ON THE COHOMOLOGY OF $GL_N(F_P)$ WITH F_P COEFFICIENTS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for

the Degree Doctor of Philosophy in the Graduate

School of the Ohio State University

By

Adrian G. Barbu, MS

* * * * *

The Ohio State University
2000

Dissertation Committee:

Avner Ash, Advisor

Warren Sinnott

Ronald Solomon

Gordon J. Aubrecht

Approved by

Advisor
Department Of Mathematics

ABSTRACT

In this thesis we will develop some tools that can be used to get a better understanding of the cohomology of $GL_n(\mathbb{F}_p)$ with $\mathbb{F}_p$ coefficients. First we study the cohomology of $U_n(\mathbb{F}_p)$, one of the p-Sylow subgroups of $GL_n(\mathbb{F}_p)$. We compute all the relations satisfied by those elements of $H^*(U_n)$ of degree two which come from the $\mathbb{Z}$ cohomology.

Then we define elements that generate a subring of the same dimension as the entire cohomology ring $H^*(U_n, \mathbb{F}_p)$. After that we concentrate on U_4 and compute all the maximal elementary abelian subgroups and, using them, all relations among the above elements, modulo nilpotents.

We then look at tools useful in finding what part of $H^*(U_n, \mathbb{F}_p)$ survives in $H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$. We compute the Hecke algebra $H(GL_n//U_n)$ and part of its action on $H^*(U_n, \mathbb{F}_p)$. We also prove a particular case of a conjecture of Ash concerning Hecke eigenclasses and Galois representations.

In the last chapter, we define a new class in $H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$ of small degree $2p-2$. This class has not been discovered until now, and we prove that it is non-zero if $p \geq n$. We conjecture that the $\mathbb{F}_p$ cohomology of $GL_n(\mathbb{F}_p)$ is zero in degrees less than $2p-3$.

to my mother, Lucia Barbu

ACKNOWLEDGMENTS

I would first like to thank my advisor, for his patience and enthusiasm in working with me, and for his precious observations and advice.

I would also like to thank Professors Alejandro Adem, Ron Solomon, N. Yagita, Zbigniew Fiedorowicz and Mark Reeder for answering all the questions that I had.

VITA

1971	Born in Sighetu Marmatiei, Romania
1995	BS in mathematics, Univ. of Bucharest, Romania
1995-present	graduate studies at Ohio State University. Research in cohomology of $GL_n(\mathbb{F}_p)$ with $\mathbb{F}_p$ coefficients, under the supervison of Prof. Avner Ash.

PUBLICATIONS

The ring generated by the elements of degree 2 in $H^*(U_n(\mathbb{F}_p), \mathbb{Z})$ - submitted for publication

Complete and Henselian Fields -Thesis, University of Bucharest, 1995

FIELDS OF STUDY

Major field: Mathematics

Specialization: Number Theory, Group Cohomology

Studies in	Elliptic Curves	Karl Rubin
	Fermat's Last Theorem	Avner Ash
	Group Cohomology	Avner Ash

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The numbers have been a fascination for human kind from the earliest ages. The arabs have developed the system of numeration as we have it today. The natural numbers are the numbers with which we count objects $(1, 2, 3, \dots)$. They have no decimals.

The Egyptians knew several triplets of natural numbers two of which are the sides of a rectangle and the third is the length of the diagonal. If we suppose that a, b are the lengths of the sides and c is the length of the diagonal, this can be written as:

$$a^2 + b^2 = c^2$$

For example $3, 4, 5$ are such natural numbers since

$$3^2 + 4^2 = 5^2$$

Then people asked if such numbers a, b, c exist when the power is not 2, but 3 or 4, or even bigger. This way one of the most famous problems in mathematics was born (stated by Fermat in 1670):

Theorem 1.1. *Let $n \geq 3$ be a natural number. There are no non-zero natural numbers a, b, c such that*

$$a^n + b^n = c^n$$

Though it seems so simple to state and understand, this problem could not be solved in its entire generality for more than 300 years. It has been proven to be true for some numbers n (first 4, then 3 and 5, etc), but it couldn't be proven to be true for *all* n. This was finally done in 1995 by Andrew Wiles.

While mathematicians were trying to solve this problem, they found it necessary to develop a lot of mathematical tools, which we know today as Number Theory. Number Theory is perhaps the most complex part of mathematics, because it uses results from all other fields of mathematics: Algebraic Geometry, Group Cohomology, Complex Analysis, Algebra, etc.

Nearly unbreakable codes for transactions over the Internet are the result of the advances in Number Theory.

The development of Number Theory catalyzed spectacular advances in the fields of mathematics described above.

One of the tools used by Number Theory is Representation Theory. This allows the mathematicians to see facts about a mathematical object (group, ring) by embedding it, or part of it, in another, more general object, whose properties can be easier understood.

The object most commonly used in Number Theory to embed in is $GL_n(K)$, the group of invertible matrices with coefficients in some field K.

A group is an abstract object whith one operation (like the addition or multiplication), a neutral element (like 0 and 1, respectively) and an inverse for every element in the group. An example of group is the set of integers (the natural numbers with 0, together with their negatives, like $-1, -2$, etc.), the operation being the

addition. Another example is the set consisting of 1 and -1 with the operation being multiplication.

There exist groups in which if one multiplies a with b *in that order* one gets a different result than when multiplying b with a. Such groups ar called non-commutative groups. $GL_n(K)$ is an example of a non-commutative group.

Non-commutative groups are used in the design of VLSI integrated circuits, in particular in the design of microprocessors.

A matrix is a square array of elements from some set. The set must have addition and multiplication, in order to be able to make a group out of those matrices. In our case that set is the field K.

Matrices are used in business, in technology to describe industrial processes, in computer graphics and computer aided design (CAD) to rotate and move images, and in quantum mechanics.

The bigger the n (the dimension of the matrix) the more complicated the group $GL_n(K)$. Also, when K is an finite field, $GL_n(K)$ is more complicated than when K is an infinite field like $\mathbb{R}$, the field of real numbers, or $\mathbb{C}$, the field of complex numbers.

An example of a finite field is the set of natural numbers from 0 to 6, with the usual addition and multiplication, and if the result of addition or multiplication is bigger than 6, we reduce it modulo 7. This field is called $\mathbb{F}_7$, the field with 7 elements. Similarly, for any prime number p, one can construct the field $\mathbb{F}_p$ with p elements.

In finite fields everything is contorted and a lot of irregular things happen, as opposed to what happens when we work with nice smooth fields like $\mathbb{R}$ and $\mathbb{C}$. If we

knew the properties of all $GL_n(K)$ for finite K, then we could make great advances in Number Theory.

But what properties of $GL_n(K)$ are worthy to be known? Usually the properties are measured by some numbers or some structures associated with our objects, which describe its behavior when interacting with other objects.

One of the main tools for extracting essential properties of an object is called Cohomology. Cohomology is like a set of small simple machines, which are useful by themselves, but they are all interacting with each other, making them more useful as an ensemble. Like the transistors in a computer, each of them is simple, but together they make up the complex and much more useful machinery the computer is.

Through cohomology we can associate numbers with geometric objects which help us distinguish them from each other. Although it seems obvious that a sphere and a donut are different, cohomology gives a mathematical technique for distinguishing them, which can then be used for distinguishing much more complicated objects, perhaps in higher dimensions. The objects in higher dimensions cannot be visualized by us. Cohomology can also help identify an unknown object when you only are given certain of its properties, as long as those properties are enough to find its cohomology.

Another byproduct of cohomology is the following interesting theorem:

Theorem. *There is always a place on Earth where there is no wind!*

This is not just a poetic phrase but a proven mathematical fact. Such a result could not be proved just by using the cohomological numbers described above. A finer structure must be obtained.

As in geometry, cohomology exhibits some essential properties of $GL_n(K)$. But this cohomology is not the cohomology of geometric objects, but the *cohomology of groups*.

In this paper we will study the cohomology of $GL_n(\mathbb{F}_p)$ with $\mathbb{F}_p$ coefficients. This cohomology has not been calculated to date except for $n \leq 3$.

The cohomology of $GL_2(\mathbb{F}_p)$ was computed by Aguadé in [Agu].

The cohomology $H^*(GL_3(\mathbb{F}_p), \mathbb{Z})_{(p)}$ was computed by Tezuka and Yagita in [TY1].

There are also complete results about $GL_4(\mathbb{F}_2)$ (in [TY2]). I have found out from Jim Milgram that considerable progress has been done in computing the cohomology of $GL_5(\mathbb{F}_2)$.

In [Qu], Quillen computed the cohomology of $GL_n(\mathbb{F}_p)$ with $\mathbb{F}_l$ coefficients for $l \neq p$ and he stated that the case $l = p$ is very difficult.

In general (see [Brn], chapter III, Theorem 10.3), the p-part of the cohomology of a finite group G can be computed from the cohomology of one of its p-Sylow subgroups H, by finding the G-invariant elements of $H^*(H)$. One way to prove that an element is G-invariant is by proving that the Hecke operators act *punctually* on it (i.e., every Hecke operator acts as multiplication by its degree). The $\mathbb{F}_p$ cohomology of $GL_n(\mathbb{F}_p)$ can therefore be computed, at least in principle, from the cohomology of one of its p-Sylow subgroups, for example $U_n(\mathbb{F}_p)$, the group of upper triangular matrices of $GL_n(\mathbb{F}_p)$ with 1 on the diagonal. Then, also in principle, by finding the action of the whole Hecke algebra $H(GL_n(\mathbb{F}_p)//U_n)$ on $H^*(U_n)$, we can find the $GL_n(\mathbb{F}_p)$-invariant elements.

Lewis computed the integral cohomology of $U_3(\mathbb{F}_p)$ in [Lew]. Tezuka and Yagita

used Lewis's result to find the cohomology of $GL_3(\mathbb{F}_p)$ by computing the GL_3-invariant elements. We see therefore that it is useful to compute the cohomology of $U_n(\mathbb{F}_p)$ with $\mathbb{Z}$ or $\mathbb{F}_p$ coefficients.

Leary computed $H^*(U_3(\mathbb{F}_p), \mathbb{F}_p)$ in [Lry].

In the Chapter 2 we will compute all the relations satisfied by those elements of $H^*(U_n)$ of degree two that come from the $\mathbb{Z}$ cohomology. The main theorem we prove is the following:

Theorem. *Let $G = U_{n+1}(\mathbb{F}_p)$ and $p \geq n+1$. The ring generated by the elements of $H^2(G, \mathbb{Z})$ in $H^*(G, \mathbb{Z})$ is isomorphic to:*

$$\mathbb{Z}[X_1, \ldots, X_n]'/(X_1^p X_2 - X_2^p X_1, X_2^p X_3 - X_3^p X_2, \ldots, X_{n-1}^p X_n - X_n^p X_{n-1})$$

where $\mathbb{Z}[X_1, \ldots, X_n]' = \mathbb{Z}[X_1, \ldots, X_n]/(pX_1, \ldots, pX_n)$.

In Chapter 3 we define elements that generate a subring of the same dimension as the entire cohomology ring $H^*(U_n, \mathbb{F}_p)$. This has also been done in [TY2], but our elements have smaller degree.

After that, in Chapter 4, we concentrate on U_4 and compute all the maximal elementary abelian subgroups. Then in Chapter 5, we find all relations among the elements defined in Chapter 3 for U_4, modulo nilpotents. We will give the ideal of relations as an intersection of 4 ideals, since it has too many generators to list directly. In [Ya], the author computes the cohomology of U_4 after inverting some cohomology classes.

In Chapter 6 we compute the Hecke algebra $H(GL_n//U_n)$. In order to get a better understanding of the Hecke action, in Chapter 8 we will find some extra properties

of the transfer map and the Hecke operators, which are not in the literature as far as we know.

Perhaps our most interesting results are in Chapters 7 and 9. In Chapter 7, we prove that certain cohomology classes that are eigenvalues for the Hecke operators correspond to Galois representations, verifying in this way a conjecture of Ash relating cohomology classes to Galois representations. More precisely, we prove:

Theorem 1.2. *Let $\beta \in H^*(U, \mathbb{F}_p)$ be an eigenclass for $T_{l,k}$ for all primes $l \neq p$, and all $1 \leq k \leq n$. Then there is an integer d such that the representation*

$$\rho = \omega^d \oplus \omega^{d+1} \oplus ... \oplus \omega^{d+n-1} : G_{\mathbb{Q}} \to GL_n(\mathbb{F}_p), \tag{1.1}$$

where $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, has the property that

$$P(\beta, l) = det(I - \rho(Frob_l)X) \text{ for all } l \neq p.$$

Chapter 8 contains some functorial properties that we will use in Chapter 9. It also contains some interesting new facts about the transfer map and the Hecke operators that we thought are worth mentioning.

In Chapter 9, we construct a new class in $H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$ of degree $2p-2$, not in the literature as far as we know, and we prove that it is nonzero for $p \geq n$. Then we state the following conjecture:

Conjecture 1.3. *If $n \geq 2$ and $p \geq 3$ then*

$$H^k(GL_n(\mathbb{F}_p), \mathbb{F}_p) = 0 \text{ for } k < 2p-3.$$

CHAPTER 2

THE RING GENERATED BY THE ELEMENTS OF DEGREE 2 IN $H^*(U_N(\mathbb{F}_P), \mathbb{Z})$

In this chapter we compute all the relations in cohomology satisfied by the elements of degree two of $H^*(U_n(\mathbb{F}_p), \mathbb{Z})$, where $p \geq n$. That is, we will compute the ring generated by the elements of degree 2 of $H^*(G, \mathbb{Z})$. We will also see that the relations between the images of these elements in $H^*(U_n, \mathbb{F}_p)$ will be the same.

The main theorem we prove in this chapter is the following:

Theorem. *Let $G = U_{n+1}(\mathbb{F}_p)$ and $p \geq n+1$. The ring generated by the elements of $H^2(G, \mathbb{Z})$ in $H^*(G, \mathbb{Z})$ is isomorphic to:*

$$\mathbb{Z}[X_1, \ldots, X_n]'/(X_1^p X_2 - X_2^p X_1, X_2^p X_3 - X_3^p X_2, \ldots, X_{n-1}^p X_n - X_n^p X_{n-1})$$

where $\mathbb{Z}[X_1, \ldots, X_n]' = \mathbb{Z}[X_1, \ldots, X_n]/(pX_1, \ldots, pX_n)$.

We will also prove that this ring is reduced and if an element of this ring restricts to zero in all proper subgroups of G then that element is zero.

Denote

$$R_n = \mathbb{Z}[X_1, \ldots, X_n]' = \mathbb{Z}[X_1, \ldots, X_n]/(pX_1, \ldots, pX_n),$$

$$I_n = (X_1^p X_2 - X_2^p X_1, X_2^p X_3 - X_3^p X_2, \ldots, X_{n-1}^p X_n - X_n^p X_{n-1}) \text{ ideal in } R_n,$$

$$J_k = I_n R_{n+1} + (X_{n+1} - kX_n)R_{n+1},\ k = 0, 1, \ldots, p-1 \text{ ideal in } R_{n+1},$$

$$J_p = I_n R_{n+1} + X_n R_{n+1} \text{ ideal in } R_{n+1},$$

where the corresponding n will be clear from the context.

Some facts about the ring $\mathbb{Z}[X_1, \ldots, X_n]'$

Observe that $R_n = \mathbb{Z}[X_1, \ldots, X_n]'$ differs from $\mathbb{F}_p[X_1, \ldots, X_n]$ only in degree zero. The canonical morphism $\mathbb{Z}[X_1, \ldots, X_n]' \to \mathbb{F}_p[X_1, \ldots, X_n],\ f \to \overline{f}$ establishes an inclusion maintaining bijection between proper ideals in $\mathbb{Z}[X_1, \ldots, X_n]'$ that do not contain constants and proper ideals in $\mathbb{F}_p[X_1, \ldots, X_n]$. This map is injective when restricted to polynomials with no constant term.

Observe also that if $f \in \mathbb{Z}[X_1, \ldots, X_n]'$ is a polynomial with no constant term (in particular if f is nonconstant homogeneous) we can talk about computing the value of $f(a_1, \ldots, a_n)$ for some $a_i \in \mathbb{F}_p$ just by computing $\overline{f}(a_1, \ldots, a_n)$.

All the results in this section work for both $\mathbb{Z}[X_1, \ldots, X_n]'$ and $\mathbb{F}_p[X_1, \ldots, X_n]$. We will only prove them for $\mathbb{Z}[X_1, \ldots, X_n]'$ since we only need them for this ring.

Proposition 2.1. *Let $n \geq 2$. Then the following statements hold:*

(a_n) *If $a_1, \ldots, a_l$ are distinct numbers from the set $\{0, \ldots, p-1\}$, then*

$$I_n R_{n+1} + X_n \prod_{k=1}^{l} (X_{n+1} - a_k X_n) R_{n+1} = J_p \cap \bigcap_{k=1}^{l} J_{a_k}.$$

(b_n) *The natural map*

$$R_{n+1}/I_{n+1} \to \prod_{k=0}^{p} R_{n+1}/J_k$$

is injective.

(c_n) *The ring* R_n/I_n *is reduced.*

Proof. First it is clear that (c_2) is true, that is $\mathbb{Z}[X,Y]'/(X^pY - XY^p)$ is reduced since $X^pY - XY^p$ is a product of $p+1$ distinct linear factors in $\mathbb{Z}[X,Y]'$.

We wil prove that $(c_n) \Longrightarrow (a_n) \Longrightarrow (b_n)$. We will also prove $(c_n) + (c_{n-1}) \Longrightarrow (c_{n+1})$ for $n \geq 3$ and $(c_2) \Longrightarrow (c_3)$. This will imply that $(a_n), (b_n), (c_n)$ are true for all $n \geq 2$.

$(c_n) \Longrightarrow (a_n)$:

We prove this by induction on l. For $l = 0$ it is trivially true. Suppose it is true for l. We prove it for $l+1$. It is clear that

$$I_nR_{n+1} + X_n \prod_{k=1}^{l+1}(X_{n+1} - a_kX_n)R_{n+1} \subset J_p \cap \bigcap_{k=1}^{l+1} J_{a_k}$$

since $X_n \prod_{k=1}^{l+1}(X_{n+1} - a_kX_n)$ is in all the J_{a_k}.

Let now $f \in J_p \cap \bigcap_{k=1}^{l+1} J_{a_k} = (J_p \cap \bigcap_{k=1}^{l} J_{a_k}) \cap (J_p \cap \bigcap_{k=1}^{l-1} J_{a_k} \cap J_{a_{l+1}})$.

By the induction hypothesis we get that:

$$f \in J_p \cap \bigcap_{k=1}^{l} J_{a_k} = I_nR_{n+1} + X_n \prod_{k=1}^{l}(X_{n+1} - a_kX_n)R \quad \text{and}$$

$$f \in J_p \cap \bigcap_{k=1}^{l-1} J_{a_k} \cap J_{a_{l+1}} = I_nR_{n+1} + X_n(X_{n+1} - a_{l+1}X_n) \prod_{k=1}^{l-1}(X_{n+1} - a_kX_n)R_{n+1}.$$

Let $Y = X_{n+1} - a_{l+1}X_n$. Let's work now in

$$R_{n+1}/I_nR_{n+1} = (R_n/I_n)\,[X_{n+1}]/(pX_{n+1}) = (R_n/I_n)\,[Y]/(pY).$$

Then, for each $1 \leq i \leq l$, we have $X_{n+1} - a_iX_n = Y - b_iX_n$ for some $b_i \in \mathbb{F}_p$ (it makes sense to multiply X_n with an element of $\mathbb{F}_p$ since $pX_n = 0$). Observe that for all i, $b_i \neq 0$ since $a_i \neq a_{l+1}$ for all $i \leq l$ and are all less then p. Then in $(R_n/I_n)[Y]/(pY)$ we have:

$$\overline{f} = x_n \prod_{k=1}^{l}(Y - b_kx_n)\; g = x_nY \prod_{k=1}^{l-1}(Y - b_kx_n)\, h \quad \text{for some } g, h \in (R_n/I_n)[Y],$$

where x_n is the image of X_n in R_n/I_n. Suppose $g = u_0 + u_1Y + \dots$ with $u_i \in R_n/I_n$. The coefficient of Y^0 in the middle product above is

$$tx_n^{l+1}u_0 \quad \text{with } t = (-1)^l \prod_{k=1}^{l} b_k \in \mathbb{F}_p^*$$

and on the right hand side is 0. Equating these coefficients we get that $x_n^{l+1}u_0 = 0$, thus $(x_nu_0)^{l+1} = 0$ and since R_n/I_n is reduced (because we supposed (c_n) to be true), we get that $x_nu_0 = 0$. Therefore:

$$\begin{aligned}
\overline{f} &= \prod_{k=1}^{l}(Y - b_kx_n)\; x_ng = \prod_{k=1}^{l}(Y - b_kx_n)(x_nu_0 + x_nu_1Y + \dots) \\
&= x_nY \prod_{k=1}^{l}(Y - b_kx_n)(u_1 + u_2Y + \dots) \\
&= x_n \prod_{k=1}^{l+1}(X_{n+1} - a_kx_n)(u_1 + u_2Y + \dots).
\end{aligned}$$

This shows that $f \in I_nR_{n+1} + X_n \prod_{k=1}^{l+1}(X_{n+1} - a_kX_n)R_{n+1}$ and therefore

$$I_nR_{n+1} + X_n \prod_{k=1}^{l+1}(X_{n+1} - a_kX_n)R_{n+1} = J_p \cap \bigcap_{k=1}^{l+1} J_{a_k}$$

and this proves that (a_n) holds.

$(a_n) \Longrightarrow (b_n)$:

We have the following embedding:

$$R_{n+1}/J_0 \cap \cdots \cap J_p \hookrightarrow \prod_{k=0}^{p} R_{n+1}/J_k.$$

Because (a_n) holds we get that:

$$I_{n+1} = I_n R_{n+1} + X_n \prod_{k=0}^{p-1}(X_{n+1} - kX_n)R_{n+1} = J_0 \cap \cdots \cap J_p$$

and thus (b_n) holds.

$(c_n) + (c_{n-1}) \Longrightarrow (c_{n+1})$ and $(c_2) \Longrightarrow (c_3)$:

Since (c_n) holds, we get from above that (a_n) and (b_n) hold. Therefore we have that

$$R_{n+1}/I_{n+1} \hookrightarrow \prod_{k=0}^{p} R_{n+1}/J_k.$$

Now let's look at the rings on the right.

$$R_{n+1}/J_k \simeq R_n/I_n[X_{n+1}]/(pX_{n+1}, X_{n+1} - kX_n) \simeq R_n/I_n \quad \text{for } k < p,\ n \geq 2, \text{ and}$$

$$R_{n+1}/J_p \simeq R_n/I_n[X_{n+1}]/(pX_{n+1}, X_n) \simeq R_{n-1}/I_{n-1}[X_{n+1}]/(pX_{n+1}) \text{ for } n \geq 3.$$

For $n = 2$ we have:

$$R_{n+1}/J_p \simeq R_n/I_n[X_{n+1}]/(pX_{n+1}, X_n) \simeq \mathbb{Z}[X, Y]'[Z]/(pZ, Y) \simeq \mathbb{Z}[X, Z]'.$$

Thus all $R_{n+1}/J_k, k = 0, \ldots, p-1$ are reduced because we supposed that (c_n) holds, and because of this R_n/I_n and R_{n-1}/I_{n-1} are reduced. If a ring A is reduced, then A[X]/(pX) is also reduced. We see that in case $n = 2$, if we suppose only (c_n)

true, we still get that all $R_{n+1}/J_k, k = 0, \ldots, p$ are reduced. Since a direct product of reduced rings is reduced, the direct product of these rings is reduced. Now R_{n+1}/I_{n+1} is a subring of this direct product, therefore it is reduced. □

Corollary 2.2.

$$I_{n+1} = J_0 \cap \cdots \cap J_p.$$

Proof. This has been proved while proving Prop.2.1. □

Lemma 2.3. $\mathbb{Z}[X_1, \ldots, X_{l-1}, X_{l+1}, \ldots, X_n]' \cap (I_n + X_l R_n) \subset I_n$.

Proof. Let $f \in \mathbb{Z}[X_1, \ldots, X_{l-1}, X_{l+1}, \ldots, X_n]' \cap (I_n + X_l R_n)$.

We have $f(X_1, \ldots, X_{l-1}, X_{l+1}, \ldots, X_n) = a(X_1, \ldots, X_n) + X_l b(X_1, \ldots, X_n)$ with $a \in I_n$. But $a \in I_n$ means:

$$a = (X_1^p X_2 - X_2^p X_1)a_1 + (X_2^p X_3 - X_3^p X_2)a_2 + \cdots + (X_{n-1}^p X_n - X_n^p X_{n-1})a_n$$

for some $a_i \in R_n$. Write $a_i = a_i' + X_l u_i$ where the a_i' do not depend on X_l. We get that

$$\begin{aligned} a = {} & (X_1^p X_2 - X_2^p X_1)a_1' + (X_2^p X_3 - X_3^p X_2)a_2' + \cdots + (X_{l-2}^p X_{l-1} - X_{l-1}^p X_{l-2})a_{l-2}' \\ & + (X_{l+1}^p X_{l+2} - X_{l+2}^p X_{l+1})a_{l+1}' + \cdots + (X_{n-1}^p X_n - X_n^p X_{n-1})a_n' + X_l u \end{aligned}$$

for some $u \in R_n$. Observe that the terms corresponding to a_{l-1} and a_l are now contained in $X_l u$.

We get in this way that $a = a' + X_l u$ with $a' \in \mathbb{Z}[X_1, \ldots, \hat{X_l}, \ldots, X_n]' \cap I_n$ and $u \in R_n$.

Then $f = a' + X_l(b + u)$, and thus $f - a' = X_l(b + u)$.

Since $f - a' \in \mathbb{Z}[X_1, \ldots, \hat{X_l}, \ldots, X_n]'$ does not depend on X_l and $X_l(b+u)$ does, we get that $f - a' = 0$. Remember that $a' \in I_n$, therefore $f = a' \in I_n$. □

Proposition 2.4.

$$\bigcap_{i=1}^{l} (I_n + X_i R_n) = I_n + X_1 \ldots X_l R_n.$$

Proof. Induction on l. The case $l = 1$ is trivial.

The general case: It is clear that $\bigcap_{i=1}^{l} (I_n + X_i R_n) \supset I_n + X_1 \ldots X_l R_n$. To show the other inclusion let $f \in \bigcap_{i=1}^{l} (I_n + X_i R_n)$. Then $f \in \bigcap_{i=1}^{l-1} (I_n + X_i R_n)$ and by the induction hypothesis we get that $f \in I_n + X_1 \ldots X_{l-1} R_n$. Thus $f = a + X_1 \ldots X_{l-1} u = b + X_l v$ (since $f \in I_n + X_l R_n$) with $a, b \in I_n$ and $u, v \in R_n$. Write $u = u_1 + X_l u_2$ with $u_1 \in \mathbb{Z}[X_1, \ldots, X_{l-1}, X_{l+1}, \ldots, X_n]'$ and $u_2 \in R_n$. Then

$$f = a + X_1 \ldots X_{l-1} u_1 + X_1 \ldots X_l u_2 = b + X_l v.$$

This implies that $X_1 \ldots X_{l-1} u_1 \in I_n + X_l R_n$, since all the other terms in the second equality above are in $I_n + X_l R_n$.

But $X_1 \ldots X_{l-1} u_1 \in \mathbb{Z}[X_1, \ldots, X_{l-1}, X_{l+1}, \ldots, X_n]'$.

By the above Lemma, we get that $X_1 \ldots X_{l-1} u_1 \in I_n$ and thus

$$f = a + X_1 \ldots X_{l-1} u_1 + X_1 \ldots X_l u_2 \in I_n + X_1 \ldots X_l R_n.$$

This means that $\bigcap_{i=1}^{l} (I_n + X_i R_n) \subset I_n + X_1 \ldots X_l R_n$ and therefore

$$\bigcap_{i=1}^{l} (I_n + X_i R_n) = I_n + X_1 \ldots X_l R_n.$$

□

Proposition 2.5. *If $f \in I_n + X_1 \dots X_n R_n$ is nonconstant and homogeneous, such that*

$$f(a_1, \dots, a_n) = 0 \quad \forall\ a_1, \dots, a_n \in \mathbb{F}_p$$

then $f \in I_n$.

Proof. Write $f = a + X_1 \dots X_n u$, with $a \in I_n, u \in R_n$. Then, since a vanishes on $\mathbb{F}_p^n$ (because $a \in I_n$), it is enough to prove that if $X_1 \dots X_n u$ vanishes on all $\mathbb{F}_p^n$, then $X_1 \dots X_n u \in I_n$. Suppose therefore that

$$f = X_1 \dots X_n u \text{ with } u \in R_n.$$

We will prove by induction on n that $f \in I_n$.

Case $n = 2$: Let $f \in \mathbb{Z}[X, Y]'$ be homogeneous, divisible by XY and $f(a, b) = 0$ for all $a, b \in \mathbb{F}_p$. Since f is homogeneous, then $f(X, Y) = Y^d g(X/Y)$ for some $g \in \mathbb{Z}[X]'$ and $d = \deg\ f$. This implies that $g(a) = 0$ for all $a \in \mathbb{F}_p$. Therefore g is divisible by $X - a$ for all $a \in \mathbb{F}_p$ thus g is divisible by $X^p - X$. From this we get that f is divisible by $X^p Y - X Y^p$ and case $n = 2$ is proved.

The general case: Write

$$\begin{aligned} u = u_1 + (X_n - X_{n-1})u_2 + (X_n - X_{n-1})(X_n - 2X_{n-1})u_3 + \dots + \\ + (X_n - X_{n-1}) \dots (X_n - (p-1)X_{n-1})u_p, \end{aligned} \tag{2.1}$$

with $u_1, \dots, u_{p-1} \in R_{n-1}$ and $u_p \in R_n$. We can do that because we can write

$$u = a_1 + X_n a_2 + X_n^2 a_3 + \dots + X_n^{p-1} a_p \quad \text{ with } a_1, \dots, a_{p-1} \in R_{n-1}, a_p \in R_n$$

(we work now in $R_n = R_{n-1}[X_n]/(pX_n)$) and $1, X_n, X_n^2, \dots, X_n^{p-1}$ are combinations of $1, (X_n - X_{n-1}), (X_n - X_{n-1})(X_n - 2X_{n-1}), \dots, (X_n - X_{n-1}) \dots (X_n - (p-1)X_{n-1})$

with coefficients in R_{n-1}. This is true because the matrix which takes the elements $\{1, X_n, X_n^2, \ldots, X_n^{p-1}\}$ to $\{1, (X_n - X_{n-1}), (X_n - X_{n-1})(X_n - 2X_{n-1}), \ldots, (X_n - X_{n-1}) \ldots (X_n - (p-1)X_{n-1})\}$ is lower triangular with 1 on the diagonal. This implies that the matrix (which has coefficients in R_{n-1}) is invertible and the inverse has also coeficients in R_{n-1}. The inverse matrix writes $1, X_n, X_n^2, \ldots, X_n^{p-1}$ as combinations of $1, (X_n - X_{n-1}), (X_n - X_{n-1})(X_n - 2X_{n-1}), \ldots, (X_n - X_{n-1}) \ldots (X_n - (p-1)X_{n-1})$ with coefficients in R_{n-1}.

Then from (2.1) we get

$$\begin{aligned} f = X_1 \ldots X_n u_1 + X_1 \ldots X_n (X_n - X_{n-1}) u_2 + \cdots + \\ + X_1 \ldots X_n (X_n - X_{n-1}) \ldots (X_n - (p-2)X_{n-1}) u_{p-1} + \\ + X_1 \ldots X_{n-1} (X_n^p X_{n-1} - X_n X_{n-1}^p) u_p. \end{aligned} \tag{2.2}$$

Observe that the last term in the above expression belongs to I_n and therefore is zero for all values of the X_i in $\mathbb{F}_p$. Let now $X_1, \ldots, X_{n-1}$ take any non-zero values in $\mathbb{F}_p$ and fix them. Let a be the value of X_{n-1}. Let X_n take the values $a, 2a, \ldots, (p-1)a$. Because $X_1, \ldots, X_{n-1}$ take some fixed values in $\mathbb{F}_p$, it follows that $u_1, \ldots, u_{p-1}$ also take some fixed values in $\mathbb{F}_p$. From (2.2) we get the following system of $p-1$ equations:

$$\begin{gathered} a u_1 = 0, \\ 2a u_1 + 2a^2 u_2 = 0, \\ \cdots \\ (p-1) a u_1 + (p-1)(p-2) a^2 u_2 + \cdots + (p-1)(p-2) \ldots (1) a^{p-1} u_{p-1} = 0, \end{gathered}$$

with the $p-1$ unknowns $au_1, a^2u_2, \ldots, a^{p-1}u_{p-1}$. Since the determinant of this system is clearly non-zero, and $a \neq 0$, we get that

$$u_1(x_1, \ldots, x_{n-1}) = 0,$$

$$u_2(x_1, \ldots, x_{n-1}) = 0,$$

$$\ldots$$

$$u_{p-1}(x_1, \ldots, x_{n-1}) = 0,$$

for all $x_1, \ldots, x_{n-1} \in \mathbb{F}_p^*$.

Considering now $x_1, \ldots, x_{n-1} \in \mathbb{F}_p$, we still get that

$$x_1 \ldots x_{n-1}u_1(x_1, \ldots, x_{n-1}) = 0,$$

$$x_1 \ldots x_{n-1}u_2(x_1, \ldots, x_{n-1}) = 0,$$

$$\ldots$$

$$x_1 \ldots x_{n-1}u_{p-1}(x_1, \ldots, x_{n-1}) = 0.$$

By the induction hypothesis, we obtain

$$X_1 \ldots X_{n-1}u_1, \ldots, X_1 \ldots X_{n-1}u_{p-1} \in I_{n-1} \subset I_n.$$

By formula (2.2), this means that $f \in I_n$. □

The Main Theorem

Let $G = U_{n+1}(\mathbb{F}_p)$ be the group of upper triangular matrices with 1 on the diagonal, with $n \geq 3$. Let's suppose that $p \geq n+1$ so that any matrix $A \in G$ has order p,

since a matrix A from G satisfies $(A-I)^{n+1}=0$ therefore $(A-I)^p=0$ so $A^p-I=0$ since we are in characteristic p. Thus $A^p=I$ for all $A\in G$.

We want to determine the part of the cohomology ring $H^*(G,\mathbb{Z})$ generated by the elements of degree 2. This part is a subring, let's denote it by R or $R(G)$. We work only in the even cohomology.

We know that $H^2(G,\mathbb{Z})\simeq Hom(G,\mathbb{Q}/\mathbb{Z})$. Therefore any $\alpha\in H^2(G,\mathbb{Z})$ corresponds to a map $\alpha':G\to\mathbb{Q}/\mathbb{Z}$, which clearly factors through $[G,G]$, since $\mathbb{Q}/\mathbb{Z}$ is abelian. Also, since any element of G has order p, any $\alpha':G\to\mathbb{Q}/\mathbb{Z}$ factors through $\mathbb{Z}/p$ in the sense that there is $\alpha'':G\to\mathbb{Z}/p$ such that $\alpha'=u\circ\alpha''$ with $u:\mathbb{Z}/p\to\mathbb{Q}/\mathbb{Z},\ u(\hat{x})=x/p$. Therefore $H^2(G,\mathbb{Z})\simeq Hom(G/[G,G],\mathbb{Z}/p)$.

We also have the following group homomorphism:

$$G\xrightarrow{\phi}(\mathbb{Z}/p)^n, \tag{2.3}$$

which takes a matrix to the vector consisting of the elements immediately above the main diagonal. The kernel of this map is exactly $[G,G]$. Thus

$$H^2(G,\mathbb{Z})\simeq Hom(G,\mathbb{Q}/\mathbb{Z})\simeq Hom(G,\mathbb{Z}/p)\simeq Hom((\mathbb{Z}/p)^n,\mathbb{Z}/p).$$

We see now that $H^2(G,\mathbb{Z})$ is a $\mathbb{Z}/p$ vector space of dimension n, generated by $\alpha_1,\ldots,\alpha_n$, where α_i corresponds to the i-th projection from $(\mathbb{Z}/p)^n$ to $\mathbb{Z}/p$, thus $\alpha_l(A)=\hat{a}_{l,l+1}$, where $A=(\hat{a}_{ij})\in G$. This implies that $R(G)=\mathbb{Z}[\alpha_1,\ldots,\alpha_n]$, the ring generated by $\alpha_1,\ldots,\alpha_n$.

Looking at the even cohomology and taking into account that $H^*((\mathbb{Z}/p)^n, \mathbb{Z})$ contains a subgroup $\mathbb{Z}[X_1, \ldots, X_n]'$ where the X_i correspond to the projections, we get from (2.3) the following ring homomorphism:

$$\mathbb{Z}[X_1, ..., X_n]' \xrightarrow{\phi^*} R(G)$$

and $\phi^*(X_i) = \alpha_i$. Therefore ϕ^* is surjective. Let $J = ker(\phi^*)$. This is an ideal in $R_n = \mathbb{Z}[X_1, ..., X_n]'$.

We will prove

Theorem 2.6. *In the above situation, $J = I_n$, thus $R(G) = R_n/I_n$. This means that the ring generated by the elements from $H^2(G, \mathbb{Z})$ in $H^*(G, \mathbb{Z})$ is isomorphic to:*

$$\mathbb{Z}[X_1, \ldots, X_n]'/(X_1^p X_2 - X_2^p X_1, X_2^p X_3 - X_3^p X_2, \ldots, X_{n-1}^p X_n - X_n^p X_{n-1}).$$

To prove this we need the following proposition:

Proposition 2.7. *a) $I_n \subset J$.*

b) J is a homogeneous ideal.

c) If $f \in J$ is a non-constant homogeneous polynomial, then $f(a_1, ..., a_n) = 0$ for all $a_1, ..., a_n \in \mathbb{F}_p$.

Proof of the Proposition. a) Let $1 \leq l \leq n-1$ be fixed. We need to prove that $X_l^p X_{l+1} - X_l X_{l+1}^p \in J$. There exists the following group homomorphism:

$$G \xrightarrow{\pi} U_3,$$

$$(a_{ij}) \to \begin{pmatrix} 1 & a_{l,l+1} & a_{l,l+2} \\ 0 & 1 & a_{l+1,l+2} \\ 0 & 0 & 1 \end{pmatrix}.$$

In cohomology, this homomorphism becomes the following ring homomorphism:

$$H^*(U_3) \xrightarrow{\pi^*} H^*(G).$$

On $H^2(\cdot)$ π^* is just:

$$Hom(U_3, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\pi^*} Hom(G, \mathbb{Q}/\mathbb{Z}),$$

$$\xi \to \pi \circ \xi.$$

We get that:

$$\pi^*(\alpha) = \alpha_l,$$

$$\pi^*(\beta) = \alpha_{l+1},$$

where

$$\alpha : U_3 \to \mathbb{Q}/\mathbb{Z}, \qquad \beta : U_3 \to \mathbb{Q}/\mathbb{Z},$$

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \to a/p, \qquad \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \to b/p.$$

Restricting π^* to the ring generated by the elements from H^2, we get:

$$R(U_3) \xrightarrow{\pi^*} R(G).$$

Now from [Lew], we know that $R(U_3) = \mathbb{Z}[\alpha, \beta] = \mathbb{Z}[X, Y]'/(X^pY - XY^p)$. Thus the map π^* is in fact:

$$\mathbb{Z}[\alpha, \beta] \xrightarrow{\pi^*} \mathbb{Z}[\alpha_1, \ldots, \alpha_n],$$

$$\alpha \to \alpha_l, \beta \to \alpha_{l+1}.$$

Since in $\mathbb{Z}[\alpha, \beta]$ there is the relation $\alpha^p\beta - \alpha\beta^p = 0$, through π^* we get the relation $\alpha_l^p\alpha_{l+1} - \alpha_l\alpha_{l+1}^p = 0$ in $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. This means that $X_l^p X_{l+1} - X_l X_{l+1}^p \in J$, therefore $I_n \subset J$.

b) We have the map:

$$\mathbb{Z}[X_1, \ldots, X_n]' \xrightarrow{\phi^*} R(G),$$

$$X_i \to \alpha_i.$$

This map is a graded ring homomorphism, therefore the kernel J is a homogeneous ideal.

c) Let $f \in J \subset \mathbb{Z}[X_1, \ldots, X_n]'$ be a non-constant homogeneous polynomial. Clearly $f(0, \ldots, 0) = 0$.

Let $(a_1, \ldots, a_n) \in \mathbb{F}_p^n - (0, \ldots, 0)$. We have to prove $f(a_1, \ldots, a_n) = 0$.

Let H be the subgroup generated by the matrix

$$A = \begin{pmatrix} 1 & a_1 & 0 & \ldots & 0 \\ 0 & 1 & a_2 & \ldots & 0 \\ & & \ldots & & \\ 0 & 0 & \ldots & 1 & a_n \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Since A has order p ($A \neq I$), we get that $H \simeq \mathbb{Z}/p$. Let $i : H \hookrightarrow G$ be the inclusion of H into G. In cohomology we get $i^* : H^*(G) \to H^*(H)$ and on $H^2(\cdot)$ it is:

$$i^* : Hom(G, \mathbb{Z}/p) \to Hom(H, \mathbb{Z}/p),$$

$$\phi \to \phi|_H$$

since we see that any homomorphism from H to $\mathbb{Q}/\mathbb{Z}$ factors through $\mathbb{Z}/p$. Observe that $Hom(H, \mathbb{Z}/p) \simeq \mathbb{Z}/p$ and is generated by $\alpha : H \to \mathbb{Z}/p,\ A^i \to \hat{i}$. Then

$$i^*(\alpha_j)(A) = \alpha_j|_H(A) = \alpha_j(A) = \hat{a}_j,$$

therefore $i^*(\alpha_j) = a_j\alpha$.

Now restricting i^* to the ring generated by the α_i we get the ring morphism i^* from the following diagram:

$$\mathbb{Z}[X_1, \ldots, X_n]' \xrightarrow{\phi^*} \mathbb{Z}[\alpha_1, \ldots, \alpha_n] \xrightarrow{i^*} \mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]'.$$

Let's call the composition map ψ. We have that $\psi(X_i) = a_iX$; therefore

$$\psi(f(X_1, \ldots, X_n)) = f(a_1X, \ldots, a_nX) = X^d f(a_1, \ldots, a_n)$$

since f is homogeneous of some degree $d > 0$. Now if $f \in J$ then $\phi^*(f) = 0$, therefore $\psi(f) = 0$ so $X^d f(a_1, \ldots, a_n) = 0$, which can only happen when

$$f(a_1, \ldots, a_n) = 0 \quad (\text{remember } f(a_1, \ldots, a_n) \in \mathbb{F}_p).$$

□

Proof of the Theorem. We will prove this by induction on n. The case $n = 2$ has been done by Lewis in [Lew]. Let's suppose the theorem is true for all $l \leq n-1$ and prove it for n.

We want first to prove that $J \subset I_n + X_lR_n$ for all $1 \leq l \leq n$. Let H_l be the subgroup of G consisting of the matrices of the form

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

with $A \in U_l$ and $B \in U_{n+1-l}$. It is easy to check now that H_l is a subgroup of G. Let H_l' be the subgroup of H_l consisting of matrices of the form

$$\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix},$$

with $A \in U_l$. Let also H_l'' be the subgroup of H_l consisting of matrices of the form

$$\begin{pmatrix} I & 0 \\ 0 & B \end{pmatrix},$$

with $B \in U_{n+1-l}$. We see that:

$$H_l \simeq H_l' \times H_l'' \simeq U_l \times U_{n+1-l}.$$

Now looking at the inclusion map $i : H_l \hookrightarrow G$ in cohomology we get:

$$H^*(G) \xrightarrow{i^*} H^*(H_l) \simeq H^*(H_l' \times H_l''), \tag{2.4}$$

which on H^2 is

$$\begin{aligned} Hom(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{i^*} Hom(H_l, \mathbb{Q}/\mathbb{Z}) &\simeq Hom(H_l', \mathbb{Q}/\mathbb{Z}) \times Hom(H_l'', \mathbb{Q}/\mathbb{Z}) \\ \phi \longrightarrow &(\phi|_{H_l'}, \phi|_{H_l''}). \end{aligned}$$

Now we have that

$$i^*(\alpha_j) = \begin{cases} 0 & \text{if } j = l \\ \alpha_j & \text{if } j \neq l. \end{cases}$$

Restricting now (2.4) to the ring generated by $\alpha_1, \ldots, \alpha_n$ we get, since $R(H_l') = \mathbb{Z}[\alpha_1, \ldots, \alpha_{l-1}]$ and $R(H_l'') = \mathbb{Z}[\alpha_{l+1}, \ldots, \alpha_n]$, that

$$\begin{aligned}\mathbb{Z}[X_1, \ldots, X_n]'/J \simeq R(G) \xrightarrow{i^*} R(H_l) \simeq R(H_l') \otimes R(H_l'') \simeq \\ \simeq \mathbb{Z}[X_1, \ldots, X_{l-1}]'/I_{l-1} \otimes \mathbb{Z}[X_{l+1}, \ldots X_n]'/(X_{l+1}^p X_{l+2} - X_{l+1} X_{l+2}^p, \ldots) \simeq \\ \simeq \mathbb{Z}[X_1, \ldots, \hat{X_l}, \ldots, X_n]'/(I_{l-1} + (X_{l+1}^p X_{l+2} - X_{l+1} X_{l+2}^p, \ldots)) = \\ = \mathbb{Z}[X_1, \ldots, X_n]'/(I_n + X_l R_n),\end{aligned}$$

and we see that this composition takes the image of X_j in $\mathbb{Z}[X_1, \ldots, X_n]'/J$ to the image of X_j in $\mathbb{Z}[X_1, \ldots, X_n]'/(I_n + X_l R_n)$ for all $j = 1, \ldots, n$. This shows that $J \subset I_n + X_l R_n$. By prop. 2.4 we get

$$J \subset \bigcap_{i=1}^{n} (I_n + X_i R_n) = I_n + X_1 \ldots X_n R_n.$$

By prop. 2.7 , J is generated by homogeneous elements. Take any $f \in J$, homogeneous. Then, by what we proved above, $f \in I_n + X_1 \ldots X_n R_n$ and from prop. 2.7, $f(a_1, ..., a_n) = 0$ for all $a_1, ..., a_n \in \mathbb{F}_p$. Now from Prop.2.5 we see that $f \in I_n$. This means that $J \subset I_n$. But we saw that $I_n \subset J$, and therefore $J = I_n$. □

Corollary 2.8. *R(G) is reduced.*

Proof. It is clear from the above theorem and what was proved in the section "Some facts about the ring $\mathbb{Z}[X_1, \ldots, X_n]'$". □

Corollary 2.9. *If $f(\alpha_1, \ldots, \alpha_n) \in H^{2d}(G)$ is such that its restriction to any proper subgroup H of G is zero, then $f(\alpha_1, \ldots, \alpha_n) = 0$.*

Proof. First we restrict $f(\alpha_1, \ldots, \alpha_n)$ to all H_l's from the proof of the theorem. From these restrictions we get that $f(X_1, \ldots, X_n) \in I_n + X_l R_n$ for all $l \leq n$; therefore

$$f(X_1, \ldots, X_n) \in \cap_{l=1}^{n} (I_n + X_l R_n) = I_n + X_1 \ldots X_n R_n.$$

But now restricting to the subgroups H that appeared in the proof of c) of prop. 2.7, we get that $f(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in \mathbb{F}_p$. These two facts imply that $f \in I_n$ which means $f(\alpha_1, \ldots, \alpha_n) = 0$. □

Corollary 2.10. *If $G = U_{n+1}$, the ring generated by the image of $H^2(G, \mathbb{Z})$ via the reduction mod p map $H^*(G, \mathbb{Z}) \to H^*(G, \mathbb{F}_p)$ is isomorphic to*

$$\mathbb{F}_p[X_1, \ldots, X_n]/(X_1^p X_2 - X_2^p X_1, X_2^p X_3 - X_3^p X_2, \ldots, X_{n-1}^p X_n - X_n^p X_{n-1}).$$

Proof. It is clear that this ring is of the form

$$\mathbb{F}_p[X_1, \ldots, X_n]/J,$$

for some homogeneous ideal J. Observe that prop. 2.7 holds for J, as it can be verified easily.

We then proceed by an induction argument similar to the proof of thm. 2.6.

The initial step $n = 2$ has been done by Leary in [Lry].

For the general case, we restrict to the same subgroups H_l as in the proof of thm. 2.6. Like there, we have $i^*(\alpha_j) = \delta_{jl}\ \alpha_j$ and then restricting i^* to the ring generated by the α_j we get $J \subset I_n + (X_l)$ and by using prop. 2.4 and prop. 2.7 we get the result. □

Remark 2.1. a) For any group G, from the exact sequence:

$$1 \to \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \to \mathbb{Z}/p \to 1$$

we obtain a long exact sequence

$$... \to H^i(G, \mathbb{Z}) \xrightarrow{\cdot p} H^i(G, \mathbb{Z}) \to H^i(G, \mathbb{Z}/p) \xrightarrow{\beta} H^{i+1}(G, \mathbb{Z}) \xrightarrow{\cdot p} ...$$

b) From the exact sequence:

$$1 \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \xrightarrow{\pi} \mathbb{Z}/p \to 1$$

we obtain a long exact sequence

$$... \to H^i(G, \mathbb{Z}/p) \to H^i(G, \mathbb{Z}/p^2) \xrightarrow{\pi} H^i(G, \mathbb{Z}/p) \xrightarrow{\delta} H^{i+1}(G, \mathbb{Z}/p) \to ...$$

c) From the exact sequence:

$$1 \to \mathbb{Z} \to \mathbb{Q} \xrightarrow{\pi} \mathbb{Q}/\mathbb{Z} \to 1$$

we obtain the exact sequence

$$H^1(G, \mathbb{Q}) \xrightarrow{\pi} H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}) \to H^2(G, \mathbb{Q})$$

and since $H^i(G, \mathbb{Q}) = 0$ for $i \geq 1$ ($\mathbb{Q}$ being divisible group and G being finite) we get $H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq H^2(G, \mathbb{Z})$.

The maps β, δ above are called Bocksteins. δ is obtained by composing β with the map induced by projection $\mathbb{Z} \to \mathbb{Z}/p$.

Proof. For a) and b) see [Ev], p. 28. □

Remark 2.2. For a finite group G, one can define elements in $H^2(G, \mathbb{F}_p)$ in the following ways:

a) a morphism $\alpha : G \to \mathbb{F}_p,\ \alpha \in Hom(G, \mathbb{F}_p) = H^1(G, \mathbb{F}_p)$ defines an element $\delta(\alpha) \in H^2(G, \mathbb{F}_p)$ via the Bockstein δ.

b) a morphism $\alpha : G \to \mathbb{Q}/\mathbb{Z},\ \alpha \in Hom(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq H^2(G, \mathbb{Z})$ defines canonically an element in $H^2(G, \mathbb{Z})$, which in turn maps via the canonical map $H^2(G, \mathbb{Z}) \to H^2(G, \mathbb{F}_p)$ to an element in $H^2(G, \mathbb{F}_p)$.

Moreover these maps are compatible with each other in the sense that using the natural embedding $\mathbb{F}_p \to \mathbb{Q}/Z,\ a \to a/p$, from a morphism $\alpha : G \to \mathbb{F}_p$, one can define elements of $H^2(G, \mathbb{F}_p)$ in the two ways described above, and the resulting elements will be equal.

CHAPTER 3

NEW CLASSES IN $H^*(U_N(\mathbb{F}_P), \mathbb{F}_P)$

In this chapter we will define some cohomology classes in $H^*(U_n(\mathbb{F}_p), \mathbb{F}_p)$, which generate a ring of the same dimension as the entire cohomology ring.

Lemma 3.1. *Let G be a group and $L \leq G$ a subgroup such that there exists a map $f : G \to L$ such that f is the identity on L. If M is any L-module, then $H^*(L, M)$ is a direct summand of $H^*(G, M)$.*

Proof. Let i be the canonical inclusion $L \hookrightarrow G$. We have the two maps

$$L \xrightarrow{i} G \xrightarrow{f} L$$

and $f \circ i = 1$. But looking at these maps in cohomology we get

$$H^*(L, M) \xrightarrow{f^*} H^*(G, M) \xrightarrow{res_L} H^*(L, M)$$

and $res_L \circ f^* = 1$. This implies that $H^*(L, M)$ is a direct summand of $H^*(G, M)$. □

For simplification we will write $H^*(G)$ instead of $H^*(G, \mathbb{F}_p)$. From now on let $G = U_n(\mathbb{F}_p)$.

Corollary 3.2. *Any $U_k(\mathbb{F}_p)$ with $k < n$ can be regarded as a subgroup of $U_n(\mathbb{F}_p)$ by identifying it with U_{km} described below:*

$$U_{km} = \{M = \begin{pmatrix} I_{m-1} & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & I_{n-m-k+1} \end{pmatrix}, \text{ such that } A \in U_k\}.$$

Then $H^*(U_{km}) \hookrightarrow H^*(U_n(\mathbb{F}_p))$.

Proof. The map $G \to U_{km}$, $(a_{ij})_{1\leq i,j\leq n} \to (a_{mn})$, which picks up exactly the elements at positions corresponding to nonzero entries in U_{km} splits. Applying the previous lemma, we obtain the result. □

Definition 3.1. Define the subgroups $A_k \leq G$ as follows

$$A_k = \{M \in G, M = \begin{pmatrix} I_k & * \\ 0 & I_{n-k} \end{pmatrix}\}$$

and $E_n = A_{[n/2]} \leq U_n$.

Remark 3.1. A_k is elementary abelian. In fact:

$$\begin{pmatrix} I_k & M \\ 0 & I_{n-k} \end{pmatrix} + \begin{pmatrix} I_k & N \\ 0 & I_{n-k} \end{pmatrix} = \begin{pmatrix} I_k & M+N \\ 0 & I_{n-k} \end{pmatrix}$$

Definition 3.2. Define the element $\gamma_n = N_{E_n \to G}\delta(x) \in H^{2l}(G, \mathbb{F}_p)$, where $N_{H\to G}()$ is the Evens norm map (see [Ev], p. 57), $l = \frac{n(n-1)}{2} - \left[\frac{n^2}{4}\right]$, and δ is the Bockstein defined at the end of the previous chapter. The element $x \in H^1(E_n, \mathbb{F}_p) = Hom(E_n, \mathbb{F}_p)$ is the morphism

$$x : E_n \to \mathbb{F}_p, \ A = (a_{ij}) \to a_{1n}.$$

Definition 3.3. Define an element $\gamma_{ij} \in H^*(U_n)$ for each position $(i,j), 1 \leq i < j \leq n$ as follows: Form a subgroup $U_{km} \leq U_n$ as described in 3.2, such that $k = j-i+1$ and $m = i$. This just means that the "upper right corner" of the nonzero entries of U_{km} is at position (i,j). Then we define γ_{ij} to be the corresponding $\gamma_k \in H^*(U_{km}) \hookrightarrow H^*(U_n)$.

Remark 3.2. We can alternatively define γ_{ij} as follows:

Form the subgroup:

$$H_{ij} = \{M \in U_n, M = \begin{pmatrix} U_{i-1} & * & * \\ 0 & E_{j-i+1} & * \\ 0 & 0 & U_{n-j} \end{pmatrix}\} \leq U_n.$$

Then there exists the following homomorphism:

$$\xi_{ij} : H_{ij} \to \mathbb{F}_p,\ \xi_{ij}((a_{kl})_{k,l}) = a_{ij}.$$

Thus $\xi_{ij} \in Hom(H_{ij}, \mathbb{F}_p) = H^1(H_{ij}, \mathbb{F}_p)$. Define $\gamma_{ij} = N_{H_{ij} \to U_n} \delta(\xi_{ij})$. These two definitions of γ_{ij} give the same elements because of the functorial property of the norm map (N5 p. 58 in [Ev]).

Proposition 3.3. *$H^*(G)$ is a ring of dimension $\left[\frac{n^2}{4}\right]$.*

Proof. From [Ev] p. 103, we get that this dimension is equal to the maximum rank of an elementary abelian subgroup of G. But this rank is $\left[\frac{n^2}{4}\right]$, as proved in [MP], p. 298, prop. 5.2. One elementary abelian subgroup with this rank is E_n. □

Proposition 3.4. *The ring generated by all γ_{ij}, $1 \leq i < j \leq n$ in $H^*(G)$ has the same dimension as $H^*(G)$.*

Proof. Let R be the ring generated by all γ_{ij}, $1 \leq i < j \leq n$ in $H^*(G)$. Since R is a subgroup of $H^*(G)$, its dimension will be at most that of $H^*(G)$, namely $\left[\frac{n^2}{4}\right]$. The dimension of $H^*(G)$ is the rank of a maximal elementary abelian subgroup. One such subgroup is $H = E_n$. To get the other inequality we use the restriction map

$$H^*(G) \xrightarrow{res_H} H^*(H).$$

Let's see the image of the elements γ_{ij}, where $1 \leq i \leq [n/2]$ and $[n/2] < j \leq n$ under this map. Observe that these are exactly the positions corresponding to nonzero entries of the elements of H.

It is known that the even cohomology of an elementary abelian group E of cardinality p^k contains the polynomial ring $\mathbb{F}_p[X_1, ..., X_k]$, where each X_i has degree 2 and corresponds to a generator of $H^2(E, \mathbb{F}_p)$. In our case $E = H$ and let $x_{ij}, 1 \leq i \leq [n/2], [n/2] < j \leq n$ be those generators. Then we have the following

Lemma 3.5. *For each $i, j, 1 \leq i \leq [n/2], [n/2] < j \leq n$, the restriction of γ_{ij} to H is of the form*

$$res_H(\gamma_{ij}) = x_{ij}^{p^m} + l.o.t,$$

where l.o.t represents terms whose power of x_{ij} is less than p^m, and only contain factors x_{kl} with $k \geq i, l \leq j$ (i.e., corresponding only to positions down and to the left of (i, j)).

Proof. Fix a pair (i, j). Then γ_{ij} is defined as the image of $N_{A \to U_{di}}\beta(x)$ under the canonical injection $H^*(U_{di}) \to H^*(G)$ where A is an elementary abelian subgroup of the form $A_k \leq U_{di}$ of maximal rank and $d = j - i + 1$. Let $U = U_{di}$ and $K = U_{di} \cap H$.

Then since the elements x_{kl} with $k \geq i, l \leq j$ come from $H^*(K)$, we can restrict ourselves to the problem of computing $res_K N_{A\to U} x_{1d}$ in $H^*(U_{di}) = H^*(U_d)$. (U_d is the group of upper triangular matrices in $GL_d(\mathbb{F}_p)$ with 1 on the diagonal) We are now in the following context:

$$U = U_d, A = \{M \in U_d, M = \begin{pmatrix} I_a & 0 & * \\ 0 & I_b & * \\ 0 & 0 & I_c \end{pmatrix}\}, K = \{M \in U_d, M = \begin{pmatrix} I_a & * & * \\ 0 & I_b & 0 \\ 0 & 0 & I_c \end{pmatrix}\}$$

or

$$U = U_d, A = \{M \in U_d, M = \begin{pmatrix} I_a & * & * \\ 0 & I_b & 0 \\ 0 & 0 & I_c \end{pmatrix}\}, K = \{M \in U_d, M = \begin{pmatrix} I_a & 0 & * \\ 0 & I_b & * \\ 0 & 0 & I_c \end{pmatrix}\}$$

for some a, b, c ($a + b = [d/2]$ in the first case and $b + c = [d/2]$ in the second case).

Since both K and A are normal in U, KA is normal in U. Then a set of double coset representatives for $K\backslash U/A$ is

$$S = \{M, M = \begin{pmatrix} B & 0 & 0 \\ 0 & C & 0 \\ 0 & 0 & D \end{pmatrix}\}.$$

Then by the Evens norm formula we have

$$res_K N_{A\to U} x_{1d} = \prod_{s\in S} N_{K\cap sAs^{-1}\to K} res_{K\cap sAs^{-1}}(s^* x_{1d}).$$

Since A is normal in U, $sAs^{-1} = A$. It can be easily computed that $s^*(x_{1d}) = x_{1d} + o.t.$

where $o.t.$ represents a linear combination of x_{kl} with $(k,l) \neq (i,j)$ corresponding only to nonzero positions of $A \cap K$. We thus get

$$res_K N_{A\to U} x_{1d} = \prod_{s\in S} N_{K\cap A\to K} res_{K\cap A}(x_{1d} + o.t.).$$

Since $N_{K\cap A\to K}(x_{1d}+o.t.) = x_{1d}^{p^r}+l.o.t$, by multiplication we get the desired result. □

To prove the proposition we will also use the following

Lemma 3.6. *Let $k[X_1,...,X_n]$ be the ring of polynomials in n indeterminates. Let $b_i = X_i^{n_i} + f_i(X_1,...,X_i)$ where f_i are polynomials such that the maximum degree of X_i in f_i is less than n_i. Then $k(b_1,...,b_n) \subset k(X_1,...,X_n)$ is a finite extension of fields.*

Proof. We proceed by induction on n. Case $n = 1$ is clear. Suppose it is true for $n-1$. Since $k(b_1,...,b_{n-1}) \subset k(X_1,...,X_{n-1})$ is finite, we also have that $k(b_1,...,b_{n-1},b_n) \subset k(X_1,...,X_{n-1},b_n)$ is finite. In the extension $k(X_1,...,X_{n-1},b_n) \subset k(X_1,...,X_{n-1},X_n)$ we have

$$X_k^{n_n} + f_n(X_1,...,X_{n-1},X_n) - b_n = 0,$$

which is an equation in X_n with coefficients in $k(X_1,...,X_{n-1},b_n)$ of degree n_n.

Thus $k(X_1,...,X_{n-1},b_n) \subset k(X_1,...,X_{n-1},X_n)$ is finite and therefore $k(b_1,...,b_n) \subset k(X_1,...,X_n)$ is finite. □

Back to the proof of our proposition. We can now define the indeterminates X_i as $X_1 = x_{k,k+1}$ $(k = [n/2])$, $X_2 = x_{k-1,k+1}, X_3 = x_{k.k+2}$ ... (counting parallel to the diagonal, starting with the lower left corner of the rectangle corresponding to non-zero

entries of matrices in H) and the b_i as the corresponding γ_{ij}. By the way we defined the X_i, we are in the context of Lemma 3.6 and thus the extension $k(x_{ij}) \subset k(\gamma_{ij})$ is finite. This implies that the Krull dimension of $k[\gamma_{ij}]$ is the same as that of $k[x_{ij}]$. But $k[x_{ij}]$ is a polynomial ring in $[n/2](n - [n/2]) = [n^2/4]$ variables and thus the dimension of $k[\gamma_{ij}]$ is at least $[n^2/4]$ and we are done. $\square$

CHAPTER 4

ALL MAXIMAL ELEMENTARY ABELIAN SUBGROUPS OF U_3 AND U_4

A maximal elementary abelian subgroup is an elementary abelian subgroup such that there are no elementary abelian subgroups that properly contain it. In this chapter we will compute all maximal elementary abelian subgroups of $U_3(\mathbb{F}_p)$ and $U_4(\mathbb{F}_p)$. This is useful when one wants to check whether a cohomology class is nilpotent. For that we use the following theorem of Quillen ([AM] p. 144):

Theorem 4.1 (Quillen). *Let G be a finite p-group and k a field of characteristic p. A cohomology class $\beta \in H^*(G,k)$ is nilpotent if and only if its restriction to all elementary abelian subgroups is nilpotent.*

From now on we will assume that $p \geq 3$. We will do the case of U_3 first, since it is easier. Let $Z = Z(U_3)$ be the center of U_3. We have

Theorem 4.2. *All maximal elementary abelian subgroups of U_3 are $H_i =< A_i, Z >$, where $i = 0, 1, ..., p$ and*

$$A_i = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \text{ for } i = 0, 1, ..., p-1 \text{ and } A_p = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Moreover these subgroups are all different.

Proof. Since $p \geq 3$, any nontrivial matrix in U_3 has order p. First any maximal elementary abelian subgroup E must contain the center Z of U_3; otherwise the subgroup ZE is elementary abelian and it strictly contains E, so E is not maximal.

Observe now that U_3 has order p^3 and is not abelian. So any maximal elementary abelian subgroup must have order at most p^2. But for any matrix $A \in U_3 - Z$, the group generated by A and Z is elementary abelian (because it is abelian and all elements have order p) and has order p^2. Since all maximal elementary abelian subgroups must contain Z, they must be of this form, generated by a matrix A and by Z.

Now any matrix A, by multiplying it with a suitable element of Z can be transformed into a matrix of the form

$$A = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}.$$

The powers of A are of the form

$$A^k = \begin{pmatrix} 1 & ka & * \\ 0 & 1 & kb \\ 0 & 0 & 1 \end{pmatrix}.$$

If $a \neq 0$, for a suitable k we can get $ka = 1$ so $A^k = A_i C$ for some $i \leq p-1$ and some $C \in Z$. If $a = 0$ then $b \neq 0$ (or else $A \in Z$) so for some k we have that $A^k = A_p C$ with $C \in Z$. Because $< A, Z > \supset < A_i, Z >$ and these groups have the same cardinality,

the group generated by A and Z is the same as the one generated by A_i and Z hence the first part of the theorem follows.

The fact that the H_i are all different is very easy to see, since $A_k \notin H_i$ for $k \neq i$. □

We now turn to the case of U_4. Let $Z = Z(U_4)$ be the center of U_4. In general, it is known that the center of U_n is isomorphic to $\mathbb{F}_p$ and consists of matrices that have only one nontrivial entry, in the upper right-hand corner. Let C be a generator of Z.

Theorem 4.3. *Let E be a maximal elementary abelian subgroup of $G = U_4(\mathbb{F}_p)$ with $p \geq 5$. Then E has one of the following forms:*

$$1)\ E = \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$2)\ E =< A, B, C > \ \textit{with}\ A = \begin{pmatrix} 1 & a & c & 0 \\ 0 & 1 & 1 & d \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & a & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where $(a, b) \neq (0, 0)$ and $d = 0$ if $b \neq 0$ and $c = 0$ if $b = 0, a \neq 0$;

3) $E =< A, B, C >$ *with* $A = \begin{pmatrix} 1 & 1 & a & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & c & 0 \\ 0 & 1 & 0 & -a \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$;

4) $E =< A, B, C >$ *with* $A = \begin{pmatrix} 1 & a & c & 0 \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & a & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$,

where $a = 1, c = 0$ *or* $a = 0, b = 1, d = 0$.

Moreover these subgroups are all different.

Proof. Since we suppose $p > 3$, every nontrivial element of U_4 has order p. Thus a subgroup is elementary abelian if and only if it is commutative. Let $\beta : U_4 \to \mathbb{Z}/p$ be the surjective homomorphism defined by

$$\begin{pmatrix} 1 & * & * & * \\ 0 & 1 & b & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix} \to b.$$

Let $H = \ker \beta$. Then H is an extraspecial p-group of order p^5.

We have two cases:

a) The first case is $E \not\subset H$. Then $\beta(E) = \mathbb{Z}/p$. Let $A \in E$ be such that $\beta(A) = 1$. Then any matrix $X \in E$ can be written as $A^k Y$ for some $k \leq p - 1$ and some Y such that $\beta(Y) = 0$, i.e., $Y \in E \cap H$. Thus E is generated by A and $E \cap H$. Let

$X \in (E \cap H) - Z$. By multiplying with elements of Z we can suppose that A and X have the following forms:

$$A = \begin{pmatrix} 1 & a & c & 0 \\ 0 & 1 & 1 & d \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 1 & x & z & 0 \\ 0 & 1 & 0 & t \\ 0 & 0 & 1 & y \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We need to have $AX = XA$ that is

$$\begin{pmatrix} 1 & a+x & c+z & at+cy \\ 0 & 1 & 1 & t+y+d \\ 0 & 0 & 1 & b+y \\ 0 & 0 & 0 & 1 \end{pmatrix} = AX = XA = \begin{pmatrix} 1 & a+x & c+x+z & dx+bz \\ 0 & 1 & 0 & t+d \\ 0 & 0 & 1 & b+y \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

From here we obtain that $x = 0, y = 0, at = bz$.

If $(a, b) = (0, 0)$ then we obtain the subgroup of 1).

If $(a, b) \neq (0, 0)$ then all matrices in H that commute with A have the form:

$$X = \begin{pmatrix} 1 & 0 & z & * \\ 0 & 1 & 0 & t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ with } at = bz.$$

It is clear that these matrices form a group of order p^2 containing Z, also containing

$$B = \begin{pmatrix} 1 & 0 & a & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \notin Z$$

Since the group generated by B and Z is also of order p^2, it must be equal to the group of matrices of H commuting with A and we thus get the case 2) of the theorem.

b) The other case is $E \subset H$. Still $E \supset Z$. Let's consider now the homomorphism $\alpha : H \to \mathbb{Z}/p$, $\alpha(a_{ij}) = a_{12}$ and let $K = \ker \alpha$.

If $E \not\subset K$, then there is a matrix $A \in E$ such that $\alpha(A) = 1$. Any matrix $X \in E$ can be written as $A^k Y$ with $k \leq p-1$ and $\alpha(Y) = 0$, i.e., $Y \in E \cap K$. Thus E is generated by A and $E \cap K$. Let $X \in E \cap K$. By multiplying A with an element of Z, we can suppose that A and X have the following forms:

$$A = \begin{pmatrix} 1 & 1 & a & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; X = \begin{pmatrix} 1 & 0 & x & t \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & z \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We need to have X commute with A. By computing AX and XA we see that the only relation that has to be satisfied is $y + az = cx$, i.e., $y = cx - az$. The set of matrices $X \in K$ that commute with A is thus a group $S = C_H(A) \cap K$ with p^3 elements.

Since $E \cap K$ is an elementary abelian subgroup of K that commutes with A, we need to have $E \cap K \subset S$. We see that S is not a commutative group (the matrices for $x = 1, z = 0, t = 0$ and $x = 0, z = 1, t = 0$ don't commute). Thus $E \cap K$ has at most p^2 elements. Since there are clearly matrices in $S - Z$, we get that, for each E, there is one more matrix that together with A and Z generates E. For $z = 0$ we get case 4. For $z \neq 0$ a power of X has $z = 1$. By dividing A by a suitable power

of X we can make $c = 0$. We will then be in case 3, where B is obtained from X by multiplying by a suitable element of Z to make $t = 0$.

The last case is $E \subset K$. Then there must be a matrix $A = (a_{ij}) \in E$ such that $a_{34} \neq 0$, otherwise E is a subgroup of the group of case 1 and, being also a subgroup of H, it is not maximal. Let $A = (a_{ij}) \in E$ be such that $a_{34} = 1$. By multiplying A by a suitable element of Z, we can make it of the form:

$$A = \begin{pmatrix} 1 & 0 & a & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since we suppose $E \subset K$, we need to see what matrices of K commute with A. By an argument we did twice in this proof, we can restrict our attention to matrices $X = (x_{ij}) \in K - Z$ which have $x_{34} = 0$. By multiplying X by an element of Z we can make it of the form:

$$X = \begin{pmatrix} 1 & 0 & x & 0 \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

By equating AX and XA, we must have that $x = 0$. This implies that $y \neq 0$, so by raising X to a power, we can make $y = 1$. It is easy to see that the X obtained commutes with A. Then by multiplying A by a suitable power of $B = X$, we can have $b = 0$ and we are in case 4.

The last thing we have to check is that all these subgroups are different. First

observe that subgroups from different cases are different. The only nontrivial part of this is to prove that a subgroup of case 3) is different from one of case 4). For that observe that if E is from case 3) then there are matrices $X \in E$ such that the pair (x_{12}, x_{34}) takes any of the p^2 diferent possibilities, whereas in case 4 this pair can only take p different values (because B and Z don't affect these entries).

We now have to check that inside each case the described subgroups are all different. In case 1) there is nothing to prove.

In case 2), let E be generated by A, B (and Z) and also by A', B'(and Z). Then $A' = A^k B^l C$ with $C \in Z$. But $A^k B^l C$ has the element at position $(2,3)$ equal to k; thus $k = 1$. So $A' = AB^l C$. Now $AB^l C$ has the element at $(1,2)$ equal to a, so $a' = a$ ($a', b', ...$ being the corresponding entries of A'). Similarly $b' = b$. Thus $B' = B$.

Looking at the elements at positions $(1,3)$ and $(2,4)$ in A' and in $AB^l C$, we get that $c' = c + la$, $d' = d + lb$. If $b \neq 0$ then $d = d' = 0$ (from the description of case 2, since $b = b'$ are nonzero), so $l = 0$ and $c' = c$. If $b = 0$ then $a \neq 0$ and $c' = c = 0$. We get that $l = 0$ and thus $d' = d$.

Similar arguments work for cases 3) and 4). □

CHAPTER 5

ALL RELATIONS MOD NILPOTENTS OF THE CLASSES DEFINED IN U_4

In this chapter, we will assume that $p \geq 5$. To compute all the relations modulo nilpotents, we will find those classes in the subring R defined in chapter 3 that restrict to 0 on all maximal elementary abelian subgroups. This will be enough because of

Lemma 5.1. *Let $R = \mathbb{F}_p[\{\gamma_{ij}\}]$ be the ring defined in chapter 3. Then an element $\alpha \in R$ is nilpotent if and only if it restricts to zero on all maximal elementary abelian subgroups.*

Proof. It is known that the $\mathbb{F}_p$ cohomology ring of an elementary abelian p-group $\mathbb{Z}/p^n$ is a tensor product of an exterior algebra with a polynomial algebra. The generators of the polynomial algebra are the elements of degree two.

Let $\alpha \in R$ and let E be an elementary abelian subgroup of rank k of $G = U_n$. Let $\mathbb{F}_p[x_1, ..., x_k]$ be the polynomial part of $H^*(E)$, with $x_1, ..., x_k$ elements of degree 2. The element γ_{ij} restricts to an element of $\mathbb{F}_p[x_1, ..., x_k]$ as one can easily see from the norm formula (since γ_{ij} is the norm of some element of degree 2). Thus also the element α, which is a polynomial in the γ_{ij}, restricts to an element of $\mathbb{F}_p[x_1, ..., x_k]$. But since $\mathbb{F}_p[x_1, ..., x_k]$ is a reduced ring, the restriction of α to E is nilpotent if and only if is zero.

The theorem of Quillen we referred at the beginning of chapter 4 states that a cohomology class is nilpotent if and only if it is nilpotent when restricted to all elementary abelian subgroups (or all maximal elementary abelian subgroups). By this theorem and the above argument, we obtain that α is nilpotent if and only if it restricts to zero an all maximal elementary abelian subgroups. $\square$

First let's denote by $H \leq G$ the subgroup of matrices $(a_{ij}) \in U$ such that $a_{23} = 0$. It is easy to see that H is an extraspecial p-group of order p^5. Also let $K \leq G$ be the subgroup of matrices $(a_{ij}) \in U$ such that $a_{34} = 0$ and let L be the subgroup of matrices $(a_{ij}) \in U$ such that $a_{12} = 0, a_{34} = 0$.

Now let's denote by x, y, z, t, u, v the elements $\gamma_{12}, \gamma_{23}, \gamma_{34}, \gamma_{13}, \gamma_{24}, \gamma_{14}$ respectively.

Define the element $t' \in H^2(H)$ corresponding to the morphism $H \ni (a_{ij}) \to a_{13}$ and $u' \in H^2(K)$ corresponding to the morphism $K \ni (a_{ij}) \to a_{24}$ Then

$$t = N_{H \to G} t', \ u = N_{K \to G} u'$$

easily results from the property N5 p. 58 of [Ev].

For an elementary abelian group $E =< A, B, C... >$ let's denote by $X_A, X_B, ...$ the elements $X_A = \delta(\phi_A)$, where $\phi_A \in H^1(E, \mathbb{F}_p) = Hom(E, \mathbb{F}_p)$ is the morphism $\phi_A(A^k B^l ...) = k$, and similar definitions for $X_B, ...$ hold. Then it is known that

$$H^*(E, \mathbb{F}_p) = \mathbb{F}_p[X_A, X_B, ...] \otimes E,$$

where E is an exterior algebra and we can view $X_A, X_B, ...$ as indeterminates.

Proposition 5.2. *The restriction of x, y, z, t, u, v to a maximal elementary abelian subgroup E is the following, corresponding to the cases from theorem 4.3:*

1) $res_E x = 0$, $res_E y = X$, $res_E z = 0$, $res_E t = Y^p - YX^{p-1}$, $res_E u = Z^p - ZX^{p-1}$, $res_E v = T^{p^2} + l.o.t.$

2) $res_E x = aX$, $res_E y = X$, $res_E z = bX$, $res_E t = a(Y^p - YX^{p-1})$, $res_E u = b(Y^p - YX^{p-1})$, $res_E v = z^{p^2} + l.o.t.$

3) $res_E x = X$, $res_E y = 0$, $res_E z = Y$, $res_E t = c(Y^p - YX^{p-1})$, $res_E u = b(X^p - XY^{p-1})$, $res_E v = z^{p^2} + l.o.t.$

4) $res_E x = aX$, $res_E y = 0$, $res_E z = bX$, $res_E t = a(Y^p - YX^{p-1})$, $res_E u = b(Y^p - YX^{p-1})$, $res_E v = z^{p^2} + l.o.t$,

where $X = X_A$, $Y = X_B$, $Z = X_C$ *(and for case 1,* $T = X_C$ *and* $Z = X_D$*) and the elementary abelian subgroup at each case can be written* $E =< A, B, C >$ *(*$E =< A, B, C, D >$ *for case 1).*

Proof. 1) $res_E x = 0$ is clear since all matrices of E have 0 in the $(1, 2)$ position. Also $res_E z = 0$ and $res_E y = X$ are clear. Since $EH = G$ in this case, by the norm formula we get:

$$res_E t = res_E N_{H\to G} t' = N_{E\cap H\to E} res_{E\cap H} t' = \prod_{q, res_{E\cap H} q = res_{E\cap H} t'} q$$
$$= \prod_{i=0}^{p-1} (Y + iX) = Y^p - YX^{p-1}.$$

Now since $K \triangleleft G$ and $E \subset K$, there are p double cosets for E and K (they are also

single cosets). A set of double coset representatives is

$$S = \{A \in U, A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & i \\ 0 & 0 & 0 & 1 \end{pmatrix}, i \in \mathbb{F}_p\};$$

thus by the norm formula:

$$res_E u = res_E N_{K\to G} u' = \prod_{s\in S} res_E s^*(u') = \prod_{i=0}^{p-1}(Z + iX) = Z^p - ZX^{p-1}.$$

The fact that $res_E v = T^{p^2} + l.o.t.$ has been done in chapter 3).

2) Since $res_E x$ and aX both come from the same morphism on E, we get that $res_E x = aX$. Also $res_E y = X$, $res_E z = bX$.

Since $EH = G$ and H is normal in G we get that

$$res_E t = res_E N_{H\to G} t' = N_{E\cap H\to E} res_{E\cap H} t' = \prod_{q, res_{E\cap H} q = res_{E\cap H} t'} q$$
$$= \prod_{i=0}^{p-1}(aY + iX) = a(Y^p - YX^{p-1})$$

since $E \cap H =< B, C >$.

For $res_E u$, if $b = 0$, $E \subset K$ and using the coset representatives for K from case 1 we get

$$res_E u = res_E N_{K\to G} u' = \prod_{s\in S} res_E s^*(u') = \prod_{i=0}^{p-1}(dX + iX) = 0$$

If $b \neq 0$ then $EK = G$ and we get

$$res_E u = res_E N_{K\to G} u' = N_{E\cap K\to E} res_{E\cap K} u' = N_{E\cap K\to E} bY = b(Y^p - YX^{p-1})$$

since $E \cap K =< B, C >$.

For $res_E v$ we have that L is normal subgroup of G and EL is of index p in G. If $a \neq 0$ (case $a = 0$ is done similarly), the set S from case 1 is a system of representatives for the $E - L$ double cosets. We get

$$\begin{aligned} res_E v &= res_E N_{L\to G} v' = \prod_{s\in S} N_{E\cap L\to E} res_{E\cap L} s^* v' = \prod_{s\in S} N_{E\cap L\to E} s^* Z \\ &= \prod_{i=0}^{p-1} N_{E\cap L\to E}(Z + iY) = N_{E\cap L\to E}(Z^p - ZY^{p-1}) \\ &= (N_{E\cap L\to E} Z)^p - N_{E\cap L\to E} Z (N_{E\cap L\to E} Y)^{p-1} \\ &= (Z^p - ZX^{p-1})^p - (Z^p - ZX^{p-1})(Y^p - YX^{p-1})^{p-1} \\ &= Z^{p^2} + l.o.t. \end{aligned}$$

Here we took into account that $E \cap L =< B, C >$ and that the norm is a ring homomorphism (see [Ev], p. 64).

3) It is clear that $res_E x = X$, $res_E y = 0$ and $res_E z = Y$.

For $res_E t$ observe that $E \subset H$ and H is normal in G. A set of $E - H$ double coset representatives is

$$T = \{A \in U, A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & i & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, i \in \mathbb{F}_p\}.$$

Then by the norm formula we get

$$res_E t = res_E N_{H\to G} t' = \prod_{s\in T} res_E s^*(t') = \prod_{i=0}^{p-1} (cY - iX) = c(Y^p - YX^{p-1}).$$

For $res_E u$ we have that $KE = G$ and K is normal in G. So by the norm formula we have

$$res_E u = res_E N_{K\to G} u' = N_{E\cap K\to E} res_{E\cap K} u' = N_{E\cap K\to E} bX = b(X^p - XY^{p-1})$$

since $E \cap K =< A, C >$.

For $res_E v$ we have that $LE = G$ and L is normal in G. So by the norm formula we have

$$res_E v = res_E N_{L\to G} v' = N_{E\cap L\to E} res_{E\cap L} v' = N_{E\cap L\to E} Z = Z^{p^2} + l.o.t$$

since $E \cap L =< C >$.

Case 4) is done similarly to case 2) □

Corollary 5.3. *Let* $f(X, Y, Z, T, U, V) \in \mathbb{F}_p[X, Y, Z, T, U, V]$.

Then $f(x, y, z, t, u, v) \in H^*(G)$ *is nilpotent if and only if the following hold:*

1) $f(0, X, 0, Y, Z, T) = 0$,

2) $f(aX, X, bX, aY, bY, Z) = 0$ *for all* $a, b \in \mathbb{F}_p$, $(a, b) \neq (0, 0)$,

3) $f(X, 0, Y, a(Y^p - YX^{p-1}), b(X^p - XY^{p-1}), Z) = 0$ *for all* $a, b \in \mathbb{F}_p$,

4) $f(aX, 0, bX, aY, bY, Z) = 0$ *for all* $a, b \in \mathbb{F}_p$, $(a, b) \neq (0, 0)$.

Proof. We saw from 5.1 that $f(x, y, z, t, u, v)$ is nilpotent if and only if it restricts to zero on all maximal elementary abelian subgroups of G. But we described all maximal elementary abelian subgroups of U_4 in the previous chapter.

By restricting to the subgroup of case 1 of 4.3, since the restriction map is a ring homomorphism and by using prop. 5.2 we obtain that:

$$f(0, X, 0, Y^p - YX^{p-1}, Z^p - ZX^{p-1}, T^{p^2} + l.o.t.) = 0.$$

But observe that $X, Y^p - YX^{p-1}, Z^p - ZX^{p-1}, T^{p^2} + l.o.t.$ are algebraically independent so we can replace them by X, Y, Z, T respectively. This way we obtain the first relation. The second relation is obtained similarly by restricting to subgroups of the second case of 4.3 and using the second result from 5.2. Here we also use that X and $Y^p - YX^{p-1}$ are algebraically independent. Relations 3) and 4) follow similarly. $\square$

Theorem 5.4. *Let N be the nilradical of $\mathbb{F}_p[x, y, z, t, u, v]$. Then $\mathbb{F}_p[x, y, z, t, u, v]/N$ is isomorphic to $\mathbb{F}_p[X, Y, Z, T, U, V]/I$ where I is*

$$I = I_1 \cap \sqrt{I_2} \cap I_3 \cap \sqrt{I_4} = \sqrt{I_1 \cap I_2 \cap I_3 \cap I_4} \text{ and}$$

$$I_1 = (X, Z),$$

$$I_2 = (UX - TZ, U^pT - UT^p, X^p - XY^{p-1}, Z^p - ZY^{p-1}),$$

$$I_3 = (Y, T^p - T(Z^p - ZX^{p-1})^{p-1}, U^p - U(X^p - XZ^{p-1})),$$

$$I_4 = (UX - TZ, U^pT - UT^p, Y, XZ^p - X^pZ).$$

Proof. We have the canonical map $\mathbb{F}_p[X, Y, Z, T, U, V] \to \mathbb{F}_p[x, y, z, t, u, v]$ defined by $X \to x, Y \to y, ...$ This map is obviously surjective. Then the induced map $\mathbb{F}_p[X, Y, Z, T, U, V] \to \mathbb{F}_p[x, y, z, t, u, v]/N$ is surjective and we only have to prove that I is its kernel. In other words, we have to prove that $f(x, y, z, t, u, v) \in N$ if and only if $f(X, Y, Z, T, U, V) \in I$. So by the previous corollary we have to prove that f satisfies conditions 1) to 4) of that corollary if and only if $f \in I$.

Observe now that $f(0, X, 0, Y, Z, T) = 0$ is equivalent to $f \in (X, Z)$. This is because we can write

$$f(X, Y, Z, T, U, V) = g(Y, T, U, V) + Xh(X, Y, Z, T, U, V) + Zk(X, Y, Z, T, U, V)$$

and $f(0,Y,0,T,U,V) = 0 = g(Y,T,U,V)$. Thus f satisfies 1) if and only if $f \in I_1$.

Condition 2) of cor. 5.3 is satisfied by f if and only if

$$f \in I_{ab} = (X - aY, Z - bY, aU - bT) \text{ for all } (a,b) \neq (0,0).$$

This is because for $a \neq 0$ we can write

$$\begin{aligned} f(X,Y,Z,T,U,V) &= g(Y,Z,T,U,V) + (X - aY)p(X,Y,Z,T,U,V) \\ &= h(Y,T,U,V) + (Z - bY)q(X,Y,Z,T,U,V) + (X - aY)p(X,Y,Z,T,U,V) \\ &= k(Y,T,V) + (aU - bT)r(X,Y,Z,T,U,V) + (Z - bY)q(X,Y,Z,T,U,V) + \\ &+ (X - aY)p(X,Y,Z,T,U,V) \end{aligned}$$

and because of condition 2) we get that $k(Y,T,V) \equiv 0$. If $a = 0$ then $b \neq 0$ and k will depend on Y,U,V, and we obtain the same thing.

We obtain this way that f satisfies condition 2) if and only if $f \in \cap_{(a,b)\neq(0,0)} I_{ab}$. So we only need to prove that

$$\cap_{(a,b)\neq(0,0)} I_{ab} = \sqrt{I_2}. \tag{5.1}$$

We will now work over the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. The above condition is equivalent to

$$V(\cap_{(a,b)\neq(0,0)} I_{ab}) = V(I_2).$$

where $V(I)$ represents the algebraic set of points $Q \in \mathbb{P}^6(\overline{\mathbb{F}_p})$ such that $g(Q) = 0, \forall g \in I$. But $V(\cap_k I_k) = \cup_k V(I_k)$ (see [ZS], p. 160) so we need to prove that

$$\cup_{(a,b)\neq(0,0)} V(I_{ab}) = V(I_2).$$

If $Q \in V(I_2), Q = (x : y : z : t : u : v)$ then

$$ux = tz$$

$x^p - xy^{p-1} = 0$ which implies $x = ky$ (for some $k \in \mathbb{F}_p$)

$z^p - zy^{p-1} = 0$ which implies $z = ly$ (for some $l \in \mathbb{F}_p$)

$u^p t - ut^p = 0$ which implies $u = mt$ (for some $m \in \mathbb{F}_p$) or $t = 0$.

If $t = 0$ then from $ux = tz$ we get that $x = 0$ or $u = 0$. If $x = 0$ then $Q \in I_{0l}$, if $u = 0$ then $Q \in I_{kl}$.

If $t \neq 0$ then $u = mt$ and since $ux = tz$, we obtain that $mtky = tly$. If $y = 0$ then $x = y = z = 0$ and we can find $(a, b) \neq (0, 0)$ such that $au = bt$, so $Q \in I_{ab}$. Otherwise $y \neq 0$ and from $mtky = tly$ we get $mk = l$, so $x = ky, z = mky, u = mt$, so $Q \in I_{ab}$, where $a = k, b = mk$.

In all cases we obtain that there is $(a, b) \neq (0, 0)$ such that $Q \in I_{ab}$, so $V(I_2) \subset \cup I_{ab}$. It is easy to verify that if $Q \in V(I_{ab})$ for some $(a, b) \neq (0, 0)$ then $Q \in V(I_2)$, so we obtain (5.1).

The fact that f satisfies condition 4) if and only if $f \in \sqrt{I_4}$ is done similarly.

We now need to prove that f satisfies condition 3) if and only if $f \in I_3$ and then we are done.

Let $\alpha(X, Z) = Z^p - ZX^{p-1}$ and $\beta(X, Z) = X^p - XZ^{p-1}$. We will prove more generally that if $\alpha, \beta \in \mathbb{F}_p[X, Y]$ and $f(X, 0, Z, a\alpha(X, Z), b\beta(X, Z), V) = 0$ for all $a, b \in \mathbb{F}_p$ then $f \in (Y, T^p - T\alpha^{p-1}, U^p - U\beta^{p-1})$.

Define the polynomials

$$M_{i,j}(X,Z,T,U) = T(T-\alpha(X,Z))...(T-(i-1)\alpha(X,Z))U(U-\beta(X,Z))...$$
$$...(U-(j-1)\beta(X,Z))$$

with $0 \leq i,j \leq p$, where $i=0$ (resp. $j=0$) means that there are no factors in the T (resp. U) variable. Observe that $M_{i,j}$ can be used instead of the monomials T^iU^j to write

$$f(X,Y,Z,T,U,V) = Yg(X,Y,Z,T,U,V) + \sum_{0\leq i,j\leq p-1} M_{i,j}f_{i,j}(X,Z,V) + \\ + M_{p,0}h(X,Y,Z,T,U,V) + M_{0,p}k(X,Y,Z,T,U,V). \tag{5.2}$$

This is because the coefficient of T^iU^j in $M_{i,j}$ is 1 and we can recursively write all $T^iU^j, i,j \leq p$ in terms of these $M_{i,j}$ with coefficients in $\mathbb{F}_p[X,Z]$.

Now by looking at $f(X,0,Z,a\alpha(X,Z),b\beta(X,Z),V) = 0$ and in (5.2) making $Y=0$, $T=a\alpha(X,Z)$ and $U=b\beta(X,Z)$, we see that all $M_{k,l}$, with $k>a$ or $l>b$, have value 0, because of the way they are defined. Now by giving the following values to (a,b):

$$(0,0),(1,0),...,(p-1,0),(0,1),(1,1),...,(p-1,1),...,(p-1,p-1),$$

we get succesively that $f_{i,j} \equiv 0, 0 \leq i,j \leq p-1$. This implies that

$$f \in (Y, M_{0,p}, M_{p,0}) = (Y, T^p - T\alpha^{p-1}, U^p - U\beta^{p-1}).$$

Reciprocally, it is clear that if $f \in I_3$ than f satisfies condition 3). □

It is impractical to compute this ideal exactly (i.e., obtaining its generators). I did this using the Macaulay II package for $p=5$ and I obtained an ideal with 45 generators!

CHAPTER 6

THE HECKE ALGEBRAS $H(G//B)$ AND $H(G//U)$

In this chapter, we will compute the Hecke algebra $H(G//B)$ and $H(G//U)$, where $G = GL_n(\mathbb{F}_p)$, B is the Borel subgroup consisting of upper triangular matrices, and $U = U_n(\mathbb{F}_p)$ is the unitary subgroup consisting of upper triangular matrices with 1 on the diagonal. We have the Bruhat decomposition:

$$B\backslash G/B = \coprod_{w \in W} BwB,$$

where W is the group of matrices obtained by permuting the lines of the identity matrix corresponding to each permutation of S_n.

Proposition 6.1. *With the above notations, $H(G//B)$ is generated by the double cosets $Bs_iB = (s_i)$ where $s_i \in W$ corresponds to the transposition $(i, i+1)$. The relations between the double cosets (s_i) in $H(G//B)$ are the following:*

$$(s_i)(s_j) = (s_j)(s_i), \text{ if } |i-j| > 1,$$

$$(s_i)(s_{i+1})(s_i) = (s_{i+1})(s_i)(s_{i+1}),$$

$$(s_i)(s_i) = p \cdot (1) + (p-1)(s_i).$$

Proof. See [Ho] p. 3. □

We now turn to $H(G//U)$. As in [Ho], for $w \in S_n$ define

$$l(w) = \min\{k, w = s_{i_1}...s_{i_k}\}.$$

Let $d(w) = \deg BwB$ (regarded as a B-double coset). Recall that $\deg BwB$ is defined as the number d of left cosets Bw_i such that:

$$BwB = \coprod_{1 \le i \le d} Bw_i.$$

It is also equal to $[B : B \cap w^{-1}Bw]$.

We have $d(w) = p^{l(w)}$ since it is enough to check this on s_i, because $d()$ is multiplicative on minimal products of s_i and $l()$ is additive on minimal products of s_i. Since U is normal in B, we have $B = \coprod_{t \in T} Ut$ where T is the group of diagonal matrices. Also observe that W normalizes T. We then have

$$\coprod_{t \in T}^{d(w)} UtwU = BwB = BwU = \coprod_{i=1}^{d(w)} Bwu_i = \coprod_{i=1,\ t \in T}^{d(w)} Utwu_i, \tag{6.1}$$

where wu_i is a system of single B-coset representatives for BwB with $u_i \in U$. Using the Bruhat decomposition, we get from here that

$$U\backslash G/U = \coprod_{w \in W, t \in T} UtwU. \tag{6.2}$$

Since

$$UtwU \supset \coprod_{i=1}^{d(w)} Utwu_i \quad \text{for each } t \in T$$

and when we take reunion for all $t \in T$ we get equality (see (6.1)), we actually have

$$UtwU = \coprod_{i=1}^{d(w)} Utwu_i \quad \text{for each } t \in T.$$

Let's denote the double coset UxU by (x). We obtain therefore that $\deg(tw) = d(w) = \deg(w)$, in $H(G//U)$.

Proposition 6.2. *With the above notations, $H(G//U)$ is generated by the double cosets (s_i) and (t) with $t \in T$. The relations between these generators in $H(G//U)$ are the following:*

$$(ts_i) = (t)(s_i), (s_it) = (s_i)(t), (tt') = (t)(t'),$$

$$(s_i)(s_j) = (s_j)(s_i), \text{ if } |i-j| > 1,$$

$$(s_i)(s_{i+1})(s_i) = (s_{i+1})(s_i)(s_{i+1}),$$

$$(s_i)(s_i) = p(1) + \sum_{kl=-1} (diag(1, .., 1, k, l, 1, ..., 1)s_i),$$

where k is at position i in $diag(1, .., 1, k, l, 1, ..., 1)$.

Proof. We saw above (in (6.2)) that $H(G//U)$ is generated by the double cosets (tw) with $t \in T, w \in W$. Let now $t, t' \in T$ and $w, w' \in W$ be such that $l(w) + l(w') = l(ww')$.

Since $(tw) \cdot (t'w')$ as a set contains $(twt'w')$ and

$$\deg(tw)\deg(t'w') = \deg(w)\deg(w') = \deg(ww') = \deg(twt'w')$$

(because we know that $\deg(ww') = \deg(t_1ww')$ and $twt'w'$ can be written as t_1ww'), we get that

$$(tw)(t'w') = (twt'w'). \tag{6.3}$$

From here, by giving appropriate values to t, t', w, w', we get that

$$(t)(w) = (tw), (w)(t) = (wt) \text{ and } (tt') = (t)(t').$$

Also from here, since for $|i-j| > 1$ we have $l(s_i) + l(s_j) = l(s_is_j)$, we get

$$(s_i)(s_j) = (s_is_j) = (s_js_i) = (s_j)(s_i).$$

If $w \in W$, write $w = s_{i_1}...s_{i_k}$, a minimal decomposition in product of transpositions. Then $l(w) = l(s_{i_1}) + l(s_{i_2}) + ... + l(s_{i_k})$ and from (6.3) we get

$$(w) = (s_{i_1})...(s_{i_k}).$$

The permutations of positions $i, i+1, i+2$ form a group isomorphic to S_3. There are three transpositions there. Two of them are s_i and s_{i+1}. The third is $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$. Since this is a minimal decomposition of this transposition (because it cannot be a product of 2 transpositions and it is not an elementary transposition s_j), we get that

$$(s_i)(s_{i+1})(s_i) = (s_i s_{i+1} s_i) = (s_{i+1} s_i s_{i+1}) = (s_{i+1})(s_i)(s_{i+1}).$$

We now want to prove the relation for $(s_i)(s_i)$. We will prove that

$$Us_iUs_iU = U1U \cup \coprod_{kl=-1} Udiag(1, ..., 1, k, l, 1, ..., 1)s_iU, \tag{6.4}$$

where k is at position i. Because

$$s_i = \begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & I_{n-i-1} \end{pmatrix} \quad \text{with } s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

we get that

$$Us_iUs_iU = \begin{pmatrix} U_{i-1} & * & * \\ 0 & U_2 s U_2 s U_2 & * \\ 0 & 0 & U_{n-i-1} \end{pmatrix}$$

so we see that without loss of generality we may assume $U = U_2$. In this case an element of U has the form $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and thus a nontrivial element of sUs is of the form

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -\frac{1}{a} \\ a & 0 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{a} \\ 0 & 1 \end{pmatrix}.$$

This implies that

$$UsUsU = U \cup \coprod_{a \neq 0} U \begin{pmatrix} 0 & -\frac{1}{a} \\ a & 0 \end{pmatrix} U = U \cup \coprod_{kl=-1} Udiag(k,l)sU.$$

We thus obtained the relation (6.4). From here we get that

$$(s_i)^2 = m(1) + \sum_{kl=-1} m_i(diag(1,...,1,k,l,1,...,1)s_i)$$

for some integers $m, m_i > 0$. Now since for any $t \in T$, $\deg(ts_i) = p$, $deg(1) = 1$ and $\deg(s_i)^2 = p^2$, we have no other choice than $m = p, m_i = 1$ so we get the following relation:

$$(s_i)^2 = p(1) + \sum_{kl=-1} (diag(1,...,1,k,l,1,...,1)s_i).$$

□

CHAPTER 7

ON A CONJECTURE OF ASH

Let $U = U_n(\mathbb{F}_p)$ and

$$U^* = \{A \in GL_n(\mathbb{F}_p), A = \begin{pmatrix} 1 & * & ... & * \\ 0 & 1 & ... & * \\ . & . & . & . \\ 0 & ... & 1 & * \\ 0 & ... & 0 & * \end{pmatrix}\}.$$

Define

$$\Gamma_U = \{M \in SL_n(\mathbb{Z}),\ \overline{M} \in U\}$$

$$S_U = \{M \in M_n(\mathbb{Z}), \det M > 0, (\det M, p) = 1,\ \overline{M} \in U^*\}$$

$$\Gamma(N) = \{M \in SL_n(\mathbb{Z}), M \equiv I_n \mod N\},\ \Gamma(1) = SL_n(\mathbb{Z})$$

$$S_K(N) = \{M \in M_n(\mathbb{Z}), \det M > 0, (\det M, K) = 1, M \equiv diag(1, 1, ..., 1, *) \mod N\}$$

$$GS_K(N) = \{M \in M_n(\mathbb{Z}), \det M \neq 0, (\det M, K) = 1, M \equiv diag(1, 1, ..., 1, *) \mod N\}$$

Definition 7.1. A Hecke pair is a pair (Γ, S), where Γ is a subgroup of $GL_n(\mathbb{Z})$ containing $\Gamma(N)$ for some N, and S is a semigroup of $GL_n(\mathbb{Q})$ such that $\Gamma \subset S$.

Definition 7.2. Two Hecke pairs (Γ, S) and (Γ', S') are said to be compatible if

1) $\Gamma \subset \Gamma', S \subset S'$,

2) $\Gamma' \cap SS^{-1} = \Gamma$, and

3) $\Gamma' S = S'$.

Lemma 7.1. *a)* $(\Gamma(p), S_p(p))$ *and* (Γ_U, S_U) *are compatible Hecke pairs.*

b) (Γ_U, S_U) *and* $(\Gamma(1), S_p(1))$ *are compatible Hecke pairs.*

Proof. a) Clearly $\Gamma(p) \subset \Gamma_U$ and $S_p(p) \subset S_U$. Suppose now $\gamma \in \Gamma_U \cap S_p(p)S_p(p)^{-1}$. Then γ is congruent to $diag(1, 1, ..., 1, *)$ mod p and has determinant 1. Thus γ is congruent to $diag(1, 1, ..., 1, 1)$ mod p, so $\gamma \in \Gamma(p)$. Since the other inclusion is trivial, we get that $\Gamma_U \cap S_p(p)S_p(p)^{-1} = \Gamma(p)$. Since any matrix from U^* can be written as a product of a matrix from U and a matrix from $diag(1, 1, ..., 1, *)$ we get that $S_U \subset \Gamma_U S_p(p)$; hence $S_U = \Gamma_U S_p(p)$. Since the three conditions have been verified, we have that $(\Gamma(p), S_p(p))$ and (Γ_U, S_U) are compatible Hecke pairs.

b) Clearly $\Gamma_U \subset \Gamma(1)$ and $S_U \subset S_p(1)$. Suppose now that $\gamma \in \Gamma(1) \cap S_U S_U^{-1}$. Then $\gamma \in SL_n(\mathbb{Z})$ and $\overline{\gamma} \in U^*$. Thus $\overline{\gamma} \in U$ so $\gamma \in \Gamma_U$. So $\Gamma(1) \cap S_U S_U^{-1} = \Gamma_U$. The last thing that we have to prove is that $\Gamma(1)S_U = S_p(1)$. But from [Ash] p.238, Lemma 1.1 a), we have $\Gamma(1)S_p(p) = Sp(1)$ and since $S_p(p) \subset S_U$, we get that $\Gamma(1)S_U = Sp(1)$. So (Γ_U, S_U) and $(\Gamma(1), S_p(1))$ are compatible Hecke pairs. □

Definition 7.3. A Hecke pair (Γ, S) is called a congruence Hecke pair of level N if the following hold:

a) $(\Gamma(N), S_N(N))$ and (Γ, S) are compatible Hecke pairs,

b) (Γ, S) and $(GL_n(\mathbb{Z}), GS_N(1))$ are compatible Hecke pairs.

Corollary 7.2. (Γ_U, S_U) *is a congruence Hecke pair of level* p.

Proof. Point a) of the above definition holds because of point a) of the previous lemma.

Point b) holds because of point b) of the previous lemma, and the fact that $(\Gamma(1), S_p(1))$ and $(GL_n(\mathbb{Z}), GS_p(1))$ are compatible Hecke pairs and the relation of compatibility is transitive (see [Ash], p. 238). □

Lemma 7.3. *Let $(\Gamma, S) \to (\Gamma', S')$ be compatible Hecke pairs. Consider a morphism $(\Gamma', S') \xrightarrow{\phi} (\Gamma_1, S_1)$ of Hecke pairs (i.e $\phi : S' \to S_1$ is a morphism of semigroups and $\Gamma_1 = \phi(\Gamma)$). Define the Hecke pair $(\overline{\Gamma}, \overline{S}) = (\phi(\Gamma), \phi(S))$.*

If $(\overline{\Gamma}, \overline{S})$ and (Γ_1, S_1) are compatible Hecke pairs then we have the following commutative diagram of Hecke algebras:

$$\begin{array}{ccc} H(S'//\Gamma') & \hookrightarrow & H(S//\Gamma) \\ \downarrow & & \downarrow \\ H(S_1//\Gamma_1) & \hookrightarrow & H(\overline{S}//\overline{\Gamma}) \end{array}$$

Proof. We have such a diagram on the Hecke algebras, we only need to prove that it is commutative.

Since (Γ, S) and (Γ', S') are compatible Hecke pairs, by property 3) of the definition of compatible Hecke pairs we get that any simple coset $\Gamma' a,\ a \in S'$ is equal to $\Gamma' s$ for some $s \in S$. We thus have the following commutative diagram of single cosets:

$$\begin{array}{ccc} \Gamma' s & \to & \Gamma s \\ \downarrow & & \downarrow \\ \Gamma_1 \phi(s) & \to & \overline{\Gamma} \phi(s) \end{array}$$

Since each of these maps on cosets gives rise to a map on double cosets by joining together the simple cosets that make up the double coset, we obtain a commutative diagram on the double cosets, and on the corresponding Hecke Algebras. □

Corollary 7.4. *Let $H(p) = H(S_p(1)//\Gamma(1))$. We have the following commutative diagram of Hecke algebras:*

$$\begin{array}{ccc} H(p) & \hookrightarrow & H(S_U//\Gamma_U) \\ \downarrow & & \downarrow \\ H(GL_n(\mathbb{F}_p)//SL_n(\mathbb{F}_p)) & \hookrightarrow & H(U^*//U). \end{array}$$

Proof. We only need to prove that $H(U^*//U)$ and $H(GL_n(\mathbb{F}_p)//SL_n(\mathbb{F}_p))$ are compatible Hecke pairs. Then by applying the previous lemma, we get the result.

It is clear that $U^* \subset GL_n(\mathbb{F}_p)$ and $U \subset SL_n(\mathbb{F}_p)$. We also have $U^*SL_n(\mathbb{F}_p) = GL_n(\mathbb{F}_p)$, since by taking a matrix A of $GL_n(\mathbb{F}_p)$ and multiplying it with the inverse of $diag(1, 1, ..., 1, \det A)$ we obtain a matrix of $SL_n(\mathbb{F}_p)$.

We need now to check that $SL_n(\mathbb{F}_p) \cap U^*U^{*-1} = U$. Since U^* is a group it implies that $U^*U^{*-1} = U^*$ so we have to prove that $SL_n(\mathbb{F}_p) \cap U^* = U$ which is obvious. □

Definition 7.4. As in [Ash], given a Hecke pair (Γ, S) and a left S-module M, we define an action of the Hecke algebra $H(S//\Gamma)$ on $H^*(\Gamma, M)$. We first define the action of $\Gamma s\Gamma$ for $s \in S$ as the Hecke operator T_s defined below:

$$T_s(\beta) = tr_{\Gamma \cap s\Gamma s^{-1} \to \Gamma} res_{\Gamma \cap s\Gamma s^{-1}} s^*(\beta) \text{ for any } \beta \in H^*(\Gamma, M).$$

We extend this action to the entire Hecke algebra $H(S//\Gamma)$ by linearity.

We also define $T_{l,k}$ to be the Hecke operator corresponding to the double coset $\Gamma diag(1, ..., 1, l, ..., l)\Gamma \in H(p)$, where l appears k times and $\Gamma = \Gamma(1)$, $S = S_p(1)$.

This action is compatible with the algebra structure because:

Proposition 7.5. *Let (Γ, S) be a Hecke pair and M be a left S-module. Then $H^*(\Gamma)$ has a structure of a right $H(S//\Gamma)$-module via the Hecke operator action described above. More precisely for any $a, b \in H(S//\Gamma)$ and any $\beta \in H^*(\Gamma, M)$:*

$$T_{ab}(\beta) = T_b(T_a(\beta)).$$

Proof. See [RW]. □

Corollary 7.6. *Under the commutative diagram from 7.4, the image of $T_{l,k} \in H(p)$ in $H(U^*//U)$ is*

$$d_{l,k}T_{Udiag(1,1,...,1,l^k)U} \text{ where } d_{l,k} = \deg(T_{l,k}) = \frac{(l^n-1)...(l^n-l^{k-1})}{(l^k-1)...(l^k-l^{k-1})}.$$

Note 7.1. The last equality has been proved in [Shi], prop. 3.18, p. 58.

Proof. The image of $T_{l,k}$ in $H(GL_n(\mathbb{F}_p)//SL_n(\mathbb{F}_p))$ is of the form $d\overline{T_{l,k}}$ where d is such that the degree is preserved. In $H(GL_n(\mathbb{F}_p)//SL_n(\mathbb{F}_p))$, $\overline{T_{l,k}}$ is in the same double coset as $diag(1, 1, ..., 1, l^k) \in U^*$. Furthermore, this double coset splits as only one single coset since $diag(1, 1, ..., 1, l^k)$ normalizes U. So $\deg \overline{T_{l,k}} = 1$. Since all maps from the above commutative diagram maintain the degree, we get that $d = d_{l,k}$. The image of $\overline{T_{l,k}}$ in $H(U^*//U)$ is $diag(1, 1, ..., 1, l^k)$, since $\overline{T_{l,k}}$ can be represented by only one single coset. Therefore the image of $T_{l,k}$ in $H(U^*//U)$ is $d_{l,k}T_{Udiag(1,1,...,1,l^k)U}$. □

Definition 7.5. Let $\beta \in H^*(U, \mathbb{F}_p)$ be an eigenclass for $T_{l,k}$ for all primes l, and all $1 \leq k \leq n$. Thus $T_{l,k}\beta = a(l, k)\beta$ for some $a(l, k) \in F_p$. Define

$$P(\beta, l) = \sum (-1)^k l^{k(k-1)/2} a(l, k) X^k.$$

Theorem 7.7. *Let $\beta \in H^*(U, \mathbb{F}_p)$ be an eigenclass for $T_{l,k}$ for all primes $l \neq p$, and all $1 \leq k \leq n$. Then there is an integer d such that the representation*

$$\rho = \omega^d \oplus \omega^{d+1} \oplus ... \oplus \omega^{d+n-1} : G_{\mathbb{Q}} \to GL_n(\mathbb{F}_p), \tag{7.1}$$

where $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, has the property that

$$P(\beta, l) = det(I - \rho(Frob_l)X) \text{ for all } l \neq p.$$

Proof. Let $T_m = T_{diag(1,1,...,1,m)}$ for any $m \in \mathbb{F}_p^*$. Then $T_{l,k} = d_{l,k}T_{l^k}$. There is a prime q that generates $\mathbb{F}_p^\times$. Since β is an eigenclass then $T_{q,1}\beta = a\beta$ for some $a \in \mathbb{F}_p^*$. The eigenvalue a is nonzero, since $a^{p-1}\beta = T_{q^{p-1}}\beta = T_1\beta = \beta$, so $a^{p-1} = 1$. But then $a = q^d$ for some $d \in \mathbb{Z}$. Then $T_{q,k}\beta = d_{l,k}(T_{q^k})\beta = d_{q,k}(T_q)^k\beta = d_{q,k}q^{dk}\beta$. For any prime l and any k we have $T_{l,k} = d_{l,k}T_{diag(1,1,...,1,l^k)} = d_{l,k}T_{q^m}$ for some m such that $l^k = q^m \pmod p$. Then $T_{l,k}\beta = d_{l,k}q^{md}\beta = d_{l,k}l^{dk}\beta$. Therefore $a(l,k) = d_{l,k}l^{dk}$ for all primes l. Then

$$\begin{aligned} P(\beta, l) &= \sum (-1)^k l^{k(k-1)/2} a(l,k) X^k = \sum (-1)^k l^{k(k-1)/2} d_{l,k} l^{kd} X^k \\ &= \sum (-1)^k l^{k(k-1)/2} d_{l,k} (l^d X)^k = \text{ (see [Shi] p.64)} \\ &= (1 - l^d X)(1 - l^{d+1}X)...(1 - l^{d+n-1}X) = \det(I - \rho(Frob_l)X) \end{aligned}$$

for the ρ given in (7.1). □

Now we prove that the Conjecture of Ash holds in our particular context:

Corollary 7.8. *The conjecture of Ash (see [Ash], p 242, Conjecture B) is true for $\Gamma = \Gamma_U, S = S_U$ and for eigenclasses $\beta \in H^*(\Gamma_U, \mathbb{F}_p)$, which are pull-backs from $H^*(U, \mathbb{F}_p)$ via the reduction mod p map $\pi : \Gamma_U \to U$.*

Proof. Recall that Conjecture B from [Ash] states:

Conjecture 7.9. *(Ash, 1992) Let (Γ, S) be a congruence Hecke pair of level N and p be a prime. Let $\mathbb{F}$ be a finite field of characteristic p. Let V be an admissible $\mathbb{F}S$ module. Suppose $\beta \in H^i(\Gamma, V)$ is an eigenclass for the action of the Hecke operators $T_{l,k}$ with eigenvalues $a(l,k) \in \mathbb{F}$ for all primes l not dividing N and all $k = 1, ..., n$.*

Then there exists a continuous semisimple representation $\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{F})$ unramified ouside pN such that

$$P(\beta, l) = det(I - \rho(Frob_l)X)$$

for all primes l not dividing pN.

In our context, $\mathbb{F} = \mathbb{F}_p$, $V = \mathbb{F}_p$, $(\Gamma, S) = (\Gamma_U, S_U)$ and $N = p$.

Since β is a pull-back from $H^*(U, \mathbb{F}_p)$, $\beta = \pi^*(\beta')$ with $\beta' \in H^*(U, \mathbb{F}_p)$. Because the map π^* is compatible with the Hecke action (see [KPS] thm. 1.3.7), β is a $T_{l,k}$-eigenclass for all primes $l \neq p$ and $k \leq n$ if and only if β' is a $T_{l,k}$-eigenclass for all primes $l \neq p$ and $k \leq n$ and the eigenvalues are the same. Thus $P(\beta, l) = P(\beta', l)$.

Now we apply the previous theorem for β' and we get the result. □

CHAPTER 8

PROPERTIES OF THE TRANSFER MAP AND OF THE HECKE OPERATORS

In this chapter we will develop some properties of the transfer map, and of the Hecke operators. We will use in Chapter 9 the properties that we will develop in the next section. We will not use the work we do in the other section, but we think that this work is important, and to our knowledge, has not been done so far.

Theorem 8.1. *Let G be a finite group and H be a subgroup of G. The transfer map $tr_{H\to G} : H^*(H, \mathbb{F}_p) \to H^*(G, \mathbb{F}_p)$ maps nilpotents to nilpotents.*

Proof. Quillen proved that an element $\alpha \in H^*(G, \mathbb{F}_p)$ is nilpotent if and only if its restriction to all elementary abelian subgroups is nilpotent.

Let thus $\alpha \in H^*(H, \mathbb{F}_p)$ be a nilpotent element. We want to prove that $tr_{H\to G}(\alpha)$ is nilpotent. We will prove that the restriction of $tr_{H\to G}(\alpha)$ to all elementary abelian subgroups is nilpotent.

Let E be an elementary abelian subgroup of G. Let $G = \cup_{g\in I} EgH$ be a double coset decomposition of G. Then

$$res_E tr_{H\to G}(\alpha) = \sum_{g\in I} tr_{E\cap gHg^{-1}\to E} res_{E\cap gHg^{-1}} g^*\alpha.$$

Now if for some $g \in I$ we have that $E \cap gHg^{-1} \neq E$ then $tr_{E\cap gHg^{-1}\to E} \equiv 0$ (see [AM] p. 72, cor 5.9). We thus get

$$res_E tr_{H\to G}(\alpha) = \sum_{g\in I, E\cap gHg^{-1}=E} res_E g^*\alpha,$$

but since α is nilpotent, $res_E g^*\alpha$ is also nilpotent so $res_E tr_{H\to G}(\alpha)$ is nilpotent (being a sum of nilpotents). Thus $tr_{H\to G}(\alpha)$ is nilpotent. □

Corollary 8.2. *The Hecke operators take nilpotents to nilpotents.*

Proof. Clear since the Hecke operators are a composition of maps (transfer, restriction and conjugation, as seen in Chapter 7) that take nilpotents to nilpotents. □

Functoriality properties of the transfer map

Lemma 8.3. *Let G be a finite group and H a normal subgroup of G. Let G' be another subgroup of G such that there exists a split exact sequence:*

$$1 \to K \to G \xrightarrow{\pi} G' \to 1$$

for some subgroup K of G. Let $H' = H \cap G'$. If $K \subset H$ then the map $G'/H' \hookrightarrow G/H$ induced by the inclusion is an isomorphism and there exists an induced split exact sequence:

$$1 \to K \to H \to H' \to 1.$$

Also $tr_{H\to G}x = tr_{H'\to G'}x$ for any $x \in H^*(H') \hookrightarrow H^*(H)$.

Proof. From the split exact sequence we have that $G'K = G$ since any element of G can be written as a product $\pi(x) \in G'$ and an element of K, namely $(\pi(x))^{-1}x$. Then

$G'H = G$ since $K \subset H$. From one of the isomorphism theorems for groups, we have that $G'/H \cap G' \simeq G'H/H$ so we get that $G'/H' \simeq G/H$, the map being that induced by the inclusion.

Now if $x \in H$ then $(\pi(x))^{-1}x \in K \subset H$, so $\pi(x) \in H$. But $\pi(x) \in G'$ so $\pi(x) \in H'$. Reciprocally, any element $y \in H'$ is in G' so $\pi(y) = y$; therefore $\pi|_H : H \to H'$ is surjective. Restricting now the given exact sequence to H, we get a split exact sequence:

$$1 \to K \to H \to H' \to 1.$$

To prove now the equality of the transfer maps, we can suppose, by dimension shifting, that $x \in H^0(H')$. Then we can find a system S of representatives for $G'/H' \simeq G/H$. Thus S will also be a system of representatives for G/H. Then

$$tr_{H' \to G'}x = \sum_{s \in G'/H'} s^*x = \sum_{s \in S} s^*x \in H^*(G') \subset H^*(G)$$

so $tr_{H' \to G'}x = \sum_{s \in S} s^*x = \sum_{s \in G/H} s^*x = tr_{H \to G}x \in H^*(G)$. □

An alternate definition of the transfer map

In this section let G be a finite group. Let $A_p(G)$ be the family of all non-trivial p-elementary abelian subgroups of G.

Definition 8.1. Define

$$\lim_{A \in A_p(G)} H^*(A, \mathbb{F}_p)$$

as the sequences $(x_A) \in \prod_{A \in A_p(G)} H^*(A, \mathbb{F}_p)$ such that $res^A_{A'}(x_A) = x_{A'}$ and $c^*_g(x_A) = x_{g^{-1}Ag}$, or equivalently $g^*(x_A) = x_{gAg^{-1}}$.

Using the restriction we can define a map

$$\phi : H^*(G, \mathbb{F}_p) \to \lim_{A \in A_p(G)} H^*(A, \mathbb{F}_p).$$

Then we have the following theorem due to Quillen:

Theorem 8.4. *(Quillen) The map ϕ has nilpotent kernel and cokernel.*

The question is whether given $H \leq G$ one can transport the transfer map

$$tr_{H \to G} : H^*(H, \mathbb{F}_p) \to H^*(G, \mathbb{F}_p)$$

to a "transfer map"

$$tr_{H \to G} : \lim_{A \in A_p(H)} H^*(A, \mathbb{F}_p) \to \lim_{A \in A_p(G)} H^*(A, \mathbb{F}_p).$$

Since $\lim_{A \in A_p(G)} H^*(A, \mathbb{F}_p)$ can in theory be computed explicitly by knowing the lattice of all the p-elementary abelian subgroups of G, we can get an explicit description of the transfer map and thus of the Hecke operators, at least modulo nilpotents.

We'll treat the simpler case $H \triangleleft G$. Let $A \in A_p(G)$. If $A \not\subset H$ let S be a system of $A - H$ double coset representatives. Then $A \cap H$ is a proper subgroup of A and by the double coset formula we have, for $x \in H^*(H)$:

$$res_A tr_{H \to G} x = \sum_{s \in S} tr_{A \cap sHs^{-1} \to A}(res^{sHs^{-1}}_{A \cap sHs^{-1}} s^* x) = \sum_{s \in S} tr_{A \cap H \to A}(res^H_{A \cap H} s^* x) = 0$$

because it is known ([AM], p. 72, Corollary 5.9) that $tr_{E' \to E} \equiv 0$ if E' is a proper subgroup of the elementary abelian group E.

If $A \subset H$, let S be a system of representatives for G/H. Then S is also a system of $A - H$ double coset representatives so by the double coset formula we have, for $x \in H^*(H)$:

$$res_A tr_{H\to G} x = \sum_{s\in S} tr_{A\cap sHs^{-1}\to A}(res^{sHs^{-1}}_{A\cap sHs^{-1}} s^* x) = \sum_{s\in S} res^H_A s^* x = \sum_{s\in S} s^* res^H_{s^{-1}As} x,$$

since $sHs^{-1} = H,\ A \cap sHs^{-1} = A$ and $tr_{A\to A}$ is the identity map. We see from here that we can give the following

Definition 8.2. If $H \triangleleft G$ define

$$tr_{H\to G} : \lim_{A\in A_p(H)} H^*(A, \mathbb{F}_p) \to \lim_{A\in A_p(G)} H^*(A, \mathbb{F}_p)$$

as follows

$$(tr_{H\to G} x)_A = \begin{cases} 0 & \text{if } A \not\subset H \\ \sum_{g\in G/H} g^*(x_{g^{-1}Ag}) & \text{if } A \subset H \end{cases}.$$

Observe that if $A \subset H$ then $g^{-1}Ag \subset g^{-1}Hg = H$ so we $x_{g^{-1}Ag}$ is defined. Also observe that in general $x_A \neq g^*(x_{g^{-1}Ag})$ since $x_A = h^*(x_{h^{-1}Ah})$ only for $h \in H$.

Proposition 8.5. *The map $tr_{H\to G}$ defined above is well defined.*

Proof. We need to check that if $A' \subset A$ then $res^A_{A'}(tr_{H\to G}x)_A = (tr_{H\to G}x)_{A'}$ and $g^*(tr_{H\to G}x)_A = (tr_{H\to G}x)_{gAg^{-1}}$ for all $g \in G$. For the first equality, if $A' \not\subset H$ then clearly $A \not\subset H$ and the equality is trivially satisfied by the definition. If $A \subset H$ then $A' \subset H$ and we have:

$$\begin{aligned} res^A_{A'}(tr_{H\to G}x)_A &= res^A_{A'} \sum_{g\in G/H} g^*(x_{g^{-1}Ag}) = \sum_{g\in G/H} g^* res^{g^{-1}Ag}_{g^{-1}A'g}(x_{g^{-1}Ag}) \\ &= \sum_{g\in G/H} g^*(x_{g^{-1}A'g}) = (tr_{H\to G}x)_{A'}. \end{aligned}$$

The last case is $A' \subset H$, $A \not\subset H$. Then we have to prove that

$$(tr_{H \to G} x)_{A'} = 0.$$

For that we need the following

Lemma 8.6. *If $E' \lhd E$ are p-groups such that there is a map $\pi : E \to E'$ such that $\pi(g) = g$ for all $g \in E'$ then*

$$\sum_{g \in E/E'} g^* x = 0 \text{ for all } x \in H^*(E').$$

Proof. If $x \in H^*(E')$ then $res_{E'} \pi^* x = x$ and therefore

$$g^* x = g^*(res_{E'} \pi^* x) = res_{E'} g^*(\pi^* x) = res_{E'}(\pi^* x) = x,$$

since g^* acts trivially on $H^*(E)$. Thus

$$\sum_{g \in E/E'} g^* x = \sum_{g \in E/E'} x = p^k x = 0.$$

□

Back now to the proof of our proposition. We can assume without loss of generality that $A' = A \cap H$ since $A' \subset A \cap H$ and the restriction from $A \cap H$ to A' has already been taken into consideration in the previous case.

Let S be a system of representatives for G/AH and $T \subset A$ be a system of representatives for A/A' thus also for $AH/H \simeq A/A \cap H = A/A'$. Then $\{ts, s \in S, t \in T\}$ is a system of representatives for G/H. We have

$$(tr_{H \to G} x)_{A'} = \sum_{s \in S, t \in T} (ts)^* (x_{(ts)^{-1} A' ts}).$$

Observe that for all $t \in T$, $tA't^{-1} \subset tAt^{-1} = A$ (since $t \in A$) and $tA't^{-1} \subset H$ so $tA't^{-1} \subset A \cap H = A'$ and by cardinality $tA't^{-1} = A'$. Thus

$$(tr_{H\to G}x)_{A'} = \sum_{s\in S, t\in T} (ts)^*(x_{s^{-1}A's})$$

but $t \in A/A'$ if and only if $u = s^{-1}ts \in s^{-1}As/s^{-1}A's$. Then $ts = su$ and

$$\begin{aligned}(tr_{H\to G}x)_{A'} &= \sum_{s\in S} \sum_{u\in s^{-1}As/s^{-1}A's} (su)^*(x_{s^{-1}A's}) = \sum_{s\in S} \sum_{u\in s^{-1}As/s^{-1}A's} s^*u^*(x_{s^{-1}A's}) \\ &= \sum_{s\in S} s^*\Big(\sum_{u\in s^{-1}As/s^{-1}A's} u^*(x_{s^{-1}A's})\Big).\end{aligned}$$

Now applying the previous lemma for the interior sum, and for $E = s^{-1}As, E' = s^{-1}A's$ (since they are elementary abelian subgroups so E' is a direct summand) we get that

$$\sum_{u\in s^{-1}As/s^{-1}A's} u^*(x_{s^{-1}A's}) = 0$$

and thus $(tr_{H\to G}x)_{A'} = 0$. We are done with the first equality.

We still have to prove the second equality, i.e., $g^*(tr_{H\to G}x)_A = (tr_{H\to G}x)_{gAg^{-1}}$ for all $g \in G$. Let $g \in G$ be fixed.

Since H is normal in G, $A \subset H$ is equivalent to $gAg^{-1} \subset H$. So if $A \not\subset H$, the equality becomes trivially satisfied.

If $A \subset H$, then $gAg^{-1} \subset H$ and

$$\begin{aligned}g^*(tr_{H\to G}x)_A &= g^*\Big(\sum_{s\in G/H} s^*(x_{s^{-1}As})\Big) = \sum_{s\in G/H} g^*s^*(x_{s^{-1}As}) \\ &= \sum_{s\in G/H} (gs)^*(x_{s^{-1}As}) = \sum_{t\in G/H} t^*(x_{t^{-1}gAg^{-1}t}) = (tr_{H\to G}x)_{g^{-1}Ag},\end{aligned}$$

where we made the substitution $t = gs$, which gives another system of representatives for G/H. □

If H is not normal in G, the problem is much harder. We can still derive a definition for the transfer map as follows:

Let A be an elementary abelian subgroup and S be a system of $A-H$ double coset representatives. Then for $x \in H^*(H)$:

$$res_A tr_{H\to G} x = \sum_{s\in S} tr_{A\cap sHs^{-1}\to A}(res^{sHs^{-1}}_{A\cap sHs^{-1}} s^* x) = \sum_{s\in S} tr_{A\cap sHs^{-1}\to A}(s^* res^H_{s^{-1}As\cap H} x).$$

If $s^{-1}As \not\subset H$ then $A \not\subset sHs^{-1}$ so $A\cap sHs^{-1}$ is a proper subgroup of A and thus the transfer map $tr_{A\cap sHs^{-1}\to A}$ is identically 0 ([AM], p. 72, Corollary 5.9). Therefore in the above sum, only the terms for which $s^{-1}As \subset H$ remain, and for those we have $A\cap sHs^{-1} = A$ so the transfer map $tr_{A\cap sHs^{-1}\to A}$ is the identity. Thus we get

$$res_A tr_{H\to G} x = \sum_{s\in S, s^{-1}As\subset H} s^* res^H_{s^{-1}As} x.$$

From here we can state the following:

Conjecture 8.7. *Define the transfer map:*

$$tr_{H\to G} : \lim_{A\in A_p(H)} H^*(A,\mathbb{F}_p) \to \lim_{A\in A_p(G)} H^*(A,\mathbb{F}_p) \text{ by}$$

$$(tr_{H\to G} x)_A = \sum_{s\in S_A, s^{-1}As\subset H} s^*(x_{s^{-1}As}),$$

where S_A is a system of $A-H$ double coset representatives.

Then this map is well defined.

CHAPTER 9

A NEW CLASS IN $H^*(GL_N(\mathbb{F}_P), \mathbb{F}_P)$

As we saw in Chapter 6, the Hecke algebra $H(GL_n(\mathbb{F}_p)//U_n)$ is generated by the double cosets of the diagonal matrices and the double cosets of the s_i, where s_i is the matrix corresponding to the transposition $(i, i+1)$.

Given a finite group G and a p-Sylow subgroup H, we know from p. 84 of [Brn] that res^G_H is a monomorphism between $H^*(G, \mathbb{F}_p)$ and $H^*(H, \mathbb{F}_p)$. We want to give a necessary and sufficient condition in terms of Hecke operators for a class in $H^*(H, \mathbb{F}_p)$ to be in $H^*(G, \mathbb{F}_p)$. The following lemma is Ex.2, p. 85 from [Brn].

Lemma 9.1. *Let G be a finite group and H be a p-Sylow subgroup. A cohomology class $\beta \in H^*(H, \mathbb{F}_p)$ is in $H^*(G, \mathbb{F}_p)$ if and only if the action of all the Hecke operators is punctual, i.e., $T_x(\beta) = \deg(x)\beta$ for all $x \in H(G//H)$.*

Proof. If $\beta \in H^*(H, \mathbb{F}_p)$ is the restriction of a class in $H^*(G, \mathbb{F}_p)$ by Theorem 10.3 p.84 of [Brn], β is G-invariant, i.e., $res^H_{H\cap gHg^{-1}}\beta = res^{gHg^{-1}}_{H\cap gHg^{-1}} g^*\beta$ for any $g \in G$. But then

$$\begin{aligned} T_g(\beta) &= tr_{H\cap gHg^{-1}\to H} res^{gHg^{-1}}_{H\cap gHg^{-1}} g^*\beta = tr_{H\cap gHg^{-1}\to H} res^H_{H\cap gHg^{-1}}\beta \\ &= (H : H\cap gHg^{-1})\beta = \deg T_g \beta. \end{aligned}$$

By linearity we get that the action of all the Hecke operators is punctual.

We now prove the other implication. Suppose that all the Hecke operators act punctually on β. Let $w = tr_{H\to G}\beta$. Let S be a system of representatives for the $H-H$ double cosets of G. Then

$$res_H w = res_H tr_{H\to G}\beta = \sum_{s\in S} tr_{H\cap sHs^{-1}\to H} res^{sHs^{-1}}_{H\cap sHs^{-1}} s^*\beta = \sum_{s\in S} T_s(\beta)$$
$$= \sum_{s\in S} (\deg T_s)\beta = \sum_{s\in S} (H : H\cap sHs^{-1})\beta = (G:H)\beta.$$

The last equality holds because $(H : H\cap sHs^{-1})$ is exactly the number of simple right cosets that compose HsH. So by taking the union of all double cosets HsH and decomposing each into simple cosets, we get all the simple cosets of G/H.

Since $(G:H)$ is prime to p, we have that $\beta = res_H \frac{1}{(G:H)} w$. □

Lemma 9.2. *A class $\beta \in H^*(U_n, \mathbb{F}_p)$ is in $H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$ if and only if:*

$T_t(\beta) = \beta$ for any $t \in T_n$ and

$T_{s_i}(\beta) = 0$ for $1 \le i \le n-1$.

Proof. By applying the previous lemma, $\beta \in H^*(U_n, \mathbb{F}_p)$ is in $H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$ if and only if all the Hecke operators act punctually on β.

Because the Hecke action is compatible with the multiplication in the Hecke algebra, it is enough to check that the elements of T_n (the subgroup of diagonal matrices) and the s_i act punctually on our class β. This is because these elements generate the Hecke algebra.

This ends our proof since the degree of the torus elements is 1 (the double coset is also a single coset since T_n normalizes U_n) and the degree of the s_i is p. □

Let's see now what is the action of T_n on the classes defined in chapter 3.

Proposition 9.3. *Let $t = diag(t_1, ..., t_n) \in T_n$. Then*

$$T_t(\gamma_{ij}) = \frac{t_j}{t_i}\gamma_{ij}.$$

Proof. Since $tU_nt^{-1} = U_n$, we have that

$$T_t(\gamma_{ij}) = tr_{U_n \to U_n} t^*(\gamma_{ij}) = t^*(\gamma_{ij});$$

observe that $\gamma_{ij} = N_{H_{ij} \to U_n}\zeta_{ij}$ where H_{ij} are defined in remark 3.2. Let $H = H_{ij}$. Then $tHt^{-1} = H$ as can be checked easily. Looking at the following morphism

$$\phi : U_n \to U_n,\ \phi(x) = t^{-1}xt$$

and using the functoriality property of the norm map (N5, p. 58 in [Ev]), we get

$$\begin{aligned} t^*(\gamma_{ij}) &= \phi^*(N_{H \to U_n}\zeta_{ij}) = N_{H \to U_n}\phi^*(\zeta_{ij}) = N_{H \to U_n}(\frac{t_j}{t_i}\zeta_{ij}) \\ &= \left(\frac{t_j}{t_i}\right)^{p^k} N_{H \to U_n}(\zeta_{ij}) = \frac{t_j}{t_i}\gamma_{ij}. \end{aligned}$$

□

For $U_2 = \mathbb{Z}/p$ we see that $H^{ev}(U_2)$ (even cohomology) is a polynomial ring in one indeterminate generated by the element $\alpha \in H^2(U_2)$ corresponding to the canonical morphism $U_2 \to \mathbb{F}_p$. From the above proposition, we see that α^k is invariant to the action of T_2 if and only if $(p-1)|k$. It is easy to see that $T_{s_1} \equiv 0$, so $\alpha^{k(p-1)} \in H^*(GL_2(\mathbb{F}_p))$. Let $\chi_2 = \alpha^{p-1}$.

For each U_n we embed U_k with $k < n$ as the U_{k1} using the notation of chapter 3. We saw that this way we have $H^*(U_k) \hookrightarrow H^*(U_n)$.

For U_3, let $\chi_3 = \chi_2 + T_{s_2}(\chi_2)$. It is easy to see that

$$U_3 \cap s_2 U_3 s_2^{-1} = \{A \in U_3, A = \begin{pmatrix} 1 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\}$$

and let's denote this subgroup by H. Then we can write

$$\chi_3 = \alpha^{p-1} + tr_{H \to U_3} s_2^*(\alpha^{p-1}).$$

Observe that $s_2^*(\alpha) = \gamma$ where $\gamma \in H^2(H)$ comes from the morphism

$$\gamma : H \to \mathbb{F}_p, \quad \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to b,$$

thus we get that

$$\chi_3 = \alpha^{p-1} + tr_{H \to U_3} \gamma^{p-1}.$$

Let us now define $\chi_3' = \beta^{p-1} + T_{s_1}(\beta^{p-1}) = \beta^{p-1} + tr_{H_p \to U_3} \gamma_1^{p-1}$, where $\beta \in H^2(U_3)$ resp. $\gamma_1 \in H^2(H_p)$ come from the morphisms

$$\beta : U_3 \to \mathbb{F}_p, \quad \begin{pmatrix} 1 & * & * \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \to b, \quad \gamma_1 : H_p \to \mathbb{F}_p, \quad \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \to c.$$

Proposition 9.4. *With the above notations we have:*

$$\chi_3 = \chi_3'.$$

Proof. First we have that χ_3 and χ_3' actually come from $H^{2(p-1)}(U_3, \mathbb{Z})$ via reduction mod p. This is easy to see, since we can define similar elements χ_3 and χ_3' in $H^{2(p-1)}(U_3, \mathbb{Z})$ and the transfer map $tr_{H \to U_3}$ commmutes with reduction mod p.

Now we will prove that $\chi_3 = \chi_3'$ in $H^*(U_3, \mathbb{Z})$ and this will give us the result, since then their images in $H^*(U_3, \mathbb{F}_p)$ will be equal. In this proof from now on, we will be working with $\mathbb{Z}$ coefficients.

Now we will prove that the restriction of χ_3 and χ_3' to all the subgroups H_i defined in thm. 4.2 is the same mod p (i.e., their difference is a multiple of p).

We first compute the restriction of χ_3 to all H_i from 4.2. Since the subgroup H from the definition of χ_3 is actually H_0, we have that $HH_i = U_3$ for $i = 1, 2, ..., p$ (since H is of index p in U_3 and HH_i is a subgroup strictly larger than H). Thus by the double coset fromula ([Ev], Thm.4.2.6, p. 41) we have

$$res_{H_i} tr_{H \to U_3} \gamma^{p-1} = tr_{H \cap H_i \to H_i} res_{H \cap H_i} \gamma^{p-1} = 0 \mod p \text{ for i=1,2,...,p}$$

since it is known (Cor. 5.9, p 72 in [AM]) that the transfer map from a proper subgroup to an elementary abelian group is zero when we are working with $\mathbb{F}_p$ coefficients, and the transfer map commutes with reduction mod p. So the image in $H^*(U_3, \mathbb{F}_p)$ of $res_{H_i} tr_{H \to U_3} \gamma^{p-1}$ is 0, so $res_{H_i} tr_{H \to U_3} \gamma^{p-1} = 0 \mod p$ in $H^*(U_3, \mathbb{Z})$. We thus have that

$$res_{H_i} \chi_3 = res_{H_i} \alpha^{p-1} \mod p \text{ for } i = 1, 2, ..., p.$$

Let $\alpha_i \in H^2(H_i)$ be defined by the morphism $\alpha_i : H_i =< A_i, Z > \to \mathbb{Q}/\mathbb{Z}$ given by

$\alpha_i(A_i^k B^l) \to k/p$ (B being a generator of $Z = Z(U_3)$). Then $res_{H_i}\alpha = \alpha_i$ if $i < p$ and $res_{H_p}\alpha = 0$ so we can rewrite the above equation as follows

$$res_{H_i}\chi_3 = \alpha_i^{p-1} \text{ for } i = 1, 2, ..., p-1 \text{ and } res_{H_p}\chi_3 = 0,$$

everything being $\mod p$. Now for $H = H_0$ the matrices $C_i = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$ with $i = 0, 1, ..., p-1$ are a complete system of double (and single) H coset representatives so we have

$$res_H\chi_3 = \alpha_0^{p-1} + res_H tr_{H\to U_3}\gamma^{p-1} = \alpha_0^{p-1} + \sum_{i=0}^{p-1} res_H C_i^*(\gamma)^{p-1}$$
$$= \alpha_0^{p-1} + \sum_{i=0}^{p-1}(res_H\gamma + i\alpha_0)^{p-1} = \alpha_0^{p-1} + (p-1)\alpha_0^{p-1} = 0,$$

also mod p. Here we used the binomial formula for each $(res_H\gamma + i\alpha_0)^{p-1}$ and we kept into account that $\sum_{i=0}^{p-1} i^k = 0 \mod p$ for $1 \le k < p-1$ and $\sum_{i=0}^{p-1} i^{p-1} = p-1 \mod p$. In conclusion, we have that $res_{H_0}\chi_3 = res_{H_p}\chi_3 = 0 \mod p$ and $res_{H_i}\chi_3 = \alpha_i^{p-1} \mod p$ for $i = 1, 2, ..., p-1$.

Similarly to what we did above, we check that $res_{H_i} tr_{H_p\to U_3}\gamma_1^{p-1} = 0 \mod p$ for $i = 0, 1, ..., p-1$ and $res_{H_p} tr_{H_p\to U_3}\gamma_1^{p-1} = -res_{H_p}\beta^{p-1} \mod p$. We also see that $res_{H_i}\beta = i\alpha_i$ for $i = 0, 1, ..., p-1$ so $res_{H_0}\beta^{p-1} = 0$ and $res_{H_i}\beta^{p-1} = \alpha_i^{p-1}$ for $i = 1, ..., p-1$.

Putting these all together, we get that $res_{H_0}\chi_3' = res_{H_p}\chi_3' = 0 \mod p$ and $res_{H_i}\chi_3' = \alpha_i^{p-1} \mod p$ for $i = 1, 2, ..., p-1$. This implies that $res_{H_i}\chi_3 = res_{H_i}\chi_3' \mod p$ for $i = 0, 1, ..., p$ i.e. χ_3 and χ_3' have the same restriction mod p on all H_i.

Looking in [Lew], p. 523, Thm. 6.26, we see that $H^{2(p-1)}(U_3, \mathbb{Z})$ is generated by $\alpha^i \beta^{p-1-i}$ $(i = 0, 1, ..., p-1)$ and χ_{p-2} (using the notation from [Lew]). Actually the α and the β have the same meaning, while χ_{p-2} is our χ_3'. These are all the generators for $H^{2(p-1)}(U_3, \mathbb{Z})$ because the other potential generators are zero. We can get other potential generators by multiplying a χ_i for $i < p-2$ with one of $\alpha, \beta, \mu, \nu, \chi_j$ $(j < p-2)$, but this product is zero. We could also get other potential generators for $p > 3$ by multiplying $\mu\nu$ with something, but $\mu\nu = \chi_2/d, d \in \mathbb{F}_p^*$ so we have already taken this potential generator into consideration.

Because of this we can write

$$\chi_3 - \chi_3' = f(\alpha, \beta) + a\chi_3',$$

where $f(X, Y) \in \mathbb{F}_p[X, Y]$ (since $p\alpha = p\beta = 0$) is a homogeneous polynomial of degree $p-1$ and $a \in \mathbb{F}_p$ (since $p\chi_3' = 0$). Restricting to all H_i we get

$$f(X, 0) = f(0, X) = 0, f(X, iX) + aX^{p-1} = 0 \text{ for i=1,2,...,p-1.}$$

From here, by considering the homogeneous polynomial $g(X, Y) = f(X, Y) + aX^{p-1}$ we get that $g(X, iX) = 0$ for $i = 1, ..., p-1$ and $g(0, X) = 0$. By making the change of variable $X \leftarrow iX$ for $i \neq 0$, we get that $g(iX, X) = 0$ for $i = 0, ..., p-1$ so the polynomial $h(X) = g(X, 1)$ has the property $h(i) = 0$ for $i = 0, ..., p-1$, but it is of degree $p-1$ so it must be identically 0. So $g(X, Y) \equiv 0$ and $f(X, Y) = -aX^{p-1}$ and from $f(X, 0) = 0$ we get that $a = 0$ so $f(X, Y) \equiv 0$. This implies that $\chi_3 - \chi_3' = 0$. $\square$

Proposition 9.5. $\chi_3 \in H^*(GL_3(\mathbb{F}_p), \mathbb{F}_p)$.

Proof. Because of Lemma 9.2, we just have to check that $T_t(\chi_3) = \chi_3$ for all $t \in T_3$ and $T_{s_i}(\chi_3) = 0$.

We have, for $t = diag(t_1, t_2, t_3)$:

$$T_t(\chi_3) = T_t(\alpha^{p-1}) + T_t(T_{s_2}\alpha^{p-1}) = (t_2/t_1)^{p-1}\alpha^{p-1} + T_{s_2 t}(\alpha^{p-1})$$
$$= \alpha^{p-1} + T_{s_2}T_{t'}(\alpha^{p-1}) = \alpha^{p-1} + T_{s_2}(\alpha^{p-1}) = \chi_3,$$

since we saw that $(s_i)(t) = (s_i t) = (t' s_i) = (t')(s_i)$ for some $t' \in T_3$.

For T_{s_1} we have

$$T_{s_1}(\chi_3) = T_{s_1}(\beta^{p-1}) + T_{(s_1)(s_1)}(\beta^{p-1}) = T_{s_1}(\beta^{p-1}) + T_{p(1)+\sum_{i=1}^{p-1}(t_i s_1)}(\beta^{p-1})$$
$$= T_{s_1}(\beta^{p-1}) + \sum_{i=1}^{p-1} T_{(t_i s_1)}(\beta^{p-1}) = pT_{s_1}(\beta^{p-1}) = 0.$$

The fact that $T_{s_2}(\chi_3) = 0$ is done similarly, but using the other definition of χ_3, namely $\chi_3 = \alpha^{p-1} + T_{s_2}(\alpha^{p-1})$. □

Definition 9.1. Define iteratively $\chi_n = \chi_{n-1} + T_{s_{n-1}}(\chi_{n-1}) \in H^*(U_n, \mathbb{F}_p)$, where χ_2 and χ_3 have already been defined. Here we used the embedding of U_{n-1} in U_n that has been described earlier in this chapter.

Definition 9.2. Define $H_k \leq U_n,\ k = 1, ..., n-1$ to be the subgroups

$$H_k = \{A \in U_n, A = (a_{ij})_{i,j}, a_{k,k+1} = 0\}.$$

Remark 9.1. It is easy to check that $H_i = U_n \cap s_i U_n s_i^{-1}$.

Theorem 9.6. $\chi_n \in H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$.

Proof. We first prove that

$$T_t(\chi_n) = \chi_n \text{ for all } t \in T_n.$$

We do that by proving that $T_t(\chi_k) = \chi_k$ in U_n, for $k = 2, ..., , n$. We proceed by induction on k.

Case $k = 2$ is trivial: $T_t(\chi_2) = T_t(\alpha^{p-1}) = (t_2/t_1)^{p-1}\alpha^{p-1} = \alpha^{p-1}$.

Suppose case k is proved; let's prove it for $k + 1$:

$$T_t(\chi_{k+1}) = T_t(\chi_k + T_{s_k}(\chi_k)) = \chi_k + T_{s_k}T_{t'}(\chi_k) = \chi_k + T_{s_k}(\chi_k) = \chi_{k+1},$$

where $t' \in T$ is such that $s_k t = t' s_k$.

We are left to prove that:

$$T_{s_i}(\chi_n) = 0 \text{ for } i = 1, 2, ..., n - 1.$$

We proceed by induction on n. We already saw that for $n = 2$ and $n = 3$ the theorem is true, so the above relation is verified.

Suppose now that the above relation is true for n and $n - 1$ and let's prove it for $n + 1$, $n \geq 3$. We have

$$T_{s_i}(\chi_{n+1}) = T_{s_i}(\chi_n) + T_{s_i}T_{s_n}(\chi_n).$$

If $i < n - 1$ we have $(s_n)(s_i) = (s_i)(s_n)$ so

$$T_{s_i}(\chi_{n+1}) = T_{s_i}(\chi_n) + T_{s_n}T_{s_i}(\chi_n) = 0 + 0 = 0,$$

because lemma 8.3 says that $T_{s_i}x,\ x \in H^*(U_{n-1})$ is the same when regarded in U_{n-1} and in U_n. The induction hypothesis implies that $T_{s_i}(\chi_n) = 0$.

For $i = n-1$ we have

$$T_{s_{n-1}}(\chi_{n+1}) = T_{s_{n-1}}(\chi_n) + T_{s_{n-1}}T_{s_n}(\chi_n) = 0 + T_{s_{n-1}}T_{s_n}(\chi_{n-1} + T_{s_{n-1}}(\chi_{n-1}))$$
$$= T_{s_{n-1}}T_{s_n}(\chi_{n-1}) + T_{s_{n-1}}T_{s_n}T_{s_{n-1}}(\chi_{n-1}) = T_{s_{n-1}}T_{s_n}(\chi_{n-1}) +$$
$$+ T_{s_n}T_{s_{n-1}}T_{s_n}(\chi_{n-1}) = 0 + 0 = 0.$$

We used here

$$T_{s_n}(\chi_{n-1}) = tr_{H_n \to G} res_{H_n}(s_n^* \chi_{n-1}) = tr_{H_n \to G}(res_{H_n}\chi_{n-1}) = p\chi_{n-1} = 0$$

and the relation $(s_{n-1})(s_n)(s_{n-1}) = (s_n)(s_{n-1})(s_n)$.

For $i = n$ we have

$$T_{s_n}(\chi_{n+1}) = T_{s_n}(\chi_n) + T_{s_n s_n}(\chi_n) = T_{s_n}(\chi_n) + \sum_{i=1}^{p-1} T_{t_i s_n}(\chi_n)$$
$$= T_{s_n}(\chi_n) + \sum_{i=1}^{p-1} T_{s_n}(\chi_n) = pT_{s_n}(\chi_n) = 0,$$

since we saw that $(s_i)^2 = p(1) + \sum_{j=1}^{p-1}(t_j)(s_i)$ where t_j are some elements of the torus T_{n+1} and we already saw that the elements of T_{n+1} act trivially on χ_n. □

Now that we proved that this class is invariant to the whole Hecke algebra, we ask ourselves: Is this class non-zero? This class is of degree $2(p-1)$ and it is known that $H^k(GL_n(\mathbb{F}_p), \mathbb{F}_p) = 0$ for $k < n$ by a theorem of Maazen (see [MP]).

So if $2(p-1) < n$ our class will be zero. But we can prove

Theorem 9.7. *If $p \geq n$ then $\chi_n \neq 0$.*

Proof. Let

$$U = \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & ... & 1 \\ 0 & 0 & 0 & ... & 0 \end{pmatrix} \in M_n(\mathbb{F}_p).$$

Then the subgroup $E =< I_n + U > \leq U_n$ is elementary abelian, because $I_n + U$ has order p. Actually $(I_n + U)^p = I_n^p + U^p = I_n$ since $U^p = 0$ ($U^n = 0$ and $p \geq n$).

We have $EH_i = U_n$ for all $i = 1, ..., n-1$ since H_i is a subgroup of index p in U_n and $E \not\subset H_i$. Because of this, the $E - H_i$ double coset decomposition of U_n has only one coset and we have

$$\begin{aligned} res_E\chi_n &= res_E\chi_{n-1} + res_E tr_{H_{n-1}\to U_n} res_{H_{n-1}}(s_{n-1}^*(\chi_{n-1})) \\ &= res_E\chi_{n-1} + tr_{0\to E} res_0(s_{n-1}^*(\chi_{n-1})) = res_E\chi_{n-1} + 0 = res_E\chi_{n-1}. \end{aligned}$$

We can repeat the computation and we successively get that

$$res_E\chi_n = res_E\chi_{n-1} = ... = res_E\chi_3 = res_E\chi_2 = res_E\alpha^{p-1} = \alpha_E^{p-1} \neq 0,$$

where $\alpha_E \in H^2(E)$ is the generator of the polynomial part of $H^*(E)$. □

Remark 9.2. Observe that for $n = 2, 3$, the class we defined is an important generator of $H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$:

The class χ_2 is the generator α^{p-1} of $H^*(GL_2(\mathbb{F}_p), \mathbb{F}_p)$. Note that $H^*(GL_2(\mathbb{F}_p), \mathbb{F}_p)$ has only two generators, one being α^{p-1} while the other is nilpotent of degree $2p-3$ (see [Agu]).

The class χ_3 is the image of the generator

$$b_{p-2} \in H^*(GL_3(\mathbb{F}_p), \mathbb{Z})_{(p)}.$$

of $H^*(GL_3(\mathbb{F}_p), \mathbb{Z})_{(p)}$(from [TY1]) via the reduction mod p map.

Remark 9.3. The only classes defined for general $H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$ that we know of have been found by Milgram and Priddy in [MP]. These classes are detected on certain maximal p-tori of block form. Our class is not one of those since our class is zero when restricted to all maximal p-tori of block form:

Proposition 9.8. *If E is an elementary abelian subgroup (p-torus) of $GL_n(\mathbb{F}_p)$ of block form, i.e., A_k from definition 3.1 for some k and $n > 2$, then $res_E \chi_n = 0$.*

Proof. We do this by induction on n.

For $n = 3$ this has been done already in the proof of Proposition 9.4, since there are only two maximal p-tori of block form in U_3, namely H_0 and H_p so E must be one of them.

Supose now that we proved that $res_E \chi_n = 0$ for all p tori E of block form of U_n, and let's prove that $res_E \chi_{n+1} = 0$. We have

$$res_E \chi_{n+1} = res_E \chi_n + res_E tr_{H_n \to U_{n+1}} s_n^* \chi_n.$$

But actually $\chi_n \in H^*(U_n)$ where the embedding of U_n in U_{n+1} has been defined earlier in this chapter. We have the commutative diagram

$$\begin{array}{ccc} E & \to & E \cap U_n \\ \downarrow & & \downarrow \\ U_{n+1} & \to & U_n, \end{array}$$

where the horizontal maps are obtained by truncating a $(n+1)\times(n+1)$ matrix to the $n\times n$ matrix from the upper left-hand corner. From here we get a commutative diagram in cohomology

$$\begin{array}{ccc} H^*(U_n) & \hookrightarrow & H^*(U_{n+1}) \\ \downarrow res & & \downarrow res \\ H^*(E\cap U_n) & \hookrightarrow & H^*(E), \end{array}$$

so we get that $res_E\chi_n = res_{E\cap U_n}\chi_n$. Since $E\cap U_n$ is a p-torus of block form in U_n, we get by the induction hypothesis that $res_{E\cap U_n}\chi_n = 0$ so $res_E\chi_n = 0$.

To compute $res_E tr_{H_n\to U_{n+1}} s_n^*\chi_n$ we have two cases.

The first case is $E\not\subset H_n$. Then $EH_n = U_{n+1}$, so by the double coset formula

$$res_E tr_{H_n\to U_{n+1}} s_n^*\chi_n = tr_{E\cap H_n\to E} res_{E\cap H_n} s_n^*\chi_n = 0,$$

since the transfer map $tr_{E'\to E}$ is identically zero if E' is a proper subgroup of the elementary abelian subgroup E. From here we get $res_E\chi_{n+1} = 0+0 = 0$.

The second case is $E\subset H_n$. Then the matrices

$$t_i = \begin{pmatrix} I_{n-1} & 0 & 0 \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \quad i = 0,...,p-1$$

form a system of representatives for the $E-H_n$ double cosets of U_{n+1}. By the double coset formula

$$res_E tr_{H_n\to U_{n+1}} s_n^*\chi_n = \sum_{i=0}^{p-1} res_E t_i^* s_n^*\chi_n = \sum_{i=0}^{p-1} t_i^* s_n^* res_E\chi_n = 0,$$

since t_i and s_n normalize E. Thus $res_E\chi_{n+1} = 0+0 = 0$. □

Looking again at the classes defined by Milgram and Priddy, we see that the only classes that they defined explicitly for $p > 2$ and $n > 2$ are of degree bigger than $2p - 2$. So our class is not even in the ring generated by these classes.

It is likely that our class is the Bockstein of a class in $H^{2p-3}(GL_n(\mathbb{F}_p), \mathbb{F}_p)$.

The question is now: Can there be non-zero classes in $H^*(GL_n(\mathbb{F}_p), \mathbb{F}_p)$ of degree less than $2p - 3$?

As referred by Milgram and Priddy in [MP], work of Quillen and of Maazen shows that for $p > 2$:

$$H^k(GL_n(\mathbb{F}_p), \mathbb{F}_p) = 0 \text{ for } k < n.$$

So the classes cannot have very low degree, but if $p \geq n$ there is still a gap between n and $2p - 3$ where there might still be some non-zero classes.

For $n = 2$ from [Agu] we get that the smallest degree of a class is $2p - 3$. So we dare to state the following

Conjecture 9.9. *If $n \geq 2$ and $p \geq 3$ then*

$$H^k(GL_n(\mathbb{F}_p), \mathbb{F}_p) = 0 \textit{ for } k < 2p - 3.$$

BIBLIOGRAPHY

[Agu] J. Aguadé. Cohomology of the GL_2 of a finite field. *Arch Math* **34** (1980) pp. 509-516

[Ash] A. Ash. Galois representations attached to mod p cohomology of $GL(n\mathbb{Z})$. *Duke Math. Journal* **65** (1992) pp. 235-255

[AM] A. Adem, J. Milgram. Cohomology of Finite Groups. Springer-Verlag, Berlin, 1994

[Brn] K. Brown. Cohomology of Groups. Springer-Verlag, New York, 1982

[Ev] L. Evens. The Cohomology of Groups. Oxford University Press, New York, 1991

[Ho] R. Howe. Harish-Chandra homomorphisms for p-adic groups. *Regional Conference Series in Mathematics* **59**, American Mathematical Society, Providence, 1985

[KPS] M. Kuga, W. Parry, C. H. Sah. Group cohomology and Hecke operators. Manifolds and Lie groups. *Progr. Math.* **14**, Birkhuser, Boston, Mass., 1981. pp. 223-266

[Lry] I. J. Leary. The mod-p cohomology rings of some p-groups. *Math. Proc. Camb. Phil. Soc.* **112** (1992), pp. 63-75

[Lew] G. Lewis. The integral cohomology rings of groups of order p^3. *Trans. Amer. Math. Soc.* **132** (1968), pp. 501-529

[MP] R.J. Milgram, S.B. Priddy. Invariant theory and $H^*(GL_n(\mathbb{F}_p); \mathbb{F}_p)$. *J. pure. appl. alg.* **44** (1987) pp. 291-302

[Qu] D. Quillen. On the Cohomology and K-theory of the general lineal group over a finite field. *Ann. of Math.* **96** (1972) pp. 552-586

[RW] Y.H. Rhie, G. Whaples. Hecke operators in cohomology of groups. *J. Math. Soc Japan.* **22** (1970) pp. 431-442

[Shi] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Princeton University Press, Princeton, NJ, 1994

[TY1] M. Tezuka, N. Yagita. The mod p Cohomology Ring of $GL_3(\mathbb{F}_p)$. *Journal of Algebra* **81** (1983), pp 295-303

[TY2] M. Tezuka, N. Yagita. The cohomology of subgroups of $GL_n(F_q)$, *Contemporary mathematics* **19** (1983), pp 379-396

[Ya] N. Yagita. Localization of the spectral sequence converging to the cohomology of an extra special p-group for odd prime p, *Osaka Journal of Mathematics* **35** (1998), pp 83-116.

[ZS] O. Zariski, P. Samuel. Commutative Algebra. vol. 2. Springer-Verlag, New York, 1975