Elliptic Curves and Modular Forms (Master)
Wintersemester 2017/18

JProf. Dr. Simon Lentner
Algebra and Number Theory
FB Mathematik, Universität Hamburg

Sheet 6

Problem 1 (2+1+1 Points)

a) Suppose a finite group G permutes a set X and acts hence on the vector space V with formal basis $(e_x)_{x\in X}$. Give a general formula for $\mathrm{Tr}(g|V)$.

   Then show that such a V always has a vector v fixed by all g (trivial 1-dimensional subrepresentation) and a subspace W of dimension $|X|-1$ with $gW=W$, such that $V=v\mathbb{C}\oplus W$. Calculate $\mathrm{Tr}(g|W)$.

b) The alternating group $\mathbb{A}_4$ has conjugacy classes $1,(12)(34),(123),(132)$ and acts naturally on 4 points. Calculate all $\mathrm{Tr}(g|V)$ and $\mathrm{Tr}(g|W)$.

c) There is a quotient $\mathbb{A}_4\to\mathbb{A}_3=\mathbb{Z}_3$, giving three 1-dimensional representations. Calculate all $\mathrm{Tr}(g|V)$ for them.

Problem 2 (2+2+2+2 Points)
Let $g:X\to X$ be an automorphism of finite order on a variety X in characteristic q with Frobenius $Fx=x^q$.
We study the trace of the induced linear map g on the ℓ-adic cohomology $H^*(X)$.

a) Define the Lefschetz number

$$\mathcal{L}(g,X)=\sum_{k=0}^{2d}(-1)^k\mathrm{Tr}(g^{-1}|H^k(X))$$

   and prove that it can be expressed without referring to ℓ-adic cohomology in terms of fixpoints of F^kg^{-1} as follows

$$\mathcal{L}(g,X)=-\lim_{T\to\infty}\sum_{k\geq 1}|X^{F^kg^{-1}}|\,T^k$$

   You may start by relating $g=\mathrm{id}$ to the local zeta function of X.

b) Let g be a diagonal invertible $d\times d$ matrix over $\mathbb{F}_q$, acting on the affine space $\mathbb{K}^d=(\mathbb{F}_{q^k})^d$. Calculate $\mathcal{L}(g,X)$ and compare it to $\mathcal{L}(\mathrm{id},X^g)$ for the set of fixpoints.

c) For an elliptic curve $y^2=4(x-e_1)(x-e_2)(x-e_3)=P(x)$ (for simplicity $e_i\in\mathbb{F}_q$) at good reduction q let the local zeta function of the projective completion be

$$Z(T)=\frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-qT)}$$

   Consider the automorphism $g:(x,y,z)\to(x,-y,z)$. Calculate with the above formula $\mathcal{L}(g,X)$. *Hint: Count the nonsquares $P(x), x\in\mathbb{F}_{q^k}$ using $Z(T)$.*

   Compare $\mathcal{L}(g,X)$ to $\mathcal{L}(\mathrm{id},X^g)$ for the set of fixpoints. Assuming g acts trivial on $H^0(X),H^2(X)$, calculate the action of g on $H^1(X)$.

d) By a theorem on ℓ-adic cohomology (SGA 4+5) if g has order not divisible by q, then $\mathcal{L}(g, X) = \mathcal{L}(\mathrm{id}, X^g)$. Using this (and assuming g acts trivial on H^0, H^2), calculate the action on the two-dimensional space $H^1(X)$ for

- The group $\mathbb{Z}_4$ generated by $g : (x, y, z) \mapsto (-x, \sqrt{-1}\ y, z)$ acting on the projective completion of our favourite elliptic curve $y^2 = x^3 - n^2 x$.
- The group $\mathbb{Z}_3 \times \mathbb{Z}_3$ generated by $g, h : (x, y, z) \mapsto (\zeta x, y, z), (x, \zeta y, z)$ on the projective completion of the Fermat curve $x^3 + y^3 = 1$ with $\zeta^3 = 1$.

Hint: Only calculating $\mathcal{L}(g, X)$ for generators g does not give enough information

Problem 3 (1+1+1+1+2+2 Points)
We study the so-called Dirichlet L-series for a character $\chi : \mathbb{Z}_N^\times \to \mathbb{C}^\times$ extended to a multiplicative function $\chi : \mathbb{Z} \to \mathbb{C}^\times$ by setting $\chi(n) = 0$ if $\mathrm{lcd}(n, N) \neq 1$

a) Show that for $\Re(s) > 1$ the following series converges

$$L_\chi(s) := \sum_{n \geq 1} \chi(n) n^{-s} = \prod_{p\ prime} \frac{1}{1 - \chi(p) p^{-s}}$$

Remark: Later in the lecture we derive a functional equation connecting $L_\chi(s)$ and $L_\chi(1 - s)$ and thus analytically continue it to a meromorphic function on $\mathbb{C}$.

b) Show that if χ comes from a nontrivial character, then the series converges even for $\Re(s) > 0$. It is known there is no zero at $s = 1$.

c) Let χ come from the trivial character 1, then express L_χ in terms of the zeta-function (for simplicity you may assume N prime). Conclude that $s = 1$ is a simple pole.

d) For any $a \in \mathbb{Z}_N^\times$ express the sum of n^{-s} over all $n \equiv a$ module N in terms of Dirichlet L-series'.

e) Deduce that for any $a \in \mathbb{Z}_N^\times$ there are infinitely many primes fulfilling $p \equiv a\ (N)$ (Dirichlet 1837). In fact one proves the slightly stronger result $\sum_{p \equiv a\ (N)} p^{-1} = \infty$.

f) Let $K = \mathbb{Q}(\sqrt{D})$, then it is known that a prime $p \in \mathbb{Z}$ considered as an ideal in the ring integers $\mathcal{O}_K \subset K$

- splits $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ into prime ideals of norm p, iff $4D$ is a square modulo p.
- inerts $(p) = \mathfrak{p}$ a prime ideal of norm p^2, iff $4D$ is a nonsquare modulo p.
- ramifies $(p) = \mathfrak{p}^2$ into a prime ideal of norm p, iff $p|4D$.

From this information, compute the Hecke series $L_{\mathcal{O}_K,1}(s)$ for trivial character in terms of Dirichlet series'.