Cohen-Lenstra sums over local rings

par CHRISTIAN WITTMANN

RéSUMÉ. On étudie des séries de la forme $\sum_{M} |\text{Aut}_R(M)|^{-1}|M|^{-u}$, où $R$ est un anneau commutatif local et $u$ est un entier non-négatif, la sommation s'étendant sur tous les $R$-modules finis, à isomorphisme prés. Ce problème est motivé par les heuristiques de Cohen et Lenstra sur les groupes des classes des corps de nombres, où de telles sommes apparaissent. Si $R$ a des propriétés additionelles, on reliera les sommes ci-dessus à une limite de fonctions zêta des modules libres $R^n$, ces fonctions zêta comptant les sous-$R$-modules d’indice fini dans $R^n$. En particulier on montrera que cela est le cas pour l’anneau de groupe $\mathbb{Z}_p[\mathbb{C}_{p^k}]$ d’un groupe cyclique d’ordre $p^k$ sur les entiers $p$-adiques. En outre on considère des sommes raffinées, où $M$ parcourt tous les modules satisfaisant des conditions cohomologiques additionnelles.

ABSTRACT. We study series of the form $\sum_{M} |\text{Aut}_R(M)|^{-1}|M|^{-u}$, where $R$ is a commutative local ring, $u$ is a non-negative integer, and the summation extends over all finite $R$-modules $M$, up to isomorphism. This problem is motivated by Cohen-Lenstra heuristics on class groups of number fields, where sums of this kind occur. If $R$ has additional properties, we will relate the above sum to a limit of zeta functions of the free modules $R^n$, where these zeta functions count $R$-submodules of finite index in $R^n$. In particular we will show that this is the case for the ring $\mathbb{Z}_p[\mathbb{C}_{p^k}]$ of a cyclic group of order $p^k$ over the $p$-adic integers. Thereby we are able to prove a conjecture from [5], stating that the above sum corresponding to $R = \mathbb{Z}_p[\mathbb{C}_{p^k}]$ and $u = 0$ converges. Moreover we consider refined sums, where $M$ runs through all modules satisfying additional cohomological conditions.
1. Introduction

A starting point for the problem investigated in this article is the following remarkable identity, published by Hall in 1938 [6]. If $p$ is a prime number, then

$$\sum_{G} |\text{Aut}(G)|^{-1} = \sum_{G} |G|^{-1},$$

where $G$ runs through all finite abelian $p$-groups, up to isomorphism. Here we will consider a more general problem. Put

$$S(R; u) = \sum_{M} |\text{Aut}_{R}(M)|^{-1} |M|^{-u},$$

where $R$ is a commutative ring, $u$ is a non-negative integer, and the sum extends over all finite $R$-modules, up to isomorphism. By $\text{Aut}_{R}(M)$ we denote the group of $R$-automorphisms of $M$. Sums of this kind occur in Cohen-Lenstra heuristics on class groups of number fields (cf. [2], [3]), so we call $S(R; u)$ a Cohen-Lenstra sum.

We want to evaluate these series in certain cases. While in [2], [3] $R$ is a maximal order of a finite dimensional semi-simple algebra over $\mathbb{Q}$, we will assume that $R$ is a local ring. We will mainly focus on the case $R = \mathbb{Z}_p[C_{p^k}]$, the group ring of a cyclic group of $p$-power order over the $p$-adic integers, which is a non-maximal order in the $\mathbb{Q}_p$-algebra $\mathbb{Q}_p[C_{p^k}]$.

In particular we are able to prove a conjecture of Greither stated in [5]:

$$S(\mathbb{Z}_p[C_{p^k}]; 0) = \sum_{M} |\text{Aut}_{\mathbb{Z}_p[C_{p^k}]}(M)|^{-1} = \left( \prod_{j=1}^{\infty} \frac{1}{1 - p^{-j}} \right)^{k+1}.$$ 

This fills a gap concerning the sums $S(\mathbb{Z}_p[\Delta]; 0)$ for an arbitrary $p$-group $\Delta$, for Greither showed in [5] that $S(\mathbb{Z}_p[\Delta]; 0)$ diverges if $\Delta$ is non-cyclic.

The outline of the paper is as follows. In section 2 we introduce the basic notions concerning Cohen-Lenstra sums over arbitrary local rings, and we will relate these sums to limits of zeta functions. If $V$ is an $R$-module, the zeta function of $V$ is defined as the series

$$\zeta_V(s) = \sum_{U \subseteq V} [V : U]^{-s} \in \mathbb{R} \cup \{\infty\},$$

where $s \in \mathbb{R}$ and $\zeta_V(s) = \infty$ iff the series diverges. The summation extends over all $R$-submodules $U$ of $V$ such that the index $[V : U]$ is finite. The main theorem of that section is 2.6, which states that under certain conditions the Cohen-Lenstra sum $S(R; u)$ can be computed if one has enough information on the zeta functions of $R^n$, viz

$$S(R; u) = \lim_{n \to \infty} \zeta_{R^n}(n + u).$$ (1)
In section 3 we derive some results on the zeta function of $V$ at $s = n$, where $V$ is a $\mathbb{Z}_p[C_p]$-module such that $p\mathbb{Z}_p[C_p]^n \subseteq V \subseteq \mathbb{Z}_p[C_p]^n$. The main ingredient will be a "recursion formula" from [14] for these zeta functions. These results will be applied in section 4 in order to prove Greither's conjecture.

In section 5 we discuss refinements of Cohen-Lenstra sums with respect to the ring $\mathbb{Z}_p[C_p]$, where the summation extends only over those modules $M$ having prescribed Tate cohomology groups $\hat{H}^i(C_p, M)$. This has some applications, e.g. in [5], where the case of cohomologically trivial modules is treated, and in [15], where sums of this kind occur as well, when studying the distribution of $p$-class groups of cyclic number fields of degree $p$.

We will use the following notations in the sequel. $\mathbb{N}$ is the set of non-negative integers, $\mathbb{R}_+$ the set of non-negative real numbers, $p$ denotes a prime number, $q = p^{-1}$, and $\mathbb{Z}_p$ is the ring of $p$-adic integers. We remark that the completion $\mathbb{Z}_p$ could be replaced by $\mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at $p$, throughout. If $m \in \mathbb{N} \cup \{\infty\}$, then

$$ (q)_m := \prod_{j=1}^{m} (1 - q^j); $$

note that the product converges for $m = \infty$ because of $0 < q < 1$. If $l, m \in \mathbb{N}$, we let $\binom{m}{l}_p$ denote the number of $l$-dimensional subspaces of an $m$-dimensional vector space over the finite field $\mathbb{F}_p$. It is well-known that

$$ \binom{m}{l}_p = \frac{(p^m - 1)(p^m - p)\ldots(p^m - p^{l-1})}{(p^l - 1)(p^l - p)\ldots(p^l - p^{l-1})} = p^{l(m-l)} \frac{(q)_m}{(q)_l(q)_{m-l}}. $$

This paper is part of my doctoral thesis. I am indebted to my advisor Prof. Cornelius Greither for many fruitful discussions and various helpful suggestions.

2. Cohen-Lenstra sums and zeta functions

Let $R$ be a commutative ring.

**Definition 2.1.** Let $u \in \mathbb{N}$. The Cohen-Lenstra sum of $R$ with respect to $u$ is defined as

$$ S(R; u) := \sum_{\text{ finite } R\text{-modules } M} |\text{Aut}_R(M)|^{-1} |M|^{-u} \in \mathbb{R}_+ \cup \{\infty\}, $$

where the sum extends over all finite $R$-modules, up to isomorphism. In the sequel, all sums over finite $R$-modules are understood to extend over modules up to isomorphism, without further mention. We denote by $v(M)$
the minimal number of generators of the finite $R$-module $M$, and we put

$$S_n(R; u) := \sum_{\nu(M) = n} |\text{Aut}_R(M)|^{-1}|M|^{-u},$$

$$S_{\leq n}(R; u) := \sum_{\nu(M) \leq n} |\text{Aut}_R(M)|^{-1}|M|^{-u}.$$ 

The following notations will be useful.

**Notations.** If $A, B$ are $R$-modules, we let

$$\text{Hom}_{R}^{\text{sur}}(A, B) := \{\psi \in \text{Hom}_R(A, B) \mid \psi \text{ surjective}\}.$$ 

If $M$ is a finite $R$-module with $\nu(M) \leq n$, there is a positive integer $n$ such that $M$ is of the form $M \cong R^n/U$ for some $R$-submodule $U$ of finite index in $R^n$. We set

$$\lambda_n^R(M) := |\{U \subseteq R^n \mid R^n/U \cong M\}|$$

and

$$s_n^R(M) := |\text{Hom}_{R}^{\text{sur}}(R^n, M)|.$$ 

The following lemma, and also Lemma 2.4, are well-known (cf. [2, Prop. 3.1]). However, we give the simple arguments for the reader’s convenience.

**Lemma 2.2.** $\lambda_n^R(M) = s_n^R(M)|\text{Aut}_R(M)|^{-1}$ for any finite $R$-module $M$.

**Proof.** Each $U \subseteq R^n$ satisfying $R^n/U \cong M$ has the form $U = \ker(\psi)$ for some surjective $\psi \in \text{Hom}_R(R^n, M)$. On the other hand, if $\psi_1, \psi_2 \in \text{Hom}_{R}^{\text{sur}}(R^n, M)$, then

$$\ker(\psi_1) = \ker(\psi_2) \iff \psi_1 = \rho \circ \psi_2$$

for some $\rho \in \text{Aut}_R(M)$, and this proves the lemma. 

**Lemma 2.3.** $S_{\leq n}(R; u) = \sum_{U \subseteq R^n} s_n^R(R^n/U)^{-1}[R^n : U]^{-u}$, where the sums extends over all $R$-submodules $U$ of finite index in $R^n$.

**Proof.** Let $M$ be a finite $R$-module with $\nu(M) \leq n$. Then $M = R^n/U$ for some $U \subseteq R^n$, and there are $\lambda_n^R(M) = \lambda_n^R(R^n/U)$ possible $U'$ with $M \cong R^n/U'$. Hence the preceding lemma implies

$$S_{\leq n}(R; u) = \sum_{U \subseteq R^n} |\text{Aut}_R(R^n/U)|^{-1} \lambda_n^R(R^n/U)^{-1}|R^n/U|^{-u}$$

$$= \sum_{U \subseteq R^n} s_n^R(R^n/U)^{-1}[R^n : U]^{-u}.$$

□
Note that the equality in Lemma 2.3 in an equality in \( \mathbb{R}_+ \cup \{\infty\} \) (as are all equalities dealing with Cohen-Lenstra sums in this article).

From now on we assume that \( R \) is a local ring with maximal ideal \( J \) and residue class field \( \mathbb{F}_p \). We set
\[
q = p^{-1}.
\]
The restriction to prime fields is not essential. We could just as well suppose that the residue class field of \( R \) is an arbitrary finite field \( \mathbb{F}_{p^\alpha} \). Then all results of this article are still valid if we accordingly set \( q = p^{-\alpha} \).

For local rings the calculation of \( s_n^R(M) \) is not difficult. Suppose that \( M \) is an \( R \)-module with \( \nu(M) \leq n \). Then
\[
\nu(M) = \dim_{R/J}(M/JM) \in \{0, \ldots, n\}
\]
by Nakayama’s Lemma.

**Lemma 2.4.** \( s_n^R(M) = |M|^n \frac{(q)_n}{(q)_{n-r}} \), where \( r := \nu(M) \).

**Proof.** The following equivalence holds for \( \psi \in \text{Hom}_R(R^n, M) \), by Nakayama’s Lemma:
\[
\psi \text{ surjective} \iff \overline{\psi} : (R/J)^n \to M/JM \text{ surjective},
\]
where \( \overline{\psi} \) is induced by reduction mod \( J \). Thus
\[
s_n^R(M) = |\text{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^n, \mathbb{F}_p^n)\{|\psi \in \text{Hom}_R(R^n, M) | \overline{\psi} = 0\}| \]
\[
= (p^n - 1) \ldots (p^n - p^{r-1}) |JM|^n \]
\[
= p^{rn} \frac{(q)_n}{(q)_{n-r}} \left( \frac{|M|}{|M/JM|} \right)^n \]
\[
= |M|^n \frac{(q)_n}{(q)_{n-r}}.
\]
\( \square \)

**Theorem 2.5.**

a) \( S_n(R; u) = \frac{q^{n(u+n)}}{(q)_n} \zeta_n(n + u) \).

b) \( S(R; u) = \sum_{n=0}^{\infty} \frac{q^{n(u+n)}}{(q)_n} \zeta_n(n + u) \).

**Proof.** It suffices to prove a). If \( M \cong R^n/U \) for some \( U \subseteq R^n \), then
\[
\nu(M) = \dim(M/JM) = \dim(R^n/(U + J^n)).
\]
Therefore \( \nu(M) = n \) if and only if \( U \subseteq J^n \). In an analogous manner as in the proof of Lemma 2.3 we infer
\[
S_n(R; u) = \sum_{U \subseteq J^n} s_n^R(R^n/U)^{-1}[R^n : U]^{-u},
\]
and using the preceding lemma we get

\[ S_n(R; u) = \frac{1}{(q)_n} \sum_{U \subseteq J_n} [R^n : U]^{-(n+u)} = \frac{q^{n(n+u)}}{(q)_n} \zeta_{J^n}(n + u). \]

**Examples.**

a) \( R : \sim_p. \)

Then \( J = 0 \) and

\[ S(\mathbb{F}_p; u) = \sum_{n=0}^{\infty} \frac{q^{n(n+u)}}{(q)_n}. \]

In particular, if \( u = 0 \) or \( u = 1 \) the identities of Rogers-Ramanujan (cf. [7, Th. 362, 363]) imply

\[ S(\mathbb{F}_p; 0) = \prod_{m=0}^{\infty} \frac{1}{(1 - q^{5m+1})(1 - q^{5m+4})}, \]

\[ S(\mathbb{F}_p; 1) = \prod_{m=0}^{\infty} \frac{1}{(1 - q^{5m+2})(1 - q^{5m+3})}. \]

b) Let \( R \) be a discrete valuation ring with residue class field \( \mathbb{F}_p. \)

Then \( J \cong R, \) and it is well-known that

\[ \zeta_{R^n}(s) = \prod_{j=0}^{n-1} (1 - p^{j-s})^{-1} \]

(cf. [1, §1]), whence

\[ S(R; u) = \sum_{n=0}^{\infty} \frac{q^{n(n+u)}(q)_u}{(q)_n(q)_{n+u}} = \frac{(q)_u}{(q)_\infty}. \]

This result is also proved in [2, Cor. 6.7].

By Theorem 2.5 we are able to compute Cohen-Lenstra sums in some cases, provided we know the zeta functions of \( J^n \) for \( n \in \mathbb{N}. \) As we will see in the next section, it may be difficult to calculate \( \zeta_{J^n}(n + u), \) whereas it is much easier to determine the values \( \zeta_{R^n}(n + u). \) In these situations the following theorem is useful.

**Theorem 2.6.** Let \( u \in \mathbb{N}, \) and recall that \( R \) is a local ring. Then:

a) \( S(R; u) \) converges \( \iff \) The sequence \( (\zeta_{R^n}(n + u))_{n \in \mathbb{N}} \) is bounded.

b) If the sequence \( (\zeta_{R^n}(n + u - 1))_{n \in \mathbb{N}} \) is bounded, then

\[ S(R; u) = \lim_{n \to \infty} \zeta_{R^n}(n + u). \]
Proof. a) The assertion follows from

\[
\zeta_{R^n}(n + u) = \sum_{r=0}^{n} \sum_{U \subseteq R^n} [R^n : U]^{-(n+u)}
\]

\[
\leq \sum_{r=0}^{n} \frac{(q)_{n-r}}{(q)_n} \sum_{\nu(R^n/U) = r} [R^n : U]^{-(n+u)}
\]

\[
= S_{\leq n}(R; u)
\]

by 2.3, 2.4

\[
\leq \frac{1}{(q)_n} \sum_{r=0}^{n} \sum_{\nu(R^n/U) = r} [R^n : U]^{-(n+u)}
\]

\[
= \frac{1}{(q)_n} \zeta_{R^n}(n + u),
\]

and the convergence of the sequence \( \left( \frac{1}{(q)_n} \right)_{n \in \mathbb{N}} \).

b) We define the following abbreviation:

\[
\gamma_u(r, n) := \sum_{\nu(R^n/U) = r} [R^n : U]^{-(n+u)}.
\]

We have to prove that the sequence

\[
(S_{\leq n}(R; u) - \zeta_{R^n}(n + u))_{n \in \mathbb{N}} = \left( \sum_{r=0}^{n} \left( \frac{(q)_{n-r}}{(q)_n} - 1 \right) \gamma_u(r, n) \right)_{n \in \mathbb{N}}
\]

tends to zero. It is easy to see that

\[
1 - \frac{(q)_n}{(q)_{n-r}} \leq q^{n-r+1} + q^{n-r+2} + \cdots + q^n \leq \frac{q^{n-r+1}}{1 - q}.
\]

Hence

\[
\sum_{r=0}^{n} \left( \frac{(q)_{n-r}}{(q)_n} - 1 \right) \gamma_u(r, n) = \sum_{r=0}^{n} \frac{(q)_{n-r}}{(q)_n} \left( 1 - \frac{(q)_n}{(q)_{n-r}} \right) \gamma_u(r, n)
\]

\[
\leq \frac{q^{n+1}}{(q)_n(1 - q)} \sum_{r=0}^{n} p^r \gamma_u(r, n).
\]

Now the claim follows if we can prove:

\[
\left( \sum_{r=0}^{n} p^r \gamma_u(r, n) \right)_{n \in \mathbb{N}}
\]

is a bounded sequence.
Since \( \nu(R^n/U) = \dim(R^n/(U + J^n)) \) we get
\[
\sum_{r=0}^{n} p^r \gamma_u(r, n) = \sum_{U \subseteq R^n} [R^n : U + J^n][R^n : U]^{-(n+u)} \leq \zeta_{R^n}(n + u - 1),
\]
and (4) follows from the assumption. \( \square \)

Sometimes it may be desirable to sum only over modules in certain isomorphism classes instead of computing the entire Cohen-Lenstra sum as in Definition 2.1. We will make use of this generalization in section 5. The following corollary is immediate.

Corollary 2.7. Let \( M \) be a set of non-isomorphic finite \( R \)-modules. If the sequence \( \zeta_{R^n}(n + u - 1) \) is bounded, then
\[
\sum_{M \in M} |\text{Aut}_R(M)|^{-1} |M|^{-u} = \lim_{n \to \infty} \sum_{M \in M} \sum_{U \subseteq R^n} [R^n : U]^{-(n+u)}.
\]

3. The zeta function of a submodule of \( \mathbb{Z}_p[C_{p^k}]^n \) at \( s = n \)

For \( k \in \mathbb{N} \) put \( R_k := \mathbb{Z}_p[C_{p^k}] \), where \( C_{p^k} \) is the multiplicative cyclic group of order \( p^k \). Our goal in the next section will be to compute the Cohen-Lenstra sum \( S(R_k; u) \) for \( u \in \mathbb{N} \), along the lines of Theorem 2.6. We therefore have to study the zeta function of \( R_k^n \) at \( s = n \), as well as the zeta function of certain submodules of \( R_k^n \) at \( s = n \), as we will see in section 4.

To this end we will use the main theorem of [14]. Let \( \sigma \) be a generator of \( C_{p^k} \), and set
\[
\phi_k = \sigma^{p^k-1(p-1)} + \sigma^{p^k-1(p-2)} + \cdots + \sigma^{p^k-1} + 1 \in R_k.
\]
We assume \( k > 0 \) and let
\[
f : R_k^n \to R_{k-1}^n
\]
be the canonical surjection, induced by the surjective homomorphism \( \mathbb{Z}_p[C_{p^k}] \to \mathbb{Z}_p[C_{p^{k-1}}] \), mapping \( \sigma \) to a fixed generator of \( C_{p^{k-1}} \).

Theorem 3.1. Let \( V \subseteq R_k^n \) be an \( R_k \)-submodule of finite index in \( R_k^n \).
Then the following formula holds for \( s \in \mathbb{R} \) with \( s > n - 1 \):
\[
\zeta_V(s) = \prod_{j=0}^{n-1} (1 - p^{j-s})^{-1} \sum_{N \subseteq V^\circ} p^{(np^{k-1} - ev_N(N))(n-s)} (N + f(V) : N)^{-s}, \tag{5}
\]
where \( V^\circ \) is given by \( pV^\circ = f(V \cap \phi_k R_k^n) \) and \( ev_N(N) = \dim_{\mathbb{F}_p}(N + pV^\circ/pV^\circ) \).

This is proved in [14, Th. 3.8, 3.9]. Note that \( f \) maps \( \phi_k R_k^n \) onto \( pR_{k-1}^n \), hence \( f(V \cap \phi_k R_k^n) \subseteq pR_{k-1}^n \). The fact that the zeta function of \( V \) is defined for all \( s \in \mathbb{R} \) with \( s > n - 1 \) is a consequence of Solomon's First Conjecture.
proved in [1], and also follows in a more elementary way from the results in [14, Sec. 5].

If we consider formula (5) with \( s = n \), it becomes much nicer:

\[
\zeta_V(n) = \frac{1}{(q)_n} \sum_{N \subseteq V^o} [N + f(V) : N]^{-n},
\]

where again \( V \subseteq R^n_k \) is a submodule of finite index.

**Theorem 3.2.** The zeta function of \( R^n_k \) at \( s = n \) equals \( \zeta_{R^n_k}(n) = \frac{1}{(q)^{k+1}} \).

**Proof.** We proceed by induction on \( k \). If \( k = 0 \) the result follows from the well-known formula

\[
\zeta_{Z_p}(s) = \prod_{j=0}^{n-1} (1 - p^{-s})^{-1},
\]

cf. [14, Th. 3.9]. If \( k > 0 \) then obviously \( (R^n_k)^o = R^n_{k-1} \), and (6) yields

\[
\zeta_{R^n_k}(n) = \frac{1}{(q)_n} \sum_{N \subseteq R^n_{k-1}} [R^n_{k-1} : N]^{-n} = \frac{1}{(q)_n} \zeta_{R^n_{k-1}}(n),
\]

whence the claim follows. \( \square \)

Using the concept of a Möbius function, we can find a more appropriate expression for (6). Thus let again \( V \subseteq R^n_k \) be a submodule of finite index, and let \( \mu \) be the Möbius function (cf. [11]) of the lattice of submodules of \( V^o \) having finite index in \( V^o \).

**Lemma 3.3.**

\[
\zeta_V(n) = \frac{1}{(q)_n} \sum_{f(V) \subseteq W \subseteq V^o} \left( \sum_{\overline{Y} \subseteq W \subseteq V^o} \mu(\overline{Y}, \overline{W})[\overline{W} : \overline{Y}]^{-n} \right) \zeta_{\overline{W}}(n),
\]

where \( f(V) \) and \( V^o \) are defined as in Theorem 3.1.

**Proof.** We have

\[
\zeta_V(n) = \frac{1}{(q)_n} \sum_{f(V) \subseteq W \subseteq V^o} \eta(W),
\]

where for \( f(V) \subseteq \overline{Y} \subseteq V^o \) we set

\[
\eta(\overline{Y}) := \sum_{N \subseteq \overline{Y}} [\overline{Y} : N]^{-n}.
\]

One easily verifies that

\[
\sum_{f(V) \subseteq \overline{Y} \subseteq \overline{W}} [\overline{W} : \overline{Y}]^{-n} \eta(\overline{Y}) = \zeta_{\overline{W}}(n)
\]
(this is analogous to the proof of Theorem 4.5 in [14]). Applying the Möbius inversion formula [11, Sec. 3, Prop. 2] yields

$$\zeta_V(n) = \frac{1}{(q)_n} \sum_{f(V) \subseteq W \subseteq V^o} \sum_{f(V) \subseteq Y \subseteq W} \mu(Y, W)[W : Y]^{-n} \zeta_Y(n),$$

and the formula stated above follows. □

For the rest of this section, we let $R = R_k$ and $\overline{R} = R_{k-1}$. Let $J, \overline{J}$ the maximal ideals of $R, \overline{R}$ respectively. We will use the above lemma to derive a formula for $\zeta_V(n)$, where $V$ is an $R$-module such that $J^n \subseteq V \subseteq R^n$.

**Lemma 3.4.** Let $J^n \subseteq V \subseteq R^n$ be a submodule. Then $\overline{J}^n \subseteq f(V) \subseteq \overline{R}^n$, and

$$\zeta_V(n) = \sum_{f(V) \subseteq Y \subseteq \overline{R}^n} \frac{1}{(q)_j(Y)} \zeta_Y(n), \quad (8)$$

where $j(Y) := \dim_{F_p}(\overline{Y}/J^n)$.

**Proof.** Clearly $f(J^n) = \overline{J}^n$, so $\overline{J}^n \subseteq f(V) \subseteq \overline{R}^n$. Since $\phi_k \in J$ we have

$$pV^o = f(V \cap \phi_k R^n) \supseteq f(J^n \cap \phi_k R^n) = f(\phi_k R^n) = pR^n,$$

thus $V^o = \overline{R}^n$. The preceding lemma implies

$$\zeta_V(n) = \frac{1}{(q)_n} \sum_{f(V) \subseteq Y \subseteq \overline{R}^n} \left( \sum_{Y \subseteq W \subseteq \overline{R}^n} \mu(Y, W)[W : Y]^{-n} \right) \zeta_Y(n). \quad (9)$$

Fix a submodule $\overline{Y}$ such that $\overline{J}^n \subseteq \overline{Y} \subseteq \overline{R}^n$, and put $j := j(\overline{Y})$. Then the lattice of $\overline{R}$-submodules of $\overline{R}^n$ containing $\overline{Y}$ is isomorphic to the lattice of $F_p$-subspaces of $F_p^{n-j}$. Consequently

$$\sum_{\overline{Y} \subseteq W \subseteq \overline{R}^n} \mu(\overline{Y}, W)[W : \overline{Y}]^{-n} = \sum_{U \subseteq F_p^{n-j}} \tilde{\mu}(0, U)|U|^{-n},$$

where $\tilde{\mu}$ is the Möbius function of the lattice of subspaces of $F_p^{n-j}$. Since

$$\tilde{\mu}(0, U) = (-1)^{\dim(U)}p^{\binom{\dim(U)}{2}}$$

([11, Sec. 5, Ex. 2]) and since there are $\left[ \begin{array}{c} n-j \\ l \end{array} \right]_p$ $F_p$-subspaces of $F_p^{n-j}$ of dimension $l$, the above sum can be written as

$$\sum_{l=0}^{n-j} \left[ \begin{array}{c} n-j \\ l \end{array} \right]_p (-1)^{\binom{l}{2}}p^{-ln} = \prod_{i=0}^{n-j-1} (1 - p^{i-n}) = \frac{(q)_n}{(q)_j},$$

where the equality of the sum and the product follows from [8, III.8.5]. Putting together this result with (9) proves the lemma. □
Using an inductive argument, the lemma shows in particular that the value \( \zeta_V(n) \) only depends on the \( \mathbb{F}_p \)-dimension of \( V/J^n \), i.e.

\[
\zeta_V(n) = \zeta_{V'}(n) \quad \text{if} \quad \dim_{\mathbb{F}_p}(V/J^n) = \dim_{\mathbb{F}_p}(V'/J^n).
\]

**Notation.** Let \( 0 \leq m \leq n \). We define

\[
c_k^n(m) := \zeta_V(n) \quad \text{for any } J^n \subseteq V \subseteq R^n \text{ with } \dim_{\mathbb{F}_p}(V/J^n) = m.
\]  

If \( k = 0 \) we have \( V \cong \mathbb{Z}_p^n \), hence by (7)

\[
c_0^n(m) = \frac{1}{(q)_n} \quad \forall \ 0 \leq m \leq n.
\]  

If \( k > 0 \) the equality \([V : J^n] = [f(V) : J^n]\), together with the preceding lemma, implies

\[
c_k^n(m) = \sum_{j=m}^{n} \left[ \frac{n-m}{j-m} \right]_p \frac{c_{k-1}^n(j)}{(q)_j},
\]  

and this recursion formula allows the explicit computation of \( \zeta_V(n) \). For example, if \( k = 1 \), i.e. \( R = \mathbb{Z}_p[C_p] \) and \( J = \text{rad}(R) \), we get

\[
\zeta_{J^n}(n) = c_1^n(0) = \frac{1}{(q)_n} \sum_{j=0}^{n} \left[ \frac{n}{j} \right]_p \frac{1}{(q)_j}.
\]

**4. Cohen-Lenstra sums over \( \mathbb{Z}_p[C_p^k] \)**

In this section we want to evaluate the Cohen-Lenstra sums \( S(\mathbb{Z}_p[C_p^k]; u) \), where \( u \in \mathbb{N} \) and \( C_p^k \) is the multiplicative cyclic group of order \( p^k \). We put

\[
R = \mathbb{Z}_p[C_p^k].
\]

By Theorem 3.2 the sequence \( (\zeta_{R^n}(n))_{n \in \mathbb{N}} \) is convergent, and thus

\[
S(R; u) = \lim_{n \to \infty} \zeta_{R^n}(n + u) \in \mathbb{R}_+ \quad \forall \ u \geq 1
\]

according to Theorem 2.6. Note that the explicit formulas in [14] for \( \zeta_{R^n}(s) \) in the cases \( k = 1, 2 \) are useful for approximating the value of \( S(R; u) \).

It remains to determine

\[
S(R; 0) = \sum_{M} |\text{Aut}_R(M)|^{-1}.
\]

Since the zeta function \( \zeta_{R^n}(s) \) is not defined for \( s = n - 1 \), Theorem 2.6 is not applicable. So first of all it is interesting to investigate whether \( S(R; 0) \) converges to real number. This question was asked by Greither in [5], and he conjectured that \( S(R; 0) \) converges to \( (q)_{\infty}^{-1}(k+1) \). We will prove this conjecture in Corollary 4.3 below.
Theorem 4.1. Let $R = \mathbb{Z}_p[C_{p^n}]$. Then

$$S(R; 0) = \lim_{n \to \infty} \zeta_{R^n}(n).$$

Proof. Let $\gamma_0(r, n)$ be defined as in (3). Following the steps in the proof of Theorem 2.6, it remains to show the assertion (4):

$$\left( \sum_{r=0}^{n} p^r \gamma_0(r, n) \right)_{n \in \mathbb{N}}$$

is a bounded sequence.

One has

$$\gamma_0(r, n) = \sum_{\substack{U \subseteq R^n \\dim(R^n/(U+J^n)) = r}} [R^n : U]^{-n} \leq q^{rn} \sum_{\substack{J^n \subseteq V \subseteq R^n \\dim(R^n/V) = r}} \zeta_V(n).$$

In the preceding section we saw that $\zeta_V(n)$ only depends on $\dim(V/J^n) = n - r$, so using the notation introduced in (10) we get

$$\gamma_0(r, n) \leq q^{rn} \left[ \begin{array}{c} n \\ r \end{array} \right] c_k^{n}(n - r) \leq \frac{q^{r^2}}{(q)_r} c_k^{n}(n - r).$$

The next lemma shows that there exists a constant $A > 0$, independent of $r$ and $n$, such that

$$\sum_{r=0}^{n} p^r \gamma_0(r, n) \leq \sum_{r=0}^{n} p^r \frac{q^{r^2}}{(q)_r} \cdot A \cdot p^{r(r+2)/2} \leq \frac{A}{(q)_\infty} \sum_{r=0}^{\infty} q^{r^2-4r}/2,$$

whence the theorem is proved. \(\square\)

Lemma 4.2. For all $k \in \mathbb{N}$ there exists a constant $A > 0$, independent of $n$ and $0 \leq r \leq n$, such that the values $c_k^{n}(n - r)$ defined in (10) satisfy the inequality

$$c_k^{n}(n - r) \leq A \cdot p^{r(r+2)/2}.$$

Proof. We proceed by induction on $k$. If $k = 0$ we can simply set $A := (q)_\infty^{-1}$ by (11). Let $k > 0$, and let $A' > 0$ be a constant satisfying

$$c_{k-1}^{n}(n - l) \leq A' \cdot p^{(l+2)/2}$$
for all \( n \) and all \( 0 \leq l \leq n \). For \( n \in \mathbb{N} \) and \( 0 \leq r \leq n \), the recursion formula (12) implies

\[
c^n_k(n - r) = \sum_{j=n-r}^{n} \binom{r}{j} \frac{c^n_{k-1}(j)}{(q)_j}
\]

\[
\leq \frac{A'}{(q)_n} \sum_{i=0}^{r} \frac{r}{i} p^{-i(i+2)/2}
\]

\[
\leq \frac{A'}{(q)_n(q)_r} \sum_{i=0}^{r} p^{-i(i+2)/2}
\]

\[
= \frac{A'}{(q)_n(q)_r} \sum_{i=0}^{\infty} q^{-i(i+2)/2}.
\]

Therefore we can put

\[
A := \frac{A'}{(q)_n(q)_r} \sum_{i=0}^{\infty} q^{-i(i+2)/2}.
\]

\[\Box\]

We remark that Corollary 2.7 holds for \( R = \mathbb{Z}_p[C_p^k] \) and \( u = 0 \) as well:

If \( \mathcal{M} \) is a set of non-isomorphic finite \( R \)-modules, then

\[
\sum_{M \in \mathcal{M}} |\text{Aut}_R(M)|^{-1} = \lim_{n \to \infty} \sum_{M \in \mathcal{M}} \sum_{R^n \subseteq U \supseteq M} [R^n : U]^{-n}.
\]

Now Greither's conjecture (cf. [5]) is a direct consequence of Theorem 4.1 and 3.2.

**Corollary 4.3.** The Cohen-Lenstra sum \( S(\mathbb{Z}_p[C_p^k]; 0) \) converges to a real number. More precisely: \( S(\mathbb{Z}_p[C_p^k]; 0) = \frac{1}{(q)^{k+1}} \).

5. Cohen-Lenstra sums over \( \mathbb{Z}_p[C_p] \) with prescribed cohomology groups

In this section we will consider some "refinements" of Cohen-Lenstra sums over the ring \( \mathbb{Z}_p[C_p] \). To be more precise, we will restrict the summation to those finite modules \( M \) having prescribed Tate cohomology groups \( \hat{H}^i(C_p, M) \). Sums of this kind may be important for applications; e.g. in [5]

\[
\sum_{M} |\text{Aut}_{\mathbb{Z}_p[A]}(M)|^{-1}
\]

is computed, where \( \Delta \) is a finite abelian \( p \)-group, and the summation extends over all cohomologically trivial \( \mathbb{Z}_p[A] \)-modules.
We use the following notations in this section. Let \( R = \mathbb{Z}_p[C_p] \), let \( \sigma \) be a generator of the cyclic group \( C_p \), and put \( \phi = 1 + \sigma + \cdots + \sigma^{p-1} \in R \) and \( I = (\sigma - 1)R \) (which is the augmentation ideal of \( R \)).

We need some basic notions of Tate cohomology of finite groups (cf. [12]). If \( M \) is a finite \( R \)-module, the Tate cohomology groups satisfy

\[
\widehat{H}^i(C_p, M) \cong \widehat{H}^{i+2}(C_p, M) \quad \forall \ i \in \mathbb{Z},
\]

for \( C_p \) is cyclic. Hence we can restrict to

\[
\widehat{H}^0(C_p, M) = M^{C_p}/\phi M \quad \text{and} \quad \widehat{H}^1(C_p, M) \cong \widehat{H}^{-1}(C_p, M) = \phi M / IM;
\]

here \( M^{C_p} \) is the submodule of elements fixed by \( C_p \), and \( \phi M \) is the kernel of the action of \( \phi \) on \( M \). Since \( M \) is finite, its Herbrand quotient is equal to 1, i.e. \( |\widehat{H}^0(C_p, M)| = |\widehat{H}^1(C_p, M)| \). Since all cohomology groups are annihilated by \( |C_p| \), we infer that there exists \( h \in \mathbb{N} \) such that

\[
\widehat{H}^0(C_p, M) \cong \widehat{H}^1(C_p, M) \cong (\mathbb{Z}/p\mathbb{Z})^h.
\]

This number \( h \) describes completely all Tate cohomology groups \( \widehat{H}^i(C_p, M) \).

We will use the following abbreviation:

\[
\widehat{H}^i(M) := \widehat{H}^i(C_p, M)
\]

for \( i = 0, 1 \).

Now let \( G \) be a finite abelian \( p \)-group and \( h, u \in \mathbb{N} \). The goal of this section is the computation of

\[
\sum_{\phi M \cong G \atop |\widehat{H}^1(M)| = p^h} |\text{Aut}_R(M)|^{-1}|M|^{-u},
\]

where of course the summation extends over all finite modules \( M \) as indicated, up to isomorphism. Note that \( \phi M \) is an \((R/I)\)-module, and \( R/I \cong \mathbb{Z}_p \).

The value of this sum will be stated in Theorem 5.6. A first step in the computation consists in relating this sum over finite modules \( M \) to a limit for \( n \to \infty \) of a sum over submodules \( U \subseteq R^n \) (a kind of “partial zeta function”), similar to the case of the full Cohen-Lenstra sum in section 2.

We denote by \( \varepsilon : R^n \to \mathbb{Z}_p^n \) the augmentation map with kernel \( I^n \), induced by \( R \to \mathbb{Z}_p, \sum_{i=0}^{p-1} a_i \sigma^i \mapsto \sum_{i=0}^{p-1} a_i \), and by \( \nu := \nu(G) = \dim_{\mathbb{F}_p}(G/pG) \) the rank of the finite abelian \( p \)-group \( G \). We further recall that all submodules of \( R^n \) are understood to have finite index in \( R^n \).
Lemma 5.1. Let $G$ be a finite abelian $p$-group, and $h, u \in \mathbb{N}$. Then for all $N \subseteq \mathbb{R}^n$ there is $\overline{N} \subseteq \mathbb{Z}_p^n$ such that $p\overline{N} = \varepsilon(N \cap \phi \mathbb{R}^n)$, and
\[
\sum_{\phi M \cong G, |\hat{H}^1(M)| = p^h} |\text{Aut}_R(M)|^{-1} |M|^{-u} = \lim_{n \to \infty} \sum_{\mathbb{Z}_p^N, N \subseteq \mathbb{R}^n, (\overline{N} : \varepsilon(N)) = p^h} [\mathbb{R}^n : N]^{-(n+u)}.
\]

Proof. The existence of $\overline{N}$ is clear. Multiplication by $\phi$ on $M$ induces a surjection $\psi : M/IM \to \phi M$ with $\hat{H}^1(M) = \ker(\psi)$. Each $M$ such that $\phi M \cong G$ and $|\hat{H}^1(M)| = p^h$ has the form $M \cong \mathbb{R}^n / N$ for some $n \geq \max\{\nu, h\}$ and $N \subseteq \mathbb{R}^n$. Thus
\[
M/IM \cong \mathbb{R}^n / (N + I^n) \cong \mathbb{Z}_p^n / \varepsilon(N)
\]
and
\[
\phi M \cong (\phi \mathbb{R}^n + N) / N \cong \phi \mathbb{R}^n / (N \cap \phi \mathbb{R}^n) \cong p\mathbb{Z}_p^n / \varepsilon(N \cap \phi \mathbb{R}^n) \cong \mathbb{Z}_p^n / \overline{N}.
\]
We therefore have a commutative diagram
\[
\begin{array}{ccc}
M/IM & \cong & \mathbb{Z}_p^n / \varepsilon(N) \\
\psi \downarrow & & \downarrow \text{can} \\
\phi M & \cong & \mathbb{Z}_p^n / \overline{N}
\end{array}
\]
hence
\[
\hat{H}^1(M) = \ker(\psi) \cong \overline{N} / \varepsilon(N).
\]
Now the lemma follows from Theorem 4.1, or more precisely from its generalization stated at the end of the preceding section. □

We now have to determine all $N \subseteq \mathbb{R}^n$ such that $\mathbb{Z}_p^n / \overline{N} \cong G$ and $[\overline{N} : \varepsilon(N)] = p^h$. In order to achieve this, we will use Morita's Theorem (cf. [9, Sec. 3.12]) and translate all submodules of $\mathbb{R}^n$ to left ideals of the matrix ring $M_n(\mathbb{R})$. The main property of Morita's Theorem that we will be using in the sequel is the following: There is an isomorphism between the lattice of $R$-submodules $U$ of finite index in $\mathbb{R}^n$ and the lattice of left ideals $I \subseteq M_n(\mathbb{R})$ of finite index. Moreover, if $U$ and $I$ correspond to each other, then one easily verifies that
\[
\]
In a similar way, submodules of $\mathbb{Z}_p^n$ correspond to left ideals of $M_n(\mathbb{Z}_p)$.

Let $n \geq \max\{\nu, h\}$. Then $G$ is a quotient of $\mathbb{Z}_p^n$, and we let $G'$ be the corresponding quotient of $M_n(\mathbb{Z}_p)$ via Morita's Theorem, so in particular
\[
|G'| = |G|^n.
\]
Now it is easy to see from the above lemma that our sum is equal to the limit for \( n \to \infty \) of
\[
x_n := \sum_{\substack{N' \subset M_n(R) \\
 \text{sat}_{M_n(R)} N' \in G' \\
 [N'] \in p^{nh}}}[M_n(R) : N']^{-(1+u/n)},
\]
where as always all ideals are of finite index, and \( \overline{N'} \) is the left ideal of \( M_n(Z_p) \) satisfying \( p\overline{N'} = \varepsilon(N' \cap \phi M_n(R)) \). Here we denote the augmentation map \( M_n(R) \to M_n(Z_p) \) by \( \varepsilon \) as well.

Thus we have to count left ideals of \( M_n(R) \). This can be done by using an idea that goes back to Reiner (cf. [10]), also applied in [14, Sec. 3]. The crucial point is that \( R = Z_p[C_p] \) is a fibre product of the two discrete valuation rings \( S = Z_p[\omega] \), where \( \omega \) is a primitive \( p \)-th root of unity, and \( Z_p \). This leads to a fibre product representation for \( M_n(R) \), viz there is a fibre product diagram with surjective maps
\[
\begin{array}{ccc}
M_n(R) & \xrightarrow{f_1} & M_n(S) \\
\varepsilon \downarrow & & \downarrow g_1 \\
M_n(Z_p) & \xrightarrow{g_2} & M_n(F_p)
\end{array}
\]
with \( f_1 \) induced by \( R \to R/(\phi) \cong S \), \( g_1 \) induced by \( S \to S/(1 - \omega) \cong F_p \), and \( g_2 \) is reduction mod \( p \). Equivalently, there is an isomorphism
\[
M_n(R) \cong \{(x, y) \in M_n(S) \times M_n(Z_p) \mid g_1(x) = g_2(y)\}.
\]

Now we can use Reiner’s method, and represent the left ideals of \( M_n(R) \) in terms of the left ideals of \( M_n(S) \) and \( M_n(Z_p) \) (both of which are principal ideal rings). If \( N' \subset M_n(R) \) is a left ideal (of finite index), then there is an \( \alpha \in M_n(S) \) with \( \det(\alpha) \neq 0 \) such that \( f_1(N') = M_n(S)\alpha \). Choose \( \beta \in M_n(Z_p) \) such that \( g_1(\alpha) = g_2(\beta) \). Then
\[
N' = M_n(R)(\alpha, \beta) + (0, p\overline{N'}), \tag{13}
\]
where \( \overline{N'} \subset M_n(Z_p) \) is the left ideal (of finite index) satisfying \( p\overline{N'} = \varepsilon(N' \cap \phi M_n(R)) = \{x \in M_n(Z_p) \mid (0, x) \in N'\} \), and \( \beta \in \overline{N'} \).

Conversely, if \( \alpha \in M_n(S) \) with \( \det(\alpha) \neq 0 \) and a left ideal \( \overline{N'} \subset M_n(Z_p) \) of finite index are given, then \( \alpha \) and \( \overline{N'} \) give rise to a left ideal \( N' \subset M_n(R) \) as in (13) if and only if \( g_1(\alpha) \in g_2(\overline{N'}) \). In this case, the number of left ideals of \( M_n(R) \) belonging to \( \alpha \) and \( \overline{N'} \) is equal to the number of \( \beta \in \overline{N'} \) distinct mod \( p\overline{N'} \) such that \( g_1(\alpha) = g_2(\beta) \).

**Notation.** We denote by \( \mathcal{R} \) a system of representatives of the generators of all left ideals of finite index in \( M_n(S) \). If \( \alpha \in \mathcal{R} \) and \( \overline{N'} \subset M_n(Z_p) \)
is a left ideal with \( g_1(\alpha) \in g_2(\overline{N'}) \) we denote by \( \theta(\alpha) \) the number of left \( M_n(R) \)-ideals of the form

\[
N' := M_n(R)(\alpha, \beta) + (0, p\overline{N'})
\]
satisfying \([N' : M_n(\mathbb{Z}_p)\beta + p\overline{N'\alpha} = p^{nh}\). Note that the latter is one of the conditions required in the summation for \( x_n \), since \( e(N') = M_n(\mathbb{Z}_p)\beta + p\overline{N'} \). We will see below in Lemma 5.3 that the value \( \theta(\alpha) \) does not depend on the particular \( \overline{N'} \), which justifies the notation.

It is shown in [14, Lemma 3.4] that

\[
[M_n(R) : N'] = [M_n(S) : M_n(S)\alpha][M_n(\mathbb{Z}_p) : \overline{N'}]
\]

for \( N' \) as in (13). Together with the above discussion, this equality yields the following formula for \( x_n \):

\[
x_n = \sum_{\overline{N'} \subseteq M_n(\mathbb{Z}_p)} \sum_{\alpha \in R} \theta(\alpha) [M_n(S) : M_n(S)\alpha][M_n(\mathbb{Z}_p) : \overline{N'}]^{-(1+u/n)},
\]
hence \( x_n = y_n z_n \) with

\[
y_n := \sum_{\overline{N'} \subseteq M_n(\mathbb{Z}_p)} |\Gamma'|^{-(1+u/n)},
\]

\[
z_n := \sum_{\alpha \in R} \theta(\alpha) [M_n(S) : M_n(S)\alpha]^{-(1+u/n)},
\]

where in the last sum \( \overline{N'} \subseteq M_n(\mathbb{Z}_p) \) is an arbitrary left ideal with \( M_n(\mathbb{Z}_p)/\overline{N'} \cong \Gamma' \).

**Lemma 5.2.** \( \lim_{n \to \infty} y_n = |\text{Aut}(G)|^{-1}|\Gamma|^{-u} \).

**Proof.** We translate everything back to submodules of \( \mathbb{Z}_p^n \) using Morita’s Theorem. Since \( |\Gamma'| = |\Gamma|^n \) we get

\[
y_n = |\Gamma|^{-(n+u)}.|\{N \subseteq \mathbb{Z}_p^n \mid \mathbb{Z}_p^n/\overline{N} \cong \Gamma\}|,
\]

and by Lemma 2.2, 2.4 we infer

\[
y_n = |\Gamma|^{-(n+u)}|\Gamma|^n (q)_n (q)_{n-\nu} |\text{Aut}(G)|^{-1},
\]

which proves the claim.

The calculation of \( \lim_{n \to \infty} z_n \) is more complicated. We start by computing \( \theta(\alpha) \), and we recall that \( \nu \) denotes the rank of the abelian \( p \)-group \( G \).
Lemma 5.3. Let $\overline{N'} \subseteq M_n(\mathbb{Z}_p)$ be a left ideal such that $M_n(\mathbb{Z}_p)/\overline{N'} \cong G'$. Furthermore let $\alpha \in \mathcal{R}$ with $g_1(\alpha) \in g_2(\overline{N'})$, and put $r := \text{rk}(g_1(\alpha))$. Then $\theta(\alpha)$ equals $\theta_r$, the number of all $\xi \in M_n(\mathbb{F}_p)$ lying in

\[
\begin{pmatrix}
1 & \cdots & 0^{r \times (n-\nu-r)} & \mathbb{F}_p^{r \times \nu} \\
\vdots & \ddots & \ddots & \ddots \\
0^{(n-r) \times r} & 0^{(n-r) \times (n-\nu-r)} & \mathbb{F}_p^{(n-r) \times \nu}
\end{pmatrix}
\]

and whose bottom right $((n - r) \times \nu)$-submatrix has rank $n - h - r$. In particular we have

\[n - \nu - h \leq r \leq \min\{n - \nu, n - h\}.
\]

Proof. Fix $\alpha$ and $\overline{N'} \subseteq M_n(\mathbb{Z}_p)$ as above. The number of left $M_n(\mathbb{R})$-ideals of the form (13) equals the number of $\beta \in \overline{N'}$ with $g_1(\alpha) = g_2(\beta)$ which are distinct mod $p\overline{N'}$. Thus, by definition of $\theta(\alpha)$,

\[
\theta(\alpha) = |\{\beta \in \overline{N'} \mod p\overline{N'} | g_1(\alpha) = g_2(\beta), [\overline{N'} : M_n(\mathbb{Z}_p)\beta + p\overline{N'}] = p^{nh}\}|
\]

Choose $\rho \in M_n(\mathbb{Z}_p)$ with $M_n(\mathbb{Z}_p)\rho = \overline{N'}$. There is an isomorphism

\[G'/pG' \cong M_n(\mathbb{F}_p)/g_2(\overline{N'}) = M_n(\mathbb{F}_p)/M_n(\mathbb{F}_p)g_2(\rho),\]

whence $\text{rk}(g_2(\rho)) = n - \nu$. Now $\theta(\alpha)$ equals the number of all $\beta' \in M_n(\mathbb{Z}_p) \mod pM_n(\mathbb{Z}_p)$ such that

\[g_1(\alpha) = g_2(\beta')g_2(\rho) \quad \text{and} \quad [M_n(\mathbb{Z}_p)\beta' + pM_n(\mathbb{Z}_p) : pM_n(\mathbb{Z}_p)] = p^{n(n-h)}.
\]

We assume without loss of generality that

\[g_2(\rho) = \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 0 \\ \cdots \\ 0 \end{pmatrix}
\]

with $n - \nu$ 1’s on the main diagonal. Then

\[g_1(\alpha) \in \left(\mathbb{F}_p^{n \times (n-\nu)} \mid 0^{n \times \nu}\right),
\]

i.e. $g_1(\alpha) = (\gamma_1|0)$ for some $\gamma_1 \in \mathbb{F}_p^{n \times (n-\nu)}$ with $\text{rk}(\gamma_1) = r$. This implies

\[
\theta(\alpha) = |\{\xi = (\xi_1|\xi_2) \in \left(\mathbb{F}_p^{n \times (n-\nu)} \mid 0^{n \times \nu}\right) | \xi_1 = \gamma_1 \text{ and } \text{rk}(\xi) = n - h\}|
\]

Obviously this number only depends on $r = \text{rk}(\gamma_1)$. Therefore we may choose $\gamma_1$ to be the matrix having $r$ 1’s as its first entries of the main diagonal, all other entries being 0. Now it is clear that $\theta(\alpha) = \theta_r$. 
Since \( g_1(\alpha) \in g_2(\overline{\mathbb{N}}) \) we have \( \theta_r = \theta(\alpha) \neq 0 \), or equivalently \( n - \nu - h \leq r \leq \min\{n - \nu, n - h\} \).

The following lemma, which is easy to prove (cf. [4, Th. 2]) gives a formula for the number of matrices of given size over a finite field having fixed rank.

**Lemma 5.4.** Let \( k, m, n \in \mathbb{N} \) with \( k \leq \min\{m, n\} \). Then

\[
p^{(n+m-k)} \frac{(q)_n(q)_m}{(q)_{n-k}(q)_{m-k}(q)_k}
\]

equals the number of matrices in \( \mathbb{F}_p^{n \times n} \) of rank \( k \).

Making use of this lemma, the number \( \theta_r \) defined in Lemma 5.3 is easily calculated:

\[
\theta_r = p^{\nu r \frac{(\nu+n-r-(n-h-r))(n-h-r)}{(q)_\nu(q)_{n-r}} \frac{(q)_\nu(q)_n}{(q)_{\nu-(n-h-r)}(q)_h(q)_{n-h-r}}}
\]

(14)

The value \( z_n \) defined above now takes the form

\[
z_n = \sum_{r = n - \nu - h}^{\min\{n - \nu, n - h\}} \sum_{\alpha \in \mathbb{F}_p^{n \times n}} \left[ M_n(S) : M_n(S)\alpha \right]^{-\frac{(1+u)}{n}},
\]

(15)

where again \( \gamma_1 \in \mathbb{F}_p^{n \times (n-\nu)} \).

**Lemma 5.5.** Let \( n - \nu - h \leq r \leq \min\{n - \nu, n - h\} \). Then

\[
\sum_{\alpha \in \mathbb{F}_p^{n \times n}} \left[ M_n(S) : M_n(S)\alpha \right]^{-\frac{(1+u)}{n}} = \left[ \begin{array}{c}
\frac{n - \nu}{r}
\end{array} \right] p^{n+u} \frac{(q)_u}{(q)_{n+u-r}},
\]

where again \( \gamma_1 \in \mathbb{F}_p^{n \times (n-\nu)} \).

**Proof.** By Morita’s Theorem we can retranslate the sum to a sum over \( S \)-submodules of \( S^n \). Thus fix an \( r \)-dimensional subspace \( F \subseteq \mathbb{F}_p^{n-\nu} \). Then we will see below that the sum

\[
\sum_{\gamma_1: \text{rk}(\gamma_1) = r \atop g_1(\alpha) = (\gamma_1|0)} [S^n : U]^{-(n+u)}
\]

does not depend on the particular \( F \) chosen. There are in fact \( \left[ \begin{array}{c}
\frac{n - \nu}{r}
\end{array} \right] p 
\)

choices for \( F \), whence the sum to be computed equals

\[
\left[ \begin{array}{c}
\frac{n - \nu}{r}
\end{array} \right] \sum_{\gamma_1: \text{rk}(\gamma_1) = r \atop g_1(\alpha) = (\gamma_1|0)} [S^n : U]^{-(n+u)}.
\]
Since both $S$ and $\mathbb{Z}_p$ are discrete valuation rings with residue field $\mathbb{F}_p$, and since $g_1, g_2$ induce isomorphisms $S^n/\text{rad}(S^n) \to \mathbb{F}_p^n$ and $\mathbb{Z}_p^n/\text{rad}(\mathbb{Z}_p^n) \to \mathbb{F}_p^n$ respectively, we get

$$
\sum_{U \subseteq S^n} [S^n : U]^{-(n+u)} = \sum_{U \subseteq \mathbb{Z}_p^n} [\mathbb{Z}_p^n : U]^{-(n+u)} = \sum_{U \subseteq \mathbb{Z}_p^n} [\mathbb{Z}_p^n : U]^{-(n+u)}
$$

with $p\mathbb{Z}_p^n \subseteq V \subseteq \mathbb{Z}_p^n$ such that $V/p\mathbb{Z}_p^n = \mathbb{F} \oplus 0^\nu$. By [14, Lemma 7.3] this equals

$$
[Z_p^n : V]^{-(n+u)} \sum_{U \subseteq V} [V : U]^{-(n+u)} = p^{-(n+u)(n-r)} \prod_{j=r}^{n-1} (1 - q^{n+u-j})^{-1} = q^{(n+u)(n-r)} \frac{(q)_u}{(q)_{n+u-r}}.
$$

This proves the lemma. $\square$

Now (15) implies

$$
z_n = \min\{n-\nu, n-h\} \frac{q^{(n+u)(n-r)} \frac{(q)_u}{(q)_{n+u-r}}}{p^{\exp_r} \frac{(q)_n r (q)_{n-r} (q)_{n-\nu} (q)_{n-h} (q)_{n-h-r} (q)_{n-\nu-r} (q)_{n+u-r}}{\frac{(q)_{n+u} r (q)_{n+u-r}}{(q)_{n+u}}}},
$$

with

$$
\exp_r := -hr + (\nu + h)(n - h) + r(n - \nu - r) - (n + u)(n - r)
$$

as $p$-exponent. Substituting $e := r - (n - \nu - h)$ yields

$$
z_n = \min\{\nu, h\} \frac{p^{\exp_e} \frac{(q)_n r (q)_{n-\nu-e} (q)_{n+u-e}}{(q)_{n+u-e}}}{\frac{(q)_n r (q)_{n-\nu-e} (q)_{n+u-e}}{(q)_{n+u-e}}}
$$

with

$$
\exp'_e := -(h^2 + hu) + h(e - \nu) + ev + eu - e^2 - \nu u.
$$

The last step consists in letting $n \to \infty$, and we get

$$
\lim_{n \to \infty} z_n = q^{h(e+u+v)}u(q)_{n+u} = (q)_{n+u}^\nu \times \sum_{e=0}^{\min\{\nu, h\}} p^{e+u+v} \frac{(q)_{n+u-e}}{(q)_{n+u-e}}.
$$

Now

$$
\lim_{n \to \infty} x_n = (\lim_{n \to \infty} y_n)(\lim_{n \to \infty} z_n)
$$
can be derived from Lemma 5.2 and (16). Since by definition \( \lim_{n \to \infty} x_n \) equals the limit occurring in Lemma 5.1, the proof of the following main theorem of this section is complete.

**Theorem 5.6.** Let \( G \) be a finite abelian \( p \)-group of rank \( \nu \), and let \( h, u \in \mathbb{N} \). Then

\[
\sum_{\phi M \cong G \atop \chi^1(M) = p^h} \left| \text{Aut}_R(M) \right|^{-1} |M|^{-u} =
\]

\[
q^{(\nu + h + u) + u} (q)^u (q)^{\nu} \kappa(\nu, h, u) |\text{Aut}(G)|^{-1} |G|^{-u},
\]

where

\[
\kappa(\nu, h, u) := \sum_{e=0}^{\min(\nu, h)} p^{(\nu + h) - e} \frac{(q)^{\nu + h - e}}{(q)^{\nu - e} (q)^{h - e} (q)^{\nu + h + u - e}}.
\]

We will conclude this section by considering this formula in the special cases \( u = 0, h = 0, \nu = 0 \) respectively.

**Corollary 5.7.** Let \( G \) be a finite abelian \( p \)-group of rank \( \nu \), and let \( h \in \mathbb{N} \). Then

\[
\sum_{\phi M \cong G \atop \chi^1(M) = p^h} \left| \text{Aut}_R(M) \right|^{-1} = \frac{q^{h^2}}{(q)^h} |\text{Aut}(G)|^{-1}.
\]

**Proof.** We put \( u := 0 \) in the preceding theorem, and thus the sum equals

\[
\frac{q^{h + \nu}}{(q)^h} \left( \sum_{e=0}^{\min(\nu, h)} p^{(\nu + h) - e} \frac{(q)^{\nu} (q)^h}{(q)^{\nu - e} (q)^{h - e}} \right) |\text{Aut}(G)|^{-1}.
\]

By Lemma 5.4, the \( e \)-th term of the expression in brackets equals the number of matrices in \( \mathbb{F}_p^{\nu \times h} \) of rank \( e \). Hence (17) can be written as

\[
\frac{q^{h + \nu}}{(q)^h} |\mathbb{F}_p^{\nu \times h}| |\text{Aut}(G)|^{-1} = \frac{q^{h^2}}{(q)^h} |\text{Aut}(G)|^{-1}.
\]

Next we consider the case \( h = 0 \), i.e. the summation extends over cohomologically trivial modules.

**Corollary 5.8.** Let \( G \) be a finite abelian \( p \)-group of rank \( \nu \), and let \( u \in \mathbb{N} \). Then

\[
\sum_{\phi M \cong G \atop M \text{ cohom. trivial}} \left| \text{Aut}_R(M) \right|^{-1} |M|^{-u} = q^{\nu u} \frac{(q)^u (q)^{\nu}}{(q)^{u + \nu}} |\text{Aut}(G)|^{-1} |G|^{-u}.
\]
Finally let $G = 0$.

**Corollary 5.9.** Let $h, u \in \mathbb{N}$. Then
\[
\sum_{\phi \in \mathbb{M} = 0} |\text{Aut}_R(M)|^{-1} |M|^{-u} = \sum_{\phi \in \mathbb{M} = 0} |\text{Aut}_R(M)|^{-1} |M|^{-u} = \frac{q^{h(h+u)}(q)_{u}}{(q)_{h}(q)_{h+u}}.
\]

**References**


