Galois Representations assignments.

Problem 1 (for 27/10). Let $K = \mathbb{Q}(i)$ and $\mathcal{O} = \mathbb{Z}[i]$, the ring of Gaussian integers. Recall that every ideal of $\mathcal{O}$ is principal: $I = (a+bi)$, $NI = a^2+b^2$.

(1) Prove that $2 = \mathfrak{p}^2$ with $\mathfrak{p} = (1+i)$. In other words, 2 ramifies in $K/\mathbb{Q}$.

(2) Use Kummer-Dedekind to show that every prime $p \equiv 1 \mod 4$ of $\mathbb{Q}$ splits $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in K, and every $p \equiv 3 \mod 4$ is inert, that is (p) is a prime ideal of K with residue field $\mathbb{F}_{p^2}$.

(3) Deduce that the Dedekind ζ-function of K factors as

$$\zeta_K(s) = \zeta(s)L(s),$$

with $\zeta(s)$ the Riemann zeta function and

$$L(s) = \sum_{n\geq 1 \text{ odd}} \frac{\chi(n)}{n^s}, \qquad \chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \mod 4 \\ -1 & \text{if } n \equiv 3 \mod 4 \end{cases}.$$

(the L-function of the non-trivial character $(\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times$).

Problem 2 (for 3/11). Let $K = \mathbb{Q}(i, \sqrt{17})$.

(1) Show that for every prime number $p \neq 2, 17$, either -1 or 17 or -17 is a square modulo p (possibly all 3).

(2) Show that $p = 17$ splits in $\mathbb{Q}(i)$ and that $p = 2$ splits in $\mathbb{Q}(\sqrt{17})$.

(3) Deduce that every prime p of $\mathbb{Q}$ splits into 2 or 4 primes of K, and consequently $\zeta_K(s)$ has every local polynomial $F_p(T)$ of the form $G_p(T)^2$ for some (usually quadratic) $G_p(T) \in \mathbb{Z}[T]$.

NB. In other words, just looking at the local factors, $\zeta_K(s)$ looks like a square of some reasonable function. But it certainly isn't! It has a simple pole at $s = 1$, so whatever $\prod_p G_p(p^{-s})^{-1}$ is, it does not have a meromorphic continuation to $\mathbb{C}$. (This gives some indication that meromorphic continuation is a subtle business, and we cannot expect it for any function with reasonable arithmetic coefficients.

Problem 3 (for 10/11). Let $K = \mathbb{Q}(\sqrt[3]{m})$ for some $m \in \mathbb{N}$, not a cube. Write $F = \mathbb{Q}(\zeta_3, \sqrt[3]{m})$ for its Galois closure, and $G = \mathrm{Gal}(F/\mathbb{Q}) \cong S_3$, the permutation group on the three roots of $x^3 - m$. Let $p \neq 3$ be a prime and $\mathfrak{p}|p$ a prime of F, with decomposition group $D < G$ and inertia group $I \triangleleft D$.

(a) Show that p, D and I must be in one of the following cases:

(1) p is unramified in $F/\mathbb{Q}$, and $D \in \{C_3, C_2, C_1\}$,

(2) p is ramified in $F/\mathbb{Q}$, and $D = S_3$, $I = C_3$,

(3) p is ramified in $F/\mathbb{Q}$, and $D = I = C_3$.

(b) All of these may indeed occur: for $m = 2$ show that $p = 7, 5, 31, 2$ cover the three cases of (1) and (2), and $m = p = 7$ covers (3).

You may find it useful to employ the standard fact that the ramification and residue degrees are multiplicative in towers: if $\mathbb{Q} \subset M \subset F$ and $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ in $\mathcal{O}_M$ and $\mathfrak{p}_1 = \mathfrak{q}_1^{E_1} \cdots \mathfrak{q}_r^{E_r}$ in $\mathcal{O}_F$, then clearly $(p) = \mathfrak{q}_1^{e_1E_1} \cdots$ in $\mathcal{O}_F$. In other words $e_{\mathfrak{q}_1}^{F/\mathbb{Q}} = e_{\mathfrak{q}_1}^{F/M} e_{\mathfrak{p}_1}^{M/\mathbb{Q}}$, and similarly, $f_{\mathfrak{q}_1}^{F/\mathbb{Q}} = f_{\mathfrak{q}_1}^{F/M} f_{\mathfrak{p}_1}^{M/\mathbb{Q}}$. Both $M = \mathbb{Q}(\zeta_3)$ and $M = K$ give useful information about the splitting of (p) in F.

Problem 4 (for 17/11). Suppose $F/\mathbb{Q}$ is Galois with Galois group S_3, and $C_2 \cong H < G$, so that $M = F^H$ is a cubic extension of $\mathbb{Q}$. Let $p \in \mathbb{Z}$ be a prime which ramifies in $F/\mathbb{Q}$.

(1) Show that, up to conjugation, there are [at most] four possibilities for the pair (D_p, I_p) in $F/\mathbb{Q}$. (Optional: construct examples F, p to show that all four do occur.)
(2) For each of the four, write down the double cosets $H\backslash G/D_p$, and the number, ramification and residue degrees of primes above p in $M/\mathbb{Q}$.
(3) Deduce the possible local factors $F_p(T)$ of Dedekind ζ-functions $\zeta_M(s)$ of cubic extensions M of $\mathbb{Q}$ at ramified primes p.

Problem 5 (for 24/11). Suppose $F/\mathbb{Q}$ is Galois with Galois group S_3. Let $K, M \subset F$ be subfields with $[K : \mathbb{Q}] = 2$, $[M : \mathbb{Q}] = 3$. Decompose $\zeta_K(s), \zeta_M(s)$ and $\zeta_F(s)$ into L-functions of irreducible Artin representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Express $\zeta_F(s)$ in terms of $\zeta_K(s)$, $\zeta_M(s)$ and Riemann $\zeta(s)$.

Problem 6 (for 24/11 as well). Let p^n be a prime power and $F = \mathbb{Q}(\zeta)$, $\zeta = \zeta_{p^n}$, the p^nth cyclotomic field. It is a standard fact that the ring of integers of K is $\mathbb{Z}[\zeta]$, and that $\pi = 1 - \zeta$ generates the unique ideal above p,

$$(\pi)^{\phi(p^n)} = (p).$$

(1) Determine the decomposition group $D = D_p = D_\pi$, the inertia group $I = I_p = I_\pi$ in $\mathrm{Gal}(F/\mathbb{Q}) = (\mathbb{Z}/p^n\mathbb{Z})^\times$, and its filtration by the higher ramification groups

$$\{1\} = I_k \triangleleft \cdots I_2 \triangleleft I_1 \triangleleft I_0 = I.$$

(2) Let χ be a primitive character of $(\mathbb{Z}/p^n\mathbb{Z})^\times$, that is of modulus p^n. Prove, by definition of the conductor, that the associated 1-dimensional Galois representation ρ_χ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ has conductor $N(\rho) = p^n$.

Hint: $\sigma \equiv \mathrm{id} \bmod \pi^k \iff v_\pi(\zeta - \sigma(\zeta)) \geq k$.
Remark: the same argument (with a bit more notation) shows that any Dirichlet character of modulus m (not necessarily a prime power) is the conductor of the associated Galois representation.

Problem 7 (for 1/12). Show that $\mathbb{Q}_p$ contains the $(p-1)$th roots of unity, in four (somewhat) different ways:

(1) If $a \equiv b \mod p^n$ with $a, b \in \mathbb{Z}$, show that $a^p \equiv b^p \mod p^{n+1}$. Deduce that for $a \in \mathbb{Z}$ the sequence $(a^{p^n})_{n \geq 1}$ is Cauchy with respect to the p-adic absolute value, and therefore converges in $\mathbb{Z}_p$ to some element that satisfies $x^p = x$ and $x \equiv a \bmod p$.

(2) Use Hensel's lemma: if $f(x) \in \mathbb{Z}_p[x]$ is a monic polynomial whose reduction $\bar{f}(x) \in \mathbb{F}_p[x]$ has a simple root $\bar{t} \in \mathbb{F}_p$, then $f(x)$ has a unique root $t \in \mathbb{Z}_p$ that reduces to $\bar{t} \bmod p$.

(3) The 'primitive element theorem' states that the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for every prime $p > 2$ and $n \geq 1$. Use it to deduce that $\mathbb{Z}_p^\times = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times$ contains a cyclic group of order $p-1$.

(4) Compute $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p-1})/\mathbb{Q})$ and take completions to deduce that $\mathbb{Q}(\zeta_{p-1}) \hookrightarrow \mathbb{Q}_p$. (There is one such embedding for every prime above p in $\mathbb{Q}(\zeta_{p-1})$.)

Problem 8 (for 8/12). Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 1/4$.

(1) On an elliptic curve $y^2 = x^3 + ax + b$ the x-coordinates of the non-trivial 3-torsion points are roots of the 3-division polynomial $x^4 + 2ax^2 + 4bx - a^2/3$. Use this to find $E[3]$.

(2) Find a basis of $E[3]$ in which $G_\mathbb{Q}$ acts on $E[3]$ as $\sigma \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi(\sigma) \end{smallmatrix}\right)$, where σ is the non-trivial 1-dimensional representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$.

(3) Considering the 3-adic Tate module T_3E, deduce that for every prime p at which E has good reduction, the local factor of the L-function $L(E/\mathbb{Q}, s)$

$$F_p(T) = \det\big(1 - \mathrm{Frob}_p^{-1} T \bigm| V_3E\big) = 1 - aT + pT^2$$

has $a \equiv 2 \mod 3$ if $p \equiv 1 \mod 3$ and $a \equiv 0 \mod 3$ if $p \equiv 2 \mod 3$.