INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

The Class Groups of Arithmetically Equivalent Algebras

by

Nicolas Arsenault

November 1996

Department of Mathematics and Statistics

McGill University, Montréal

Canada

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Master of Science

Acknowledgements

I am very grateful to Professor Henri Darmon. Without his advice and ideas, his wise guidance as a pedagogue and natural generosity this work could not have been presented. I am very proud to be in his first group of students. My only wish is to continue to benefit from his presence in my future studies. Thank you Henri.

I want to thank professors John McKay and David Ford, the first for providing me an article on group representation theory and the second for spending a good afternoon on checking the validity of computer results. I acknowledge the financing of NSERC for all the time I worked on my thesis. It allowed me to concentrate on my studies instead of financial concerns. I thank the staff at the Department of Mathematics and Statistics at McGill University for their kindness. I also mention the chance I had to share my office with great persons. I certainly worked in a pleasant atmosphere.

To my friends and my family: Maman, Papa and his wife Marthe, Sophie, Gilbert, Isabelle, Christophe and my two week old niece Florence, I love you all.

Abstract

Two number fields having the same Dedekind Zeta function need not have isomorphic class groups. However, the p-parts of these class groups are isomorphic except possibly for a finite number of exceptional primes p. These exceptional prime numbers divide the degree of the normal closure of the number field. In this thesis we extend this result to étale algebras having the same Dedekind Zeta function. These algebras consist of direct sums of a finite number of number fields. We apply this to the study of the class groups of subfields of normal extensions having Galois group isomorphic to $\mathbf{GL}_2(\mathbf{F}_p)$.

Résumé

Deux corps de nombres qui possèdent la même fonction Zéta de Dedekind n'ont pas forcément des groupes de classes isomorphes. On sait cependant que les p-parties de ces groupes de classes sont égales en dehors d'un nombre fini de nombres premiers p exceptionnels. Ces nombres premiers exceptionnels divisent tous le degré de le clôture galoisienne du corps de nombres. Dans cette thèse nous généralisons ce résultat aux algèbres étales qui ont des fonctions Zéta de Dedekind identiques. Ces algèbres sont des sommes directes d'un nombre fini de corps de nombres. On applique cette théorie pour étudier les groupes de classes de certains sous corps d'extensions galoisiennes qui ont un groupe de Galois isomorphe à $\mathbf{GL}_2(\mathbf{F}_p)$.

Contents

Chapter 1

Introduction

Since the time of Dedekind, one customary starting point for analysing the arithmetic of algebraic number fields has been the map

$$K \longmapsto \zeta_K(x)$$

assigning to each number field its *Dedekind zeta function*

$$\zeta_K(x) = \sum_{I \in \mathcal{O}_K} \frac{1}{N(I)^x} \text{ for } x \in (1, \infty)$$

where I runs through all the ideals of the number ring $\mathcal{O}_K$ and $N(I) = |\mathcal{O}_K/I|$. This function is known to converge for all $x > 1$ (see, for example [Fr-Ta] p.283). Moreover, it extends to a meromorphic function of $x \in \mathbf{C}$ having a simple pole at $x = 1$. The Dedekind zeta function of a number field encodes many of its invariants. If two number fields K and K' have the same Dedekind zeta function, we say that K and K' are *arithmetically equivalent number fields.* They share degrees $[K : \mathbf{Q}] = [K' : \mathbf{Q}]$ and discriminants $D_K = D_{K'}$, have the same number of real embeddings $s(K) = s(K')$ and of pairs of complex embeddings $t(K) = t(K')$, have isomorphic unit groups $U_K \simeq U_{K'}$, and they determine the same normal closure L over $\mathbf{Q}$ (for an introduction of the above concepts read for example [Ma] or [Fr-Ta]). Denoting $G = \mathrm{Gal}(L/\mathbf{Q})$, $H = \mathrm{Gal}(L/K)$ and $H' = \mathrm{Gal}(L/K')$ we have the following equivalence (see [Pe2])

$$\zeta_K(x) = \zeta_{K'}(x) \text{ if and only if } 1_H^G = 1_{H'}^G$$

where 1_H^G (respectively $1_{H'}^G$) is the trivial representation of H (or H') induced to G (see chapter 2 section 3 for definitions).

The first example of nonisomorphic arithmetically equivalent number fields was discovered in 1925 by Gassman [Ga] with K and K' of degree 180. Later Perlis [Pe1] constructed infinite families of pairs of nonisomorphic arithmetically equivalent fields. In that same article Perlis proved that the smallest degree for which there exist pairs of nonisomorphic arithmetically equivalent fields is 7.

The *Ideal Class Group* of a number field K, denote Cl_K, is the quotient of the group I_K of fractional ideals by the group P_K of principal ideals. This group is abelian, and is therefore isomorphic to the direct sum of its p-Sylow subgroups (in fact every nilpotent group has that property, cf.[Ha] theorem 10.3.4 page 155). In other words we have $Cl_K = \oplus_p Cl_K^{(p)}$. It is a classic result that the class group of a number field is finite (see again [Ma] or [Fr-Ta]). By computing the residue at the simple pole $x = 1$ of the Dedekind zeta function of K one obtains ([Fr-Ta] p.284)

$$\lim_{x \to 1^+} (x-1)\zeta_K(x) = \frac{2^{s+t}\pi^t R_K h_K}{W_K |D_K|^{1/2}}$$

where R_K is the regulator of K, h_K is the *class number* (which is the number of elements in Cl_K), and W_K is the number of roots of unity in K. Comparing those residues at $x = 1$ for a pair of arithmetically equivalent number fields K and K' we get

$$h_K \cdot R_K = h_{K'} \cdot R_{K'}.$$

This equation motivated Perlis to explore the relation between class groups of arithmetically equivalent number fields K and K'. Perlis [Pe2] introduced a group-theoretic invariant, a natural number $\nu = \nu(\mathrm{G}, H, H')$, whose definition depends on G, H, H' and not on L, K or K' such that for all prime p not dividing ν we have

$$Cl_K^{(p)} \simeq Cl_{K'}^{(p)}.$$

He also showed that the primes dividing ν must divide $|H| = |H'|$. In the same

paper he was able of computing explicitly the natural number ν in two concrete examples.

Before describing the general structure of this thesis we need to define the Dedekind zeta function of an algebra. The algebras we study are finite direct sums of number fields. Let $\mathcal{L} = \oplus K_i$ be such an algebra. Then we define $\zeta_{\mathcal{L}}(x)$ to be $\prod_i \zeta_{K_i}(x)$.

We also introduce the *Artin-L function* $L(x, \rho)$, where ρ is a representation of $G = \mathrm{Gal}(K/\mathbf{Q})$. Let $\mathcal{P}$ be a prime lying over p and denote $D_p = \{\sigma \in G; \sigma\mathcal{P} = \mathcal{P}\}$ the decomposition group at $\mathcal{P}$. Let $I_p = \{\sigma \in G; \sigma(\alpha) \equiv \alpha (\mathrm{mod}\ \mathcal{P})$ for all $\alpha \in \mathcal{O}_K\}$ be the inertia group at $\mathcal{P}$. Finally denote by $\sigma_p \in D_p/I_p$ the *Frobenius automorphism* at $\mathcal{P}$, i.e σ_p is an element whose restriction to the inertia field K^{I_p} is the Frobenius automorphism. If V is the vector space on which G acts via ρ, we define the Artin L-function as follows

$$L(x, \rho) = \prod_p \det_{V^{I_p}}(1 - \sigma_p p^{-x})^{-1} \quad (x > 1).$$

Using this definition one shows (see for example [Fr-Ta] p.311) that

$$L(x, 1_H^G) = \zeta_{K^H}(x)$$

and that

$$L(x, \rho + \psi) = L(x, \rho) \cdot L(x, \psi)$$

where ρ and ψ are two representations of G and $\rho + \psi$ is the direct sum of these representations.

In chapter 2, we study the group $\mathbf{GL}_2(\mathbf{F}_p)$. On that group we define the split and non-split Cartan subgroup, denoted C and C', and the Borel subgroup, denoted B. We also construct the character table of G. In chapter 3 we use that character table to prove the following relation on induced representations

$$1_N^G + 1 = 1_{N'}^G + 1_B^G$$

where N and N' are respectively the normalizers of C and C'. By the basic properties of the Artin L-functions (see above) one sees that $L(x, 1_N^G + 1) = L(x, 1_N^G)L(x, 1)$ $= \zeta_{K^N}(x)\zeta(x)$ and similarly $L(x, 1_{N'}^G + 1_B^G) = \zeta_{K^{N'}}(x)\zeta_{K^B}(x)$ where for example K^B denotes the fixed field of K by B. Hence we have

$$\zeta_{K^N}(x)\zeta(x) = \zeta_{K^{N'}}(x)\zeta_{K^B}(x).$$

It follows that the two algebras $\mathcal{L} = K^N \oplus \mathbf{Q}$ and $\mathcal{L}' = K^{N'} \oplus K^B$ share the same Dedekind zeta function. They are then said to be *arithmetically equivalent*. In chapter 4 we extend Perlis' result to arithmetically equivalent algebras by constructing a positive integer ν such that for all prime ℓ not dividing ν we have

$$Cl_{K^N}^{(\ell)} \simeq Cl_{K^{N'}}^{(\ell)} \oplus Cl_{K^B}^{(\ell)}.$$

We also show that the primes dividing ν divide the order of G. In chapter 5 we apply the theory developed so far to a concrete family of examples arising from the 3-division points of elliptic curves. In these examples we prove that ν is a power of 2.

Chapter 2

A brief study of $G = \mathbf{GL}_2(\mathbf{F}_p)$

2.1 The conjugacy classes of G

Consider $G = \mathbf{GL}_2(\mathbf{F}_p)$, the group of 2×2 invertible square matrices with entries in the finite field $\mathbf{F}_p$ of p elements. It can also be seen as the group of automorphisms of the vector space $V = \mathbf{F}_p \times \mathbf{F}_p$ over $\mathbf{F}_p$. The cardinality of G is equal to the number of bases of V. For the first vector of the basis, there are $p^2 - 1$ choices (rejecting (0,0)). For the second, you need to take out all the vectors spanned by the first one and you get $(p^2 - 1) - (p - 1) = (p^2 - p)$ choices. Therefore $|G| = (p^2 - 1)(p^2 - p) = p(p + 1)(p - 1)^2$.

Given $g \in G$, consider its characteristic polynomial $p_g(x) = x^2 - tx + n$ where t =trace(g) and n =det(g) (the norm). We know from basic linear algebra that $p_g(x) = p_{\sigma g \sigma^{-1}}(x)$ for any $\sigma \in G$. In other words $p_g(x)$ is invariant by conjugation. Furthermore, a conjugacy class is completely determined by its characteristic polynomial. There are four possibilities for $p_g(x)$.

The first case; $p_g(x) = (x - a)^2$ and the eigenspace associated to a is of dimension two. In that case $g = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. The matrix g is scalar and $(p - 1)$ such classes exist. When the matrix g is scalar we denote it by: $g \sim A_1$.

The second case; $p_g(x) = (x-a)^2$ but the eigenspace associated to a is of dimension one. By the theory of the Jordan canonical form (see for example [Ja] section 3.10 p. 200), g is conjugate to $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$. Here again $(p-1)$ such classes exist. When g is of the second case we denote it by: $g \sim A_2$.

The third case ; $p_g(x)$ has two distinct roots, a and b in $\mathbf{F}_p$. By the Jordan canonical form, g is diagonalisable and is conjugate to $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. There are $\frac{(p-1)(p-2)}{2}$ such classes corresponding to subsets of two elements in $\mathbf{F}_p^*$. When g is of the third case, it is denoted by: $g \sim A_3$.

The fourth case; $p_g(x)$ is irreducible over $\mathbf{F}_p^*$. Let $\mathbf{F}_{p^2}$ be a fixed quadratic extension of $\mathbf{F}_p$. The irreducible monic polynomials of degree two over $\mathbf{F}_p$ are in bijection with $(\mathbf{F}_{p^2} \setminus \mathbf{F}_p)/t$, where t is the Galois automorphism. Hence there are $\frac{p(p-1)}{2}$ of them. When g has irreducible characteristic polynomial, we denote it by: $g \sim B_1$.

Now we compute the sizes of each of these four types of conjugacy classes. The general strategy is the following. Given a conjugacy class C, the group G acts transitively on C via conjugation. By a basic fact in group action theory (see [Ja] section 1.12 p.71) we have $|C| = \sum_{orbits}[G : Z(x_i)]$ where $x \in C$ and $Z(x)$ is the centralizer of x. We therefore have

$$|C| = [G : Z(g)] \quad \text{for any } g \in C \tag{2.1}$$

For the **first** case when g is in the center, we have $|A_1(g)| = 1$. In other words the number of element in the conjugacy class of $g \sim A_1$ is one because then g belongs to the center of G.

For the **second case**, $g \sim A_2$, let $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $g = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$. A computation shows that $xg = gx$ if and only if $c = 0$ and $a = d$. Hence

$$Z(g) = \left\{ x \in G \ : \ x = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \right\}.$$

Thus $|Z(g)| = (p-1)p$ and $|A_2(g)| = (p-1)(p+1)$ by equation (2.1).

For the **third case**, $g \sim A_3$, let $g = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$. Then $xg = gx$ if and only if $(b, c) = (0, 0)$. Hence

$$Z(g) = \left\{ x \in G \ : \ x = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right\}.$$

Thus $|Z(g)| = (p-1)^2$ and $|A_3(g)| = p(p+1)$ by equation (2.1).

For the **fourth case**, $g \sim B_1$, let α be a root of $p_g(x)$. Then g belongs to the conjugacy class of $g' = \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix}$. Let $x \in \mathbf{GL}_2(\mathbf{F}_{p^2})$ be such that $g' = xgx^{-1}$ then $xZ(g)x^{-1}$ is contained in

$$Z(g') = \left\{ x \in G' \ : \ x = \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} \right\}.$$

Moreover it consists exactly of the matrices in $Z(g')$ satisfying $\gamma_1 = \overline{\gamma_2}$. Thus $Z(g)$ is isomorphic to $\mathbf{F}_{p^2}^*$ and

$$|Z(g)| = p^2 - 1.$$

By equation (2.1) we get $|B_1(g)| = p(p-1)$. The results are summarized in the following table.

Table 1 *Conjugacy classes of* G

Conjugacy	class	# of classes	# element/class
$g \sim A_1$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$(p-1)$	1
$g \sim A_2$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$(p-1)$	p^2-1
$g \sim A_3$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\frac{(p-1)(p-2)}{2}$	$p(p+1)$
$g \sim B_1$	non-split	$\frac{p(p-1)}{2}$	$p(p-1)$

2.2 Definition of the split and non-split Cartan subgroup

This section is inspired from ([La1] chapter 18, section 12). A *split Cartan subgroup* of G is a conjugate to the group of diagonal matrices.

$$C = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \text{ with } a, b \in \mathbf{F}_p^* \right\}$$

Let $\mathbf{F}_{p^2}$ be a separable quadratic extension of $\mathbf{F}_p$. Let $\{w_1, w_2\}$ be a basis of $\mathbf{F}_{p^2}$ over $\mathbf{F}_p$. Then $\mathbf{F}_{p^2}^*$ acts on $\mathbf{F}_p \times \mathbf{F}_p$ with respect to the chosen basis via multiplication. We can therefore view $\mathbf{F}_{p^2}^*$ as a subgroup of G. We denote by C' this subgroup. A different choice a basis of $\mathbf{F}_{p^2}$ corresponds to conjugation of C' in G. We call C' a *non-split Cartan subgroup* . The subalgebra $\mathbf{F}_p[C'] \subset \mathrm{Mat}_2(\mathbf{F}_p)$ is isomorphic to $\mathbf{F}_{p^2}$ itself while the units of the algebra are the elements of $C' = \mathbf{F}_{p^2}^*$. Consider $\{1, \alpha\}$ as a basis for $\mathbf{F}_{p^2}$ over $\mathbf{F}_p$. For example, when $p \neq 2$, α can be taken as a root of $x^2 - a$ where a is not a square in $\mathbf{F}_p$. In that case we describe the elements of C' in the natural basis $\{1, \alpha\}$ of $\mathbf{F}_{p^2}$ and we have

$$C' = \left\{ \begin{pmatrix} x & ay \\ y & x \end{pmatrix} : (x, y) \neq (0, 0) \right\}.$$

Before continuing the analysis of our Cartan subgroups we need the following classical theorem found for example in ([Ja] p.207).

Theorem 1 (Frobenius Theorem) *Let $A \in M_n(F)$, F a field, and let $det(\lambda I - A) = d_1(\lambda) \cdots d_s(\lambda)$ be the characteristic polynomial expressed in irreducible factors over $F[\lambda]$. Let $n_i = deg\ d_i(\lambda)$. Then the dimension of the vector space over F of matrices commuting with A is given by the formula*

$$N = \sum_{j=1}^{s} (2s - 2j + 1) n_j.$$

We are now ready to resume our study of the Cartan subgroups.

Lemma 1 *The subgroup C' is a maximal commutative subgroup*

Proof. Clearly C' is a commutative subgroup. Now suppose $x \in G$ commutes with all elements of C'. The matrix endomorphisms, $\mathrm{Mat}_2(\mathbf{F}_p)$, is an $\mathbf{F}_p$-algebra. Consider $\mathbf{F}_p[C']$ as a subalgebra of $\mathrm{Mat}_2(\mathbf{F}_p)$. We know $|\mathbf{F}_p[C']| = p^2$. For $x \notin \mathbf{F}_p[C']$, we have $|\mathbf{F}_p[C', x]| \geq p^2 + 1$. Now by the formula of Theorem 1 the dimension of the vector space over $\mathbf{F}_p$ of matrices commuting with x can't be equal to 3 (analyse the possible s), hence $|\mathbf{F}_p[C', x]| \neq p^3$. Since $|\mathbf{F}_p[C', x]|$ divides $|\mathrm{Mat}_2(\mathbf{F}_p)|$ it implies that $|\mathbf{F}_p[C', x]| = |\mathrm{Mat}_2(\mathbf{F}_p)|$ but then $\mathrm{Mat}_2(\mathbf{F}_p)$ would be commutative which is not the case. Therefore $x \in \mathbf{F}_p[C']$. But x is invertible, so $x \in C'$. **QED.**

A *Cartan subgroup* is a subgroup conjugate to the split Cartan subgroup or to one of the subgroups described above (one of the C'). Here is a more conceptual way of seeing the Cartan subgroups.

Lemma 2 *Every maximal commutative subgroup of $\mathbf{GL}_2(\mathbf{F}_p)$ is a Cartan subgroup, and conversely.*

Proof. Clearly the split Cartan subgroup is a maximal commutative subgroup of G. Suppose H is a maximal commutative subgroup of G. We say that H is *diagonalizable* if and only if all its elements are diagonalizable with respect to a fixed basis. If H is diagonalizable over $\mathbf{F}_p$, then H is contained in a conjugate of the split Cartan subgroup. On the other hand, suppose H is not diagonalizable over $\mathbf{F}_p$. It is diagonalizable over $\mathbf{F}_p^s$, the separable closure of $\mathbf{F}_p$ (in the basis $\{(1,0),(0,1)\}$

of $\mathbf{F}_p^s = \mathbf{F}_p \oplus \mathbf{F}_p$, any element $\alpha \in H$ is equivalent to the diagonal matrix $\begin{pmatrix} x & 0 \\ 0 & \overline{x} \end{pmatrix}$ where x and $\overline{x}$ are the eigenvalues of α), and the two eigenspaces of dimension 1 give rise to two characters

$$\phi, \phi' : H \longrightarrow \mathbf{F}_p^{s*}$$

of H in the multiplicative group of the separable closure. For each element $\alpha \in H$ the values $\phi(\alpha)$ and $\phi'(\alpha)$ are the two eigenvalues of α. At least for one $\alpha \in H$, these eigenvalue are distinct because H is not diagonalizable. Hence the pair of elements $\phi(\alpha), \phi'(\alpha)$ are conjugate over F. The image $\phi(H)$ is cyclic, and if $\phi(\alpha)$ generates this image, then we see that $\phi(\alpha)$ generates a quadratic extension $\mathbf{F}_{p^2}$ of $\mathbf{F}_p$. The map

$$\alpha \longmapsto \phi(\alpha) \text{ with } \alpha \in H$$

extends to an $\mathbf{F}_p$-linear mapping, also denoted by ϕ, of the algebra $\mathbf{F}_p[H]$ into $\mathbf{F}_{p^2}$. It follows that $\phi : \mathbf{F}_p[H] \longrightarrow \mathbf{F}_{p^2}$ is an isomorphism. Hence ϕ maps H into $\mathbf{F}_{p^2}^*$, and in fact maps H onto $\mathbf{F}_{p^2}^*$ because H was taken to be maximal. **QED.**

The normalizers of C and C'.

We also want to describe what are the normalizer of C and C'. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ and $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in C$, then

$$g \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} g^{-1} = \frac{1}{\det(g)} \begin{pmatrix} adx - bcy & -abx + aby \\ cdx - cdy & -bcx + ady \end{pmatrix} \in C$$

if and only if $(a, d) = (0, 0)$ or $(b, c) = (0, 0)$. Therefore the normalizer of C is

$$N = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} : a, b, c, d \in \mathbf{F}_p^* \right\}.$$

Before computing N', the normalizer of C' we need two lemmas.

Lemma 3 *Let t be the linear automorphism of $\mathbf{F}_{p^2}$ given by the galois conjugation. (In the basis $\{1, \alpha\}$ of $\mathbf{F}_{p^2}$ chosen above, it is described by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.)*

Then

$$tx = \overline{x}t \text{ for all } x \in \mathbf{F}_{p^2}$$

Proof: A direct verification.

Since t does not commute with C', it follows from lemma 3 that $t \in N' - C'$.

Lemma 4 $(N' : C') = 2$

Proof (see [Se1] p.279): If $s \in N'$, the application $x \longmapsto sxs^{-1}$ gives rise to an auto morphidm of $\mathbf{F}_p[C']$ fixing $\mathbf{F}_p$. Let $\psi : N' \longrightarrow \{\pm 1\} = \mathrm{Aut}(\mathbf{F}_{p^2})$ be the homomorphism which sends s to this automorphism. If $\psi(s)$ is the identity then s commutes with C' and hence belongs to C' by lemma 1. Hence $\ker(\psi) = C'$. But ψ is surjective by lemma 3. **QED.**

Lemma 4 implies

$$\begin{aligned} N' &= C' \cup tC' \\ &= \left\{ \begin{pmatrix} x & ay \\ y & x \end{pmatrix}, \begin{pmatrix} x & ay \\ -y & -x \end{pmatrix} : (x,y) \neq (0,0),\ a \neq \square \right\} \end{aligned}$$

2.3 The character table of G

2.3.1 Representation theory of groups

We review the basic facts of representation theory of groups (see for example [Se2]). Given a finite group G, a homomorphism $\rho : G \longrightarrow \mathbf{GL}(V)$ from G into the automorphism group of a vector space V over F (a field) is called a *representation of* G. If ρ is a representation of G, $\rho(g)$ can be viewed as an invertible (dimV) $\times$ (dimV) square matrix. We say that $\rho : G \longrightarrow \mathbf{GL}(V)$ and $\rho' : G \longrightarrow \mathbf{GL}(V')$ are isomorphic representations if and only if there exist an invertible $n \times n$ matrix M (where $n = \dim(V) = \dim(V')$) such that for all $g \in G$ we have

$$\rho(g)M = M\rho'(g).$$

For any representation ρ of G we can write ρ as a direct sum of *irreducible representations*. The set of irreducible representations is defined to be the smallest set

of representations having the above property. To the representation ρ we associate the *character* $\chi_\rho : G \longrightarrow F$ defined by

$$\chi_\rho(g) = \text{trace } \rho(g).$$

Proposition 1 *When F has characteristic zero, two representations having the same character are isomorphic.*

This is why we often focus our study on the characters of G instead of its representations. For any character χ the dimension of χ is defined to be equal to the dimension of the vector space V on which G acts. Since the trace is invariant under conjugation, χ is a class function. In other words for all the g's in a conjugacy class C_1 of G their images by χ are equal.

Given χ and χ', two characters of G, we define

$$(\chi, \chi') = \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi'(g^{-1}).$$

Proposition 2 *If χ and χ' are two irreducible characters of G then*

$$(\chi, \chi') = \begin{cases} 1 & \text{if } \chi = \chi' \\ 0 & \text{otherwise} \end{cases}.$$

Any character of G can be expressed as a linear combination of irreducible characters. The *character table* of G is defined by the gathering of all the irreducible characters of G in a table. We also know that the number of irreducible characters of G is equal to the number of conjugacy classes of G.

Given H a proper subgroup of G, then any representation $\rho : H \longrightarrow \mathbf{GL}(V)$ gives rise to an *induced representation* $\rho_H^G : G \longrightarrow \text{Aut}(W)$, where W is the space of functions from G to V satisfying $f(hx) = \rho(h)f(x)$ for all $h \in H$, and the action of G on W is given by $gf(x) = f(xg)$. The character of ρ_H^G, called the *induced character* χ_H^G, is defined as follows

$$\chi_H^G(g) = \frac{1}{|H|} \sum_{x \in G} \dot{\chi}(x^{-1}gx)$$

where $\dot{\chi}(g) = \begin{cases} \chi(g) & \text{if } g \in H \\ 0 & \text{otherwise} \end{cases}$.

A special type of induced character is obtained when one consider the trivial character $1_H : H \longrightarrow C$ where $1_H(h) = 1$ for all $h \in H$. Then you construct 1_H^G with the above definition. Actually 1_H^G is the character associated to the permutation representation of the coset space $[G/H]\mathbf{Q}$. For $g \in G$, $1_H^G(g)$ is equal to the dimension of the subspace S where $S = \{x \in [G/H]\mathbf{Q} : gx = x\}$.
We now introduce an important theorem that is going to play a major role in the contruction of the character table of $\mathbf{GL_2(F_p)}$.

Theorem 2 (Frobenius Reciprocity) *Let χ be a character of G and ψ be a character of H, where H is a subgroup of G. Then*

$$(\chi, \psi_H^G)_G = (\chi_H, \psi)_H$$

where χ_H is the restriction of χ on H.

2.3.2 The computation of the character table of G

Again this part is based on ([La1] chapter 18, section 12). Here are some definitions we need in the course of computing the character table of G.

$$\begin{aligned} A &= \text{Diagonal subgroup of } G \\ Z &= \text{Center of } G \\ U &= \text{Group of unipotent elements} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \\ B &= \text{Borel subgroup } = UA = AU \end{aligned}$$

Then $|B| = p(p-1)^2$. We will construct the irreducible characters of G by inducing characters from B. There are four types of irreducible characters of G .

First type

Let $\mu : \mathbf{F}_p^* \longrightarrow \mathbf{C}^*$ denote a complex character. Then $\mu \circ \det : G \longrightarrow \mathbf{C}^*$ are the characters of the **first type** of dimension one. Its values on the conjugacy classes are given in the following table.

Table 2

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} a \neq d$	$\beta \in C' \setminus \mathbf{F}_p^*$
$\mu \circ \det$	$\mu(a)^2$	$\mu(a)^2$	$\mu(ad)$	$\mu \circ \det(\beta)$

There are $(p-1)$ characters of first type, because $|\mathbf{F}_p^*| = (p-1)$. Note that they are all irreducible, since they are of dimension 1.

Second type

Let

$$\psi_\mu \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \mu(ad).$$

We obtain the induced character

$$\psi_\mu^G = Ind_B^G(\psi_\mu)$$

where

$$Ind_B^G(\psi_\mu)(x) = \frac{1}{|B|} \sum_{g \in G} \dot{\psi}_\mu(gxg^{-1}) \quad \text{and } \dot{\psi}_\mu(g) = \begin{cases} \psi_\mu(g) & \text{if } g \in B \\ 0 & \text{otherwise} \end{cases}.$$

Note that ψ_μ^G is not irreducible because it contains $\mu \circ \det$. Indeed using the Frobenius Reciprocity Theorem we get

$$\begin{aligned} (\psi_\mu^G, \mu \circ \det)_G &= (\psi_\mu, \mu \circ \det)_B \\ &= \frac{1}{|B|} \sum_{g \in B} \psi_\mu(g)(\mu \circ \det)(g)^* \quad \text{where * means conjugate} \\ &= \frac{1}{|B|} \sum_{g \in B} |\mu(g)|^2 \\ &= 1. \end{aligned}$$

The characters $\chi = \psi_\mu^G - \mu \circ \det$ are called of **second type**. Let's study the values that ψ_μ^G takes on the different conjugacy classes.

For an element in the center we get

$$\psi_\mu^G \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \frac{|G|}{|B|} \psi_\mu^G \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = (p+1)\mu(a)^2.$$

For an element in a conjugacy class of the form A_2 we have for $x = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ in G that $x\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}x^{-1} = \frac{1}{\det(x)}\begin{pmatrix} x_1x_4a - x_1x_3 - x_2x_3a & x_1^2 \\ -x_3^2 & x_1x_3 - x_2x_3a + ax_1x_4 \end{pmatrix}$ belongs to B if and only if $x \in B$. So we obtain

$$\begin{aligned} \psi_\mu^G\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} &= \frac{1}{|B|}\sum_{g\in G}\dot{\psi}_\mu\left(g\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}g^{-1}\right) \\ &= \frac{1}{|B|}\sum_{g\in B}\psi_\mu(g)\mu(a)^2\psi_\mu(g^{-1}) \\ &= \mu(a)^2. \end{aligned}$$

For an element in a conjugacy class of the form A_3 and for a given $x \in G$ we have

$$x\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}x^{-1} = \frac{1}{\det(x)}\begin{pmatrix} x_1x_4a - x_2x_3b & -x_1x_2a + x_1x_2b \\ x_3x_4a - x_3x_4b & -x_3x_2a + x_1x_4b \end{pmatrix}$$

belongs to B if and only if x_3 or x_4 is equal to zero. So we obtain

$$\begin{aligned} \psi_\mu^G\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} &= \frac{1}{|B|}\sum_{g\in G}\dot{\psi}_\mu\left(g\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}g^{-1}\right) \\ &= \frac{2|B|}{|B|}\psi_\mu\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = 2\mu(ab). \end{aligned}$$

Lastly for an element $\beta \in C' - \mathbf{F}_p^*$ (i.e β is of the form B_1) we have that any conjugate of β does not belong in B because $p_\beta(x)$ is invariant via conjugation and $p_\beta(x)$ is irreducible while for all $g \in B$, $p_g(x)$ is reducible. So we have

$$\psi_\mu^G(\beta \in C' \setminus \mathbf{F}_p^*) = 0$$

In the following table we reproduce the characters of type two.

Table 3

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} a \neq d$	$\beta \in C' \setminus \mathbf{F}_p^*$
$\psi_\mu^G - \mu \circ \det$	$p\mu(a)^2$	0	$\mu(ad)$	$-\mu \circ \det(\beta)$

These type-two characters are all irreducible; indeed, using Table 1 we find

$$\begin{aligned}
|G|(\chi,\chi) &= \sum_{g\in G}|\chi(g)|^2 \\
&= \sum_{a=1}^{p-1}|p\mu(a)^2|^2 + \\
&\quad p(p+1)\sum_{a<d}^{p-1}|\mu(ad)|^2 + p(p-1)\sum_{\beta\in C'\setminus \mathbf{F}_p^*}|-\mu\circ\det(\beta)|^2 \\
&= p^2(p-1)+\frac{(p-1)(p-2)(p+1)p}{2}+\frac{(p-1)^2p^2}{2} \\
&= \frac{p(p-1)}{2}(2p^2-2) \\
&= |G|
\end{aligned}$$

There are $(p-1)$ such characters of type two corresponding to the different possible μ.

Third type

Let $\psi : A \longrightarrow \mathbf{C}^*$ denote a homomorphism. Take $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in N \setminus A$. Then $w = w^{-1}$ and $w\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}w = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix} = g^w$ if $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. Thus conjugation by w is an automorphism of order 2 on A. Let $[w]\psi$ be the conjugate character; i.e.$([w]\psi(g)) = \psi(wgw^{-1}) = \psi(g^w)$ for $g \in A$. Then $[w]\mu = \mu$ (because $[w]\mu(g) = \mu(g^w) = \mu(g)$). The characters μ on A are precisely those which are invariant under $[w]$. The others can be written in the form

$$\psi\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \psi_1(a)\psi_2(b)$$

with distinct characters $\psi_1, \psi_2 : \mathbf{F}_p^* \longrightarrow \mathbf{C}^*$. We amy consider the induced character $\psi^G = Ind_B^G([w]\psi)$ with ψ such that $w\psi \neq \psi$. Those characters $\chi = \psi^G$ will be called of the **third type**. Let us study the values that ψ^G takes on the different conjugacy classes.

For an element in the center we have

$$\psi^G\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \frac{1}{|B|}\sum_{g\in G}\dot{\psi}\left(g\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}g^{-1}\right)$$
$$= \frac{|G|}{|B|}\psi\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = (p+1)\psi(a).$$

For an element in the conjugacy class of the form A_2 we already know that $g\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}g^{-1} \in B$ if and only if $g \in B$. Hence we have

$$\psi^G\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \frac{|B|}{|B|}\psi\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \psi(a).$$

For an element in a conjugacy class of the form A_3 we define

$$N(B) = \left\{x \in G \ : x\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}x^{-1} \in B\right\} = B \cup \left\{\begin{pmatrix} x_1 & x_2 \\ x_3 & 0 \end{pmatrix} \ : x_2, x_3 \neq 0\right\}.$$

There are two alternatives for an $g \in N(B)$. In the first $g \in B$ and then $\psi^G\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ $= \psi\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. In the second possibility $g \in N(B) - B$ then we know that $N(B) = B \cup Bw$. This is right because

$$\begin{pmatrix} x_1 & x_2 \\ 0 & x_3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_2 & x_1 \\ x_3 & 0 \end{pmatrix}.$$

Therefore for such a g we have that $g = g_0 w$ for some $g_0 \in G$ and we get

$$\psi\left(g\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}g^{-1}\right) = \psi\left(g_0\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^w g_0^{-1}\right) = \psi(x^w)$$

where $x = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. So when we evaluate ψ^G on an element $x = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ we get

$$\psi^G(x) = \frac{1}{|B|}(|B|\psi(x) + |B|\psi(x^w)) = \psi(x) + \psi(x^w).$$

Lastly for an element $\beta \in C' - \mathbf{F}_p^*$ we have $\psi^G(\beta) = 0$ because there exist no $g \in G$ such that $g\beta g^{-1} \in B$.

The characters of type three are reproduced in the table below.

Table 4

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$x = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} a \neq b$	$\beta \in C' \setminus \mathbf{F}_p^*$
$\psi^G[w]\psi \neq \psi$	$(p+1)\psi(a)$	$\psi(a)$	$\psi(x) + \psi(x^w)$	0

Moreover a character ψ^G of the third type is irreducible. To show this, let us compute $\sum_{g\in G} |\chi(g)|^2$. We remark first that two elements g and $g' \in A$ are in the same conjugacy class if and only if $g = g'$ or $g = [w]g'$. Now we have , using Table 1 and Table 4

$$\begin{aligned}\sum_{g\in G} |\psi^G(g)|^2 &= (p+1)^2 \sum_{a=1}^{p-1} |\psi(a)|^2 + (p^2-1) \sum_{a=1}^{p-1} |\psi(a)|^2 \\ &\quad + p(p+1) \sum_{x\in(A\setminus\mathbf{F}_p^*)/w} |\psi(x) + \psi(x^w)|^2\end{aligned}$$

The third term of this sum is equal to

$$\begin{aligned}&\frac{(p+1)p}{2} \sum_{x\in A\setminus\mathbf{F}_p^*} (\psi(x) + \psi(x^w))(\psi(x^{-1}) + \psi(x^{-w})) \\ &= \frac{p(p+1)}{2} \sum_{x\in A\setminus\mathbf{F}_p^*} (1 + 1 + \psi(x^{1-w}) + \psi(x^{w-1}))\end{aligned}$$

We write the sum over $x \in A \setminus \mathbf{F}_p^*$ as a sum for $x \in A$ minus a sum for $x \in \mathbf{F}_p^*$. If $x \in \mathbf{F}_p^*$ then $x^{w-1} = x^{1-w} = 1$. By assumption on ψ, the character $x \longmapsto \psi(x^{1-w})$ for $x \in A$ is non trivial, and therefore the sum over $x \in A$ is equal to zero. So we get that the third term is equal to

$$\frac{p(p+1)}{2}[2(p-1)(p-2) - 2(p-1)] = p(p+1)(p-1)(p-3)$$

and

$$\begin{aligned}\sum_{g\in G} |\psi^G(g)|^2 &= (p+1)(p^2-1) + (p-1)(p^2-1) + p(p+1)(p-1)(p-3) \\ &= p(p-1)(p^2-1) = |G|.\end{aligned}$$

Proving that ψ^G is irreducible. Finally there are $\frac{(p-1)(p-2)}{2}$ characters of the third type. Because this is the number of characters ψ such that $\psi \neq [w]\psi$, divided by two because ψ and $[w]\psi$ induced the same character ψ^G in G.

Fourth type

Let $\theta : \mathbf{F}_{p^2}^* \longrightarrow \mathbf{C}$ denote a homomorphism, which is viewed as a character on C' (the non-split Cartan subgroup). Consider $t = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in N' \setminus C'$. We have that $t = t^{-1}$. So

$$\beta \longmapsto t\beta t = [t]\beta$$

is an automorphism of C' which is also a field automorphism of $\mathbf{F}_p[C'] \simeq \mathbf{F}_{p^2}$ over $\mathbf{F}_p$. Since $[\mathbf{F}_{p^2} : \mathbf{F}_p] = 2$, it follows that conjugation by t is the automorphism $\beta \longmapsto \beta^p$. As a result we obtain the conjugate character $[t]\theta$ such that

$$([t]\theta)(\beta) = \theta([t]\beta) = \theta(\beta^t),$$

and we get the induced character

$$\theta^G = ind_{C'}^G(\theta) = ind_{C'}^G([t]\theta).$$

Let $\mu : \mathbf{F}_p^* \longrightarrow C$ denote a homomorphism as in the first type.
And $\lambda : \mathbf{F}_p^+ \longrightarrow C$ be a non-trivial homomorphism. Consider (μ, λ) = the character on ZU such that

$$(\mu, \lambda)\left(\begin{pmatrix} a & ax \\ 0 & a \end{pmatrix}\right) = \mu(a)\lambda(x).$$

$(\mu, \lambda)^G = ind_{ZU}^G(\mu, \lambda)$. Now what we want is the value of θ^G and $(\mu, \lambda)^G$ on the conjugacy classes of G. We now compute θ^G on the different conjugacy classes of G.

For an element in the center we get

$$\theta^G\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \frac{|G|}{|C'|}([t]\theta)\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = p(p-1)\theta(a).$$

For an element $x = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ in a conjugacy class of the form A_2 we have

$$\theta^G(x) = \frac{1}{|C'|}\sum_{g \in G} \dot{\theta}(gxg^{-1}) = 0$$

because $gxg^{-1} \notin C'$ for all $g \in G$.

For an element $x = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} a \neq b$, in a conjugacy class of the form A_3 we have $gxg^{-1} \notin C'$ for all $g \in G$. This implies $\theta^G(x) = 0$.

Lastly for an element $\beta \in (C' \setminus \mathbf{F}_p^*)$, we have $g\beta g^{-1} \in C'$ if and only if $g \in N'$ so

$$\begin{aligned} \theta^G(\beta) &= \frac{1}{|C'|} \sum_{g \in C'} \dot{\theta}(g\beta g^{-1}) + \frac{1}{|N' \setminus C'|} \dot{\theta}(g\beta g^{-1}) \\ &= \theta(\beta) + \theta(\beta^t). \end{aligned}$$

We now study $(\mu, \lambda)^G$ on the different conjugacy classes of G. For an element in the center, $(\mu, \lambda)^G \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \frac{|G|}{|ZU|}(\mu, \lambda)(a) = (p^2 - 1)\mu(a)$.

For an element ,$g = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, and $x = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \in G$ we have $xgx^{-1} \in ZU$ if and only if $x_3 = 0$. Call S the set $\{x \in G : x_3 = 0\}$, For $x \in S$ we have $xgx^{-1} = \begin{pmatrix} a & a(x_1 x_4^{-1} a^{-1}) \\ 0 & a \end{pmatrix}$ and our computation comes down to

$$\begin{aligned} (\mu, \lambda)^G(g) &= \frac{1}{|ZU|} \sum_{x \in S} (\mu, \lambda)(xgx^{-1}) \\ &= \frac{1}{|ZU|} \sum_{x \in S} \mu(a)\lambda(x_1 x_4^{-1} a^{-1}) \\ &= \frac{p\mu(a)}{|ZU|} \sum_{x_1, x_4 = 1}^{p-1} \lambda(x_1 x_4^{-1} a^{-1}) \\ &= \frac{\mu(a)}{(p-1)} \sum_{x_1=1}^{p-1} \sum_{x_4=1}^{p-1} \rho^{x_4} \quad \text{where } \rho \text{ is a } p^{th} \text{ root of unity} \\ &= \frac{\mu(a)}{(p-1)} \sum_{x_1=1}^{p-1} \left(\frac{\rho^p - 1}{\rho - 1} - 1 \right) \\ &= -\mu(a). \end{aligned}$$

For an element $g = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a \neq b$ we have

$$xgx^{-1} = \frac{1}{\det(x)} \begin{pmatrix} x_1 x_4 (a-b) & x_1 x_2 (b-a) \\ x_3 x_4 (a-b) & x_2 x_3 (b-a) \end{pmatrix}.$$

This belong to ZU if and only if $x_3x_4(b-a)=0$ and $(b-a)(x_1x_4+x_2x_3)=0$ which is impossible. Thus $(\mu,\lambda)^G(g)=0$.

For an element $\beta \in C'\backslash \mathbf{F}_p^*$, then $g\beta g^{-1} \notin ZU$ for all $g \in G$. Thus $(\mu,\lambda)^g(\beta)=0$. The information obtained on the two characters θ^G and $(\mu,\lambda)^G$ is reorganized in the following table.

Table 5

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} a \neq b$	$\beta \in C' \setminus \mathbf{F}_p^*$
θ^G	$p(p-1)\theta(a)$	0	0	$\theta(\beta)+\theta(\beta^t)$
$(\mu,\lambda)^G$	$(p^2-1)\mu(a)$	$-\mu(a)$	0	0

Now consider the character $(res\theta,\lambda)^G$, where $res\theta$ is the restriction of θ to $\mathbf{F}_p^*$. Then by the Frobenius Reciprocity Theorem we have

$$((res\theta,\lambda)^G,\theta^G)=((res\theta,\lambda),\theta)_{\mathbf{F}_p^*}=\frac{1}{(p-1)}\sum_{a\in\mathbf{F}_p^*}|\theta^2(a)|^2=1$$

So θ^G occurs in the character of $(res\theta,\lambda)^G$. Thus we define $\theta'=(res\theta,\lambda)^G-\theta^G=([t]\theta)'$. A character θ' is said to be of the **fourth type** if θ is such that $\theta \neq [t]\theta$. Using Table 5 we get the following table

Table 6

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} a \neq b$	$\beta \in C' \setminus \mathbf{F}_p^*$
$\theta', \theta \neq [t]\theta$	$(p-1)\theta(a)$	$-\theta(a)$	0	$-\theta(\beta)-\theta(\beta^t)$

Lemma 5 *θ' of the fourth type is irreducible.*

Proof:

$$\begin{aligned}\sum_{g\in G}|\theta'(g)|^2 &= (p-1)^2(p-1)+(p-1)(p^2-1)\\ &\quad +\frac{p(p-1)}{2}\sum_{\beta\in C'\backslash\mathbf{F}_p^*}|\theta(\beta)+\theta(\beta^t)|^2.\end{aligned}$$

The third sum is equal to

$$\frac{p(p-1)}{2}\sum_{\beta\in C'\setminus\mathbf{F}_p^*}(\theta(\beta)+\theta(\beta^t))(\theta(\beta^{-1})+\theta(\beta^{-t}))$$
$$=\frac{p(p-1)}{2}\sum_{\beta\in C'\setminus\mathbf{F}_p^*}(1+1+\theta(\beta^{1-t})+\theta(\beta^{t-1})).$$

We write the sum over $\beta\in C'\setminus\mathbf{F}_p^*$ as a sum for $\beta\in C'$ minus a sum for $\beta\in\mathbf{F}_p^*$. If $\beta\in\mathbf{F}_p^*$ then $\beta^{1-t}=\beta^{t-1}=1$. By the assumption on θ ($\theta\neq[t]\theta$), the character

$$\beta\longmapsto\theta(\beta^{1-t})$$

for $\beta\in C'$ is non-trivial and therefore the sum over $\beta\in C'$ is equal to zero. So we get that the third term is equal to

$$\frac{p(p-1)}{2}[2(p-1)p-2(p-1)]=p(p-1)^3$$

and

$$\begin{aligned}\sum_{g\in G}|\theta'(g)|^2 &= (p-1)^3+(p-1)^2(p+1)+p(p-1)^3\\ &= (p-1)^2[(p-1)+(p+1)+p^2]=|G|\end{aligned}$$

So $(\theta',\theta')=1$ implies that θ' is irreducible. **QED.**

The table also shows that there are $\frac{1}{2}|(C'\setminus\mathbf{F}_p^*)|=\frac{p(p-1)}{2}$ distinct characters of the fourth type. We thus come to the final result of this section, namely the character table of G.

Table 7 *Character table of* $\mathbf{GL}_2(\mathbf{F}_p)$

	Type	number of that type	dimension
I	$\mu\circ\det$	$(p-1)$	1
II	$\psi_\mu^G-\mu\circ\det$	$(p-1)$	p
III	$\psi^G,\ \psi\neq[w]\psi$	$\frac{(p-1)(p-2)}{2}$	$(p+1)$
IV	$\theta',\ \theta\neq[t]\theta$	$\frac{p(p-1)}{2}$	$(p-1)$

To verify that there are no more irreducible character of G, one shows that the total number of characters in Table 7 is equal to the number of conjugacy classes in Table 1.

Chapter 3

Induced representations from the normalizers of the split and non-split Cartan subgroups

Let us denote 1_N^G and $1_{N'}^G$ the two induced characters. Our goal in this section will be to compare them. We will prove that

$$1_N^G - 1_{N'}^G = 1_B^G - 1$$

where B is the Borel subgroup as defined in the last chapter.

As we have seen, to understand better the induced representation of the subgroup N (resp. N') in G, it is a good strategy to find a set X (resp. X') on which G acts transitively and such that for an $x \in X$ the $\mathrm{Stab}(x) = N$. When we do find such an X then $1_N^G(g)$ is equal to the number of fixed points of g in X. To construct these two sets , X and X', we will exploit the Mobius transformations acting on a projective space.

3.1 Mobius transformations acting on $\mathbf{P}_1(\mathbf{F}_p)$

Consider the natural action of $G = \mathbf{GL}_2(\mathbf{F}_p)$ on the projective lines over $\mathbf{F}_p$, i.e. $\mathbf{P}_1(\mathbf{F}_p) = \mathbf{F}_p \cup \{\infty\}$. This natural action is via the Mobius transformations

$$gx = \begin{pmatrix} a & b \\ c & d \end{pmatrix} x = \frac{ax+b}{cx+d},$$

where $x \in \mathbf{P}_1(\mathbf{F}_p)$, with the convention that $a/0 = \infty$, $g\infty = a/c$ if $c \neq 0$ and $g\infty = \infty$ if $c = 0$.

Lemma 6 *If $g \neq \lambda I$, then g has at most two fixed points in $\mathbf{P}_1(\mathbf{F}_p)$.*

Proof (see for example [La2] p.231 lemma 5.5): Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $c = 0$ then g has one or two fixed points depending if a is equal to d or not. In that case ∞ is always fixed. If $c \neq 0$ then for $x \neq -d/c$ (because $g(-d/c) = \infty$) we have $gx = x$ if and only if

$$cx^2 + x(d-a) - d = 0. \tag{3.1}$$

But this equation has at most two solutions different from $\{\infty\}$ and $g(\infty) = a/c \neq \infty$ so ∞ is not fixed by g. **QED**.

So the number of fixed points of g depends only on the number of solutions of (3.1) and we get

$$\#_{fp}(g) = \begin{cases} 0 & \text{when } (d-a)^2 + 4bc \neq \square \\ 1 & \text{when } (d-a)^2 + 4bc = 0 \\ 2 & \text{when } (d-a)^2 + 4bc = \square \end{cases}$$

where $a = \square$ means that a is a square number in $\mathbf{F}_p$. To compare with the conjugacy classes of G we now consider $p_g(y)$, the characteristic polynomial of g. The roots of $p_g(y) = y^2 - y(a+d) + ad - cd$ are given by the quadratic formula

$$y = \frac{a+d \pm \sqrt{(d-a)^2 + 4cb}}{2}.$$

So the number of distinct roots of the $p_g(y)$ is $\begin{cases} 0 & \text{when } (d-a)^2+4bc \neq \square \\ 1 & \text{when } (d-a)^2+4bc = 0 \\ 2 & \text{when } (d-a)^2+4bc = \square \end{cases}$.

Remembering the conjugacy class of an element $g \in G$ is completely determined by the roots of its characteristic polynomial and by comparing (when $c = 0$ and when $c \neq 0$) the distinct roots and the fixed points of g we see that

$$\begin{aligned} \#_{fp}(g \sim A_1) &= p+1 \\ \#_{fp}(g \sim A_2) &= 1 \\ \#_{fp}(g \sim A_3) &= 2 \\ \#_{fp}(g \sim B_1) &= 0 \end{aligned}$$

3.2 Mobius transformations acting on X.

Let X be set consisting of all subsets of two elements of $\mathbf{P}_1(\mathbf{F}_p)$. Then $|X| = \frac{(p+1)^2-(p+1)}{2} = \frac{(p+1)p}{2}$. The action of G on $\mathbf{P}_1(\mathbf{F}_p)$ by Mobius transformations gives rise naturally to an action of G on X by $g\{x_1, x_2\} = \{gx_1, gx_2\}$.

Lemma 7 *This action of G on X is transitive, and $Stab\{0,\infty\} = N$.*

Proof. Let $a, b \in \mathbf{F}_p$. Then we have $\begin{pmatrix} a & 0 \\ 1 & 1 \end{pmatrix}\{0,\infty\} = \{0, a\}$, $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\{0,\infty\} = \{a,\infty\}$ and $\begin{pmatrix} b & a \\ 1 & 1 \end{pmatrix}\{0,\infty\} = \{a, b\}$ which shows the transitivity.

Setting $x = \{0,\infty\} \in X$ we have

$$\begin{aligned} \text{Stab}(x) &= \{g \in G : gx = x\} \\ &= \{g \in G : g(0,\infty) = (0,\infty)\} \cup \{g \in G : g(0,\infty) = (\infty, 0)\} \end{aligned}$$

Denote S_1 and S_2 the two sets in the last equation. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, g belongs to S_1 if and only if $b = 0$ and $c = 0$. On the other hand g belongs to S_2 if and only if $d = 0$ and $a = 0$. We therefore have

$$\mathrm{Stab}\{0,\infty\} = \left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}\right\} = N \tag{3.2}$$

which completes the proof of the lemma. **QED.**

Theorem 3 *The values of $1_N^G(g)$ on the different conjugacy classes of G (which is equal to the number of fixed points of g with respect to the action of G on X described above) are given in the table below.*

Table 8 *Values taken by $1_N^G(g)$*

conj. class		#of classes	#elements per class	$1_N^G(g)$
$g \sim A_1$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$p-1$	1	$\frac{p(p+1)}{2}$
$g \sim A_2$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$p-1$	p^2-1	0
$g \sim A_3$ $a/b \neq -1$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\frac{(p-1)(p-3)}{2}$	$p(p+1)$	1
$g \sim A_3$ $a/b = -1$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\frac{p-1}{2}$	$p(p+1)$	$\frac{p+1}{2}$
$g \sim B_1$ $t \neq 0$	non − split	$\frac{(p-1)^2}{2}$	$p(p-1)$	0
$g \sim B_1$ $t = 0$	non − split	$\frac{p-1}{2}$	$p(p-1)$	$\frac{p+1}{2}$

Proof. If g is in the center then g is the identity when it acts on X. Therefore the number of points fixed by g is $\frac{p(p+1)}{2}$.

If $g = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ we saw that g fixes ∞ in $\mathbf{P}_1(\mathbf{F}_p)$. We will use the fact that g as a Mobius transformation has order p. Indeed,

$$g^2 = \begin{pmatrix} a^2 & 2a \\ 0 & a^2 \end{pmatrix}$$

$$\begin{aligned} \vdots &= \vdots \\ g^{p-1} &= \begin{pmatrix} a^{p-1} & -a \\ 0 & a^{p-1} \end{pmatrix} \\ g^p &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \end{aligned}$$

So we rewrite g as

$$g = (p - \text{cycle})(\infty) = (x_1, g(x_1), g^2(x_1), \ldots, g^{p-1}(x_1))(\infty)$$

where x_1 is any point different from ∞. The number of fixed point of such a g is the number of subsets of two elements in $\mathbf{P}_1(\mathbf{F}_p)$ fixed by the $g - action$. When you look at g decomposed in cycles it is clear that there are no such fixed point.

If $g = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ where $a \neq b$, we know g fixes two points, 0 and ∞ in $\mathbf{P}_1(\mathbf{F}_p)$. We will use the fact that the order of g divides $(p-1)$. Indeed

$$\begin{aligned} g^2 &= \begin{pmatrix} a^2 & 0 \\ 0 & b^2 \end{pmatrix} \\ \vdots &= \vdots \\ g^{p-1} &= \begin{pmatrix} a^{p-1} & 0 \\ 0 & b^{p-1} \end{pmatrix} \\ &= I. \end{aligned}$$

We write g with cycles and we obtain more subsets of two elements fixed by g, apart from the subset $\{0, \infty\}$ which is always fixed, if and only if the order of g is equal to two. Then we have $(p-1)/2$ more subsets. The order of g is two if and only if $g = \lambda \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The number of fixed points of g in X is $(p+1)/2$ if g has order two and 1 otherwise.

If $g = \begin{pmatrix} t & -1 \\ n & 0 \end{pmatrix}$ where t is the trace and n the norm and such that $p_g(x) = x^2 - tx + n$ is irreducible, we know from the first section of this chapter that g has no fixed points in $\mathbf{P}_1(\mathbf{F}_p)$. By the same reasoning, to have any subset of two elements

fixed by g, we must have g of order 2.

$$g^2 = \begin{pmatrix} t^2 - n & -t \\ nt & -n \end{pmatrix} = \lambda I$$

if and only if $t = 0$. So when $t = 0$, then we obtain $(p+1)/2$ subsets of two elements fixed by g because

$$g = (x_1, gx_1)(x_2, gx_2) \cdots (x_{\frac{p+1}{2}}, gx_{\frac{p+1}{2}}).$$

Therefore the number of fixed points of g is $\frac{p+1}{2}$ if trace$(g) = 0$ and zero otherwise. There are $\frac{(p-1)}{2}$ conjugacy classes of the form B_1 with their trace $= 0$. Indeed, if $t = 0$ we get $g = \begin{pmatrix} 0 & -1 \\ n & 0 \end{pmatrix}$ and $p_g(x) = x^2 + n$ must be irreducible. This is true if and only if $-n$ is not a square in $\mathbf{F}_p$. Which is true half of the values that n can take, $\frac{p-1}{2}$. **QED.**

3.3 Mobius transformations acting on $\mathbf{P}_1(\mathbf{F}_{p^2})$

Before constructing our set X' we analyse the action via Mobius transformations of G on $\mathbf{P}_1(\mathbf{F}_{p^2}) = \mathbf{F}_p(\alpha) \cup \{\infty\}$.

Lemma 8 *When G acts on $\mathbf{P}_1(\mathbf{F}_{p^2})$ via the Mobius transformations action we have*

$$\begin{aligned} \#_{fp}(g)(g \sim A_1) &= p^2 + 1 \\ \#_{fp}(g)(g \sim A_2) &= 1 \\ \#_{fp}(g)(g \sim A_3) &= 2 \\ \#_{fp}(g)(g \sim B_1) &= 2 \end{aligned}$$

Proof: Using lemma 6 we get again that for $g \neq \lambda I$ then g has at most two fixed points. By the same logic presented in section 3.1 it suffices to study $p_g(x)$ to find the number of fixed points of g . So for the g not in a conjugacy class of the form $g \sim B_1$ we get the desired number of fixed points.

It remains only to study the case $p_g(x)$ is irreducible for $g \in G$. Here $p_g(x)$ is irreducible in $\mathbf{F}_p$ but not in $\mathbf{F}_p(\alpha)$. So in $\mathbf{F}_p(\alpha)$, $p_g(x) = (x - \lambda)(x - \overline{\lambda})$ where

$\lambda \in \mathbf{F}_p{}^2 - \mathbf{F}_p$. The numbers λ and $\overline{\lambda}$ are the eigenvalues of g . Now consider W and W' (see [La2] p.235 exercice 14) the two eigenvectors associated to λ and $\overline{\lambda}$. Then W and W' can be written in the following way:

$$W = \begin{pmatrix} w \\ 1 \end{pmatrix}, W' = \begin{pmatrix} w' \\ 1 \end{pmatrix}$$

Indeed, suppose $W = \begin{pmatrix} w \\ 0 \end{pmatrix}$ then

$$\lambda \begin{pmatrix} w \\ 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w \\ 0 \end{pmatrix} = \begin{pmatrix} aw \\ cw \end{pmatrix} = \lambda \begin{pmatrix} w \\ 0 \end{pmatrix}$$

is possible if and only if $c = 0$ which contradicts the fact that $p_g(x)$ is irreducible over $\mathbf{F}_p$. Actually $w' = \overline{w}$ because when you fix $W = \begin{pmatrix} w \\ 1 \end{pmatrix}$ you force W' to be $\begin{pmatrix} \overline{w} \\ 1 \end{pmatrix}$. One verifies this in the equation $gW' = \overline{\lambda} W'$ using that $gW = \lambda W$. Let $S = (W, W') = \begin{pmatrix} w & \overline{w} \\ 1 & 1 \end{pmatrix}$ then using that

$$gS = g(W, W') = (\lambda W, \overline{\lambda} W') = (W, W') \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} = S \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}$$

we find that

$$S^{-1} g S = \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}.$$

Thus S is a matrix that conjugates g to a diagonal matrix in $\mathbf{GL}_2(\mathbf{F}_{p^2})$. Now we claim that w and $\overline{w}$ are fixed points of g. Indeed,

$$\begin{aligned} gw &= S \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} S^{-1}(w) \\ &= S \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} \begin{pmatrix} 1/d & -\overline{w}/d \\ -1/d & w/d \end{pmatrix} (w) \end{aligned}$$

$$
\begin{aligned}
&= S\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}(\infty) \\
&= S(\infty) \\
&= w
\end{aligned}
$$

In a similar way one shows $g(\overline{w}) = \overline{w}$. By *lemma* 6 , we obtain that g has exactly two fixed points , w and $\overline{w}$. **QED.**

3.4 Mobius transformations acting on X'.

The group G acts on $X' = (\mathbf{F}_{p^2} \setminus \mathbf{F}_p)/conj.$ by Mobius transformations. (This follows because if $x \in \mathbf{F}_{p^2}$, then $\overline{g(x)} = g(\overline{x})$.)

Lemma 9 *The action of G on X' is transitive, and the* Stab*ilizer* Stab(x) *is equal to N', if $x = [\alpha] \in X'$.*

Proof. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$; then $g(\alpha) = \alpha$ if and only if

$$\frac{a\alpha + b}{c\alpha + d} = \alpha \text{ or } \frac{a\alpha + b}{c\alpha + d} = -\alpha.$$

one checks that this is true if and only if $g \in N'$. The transitivity of the G-action follows from a counting argument: the orbit of $[\alpha]$ has size $\frac{|G|}{|\mathrm{Stab}([\alpha])|} = \frac{p(p-1)^2(p+1)}{2(p-1)(p+1)} = \frac{p(p-1)}{2} = |X'|$. **QED.**

From the preceding section, when G acts on $P_1(\mathbf{F}_{p^2})$ we have

$$
\begin{aligned}
\#_{fp}(g \sim A_1) &= p^2 + 1 \\
\#_{fp}(g \sim A_2) &= 1 \\
\#_{fp}(g \sim A_3) &= 2 \\
\#_{fp}(g \sim B_1) &= 2
\end{aligned}
$$

We will use this to calculate the number of fixed points of an arbitrary $g \in G$ with respect to the action on X'. The computation will prove the following theorem.

Theorem 4 *The values of $1_{N'}^{G}(g)$ on the diffent conjugacy classes of G (which is equal to the number of fixed points of g with respect to the action of G on X' defined above) are compiled in the table below.*

Table 9 *Values taken by $1_{N'}^{G}(g)$*

	conj. class	*#of classes*	*#elements per class*	$1_{N'}^{G}(g)$
$g \sim A_1$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$p-1$	1	$\frac{p(p-1)}{2}$
$g \sim A_2$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$p-1$	p^2-1	0
$g \sim A_3$ $a/b \neq -1$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\frac{(p-1)(p-3)}{2}$	$p(p+1)$	0
$g \sim A_3$ $a/b = -1$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\frac{p-1}{2}$	$p(p+1)$	$\frac{p-1}{2}$
$g \sim B_1$ $t \neq 0$	non − split	$\frac{(p-1)^2}{2}$	$p(p-1)$	1
$g \sim B_1$ $t = 0$	non − split	$\frac{p-1}{2}$	$p(p-1)$	$\frac{p+3}{2}$

Proof: For g in the center the number of fixed points by g is $|X'| = \frac{p(p-1)}{2}$.

For the case where $g = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, there is no $x \in \mathbf{F}_p(\alpha)$ such that $g(x) = x$ (the point $\{\infty\}$ being the only one in $P_1(\mathbf{F}_p(\alpha))$). So the only possible case is when an element is sent into its conjugate by g. We have $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}(x_1 + x_2\alpha) = (x_1 - x_2\alpha)$ if and only if $2ax_2\alpha = -1$, which is impossible because $2ax_2\alpha \notin \mathbf{F}_p$ while -1 does belong to $\mathbf{F}_p$. So the number of fixed points of such a g is zero.

For the case where $g = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $a \neq b$ then g has two fixed points in $\mathbf{P}_1(\mathbf{F}_p(\alpha))$ namely ∞ and $\{0\}$. But those two do not belong in $\mathbf{F}_{p^2} - \mathbf{F}_p$. Therefore again our only hope is to find an x such that $g(x) = \overline{x}$. So this condition says $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}(x_1 +$

$x_2\alpha) = x_1 - x_2\alpha$ if and only if $(a-b)x_1 + (a+b)x_2\alpha = 0$. We know $x_2 \neq 0$, it implies that $(a+b) = 0$. Since $(a+b) = 0$ then $(a-b)$ just can't be equal to zero and x_1 must be zero. Hence g has a fixed point if and only if $x_1 = 0$ and $a/b = -1$. When $a/b = -1$ the number of fixed points is equal to the number of different values taken by x_2. Since $x_2\alpha = -x_2\alpha$ in X', we have that this number is $(p-1)/2$. Therefore the number of fixed points of such a g is $\begin{cases} \frac{p-1}{2} & a/b = -1 \\ 0 & \text{otherwise} \end{cases}$.

For the case $g = \begin{pmatrix} t & -1 \\ n & 0 \end{pmatrix}$ where $x^2 - tx + n$ is irreducible, the argument is less straightforward. From our earlier result, we know there exist $w, \overline{w} \in \mathbf{F}_p(\alpha) - \mathbf{F}_p$ such that $g(w) = w$ and $g(\overline{w}) = \overline{w}$. So in any case, we certainly have one element in X' fixed by g . If there are more fixed points they must satisfy $g(x) = \overline{x}$ where $x \in \mathbf{F}_p(\alpha) - \mathbf{F}_p$. This is true if and only if $\frac{tx-1}{nx} = \overline{x}$ if and only if $tx - 1 = n(x\overline{x})$. So we deduce that t must be equal to zero because $x\overline{x} \in \mathbf{F}_p$ while $x \notin \mathbf{F}_p$. When $t = 0$ we have that $\begin{pmatrix} 0 & -1 \\ n & 0 \end{pmatrix}(x) = \overline{x}$ if and only if $nx\overline{x} = -1$. So we are looking for the number of x satisfying

$$x\overline{x} = \frac{-1}{n}. \tag{3.3}$$

Lemma 10 *The following sequence of mappings is exact.*

$$1 \longrightarrow \ker N \longrightarrow \mathbf{F}_{p^2}^{\star} \xrightarrow{\text{Norm}} \mathbf{F}_p^{\star} \longrightarrow 1$$

Proof: The norm of an element $x \in \mathbf{F}_{p^2}$ is defined as $\text{Norm}(x) = x\overline{x}$. One checks that the norm is a homomorphism. If $x = x_1 + x_2\alpha$, its norm is

$$\text{Norm}(x) = (x_1 + x_2\alpha)(x_1 - x_2\alpha) = x_1^2 - x_2^2\alpha^2$$

where $m \in \mathbf{F}_p - \{0\}$. First, the cardinality of $\ker(N)$ is at most $2p$ because for a fixed x_1 there is at most two values of x_2 such that $\text{Norm}(x) = 1$. On the other hand the cardinality of $\ker(N)$ is at least $(p+1)$ because $(p+1)$ divides $|\ker(N)|$ since it is the kernel of an homomorphism $\mathbf{F}_{p^2}^{*} \longrightarrow \mathbf{F}_p^{*}$. We deduce that $|\ker(N)| = (p+1)$. So the sequence is in fact an *exact sequence*, hence $\mathbf{F}_{p^2}^{*}/\ker(N)$ is isomorphic to $\mathbf{F}_p^{*}$. **QED.**

Lemma 10 implies that for $-1/n$ there are $p+1$ elements in $\mathbf{F}_{p^2}^*$ (one whole coset of $\ker(N)$) such that $\text{Norm}(x) = -1/n$. For such an x with norm equal to $-1/n$ we have that $x \notin \mathbf{F}_p^*$. Indeed if it were then $x^2 = -1/n$ which implies $x^2 + 1/n = 0$ has a solution in $\mathbf{F}_p$. This contradicts our choice of g. Therefore the number of fixed points of g in X' is equal to $1 + \frac{(p-1)}{2} = \frac{(p+1)}{2}$. **QED.**

3.5 The link between 1_N^G and $1_{N'}^G$

We now deduce the link between 1_N^G and $1_{N'}^G$. Consider the character $\chi = 1_N^G - 1_{N'}^G$. Using tables 8 and 9 we have that

$$\begin{aligned}
\chi(g \sim A_1) &= p \\
\chi(g \sim A_2) &= 0 \\
\chi(g \sim A_3) &= 1 \\
\chi(g \sim B_1) &= -1.
\end{aligned}$$

On the other hand, we remark that the irreducible character of G of type two $\psi_\mu^G - \mu \circ det$ (see table 3 chapter 2) is exactly equal to χ when $\mu : \mathbf{F}_p^* \longrightarrow \mathbf{C}^*$ is the trivial homomorphism. But $\psi_1^G - 1 = 1_B^G - 1$.

Theorem 5 *Let $G = \mathbf{GL}_2(\mathbf{F}_p)$ with the subgroups N, N' and B as defined in chapter 2. We have the following relation on the induced characters*

$$\boxed{1_N^G - 1_{N'}^G = 1_B^G - 1}. \tag{3.4}$$

The dimension equation is now verified.

$$\begin{aligned}
\dim(1_N^G) - \dim(1_{N'}^G) &= \frac{p(p+1)}{2} - \frac{p(p-1)}{2} \\
&= p \\
&= \dim(1_B^G) - \dim(1).
\end{aligned}$$

Chapter 4

Extension of Perlis' result

In this chapter we will extend Perlis' method of comparing the Class Groups of arithmetically equivalent fields to the fixed fields of the normalizers of the split and non-split Cartan subgroup and the Borel subgroup. The construction we will encounter in this chapter is an analogue of the one of Perlis found in [Pe2].

The first section is devoted to defining the group theoretic invariant, a positive integer number ν, in terms of the induced representations of $G = \mathbf{GL}_2(\mathbf{F}_p)$ from the latter subgroups and in showing that its prime divisors must divide the order of G. In the second section we construct an isomorphism between the ℓ-part of the ideal class group of the fixed field of N onto the ℓ-part of direct sum of the class group of N' and the class group of B, and this for all primes ℓ not dividing ν. In the last section we discuss the difference between the main theorem of this chapter and Nehrkorn's theorem established in [Wa]. We will see how important it is to find concrete examples where the set of prime divisors of ν is strictly contained in the set of prime divisors of $|G|$ to make our result effective.

4.1 Definition and divisors of ν

Let K be a normal extension of $\mathbf{Q}$ with Galois group G. Consider N, N', B the three subgroups defined in chapter 2 and their respective fixed fields K^N, $K^{N'}$, K^B. We have that $[K : \mathbf{Q}] = |G| = p(p-1)^2(p+1)$, $[K^N : \mathbf{Q}] = |G/N| = \frac{p(p+1)}{2}$,

$[K^{N'} : \mathbf{Q}] = |G/N'| = \frac{p(p-1)}{2}$, $[K^B : \mathbf{Q}] = |G/B| = (p+1)$, and from chapter 3, we know that $1_N^G + 1 = 1_{N'}^G + 1_B^G$. Let us denote by χ the character $1_N^G + 1$ and by χ' the character $1_{N'}^G + 1_B^G$. Their respective representations, D and $D' : G \longrightarrow \mathbf{GL}_k(\mathbf{Q})$, are isomorphic, where $k = 1 + |G/N| = |G/N'| + |G/B| = \frac{p^2+p+2}{2}$. Those two representations are the permutation representation of G on $V = \mathbf{Q}[G/N] \ni \mathbf{Q}$ and $V' = \mathbf{Q}[G/N'] \oplus \mathbf{Q}[G/B]$. Since they are isomorphic there exist a rational $k \times k$ invertible matrix M such that

$$D(g)M = MD'(g) \tag{4.1}$$

for all $g \in G$. By clearing denominators, we may assume that the coefficients of M are integers. For the moment we ignore invertibility and we look at all integral matrices satisfying (4.1). To see what M looks like when it satisfies (4.1) we describe D and D' explicitly. Let $\rho_1 = 1, \rho_2, \rho_3, \ldots, \rho_{|G/N|}$ be representatives for the left cosets of G by N and let $\rho_k = 1$ be a representative for the coset G. Now let $\rho'_1 = 1, \rho'_2, \ldots, \rho'_{|G/N'|}$ be representatives for the left cosets of G by N' and let $\rho'_{k-p}, \ldots, \rho'_k = 1$ be representatives for the left cosets of G by B. The action of G on these cosets describes two homomorphisms π and π' from G into the symmetric group $\mathbf{S}_k$ given by $\pi_g(i) = j$, where $g\rho_i N = \rho_j N$ for $1 \leq i \leq |G/N|$ and $\pi_g(k) = 1$ and $\pi'_g(i) = j$, where $g\rho'_i N' = \rho'_j N'$ for $1 \leq i \leq |G/N'|$ and $g\rho'_i B = \rho'_j B$ for $i > |G/N'|$. Associating i with the ith basis element of an k-dimensional vector space over $\mathbf{Q}$ then identifies π_g and π'_g with the matrices

$$D(g) = (\delta_{i,\pi_g j}) \text{ and } D'(g) = (\delta_{i,\pi'_g j}),$$

the displayed term being the (i,j)th element and δ being the Kronecker δ function. By comparing the coefficients one sees that a $k \times k$ matrix $M = (m_{ij})$ satisfies (4.1) if and only if

$$m_{ij} = m_{\pi_g i, \pi'_g j} \tag{4.2}$$

for all $g \in G$. That is, if and only if M is *constant on the orbits of G under the action* $g(i,j) = (\pi_g i, \pi'_g j)$.

Let $\mathcal{M}$ be the set of all integral $k \times k$ matrices satisfying the equivalent conditions (4.1) and (4.2) and let

$$\nu = \gcd\{|\det M|, M \in \mathcal{M}\}. \tag{4.3}$$

Since $\chi = \chi'$, there exist at least one $M \in \mathcal{M}$ with nonzero determinant. Thus ν is a well defined positive integer.

Remark 1 By interchanging χ and χ' (D and D') we obtain another set $\mathcal{M}'$ and this does not change ν. Then a matrix M belongs to $\mathcal{M}$ if and only if its transpose M^t belongs to $\mathcal{M}'$. We will need the set $\mathcal{M}'$ in the next section.

We now turn our attention to the prime divisors of ν. We want to show that these primes divide the order of G. The group G acts in two ways on the free module $\mathbf{Z}_\ell x_1 \oplus \mathbf{Z}_\ell x_2 \oplus \cdots \oplus \mathbf{Z}_\ell x_k$ over the ring of ℓ-adic integer $\mathbf{Z}_\ell$ by permuting the x_i's by the rules of π and π'. That is, the element $g \in G$ acts on these free module via the matrices $D(g)$ and $D'(g)$. This gives us two $\mathbf{Z}_\ell[G]$-modules which we denote V_ℓ and V'_ℓ.

Lemma 11 *The prime divisors of ν are precisely the primes ℓ for which the $\mathbf{Z}_\ell[G]$-modules V_ℓ and V'_ℓ are not isomorphic.*

Proof: Suppose V_ℓ and V'_ℓ are isomorphic. A $\mathbf{Z}_\ell[G]$-isomorphism from V_ℓ to V'_ℓ is described in term of the basis $x_1, x_2, \ldots, x_k$ by a matrix $N = (n_{ij})$ in $\mathbf{GL}_k(\mathbf{Z}_\ell)$ satisfying

$$D(g)N = ND'(g)$$

for all $g \in G$. That is N satisfies (4.2) and $\det N \not\equiv 0 \pmod{\ell}$. Let $M = (m_{ij})$ be the matrix with coefficients in $\mathbf{Z}$ uniquely determined by $0 \leq m_{ij} < \ell$ and $m_{ij} \equiv n_{ij} \pmod{\ell}$. Then $M \in \mathcal{M}$ (by verifying equation (4.2)) and $\det M \equiv \det N \not\equiv 0 \pmod{\ell}$. So we have ℓ does not divide ν . Conversely, if ℓ does not divide ν, then there is a matrix $M \in \mathcal{M}$ whose determinant is not divisible by ℓ. Thus M is invertible over $\mathbf{Z}_\ell$ and yields an isomorphism from V_ℓ to V'_ℓ. **QED.**

With this lemma, we will know the prime divisors of ν as soon as we have a way of recognizing the primes ℓ for which V_ℓ and V'_ℓ are isomorphic.

Lemma 12 *Let ℓ be any prime number not dividing the order of G. Then V_ℓ and V'_ℓ are projective $\mathbf{Z}_\ell[G]$-modules.*

Proof: We first show V_ℓ is projective. Let $e : V_\ell \longrightarrow Y$ and $f : F \longrightarrow Y$ be any two $\mathbf{Z}_\ell[G]$-homomorphisms where f is surjective. By definition V_ℓ is projective if and only if there exist $\psi : V_\ell \longrightarrow F$ a $\mathbf{Z}_\ell[G]$-homomorphism such that $f\psi = e$. Since G permutes the x_i's in a two orbits action, any $\mathbf{Z}_\ell[G]$-homomorphism is completely determined by the image of x_1 and x_k. Furthermore, an assignment of x_1 and x_k extends to a $\mathbf{Z}_\ell[G]$-homomorphism from V_ℓ if and only if the stabilizer of x_1 also stabilizes its image and the stabilizer of x_k also stabilizes its image. The stabilizer of x_1 is N and the stabilizer of x_k is G. Hence N also stabilizes $e(x_1)$ and G stabilizes $e(x_k)$ in Y. Let $z_1 \in F$ be any preimage of $e(x_1)$ and $z_k \in F$ be any preimage of $e(x_k)$. Since $|N|$ and $|G|$ are not divisible by ℓ they are invertible in $\mathbf{Z}_\ell$. We now set $z'_1 = |N|^{-1} \sum_{n\in N} nz_1$ and $z'_k = |G|^{-1} \sum_{g\in G} gz_k$. Then we have

$$\begin{aligned} f(z'_1) &= f(|N|^{-1} \sum_{n\in N} nz_1) \\ &= |N|^{-1} \sum_{n\in N} nf(z_1) \\ &= \frac{1}{|N|} \sum_{n\in N} ne(x_1) = e(x_1) \end{aligned}$$

because $n \in \mathrm{Stab}(e(x_1))$. Similarly we have $f(z'_k) = e(x_k)$. So the map $\psi : x_1 \longmapsto z'_1$ and $x_k \longmapsto z'_k$ defines the desired $\mathbf{Z}_\ell[G]$-homomorphism that satisfies $f\psi = e$. Indeed, on one hand one verifies that $n_0\psi(x_1) = \psi(x_1)$ for all $n_0 \in N$ and $g_0\psi(x_k) = \psi(x_k)$ for all $g_0 \in G$ to show that ψ is an homomorphism. On the other hand one checks that $f \circ g(x_1) = e(x_1)$ and $f \circ g(x_k) = e(x_k)$. We therefore have that V_ℓ is a projective $\mathbf{Z}_\ell[G]$-module.

One shows in a similar fashion that V'_ℓ is projective by studying the images of x_1, x_{k-p} and their corresponding stabilizers N', B and by using the fact that $|N'|$ and $|B|$ are invertible in $\mathbf{Z}_\ell$. **QED.**

We now obtain the main result of this section.

Theorem 6 *Every prime number dividing ν divides the order of G.*

Proof: Given a prime ℓ not dividing $|G|$. We will show that ℓ does not divide ν. For this, by lemma 11, we must show $V_\ell \simeq V'_\ell$ as $\mathbf{Z}_\ell[G]$-modules. The representations D, D' of G on V_ℓ and V'_ℓ have the same character. Furthermore since ℓ does not divide $|G|$ it implies that V_ℓ and V'_ℓ are projective. And projective $\mathbf{Z}_\ell[G]$-modules are determined up to isomorphism by their characters (see [Se2] section 16.1, corollary 2 to theorem 34). We need this fact about projective Z_ℓ-modules because $\mathbf{Z}_\ell$ representations are not always determined by their characters (for example, let V_1 and $V_{(p+1)}$ be two vector spaces over $\mathbf{F}_p$ with dimension 1 and $(p+1)$. Consider now ρ_1 and $\rho_{(p+1)}$ the respective trivial representations of G acting on V_1 and $V_{(p+1)}$; every $g \in G$ is sent in the identity automorphism. The characters are equal even if the representations are not isomorphic). This shows that V_ℓ and V'_ℓ are isomorphic. **QED.**

4.2 The isomorphism $\mathrm{Cl}^{(\ell)}_{K^N} \simeq \mathrm{Cl}^{(\ell)}_{K^{N'}} \oplus \mathrm{Cl}^{(\ell)}_{K^B}$ for ℓ not dividing ν.

The ideal class group Cl_K (for any number field K) is the direct sum of its ℓ-Sylow subgroups. This section contains a proof that $\mathrm{Cl}^{(\ell)}_{K^N} \simeq \mathrm{Cl}^{(\ell)}_{K^{N'}} \oplus \mathrm{Cl}^{(\ell)}_{K^B}$ whenever ℓ does not divide ν. We begin by considering the following two *arithmetically equivalent* algebras (see introduction) $L = K^N \oplus \mathbf{Q}$ and $L' = K^{N'} \oplus K^B$. Let $M = (m_{ij})$ be a matrix in $\mathcal{M}$. We now define a map $\mu_M : L^* \longrightarrow L'^*$; for $a = a_N \oplus a_1 \in L^*$ we set

$$\mu_M(a) = \prod_{i=1}^{k-1} \rho_i(a_N)^{m_{i1}}(a_1)^{m_{k1}} \oplus \prod_{i=1}^{k-1} \rho_i(a_N)^{m_{ik}}(a_1)^{m_{kk}}$$

Lemma 13 *For matrices A and B in $\mathcal{M}$ and for $a = a_N \oplus a_1 \in L^*$ we have*

(*i*) μ_M *is a homomorphism (of multiplicative groups) from* $L^* \to L'^*$.

(*ii*) $\mu_{(A+B)}(a) = \mu_A(a)\mu_B(a)$.

(*iii*) $(\mu_{B^t}) \circ (\mu_A) = \mu_{(AB^t)}$.

Proof. (i) We certainly have that $\mu_A(a)$ is nonzero and lies in $K \oplus K$. For $n' \in N' = \mathrm{Gal}(K/K^{N'})$ we have $\pi'_{n'}(1) = 1$ and for $b \in B = \mathrm{Gal}(K/K^B)$ we have $\pi'_b(k) = k$. Writing $A = (m_{ij})$ and setting $\pi_{n'}(i) = r$ and $\pi_b(i) = l$, from (4.2) we then have $m_{i1} = m_{k1}$ and $m_{ik} = m_{lk}$. Thus we get

$$\begin{aligned}(n' \oplus b)\mu_A(a) &= \prod_{i=1}^{k-1} n'\rho_{i=1}(a_N)^{m_{i1}} n'(a_1)^{m_{k1}} \oplus \prod_{i}^{k-1} b\rho_i(a_N)^{m_{ik}} b(a_1)^{m_{kk}} \\ &= \prod_{r=1}^{k-1} \rho_r(a_N)^{m_{r1}}(a_1)^{m_{r1}} \oplus \prod_{l=1}^{k-1} \rho_l(a_N)^{m_{lk}}(a_1)^{m_{kk}} \\ &= \mu_A(a),\end{aligned}$$

so the image $\mu_A(a)$ lies in the algebra $K^{N'} \oplus K^B$ since n' and b were taken arbitrary. Clearly μ_A is multiplicative so we conclude that it is a group homomorphism.

(ii) It follows directly from the definitions

(iii) Recall that for $B \in \mathcal{M}$ its transpose belongs to $\mathcal{M}'$ (see remark 1). Just as each matrix in $\mathcal{M}$ gives rise to a homomorphism from L^* to L'^*, the matrix B^t gives rise to a homomorphism μ_{B^t} in the opposite direction, namely for $a' = a_{N'} \oplus a_B$ and $B^t = (b_{ij})$ we have

$$\mu_{B^t}(a') = \prod_{i=1}^{|G/N'|} \rho'_i(a_{N'})^{b_{i1}} \cdot \prod_{i=|G/N'|+1}^{k} \rho'_i(a_B)^{b_{i1}} \oplus \prod_{i=1}^{|G/N'|} \rho'_i(a_{N'})^{b_{ik}} \cdot \prod_{1=|G/N'|+1}^{k} \rho'_i(a_B)^{b_{1k}}.$$

We also have that the matrix product yields $\mu_{AB^t} : L \longrightarrow L'$. The composition $(\mu_{B^t}) \circ (\mu_A)$ also maps L onto itself. One checks the validity of (iii) by a straightforward computation using (4.2) to convert indices like we did in the proof of (i) above. **QED.**

The maps μ_M will be used to define homomorphisms between the class groups of L and L'. This is accomplished in several steps. First, for any matrix M, let M^+ be the matrix obtained by replacing the negative components of M by zero, and let $M^- = (-M)^+$. Then both M^+ and M^- have nonnegative entries, and $M = M^+ - M^-$. By looking at condition (4.2) we see that when $M \in \mathcal{M}$ we also have M^+ and M^- both belong to $\mathcal{M}$.

Next, we consider a nonnegative matrix $M^+ \in \mathcal{M}$ and observe that if $x \in L^*$ is the direct sum of two integers (in K^N and $\mathbf{Q}$) then $\mu_{M^+}(x)$ is also the direct

sum of two integers (in $K^{N'}$ and K^B). For the integral ideals $\mathcal{U}$, $\mathcal{A}$ of K^N and $\mathbf{Q}$ respectively we define

$$\mu_{M^+}(\mathcal{U} \oplus \mathcal{A}) = \langle \mu_{M^+}(u \oplus a), u \in \mathcal{U} \text{ and } a \in \mathcal{A} \rangle$$

to be the L'-ideal generated by the images of elements of $\mathcal{U} \oplus \mathcal{A}$. This definition extends immediately to direct sums of fractional ideals (of K^N and $\mathbf{Q}$).

Finally, for $M = M^+ - M^-$ in $\mathcal{M}$ and for any fractional ideal $\mathcal{U} \oplus \mathcal{A}$ of L', we set

$$\mu_M(\mathcal{U} \oplus \mathcal{A}) = (\mu_{M^+}(\mathcal{U} \oplus \mathcal{A})) \cdot (\mu_{M^-}(\mathcal{U} \oplus \mathcal{A}))^{-1}.$$

This is a well-defined map on $I_N \oplus I$, where I_N and I are the ideal groups [1] of K^N and $\mathbf{Q}$ respectively. By denoting the ideal groups of $K^{N'}$ and K^B by $I_{N'}$ and I_B we have the following lemma.

Lemma 14 *The map $\mathcal{U} \oplus \mathcal{A} \longmapsto \mu_M(\mathcal{U} \oplus \mathcal{A})$ is a group homomorphism from $I_N \oplus I$ to $I_{N'} \oplus I_B$.*

Proof: Let $\mathcal{U} \oplus \mathcal{A}$ and $\mathcal{V} \oplus \mathcal{B}$ be two elements in $I_N \oplus I$. In order to show $\mu_M((\mathcal{U} \oplus \mathcal{A})(\mathcal{V} \oplus \mathcal{B})) = \mu_M(\mathcal{U} \oplus \mathcal{A}) \cdot \mu_M(\mathcal{V} \oplus \mathcal{B})$ it suffices to check that equality holds when both sides are extended to $K \oplus K$. Writing the extended ideals in square braquets, we must show $[\mu_M((\mathcal{U} \oplus \mathcal{A})(\mathcal{V} \oplus \mathcal{B}))] = [\mu_M(\mathcal{U} \oplus \mathcal{A})][\mu_M(\mathcal{V} \oplus \mathcal{B})]$. This latter equality is an immediate consequence of the following *claim*:
For every direct sum of ideals $\mathcal{W} \oplus \mathcal{C}$ of $K^N \oplus \mathbf{Q}$ we have

$$[\mu_M(\mathcal{W} \oplus \mathcal{C})] = \prod_{i=1}^{k} \rho_i[\mathcal{W}]^{m_{i1}} \oplus \prod_{i=1}^{k} \rho_i[\mathcal{C}]^{m_{ik}} \tag{4.4}$$

the right hand side brackets denote extended ideals to K and we consider product of ideals in K. To prove this claim it is sufficient to consider M with nonnegative coefficients and $\mathcal{W}, \mathcal{C}$ are integral ideals in their respective number ring.
The left hand side of (4.4) is generated by the images $\mu_M(w \oplus c)$ of elements in

[1] The ideal group of a number field K is the group of the fractional ideals containing the integral ideals with the natural multiplication of ideals.

$\mathcal{W} \oplus \mathcal{C}$, so the we have the inclusion $\subseteq$. Denote by the right hand side of (4.4) by $[\mathcal{W}]^{M_1} \oplus [\mathcal{C}]^{M_k}$. Write $\mathcal{W} = (w_1, w_2)$ and $\mathcal{C} = (c_1, c_2)$ (see for example [Ma] p. 61). Then $(w_1) = \mathcal{W} \cdot \mathcal{D}_1^w$ and $(w_2) = \mathcal{W} \cdot \mathcal{D}_2^w$ with integral ideals $\mathcal{D}_1^w, \mathcal{D}_2^w$. The generators can be chosen so that $\mathcal{D}_1^w$ is relatively prime to the norm of $\mathcal{D}_2^w$; so that $[\mathcal{D}_1^w]$ is relatively prime to every conjugate of $[\mathcal{D}_1^w]$ (see, for example [He], Satz 74). By a similar construction we obtain $\mathcal{D}_1^c$ and $\mathcal{D}_2^c$ with the same property where $(c_1) = \mathcal{C} \cdot \mathcal{D}_1^c$ and $(c_2) = \mathcal{C} \cdot \mathcal{D}_2^c$.

Now the claimed equality is clearly true for principal ideals, and the map $\mathcal{W} \oplus \mathcal{C} \longmapsto [\mathcal{W}]^{M_1} \oplus [\mathcal{C}]^{M_k}$ is multiplicative, so

$$[\mu_M(w_1 \oplus c_1)] = [\mathcal{W}]^{M_1} \cdot [\mathcal{D}_1^w]^{M_1} \oplus [\mathcal{C}]^{M_k} \cdot [\mathcal{D}_1^c]^{M_k}$$

$$[\mu_M(w_2 \oplus c_2)] = [\mathcal{W}]^{M_1} \cdot [\mathcal{D}_2^w]^{M_1} \oplus [\mathcal{C}]^{M_k} \cdot [\mathcal{D}_2^c]^{M_k}.$$

The gcd of these two principal ideals of $I_K \oplus I_K$ is $[\mu_M(w_1 \oplus c_1), \mu_M(w_2 \oplus c_2)] = [\mathcal{W}]^{M_1} \oplus [\mathcal{C}]^{M_k}$, showing that the right side of (4.4) is contained in the left side. This gives the proof of the lemma. **QED.**

Since the μ_M take principal ideals of $I_N \oplus I_{\mathbf{Q}}$ to principal ideals of $I_{N'} \oplus I_B$, we obtain a family of homomorphisms between Cl_{K^N} and $\mathrm{Cl}_{K^{N'}} \oplus \mathrm{Cl}_{K^B}$ for each $M \in \mathcal{M}$. The next theorem studies these homomorphisms when they are restricted to the ℓ-Sylow subgroups of the ideal class groups.

Theorem 7 *Let $K^N, K^{N'}$ and K^B be as before. Then for all prime numbers ℓ not dividing ν we have $Cl_{K^N}^{(\ell)} \simeq Cl_{K^{N'}}^{(\ell)} \oplus Cl_{K^B}^{(\ell)}$.*

Proof. Since ℓ does not divide ν there is a matrix $A \in \mathcal{M}$ with ℓ not dividing $\det A$. Let B be the matrix whose transpose is $B^t = (\det A) \cdot A^{-1}$. Then B also belongs to $\mathcal{M}$. Let $\overline{\mathcal{U}} \in \mathrm{Cl}_{K^N}^{(\ell)}$ lie in the kernel of μ_M. Then $\mu_M \overline{\mathcal{U}} = 1$, so $1 = \mu_{(B^t)}(\mu_A \overline{\mathcal{U}}) = \mu_{AB^t} \overline{\mathcal{U}} = \overline{\mathcal{U}}^{(\det A)}$, by lemma 13. Since $\overline{\mathcal{U}}$ is killed by a power of ℓ and by $\det A$, it follows that $\overline{\mathcal{U}} = 1$, so the restriction of μ_A to $\mathrm{Cl}_{K^N}^{(\ell)}$ is injective. Since our arithmetically equivalent algebras, L and L', have symmetric roles, exchanging them yields an injection in the opposite direction, implying that the finite groups $\mathrm{Cl}_{K^N}^{(\ell)}$ and $\mathrm{Cl}_{K^{N'}}^{(\ell)} \oplus \mathrm{Cl}_{K^B}^{(\ell)}$ are isomorphic. **QED.**

4.3 Discussion on the Brauer's class number relation

In Brauer relation theory we study the relation between class groups of subfields L^H of L when we have an equation relating their respective induced representations in G =Gal$(L/\mathbf{Q})$ in the following way

$$\sum_{H \leq G} a_H 1_H^G = \sum_{H \leq G} b_H 1_H^G, \tag{4.5}$$

and $a_H, b_H \in \mathbf{Z}^{\geq 0}$. For example when all the a_H, b_H's are equal to zero but for one $H < G$ and one $H' < G, H \neq H'$ we have $a_H = b_{H'} = 1$, then L^H and $L^{H'}$ are arithmetically equivalent. Walter, in his article [Wa] published in 1979 (almost at same time Perlis proved his result on the class groups of arithmetically equivalent fields), showed the following theorem.

Theorem 8 (Nehrkorn's theorem) *Let L be a normal extension $\mathbf{Q}$ and suppose the equation (4.5) is satisfied on the induced representation for some a_H, b_H. Then for all the primes p not dividing the order of G=Gal$(L/\mathbf{Q})$, we have the following isomorphism on the p-part of the subgroups*

$$\oplus_H (Cl_{L^H}^{(p)})^{a_H} \simeq \oplus_H (Cl_{L^H}^{(p)})^{b_H}.$$

Nehrkorn's theorem already tells us that for all the primes not dividing the order of $\mathbf{GL}_2(\mathbf{F}_p)$ we have the desired isomorphism of Theorem 7 between the class groups. In other words, if it is impossible to find concrete examples where the set of prime divisors of the integer ν is strictly contained in the set prime of divisors of $|G|$, then Theorem 7 would not be very interesting. In the next section, we will study an example where the only prime divisor of ν is 2 while the prime divisors of $|G|$ are 2 and 3.

Perlis' construction can be extended, mutatis mutandis, to the more general context of equation (4.5). It is possible to construct a ν-Perlis integer with its

associated extended relation on the class groups. But without concrete examples and the possibility of computing the integer ν these results would not tell us much more than what we extract from Nehrkorn's theorem.

Chapter 5

Numerical examples

In this section we study some concrete examples. First, we find normal extensions of $\mathbf{Q}$ with Galois group $\mathbf{PGL_2(F_3)}$, by studying elliptic curves. Second, we apply theorem 7 to the class groups of arithmetically equivalent algebras by computing explicitly the integer ν.

5.1 The field of 3-division points on E.

We have for $G = \mathbf{GL_2(F}_p)$ that $1_N^G + 1 = 1_{N'}^G + 1_B^G$ (see 3.4). These four characters are also characters of $\mathbf{PGL_2(F}_p) = G/Z$ which is denoted by $\overline{G}$. Now we denote in a similar way $\overline{N} = N/Z, \overline{B} = B/Z$ and $\overline{N'} = N'/Z$. Using the fact that Z is the center of G, one shows $1_N^G(\overline{g}\overline{h}) = 1_N^G(\overline{g})1_N^G(\overline{h})$. We observe also that $1_N^G = 1_{\overline{N}}^{\overline{G}}$ when we consider these characters as characters of $\overline{G}$. Note that in the following $\overline{x} = xZ$.

$$\begin{aligned} 1_{\overline{N}}^{\overline{G}}(\overline{h}) &= \frac{1}{\overline{G}} \sum_{\overline{x} \in \overline{G}} \overline{1_N}(\overline{x}\overline{h}\overline{x}^{-1}) \\ &= \frac{1}{\overline{G}Z} \sum_{x \in G} \overline{1_N}(xhx^{-1}Z) \\ &= \frac{1}{G} \sum_{x \in G} \overline{1_N}(xhx^{-1}) = 1_N^G(h) \end{aligned}$$

So we have a similar relation of characters in $\overline{G}$, namely $\boxed{1_{\overline{N}}^{\overline{G}} + 1 = 1_{\overline{N'}}^{\overline{G}} + 1_{\overline{B}}^{\overline{G}}}$.

Our goal is to find a normal extension L of $\mathbf{Q}$ with Galois group isomorphic to $\overline{G}$. This is achieved by considering the p-division field of an elliptic curve $\mathbf{E}$ defined over $\mathbf{Q}$ (i.e the a_i's are in $\mathbf{Q}$). To make possible any calculation we fix $p = 3$. Let $\mathbf{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\mathbf{Q}$. A fundamental fact in the theory of elliptic curve is that $\mathbf{E} = \{P = (x, y)$ satisfying the equation that defines $\mathbf{E}\}$ has a group structure. This group is described in Silverman's book ([Si] chap.3).

Now in that group consider $\mathbf{E}[3]$ the subgroup of $\mathbf{E}$ consisting of the 3-division points, $\mathbf{E}[3] = \{P \in \mathbf{E}$ such that $3P = 0\}$. Let us denote by $L_{\mathbf{E}[3]}$ the field of 3-division points of $\mathbf{E}$. In other words $L_{\mathbf{E}[3]}$ is the smallest field containing the x and y coordinates of all the P's in $\mathbf{E}[3]$. We know that $L_{\mathbf{E}[3]}$ is a finite extension of $\mathbf{Q}$ with the property that $\mathrm{Gal}(L_{\mathbf{E}[3]}/\mathbf{Q}) \leq \mathbf{GL}_2(\mathbf{F}_3)$ (see [Si] p.90). A P is in $\mathbf{E}[3]$ if and only if $2P = -P$. This will be more manageable since we have formulas to compute $2P$ and $-P$. Given $P = (x, y) \in \mathbf{E}$ we use the Duplication Formula ([Si] p.59) and we obtain that the x-coordinate of $2P$ is the following,

$$x[2P] = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. On the other hand $x[-P] = x$. Therefore if $P = (x_0, y_0) \in \mathbf{E}[3]$, x_0 must be a root of $F(x) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8$. We denote the splitting field of $F(x)$ by L. Let us look at the y-coordinate of a $P = (x_0, y_0) \in \mathbf{E}[3]$.

$$\begin{aligned} y[2P] &= -\left(\frac{3x_0^2 + 2a_2x_0 + a_4 - a_1y_0}{2y_0 + a_1x_0 + a_3} + a_1\right) x[2P] \\ &\quad -\left(\frac{-x_0^3 + a_4x_0 + 2a_6 - a_3y_0}{2y_0 + a_1x_0 + a_3}\right) - a_3 \quad ([\mathrm{Si}]p.59) \end{aligned}$$

On the other hand $y[-P] = -y_0 - a_1x_0 - a_3$. From this, one checks that y_0 is a root of an irreducible polynomial of degree two with coefficients in L. So we have that $L_{\mathbf{E}[3]}$ is a quadratic extension of L. From now on we will be working on the field L. By classical Galois theory we know that the Galois group of L over $\mathbf{Q}$ is a subgroup of $\mathbf{S}_4$, the permutation group of 4 elements, because $F(x)$ is a quartic polynomial

([Ga] part 14). In our study we will only consider the elliptic curves $\mathbf{E}$ such that $\mathrm{Gal}(L/\mathbf{Q}) = \mathbf{S}_4$. We remark that $\mathbf{S}_4 = \mathbf{PGL}_2(\mathbf{F}_3) = \overline{G}$; to see that consider the natural action of $\overline{G}$ on $\mathbf{P}_1(\mathbf{F}_3)$ via the Mobius transformations. Hence we have the desired L.

When we look carefully at $\overline{B}, \overline{N'}$ and $\overline{N}$ as subgroups of $\mathbf{S}_4$ we note that $\overline{B} = \mathbf{S}_3$, $\overline{N'} = \mathbf{D}_8$ the dihedral group of 8 elements generated by $\langle (1,2,3,4), (1,3)(2,4) \rangle$ and $\overline{N} = \{1, (1,2), (3,4), (1,2)(3,4)\}$ isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. The objective now is to find three irreducible polynomials $f(x), g(x)$ and $h(x)$ such that for any root α of $f(x)$ we have $\mathbf{Q}(\alpha) = L^{\overline{B}}$, for any root β of $g(x)$ we have $\mathbf{Q}(\beta) = L^{\overline{N'}}$ and for any root γ of $h(x)$ we have $\mathbf{Q}(\gamma) = L^{\overline{N}}$. The reason for this requirement is that GP-PARI (version 1.39.03) computes the Ideal Class Group of the number field $\mathbf{Q}(\alpha)$ where α is any root of an irreducible polynomial $f(x)$ entered by the user. By a simple substitution $F(x)$ is rewritten as $f(y) = y^4 + py^2 + qy + r$; $p, q, r \in \mathbf{Q}$ (namely you divide $F(x)$ by 3 and then you let $y = x + \frac{b_2}{12}$). The splitting field of $f(y)$ is isomorphic to the one of $F(x)$ so we keep the same notation for the field, namely L. Let $\alpha_1, \alpha_2, \alpha_3$ and α_4 be the roots of $f(y)$ then $\mathbf{Q}(\alpha_i) = L^{\overline{B}}$ because $\mathrm{Gal}(L/\mathbf{Q}(\alpha_i)) = \mathbf{S}_3$. Now if we define

$$\begin{aligned} \beta_1 &= -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ \beta_2 &= -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ \beta_3 &= -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3), \end{aligned}$$

then $\mathbf{Q}(\beta_i)$ is isomorphic to $L^{\overline{N'}}$ because $\mathrm{Gal}(L/\mathbf{Q}(\beta_i)) = \mathbf{D}_8$ the dihedral group of eight elements. After some calculation we get

$$\begin{aligned} \beta_1 + \beta_2 + \beta_3 &= -2p \\ \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 &= p^2 - 4r \\ \text{and} \quad \beta_1\beta_2\beta_3 &= q^2. \end{aligned}$$

This implies that our $g(x) = x^3 + 2px^2 + (p^2 - 4r)x - q^2$ is the *resolvent* for $f(x)$ ([Ga] part 14).

Finally, if we construct $h(x)$ by defining the following values

$$\begin{aligned}
\gamma_1 &= (\alpha_1+\alpha_2)-(\alpha_3+\alpha_4) = 2(\alpha_1+\alpha_2)\\
\gamma_2 &= 2(\alpha_1+\alpha_3)\\
\gamma_3 &= 2(\alpha_1+\alpha_4)\\
\gamma_4 &= -\gamma_1\\
\gamma_5 &= -\gamma_2\\
\gamma_6 &= -\gamma_3,
\end{aligned}$$

then $\mathbf{Q}(\gamma_i)$ is isomorphic to $L^{\overline{N}}$ because $\mathrm{Gal}(L/\mathbf{Q}(\gamma_i)) = \overline{N}$. We verify that

$$\begin{aligned}
\gamma_1^2+\gamma_2^2+\gamma_3^2 &= -8p\\
\gamma_1^2\gamma_2^2+\gamma_1^2\gamma_3^2+\gamma_2^2\gamma_3^2 &= 16(p^2-4r)\\
\gamma_1^2\gamma_2^2\gamma_3^2 &= 64q^2\ .
\end{aligned}$$

So when we consider

$\prod_{i=1}^{6}(x-\gamma_i) = x^6-(\gamma_1^2+\gamma_2^2+\gamma_3^2)x^4+(\gamma_1^2\gamma_2^2+\gamma_1^2\gamma_3^2+\gamma_2^2\gamma_3^3)x^2-\gamma_1^2\gamma_2^2\gamma_3^2$
we see that $h(x) = x^6+8x^4+16(p^2-4r)x^2-64q^2$.

We are ready to compute concrete examples. Given an elliptic curve $\mathbf{E}$ over $\mathbf{Q}$ picked in the tables of Cremona [Cr] we first make sure that the Galois group of the splitting field of $F(x)$ is $\mathbf{S}_4$ (using a function of GP-PARI). Then we construct $f(x), g(x), h(x)$. Lastly we feed in GP-PARI with these three polynomials and it gives us back the corresponding Ideal Class Group denoted respectively $Cl_{\mathbf{L}^{\overline{\mathbf{B}}}}$, $Cl_{\mathbf{L}^{\overline{\mathbf{N}'}}}$ and $Cl_{\mathbf{L}^{\overline{\mathbf{N}}}}$. A sample of the computations we obtained is reproduced below.

Table 10 *The Class Groups in function of the elliptic curve* $\mathbf{E}$

The elliptic curve $\mathbf{E}$	$Cl_{\mathbf{L}^{\overline{B}}}$	$Cl_{\mathbf{L}^{\overline{N'}}}$	$Cl_{\mathbf{L}^{\overline{N}}}$
$15A8$	1	2	2
$17A4$	1	1	1
$26B1$	1	3	3
$37A1$	1	3	3
$43A1$	1	12, [12]	6, [6]
$46A1$	1	2	1
$114C1$	1	6, [6]	3
$115A1$	1	1	1
$117A1$	1	6, [6]	3
$120A1$	1	3	3
$122A1$	1	12, [12]	6, [6]
$123A1$	1	4, [4]	2
$130B1$	2	6, [6]	6, [6]
$252B1$	1	6, [6]	3
$258G1$	2	12, [6, 2]	12, [6, 2]
$259A1$	1	3	3
$262B1$	1	30, [30]	15, [15]
$264A1$	1	6, [6]	6, [6]

For a given elliptic curve $\mathbf{E}$ taken from Cremona's table [Cr], you read in the above table the class number followed by a description of the class group as a direct sum of cyclic groups (in square brackets) for our three subfields of L. When we observe table 10 we remark that for all these elliptic curves $Cl^{(3)}_{L^{\overline{N}}} \simeq Cl^{(3)}_{L^{\overline{B}}} \oplus Cl^{(3)}_{L^{\overline{N'}}}$, while in general there is no isomorphism between the 2-part (even if they do not differ by much!). From this there is hope that only the prime 2 divides $\nu = \nu(\overline{G}, \overline{N}, \overline{B}, \overline{N'})$. Actually we know that 2 divides ν just by looking at table 10. We will now show that 3 does not divide ν by exhibiting a matrix $M \in \mathcal{M}$ such that 3 does not divide $|\det M|$.

5.2 Computation of ν

We now construct a general matrix $M \in \mathcal{M}$. Such a matrix must satisfy equation (4.2). To study the action of $\overline{G}$ on the couples (i,j), we first identify the coset representatives of $\overline{G}/\overline{N}$ by the elements of X (where X is defined in section 3.2), then those of $\overline{G}/\overline{N'}$ by the elements of X' (defined in section 3.4) and finally those of $\overline{G}/\overline{B}$ by the elements of $\mathbf{P}_1(\mathbf{F}_3)$. Denoting the elements of $\overline{G}$ by the numbers 1 to 24 and by letting $\overline{G}$ act on X, X' and $\mathbf{P}_1(\mathbf{F}_3)$ one shows without difficulty that M with integer coefficient satisfies equation (4.2) for all $g \in \overline{G}$ if an only if M has the following form

$$\begin{pmatrix} A & B & B & D & C & C & D \\ B & A & B & C & D & C & D \\ B & B & A & C & C & D & D \\ B & B & A & D & D & C & C \\ B & A & B & D & C & D & C \\ A & B & B & C & D & D & C \\ E & E & E & F & F & F & F \end{pmatrix} \tag{5.1}$$

where A, B, C, D, E, F are integers. When we specialized $A = D = F = 1$ and $B = C = E = 0$ we get a matrix with $|\det M| = 2^4$. Another specialization ($A = D = E = 1$ and $B = C = F = 0$) gives us a matrix M with $|\det M| = 24$. So the integer ν is a power of 2 and is equal to 2, 4 or 8. We now apply theorem 7 to obtain the following result.

Theorem 9 *For all prime ℓ different from 2 we have*

$$Cl_{L^{\overline{N}}}^{(\ell)} \simeq Cl_{L^{\overline{B}}}^{(\ell)} \oplus Cl_{L^{\overline{N'}}}^{(\ell)}$$

where L is any number field (normal extension) such that its Galois group is isomorphic to $\mathbf{S}_4$ $(= \overline{G})$.

This result tells us that in concrete examples it is possible to compute the ν of theorem 7 and obtain that ν has less prime divisors (only the prime 2) than the order of G (the primes 2 and 3). From the family of examples we studied we can

also believe that theorem 7 is optimal in the following sense: when 2 divided ν, we found specific elliptic curves (see table 10) where the 2-part of the class group equation was not satisfied. This may well be true in general.

To conclude let us say there is still much more to do with arithmetically equivalent algebras. First, by looking at table 10 we see that the 2-part of these class groups differ at most by a factor 2. There is certainly a way to bound the ratio h_2/h_2' in function of our integer ν. We can look at Perlis' work (in [Pe2]) for a similar problem and try to find an integer $i = i(\nu)$ such that $2^{-i} \leq h_2/h_2' \leq 2^i$. We would need to calculate ν explicitly in that case. Second, we would like to generalize theorem 9 for all normal extensions with Galois group $\mathbf{GL}_2(F_p)$ for any prime p. The method one should use is to exhibit a $\frac{p^2+p+2}{2} \times \frac{p^2+p+2}{2}$ matrix satisfying equation (4.2) such that its determinant has only a few prime factors. Let L be a Galois extension with Galois group $G = \mathbf{GL}_2(\mathbf{F}_p)$. Is it true that for primes $\ell \neq 2$ we have $Cl_{L^N}^{(\ell)} \simeq Cl_{L^B}^{(\ell)} \oplus Cl_{L^{N'}}^{(\ell)}$, and similarly for $G = \mathbf{PGL}_2(\mathbf{F}_p)$? Our hope is to answer this question by the affirmative.

Bibliography

[Cr] J.E. Cremona, "Algorithms for modular elliptic curves," Cambridge University Press, 1992.

[Fr-Ta] A.Frolich and M.J.Taylor, "Algebraic number theory", Cambridge University Press, 1991.

[Ga] D.J.H. Garling, "A course in galois theory," Cambridge University Press, 1986.

[Ga] F. Gassman, Bemerkungen zur vorstehenden Arbeit von Hurwitz, *Math. Z.* **25** (1926), 124-143.

[Ha] Marshall Hall, " The theory of groups", The Macmillan Company, New York, 1959.

[He] E. Hecke, "Vorlesungen uber die Theorie der Algebraischen Zahlen," Chelsea, New York, 1970.

[Ja] N. Jacobson, "Basic Algebra 1", 2nd edition, W.H. Freeman and Company, New York, 1985.

[Ma] Daniel A. Marcus, "Number fields," Springer-Verlag, New York, 1977.

[La1] Serge Lang, "Algebra," 3rd Ed, Addison-Wesley, 1984.

[La2] Serge Lang, "Complex analysis," 3rd Ed, Springer-Verlag, New York, 1993.

[Pe1] R.Perlis, On the equation $\zeta_{\mathbf{K}}(s) = \zeta_{\mathbf{K}'}(s)$, *J. Number Theory* **9** (1977), 342-360.

[Pe2] Robert Perlis, On the class numbers of arithmetically equivalent fields, *J. Number Theory* **10** (1978), 489-509.

[Pe3] Robert Perlis and Bart De Smit, Zeta Functions do not determine class numbers, *Bull. Amer. Math. Soc* **31** (1994), 213-215.

[Se1] Jean-Pierre Serre, Proprietes galoisiennes des points d'ordre fini des courbes elliptiques, *Inv. Math.* **15** (1972), 259-331.

[Se2] Jean-Pierre Serre, "Representations lineaires des groupes finis," 2nd Ed, Hermann, Paris, 1971.

[Si] Joseph H. Silverman, " The arithmetic of elliptic curved," Springer-Verlag, New York, 1986.

[Wa] C.D. Walter, Brauer's class number relation, *Acta A.* **35** (1979), 33-40.

150mm

6″

APPLIED IMAGE, Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989