Abelian l-Adic Representations

by

SIVA SANKAR C. NAIR

AN ESSAY SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN MATHEMATICS

Supervised by

PROF. SUJATHA RAMDORAI AND PROF. VINAYAK VATSAL

Department of Mathematics
University of British Columbia
Vancouver

August 2019

Contents

Acknowledgements

I would like to express my deep gratitude to my supervisors Professor Sujatha Ramdorai and Professor Vinayak Vatsal, for their valuable guidance and motivation throughout the program. I also thank the faculty and staff at the Department of Mathematics for the knowledge and insights that I have gained during the last two years as well as their support outside of academic life. Thanks are also due to my friends who have been a source of great moral support and comfort, especially during difficult times. My family has been a pillar of strength for me and I will always be grateful for their love and affection. Finally, I would like to thank MITACS for their financial support during my study at the University of British Columbia, Vancouver.

Introduction

The theory of l-adic representations is one that finds great importance in several famous results in Number Theory, including Wiles' proof of Fermat's Last Theorem. This essay is an exposition of the theory of Abelian l-adic representations of number fields, as laid out by Serre in [9]. The broad aim is to construct a system of Abelian l-adic representations and show that any Abelian l-adic representation that satisfies certain properties is obtained from this construction. We begin with a quick introduction to algebraic groups and their associated characters. This is followed by an overview of representations of algebraic groups and groups of multiplicative type, presenting key results that shall be called upon extensively in the following sections. We introduce the notion of an l-adic representation in chapter 2 and proceed to lay out a method to construct a certain family of Abelian l-adic representations. This construction is carried out first by defining the group $S_{\mathfrak{m}}$ over $\mathbb{Q}$ using algebraic tori and tools from class field theory. These groups $S_{\mathfrak{m}}$ are groups of multiplicative type and with the help of results described in the first chapter, we see that linear representations of $S_{\mathfrak{m}}$ lead to the required system of Abelian l-adic representations. In chapter 3, we investigate the condition that an Abelian l-adic representation should satisfy in order for it to arise via the groups $S_{\mathfrak{m}}$ as described above. The required condition is local algebraicity and is the subject matter of this chapter. We end with a short discussion of l-adic representations of elliptic curves and understand how these representations differ greatly in the two cases when the elliptic curve has complex multiplication (CM) and when it does not. In the CM case, the representation is always Abelian (in particular, it is not surjective) and can be obtained from one of the groups $S_{\mathfrak{m}}$, whereas in the non-CM case, it is almost always surjective.

1 Algebraic Groups

In this chapter, we will introduce the basic definitions of Algebraic Groups and other related topics that will turn out to be useful in subsequent chapters. We will follow the approach laid out by Milne in [6] in making these definitions. In particular, as we will be working with affine schemes over a field with characteristic zero, it is convenient to ignore non-closed points. Consequently, we will be concerned with maximal spectrums (Spm) rather than the spectrum of prime ideals of a ring (for a dictionary between Spm and Spec, refer to ([6], appendix A)). Throughout our discussions, if k is a field, then $\overline{k}$ denotes the algebraic closure of k. Again, since only fields with characteristic zero are considered, the separable closure of k, denoted k^{sep}, coincides with $\overline{k}$.

1.1 Definitions and Examples

Definition 1 (Algebraic Group)**.** An algebraic group G over a field k is an algebraic scheme over k along with

1. an element e in G, called the identity,
2. a morphism of algebraic schemes $m : G \times G \to G$ over k, called the multiplication map, and
3. a morphism of algebraic schemes $i : G \to G$ over k, called the inverse map,

which endow a group structure to G.

If G is an affine scheme i.e., it is isomorphic to $\text{Spm}(A)$ for a finitely-generated k-algebra A, then G is said to be an affine algebraic group. For such a group G, we say A is the *coordinate ring* of G, denoted by $k[G]$. Since we shall be exclusively dealing with affine algebraic groups in this essay, the following discussion shows how the structure of such an affine group G can be re-interpreted in terms of its coordinate ring A.[1]

[1] For more details, refer to (Borel [1], chap. 1, §5), or (Milne [6], chap. 3)

1. Corresponding to the identity element e of G, we have the evaluation at e homomorphism:
$$\begin{gathered}\epsilon : A \to k \\ \epsilon(f) = f(e).\end{gathered}$$

2. Note that $\mathrm{Spm}(A \otimes A) \cong \mathrm{Spm}(A) \times \mathrm{Spm}(A)$, and thus the morphism m gives rise to the k-algebra homomorphism $\Delta : A \to A \otimes A$. The map Δ is such that if $\Delta(f) = \sum g_i \otimes h_i$, then $f(xy) = \sum g_i(x)h_i(y)$, for $x, y \in G$ and $f, g_i, h_i \in A$.

3. Corresponding to the inverse morphism i, there is the k-homomorphism $i_0 : A \to A$, such that for all x in G and f in A, $i_0(f)(x) = f(x^{-1})$.

In order to translate the group axioms of G, we also introduce a homomorphism $p_0 : A \to A$ corresponding to the trivial morphism $p : G \to G$, where $p(x) = e$ for all x in G. Thus, $p_0(f)(x) = f(e)$ for all f in A. In other words, p_0 is simply the composite of ϵ with the inclusion of k into A. The group axioms defining G can now be translated in terms of the following diagrams being commutative[2]:

$$\begin{tikzcd}
A \arrow[r, "\mu_0"] \arrow[d, "\mu_0"] & A \otimes A \arrow[d, "\mu_0 \otimes \mathrm{Id}"] & A \arrow[r, "\Delta"] \arrow[d, "\Delta"] & A \otimes A \arrow[d, "(p_0{,}\mathrm{Id})"] & A \arrow[r, "\Delta"] \arrow[d, "\Delta"] \arrow[dr, "p_0"] & A \otimes A \arrow[d, "(i_0{,}\mathrm{Id})"] \\
A \otimes A \arrow[r, "\mathrm{Id} \otimes \mu_0"] & A \otimes A \otimes A & A \otimes A \arrow[r, "(\mathrm{Id}{,}p_0)"] & A \arrow[ul, "\mathrm{Id}"'] & A \otimes A \arrow[r, "(\mathrm{Id}{,}i_0)"] & A
\end{tikzcd} \tag{1}$$

Note that these three diagrams are obtained from the corresponding diagrams describing the associativity, the identity element and the existence of the inverse in G respectively.

Conversely, if A is a finitely generated k-algebra and the homomorphisms (Δ, ϵ, i_0) as before are such that the diagrams given above commute, then the affine scheme $G = \mathrm{Spm}(A)$ is an affine algebraic group with the multiplication map, the inverse map and the identity element obtained from this data. The k-algebra A forms what is called a Hopf algebra with Δ called the comultiplication map, ϵ the co-identity map and i_0 called the antipode.

[2] Here the following notation is used: if $f, g : A \to A$ are two k-algebra homomorphisms, then (f, g) denotes the homomorphism from $A \otimes A \to A$ defined by $a \otimes b \mapsto f(a)g(b)$

Example 1.1 (Additive Group)*.* If $k[X]$ is the polynomial ring in the variable X, then the k-variety $\mathbb{G}_a = \operatorname{Spm} k[X]$ is an algebraic group called the Additive Group. Here, $\Delta(X) = X \otimes 1 + 1 \otimes X$ and $i_0(X) = -X$ and $\epsilon(X) = 0$.

Example 1.2 (General Linear Group)*.* The affine variety

$$\mathrm{GL}_n = \operatorname{Spm} k[X_{11}, X_{12}, \ldots, X_{nn}, \det(X_{ij})^{-1}]$$

is another affine algebraic group called the general linear group. In this case, we have $\epsilon(X_{ij}) = \delta_{ij}$, $\Delta(X_{ij}) = \sum_{1 \leq k \leq n} X_{ik} \otimes X_{kj}$, and $i_0(X_{ij}) = (-1)^{i+j}(\det(X_{ij})^{-1})M_{ij}$, where M_{ij} denotes the determinant of the matrix obtained from (X_{ij}) by removing the j^{th} row and i^{th} column. Similary the affine variety SL_n is also an affine group.

Example 1.3 (Multiplicative Group)*.* The affine group GL_1, often denoted $\mathbb{G}_m$, is of fundamental importance in our discussion of algebraic tori and is called the Multiplicative Group. It is the max-spectrum of the ring $k[X, X^{-1}]$.

Example 1.4 (Roots of Unity)*.* For an integer $n \geq 1$, we have the following affine group $\mu_n = \operatorname{Spm}(k[T]/(T^n - 1))$, which has its comultiplication map induced from that of $\mathbb{G}_m$.

Definition 2 (Homomorphisms)**.** A Homomorphism of k-algebraic groups is a morphism of schemes over k that is also a homomorphism of groups. Again, only affine groups are considered in this discussion and describing a homomorphism $\alpha : G \to H$ between affine groups is equivalent to giving a homomorphism of k-algebras $\alpha^* : k[H] \to k[G]$ such that the following diagram commutes:

$$\begin{tikzcd}
k[H] \arrow[r, "\alpha^*"] \arrow[d, "\Delta_H"] & k[G] \arrow[d, "\Delta_G"] \\
k[H] \otimes_k k[H] \arrow[r, "\alpha^* \otimes \alpha^*"] & k[G] \otimes_k k[G].
\end{tikzcd} \tag{2}$$

Let $G = \operatorname{Spm}(A)$ be an affine algebraic group over k with coordinate ring A. For a k-algebra R, we denote $G(R)$ to be the set of points in G with coordinates in R i.e.,

$$G(R) \overset{\text{def}}{=} \operatorname{Hom}_{k-\text{alg}}(A, R).$$

1.2 Weil Restriction of Scalars

We discuss the Weil Restriction of Scalars for affine varieties. For a more general construction, see for instance (A. Weil [11], §1.3). Let k be a number field and K, a finite extension of k of degree d. Let V be an affine variety over K with $V = \operatorname{Spm} K[t_1, \dots, t_n]/(f_1, \dots, f_m)$. Choose a basis $\{e_1, \dots, e_d\}$ of K over k. For $1 \leq i \leq n$ and $1 \leq j \leq d$ introduce new variables y_{ij} and write $x_i = y_{i1}e_1 + \cdots + y_{id}e_d$. Substituting these expressions into each of the polynomials f_r, we obtain, for $1 \leq r \leq m$,

$$f_r(x_1, \dots, x_n) = p_{r,1}e_1 + \cdots + p_{r,d}e_d,$$

where $p_{r,s}$ are polynomials in the variables y_{ij} with coefficients in k. Then, the Weil restriction of V from K to k is defined as the k-variety $\operatorname{Res}_{K/k}(V) = \operatorname{Spm} k[\{y_ij\}]/(\{p_{r,s}\})$.
There is a natural morphism $p : \operatorname{Res}_{K/k}(V) \to V$ defined over K and the pair $(\operatorname{Res}_{K/k}(V), p)$ satisfy the following universal property:

> Let X be a variety defined over k and let $f : X \to V$ be a morphism defined over K. Then there is a unique $\phi : X \to \operatorname{Res}_{K/k}(V)$ defined over k, such that $f = p \circ \phi$.

1.3 The Character Group

Definition 3 (Character of an Algebraic Group)**.** A character of an algebraic k-group G is a homomorphism $\chi : G \to \mathbb{G}_m$ of algebraic groups over k.

Note that the set of all characters of G, denoted $X(G)$, forms an abelian group under point-wise multiplication: $(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g)$. We say $X(G)$ is the Group of Rational Characters of G.

Let G be an affine algebraic group over k and $k[G] = A$. Recall that giving a homomorphism of affine algebraic groups is equivalent to giving a homomorphism between their coordinate rings. Since $k[\mathbb{G}_m] = k[t, t^{-1}]$ and $\Delta_{\mathbb{G}_m}(t) = t \otimes t$, this means that a character χ of G corresponds to a homomorphism $\chi^* : k[t, t^{-1}] \to A$ that makes diagram (2) commutative. Such a homomorphism is determined by the image of the indeterminate t, which must be mapped to a unit in A. Thus, every such homomorphism corresponds to a unit $\alpha_\chi = \chi^*(t)$ in A that satisfies $\Delta_G(\alpha_\chi) = \alpha_\chi \otimes \alpha_\chi$. Such elements α in $A = k[G]$ that are invertible and satisfy $\Delta_G(\alpha) = \alpha \otimes \alpha$ are called group-like elements of $k[G]$. In conclusion, there is a one-to-one correspondence between the characters of G and the group-like elements in $k[G]$.

Example 1.5. When $G = \mathbb{G}_m$, then any homomorphism $\chi : \mathbb{G}_m \to \mathbb{G}_m$ must be of the form $t \mapsto t^n$ for an integer n, and hence $X(\mathbb{G}_m) \cong \mathbb{Z}$.

1.4 Algebraic Tori

We will now study a fundamental class of algebraic groups known as *algebraic tori*, that find great importance in number theory.

Definition 4 (Split Torus)**.** An algebraic group G over k is said to be a split k-torus if it is isomorphic to a finite product of copies of $\mathbb{G}_m$ over k.

Definition 5 (Torus)**.** An algebraic group G over k is a torus if $G_{k^{sep}}$, obtained by extending scalars from k to its separable closure k^{sep}, is a split k^{sep}-torus. For such a torus G, with $G_{k^{sep}} \cong \prod_{i=1}^{d} \mathbb{G}_m$, we say d is the dimension of G.

It is well known that a torus T actually splits not just over k^{sep}, but over a unique minimal finite extension L of k called the splitting field of T, i.e., T_L is a split L-torus.

Remark. Let k' be a finite separable field extension of k and let G be a k'-group. Now let K be a field containing the Galois closure of k' and let Σ denote the set of k-embeddings from k' to K. Clearly, $|\Sigma| = [k' : k]$. We first restrict G by scalars to k and then extend by K to obtain

$$(\mathrm{Res}_{k'/k} G)_K \cong \prod_{\alpha \in \Sigma} G_\alpha, \tag{3}$$

where G_α is the affine K-group obtained from G by extension of scalars from k' to K and K is considered to be a k'-algebra with respect to the homomorphism α.

Example 1.6. We present an example that will be studied in greater detail in the coming sections. Let K be a number field and let $T = \mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$ be the algebraic group over $\mathbb{Q}$ obtained by restriction of scalars. Now $\mathbb{Q}^{sep} = \overline{\mathbb{Q}}$. Then by (3),

$$T_{\mathbb{Q}^{sep}} = T_{\overline{\mathbb{Q}}} \cong \prod_{\alpha : K \hookrightarrow \overline{\mathbb{Q}}} (\mathbb{G}_m)_\alpha = \prod_{\alpha : K \hookrightarrow \overline{\mathbb{Q}}} \mathbb{G}_{m/\overline{\mathbb{Q}}}, \tag{4}$$

where $\mathbb{G}_{m/\overline{\mathbb{Q}}}$ is just the multiplicative group over $\overline{\mathbb{Q}}$. Thus T is a $\mathbb{Q}$-torus.

1.4.1 The Character Group of a Torus

Recall that the group of rational characters on the k-group G is the set

$$X(G) = \mathrm{Mor}_k(G, \mathbb{G}_m),$$

which turned out to be an Abelian group. Following along the lines of example 1.5, if T is the split k-torus $\prod_{i=1}^{d} \mathbb{G}_{m/K}$ of dimension d, then any character of T is of the form $(t_1, \ldots, t_d) \mapsto t_1^{n_1} \cdots t_d^{n_d}$, and hence $X(G) \cong \mathbb{Z}^d$. Thus if T is a k-torus of dimension d, then $X(T_{k^{sep}}) \cong \mathbb{Z}^d$. Thus a d-dimensional torus gives rise to a finitely generated free abelian group of rank d. This character group will be studied in greater detail in later sections.

1.5 A Specific Example Relating to Number Theory

We shall now resume our discussion from Example 2.1. Recall that $T = \mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$ turned out to be a $\mathbb{Q}$-torus of dimension d for a number field K with degree d over $\mathbb{Q}$. Thus $X(T_{\overline{\mathbb{Q}}}) \cong \mathbb{Z}^d$. Let us examine this group in a little more detail. Let $\Sigma = \mathrm{Hom}(K, \overline{\mathbb{Q}})$ denote the set of d distinct embeddings of K into $\overline{\mathbb{Q}}$, and let $\sigma \in \Sigma$. Then σ can be extended to a homomorphism of $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ to $\overline{\mathbb{Q}}$, by taking $x \otimes y$ to $\sigma(x) \cdot y$, for x in K and y in $\overline{\mathbb{Q}}$. This gives a morphism of $\overline{\mathbb{Q}}$-groups

$$\widehat{\sigma} : T_{\overline{\mathbb{Q}}} \to \mathbb{G}_{m/\overline{\mathbb{Q}}},$$

and hence a character of $T_{\overline{\mathbb{Q}}}$. In fact, the collection of all $\widehat{\sigma}$'s forms a basis for the character group $X(T_{\overline{\mathbb{Q}}})$. In addition, $X(T_{\overline{\mathbb{Q}}})$ also admits an action by the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ via permutation of the $\widehat{\sigma}$'s. Any character χ in $X(T_{\overline{\mathbb{Q}}})$ would thus look like

$$\prod_{\sigma \in \Sigma} (\widehat{\sigma})^{n_\sigma},$$

where n_σ are integers.

Let E be a subgroup of the group of $\mathbb{Q}$-rational points on T. Then the Zariski closure of E in T, say $\overline{E}$, is an algebraic subgroup of T. Consider the quotient group $T/\overline{E}$, which we denote by T_E. T_E is a $\mathbb{Q}$-torus. Let X_E denote its character group $X(T_E)$. Then X_E is the subgroup of $X(T)$ consisting of those characters that are trivial on E, i.e.

$$X_E = \left\{ \prod_{\sigma \in \Sigma} (\widehat{\sigma})^{n_\sigma} \in X(T) : \prod_{\sigma \in \Sigma} \sigma(x)^{n_\sigma} = 1 \ \text{ for all } x \in E \right\}.$$

We will make use of the above observations to work out the dimension of the torus T_E in the following example.

Example 1.7. Let K be a quadratic extension of $\mathbb{Q}$ and let E be the group of units in the ring of integers of K, a subgroup of $T(\mathbb{Q}) = K^*$. The group E is finite if K is imaginary and has rank 1 if it is a real extension. When E is finite, then it is already Zariski-closed, and hence $\overline{E}$ is finite. T_E is then a quotient of a torus by a finite group and hence is still a torus of the same dimension.

Consider the case when K is real. Recall that the rank of the character group of a torus is the same as the dimension of the torus. Let us try computing the former. The group X_E consists of all characters $\chi = \prod_{\sigma\in\Sigma}(\widehat{\sigma})^{n_\sigma}$ such that $\prod_{\sigma\in\Sigma}\sigma(x)^{n_\sigma} = 1$ for all x in E. Since E is the group of units, the norm $N_{K/\mathbb{Q}}(x) = \prod_{\sigma\in\Sigma}\sigma(x) = 1$. K is a real quadratic extension and hence Σ has two elements the identity and the non-trivial embedding, say σ. Thus, for all x in E, $x \cdot \sigma(x) = 1$. We now determine all the possibilities of the integers n_σ, which would give us the rank of X_E. For ease of notation, denote these integers as n_1 and n_2 corresponding to the identity and the embedding σ respectively. Now $x^{n_1} \cdot \sigma(x)^{n_2}$ must be equal to 1, but $x \cdot \sigma(x) = 1$. This implies that we actually just need $\sigma(x)^{n_2-n_1} = 1$. If $n_1 \neq n_2$ this is equivalent to saying that $\sigma(x)$ must be a root of unity for all x in E. But K is real and hence E is infinite and cannot consist only of roots of unity. Thus n_1 must equal n_2. This means that the rank of X_E, and hence the dimension of T_E, must be 1.

1.6 Characters Revisited

In the following sections, we shall go through some more properties of the character group and present some elementary facts about representations of affine algebraic groups. We will restrict our attention to algebraic groups defined over number fields in this discussion.

Let H be an affine commutative algebraic group over a number field K. Recall that $X(H_{\overline{K}})$ denotes the group of characters of the algebraic group $H_{\overline{K}}$ over the algebraic closure $\overline{K}$ i.e.

$$X(H_{\overline{K}}) = \mathrm{Mor}_{\overline{K}}(H_{\overline{K}}, \mathbb{G}_m).$$

Then the Galois group $G = \mathrm{Gal}(\overline{K}/K)$ acts on $X(H_{\overline{K}})$ as follows:

For $\sigma \in G$, σ acts on $H_{\overline{K}}$ via its action on the coordinates and let $\sigma_{H_{\overline{K}}}$ denote the automorphism of $H_{\overline{K}}$ defined by this action. Then the action of G on $X(H_{\overline{K}})$ is defined by

$$\sigma \cdot \chi = \sigma_{\mathbb{G}_m} \circ \chi \circ \left(\sigma_{H_{\overline{K}}}\right)^{-1},$$

for any $\chi \in X(H_{\overline{K}})$.

Note that $\sigma \cdot \chi = \chi$ if and only if χ is defined over K. Now, if $\overline{K}[X(H_{\overline{K}})]$ denotes the group algebra of $X(H_{\overline{K}})$ over $\overline{K}$, we can define a G-action on it as

$$\sigma \cdot \left(\sum a_\chi \chi\right) = \sum \sigma(a_\chi)(\sigma \cdot \chi),$$

for any $\sum a_\chi \chi \in \overline{K}[X(H_{\overline{K}})]$.

If $H = \mathrm{Spm}(A)$, where A is the coordinate ring of H, then the coordinate ring of $H_{\overline{K}}$ is $\overline{A} = A \otimes \overline{K}$. Recall from our previous discussion on characters of affine algebraic groups (§1.3) that each $\chi : H_{\overline{K}} \to \mathbb{G}_m$ in $X(H_{\overline{K}})$ corresponds to a group-like element α_χ in $\overline{A}$. This gives a map $\alpha : X(H_{\overline{K}}) \to \overline{A}$ defined by $\alpha(\chi) = \alpha_\chi$, which can be extended by linearity to obtain a homomorphism from the group algebra $\overline{K}[X(H_{\overline{K}})]$ to $\overline{A}$:

$$\alpha : \overline{K}[X(H_{\overline{K}})] \longrightarrow \overline{A}.$$

This is actually a G-homomorphism for the action of G on $\overline{K}[X(H_{\overline{K}})]$ defined above.

Proposition 1. *The homomorphism α is injective.*

Proof. Let $\sum a_\chi \chi \in \overline{K}[X(H_{\overline{K}})]$ lie in the kernel of α. It follows that

$$\begin{gathered} \alpha(\sum a_\chi \chi) = 0 \\ \Longrightarrow \sum a_\chi \alpha(\chi) = 0. \end{gathered}$$

The following lemma is needed to complete the proof.

Lemma 2. *Let A be a Hopf Algebra over a field k. Then the set of group-like elements in A are linearly independent.*

Proof. (of Lemma)
We begin with the following observation. If f is a group-like element of A

i.e., a unit in A that satisfies $\Delta(f) = f \otimes f$, then from the commutativity of diagram (1), $f = ((\epsilon, \mathrm{Id_A}) \circ \Delta)(f)$. But since f is group-like, $((\epsilon, \mathrm{Id_A}) \circ \Delta)(f) = (\epsilon, \mathrm{Id_A})(f \otimes f) = f\epsilon(f)$. Thus $\epsilon(f) = 1$ for all group-like elements f in A.

Assume that the set of group-like elements is not linearly independent. Let $n \geq 1$ be the greatest integer such that there exists a set $\{f_1, \ldots, f_n\}$ of group-like elements in A that are linearly independent. Then, by assumption, there exists f in A which is group-like, $f \neq f_i$ for any i and satisfies the following relation

$$f = \sum_{i=1}^{n} a_i f_i, \quad a_i \in k.$$

As $f \neq 0$, $a_t \neq 0$ for some $1 \leq t \leq n$. The following equations hold:

$$\Delta(f) = f \otimes f = \sum_{1 \leq i,j \leq n} a_i a_j (f_i \otimes f_j),$$
$$\Delta(f) = \sum_{i=1}^{n} a_i \Delta(f_i) = \sum_{i=1}^{n} a_i (f_i \otimes f_i).$$

Since the elements $\{f_i \otimes f_j\}_{1 \leq i,j \leq n}$ are also linearly independent, comparing the above equations implies that $a_i a_j = 0$ for all $i \neq j$, and $a_i^2 = a_i$ for all i. Recall that $a_t \neq 0$, which means $a_i = 0$ for all $i \neq t$, and that $a_t^2 = a_t$, implying $a_t = 1$. But this means $f = f_t$, a contradiction to our choice of f. Thus, all group-like elements in A are linearly independent. [3] □

Coming back to the proof of the proposition, since $\alpha(\chi)$ is group-like for each χ, $\sum a_\chi \alpha(\chi) = 0$ would mean each $a_\chi = 0$ using the above lemma. Thus $\sum a_\chi \chi = 0$, implying that α is injective. □

Thus, the proposition tells us that we may view $\overline{K}[X(H_{\overline{K}})]$ as a subalgebra of $\overline{A} = A \otimes \overline{K}$.

1.7 Linear Representations of Algebraic Groups

Let G be an affine algebraic group over a field k, and A be its coordinate ring. Let V be a finite-dimensional vector space over k, and let $n = \dim_k(V)$.

[3] Using the correspondence of characters of H and the group-like elements of A, a corollary to this lemma would be that the characters are linearly independent as functions from $H \to \mathbb{A}^1$. This is a well-known result due to Artin.

Then by GL_V, we mean the affine k-algebraic group GL_n for a fixed basis of V over k.

Definition 6 (Linear Representation)**.** A homomorphism of k-algebraic groups $\phi : G \to \mathrm{GL}_V$ is said to be a linear representation of G into V, denoted by (ϕ, V).

If W is a subspace of V that is stable under G, i.e., $\rho(g)(W) \subset W$ for all $g \in G$, then the homomorphism $\rho^W : G \to \mathrm{GL}_W$, obtained by restricting $\rho(g)$ to W, is called a subrepresentation of G. For simplicity, we say V is a representation of G and W is a subrepresentation of V.

Definition 7 (Simple and semi-simple Representations)**.** A non-zero representation V of G is said to be simple if the only subrepresentations of V are $\{0\}$ and itself. It is called semi-simple if it can be expressed as the direct sum of simple representations.

Example 1.8. For a group G, any character $\chi \in X(G)$ is a one-dimensional representation of G, and since such representations cannot contain any non-trivial subrepresentations, they are also simple. We will later see that for a certain class of algebraic groups called *diagonalizable* groups, the set of characters are the only simple representations.

1.8 Diagonalizable Groups

Let M be a finitely generated Abelian abstract group and let $k[M]$ be the group algebra of M over k. Since M is finitely generated as an Abelian group, $k[M]$ is also finitely generated as an algebra over k, using the same generators. We can define a Hopf algebra structure on $k[M]$ by defining the co-multiplication, co-identity and antipode maps as follows:

$$\Delta(m) = m \otimes m, \quad \epsilon(m) = 1, \quad i_0(m) = m^{-1},$$

for all $m \in M$. Hence, denote by $D(M)$, the affine algebraic group $\mathrm{Spm}(k[M])$.

Example 1.9. 1. If $M = \mathbb{Z}$, then $D(M) \cong \mathbb{G}_m$.

2. If $M = \mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$, then $D(M) \cong \mu_n$.

Note that for two such Abelian groups M_1 and M_2, there is a natural k-algebra isomorphism $k[M_1 \times M_2] \simeq k[M_1] \otimes k[M_2]$ which preserves the respective Hopf algebra structures. It follows that if

$$M \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_t\mathbb{Z}),$$

for a fixed basis of M as a $\mathbb{Z}$-module, then

$$D(M) \cong \mathbb{G}_m \times \cdots \times \mathbb{G}_m \times \mu_{n_1} \times \cdots \times \mu_{n_t}.$$

In addition, if $f \in k[M]$ is a group-like element, then $f = \sum a_i m_i$ for some $a_i \in k$ and $m_i \in M$. Following the proof of lemma (2), this means $f = m_i$ for some i, which implies that the group-like elements of $k[M]$ are precisely the elements in M. It follows that the character group $X(D(M))$ is isomorphic to M. We will now define what it means for a group to be diagonalizable and see how they are related to the groups $D(M)$.

Definition 8 (Diagonalizable Groups)**.** An algebraic group G over k is said to be diagonalizable if the group-like elements in $A = k[G]$ span it as a k-vector space.

From the previous discussion, it follows that all algebraic groups $D(M)$ are diagonalizable. Now, given a diagonalizable group G, let M be the group like elements in $k[G]$. From lemma (2), M is a linearly independent set. These two facts together imply that $k[M]$ is isomorphic to $k[G]$ and since the co-multiplication, co-identity and antipode maps are defined on each $m \in M$ and extended k-linearly on $k[M]$ and $k[G]$ respectively, this isomorphism respects the Hopf algebra structures. Thus $D(M) \cong G$, giving us the following theorem:

Theorem 3. *An algebraic group is diagonalizable if and only if it is isomorphic to $D(M)$ for some finitely generated Abelian (abstract) group M.*

The theorem below is also true, the proof for which has been omitted and can be found in ([6], chap. 12 , theorem 12.9):

Theorem 4. *The functor from the category of finitely generated Abelian groups to the category of diagonalizable algebraic groups, sending M to $D(M)$, is a contravariant equivalence. The quasi-inverse is given by the functor sending the diagonalizable group G to its character group $X(G)$. Moreover, both these functors are exact.*

Now, for $n \geq 1$, let $\mathbb{D}_n$ denote the affine k-group

$$\mathrm{Spm}(k[T_1, \ldots, T_n, T_1^{-1}, \ldots, T_n^{-1}]) \cong D(\mathbb{Z}^n) \cong \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{n \text{ times}}.$$

It is the group of invertible diagonal $n \times n$ matrices, and hence a subgroup of GL_n. Note that any torus T becomes isomorphic to $\mathbb{D}_n$ over the separable closure of k.

Definition 9. A finite-dimensional representation $\phi : G \to \mathrm{GL}_n$ of G is said to be diagonalizable if the image $\phi(G) \subseteq \mathbb{D}_n$, or equivalently, the representation is a direct sum of one-dimensional subrepresentations.

It is known ([6], chap. 12, theorem 12.12) that an algebraic group G is diagonalizable if and only if every representation of G is diagonalizable. Moreover, the one-dimensional representations of G are precisely the characters of G. Thus, every representation of a diagonalizable group is semi-simple, with the characters forming the simple objects.

1.9 Groups of Multiplicative Type

Definition 10. An algebraic group H over k is said to be a group of multiplicative type if it becomes diagonalizable over some extension of k.

An immediate example would be any torus over k, as it becomes diagonalizable over k^{sep}.

It can be shown that any group of multiplicative type, in fact, becomes diagonalizable over a finite separable extension of k, which makes such groups susceptible to Galois theory. This is particularly useful in drawing an equivalence between these groups and a certain class of finitely generated $\mathbb{Z}$-modules as we shall see below.

Let $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$, equipped with the Krull topology, M be a finitely generated Abelian group, and suppose Γ acts on M. Recall from ([2], chap. V, §2.3) that M is said to be a *discrete* Γ-module if this action is continuous for the discrete topology on M. Equivalently, M is a discrete Γ-module if the stabilizer in Γ of every element of M is an open subgroup of Γ.

Let H be an algebraic group over k and let $X^*(H)$ be the character group of $H_{k^{\mathrm{sep}}}$. We have seen in §1.6 that the Galois group Γ acts on $X^*(H)$. Also recall that $X^*(H)^\Gamma$, the subgroup fixed by Γ, is precisely $X(G)$. Every character $\chi : H_{k^{\mathrm{sep}}} \to \mathbb{G}_{m,k^{\mathrm{sep}}}$ defined over k^{sep} is in fact defined over a finite separable extension E of k, and is thus stabilized by the open subgroup $\mathrm{Gal}(k^{\mathrm{sep}}/E)$. We conclude that Γ acts continuously on $X^*(H)$, giving us a contravariant functor X^*, from algebraic groups over k to finitely generated Abelian groups equipped with a continuous action of Γ.

On the other hand, let M be a finitely generated Abelian group equipped with a continuous action of Γ. Let $D(M_0)$ denote the diagonalizable group over k^{sep} obtained from the construction in the previous section. Then the coordinate ring of $D(M_0)$ is $k^{\mathrm{sep}}[M]$ and the character group $X(D(M_0)) = M$. Now let $D'(M)$ denote the algebraic group defined over k that has coordinate ring $(k^{\mathrm{sep}}[M])^{\Gamma} = k[M^{\Gamma}]$. Using the isomorphism[4]

$$k^{\mathrm{sep}} \otimes k[M^{\Gamma}] \cong k^{\mathrm{sep}}[M],$$

it follows that on extending scalars from k to k^{sep} we get $D'(M)_{k^{\mathrm{sep}}} \cong D(M_0)$, since their coordinate rings are isomorphic. This implies that $D'(M)$ is a group of multiplicative type and the character group $X^*(D'(M)) = X(D'(M)_{k^{\mathrm{sep}}}) = M$. The functor $M \rightsquigarrow D'(M)$ is thus a contravariant functor from finitely generated Abelian groups with a continuous action of Γ, to groups of multiplicative type over k.

Theorem 5. *The functor X^* is an equivalence between the category of groups of multiplicative type over k and the category of finitely generated Abelian groups with a continuous action of Γ, with quasi-inverse given by the functor D'. Both these functors are exact.*

Remark. Tori are those groups of multiplicative type for which $X^*(T)$ is torsion-free.

Representations of Groups of Multiplicative Type

Let H be a k-algebraic group with coordinate ring $k[H] = A$, and let $\mathrm{Rep}_k(H)$ denote the set of isomorphism classes of linear representations of H over k. If H is diagonalizable, then every representation of H is semi-simple, i.e. $\mathrm{Rep}_k(H)$ is a semi-simple category with the characters in $X(H)$ being the simple objects. When H is a group of multiplicative type, the following proposition will show that in this case too, $\mathrm{Rep}_k(H)$ is a semi-simple category, however the simple objects are classified by the orbits of $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ acting on $X^*(H)$.

[4] Refer to proposition 16.15, chapter 16, in Milne's course notes on Algebraic Geometry `https://www.jmilne.org/math/CourseNotes/AG16.pdf`.

Let $\phi : H \to \mathrm{GL}_V$ be a linear representation of H into a finite-dimensional k-vector space V. Since H is of multplicative type, when considered over k^{sep}, it becomes diagonalizable, and hence ϕ decomposes into sums of characters from $X^*(H)$ over k^{sep}. Let $n_\chi(\phi)$ denote the multiplicity of $\chi \in X^*(H)$ in the decomposition of ϕ over k^{sep}.

Definition 11 (Trace)**.** The trace of ϕ is the element $\theta_\phi = \sum_\chi n_\chi(\phi)\chi$ in $\mathbb{Z}[X^*(H)]$.

Note that if R is an Abelian k-algebra, and $h \in H(R)$, then $\theta_\phi(h)$ is the trace of the matrix $\phi(h) \in \mathrm{GL}_V(R)$. Also, from proposition (1) in §1.6, $k^{\mathrm{sep}}[X^*(H)]$ can be embedded into $A \otimes k^{\mathrm{sep}}$, and in particular, $\theta_\phi \in A \otimes k^{\mathrm{sep}}$.

Proposition 6. *The map $\phi \to \theta_\phi$ is a bijection between $\mathrm{Rep}_k(H)$ and the set of elements $\theta = \sum_\chi n_\chi \chi \in \mathbb{Z}[X^*(H)]$ where $n_\chi \geq 0$ and $n_\chi = n_{\sigma\cdot\chi}$ for all $\sigma \in \Gamma$ and $\chi \in X^*(H)$.*

Proof. We prove surjectivity first. Let χ be a character in $X^*(H)$ and let Γ_χ be the stabilizer of χ. Since $X^*(H)$ is a discrete Γ-module, Γ_χ is an open subgroup, and hence has finite index (as Γ is compact). Thus, χ has finitely many conjugates under the action of Γ, one corresponding to each element in the orbit O_χ of χ. Moreover, there is a bijection between O_χ and Γ/Γ_χ. Let $\{\chi_1 = \chi, \chi_2, \dots, \chi_r\} = \{\sigma \cdot \chi : \quad \overline{\sigma} \in \Gamma/\Gamma_\chi\}$ be the set of distinct conjugates of χ, and let

$$\theta = \sum_{i=1}^{r} \chi_i. \tag{5}$$

If k_χ denotes the fixed field of Γ_χ, then it is a finite extension of k with degree equal to the index $[\Gamma : \Gamma_\chi]$. In addition, it is the smallest subfield of k^{sep}, such that χ is defined over k_χ, or equivalently, the smallest subfield such that $\chi \in A \otimes k_\chi$[5]. Thus, $\chi : H_{k_\chi} \to \mathbb{G}_{m,k_\chi}$ is a character and a one-dimensional representation of H_{k_χ}. By restriction of scalars to k, we obtain a representation, say ϕ, of H with degree $[k_\chi : k]$. Note that the trace θ_ϕ of ϕ, would then be equal to θ, showing that θ has a pre-image under the given map. Now, any θ satisfying the conditions of the proposition is a sum of elements of the form 5, and hence has a pre-image, giving us the surjectivity of the map.

Injectivity of the map follows from the following lemma:

[5] Here we are using the fact that $X^*(H)$ embeds into the coordinate ring $A^{\mathrm{sep}} = A \otimes k^{\mathrm{sep}}$ of $H_{k^{\mathrm{sep}}}$ as a result of proposition (1).

Lemma 7 (Bourbaki, Corollary 3.8, Chapter XVII, [4])**.** *Let k be a field of characteristic 0, R be a k-algebra, and E, F be semi-simple R-modules, with finite dimensions over k. For each $\alpha \in R$, let α_E and α_F, denote the corresponding k-endomorphisms on E and F respectively. If the traces $\mathrm{Tr}(\alpha_E)$ and $\mathrm{Tr}(\alpha_F)$ are equal for all $\alpha \in R$, then E and F are isomorphic as R-modules.*

If (ϕ_1, V_1) and (ϕ_2, V_2) are elements in $\mathrm{Rep}(k)$, such that their traces are equal, $\theta_{\phi_1} = \theta_{\phi_2}$, then the above lemma with $R = k[H], E = V_1$ and $F = V_2$ implies that $V_1 \cong V_2$, and hence the required injectivity follows. □

Note that if E is an extension of k and $\phi \in \mathrm{Rep}_k(H)$, then by extension of scalars from k to E we obtain a representation in $\mathrm{Rep}_E(H_E)$. This gives an embedding of $\mathrm{Rep}_k(H)$ into $\mathrm{Rep}_E(H_E)$.

Definition 12. Linear representations of an algebraic group over E are said to be defined over k if they fall under the image of the embedding $\mathrm{Rep}_k(H) \hookrightarrow \mathrm{Rep}_E(H_E)$.

With this embedding in mind, the following corollary is immediate from the above proposition:

Corollary 8. *Suppose $\psi \in \mathrm{Rep}_E(H_E)$. Then ψ can be defined over k if and only if θ_ψ, which is naturally an element of $A \otimes_k E$, in fact belongs to A.*

2 Construction of Abelian l-adic Representations

Let K be a number field and $G = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ denote the absolute Galois group of K. For a prime l, let V be a finite-dimensional vector space over $\mathbb{Q}_l$ with dimension n. We endow $\mathrm{End}(V) \simeq \mathrm{M}_n(\mathbb{Q}_l)$ with the topology induced from $\mathbb{Q}_l$. Then $\mathrm{Aut}(V) \cong \mathrm{GL}_n(\mathbb{Q}_l)$ and it is an l-adic Lie group with topology induced from that of $\mathrm{End}(V)$.

Definition 13 (l-adic Representation)**.** Consider the Krull topology on the group G. A continuous homomorphism $\rho : G \to \mathrm{Aut}(V)$ is called an l-adic representation of G (or of K).

Example 2.1 (Roots of Unity). Let μ_{l^m} denote the group of $(l^m)^{\text{th}}$ roots of unity in $\overline{\mathbb{Q}}$. Then, G acts continuously on the finite groups μ_{l^m} for all m. Moreover, the sets μ_{l^m} form an inverse system under the exponentiation by l map, and the action of G commutes with these exponentiation maps. Thus, if we let $T_l(\mu)$ denote the inverse limit $\varprojlim_m \mu_{l^m}$ then G acts continuously on $T_l(\mu)$. Since $\mu_{l^m} \cong \mathbb{Z}/l^m\mathbb{Z}$, $T_l(\mu)$ is a free $\mathbb{Z}_l$-module of rank 1. Let $V_l(\mu)$ denote the one-dimensional $\mathbb{Q}_l$-vector space $T_l(\mu) \otimes \mathbb{Q}_l$ with G-action induced by the action on $T_l(\mu)$. Then

$$\chi_l : G \to \mathrm{Aut}(V_l) = \mathbb{Q}_l^*$$

is a one-dimensional l-adic representation of G.

Example 2.2 (Elliptic Curves). Let E denote an elliptic curve defined over K and let E_{l^m} denote the kernel of the multiplication by l^m map in $E(\overline{\mathbb{Q}})$. It is known that $E_{l^m} \cong (\mathbb{Z}/l^m\mathbb{Z})^2$. The sets E_{l^m} form an inverse system and $T_l(E) = \varprojlim_m E_{l^m} \cong \mathbb{Z}_l^2$ is called the Tate module of the elliptic curve E. Once again, G acts continuously on each group E_{l^m} and also commutes with the multiplication by l map that forms the inverse limit. Thus, G has a continuous action on the Tate module $T_l(E)$ of E, and for a fixed basis of $T_l(E)$ as a $\mathbb{Z}_l$-module, we get a continuous homomorphism:

$$\rho_l : G \to \mathrm{Aut}(T_l(E)) \cong \mathrm{GL}_2(\mathbb{Z}_l).$$

If $V_l(E)$ is the two-dimensional $\mathbb{Q}_l$-vector space $T_l(E) \otimes \mathbb{Q}_l$ along with the action of G, then by the natural inclusion of $\mathbb{Z}_l \subset \mathbb{Q}_l$, we obtain a continuous homomorphism:

$$\rho_l : G \to \mathrm{Aut}(V_l(E)) \cong \mathrm{GL}_2(\mathbb{Q}_l).$$

The homomorphism ρ_l is called the l-adic representation of G associated to E.

2.1 l-adic Representations of Number Fields

Let K be a number field and M_K denote the set of all finite (non-Archimedean) places of K. If v is such a place, then we denote by κ_v the residue field at v, f_v the residue degree, e_v the ramification index and p_v the rational prime below v (or the characteristic of κ_v). Then, κ_v is an extension of the finite field $\mathbb{F}_{p_v}$ with degree $[\kappa_v : \mathbb{F}_{p_v}] = f_v$. The completion of K with respect to the valuation v will be denoted by K_v.

Now, suppose L is a finite Galois extension of K, with Galois group G. If $w \in M_L$, then the decomposition group of w is the subgroup of G defined by $D_w = \{\sigma \in G : \ \sigma(w) = w\}$. If w lies above $v \in M_K$, then D_w is the Galois group of L_w over K_v. There is a homomorphism of D_w onto the Galois group $\mathrm{Gal}(l_w/\kappa_v)$ of the residue fields, and the kernel of this map is called the inertia group I_w of w. This leads to an isomorphism $D_w/I_w \cong \mathrm{Gal}(l_w/\kappa_v)$. In addition, since l_w/κ_v is an extension of finite fields, its Galois group is cyclic and is generated by the Frobenius map. The corresponding generator in D_w/I_w under the above isomorphism will be denoted by F_w and will be called the Frobenius element.

We say w is unramified if I_w is trivial. Note that for all $w \in M_L$ that divide $v \in M_K$, the inertia groups I_w (resp. the decomposition groups D_w) are conjugate to each other. Accordingly, we may also say that v is unramified if for any (and hence all) $w \mid v$, I_w is trivial. Moreover, if v is indeed unramified, all the Frobenius elements $F_w \in D_w$ will be conjugate to each other for all $w \mid v$. Thus, the conjugacy class of F_w in G depends only on v and will be denoted by F_v.

We now extend the above definitions to arbitrary extensions K over $\mathbb{Q}$. In this case, M_K is defined to be the projective limit of the sets M_{E_λ}, where E_λ varies over the finite extensions of $\mathbb{Q}$ contained in K. Likewise, if L/K is an arbitrary Galois extension, and $w \in M_L$ is such that it divides $v \in M_K$, we define D_w, I_w, F_w and, if v is unramified, F_v the same way as above .

With these notations in mind, we have the following definition of unramified representations.

Definition 14 (Unramified Representation)**.** If $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V)$ is an l-adic representation of K and $v \in M_K$, then ρ is said to be unramified at v if $\rho(I_w)$ is trivial for any $w \in M_{\overline{K}}$ dividing v.

If ρ is unramified at v, then for all w dividing v, we obtain a homomorphism $\rho : D_w/I_w \to \mathrm{Aut}(V)$. Recall the Frobenius element F_w lies in D_w/I_w, so the element $F_{w,\rho} := \rho(F_w)$ will be called the Frobenius of w in the representation ρ. Again, since D_w's (respectively I_w's) are conjugate for all w dividing v, we see that the conjugacy class of $F_{w,\rho}$ in $\mathrm{Aut}(V)$ depends only on v, and will be denoted by $F_{v,\rho}$.

Definition 15 (Rational l-adic Representations)**.** Let ρ be an l-adic representation unramified at $v \in M_K$ and let $P_{v,\rho}(X)$ denote the polynomial $\det(1 - X \cdot F_{v,\rho})$ in the variable X with coefficients in Q_l. [6] Then ρ is said to be rational (resp. integral) if there is a finite subset S of M_K such that ρ is unramified outside S, and for all $v \notin S$, the coefficients of $P_{v,\rho}(X)$ are rational (resp. integral).

One may verify that the l-adic representations described in examples (2.1) and (2.2) are both rational (in fact integral) representations.

Rather than studying a single l-adic representation ρ_l for a given prime l, it is often more fruitful to consider a *system* of l-adic representations for multiple primes l, that are compatible with each other in a certain sense. We introduce this notion of compatibility in the following definitions and shall construct such a system of compatible representations in §2.4.

Definition 16 (Compatible Representations)**.** Let l, l' be two distinct primes and ρ, ρ' be rational l-adic and l'-adic representations respectively. We say ρ and ρ' are compatible if there exists a finite subset S of M_K such that they are unramified outside of S and the respective characteristic polynomials of the Frobenius elements are the same for all v not in S (or equivalently $P_{v,\rho}(X) = P_{v,\rho'}(X)$ for all $v \notin S$).

Definition 17 (Compatible System)**.** A Compatible System is a collection $\{\rho_l\}_l$ of rational l-adic representations for every prime l, such that for any two primes l and l', ρ_l and $\rho_{l'}$ are compatible. The system is *strictly* compatible

[6] Here, by $F_{v,\rho}$, we mean any representative of the conjugacy class in $\mathrm{Aut}(V)$. $P_{v,\rho}(X)$ can also be obtained by reversing the order of the coefficients of the characteristic polynomial of this representative

if there exists a finite set $S \subset M_K$ such that for all valuations v outside S not dividing l, ρ_l is unramified at v, the coefficients of $P_{v,\rho_l}(X)$ are rational, and, if v does not divide l', then $P_{v,\rho_l}(X) = P_{v,\rho_{l'}}(X)$.

Now, we define the class of l-adic representations with values in an affine algebraic group.

Definition 18. Let H be an affine algebraic group over $\mathbb{Q}$, and K a number field. Let l be a prime and consider $H(\mathbb{Q}_l)$ endowed with the natural topology induced from that of $\mathbb{Q}_l$. A continuous homomorphism $\rho : \mathrm{Gal}(\overline{K}/K) \to H(\mathbb{Q}_l)$ is called an l-adic representation of K with values in H.

Suppose A is the coordinate ring of such a group H over $\mathbb{Q}$. An element ϕ in A is said to be central if $\phi(xy) = \phi(yx)$ for any x, y in $H(R)$ and any commutative $\mathbb{Q}$-algebra R. For such an x, the conjugacy class of x in H is rational if $\phi(x)$ lies in $\mathbb{Q}$ for every central element ϕ.

We say ρ is rational if it is unramified outside a finite set of places of K, and if, for these places v where ρ is unramified, the conjugacy class $F_{v,\rho}$ is rational over $\mathbb{Q}$ in the sense defined above. Note that if H is Abelian, then this just means $F_{v,\rho}$ should lie in $H(\mathbb{Q})$. If l and l' are two primes and ρ, ρ' are two rational l-adic and l'-adic representations respectively, then they are said to be compatible if there exists a finite set of places S outside of which these representations are unramified and for any central element ϕ in A, $\phi(F_{v,\rho}) = \phi(F_{v,\rho'})$ for all finite places v outside S. The definition of compatible systems follows similarly.

2.2 Chebotarev's Density Theorem

Here, we shall study an important result due to Chebotarev and a few immediate corollaries that shall prove to be useful in later sections.

Definition 19 (Density)**.** Let $P \subseteq M_K$, and for each integer $n \geq 1$, we set $a_n(P)$ to be the number of valuations $v \in P$ such that $p_v^{f_v} \leq n$. If the limit

$$a = \lim_{n \to \infty} \frac{a_n(P)}{a_n(M_K)}$$

exists, then we say P has density a.

Note that $p_v^{f_v}$ is the number of elements in the residue field κ_v. Also, a finite set always has zero density.

Theorem 9 (Chebotarev's Density Theorem). *Let L be a finite Galois extension of the number field K with Galois group G. Suppose X is a subset of G which is stable under conjugation by elements in G, and P_X is the set of places in M_K that are unramified in L and the Frobenius class F_v lies in X for all $v \in P_X$. Then P_X has density ${}^{|X|}/_{|G|}$.*

Refer to [theorem 10, chap VIII, [5]] for a proof.

Corollary 10. *For each $\sigma \in G$, there exist infinitely many unramified places $w \in M_L$ in L such that their Frobenius element F_w is equal to σ.*

Proof. Taking X to be the conjugacy class of σ in G and applying the above theorem, we see that the set P_X has non-zero density and in particular, has infinite cardinality. This means each v in P_X is unramified in L and for every $w \mid v$ in L, $F_w \in X$. Thus every such F_w is conjugate to σ, and by applying the reverse conjugation, we can find a w' such that $F_{w'}$ is exactly σ. Since there are infinitely many such v's, the result follows. □

Now suppose L is an arbitrary (possibly infinite) Galois extension of K unramified outside a finite set of places $S \subset M_K$. Let G be the Galois group of L over K, equipped with the Krull topology. Consider the following proposition:

Proposition 11. *The set of Frobenius elements of the unramified places in L is dense in G.*

Proof. Let $\sigma \in G$ and let U be an open neighborhood of σ in G. By definition of the Krull topology, the set of subgroups $\mathrm{Gal}(L/E)$, with E a finite Galois subextension of K in L, form a basis of open neighborhoods of the identity. Thus, U must contain a coset of $\mathrm{Gal}(L/E)$ in G for some such E. This coset can be uniquely identified with an element of $\mathrm{Gal}(E/K)$. Assume $\tau \in G$ is a representative of this coset and let $\overline{\tau}$ be the corresponding element in $\mathrm{Gal}(E/K)$. By the above corollary, there is an unramified place $w' \in M_E$ in E such that $F_{w'} = \overline{\tau}$ (in fact there are infinitely many such w'). Note that for any place w_1 in L that is unramified over K and restricts to a place w_1' in E, the Frobenius element F_{w_1} in G maps to $F_{w_1'}$ in $\mathrm{Gal}(E/K)$. This implies that we can find a w in L such that its restriction to $\mathrm{Gal}(E/K)$ is w', and hence $F_w = \tau$. We have thus shown that for each element σ in G and any open neighborhood U of σ, there exists an unramified place w in L such that the Frobenius element F_w lies in U. It follows that the set of Frobenius elements is dense in G. □

2.3 Adeles and Ideles

Recall that M_K denotes the set of finite places of the number field K. We let M_K^∞ denote the set of Archimedean or infinite places of K, and $\overline{M_K}$ be the union of the finite and infinite places. Thus, if $v \in \overline{M_K}$, then the completion of K at v, K_v, will be either $\mathbb{R}$ or $\mathbb{C}$ if v is infinite, and is a non-Archimedean valued field if v is finite. In the latter case, we know K_v is locally compact and we will denote the valuation ring of K_v by R_v (a compact subring of K_v), the group of units in the valuation ring by U_v and the uniformizer by π_v. Now, let S be a finite subset of $\overline{M_K}$ containing all the infinite places. Consider

$$\mathbb{A}_K(S) = \prod_{v \in S} K_v \times \prod_{v \notin S} R_v,$$

which, under the usual product topology, is locally compact. Under componentwise addition and multiplication, $\mathbb{A}_K(S)$ is also a topological ring. We denote by $\mathbb{A}_K$, the union of all the sets $\mathbb{A}_K(S)$ and prescribe the topology on $\mathbb{A}_K$ by decreeing that all sets $\mathbb{A}_K(S)$ be open subrings [7]. $\mathbb{A}_K$, called the adele (*adèle*) ring of the number field K, is hence a locally compact topological ring. It consists of elements of the form $(x_v) \in \prod K_v$ such that $|x_v|_v \leq 1$ for almost all v. In addition, we may obtain a fundamental system of neighborhoods of 0 in $\mathbb{A}_K$ by taking all sets of the form $\prod X_v$, where each X_v is a neighborhood of 0 in K_v and $X_v = R_v$ for almost all v. Also, the natural embedding of K into $\prod K_v$ actually lands in A_K, i.e. if $x \in K$, then the element (x_v) given by $x_v = x$ for all v, lies in A_K. The image of K under this injection is called the ring of principal adeles.

We now define the idele *(idèle)* group $\mathbb{I}_K$ associated to K. Set-theoretically, it is the group of units in A_K: it consists of elements of the form $(x_v) \in \prod K_v^*$, such that x_v lies in U_v for almost all finite v. However, under the subspace topology, it is not a topological group since inversion is not continuous. We thus give it the coarsest topology for which both inversion and the embedding of $I_K \hookrightarrow A_K$ are continuous maps. We define the Idele Class group to be the quotient $C = \mathbb{I}/K^*$. As before, the injection of K^* into $\mathbb{I}_K$ gives the

[7] Note that the sets $\mathbb{A}_K(S)$ form a directed system over all finite sets S: if $S \subset S'$, then $\mathbb{A}_K(S)$ embeds as an open subgroup of $\mathbb{A}_K(S')$. We may thus give an equivalent definition of $\mathbb{A}_K$ as the direct limit of these sets along with the direct limit topology

group of principal ideles, and we will often denote these principal ideles by K^* itself.

2.4 The Groups $S_{\mathfrak{m}}$

Definition 20 (Modulus)**.** A modulus $\mathfrak{m}$ of K is a collection of non-negative integers $\{m_v\}_{v \in M_K}$, such that $m_v = 0$ for all but finitely many v in M_K. The finite subset of M_K consisting of all v for which m_v is non-zero is called the support of $\mathfrak{m}$ and will be denoted by $\mathrm{Supp}(\mathfrak{m})$.

For such a modulus $\mathfrak{m}$ and a valuation $v \in M_K$, consider the following set:

$$U_{v,\mathfrak{m}} = \begin{cases} \text{conn. comp of } K_v^* & \text{if } v \in M_K^\infty \\ 1 + \pi_v^{m_v} R_v & \text{if } v \in \mathrm{Supp}(\mathfrak{m}) \\ U_v & \text{otherwise.} \end{cases} \tag{6}$$

Note that the connected component of K_v^* is either $\mathbb{R}_{>0}$ or $\mathbb{C}^*$, if $v \in M_K^\infty$. Then $U_{\mathfrak{m}} = \prod_v U_{v,\mathfrak{m}}$, is an open subgroup of $\mathbb{I}_K$.
Let

$$\begin{aligned} &E \text{ be the group of units in } K, \\ &E_{\mathfrak{m}} = E \cap U_{\mathfrak{m}}, \\ &I_{\mathfrak{m}} = \mathbb{I}_K / U_{\mathfrak{m}}, \text{ and} \\ &C_{\mathfrak{m}} = \mathbb{I}_K / (K^* U_{\mathfrak{m}}). \end{aligned}$$

Moreover, if $x = (x_v)$ is a principal idele and if x lies in $U_{\mathfrak{m}}$, then x must be a unit in K. Thus $E_{\mathfrak{m}}$ may be equivalently defined as $K^* \cap U_{\mathfrak{m}}$ and we obtain the exact sequence:

$$1 \to K^*/E_{\mathfrak{m}} \to I_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 1. \tag{7}$$

$C_{\mathfrak{m}}$ is the ray class group associated to $\mathfrak{m}$ and is known to have finite cardinality. By class field theory, if D denotes the connected component of unity in the idele class group C, then the quotient C/D is isomorphic to the Galois group of the maximal Abelian extension of K and is infact the inverse limit of the $C_{\mathfrak{m}}$'s.

Now, let T denote the torus $\mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$. Then $E_{\mathfrak{m}}$ is a subgroup of the $\mathbb{Q}$-rational points $T(\mathbb{Q})$. Let $\overline{E_{\mathfrak{m}}}$ denote the Zariski closure of $E_{\mathfrak{m}}$ in T.

The quotient group $T/\overline{E_{\mathfrak{m}}}$, which we denote by $T_{\mathfrak{m}}$, is also a $\mathbb{Q}$-torus. We immediately obtain a homomorphism $K^*/E_{\mathfrak{m}} \to T_{\mathfrak{m}}(\mathbb{Q})$. This gives us a diagram of the form:

$$\begin{tikzcd}
K^*/E_{\mathfrak{m}} \arrow[r] \arrow[d] & I_{\mathfrak{m}} \\
T_{\mathfrak{m}}(\mathbb{Q}).
\end{tikzcd}$$

Using the above diagram and the exact sequence (7), we construct a $\mathbb{Q}$-algebraic group $S_{\mathfrak{m}}$ such that $S_{\mathfrak{m}}(\mathbb{Q})$ is the push-out of the above diagram. If the finite group $C_{\mathfrak{m}} \cong I_{\mathfrak{m}}/(K^*/E_{\mathfrak{m}})$ has cardinality r, then $S_{\mathfrak{m}}$ is the disjoint union of r copies of $T_{\mathfrak{m}}$. $S_{\mathfrak{m}}$ is said to be the extension of the constant algebraic group $C_{\mathfrak{m}}$ by $T_{\mathfrak{m}}$, yielding the following exact sequence of algebraic groups:

$$1 \longrightarrow T_{\mathfrak{m}} \longrightarrow S_{\mathfrak{m}} \longrightarrow C_{\mathfrak{m}} \longrightarrow 1. \tag{8}$$

Combining this with the previous exact sequence, we obtain the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & K^*/E_{\mathfrak{m}} \arrow[r] \arrow[d] & I_{\mathfrak{m}} \arrow[r] \arrow[d] & C_{\mathfrak{m}} \arrow[r] \arrow[d, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & T_{\mathfrak{m}}(\mathbb{Q}) \arrow[r] & S_{\mathfrak{m}}(\mathbb{Q}) \arrow[r] & C_{\mathfrak{m}} \arrow[r] & 1.
\end{tikzcd} \tag{9}$$

Note that, by construction of $S_{\mathfrak{m}}$ as a pushout, it satisfies the following universal property:

> If H is an algebraic group over $\mathbb{Q}$ with morphisms $a : T_{\mathfrak{m}} \to H$ and $b : I_{\mathfrak{m}} \to H(\mathbb{Q})$ such that the following diagram commutes
>
> $$\begin{tikzcd}
K^*/E_{\mathfrak{m}} \arrow[r] \arrow[d] & I_{\mathfrak{m}} \arrow[d] \\
T_{\mathfrak{m}}(\mathbb{Q}) \arrow[r] & H(\mathbb{Q}),
\end{tikzcd} \tag{10}$$
>
> then there exists a unique morphism $\delta : S_{\mathfrak{m}} \to H$ defined over $\mathbb{Q}$, such that a and b are obtained by composing the corresponding morphisms of $S_{\mathfrak{m}}$ with δ.

Remark. The algebraic group $S_{\mathfrak{m}}$ over $\mathbb{Q}$ is a group of multiplicative type by construction, since after a suitable finite extension of $\mathbb{Q}$, it becomes isomorphic to the product of a torus and finite Abelian group.

We denote by ϵ the homomorphism $\epsilon : \mathbb{I}_K \to I_{\mathfrak{m}} \to S_{\mathfrak{m}}(\mathbb{Q})$ and by π the algebraic morphism $T \to T_{\mathfrak{m}} \to S_{\mathfrak{m}}$, both obtained from the above construction. Considering the $\mathbb{Q}_l$-rational points gives the homomorphism

$$\pi_l : T(\mathbb{Q}_l) \to S_{\mathfrak{m}}(\mathbb{Q}_l). \tag{11}$$

As $K \otimes \mathbb{Q}_l = \prod_{v|l} K_v$, we note that $T(\mathbb{Q}_l) = (K \otimes \mathbb{Q}_l)^* = \prod_{v|l} K_v^*$. This is a direct factor of the idele group $\mathbb{I}_K$ and we denote the projection of $\mathbb{I}_K$ onto $T(\mathbb{Q}_l)$ by proj_l. For $x \in \mathbb{I}_K$, we say that $\mathrm{proj}_l(x)$ is the *l-component* of x. The composition $\pi_l \circ \mathrm{proj}_l : \mathbb{I}_K \to S_{\mathfrak{m}}(\mathbb{Q}_l)$ is a continuous homomorphism which we denote by α_l.

It is easy to see that the following diagram is commutative:

$$\begin{tikzcd}
K^* \arrow[r, hook] \arrow[d] & \mathbb{I}_K \arrow[d] \\
K^*/E_{\mathfrak{m}} \arrow[r, hook] & I_{\mathfrak{m}}
\end{tikzcd}$$

Combining this diagram with (9) shows that α_l and ϵ agree on K^*. If

$$\epsilon_l : \mathbb{I}_K \to S_{\mathfrak{m}}(\mathbb{Q}_l) \tag{12}$$

denotes the homomorphism defined by $\epsilon_l(x) = \epsilon(x) \cdot \alpha_l(x^{-1})$, then ϵ_l is trivial on K^*, and thus factors through the quotient $\mathbb{I}_K/K^*$ which is precisely the idele class group C of K, giving us a map from C to $S_{\mathfrak{m}}(Q_l)$. In addition, since the continuous image of a connected set is connected and $S_{\mathfrak{m}}(Q_l)$, being an l-adic Lie group, is totally disconnected, the image of the set $D \subset C$ must be trivial. As noted previously, the quotient C/D is isomorphic to the Galois group G^{ab} of the maximal Abelian extension of K, and as a result, we obtain an l-adic representation of G^{ab} with values in $S_{\mathfrak{m}}$:

$$\epsilon_l : G^{\mathrm{ab}} \to S_{\mathfrak{m}}(\mathbb{Q}_l) \tag{13}$$

Proposition 12. *The representation ϵ_l is a rational and Abelian l-adic representation. It is unramified outside* $\mathrm{Supp}(\mathfrak{m}) \cup \{v \in M_K : v \mid l\}$*. If ϵ_l is unramified at v and f_v denotes the idele* $(1, 1, \ldots, \pi_v, \ldots)$*, with the uniformizing parameter π_v in the v-component, then $\epsilon(f_v) \in S_{\mathfrak{m}}(\mathbb{Q})$ is the Frobenius class F_{v,ϵ_l} associated to ϵ_l.*

Proof. Before beginning the proof, we shall recall a few facts from Class Field Theory. Firstly, there is a natural embedding of K_v^* into $\mathbb{I}_K$ as follows: $a \in K_v^*$ is identified with the idele $(1, 1, \dots, a, \dots)$, with a in the v-position. With this embedding in mind, the group of units U_v is mapped onto the inertia subgroup of v in G^{ab} under the class field isomorphism $C/D \xrightarrow{\simeq} G^{\mathrm{ab}}$. Similarly, the uniformizing parameter π_v in K_v^* is mapped onto the Frobenius class of v in G^{ab} (which is a singleton in this case).
Now suppose $v \notin \mathrm{Supp}(\mathfrak{m})$ and let $a \in U_v$. Then under the aforementioned embedding of K_v^* into $\mathbb{I}_K$, a belongs to the group $U_{\mathfrak{m}}$. Since the map ϵ is obtained after modding out by $U_{\mathfrak{m}}$, $\epsilon(a) = 1$. Further, if $v \nmid l$ (i.e. $p_v \neq l$), then the l-component $\mathrm{proj}_l(a)$ of a is trivial and hence $\alpha_l(a^{-1}) = 1$. This shows that $\epsilon_l(a) = \epsilon(a) \cdot \alpha_l(a^{-1}) = 1$ for all a in U_v, where $v \notin \mathrm{Supp}(\mathfrak{m})$ and $v \nmid l$. Since U_v is mapped onto the inertia subgroup of v in G^{ab}, it can be concluded that ϵ_l is trivial on this inertia group and hence unramified at all such v.
Finally, for such a finite place v, $\epsilon_l(f_v) = \epsilon(f_v)\alpha_l(f_v^{-1})$ which is simply $\epsilon(f_v)$ as the l-component of f_v is trivial. Now, since $S_{\mathfrak{m}}$ is Abelian, the Frobenius class is a singleton and hence the element $\epsilon(f_v)$ is the required Frobenius element F_{v,ϵ_l}. Note that $\epsilon(f_v)$ actually lies in $S_{\mathfrak{m}}(\mathbb{Q})$, which means the coefficients of its characteristic polynomial would be rational, and thus, ϵ_l is a rational l-adic representation. □

Moreover, it can be seen from their respective definitions that both f_v and the map ϵ are independent of the prime l. Thus, the Frobenius element $F_{v,\epsilon_l} = \epsilon(f_v)$ stays the same as we vary the prime l, i.e. for any two primes l and l' and $v \notin \mathrm{Supp}(\mathfrak{m}) \cup \{v \in M_K : \ v \mid l \text{ or } v \mid l'\}$, $\epsilon_l(f_v) = \epsilon_{l'}(f_v) = \epsilon(f_v)$. This means that the collection $\{\epsilon_l\}_l$ form a strictly compatible system of rational Abelian l-adic representations. Since F_{v,ϵ_l} is independent of the prime l, we denote it by F_v, the Frobenius element associated to the system $\{\epsilon_l\}_l$. The following lemmas will establish that the set of all Frobenius elements F_v is Zariski-dense in $S_{\mathfrak{m}}$.

Lemma 13. *The image* $\mathrm{Im}(\epsilon_l) = \epsilon_l(G^{\mathrm{ab}})$ *of the representation* ϵ_l *is Zariski-dense in* $S_{\mathfrak{m}}$.

Proof. Suppose x belongs to the open subgroup

$$U_{l,\mathfrak{m}} = \prod_{v \mid l} U_{v,\mathfrak{m}}$$

in $K_l^* = \prod_{v|l} K_v^* = T(\mathbb{Q}_l)$. Embedding this subgroup into the ideles $\mathbb{I}_K$ (with 1's at all places not dividing l), we see that $\epsilon(x) = 1$ since $x \in U_{\mathfrak{m}}$, and $\alpha_l(x^{-1}) = \pi_l(x^{-1})$. Thus, by definition of ϵ_l in (12), $\epsilon_l(x) = \pi_l(x^{-1})$ on the open subgroup $U_{l,\mathfrak{m}}$. Since the map $T_{\mathfrak{m}}(\mathbb{Q}_l) \to S_{\mathfrak{m}}(\mathbb{Q}_l)$ is injective, we have $\pi_l(U_{l,\mathfrak{m}}) \subset T_{\mathfrak{m}}(\mathbb{Q}_l) \subset S_{\mathfrak{m}}(\mathbb{Q}_l)$, and this image is open. Thus $\mathrm{Im}(\epsilon_l)$ contains an open subgroup and is therefore open in $S_{\mathfrak{m}}(\mathbb{Q}_l)$. Moreover, $\pi_l(U_{l,\mathfrak{m}})$ is a non-empty open set of $T_{\mathfrak{m}}(\mathbb{Q}_l)$ and is thus dense in $T_{\mathfrak{m}}$. Finally, consider the following diagram:

$$\begin{tikzcd}
 & & \mathbb{I}_k \arrow[d] & & \\
1 \arrow[r] & K^*/E_{\mathfrak{m}} \arrow[r] \arrow[d] & I_{\mathfrak{m}} \arrow[r] \arrow[d] & C_{\mathfrak{m}} \arrow[r] \arrow[d, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & T_{\mathfrak{m}}(\mathbb{Q}_l) \arrow[r] & S_{\mathfrak{m}}(\mathbb{Q}_l) \arrow[r] & C_{\mathfrak{m}} \arrow[r] & 1 \\
 & \mathbb{I}_K \arrow[u] & & & .
\end{tikzcd}$$

Again, ϵ_l has two parts: one corresponding to ϵ and the other to α_l. On composition with the map $S_{\mathfrak{m}}(\mathbb{Q}_l) \to C_{\mathfrak{m}}$, α_l corresponds to the route $\mathbb{I}_K \to T_{\mathfrak{m}}(\mathbb{Q}_l) \to S_m(\mathbb{Q}_l) \to C_{\mathfrak{m}}$ and is thus trivial by exactness of the bottom row in the above diagram. On the other hand, ϵ corresponds to the route $\mathbb{I}_K \to I_{\mathfrak{m}} \to C_{\mathfrak{m}} \overset{\mathrm{Id}}{\to} C_{\mathfrak{m}}$, and maps onto $C_{\mathfrak{m}}$ as $I_{\mathfrak{m}} \to C_{\mathfrak{m}}$ is surjective. We therefore have that $\mathrm{Im}(\epsilon_l)$ is an open subgroup of $S_{\mathfrak{m}}(\mathbb{Q}_l)$ that is dense in $T_{\mathfrak{m}}$ and maps onto $C_{\mathfrak{m}}$. Thus it must be dense in $S_{\mathfrak{m}}$, being the extension of $C_{\mathfrak{m}}$ by $T_{\mathfrak{m}}$. □

Lemma 14. *The set of all Frobenius elements F_v associated to the system $\{\epsilon_l\}_l$ for every $v \in M_K$ is Zariski-dense in $S_{\mathfrak{m}}$.*

Proof. Let X be the set of all F_v as v varies over M_K. Let $\overline{X} \subset S_{\mathfrak{m}}$ denote the Zariski-closure of X in $S_{\mathfrak{m}}$ and $\overline{X_l} \subset S_{\mathfrak{m}}(\mathbb{Q}_l)$ the closure in the l-adic topology in $S_{\mathfrak{m}}(\mathbb{Q}_l)$ for a prime l. Note that the pre-image of X under ϵ_l contains the set of all Frobenius elements in G^{ab}, which we know is dense under the Krull topology (refer to proposition (11)). Thus, $\overline{X_l} = \mathrm{Im}(\epsilon_l)$. As the Zariski topology is coarser than the l-adic topology, $\mathrm{Im}(\epsilon_l) = \overline{X_l} \subseteq \overline{X}(\mathbb{Q}_l)$. But the previous lemma asserts that $\mathrm{Im}(\epsilon_l)$ is Zariski-dense in $S_{\mathfrak{m}}$, and thus $\overline{X} = S_{\mathfrak{m}}$. □

2.5 Linear Representations of $S_{\mathfrak{m}}$

We will now study representations of $S_{\mathfrak{m}}$. Recall that $S_{\mathfrak{m}}$ is an extension of the finite Abelian group $C_{\mathfrak{m}}$ by the torus $T_{\mathfrak{m}}$. It is thus a group of multiplicative type, as it becomes isomorphic to a product of the torus and finite Abelian group over a suitable extension of the base field $\mathbb{Q}$. The proposition below follows from discussions in chapter one:

Proposition 15. *Suppose E is an extension of $\mathbb{Q}$ and $\phi \in \mathrm{Rep}_E(S_{\mathfrak{m},E})$. Then the following are equivalent:*

1. *The representation ϕ can be defined over $\mathbb{Q}$.*
2. *If v is a finite place outside $\mathrm{Supp}(\mathfrak{m})$, then the coefficients of the characteristic polynomial of $\phi(F_v)$ are rational (recall that $F_v = F_{v,\epsilon_l} = \epsilon(f_v)$ is the Frobenius element associated to the representation ϵ_l defined in §2.4).*
3. *There exists a set of places M (or primes) of $\mathbb{Q}$ with density 1 (in the sense of (19)) such that the trace $\mathrm{Tr}(\phi(F_v)) \in \mathbb{Q}$ for all v in M.*

Proof. If ϕ is defined over $\mathbb{Q}$, then clearly $\phi(F_v)$ is a matrix with rational coefficients and part (2) follows. If part (2) holds, then (3) is immediate, since the trace occurs as the coefficient of one of the terms in the characteristic polynomial and $\mathrm{Supp}(\mathfrak{m})$ is a finite set and hence $M_K \setminus \mathrm{Supp}(\mathfrak{m})$ has density 1.

Now assume part (3) is true, and let A be the coordinate ring of $S_{\mathfrak{m},E}$ over E. Let $\theta_\phi \in A \otimes E$ be the trace of ϕ (see (11)). Let $\{e_i\}_{i\in I}$ be a basis of E as a vector space over $\mathbb{Q}$, where i varies over an index set I, and let $e_j = 1$ for some index $j \in I$. Then, by linearity

$$\theta_\phi = \sum_i a_i \otimes e_i,$$

for $a_i \in A$. Recall that that if $h \in S_{\mathfrak{m}}(E)$, then the trace $\mathrm{Tr}(\phi(h))$ of the matrix $\phi(h)$ is equal to $\theta_\phi(h) = \sum_i a_i(h)e_i$. Choose h to be $F_v \in S_{\mathfrak{m}}(\mathbb{Q})$ for all $v \in M$. Then, $a_i(F_v)$ will be an element in $\mathbb{Q}$ for all $i \in I$ and $v \in M$. But it is given that $\mathrm{Tr}(\phi(F_v)) \in \mathbb{Q}$ for all $v \in M$, and by the linear independence of the e_i's, we must have $a_i(F_v) = 0$ for all $i \neq j$ and $v \in M$. Lemma (14) tells us that the Frobenius elements F_v are dense in $S_{\mathfrak{m}}$, and thus, if $a_i(F_v) = 0$ on all $v \in M$, then a_i must be zero for all $i \neq j$. Thus $\theta_\phi = a_j$ and hence belongs to A which means that ϕ can be defined over $\mathbb{Q}$ using corollary (8). □

2.6 l-adic Representations Attached to Representations of $S_{\mathfrak{m}}$

We will now describe the l-adic representations associated to certain linear representations of the $\mathbb{Q}$-algebraic group $S_{\mathfrak{m}}$. Consider the case when a representation of $S_{\mathfrak{m},\mathbb{Q}_l}$, the algebraic group obtained from $S_{\mathfrak{m}}$ via extension by scalars from $\mathbb{Q}$ to $\mathbb{Q}_l$, is given. Let V_l be a finite-dimensional vector space over $\mathbb{Q}_l$, and (V_l, ϕ) be such a representation, i.e., a homomorphism

$$\phi : S_{\mathfrak{m},\mathbb{Q}_l} \to \mathrm{GL}_{V_l},$$

defined over $\mathbb{Q}_l$. Looking at the $\mathbb{Q}_l$-rational points, we get a continuous homomorphism $\phi : S_{\mathfrak{m}}(\mathbb{Q}_l) \to \mathrm{GL}_{V_l}(\mathbb{Q}_l) = \mathrm{Aut}(V_l)$. Composing with $\epsilon_l : G^{\mathrm{ab}} \to S_{\mathfrak{m}}(\mathbb{Q}_l)$ from (13), leads to the following Abelian l-adic representation of K in V_l:

$$\phi_l = \phi \circ \epsilon_l : G^{\mathrm{ab}} \to \mathrm{Aut}(V_l).$$

Proposition 16. *1. The representation ϕ_l is semi-simple.*

2. It is unramified at all finite places v that do not belong to Supp$(\mathfrak{m})$ and do not lie above the prime l. The Frobenius element associated to ϕ_l, F_{v,ϕ_l} is equal to $\phi(F_v)$.

3. It is rational if and only if the original representation $\phi : S_{\mathfrak{m},\mathbb{Q}_l} \to \mathrm{GL}_{V_l}$ can be defined over $\mathbb{Q}$, in the sense of (12).

Proof. Part (1) follows from the fact that $S_{\mathfrak{m}}$ is a group of multiplicative type and hence all representations of $S_{\mathfrak{m}}$ are semi-simple, as discussed in §1.9. Part (2) follows from proposition (12) and part (3) from proposition (15). □

Next, we shall study the case when a rational representation of $S_{\mathfrak{m}}$ is given, i.e. a representation $\phi_0 : S_{\mathfrak{m}} \to \mathrm{GL}_V$ defined over $\mathbb{Q}$, where V is a finite-dimensional vector space over $\mathbb{Q}$. If l is a prime, then by extension of scalars, we obtain a representation $\phi_0^{(l)} : S_{\mathfrak{m},\mathbb{Q}_l} \to \mathrm{GL}_{V_l}$, where $V_l = V \otimes_{\mathbb{Q}} \mathbb{Q}_l$. We can now apply the previous construction on $\phi_0^{(l)}$ to obtain an Abelian l-adic representation $\phi_l : G^{\mathrm{ab}} \to \mathrm{Aut}(V_l)$ for each prime l, and the following proposition follows:

Proposition 17. *1. The system $\{\phi_l\}$ form a strictly compatible system of rational Abelian l-adic representations, all of which are semi-simple. In particular, if $v \notin \mathrm{Supp}(\mathfrak{m})$, then the Frobenius element associated to the entire system $\{\phi_l\}$ at v, is equal to $\phi_0(F_v) \in \mathrm{Aut}(V)$.*

2. *There are infinitely many primes l such that ϕ_l is diagonalizable over $\mathbb{Q}_l$.*

Proof. From part (1) of proposition (16), we see that for a given prime l, ϕ_l is semi-simple. From part (3) of the same proposition, it is rational since it arises from the representation ϕ_0 defined over $\mathbb{Q}$. Fianlly, from part (2), for $v \notin \mathrm{Supp}(\mathfrak{m}) \cup \{v \in M_K : v \mid l\}$, the Frobenius element at v, associated to the representation ϕ_l is $\phi_0^{(l)}(F_v)$. However, note that F_v belongs to $S_{\mathfrak{m}}(\mathbb{Q})$, and hence $\phi_0^{(l)}(F_v) = \phi_0(F_v)$. Since $\phi_0(F_v)$ does not depend on the prime l, the system $\{\phi_l\}$ is strictly compatible.

Now, since $S_{\mathfrak{m}}$ is a group of multiplicative type, ϕ_0 becomes a diagonalizable representation over a finite extension E of $\mathbb{Q}$. If we can somehow find a prime l such that l is completely split in E, then E can be embedded into $\mathbb{Q}_l$ for this prime l, and thus the representation ϕ_l becomes diagonalizable. All that remains is to show there are infinitely many primes l that split completely in the number field E. Without loss of generality, assume E is Galois over $\mathbb{Q}$. Recall that l is split in E if and only if the completion E_w of E at all places w lying above l is exactly $\mathbb{Q}_l$. Note that $E_w \cong \mathbb{Q}_l$ for all $w \mid l$ if and only if the Frobenius element F_w is trivial for any $w \mid l$ (as the F_w's are conjugate for all $w \mid l$). Hence, all we need to prove is that there are infinitely many places w in E such that the Frobenius element $F_w = \{1\}$, but this follows from corollary (10). □

In conclusion, in this chapter we constructed a system of rational Abelian l-adic representations of a number field K. We began with a modulus $\mathfrak{m}$, and using the torus $T = \mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$, we obtained the $\mathbb{Q}$-algebraic group $S_{\mathfrak{m}}$ associated to $\mathfrak{m}$. Using this group $S_{\mathfrak{m}}$, we constructed Abelian l-adic representations ϵ_l with values in $S_{\mathfrak{m}}$. Next, we saw how one can associate Abelian l-adic representations to linear representations of $S_{\mathfrak{m}}$ utilizing the previous construction. In the next chapter, we will see how any Abelian l-adic representation of K, satisfying certain conditions (namely *Local Algebraicity*), actually arise from the above method.

3 Locally Algebraic Representations

We begin this chapter by revisiting proposition (16), where we constructed ϕ_l, an Abelian l-adic representation of the number field K into V_l. Recall that V_l is a finite-dimensional $\mathbb{Q}_l$-vector space and that ϕ_l was obtained from a linear representation $\phi : S_{\mathfrak{m},\mathbb{Q}_l} \to \mathrm{GL}_{V_l}$ of $S_{\mathfrak{m},\mathbb{Q}_l}$, composed with the representation ϵ_l (13), i.e. $\phi_l = \phi \circ \epsilon_l$. Moreover, ϵ_l was orginally obtained as a continuous homomorphism $\epsilon_l : \mathbb{I}_K \to S_{\mathfrak{m}}(\mathbb{Q}_l)$ as seen from (12), and we shall, in this discussion, identify ϕ_l by the map $\phi_l : \mathbb{I}_K \to \mathrm{Aut}(V_l)$. Also, we have the algebraic morphism $\pi : T \to T_{\mathfrak{m}} \to S_{\mathfrak{m}}$ from the construction of $S_{\mathfrak{m}}$ (8). By extension of scalars from $\mathbb{Q}$ to $\mathbb{Q}_l$, we obtain a morphism $\pi^{(l)} : T_{\mathbb{Q}_l} \to S_{\mathfrak{m},\mathbb{Q}_l}$ of $\mathbb{Q}_l$-groups. Compose with ϕ to get the following representation of $T_{\mathbb{Q}_l}$, which we denote by ϕ_T:

$$\phi_T = \phi \circ \pi^{(l)} : T_{\mathbb{Q}_l} \to \mathrm{GL}_{V_l}. \tag{14}$$

Note that on the $\mathbb{Q}_l$ rational points, $\pi^{(l)}$ coincides with π_l defined in (11). Now let x be an element of the open subgroup

$$U_{l,\mathfrak{m}} = \prod_{v|l} U_{v,\mathfrak{m}},$$

of $T(\mathbb{Q}_l) = \prod_{v|l} K_v^*$ (recall the definition of $U_{v,\mathfrak{m}}$ from 6). Since each component of x is a unit in $U_{v,\mathfrak{m}}$, $x^{-1} \in U_{l,\mathfrak{m}}$. Then, $\phi_T(x^{-1}) = \phi(\pi^{(l)}(x^{-1})) = \phi(\pi_l(x^{-1}))$.

We can also view x as an element of the idele group $\mathbb{I}_K$ by mapping it to the element in $\mathbb{I}_K$, which coincides with x on the l-component and has 1's everywhere else. Thus,

$$\begin{aligned}\phi_l(x) = \phi(\epsilon_l(x)) &= \phi(\epsilon(x) \cdot \alpha(x^{-1})) \\ &= \phi(\epsilon(x)\pi_l(x^{-1})) \\ &= \phi(\pi_l(x^{-1})) \qquad \text{(as } x \in U_{\mathfrak{m}} \text{ and } \epsilon \text{ is trivial on } U_{\mathfrak{m}}\text{)}.\end{aligned}$$

Thus, for x in $U_{l,\mathfrak{m}}$,

$$\phi_l(x) = \phi_T(x^{-1}). \tag{15}$$

This property is what defines local algebraicity and ensures that any rational Abelian l-adic representation arises from a linear representation of one the groups $S_{\mathfrak{m}}$, as we shall see in the following sections.

3.1 Definitions

3.1.1 The Local Case

Let p be a prime and let k be a finite extension of $\mathbb{Q}_p$. Denote by T the $\mathbb{Q}_p$-torus defined by $\mathrm{Res}_{k/\mathbb{Q}_p}(\mathbb{G}_m)$. Note that $T(\mathbb{Q}_p) = k^*$. Let V be a finite-dimensional $\mathbb{Q}_p$-vector space and GL_V the associated general linear group. From local class field theory, that there is a homomorphism

$$\theta : k^* \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$$

called the local Artin homomorphism for k. Now suppose

$$\rho : \mathrm{Gal}(k^{\mathrm{ab}}/k) \to \mathrm{GL}_V(\mathbb{Q}_p) = \mathrm{Aut}(V)$$

is an Abelian p-adic representation of k in V. Composing with θ, we get a continuous homomorphism $\rho \circ \theta$ from $k^* = T(\mathbb{Q}_p)$ into $\mathrm{Aut}(V)$.

Definition 21. The representation ρ is said to be locally algebraic if there is an algebraic morphism $r : T \to \mathrm{GL}_V$ over $\mathbb{Q}_p$ such that

$$\rho \circ \theta(x) = r(x^{-1}),$$

for all $x \in k^*$ close enough to 1.

Note that for the $\mathbb{Q}_p$-torus T, any non-trivial open subset of the $\mathbb{Q}_p$-rational points, i.e. $T(\mathbb{Q}_p) = k^*$, is Zariski-dense in T. Thus, the morphism r mentioned above is unique, since it is determined by its values on a dense open neighborhood of 1. When ρ is locally algebraic, r is called the algebraic morphism associated to ρ.

3.1.2 The Global Case

As usual, let K be a number field, l a prime, V_l a finite-dimensional $\mathbb{Q}_l$-vector space and $\rho : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Aut}(V_l)$ an Abelian l-adic representation of K in V_l. If v is a finite place of K lying above l. Then, the decomposition subgroup at v, $D_v \subset \mathrm{Gal}(K^{\mathrm{ab}}/K)$, is isomorphic to the local Galois group $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$. Thus, by restricting ρ to this subgroup, we obtain an l-adic representation of K_v:

$$\rho_v : \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \to \mathrm{Aut}(V_l).$$

Since $v \mid l$, we are reduced to the local case of the previous section.

Definition 22. The representation ρ is said to be locally algebraic if the local representations ρ_v are locally algebraic for all v dividing the prime l.

As in the local case, we can interpret local algebraicity of ρ in terms of a representation of the torus $T = \mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_m)$. Let $T_{\mathbb{Q}_l}$ be the $\mathbb{Q}_l$-torus obtained by extension of scalars on T. Then,

$$T_{\mathbb{Q}_l}(\mathbb{Q}_l) = T(\mathbb{Q}_l) = (K \otimes_{\mathbb{Q}} \mathbb{Q}_l)^* = \prod_{v|l} K_v^*.$$

By global class field theory, we have the global Artin homomorphism $\theta : \mathbb{I}_k \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, where $\mathbb{I}_K$ is the idele group of K. Also, as mentioned in the beginning of this chapter, we can embed $\prod_{v|l} K_v^*$ into $\mathbb{I}_K$ by the map $x \mapsto (1, \ldots, 1, x, 1, \ldots)$, with x at the l-component. By composing this embedding with the Artin homomorphism, we obtain

$$\theta_l : \prod_{v|l} K_v^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Proposition 18. *The representation ρ is locally algebraic if and only if there is an algebraic morphism $f : T_{\mathbb{Q}_l} \to \mathrm{GL}_{V_l}$ of $\mathbb{Q}_l$-groups such that*

$$\rho \circ \theta_l(x) = f(x^{-1}),$$

for all x in $\prod_{v|l} K_v^*$ close enough to 1.

Proof. Note that the torus $T_{\mathbb{Q}_l}$ can be written as the product $\prod_{v|l} T_v$ over $\mathbb{Q}_l$, where $T_v = \mathrm{Res}_{K_v/\mathbb{Q}_l}(\mathbb{G}_m)$. From the local case there are algebraic morphisms r_v associated to each ρ_v, and the proposition follows with f being the product of the r_v's. □

As in the local case, the morphism f is unique and is called the algebraic morphism associated to ρ.

3.2 Modulus of a Locally Algebraic Representation

Let $\rho : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Aut}(V_l)$ an Abelian l-adic representation of the number field K, and suppose it is also locally algebraic with $f : T_{\mathbb{Q}_l} \to \mathrm{GL}_{V_l}$ as the associated algebraic morphism. Let θ and θ_l be as defined in the previous section.

Definition 23. Let $\mathfrak{m}$ be a modulus in the sense of definition (20). The representation ρ is said to be definied mod $\mathfrak{m}$ if the following are true:

1. The composition $\rho \circ \theta : \mathbb{I}_k \to \mathrm{Aut}(V_l)$ is trivial on $U_{v,\mathfrak{m}}$ for $v \nmid l$.
2. The equality $\rho \circ \theta_l(x) = f(x^{-1})$ holds for all x in the open subgroup $U_{l,\mathfrak{m}} = \prod_{v|l} U_{v,\mathfrak{m}}$ of $T_{\mathbb{Q}_l}(\mathbb{Q}_l)$.

Remark. Note that we can have multiple moduli of definition for a representation ρ, however, there is always a smallest one, which is called the conductor of ρ.

We shall now prove that all locally algebraic representations have a modulus of definition.

Proposition 19. *Every locally algebraic l-adic representation has a modulus of definition.*

Proof. First, suppose v is a place of the number field K such that v lies above a prime p not equal to l, and let α denote the composition $\rho \circ \theta : \mathbb{I}_k \to \mathrm{Aut}(V_l)$. Consider the restriction of α to K_v^*. The group K_v^* is a p-adic Lie group and a homomorphism from a p-adic Lie group to an l-adic one must be locally trivial if $p \neq l$. Thus, whenever $v \nmid l$, α is trivial on an open subgroup of K_v^*.

Now, by Lie theory, we can find a neighborhood N of unity in $\mathrm{Aut}(V_l)$, such that N contains no non-trivial finite subgroup. Since it is open, $\alpha^{-1}(N)$ is open in the idele topology and hence must contain U_v for almost all v's. From the above discussion, if $v \nmid l$, then α is trivial on an open subgroup of $Q_v \subset U_v$. As U_v is compact, Q_v has finite index in U_v, which means $\alpha(U_v)$ is finite. By choice of N, we see that $\alpha(U_v) = \{1\}$ for almost all v's. This further implies that ρ is unramified at almost all finite places, since U_v maps onto the inertia subgroup at v in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Thus, if we denote by X, the set of finite places v of K, such that $v \nmid l$, and ρ is ramified at v, then X is finite.

We showed that whenever $v \nmid l$, α is trivial on an open subgroup of K_v^*. Thus, we can find a modulus $\mathfrak{m}$ such that for all $v \in X$, α is trivial on $U_{v,\mathfrak{m}}$. Note that for $v \notin X$, v either divides l or ρ is unramified at v, i.e. $\alpha(U_v)$ is trivial. Since ρ is locally algebraic, we also have the equality $\rho \circ \theta_l(x) = f(x^{-1})$ for all x in an open neighborhood of unity in $\prod_{v|l} K_v^*$. Thus, by choosing a larger modulus $\mathfrak{m}$ if necessary, we can ensure that this equality holds for all $x \in U_{l,\mathfrak{m}} = \prod_{v|l} U_{v,\mathfrak{m}}$, which shows that ρ is defined mod $\mathfrak{m}$. □

3.3 Relation with the group $S_\mathfrak{m}$

Recall our discussion in the beginning of this chapter (15), where we ended up proving the following theorem:

Theorem 20. *The l-adic representation ϕ_l obtained from the group $S_\mathfrak{m}$, is locally algebraic and defined mod $\mathfrak{m}$, with ϕ_T (see 14) being the associated algebraic morphism.*

The converse of the above theorem is also true, showing that every Abelian l-adic representation arises from the construction laid out in chapter 2, for some group $S_\mathfrak{m}$. We shall prove the converse for rational representations.

Theorem 21. *Let $\rho : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Aut}(V_l)$ an Abelian l-adic representation of the number field K, which is rational and locally algebraic with $\mathfrak{m}$ as the modulus of definition. Then, there exists a rational vector subspace V_0 of V_l, with that $V_l = V_0 \otimes_\mathbb{Q} \mathbb{Q}_l$, an algebraic morphism $\phi_0 : S_\mathfrak{m} \to \mathrm{GL}_{V_0}$ defined over $\mathbb{Q}$, such that ρ is precisely the l-adic representation ϕ_l attached to ϕ_0 (in the sense of §2.6)*

Proof. Let $r : T_{\mathbb{Q}_l} \to \mathrm{GL}_{V_l}$ be the algebraic morphism associated to ρ. Let $\psi : \mathbb{I}_K \to \mathrm{Aut}(V_l)$ be the homomorphism given by

$$\psi(x) = \rho \circ \theta(x) \cdot r(x_l),$$

where x_l is the l-component of x. Since ρ is defined mod $\mathfrak{m}$, by the part (1) of definition (23), $\rho \circ \theta$ is trivial on $U_{v,\mathfrak{m}}$ for all $v \nmid l$, and by part (2), it coincides with $r(x^{-1})$ on $U_{l,\mathfrak{m}}$. Thus, on $U_\mathfrak{m} = \prod_v U_{v,\mathfrak{m}}$, $\rho \circ \theta$ is equal to $r(x_l^{-1})$, and hence ψ is trivial on $U_\mathfrak{m}$. Moreover, by class field theory, θ is trivial on K^*, and thus ψ coincides with r on K^*. We conclude that r is trivial on $K^* \cap U_\mathfrak{m}$ and induces the algebraic morphism $r_\mathfrak{m} : T_{\mathfrak{m},\mathbb{Q}_l} \to \mathrm{GL}_{V_l}$, by definition of the torus $T_\mathfrak{m}$ (refer to §2.4). Using the morphism $r_\mathfrak{m}$ and the map ψ, we invoke the universal property of $S_\mathfrak{m}$ (see (10). This gives us a unique algebraic morphism defined over $\mathbb{Q}_l$, which we denote by ϕ:

$$\phi : S_{\mathfrak{m},\mathbb{Q}_l} \to \mathrm{GL}_{V_l}.$$

If $\pi : T_{\mathfrak{m},\mathbb{Q}_l} \to S_{\mathfrak{m},\mathbb{Q}_l}$ denotes the morphism from (8) and $\epsilon : \mathbb{I}_K \to I_\mathfrak{m} \to S_\mathfrak{m}(\mathbb{Q}_l)$ the corresponding map from (9), it follows from the universal property that $r_\mathfrak{m} = \phi \circ \pi$ and $\phi \circ \epsilon : \mathbb{I}_K \to \mathrm{Aut}(V_l)$ is ψ.

Now, let ϕ_l be the l-adic representation attached to the above representation ϕ, and let $x \in \mathbb{I}_K$. Then, using the above properties and the maps defined in (12) and §2.6, it follows that

$$\begin{aligned} \phi_l \circ \theta(x) &= \phi \circ \epsilon_l(x) \\ &= \phi(\epsilon(x) \cdot \alpha_l(x^{-1})) \\ &= \phi(\epsilon(x))\phi(\alpha_l(x^{-1})) \\ &= \psi(x)\phi(\pi_l(x_l^{-1})) \\ &= \rho \circ \theta(x) r(x_l) \cdot r(x_l^{-1}) \\ &= \rho \circ \theta. \end{aligned}$$

As $\phi_l \circ \theta$ and $\rho \circ \theta$ agree on $\mathbb{I}_K$, passing on to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ using the class field isomorphism, we see that $\phi_l = \rho$. Finally, since ρ is a rational representation, the representation ϕ can be defined over $\mathbb{Q}$, by proposition (16). This gives us ϕ_0 and the vector space V_0, completing the proof. □

Corollary 22. *For each prime l', there exists an l'-adic representation $\rho_{l'}$ of K that is Abelain, rational, semi-simple and also compatible with ρ from theorem (21). This gives a strictly compatible system of representations $\{\rho_{l'}\}_{l'}$ and for an infinite number of primes l', $\rho_{l'}$ is diagonalizable over $\mathbb{Q}_{l'}$.*

Proof. The required representation is $\rho_{l'}$ is the l'-adic representation $\phi_{l'}$ attached to ϕ obtained in theorem (21). The remaining assertions follow from proposition (17). □

Remark. The representation $\rho_{l'}$ obtained above is in fact unique upto isomorphism for each prime l'. This follows from the theorem in ([9], chap. I, §2.3).

3.4 l-Adic Representations of Elliptic Curves

We now give a brief description of the l-adic representations associated to an elliptic curve E and state some important results in both cases: when E has *complex multiplication* (CM) and when E is non-CM. Such representations are always Abelian in the CM case, and surjective for almost all primes l in the non-CM case.

Preliminaries

Let E be an elliptic curve defined over the number field K and let $\mathrm{End}_K(E)$ denote its ring of endomorphisms defined over K. Since for any integer m, the *multiplication-by-m* map is an endomorphism of E, it follows that $\mathbb{Z} \subseteq \mathrm{End}_K(E)$. If $\mathrm{End}_K(E) \cong \mathbb{Z}$, we say E has no complex multiplication over K. If the endomorphism ring remains isomorphic to $\mathbb{Z}$ for all finite extensions of K, we say that E has no complex multiplication.

On the other hand, when $\mathrm{End}_K(E)$ is strictly larger than $\mathbb{Z}$, we say E has complex multiplication over K. If E has complex multiplication, then its endomorphism ring is an order[8] $\mathcal{R}_F$ in an imaginary quadratic field, say F (refer to corollary 9.4, chap. III, [10]). We say that E has complex multiplication by F over K.

Recall the l-adic representation associated to E discussed in example (2.2)

$$\rho_l : G \to \mathrm{Aut}(V_l(E)) \cong \mathrm{GL}_2(\mathbb{Q}_l). \tag{16}$$

Here, $G = \mathrm{Gal}(\overline{K}/K)$, $T_l(E)$ is the Tate module attached to E, and $V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is a two-dimensional vector space over $\mathbb{Q}_l$. Since any endomorphism $[\alpha] \in \mathrm{End}_K(E)$ is defined over K, it commutes with the action of G, which means

$$\sigma \cdot ([\alpha]P) = [\alpha](\sigma \cdot P),$$

for all $\sigma \in G$ and $P \in T_l(E)$. Now, let $\mathrm{End}_K(T_l(E))$ denote the ring of $\mathbb{Z}_l$-linear endomorphisms of $T_l(E)$ that commute with the action of G as prescribed by ρ_l. Then by [Thereom 7.4, chap. III, [10]], there is an injective homomorphism:

$$\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Z}_l \hookrightarrow \mathrm{End}_K(T_l(E)). \tag{17}$$

In his famous paper [3] Faltings proved the following results, known as the Tate conjectures:

Theorem 23 (Tate Conjectures). 1. *The representation ρ_l on $V_l(E)$ is semi-simple.*

2. *The map*

$$\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{End}_K(T_l(E))$$

is an isomorphism.

[8] An order $\mathcal{R}_F$ in a finitely generated $\mathbb{Q}$-algebra F, is a subring of F that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{R}_F \otimes_{\mathbb{Z}} \mathbb{Q} \cong F$.

Elliptic Curves with Complex Multiplication

If E has complex multiplication by F over K, then as mentioned before, $\mathrm{End}_K(E)$ is isomorphic to an order $\mathcal{R}_F$ in the imaginary quadratic field F. Let R_l denote the $\mathbb{Z}_l$-module $\mathcal{R}_F \otimes_{\mathbb{Z}} \mathbb{Z}_l$, and let F_l be the $\mathbb{Q}_l$-module $R_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Note that $F_l \cong \mathcal{R}_F \otimes_{\mathbb{Z}} \mathbb{Q}_l \cong F \otimes_{\mathbb{Q}} \mathbb{Q}_l$. Thus, (17) above tells us that $T_l(E)$ is an R_l-module, and hence, tensoring with $\mathbb{Q}_l$ gives a faithful F_l-module structure on $V_l(E)$. Since F is an imaginary quadratic field, F_l is a two-dimensional $\mathbb{Q}_l$-vector space, and so is $V_l(E)$. Thus, $V_l(E)$ is a free F_l-module of dimension one. Moreover, since this F_l-module structure on V_l commutes with the action of G as given by ρ_l, we see that ρ_l must be given by 1×1 invertible matrices, i.e. it can be written as a homomorphism:

$$\rho_l : G \to \mathrm{GL}_1(F_l) = F_l^*, \tag{18}$$

for a fixed basis of $V_l(E)$ over F_l. Since $\mathrm{GL}_1(F_l)$ is Abelian, the image $\rho_l(G)$ must also be Abelian, and hence ρ_l is an Abelian l-adic representation of K.

Let $T_F = \mathrm{Res}_{F/\mathbb{Q}}(\mathbb{G}_m)$ be the two-dimensional torus attached to F, so that $T_F(\mathbb{Q}_l) = F_l^*$ and ρ_l takes values in $T_F(\mathbb{Q}_l)$. Then, in [§2.8, chap. II, [9]], Serre proves the following theorem, proving in particular that ρ_l is locally algebraic:

Theorem 24. *Let K be a number field and E be an elliptic curve with complex multiplication over K. The system $\{\rho_l\}_l$ of l-adic representations attached to the elliptic curve E, is a strictly compatible system of Abelian rational l-adic representations of K with values in T_F. Moreover, there exists a modulus $\mathfrak{m}$ and an algebraic morphism $\phi : S_{\mathfrak{m}} \to T_F$, such that ρ_l is the composition of ϕ with the system of l-adic representations $\{\epsilon_l\}_l$ attached to $S_{\mathfrak{m}}$.*

This theorem, as shown by Serre, is true not just for elliptic curves with complex multiplication, but also for any Abelian variety with complex multiplication.

Elliptic Curves without Complex Multiplication

We saw in the previous section that for elliptic curves with complex multiplication, the representation ρ_l is Abelian, and in particular, can not be surjective. However, in the non-CM case, for almost all primes l, the image of ρ_l is surjective i.e., $\rho_l(G) = \mathrm{Aut}(T_l(E)) = \mathrm{GL}_2(\mathbb{Z}_l)$. Serre proves the following theorem in [Chap. IV, [9]]:

Theorem 25. *Let K be a number field and E an elliptic curve over K with no complex multiplication. Then the image $\rho_l(G)$ is an open subgroup in $Aut(T_l(E))$ and for almost all primes l, it is the whole set $Aut(T_l(E))$.*

Following Faltings' proof of the Tate conjectures, a modern proof of the above theorem can be found in [8].

References

[1] A. BOREL - *Linear Algebraic Groups (Second Enl. Edit.).* Graduate Texts in Mathematics, 1991.

[2] J. CASSELS and A. FRÖHLICH - *Algebraic Number Theory.* Academic Press Inc., 1967.

[3] G. FALTINGS - *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73**, 349-366, 1983. English translation by E. SHIPZ in *Arithmetic Geometry* edited by G. CORNELL and J. H. SILVERMAN. Springer-Verlag, 1986.

[4] S. LANG - *Algebra (Rev. 3rd Edit.).* Graduate Texts in Mathematics, Springer, 2002.

[5] S. LANG - *Algebraic Number Theory (Second Edition).* Graduate Texts in Mathematics, Springer, 1994.

[6] J. S. MILNE - *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field.* Cambridge University Press, 2017.

[7] B. POONEN - *Rational Points on Varities.* American Mathematical Society, 2017.

[8] K. A. RIBET - *Book Review: Abelian l-Adic Representations and Elliptic Curves.* Bulettin of the American Mathematical Society, Vol. 22, Issue 1, pp 214-219, 1990.

[9] J.-P. SERRE - *Abelian l-adic Representations and Elliptic Curves.* W. A. Benjamin, Inc., 1968.

[10] J. H. SILVERMAN - *The Arithmetic of Elliptic Curves (Second Edition).* Graduate Texts in Mathematics, Springer, 2009.

[11] A. WEIL - *Adèles and Algebraic Groups.* Birkhäuser Boston, 1982.

[12] A. WEIL - *Basic Number Theory.* Springer, 1974.