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

ADRIAN BARBU
THE OHIO STATE UNIVERSITY
231 W. 18-TH AVE., COLUMBUS, OH 43210, USA

Abstract. We compute all the relations in cohomology satisfied by the elements of degree two of $H^*(U_n(\mathbb{F}_p), \mathbb{Z})$ where $p \geq n$ and $U_n(\mathbb{F}_p)$ is the group of of upper triangular matrices of $GL_n(\mathbb{F}_p)$ with 1 on the main diagonal.

e-mail: abarbu@math.ohio-state.edu

1. Introduction

The cohomology of $GL_n(\mathbb{F}_p)$ with $\mathbb{Z}$ or $\mathbb{F}_p$ coefficients has not been calculated to date except for $n \leq 3$. The mod p cohomology of $GL_3(\mathbb{F}_p)$ has been 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 $\mathbb{F}_q$ coefficients for $q \neq p$ and he stated that the case $p = q$ is very difficult.

In general (see [Br], chapter III, Theorem 10.3) the p-part of the cohomology of a group G can be computed from the cohomology of one of its p-Sylow subgroups H, by finding the G-invariant elements of $H^*(H)$. The mod 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, namely $U_n(\mathbb{F}_p)$, the group of upper triangular matrices of $GL_n(\mathbb{F}_p)$ with 1 on the diagonal.

Lewis computed the integral cohomology of $U_3(\mathbb{F}_p)$ in [Le]. Tezuka and Yagita used Lewis's result to find the mod p cohomology of $GL_3(\mathbb{F}_p)$ using exactly the method described above.

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.

In this paper 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 $H^*(U_n, \mathbb{Z})$. It will be easy to see that this ring has dimension $\left[\frac{n}{2}\right]$. The Krull dimension of the ring $H^*(U_n)$ is $\left[\frac{n^2}{4}\right]$. This is because of a result due to Quillen, that the Krull dimension of $H^*(G)$ for some group G is equal to the maximal rank of an elementary abelian subgroup of G (see [AM], p. 143). From [MP], prop. 5.2 we find out that the maximal rank of an elementary abelian subgroup of U_n is $\left[\frac{n^2}{4}\right]$. So it is clear that there is always more than just the cohomology that comes from degree 2.

Date: June 15, 2000.

In a subsequent paper we will define some more cohomology classes that together with the classes of degree 2 will generate a ring of the same dimension as the entire cohomology ring. This has also been done in [TY2] but our classes have smaller degree. In [Ya] the author computes the cohomology of U_4 after inverting some cohomology classes. We will compute the ideal of relations between the classes mentioned above modulo nilpotents in the case of U_4.

The main theorem we prove in this paper 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:*

$$\mathbb{Z}[X_1,\dots,X_n]'/(X_1^pX_2 - X_2^pX_1, X_2^pX_3 - X_3^pX_2, \dots, X_{n-1}^pX_n - X_n^pX_{n-1})$$

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

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.

The methods used in proving this result are purely algebraic. No spectral sequences or topological methods are used, except for those implicit in our use of Lewis's results.

2. Notations

Let $k = \mathbb{F}_p$. Denote

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

$I_n = (X_1^pX_2 - X_2^pX_1, X_2^pX_3 - X_3^pX_2, \dots, X_{n-1}^pX_n - X_n^pX_{n-1})$ ideal in R_n

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

$J_p = I_nR_{n+1} + X_nR_{n+1}$ ideal in R_{n+1}

where the corresponding n will be clear from the context.

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

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

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

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

Proposition 3.1. *Let $n \geq 2$. Then the following statements hold:*

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

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

(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 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 $b_i \in k$ (it makes sense to multiply X_n with an element of k 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 $g = u_0 + u_1Y + \ldots$ with $u_i \in R_n/I_n$. The coefficient of Y^0 in the middle product above is

$$tx_n^{l+1}u_0 \quad \text{with } t = (-1)^l \prod_{k=1}^{l} b_k \in k - \{0\}$$

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 $x_n u_0 = 0$. Therefore:

$$\begin{aligned}\overline{f} &= \prod_{k=1}^{l}(Y - b_k x_n)\; x_n g = \prod_{k=1}^{l}(Y - b_k x_n)(x_n u_0 + x_n u_1 Y + \dots)\\ &= x_n Y \prod_{k=1}^{l}(Y - b_k x_n)(u_1 + u_2 Y + \dots)\\ &= x_n \prod_{k=1}^{l+1}(X_{n+1} - a_k x_n)(u_1 + u_2 Y + \dots)\end{aligned}$$

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

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

and this proves that (a_n) holds.

$(a_n) \Longrightarrow (b_n)$:

We have the following embedding:

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

Because (a_n) holds we get that:

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

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 $R_{n+1}/J_k, k = 0, \dots, p-1$ are reduced since we supposed (c_n) holds, and because of this R_n/I_n and R_{n-1}/I_{n-1} are reduced and 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 $R_{n+1}/J_k, k = 0, \dots, p$ 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 3.2.

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

Proof. This has been proved while proving Prop.3.1. □

Lemma 3.3. $\mathbb{Z}[X_1,\dots,X_{l-1},X_{l+1},\dots,X_n]'\cap(I_n+X_lR_n)\subset I_n$.

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

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

$$a=(X_1^pX_2-X_2^pX_1)a_1+(X_2^pX_3-X_3^pX_2)a_2+\dots+(X_{n-1}^pX_n-X_n^pX_{n-1})a_n$$

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

$$a=(X_1^pX_2-X_2^pX_1)a_1'+(X_2^pX_3-X_3^pX_2)a_2'+\dots+(X_{l-2}^pX_{l-1}-X_{l-1}^pX_{l-2})a_{l-2}'$$
$$+(X_{l+1}^pX_{l+2}-X_{l+2}^pX_{l+1})a_{l+1}'+\dots+(X_{n-1}^pX_n-X_n^pX_{n-1})a_n'+X_lu$$

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

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

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

Since $f-a'\in\mathbb{Z}[X_1,\dots,\hat{X}_l,\dots,X_n]'$ 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 3.4.

$$\bigcap_{i=1}^{l}(I_n+X_iR_n)=I_n+X_1\dots X_lR_n$$

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

The general case: It is clear that $\bigcap_{i=1}^{l}(I_n+X_iR_n)\supset I_n+X_1\dots X_lR_n$. To show the other inclusion let $f\in\bigcap_{i=1}^{l}(I_n+X_iR_n)$. Then $f\in\bigcap_{i=1}^{l-1}(I_n+X_iR_n)$ and by the induction hypothesis we get that $f\in I_n+X_1\dots X_{l-1}R_n$. Thus $f=a+X_1\dots X_{l-1}u=b+X_lv$ (since $f\in I_n+X_lR_n$) with $a,b\in I_n$ and $u,v\in R_n$. Write $u=u_1+X_lu_2$ with $u_1\in\mathbb{Z}[X_1,\dots,X_{l-1},X_{l+1},\dots,X_n]'$ and $u_2\in R_n$. Then

$$f=a+X_1\dots X_{l-1}u_1+X_1\dots X_lu_2=b+X_lv.$$

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

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

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

$$f=a+X_1\dots X_{l-1}u_1+X_1\dots X_lu_2\in I_n+X_1\dots X_lR_n.$$

This means that $\bigcap_{i=1}^{l}(I_n+X_iR_n)\subset I_n+X_1\dots X_lR_n$ and therefore

$$\bigcap_{i=1}^{l}(I_n+X_iR_n)=I_n+X_1\dots X_lR_n.$$

□

Proposition 3.5. *If $f\in I_n+X_1\dots X_nR_n$ is nonconstant and homogeneous, such that*

$$f(a_1,\dots,a_n)=0\quad\forall\ a_1,\dots,a_n\in k$$

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 k^n (because $a \in I_n$), it is enough to prove that if $X_1 \dots X_n u$ vanishes on all k^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 $a, b \in k$. 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 $a \in k$. Therefore g is divisible by $X - a$ for all $a \in k$ thus g is divisible by $X^p - X$. From this we get that f is divisible by $X^p Y - XY^p$ and case $n = 2$ is proved.

The general case: Write

$$\begin{aligned} u = u_1 + (X_n - X_{n-1})u_2 + (X_n - X_{n-1})(X_n - 2X_{n-1})u_3 + \dots + \\ + (X_n - X_{n-1}) \dots (X_n - (p-1)X_{n-1})u_p \end{aligned} \tag{3.1}$$

with $u_1, \dots, u_{p-1} \in R_{n-1}$ and $u_p \in R_n$. This is possible since 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 look 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 $\{1, X_n, X_n^2, \dots, X_n^{p-1}\}$ to $\{1, (X_n - X_{n-1}), (X_n - X_{n-1})(X_n - 2X_{n-1}), \dots, (X_n - X_{n-1}) \dots (X_n - (p-1)X_{n-1})\}$ 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 $1, X_n, X_n^2, \dots, X_n^{p-1}$ as 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}.

Then from (3.1) we get

$$\begin{aligned} f = X_1 \dots X_n u_1 + X_1 \dots X_n (X_n - X_{n-1})u_2 + \dots + \\ + X_1 \dots X_n (X_n - X_{n-1}) \dots (X_n - (p-2)X_{n-1})u_{p-1} + \\ + X_1 \dots X_{n-1}(X_n^p X_{n-1} - X_n X_{n-1}^p)u_p. \end{aligned} \tag{3.2}$$

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 k. Let now $X_1, \dots, X_{n-1}$ take any non-zero values in k and fix them. Let a be the value of X_{n-1}. Let X_n take the values $a, 2a, \dots, (p-1)a$. Because $X_1, \dots, X_{n-1}$ take some fixed values in k, it follows that $u_1, \dots, u_{p-1}$ also take some fixed values in k. From (3.2) we get the following system of $p - 1$ equations:

$$au_1 = 0$$
$$2au_1 + 2a^2 u_2 = 0$$
$$\dots$$
$$(p-1)au_1 + (p-1)(p-2)a^2 u_2 + \dots + (p-1)(p-2) \dots (1)a^{p-1} u_{p-1} = 0$$

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

$$\begin{aligned} u_1(x_1, \dots, x_{n-1}) &= 0 \\ u_2(x_1, \dots, x_{n-1}) &= 0 \\ &\dots \\ u_{p-1}(x_1, \dots, x_{n-1}) &= 0 \end{aligned}$$

for all $x_1, \dots, x_{n-1} \in k - \{0\}$.

Considering now $x_1, \dots, x_{n-1} \in k$, we still get that

$$\begin{aligned} x_1 \dots x_{n-1} u_1(x_1, \dots, x_{n-1}) &= 0 \\ x_1 \dots x_{n-1} u_2(x_1, \dots, x_{n-1}) &= 0 \\ &\dots \\ x_1 \dots x_{n-1} u_{p-1}(x_1, \dots, x_{n-1}) &= 0. \end{aligned}$$

By the induction hypothesis, we get

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

By formula (3.2) we get that $f \in I_n$. □

4. 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 $R(G)$. Therefore 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:

$$G \xrightarrow{\phi} (\mathbb{Z}/p)^n \tag{4.1}$$

which takes a matrix to the vector consisting of the elements imediately 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 $\alpha_1, \dots, \alpha_n$, 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 $R(G) = \mathbb{Z}[\alpha_1, \dots, \alpha_n]$, the ring generated by $\alpha_1, \dots, \alpha_n$.

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 (4.1) 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 4.1. *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 4.2. *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 $a_1, ..., a_n \in k$.

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 now to the ring generated by the elements from H^2 we get:

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

Now from [Le], 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:

$$\mathbb{Z}[\alpha, \beta] \xrightarrow{\pi^*} \mathbb{Z}[\alpha_1, \dots, \alpha_n],$$
$$\alpha \to \alpha_l, \beta \to \alpha_{l+1}.$$

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 $\mathbb{Z}[\alpha_1, \dots, \alpha_n]$. This means that $X_l^pX_{l+1} - X_lX_{l+1}^p \in J$, therefore $I_n \subset J$.

b) We have the map:

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

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

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

Let $(a_1, \dots, a_n) \in k^n - (0, \dots, 0)$. We have to prove $f(a_1, \dots, a_n) = 0$.

Let H be the subgroup generated by the matrix

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

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:

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

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

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

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

$$f(a_1, \dots, a_n) = 0 \quad (\text{remember } f(a_1, \dots, a_n) \in k)$$

□

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

We want first to prove that $J \subset I_n + X_l R_n$ for all $1 \le l \le n$. 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's 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:

$$H^*(G) \xrightarrow{i^*} H^*(H_l) \simeq H^*(H_l' \times H_l'') \tag{4.2}$$

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

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

Restricting now (4.2) to the ring generated by $\alpha_1, \dots, \alpha_n$ we get, since $R(H_l') = \mathbb{Z}[\alpha_1, \dots, \alpha_{l-1}]$ and $R(H_l'') = \mathbb{Z}[\alpha_{l+1}, \dots, \alpha_n]$, that

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

and we see that this composition takes the image of X_j in $\mathbb{Z}[X_1, \dots, X_n]'/J$ to the image of X_j in $\mathbb{Z}[X_1, \dots, X_n]'/(I_n + X_l R_n)$ for all $j = 1, \dots, n$. This shows that $J \subset I_n + X_l R_n$. By prop. 3.4 we get

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

By prop. 4.2 , J is generated by homogeneous elements. Take any $f \in J$, homogeneous. Then, by what we proved above, $f \in I_n + X_1 \dots X_n R_n$ and from prop. 4.2, $f(a_1, ..., a_n) = 0$ for all $a_1, ..., a_n \in k$. Now from Prop.3.5 we get that $f \in I_n$. This means that $J \subset I_n$. But we saw that $I_n \subset J$ therefore $J = I_n$. □

Corollary 4.3. *R(G) is reduced.*

Proof. It is clear from the above theorem and what was proved in section 3. □

Corollary 4.4. *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 here 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. 4.2, we get that $f(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. These two facts imply that $f \in I_n$ which means $f(\alpha_1, \ldots, \alpha_n) = 0$. □

References

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

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

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

[Le] 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 linear group over a finite field. *Ann. of Math.* **96** (1972) 552-586

[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.