EXERCISES: GALOIS REPRESENTATIONS AND MODULAR FORMS 2023 SAGA WINTER SCHOOL, CIRM, LUMINY

ALEXANDRU GHITZA AND ANNA MEDVEDOVSKY
WITH EMILIANO TORTI (TA)

Exercises Day 1 Exercises Day 2 Exercises Day 3

Exercises Day 1 Back

1. Galois groups

General topological groups (relatively straightforward; skip if you know this story).

Recall that a *topological group* is a group G with a topology so that the multiplication map $G \times G \to G$ and the inversion map $G \to G$ are both continuous.

Let G be a topological group.

(1) Let H be a subgroup of G.
  (a) Show that H is open if and only if it contains a neighborhood of one of its points.
  (b) If H is open, show that it is also closed.
  (c) If H is closed and of finite index, show that H is also open.

(2) Let C be the connected component of the identity element e of G.
  (a) Show that C is a subgroup of G.
  (b) A space is *totally disconnected* if the connected component of every point is that point. Show that G is totally disconnected if and only if $C = \{e\}$.

(3) Now assume that G is compact, and that $H \subseteq G$ is an open subgroup.
  (a) Show that H has finite index.
  (b) Show that H contains a normal open subgroup.

Profinite groups, Krull topology on Galois groups

(4) Show that any finite-index subgroup of $\mathbb{Z}_p$ or $\mathbb{Z}_p^\times$ or $\widehat{\mathbb{Z}}$ is automatically open.

(5) Prove that $\widehat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$ as topological groups (or as even rings).

(6) Let $H = \mathbb{Z}$ be the subgroup of $G_{\mathbb{F}_p}$ generated by the Frobenius automorphism $\alpha \mapsto \alpha^p$. What is the subfield of $\overline{\mathbb{F}}_p$ fixed by H?

(7) Let $G = \prod_{n\geq 0} \mathbb{Z}/2\mathbb{Z}$ with its product topology.

  (a) Show that G is a profinite group.

  (b) Construct a Galois extension L of $\mathbb{Q}$ so that $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$.

  In contrast to (4), one can show that the group G has dense index-2 subgroups (which are therefore not open).

(8) Find a Galois extension $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}_p$. Can you find a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}_p \times \mathbb{Z}_p$? What about $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$? $\prod_{n\geq 0} \mathbb{Z}/p\mathbb{Z}$?

A 2003 theorem of Nikolov and Segal (generalizing an earlier theorem of Serre for pro-p groups) says that any finite-index subgroup of a topologically finitely generated profinite group is automatically open.

Sundries

(9) **Tame inertia of a p-adic local field:** Fix a p-adic local field K with residue field k.

  A finite extension L/K of a p-adic local field K is *tamely ramified* if it is ramified and its ramification index $e = e(L/K)$ is prime to p. It is *at most tamely ramified* if it is either unramified or tamely ramified.

  What does it mean for an infinite extension L/K to be (at most) tamely ramified?

  (a) Let M/K be an unramified algebraic extension and L/K any finite extension. Show that $e(LM/M) = e(L/K)$.

  (b) Let K^{ur} be the maximal unramified extension of K, and fix a uniformizer π of K. Show that a tamely ramified finite extension L of K^{ur} is a Kummer extension: there exists $n > 1$ coprime to p such that $L = K^{\mathrm{ur}}(\pi^{1/n})$.

  In particular, such an extension is automatically Galois. What is $\mathrm{Gal}(L/K^{\mathrm{ur}})$?

  (c) Deduce that if L/K^{ur} and M/K^{ur} are two finite tamely ramified extensions, then so is LM/K^{ur}.

  (d) Conclude that any extension L/K has a maximal at-most-tamely-ramified subextension L^{tr}. (*Hint:* To show that at-most-tamely-ramified extensions behave well in composita, translate up to K^{ur}.)

  (e) Let K^{tr} be the maximal at-most-tamely-ramified extension of K, containing K^{ur} as a subextension. Show that the *tame inertia* $I_K^{\mathrm{tr}} := \mathrm{Gal}(K^{\mathrm{tr}}/K^{\mathrm{ur}})$ is procyclic, isomorphic to $\prod_{\ell\neq p} \mathbb{Z}_\ell$.

  To continue this line of investigation, see (29) and (31).

  The kernel of the map $I_K \to I_K^{\mathrm{tr}}$ is the *wild inertia* $I_K^{\mathrm{wild}} := \mathrm{Gal}(\overline{K}/K^{\mathrm{tr}})$. One can show that the wild inertia is pro-p, so that it is the (normal, hence unique) p-Sylow subgroup of I_K. In other words, the degree $[L^{\mathrm{tr}} : L^{\mathrm{ur}}]$ in every finite Galois L/K is exactly the prime-to-p part of $e(L/K)$. It follows that G_K is a solvable group.

(10) **Unramified elements of p-adic local field:** Let $\mathbb{Q}_p$ be a p-adic local field, and $\alpha \in \overline{\mathbb{Q}}_p$ an algebraic element. Call α *unramified* if $\mathbb{Q}_p(\alpha)$ is an unramified

extension of $\mathbb{Q}_p$. Can you find a simple criterion determining whether α is an unramified element or not? What if α is a tamely ramified element, as in (9)? Open-ended question; tell us if you come up with something good.

(11) **Chebotarev density theorem:** The classical theorem of Chebotarev is about the density of primes whose Frobenius elements fall into particular conjugacy classes in a Galois group. Specifically, let L/K be a finite Galois extension of number fields, and $C \subset \mathrm{Gal}(L/K)$ a conjugacy class. The theorem states that the set of primes of K that are unramified in L and whose Frobenius elements fall into C is $\frac{\# C}{\# \mathrm{Gal}(L/K)}$.

In the context of Galois representations, we want to know about the density of Frobenius conjugacy classes at unramified primes in an infinite Galois group — a completely different use of the word density. Use the classical Chebotarev density theorem to deduce the following useful statement:
For a number field K and a finite set S of primes of K, the conjugacy classes of Frobenius elements at primes not in S is dense in $G_{K,S}$.

(12) **Absolute values:** An *absolute value* on a field K is a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ that's nondegenerate ($|x| = 0$ if and only if $x = 0$), multiplicative ($|xy| = |x||y|$), and subadditive (triangle inequality: $|x + y| \leq |x| + |y|$).

An absolute value induces a metric topology on K.

(a) Show that the map $|x| = \left\{\begin{matrix} 0 & \text{if } x = 0 \\ 1 & \text{otherwise} \end{matrix}\right\}$ is an absolute value on any field. What topology does it induce?

(b) Let K is a p-adic local field and $v : K \to \mathbb{Z} \cup \{\infty\}$ its valuation. For any $a \in (0, 1)$ show that $|x| = a^{v(x)}$ is an absolute value on K that is *ultrametric* (also, *nonarchimedian*): it satisfies $|x + y| \leq \max\{|x|, |y|\}$.

(c) Let K be a field, and $|\cdot|_1$ and $|\cdot|_2$ absolute values on K. Prove (or look up a proof) that the following are equivalent.

(i) The absolute values $|\cdot|_1$ and $|\cdot|_2$ induce the same topology on K.

(ii) The sets $U_1 := \{x \in K : |x|_1 < 1\}$ and $U_2 := \{x \in K : |x|_2 < 1\}$ coincide.

(iii) There exists a positive real number c so that $|x|_1^c = |x|_2$ for all $x \in K$.

If these properties are satisfied, then $|\cdot|_1$ and $|\cdot|_2$ are said to be *equivalent*.

In fact, you can relax property (ii) above to (a priori) one-sided containment. See Corollary 2.4 in Keith Conrad's writeup Equivalence of absolute values.

Ostrowski's theorem (generalized) says that if K is a number field, then the inequivalent absolute values on K are exactly those induced by the valuations corresponding to the prime ideals K and the archimedian absolute values induced from embeddings $K \hookrightarrow \mathbb{R}$ and pairs of conjugate embeddings $K \hookrightarrow \mathbb{C}$. See, for example, Conrad's writeup Ostrowski for number fields.

Exercises Day 2 Back

2. Galois representations

Recommendation: start with (17), (19), and maybe (18). Move on to (25)–(28). Maybe visit (33) at the end. Then come back.

Representations over a field

(13) Let F be a field, V an F-vector space of dimension n.
Let G be a group and $\rho : G \to \mathrm{GL}(V)$ be a representation.

(a) Let D be the set of all endomorphisms of the representation (ρ, V). Then D is naturally an F-subalgebra of $\mathrm{End}_F V$. Show that if V is irreducible, then D is a division ring. (This is Schur's lemma.)

(b) Let R be the F-subspace of $\mathrm{End}_F V$ generated by the image of ρ. Show that R is also an F-subalgebra of $\mathrm{End}_F V$. Show that D is the centralizer $Z(R)$ of R inside $\mathrm{End}_F V$.

(The *centralizer* $Z(R)$ of R is the set of elements that commute with R.)

(c) The *double centralizer theorem* says that if V is irreducible, then $R = Z(D)$ as well. Prove this, look up a proof, or simply take it on faith.

(d) Assume that V is irreducible. Show that $R = \mathrm{End}_F V$ if and only if $D = F$. Show that both of these hold when F is algebraically closed.

(14) **Base field extension; absolute irreducibility:** Continue with the notation of (13). Let E be an extension of F, and let (ρ_E, V_E) be the representations $\rho_E : G \to \mathrm{GL}_E(V \otimes_F E)$ obtained by composing ρ with the natural injection $\mathrm{GL}_F(V) \to \mathrm{GL}_E(V \otimes E)$. Denote by R_E and D_E the R and D corresponding to this representation over E.

(a) Show that $\dim_E R_E = \dim_F R$ and $\dim_E D_E = \dim_F D$.

(b) Show that the following properties are equivalent.

(i) ρ_E is irreducible for all extensions E of F

(ii) ρ_E is irreducible for all finite extensions E of F

(iii) ρ_E is irreducible for E an algebraic closure of F.

(iv) $R = \mathrm{End}_F V$.

If these properties hold, V is said to be *absolutely irreducible*.

(c) Give an example of a representation of dimension 2 that is irreducible but not absolutely irreducible. Show that in any such example, D is a commutative field, namely a quadratic extension of F; and if $E = D$, then ρ_E is not irreducible.

(15) **Strong irreducibility:** Let G be a compact topological group and (ρ, V) a representation of G. We say that V is *strongly irreducible* if the restriction of ρ to any open subgroup of G is still irreducible. Give an example of a strongly but not absolutely irreducible representation, and of an absolutely but not strongly irreducible representation.

Artin representations

(16) **Artin representations have finite image:** For any field K, show that a continuous representation $\rho : G_K \to \mathrm{GL}_n(\mathbb{C})$ has finite image as follows.

  (a) First prove the following

  Lemma.
  There is a neighborhood U of 1 in $\mathrm{GL}_n(\mathbb{C})$ that contains no nontrivial subgroups.

  Here's how: consider $\exp : M_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ defined by the power series

$$\exp A = \sum_{n \geq 0} \frac{A^n}{n!}.$$

  This is a diffeomorphism from an open neighborhood W of 0 in $M_n(\mathbb{C})$ to an open neighborhood of 1 in $\mathrm{GL}_n(\mathbb{C})$.

   (i) Show that if $A, B \in M_n(\mathbb{C})$ commute, then $\exp(A + B) = \exp(A)\exp(B)$. (Don't get stuck on this one — just assume it and move on if necessary.)

   (ii) Now take $B_r(0)$ (a ball of radius r around 0) contained in W, and let $U := \exp\big(B_{r/2}(0)\big)$. Suppose U contains a subgroup of $\mathrm{GL}_n(\mathbb{C})$ with a nontrivial element $g = \exp(A)$ for some A in $B_{r/2}(0)$. Find n so that $g^n \notin U$ to get a contradiction.

  (b) Use the lemma to finish the proof!

(17) **A one-dimensional Artin representation:** Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic extension of $\mathbb{Q}$. Define the Artin representation

$$\chi : G_{\mathbb{Q}} \to \mathrm{Gal}(L/\mathbb{Q}) \simeq \{\pm 1\} \subset \mathrm{GL}_1(\mathbb{C}).$$

Suppose p is a prime unramified in L (assume that $p \nmid 2d$ to be safe).
What is $\chi(\mathrm{Frob}_p)$?

(18) **One-dimensional Artin representations of $G_{\mathbb{Q}}$ and Dirichlet characters:** More generally, let $\chi : G_{\mathbb{Q}} \to \mathbb{C}^\times$ be a character (continuous, of course!). Show that there is a Dirichlet character ψ so that $\chi(\mathrm{Frob}_p) = \psi(p)$ for all but finitely many primes p.

(19) **A two-dimensional Artin representation:** Let $L/\mathbb{Q}$ be a degree-6 extension, the splitting field of an irreducible monic cubic polynomial $f(x)$ in $\mathbb{Z}[X]$, so that $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$.

Let $\sigma : S_3 \to \mathrm{GL}_2(\mathbb{C})$ be the irreducible two-dimensional representation. (This is the *standard representation* of S_3, which you can realize as follows. Let S_3 act on $\mathbb{C}^3$ by permuting the coordinates, and take the subrepresentation on the plane $x+y+z=0$.)

We thus obtain the Artin representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{Gal}(L/\mathbb{Q}) \simeq S_3 \xrightarrow{\sigma} \mathrm{GL}_2(\mathbb{C}).$$

Determine $\mathrm{tr}\rho(\mathrm{Frob}_p)$ for p unramified in L; it will depend on some property of $f(x)$ relative to p.

To fix ideas, you may assume that $f(x) = x^3 - x^2 + 1$ if you like. (In this case you may eventually want to explore the connection between ρ and the modular form https://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/23/1/b/a/.)

(20) Following from (19), what can you say more generally about the case of irreducible f of degree n? Keith Conrad's writeup Factoring after Dedekind may be helpful. Or see Tim and Vladimir Dokchitser's Identifying Frobenius elements in Galois groups from 2010.

Brauer-Nesbitt theorem

(21) Give an example of two nonisomorphic representations of a group over a characteristic-zero field that have the same trace function.

(22) Give an example of two nonisomorphic semisimple representations of a group over a field of characteristic p with the same trace function.

(23) The full Brauer-Nesbitt theorem says that if $\rho_1, \rho_2 : G \to \mathrm{GL}_n(F)$ are two semisimple representations of a group G over any field F, then $\rho_1 \simeq \rho_2$ if and only if we have

$$\operatorname{charpoly}\big(\rho_1(g)\big) = \operatorname{charpoly}\big(\rho_2(g)\big) \qquad \text{in } F[X]$$

for every $g \in G$.

If $\operatorname{char} F = 0$, deduce that it suffices to know $\mathrm{tr}\rho_1(g) = \mathrm{tr}\rho_2(g)$ in F for every $g \in G$. Can you ever use this trace version if $\operatorname{char} F = p$?

Invariant lattice in a representation of a compact group over a p-adic local field

(24) Let F be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}$ its ring of integers, and V a finite-dimensional vector space over F. A *lattice* Λ in V is a finite $\mathcal{O}$-submodule that generates V as a vector space.

(a) Show that if Λ is a lattice, then there is a basis of V such that Λ is the set of vectors that have coefficients in $\mathcal{O}$ in that basis.

(b) Show that if Λ and Λ' are lattices, so is $\Lambda + \Lambda'$.

(c) Let (ρ, V) be a continuous representation of a compact topological group G. Show that there is a lattice in V stable by $\rho(G)$.

Cyclotomic characters

(25) What is the p-adic cyclotomic character on G_K for $K = \mathbb{R}$? Explain.

(26) (a) How big is the extension $\mathbb{F}_7(\zeta_{19})/\mathbb{F}_7$?
Describe the image of its Galois group in $(\mathbb{Z}/19\mathbb{Z})^\times$.

(b) Describe the p-adic cyclotomic character on G_K for $K = \mathbb{F}_\ell$. (Here $\ell \neq p$.)

(27) Describe the p-adic cyclotomic character on G_K for K a finite extension of $\mathbb{Q}_\ell$? (Here again $\ell \neq p$.)

(28) Describe the p-adic cyclotomic character on G_K for K a number field.

(29) **More tame inertia:** Let K be a p-adic local field and k its residue field; let I_K^{tr} be the tame inertia of K as in (9). Show that the action of $G_k \simeq \mathrm{Gal}(K^{\mathrm{ur}}/K)$ induced by the exact sequence

$$1 \to I_K^{\mathrm{tr}} \to \mathrm{Gal}(K^{\mathrm{tr}}/K) \to G_k \to 1$$

is by the ℓ-adic cyclotomic character $G_k \to \mathbb{Z}_\ell^\times$ on the the ℓ-component of I_K^{tr}. This is sometimes captured in the notation $I_K^{\mathrm{tr}} = \prod_{\ell \neq p} \mathbb{Z}_\ell(1)$.

(30) (Don't get stuck on this one — come back to it if you need to!)
Consider the group homomorphism $\chi : \mathbb{Z} \to \mathbb{Z}_p^\times$ defined by $\chi(1) = \alpha$ in $\mathbb{Z}_p^\times$.

(a) For which α does χ extend to a continuous character $\mathbb{Z}_p \to \mathbb{Z}_p^\times$?

(b) For which α does χ extend to a continuous character $\mathbb{Z}_\ell \to \mathbb{Z}_p^\times$ for $\ell \neq p$?

(c) For which α does χ extend to a continuous character $\widehat{\mathbb{Z}} \to \mathbb{Z}_p^\times$?

(31) Let K be a p-adic local field. Show that an unramified n-dimensional representation of G_K is determined by a single matrix in $\mathrm{GL}_n(\mathbb{Q}_p)$ with invertible integral eigenvalues. What can you say about a tamely ramified representation of G_K?

3. Tate modules of elliptic curves

(32) **Isogenies as rational maps**

Let K be a field of characteristic $\neq 2, 3$. You may assume that all the elliptic curves we consider have a simplified Weierstrass equation of the form

$$y^2 = x^3 + Ax + B.$$

Consider an isogeny $\alpha \colon E_1 \to E_2$. In homogeneous coordinates it is of the form $\alpha([X : Y : Z]) = [\alpha_X : \alpha_Y : \alpha_Z]$ with $\alpha_X, \alpha_Y, \alpha_Z \dots$. On the affine piece $E_1 \setminus \{\mathcal{O}\}$ we have

$$\alpha(x, y) = (r_1(x, y), r_2(x, y)), \qquad \text{with } r_1, r_2 \in K(x, y).$$

(a) Show that

$$r_1(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}, \qquad \text{with } p_i \in K[x]. \tag{3.0.1}$$

(b) Refining this, show that

$$r_1(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}, \qquad \text{with } q_i \in K[x].$$

(Hint: Multiply numerator and denominator of Eq. (3.0.1) by $p_3(x) - p_4(x)y$.)

(c) Use the multiplication by -1 on E_1 and the fact that α is a group homomorphism to deduce that $r_1(x, y) = r_1(x, -y)$ and therefore that $q_2 = 0$.

(d) Proceed with $r_2(x,y)$ in a similar manner and conclude that α is given by the *standard form*

$$\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}\, y\right)$$

with $u, v, s, t \in K[x]$ such that u, v are relatively prime, and s, t are relatively prime.

(e) With the notation above, let $f_1 \in K[x]$ be such that E_1 is given by $y^2 = f_1(x)$. Show that $v^3 \mid t^2$ and $t^2 \mid v^3 f_1$. Conclude that v and t have the same roots in $\overline{K}$.

(f) (This one's a bit nasty. Feel free to skip, or have a look at Corollary 5.23 of Andrew Sutherland's 2015 notes on elliptic curves, the section on isogenies.)

Show that the kernel of α consists of the point at infinity $\mathcal{O}$ together with the set

$$\ker\alpha = \{\mathcal{O} = [0\colon 1\colon 0]\} \cup \{[x_0\colon y_0\colon 1] \in E(\overline{K})\colon v(x_0) = 0\}.$$

Conclude that $\ker\alpha$ is finite.

(g) Take it for granted that, given the standard form of α described above, the degree of α equals $\max\{\deg(u), \deg(v)\}$, and that α is separable if the derivative $(u/v)'$ is nonzero.

Let $p > 2$ be prime. Find the standard form of the Frobenius isogeny $F\colon E \to E$, $F(x,y) = (x^p, y^p)$ and use it to: determine the degree of F, show that F is inseparable, and show that $1 - F$ is separable.

Tate modules of elliptic curves over arbitrary fields

(33) Let E_1 and E_2 be two elliptic curves over a field K, and let $\alpha : E_1 \to E_2$ be an isogeny (nonzero by definition) defined over an extension L of K.

Fix a prime p; feel free to assume that $p \neq \operatorname{char} K$.

(a) Show that α induces a G_L-equivariant embedding of Tate modules $T_p(E_1) \hookrightarrow T_p(E_2)$.

(b) Show by example that this embedding need not be surjective.

(c) Show that in any case α induces an isomorphism of G_L-representations

$$T_p(\alpha) : V_p(E_1) \xrightarrow{\sim} V_p(E_2).$$

(d) Show that the resulting map $\operatorname{Hom}(E_1, E_2) \to \operatorname{Hom}\big(T_p(E_1), T_p(E_2)\big)$ is an injective homomorphism of abelian groups.

More precisely, for every extension L of K, isogenies defined over L induce G_L-equivariant maps on Tate modules: $\operatorname{Hom}_L(E_1, E_2) \to \operatorname{Hom}_{G_L}\big(T_p(E_1), T_p(E_2)\big)$.

(In fact, these maps stay injective when $\operatorname{Hom}(E_1, E_2)$ is replaced by $\operatorname{Hom}(E_1, E_2) \otimes \mathbb{Z}_p$; see Silverman, Theorem III.7.4.)

(e) Finally, if $E_1 = E_2 = E$ and L is an extension of K, then we get a ring homomorphism $\operatorname{End}_L(E) \hookrightarrow \operatorname{End}_{G_L}\big(V_p(E)\big)$.

(34) Now let E be an elliptic curve defined over K.

(a) Suppose that $V_p(E)$ is absolutely irreducible as a G_L-representation for some extension L of K. Show that any isogeny from E to E defined over L is actually defined over K.

(b) If $V_p(E)$ is absolutely irreducible as a G_K-representation, show that $\mathrm{End}_K(E) = \mathbb{Z}$.

(c) If $V_p(E)$ is *strongly* absolutely irreducible as a G_K-representation (that is, $V_p(E)$ stays absolutely irreducible when restricted to G_L for any finite extension L of K), show that $\mathrm{End}_{\bar{K}}(E) = \mathbb{Z}$.

(d) Show that the converse (that is, $\mathrm{End}_K(E) = \mathbb{Z}$ means $V_p(E)$ is absolutely irreducible as a G_K-representation) is false in general.

However, it's true for number fields, by a theorem of Serre. In particular, if $K = \mathbb{Q}$, then $V_p(E)$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation, as $\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$.

More on this topic next time!

Exercises Day 3 Back

4. Tate modules of elliptic curves, continued

(35) **Weil pairing, complex version**

(For the purposes of this question only, you may assume that every elliptic curve is defined over the complex numbers and use the complex uniformization $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Note however that all the definitions and statements from this question hold for elliptic curves over arbitrary fields—obviously, different proofs may be needed then.)

Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$ with $\omega_1/\omega_2 \in \mathbb{H}$ and let $E = \mathbb{C}/\Lambda$ be the complex elliptic curve it defines. Let $N \geq 1$.

(a) Fix $P, Q \in E[N]$. Show that there exists $\gamma \in M_2(\mathbb{Z}/N\mathbb{Z})$ such that

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} \frac{\omega_1}{N} + \Lambda \\ \frac{\omega_2}{N} + \Lambda \end{pmatrix}.$$

(b) Set

$$e_N(P, Q) = e^{(2\pi i \det \gamma)/N}.$$

Show that e_N is independent of the various apparent choices, including the choice of basis $\{\omega_1, \omega_2\}$ of Λ with $\omega_1/\omega_2 \in \mathbb{H}$.

(c) Show that e_N is a bilinear, alternating, non-degenerate pairing (part of the work is figuring out what these words should mean in this setting, keeping in mind that $E[N]$ is additive and μ_N is multiplicative):

$$e_N \colon E[N] \times E[N] \longrightarrow \mu_N.$$

such that for any integers N and M we have

$$e_N(MP, Q) = e_{MN}(P, Q) \qquad \text{for all } P \in E[MN], Q \in E[N].$$

(d) Let $\psi\colon E_1 \to E_2$ be an isogeny. Show that

$$e_N(\psi(P), Q) = e_N(P, \psi^\vee(Q)) \qquad \text{for all } P \in E_1[N], Q \in E_2[N].$$

(e) Show that there is an ℓ-adic Weil pairing

$$e\colon T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\mu) := \varprojlim_n \mu_{\ell^n}$$

that is bilinear, alternating, and nondegenerate.

(f) Let $\psi\colon E_1 \to E_2$ be an isogeny and let $\psi_\ell\colon T_\ell(E_1) \to T_\ell(E_2)$ denote the induced map on Tate modules. Then

$$e(\psi_\ell(v), w) = e(v, \psi_\ell^\vee(w)) \qquad \text{for all } v \in T_\ell(E_1), w \in T_\ell(E_2).$$

(g) Let $\psi \in \mathrm{End}(E)$ and let ℓ be prime. Let $\psi_\ell \in \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E))$ be the induced map on the Tate module. Show that

$$\det(\psi_\ell) = \deg(\psi), \qquad \mathrm{Tr}(\psi_\ell) = 1 + \deg(\psi) - \deg(1 - \psi).$$

(*Hint*: Choose basis vectors v_1, v_2 for $T_\ell(E)$ and use the properties of the Weil pairing to show that $e(v_1, v_2)^{\deg(\psi)} = e(v_1, v_2)^{\det(\psi_\ell)}$. For the statement about the trace, show that the relevant claim relating trace and determinants holds for any 2×2 matrix.)

(36) **Bad reduction examples**

(a) Show that $E/\mathbb{Q}_5$ given by $y^2 = x^3 - x^2 + 35$ has split multiplicative reduction.

(b) Show that $E/\mathbb{Q}_7$ given by $y^2 = x^3 - x^2 + 35$ has nonsplit multiplicative reduction. Find an extension K of $\mathbb{Q}_7$ over which E acquires split multiplicative reduction.

(c) Show that $E/\mathbb{Q}_5$ given by $y^2 = x^3 + 5$ has additive reduction. Find an extension K of $\mathbb{Q}_5$ over which E acquires good or split multiplicative reduction.

[One possibility is to follow the proof of the Semistable Reduction Theorem (Silverman, Proposition VII.5.4).]

Isomorphic Tate modules vs. isogenous curves

(37) **Over finite fields:** Let E_1 and E_2 be two elliptic curves over a finite field $K = \mathbb{F}_p$. Show that the following are equivalent.

(a) $V_\ell(E_1) \simeq V_\ell(E_2)$ as G_K-representations for one prime $\ell \neq p$

(b) $V_\ell(E_1) \simeq V_\ell(E_2)$ as G_K-representations for all primes $\ell \neq p$

(c) $\#E_1(K) = \#E_2(K)$

Does the same argument work over $K = \mathbb{F}_{p^2}$?

A theorem of Tate (see "Endomorphisms of abelian varieties over finite fields," Invent. Math. 1966) says that the equivalence holds over any finite field, and that these properties are equivalent to E_1 and E_2 being isogenous.

(38) **Over number fields:** Let E_1 and E_2 be two elliptic curves over a number field K.

(a) Show that the following are equivalent.

(i) $V_\ell(E_1) \simeq V_\ell(E_2)$ as G_K-representations for one prime ℓ.

(ii) $V_\ell(E_1) \simeq V_\ell(E_2)$ as G_K-representations for all primes ℓ.

(iii) For almost all finite places v of K for which E_1 and E_2 have good reduction at v, we have $\#\widetilde{E}_{1,v}(k_v) = \#\widetilde{E}_{2,v}(k_v)$. Here $E_{i,v}$ is E_i over the completion K_v, and $\widetilde{E}_{i,v}$ is E_i over the residue field k_v.

(b) Show that these properties hold if E_1 and E_2 are isogenous over K.

A theorem of Faltings tells us that these properties hold if **and only if** E_1 and E_2 are isogenous.

(39) **Over p-adic local fields:** Show that there exist two elliptic curves E_1 and E_2 over $\mathbb{Q}_p$ whose Galois representations $V_\ell(E_1)$ and $V_\ell(E_2)$ are isomorphic but that are not isogenous over $\mathbb{Q}_p$. Proceed as follows.

(a) Let E_1 and E_2 be two curves over $\mathbb{Q}_p$ both with good reduction. Show that if $\#\widetilde{E}_1(\mathbb{F}_p) = \#\widetilde{E}_2(\mathbb{F}_p)$, then $V_\ell(E_1) \simeq V_\ell(E_2)$ as representations of $G_{\mathbb{Q}_p}$ for all primes ℓ.

(b) Deduce that there are only a finite number of isomorphism classes of Galois representations of $G_{\mathbb{Q}_p}$ of the form $V_\ell(E)$ when E runs over all elliptic curves over $\mathbb{Q}_p$ with good reduction.

(c) Show that the set of $\mathbb{Q}_p$-isomorphism classes of elliptic curves having good reduction is uncountable.

(d) Show that the isogeny class (over a fixed base field) of an elliptic curve has at most countably many isomorphism classes of elliptic curves.

(e) Conclude.

Surprisingly, if one assumes that E_1, E_2 over $\mathbb{Q}_p$ do *not* have good reduction but do have isomorphic Galois representations, then they are in fact isogenous. This is a theorem of Serre and Tate.

(40) **Tate modules for ECs with multiplicative reduction over p-adic local fields:** Tate's p-adic uniformization (stated below in full; see Silverman II) tells us that, given an elliptic curve E over a p-adic local field K with split multiplicative reduction, there is a unique nonzero q in the maximal ideal of K so that there is an isomorphism

$$E(\overline{K}) \simeq (\overline{K})^\times / q^{\mathbb{Z}}$$

commuting with the action of G_K.

Now let E be such an elliptic curve over such a K, and fix a prime ℓ.

(a) Compute $E[\ell]$ and $E[\ell^n]$.

(b) Compute $T_\ell(E)$ with its G_K-action.

(c) Assume $\ell \neq p$.

(i) Show that $T_\ell(E)$ is at most tamely ramified.

(ii) Consider the representation $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$ carried by $E[\ell] = T_\ell(E) \otimes \mathbb{F}_\ell$. Under what conditions is $\bar{\rho}$ unramified?

(iii) What is the connection with Ribet's level-lowering theorem discussed by Samir and Samuele?

(d) Assume $K = \mathbb{Q}_p$. What can you say about $T_p(E)$? Must it be wildly ramified? Is it possible that $E[p] = T_p(E) \otimes \mathbb{F}_p$ is tamely ramified?

(e) Start over, and now suppose that E is isomorphic to E_q defined below only over L, where L/K is the unique unramified extension of K, and not over K. Anything you can say?

Theorem (Tate p-adic uniformization)**.**
Let K be a finite extension of $\mathbb{Q}_p$, with absolute value $|\cdot|$.

(a) If $q \in K^\times$ satisfies $|q| < 1$, then the equation

$$E_q \colon y^2 + xy = x^3 + a_4(q)x + a_6(q),$$

where $a_4(q) = -5s_3(q)$ and $a_6(q) = -\frac{1}{12}\big(5s_3(q) + 7s_5(q)\big)$ for $s_k(q) = \sum_{n=1}^\infty \frac{n^k q^n}{1-q^n}$, defines an elliptic curve over K with discriminant $\Delta(E_q) = q\prod_{n\geq 1}(1-q^n)^{24}$ and j-invariant $j(E_q) = \frac{1}{q} + 744 + 196884q + \cdots$.

(b) There is an isomorphism $(\overline{K})^\times/q^{\mathbb{Z}} \to E_q(\overline{K})$ that commutes with the action of G_K. In particular, this gives an isomorphism $L^\times/q^{\mathbb{Z}} \to E_q(L)$ for any algebraic extension L of K.

(c) If E is an elliptic curve over K with $|j(E)| > 1$, then there is a unique $q \in \overline{K}^\times$ with $|q| < 1$ such that $E \simeq E_q$ over $\overline{K}$. Moreover, $q \in K^\times$.

(d) In the previous part, $E \simeq E_q$ over K if and only if E has split multiplicative reduction.

5. Modular forms and Galois representations

(41) **Eisenstein series:** For an integer $k > 2$, consider

$$G_k(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^k}.$$

(a) Show that the series converges absolutely for all $z \in \mathbb{H}$.

(b) Conclude that $G_k \colon \mathbb{H} \to \mathbb{C}$ is holomorphic.

(c) Show that if k is odd then G_k is identically zero.

(d) The behavior of G_k at $i\infty$ is governed by the summands with $m = 0$, that is

$$G_k(i\infty) = \sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{1}{n^k} = 2\zeta(k).$$

(e) Show that

$$G_k(z+1) = G_k(z) \quad \text{and} \quad G_k(-1/z) = z^k G_k(z)$$

for all $z \in \mathbb{H}$ and conclude that G_k is a modular form of weight k on $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.

(f) Take for granted the crazy-looking infinite product expansion

$$\sin(\pi z) = \pi z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2}\right).$$

Show that

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n}\right) = \sum_{n\in\mathbb{Z}} \frac{1}{z+n}. \tag{5.0.1}$$

(*Hint:* take logarithmic derivative.)

(g) Using the definition of the cotangent function, show that

$$\pi \cot(\pi z) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n, \tag{5.0.2}$$

where, as usual, $q = e^{2\pi i z}$.

(h) Combining Eqs. (5.0.1) and (5.0.2), show that for any $k \geq 2$ we have

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n,$$

where $q = e^{2\pi i z}$ with $z \in \mathbb{H}$.

(i) Show that for any $k > 2$ even

$$G_k(z) = 2\zeta(k) + \frac{2(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n,$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

(j) What is the ℓ-adic Galois representation of $G_{\mathbb{Q}}$ attached to G_k?

(42) (a) The Hecke operator T_n ($n \in \mathbb{N}$) on $S_k(1, \mathbf{1})$ is given on Fourier expansions by

$$T_n f = \sum_{m=1}^{\infty} \sum_{d|\gcd(m,n)} d^{k-1} a_{mn/d^2} q^m.$$

Let $f \in S_k(1, \mathbf{1})$, $f(z) = \sum_{n=1}^{\infty} a_n q^n$, be an eigenvector for all Hecke operators T_n ($n \in \mathbb{N}$) with eigenvalues λ_n. Show that $a_1 \neq 0$ and $a_n = \lambda_n a_1$ for all $n \geq 1$. (The same statement holds for **newforms** $f \in S_k(N, \varepsilon)$.)

(b) Let $V \subset M_k(\Gamma_1(N))$ be a subspace that is stable under the action of T_p for all $p \nmid N$. Let $\mathbb{T}$ denote the $\mathbb{Z}$-subalgebra of $\mathrm{End}(V)$ generated by the Hecke operators T_p with $p \nmid N$. Let $\mathbb{T}_{\mathbb{C}} = \mathbb{T} \otimes \mathbb{C}$. Show that

$$\mathbb{T}_{\mathbb{C}} \times V \to \mathbb{C}$$

given by $\langle T, f\rangle = a_1(T(f))$ is a perfect pairing.

Show that the two resulting isomorphisms $\mathbb{T}_{\mathbb{C}} \to V^\vee$ and $V \to \mathbb{T}_{\mathbb{C}}^\vee$ are $\mathbb{T}_{\mathbb{C}}$-equivariant.

(c) Show that $\mathbb{T}$ has finite $\mathbb{Z}$-rank.

(d) Let $f \in M_k(\Gamma_1(N))$ be an eigenvector for all Hecke operators T_p with $p \nmid N$, with eigenvalues a_p, and let

$$K_f = \mathbb{Q}\big(\{a_p : p \nmid N\}\big).$$

Show that K_f is a number field.

(43) **Modular forms for $\Gamma_1(N)$:** Given an integer $N \geq 1$, consider the subgroup

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon c \equiv 0 \pmod N, a \equiv d \equiv 1 \pmod N \right\}.$$

Let $M_k(\Gamma_1(N))$ denote the vector space of holomorphic functions $f \colon \mathbb{H} \to \mathbb{C}$ that are holomorphic at the cusps and satisfy

$$f|_k[\alpha] = f \qquad \text{for all } \alpha \in \Gamma_1(N),$$

where the slash operator is defined by

$$f|_k[\alpha](z) = \det(\alpha)^{k/2}(cz+d)^{-k} f(\alpha \cdot z), \qquad \alpha \cdot z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

(a) Show that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$.

(b) Show that $f|_k[\alpha] \in M_k(\Gamma_1(N))$ for all $f \in M_k(\Gamma_1(N))$ and all $\alpha \in \Gamma_0(N)$.

(c) Fix $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Show that $f \mapsto \langle d \rangle f := f|_k[\alpha]$ for any $\alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$ with $\delta \equiv d \pmod N$, gives a well-defined map

$$\langle d \rangle \colon M_k\big(\Gamma_1(N)\big) \to M_k\big(\Gamma_1(N)\big).$$

(d) Show that

$$M_k\big(\Gamma_1(N)\big) = \bigoplus_{\varepsilon} M_k(N, \varepsilon),$$

where the sum ranges over all Dirichlet characters ε modulo N.
(*Hint:* for any ε, show that

$$\pi_\varepsilon = \frac{1}{\varphi(N)} \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \varepsilon^{-1}(d) \langle d \rangle$$

defines a projection operator $\pi_\varepsilon \colon M_k(\Gamma_1(N)) \to M_k(N, \varepsilon)$.)

(44) **Induction of a character:** Let G be a group, and $H \subset G$ a subgroup of index 2. Let F be a field with $\operatorname{char} F \neq 2$. Let $\chi : H \to F^\times$ be a character. Choose $c \in G - H$.

(a) Define ${}^c\chi : H \to F^\times$ by ${}^c\chi(h) = \chi(c^{-1}hc)$ for $h \in H$. Prove that ${}^c\chi$ is a character of H. Prove that ${}^c\chi$ is independent of the choice of c.

(Alternative formulation: For *any* $c \in G$, set $c \cdot \chi := {}^c\chi$ as above and show that this defines an action (right or left?) of G on the set of characters $H \to F^\times$. Show that the action factors through G/H.)

Let $\eta : G \to \{\pm 1\} \subseteq F^\times$ be the quadratic character with kernel H.

(b) Show that the following defines a representation $\rho : G \to \mathrm{GL}_2(F)$:

$$g \mapsto \begin{cases} \begin{pmatrix} \chi(g) & 0 \\ 0 & {}^c\chi(g) \end{pmatrix} & \text{if } g \in H \\ \\ \begin{pmatrix} 0 & \chi(gc) \\ {}^c\chi(gc^{-1}) & 0 \end{pmatrix} & \text{if } g \notin H. \end{cases}$$

This is the *induced* representation $\rho = \mathrm{Ind}_H^G \chi$.

(c) Show that $\rho = \mathrm{Ind}_H^G \chi$ satisfies $\rho \otimes \eta \simeq \rho$.

(d) If $\chi \neq {}^c\chi$, show that χ does not extend to G and that $\mathrm{Ind}_H^G \chi$ is an irreducible representation of G.

(e) On the other hand, if $\chi = {}^c\chi$, show that χ extends to all of G, in exactly two ways. Show that $\mathrm{Ind}_H^G \chi$ is reducible, a sum of two characters. Which ones?

(f) Show that the complex representation in (19) is of the form $\mathrm{Ind}_H^G \chi$ for some G, H, χ. Explain everything.

(45) Continuing the notation for G, F from (44), now suppose that $\rho : G \to \mathrm{GL}_2(F)$ is irreducible and satisfies $\rho \otimes \eta \simeq \rho$ for some nontrivial character $\eta : G \to F^\times$. Show that ρ is induced from a character of $\ker \eta \subset G$ as follows.

(a) Show that η is quadratic.

Set $H = \ker \eta$. Show that $\rho(H)$ is abelian as follows.

(b) Show that there is a matrix $M \in \mathrm{GL}_2(F)$ so that $M\rho(g)M^{-1} = \rho(g)\eta(g)$ for all $g \in G$. Up to passing to a quadratic extension of F, you may assume that M is upper-triangular (why?). Show that M has distinct eigenvalues by considering $g \in H$ and $g \notin H$.

(c) Conclude that $\rho(H)$ is abelian.

(d) Prove that ρ is induced from a character of H.

(46) A modular eigenform f of weight $k \geq 2$ is called *CM* if there is a Dirichlet character χ so that $a_p(\ell)\chi(\ell) = a_p(\ell)$ for all but finitely many primes ℓ.

(a) Suppose f has rational coefficients. Let p be a prime not dividing the level of f. Show that the associated p-adic Galois representation $\rho_{f,\ell}$ is induced from a character of a quadratic extension K of $\mathbb{Q}$.

(b) Find a CM modular form in weight 2 and level 27. What is the character χ? What is the field K?

(47) Let $f = \sum a_n q^n$ be an eigenform of some weight k and some level N. Fix a prime $\mathfrak{p}$ of the Hecke eigenvalue field K lying over a rational prime p, and reduce f modulo $\mathfrak{p}$ to obtain a modular form over a finite extension $\mathbb{F}$ or $\mathbb{F}_p$.

(a) Prove that there exists a positive density of primes ℓ such that $a_\ell(f) \equiv 0 \pmod{\mathfrak{p}}$. (*Hint*: Chebotarev density for the mod-$\mathfrak{p}$ Galois representation attached to f.)

(b) If $p \neq 2$, prove that there is also a positive density of primes ℓ such that $a_\ell(f) \not\equiv 0 \pmod{\mathfrak{p}}$.

(c) Find a counterexample for $p = 2$ to (47b).

How much of this can be extended to forms that are not necessarily eigenforms?

(48) Connect the mod-23 representation associated to Δ to something on these exercises.