Fitting ideals
and the Gorenstein property

Burcu Baran
Department of Mathematics,
Stanford University,
Stanford, CA 94305, USA.

Abstract: Let $p$ be a prime number and $G$ be a finite commutative group such that $p^2$ does not divide the order of $G$. In this note we prove that for every finite module $M$ over the group ring $\mathbb{Z}_p[G]$, the inequality $\# M \leq \# \mathbb{Z}_p[G]/\text{Fit}_{\mathbb{Z}_p[G]}(M)$ holds. Here, $\text{Fit}_{\mathbb{Z}_p[G]}(M)$ is the $\mathbb{Z}_p[G]$-Fitting ideal of $M$.

1. Introduction

Let $R$ be a commutative ring with identity. For a finitely generated $R$-module $M$, we denote the $R$-Fitting ideal of $M$ by $\text{Fit}_R(M)$. When $R$ is a discrete valuation ring, it is well known that

$$\text{length } M = \text{length } R/\text{Fit}_R(M).$$

for every finite-length $R$-module $M$. (In fact, this is known for one-dimensional local Cohen-Macaulay rings and $M$ of finite length and finite projective dimension; see [2, Lemma 21.10.17.3] and [4, Thm. 19.1]). The equality does not hold when $R$ is not a DVR. Indeed, suppose $R$ is a local ring with maximal ideal $m$ and residue field $k$ such that $R$ is not a DVR. Let $M = k \times k$, so the length of $M$ is 2. The Fitting ideal $\text{Fit}_R(M)$ is $m^2$, so the length of $R/\text{Fit}_R(M)$ is $1 + \dim_k m/m^2$, which is greater than 2. Hence, we have a strict inequality

$$\text{length } M < \text{length } R/\text{Fit}_R(M).$$

Thus, we ask if for certain rings $R$ it is at least true that for every finite-length $R$-module $M$ we have the inequality $\text{length } M \leq \text{length } R/\text{Fit}_R(M)$. Let $p$ be a prime number. We consider this question for $R = A[C]$ where $C$ is a group of prime order $p$ and $A$ is the ring of integers of an unramified finite extension of $\mathbb{Q}_p$. The following is the main result of this paper. It gives an affirmative answer to our question.

Theorem 1.1. Let $M$ be a finite $A[C]$-module where $C$ is a group of prime order $p$ and $A$ is the ring of integers of an unramified finite extension of $\mathbb{Q}_p$. We have the following inequality

$$\# M \leq \# A[C]/\text{Fit}_{A[C]}(M).$$
If the ideal $\text{Fit}_{A[C]}(M)$ is a principal ideal then we have an equality.

For any finite abelian group $G$ of order not divisible by $p^2$, the group ring $\mathbb{Z}_p[G]$ is a product of rings of the form $A[C]$ as in Theorem 1.1. If Theorem 1.1 is true for rings $S$ and $S'$ then it is also true for their direct product $S \times S'$. Hence, the following is a corollary of Theorem 1.1.

**Corollary 1.2.** Let $p$ be a prime and let $G$ be a finite commutative group for which $p^2 \nmid \# G$. Then for every finite $\mathbb{Z}_p[G]$-module $M$ we have the following inequality

$$\# M \leq \# \mathbb{Z}_p[G]/\text{Fit}_{\mathbb{Z}_p[G]}(M).$$

If the ideal $\text{Fit}_{\mathbb{Z}_p[G]}(M)$ is a principal ideal then we have an equality.

The local ring $A[C]$ is a Gorenstein ring. This plays a very important role in the proof of Theorem 1.1. In Section 3, we prove Proposition 3.6 relating ideals in $A[C]$ and in its normalization; this is the key proposition. It is an application of a result (Proposition 3.5) proved in [1]. In the rest of the paper, we use Proposition 3.6 to exploit the Gorenstein property of $A[C]$. In Section 4, we fix a short exact sequence $0 \rightarrow K \rightarrow A[C]^t \rightarrow M \rightarrow 0$ for a finite $A[C]$-module $M$. Let $F_q$ be the residue field of $A$. We prove that $K/\mathfrak{m}K$ is an $F_q$-vector space of dimension $t$ if and only if $\text{Fit}_{A[C]}(M)$ is a principal ideal. By using that, in Section 5 we prove the main result (Theorem 1.1).

I would like to thank René Schoof for his continuous guidance and support.

2. The definition of a Fitting ideal

Let $R$ be a commutative ring with identity and $M$ be a finitely generated $R$-module. Choose a surjective $R$-morphism $f : R^t \rightarrow M$. The $R$-ideal generated by $\det(v_1, v_2, \ldots, v_t)$, where $v_1, v_2, \ldots, v_t \in \ker f$, does not depend on $f$ [see 3, p.741]. It only depends on the $R$-module $M$.

**Definition 2.1.** The $R$-ideal generated by all $\det(v_1, v_2, \ldots, v_t)$, where $v_1, v_2, \ldots, v_t \in \ker f$, is called the $R$-Fitting ideal of $M$. It is denoted by $\text{Fit}_R(M)$.

We have the following proposition.

**Proposition 2.2.** For a finitely generated $R$-module $M$, the following hold.

1. If $M = R/I$ for an ideal $I$ of $R$, then $\text{Fit}_R(M) = I$.

2. If $N$ is another finitely generated $R$-module, then $\text{Fit}_R(M \times N) = \text{Fit}_R(M)\text{Fit}_R(N)$.

3. For any $R$-algebra $B$, we have $\text{Fit}_B(M \otimes_R B) = \text{Fit}_R(M)B$.

**Proof:** These follow immediately from the definition of a Fitting ideal and properties of the tensor product.

**Example 2.3.** Suppose $L$ is a finitely generated module over a principal ideal domain $D$. Then we have

$$L \cong \bigoplus_{i=1}^t D/a_i D,$$
for certain elements \(a_i\) in \(D\). There exists a natural surjective \(D\)-morphism

\[ f : D^i \longrightarrow L \]

whose kernel is generated by the vectors \((a_1, 0, \ldots, 0), (0, a_2, \ldots, 0), \ldots, (0, 0, \ldots, a_t)\). Therefore, the \(D\)-ideal \(\text{Fit}_D(L)\) is generated by the product \(a_1 a_2 \cdots a_t\). With this example we see that if \(L\) were to be a finite \(D\)-module then we would have \(\#L = \#D/\text{Fit}_D(L)\).

3. The Gorenstein group ring \(A[C]\)

In the rest of the paper, we assume that \(R = A[C]\) where \(C\) is a cyclic group of prime order \(p\) and \(A\) is the ring of integers of an unramified finite extension of \(\mathbb{Q}_p\). Let \(\mathbb{F}_q\) be the residue field of \(A\), so \(q\) is a power of \(p\). Suppose \(c\) is a generator of \(C\). We have the isomorphism

\[ \phi : R \longrightarrow A[T]/((1 + T)^p - 1) \]

given by \(\phi(c) = 1 + T\). The ring \(A[T]/((1 + T)^p - 1)\) is a local ring with maximal ideal \((p, T)\) and residue field \(\mathbb{F}_q\). As the depth and the Krull dimension of \(R\) are both equal to 1, the local ring \(R\) is a Cohen-Macaulay ring. The element \(p\) in the maximal ideal of \(R\) is an \(R\)-regular sequence which generates an irreducible ideal in \(R\). Therefore, \(R\) is a Gorenstein ring. In other words, it has finite injective dimension. In fact, its injective dimension is equal to its Krull dimension which is 1.

**Notation 3.1.** We denote the unique maximal ideal of \(R\) by \(m\).

**Remark 3.2.** The normalization \(\tilde{R}\) of \(R\) in its total quotient ring is \(A \times A[\zeta_p]\). Here \(\zeta_p\) is a primitive \(p\)-th root of unity. The ring \(\tilde{R}\) is isomorphic to the product \(A[T]/(T) \times A[T]/(N)\) where \(N = \frac{(1+T)^p-1}{T}\). The ring \(\tilde{R}\) is a principal ideal ring. We have the short exact sequence

\[ 0 \longrightarrow R \longrightarrow \tilde{R} \longrightarrow R/m \longrightarrow 0, \]

where the map \(\eta\) is given by \(\eta(r) = (r \mod T, r \mod N)\) for every \(r \in R\), and the map \(\vartheta\) is given by \(\vartheta(r_1, r_2) = r_1 - r_2 \mod m\) for every \((r_1, r_2) \in \tilde{R}\). Thus, the \(A\)-module \(\tilde{R}/R\) is isomorphic to the residue field \(\mathbb{F}_q\) of \(R\), and so the quotient \(A\)-module \(\tilde{R}/R\) has length 1.

**Notation 3.3.** For any \(R\)-module \(M\), we denote the tensor product \(M \otimes_R \tilde{R}\) by \(\tilde{M}\).

For an \(R\)-module \(M\), there is always the natural \(R\)-morphism \(\psi\) from \(M\) to \(\tilde{M}\) given by \(\psi(m) = m \otimes 1\). We have the following proposition.

**Proposition 3.4.** Let \(M\) be an \(R\)-module and \(m\) be the maximal ideal of \(R\). Consider the natural \(R\)-morphism \(\psi : M \longrightarrow \tilde{M}\). The cokernel of \(\psi\) is isomorphic to \(M/mM\) through the map \(\tau\) given by \(\tau(m \otimes (\lambda, \mu)) = (\lambda - \mu)m \mod mM\), for every \(m \otimes (\lambda, \mu) \in \tilde{M}\). The kernel of \(\psi\) is killed by \(m\), so if \(M\) is \(\mathbb{Z}_p\)-torsion free then the map \(\psi\) is injective.

**Proof:** While proving this proposition, to make the computations easy, we identify the ring \(R\) with \(A[T]/((1 + T)^p - 1)\) via the isomorphism \(\phi\) above. Thus, the maximal ideal \(m\) of \(R\) is \((p, T)\) and \(\tilde{R}\) is equal to \(A[T]/(T) \times A[T]/(N)\) where \(N = \frac{(1+T)^p-1}{T}\). Consider the
short exact sequence in Remark 3.2. Tensoring this short exact sequence over $A$ with the $R$-module $M$, we obtain the exact sequence

$$0 \longrightarrow K \longrightarrow M \xrightarrow{\psi} \tilde{M} \xrightarrow{\tau} M/\mathfrak{m}M \longrightarrow 0.$$  

Since we identified $\tilde{R}$ with $A[T]/(T) \times A[T]/(N)$, we also identify $\tilde{M}$ with $M/\mathfrak{T}M \times M/\mathfrak{N}M$. In this exact sequence, the map $\psi$ is given by $\psi(m) = (m \mod T, m \mod N)$ for every $m \in M$, and the map $\tau$ is given by $\tau(m_1, m_2) = m_1 - m_2 \mod \mathfrak{m}M$ for every $(m_1, m_2) \in \tilde{M}$. The map $\tau$ that we defined here coincides with the map $\tau$ that we defined in the proposition by the identification of $\tilde{M}$ with $M/\mathfrak{T}M \times M/\mathfrak{N}M$. With this exact sequence it is clear that the cokernel of $\psi$ is isomorphic to $M/\mathfrak{m}M$ through the map $\tau$. Now consider the kernel $K$ of $\psi$ in the above exact sequence. The $R$-module $K$ is equal to $\mathfrak{T}M \cap \mathfrak{N}M$, so it is killed by the ideal $(\mathfrak{N}, \mathfrak{T})$. Since $p \in (\mathfrak{N}, \mathfrak{T})$ and the ideal $(p, \mathfrak{T})$ is the maximal ideal, we have $(\mathfrak{N}, \mathfrak{T}) = (p, \mathfrak{T})$. It follows that $K$ is killed by the maximal ideal $\mathfrak{m}$ of $R$, and in particular by $p$. Thus, if $M$ is a $\mathbb{Z}_p$-torsion free $R$-module then $K = 0$. Hence, we proved the proposition.

Consider the following proposition concerning general Gorenstein orders over principal ideal domains.

**Proposition 3.5.** Let $\mathcal{O}$ be an order over a principal ideal domain. Then the following properties are equivalent:

- $\mathcal{O}$ is Gorenstein,
- for any fractional $\mathcal{O}$-ideal $a$, we have $(a : a) := \{ r \in \tilde{\mathcal{O}} : ra \subset a \}$ is equal to $\mathcal{O}$ if and only if $a$ is invertible. Here, $\tilde{\mathcal{O}}$ is the normalization of $\mathcal{O}$ in its total quotient ring.

**Proof:** This is Proposition 2.7 in [1].

Let $J$ be any ideal of $R$, then $(J : J) := \{ r \in \tilde{R} : rJ \subset J \}$ is a ring and we have

$$R \subset (J : J) \subset \tilde{R}.$$  

Since the quotient $A$-module $\tilde{R}/R$ has length 1 (see Remark 3.2), the ring $(J : J)$ is equal to either $R$ or $\tilde{R}$. In the sequel, to prove the main theorem in Section 5, we will use the following proposition very often to exploit the fact that $R$ is a Gorenstein ring.

**Proposition 3.6.** If the ideal $J$ of $R$ is not a principal ideal, then it is also an $\tilde{R}$-ideal.

**Proof:** Suppose $J$ is an ideal of $R$ which is not a principal ideal. By the above explanation, $(J : J)$ is either $R$ or $\tilde{R}$. Suppose it is equal to $\tilde{R}$. Since $R$ is an order over the principal ideal domain $A$, we use Proposition 3.5 and we obtain that the $R$-ideal $J$ is invertible. Since $R$ is a local ring, this occurs only when $J$ is a principal ideal generated by an element which is not a zero-divisor. But this contradicts our assumption that $J$ is not a principal ideal. Thus, we have $(J : J) = R$. Hence, $J$ is also an $\tilde{R}$-ideal.
4. Finite modules over $A[C]$

In this section, we prove some propositions which we will use in Section 5 in our proof of the main theorem. From now on, we assume that $M$ is a finite $R$-module. Recall that $C$ has prime order $p$ and $A$ is the ring of integers of an unramified finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$ and that $R = A[C]$ is a local ring with unique maximal ideal $m$ and residue field $\mathbb{F}_q$. We fix a short exact sequence

$$0 \rightarrow K \rightarrow R^t \rightarrow M \rightarrow 0 \quad (4.1)$$

of $R$-modules.

**Proposition 4.1.** Consider the $R$-module $K$ in the short exact sequence (4.1). The quotient $K/mK$ is an $\mathbb{F}_q$-vector space. We have

$$\dim_{\mathbb{F}_q}(K/mK) \geq t,$$

with equality holding if and only if $K$ is $R$-free of rank $t$.

**Proof:** Since the residue field of the local ring $R$ is $\mathbb{F}_q$, the quotient $K/mK$ is an $\mathbb{F}_q$-vector space. Let $d = \dim_{\mathbb{F}_q}(K/mK)$, so $K$ admits $d$ generators as an $R$-module, by Nakayama’s Lemma. By choosing a surjective map $\varphi : R^d \rightarrow K$, we get an exact sequence

$$R^d \xrightarrow{\varphi'} R^t \rightarrow M \rightarrow 0.$$\

We tensor this exact sequence over $A$ with $A[1/p] = F$. Since $M$ is a finite $R$-module and $R$ is a free $A$-module of rank $p$, we obtain a surjection

$$(F)^{pd} \xrightarrow{\varphi''} (F)^{pt} \rightarrow 0.$$

Hence, this shows that $d \geq t$. Now, suppose $d = t$. Then the surjection $\varphi'$ is an isomorphism, implying that $\operatorname{Ker} \varphi' \otimes_A F = 0$. Since $\operatorname{Ker} \varphi' \subset R^d$, it does not have nonzero $A$-torsion. This shows that $\operatorname{Ker} \varphi' = 0$, and so $\operatorname{Ker} \varphi = 0$. Therefore, the map $\varphi$ is an isomorphism, implying that $K$ is $R$-free of rank $t$. Hence, the proposition follows.

**Proposition 4.2.** Let $M$ be a finite $R$-module. Consider the short exact sequence (4.1). The $R$-module $K$ is free if and only if $\operatorname{Fit}_R(M)$ is a principal ideal of $R$.

**Proof:** Suppose $K$ is a free $R$-module. Since $M$ is a finite $R$-module, the rank of $K$ is equal to $t$. Then, by definition of the Fitting ideal, the $R$-ideal $\operatorname{Fit}_R(M)$ is generated by the determinant of the map from $K$ to $R^t$, implying that $\operatorname{Fit}_R(M)$ is a principal ideal. Now, assume that $\operatorname{Fit}_R(M)$ is a principal ideal of $R$. Let $\operatorname{Fit}_R(M) = \alpha R$ where $\alpha \in R$. Note that $\alpha \in R[1/p]^\times$ since $M$ is finite. Thus, $\alpha$ is not a zero-divisor in $R$. We claim that there exist $v_1, v_2, \ldots, v_t \in K$ such that $\det(v_1, v_2, \ldots, v_t) = \alpha u$, where $u$ is a unit in $R$. If this were not to be the case, then for every $w_1, w_2, \ldots, w_t \in K$ we would have

$$(\det(w_1, w_2, \ldots, w_t)) \subseteq \alpha m$$
where \( m \) is the unique maximal ideal of \( R \). Then we would have \( \text{Fit}_R(M) \subset m \text{Fit}_R(M) \), so Nakayama’s Lemma would imply that \( \text{Fit}_R(M) = 0 \). But this would contradict with the fact that \( M \) is finite.

Let \( r \) be any element of \( K \). We solve the linear system
\[
\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_t v_t = r
\]
with Cramer’s Rule. We get that \( \lambda_i = \delta_i/\alpha \) for some \( \delta_i \in \text{Fit}_R(M) \). Thus, in particular, all \( \lambda_i \)'s are in \( R \). This shows that the vectors \( v_1, v_2, \ldots, v_t \) generate \( K \) over \( R \). Now suppose
\[
\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_t v_t = 0,
\]
for \( \lambda_i \)'s which are not all zero. This implies that \( \det(v_1, v_2, \ldots, v_t) = \alpha u = 0 \), so that \( \alpha = 0 \). This again contradicts with the finiteness of \( M \). Thus, all \( \lambda_i \)'s are zero. As a result, we proved that \( K \) is a free \( R \)-module of rank \( t \). Hence, the proposition follows.

We tensor the short exact sequence (4.1) over \( R \) with \( \tilde{R} \) and we obtain the following commutative diagram:
\[
\begin{array}{cccccc}
0 & \rightarrow & K & \rightarrow & R^t & \rightarrow & M & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\tilde{K} & \rightarrow & \tilde{R}^t & \rightarrow & \tilde{M} & \rightarrow & 0
\end{array}
\]

Let \( H \) be the image of \( \tilde{K} \) in \( \tilde{R}^t \). We have \( H = \tilde{R}K \) inside \( \tilde{R}^t \), and we also have the commutative diagram of exact sequences.
\[
\begin{array}{cccccc}
0 & \rightarrow & K & \rightarrow & R^t & \rightarrow & M & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & H & \rightarrow & \tilde{R}^t & \rightarrow & \tilde{M} & \rightarrow & 0
\end{array}
\]  \hspace{1cm} (4.2)

**Proposition 4.3.** Consider the \( R \)-modules \( K \) and \( H \) in the commutative diagram (4.2). The \( R \)-module \( H/K \) is killed by the maximal ideal \( m \) of \( R \).

**Proof:** Since \( H = \tilde{R}K \), we have \( mH = m\tilde{R}K \). As \( \tilde{R}/R \) is isomorphic to \( R/m \), it follows that \( m\tilde{R} \subset R \), and so \( mH \subset K \). Hence, \( m \) kills the quotient \( H/K \).

**Proposition 4.4.** Consider the \( \tilde{R} \)-module \( H \) in the commutative diagram (4.2). It is free of rank \( t \), and \( H/mH \) is an \( F_q \)-vector space of dimension \( 2t \).

**Proof:** In the commutative diagram (4.2), we see that \( H \) is a \( \tilde{R} \)-submodule of \( \tilde{R}^t \). Since \( \tilde{R} \) is a product of two discrete valuation rings and the quotient \( \tilde{R}^t/H \) is isomorphic to the finite \( \tilde{R} \)-module \( \tilde{M} \), the \( \tilde{R} \)-module \( H \) is free of rank \( t \). Hence, \( H \) is isomorphic to \( \tilde{R}^t \). Since the residue field of \( R \) is \( F_q \) and the quotient \( \tilde{R}/R \) is \( F_q \), we have \( \tilde{R}/m = F_q \times F_q \). Here we use that the maximal ideal \( m \) of \( R \) is also an \( \tilde{R} \)-ideal (by Proposition 3.6). Therefore, the quotient \( H/mH \) is isomorphic to \( \tilde{R}^t/m\tilde{R}^t \) which is an \( F_q \)-vector space of dimension \( 2t \). Hence, we proved the proposition.
5. The main theorem
Recall that $M$ is a finite $R$-module and we have the short exact sequence (4.1). In this section, our aim is to prove the following theorem.

**Theorem 5.1.** Let $M$ be a finite $R$-module. We have

$$\#M \leq \#R/\text{Fit}_R(M),$$

with equality holding when $\dim_{F_q}(K/\mathfrak{m}K) = t$.

**Proof:** Consider the short exact sequence (4.1). In Proposition 4.1 we proved that $\dim_{F_q}(K/\mathfrak{m}K) \geq t$. Thus, we split the proof of this theorem in two cases.

**Case 1:** Suppose $\dim_{F_q}(K/\mathfrak{m}K) = t$.

Consider the short exact sequence (4.1) for a finite $R$-module $M$. By Proposition 4.1 the $R$-module $K$ is free of rank $t$. Tensoring the short exact sequence (4.1) over $R$ with $\tilde{R}$, we obtain the following commutative diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & 0 & \longrightarrow & R^t & \overset{\varphi}{\longrightarrow} & R^t & \longrightarrow & M & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \text{Ker } \tilde{\varphi} & \longrightarrow & \tilde{R}^t & \overset{\tilde{\varphi}}{\longrightarrow} & \tilde{R}^t & \longrightarrow & \tilde{M} & \longrightarrow & 0 \\
\end{array}
$$

Consider the bottom exact sequence. We tensor it over $A$ with $F := A[1/p]$. Since $F$ is $A$-flat, we obtain an isomorphism

$$0 \longrightarrow F^{pt} \overset{\tilde{\varphi}}{\longrightarrow} F^{pt} \longrightarrow 0.$$

As $\text{Ker } \tilde{\varphi} \subset \tilde{R}^t$, it does not have $A$-torsion. Hence, we have $\text{Ker } \tilde{\varphi} = 0$. Now, we apply the snake lemma to this commutative diagram. Since $\tilde{R}^t/R^t$ is $F_q$, we see that $\# \text{Ker } \psi = \# \text{Coker } \psi$. This implies that

$$\# M = \# \tilde{M}.$$

Now consider the short exact sequence

$$0 \longrightarrow R \longrightarrow R \longrightarrow R/(\det \varphi) R \longrightarrow 0$$

where the first map is given by multiplying by $\det \varphi$ and the second map is the natural quotient map. Since $\det \varphi$ is not a zero-divisor, the quotient $R/(\det \varphi) R$ is finite. In the same way, we tensor this short exact sequence over $R$ with $\tilde{R}$. Then, we obtain a commutative diagram to which we also apply the snake lemma and get

$$\# R/(\det \varphi) R = \# \tilde{R}/(\det \varphi) \tilde{R}.$$

The $R$-Fitting ideal of $M$ is generated by $\det \varphi$. By Proposition 2.2(3), the $\tilde{R}$-Fitting ideal of $\tilde{M}$ is also generated by $\det \varphi$. Since $\tilde{R}$ is the product of principal ideal domains,
we have the equality \( \# \widetilde{M} = \# \widetilde{R}/\text{Fit}_R(\widetilde{M}) \) (see Example 2.3). Therefore, the equality \( \# M = \# R/\text{Fit}_R(M) \) follows, as required.

**Case 2:** Suppose \( \dim_{F_q}(K/m) > t \).

Consider the short exact sequence (4.1). By Proposition 4.1 the \( R \)-module \( K \) is not free. Hence, by Proposition 4.2 the \( R \)-ideal \( \text{Fit}_R(M) \) is not a principal ideal. We have the following equalities.

\[
\# \widetilde{M} = \# \widetilde{R}/\text{Fit}_R(\widetilde{M}) \quad \text{by Example 2.3},
\]
\[
= \# \widetilde{R}/\text{Fit}_R(M) \bar{R} \quad \text{by Proposition 2.2(3)},
\]
\[
= \# \widetilde{R}/\text{Fit}_R(M) \quad \text{by Proposition 3.6},
\]
\[
= \# \widetilde{R}/R \cdot \# R/\text{Fit}_R(M)
\]
\[
= q \cdot \# R/\text{Fit}_R(M).
\]

Thus, to show that \( \# M \leq \# R/\text{Fit}_R(M) \), it is enough to show \( q \cdot \# M \leq \# \widetilde{M} \). Let \( N \) and \( N' \) be the finite \( R \)-modules fitting into an sequence

\[
0 \rightarrow N \rightarrow M \xrightarrow{\psi} \widetilde{M} \rightarrow N' \rightarrow 0
\]

with the natural map \( \psi \). Applying the snake lemma to (4.2) then yields the exact sequence of \( F_q \)-vector spaces (see Proposition 4.3).

\[
0 \rightarrow N \rightarrow H/K \rightarrow F_q^t \rightarrow N' \rightarrow 0.
\]

It follows that

\[
\# \widetilde{M}/\# M \cdot \# H/K = q^t.
\]

Hence, to show that \( q \cdot \# M \leq \# \widetilde{M} \), we only need to show that \( \# H/K < q^t \). By Proposition 4.3, we have

\[
mH \subset K \subset H.
\]

Since \( mH = m\widetilde{R}K \), we have \( mH = mK \) by Proposition 3.6. Thus, we have \( [K : mH] = [K : mK] \), which is greater than \( q^t \) by assumption. By Proposition 4.4, the order of \( H/mH \) is equal to \( q^{2t} \). Therefore, the equality

\[
\# H/mH = \# H/K \cdot \# K/mK
\]

implies that \( \# H/K < q^t \). Hence, the theorem follows.

**REFERENCES**

[1] Buchmann, A. J. and Lenstra, H. W., *Approximating rings of integers in number fields*, Journal de Théorie des Nombres de Bordeaux 6 (1994), 221–260.

[2] Grothendieck, A. and Dieudonné J., *EGA IV4 Etude locale des schémas et des morphismes de schémas*, Publ. Math. IHES 32 (1967).

[3] Lang, S., *Algebra*, Graduate Texts in Mathematics 211 (2002), Springer.

[4] Matsumura, H., *Commutative ring theory*, Cambridge studies in advanced mathematics 8 (1986), Cambridge University Press.