The Kronecker–Weber Theorem via Galois Deformations and Congruences Modulo p

Brian Hwang

To the memory of Jerrold Bates Tunnell (1950–2022).

ABSTRACT. We give a proof of the Kronecker–Weber theorem using the deformation theory of one-dimensional Galois representations associated with algebraic Hecke characters and corresponding "level-lowering" and "modularity lifting" theorems for such representations.

CONTENTS

1. INTRODUCTION

One of the first definitive results in what we now know as class field theory is the Kronecker–Weber theorem, which is commonly stated as follows.

Theorem 1.1. *(Kronecker–Weber) Any finite abelian extension of $\mathbf{Q}$ is contained in a cyclotomic extension of $\mathbf{Q}$.*

There exist a multitude of proofs of the result, from strictly elementary treatments (e.g. [Mar77, Exer. 4.29–38]) to ones that derive it from the statements of class field theory, either local or global. (See [Neu81, §6] for a historical overview and references to a number of different proofs, and [Sch98, §2] for some additional context.) However, our approach—using the deformation theory of Galois representations and an appropriate "R = T" theorem obtained by comparing numerical invariants from commutative algebra—does not yet seem to exist in the literature. It is not the

most direct proof and far from the shortest, but it turns out to be natural in many ways. Indeed, the key steps follow from one-dimensional analogues of the results needed for the modularity theorem (a.k.a. Taniyama–Shimura–Weil conjecture) for semistable elliptic curves over $\mathbf{Q}$ as proved by Wiles [Wil95] and Taylor–Wiles [TW95] towards a proof of Fermat's Last Theorem. So in a concrete sense, not only is the modularity theorem a "higher Kronecker–Weber theorem," but we can also adapt its method of proof to reprove the classical result.

With this in mind, we reformulate the Kronecker–Weber theorem in the following fashion, which resembles the L-function form of the modularity theorem for elliptic curves over $\mathbf{Q}$ [BCDT01].

Theorem 1.2. *Let K be an abelian extension of $\mathbf{Q}$ with Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Given a continuous representation $\rho : G \to \mathrm{GL}_1(\mathbf{C})$, there exists a unique primitive Dirichlet character χ such that*

$$L(\rho, s) = L(\chi, s).$$

(See §6.2 for details and how this implies Theorem 1.1.) To prove Theorem 1.2, we show that for any such character ρ, its corresponding representation of the absolute Galois group $G_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is "modular," in the sense that it is associated with an algebraic Hecke character—the one-dimensional or abelian analogue of the Hecke eigenforms that are associated with elliptic curves over $\mathbf{Q}$ in the modularity theorem.

The main technical result required for our proof of Theorem 1.2 is the following one-dimensional version of a theorem of Ribet [Rib90], which essentially says that the property of being modular is preserved under congruences modulo p ("modularity is contagious") and can be viewed as "modularity lifting theorem" in this context. The bulk of the paper is devoted to making the relevant notions precise and in assembling the ingredients required for its proof.

Theorem 1.3. *Let $(\mathcal{O}, \mathfrak{m}_{\mathcal{O}})$ be a complete noetherian local ring with finite residue field $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}$ and let $\rho_0 : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O})$ be a Galois representation that is modular, in other words, $\rho_0 \cong \rho_{\chi_0}$ for some algebraic Hecke character χ_0 (see Proposition 2.8; in particular, this implies that $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbf{Q}_p$). If*

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O})$$

is any Galois representation such that its residual representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}/\mathfrak{m}_{\mathcal{O}})$ is isomorphic to the residual representation $\overline{\rho_0} : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}/\mathfrak{m}_{\mathcal{O}})$ of ρ_0, then ρ is also modular.

Theorem 1.3 is used to "eliminate primes from the level," allowing for an induction argument on the set of ramified primes in our abelian extension of $\mathbf{Q}$. Once we have applied Theorem 1.3, we are reduced to analyzing certain classes of deformations of these *modular* residual Galois representations, where we can appeal to some general results in algebra that are used to address the analogous questions

for two-dimensional Galois representations. The theory simplifies considerably in the one-dimensional setting; many of the intermediary results can be given bare-handed proofs, in contrast to those in the two-dimensional setting, which often require deep inputs from Galois cohomology or the geometry of Shimura curves. This has the pleasing consequence of making our entire argument more or less self-contained—including the deformation-theoretic aspects—with the sole exceptions being a couple of results from commutative algebra (§4.4) that we quote for the sake of brevity, as they are not simplified by specializing to GL_1. To avoid any chance of a circular argument, we take pains to avoid relying on any general results from class field theory, only using a simple statement from Kummer theory (Theorem 5.3) that we need as an input from the theory of cyclotomic fields. (For a proof of the Kronecker–Weber theorem via generalized Selmer groups that *does* use class field theory, see [CSS97, IV, §5, p.112-3].) In particular, we do not make use of the Poitou–Tate exact sequence or cohomological duality theorems, which are crucial for the corresponding proofs of the theorems for two-dimensional Galois representations.

Like many number-theoretic results, proofs of the Kronecker–Weber theorem require special considerations at the prime $p = 2$, with the case of extensions of $\mathbf{Q}$ with degree a power of two being tricky to address and a notorious source of errors in both initial attempts at a proof (see, e.g. [Neu81, §4–5]) as well as in potential generalizations (see, e.g. [Sch98, §3]). Our deformation-theoretic approach is no exception to this rule, and we deal with the $p = 2$ case in each result where the assumption plays a role. Our input from local fields (Lem. 5.1) also requires us to separate these two cases, due to the different structure of the p-extensions of $\mathbf{Q}_p$. However, encoding this separation in general lemmas allows us to treat all primes uniformly in our culminating argument.

One motivation for pursuing this kind of proof of the Kronecker–Weber theorem is that the objects involved tend to generalize better to number fields other than $\mathbf{Q}$. Indeed, the naive generalization of the Kronecker–Weber theorem in its classical form (Theorem 1.1) to number fields beyond $\mathbf{Q}$ is false; the abelian extensions of even a quadratic extension of $\mathbf{Q}$ are not necessarily contained in a cyclotomic extension (e.g. the extension $\mathbf{Q}(\sqrt[4]{2})$ over $\mathbf{Q}(\sqrt{2})$). However, generalizations of the statement of Theorem 1.2 are more robust. Of course, any such generalizations of Theorem 1.1 and 1.2 require care in establishing *relations* between them. At several crucial points, the arguments establishing the connection in the case of $\mathbf{Q}$ in §6.2—and importantly, certain key lemmas for our main argument and Theorem 1.3—rely on certain facts that are special to $\mathbf{Q}$. Many of the difficulties in generalizing the Kronecker–Weber theorem are well-known and long-standing. Importantly, aside from the case of CM-fields, which can be approached with the theory of complex multiplication, it is still unknown what class of extensions of the base field (analogous to the cyclotomic fields for $\mathbf{Q}$) are required to contain all

the abelian extensions, even for the case of real quadratic extensions (cf. Hilbert's 12th problem or Kronecker's *Jugendtraum*). However, some recent advances in the subject also rely on inputs from automorphic forms and Galois representations extending the results of Ribet [Rib90] as well as novel p-adic methods, especially in the case of totally real fields (see, e.g. [DK22] for a recent survey). Do such thematic reprisals point to a potential summit or merely indicate a scenic vista at which to collect ourselves for a more arduous journey? Only time will tell.

$\mathrm{GL}_2(\mathbf{Q})$	$\mathrm{GL}_1(\mathbf{Q})$
modularity theorem	Kronecker–Weber theorem
Hecke eigenform	algebraic Hecke character
level $N \geq 1$	conductor $N \geq 1$
weight 2	weight 0
modular curve $X_0(N)$	$(\mathbf{Z}/N\mathbf{Z})^\times \simeq \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q})$
its Jacobian $J_0(N)$	$(\mathbf{Z}/N\mathbf{Z})^\times \simeq \mathbf{G}_m(\mathbf{Z}/N\mathbf{Z})$
Hecke algebra $\mathbb{T}_N \subset \mathrm{End}(J_0(N))$	the group ring $\mathcal{O}[\![(\mathbf{Z}/N\mathbf{Z})^\times]\!]$

FIGURE 1. Analogous objects in the $\mathrm{GL}_2(\mathbf{Q})$ and $\mathrm{GL}_1(\mathbf{Q})$ cases.

"Surely this must be written down somewhere...". The fact that a "GL_1-version of the modularity theorem" would lead to the Kronecker–Weber theorem seems to have long been a part of the folklore, but the only concrete reference we could find was a passing remark of Kowalski [Kow03, Rem. 5.4] that refers to a Rutgers University graduate course taught by Tunnell in academic year 1995–1996. We dedicate this article to Jerry's memory. (May our cycles continue to spin, far beyond the Finger Lakes.) We hope that our streamlined presentation at least improves upon the argument's accessibility.

In the years following the proof of Fermat's Last Theorem, there have been a number of references summarizing and elucidating various aspects of the argument. We recommend [DDT94] and [CSS97] for comprehensive treatments and elaborations of the themes that we touch upon here, and [Dar95] and [DI95] in particular among the abridged treatments, as they take useful perspectives and highlight connections that are less emphasized in the longer works above but were useful in making clear the analogies between the GL_2 and GL_1 cases (Fig. 1) that guide our approach.

2. Algebraic Hecke characters over $\mathbf{Q}$

The "modular" or "automorphic" objects that we wish to associate with our one-dimensional Galois representations are the algebraic Hecke characters (a.k.a. Grossencharacters of type (A_0) [Wei56]) over $\mathbf{Q}$, which are often studied today as

the algebraic automorphic representations for GL_1 over $\mathbf{Q}$. (The modular forms of weight 2 associated with elliptic curves over $\mathbf{Q}$ correspond to certain algebraic automorphic representations of GL_2 over $\mathbf{Q}$.) As we do not require the additional flexibility of the adelic formulation for our argument, we give a treatment in the classical idèlic language, following [Del77, Ch. 6, §5], specialized to the case of $\mathbf{Q}$. We are primarily interested in the conductor of an algebraic Hecke character and its behavior under congruences, and the relevant phenomena are more concrete when phrased in terms of the idèles.

2.1. **Definition and classification of algebraic Hecke characters over Q.** Let E be a number field, $N \geq 1$ an integer (equivalently, a ideal of $\mathbf{Z}$), and $T = \sum n_\sigma \sigma \in \mathbf{Z}[\mathrm{Hom}(\mathbf{Q}, \overline{E})]$ a $\mathbf{Z}$-linear combination of embeddings of $\mathbf{Q}$ into a fixed choice of algebraic closure $\overline{E}$ for E.

Definition 2.1. Let I_N denote the group of fractional ideals of $\mathbf{Z}$ (a.k.a. ideals of $\mathbf{Q}$) that are prime to N. An **E-valued algebraic Hecke character χ (over $\mathbf{Q}$) of infinity-type T and conductor dividing** N is a group homomorphism

$$\chi : I_N \to E^\times,$$

with the following property: for any principal ideal $(\alpha) \in I_N$ generated by an $\alpha \in \mathbf{Q}^\times$ such that $\alpha \equiv 1 \pmod{N}$, we have

$$\chi((\alpha)) = \alpha^T = \prod_\sigma (\alpha^\sigma)^{n_\sigma} = \alpha^m \tag{2.2}$$

for a fixed integer $m \in \mathbf{Z}$.

We note, in particular, that the choice of infinity-type T of an algebraic Hecke character is equivalent to the choice of $m \in \mathbf{Z}$ in this setting.

Remark 2.3. Definition 2.1 is equivalent to the notion that the corresponding automorphic representation of $\mathrm{GL}_1(\mathbf{Q})$ is algebraic—indeed, it is the case that inspired the definition [Clo90]. It is also equivalent to the condition that the corresponding Galois representation (see Prop. 2.8) is de Rham at the prime equal to the residue characteristic.

If $N \mid N'$, the characters of conductor dividing N can be identified with the corresponding characters of conductor dividing N' under the restriction to $I_{N'} \subseteq I_N$. The smallest N (with respect to ordering by divisibility) such that χ extends to a character of conductor dividing N is called the **conductor of** χ, which we denote by $N(\chi)$. A Hecke character χ of conductor dividing $N(\chi)$ is said to be **primitive**.

Remark 2.4. It is traditional to denote the conductor of a Hecke character by $\mathfrak{f}$ (for the German term *Führer*), but we use N (for the French term *niveau*) so as to more closely reflect the notation and analogy with the *level* of a modular form and its Galois representation.

While we do not describe general Hecke characters, as non-algebraic Hecke characters play no role in our argument, it is worth noting that whether a Hecke character is algebraic or not depends only on its infinity-type T; the integer N plays no role in algebraicity. Namely, in the context of Hecke characters over $\mathbf{Q}$, being algebraic means that the corresponding m in condition (2.2) is an *integer* and not, say, an arbitrary real or complex number. The seemingly innocent "integral" property of the infinity-type yields some significant consequences.

For example, all algebraic Hecke characters χ satisfy a strong homogeneity condition: for any embedding $\overline{E} \hookrightarrow \mathbf{C}$, we have an induced action of complex conjugation $^-$ on $\mathrm{Hom}(\mathbf{Q}, \overline{E})$ and for any $\sigma \in \mathrm{Hom}(\mathbf{Q}, \overline{E})$[1], we have

$$n_\sigma + n_{\overline{\sigma}} = k \in \mathbf{Z},$$

where k is called the **weight of** χ (or more precisely, of its infinity type T). Thus, for any complex conjugation on $\overline{E}$, we have

$$\chi \cdot \overline{\chi} = \mathfrak{N}^k,$$

where $\mathfrak{N}$ is the norm, that is, $\mathfrak{N}(\mathfrak{a}) = \#(\mathbf{Z}/\mathfrak{a})$ for any integral ideal $\mathfrak{a}$ of $\mathbf{Q}$ (i.e. ideal of $\mathbf{Z}$). Hence, the values of an algebraic Hecke character are *pure*, in the sense that all its embeddings into $\mathbf{C}$ have the same absolute value.

To illustrate these more abstract concepts, we describe the two "extremal" cases of algebraic Hecke characters.

Example 2.5. Dirichlet characters are the ur-examples of algebraic Hecke characters and the source of much of the terminology. Any Dirichlet character (i.e. group homomorphism) $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ can be viewed as an algebraic Hecke character of weight 0 and conductor dividing N, and vice versa. If the Dirichlet character χ is primitive, then $N(\chi) = N$.

Example 2.6. The norm character $\mathfrak{N}$ is itself an algebraic Hecke character of conductor $N(\mathfrak{N}) = 1$.

Algebraic Hecke characters of finite order are precisely those with trivial infinity-type (equivalently, weight $k = 0$). In particular, this implies that every algebraic Hecke character χ over $\mathbf{Q}$ is of the form

$$\chi = \mu \cdot \mathfrak{N}^r$$

where μ is of finite order and $r \in \mathbf{Z}$. (Over nontrivial extensions of $\mathbf{Q}$, the classification is not as simple, so this is already one place where working over $\mathbf{Q}$ makes things easier.) This factorization of algebraic Hecke characters over $\mathbf{Q}$ is useful almost everywhere they appear. Using the identification between finite-order characters and Dirichlet characters, we write $\mu = \chi_{\mathrm{Dir}}$ for this "finite order part" of χ, where $\chi_{\mathrm{Dir}} : (\mathbf{Z}/N(\chi)\mathbf{Z})^\times \to \mathbf{C}^\times$ is the corresponding Dirichlet character.

[1] Again, there is really just one here, but we maintain this distinction for the sake of clarity.

The field of values of an algebraic Hecke character is a finite extension L_χ of $\mathbf{Q}$. Indeed, L_χ is either $\mathbf{Q}$ or a CM field; this property also leads to interesting arithmetic phenomena, but such properties don't play a role in the proof of our main theorem, so we content ourselves with this passing remark.

2.2. **Attaching λ-adic Galois representations to algebraic Hecke characters over $\mathbf{Q}$.** Let χ be an algebraic Hecke character over $\mathbf{Q}$, so it is of the form

$$\chi = \chi_{\mathrm{Dir}} \cdot \mathfrak{N}^r, \tag{2.7}$$

where χ_{Dir} is a Dirichlet character of conductor N, where $\mathfrak{N}$ is the norm character, and $r \in \mathbf{Z}$. Let $L = L_\chi$ be the number field generated by the values of χ.

The following result is the main route through which we pass from objects on the "modular" (a.k.a. "automorphic") side to those on the "Galois" side. In our main argument towards the proof of Theorem 1.3, we are primarily interested in the completions of L at primes dividing our fixed choice of residue characteristic p, but the construction is insensitive to the primes in question, so we state it in this more general form.

Proposition 2.8. *Let χ be an algebraic Hecke character over $\mathbf{Q}$. Given a prime ideal λ of the ring of integers $\mathcal{O}_L$ of $L = L_\chi$, there exists a one-dimensional λ-adic Galois representation*

$$\rho_{\chi,\lambda} : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda})$$

where $\mathcal{O}_{L,\lambda}$ denotes the completion of $\mathcal{O}_L$ at λ, with the following property: for all but finitely many rational primes q, we have

$$\rho_{\chi,\lambda}(\mathrm{Frob}_q) = \chi_{\mathrm{Dir}}(q)\mathfrak{N}(q)^r,$$

where Frob_q denotes a Frobenius element for q, and where we write $\chi = \chi_{\mathrm{Dir}} \cdot \mathfrak{N}^r$ by (2.7).

Proof. Case 1 (Finite order). Suppose that $\chi = \chi_{\mathrm{Dir}}$ is a Dirichlet character of conductor N. Then we have a series of maps

$$G_{\mathbf{Q}} \twoheadrightarrow (\mathbf{Z}/N\mathbf{Z})^\times \xrightarrow{\chi} \mathcal{O}_L^\times \hookrightarrow L^\times \hookrightarrow L_\lambda^\times$$

and so define $\rho_{\chi,\lambda} : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda})$ to be the composition of all of these maps. Note that for almost all primes q—namely, those that do not divide N—we have

$$\rho_{\chi,\lambda}(\mathrm{Frob}_q) = \chi(q).$$

Case 2 (Norm). Suppose that $\chi = \mathfrak{N} = |\cdot|$ the norm map, which has $L = L_\chi = \mathbf{Q}$. Pick a prime ℓ of $\mathcal{O}_L = \mathbf{Z}$. Since the norm character is of infinite order, it does not correspond to any Dirichlet character. Instead, we associate with $\mathfrak{N}$ the *ℓ-adic cyclotomic character*

$$\chi_\ell : G_{\mathbf{Q}} \to \mathbf{Z}_\ell^\times, \tag{2.9}$$

which is defined by mapping $\sigma \in G_{\mathbf{Q}}$ to the inverse system

$$(a_\sigma(n))_{n\geq 1} \in \varprojlim_n (\mathbf{Z}/\ell^n\mathbf{Z})^\times \cong \mathbf{Z}_\ell^\times$$

where $a_\sigma(n)$ is defined as the element satisfying

$$\sigma(\zeta_{\ell^n}) = \zeta_{\ell^n}^{a_\sigma(n)}$$

for ζ_{ℓ^n} a compatible choice of primitive ℓ^n-th root of unity for all n. It has the property that $\chi_\ell(\mathrm{Frob}_q) = q = \mathfrak{N}(q)$ for any prime $q \neq \ell$. So $\rho_{\mathfrak{N},\ell} = \chi_\ell$.

General case. We have $\chi = \chi_{\mathrm{Dir}} \cdot (\mathfrak{N})^r$ and consider the Galois representation $\rho_\chi : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda})$ defined by $\rho_\chi = \rho_{\chi_{\mathrm{Dir}}}(\rho_{\mathfrak{N}})^r$. Then for almost all primes q, we have $\rho_{\chi,\lambda}(\mathrm{Frob}_q) = \chi_{\mathrm{Dir}}(q)\mathfrak{N}(q)^r$. □

Given a Galois representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda})$, its kernel $\mathrm{Ker}(\rho)$ is an open subgroup of $G_{\mathbf{Q}}$ and it is natural to study the ramification of primes in the corresponding fixed field $\overline{\mathbf{Q}}^{\mathrm{Ker}(\rho)}$, which is a number field. A Galois representation ρ is said to be *ramified* at a prime q if its inertia subgroup I_q at q acts nontrivially. Note that a prime q ramifies in $\overline{\mathbf{Q}}^{\mathrm{Ker}(\rho)}$ if and only if ρ is ramified at q.

By the construction given in the proof of Proposition 2.8, we immediately obtain the following result, which we will refer to later.

Corollary 2.10. *If q is a prime at which $\rho_{\chi,\lambda}$ is ramified, then $q \mid \ell N$, where N is the conductor of the Dirichlet character χ_{Dir} and ℓ is the rational prime under λ (i.e. $\lambda \mid \ell$).*

3. Modular one-dimensional representations of $G_{\mathbf{Q}}$ and congruences

If $\rho : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda})$ is a Galois representation such that $\rho \cong \rho_\chi$ for some algebraic Hecke character χ (as in Proposition 2.8), we say that ρ is **modular** (or **automorphic**). Modular one-dimensional Galois representations are distinguished from general one-dimensional Galois representations by certain special properties, such as strong conditions on the values of ρ under Frobenius (Proposition 2.8, which can be interpreted as a purity property) and the restrictions on ramification (Proposition 2.10). Indeed, these two conditions also turn out to be essentially *sufficient* for modularity, as the Fontaine–Mazur conjecture holds for GL_1 over general number fields (see e.g. [Far06, §8]), but our argument does not require this fact. Alternatively, there is a characterization of algebraic Hecke characters in terms of Galois-theoretic data due to Taniyama [Tan57, §1.2].

Since we are pursuing a deformation-theoretic approach to deduce modularity, we are most interested in how the property of modularity behaves *under congruences*, and so we prove two results in this vein: a level-lowering result and our main technical result, which says that modularity for one-dimensional Galois representations is preserved under congruences.

3.1. **Level-lowering for modular one-dimensional Galois representations.** The *level* of a modular one-dimensional Galois representation ρ_χ is the conductor of the corresponding (primitive) Hecke character χ. While level-lowering results are usually stated in terms of Galois representations, in the one-dimensional setting, there is little distinction between an algebraic Hecke character and its associated Galois representation, in contrast to the case of modular forms. Thus, we phrase the main lemma (Lem. 3.5) in terms of the conductors of the algebraic Hecke characters as it leads to more direct arguments.

Before we state the result and give its proof, however, we give an example of the kind of behavior under congruences that we are trying to characterize.

Example 3.1. Let ℓ be an odd prime and consider the Dirichlet character

$$\chi := \chi_{c,\ell} : (\mathbf{Z}/\ell\mathbf{Z})^\times \to \mathbf{C}^\times$$

defined by mapping a generator of $(\mathbf{Z}/\ell\mathbf{Z})^\times$ to the primitive ℓ-th root of unity $e^{2\pi i/\ell} = \zeta_\ell$. Despite χ being a Dirichlet character, observe that, conceptually, this is also a choice for the first stage of the construction of the ℓ-adic cyclotomic character (2.9), albeit with values in $\mathbf{C}^\times = \mathrm{GL}_1(\mathbf{C})$. We can view the λ-adic Galois representation associated with χ as taking values in the invertible elements of a completion of the ring of integers $\mathbf{Z}[\zeta_\ell]$ of the ℓth cyclotomic extension $\mathbf{Q}(\zeta_\ell)$ of $\mathbf{Q}$, that is,

$$\rho_\chi : G_\mathbf{Q} \to \mathrm{GL}_1(\mathbf{Z}[e^{2\pi i/\ell}]_\lambda), \tag{3.2}$$

reminding ourselves that ρ_χ factors through $(\mathbf{Z}/\ell\mathbf{Z})^\times$. We want to exhibit a congruence between ρ_χ at a prime $\lambda \mid \ell$ and the ℓ-adic cyclotomic character $\chi_\ell = \rho_\mathfrak{N} : G_\mathbf{Q} \to \mathrm{GL}_1(\mathbf{Z}_\ell)$ (2.9).

The prime ℓ is totally ramified in $\mathbf{Q}(\zeta_\ell)$, so $\ell = (\lambda)^{\ell-1}$ in $\mathbf{Z}[\zeta_\ell]$ and thus $\mathbf{Z}[\zeta_\ell]_\lambda \cong \mathbf{Z}_\ell$. Recall that there exists the Teichmüller lift (a.k.a. Teichmüller character) at ℓ:

$$\omega : (\mathbf{Z}/\ell\mathbf{Z})^\times \hookrightarrow \mathbf{Z}_\ell^\times \tag{3.3}$$

where the value $\omega(x)$ is defined to be the unique solution of $\omega(x)^\ell = \omega(x)$ that is congruent to x modulo ℓ; it is the unique multiplicative section of the surjection $r_\ell : \mathbf{Z}_\ell^\times \to (\mathbf{Z}/\ell)^\times$ given by reduction modulo ℓ. This splitting of the reduction map allows us to identify $(\mathbf{Z}/\ell\mathbf{Z})^\times \cong \mathbf{F}_\ell^\times$ with the $(\ell-1)$th roots of unity of $\mathbf{Z}_\ell^\times$. Therefore, the mod ℓ reductions $\overline{\rho_\chi} = r_\ell \circ \rho_\chi$ and $\overline{\rho_\mathfrak{N}} = r_\ell \circ \rho_\mathfrak{N}$ are the same canonical map $\mathbf{Z}_\ell^\times \to (\mathbf{Z}/\ell\mathbf{Z})^\times$ once the latter is identified with the $(\ell-1)$th roots of unity, so ρ_χ and $\rho_\mathfrak{N}$ are congruent modulo ℓ.

The level of ρ_χ is $N(\chi) = \ell$, as χ is a primitive Dirichlet character, but its mod ℓ residual representation $\overline{\rho_\chi}$ is not ramified at ℓ, and so happens to be congruent to the Galois representation $\rho_\mathfrak{N}$ of level $N(\mathfrak{N}) = 1$ (Example 3.1) modulo ℓ. $\diamond$

Remark 3.4. The same argument works for $\ell = 2$ with the Dirichlet character $\chi_{c,2} : (\mathbf{Z}/4\mathbf{Z})^\times \to \mathbf{C}^\times$, as the Teichmuüller lift at 2 is given by $\omega : (\mathbf{Z}/4\mathbf{Z})^\times \hookrightarrow \mathbf{Z}_2^\times \cong \{\pm 1\} \times (1 + 4\mathbf{Z}_2)$.

We want to codify this kind of phenomenon into a general level-lowering result. The basic idea is that if a prime dividing the level of a modular Galois representation ρ_χ becomes unramified upon passing to the residual representation $\overline{\rho_\chi}$, this should be witnessed by a congruence between ρ_χ and *another* modular Galois representation $\rho_{\chi'}$ where the prime does not divide the conductor $N(\chi')$ of χ'.

Lemma 3.5. *Let χ be an algebraic Hecke character over $\boldsymbol{Q}$ of conductor N and weight k with values in $L = L_\chi$. Given a prime $\lambda \mid \ell$ of $\mathcal{O}_L$ such that its corresponding residual representation*

$$\overline{\rho_\chi} : G_Q \to GL_1(\mathcal{O}_{L,\lambda}/\lambda\mathcal{O}_{L,\lambda})$$

is unramified at a prime $q \mid N$, there exists an algebraic Hecke character χ' of conductor N' and weight $k' = k$ such that $q \nmid N'$ and $\overline{\rho_{\chi'}} \cong \overline{\rho_\chi}$.

Moreover, if $\overline{\rho_\chi}$ is unramified at $q = \ell$, where ℓ is the characteristic of the field $(\mathcal{O}_{L,\lambda}/\lambda\mathcal{O}_{L,\lambda})$, we can take χ' to be a Dirichlet *character (i.e. weight 0) of conductor M where $q \nmid M$.*

Proof. We prove our result by constructing such a χ' in the two contrasting cases for a prime $q \mid N$: when $q \neq \ell$ and when $q = \ell$.

Case 1 (Away from ℓ). Suppose that $q \neq \ell$. The norm character $\mathfrak{N}$ does not have ramification at q and the cyclotomic character $\rho_{\mathfrak{N}} \cong \chi_\ell$ is not ramified at q. Thus, the residual representation $\overline{\rho_{\chi_{\mathrm{Dir}}}}$ obtained by taking the mod λ reduction must be unramified at q, by our hypotheses. We have a decomposition

$$\mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^\times \cong (\mathbf{Z}/q^r\mathbf{Z})^\times \times (\mathbf{Z}/N'\mathbf{Z})^\times$$

for some $r, N' \in \mathbf{N}$ with $\gcd(q, N') = 1$. As $\overline{\rho_{\chi_{\mathrm{Dir}}}}$ is unramified at q, we must have

$$\eta := \chi_{\mathrm{Dir}}|_{(\mathbf{Z}/q^r\mathbf{Z})^\times} \equiv 1 \pmod{\lambda}, \tag{3.6}$$

that is, η is an $\mathcal{O}_{L,\lambda}$-valued Dirichlet character of conductor dividing q^r whose reduction modulo λ is trivial.

Consider the algebraic Hecke character

$$\chi' = \chi\eta^{-1}.$$

We have $\overline{\rho_\chi} = \overline{\rho_{\chi'}}$ by (3.6) and χ' is of conductor N/q^r. As Dirichlet characters are of weight 0 (Example 2.5), we see that the weight of χ' is $k' = k$.

Case 2 (At ℓ). Suppose that $q = \ell$. We prove this in two steps.

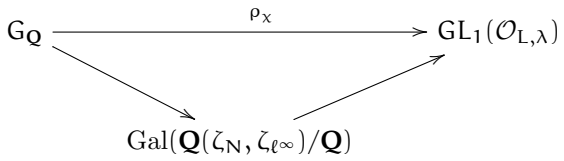
Case 2(a) (Congruent to trivial). The simple sub-case is when we can proceed as in Example 3.1. Let ℓ be an odd prime. Consider $\chi = \mathfrak{N}\chi_{c,\ell}^{-1}$ where $\chi_{c,\ell} : (\mathbf{Z}/\ell\mathbf{Z})^\times \to \mathbf{C}^\times$ is as in (3.2). We have the injection $(\mathbf{Z}/\ell\mathbf{Z})^\times \hookrightarrow \mathbf{Z}_\ell^\times$ given by the Teichmüller lift. The conductor of χ is ℓ, but $\overline{\rho_\chi}$ is unramified at ℓ, so it follows that

$$\rho_\chi \cong \rho_{\chi'} \pmod{\lambda}$$

where χ' is the trivial character, which has conductor 1 and weight 0.

When $\ell = 2$, we proceed in the same way, but as the Teichmüller lift is given by $\omega : (\mathbf{Z}/4\mathbf{Z})^\times \hookrightarrow \mathbf{Z}_2^\times$ instead of from $\mathbf{Z}/\ell\mathbf{Z}$, the conductor of χ is 4 and not 2. However, the conclusion remains unchanged.

Case 2(b) (General case at ℓ). We have $\rho_\chi : G_\mathbf{Q} \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda})$ such that $\overline{\rho_\chi} : G_\mathbf{Q} \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda}/\lambda)$ is unramified at ℓ. By construction (Proposition 2.8), we have $\rho_\chi = \rho_{\chi_{\mathrm{Dir}}} \cdot \rho_\mathfrak{N}^r$ and so ρ_χ admits a factorization:



through the Galois group of the compositum of the cyclotomic fields $\mathbf{Q}(\zeta_N)$ and $\mathbf{Q}(\zeta_{\ell^\infty})$. By reducing modulo λ, we get

$$\overline{\rho_\chi} : G_\mathbf{Q} \to \mathrm{GL}_1(\mathbf{F}),$$

where $\mathbf{F} \cong \mathcal{O}_{L,\lambda}/\lambda\mathcal{O}_{L,\lambda}$ is a field of characteristic ℓ, and so $\mathrm{GL}_1(\mathbf{F}) = \mathbf{F}^\times$ has order prime to ℓ.

In the mod λ reduction, the ℓ-part is killed by an ℓ-group, and since $\overline{\rho_\chi}$ is unramified at ℓ and the ℓ-adic cyclotomic character $\chi_\ell \cong \rho_\mathfrak{N}$ is ramified at ℓ, we must have

$$\chi\big|_{(\mathbf{Z}/\ell^{\nu_\ell(N)}\mathbf{Z})^\times} \equiv \chi_\ell^{-r} \pmod{\lambda},$$

where $\ell^{\nu_\ell(N)}$ is the highest power of ℓ to divide $N = N(\chi)$ (i.e. $\nu_\ell(N)$ is the ℓ-adic valuation of N). Consider the algebraic Hecke character

$$\chi' = \chi_{\mathrm{Dir}}(\chi_{\mathrm{Dir}}\big|_{(\mathbf{Z}/(\ell^{\nu_\ell(N)}\mathbf{Z}))^\times})^{-1}$$

of conductor $N' = N/\ell^{\nu_\ell(N)}$, noting that $\rho_{\chi'}$ is unramified at ℓ. We calculate that the mod λ residual representations coincide:

$$\overline{\rho_{\chi'}} \cong \overline{\rho_{\chi_{\mathrm{Dir}}}} \cdot \overline{\rho_{\chi_{\mathrm{Dir}}\big|_{(\mathbf{Z}/(\ell^{\nu_\ell(N)}\mathbf{Z}))^\times}}}^{-1} \cong (\overline{\rho_{\chi_{\mathrm{Dir}}}} \cdot \overline{\rho}_\mathfrak{N}^r) \cong \overline{\rho_\chi}.$$

We conclude that χ' can be taken to be a Dirichlet character of level $N/\ell^{\nu_\ell(N)}$ and thus of weight 0. □

Remark 3.7. In effect, repeated applications of Lemma 3.5 allows us to remove primes from the level via congruences. But how far can this result take us? Determining the *minimal* level of a general modular Galois representation—that is, the smallest level among all the Galois representations in the equivalence class of ρ under the relation of congruences modulo all possible primes—is connected to a number of rich arithmetic phenomena and exhibits a number of subtleties that make it difficult to calculate explicitly. For example, a naive approach would require looking at congruences modulo all possible primes! But in the GL_1 case, there is an interpretation that is highlighted our proof of the Kronecker–Weber theorem (§6.1). In this context, determining the minimal level of a ρ_χ is equivalent

to determining the *smallest* N such that the associated finite abelian extension of $\mathbf{Q}$ is contained in the cyclotomic field $\mathbf{Q}(\zeta_N)$.

3.2. **Modularity for one-dimensional Galois representations is contagious.** Let $\rho_0 : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda})$ be a modular Galois representation, so $\rho_0 \cong \rho_{\chi_0}$ for an algebraic Hecke character χ_0 of some conductor N_0. Write $\overline{\rho_0} : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda}/\lambda)$ for its corresponding residual representation.

We want to prove the following result, which can be viewed as a modularity lifting theorem for one-dimensional Galois representations.

Theorem 3.8. *Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}_{L,\lambda})$ be an arbitrary Galois representation such that its residual representation $\overline{\rho} \cong \overline{\rho_0}$. Then ρ is modular, that is, there exists an algebraic Hecke character χ such that $\rho \cong \rho_\chi$.*

To prove this result, we develop the deformation theory of one-dimensional Galois representations that are modular, taking care to remember the weight and conductor of the corresponding algebraic Hecke characters.

4. The deformation theory of modular Galois characters

The deformation theory of one-dimensional Galois representations when no conditions are imposed on the deformations is simple: since any one-dimensional residual representation $\overline{\rho}$ of $G_{\mathbf{Q},S}$ is projectively equivalent to another, the corresponding universal deformation ring only depends on the residue field k (and not a specific $\overline{\rho}$), and it is not hard to show—as the existence of the Teichmüller lift (3.3) essentially reduces the argument to the trivial case—that this deformation ring is isomorphic to $W(k)[\![G_{\mathbf{Q},S}^{\mathrm{ab},p}]\!]$, the completed group ring of the abelianized p-completion of $G_{\mathbf{Q},S}$ with coefficients in the ring of Witt vectors $W(k)$ [Maz89, §1.4]. Thus, the difficulty is not in *finding* deformations—as they exist in abundance—but rather being able to select for ones that are *modular*, which necessitates the more delicate developments of this section.

For the proof of Theorem 1.2, the main arithmetic objects to understand are the *primes at which a modular Galois representation ρ_χ is ramified*. Ultimately, this is because we need to show that the number field $\overline{\mathbf{Q}}^{\mathrm{Ker}(\rho_\chi)}$ cut out by ρ_χ is contained in some cyclotomic field, and cyclotomic fields have tightly controlled ramification behavior. As it is only the finite-order Dirichlet part χ_{Dir} of an algebraic Hecke character χ that contributes to the ramification of ρ_χ, *we can restrict ourselves to the case of Galois representations attached to Dirichlet characters*.

4.1. **The deformation problem.** Let k be a finite field. Given a residual representation

$$\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_1(k)$$

that is assumed to arise as the reduction of a Galois representation ρ_χ associated with some Dirichlet character χ, we want to study its *deformations*, that is, the Galois representations $\rho : G_{\mathbf{Q}} \to GL_1(\mathcal{O})$ whose mod $\mathfrak{m}_\mathcal{O}$ reductions are isomorphic to $\overline{\rho}$. More precisely, we want to study the structure of a particular subset of these deformations, obtained by imposing conditions (Def. 4.3) that correspond to our specific arithmetic problem. These conditions will turn out to characterize the deformations associated with Dirichlet characters.

We begin by collecting some facts about Dirichlet characters, their reductions, and the behavior of conductors under congruences. Throughout this section, we write $\mathcal{O}$ for a complete noetherian local ring with maximal ideal $\mathfrak{m}_\mathcal{O}$ and finite residue field $\mathcal{O}/\mathfrak{m}_\mathcal{O} = k$ of characteristic $p > 0$. If such an $\mathcal{O}$ is coming from a modular Galois representation (Prop. 2.8), it is necessarily the ring of integers of a finite extension of $\mathbf{Q}_p$.

Remark 4.1. Note that we are using p to denote the characteristic of the residue field k. The prime p will be thought of as being *fixed* throughout this section, as opposed to the varying ℓ's (and λ's) that we used for residue characteristics in previous sections. We hope that this distinction in notation clarifies more than it confuses.

Recall that a Dirichlet character χ is of conductor $N = N(\chi)$ if $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to GL_1(\mathcal{O})$ is not a character of $(\mathbf{Z}/N'\mathbf{Z})^\times$ for any $N' \mid N$ with $N' \neq N$. Given an $\mathcal{O}$-valued Dirichlet character χ, we can also consider its mod $\mathfrak{m}_\mathcal{O}$ reduction

$$\overline{\chi} : (\mathbf{Z}/N(\overline{\chi})\mathbf{Z})^\times \to GL_1(\mathcal{O}/\mathfrak{m}_\mathcal{O})$$

and its corresponding conductor $N(\overline{\chi})$. As the associated Galois representation ρ_χ and similarly its reduction $\overline{\rho_\chi}$ are just obtained by precomposition with the natural quotient map $G_{\mathbf{Q}} \to (\mathbf{Z}/N(\chi)\mathbf{Z})^\times$ (Prop. 2.8), in this section we can again work with the Dirichlet characters and their reductions directly.

A key phenomenon that occurs in this setting is that there can exist two $\mathcal{O}$-valued Dirichlet characters that have different conductors, but whose mod $\mathfrak{m}_\mathcal{O}$ reductions are the same. We have already seen this kind of behavior for modular Galois representations in our level-lowering result (Lemma 3.5). The next result shows how we can refine this if we only allow for congruences between Galois representations coming only from *Dirichlet* characters instead of algebraic Hecke characters in general. Namely, for almost all primes ℓ, mod $\mathfrak{m}_\mathcal{O}$ congruences can possibly contribute ℓ to the conductor, but not higher powers of ℓ.

Lemma 4.2. *Let χ be an $\mathcal{O}$-valued Dirichlet character. If $\ell \neq p = char(\mathcal{O}/\mathfrak{m}_\mathcal{O})$ is a prime such that $\ell \nmid N(\overline{\chi})$ but $\ell \mid N(\chi)$, then $\ell \parallel N(\chi)$, that is, $\ell \nmid (N(\chi)/\ell)$.*

Proof. Recall that $M \mid N$ corresponds to the existence of a nontrivial homomorphism $(\mathbf{Z}/N\mathbf{Z})^\times \to (\mathbf{Z}/M\mathbf{Z})^\times$. We have the decomposition

$$(\mathbf{Z}/N(\chi)\mathbf{Z})^\times = \prod_q (\mathbf{Z}/q^{m_q}\ \mathbf{Z})^\times$$

as q runs over the primes, with m_q a non-negative integer. Let ℓ be a prime that corresponds to a nontrivial factor in this decomposition, that is, $m_\ell > 0$. The mod $\mathfrak{m}_\mathcal{O}$ reduction $\overline{\chi}$ of $\chi : (\mathbf{Z}/N(\chi)\mathbf{Z})^\times \to \mathrm{GL}_1(\mathcal{O})$ factors through $(\mathbf{Z}/N(\overline{\chi})\mathbf{Z})^\times$:

$$\begin{array}{ccc} (\mathbf{Z}/N(\chi)\mathbf{Z})^\times \cong (\mathbf{Z}/\ell^{m_\ell}\mathbf{Z})^\times \times \prod_{q\neq\ell}(\mathbf{Z}/q^{m_q}\mathbf{Z})^\times & \xrightarrow{\overline{\chi}} & \mathrm{GL}_1(\mathcal{O}/\mathfrak{m}_\mathcal{O}) \\ & \searrow \quad \nearrow & \\ & (\mathbf{Z}/N(\overline{\chi})\mathbf{Z})^\times & \end{array}$$

which implies that $\chi|_{(\mathbf{Z}/\ell^{m_\ell}\mathbf{Z})^\times} \equiv 1 \pmod{\mathfrak{m}_\mathcal{O}}$ as ℓ does not occur in $N(\overline{\chi})$ by assumption. Thus, this restriction $\chi|_{(\mathbf{Z}/\ell^{m_\ell}\mathbf{Z})^\times} : (\mathbf{Z}/\ell^{m_\ell}\mathbf{Z})^\times \to \mathrm{GL}_1(\mathcal{O})$ must have order a power of the characteristic of $\mathcal{O}/\mathfrak{m}_\mathcal{O}$, that is,

$$|(\mathbf{Z}/\ell^{m_i}\mathbf{Z})^\times| = \phi(\ell^{m_\ell}) = (\ell-1)\ell^{m_\ell-1}$$

is a power of p. Hence, $m_\ell = 1$, because otherwise, χ would be trivial on the ℓ-part of the decomposition and so the conductor $N(\chi)$ should have been smaller. □

For Dirichlet characters χ, we want to classify deformations of $\overline{\rho_\chi} : G_\mathbf{Q} \to \mathrm{GL}_1(\mathcal{O}/\mathfrak{m}_\mathcal{O})$ associated with a choice of datum

$$\mathcal{D} = (\Sigma, p^r)$$

where Σ is a finite set of primes and p^r is a given power of p.

Definition 4.3. Let A be a complete noetherian local $\mathcal{O}$-algebra with residue field k of characteristic $p > 0$. Let Σ be a finite set of places of $\mathbf{Q}$. We say that a representation $\rho : G_\mathbf{Q} \to \mathrm{GL}_1(A)$ is of *type* $\mathcal{D} = (\Sigma, p^r)$ if

(i) ρ is unramified outside of Σ, that is, $\rho|_{I_q} \cong 1$ for all primes $q \notin \Sigma$, where I_q denotes the inertia subgroup at q; and
(ii) $\rho|_{D_p}$ factors through $\mathrm{Gal}(\mathbf{Q}_p(\mu_{p^r})/\mathbf{Q}_p)$, where D_p denotes the decomposition subgroup at p.

Given a residual representation $\overline{\rho} : G_\mathbf{Q} \to \mathrm{GL}_1(k)$, we write $\mathrm{Def}_\mathcal{D}(\overline{\rho}, A)$ for the set of deformations $G_\mathbf{Q} \to \mathrm{GL}_1(A)$ of $\overline{\rho}$ of type $\mathcal{D}$.

Restricting the residual representation that we consider to those coming from reductions of Dirichlet characters and the deformations to those of type $\mathcal{D}$ together impose strong conditions on our deformation problem.

Lemma 4.4. *Let χ be an $\mathcal{O}$-valued Dirichlet character. A Dirichlet character χ' of conductor $N(\chi')$ that satisfies $\chi' \equiv \chi \mod \mathfrak{m}_{\mathcal{O}}$ is of type $\mathcal{D} = (\Sigma, p^r)$ if and only if*

$$N(\chi') \mid p^r N^{(p)}(\overline{\chi}) \prod_{\substack{q \in \Sigma \setminus \{p\} \\ q \nmid N^{(p)}(\overline{\chi})}} q, \tag{4.5}$$

where $N^{(p)}(\overline{\chi})$ denotes the prime-to-p part of the conductor of $\overline{\chi}$ and $\mathfrak{m}_q \in \boldsymbol{N}$.

In other words, deformations of type $\mathcal{D} = (\Sigma, p^r)$ are quite restricted in what primes they can add to the level: namely, they can only add at most p^r (no higher powers of p are possible) or primes that are in Σ but not in already in the conductor of the original $\overline{\rho_\chi}$.

Proof. If the divisibility condition (4.5) is satisfied, it is immediate that χ' is of type $\mathcal{D}$, so it remains to prove the "only if" direction. Suppose that χ' is a Dirichlet character of type $\mathcal{D}$ such that $\chi' \equiv \chi \mod \mathfrak{m}_{\mathcal{O}}$. If $q \neq p$ and $q \nmid N(\overline{\chi})$, then q divides $N(\chi')$ at most once by Lemma 4.2. Since χ' is of type $\mathcal{D}$, if $q \notin \Sigma$, then q does not divide $N(\chi')$.

For the residue characteristic p, we have

$$\chi' : \mathrm{Gal}(\mathbf{Q}(\mu_{N(\chi')})/\mathbf{Q}) \cong (\mathbf{Z}/N(\chi')\mathbf{Z})^\times \to \mathrm{GL}_1(\mathcal{O})$$

and write $(\mathbf{Z}/p^m\mathbf{Z})^\times$ for the largest such m that χ' factors through. By restricting to the decomposition group D_p, we see that χ' factors through $\mathrm{Gal}(\mathbf{Q}_p(\mu_{p^m})/\mathbf{Q}_p)$ only if $m \leq r$ as χ' is of type $\mathcal{D}$.

Finally, suppose that $q \mid N^{(p)}(\overline{\chi})$. As the reduction $\overline{\chi'}$ factors through $\overline{\chi}$, so does its restriction to the respective $(\mathbf{Z}/q^m\mathbf{Z})^\times$ factors. If there were a nontrivial kernel to this induced map, then χ' must be trivial on some part of the $(\mathbf{Z}/q^m\mathbf{Z})^\times$ factor of $N(\chi')$, which is a contradiction. □

4.2. **Existence of the deformation ring.** In this subsection, we establish the existence of the universal deformation ring parameterizing the deformations of type $\mathcal{D}$ (Def. 4.3). There are a number of ways to prove this result—via Schlessinger's criteria, via pseudocharacters, etc.—we give a sort of "generators and relations" argument that adapts one given by Faltings for n-dimensional Galois representations (cf. [DDT94, Thm. 2.3], see also [dSL97] for a different explicit approach), as we find it to be the simplest to build up from first principles.

For the method of proof to work, we need to first establish a couple of finiteness results. We begin by proving the following simple group-theoretic fact. Recall that a (topological) group G is said to be *topologically finitely generated* if there exists a finite set of elements that generate a dense subgroup of G.

Lemma 4.6. *Let G be an abelian profinite group that is pro-p and topologically finitely generated. If the images of $g_1, \ldots, g_n \in G$ generate G/pG, then $g_1, \ldots, g_n$ topologically generate G.*

Proof. A pro-p group that is topologically finitely generated is known to be *strongly complete*, that is, it is equal to its profinite completion (see, e.g. [Ser02, I.§4.2, Prop. 25]). In other words, $G \cong \varprojlim_U G/U$ where the limit is taken over the (normal) subgroups of finite index. Thus, to show that some set $S \subset G$ is dense, it suffices to check that the image of $S \to G/U$ is dense for each subgroups U of finite index.

Let U be a subgroup of pG of finite index (and so a subgroup of G of finite index). It suffices to show that G/U is (topologically) generated by the images of $g_1, \dots, g_n$. Since G is an abelian pro-p group, the quotient map $G/U \to G/pG$ is of the form

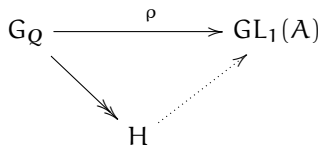
$$G/U \cong \mathbf{Z}/p^{m_1}\mathbf{Z} \times \mathbf{Z}/p^{m_2}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{m_s}\mathbf{Z} \to (\mathbf{Z}/p\mathbf{Z})^s \cong G/pG.$$

As $g_1, \dots, g_n$ generate G/pG, it follows that the numbers of factors s is bounded by n: namely, $s \leq n$ as $|G/pG| \leq p^n$. Hence, $g_1, \dots, g_n$ generate G/U, yielding our result. □

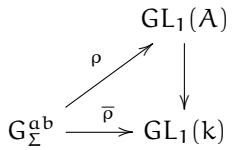
Using this, we can show that representations that satisfy condition (i) of Definition 4.3 all factor through a quotient that is topologically of finite type.

Proposition 4.7. *Let $\overline{\rho}_0 : G_Q \to GL_1(k)$ be a representation that is unramified outside of a finite set Σ of primes. There exists an abelian quotient H of G_Q that is*

(i) *topologically finitely generated, and*
(ii) *has the following property: for any complete noetherian local $\mathcal{O}$-algebra A, if $\rho : G_Q \to GL_1(A)$ is a deformation of $\overline{\rho}$ that is also unramified outside of Σ, then we have a factorization*



Proof. We first note that both $\overline{\rho_0}$ and the deformation ρ factors through the abelianization $G_{\mathbf{Q}}^{ab}$ of $G_{\mathbf{Q}}$, and further, through G_Σ^{ab}, the Galois group of the maximal abelian extension of $\mathbf{Q}$ that is unramified outside of Σ. Writing $\overline{\rho_0}$ and ρ for the maps from G_Σ^{ab} induced by $\overline{\rho_0}$ and ρ, we have the commutative diagram



Consider the subgroup $G_0 = \mathrm{Ker}(\overline{\rho})$ of G_Σ^{ab}; it is of finite index due to the following standard "no small subgroups" argument that is ubiquitous in the theory of Galois representation. Let U be an open subset of $GL_1(k)$ that contains the identity, but is small enough so that it contains no nontrivial subgroup. The inverse image $\overline{\rho}^{-1}(U)$ is an open subset containing the identity and so itself contains an open

subgroup U' of G_Σ^{ab} as G_Σ^{ab} is profinite. The image $\overline{\rho}(U')$ is a subgroup of $GL_1(k)$ inside of U and so is trivial, hence the kernel G_0 of $\overline{\rho}$ contains an open subgroup U' and open subgroups of compact groups (like profinite groups) have finite index.

Now, under ρ we have $\rho(G_0) \subset 1 + \mathfrak{m}_A$. We have the natural filtration

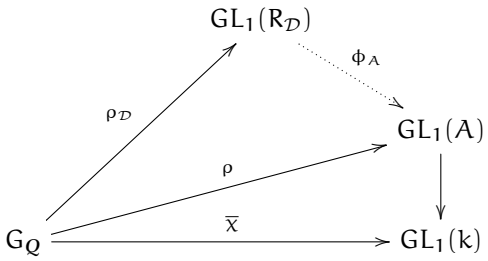
$$1 + \mathfrak{m}_A \supset 1 + \mathfrak{m}_A^2 \supset \cdots \supset 1 + \mathfrak{m}_A^m \supset \cdots$$

where the successive quotients are p-groups. Thus, the restriction $\rho|_{G_0}$ factors through an abelian pro-p group H.

To finish the proof and establish (i), we want to show that G_0 is topologically finitely generated. By Lemma 4.6, it is enough to find the generators of G_0/pG_0. Consider the number field $K = \overline{\mathbf{Q}}^{G_0}$ and let $K_1, K_2, \ldots$ denote the degree p (necessarily abelian) extensions of K that are unramified outside of Σ. Such extensions are of bounded degree and are unramified outside of Σ, and as a consequence of the Hermite–Minkowski theorem (see, e.g. [Neu99, Thm. III.2.13]), we know there are only finitely many such extensions. □

With these algebraic results in hand, it is easy to establish the existence of the deformation ring for deformations of type $\mathcal{D}$.

Theorem 4.8. *There exists a complete noetherian local $\mathcal{O}$-algebra $R_\mathcal{D}$ and a deformation $\rho_\mathcal{D} : G_Q \to GL_1(R_\mathcal{D})$ such that if $\rho : G_Q \to GL_1(A)$ is a deformation of type $\mathcal{D}$ of $\overline{\chi} : G_Q \to GL_1(k)$, there exists a homomorphism $\phi_A : R_\mathcal{D} \to A$ such that the diagram*



commutes.

Proof. As a deformation of type $\mathcal{D} = (\Sigma, p^r)$ is necessarily unramified outside of Σ, we know that it factors through a profinite, topologically finitely generated, abelian group G by Proposition 4.7. Fix a set $g_1, \ldots, g_r$ of topological generators for G. Pick liftings $M_1, \ldots, M_r$ to $GL_1(\mathcal{O}) = \mathcal{O}^\times$ of $\overline{\rho}(g_1), \ldots, \overline{\rho}(g_r)$. Consider the ideals $J \subset \mathcal{O}[\![T_1, \ldots, T_r]\!]$ with the property that there exists a representation

$$G \to GL_1(\mathcal{O}[\![T_1, \ldots, T_r]\!]/J)$$

of type $\mathcal{D}$ that sends g_i to $M_i + T_i$, and let I denote the intersection of all such ideals. We claim that the $R = \mathcal{O}[\![T_1, \ldots, T_r]\!]/I$—which is necessarily a complete noetherian local ring by the Cohen structure theorem—has the required property and so is the ring $R_\mathcal{D}$ that we desire.

It remains to check the universal property. We have a map $\rho^{univ} : G \to GL_1(R)$ given by $\rho^{univ}(g_i) = M_i + T_i \pmod{I}$. Note that this is a group homomorphism as it is obtained as the quotient of the intersection of ideals J that have this property and that $\overline{\rho^{univ}} \cong \overline{\rho_0}$ as T_i lies in the maximal ideal of $\mathcal{O}[\![T_1, \ldots, T_r]\!]$. Given a deformation $\rho : G_Q \to GL_1(A)$ of $\overline{\rho}$ of type $\mathcal{D}$, we define a map $\phi_A : R \to A$ as follows: consider the map $\widetilde{\phi_A} : \mathcal{O}[\![T_1, \ldots, T_r]\!] \to A$ defined by

$$\widetilde{\phi_A}(T_i) = \rho(g_i) - M_i \tag{4.9}$$

and writing $J = \mathrm{Ker}(\widetilde{\phi_A})$, take ϕ_A to be the composition $R \to \mathcal{O}[\![T_1, \ldots, T_r]\!]/J \to A$. We thus have a homomorphism $G \to GL_1(\mathcal{O}[\![T_1, \ldots, T_r]\!]/J)$ given by

$$g_i \mapsto M_i + T_i \quad (\text{“} = \rho(g_i)\text{”}) \tag{4.10}$$

for $i = 1, \ldots, m$, which yields our desired factoring through $GL_1(R)$. □

4.3. **The Hecke algebra for GL_1.** The more concrete side of an “R = T” theorem (a.k.a. modularity theorem) tends to be the “T” side, which is an algebra generated by a set of *Hecke operators*—for modular forms, these are usually thought of as certain endomorphisms of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ of a given level N—and is called a *Hecke algebra*. Here, we describe its analogue in the case of $GL_1(\mathbf{Q})$.

Fix an integer $N \geq 1$ and a complete noetherian local ring $\mathcal{O}$. Write $G_N = (\mathbf{Z}/N\mathbf{Z})^\times \simeq \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q})$. Consider the group ring

$$V = \mathcal{O}[G_N]$$

which we can view as the $\mathcal{O}$-module consisting of functions $G_N \to \mathcal{O}$. The $\mathcal{O}$-algebra is free of rank $|G_N| = \varphi(N)$, where φ is the Euler totient function, with a natural basis given by the characteristic functions $[n] := 1_n : G_N \to \mathcal{O}$ for $n \in G_N$.

For any integer $m \geq 1$, we have the m*th Hecke operator* $T_m \in \mathrm{End}(V)$, which is defined on functions $f \in V$ via

$$(T_m f)(g) = f(mg)$$

for any $g \in G_N$. The *Hecke algebra of level* N is the subalgebra

$$\mathbb{T}_N \subset \mathrm{End}(V)$$

generated over $\mathcal{O}$ by all Hecke operators T_m for integers $m \geq 1$ such that $\gcd(m, N) = 1$. As an $\mathcal{O}$-algebra, this turns out to be nothing other than $V = \mathcal{O}[G_N]$.

Proposition 4.11. *There is an $\mathcal{O}$-algebra isomorphism $\phi : \mathbb{T}_N \xrightarrow{\sim} \mathcal{O}[(\mathbf{Z}/N\mathbf{Z})^\times]$ where*

$$\phi\left(\sum_n a_n T_n\right) = \sum a_n [n].$$

Proof. First, we check that ϕ is an $\mathcal{O}$-algebra homomorphism. This follows because for all positive integers m and n, we have

$$(T_m T_n f)(g) = (T_m f)(ng) = f(mng) = (T_{mn} f)(g)$$

for all $f \in V$ and $g \in G \in G_N$, and this is compatible with the corresponding multiplication $[m][n] = [mn]$ in the group algebra $\mathcal{O}[(\mathbf{Z}/N\mathbf{Z})^\times]$.

Surjectivity is immediate, so it only remains to show injectivity. To calculate the kernel of ϕ, we can assume without loss of generality that $\mathcal{O}$ contains the $\varphi(N)$-th roots of unity by embedding $\mathcal{O}[G_N]$ into $\mathcal{O}(\mu_{\varphi(N)})[G_N]$, where $\mathcal{O}(\mu_{\varphi(N)})$ denotes $\mathcal{O}$ with these $\varphi(N)$-th roots of unity adjoined. Given a character $\chi \in V$—that is, a homomorphism $\chi : G_N \to \mathcal{O}$ and not just a function—we have

$$(T_m\chi)(g) = \chi(mg) = \chi(m)\chi(g).$$

Recall that as G is finite and abelian, so characters form a basis for $V = \mathcal{O}[G_N]$. Now, suppose that

$$\sum_{\substack{n\geq 1\\(n,N)=1}} a_n T_n = 0.$$

Then for any character $\chi \in V$, we have

$$\sum_{\substack{n\geq 1\\(n,N)=1}} a_n\chi(n) = 0.$$

Thus, the character of G_N defined by $n \mapsto a_n$ is orthogonal to all characters $\chi \in V$ and so must be 0. Hence, $\operatorname{Ker}\phi = 0$ and so ϕ is injective. □

4.4. **Ingredients from commutative algebra: two invariants and the Wiles–Lenstra isomorphism criterion.** In [Wil95, Appx.], two commutative algebra invariants associated with a prime ideal $\mathfrak{p}$ of certain local $\mathcal{O}$-algebras T are singled out: the $\mathcal{O}$-module $\mathfrak{p}/\mathfrak{p}^2$ and the annihilator ideal $\eta_T = \operatorname{Ann}_{\mathcal{O}} \mathfrak{p} \subset \mathcal{O}$. Wiles had noticed that $\mathfrak{p}/\mathfrak{p}^2$ could be used to test for isomorphisms between complete intersections, and η_T was used by Kunz to test for isomorphisms between Gorenstein rings [Kun74]. An equality of these invariants turns out to be a criterion for a Gorenstein ring to be a complete intersection (Lem. 4.30). In this section we'll describe these invariants and how they are applied, culminating in the isomorphism criterion that we wish to apply.

For us, $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbf{Q}_p$. Suppose that we have the following commutative diagram of surjective homomorphisms of complete Noetherian local $\mathcal{O}$-algebras:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & T \\ & {\scriptstyle\pi_R}\searrow \quad \swarrow{\scriptstyle\pi_T} & \\ & \mathcal{O} & \end{array} \tag{4.12}$$

where we assume that T is a finite flat $\mathcal{O}$-algebra (i.e. finitely generated and free as a $\mathcal{O}$-module). We set

$$I_R = \operatorname{Ker}\pi_R \quad \text{and } I_T = \operatorname{Ker}\pi_T.$$

The first invariant of interest is the $\mathcal{O}$-module I_R/I_R^2, denoted by

$$\Phi_R = I_R/I_R^2 \tag{4.13}$$

(not be confused with with the surjection $\phi : R \to T$ that we are trying to show is an isomorphism). It can be thought of as the "tangent space for R." (More precisely, it is the *cotangent space* of the affine scheme $\mathrm{Spec}(R)$ *at* I_R, though we do not require the use of this perspective nor any related algebro-geometric language in our main argument.)

The other invariant of interest is the *congruence ideal* η_T *of* T, defined to be the ideal

$$\eta_T = \pi_T \operatorname{Ann}_T(I_T) \tag{4.14}$$

in $\mathcal{O}$. It essentially measures the "highest power congruence" that can be used to define the ring T.

We give a couple of examples (with $R = T$ for simplicity) to illustrate these invariants and perhaps justify their names.

Example 4.15. Let ϖ denote a choice of uniformizer for $\mathcal{O}$. Consider

$$T = \{(a, b) \in \mathcal{O} \times \mathcal{O}, a \equiv b \pmod{\varpi^n}\} \cong \mathcal{O}[\![X]\!]/(X(X - \varpi^n))$$

where $\pi(a, b) = a$ denotes the projection map onto the first factor, then $\Phi_T = \mathcal{O}/\varpi^n\mathcal{O}$ and $\eta_T = (\varpi^n)$. $\diamond$

Example 4.16. Suppose that we have a ring of the form

$$T = \mathcal{O}[\![X]\!]/(f(X))$$

where the defining power series is such that $f(0) = 0$, and write

$$f(X) = a_1X + a_2X^2 + \cdots \in \mathcal{O}[\![X]\!].$$

We have the *constant term* map $\pi : T \to \mathcal{O}$ defined by

$$\pi(g) = g(0) \tag{4.17}$$

for any $g \in T$. Then

$$I_T = \mathrm{Ker}(\pi) = (X) = XT$$

and so $\mathrm{Ann}(I_T) = \mathrm{Ann}(X) = \left(\frac{f(X)}{X}\right)$. Therefore

$$\eta_T = \pi(\mathrm{Ann}(I_T)) = \pi\left(f(X)/X\right) = (a_1).$$

On the other hand, the surjective map $I_T \to \mathcal{O}/(a_1)$ given by $g \mapsto \frac{dg}{dX}(0)$ has kernel $(X^2) = I_T^2$ and so

$$\Phi_T = I_T/I_T^2 \cong \mathcal{O}/(a_1) = \mathcal{O}/\eta_T. \diamond$$

Example 4.18. Consider $T = \mathcal{O}[\![X_1, \ldots, X_n]\!]$ with the constant term map $\pi : T \to \mathcal{O}$ again. Then $I_T = (X_1, \ldots, X_n)$ and $I_T^2 = (X_iX_i \mid 1 \leq i, j \leq n)$, so

$$\begin{aligned} \Phi_T = I_T/I_T^2 &\cong \mathcal{O}^n \\ g &\mapsto \left(\frac{\partial g}{\partial x_1}(0), \ldots, \frac{\partial g}{\partial x_n}(0)\right). \end{aligned}$$

As T is an integral domain, we have $\operatorname{Ann} I_T = 0$ and so $\eta_T = (0)$. $\diamond$

Example 4.19. More generally, suppose that we have a ring of the form

$$T = \mathcal{O}[\![X_1, \ldots, X_n]\!]/(f_1, \ldots, f_n).$$

Such a ring T, which admits as many relations as there are generators, is called a *complete intersection*. Let $\pi : T \to \mathcal{O}$ be the constant term map (4.17), and note that $I_T = \operatorname{Ker}(\pi) = (X_1, \ldots, X_n)$. We have a natural map

$$\begin{aligned} d : I_T &\to \mathcal{O}^n / \left\{ \left(\frac{\partial f_i}{\partial X_1}(0), \ldots, \frac{\partial f_i}{X_n}(0)\right) : i = 1, \ldots, n \right\} \\ g &\mapsto \left(\frac{\partial g}{\partial X_1}(0), \ldots, \frac{\partial g}{\partial X_n}(0)\right) \end{aligned}$$

whose kernel is I_T^2, so

$$\Phi_T = I_T/I_T^2 \cong \mathcal{O}^n / \left\{ \left(\frac{\partial f_i}{\partial X_1}(0), \ldots, \frac{\partial f_i}{X_n}(0)\right) : i = 1, \ldots, n \right\}. \diamond$$

It is more difficult to give a closed form expression for the congruence ideal η_T in the complete intersection case without getting into the intricacies and explicit expressions for the f_i's, but it is usually not too difficult to calculate in examples. We give a simple example of how this can be done.

Example 4.20. Consider $T = \mathbf{Z}_\ell[\![X, Y]\!]/(X(X - \ell), Y(Y - \ell))$ with $\pi : T \to \mathcal{O}$ the constant term map, so $I_T = (X, Y)T$. By Example 4.19, we have

$$\Phi_T = I_T/I_T^2 = (\mathbf{Z}_\ell \oplus \mathbf{Z}_\ell)/((-\ell, 0), (0, -\ell)) \cong \mathbf{Z}/\ell\mathbf{Z} \oplus \mathbf{Z}/\ell\mathbf{Z}.$$

To calculate the congruence ideal, we note that $(X - \ell)(Y - \ell) \in \operatorname{Ann} I_T$ and so $(\ell^2) \subset \eta_T$. We want to show that this is in fact an equality.

Suppose that $g = a + bX + cY + dXY \in \operatorname{Ann} I_T$. Since

$$Xg = aX + bX^2 + cXY + dX^2Y = aX + b\ell X + cXY + d\ell XY = 0,$$

we must have $a + b\ell = 0$ and $c + d\ell = 0$. Similarly,

$$Yg = aY + bXY + cY^2 + dXY^2 = aY + bXY + c\ell Y + d\ell XY = 0$$

and so $a + c\ell = 0$ and $b + c\ell = 0$. Thus,

$$a = -\ell c = -\ell(-d\ell) = \ell^2 d$$

and so $\eta_T \subset (\ell^2)$. Hence, $\eta_T = (\ell^2)$. $\diamond$

In the last example, we had $|\Phi_T| = |\eta_T|$. We'll give an example of what happens when we add a relation to the quotient ideal and are no longer a complete intersection.

Example 4.21. Let $T = \mathbf{Z}_\ell[\![X, Y]\!]/(X(X-\ell), Y(Y-\ell), XY)$ with π the constant term map again, so $I_T = (X, Y)T$ and

$$\Phi_T = \mathbf{Z}/\ell\mathbf{Z} \oplus \mathbf{Z}/\ell\mathbf{Z}$$

as in Example 4.20. To calculate the congruence ideal η_T, we note that here we have

$$X - Y - \ell \in \operatorname{Ann} I_T$$

and so $(\ell) \subset \eta_T$. We claim that $\eta_T = (\ell)$.

Suppose that $g = a + bX + cY \in \operatorname{Ann} I_T$, and so

$$Xg = aX + bX^2 + cXY = aX + b\ell X,$$

which means that $a = -b\ell$ and thus $\eta_T \subset (\ell)$ giving us $\eta_T = (\ell)$. $\diamond$

Thus, we see that we have an explicit pair of invariants associated with a ring, which (a) can be calculated with some thought, and (b) seem to be inverse to each other in some sense, at least for well-behaved rings like the examples above. We now want to focus on more general properties and applications. However, this is the only ingredient in the proof of our main theorem that is *not* simplified by restricting to our one-dimensional or abelian setting. Thus, we content ourselves to giving a sense for how the invariants are calculated and used and referring to other resources for full proofs (e.g. [DDT94, §5]).

The criterion that we ultimately wish to apply (Thm. 4.30) requires calculating lengths of $\mathcal{O}$-modules. Recall that an $\mathcal{O}$-module M has length $\ell(M) = n$ if there exists a chain of submodules

$$M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

and there is no other longer chain of submodules. To this end, it is natural to try and find a way to study obstructions to generating a module by a certain number of elements. This is precisely what is measured by Fitting ideals. Given a finitely generated module M and a choice of short exact sequence

$$0 \to M' \to \mathcal{O}^n \to M \to 0,$$

the *Fitting ideal* $\operatorname{Fitt}(M) = \operatorname{Fitt}_{\mathcal{O}}(M)$ of M is the ideal of $\mathcal{O}$ generated by the determinants of $\det(v_1, \ldots, v_n)$ as $v_i \in \mathcal{O}^n$ ranges over all choices of elements of $M' \subset \mathcal{O}$. Note that $\operatorname{Fitt}(M) \subset \operatorname{Ann}_{\mathcal{O}}(M)$. It is independent of the choice of exact sequence and so is an invariant of M.

Example 4.22. If M is a finitely generated $\mathcal{O}$-module—recall that $\mathcal{O}$ is a discrete valuation ring with maximal ideal $\mathfrak{m} = \mathfrak{m}_{\mathcal{O}}$ in our setting—then M admits a presentation

$$M \cong \mathcal{O}^r \oplus \mathcal{O}/\mathfrak{m}^{n_1} \oplus \mathcal{O}/\mathfrak{m}^{n_2} \oplus \cdots \oplus \mathcal{O}/\mathfrak{m}^{n_m}.$$

Here, the Fitting ideal is

$$\operatorname{Fitt}(M) = \begin{cases} \mathfrak{m}^{n_1+\cdots+n_k}, & \text{if } r = 0, \\ (0), & \text{if } r > 0. \end{cases}$$

In particular, if M is a *finite* $\mathcal{O}$-module, then $\#M = \#(\mathcal{O}/\operatorname{Fitt}(M))$. $\diamond$

For us, the most important property of Fitting ideals is their behavior under tensor products: if M is a finitely generated T-module (with T as in our setup (4.12))

$$\pi_T(\operatorname{Fitt}_T(M)) = \operatorname{Fitt}_{\mathcal{O}}(M \otimes_T \mathcal{O}), \tag{4.23}$$

where the tensor product is taken with respect to $\pi_T : T \to \mathcal{O}$. This allows us to directly relate the Φ- and η-invariants, as when $M = \operatorname{Ker} \pi_T$, we have

$$\operatorname{Fitt}_{\mathcal{O}}(\Phi_T) = \pi_T(\operatorname{Fitt}_T(\operatorname{Ker} \pi_T)) \subset \pi_T(\operatorname{Ann}_T \operatorname{Ker} \pi_T) = \eta_T,$$

which tells us that

$$\#\Phi_T \geq \#(\mathcal{O}/\eta_T). \tag{4.24}$$

We recall Wiles's observation about the Φ-invariant (see, e.g. [DDT94, Thm. 5.21]).

Lemma 4.25. *In our setup (4.12), if*

(i) T *is a (finite, flat) complete intersection, and*
(ii) $\Phi_R = I_R/I_R^2 \cong I_T/I_T^2$ *as $\mathcal{O}$-modules and are of finite length,*

then ϕ is an isomorphism.

Remark 4.26. Both of the hypotheses in Lemma 4.25 are necessary. For the first, we note that the natural surjection

$$\mathbf{Z}_\ell[\![X,Y]\!]/(X(X-\ell), Y(Y-\ell)) \to \mathbf{Z}_\ell[\![X,Y]\!]/(X(X-\ell), Y(Y-\ell), XY)$$

between the rings of Example 4.20 and Example 4.21 is not an isomorphism despite having isomorphic Φ-invariants, due to the latter not being a complete intersection. For the second, the surjective map

$$R = \mathcal{O}[\![T]\!]/(T^3) \to B = \mathcal{O}[\![T]\!]/(T^2)$$

induced by $T \mapsto T$ is not an isomorphism despite the fact that $I_R/I_R^2 \simeq \mathcal{O} \simeq I_B/I_B^2$ as it is not of finite length due to the existence of the infinite chain of ideals $(\mathfrak{m}_{\mathcal{O}}^i)_{i=1}^{\infty}$.

We also recall an effective version of Kunz's criterion ([DDT94, Thm. 5.24]). Recall that a finite flat $\mathcal{O}$-algebra A is *Gorenstein* if $\mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O}) \cong A$ as A-modules, and if such an A is a complete intersection, then it is Gorenstein.

Lemma 4.27. *In our setup (4.12), assume that both R and T are finite and flat (and thus free) $\mathcal{O}$-algebras. If*

(i) *R is Gorenstein; and*
(ii) *$0 \neq \eta_R = \eta_T$,*

then ϕ is an isomorphism.

In general, we can "resolve" finite, flat $\mathcal{O}$-algebras by complete intersections (see, e.g. [DDT94, Thm. 5.26]).

Lemma 4.28. *If B is a free $\mathcal{O}$-algebra of finite rank that is local, and $\pi : B \to \mathcal{O}$ is a surjection, then there exists a surjection*

$$\phi : A \to B$$

where A is a complete intersection and induces an isomorphism $I_A/I_A^2 \cong I_B/I_B^2$ of $\mathcal{O}$-modules.

The above lemmas can be combined to yield to snappy proofs of results that indicate how these invariants interact.

Proposition 4.29. *Let T be a locally free $\mathcal{O}$-algebra of finite rank equipped with a (local) surjection $\pi : T \to \mathcal{O}$. If $\eta_T \neq 0$, then T is a complete intersection if and only if $\mathrm{Fitt}_{\mathcal{O}}(I_T/I_T^2) = \eta_T$.*

Proof. By Lemma 4.28, there exists a complete intersection R and a surjection $\phi : R \to T$ that induces an isomorphism $I_R/I_R^2 \cong I_T/I_T^2$.

If T is a complete intersection, by Lemma 4.25, ϕ is an isomorphism, and Lemma 4.28 applied to R implies that

$$\eta_T = \eta_R = \mathrm{Fitt}(I_R/I_R^2) = \mathrm{Fitt}(I_T/I_T^2).$$

Conversely, if $\eta_T = \mathrm{Fitt}(I_T/I_T^2)$, then

$$0 \neq \eta_B = \mathrm{Fitt}(I_T/I_T^2) = \mathrm{Fitt}(I_R/I_R^2) = \eta_R$$

and R is Gorenstein, so Lemma 4.27 says that ϕ is an isomorphism, so T is a complete intersection. □

We can now state and prove the main isomorphism criterion that we want to apply in the proof of our main theorem.

Theorem 4.30. *(Wiles–Lenstra Isomorphism Theorem)* [Wil95, Appx., Prop. 2] [Len95] *Let $\mathcal{O}$ be a complete discrete valuation ring, R a complete noetherian local $\mathcal{O}$-algebra, and T a finite flat local $\mathcal{O}$-algebra. Suppose that we have surjective $\mathcal{O}$-algebra homomorphisms $\pi : T \to \mathcal{O}$ and $\phi : R \to T$. Then the following conditions are equivalent:*

(i) $\ell(\Phi_R) \leq \ell(\mathcal{O}/\eta_T) < \infty$
(ii) $\ell(\Phi_R) = \ell(\mathcal{O}/\eta_T) < \infty$
(iii) ϕ *is an isomorphism,* $\eta_T \neq 0$*, and* T *is a complete intersection.*

Proof. *(iii)* $\Rightarrow$ *(ii)*: By Proposition 4.29,

$$\eta_T = \mathrm{Fitt}(I_T/I_T^2) = \mathfrak{m}_{\mathcal{O}}^{\ell(I_R/I_R^2)}.$$

As $\eta_T \neq 0$ we have $\ell(\mathcal{O}/\eta_T) < \infty$ and $\ell(\mathcal{O}/\eta_T) = \ell(I_R/I_R^2) = \ell(\Phi_R)$.

(ii) $\Rightarrow$ *(i)*: is immediate.

(i) $\Rightarrow$ *(iii)*: We have

$$\#(\mathcal{O}/\eta_T) \leq \#\Phi_T \leq \#\Phi_R \leq \#(\mathcal{O}/\eta_T)$$

by (4.24), the surjectivity of ϕ, and our hypothesis (i), respectively. Thus $\Phi_T = \#(\mathcal{O}/\eta_T)$ and so T is a complete intersection by Proposition 4.29. Since $\#\Phi_R = \#\Phi_T$, the map ϕ induces an isomorphism between the Φ-invariants, so ϕ is an isomorphism by Lemma 4.25. □

4.5. **A presentation for a localization of the Hecke algebra.** The lack of a closed-form formula for a congruence ideal η is a problem in general arguments, as the Wiles–Lenstra isomorphism theorem (Lem. 4.30) requires us to compute the length of the quotient $\mathcal{O}/\eta$. Luckily for us, for a relevant subclass of complete intersection rings, such a formula is available.

Let G be a finite abelian group, so

$$G = \prod_{i=1}^{m} G_i, \tag{4.31}$$

where $G_i = \langle g_i \rangle$ is a cyclic group of prime power order. We write $n_i = |G_i|$ for the sizes of these factors and $n = |G|$. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbf{Q}_p$, assumed to contain the n-th roots of unity. Given a group homomorphism $\chi : G \to \mathrm{GL}_1(\mathcal{O})$, we have an induced map of $\mathcal{O}$-algebras $\pi_\chi : \mathcal{O}[G] \to \mathcal{O}$ given by

$$\pi_\chi(g_i) = \chi(g_i)$$

for all i. We want to study the localization of the group ring $\mathcal{O}[G]$ at the maximal ideal

$$\mathfrak{m} = \mathrm{Ker}\left(\mathcal{O}[G] \xrightarrow{\pi_\chi} \mathcal{O} \to \mathcal{O}/\mathfrak{m}_{\mathcal{O}}\right),$$

which we denote by

$$A = \mathcal{O}[G]_{\mathfrak{m}}.$$

By realizing A as a universal deformation ring, we can obtain an explicit presentation of A and compute its Φ-invariant and η-invariant.

Proposition 4.32.

(i) *The ring A is a free $\mathcal{O}$-algebra of finite rank over $\mathcal{O}$ and is complete, noetherian, and local. There is an isomorphism*

$$A \cong \mathcal{O}[\![T_i, \dots, T_m]\!]/((T_1 + \chi(g_i))^{n_i} - 1 \mid i = 1, \dots, m),$$

so, in particular, A is a complete intersection. Under this identification, $\pi(T_i) = 0$ for all i.

(ii) *We have*

$$\Phi_A = I_A/I_A^2 \cong \mathcal{O}/n_1\mathcal{O} \times \cdots \times \mathcal{O}/n_m\mathcal{O}.$$

(iii) *We have*

$$\eta_A \cong |G|\mathcal{O} = n\mathcal{O}.$$

Proof. From our decomposition of G into cyclic factors (4.31), we can write

$$\mathcal{O}[G] \cong \mathcal{O}[x_1, \dots, x_n]/(x_1^{n_1} - 1, \dots, u_m^{n_m} - 1)$$

and by changing variables $x_i \leftrightarrow T_i + \chi(g_i)$ where $G_i = \langle g_i \rangle$, we get

$$\mathcal{O}[G] = \mathcal{O}[T_1, \dots, T_m]/((T_1 + \chi(g_i))^{n_i} - 1 \mid i = 1, \dots, m).$$

We want to formulate a deformation problem with A as its universal deformation ring and where our desired isomorphism is realized as that of the universal deformation. Let $\overline{\chi} : G \to GL_1(\mathcal{O}/\mathfrak{m}_\mathcal{O})$ denote the mod $\mathfrak{m}_\mathcal{O}$ reduction of our group homomorphism χ. As G is finitely generated, there exists a universal deformation ring R classifying these deformations (e.g. by following the proof of Theorem 4.7), so

$$\mathrm{Def}(\overline{\chi}, B) \cong \mathrm{Hom}_\mathcal{O}(R, B)$$

for complete Noetherian local $\mathcal{O}$-algebras B with residue field $B/\mathfrak{m}_B \cong \mathcal{O}/\mathfrak{m}_\mathcal{O}$. Moreover, we have $A \cong R$ by (4.9) and (4.10).

We now want to produce an isomorphism between R and our desired presentation

$$\widetilde{R} = \mathcal{O}[\![T_1, \dots, T_m]\!]/((T_i + \chi(g_i))^{n_i} - 1 \mid i = 1, \dots, m).$$

We have the natural map $\rho^{univ} : G \to GL_1(\widetilde{R})$ defined by

$$\rho^{univ}(g_i) = T_i - \chi(g_i)$$

for a generator g_i of G_i. Given a deformation $\rho : G \to GL_1(B)$ of $\overline{\chi}$, we have the map $\psi : \widetilde{R} \to B$ defined by

$$\psi(T_i) = \rho(g_i) - \chi(g_i)$$

with the property that $\rho(g_i) - \chi(g_i) \in \mathfrak{m}_B$ for all i as ρ is a deformation of $\overline{\chi}$. Thus, by post-composing the induced map of ψ with ρ^{univ}, we get ρ. Hence, we obtain the properties of (i). In particular, as A is a complete intersection, we get (ii) from Example 4.19 and (iii) from the fact that $\eta_A = \mathrm{Fitt}_\mathcal{O}(\Phi_A)$ (Prop. 4.29). □

4.6. **Proving the "R = T" theorem.** Recall that $\overline{\chi} := \overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O}/\mathfrak{m}_{\mathcal{O}})$ is a representation obtained as the mod $\mathfrak{m}_{\mathcal{O}}$ reduction of a Galois representation ρ_χ attached to some Dirichlet character χ as in Proposition 2.8. Let $R_{\mathcal{D}}$ denote the universal deformation representing the deformations of $\overline{\rho}$ of type $\mathcal{D} = (\Sigma, p^r)$ (Thm. 4.8). Let $\mathbb{T}_{\mathcal{D}}$ denote the Dirichlet deformations $\chi' : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O})$ of $\overline{\chi}$ of type $\mathcal{D}$, which we know must have conductor

$$N(\chi') \mid p^r N^{(p)}(\overline{\chi}) \prod_{\substack{q \in \Sigma \setminus \{p\} \\ q \nmid N(\overline{\chi})}} q$$

by Lemma 4.4 and so $\mathbb{T}_{\mathcal{D}}$ admits a presentation following Proposition 4.32. We want to show that the corresponding map

$$\phi : R_{\mathcal{D}} \to \mathbb{T}_{\mathcal{D}}$$

(Thm. 4.8) is an isomorphism, giving us an "R = T" theorem. This map is surjective, as any Dirichlet character χ' lying in $\mathbb{T}_{\mathcal{D}}$ has its associated $\mathcal{O}$-valued Galois representation $\rho_{\chi'}$ by Proposition 2.8. Thus, we have two surjective $\mathcal{O}$-algebra homomorphisms

$$R_{\mathcal{D}} \xrightarrow{\phi} \mathbb{T}_{\mathcal{D}} \longrightarrow \mathcal{O}$$

where the latter is the constant term map (4.17) and so can place ourselves in the setting of §4.4. We want to apply Theorem 4.30 to show that ϕ is an isomorphism, and to this end, reduce ourselves to verifying condition (i) of the theorem in our context.

We begin by recalling a simple algebraic observation, which we later apply to study $\Phi_D := \Phi_{R_D}$.

Lemma 4.33. *If $\mathcal{O}$ is a discrete valuation ring and M is a finitely generated $\mathcal{O}$-module, then*

$$\mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k) \cong M/\mathfrak{m}_{\mathcal{O}}^k M.$$

In particular, $\ell(\mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O}/\mathfrak{m}_{\mathcal{O}})) = \ell(M/\mathfrak{m}_{\mathcal{O}}M)$ is equal to the number of cyclic factors of M. We can also use this to calculate the length of an $\mathcal{O}$-module asymptotically:

$$\lim_{k \to \infty} \ell(\mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k)) = \ell(M)$$

Proof. We have a decomposition

$$M \cong \mathcal{O}^r \oplus \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^{n_1} \oplus \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^{n_2} \oplus \cdots \oplus \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^{n_m}. \tag{4.34}$$

By the additivity of Hom, it suffices to prove our result when M is cyclic. If $M = \mathcal{O}$, then

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k) \cong \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k \cong M/\mathfrak{m}_{\mathcal{O}}^k M.$$

If $M = \mathcal{O}/a_i\mathcal{O}$, we know that $M \cong \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^i$ for some i as $\mathcal{O}$ is a discrete valuation ring and

$$\begin{aligned}\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^i, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k) &\cong \mathcal{O}/(\mathfrak{m}_{\mathcal{O}}^i + \mathfrak{m}_{\mathcal{O}}^k) \cong \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^{\min(i,k)} \\ &\cong \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k \otimes \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^i \cong M/\mathfrak{m}_{\mathcal{O}}^k M.\end{aligned}$$

The final statement in our lemma holds because if M is torsion, then $M/\mathfrak{m}_{\mathcal{O}}^k M = M$ for sufficiently large k. $\square$

We now want to understand the relevance of the Φ-invariant (4.13)

$$\Phi_{\mathcal{D}} := \Phi_{R_{\mathcal{D}}} = I_{R_{\mathcal{D}}}/I_{R_{\mathcal{D}}}^2$$

in our arithmetic context. Recall that we have a short exact sequence

$$0 \to I_{R_{\mathcal{D}}} \to R_{\mathcal{D}} \xrightarrow{\pi_R} \mathcal{O} \to 0 \tag{4.35}$$

and so can express any element of $R_{\mathcal{D}} = \mathcal{O} + I_{R_{\mathcal{D}}}$ in terms of its summands. Furthermore, from the surjection $R_{\mathcal{D}}/I_{R_{\mathcal{D}}}^2 \to R_{\mathcal{D}}/I_{R_{\mathcal{D}}} \cong \mathcal{O}$, we obtain the short exact sequence

$$0 \to \Phi_{\mathcal{D}} \to R_{\mathcal{D}}/I_{R_{\mathcal{D}}}^2 \to \mathcal{O} \to 0. \tag{4.36}$$

The following result allows us to connect $\Phi_{\mathcal{D}}$ more directly with Galois representations.

Proposition 4.37. *For any $k \geq 1$, there is an isomorphism of $\mathcal{O}$-modules*

$$\mathrm{Hom}_{\mathcal{O}}(\Phi_{\mathcal{D}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n) \cong \mathrm{Hom}_{\mathcal{D}}(G_{\mathbb{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n),$$

where $\mathrm{Hom}_{\mathcal{D}}(G_{\mathbb{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k)$ denotes the mod $\mathfrak{m}_{\mathcal{O}}^k$ representations of $G_{\mathbb{Q}}$ of type $\mathcal{D} = (\Sigma, p^r)$ (Def. 4.3).

Proof. (Case 1, $n = 1$.) We prove this by producing our desired isomorphism as the composition of two other isomorphisms. For any complete noetherian local $\mathcal{O}$-algebra A, we have $\mathrm{Def}_{\mathcal{D}}(\overline{\chi}, A) = \mathrm{Hom}_{\mathcal{O}-alg}(R_{\mathcal{D}}, A)$. Letting $k = \mathcal{O}/\mathfrak{m}_{\mathcal{O}}$ denote the residue field and taking $A = k[\epsilon]/(\epsilon^2)$ to denote the ring of dual numbers over k, we first want to show that

$$\mathrm{Hom}_{\mathcal{O}}(\Phi_{\mathcal{D}}, k) \cong \mathrm{Hom}_{\mathcal{O}-alg}(R_{\mathcal{D}}, k[\epsilon]/(\epsilon^2)). \tag{4.38}$$

As any $f \in \mathrm{Hom}_{\mathcal{O}-alg}(R_{\mathcal{D}}, k[\epsilon]/(\epsilon^2))$ is a local homomorphism, it is determined by its restriction to $I_{R_{\mathcal{D}}}$ (4.35), and $f|_{I_{R_{\mathcal{D}}}}(x)$ induces a homomorphism

$$\alpha : I_{R_D}/I_{R_D}^2 = \Phi_{\mathcal{D}} \to k.$$

Conversely any such homomorphism α defines for us an $\mathcal{O}$-algebra homomorphism, establishing (4.38).

We now want to show that

$$\mathrm{Def}_{\mathcal{D}}(\overline{\chi}, k[\epsilon]/(\epsilon^2)) \cong \mathrm{Hom}_{\mathcal{D}}(G_{\mathbb{Q}}, k) \tag{4.39}$$

by calculating the former. Let $\rho \in \mathrm{Def}_{\mathcal{D}}(\overline{\chi}, k[\epsilon]/(\epsilon^2))$, which we can write as

$$\rho(g) = \overline{\chi}(g)(1 + \chi_\rho(g)\epsilon) \tag{4.40}$$

for some function $\chi_\rho : G_{\mathbf{Q}} \to k$ for all $g \in G_{\mathbf{Q}}$. Since $\rho(gh) = \rho(g)\rho(h)$ for all $g, h \in G_{\mathbf{Q}}$ and using that $\epsilon^2 = 0$ in $k[\epsilon]/(\epsilon^2)$, we see that

$$\begin{aligned}\overline{\chi}(gh)(1+\chi_\rho(gh)\epsilon) &= \overline{\chi}(g)(1+\chi_\rho(g)\epsilon)\overline{\chi}(h)(1+\chi_\rho(h)) \\ &= \overline{\chi}(g)\overline{\chi}(h)(1+\chi_\rho(g)\epsilon)(1+\chi_\rho(h)\epsilon)\end{aligned}$$

so $\chi_\rho(gh) = \chi_\rho(g) + \chi_\rho(h)$, and thus $\chi_\rho : G_{\mathbf{Q}} \to k$ is also a group homomorphism. Since ρ is of type $\mathcal{D} = (\Sigma, p^r)$, we must also have $\chi_\rho|_{I_q}$ trivial for $q \notin \Sigma$ and $\chi_\rho|_{D_p}$ factors through $\mathrm{Gal}(\mathbf{Q}_p(\mu_{p^r})/\mathbf{Q}_p)$, so we have $\chi_\rho \in \mathrm{Hom}_{\mathcal{D}}(G_{\mathbf{Q}}, k)$. Conversely, such a homomorphism χ_ρ uniquely determines a $\rho \in \mathrm{Def}_{\mathcal{D}}(\overline{\chi}, k[\epsilon]/(\epsilon^2))$ via (4.40). This establishes (4.39) and completes our proof of the case $n = 1$.

Case 2, arbitrary $n \geq 1$. Consider the ring

$$A_n = \mathcal{O}[\epsilon]/(\mathfrak{m}_{\mathcal{O}}^n \epsilon, \epsilon^2) = \{a_0 + a_1\epsilon : a_0 \in \mathcal{O}, a_1 \in \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n\}.$$

As in the $n = 1$ case above, we want to establish our desired isomorphism by passing through

$$\mathrm{Def}_{\mathcal{D}}(\overline{\chi}, A_n) \cong \mathrm{Hom}(R_{\mathcal{D}}, A_n)$$

as an intermediary.

Given $\alpha \in \mathrm{Hom}_{\mathcal{D}}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$, we construct a deformation $\rho_\alpha : G_{\mathbf{Q}} \to \mathrm{GL}_1(A_n)$ via

$$\rho_\alpha(g) = \chi(g)(1 + \alpha(g)\epsilon),$$

which is of type $\mathcal{D}$ as χ—the $\mathcal{O}$-valued Dirichlet character that we assume our residual representation $\overline{\chi}$ is the reduction of—is of type $\mathcal{D}$ by Lemma 4.5. By the universal property of $R_{\mathcal{D}}$, we have an $\mathcal{O}$-algebra homomorphism

$$\phi_\alpha : R_{\mathcal{D}} \to A_n$$

corresponding to ρ_α. The map ϕ_α of $\mathcal{O}$-algebras is determined by its restriction

$$\phi_\alpha|_{I_{\mathcal{D}}} : I_{\mathcal{D}} \to \epsilon\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$$

and thus induces a map

$$\psi_\alpha : \Phi_{\mathcal{D}} \to \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$$

which yields our desired isomorphism.

Conversely, let $\psi \in \mathrm{Hom}_{\mathcal{O}}(\Phi_{\mathcal{D}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$. By post-composing the universal deformation $\rho_{\mathcal{D}} : G_{\mathbf{Q}} \to \mathrm{GL}_1(R_{\mathcal{D}})$ with the quotient map, we get

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_1(R_{\mathcal{D}}/I_{\mathcal{D}}^2).$$

Similarly, by post-composing $\rho_\chi : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O})$ with the quotient map, we get

$$\rho' : G_{\mathbf{Q}} \to \mathrm{GL}_1(R_{\mathcal{D}}/I_{\mathcal{D}}^2).$$

Consider the map $\rho\rho'^{-1} : G_{\mathbf{Q}} \to \mathrm{GL}_1(R_{\mathcal{D}}/I_{\mathcal{D}}^2)$ obtained by taking the product, which satisfies

$$\rho\rho'^{-1} \equiv 1 \pmod{I_{\mathcal{D}}}.$$

Recall that we have the short exact sequence (4.36)

$$0 \to \Phi_{\mathcal{D}} \to R_{\mathcal{D}}/I_{\mathcal{D}}^2 \to \mathcal{O} \to 0,$$

which induces the short exact sequence

$$1 \to (1 + I_{\mathcal{D}})/I_{\mathcal{D}}^2 \to GL_1(R_{\mathcal{D}}/I_{\mathcal{D}}^2) \to GL_1(\mathcal{O}) \to 1,$$

noting that we can identify $I_{\mathcal{D}}/I_{\mathcal{D}}^2 \cong (1 + I_{\mathcal{D}})/I_{\mathcal{D}}^2$ via $x \mapsto 1 + x$. This gives us

$$\alpha = \rho\rho'^{-1} : G_{\mathbf{Q}} \to \Phi_{\mathcal{D}}$$

which by composition with ψ gives us an element of $\mathrm{Hom}_{\mathcal{D}}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$. □

Remark 4.41. The groups $\mathrm{Hom}_{\mathcal{D}}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$ can thought of as examples of *Selmer groups* (a.k.a. generalized class groups). In Wiles's proof of Fermat's Last Theorem, various generalized cotangent spaces are interpreted as Selmer groups [Wil95, Prop. 1.2.] as in Proposition 4.37. A key technical step—and source of the infamous gap in the original approach—was in calculating a precise upper bound for the size of the relevant Selmer groups [Wil95, p.452–453]. While our main argument follows this strategy, many subtleties involved in the two-dimensional case simply do not arise in the one-dimensional setting. For example, a great difficulty encountered in Wiles's proof is the critical case of *reducible* mod 3 representations, but all one-dimensional representations are irreducible.

We endow the set of possible deformation data with the following partial ordering.

Definition 4.42. Given $\mathcal{D} = (\Sigma, p^r)$ and $\mathcal{D}' = (\Sigma', p^{r'})$, we say that

$$\mathcal{D}' \geq \mathcal{D}$$

if $r' \geq r$ and $\Sigma' \supset \Sigma$.

The following result allows us to drastically reduce the checks on the hypotheses needed to apply our desired isomorphism theorem for rings (Theorem 4.30).

Lemma 4.43. *(Induction on $\mathcal{D}$) Let $\mathcal{D}' \geq \mathcal{D}$. If*

$$\ell(\Phi_{\mathcal{D}}) \leq \ell(\mathcal{O}/\eta_{\mathcal{D}}),$$

then

$$\ell(\Phi_{\mathcal{D}'}) \leq \ell(\mathcal{O}/\eta_{\mathcal{D}'}).$$

Proof. We have two cases to consider for a given datum $\mathcal{D} = (\Sigma, p^r)$: (a) when we augment the set of ramified primes Σ, and (b) when we increase the prime power to $p^{r'}$ for $r' > r$.

Case (a): Suppose that $\Sigma' = \Sigma \cup \{q\}$ where $q \notin \Sigma$. Recall that

$$\eta_{\mathcal{D}} = |(\mathbf{Z}/N\mathbf{Z})^\times|\mathcal{O} \quad \text{and } \eta_{\mathcal{D}'} = |(\mathbf{Z}/qN\mathbf{Z})^\times|\mathcal{O}$$

by Proposition 4.32 and so

$$\ell(\mathcal{O}/\eta_{\mathcal{D}'}) - \ell(\mathcal{O}/\eta_{\mathcal{D}}) = \ell(\mathcal{O}/(q-1)\mathcal{O}) = v_p(q-1).$$

Thus, it suffices to show that

$$\ell(\Phi_{\mathcal{D}'}) - \ell(\Phi_{\mathcal{D}}) \leq \ell(\mathcal{O}/(q-1)\mathcal{O}).$$

Recall that

$$\mathrm{Hom}_{\mathcal{O}}(\Phi_{\mathcal{D}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n) \cong \mathrm{Hom}_{\mathcal{D}}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$$

for any integer $n \geq 1$ by Proposition 4.37. The restriction map

$$\mathrm{Hom}_{\mathcal{D}'}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n) \to \mathrm{Hom}(I_q, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$$

where I_q is the inertia subgroup at q induces the exact sequence

$$0 \to \mathrm{Hom}_{\mathcal{D}}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n) \to \mathrm{Hom}_{\mathcal{D}'}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n) \to \mathrm{Hom}(I_q, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n),$$

and so it follows that

$$\ell(\mathrm{Hom}_{\mathcal{O}}(\Phi_{\mathcal{D}'}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)) \leq \ell(\mathrm{Hom}_{\mathcal{D}}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)) + \ell(\mathrm{Hom}(I_q, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)).$$

We now want to calculate $\ell(\mathrm{Hom}(I_q, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n))$. More precisely, it suffices to show that for sufficiently large n

$$\ell(\mathrm{Hom}(I_q, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)) \leq \ell(\mathcal{O}/\eta_{\mathcal{D}'}) - \ell(\mathcal{O}/\eta_{\mathcal{D}}).$$

as our desired result would follow from it by allowing $n \to \infty$ by Lemma 4.33. To prove this claim, we recall some facts about inertia subgroups.

> **Facts.** (see, e.g. [Ser79, IV, §1–2]) Let $q \neq p$ be a prime number, and write $G_q = \mathrm{Gal}(\overline{\mathbf{Q}_q}/\mathbf{Q}_q)$.
>
> (i) There is a subnormal composition series
>
> $$G_q \rhd I_q \rhd I_1$$
>
> where I_q denotes the inertia subgroup at q and I_1 denotes the wild inertia subgroup at q (i.e. the pro-q Sylow subgroup of I_q). The successive quotients admit isomorphisms
>
> $$G_q/I_q \cong \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q) \quad \text{and} \quad I_q/I_1 \cong \varprojlim_n (\mathbf{F}_{q^n})^\times.$$
>
> (ii) Given a generator $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q) \cong G_q/I_q$, we have
>
> $$(\mathrm{Frob}_q)\sigma(\mathrm{Frob}_q)^{-1} = \sigma^q$$
>
> for $\sigma \in I_q/I_1$.

Since the order of $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$ is a power of p, any map $\alpha \in \mathrm{Hom}(I_{q'}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)$ must factor through the tame quotient $I_{q'}/I_1$. Similarly, as α comes by restricting from $G_{\mathbf{Q}}$, (ii) shows that α comes from $(\mathbf{F}_q)^\times$, the lowest possible degree, as it implies

that $\alpha(\sigma) = \alpha(\sigma)^q$, which means that $\alpha(\sigma)^{q-1} = 0$. More precisely, as $q \nmid |\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n|$, we have

$$\begin{aligned}\mathrm{Im}\,(\mathrm{Res} : \mathrm{Hom}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}h^n) \to \mathrm{Hom}(I_q, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)) &\cong \mathrm{Hom}_{G_{\mathbf{Q}}}(I_q/I_1, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n) \\ &\cong \mathrm{Hom}_{G_{\mathbf{Q}}}\left(\varprojlim_n (\mathbf{F}_{q^n})^\times, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n\right) \\ &\cong \mathrm{Hom}(\mathbf{F}_q^\times, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)\end{aligned}$$

where $\mathrm{Hom}_{G_{\mathbf{Q}}}$ denotes the subset of homomorphisms that extend to one coming from $G_{\mathbf{Q}}$ and the final isomorphism holds by (ii) and the fact that $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$ is commutative. Hence, for n sufficiently large,

$$\ell(\mathrm{Hom}(I_q, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)) \leq \ell(\mathcal{O}/(q-1)\mathcal{O}) = \ell(\mathcal{O}/\eta_{\mathcal{D}'}) - \ell(\mathcal{O}/\eta_{\mathcal{D}}),$$

establishing our claim.

Case (b): Now suppose that $\mathcal{D} = (\Sigma, p^r)$ and $\mathcal{D}' = (\Sigma, p^{r+1})$. The approach is similar to Case (a) in that we want to use Proposition 4.37 and a similar exact sequence to obtain our inequality on lengths, but now we consider the restriction maps

$$\mathrm{Hom}_{\mathcal{D}'}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n) \to \mathrm{Hom}((I_p \cap G_{p^r})/(I_p \cap G_{p^{r+1}}))$$

where $G_{p^i} = \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^i})/\mathbf{Q}_p)$. Note that we have a map

$$(I_p \cap G_{p^r})/(I_p \cap G_{p^{r+1}}) \to \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^{r+1}})/\mathbf{Q}_p(\mu_{p^r})) \cong \begin{cases} (\mathbf{Z}/p\mathbf{Z})^\times, & \text{if } r = 0 \\ (\mathbf{Z}/p\mathbf{Z}), & \text{if } r \geq 0. \end{cases}$$

Inspired by this, we define the integer

$$\ell_r = \begin{cases} 0, & \text{if } j = 0 \\ \ell(\mathcal{O}/p\mathcal{O}), & \text{if } j \geq 0. \end{cases}$$

Thus, from the exact sequence corresponding to the restriction map above and the kernel, we obtain

$$\begin{aligned}\ell(\mathrm{Hom}_{\mathcal{D}'}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)) &\leq \ell(\mathrm{Hom}_{\mathcal{D}}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n)) + \ell_r \\ &\leq \ell(\mathcal{O}/\eta_{\mathcal{D}}) + \ell_r \\ &= \ell(\mathcal{O}/\eta_{\mathcal{D}'})\end{aligned}$$

as $\mathcal{O}/\eta_{\mathcal{D}'} = \mathcal{O}/|(\mathbf{Z}/pN\mathbf{Z})^\times|\mathcal{O}$ by Proposition 4.32. □

We can now establish our "R = T" theorem by checking that it holds for the minimal datum $\mathcal{D}$.

Theorem 4.44. *Let A be any complete noetherian local $\mathcal{O}$-algebra. Let $\rho : G_{\mathbf{Q}} \to GL_1(A)$ be a deformation of type $\mathcal{D}$ such that $\overline{\rho} = 1 \pmod{\mathfrak{m}_A}$. Then $\rho \cong \rho_\chi$ for some Dirichlet character χ.*

Proof. Consider the minimal deformation datum $\mathcal{D}_0 = (\emptyset, p^0)$. By Lemma 4.43, it suffices to show that the quantities $\ell(\Phi_{\mathcal{D}_0})$ and $\ell(\mathcal{O}/\eta_{\mathcal{D}_0})$ are equal.

For sufficiently large k, we have

$$\ell(\Phi_{\mathcal{D}_0}) = \dim \mathrm{Hom}_{\mathcal{D}_0}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k),$$

by Proposition 4.37. But then if $\varphi \in \mathrm{Hom}_{\mathcal{D}_0}(G_{\mathbf{Q}}, \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^k)$, its kernel $\mathrm{Ker}(\varphi)$ would be a closed subgroup that correponds to an everywhere unramified abelian extension of $\mathbf{Q}$, which must be $\mathbf{Q}$ by Minkowski's theorem (see e.g. [Neu99, III, Thm. 2.17–18]), hence $\mathrm{Ker}(\varphi) = G_{\mathbf{Q}}$ and so $\ell(\Phi_{\mathcal{D}_0}) = 0$. On the other side, we have

$$\ell(\mathcal{O}/\eta_{\mathcal{D}_0}) = \ell(\mathcal{O}/((\mathbf{Z}/\mathbf{Z})^\times \mathcal{O})) = 0,$$

giving us the desired result. □

Of course, this finally yields Theorem 3.8 as a corollary by applying Theorem 4.44 to $\rho\rho_0^{-1}$ and multiplying the result by ρ_0.

5. Input from the theory of cyclotomic extensions

So far, we have been able to avoid using too many specifics about cyclotomic fields, aside from the elementary property that $\mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^\times$. Nonetheless, an additional spark is needed to activate the modular deformation theory machinery (§4) for our proof of the Kronecker–Weber theorem. Different proofs of the Kronecker–Weber theorem tend to exploit different structures of cyclotomic fields, whether it is the units, the ideal class group, ramification groups, a decomposition of a certain ideal generated by a Gauss sum upon a cyclotomic extension, etc. In proofs of the Kronecker–Weber theorem that rely on an input from local fields, a classification of the p-*extensions* of $\mathbf{Q}_p$—that is, the Galois extensions with a Galois group of p-power order—is often what is required. We adopt this approach, as we can naturally classify these p-extensions in terms of the mod p cyclotomic character (Cor. 4.31) and its characterization in terms of a Galois character is closely related to our deformation theoretic approach. The most direct way to establish this relation is through Galois cohomology, but this more abstract approach—which is essential in the $\mathrm{GL}(2)$ version for modular forms—is not really needed for our ultimate goal and would obscure the main thread of the argument.

Our goal in this section is to prove the following result, a sort of "weak local Kronecker–Weber theorem for p-extensions."

Lemma 5.1. *Let E be a finite (abelian) p-extension of $\mathbf{Q}_p$. There exists an integer $r \geq 1$ such that*

$$E \subset F(\mu_{p^r}),$$

where $F(\mu_{p^r})$ is an abelian extension obtained by adjoining the p^r-th roots of unity to an unramified extension F of $\mathbf{Q}_p$.

Remark 5.2. If we could replace E with *any* abelian extension of $\mathbf{Q}_p$ and if we could always take the unramified extension F in this lemma to be *trivial*, then this would give a "local Kronecker–Weber theorem" more deserving of the name. However, this stronger statement—which is more involved than our proof of Theorem 5.1—is easily seen to be equivalent to the "global" Kronecker–Weber theorem of Theorem 1.1, see [Was97, Ch. 14]. (See also [Neu99, V.1.9–10]).

To prove Lemma 5.1, we restrict ourselves to a basic form of *Kummer theory*, which is concerned with field extensions obtained by adjoining an nth root. The cases of odd primes p and $p = 2$ must be treated separately, as the p-extensions of $\mathbf{Q}_p$ in these two cases are structured differently.

5.1. **Cyclic p-extensions of $\mathbf{Q}_p(\mu_p)$ and $\mathbf{Q}_p$.** We first recall the statements from Kummer theory that we will use, see e.g. [Bir67, §2, Lem. 2 & 3].

Lemma 5.3. *(Kummer theory) Let K be a field containing a primitive mth root of unity.*

(i) *All cyclic extensions of K of degree m are of the form $K(\sqrt[m]{\alpha})$ for an $\alpha \in K$.*
(ii) *If $K(\sqrt[m]{\alpha}) = K(\sqrt[m]{\beta})$, then α and β generate the same subgroup in $K^\times/(K^\times)^m$, that is, $\alpha = \beta^t\gamma^m$ for some $\gamma \in K$ and $t \in \mathbf{Z}$ with $\gcd(m, t) = 1$.*

We use this to get the following characterization of cyclic p-extensions and introduce the primary object of study in the proof of Lemma 5.1.

Corollary 5.4. *The cyclic extensions of degree p of $\mathbf{Q}_p(\mu_p)$ that are abelian over $\mathbf{Q}_p$ and correspond to the subgroups of order p of the $\mathrm{Gal}(\mathbf{Q}_p(\mu_p)/\mathbf{Q}_p)$-module*

$$[\mathbf{Q}_p(\mu_p)^\times/(\mathbf{Q}_p(\mu_p)^\times)^p]^\chi :=$$
$$\{\alpha \in \mathbf{Q}_p(\mu_p)^\times/(\mathbf{Q}_p(\mu_p)^\times)^p \mid \sigma(\alpha) = \chi(\sigma)\cdot\alpha = \alpha^{\chi(\sigma)} \text{ for } \sigma \in \mathrm{Gal}(\mathbf{Q}_p(\mu_p)/\mathbf{Q}_p)\},$$

where $\chi = \overline{\chi_p} : \mathrm{Gal}(\mathbf{Q}_p(\mu_p)/\mathbf{Q}_p) \to \mathrm{GL}_1(\boldsymbol{F}_p)$ denotes the mod p cyclotomic character.

Proof. Let E be a cyclic extension of $\mathbf{Q}_p(\mu_p)$ of degree p, so E is an abelian extension of $\mathbf{Q}_p$ and $E = \mathbf{Q}_p(\mu_p)(\sqrt[p]{\alpha})$ for some $\alpha \in \mathbf{Q}_p(\mu_p)$ by Lemma 5.3(i). Given $\sigma \in \mathrm{Gal}(\mathbf{Q}_p(\mu_p)/\mathbf{Q}_p)$, let $\widetilde{\sigma} \in \mathrm{Gal}(E/\mathbf{Q}_p)$ be an element such that $\widetilde{\sigma}|_{\mathbf{Q}_p(\mu_p)} = \sigma$. Then $\widetilde{\sigma}(\sqrt[p]{\alpha}) \in E$ and

$$\sigma(\alpha) = \alpha^t\alpha_0^p$$

for some $\alpha_0 \in \mathbf{Q}_p(\mu_p)$ and a $t \in \mathbf{Z}$ that is not divisible by p by Lemma 5.3(ii). To obtain our result, we want to determine this exponent t.

Let $\tau \in \mathrm{Gal}(E/\mathbf{Q}_p(\mu_p))$ be the element where $\tau(\sqrt[p]{\alpha}) = \zeta_p\sqrt[p]{\alpha}$. Since $\widetilde{\sigma}(\zeta_p) = \zeta_p^{\chi(\sigma)}$ and we want $\mathrm{Gal}(E/\mathbf{Q}_p)$ to be abelian, we have

$$\begin{aligned}\zeta_p^t\widetilde{\sigma}(\sqrt[p]{\alpha}) &= \zeta_p^t\alpha^{t/p}\alpha_0 = \tau(\alpha^{t/p}\alpha_0) = \tau\widetilde{\sigma}(\sqrt[p]{\alpha})\\ &= \widetilde{\sigma}\tau(\sqrt[p]{\alpha}) = \widetilde{\sigma}(\zeta_p\sqrt[p]{\alpha}) = \zeta_p^{\chi(\sigma)}\widetilde{\sigma}(\sqrt[p]{\alpha})\end{aligned}$$

and so $t = \chi(\sigma) = \overline{\chi_p}(\sigma)$. □

For notational simplicity, let $\zeta = \zeta_p$ denote a primitive pth root of unity and $\chi = \overline{\chi_p}$ denote the mod p cyclotomic character for the remainder of the section.

Lemma 5.5. *Assume that $p \neq 2$. Let $\mathcal{O} = \mathbf{Z}_p[\zeta]$ and write $\pi = 1 - \zeta$, which is a uniformizer for $\mathcal{O}$ (i.e. $\mathfrak{m}_{\mathcal{O}} = (\pi)$).*

(i) *The set of pth powers of $1 + \pi\mathcal{O}$ is $1 + \pi^{p+1}\mathcal{O}$.*

(ii) *If $p \neq 2$, the natural inclusion of the finite group*

$$(1 + \pi\mathcal{O})/(1 + \pi^{p+1}\mathcal{O}) \hookrightarrow \boldsymbol{Q}_p(\mu_p)^\times/(\boldsymbol{Q}_p(\mu_p)^\times)^p \tag{5.6}$$

induces an isomorphism of corresponding χ-eigenspaces.

Proof of (i). Let $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ denote the p-th cyclotomic polynomial. We have

$$\begin{aligned} p = \Phi_p(1) &= (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1}) \\ &= (1-\zeta)^{p-1}\frac{(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1})}{(1-\zeta)^{p-1}} \\ &= (1-\zeta)^{p-1}u_0 = \pi^{p-1}u_0 \end{aligned}$$

where

$$u_0 = (1+\zeta)(1+\zeta+\zeta^2)\cdots(1+\zeta+\cdots+\zeta^{p-2}) \in \mathcal{O}^\times.$$

Modulo $\pi = 1 - \zeta$, we have

$$u_0 \equiv 2 \cdot 3 \cdot \cdots (p-1) \equiv (p-1)! \equiv -1 \pmod{\pi} \tag{5.7}$$

by Wilson's theorem, as $\pi \mid p$.

Now, if $x \in 1 + \pi\mathcal{O}$, we can write

$$x = 1 + \pi a + \pi^2 b$$

for some $a, b \in \mathcal{O}$. Thus, we have

$$\begin{aligned} x^p &\equiv (1 + \pi a + \pi^2 b)^p \equiv 1 + p\pi a + \pi^p a^p \pmod{\pi^{p+1}} \\ &\equiv 1 + (\pi^{p-1}u_0)\pi a + \pi^p a^p \pmod{\pi^{p+1}} \\ &\equiv 1 + \pi^p(au_0 + a^p) \pmod{\pi^{p+1}}. \end{aligned}$$

Note that $au_0 + a^p \equiv -a + a^p \pmod{\pi}$ by (5.7). As $a \in \mathcal{O}$, we can write $a = \alpha + \beta\zeta$ for $\alpha, \beta \in \mathbf{Z}_p$. Using the fact that $\pi \mid p$, we see that

$$a^p - a \equiv (\alpha + \beta\zeta)^p - \alpha + \beta\zeta \equiv \alpha^p - \alpha + \beta^p - \beta \equiv 0 \pmod{\pi},$$

as Fermat's little theorem $\gamma^p \equiv \gamma \pmod{p}$ holds for elements $\gamma \in \mathbf{Z}_p$. Thus, we have $\pi \mid (a^p - a)$ and so $(1 + \pi\mathcal{O})^p \subset 1 + \pi^{p+1}\mathcal{O}$.

Conversely, suppose that $\alpha \equiv 1 \pmod{\pi^{p+1}}$. We want to find an $x \in \mathcal{O}$ such that $x^p = \alpha$ and $x \equiv 1 \pmod{\pi}$. To do so, we use the following argument, which is along the lines of Hensel's lemma. It suffices to construct a sequence $\{x_i\}$ where $x_i \in 1 + \pi\mathcal{O}$ for $i \geq p + 1$ with the properties

$$x_i^p \equiv \alpha \pmod{\pi^i} \quad \text{and } x_i \equiv x_{i+1} \pmod{\pi^{i+1-p}} \tag{5.8}$$

as then $x_i \to x$ and $x^p = \alpha$. We construct this sequence as follows. Set $x_{p+1} = 1$. Given any x_i, we have

$$\frac{\alpha}{x_i^p} \equiv 1 + c_i u_0 \pi^i \pmod{\pi^{i+1}}$$

for some $c_i \in \mathcal{O}$ by the first property of (5.8), so we define

$$x_{i+1} = x_i(1 + c_i u_0 \pi^{i+1-p}).$$

This satisfies the second property of (5.8), so it remains to check the first. Using that $p = \pi^{p-1} u_0$, we verify that

$$\begin{aligned} x_{i+1}^p \equiv x_i^p (1 + c_i \pi^{i+1-p})^p &\equiv x_i^p (1 + c_i p \pi^{i+1-p}) \pmod{\pi^{i+1}} \\ &\equiv x_i^p (1 + c_i u_0 \pi^i) \pmod{\pi^{i+1}} \\ &\equiv \alpha \pmod{\pi^{i+1}}. \end{aligned}$$

Hence, we conclude that $1 + \pi^{p+1}\mathcal{O} \subset (1 + \pi\mathcal{O})^p$ as desired. □

Proof of (ii). Given $\alpha \in \mathbf{Q}_p(\mu_p)^\times / (\mathbf{Q}_p(\mu_p)^\times)^p$, let $\widehat{\alpha} \in \mathbf{Q}_p(\mu_p)$ be a choice of representative. We can write

$$\widehat{\alpha} = \pi^h \eta$$

for some $h \in \mathbf{Z}$ and $\eta \in \mathcal{O}^\times$. The condition that $\alpha \in [\mathbf{Q}_p(\mu_p)^\times / (\mathbf{Q}_p(\mu_p)^\times)^p]^\chi$ (as in Cor. 5.4) is that for $\sigma \in \mathrm{Gal}(\mathbf{Q}_p(\mu_p)/\mathbf{Q}_p)$, we have

$$\sigma(\pi)^h \sigma(\eta) = \sigma(\widehat{\alpha}) = \widehat{\alpha}^{\chi(\sigma)} \beta^p = \pi^{\chi(\sigma)h} \eta^{\chi(\sigma)} \beta^p.$$

for some $\beta \in \mathbf{Q}_p(\mu_p)^\times$ and so is equivalent to $\chi(\sigma)h \equiv h \pmod{p}$. As $p \neq 2$, we have $\chi(\sigma) \neq 1$ and so $h \equiv 0 \pmod{p}$, so if α lies in the χ-eigenspace, we can take $\widehat{\alpha} = \gamma \in \mathbf{Q}_p(\mu_p)^\times / (\mathbf{Q}_p(\mu_p)^\times)^p$ where $\gamma \in \mathcal{O}$. In particular, this applies to the image of $(1 + \pi\mathcal{O})/(1 + \pi^{p+1}\mathcal{O})$ in $\alpha \in \mathbf{Q}_p(\mu_p)^\times / (\mathbf{Q}_p(\mu_p)^\times)^p$ under the inclusion map (5.6) of part (i) and so if $x \in [\mathbf{Q}_p(\mu_p)^\times / (\mathbf{Q}_p(\mu_p)^\times)^p]^\chi$ then, it lies in this image. □

We can now establish the key fact about abelian p-extensions of $\mathbf{Q}_p$ that is needed to prove Lemma 5.1.

Corollary 5.9. *If $p \neq 2$, the maximal abelian extension of $\mathbf{Q}_p$ of exponent p is of degree p^2 and is obtained by joining the p^2-th roots of unity to an unramified extension of degree p.*

Proof. Let $V = (1 + \pi\mathcal{O})/(1 + \pi^{p+1}\mathcal{O})$. We want to show that its χ-eigenspace has the property

$$|V^\chi| = p^2.$$

Note that $\zeta \in V^\chi$, as $\sigma(1 - \pi) = \sigma(\zeta) = \zeta^{\chi(\sigma)}$, and we have the identity

$$\frac{\sigma(\pi)}{\pi} \equiv \frac{1 - \zeta^{\chi(\sigma)}}{1 - \zeta} \equiv 1 + \zeta + \cdots + \zeta^{\chi(\sigma)-1} \equiv \chi(\sigma) \pmod{\pi}. \tag{5.10}$$

Let $\nu \in V^\chi$. By multiplying with an appropriate power of ζ, we can assume that $\nu \equiv 1 \pmod{\pi^2}$ and more generally that

$$\nu \equiv 1 + a_i \pi^i \pmod{\pi^{i+1}}$$

for some $a_i \in \mathbf{Z}$. As (5.10) holds and $\nu \in V^\chi$, we have

$$\begin{aligned} 1 + a_i \pi^i \chi(\sigma)^i &\equiv \sigma(\nu) \pmod{\pi^{i+1}} \\ &\equiv \nu^{\chi(\sigma)} \pmod{\pi^{i+1}} \\ &\equiv (1 + a_i \pi^i)^{\chi(\sigma)} \pmod{\pi^{i+1}} \end{aligned}$$

and so

$$a_i \chi(\sigma)^i \equiv a_i \chi(\sigma) \pmod{\pi}$$

which implies that $a_i \equiv 0 \pmod{\pi}$ or $i = p$. Thus, we can write $\nu = 1 + a\pi^p \pmod{\pi^{p+1}}$ and so

$$V^\chi = \langle \zeta, 1 + \pi^p \rangle,$$

and so $|V^\chi| = p^2$, as desired. □

5.2. **Proof of Lemma 5.1 for p odd.** Recall that the finite unramified extensions of $\mathbf{Q}_p$ correspond to finite extensions of the residue field $\mathbf{F}_p$ and so for any integer $n \geq 1$, there is a unique unramified extension of $\mathbf{Q}_p$ of degree n. (For this and other facts about extensions of $\mathbf{Q}_p$ that we use here, see [Ser79, IV.4].)

To prove the lemma, our strategy is to determine $\mathbf{Q}_p(m)$, the maximal abelian extension of $\mathbf{Q}_p$ of exponent p^m, which contains in particular, the unramified extension of degree p^m and the degree p^m extension included in $\mathbf{Q}_p(\mu_{p^{m+1}})$. We can express $\mathrm{Gal}(\mathbf{Q}_p(m)/\mathbf{Q}_p) \cong \prod_{i=1}^k \mathbf{Z}/p^m\mathbf{Z}$. We want to determine the number of factors k that occur. The number of factors is the same as that of $\mathrm{Gal}(\mathbf{Q}_p(1)/\mathbf{Q}_p)$. As $p \neq 2$, we have $[\mathbf{Q}_p(1) : \mathbf{Q}_p] = p^2$ by Corollary 5.9, so $\mathrm{Gal}(\mathbf{Q}_p(m)/\mathbf{Q}_p)$ admits a presentation with at most two generators. As we know two linearly disjoint extensions in $\mathbf{Q}_p(1)$—the unramified extension of degree p and the totally ramified degree-p subextension of $\mathbf{Q}_p(\mu_{p^2})$—we must have

$$\mathrm{Gal}(\mathbf{Q}_p(1)/\mathbf{Q}_p) \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}.$$

Hence, for any $m \geq 1$, we have

$$\mathrm{Gal}(\mathbf{Q}_p(m)/\mathbf{Q}_p) \cong \mathbf{Z}/p^m\mathbf{Z} \times \mathbf{Z}/p^m\mathbf{Z}.$$

giving us the result in this case. □

5.3. **Proof of Lemma 5.1 for $p = 2$.** As Lemma 5.5 and Corollary 5.9 rely on the prime p being odd, we require a different argument to tackle the $p = 2$ case. In this setting, we simply determine the structure of the Galois groups directly.

For any integer $m \geq 0$, we have

$$\mathrm{Gal}(\mathbf{Q}_2(\mu_{2^{m+2}})/\mathbf{Q}_2) \cong (\mathbf{Z}/2^{m+2}\mathbf{Z})^\times \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^m\mathbf{Z}. \tag{5.11}$$

Our goal is to show that

$$\mathrm{Gal}(\mathbf{Q}_2(m)/\mathbf{Q}_2) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^m\mathbf{Z} \times \mathbf{Z}/2^m\mathbf{Z},$$

where the first two factors come from $\mathrm{Gal}(\mathbf{Q}_2(\mu_{2^{m+2}})/\mathbf{Q}_2)$ and the remaining $\mathbf{Z}/2^m\mathbf{Z}$ factor corresponds to the unramified extensions. We prove this in stages.

Case $m = 1$. Since $\mathbf{Q}_2(1)$ is just the compositum of the quadratic extensions of $\mathbf{Q}_2$, we look for these directly. By Kummer theory (Theorem 5.3), these are classified by subgroups of

$$\mathbf{Q}_2^\times/(\mathbf{Q}_2^\times)^2 \cong \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2 \cong \{2^a(-1)^b5^c\}$$

(see, e.g. [Ser73, II, §3.3, Cor. of Thm 4]). The three factors here correspond to $\mathbf{Q}_2(\sqrt{2})$, $\mathbf{Q}_2(\sqrt{-1})$, and $\mathbf{Q}_2(\sqrt{5})$, of which $\mathbf{Q}_2(\sqrt{-1})$ denotes the sole unramified extension. Hence,

$$\mathrm{Gal}(\mathbf{Q}_2(1)/\mathbf{Q}_2) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}. \tag{5.12}$$

General case. Since we know that $\mathrm{Gal}(\mathbf{Q}_2(m)/\mathbf{Q}_2)$ has two disjoint quotients of order 2^m—the unramified extension and totally ramified one from (5.11)—and (5.12) from the $m = 1$ case, the Galois group of $\mathbf{Q}_2(m)$ over $\mathbf{Q}_2$ must be of the form

$$\mathrm{Gal}(\mathbf{Q}_2(m)/\mathbf{Q}_2) \cong \mathbf{Z}/2^m\mathbf{Z} \times \mathbf{Z}/2^m\mathbf{Z} \times \mathbf{Z}/2^k\mathbf{Z}$$

for some integer $k \geq 1$. We will show that $k = 1$ regardless of our choice of integer m by computing $\mathrm{Gal}(\mathbf{Q}_2(2)/\mathbf{Q}_2)$.

Abstractly, $\mathrm{Gal}(\mathbf{Q}_2(2)/\mathbf{Q}_2) \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2^k\mathbf{Z}$. Suppose for the sake of contradiction that $k \neq 1$. Then $\mathrm{Gal}(\mathbf{Q}_2(2)/\mathbf{Q}_2) \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. This would imply that all quadratic extensions of $\mathbf{Q}_2$—which would all be contained in $\mathbf{Q}_2(2)$—arise as subfields of a $\mathbf{Z}/4\mathbf{Z}$-extension. We will show that this is false, via the following characterization of such fields.

> *Claim.* Let F be a field of characteristic not equal to 2. If $F(\sqrt{\alpha})$ is contained in a cyclic extension of degree 4, then $\alpha = x^2 + y^2$ for some $x, y \in F$.
>
> *Proof of Claim.* Suppose that $F(\sqrt{\alpha}) \subset K$, where K is a cyclic extension of F of degree 4. Then
>
> $$K = F\left(\sqrt{\alpha}, \sqrt{u + v\sqrt{\alpha}}\right)$$
>
> for some $u, v \in F$ by Theorem 5.3(i). The Galois closure of K is $F(\sqrt{\alpha}, \sqrt{u + v\sqrt{\alpha}}, \sqrt{u - v\sqrt{\alpha}})$ and as K/F is Galois with Galois group $G = \mathbf{Z}/4\mathbf{Z}$, we must have
>
> $$K^G = F = F(\sqrt{\alpha(u^2 - v^2\alpha)}) \subsetneq F(\sqrt{\alpha}, \sqrt{u^2 - v^2\alpha})$$
>
> which is equivalent to α not being a square and $\alpha(u^2 - v^2\alpha)$ being a square in F.

Write $\alpha(u^2 - v^2\alpha) = c^2$ for some $c \in F$, so $\alpha u^2 = c^2 + v^2\alpha^2$, and thus

$$\alpha = \left(\frac{c}{u}\right)^2 + \left(\frac{v\alpha}{u}\right)^2$$

as desired. $\diamond$

We apply this claim to $\mathbf{Q}_2(\sqrt{-1})$. Here we find that $\mathbf{Q}_2(\sqrt{-1})$ cannot be contained in a cyclic extension of degree 4, as $-1 = x^2 + y^2$ cannot hold modulo 4, as only 0 and 1 are quadratic residues modulo 4. Thus, we have a contradiction and so we must have $k = 1$. $\square$

6. Proofs of the main theorems

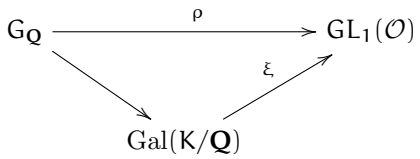
We can now assemble our preliminary results and prove our main theorems.

6.1. **Proof of the "modular" Kronecker–Weber Theorem (Theorem 1.2).** Let K be a finite abelian extension of $\mathbf{Q}$ and write $G = \mathrm{Gal}(K/\mathbf{Q})$ for its Galois group. By the classification of finitely generated abelian groups, G must be a product of cyclic groups of prime-power order. Since K can be expressed as a compositum of appropriate intermediate extensions of prime-power degree, we are reduced to the case where $|G| = p^n$ for some prime p.

Thus, let K be a $\mathbf{Z}/p^n\mathbf{Z}$-extension of $\mathbf{Q}$ and let $\mathcal{O}$ denote the ring of integers of the local field $\mathbf{Q}_p(\mu_{p^n})$, writing $\mathfrak{m}_{\mathcal{O}}$ for its maximal ideal. We have a homomorphism

$$\xi : \mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/p^n\mathbf{Z} \to \mathrm{GL}_1(\mathcal{O})$$

where $\xi(1) = \zeta_{p^n}$, a primitive p^n-th root of unity. Under the quotient $G_{\mathbf{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbf{Q})$, we get a homomorphism $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_1(\mathcal{O})$ that factors through ξ:



As the residue field $k = \mathcal{O}/\mathfrak{m}_{\mathcal{O}}$ is of characteristic p, we must have $\rho \equiv 1 \pmod{\mathfrak{m}_{\mathcal{O}}}$, that is, the residual representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_1(k)$ obtained by composing ρ with the quotient map $\mathrm{GL}_1(\mathcal{O}) \to \mathrm{GL}_1(k)$ is trivial. We want to show that ρ is a *modular* deformation of the trivial residual representation $\overline{1} = 1 \pmod{\mathfrak{m}_{\mathcal{O}}} : G_{\mathbf{Q}} \to \mathrm{GL}_1(k)$ for some prescribed deformation datum $\mathcal{D}$ (Def. 4.3).

Note that ρ is unramified outside of the finite set of places Σ at which K is ramified. By Lemma 5.1, ρ is a deformation of $\overline{1}$ of type $\mathcal{D} = (\Sigma, p^r)$ for some integer $r \geq 1$. By Theorem 4.44, this implies that $\rho \cong \rho_\chi$, where χ is a Dirichlet character of some conductor N and so $K \subseteq \overline{\mathbf{Q}}^{\mathrm{Ker}(\rho)} = \overline{\mathbf{Q}}^{\mathrm{Ker}(\rho_\chi)} \subseteq \mathbf{Q}(\zeta_N)$. $\square$

6.2. **The classical Kronecker–Weber theorem (Theorem 1.1).** We now show that Theorem 1.2 implies the familiar form of the Kronecker–Weber theorem (Theorem 1.1).

Let K be a finite Galois extension of $\mathbf{Q}$ with abelian Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Since the formation of Artin L-functions is invariant under induction (see e.g. [Lan94, XII, §2–3]), the Dedekind zeta function $\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subset \mathcal{O}_K} \frac{1}{(\mathfrak{N}\mathfrak{a})^s}$ for K admits the factorization

$$\zeta_K(s) = \prod_{\rho \in \widehat{G}} L(\rho, s), \tag{6.1}$$

where $\widehat{G}$ denotes the group of characters of G and

$$L(\rho, s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1 - \rho(\mathrm{Frob}_\mathfrak{p})(\mathfrak{N}\mathfrak{p})^{-s}},$$

where $\rho(\mathrm{Frob}_\mathfrak{p})$ refers to the image of the Frobenius element at $\mathfrak{p}$ in the induced Galois representation on $\mathbf{C}^{I_\mathfrak{p}}$ for $I_\mathfrak{p}$ the inertia group at $\mathfrak{p}$.

Using this interpretation, we can exploit the modularity of ρ via Theorem 1.2 to finally prove the classical Kronecker–Weber theorem (Theorem 1.1).

Corollary 6.2. *Let K be an abelian extension of $\mathbf{Q}$. Then there exists an integer $m \geq 1$ such that $K \subset \mathbf{Q}(\mu_m)$, the m-th cyclotomic field.*

Proof. By passing to the Galois closure, we can assume without loss of generality that K is a Galois extension of $\mathbf{Q}$. By (6.1) and Theorem 1.2, we have a factorization

$$\zeta_K(s) = \prod_{i=1}^{m} L(\chi_i, s)$$

where the product runs over some finite set of Dirichlet characters $\{\chi_1, \ldots, \chi_m\}$ and $L(\chi_i, s) = \sum_{n=1}^{\infty} \frac{\chi_i(n)}{n^s}$ denotes the corresponding Dirichlet L-function. Let m be the least common multiple of the conductors $N(\chi_i)$ of χ_i for all i. We want to show that $K \subset \mathbf{Q}(\mu_m)$.

Recall that $E/\mathbf{Q}$ is an intermediate Galois extension of a number field $F/\mathbf{Q}$ if and only if all but finitely many of the rational primes p that split completely in F also split completely in E (e.g. [Mar77, Thm. 29, Cor.]). We want to apply this to $E = K$ and $F = \mathbf{Q}(\mu_m)$. If $p \nmid m$, then p splits completely in $\mathbf{Q}(\mu_m)$ if and only if $p \equiv 1 \pmod{m}$ (e.g. [Bir67, Cor., p.88]). Pick such a prime p. For any character χ modulo m, we thus have $\chi(p) = 1$, so for any Dirichlet character χ_i above, we have $\chi_i(p) = 1$. By Theorem 1.2, we must have $\rho(\mathrm{Frob}_p) = 1$ for all $\rho \in \widehat{G}$, so $\mathrm{Frob}_p = 1 \in G$. Hence, p splits completely in K. We conclude that $K \subset \mathbf{Q}(\mu_m)$. □

References

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[Bir67] B. J. Birch, *Cyclotomic fields and Kummer extensions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 85–93.

[Clo90] Laurent Clozel, *Motifs et formes automorphes: applications du principe de fonctorialité*, Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988), Perspect. Math., vol. 10, Academic Press, Boston, MA, 1990, pp. 77–159.

[CSS97] Gary Cornell, Joseph H. Silverman, and Glenn Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer-Verlag, New York, 1997, Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[Dar95] H. Darmon, *The Shimura-Taniyama conjecture (after Wiles)*, Uspekhi Mat. Nauk **50** (1995), no. 3(303), 33–82.

[DDT94] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154.

[Del77] P. Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, vol. 569, Springer-Verlag, Berlin, 1977, Séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$.

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133.

[DK22] Samit Dasgupta and Mahesh Kakde, *On the Brumer-Stark Conjecture and Refinements*, Survey article for ICM Proceedings 2022, https://arxiv.org/abs/2204.09037 (2022).

[dSL97] Bart de Smit and Hendrik W. Lenstra, Jr., *Explicit construction of universal deformation rings*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 313–326.

[Far06] Laurent Fargues, *Motives and automorphic forms: The (potentially) abelian case*, https://webusers.imj-prg.fr/~laurent.fargues/Motifs_abeliens.pdf (2006), 1–42.

[Kow03] E. Kowalski, *Elementary theory of* L*-functions. I*, An introduction to the Langlands program (Jerusalem, 2001), Birkhäuser Boston, Boston, MA, 2003, pp. 1–20, (See also https://blogs.ethz.ch/kowalski/2009/07/14/kronecker--weber--by--deformation--or--another--bad--reference/).

[Kun74] Ernst Kunz, *Almost complete intersections are not Gorenstein rings*, J. Algebra **28** (1974), 111–115.

[Lan94] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[Len95] H. W. Lenstra, Jr., *Complete intersections and Gorenstein rings*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 99–109.

[Mar77] Daniel A. Marcus, *Number fields*, Springer-Verlag, New York-Heidelberg, 1977, Universitext.

[Maz89] B. Mazur, *Deforming Galois representations*, Galois groups over $\mathbf{Q}$ (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 385–437.

[Neu81] Olaf Neumann, *Two proofs of the Kronecker-Weber theorem "according to Kronecker, and Weber"*, J. Reine Angew. Math. **323** (1981), 105–126.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Rib90] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[Sch98] Norbert Schappacher, *On the history of Hilbert's twelfth problem: a comedy of errors*, Matériaux pour l'histoire des mathématiques au XX^{e} siècle (Nice, 1996), Sémin. Congr., vol. 3, Soc. Math. France, Paris, 1998, pp. 243–273.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[Ser79] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg.

[Ser02] ———, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author.

[Tan57] Yutaka Taniyama, L*-functions of number fields and zeta functions of abelian varieties*, J. Math. Soc. Japan **9** (1957), 330–366.

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[Wei56] André Weil, *On a certain type of characters of the idèle-class group of an algebraic number-field*, Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, Science Council of Japan, Tokyo, 1956, pp. 1–7.

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.