General Gauss sums

January 18, 2014

Last time we were studying the sum

$$G = \sum_{a \in \mathbb{F}_p} \chi(a)\zeta_p^a,$$

where p is an odd prime, and χ is the unique non-trivial homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to \pm 1$. This expression has a hybrid nature: it pairs together the multiplicative character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ with the additive character $a \mapsto \zeta_p^a : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}^\times$. Today we'll investigate such sums in a general setting.

Instead of just $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, we'll consider an arbitrary finite field $\mathbb{F}_q$ of size q. Recall that this implies that $q = p^d$ for some prime p, namely the characteristic of $\mathbb{F}_q$. This is because $\mathbb{F}_q$ is then a finite-dimensional vector space over $\mathbb{F}_p$, and the dimension gives the exponent d. Fix also a homomorphism $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ ("multiplicative character").

To make a Gauss sum we also need an additive character $\sigma : \mathbb{F}_q \to \mathbb{C}^\times$. But instead of allowing σ to vary, we'll actually fix a choice, namely:

$$\sigma(a) = \zeta_p^{Tr(a)}.$$

Here $Tr : \mathbb{F}_q \to \mathbb{F}_p$ is the linear map which sends a to the trace of multiplication by a acting on the $\mathbb{F}_p$-vector space $\mathbb{F}_q$. Equivalently (by calculating the trace over $\overline{\mathbb{F}_p}$ and diagonalizing), $Tr(a)$ is the sum of all the Galois conjugates of a, i.e.

$$Tr(a) = a + a^p + \ldots + a^{p^{d-1}}.$$

Note that this is the additive analog of the "norm" operation we found so useful when studying number fields.

So, let's fix σ as above. Then given a homomorphism $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$, we define the *Gauss sum*

$$G(\chi) = \sum_{a \in \mathbb{F}_q} \chi(a)\sigma(a).$$

(Here by convention we set $\chi(0) = 0$.) Note that $G(\chi)$ lies in the "mixed" cyclotomic field $\mathbb{Q}(\zeta_p, \zeta_{q-1})$, since the values of χ lies in $\mathbb{Q}(\zeta_{p-1})$ and the values of σ lie in $\mathbb{Q}(\zeta_p)$. This is something that didn't come up with the Gauss sum of the previous lecture, because our characters took values in $\pm 1 \subset \mathbb{Q}$. Note that this mixed cycltomic field is something we've already studied in a different guise, because actually it's just the same as the pure cyclotomic field $\mathbb{Q}(\zeta_{p\cdot(q-1)})$: one containment is because $\zeta_{p(q-1)} = \zeta_p \cdot \zeta_{q-1}$ (this uses that p and $q-1$ are relatively prime) and the other is because $\zeta_p = \zeta_{p\cdot(q-1)}^{q-1}$ and $\zeta_{q-1} = \zeta_{p\cdot(q-1)}^{p}$.

Actually, this Gauss sum $G(\chi)$ already came up for us in our analysis of the Dirichlet L-series (at least in the case $q = p$). But now we're interested in it for a different (though tantalizingly related) reason. Namely, the pattern of the maximal ideal factorization of $G(\chi)$ in $\mathbb{Q}(\zeta_p, \zeta_{q-1})$ will give us relations in the class group of this field (and its subfields).

In other words, in coarse terms, we're interested in the multiplicative behavior of these sums $G(\chi)$. To get going on this, let's just see what happens when we multiply two of them together. So, let χ, χ' be two multiplicative characters. Then

$$G(\chi) \cdot G(\chi') = \sum_{a,b \in \mathbb{F}_q} \chi(a)\chi'(b)\sigma(a)\sigma(b).$$

(By the way, what we're doing right now should be similar to what we did in calculating the constant term $P_H \cdot P_{\neq H}$ of the minimal polynomial for the quadratic Gauss period.) Now, let's make a change of variables $a \mapsto a$, $b \mapsto b - a$, to get some cancellation in the σ's. This gives

$$G(\chi) \cdot G(\chi') = \sum_{a,b \in \mathbb{F}_q} \chi(a)\chi'(b-a)\sigma(a)\sigma(b-a) = \sum_{a,b \in \mathbb{F}_q} \chi(a)\chi'(b-a)\sigma(b).$$

Now, we split up this sum according as to whether $b = 0$ or not. The $b = 0$ term gives $\sum_{a \in \mathbb{F}_q} \chi(a)\chi'(-a)$; we'll come back to this term at the end. When $b \neq 0$, we can equivalently replace a by ab. Thus the $b \neq 0$ term is

$$\sum_{a \in \mathbb{F}_q, b \neq 0} \chi(ab)\chi'(b-ab)\sigma(b) = \sum_{a \in \mathbb{F}_q, b \neq 0} \chi(b)\chi'(b)\sigma(b)\chi(a)\chi(1-a).$$

Now the sum is split: the a's and b's don't interact. So it just evaluates to

$$\left(\sum_{a \in \mathbb{F}_q} \chi(a)\chi'(1-a) \right) \cdot \left(\sum_{b \neq 0} \chi(b)\chi'(b)\sigma(b) \right).$$

Both of the terms in this product have names. The first is called the "Jacobi sum" $J(\chi, \chi')$. It differs from the Gauss sum in that it only involves multiplicative characters, not additive characters. So it lives in $\mathbb{Q}(\zeta_{q-1})$. And the second term is just another Gauss sum, namely $G(\chi\chi')$, the Gauss sum of the product of the characters χ and χ'.

Now let's go back and analyze the $b = 0$ term. It was

$$\sum_{a \in \mathbb{F}_q} \chi(a)\chi'(-a) = \chi'(-1) \cdot \sum_{a \in \mathbb{F}_q} (\chi\chi')(a).$$

Now, recall from our discussion of Dirichlet L-series that the sum of the values of a character is 0 as long as the character is nontrivial. Thus this term is 0 unless $\chi\chi' = 1$, in which case it's $\chi'(-1) \cdot q$.

By the way, when $\chi\chi' = 1$, the Gauss sum $G(\chi\chi')$ that was in the other term evaluates to zero, because it's the sum of the values of the nontrivial additive character σ. The conclusion is the following:

Proposition 0.1. *Let $\chi, \chi' : \mathbb{F}_q^\times \to \mathbb{C}^\times$. Then if $\chi\chi' = 1$, we have*

$$G(\chi) \cdot G(\chi') = \chi'(-1) \cdot q = \chi(-1) \cdot q$$

whereas if $\chi\chi' \neq 1$, then

$$G(\chi) \cdot G(\chi') = J(\chi, \chi') \cdot G(\chi\chi'),$$

where $J(\chi, \chi')$ lives in $\mathbb{Z}[\zeta_{q-1}]$.

Note that given any χ, we can always define a χ' so that $\chi\chi' = 1$. Thus the first formula says in particular that every Gauss sum $G(\chi)$ is a divisor of a power of p. (The $\chi(-1)$ is always just ± 1: a unit.) Thus the unique maximal ideal factorization of $G(\chi)$ can only involve maximal ideals of $\mathcal{O}_{\mathbb{Q}(\zeta_p,\zeta_{q-1})}$ which lie above p.

There's one more relationship we'll need to use about these Gauss sums. This one justifies our choice of the special additive character σ. Namely, for any character χ, we have

$$G(\chi^p) = G(\chi).$$

This follows easily from the fact that the Frobenius $a \mapsto a^p$ is an automorphism of $\mathbb{F}_q$, and that $\sigma(a^p) = \sigma(a)$ (because $Tr(a)$ is the sum of the conjugates of a, so is invariant under Galois).

Now, as I said, our goal is going to be to use the Gauss sums to find relationships in the ideal class groups of cyclotomic fields. One potentially surprising thing, especially considering our discussion so far, is that the cyclotomic field we'll be focussing on is not actually $\mathbb{Q}(\zeta_p)$, but $\mathbb{Q}(\zeta_{q-1})$. So it's the multiplicative characters that are doing the work for us. Actually, this makes sense: we know from the first formula above that the Gauss sums live "at p". But on the other hand we already know that the unique maximal ideal lying above p in $\mathbb{Z}[\zeta_p]$ is principal. So we couldn't get any nontrivial information about the class group there. But the maximal ideal factorization of p in $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ stands to be pretty interesting. Indeed, note that if $q = p^f$, then f is the order of p in $(\mathbb{Z}/(q-1)\mathbb{Z})^\times$. Thus, recalling our discussion of maximal ideals in cyclotomic fields (which came up when we talked about the Dedekind zeta function of a cyclotomic field), it follows that p splits into $\phi(q-1)/f$ distinct maximal ideals P, and each quotient $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/P$ is a finite field of size q.

On the other hand, it is true that we are especially interested in the prime cyclotomic fields, and $\mathbb{Q}(\zeta_{q-1})$ is not a prime cyclotomic field. But it's actually good enough: given any prime $\ell \neq p$, we can find a $q = p^f$ so that $\mathbb{Q}(\zeta_\ell)$ is a subfield of $\mathbb{Q}(\zeta_{q-1})$. (Just let f be the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$.) Thereby we'll be able to descend our knowledge of ideal factorizations in $\mathbb{Q}(\zeta_{q-1})$ to the prime cyclotomic field $\mathbb{Q}(\zeta_\ell)$.

But for now let's stay in $\mathbb{Q}(\zeta_{q-1})$. We start by making an arbitrary choice P of a maximal ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ lying above p. This already gives us a finite field $\mathbb{F}_P = \mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/P$ of size q to work with. A more nuanced fact is that this choice also provides us with a canonical multiplicative character $\omega : \mathbb{F}_P^\times \to \mathbb{C}^\times$. This is due to the following lemma:

Lemma 0.2. *Let P be a maximal ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ lying above p, and let $\mathbb{F}_P$ denote the quotient. Then for every $a \in \mathbb{F}_P^\times$, there is a unique $(q-1)^{st}$ root of unity $\zeta \in \mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ such that ζ is congruent to a (mod P).*

Granting this lemma, associating $a \mapsto \zeta$ gives the desired character ω. It's both well-defined and multiplicative by uniqueness of ζ. In a sense, this ω is a version of the Teichmuller character from your problem set.

Proof. Consider the map $\{z^{q-1} = 1\} \to \mathbb{F}_P$ given by reduction of $(q-1)^{st}$ roots of unity modulo P. This map is clearly multiplicative; thus, since the source is a group, the image must lie in $\mathbb{F}_P^\times$, and we get a homomorphism $\{z^{q-1} = 1\} \to \mathbb{F}_P^\times$. We are trying to show that this homomorphism is an isomorphism. Both sides have the same cardinality, so it suffices to see that the kernel is trivial. But if the kernel weren't trivial, it would contain a primitive ℓ^{th} root of unity ζ_ℓ for some prime ℓ dividing $q-1$. Then we'd have $\zeta_\ell - 1$ inside a maximal ideal of $\mathbb{Z}[\zeta_\ell]$ lying above p (namely, the intersection of

P with $\mathbb{Z}[\zeta_\ell]$). But we know $\zeta_\ell - 1$ generates the unique maximal ideal of $\mathbb{Z}[\zeta_\ell]$ lying above ℓ. Since $\ell \neq p$, we get a contradiction. $\square$

So, our initial choice of P gives us a finite field of size q and a multiplicative character ω of that field. Actually, since this multiplicative character is in fact an isomorphism from $\mathbb{F}_P^\times$ to the group $(q-1)^{st}$ roots of unity, it is a generator for the group of all characters of $\mathbb{F}_P^\times$. Thus the collection of all these characters is just

$$\{1, \omega, \omega^2, \ldots, \omega^{q-2}\},$$

and we can consider all the Gauss sums $G(\omega^k)$ for $k = 0, \ldots, q-2$. All these Gauss sums live in $\mathcal{O}_{\mathbb{Q}(\zeta_p, \zeta_{q-1})}$, and we're interested in their maximal ideal factorization, which we know must only involve maximal ideals lying above p. Now here's the last lemma:

Lemma 0.3. *The operation $\widetilde{P} \mapsto P = \widetilde{P} \cap \mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ gives a bijection between maximal ideals of $\mathbb{Q}(\zeta_p, \zeta_{q-1})$ lying above p and maximal ideals of $\mathbb{Q}(\zeta_{q-1})$ lying above p.*

It is a general fact that such intersections always send maximal ideals to maximal ideals: this follows from the facts that an ideal is maximal if and only if the quotient is a field, and a subring of a finite field is also a finite field (exercise). It's also clear that they send maximal ideals lying above p to maximal ideals lying above p, since to lie above p is just to contain p. So the operation $\widetilde{P} \mapsto P$ is well-defined.

The idea for why it's a bijection is that we know this to be the case if we "disappear" the $\mathbb{Q}(\zeta_{q-1})$, and imagine the analogous claim for the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. (There's it's the same old fact that there's a unique maximal ideal of $\mathbb{Q}(\zeta_p)$ lying above p.) Then the fact that $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_{q-1})$ are "independent" over $\mathbb{Q}$ (since p and $q-1$ are relatively prime) will show that this claim persists when we stick the $\mathbb{Q}(\zeta_{q-1})$ back in.

More explicitly, we can just write down the inverse to $\widetilde{P} \mapsto P$: it's given by $P \mapsto P \cdot A + (\zeta_p - 1) \cdot A$, where we abbreviate $A = \mathcal{O}_{\mathbb{Q}(\zeta_p, \zeta_{q-1})}$. But let me omit the proof that these operations are actually inverse.

Now we're all set up to make the main claim, which we'll prove next time:

Theorem 0.4. *Let q be a power of a prime p, and let P be a maximal ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}$ lying above p. Denote by $\widetilde{P}$ the unique maximal ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1}, \zeta_p)}$ lying above P, and let $\omega : \mathbb{F}_P^\times = (\mathcal{O}_{\mathbb{Q}(\zeta_{q-1})}/P)^\times \to \mathbb{Q}(\zeta_{q-1})^\times$ be the character which sends a to the unique $(q-1)^{st}$ root of unity ζ which is congruent to a (mod P).*

Let $k \in \{0, 1, \ldots, q-1\}$. Then in the unique maximal ideal factorization of the Gauss sum

$$G(\omega^k) = \sum_{a \in \mathbb{F}_P} \omega(a)^k \cdot \zeta_p^{Tr(a)} \in \mathcal{O}_{\mathbb{Q}(\zeta_{q-1}, \zeta_p)},$$

the maximal ideal $\widetilde{P}$ occurs to the power c_k, where c_k is the sum of the digits of k written in base p.

One may wonder about the full maximal ideal factorization of $G(\omega^k)$, i.e., what about the other maximal ideals of $\mathcal{O}_{\mathbb{Q}(\zeta_{q-1}, \zeta_p)}$ lying above p? Actually, we'll be able to figure that out just from the above theorem by using the Galois action. We'll discuss that when the time comes.