* in K/K_0.

The next proposition gives a characterization of the ramification behavior of prime ideals using the discriminant.

Proposition 2.50. *With the notation from the last definition the following holds.*

(a) The prime ideal $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_{K_0})$ *is ramified in* K/K_0 *if and only if* $\mathfrak{p}$ *divides* $D(K/K_0)$*.*

(b) If $D(K/K_0)$ is the unit ideal then all primes are unramified. In such a situation we call the extension K/K_0 unramified.

Proof. See [43, Chap. III, (2.12)]. □

Chapter 3

The distribution of class groups of number fields

In this chapter we consider class groups of number fields or to be more specific their Sylow p-subgroups and try to say something about the distribution of such objects. In particular we would like to understand how a typical class group looks like. Unfortunately there are not many proven results about this issue, but there is, however, a bunch of conjectures based on the famous Cohen-Lenstra heuristic which fit very well together with numerical data. In the following we present the crucial statements about this topic from the last thirty years and give a brief overview of the corresponding function field case.

3.1 The Cohen-Lenstra heuristic

Here we recall the most important ideas and definitions of the celebrated paper [11] written by H. Cohen and H.W. Lenstra in 1983.
Along the lines of: "we start in a small way", Cohen and Lenstra considered imaginary quadratic number fields and studied computational data on some class groups for this case. By doing so they realized the phenomenon that certain groups, such as $\mathbb{Z}/p\mathbb{Z}$, appear much more often as class groups than others, such as $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. They "explained" this fact by the reason that the latter group has many more automorphisms than the former. So a straightforward conclusion of this observation was to equip every group with the following weight.

Definition 3.1. Given a finite group G we define the *CL-weight* of G by $\omega(G) := \dfrac{1}{|\mathrm{Aut}(G)|}$.

Proposition 3.2. *Let $\mathcal{G}_p$ denote the set of all isomorphism classes of finite abelian p-groups. Then*

$$\sum_{G \in \mathcal{G}_p} \omega(G) = (p)_\infty^{-1} < \infty.$$

Proof. See [33, Thm. 2.1.2]. □

Using the fact from the last proposition we obtain the following probability distribution on the set of all isomorphism classes of finite abelian p-groups.

Corollary 3.3. *The distribution given by*

$$P_{CL} : \mathcal{G}_p \longrightarrow [0,1],\ G \mapsto \frac{(p)_\infty}{|\mathrm{Aut}(G)|},$$

defines a probability distribution on $\mathcal{G}_p$.

It turned out that P_{CL} plays the role of a kind of natural distribution on the set of finite abelian p-groups and occurs also in many other contexts. See [34] for an overview of this issue.
As next we compute some concrete P_{CL} probabilities where we use the following notation.

Notation 3.4. Given a property $\mathcal{A}$ of a finite abelian p-group G (e.g.: G is cyclic) we define

$$P_{CL}(\text{"}G \text{ fulfills } \mathcal{A}\text{"}) := \sum_{\substack{G \in \mathcal{G}_p \\ G \text{ fulfills } \mathcal{A}}} P_{CL}(G).$$

Example 3.5. (a) $P_{CL}(\mathrm{id}) = (p)_\infty$.

(b)

$$\begin{aligned} P_{CL}(\text{"}G \text{ cyclic"}) &= \sum_{G \text{ cyclic}} \frac{(p)_\infty}{|\mathrm{Aut}(G)|} = (p)_\infty \cdot \left(1 + \sum_{\alpha=1}^{\infty} \frac{1}{p^{\alpha-1}(p-1)}\right) \\ &= (p)_\infty \cdot \left(1 + \frac{p}{(p-1)^2}\right) \\ &= (p)_\infty \cdot \frac{p^2 - p + 1}{(p-1)^2}. \end{aligned}$$

(c) $P_{CL}(\text{"}\mathrm{rk}_p(G) = r\text{"}) = \dfrac{(p)_\infty}{p^{r^2}(p)_r^2}$, see [11, Thm. 6.3].

(d) $P_{CL}(\text{"}|G| = p^n\text{"}) = \dfrac{(p)_\infty}{p^n (p)_n}$, see [11, Cor. 3.8].

Notation 3.6. Write $\mathcal{I}$ for the set of all imaginary quadratic extensions of $\mathbb{Q}$ inside a fixed algebraic closure of $\mathbb{Q}$. Then given a finite abelian p-group G we set

$$\mathcal{M}(G) := \lim_{x \to \infty} \frac{|\{K \in \mathcal{I} \mid 0 \le |D(K)| \le x,\ \mathrm{Cl}(K)_p \cong G\}|}{|\{K \in \mathcal{I} \mid 0 \le |D(K)| \le x\}|}.$$

Using this notation we can formulate the first conjecture stated by Cohen and Lenstra which makes predictions about the behavior of p-parts of class groups of imaginary quadratic number fields.

Conjecture 3.7. *Let p be an odd prime. Then for a finite abelian p-group G the limit $\mathcal{M}(G)$ exists and is equal to $P_{CL}(G)$.*

Of course, this statement was a breakthrough in the field of algebraic number theory and provides the motivation to consider more general number fields.

3.2 Cohen-Martinet and bad primes

Cohen and J. Martinet [12] continued the ideas presented in the last section and formulated an analogue conjecture to 3.7 for arbitrary extensions of a number field K_0. Before we can present their result we need to introduce the following set up.

Definition 3.8. We call a triple $\Sigma := (H, K_0, \sigma)$ a *situation*, where

(a) $H \leq S_n$ is a transitive permutation group of degree $n \geq 2$,

(b) K_0 is a number field and

(c) σ is a signature, which may occur as signature of a degree n extension K/K_0 (inside a fixed algebraic closure) with Galois group (of the Galois closure) permutation isomorphic to H.

Moreover we define for a situation $\Sigma = (H, K_0, \sigma)$ the set $\mathcal{K}(\Sigma)$ of number fields K/K_0 as described in (c).

Next we adopt a few terms related to a situation Σ.

Notation 3.9. To a given situation Σ one can attach a finite set of primes $S(\Sigma)$, the so called *bad primes*, a non-negative rational number (in general not an integer) $u(\Sigma)$, the *unit rank* and a ring $\mathcal{O}(\Sigma)$. For the precise definition of the above terms see [12, Chap. 6].

Notation 3.10. Given a finite abelian p-group G and a situation $\Sigma = (H, K_0, \sigma)$ we set

$$\mathcal{N}(\Sigma, G) := \lim_{x \to \infty} \frac{|\{K \in \mathcal{K}(\Sigma) \mid 0 \leq |D(K/K_0)| \leq x, \ \mathrm{Cl}(K/K_0)_p \cong G\}|}{|\{K \in \mathcal{K}(\Sigma) \mid 0 \leq |D(K/K_0)| \leq x\}|}.$$

With this we can present the conjecture of Cohen and Martinet (in the case $\mathcal{O}(\Sigma) = \mathbb{Z}$) which predicts the distribution of p-parts of relative class groups of number fields over K_0.

Conjecture 3.11. $\mathcal{N}(\Sigma, G)$ *exists for all* $p \notin S(\Sigma)$ *and is given by the following limit*

$$\lim_{x\to\infty} \frac{\sum\limits_{A\in\mathcal{G}_p,\ |A|\leq x} |A|^{-u} \cdot \omega(A) \cdot |\{\varphi \in \mathrm{Hom}(\mathbb{Z}^u, A) \mid A/\mathrm{Im}(\varphi) \cong G\}|}{\sum\limits_{A\in\mathcal{G}_p,\ |A|\leq x} |A|^{-u} \cdot \omega(A) \cdot |\mathrm{Hom}(\mathbb{Z}^u, A)|},$$

where $u := u(\Sigma)$*.*

The limit from the latter conjecture could be computed by Cohen and Martinet using zeta functions (see [12, Chap. 5]).

In the following years it was noticed by many people that this conjecture is not true for all primes which were allowed by Cohen and Martinet. So we need to lay the focus a bit more on the set $S(\Sigma)$. In the following we outline the expansion of $S(\Sigma)$ with $\Sigma = (H, K_0, \sigma)$. In their original paper Cohen and Martinet [12] excluded the primes that divided the extension degree $n = [K : K_0]$ and they did it for a good reason, namely one can show by genus theory that these primes are indeed bad meaning that the conjecture cannot be true for such primes. A few years later and after more computations Cohen and Martinet [13] were forced to enlarge the set of bad primes by those which divide the order of the common Galois group H of the situation Σ. For the bad behavior of these primes one can find theoretical arguments in the manner of genus theory, too. But this is still not the end of the story. Since it was first noticed by G. Malle in [37] and later confirmed in [38] by a big numerical support that the existence of pth roots of unity in the base fields K_0 does play a role for the distribution of p-parts of class groups of number fields. However, there is no known theoretical reason for the badness of these primes. So one might have the hope to formulate conjectures in the manner of 3.7 and 3.11 for such primes, as well. In the next section we are going to answer the question if the hope was reasonable or not.

3.3 Roots of unity

In the last section we have mentioned that the presence of pth roots of unity in the base field K_0 seems to play a role for the distribution of p-parts of class groups of number fields over K_0.

Here we firstly consider the analogue situation in the function field case and later present a conjecture of Malle which predicts a distribution in the desired setting.

3.3.1 The function field case

It is not surprising that we look here at the function field case. Since it is a common strategy in the theory of global fields to switch between number fields and function fields or at least to consult the other type. In doing so we summarize here the knowledge about the distribution of class groups of function fields and try to derive some ideas and concepts from it to the number field case in the following parts of the text.

It has taken three years after the publication of the celebrated paper of Cohen and Lenstra [11] that the analogue case on the function field side was treated in a published work. Given two coprime prime numbers l and p, E. Friedman and L.C. Washington [20, 1987] considered quadratic extensions of $\mathbb{F}_l(t)$ and linked the distribution of p-parts of the divisor class groups of degree 0 defined over $\mathbb{F}_l$ to equidistributed sequences of matrices over finite fields. J. Achter took up this suggestion in his 2006 paper [4] and continued his work in [5] proving that, to put it simply, the distribution of class groups of quadratic function fields and the distribution of elements in symplectic similitude groups are the same. At this point we need to go a bit more into details to shine a light on Achter's work. For that let $\mathcal{H}_g(\mathbb{F}_l)$ denote the set of monic separable polynomials of degree g over the finite field $\mathbb{F}_l$ and let $\mathcal{C}_{g,f}$ be the smooth curve of genus g defined by $f \in \mathcal{H}_{2g+2}(\mathbb{F}_l)$. With this we define for a finite abelian p-group G the proportion

$$\beta_p(g, \mathbb{F}_l, G) := \frac{|\{f \in \mathcal{H}_{2g+2}(\mathbb{F}_l) \mid \mathrm{Cl}^0(\mathcal{C}_{g,f})_p \cong G\}|}{|\mathcal{H}_{2g+2}(\mathbb{F}_l)|},$$

where $\mathrm{Cl}^0(\mathcal{C}_{g,f})_p$ is the Sylow p-subgroup of the Jacobian of $\mathcal{C}_{g,f}$. Among other things Achter showed the following relation

$$\lim_{|\mathbb{F}_l|\to\infty} \beta_p(g, \mathbb{F}_l, G) = \frac{|\{x \in \mathrm{Sp}_{2g}(\mathbb{F}_p) \mid \ker(x - \mathbf{1}_{2n}) \cong G\}|}{|\mathrm{Sp}_{2g}(\mathbb{F}_p)|}$$

where here G is a finite elementary abelian p-group. Later in his work Achter considered symplectic similitude groups over finite rings and established a correspondence between a distribution in such groups and the distribution of the Jacobian of hyperelliptic curves. (Consult [5, Thm 3.1] for more details.) However, Achter did not compute the distribution in the symplectic similitude groups explicitly. This step has been done in a joint work by J. S. Ellenberg, A. Venkatesh and C. Westerland [18] and one consequence of their work was that the distribution of the p-parts of divisor class groups of degree 0 of quadratic function fields over $\mathbb{F}_l$ with $p \nmid l-1$[1] matches the distributions predicted by Cohen-Lenstra and Friedman-Washington. The case where $p \mid l-1$ was treated by D. Garton, a student of Ellenberg, in his recent thesis [26], where he presented a distribution for this situation [26, Thm. 7.2.3] which corresponds to our results (see 4.24 and Chapter 5) in the number field case.

3.3.2 Malle's conjecture

Malle [37] presented numerical data concerning distributions of p-parts of class groups of certain number fields that show a disagreement with the predicted formulas of Cohen and Martinet. He explained this phenomenon by the fact that pth roots of unity contained in the base field do play a role for the distribution of the p-parts of the corresponding class groups. So such primes need to be treated in a special way. Two years later Malle [38] formulated a conjecture in the spirit of Cohen and Martinet for these primes, too, and provided evidence for his conjecture by more computational data:

Conjecture 3.12. *Let $\Sigma = (H, K_0, \sigma)$ be a situation, such that $\gcd(p, |H|) = 1$ and K_0 be a number field with pth but not the p^2rd roots of unity. Then a given finite abelian p-group G of p-rank r appears as the p-part of a relative class group $\mathrm{Cl}(K/K_0)$ for $K \in \mathcal{K}(\Sigma)$ with probability*

$$\frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty} \cdot \frac{(p)_{r+u}p^{\binom{r}{2}}}{(p)_u|G|^u|\mathrm{Aut}(G)|}$$

where $u = u(\Sigma)$.

Remark 3.13. At this point we should mention the thesis of Maximilian Boy[2] [7] where he considers the situation $\Sigma = (H, \mathbb{Q}, \text{totally real})$ with $H \cong C_2 \ltimes_{inv} D$ is the semidirect product of a finite abelian group D of odd order and C_2, where the generator of C_2 acts by inversion on D (see [7, Sect. 2.1]). Boy states a probability distribution on the set of finite $e\mathbb{Z}_{\langle 2\rangle}H$-modules which should describe the behavior of the 2-parts of class groups in the situation Σ ([7, Conjecture 2]) where e is a central idempotent of the group algebra $\mathbb{Q}H$ and $\mathbb{Z}_{\langle 2\rangle}$ is the localization of $\mathbb{Z}$ at 2. Although Boy only considers a very special case he extends the coverage of Conjecture 3.12 to modules and enables so a more general treatment of this issue.

[1] This corresponds on the number field side to the case where pth roots of unity are not contained in the base field.

[2] M. Boy is a former Ph.D. student of Malle.

In [38, Sect. 3] Malle also proposed that the results of Achter [4] about the correspondence between the distribution of divisor class groups and the distribution of eigenspaces in symplectic similitude groups might have an analogue version in the number field case. At least there should be a link between the distribution of p-parts of class groups of number fields and the distribution of eigenspaces in certain matrix groups over finite rings. So our hope is to establish a connection in the vein of the following diagram

$$\boxed{\begin{array}{ccc} \text{number fields} & \longleftrightarrow & \text{matrix theory} \\ & & \\ \left\{\begin{array}{c}\text{distribution of } p\text{-parts}\\ \text{of class groups of number fields}\end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c}\text{distribution of eigenspaces}\\ \text{in certain matrix groups}\\ \text{of dimension } g \text{ for } g \to \infty\end{array}\right\}\end{array}}$$

As we have seen in our discussion of Achter's results above the dimension of matrix groups corresponds to the genus of function fields which for its part can be related to the discriminant of number fields (see [27, Sect. 6] for this analogy). So this is the reason why we want to consider the limit $g \to \infty$.

Motivated by these ideas we study the distribution of eigenspaces in matrix groups in the next chapter of this document and in Chapter 5 we relate the obtained results to questions about the distribution of class groups of number fields.

3.4 State of the art

In this part we collect the very few proven statements about the distribution of class groups and present some results in related areas.

Long way before Cohen and Lenstra published their heuristic principle for the behavior of class groups of number fields it was known by Gauss (see [42, Thm. 8.8]) that the 2-rank of the class group of a quadratic number field K is equal to $t-1$, where t is the number of distinct prime divisors of the discriminant of K. By definition the p-rank of $\mathrm{Cl}(K)$ is given by

$$\mathrm{rk}_p(\mathrm{Cl}(K)) := \dim_{\mathbb{F}_p}(\mathrm{Cl}(K)/\mathrm{Cl}(K)^p).$$

Using the theory of Davenport and Heilbronn [14] about cubic fields one can derive some statements about the distribution of the Sylow 3-subgroups of class groups of quadratic number fields. In [35] F. Luca and A. Pacelli present some bounds for the 3-rank of class groups of quadratic number fields.

We recall that the original conjecture of Cohen and Lenstra was only formulated for odd primes (see 3.7). The extension to $p = 2$ has been done by F. Gerth, in particular he studied the 4-rank of $\mathrm{Cl}(K)$ defined as

$$\mathrm{rk}_4(\mathrm{Cl}(K)) := \dim_{\mathbb{F}_2}(\mathrm{Cl}(K)^2/\mathrm{Cl}(K)^4)$$

and presented some results (see [28]) which were confirmed and extended by E. Fouvry and J. Klüners in [19]. So the probability that the 4-rank of the class group of a real quadratic number field is equal to r with $r \in \mathbb{N}$ is given by

$$\frac{1}{2^{r(r+1)}} \cdot \frac{(2)_\infty}{(2)_r(2)_{r+1}},$$

while in the case of imaginary quadratic fields the probability is equal to

$$\frac{1}{2^{r^2}} \cdot \frac{(2)_\infty}{(2)_r^2}.$$

C. Wittmann considered the analogue question in the function field case. So he studied the behavior of the 4-class ranks in quadratic function fields over finite fields $\mathbb{F}_l$ of odd characteristic and obtained in the case where $l \equiv 3$ modulo 4 the same proportion of fields having 4-class rank r as in the case of imaginary quadratic number fields (see [46, (1.2)])[3].

Exploiting the duality between number fields and elliptic curves C. Delaunay introduced a heuristic principle for the distribution of Tate-Shafarevich groups of elliptic curves over the rationals and stated some conjectural results for this set-up in the spirit of Cohen and Lenstra (see [15, 16]). M. Bhargava et al. [6] generalized this ideas to elliptic curves over global fields and formulated a conjecture about the distribution of exact sequences

$$0 \longrightarrow E(k) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty} E \longrightarrow Ш[p^\infty] \longrightarrow 0$$

which has lots of crucial results as consequence like the finiteness of the Tate-Shafarevich group (see [6, Thm. 5.14]).

[3] Since $l \equiv 3$ modulo 4 we have $2^2 = 4 \nmid l - 1$ and so we are in the same situation as in Sect. 3.3.1.

Chapter 4

The distribution of eigenspaces in classical groups over finite rings

As mentioned in the previous chapter this part is motivated by the works of Achter [4, 5] and Malle [37, 38]. Here by a ring $\mathcal{O}$ we always mean a ring of integers of a number field. The main part of this chapter addresses the following issue. Given a prime ideal $\mathfrak{p} \trianglelefteq \mathcal{O}$ of $\mathcal{O}$ with $q = |\mathcal{O}/\mathfrak{p}|$ and a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module

$$\mathcal{A} = (\mathcal{O}/\mathfrak{p}^{\alpha_1})^{k_1} \oplus \cdots \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t}$$

we determine the probability for $\mathcal{A}$ to be isomorphic to the eigenspace $\ker(g - \mathbf{1}_n)$, for certain matrices g. Recall that $\mathcal{O}$ is a Dedekind domain (see [45, Ex. 11.88]) and than the structure of $\mathfrak{p}$-torsion $\mathcal{O}$-modules is given as above (see 2.42). To be specific we calculate the limits

(a) $P_{\mathrm{GL},\infty,q,f}(\mathcal{A}) := \lim\limits_{n\to\infty} P_{\mathrm{GL},n,q,f}(\mathcal{A}) := \lim\limits_{n\to\infty} \dfrac{|\{g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^f) \mid \ker(g - \mathbf{1}_n) \cong \mathcal{A}\}|}{|\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^f)|}$,

(b) $P_{\mathrm{Sp},\infty,q,f}(\mathcal{A}) := \lim\limits_{n\to\infty} P_{\mathrm{Sp},n,q,f}(\mathcal{A}) := \lim\limits_{n\to\infty} \dfrac{|\{g \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^f) \mid \ker(g - \mathbf{1}_{2n}) \cong \mathcal{A}\}|}{|\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^f)|}$,

(c) $P_{\mathrm{Sp}^{(m)},\infty,q,f}(\mathcal{A}) := \lim\limits_{n\to\infty} P_{\mathrm{Sp}^{(m)},n,q,f}(\mathcal{A}) := \lim\limits_{n\to\infty} \dfrac{|\{g \in \mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^f) \mid \ker(g - \mathbf{1}_{2n}) \cong \mathcal{A}\}|}{|\mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^f)|}$,

(d) $P_{\mathrm{O},\infty,q,f}(\mathcal{A}) := \lim\limits_{n\to\infty} P_{\mathrm{O},n,q,f}(\mathcal{A}) := \lim\limits_{n\to\infty} \dfrac{|\{g \in \mathrm{O}_n(\mathcal{O}/\mathfrak{p}^f) \mid \ker(g - \mathbf{1}_n) \cong \mathcal{A}\}|}{|\mathrm{O}_n(\mathcal{O}/\mathfrak{p}^f)|}$,

see Section 2.3 for the definition of these groups.

In the last part of this chapter we show how to derive a distribution on the set of finite abelian p-groups from one on the set of $\mathcal{O}$-modules.

Before we start the respective cases, we need to introduce a further notation.

Notation 4.1. Given $t \in \mathbb{N}$ and natural numbers $k_1, \dots, k_t$ we set

$$s_0 := 0, \quad s_j := \sum_{i=1}^{j} k_i.$$

for $j \in \{1, \dots, t\}$.

4.1 The general linear groups

Before determining $P_{\mathrm{GL},\infty,q,f}(\mathcal{A})$ we need some more notations and technical results.

Notation 4.2. For natural numbers $k \leq n$ and a prime power q we set

$$R_{\mathrm{GL},n,q}(k) := |\{g \in \mathrm{Mat}_n(\mathbb{F}_q) \mid \dim(\ker(g)) = k\}|$$

to be the number of $n \times n$-matrices over $\mathbb{F}_q$ with a k-dimensional kernel. Moreover, we write $R_{\mathrm{GL},i,q} := R_{\mathrm{GL},s_i,q}(s_{i-1})$ for $i \in \{1, \dots, t\}$ and s_i from Notation 4.1.

The value of $R_{\mathrm{GL},n,q}(k)$ is given by the next lemma.

Lemma 4.3. *With the notations above we get*

$$R_{\mathrm{GL},n,q}(k) = \binom{n}{k}_q \cdot (q^n - 1) \cdots (q^n - q^{n-k-1}) \text{ if } k < n, \text{ and } R_{\mathrm{GL},n,q}(n) = 1.$$

Proof. See [41, 1.7]. □

The next results will be used to simplify the proof of the main theorem.

Lemma 4.4. *For $\alpha_1, \dots, \alpha_t \in \mathbb{N}$ with $\alpha_1 > \cdots > \alpha_t$ and $k_1, \dots, k_t \in \mathbb{N}$ the following holds for all $t \geq 2$:*

$$\sum_{i=1}^{t-1} s_i^2(\alpha_i - \alpha_{i+1}) + s_t^2 \alpha_t = \sum_{1 \leq i,j \leq t} \min\{\alpha_i, \alpha_j\} k_i k_j.$$

Proof. We prove this by induction on t. For the case $t = 2$ we obtain

$$\begin{aligned}\sum_{i=1}^{1} s_i^2(\alpha_i - \alpha_{i+1}) + s_2^2\alpha_2 &= k_1^2(\alpha_1 - \alpha_2) + (k_1 + k_2)^2\alpha_2 \\ &= k_1^2\alpha_1 - k_1^2\alpha_2 + k_1^2\alpha_2 + 2k_1k_2\alpha_2 + k_2^2\alpha_2 \\ &= \sum_{1\le i,j\le 2} \min\{\alpha_i, \alpha_j\}k_ik_j.\end{aligned}$$

For the induction step we get

$$\begin{aligned}\sum_{i=1}^{t-1} s_i^2(\alpha_i - \alpha_{i+1}) + s_t^2\alpha_t &= \sum_{i=1}^{t-2} s_i^2(\alpha_i - \alpha_{i+1}) + s_{t-1}^2\alpha_{t-1} - s_{t-1}^2\alpha_t + s_t^2\alpha_t \\ &= \sum_{1\le i,j\le t-1} \min\{\alpha_i, \alpha_j\}k_ik_j - s_{t-1}^2\alpha_t + (s_{t-1} + k_t)^2\alpha_t \\ &= \sum_{1\le i,j\le t-1} \min\{\alpha_i, \alpha_j\}k_ik_j + 2s_{t-1}k_t\alpha_t + k_t^2\alpha_t \\ &= \sum_{1\le i,j\le t} \min\{\alpha_i, \alpha_j\}k_ik_j\end{aligned}$$

and the claim is proven. □

Lemma 4.5. *Let $k_1, \ldots, k_t$ be natural numbers, s_i as in Notation 4.1 and $R_{\mathrm{GL},i,q}$ as in Notation 4.2. Then the following is true for all $t \in \mathbb{N}$.*

$$\prod_{i=1}^{t} R_{\mathrm{GL},i,q} = \frac{(q)_{s_t}^2 \cdot q^{s_t^2}}{\prod_{i=1}^{t}(q)_{k_i}}.$$

Proof. We do induction on t. In the case $t = 1$ we obtain for the left hand side

$$R_{\mathrm{GL},1,q} = q^{\binom{s_1}{2}} \prod_{i=1}^{s_1}(q^i - 1)$$

and for the right hand side

$$\frac{(q)_{s_1}^2 \cdot q^{s_1^2}}{(q)_{s_1}} = \frac{\prod_{i=1}^{s_1}(q^i - 1)}{q^{\binom{s_1+1}{2}}} \cdot q^{s_1^2} = q^{\binom{s_1}{2}} \prod_{i=1}^{s_1}(q^i - 1),$$

the same term. Now we use the induction hypothesis to get

$$\prod_{i=1}^{t} R_{\mathrm{GL},i,q} = \prod_{i=1}^{t-1} R_{\mathrm{GL},i,q} \cdot R_{\mathrm{GL},t,q} = \frac{(q)_{s_{t-1}}^2 \cdot q^{s_{t-1}^2}}{\prod_{i=1}^{t-1} (q)_{k_i}} \cdot \binom{s_t}{s_{t-1}}_q (q^{s_t} - 1) \cdots (q^{s_t} - q^{k_t - 1})$$

$$= \frac{\prod_{i=1}^{s_{t-1}} (q^i - 1)^2}{q^{s_{t-1}} \cdot \prod_{i=1}^{t-1} (q)_{k_i}} \cdot \frac{\prod_{i=k_t+1}^{s_t} (q^i - 1) \cdot \prod_{i=s_{t-1}+1}^{s_t} (q^i - 1) \cdot q^{\binom{k_t}{2}}}{\prod_{i=1}^{s_{t-1}} (q^i - 1)}$$

$$= \frac{\prod_{i=1}^{s_t} (q^i - 1)^2 \cdot q^{\binom{k_t}{2}}}{q^{s_{t-1}} \cdot \prod_{i=1}^{t-1} (q)_{k_i} \cdot \prod_{i=1}^{k_t} (q^i - 1)} = \frac{(q)_{s_t}^2 \cdot q^{s_t^2 + s_t} \cdot q^{\binom{k_t}{2}}}{q^{s_{t-1}} \cdot \prod_{i=1}^{t} (q)_{k_i} \cdot q^{\binom{k_t+1}{2}}} = \frac{(q)_{s_t}^2 \cdot q^{s_t^2}}{\prod_{i=1}^{t} (q)_{k_i}}$$

and the result is shown. □

Lemma 4.6. *Let $\mathcal{O}$ be a ring and let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. For natural numbers α, n and any $g \in \mathrm{Mat}_n(\mathfrak{p}^\alpha/\mathfrak{p}^{\alpha+1})$ we have $g + \mathbf{1}_n \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha+1})$.*

Proof. It is easy to see that the determinant of $g + \mathbf{1}_n$ is a unit in $\mathcal{O}/\mathfrak{p}^{\alpha+1}$. □

We need one last statement to prove the main result of this section. Namely it is the fruit of Jason Fulman's work in [22].

Theorem 4.7. *Let n and r be natural numbers and let $\mathcal{O}$ be a ring with a prime ideal $\mathfrak{p} \trianglelefteq \mathcal{O}$, which satisfies $q = |\mathcal{O}/\mathfrak{p}|$. Then for a finite free $\mathcal{O}/\mathfrak{p}$-module $\mathcal{A}$ of rank r the following holds.*

(a) $P_{\mathrm{GL},n,q,1}(\mathcal{A}) = \dfrac{1}{|\mathrm{GL}_r(\mathcal{O}/\mathfrak{p})|} \cdot \displaystyle\sum_{i=0}^{n-r} \frac{(-1)^i q^{-ri}}{(q^i - 1) \cdots (q - 1)}$,

(b) $P_{\mathrm{GL},\infty,q,1}(\mathcal{A}) = \dfrac{(q)_\infty}{(q)_r^2 \cdot q^{r^2}}$

Proof. See [22, Thm. 6]. □

Now we are ready to determine $P_{\mathrm{GL},\infty,q,f}(\mathcal{A})$ for arbitrary finite $\mathfrak{p}$-torsion modules $\mathcal{A}$.

Theorem 4.8. *Let $\mathcal{O}$ be a ring and let $\mathfrak{p} \trianglelefteq \mathcal{O}$ be a prime ideal with $q = |\mathcal{O}/\mathfrak{p}|$. Further let n, f, t, $\alpha_1, \ldots, \alpha_t$, $k_1, \ldots, k_t$ be natural numbers so that $f > \alpha_1 > \cdots > \alpha_t$ and let*

$$\mathcal{A} = (\mathcal{O}/\mathfrak{p}^{\alpha_1})^{k_1} \oplus \cdots \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t}$$

be a finite $\mathfrak{p}$*-torsion* $\mathcal{O}$*-module of rank* $r := \operatorname{rank}(\mathcal{A}) = \sum_{i=1}^{t} k_i$. *Then with* $R_{\mathrm{GL},i,q}$ *as in Notation 4.2 we have*

(a) $P_{\mathrm{GL},n,q,f}(\mathcal{A}) = P_{\mathrm{GL},n,q,1}((\mathcal{O}/\mathfrak{p})^r) \cdot \dfrac{\prod_{i=1}^{t} R_{\mathrm{GL},i,q}}{q^{\sum_{1\leq i,j\leq t}\min\{\alpha_i,\alpha_j\}k_ik_j}}$,

(b) $P_{\mathrm{GL},\infty,q,f}(\mathcal{A}) = (q)_\infty \cdot \dfrac{1}{|\mathrm{Aut}_{\mathcal{O}}(\mathcal{A})|}$.

Proof. We use the notation from the theorem. So let $\mathcal{A}$ be a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module of rank r and let s_i and $R_{\mathrm{GL},i,q}$ be as introduced in the notations above. In order to determine $P_{\mathrm{GL},n,q,f}(\mathcal{A})$ we define the natural epimorphisms

$$\begin{aligned}
\pi_0 &: (\mathcal{O}/\mathfrak{p}^f)^n \to (\mathcal{O}/\mathfrak{p})^n\\
\pi_1 &: (\mathcal{O}/\mathfrak{p}^f)^n \to (\mathcal{O}/\mathfrak{p}^{\alpha_t})^n\\
\pi_2 &: (\mathcal{O}/\mathfrak{p}^f)^n \to (\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^n\\
\pi_3 &: (\mathcal{O}/\mathfrak{p}^f)^n \to (\mathcal{O}/\mathfrak{p}^{\alpha_{t-1}})^n\\
\pi_4 &: (\mathcal{O}/\mathfrak{p}^f)^n \to (\mathcal{O}/\mathfrak{p}^{\alpha_{t-1}+1})^n
\end{aligned}$$

Furthermore using the assumption $\alpha_{t-1} > \alpha_t$ we introduce the following canonical epimorphisms on the general linear groups

$$\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_{t-1}+1}) \xrightarrow{\kappa_4} \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_{t-1}}) \xrightarrow{\kappa_3} \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t+1}) \xrightarrow{\kappa_2} \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t}) \xrightarrow{\kappa_1} \mathrm{GL}_n(\mathcal{O}/\mathfrak{p})$$

and at last point we should say what we mean by $\mathcal{A} \cong \ker(g - \mathbf{1}_n)$ for $g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^f)$. First of all the general linear group $\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^f)$ operates as a $\mathcal{O}/\mathfrak{p}^f$-module automorphism on $(\mathcal{O}/\mathfrak{p}^f)^n$ via matrix multiplication from the left. Moreover the isomorphism classes of $\mathcal{O}/\mathfrak{p}^f$-submodules of $(\mathcal{O}/\mathfrak{p}^f)^n$ are exactly of the form of $\mathcal{A}$, so it makes sense to consider $\mathcal{A} \cong \ker(g - \mathbf{1}_n)$. Before we come to business we may assume $n \geq r$, since otherwise already both sides of the equation in (a) are 0, and set

$$\begin{aligned}
\mathcal{A}_0 &:= \pi_0(\mathcal{A}) = (\mathcal{O}/\mathfrak{p})^r\\
\mathcal{A}_1 &:= \pi_1(\mathcal{A}) = (\mathcal{O}/\mathfrak{p}^{\alpha_t})^r\\
\mathcal{A}_2 &:= \pi_2(\mathcal{A}) = (\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^{s_{t-1}} \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t}\\
\mathcal{A}_3 &:= \pi_3(\mathcal{A}) = (\mathcal{O}/\mathfrak{p}^{\alpha_{t-1}})^{s_{t-1}} \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t}\\
\mathcal{A}_4 &:= \pi_4(\mathcal{A}) = (\mathcal{O}/\mathfrak{p}^{\alpha_{t-1}+1})^{s_{t-2}} \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_{t-1}})^{k_{t-1}} \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t}
\end{aligned}$$

Now we initially determine the proportion of matrices $g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p})$ with $\ker(g - \mathbf{1}_n) \cong \mathcal{A}_0$, in other words we want to calculate $P_{\mathrm{GL},n,q,1}(\mathcal{A}_0)$, but this is given by Fulman (4.7 (a)). Let $g = (g_{ij})_{1\leq i,j\leq n} \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p})$ be a matrix with $\ker(g - \mathbf{1}_n) \cong \mathcal{A}_0$. We want to specify the number of elements $h \in \kappa_1^{-1}(g) \subseteq \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t})$ with $\ker(h - \mathbf{1}_n) \cong \mathcal{A}_1$. So let $h \in \kappa_1^{-1}(g)$ such that $\ker(h - \mathbf{1}_n) \cong \mathcal{A}_1$, then we observe

$$\ker(h - \mathbf{1}_n) \cong (\mathcal{O}/\mathfrak{p}^{\alpha_t})^r. \tag{4.1}$$

With this we have free choice for h_{ij} with $i > r$ or $j > r$ and so we obtain $q^{(n^2-r^2)(\alpha_t-1)}$ possibilities. On the other hand the condition (4.1) implies

$$h - \mathbf{1}_n\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t})^r} = 0.$$

So all in all we obtain

$$q^{(n^2-r^2)(\alpha_t-1)} = |\{h \in \kappa_1^{-1}(g) \mid \ker(h - \mathbf{1}_n) \cong \mathcal{A}_1\}|$$

for a fixed $g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p})$. We collect the last considerations and arrive at

$$\begin{aligned} P_{\mathrm{GL},n,q,\alpha_t}(\mathcal{A}_1) &= \frac{|\{g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}) \mid \ker(g - \mathbf{1}_n) \cong \mathcal{A}_0\}| \cdot q^{(n^2-r^2)(\alpha_t-1)}}{|\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t})|} \\ &= P_{\mathrm{GL},n,q,1}(\mathcal{A}_0) \cdot \frac{q^{(n^2-r^2)(\alpha_t-1)}}{q^{n^2(\alpha_t-1)}}, \end{aligned}$$

where we use $|\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t})| = |\mathrm{GL}_n(\mathcal{O}/\mathfrak{p})| \cdot q^{n^2(\alpha_t-1)}$ (see 2.6.(a)) for the second equality.
For the next step let $g = (g_{ij})_{1\leq i,j\leq n} \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t})$ be a matrix with $\ker(g - \mathbf{1}_n) \cong \mathcal{A}_1$. Here we count the number of matrices $h \in \kappa_2^{-1}(g) \subseteq \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})$ so that $\ker(h - \mathbf{1}_n) \cong \mathcal{A}_2$ holds. The condition $\ker(h - \mathbf{1}_n) \subseteq (\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r$ yields q possibilities for every h_{ij} with $i > r$ or $j > r$ since $q = |\mathfrak{p}^{\alpha_t}/\mathfrak{p}^{\alpha_t+1}|$. Moreover we have $g - \mathbf{1}_n\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t})^r} \equiv 0 \bmod \mathfrak{p}^{\alpha_t}$ and so

$$h - \mathbf{1}_n\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r} \equiv B \bmod \mathfrak{p}^{\alpha_t+1},$$

for an $B \in \mathrm{Mat}_r(\mathfrak{p}^{\alpha_t}/\mathfrak{p}^{\alpha_t+1})$. By Lemma 4.6 the condition $B + \mathbf{1}_r = h \in \mathrm{GL}_r(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})$ is true for any B. Furthermore we have the isomorphism of $\mathcal{O}/\mathfrak{p}^f$-modules

$$\ker(h - \mathbf{1}_n)/(\mathcal{O}/\mathfrak{p}^{\alpha_t})^r \cong (\mathcal{O}/\mathfrak{p})^{s_{t-1}}.$$

Now we combine the last two conditions and obtain that the number of lifts $h\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r}$ with

$$\ker\left(h - \mathbf{1}_n\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r}\right) \cong (\mathcal{O}/\mathfrak{p})^{s_{t-1}}$$

is the order of the following set

$$\{g \in \mathrm{Mat}_r(\mathcal{O}/\mathfrak{p}) \mid \dim(\ker(g)) = s_{t-1}\}.$$

In other words, what we need to know is $R_{\mathrm{GL},t,q}$, but this value is given by Lemma 4.3. We summarize the last results and obtain

$$\begin{aligned}
P_{\mathrm{GL},n,q,\alpha_t+1}(\mathcal{A}_2) &= \frac{|\{g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t}) \mid \ker(g-1) \cong \mathcal{A}_1\}| \cdot R_{\mathrm{GL},t,q} \cdot q^{n^2-r^2}}{|\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})|} \\
&= \frac{|\{g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t}) \mid \ker(g-1) \cong \mathcal{A}_1\}| \cdot R_{\mathrm{GL},t,q} \cdot q^{n^2-r^2}}{|\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t})| \cdot q^{n^2}} \\
&= P_{\mathrm{GL},n,q,1}(\mathcal{A}_0) \cdot \frac{q^{(n^2-r^2)(\alpha_t-1)} \cdot R_{\mathrm{GL},t,q} \cdot q^{n^2-r^2}}{q^{n^2} \cdot q^{n^2(\alpha_t-1)}} \\
&= P_{\mathrm{GL},n,q,1}(\mathcal{A}_0) \cdot \frac{R_{\mathrm{GL},t,q}}{q^{r^2\alpha_t}}.
\end{aligned}$$

Now we repeat this procedure for the groups $\mathcal{A}_3$ and $\mathcal{A}_4$ and get

$$\begin{aligned}
P_{\mathrm{GL},n,q,\alpha_{t-1}+1}(\mathcal{A}_4) &= P_{\mathrm{GL},n,q,1}(\mathcal{A}_0) \cdot \frac{q^{(n^2-r^2)\alpha_t} \cdot q^{(n^2-s_{t-1}^2)(\alpha_{t-1}-\alpha_t)}}{q^{n^2\alpha_t} \cdot q^{n^2(\alpha_{t-1}-\alpha_t)}} \cdot R_{\mathrm{GL},t,q} \cdot R_{\mathrm{GL},t-1,q} \\
&= P_{\mathrm{GL},n,q,1}(\mathcal{A}_0) \cdot \frac{R_{\mathrm{GL},t,q} \cdot R_{\mathrm{GL},t-1,q}}{q^{r^2\alpha_t + s_{t-1}^2(\alpha_{t-1}-\alpha_t)}}.
\end{aligned}$$

We continue this method until we reach $\mathcal{A}$ and obtain using Lemma 4.4 the formula

$$P_{\mathrm{GL},n,q,\alpha_1+1}(\mathcal{A}) = P_{\mathrm{GL},n,q,1}(\mathcal{A}_0) \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{GL},i,q}}{q^{\sum_{1\le i,j\le t}\min\{\alpha_i,\alpha_j\}k_ik_j}}.$$

The step from $\alpha_1 + 1$ to f is more or less trivial, because the proportion does not change.

Namely we have

$$\begin{aligned}P_{\mathrm{GL},n,q,f}(\mathcal{A}) &= \frac{|\{g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_1+1}) \mid \ker(g-1) \cong \mathcal{A}\}| \cdot q^{n^2(f-\alpha_1-1)}}{|\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^f)|} \\ &= \frac{|\{g \in \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_1+1}) \mid \ker(g-1) \cong \mathcal{A}\}| \cdot q^{n^2(f-\alpha_1-1)}}{|\mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^{\alpha_1+1}) \cdot q^{n^2(f-\alpha_1-1)}|} \\ &= P_{\mathrm{GL},n,q,\alpha_1+1}(\mathcal{A})\end{aligned}$$

and part (a) is shown.
For the second part we use Theorem 4.7.(b) to get

$$\begin{aligned}P_{\mathrm{GL},\infty,q,f}(\mathcal{A}) &= \lim_{n\to\infty} P_{\mathrm{GL},n,q,f}(\mathcal{A}) \\ &= \lim_{n\to\infty} P_{\mathrm{GL},n,q,1}(\mathcal{A}_0) \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{GL},i,q}}{q^{\sum_{1\le i,j\le t}\min\{\alpha_i,\alpha_j\}k_ik_j}} \\ &= (q)_\infty \cdot \frac{1}{|\mathrm{Aut}_{\mathcal{O}}(\mathcal{A})|}\end{aligned}$$

where we use Lemma 4.5 and Theorem 2.44.(c) for the last equality. □

Remark 4.9. We have seen in the proof that $P_{\mathrm{GL},n,q,f}$ is independent of f. But we need to take care of the condition $f > \alpha_1$, because in the case $f = \alpha_1$ we get another distribution as the case of finite free $\mathcal{O}/\mathfrak{p}$-modules shows.

Remark 4.10. In the case $\mathcal{O} = \mathbb{Z}$ the result of the theorem corresponds to the conjecture of Cohen and Lenstra (see Cor. 3.3 and Conj. 3.7).

We finish this section with an example.

Corollary 4.11. *Let $\mathcal{A} \cong \mathbb{Z}/p^\alpha\mathbb{Z}$ be a cyclic group of order p^α with p prime. Then we have*

(a) $P_{\mathrm{GL},n,p,f}(\mathcal{A}) = P_{\mathrm{GL},n,p,1}(\mathbb{Z}/p\mathbb{Z}) \cdot \dfrac{(p-1)}{p^\alpha}$,

(b) $P_{\mathrm{GL},\infty,p,f}(\mathcal{A}) = (p)_\infty \cdot \dfrac{1}{p^{\alpha-1}(p-1)}$.

4.2 The symplectic groups

In this section we determine $P_{\mathrm{Sp},\infty,q,f}(\mathcal{A})$. Before we can do this we need to invest some work in technical results.

Lemma 4.12. *Given natural numbers $\alpha_1, \ldots, \alpha_t,\ k_1, \ldots, k_t$ with $\alpha_1 > \cdots > \alpha_t$ we have for all $t \geq 2$:*

$$\sum_{i=1}^{t-1} s_i(\alpha_i - \alpha_{i+1}) + s_t\alpha_t = \sum_{i=1}^{t} \alpha_i k_i$$

where s_i is introduced in Notation 4.1.

Proof. We do induction on t. For $t = 2$ we get

$$\begin{aligned} s_1(\alpha_1 - \alpha_2) + s_2\alpha_2 &= k_1\alpha_1 - k_1\alpha_2 + k_1\alpha_2 + k_2\alpha_2 \\ &= k_1\alpha_1 + k_2\alpha_2. \end{aligned}$$

For the induction step we obtain

$$\begin{aligned} \sum_{i=1}^{t-1} s_i(\alpha_i - \alpha_{i+1}) + s_t\alpha_t &= \sum_{i=1}^{t-2} s_i(\alpha_i - \alpha_{i+1}) + s_{t-1}(\alpha_{t-1} - \alpha_t) + s_t\alpha_t \\ &= \sum_{i=1}^{t-2} s_i(\alpha_i - \alpha_{i+1}) + s_{t-1}\alpha_{t-1} + (s_t - s_{t-1})\alpha_t \\ &= \sum_{i=1}^{t} \alpha_i k_i \end{aligned}$$

and the statement is shown. □

The next result combines the last lemma and Lemma 4.4.

Corollary 4.13. *With the same notation as in Lemma 4.12 we get*

$$\sum_{i=1}^{t-1} \binom{s_i + 1}{2}(\alpha_i - \alpha_{i+1}) + \binom{s_t + 1}{2}\alpha_t = \frac{1}{2}\left(\sum_{1 \leq i,j \leq t} \min\{\alpha_i, \alpha_j\}k_ik_j + \sum_{i=1}^{t} \alpha_i k_i\right).$$

Now we want to define the analogue values for $R_{\mathrm{GL},n,q}(k)$ in the symplectic case.

Lemma 4.14. *Let n and α be natural numbers. Given a ring $\mathcal{O}$ and a non-zero prime ideal $\mathfrak{p} \trianglelefteq \mathcal{O}$ of $\mathcal{O}$ there is a bijection between the sets M and N, where*

$$M := \{g \in \mathrm{Mat}_{2n}(\mathfrak{p}^\alpha/\mathfrak{p}^{\alpha+1}) \mid g + \mathbf{1}_{2n} \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha+1})\}$$

and

$$N := \{\begin{pmatrix} A & B \\ C & -A^t \end{pmatrix} \in \mathrm{Mat}_{2n}(\mathcal{O}/\mathfrak{p}) \mid A, B, C \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{p}) \text{ and } B = B^t, C = C^t\}. \tag{4.2}$$

Proof. Let M and N be as in the statement. Then $g \in \mathrm{Mat}_{2n}(\mathcal{O}/\mathfrak{p})$ is an element of M if and only if the following equation holds

$$(g + \mathbf{1}_{2n})^t \cdot J_n \cdot (g + \mathbf{1}_{2n}) = J_n.$$

Since $g^t J_n g = 0_n$ this is equivalent to

$$g^t J_n + J_n g = 0_n. \tag{4.3}$$

Now we write $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ as a block matrix with blocks of size n and obtain by equation (4.3) the following relations

$$B = B^t,\ C = C^t,\ D = -A^t.$$

The isomorphism $\mathfrak{p}^\alpha/\mathfrak{p}^{\alpha+1} \cong \mathcal{O}/\mathfrak{p}$ implies the statement. □

Notation 4.15. For a natural number n we denote by

$$\mathrm{Sym}_n(\mathcal{O}/\mathfrak{p}^f) := \{g \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{p}^f) \mid g = g^t\}$$

the set of symmetric $n \times n$-matrices over $\mathcal{O}/\mathfrak{p}^f$.

Lemma 4.16. *Let N be given by (4.2). Then there exists a bijective map f from N into $\mathrm{Sym}_{2n}(\mathcal{O}/\mathfrak{p})$ with the property that $\mathrm{rank}(g) = \mathrm{rank}(f(g))$ for all $g \in N$.*

Proof. For $g = \begin{pmatrix} A & B \\ C & -A^t \end{pmatrix} \in N$ we define the map

$$\tilde{f} : N \to \mathrm{Mat}_{2n}(\mathcal{O}/\mathfrak{p}), \quad \tilde{f}(g) := \begin{pmatrix} B & A \\ A^t & -C \end{pmatrix}.$$

Obviously $\tilde{f}$ is injective and since $\tilde{f}$ just permutes columns and multiplies rows by -1, it preserves the rank of g. Moreover clearly $\tilde{f}(N) \subseteq \mathrm{Sym}_{2n}(\mathcal{O}/\mathfrak{p})$ and in addition

$$|\tilde{f}(N)| = q^{2n^2+n} = |\mathrm{Sym}_{2n}(\mathcal{O}/\mathfrak{p})|,$$

so $f : N \to \mathrm{Im}(\tilde{f})$ is a map as required. □

Notation 4.17. Let n and k be natural numbers with $k \leq n$ and let q be a prime power. Then we write

$$\begin{aligned} R_{\mathrm{Sp},2n,q}(k) &:= |\{g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Mat}_{2n}(\mathbb{F}_q) \mid D = -A^t, B = B^t, C = C^t \text{ and } \dim(\ker(g)) = k\}| \\ &= |\{g \in \mathrm{Sym}_{2n}(\mathbb{F}_q) \mid \dim(\ker(g)) = k\}| \end{aligned}$$

for the number of symmetric $2n \times 2n$-matrices having a k-dimensional kernel. Furthermore we define

$$R_{\mathrm{Sp},2n+1,q}(k) := |\{g \in \mathrm{Sym}_{2n+1}(\mathbb{F}_q) \mid \dim(\ker(g)) = k\}|$$

and we write $R_{\mathrm{Sp},i,q} := R_{\mathrm{Sp},s_i,q}(s_{i-1})$ with s_i from Notation 4.1.

In the next lemma we determine the values $R_{\mathrm{Sp},n,q}(k)$.

Lemma 4.18. *With the notations from above we get*

(a) $R_{\mathrm{Sp},n,q}(n) = 1.$

(b) $R_{\mathrm{Sp},2n,q}(2k) = \prod_{i=1}^{n-k} \frac{q^{2i}}{(q^{2i}-1)} \cdot \prod_{i=0}^{2(n-k)-1} (q^{2n-i}-1),$ *for* $0 \leq k \leq n-1.$

(c) $R_{\mathrm{Sp},2n,q}(2k+1) = \prod_{i=1}^{n-k-1} \frac{q^{2i}}{(q^{2i}-1)} \cdot \prod_{i=0}^{2(n-k-1)} (q^{2n-i}-1),$ *for* $0 \leq k \leq n-1.$

(d) $R_{\mathrm{Sp},2n+1,q}(2k) = \prod_{i=1}^{n-k} \frac{q^{2i}}{(q^{2i}-1)} \cdot \prod_{i=0}^{2(n-k)} (q^{2n-i}-1),$ *for* $0 \leq k \leq n.$

(e) $R_{\mathrm{Sp},2n+1,q}(2k+1) = \prod_{i=1}^{n-k} \frac{q^{2i}}{(q^{2i}-1)} \cdot \prod_{i=0}^{2(n-k)-1} (q^{2n-i}-1)$, *for* $0 \leq k \leq n-1$.

Proof. Jessie Mac Williams determines in [40, Thm. 2] the number of symmetric $n \times n$-matrices over a finite field having rank r. Since $\dim(\ker(g)) = n - r$ we can easily deduce the values $R_{\mathrm{Sp},n,q}(k)$ by Williams work. □

Similarly to the case of the general linear groups we repeat here a theorem of Fulman as an important ingredient of the proof of Theorem 4.20.

Theorem 4.19. *Let n and r be natural numbers. Given a ring $\mathcal{O}$ and a prime ideal $\mathfrak{p} \trianglelefteq \mathcal{O}$ with $q = |\mathcal{O}/\mathfrak{p}|$ we obtain for a finite free $\mathcal{O}/\mathfrak{p}$-module $\mathcal{A}$ of rank r*

(a) $P_{\mathrm{Sp},2n,q,1}(\mathcal{A}) = \frac{1}{|\mathrm{Sp}_{2k}(\mathcal{O}/\mathfrak{p})|} \cdot \sum_{i=0}^{n-k} \frac{(-1)^i q^{i(i+1)}}{|\mathrm{Sp}_{2i}(\mathcal{O}/\mathfrak{p})| q^{2ik}}$, *if* $r = 2k$,

(b) $P_{\mathrm{Sp},2n,q,1}(\mathcal{A}) = \frac{1}{q^{2k+1}|\mathrm{Sp}_{2k}(\mathcal{O}/\mathfrak{p})|} \cdot \sum_{i=0}^{n-k-1} \frac{(-1)^i q^{i(i+1)}}{|\mathrm{Sp}_{2i}(\mathcal{O}/\mathfrak{p})| q^{2i(k+1)}}$, *if* $r = 2k+1$,

(c) $P_{\mathrm{Sp},\infty,q,1}(\mathcal{A}) = \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{1}{q^{\binom{r+1}{2}}(q)_r}$.

Proof. See [23, Cor. 7] for (a) and (b) and [38, Prop. 3.1] for (c). □

Theorem 4.20. *Let $\mathcal{O}$ be a ring and let $\mathfrak{p} \trianglelefteq \mathcal{O}$ be a prime ideal with $q = |\mathcal{O}/\mathfrak{p}|$. Further let n, f, t, $\alpha_1, \ldots, \alpha_t$, $k_1, \ldots, k_t$ be natural numbers so that $f > \alpha_1 > \cdots > \alpha_t$ and let*

$$\mathcal{A} = (\mathcal{O}/\mathfrak{p}^{\alpha_1})^{k_1} \oplus \cdots \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t}$$

be a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module of rank $r := \mathrm{rank}(\mathcal{A}) = \sum_{i=1}^{t} k_i$. With $R_{\mathrm{Sp},i,q}$ as in 4.17 we get

(a) $P_{\mathrm{Sp},2n,q,f}(\mathcal{A}) = P_{\mathrm{Sp},2n,q,1}((\mathcal{O}/\mathfrak{p})^r) \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{Sp},i,q}}{q^{\frac{1}{2}(\sum_{1 \leq i,j \leq t} \min\{\alpha_i,\alpha_j\} k_i k_j + \sum_{i=1}^{t} \alpha_i k_i)}}$,

(b) $P_{\mathrm{Sp},\infty,q,f}(\mathcal{A}) = \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{1}{q^{\binom{r+1}{2}}(q)_r} \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{Sp},i,q}}{q^{\frac{1}{2}(\sum_{1 \leq i,j \leq t} \min\{\alpha_i,\alpha_j\} k_i k_j + \sum_{i=1}^{t} \alpha_i k_i)}}$.

Proof. We pick up the notations and the main idea of the proof of Theorem 4.8 to determine $P_{\mathrm{Sp},2n,q,f}(\mathcal{A})$, where now κ_i are the corresponding maps between the respective symplectic groups. The proportion $P_{\mathrm{Sp},2n,q,1}(\mathcal{A}_0)$ of matrices $g \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p})$ with $\ker(g-\mathbf{1}_{2n}) \cong \mathcal{A}_0$ is given by Theorem 4.19.(a). Now we compute the number of preimages $h \in \kappa_1^{-1}(g) \subseteq \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t})$ of $g = (g_{ij})_{1\leq i,j\leq 2n} \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p})$ having $\ker(g-\mathbf{1}_{2n}) \cong \mathcal{A}_0$, which satisfy $\ker(h-\mathbf{1}_{2n}) \cong \mathcal{A}_1$. Given $h \in \kappa_1^{-1}(g)$ with $\ker(h-\mathbf{1}_{2n}) \cong \mathcal{A}_1$ the isomorphism

$$\ker(h-\mathbf{1}_{2n}) \cong (\mathcal{O}/\mathfrak{p}^{\alpha_t})^r \tag{4.4}$$

implies that there are $q^{(\binom{2n+1}{2}-\binom{r+1}{2})(\alpha_t-1)}$ possibilities for h_{ij} with $i > r$ or $j > r$. On the other hand we use (4.4) to get

$$h-\mathbf{1}_{2n}\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t})^r} = 0.$$

Now putting this together we obtain

$$\begin{aligned} P_{\mathrm{Sp},2n,q,\alpha_t}(\mathcal{A}_1) &= \frac{|\{g \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}) \mid \ker(g-\mathbf{1}_{2n}) \cong \mathcal{A}_0\}| \cdot q^{(\binom{2n+1}{2}-\binom{r+1}{2})(\alpha_t-1)}}{|\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t})|} \\ &= P_{\mathrm{Sp},2n,q,1}(\mathcal{A}_0) \cdot \frac{q^{(\binom{2n+1}{2}-\binom{r+1}{2})(\alpha_t-1)}}{q^{\binom{2n+1}{2}(\alpha_t-1)}}, \end{aligned}$$

where the last equality follows from $|\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t})| = |\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p})| \cdot q^{\binom{2n+1}{2}(\alpha_t-1)}$ (see 2.6.(b)). For the next step we consider $g = (g_{ij})_{1\leq i,j\leq 2n} \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t})$ with $\ker(g-\mathbf{1}_{2n}) \cong \mathcal{A}_1$ and determine the number of preimages $h \in \kappa_2^{-1}(g) \subseteq \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})$, so that $\ker(h-\mathbf{1}_{2n}) \cong \mathcal{A}_2$ holds. Using the inclusion $\ker(h-\mathbf{1}_{2n}) \subseteq (\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r$ we get, that for h_{ij} with $i > r$ or $j > r$ there is free choice, so this provides q possibilities for every h_{ij}. Otherwise we have $g-\mathbf{1}_{2n}\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t})^r} \equiv 0 \bmod \mathfrak{p}^{\alpha_t}$ and so we get

$$h-\mathbf{1}_{2n}\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r} = B\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r}$$

for a suitable $B \in \mathrm{Mat}_{2n}(\mathfrak{p}^{\alpha_t}/\mathfrak{p}^{\alpha_t+1})$. By Lemma 4.14 the condition

$$B + \mathbf{1}_{2n} \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})$$

is equivalent to B being of the form

$$B = \begin{pmatrix} A & B \\ C & -A^t \end{pmatrix}.$$

But by Lemma 4.16 counting such B's is the same as counting symmetric matrices. Now we use

$$\ker(h-\mathbf{1}_{2n})\big|_{(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r} \cong (\mathcal{O}/\mathfrak{p})^{s_{t-1}}$$

to deduce that there are $|\{g \in \mathrm{Sym}_r(\mathcal{O}/\mathfrak{p}) \mid \dim(\ker(g)) = s_{t-1}\}| = R_{\mathrm{Sp},t,q}$ possible lifts for a fixed g on $(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})^r$. By summarizing the last results we get

$$\begin{aligned} P_{\mathrm{Sp},2n,q,\alpha_t+1}(\mathcal{A}_2) &= \frac{|\{g \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t}) \mid \ker(g-1) \cong \mathcal{A}_1\}| \cdot R_{\mathrm{Sp},t,q} \cdot q^{\binom{2n+1}{2}-\binom{r+1}{2}}}{|\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})|} \\ &= \frac{|\{g \in \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t}) \mid \ker(g-1) \cong \mathcal{A}_1\}| \cdot R_{\mathrm{Sp},t,q} \cdot q^{\binom{2n+1}{2}-\binom{r+1}{2}}}{|\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha_t})| \cdot q^{\binom{2n+1}{2}}} \\ &= P_{\mathrm{Sp},2n,q,1}(\mathcal{A}_0) \cdot \frac{q^{(\binom{2n+1}{2}-\binom{r+1}{2})(\alpha_t-1)} \cdot R_{\mathrm{Sp},t,q} \cdot q^{\binom{2n+1}{2}-\binom{r+1}{2}}}{q^{\binom{2n+1}{2}} \cdot q^{\binom{2n+1}{2}(\alpha_t-1)}} \\ &= P_{\mathrm{Sp},2n,q,1}(\mathcal{A}_0) \cdot \frac{R_{\mathrm{Sp},t,q}}{q^{\binom{r+1}{2}\alpha_t}}. \end{aligned}$$

We repeat the same procedure until we reach the module $\mathcal{A}$ and get the following result using Lemma 4.13:

$$P_{\mathrm{Sp},2n,q,\alpha_1+1}(\mathcal{A}) = P_{\mathrm{Sp},2n,q,1}(\mathcal{A}_0) \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{Sp},i,q}}{q^{\frac{1}{2}(\sum_{1\le i,j\le t}\min\{\alpha_i,\alpha_j\}k_ik_j+\sum_{i=1}^{t}\alpha_ik_i)}}.$$

As seen in the case of the general linear groups the step from α_1+1 to f does not change anything.

For the second part we use Theorem 4.19.(c) and obtain by

$$\begin{aligned} P_{\mathrm{Sp},\infty,q,f}(\mathcal{A}) &= \lim_{n\to\infty} P_{\mathrm{Sp},2n,q,f}(\mathcal{A}) \\ &= \lim_{n\to\infty} P_{\mathrm{Sp},2n,q,1}(\mathcal{A}_0) \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{Sp},i,q}}{q^{\frac{1}{2}(\sum_{1\le i,j\le t}\min\{\alpha_i,\alpha_j\}k_ik_j+\sum_{i=1}^{t}\alpha_ik_i)}} \\ &= \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{1}{q^{\binom{r+1}{2}}(q)_r} \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{Sp},i,q}}{q^{\frac{1}{2}(\sum_{1\le i,j\le t}\min\{\alpha_i,\alpha_j\}k_ik_j+\sum_{i=1}^{t}\alpha_ik_i)}} \end{aligned}$$

the result. □

As in the case of the general linear groups we finish this section with an example.

Corollary 4.21. *Given a cyclic group $\mathcal{A} \cong \mathbb{Z}/p^\alpha\mathbb{Z}$ of order p^α we get*

(a) $P_{\mathrm{Sp},2n,p,f}(\mathcal{A}) = P_{\mathrm{Sp},2n,p,1}(\mathbb{Z}/p\mathbb{Z}) \cdot \dfrac{(p-1)}{p^\alpha}$,

(b) $P_{\mathrm{Sp},\infty,p,f}(\mathcal{A}) = \dfrac{(p)_\infty}{(p^2)_\infty} \cdot \dfrac{1}{p^\alpha}$.

4.3 The m-th symplectic groups

Here we compute $P_{\mathrm{Sp}^{(1)},\infty,q,f}(\mathcal{A})$ and give the general idea how to determine $P_{\mathrm{Sp}^{(m)},2n,q,f}(\mathcal{A})$, for $m \geq 2$, because of technical reasons it seems out of reach to give a closed formula for $P_{\mathrm{Sp}^{(m)},2n,q,f}(\mathcal{A})$ for arbitrary m. Before we can start computing $P_{\mathrm{Sp}^{(1)},\infty,q,f}(\mathcal{A})$ we need the following results.

Lemma 4.22. *Let s_i be like in Notation 4.1 and let $R_{\mathrm{GL},i,q}$ be as in 4.2. Then for a prime power q and for all $t \in \mathbb{N}$ the following is true*

$$\frac{1}{q^{\binom{s_t+1}{2}}(q)_{s_t}} \cdot \prod_{i=1}^{t} R_{\mathrm{GL},i,q} = \prod_{i=1}^{s_t}(q^i - 1) \cdot \frac{1}{q^{s_t} \cdot \prod_{i=1}^{t}(q)_{k_i}}.$$

Proof. With similar arguments like in Lemma 4.5. □

Lemma 4.23. *Let $\mathcal{O}$ be a ring and let $\mathfrak{p} \trianglelefteq \mathcal{O}$ be a prime ideal, which satisfies $q = |\mathcal{O}/\mathfrak{p}|$. Let n and α be natural numbers. Then $g + \mathbf{1}_{2n} \in \mathrm{Sp}_{2n}^{(1)}(\mathcal{O}/\mathfrak{p}^{\alpha+1})$ for all $g \in \mathrm{Mat}_{2n}(\mathfrak{p}^\alpha/\mathfrak{p}^{\alpha+1})$.*

Proof. Let $g \in \mathrm{Mat}_{2n}(\mathfrak{p}^\alpha/\mathfrak{p}^{\alpha+1})$ be a matrix. Then $g + \mathbf{1}_{2n}$ is an element of $\mathrm{Sp}_{2n}^{(1)}(\mathcal{O}/\mathfrak{p}^{\alpha+1})$ if and only if $g + \mathbf{1}_{2n}$ is an element of $\mathrm{GL}_{2n}(\mathcal{O}/\mathfrak{p}^{\alpha+1})$ and the equation

$$(g + \mathbf{1}_{2n})^t \cdot J_n \cdot (g + \mathbf{1}_{2n}) \equiv J_n \bmod \mathfrak{p}$$

holds. The first condition is true by Lemma 4.6 and the second is trivial. □

Now we can prove the main result of this section.

Theorem 4.24. *Let $\mathcal{O}$ be a ring and let $\mathfrak{p} \trianglelefteq \mathcal{O}$ be a prime ideal with $q = |\mathcal{O}/\mathfrak{p}|$. Let $n,\ f,\ t,\ \alpha_1, \dots, \alpha_t,\ k_1, \dots, k_t$ be natural numbers so that $f > \alpha_1 > \dots > \alpha_t$ and let*

$$\mathcal{A} = (\mathcal{O}/\mathfrak{p}^{\alpha_1})^{k_1} \oplus \dots \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t}$$

be a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module of rank $r := \operatorname{rank}(\mathcal{A}) = \sum_{i=1}^{t} k_i$. For $R_{\mathrm{GL},i,q}$ as in 4.2 we obtain

(a) $P_{\mathrm{Sp}^{(1)},2n,q,f}(\mathcal{A}) = P_{\mathrm{Sp},2n,q,1}((\mathcal{O}/\mathfrak{p})^r) \cdot \dfrac{\prod_{i=1}^{t} R_{\mathrm{GL},i,q}}{q^{\sum_{1 \le i,j \le t} \min\{\alpha_i,\alpha_j\} k_i k_j}},$

(b) $P_{\mathrm{Sp}^{(1)},\infty,q,f}(\mathcal{A}) = \dfrac{(q)_\infty}{(q^2)_\infty} \cdot \dfrac{(q)_r \cdot q^{\binom{r}{2}}}{|\mathrm{Aut}_{\mathcal{O}}(\mathcal{A})|}.$

Proof. We keep the notations of the proof of Theorem 4.8, where we modify the κ_i to be the maps between the corresponding 1-st symplectic groups. So we need to determine the number of elements $g \in \mathrm{Sp}_{2n}^{(1)}(\mathcal{O}/\mathfrak{p}^f)$ so that $\ker(g - \mathbf{1}_{2n}) \cong \mathcal{A}$. In the first step we want to know the proportion of elements $g \in \mathrm{Sp}_{2n}^{(1)}(\mathcal{O}/\mathfrak{p})$ satisfying $\ker(g - \mathbf{1}_{2n}) \cong \mathcal{A}_0$. But since $\mathrm{Sp}_{2n}^{(1)}(\mathcal{O}/\mathfrak{p}) = \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p})$ this is given by Theorem 4.19.(a). Because of Lemma 4.23 and the definition of $\mathrm{Sp}_{2n}^{(1)}(\mathcal{O}/\mathfrak{p}^f)$ the next steps of the proof can be done in the same way as in the proof of 4.8. All in all we obtain the stated result. For part (b) we obtain by Theorem 4.19.(c)

$$\begin{aligned}
P_{\mathrm{Sp}^{(1)},\infty,q,f}(\mathcal{A}) &= \lim_{n\to\infty} P_{\mathrm{Sp}^{(1)},2n,q,f}(\mathcal{A}) = \lim_{n\to\infty} P_{\mathrm{Sp}^{(1)},2n,q,1}(\mathcal{A}_0) \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{GL},i,q}}{q^{\sum_{1 \le i,j \le t} \min\{\alpha_i,\alpha_j\} k_i k_j}} \\
&= \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{1}{q^{\binom{r+1}{2}} (q)_r} \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{GL},i,q}}{q^{\sum_{1 \le i,j \le t} \min\{\alpha_i,\alpha_j\} k_i k_j}} \\
&= \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{\prod_{i=1}^{r} (q^i - 1)}{q^r \cdot \prod_{i=1}^{t} (q)_{k_i}} \cdot \frac{1}{q^{\sum_{1 \le i,j \le t} \min\{\alpha_i,\alpha_j\} k_i k_j}} \\
&= \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{\prod_{i=1}^{r} (q^i - 1)}{q^r} \frac{1}{|\mathrm{Aut}_{\mathcal{O}}(\mathcal{A})|} = \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{(q)_r \cdot q^{\binom{r}{2}}}{|\mathrm{Aut}_{\mathcal{O}}(\mathcal{A})|},
\end{aligned}$$

where we use Lemma 4.22 and Theorem 2.44 for the transformations. □

Remark 4.25. The term in (b) for $\mathcal{O} = \mathbb{Z}$ is exactly the formula (case $u = 0$) conjectured by G. Malle (see [38, Conj. 2.1]) for the probability that a finite p-group occurs as the p-part of the class group $\mathrm{Cl}(K/K_0)$, where K_0 is a number field and contains the pth but not the p^2rd roots of unity.

For the cyclic groups we get the following result.

Corollary 4.26. *Let $\mathcal{A} \cong \mathbb{Z}/p^\alpha\mathbb{Z}$ be a cyclic group. Then we have*

$$P_{\mathrm{Sp}^{(1)},\infty,p,f}(\mathcal{A}) = \frac{(p)_\infty}{(p^2)_\infty} \cdot \frac{p-1}{p^\alpha}.$$

Remark 4.27. To determine $P_{\mathrm{Sp}^{(m)},\infty,q,f}(\mathcal{A})$, for arbitrary m, one can actually use the same idea we took in the last proof. To be more precise one deals with the groups $\mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^\alpha)$, for $\alpha \leq m$, like in the symplectic case and uses the corresponding formulas while for $\alpha > m$ the groups $\mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^\alpha)$ behave like general linear groups and so one treats them in such a way. For $m = 2$ we obtain

$$P_{\mathrm{Sp}^{(2)},\infty,q,f}(\mathcal{A}) = \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{q^{\binom{r}{2}} q^{\binom{s}{2}} (q)_s}{|\mathrm{Aut}_{\mathcal{O}}(\mathcal{A})|} \cdot \prod_{i=1}^{\lceil \frac{r-s}{2} \rceil} (1 - q^{-(2i-1)})$$

where r is the $\mathfrak{p}$-rank and s the $\mathfrak{p}^2$-rank of $\mathcal{A}$. By $\lceil \cdot \rceil$ we denote the ceiling function.

4.4 The orthogonal groups

In this section we shall calculate $P_{\mathrm{O},\infty,q,f}(\mathcal{A})$. In advance we need a few further notations and special results.

Lemma 4.28. *For all $t \geq 2$ and for natural numbers $\alpha_1, \dots, \alpha_t,\ k_1, \dots, k_t$ with $\alpha_1 > \cdots > \alpha_t$ we have*

$$\sum_{i=1}^{t-1} \binom{s_i}{2} (\alpha_i - \alpha_{i+1}) + \binom{s_t}{2} \alpha_t = \sum_{1 \leq i < j \leq t} \alpha_j k_i k_j + \sum_{i=1}^{t} \binom{k_i}{2} \alpha_i$$

where s_i is defined in Notation 4.1.

Proof. We prove the claim using induction on t. For $t = 2$ we have

$$\begin{aligned}\binom{s_2}{2}\alpha_2 + \binom{s_1}{2}(\alpha_1 - \alpha_2) &= \left(\binom{k_1 + k_2}{2} - \binom{k_1}{2}\right)\alpha_2 + \binom{k_1}{2}\alpha_1 \\ &= k_1 k_2 \alpha_2 + \binom{k_2}{2}\alpha_2 + \binom{k_1}{2}\alpha_1.\end{aligned}$$

For the induction step we get

$$\begin{aligned}\sum_{i=1}^{t-1}\binom{s_i}{2}(\alpha_i - \alpha_{i+1}) + \binom{s_t}{2}\alpha_t &= \sum_{i=1}^{t-2}\binom{s_i}{2}(\alpha_i - \alpha_{i+1}) + \binom{s_{t-1}}{2}(\alpha_{t-1} - \alpha_t) + \binom{s_t}{2}\alpha_t \\ &= \sum_{1 \le i < j \le t-1} \alpha_j k_i k_j + \sum_{i=1}^{t-1}\binom{k_i}{2}\alpha_i + \left(\binom{s_{t-1} + k_t}{2} - \binom{s_{t-1}}{2}\right)\alpha_t \\ &= \sum_{1 \le i < j \le t-1} \alpha_j k_i k_j + \sum_{i=1}^{t-1}\binom{k_i}{2}\alpha_i + s_{t-1}k_t\alpha_t + \binom{k_t}{2}\alpha_t\end{aligned}$$

and this leads to the statement. □

Our next goal is to define and determine the analogue of $R_{\mathrm{GL},n,q}(k)$ for the orthogonal case.

Lemma 4.29. *Let $\mathcal{O}$ be a ring and let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. For natural numbers α, n and any $g \in \mathrm{Mat}_n(\mathfrak{p}^\alpha/\mathfrak{p}^{\alpha+1})$ we have $g + \mathbf{1}_n \in \mathrm{O}_n(\mathcal{O}/\mathfrak{p}^{\alpha+1})$ if and only if g is skew-symmetric, i.e. $g = -g^t$.*

Proof. Let be $g \in \mathrm{Mat}_n(\mathfrak{p}^\alpha/\mathfrak{p}^{\alpha+1})$ with $g + \mathbf{1}_n \in \mathrm{O}_n(\mathcal{O}/\mathfrak{p}^{\alpha+1})$. That is

$$(g + \mathbf{1}_n)(g + \mathbf{1}_n)^t = \mathbf{1}_n$$

which is equivalent to $g = -g^t$. □

Lemma 4.30. *Let p be an odd prime and q a power of p. Then the rank of any skew-symmetric matrix over $\mathbb{F}_q$ is even.*

Proof. See [39, Thm. IV.1]. □

Notation 4.31. Let n and k be natural numbers with $k \le n$ and let q be a power of an odd prime. Then we set

$$R_{\mathrm{O},n,q}(k) := \{g \in \mathrm{Mat}_n(\mathbb{F}_q) \mid g = -g^t \text{ and } \dim(\ker(g)) = k\}.$$

Moreover we write $R_{\mathrm{O},i,q} := R_{\mathrm{O},s_i,q}(s_{i-1})$ for $i \in \{1, \ldots, t\}$ and s_i from Notation 4.1.

Proposition 4.32. *With the notation introduced above we have*

(a) $R_{\mathrm{O},2n,q}(2k+1) = 0,$ *for* $0 \le k \le n-1.$

(b) $R_{\mathrm{O},2n+1,q}(2k) = 0,$ *for* $0 \le k \le n.$

(c) $R_{\mathrm{O},n,q}(n) = 1.$

(d) $R_{\mathrm{O},2n,q}(2k) = \prod_{i=1}^{n-k} \frac{q^{2i-2}}{q^{2i}-1} \cdot \prod_{i=0}^{2(n-k)-1} q^{2n-i} - 1,$ *for* $0 \le k \le n-1.$

(e) $R_{\mathrm{O},2n+1,q}(2k+1) = \prod_{i=1}^{n-k} \frac{q^{2i-2}}{q^{2i}-1} \cdot \prod_{i=0}^{2(n-k)-1} q^{2n+1-i} - 1,$ *for* $0 \le k \le n-1.$

Proof. Part (a) and (b) follow directly from Lemma 4.30, (c) is clear. In [9, Thm. 3] Leonard Carlitz computes the number of $n \times n$ skew-symmetric matrices over $\mathbb{F}_q$ having a fixed rank. From this we easily derive the formulae in (d) and (e). □

We need one further preliminary outcome for our central result of this section.

Theorem 4.33. *Let* n *and* r *be natural numbers. Given a ring* $\mathcal{O}$ *and a prime ideal* $\mathfrak{p} \trianglelefteq \mathcal{O}$ *with* $q = |\mathcal{O}/\mathfrak{p}|$ *we obtain for a finite free* $\mathcal{O}/\mathfrak{p}$*-module* $\mathcal{A}$ *of rank* r

$$P_{\mathrm{O},\infty,q,1}(\mathcal{A}) = \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{1}{q^{\binom{r}{2}}(q)_r}.$$

Proof. See [21, Sect. 6.6]. □

Now we are in the situation to prove the main theorem.

Theorem 4.34. *Let* $\mathcal{O}$ *be a ring and let* $\mathfrak{p} \trianglelefteq \mathcal{O}$ *be a prime ideal with* $q = |\mathcal{O}/\mathfrak{p}|$*. Given* $n,\ f,\ t,\ \alpha_1, \ldots, \alpha_t,\ k_1, \ldots, k_t \in \mathbb{N}$ *so that* $f > \alpha_1 > \cdots > \alpha_t$ *and let*

$$\mathcal{A} = (\mathcal{O}/\mathfrak{p}^{\alpha_1})^{k_1} \oplus \cdots \oplus (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t}$$

be a finite $\mathfrak{p}$*-torsion* $\mathcal{O}$*-module of rank* $r := \mathrm{rank}(\mathcal{A}) = \sum_{i=1}^{t} k_i$*. Then we have*

(a) $P_{\mathrm{O},\infty,q,f}(\mathcal{A}) = 0,$ *if there exists* $i \in \{1, \ldots, t\}$ *such that* $k_i \not\equiv 0 \bmod 2,$

(b) $P_{\mathrm{O},\infty,q,f}(\mathcal{A}) = \dfrac{(q)_\infty}{(q^2)_\infty} \cdot \dfrac{1}{q^{\binom{r}{2}}(q)_r} \cdot \dfrac{\prod_{i=1}^{t} R_{\mathrm{O},i,q}}{q^{\sum_{1\le i<j\le t}\alpha_j k_i k_j + \sum_{i=1}^{t}\binom{k_i}{2}\alpha_i}}$, *if* $k_i \equiv 0 \bmod 2$ *for all* $1 \le i \le t$.

Proof. Basically the statement can be shown using the same ideas like in the proof of Theorem 4.8. We transfer the notations from 4.8 to the corresponding objects in the orthogonal case and get

$$P_{\mathrm{O},n,q,\alpha_t}(\mathcal{A}_1) = P_{\mathrm{O},n,q,1}(\mathcal{A}_0) \cdot \frac{q^{\left(\binom{n}{2}-\binom{r}{2}\right)(\alpha_t-1)}}{q^{\binom{n}{2}(\alpha_t-1)}}$$

using $|\mathrm{O}_n(\mathcal{O}/\mathfrak{p}^{\alpha_t})| = q^{\binom{n}{2}(\alpha_t-1)}|\mathrm{O}_n(\mathcal{O}/\mathfrak{p})|$. For the next step, following the arguments in the proofs of 4.8 and 4.20, we have to determine the number of matrices $B \in \mathrm{Mat}_r(\mathfrak{p}^{\alpha_t}/\mathfrak{p}^{\alpha_t+1})$ having $\dim(\ker(B)) = s_{t-1}$ such that $B + \mathbf{1}_r \in \mathrm{O}_r(\mathcal{O}/\mathfrak{p}^{\alpha_t+1})$. By Lemma 4.29 the latter condition on B is equivalent to the situation that B is skew-symmetric. With this the number we are looking for is $R_{\mathrm{O},t,q}$ which by Proposition 4.32 is non-zero if and only if $s_{t-1} \equiv s_t \bmod 2$, which implies that k_t is divisible by 2. So we obtain

$$P_{\mathrm{O},n,q,\alpha_t+1}(\mathcal{A}_2) = P_{\mathrm{O},n,q,1}(\mathcal{A}_0) \cdot \frac{R_{\mathrm{O},t,q}}{q^{\binom{r}{2}\alpha_t}}.$$

Inductively we get the conditions that $R_{\mathrm{O},i,q}$ is non-zero if and only if $s_{i-1} \equiv s_i \bmod 2$. From this we arrive at the requirement that all k_i have to be divisible by 2 since otherwise $P_{\mathrm{O},n,q,f}(\mathcal{A}) = 0$. So for this case we obtain the final result by

$$\begin{aligned} P_{\mathrm{O},\infty,q,f}(\mathcal{A}) = \lim_{n\to\infty} P_{\mathrm{O},n,q,f}(\mathcal{A}) &= \lim_{n\to\infty} P_{\mathrm{O},n,q,1}(\mathcal{A}_0) \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{O},i,q}}{q^{\sum_{1\le i<j\le t}\alpha_j k_i k_j + \sum_{i=1}^{t}\binom{k_i}{2}\alpha_i}} \\ &= \frac{(q)_\infty}{(q^2)_\infty} \cdot \frac{1}{q^{\binom{r}{2}}(q)_r} \cdot \frac{\prod_{i=1}^{t} R_{\mathrm{O},i,q}}{q^{\sum_{1\le i<j\le t}\alpha_j k_i k_j + \sum_{i=1}^{t}\binom{k_i}{2}\alpha_i}} \end{aligned}$$

using Lemma 4.28 and Theorem 4.33. □

4.5 From Modules to Groups

In this section we show the transition how to get from a distribution on the set of $\mathcal{O}$-modules to a statement about finite abelian p-groups. The basic idea of this procedure looks as follows.

Given a group G we determine how many $\mathcal{O}$-modules $\mathcal{A}$ there are such that G and $\mathcal{A}$ are isomorphic as abstract groups, afterwards we sum up the given probabilities over all these possibilities.
The structure of this section is given by the possible ramification behavior of the prime number p in $\mathcal{O}$.

Notation 4.35. For the rest of this section let K be a number field of degree n and let $\mathcal{O}$ be its ring of integers.

Notation 4.36. We denote by "$\cong_{\mathrm{A}}$" the isomorphism between abstract groups.

Example 4.37. Let K be a number field of degree 2 and let p be a prime with $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$. Then we have

$$\mathcal{O}/\mathfrak{p}_1 \cong_{\mathrm{A}} \mathbb{Z}/p\mathbb{Z} \cong_{\mathrm{A}} \mathcal{O}/\mathfrak{p}_2.$$

Before we can state the main results we should introduce the essential notion of this issue.

Definition 4.38. Let K be a number field. Given a prime p let

$$p\mathcal{O} = \prod_{i=1}^{w} \mathfrak{p}_i^{e_{\mathfrak{p}_i/p}}$$

be the prime ideal decomposition of $p\mathcal{O}$ in $\mathcal{O}$. Let further be $P_{\mathfrak{p}_i}$ a probability distribution on the set of finite $\mathfrak{p}_i$-torsion $\mathcal{O}$-modules for all $i \in \{1, \dots, w\}$. Assuming that the $P_{\mathfrak{p}_i}$ are independent we define a probability distribution on the set of finite abelian p-groups by

$$P_p : \mathcal{G}_p \longrightarrow [0,1],\ P_p(G) := \sum_{\substack{\mathcal{A} \cong \mathcal{A}_1 \times \cdots \times \mathcal{A}_w \\ \mathcal{A} \cong_{\mathrm{A}} \mathcal{G}}} \prod_{i=1}^{w} P_{\mathfrak{p}_i}(\mathcal{A}_i)$$

where the sum runs over isomorphism classes of $\mathcal{O}$-modules.

Now we start treating the different cases of the ramification behavior of prime numbers and begin with those which are unramified and do not split, so remain inert.

Lemma 4.39. *Given a prime p with $p\mathcal{O} = \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ we have*

$$(\mathcal{O}/\mathfrak{p}^{\alpha_1})^{k_1} \times \cdots \times (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t} \cong_{\mathrm{A}} (\mathbb{Z}/p^{\alpha_1}\mathbb{Z})^{nk_1} \times \cdots \times (\mathbb{Z}/p^{\alpha_t}\mathbb{Z})^{nk_t}$$

for some natural numbers $t,\ k_1, \dots, k_t,\ \alpha_1, \dots, \alpha_t$ with $\alpha_t < \cdots < \alpha_1$.

Proof. Let p be a prime number such that $\mathfrak{p} := p\mathcal{O}$ is a prime ideal of $\mathcal{O}$. Then by Proposition 2.48 we obtain

$$|\mathcal{O}/\mathfrak{p}| = p^n.$$

So $\mathcal{O}/\mathfrak{p}$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space of dimension n. With this we get the following isomorphism of abelian groups

$$\mathcal{O}/\mathfrak{p}^\alpha \cong_{\mathrm{A}} (\mathbb{Z}/p^\alpha\mathbb{Z})^n,$$

where $\alpha \in \mathbb{N}$. From this the claim follows easily. □

Corollary 4.40. *In the situation of the latter lemma we have*

$$P_p((\mathbb{Z}/p^{\alpha_1}\mathbb{Z})^{nk_1} \times \cdots \times (\mathbb{Z}/p^{\alpha_t}\mathbb{Z})^{nk_t}) = P_{\mathfrak{p}}((\mathcal{O}/\mathfrak{p}^{\alpha_1})^{k_1} \times \cdots \times (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t})$$

where $t,\ k_1, \dots, k_t,\ \alpha_1, \dots, \alpha_t$ are natural numbers with $\alpha_t < \cdots < \alpha_1$. For all other finite abelian p-groups F we get $P_p(F) = 0$.

Proof. This is a direct consequence of Definition 4.38 and Lemma 4.39. □

Corollary 4.41. *Let p be a prime with $p\mathcal{O} \in \operatorname{Spec}(\mathcal{O})$. Then for a finite abelian p-group*

$$G = (\mathbb{Z}/p^{\alpha_1}\mathbb{Z})^{nk_1} \times \cdots \times (\mathbb{Z}/p^{\alpha_t}\mathbb{Z})^{nk_t}$$

of p-rank nr the following is true:

(a) $(P_{\mathrm{GL},\infty,p^n,f})_p(G) = (p^n)_\infty \cdot \dfrac{1}{p^{n \cdot \sum_{1\le i,j\le t} \min\{\alpha_i,\alpha_j\}k_ik_j} \cdot \prod_{i=1}^{t} (p^n)_{k_i}},$

(b) $(P_{\mathrm{Sp}^{(1)},\infty,p^n,f})_p(G) = \dfrac{(p^n)_\infty}{((p^n)^2)_\infty} \cdot \dfrac{(p^n)_r \cdot (p^n)^{\binom{r}{2}}}{p^{n \cdot \sum_{1\le i,j\le t} \min\{\alpha_i,\alpha_j\}k_ik_j} \cdot \prod_{i=1}^{t} (p^n)_{k_i}}.$

Proof. Part (a) follows immediately from Theorem 4.8 and for part (b) we used Theorem 4.24. □

The next case deals with totally ramified primes.

Lemma 4.42. *Given a prime p with $p\mathcal{O} = \mathfrak{p}^n$ for $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O})$ we obtain*

$$P_p((\mathbb{Z}/p^{\alpha_1}\mathbb{Z})^{k_1} \times \cdots \times (\mathbb{Z}/p^{\alpha_t}\mathbb{Z})^{k_t}) = P_{\mathfrak{p}}((\mathcal{O}/\mathfrak{p}^{\alpha_1})^{k_1} \times \cdots \times (\mathcal{O}/\mathfrak{p}^{\alpha_t})^{k_t})$$

for all $t,\ k_1, \ldots, k_t,\ \alpha_1, \ldots, \alpha_t \in \mathbb{N}$ with $\alpha_t < \cdots < \alpha_1$.

Proof. Since $p\mathcal{O} = \mathfrak{p}^n$ we have $\mathcal{O}/\mathfrak{p} \cong_{\mathrm{A}} \mathbb{Z}/p\mathbb{Z}$. The rest follows from Definition 4.38. □

Corollary 4.43. *In the situation of Lemma 4.42 we get*

(a) $(P_{\mathrm{GL},\infty,p,f})_p(G) = (p)_\infty \cdot \dfrac{1}{|\mathrm{Aut}(G)|}$,

(b) $(P_{\mathrm{Sp}^{(1)},\infty,p,f})_p(G) = \dfrac{(p)_\infty}{(p^2)_\infty} \cdot \dfrac{(p)_r \cdot p^{\binom{r}{2}}}{|\mathrm{Aut}(G)|}$

where $G \cong (\mathbb{Z}/p^{\alpha_1}\mathbb{Z})^{k_1} \times \cdots \times (\mathbb{Z}/p^{\alpha_t}\mathbb{Z})^{k_t}$ and r is the p-rank of G.

Proof. Using Lemma 4.42 part (a) follows from Theorem 4.8 and Theorem 4.24 implies part (b). □

The last case we consider here concerns the primes which split completely.

Proposition 4.44. *Given a prime p with $p\mathcal{O} = \prod_{i=1}^n \mathfrak{p}_i$ where $\mathfrak{p}_i$ are pairwise different non-zero prime ideals of $\mathcal{O}$ and a finite abelian p-group $G = (\mathbb{Z}/p^{\alpha_1}\mathbb{Z})^{k_1} \times \cdots \times (\mathbb{Z}/p^{\alpha_t}\mathbb{Z})^{k_t}$ we have*

$$P_p(G) = \sum_{0 \le w_{1,1},\ldots,w_{1,n} \le k_1} \cdots \sum_{0 \le w_{t,1},\ldots,w_{t,n} \le k_t} \prod_{i=1}^{n} P_{\mathfrak{p}_i}((\mathcal{O}/\mathfrak{p}_i^{\alpha_1})^{w_{1,i}} \times \cdots \times (\mathcal{O}/\mathfrak{p}_i^{\alpha_t})^{w_{t,i}})$$

with the additional restrictive condition $\sum_{i=1}^n w_{j,i} = k_j$ on the non-negative natural numbers $w_{j,i}$ for all $j \in \{1, \ldots, t\}$.

Proof. The assumption that p splits completely leads us to the condition $\mathcal{O}/\mathfrak{p}_i \cong_{\mathrm{A}} \mathbb{Z}/p\mathbb{Z}$ for all i. So every $\mathfrak{p}_i$ can be treated equally and we just need to list the possible combinations of factors to get G. Since the $P_{\mathfrak{p}_i}$ were assumed to be independent, straightforwardly this task arrives at the stated result. □

Remark 4.45. At this point we should mention that the computations we did here for the general linear and the 1st symplectic groups can be also done for the symplectic and the orthogonal groups. But because of the reason that the formulas for these groups are not given in a nice and compact way we spare the reader the details.

Remark 4.46. For $n = 2$ all possible cases have been treated here. For $n \geq 3$ the remaining cases of ramification behavior become too hard to handle. So we will not do this here. But in principle the strategy is the same as in the last proposition with the difference that the inertia degrees can vary from prime ideal to prime ideal and so one gets a mass of possibilities for the isomorphisms.

Chapter 5

u-Probabilities

In this chapter we combine the results from the last chapter and a notion from the original paper of Cohen and Lenstra to deduce some statements about the distribution of finite abelian p-groups and link these results to the distribution of p-parts of class groups of number fields. In particular we give a theoretical backup for Malle's conjecture.
For that we consider the 1st symplectic groups over the ring $\mathbb{Z}/p^f\mathbb{Z}$ and extend the distribution $P_{\mathrm{Sp}^{(1)},\infty,p,f}$ of finite abelian p-groups given by Theorem 4.24 by the following notion, which is formulated in a general way.

Definition 5.1. Given a probability distribution P on the set of all finite abelian p-groups we define for a natural number u the *u-probability distribution* with respect to P by the following recursion formula

$$P^{(u)} : \mathcal{G}_p \longrightarrow \mathbb{R},\ P^{(u)}(G) := \sum_{H \in \mathcal{G}_p} \sum_{\substack{y \in H \\ H/\langle y\rangle \cong G}} \frac{P^{(u-1)}(H)}{|H|},$$

where $P^{(0)}(G) := P(G)$ for $G \in \mathcal{G}_p$. We call $P^{(u)}(G)$ the *u-probability* of G (w.r.t. P) if it exists.

As seen in the last chapter (4.24) $P_{\mathrm{Sp}^{(1)},\infty,p,f}$ is independent of f and to simplify this expression we use the following notation.

Notation 5.2. For a finite abelian p-group G we set $P_{1,p}(G) := P_{\mathrm{Sp}^{(1)},\infty,p,f}(G)$.

Using this notation we formulate the following conjecture.

Conjecture 5.3. *For a finite abelian p-group G of p-rank r and a non-negative integer u we have the following explicit formula*

$$P_{1,p}^{(u)}(G) = \frac{(p^2)_u (p)_\infty}{(p)_u (p^2)_\infty} \cdot \frac{(p)_{r+u} p^{\binom{r}{2}}}{(p)_u |G|^u |\mathrm{Aut}(G)|}.$$

The alert reader recognizes that the right hand side of the formula matches Malle's conjecture (see 3.12). So one could think: "what else is new?". But in the following we prove our conjecture for a reasonable set of finite abelian p-groups and so we can think of this as a theoretical evidence for Malle's conjecture at least in some special cases. For this we need some more notations and preliminary results.

Notation 5.4. Given a finite abelian p-group G and an integer $u \geq 0$ we set

$$P_{CL}(G)_u := \frac{(p)_\infty}{(p)_u} \cdot \frac{1}{|G|^u |\mathrm{Aut}(G)|}.$$

Remark 5.5. We would like to point out that $P_{CL}(\cdot)_u$ defines a probability distribution on the set $\mathcal{G}_p$ (see [11, Ex. 5.10]).

Proposition 5.6. *For a finite abelian p-group G we have*

$$P_{CL}^{(u+1)}(G) = P_{CL}(G)_{u+1} = \sum_{H \in \mathcal{G}_p} \sum_{\substack{y \in H \\ H/\langle y \rangle \cong G}} \frac{P_{CL}(H)_u}{|H|}$$

for all integers $u \geq 0$.

Proof. Given finite abelian p-groups G and J we have by [11, Thm. 3.5]

$$\sum_{H \in \mathcal{G}_p} \frac{|\{H_1 \leq H \mid H_1 \cong J,\ H/H_1 \cong G\}|}{|\mathrm{Aut}(H)|} = \frac{1}{|\mathrm{Aut}(J)||\mathrm{Aut}(G)|}.$$

From this we get

$$\sum_{\substack{H \in \mathcal{G}_p, \\ |H| = p^n |G|}} \frac{|\{y \in H \mid \mathrm{ord}(y) = p^n,\ H/\langle y \rangle \cong G\}|}{|\mathrm{Aut}(H)|} = \frac{1}{|\mathrm{Aut}(G)|}.$$

Now we multiply this equation by $(p^n|G|)^{-(u+1)} \cdot (p)_\infty/(p)_u$ and take the sum over all $n \in \mathbb{N}$. So we firstly obtain

$$\sum_{n \geq 0} \sum_{\substack{H \in \mathcal{G}_p \\ |H| = p^n |G|}} \frac{(p)_\infty}{(p)_u} \cdot \frac{|\{y \in H \mid \mathrm{ord}(y) = p^n,\ H/\langle y \rangle \cong G\}|}{|H|^{u+1} |\mathrm{Aut}(H)|} = \sum_{n \geq 0} \frac{(p)_\infty}{(p)_u} \cdot \frac{1}{|G|^{u+1} |\mathrm{Aut}(G)|} \cdot \left(\frac{1}{p^{u+1}}\right)^n$$

and with this

$$\begin{aligned}\sum_{H\in\mathcal{G}_p}\sum_{\substack{y\in H\\ H/\langle y\rangle\cong G}}\frac{P_{CL}(H)_u}{|H|} &= \frac{(p)_\infty}{(p)_u}\cdot\frac{1}{|G|^{u+1}|\mathrm{Aut}(G)|}\sum_{n\geq 0}\left(\frac{1}{p^{u+1}}\right)^n\\ &= \frac{(p)_\infty}{(p)_{u+1}}\cdot\frac{1}{|G|^{u+1}|\mathrm{Aut}(G)|}\\ &= P_{CL}(G)_{u+1}.\end{aligned}$$

□

Notice that for the probability distribution P_{CL} defined in Chapter 3 the recursion formula from the first definition of this chapter is not given by a definition but by a proven fact. In the next lemma we give an equivalent version of our conjecture which is easier to handle.

Lemma 5.7. *Let G be a finite abelian p-group with p-rank r. Then Conjecture 5.3 is true for G if and only if the following condition holds*

$$\sum_{\substack{H\in\mathcal{G}_p\\ \mathrm{rk}_p(H)=r}}\sum_{\substack{y\in H\\ H/\langle y\rangle\cong G}}\frac{P_{CL}^{(u)}(H)}{|H|}=\frac{p^{r+u+1}-1}{p^{r+u+1}}\cdot P_{CL}^{(u+1)}(G).$$

Proof. Let G be a finite abelian p-group with p-rank r. Then by Definition 5.1 Conjecture 5.3 is true for G if and only if the following equation holds

$$\begin{aligned}\frac{(p^2)_{u+1}(p)_\infty}{(p)_{u+1}(p^2)_\infty}\cdot\frac{(p)_{r+u+1}p^{\binom{r}{2}}}{(p)_{u+1}|G|^{u+1}|\mathrm{Aut}(G)|} &= \sum_{\substack{H\in\mathcal{G}_p\\ \mathrm{rk}_p(H)=r}}\sum_{\substack{y\in H\\ H/\langle y\rangle\cong G}}\frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty}\cdot\frac{(p)_{r+u}p^{\binom{r}{2}}}{(p)_u|H|^{u+1}|\mathrm{Aut}(H)|}\\ &+\sum_{\substack{H\in\mathrm{G}_p\\ \mathrm{rk}_p(H)=r+1}}\sum_{\substack{y\in H\\ H/\langle y\rangle\cong G}}\frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty}\cdot\frac{(p)_{r+1+u}p^{\binom{r+1}{2}}}{(p)_u|H|^{u+1}|\mathrm{Aut}(H)|}.\end{aligned}$$

Now we set

$$\begin{aligned}X(r) &:= \sum_{\substack{H\in\mathrm{G}_p\\ \mathrm{rk}_p(H)=r}}\sum_{\substack{y\in H\\ H/\langle y\rangle\cong G}}\frac{1}{(p)_u|H|^{u+1}|\mathrm{Aut}(H)|},\\ Y &:= \frac{1}{(p)_{u+1}|G|^{u+1}|\mathrm{Aut}(G)|}.\end{aligned}$$

With this notation the last equation is equivalent to

$$\frac{(p^2)_{u+1}(p)_{r+u+1}p^{\binom{r}{2}}}{(p)_{u+1}} \cdot Y = \frac{(p^2)_u(p)_{r+u}p^{\binom{r}{2}}}{(p)_u} \cdot X(r) + \frac{(p^2)_u(p)_{r+u+1}p^{\binom{r+1}{2}}}{(p)_u} \cdot X(r+1).$$

Using the identity $Y = X(r) + X(r+1)$, which is true by Proposition 5.6, we rephrase the latter equation and obtain

$$(p)_{r+u+1}p^{\binom{r}{2}} \left(\frac{p^{u+1}+1}{p^{u+1}} - p^r \right) \cdot Y = (p)_{r+u+1}p^{\binom{r}{2}} \left(\frac{p^{r+u+1}}{p^{r+u+1}-1} - p^r \right) \cdot X(r).$$

From this we finally get

$$X(r) = \frac{p^{r+u+1}-1}{p^{r+u+1}} \cdot Y$$

which is equivalent to

$$\sum_{\substack{H \in \mathcal{G}_p \\ \mathrm{rk}_p(H)=r}} \sum_{\substack{y \in H \\ H/\langle y \rangle \cong G}} \frac{P_{CL}^{(u)}(H)}{|H|} = \frac{p^{r+u+1}-1}{p^{r+u+1}} \cdot P_{CL}^{(u+1)}(G).$$

□

The following corollary gives a reformulation of the above lemma and will be used to prove the subsequent theorems.

Corollary 5.8. *Let G be a finite abelian p-group of p-rank r. Then Conjecture 5.3 is true for G if and only if the following condition holds*

$$\sum_{\substack{H \in \mathcal{G}_p \\ \mathrm{rk}_p(H)=r}} \frac{|\{y \in H \mid H/\langle y \rangle \cong G\}|}{|H|^{u+1}|\mathrm{Aut}(H)|} = \frac{p^{r+u+1}-1}{p^{r+u+1}} \cdot \frac{(p)_u}{(p)_{u+1}|G|^{u+1}|\mathrm{Aut}(G)|}.$$

Finally we are in the situation to prove something substantial. The following theorems show that Conjecture 5.3 is true for the stated types of groups.

Theorem 5.9. *Conjecture 5.3 is true for all homocyclic groups, i.e., for all groups of type $(\mathbb{Z}/p^\alpha\mathbb{Z})^r$ with $\alpha,\ r \in \mathbb{N}$.*

Proof. Let $G = (\mathbb{Z}/p^\alpha\mathbb{Z})^r$ and u a non-negative integer. Using Corollary 5.8 we need to show the following equality to verify the claim

$$\sum_{\substack{H\in\mathcal{G}_p \\ \mathrm{rk}_p(H)=r}} \frac{|\{y\in H \mid H/\langle y\rangle \cong G\}|}{|H|^{u+1}|\mathrm{Aut}(H)|} = \frac{p^{r+u+1}-1}{p^{r+u+1}} \cdot \frac{(p)_u}{(p)_{u+1}|G|^{u+1}|\mathrm{Aut}(G)|}.$$

For the right hand side we get

$$\begin{aligned}\frac{p^{r+u+1}-1}{p^{r+u+1}} \cdot \frac{(p)_u}{(p)_{u+1}|G|^{u+1}|\mathrm{Aut}(G)|} &= \frac{(p^{r+u+1}-1)p^{u+1}}{p^{r+u+1}(p^{u+1}-1)} \cdot \frac{1}{p^{r\alpha(u+1)}p^{r^2(\alpha-1)}p^{\binom{r}{2}}\prod_{i=1}^{r}(p^i-1)} \\ &= \frac{p^{r+u+1}-1}{(p^{u+1}-1)p^r p^{r\alpha(u+1)}p^{r^2(\alpha-1)}p^{\binom{r}{2}}\prod_{i=1}^{r}(p^i-1)}.\end{aligned}$$

By Lemma 2.16 and Proposition 2.17 the summation on the left hand side runs over the groups $H = G$ and $H = \mathbb{Z}/p^\beta\mathbb{Z} \times (\mathbb{Z}/p^\alpha\mathbb{Z})^{r-1}$ with $\beta > \alpha$. So we need to compute the term

$$\tau(H) := \frac{|\{y\in H \mid H/\langle y\rangle \cong G\}|}{|H|^{u+1}|\mathrm{Aut}(H)|}$$

for these groups. For $H = G$ we get

$$\tau(H) = \frac{1}{p^{r\alpha(u+1)}p^{r^2(\alpha-1)}p^{\binom{r}{2}}\prod_{i=1}^{r}(p^i-1)}.$$

Now let $H = \mathbb{Z}/p^\beta\mathbb{Z} \times (\mathbb{Z}/p^\alpha\mathbb{Z})^{r-1}$ with $\beta > \alpha$. So H is of type $\lambda = (\beta, \alpha, \ldots, \alpha)$ and G is of type $\mu = (\alpha, \ldots, \alpha)$. With this we have

$$\tau(H) = \frac{g^{\lambda}_{\mu,(\beta-\alpha)}(p) \cdot (p^{\beta-\alpha} - p^{\beta-\alpha-1})}{|H|^{u+1}|\mathrm{Aut}(H)|}.$$

But the numerator of $\tau(H)$ is exactly $|O_{p,I}|$, where $I \subset P_\lambda$ is the uniquely ideal determined by λ and μ. Using the notation of Corollary 2.38 we compute $|O_{p,I}|$. First of all $\nu = (\alpha, \ldots, \alpha)$. Hence $[I] = \beta - \alpha$ and therefore $|O_{p,I}| = p^{\beta-\alpha-1} \cdot (p-1)$. Now we sum over all $\beta > \alpha$ and obtain

$$\begin{aligned}
\sum_{\beta>\alpha} \frac{p^{\beta-\alpha-1}(p-1)}{p^{(\beta+\alpha(r-1))(u+1)}p^{\beta+2\alpha(r-1)+\alpha(r-1)^2}(p)_1(p)_{r-1}} &= \frac{p^{\binom{r}{2}}}{p^{\alpha(r-1)(u+1)+2\alpha r-\alpha+\alpha(r-1)^2}\prod_{i=1}^{r-1}(p^i-1)} \sum_{\beta>\alpha}\left(\frac{1}{p^{u+1}}\right)^{\beta} \\
&= \frac{p^{\binom{r}{2}}p^{u+1}}{p^{\alpha r u+\alpha r+u+1+\alpha r^2}(p^{u+1}-1)\prod_{i=1}^{r-1}(p^i-1)} \\
&= \frac{p^{\binom{r}{2}}}{p^{r\alpha(u+1)}p^{\alpha r^2}(p^{u+1}-1)\prod_{i=1}^{r-1}(p^i-1)}.
\end{aligned}$$

Finally we form the sum over all possible H and get for the left hand side of the starting equation

$$\frac{p^{r+u+1}-1}{(p^{u+1}-1)p^r p^{r\alpha(u+1)}p^{r^2(\alpha-1)}p^{\binom{r}{2}}\prod_{i=1}^{r}(p^i-1)},$$

but this is exactly what we claimed. □

Theorem 5.10. *Conjecture 5.3 is true for all groups of rank at most 2, i.e., for all groups of type $\mathbb{Z}/p^\alpha\mathbb{Z}\times\mathbb{Z}/p^\beta\mathbb{Z}$ with $\alpha,\ \beta\in\mathbb{N}$.*

Proof. Let $G=\mathbb{Z}/p^\alpha\mathbb{Z}\times\mathbb{Z}/p^\beta\mathbb{Z}$ with $\alpha>\beta$ (the case $\alpha=\beta$ is given by the latter theorem) and $0\le u\in\mathbb{Z}$. By Corollary 5.8 we have to show the following equality

$$\sum_{\substack{H\in\mathcal{G}_p\\ \mathrm{rk}_p(H)=2}} \frac{|\{y\in H \mid H/\langle y\rangle\cong G\}|}{|H|^{u+1}|\mathrm{Aut}(H)|} = \frac{p^{2+u+1}-1}{p^{2+u+1}}\cdot\frac{(p)_u}{(p)_{u+1}|G|^{u+1}|\mathrm{Aut}(G)|}.$$

For the right hand side we obtain

$$\frac{(p^{3+u}-1)p^{u+1}}{p^{3+u}(p^{u+1}-1)}\cdot\frac{1}{p^{(\alpha+\beta)(u+1)}p^{\alpha-1}p^{\beta-1}p^{2\beta}(p-1)^2} = \frac{p^{3+u}-1}{p^{\alpha(u+2)}p^{\beta(u+2)}p^{2\beta}(p^{u+1}-1)(p-1)^2}.$$

The sum on the left hand side runs over the following groups

(1) $H=G$,

(2) $H=\mathbb{Z}/p^\alpha\mathbb{Z}\times\mathbb{Z}/p^\alpha\mathbb{Z}$,

(3) $H = \mathbb{Z}/p^{\alpha}\mathbb{Z} \times \mathbb{Z}/p^{\delta}\mathbb{Z}$ with $\alpha > \delta > \beta$,

(4) $H = \mathbb{Z}/p^{\gamma}\mathbb{Z} \times \mathbb{Z}/p^{\beta}\mathbb{Z}$ with $\gamma > \alpha$,

(5) $H = \mathbb{Z}/p^{\gamma}\mathbb{Z} \times \mathbb{Z}/p^{\alpha}\mathbb{Z}$ with $\gamma > \alpha$ and

(6) $H = \mathbb{Z}/p^{\gamma}\mathbb{Z} \times \mathbb{Z}/p^{\delta}\mathbb{Z}$ with $\gamma > \alpha > \delta > \beta$.

Using the notation from the last proof we compute now the term $\tau(H)$ where H runs over the above groups. For $H = G$ we get

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

In the case (2) we have $\lambda = (\alpha, \alpha)$ and $\mu = (\alpha, \beta)$, so $\nu = (\beta, \beta)$ and therefore $[I_\lambda(\tilde{\nu})] = 2(\alpha - \beta)$, where $\tilde{\nu} := (p^\beta, p^\beta)$. Hence $|O_{p,I_\lambda(\tilde{\nu})}| = p^{2(\alpha-\beta-1)}(p^2-1)$ and we obtain for $H = \mathbb{Z}/p^{\alpha}\mathbb{Z} \times \mathbb{Z}/p^{\alpha}\mathbb{Z}$

$$\frac{p^{2(\alpha-\beta-1)}(p^2-1)}{p^{2\alpha(u+1)}p(p^2-1)(p-1)p^{4\alpha-4}} = \frac{p}{p^{2\alpha(u+2)}p^{2\beta}(p-1)}.$$

In the third case $\lambda = (\alpha, \delta)$ and $\mu = (\alpha, \beta)$. So $\nu = (\alpha - \delta + \beta, \beta)$ and $[I_\lambda(\tilde{\nu})] = 2(\delta - \beta)$, because p^β degenerates to $p^{\alpha-\delta+\beta}$ by Lemma 2.19 and so there is only one maximal element in $I_\lambda(\tilde{\nu})$, where $\tilde{\nu} := (p^{\alpha-\delta+\beta}, p^\beta)$. With that we get $|O_{p,I_\lambda(\tilde{\nu})}| = p^{2(\delta-\beta)-1}(p-1)$ and finally

$$\tau(H) = \frac{p^{2(\delta-\beta)-1}(p-1)}{p^{(\alpha+\delta)(u+1)}p^{\alpha-1}p^{\delta-1}p^{2\delta}(p-1)^2}.$$

Now we sum over all δ between β and α and get

$$\begin{aligned}
\sum_{\beta<\delta<\alpha} \frac{p^{2(\delta-\beta)-1}(p-1)}{p^{(\alpha+\delta)(u+1)}p^{\alpha-1}p^{\delta-1}p^{2\delta}(p-1)^2} &= \frac{p}{p^{\alpha(u+2)}p^{2\beta}(p-1)} \sum_{\beta<\delta<\alpha} \left(\frac{1}{p^{u+2}}\right)^\delta \\
&= \frac{p}{p^{\alpha(u+2)}p^{\beta(u+2)}p^{2\beta}p^{u+2}(p-1)} \sum_{\delta=0}^{\alpha-\beta-2} \left(\frac{1}{p^{u+2}}\right)^\delta \\
&= \frac{p(p^{(u+2)(\alpha-\beta-1)}-1)}{p^{\alpha(u+2)}p^{\beta(u+2)}p^{2\beta}p^{(u+2)(\alpha-\beta-1)}(p-1)(p^{u+2}-1)} \\
&= \frac{p^{u+3}(p^{(u+2)(\alpha-\beta-1)}-1)}{p^{2\alpha(u+2)}p^{2\beta}(p^{u+2}-1)(p-1)}.
\end{aligned}$$

Applying the same procedure to the remaining cases we obtain the following results. In case

(4) we have

$$\frac{p}{p^{\alpha(u+2)}p^{\beta(u+2)}p^{2\beta}(p^{u+1}-1)(p-1)}.$$

For case (5) we get

$$\frac{p}{p^{2\alpha(u+2)}p^{2\beta}(p^{u+1}-1)(p-1)}$$

and for the last case we obtain

$$\frac{p^{u+2}(p^{(u+2)(\alpha-\beta-1)}-1)}{p^{2\alpha(u+2)}p^{2\beta}(p^{u+2}-1)(p^{u+1}-1)}.$$

After summation of the calculated terms we retrieve the same result as for the right hand side. □

Theorem 5.11. *Conjecture 5.3 is true for all groups of exponent at most p^2, i.e., for all groups of type $(\mathbb{Z}/p^2\mathbb{Z})^r \times (\mathbb{Z}/p\mathbb{Z})^s$ with $s,\ r \in \mathbb{N}$.*

Proof. Let $G = (\mathbb{Z}/p^2\mathbb{Z})^r \times (\mathbb{Z}/p\mathbb{Z})^s$ and u a non-negative integer. We have to show that

$$\sum_{\substack{H\in\mathcal{G}_p\\ \mathrm{rk}_p(H)=r+s}} \frac{|\{y \in H \mid H/\langle y\rangle \cong G\}|}{|H|^{u+1}|\mathrm{Aut}(H)|} = \frac{p^{r+s+u+1}-1}{p^{r+s+u+1}} \cdot \frac{(p)_u}{(p)_{u+1}|G|^{u+1}|\mathrm{Aut}(G)|}.$$

The right hand side is equal to

$$\frac{(p^{r+s+u+1}-1)p^{u+1}}{p^{r+s+u+1}(p^{u+1}-1)p^{(2r+s)(u+1)}p^{2r^2+2rs+s^2}(p)_r(p)_s} = \frac{p^{r+s+u+1}-1}{p^{r+s}p^{2r(u+1)}p^{s(u+1)}p^{2r^2+2rs+s^2}(p^{u+1}-1)(p)_r(p)_s}.$$

The summation on the left hand side runs over the following groups

(1) $H = G$,

(2) $H = (\mathbb{Z}/p^2\mathbb{Z})^{r+1} \times (\mathbb{Z}/p\mathbb{Z})^{s-1}$,

(3) $H = \mathbb{Z}/p^\alpha\mathbb{Z} \times (\mathbb{Z}/p^2\mathbb{Z})^{r-1} \times (\mathbb{Z}/p\mathbb{Z})^s$ with $\alpha > 2$ and

(4) $H = \mathbb{Z}/p^\alpha\mathbb{Z} \times (\mathbb{Z}/p^2\mathbb{Z})^{r} \times (\mathbb{Z}/p\mathbb{Z})^{s-1}$ with $\alpha > 2$.

With the same procedure as in the last theorem we compute $\tau(H)$, in the cases (3) and (4) we form the sum over $\alpha > 2$ and get the following results.

In the first case we obtain

$$\frac{1}{p^{2r(u+1)}p^{s(u+1)}p^{2r^2}p^{2rs}p^{s^2}(p)_r(p)_s}.$$

In the second case we have

$$\frac{p^s-1}{p^{2r(u+1)}p^{s(u+1)}p^{u+1}p^{2r^2}p^r p^{2rs}p^{s^2}p^s(p)_r(p)_s}.$$

For case (3) we get

$$\frac{p^r-1}{p^{2r(u+1)}p^{s(u+1)}p^{2r^2}p^r p^{2rs}p^{s^2}(p)_r(p)_s(p^{u+1}-1)}$$

and case (4) yields

$$\frac{p^s-1}{p^{2r(u+1)}p^{s(u+1)}p^{u+1}p^{2r^2}p^r p^{2rs}p^{s^2}p^s(p)_r(p)_s(p^{u+1}-1)}.$$

Finally we sum up the calculated terms and get

$$\frac{p^{r+s+u+1}-1}{p^{2r(u+1)}p^{s(u+1)}p^{2r^2}p^r p^{2rs}p^{s^2}p^s(p)_r(p)_s(p^{u+1}-1)},$$

which coincides with the result computed for the right hand side. □

As a direct consequence of Conjecture 5.3 we can derive a statement about the distribution of ranks.

Corollary 5.12. *Given a finite abelian p-group G and natural numbers r and u we have*

$$P_{1,p}^{(u)}(\text{"rk}_p(G)=r\text{"}) = \frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty}\cdot\frac{1}{p^{r(r+2u+1)/2}(p)_r}.$$

Proof. Using the equation

$$\sum_{\substack{G\in\mathcal{G}_p\\ \text{rk}_p(G)=r}}\frac{(p)_\infty}{(p)_u|G|^u|\text{Aut}(G)|}=\frac{(p)_\infty}{p^{r(r+u)}(p)_r(p)_{r+u}}$$

given by [11, Thm. 6.3] we obtain

$$\begin{aligned}\sum_{\substack{G\in\mathcal{G}_p\\ \mathrm{rl}_p(G)=r}} P^{(u)}_{1,p}(G) &= \sum_{\substack{G\in\mathcal{G}_p\\ \mathrm{rl}_p(G)=r}} \frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty}\cdot\frac{(p)_{r+u}p^{\binom{r}{2}}}{(p)_u|G|^u|\mathrm{Aut}(G)|}\\ &= \frac{(p^2)_u(p)_{r+u}p^{\binom{r}{2}}}{(p)_u(p^2)_\infty}\cdot\sum_{\substack{G\in\mathcal{G}_p\\ \mathrm{rk}_p(G)=r}}\frac{(p)_\infty}{(p)_u|G|^u|\mathrm{Aut}(G)|}\\ &= \frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty}\cdot\frac{1}{p^{r(r+2u+1)/2}(p)_r}\end{aligned}$$

after some easy transformations. □

Remark 5.13. Here we should point out again the meaning of the above results. We did not prove any statements about the distribution of class groups of number fields but computed some distributions of finite abelian p-groups coming from a distribution in the 1st symplectic groups. It turned out that the obtained results match the predicted distribution by Malle and so we can say that there should be a connection between these two things, not least since this correspondence exists in the function field case.

Now we leave the special case of the 1st symplectic groups where we could prove some results and formulate a conjectural statement for the general setting.

Conjecture 5.14. *Let* $\Sigma = (H, K_0, \sigma)$ *be a situation with* $\mathcal{O}(\Sigma) = \mathbb{Z}$*, such that* $\gcd(p, |H|) = 1$ *and* K_0 *be a number field with* p^m*th but not the* p^{m+1}*st roots of unity. Then a given finite abelian* p*-group* G *of* p*-rank* r *appears as the* p*-part of a relative class group* $\mathrm{Cl}(K/K_0)$ *for* $K \in \mathcal{K}(\Sigma)$ *with probability* $P^{(u)}_{\mathrm{Sp}^{(m)},\infty,p,f}(G)$*, where* $u = u(\Sigma)$*.*

Remark 5.15. There is no known method, so far, to prove this conjecture. But this statement fits with our general idea and concept very well.

Remark 5.16. As last point we need to outline that our method seems not to work in the case $\mathcal{O}(\Sigma) \neq \mathbb{Z}$.
For instance consider the situation $\Sigma = (\mathbb{Z}/3\mathbb{Z}, \mathbb{Q}(\sqrt{-1}), complex)$. So the base field containing the 4th roots of unity. The unit rank equals $u = 1$ and $\mathcal{O}(\Sigma) = \mathbb{Z}[\mu_3]$, where μ_3 is a primitive third root of unity. Extending the concept of u-probabilities to $\mathcal{O}$-modules, where $\mathcal{O}$ is finite over $\mathbb{Z}$ and applying the translation from modules to groups introduced in Section 4.5 we obtain

0.92 for the probability that the 2-part of the class group is trivial and 0.072 for the probability that the 2-part of the class group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In contrast to it we have the data presented by Malle [38] which predict 0.853 for the probability that the 2-part of the class group is trivial and 0.125 that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ occur as the 2-part of the class group.

Bibliography

[1] Michael Adam: *On the distribution of eigenspaces in classical groups over finite rings.* Linear Algebra Appl. 443 (2014), 50–65.

[2] George E. Andrews: *The theory of partitions.* Reading, Mass.: Addison-Wesley, 1976.

[3] Emil Artin: *Geometric Algebra.* New York: Interscience, 1957.

[4] Jeffrey D. Achter: *The distribution of class groups of function fields.* J. Pure and Appl. Algebra 204 (2006), no 2, 316–333.

[5] ———: *Results of Cohen-Lenstra type for quadratic function fields.* Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 1–7.

[6] Manjul Bhargava et al.: *Modeling the distribution of ranks, Selmer groups and Shafarevich-Tate groups of elliptic curves.* arXiv:1304.3971 [math.NT], 2013.

[7] Maximilian Boy: *On the second class group of real quadratic number fields.* Dissertation. TU Kaiserslautern, 2012.

[8] John R. Britnell: *Cyclic, separable and semisimple matrices in the special linear groups over a finite field.* J. London Math. Soc. (2) 66 (2002), 605–622.

[9] Leonard Carlitz: *Representations by skew forms in a finite field.* Archiv der Math. 5 (1954), 19–31.

[10] Henri Cohen: *Advanced topics in computational number theory.* New York: Springer, 2000.

[11] Henri Cohen, Hendrik W. Lenstra Jr.: *Heuristics on class groups of number fields.* In Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983). Berlin: Springer 1984, 1068 of Lecture Notes in Math., 33–62.

[12] Henri Cohen, Jacques Martinet: *Étude heuristique des groupes de classes des corps de nombres.* J. reine angew. Math. 404 (1990), 39–76.

[13] ―――――: *Heuristics on class groups: some good primes are not too good.* Math. Comp. 63 (1994), no. 207, 329–334.

[14] Harold Davenport, Hans Heilbronn: *On the density of discriminants of cubic fields. II.* Proc. Roy. Soc. Lond. A. 322 (1971), 405–420.

[15] Christophe Delaunay: *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$. Experiment. Math. 10, Issue 2 (2001), 191–196.

[16] ―――――: *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics.* Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 341 (2007), 323–340.

[17] Kunal Dutta, Amritanshu Prasad: *Degenerations and orbits in finite abelian groups.* J. Comb. Theory, Ser. A 118(6): 1685–1694 (2011).

[18] Jordan S. Ellenberg, Akshay Venkatesh, Craig Westerland: *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields.* preprint: arXiv:0912.0325 (2009).

[19] Étienne Fouvry, Jürgen Klüners: *On the 4-rank of class groups of quadratic number fields.* Invent. Math. 167 (2007), 455–513.

[20] Eduardo Friedman, Lawrence C. Washington: *On the distribution of divisor class groups of curves over a finite field.* Théorie des nombres (Quebec, PQ, 1987), Berlin: de Gruyter, 1989, pp. 227–239.

[21] Jason Fulman: *Probability in the Classical Groups over Finite Fields: Symmetric Functions, Probabilistic Algorithms, and Cycle Indices.* Ph.D. thesis, Harvard University, 1997.

[22] ―――――: *A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups.* J. Algebra 212, No. 2, 1999, 557–590.

[23] ―――――: *A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups.* J. Algebra 234, 2000, 207–224.

[24] ―――――: *Random matrix theory over finite fields.* Bull. Amer. Math. Soc. (N.S.) 39 (2002), no. 1, 51–85.

[25] Jason Fulman, Peter M. Neumann, Cheryl E. Praeger: *A generating function approach to the enumeration of matrices in classical groups over finite fields.* Mem. Amer. Math. Soc. 176 (2005), Providence, RI: American Mathematical Society, 2005.

[26] Derek Garton: *Random matrices and Cohen-Lenstra statistics for global fields with roots of unity.* Ph.D. thesis, UW Madison, 2012.

[27] Gerard van der Geer, René Schoof: *Effectivity of Arakelov divisors and the analogue of the theta divisor of a number field.* Selecta Math. New Ser. 6 (2000), 377–398.

[28] Frank Gerth: *The 4-class ranks of quadratic fields.* Invent. Math. 77 (1984), 489–515.

[29] Jay Goldman, Gian-Carlo Rota: *On the foundations of combinatorial theory IV, finite vector spaces and eulerian generating functions.* Studies in Applied Math. 49 (1970), p. 239–258.

[30] Juncheol Han: *The general linear group over a ring.* Bull. Korean Math. Soc. 43 (2006), No.3, p. 619–626.

[31] Gerald J. Janusz: *Algebraic number fields.* Second edition. Graduate Studies in Mathematics, 7. Providence, RI: American Mathematical Society, 1996.

[32] Franz Lemmermeyer: *Galois action on class groups.* J. Algebra 264 (2003), 553–564.

[33] Johannes Lengler: *The Cohen Lenstra heuristic for finite abelian groups.* Dissertation, Universität des Saarlandes, 2009.

[34] ――――――: *The Cohen-Lenstra heuristic: methodology and results.* J. Algebra 323 (2010), 2960–2976.

[35] Florian Luca, Allison M. Pacelli: *Class groups of quadratic fields of 3-rank at least 2: Effective bounds.* J. Number Theory 128 (2008), 796–804.

[36] Ian G. Macdonald: *Symmetric functions and Hall polynomials.* New York: Oxford Science Publications, second edition, 1995.

[37] Gunter Malle: *Cohen-Lenstra heuristic and roots of unity.* J. Number Theory 128 (2008), 2823–2835.

[38] ――――――: *On the distribution of class groups of number fields.* Experiment. Math. 19 (2010), 465–474.

[39] Morris Newman: *Integral matrices.* New York: Academic Press, 1972.

[40] Jessie Mac Williams: *Orthogonal matrices over finite fields.* Amer. Math. Monthly 76 (1969), no. 2, p. 152–164.

[41] Kent Morrison: *Integer sequences and matrices over finite fields.* J. Integer Seq. 9 (2006) Article 06.2.1.

[42] Wladyslaw Narkiewicz: *Elementary and analytic theory of algebraic numbers.* 2nd ed. Berlin: Springer, 1990.

[43] Jürgen Neukirch: *Algebraische Zahlentheorie.* Berlin, Heidelberg: Springer, 1992.

[44] Amritanshu Prasad, David Speyer: Discussion on the following website: http://mathoverflow.net/questions/95233/hall-polynomial-when-the-subgroup-is-cyclic.

[45] Joseph J. Rotman: *Advanced modern Algebra.* Upper Saddle River, NJ: Prentice Hall, 2nd printing, 2003.

[46] Christian Wittmann: *Densities for 4-class ranks of quadratic function fields.* J. Number Theory 129 (2009), 2635–2645.

Wissenschaftlicher Werdegang

1986	geboren in Kemerowo, Russland
2006	Abitur
seit 2006	Studium der Mathematik an der TU Kaiserslautern
2010	Diplom in Mathematik, TU Kaiserslautern
seit 2011	Promotion bei Prof. Dr. Gunter Malle, TU Kaiserslautern

Curriculum Vitae

1986	born in Kemerowo, Russia
2006	Abitur
since 2006	Study of mathematics at TU Kaiserslautern, Germany
2010	Diploma in mathematics, TU Kaiserslautern
since 2011	Doctoral thesis with Prof. Dr. Gunter Malle, TU Kaiserslautern