Modular forms: problem set 2

Due July 13

***Exercise 1.** Let $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ be the Frobenius automorphism. Show that the subgroup $\langle\sigma_p\rangle$ generated by σ_p is dense in $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. An element with this property is called a *topological generator*.

Exercise 2. For each prime p and each embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, choose a preimage $\sigma_{p,\iota}$ of the Frobenius under the induced map $D_p \to G_{\mathbb{F}_p}$. Using the Chebotarev Density Theorem, show that the set $\{\sigma_{p,\iota}\}_{p,\iota}$ is dense in $G_{\mathbb{Q}}$.

Exercise 3. Recall that the topology on $\overline{\mathbb{Q}}_p$ is defined via the unique absolute value $|\cdot|$ on $\overline{\mathbb{Q}}_p$ extending the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}_p$. Explicitly, for any $\alpha \in \overline{\mathbb{Q}}_p$ we have

$$|\alpha| = \left|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|_p^{1/[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]}.$$

Show that if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and $\alpha \in \overline{\mathbb{Q}}_p$ then $|\sigma(\alpha)| = |\alpha|$. Conclude that if $K/\mathbb{Q}_p$ is an algebraic extension, then any field automorphism of K is automatically *continuous*. In particular, show that the only automorphism of $\mathbb{Q}_p$ is the identity.

***Exercise 4.** This exercise defines the map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ and establishes its basic properties (not including surjectivity). The following exercise 5 gives a more sophisticated (albeit conceptually cleaner) perspective on this map, which automatically shows it is surjective.

(1) Show that the residue field of $\overline{\mathbb{Q}}_p$ is $\overline{\mathbb{F}}_p$.

(2) Use exercise 3 to show that any $\sigma \in G_{\mathbb{Q}_p}$ preserves the valuation ring $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ and maximal ideal $\mathfrak{p}$ of $\overline{\mathbb{Q}}_p$.

(3) Use parts (1) and (2) to define a homomorphism $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$.

(4) Show that the homomorphism $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ is continuous.

Exercise 5. This exercise uses unramified extensions to give a conceptually cleaner perspective on the map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$. Specifically, we show there is a canonical isomorphism $G_{\mathbb{F}_p} \cong \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$ where $\mathbb{Q}_p^{ur}$ is the maximal unramified extension of $\mathbb{Q}_p$, and this isomorphism identifies the map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ with the restriction $G_{\mathbb{Q}_p} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$, which is automatically surjective.

Recall that a finite extension $K/\mathbb{Q}_p$ is *unramified* if

$$[K : \mathbb{Q}_p] = [\kappa : \mathbb{F}_p]$$

where $\kappa = \mathcal{O}_K/\mathfrak{p}$ is the residue field of K. Equivalently, $K/\mathbb{Q}_p$ is unramified if $\mathfrak{p} = p\mathcal{O}_K$.

(1) Let K, K' be unramified extensions of $\mathbb{Q}_p$. Show that a $\mathbb{Q}_p$-linear map $f : K \to K'$ has $f(\mathcal{O}_K) \subseteq \mathcal{O}_{K'}$ and $f(\mathfrak{p}_K) \subseteq \mathfrak{p}_{K'}$.

(2) Deduce that we have a functor

$$\mathcal{F} : \left\{ \begin{array}{c} \text{finite unramified extensions} \\ K/\mathbb{Q}_p \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{finite extensions} \\ \kappa/\mathbb{F}_p \end{array} \right\}$$

via $\mathcal{F}(K) = \mathcal{O}_K/\mathfrak{p}_K$, the residue field of K. The morphisms on both sides are field homomorphisms (which automatically fix $\mathbb{Q}_p$ on the left or $\mathbb{F}_p$ on the right).

(3) Use the primitive element theorem and Hensel's lemma to show that the functor $\mathcal{F}$ is essentially surjective, i.e. for every finite extension $\kappa/\mathbb{F}_p$ there is a finite unramified $K/\mathbb{Q}_p$ with residue field κ.

(4) Again use the primitive element theorem and Hensel's lemma to show that $\mathcal{F}$ is fully faithful, i.e. if K, K' are unramified extensions with residue fields κ, κ' then the map

$$\mathrm{Hom}(K, K') \longrightarrow \mathrm{Hom}(\kappa, \kappa')$$

via $f \mapsto \mathcal{F}(f)$ is a bijection.

(5) By parts (3) and (4), the functor $\mathcal{F}$ is an equivalence of categories. Deduce that we have a natural isomorphism $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathrm{Gal}(\kappa/\mathbb{Q}_p)$ where κ is the residue field of the finite unramified extension $K/\mathbb{Q}_p$.

(6) As the compositum of two finite unramified extensions is again finite unramified, we can let the *maximal unramified extension* $\mathbb{Q}_p^{ur}/\mathbb{Q}_p$ be the union of all finite unramified extensions. Show that the residue field of $\mathbb{Q}_p^{ur}$ is $\overline{\mathbb{F}}_p$. Also show that $\mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \cong G_{\mathbb{F}_p}$ and that the map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ factors as

$$G_{\mathbb{Q}_p} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \xrightarrow{\sim} G_{\mathbb{F}_p}.$$

Hence this map is automatically surjective and continuous.

Exercise 6. This exercise shows that the map $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$ is injective. The key input is *Krasner's lemma*. Part (5) also uses Krasner's lemma to show that the completion of $\overline{\mathbb{Q}}_p$ is still algebraically closed; we denote this field by $\mathbb{C}_p$.

(1) Let $\alpha, \beta \in \overline{\mathbb{Q}}_p$ such that

$$|\alpha - \beta| < |\sigma(\alpha) - \alpha|$$

for all $\sigma \in G_{\mathbb{Q}_p}$ such that $\sigma(\alpha) \neq \alpha$. In other words, suppose that β is closer to α than any of α's conjugates are. Prove that $\mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\beta)$. This is Krasner's lemma.

(2) Let $P(X) = \sum p_i X^i \in \mathbb{Q}_p[X]$ be a monic irreducible polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$. Using part (1), show that there is an $\epsilon > 0$ so that if $Q(X) = \sum q_i X^i \in \mathbb{Q}_p[X]$ is a monic irreducible polynomial of degree n with roots $\beta_1, \ldots, \beta_n$ such that

$$|p_i - q_i|_p < \epsilon \qquad \text{for all } i = 0, \ldots, n-1,$$

then (possibly after reordering the β_i) we have $\mathbb{Q}_p(\alpha_i) = \mathbb{Q}_p(\beta_i)$ for all $i = 1, \ldots, n$. In other words, if two polynomials are "sufficiently close" then they generate the same extensions of $\mathbb{Q}_p$.

(3) Use the primitive element theorem and part (2) to show that if $K/\mathbb{Q}_p$ is a finite extension, then there is a number field $L/\mathbb{Q}$ and an absolute value $|\cdot|$ on L so that K is the completion of L with respect to $|\cdot|$.

(4) Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Arguing as in part (3), show that $\mathbb{Q}_p\overline{\mathbb{Q}} = \overline{\mathbb{Q}}_p$. Deduce that the map $G_{\mathbb{Q}_p} \to G_{\mathbb{Q}}$ induced by our choice of embedding is injective.

(5) Show that the completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}}_p$ with respect to the canonical absolute value on $\overline{\mathbb{Q}}_p$ is algebraically closed.