Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Problem Set 11: More Cyclotomic Fields
Due in class Wednesday, November 21

Please submit eight of the following problems. (Note: this version includes known corrections as of class on November 14.)

More on cyclotomic fields.

Let ζ_n denote a primitive n-th root of unity and let $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

1. Prove that K is the maximal totally real subfield of $\mathbb{Q}(\zeta_n)$. (Recall that a number field is *totally real* if all of its embeddings into $\mathbb{C}$ are real, i.e., have their image in $\mathbb{R}$.)

2. Prove that $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ is the ring of integers of K.

3. Let E be the group of units of $\mathbb{Z}[\zeta_n]$ and let F be the group of units of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. Prove that F and the roots of unity of $\mathbb{Q}(\zeta_n)$ generate a subgroup of E of index at most 2. (Hint: this problem generalizes one of the problems from Problem Set 5.)

4. Let $\mathfrak{a}$ be an ideal of $\mathfrak{o}_K$ which becomes principal in $\mathbb{Z}[\zeta_n]$. Prove that $\mathfrak{a}$ is principal. That is, the natural map from $\mathrm{Cl}(\mathfrak{o}_K)$ to $\mathrm{Cl}(\mathbb{Z}[\zeta_n])$ is injective.

Gauss sums and Stickelberger's theorem.

Reminders: given a character $\chi : \mathbb{F}_q \to \mathbb{Q}(\zeta_m)$, the Gauss sum $G(\chi)$ is given by

$$G(\chi) = -\sum_{a \in \mathbb{F}_q^*} \chi(a) \zeta_p^{\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_p}(a)}$$

(note the minus sign here!); given characters χ_1, χ_2, the Jacobi sum $J(\chi_1, \chi_2)$ is given by

$$J(\chi_1, \chi_2) = -\sum_{a \in \mathbb{F}_q} \chi_1(a)\chi_2(1-a).$$

1. Verify the properties of Jacobi sums not proved in class:

$$J(\chi_1, \chi_2) = \begin{cases} \chi_1(-1) & \chi_1\chi_2 = 1 \\ G(\chi_1)G(\chi_2)/G(\chi_1\chi_2) & \chi_1\chi_2 \neq 1. \end{cases}$$

(Hint: write $G(\chi_1)$ as a sum over a, $G(\chi_2)$ as a sum over b, then rewrite $G(\chi_1)G(\chi_2)$ as a double sum in which $a + b$ is one of the indices.)

2. Stickelberger's theorem, in full generality, actually says that for any subfield M of $\mathbb{Q}(\zeta_m)$ and any fractional ideal $\mathfrak{a}$, $\mathfrak{a}^{\beta\theta}$ is principal, where $\theta = \sum_a \left\{\frac{a}{m}\right\} \sigma_a^{-1}$ is the Stickelberger element. Deduce this from the case $M = \mathbb{Q}(\zeta_m)$ proved in class. (Again, it suffices to work with $\mathfrak{a}$ being a prime not dividing m.)

3. Let $p \equiv 3 \pmod 4$ be a prime, and let R and N be the number of quadratic residues and nonresidues, respectively, mod p in the interval $(0, p/2)$. Prove that for every fractional ideal $\mathfrak{a}$ of $\mathbb{Q}(\sqrt{-p})$, $\mathfrak{a}^{R-N}$ is principal. (Hint: use the previous exercise.)

Interlude: the Weil Conjectures.

For q a prime power and d a positive integer, let $N(d,q)$ denote the number of solutions of the equation $x^d + y^d = z^d$ with $x, y, z \in \mathbb{F}_q$ not all zero, divided by $q-1$. (The result is an integer by homogeneity.) In these exercises, we reconstruct Weil's motivation for proposing the powerful *Weil Conjectures* about the number of solutions of polynomial equations (i.e., points on algebraic varieties) over finite fields.

1. Suppose d divides $q-1$, and let $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ be a character of order d. Show that
$$N(d,q) = q + 1 - \sum_{a,b} J(\chi^a, \chi^b),$$
where the sum runs over $a, b = 1, \dots, d-1$ but excluding pairs with $a + b = d$. (Hint: show that the number of d-th roots of $u \in \mathbb{F}_q^*$ is $\sum_{a=1}^{d} \chi^a(u)$.)

2. Show that $|N(d,q) - (q+1)| \le (d-1)(d-2)\sqrt{q}$. (Hint: reduce to the case where d divides $q-1$.)

3. (Davenport-Hasse) Given a character $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$, define a character $\chi' : \mathbb{F}_{q^r}^* \to \mathbb{C}^*$ by setting $\chi'(a) = \chi(\mathrm{Norm}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a))$. Show that $G(\chi') = G(\chi)^r$; you may assume $p > 2$ if it helps. (Hint: first show $G(\chi')/G(\chi)^r$ is a unit and has absolute value 1, so is a root of unity. Then show it is congruent to 1 modulo primes above p. For more details, see Washington, *Introduction to Cyclotomic Fields*, Chapter 6.)

4. Suppose d divides $q-1$, and let $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ be a character of order d. Show that
$$N(d,q^r) = q^r + 1 - \sum_{a,b} J(\chi^a, \chi^b)^r,$$
where the sum runs over a, b as above.

5. Show that $|J(\chi^a, \chi^b)| = \sqrt{q}$ for all a, b as above. This is the "Riemann hypothesis" for the zeta function of the curve $x^d + y^d = z^d$ in the projective plane. (Hint: consider the power series $\sum_i (1 - \alpha_i z)^{-1}$ in z, where α_i runs over the $J(\chi^a, \chi^b)$, and use the earlier exercises to bound its coefficients. Or use the fact that $|G(\chi)| = \sqrt{q}$ if χ is a character on $\mathbb{F}_q$.)