The minus part of the class group of $\mathbb{Q}(\zeta_p)$

January 28, 2014

Today we're going to put it all together. Let me remind you of the pieces:

1. Let p be a prime. Then
$$\zeta_{\mathbb{Q}(\zeta_p)}(s) = \zeta_{\mathbb{Q}}(s) \cdot \prod_{\chi \neq 1} L(s, \chi),$$
where $\zeta_F(s)$ is the Dedekind zeta function of a number field F, and $L(s, \chi)$ for a nontrivial character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ is the Dirichlet L-series for χ.

   More generally, if $F \subset \mathbb{Q}(\zeta_p)$ is a subfield with Galois-corresponding subgroup $H \subset (\mathbb{Z}/p\mathbb{Z})^\times$, then
$$\zeta_F(s) = \zeta_{\mathbb{Q}}(s) \cdot \prod_{\chi \neq 1, \chi(H)=1} L(s, \chi).$$

2. Let $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ be *odd*, i.e. $\chi(-1) = -1$. Then
$$L(1, \chi) = \frac{1}{p} \cdot \pi \cdot i \cdot g(\chi) \cdot B_{1,\overline{\chi}},$$
where $g(\chi) = \sum_{k=1}^{p-1} \chi(k) \cdot \zeta_p^k$ and $B_{1,\overline{\chi}} = \sum_{r=1}^{p-1} \overline{\chi(r)} \cdot \frac{r}{p}$. (There was also a formula when χ is even and nontrivial, but it was more complicated, with log's of algebraic integers in it.)

3. Let F be a number field. Then
$$lim_{s \to 1^+}(s-1)\zeta_F(s) = \frac{M \cdot h}{A},$$
where:

   (a) h is the class number of F, i.e. the order of the class group of F.

   (b) A is the volume of a fundamental domain for the ring of integers $\mathcal{O}_F$ inside Minkowski space $F_{\mathbb{R}}$.

   (c) M is the volume of $X_{\leq 1}$, where X is a fundamental cone for the action of the units $\mathcal{O}_F^\times$ on Minkowski space $F_{\mathbb{R}}$, and $X_{\leq 1} \subset X$ is the subset of elements x with $|N(x)| \leq 1$.

To combine these facts, multiply the first fact by $s-1$ and let $s \to 1^+$. Using the third fact, we get that for a number field $F \subset \mathbb{Q}(\zeta_p)$ with Galois-corresponding subgroup $H \subset (\mathbb{Z}/p\mathbb{Z})^\times$, we have

$$\frac{M \cdot h}{A} = \prod_{\chi \neq 1, \chi(H)=1} L(1, \chi).$$

Now, we want to isolate the odd characters in this product. For this, suppose (from now on) that $p > 2$, and let F be one of the following two fields:

1. $K := \mathbb{Q}(\zeta_p)$, the full cyclotomic field. This corresponds to $H = 1$.
2. $K^+ := \mathbb{Q}(\zeta_p) \cap \mathbb{R}$, the subfield of real cycltomic numbers. This corresponds to $H = \pm 1$: that is, K^+ is the fixed field of complex conjugation acting on K.

If we look at the above formula when $F = K$ and $F = K^+$, then take the quotient, we find

$$\frac{(M/M^+) \cdot (h/h^+)}{(A/A^+)} = \prod_{\chi(-1)=-1} L(1, \chi) = \prod_{\chi(-1)=-1} \frac{1}{p} \pi i g(\chi) B_{1,\overline{\chi}}.$$

Now, we're going to try to extract from this a reasonable formula for h/h^+ in terms of the $B_{1,\overline{\chi}}$. To do so requires identifying some of the mysterious numbers on both sides. Let us say the result now, and explain the more relevant pieces of it later.

Proposition 0.1. *We have the following calculations:*

1. $M/M^+ = \frac{1}{2p}(2\pi)^{\frac{p-1}{2}}$.
2. $A/A^+ = \sqrt{p}^{\frac{p-1}{2}}$.
3. h/h^+ *is an integer.*
4. $\prod_{\chi(-1)=-1} g(\chi) = (i\sqrt{p})^{\frac{p-1}{2}}$.

Plugging this in and observing some cancellations, we get

$$h/h^+ = 2p \cdot \prod_{\chi(-1)=-1} -\frac{1}{2} B_{1,\overline{\chi}}.$$

This is the formula we were aiming for.

Before explaining the above calculations, let me say a word about the historical context of this formula (as I understand it — I admittedly haven't looked too deeply into the history). Why were people interested in the class number of $\mathbb{Q}(\zeta_p)$? It has to do with Fermat's Last Theorem, which predicted that there are no nontrivial integer solutions to

$$x^n + y^n = z^n$$

when $n \geq 3$. Of course, we can assume $n = p$ is prime. Then the remark is that we can rewrite this equation in $\mathbb{Z}[\zeta_p]$ as

$$x^p = (z - \zeta_p y)(z - \zeta_p^2 y) \dots (z - \zeta_p^{p-1} y).$$

Now, the point is that the left hand side is a p^{th} power, but the factors on the right hand side are (nearly) relatively prime. If we had unique prime factorization in $\mathbb{Z}[\zeta_p]$, then we could conclude that each of the factors on the right is, up to a unit, (nearly) a p^{th} power. And from there it's not too much work to derive a contradiction.

Unfortunately, it seems that for large primes p the ring $\mathbb{Z}[\zeta_p]$ rarely has unique prime factorization, so this argument hits a serious roadblock. But Kummer realized that you don't actually need the full strength of unique prime factorization to make the argument go through. It's enough to assume that p doesn't divide the class number of $\mathbb{Q}(\zeta_p)$. That assumption implies that if the p^{th} power of an ideal is principal, then the ideal itself is principal. (This is a general fact about abelian groups: if $p \nmid \#A$, then multiplication by p is an isomorphism from A to itself.) And that's all one really needs for the above purposes.

This raises the question: given a prime p, how can we tell whether or not p divides the class number h of $\mathbb{Q}(\zeta_p)$? Kummer showed that p divides h if and only if it divides h/h^+. (This is a subtle claim, because it's unknown whether p can divide h^+.) Thus the above formula for h/h^+ makes it just a simple calculation to see whether or not $p \nmid h$, so whether or not the above argument proves Fermat's last theorem for the exponent p.

That's where it all came from. Now let me also say a word or two about what happened afterwards. A lot of later work on this subject centered around the idea of embodying the above numerical formula in the class group of $\mathbb{Q}(\zeta_p)$. Meaning, one wants some sort of interpretation of the individual factors on the right in terms of class groups. This is a subtle business, because the above formula really came from complex (or at least real) analysis, which deals with numbers, but not group structures. The first major step in this direction was taken by Herbrand, and we'll turn to his work at the end of this class. But it seems that, from a philosophical perspective, the decisive observations came from Iwasawa in the mid-20^{th} century.

Iwasawa found a seemingly natural, though mysterious, bridge between the complex analysis and class groups, which gives more information than the classical story we've been telling, based on work of Dirichlet. He found that the natural intermediary is p-adic analysis. He showed how to go from complex analysis to p-adic analysis in the case of Dirichlet L-series, and he made a conjecture explaining how to go from p-adic analysis to class groups. This conjecture was later proven by Mazur and Wiles, and now there's more than one proof known, and actually Iwasawa theory is a big field. But anyway, at the end of this, one does see that the factorization on the right-hand side of the equation for h/h^+ indeed has a nice reflection in the structure of the class group of $\mathbb{Q}(\zeta_p)$.

Getting back to business, we should now explain the first three parts of the above proposition, the ones about A/A^+, M/M^+, and h/h^+. (We'll leave the last one alone, the one about the Gauss sums, since it's a bit off-topic). They all concern the relationship between arithmetic in K and K^+. Here are the main claims which imply them.

Proposition 0.2. *Recall, $K = \mathbb{Q}(\zeta_p)$ and $K^+ = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$ for an odd prime p. Let $U_K = \mathcal{O}_K^\times$ and $U_{K^+} = \mathcal{O}_{K^+}^\times$ be the respective unit groups of these number fields, and let C_K and C_{K^+} be their respective class groups. Then:*

1. *The ring of integers $\mathcal{O}_{K^+}$ is $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, and the volume of $K_{\mathbb{R}}^+/\mathcal{O}_{K^+}$ is*

$$A^+ = \sqrt{p}^{\frac{p-3}{2}}.$$

2. *The cokernel of the natural inclusion $U_{K^+} \to U_K$ is finite, and in fact it identifies with the group $\{z^p = 1\}$ of p^{th} roots of unity.*

3. *The natural map $C_{K^+} \to C_K$ is injective.*

To prove these claims, we'll need to understand K^+ about as well as we understand K. The first step is to investigate the ring of integers $\mathcal{O}_{K^+}$. Recall that a crucial ingredient of our understanding of K was the factorization

$$p = (1-\zeta_p)(1-\zeta_p^2)\dots(1-\zeta_p^{p-1})$$

in $\mathbb{Z}[\zeta_p]$. The important thing was that each $1-\zeta_p^i$ is a unit multiple of $\pi = 1-\zeta_p$, so this means p is a unit times π^{p-1} in $\mathbb{Z}[\zeta_p]$. Thus $(p) = (\pi)^{p-1}$ is the unique maximal ideal factorization of (p), and so (π) is the unique maximal ideal of $\mathcal{O}_K$ lying above p.

Now let's find the analogous factorization in $\mathbb{Z}[\zeta_p + \zeta_p^{-1}] \subset K^+$. Here is a lemma:

Lemma 0.3. *If $\alpha \in \mathbb{Z}[\zeta_p]$, then $\alpha\overline{\alpha} \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.*

Proof. If you write $\alpha = a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2}$, you'll see that $\alpha\overline{\alpha}$ lies in the span of the $\zeta_p^i + \zeta_p^{-i}$ for $i = 0, 1, \dots, p-2$. So it suffices to see that all of these are polynomials in $\zeta_p + \zeta_p^{-1}$. That follows by expanding $(\zeta_p + \zeta_p^{-1})^i$ and using induction. □

Now we just take our expression for p and multiply it by its complex conjugate. This gives

$$p^2 = u \cdot (\pi\overline{\pi})^{p-1}$$

with u a unit, and everything is in $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ by the lemma.

Starting from this factorization, we can run a similar game in $\mathcal{O}_{K^+}$ as to what we did in $\mathcal{O}_K$. Consider the quotient $\mathcal{O}_{K^+}/p^2$. By the above factorization, it is built up out of $p-1$ copies of $\mathcal{O}_{K^+}/(\pi\overline{\pi})$. On the other hand, since K^+ has degree $\frac{p-1}{2}$ over $\mathbb{Q}$ (it corresponds to the order-2 subgroup ± 1 of the Galois group of K), we know that $\mathcal{O}_{K^+}$ is free of rank $\frac{p-1}{2}$, and hence $\mathcal{O}_{K^+}/p^2$ has cardinality p^{p-1}. It follows that $\mathcal{O}_{K^+}/(\pi\overline{\pi})$ has cardinality p, and so must be $\mathbb{F}_p$. In particular, $(\pi\overline{\pi})$ is a maximal ideal of $\mathcal{O}_{K^+}$, and so by uniqueness of maximal ideal factorizations, the above factorization of p^2 implies that there must exist a factorization of ideals of $\mathcal{O}_{K^+}$

$$(p) = (\pi\overline{\pi})^{\frac{p-1}{2}}.$$

We can also use this to check that $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ just as we showed that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. One calculates the volume $Vol(K^+_{\mathbb{R}}/\mathbb{Z}[\zeta_p + \zeta_p^{-1}])$ as a Vandermonde determinant, and finds that it equals

$$\sqrt{p}^{\frac{p-3}{2}}.$$

Thus Vol^2 is a power of p, and so we deduce that $\mathbb{Z}[\zeta_p + \zeta_p^{-1}] \subset \mathcal{O}_{K^+}$ has index a power of p. But on the other hand, by comparing the long factorization $p^2 = u \cdot (\pi\overline{\pi})^{p-1}$ in both these rings we see that the index must be prime to p. Therefore the index is one, and we deduce both that $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ and that $A^+ = \sqrt{p}^{\frac{p-1}{2}}$.

That handles the first claim of the above proposition. We can also extract the following:

Corollary 0.4. *Let I be any nonzero ideal of $\mathcal{O}_{K^+}$. Consider the extended ideal $I\mathcal{O}_K$ of $\mathcal{O}_K$: i.e., $I\mathcal{O}_K$ is the smallest ideal of $\mathcal{O}_K$ containing I, or in other words it's the set of all finite sums of elements of the form $i \cdot \alpha$ with $i \in I$ and $\alpha \in \mathcal{O}_K$. When we take the unique maximal ideal factorization of $I\mathcal{O}_K$, then the maximal ideal (π) occurs to an even power.*

Before giving the proof, let's say some words about this operation $I \mapsto I\mathcal{O}_K$ of extending ideals from $\mathcal{O}_{K^+}$ to $\mathcal{O}_K$. This will be useful later, since it's what gives the natural map $C_{K^+} \to C_K$ on class groups. The first thing to say is that this operation of extension is multiplicative: it sends products of ideals in $\mathcal{O}_{K^+}$ to products of ideals in $\mathcal{O}_K$. That's obvious. The second thing is that if P is a maximal ideal of $\mathcal{O}_{K^+}$ lying above a prime p, then $P\mathcal{O}_K$ also lies above p. That's obvious too, since lying above p just means that $p \in P$. Finally, the last thing is that we can recover I from the extended ideal $I\mathcal{O}_K$. Namely, $I = (I\mathcal{O}_K) \cap \mathcal{O}_{K^+}$. That's not obvious, but I'll leave it as an exercise.

OK, now let's prove the corollary.

Proof. If we consider the unique maximal ideal factorization of I, then only the maximal ideals lying above p will contribute to powers of (π) once we extend to $\mathcal{O}_K$. But we just saw that there's a unique maximal ideal lying above p, namely $(\pi\overline{\pi})$. Thus it suffices to see that $(\pi\overline{\pi})$, when extended to $\mathcal{O}_K$, is an even power of (π). But of course, $\overline{\pi}$ and π are unit multiples of each other in $\mathcal{O}_K$. □

Now let's turn to the map on units $U_{K^+} \to U_K$. This is certainly injective: it just comes from the inclusion of rings $\mathcal{O}_{K^+} \subset \mathcal{O}_K$. Furthermore, its image is easy to characterize: it is the set of $u \in U_K$ such that $u = \overline{u}$. This is just the Galois fact that K^+ is the fixed field of complex conjugation acting on K, together with the fact that an algebraic integer is a unit in one number field if and only if it's a unit in any bigger number field, which is obvious from the definitions.

Another way of saying that $u = \overline{u}$ is to say that $\overline{u}/u = 1$. Now, here is the main claim:

Proposition 0.5. *Suppose α is a nonzero element of K for which $\overline{\alpha}/\alpha$ is a unit in $\mathcal{O}_K$. Then in fact $\overline{\alpha}/\alpha$ is a root of unity. Moreover, in the case where α itself is a unit, then $\overline{\alpha}/\alpha$ is a p^{th} root of unity. Finally, the resulting sequence*

$$U_{K^+} \to U_K \stackrel{u \mapsto \overline{u}/u}{\longrightarrow} \{z^p = 1\}$$

is a short exact sequence of abelian groups. (This means that all the maps are homomorphisms, the first map is injective, the last map is surjective, and the kernel of the last map equals the image of the first map. Thus, the quotient U_K/U_{K^+} identifies with $\{z^p = 1\}$.)

We need this general lemma:

Lemma 0.6. *Let F be a number field, and suppose $x \in \mathcal{O}_F$ satisfies $|\sigma(x)| = 1$ for all field embeddings $\sigma : F \to \mathbb{C}$. Then x is a root of unity.*

The lemma is false if we don't assume $x \in \mathcal{O}_F$: consider $\frac{3+4i}{5} \in \mathbb{Q}(i)$.

Proof. The locus of x for which $|\sigma(x)| = 1$ for all σ defines a closed and bounded, hence compact, region in Minkowski space $F_{\mathbb{R}}$. But we know that $\mathcal{O}_F$ is discrete in Minkowski space. Discrete plus compact implies finite, so there are only finitely many x satisfying our conditions. But on the other hand, if x satisfies these conditions, then so does every power of x. So we must have $x^n = x^m$ for some distinct n and m. Thus x is a root of unity. □

Now we prove the proposition.

Proof. To see that $\overline{\alpha}/\alpha$ is a root of unity, we apply the lemma. Note that every field embedding $\sigma : K \to \mathbb{C}$ commutes with complex conjugation, because $Gal(K/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$ is commutative. Thus we have

$$\sigma\left(\overline{\alpha}\alpha\right) = (\overline{\sigma\alpha})/(\sigma\alpha).$$

This is of the form $\overline{z}z$, so it has norm 1. So the lemma implies that $\overline{\alpha}/\alpha$ is a root of unity. Furthermore, $\alpha \mapsto \overline{\alpha}/\alpha$ is certainly multiplicative.

Now assume that $\alpha = u$ lies in U_K. We need to see that this root of unity is actually a p^{th} root of unity. Since every root of unity in K is a $(2p)^{th}$ root of unity (there can't be others: this follows from our knowledge of the degrees of cyclotomic fields), it suffices to see that $\overline{u}/u$ can't be a primitive $(2p)^{th}$ root of unity, i.e. that we can't have

$$\overline{u}/u = -\zeta_p^{-1}.$$

But note that $-\zeta_p^{-1} = \overline{\pi}/\pi$. So if we were to have the above, then $u\overline{\pi}$ would be fixed by complex conjugation, and hence would lie in $\mathcal{O}_{K^+}$. But this contradicts Corollary 0.4 above, since $(u\overline{\pi}) = (\pi)$ is an odd power of (π).

The last thing to see is that the sequence is short exact. The only thing that's not obvious is that the last map is surjective, i.e. that every p^{th} root of unity is of the form $\overline{u}/u$ for some unit $u \in U_K$. But actually, if we take $u = \zeta_p$, then we get $\overline{u}/u = \zeta^{-2}$. That's just another primitive p^{th} root of unity, so all p^{th} roots of unity must be hit. □

All that's left is seeing that the map $C_{K^+} \to C_K$ is injective. In other words, we need to know that if a nonzero ideal I of $\mathcal{O}_{K^+}$ is such that $I\mathcal{O}_K$ is principal, then I itself is principal. So suppose $I\mathcal{O}_K = (\alpha)$ with $\alpha \in \mathcal{O}_K$. Because I came from $\mathcal{O}_{K^+}$, complex conjugation leaves the ideal $I\mathcal{O}_K$ invariant. Thus $(\alpha) = (\overline{\alpha})$, so $\overline{\alpha}/\alpha$ is a unit, and in particular an algebraic integer. Thus, by the above lemma, it must in fact be a root of unity.

The key claim is that it too must be a p^{th} root of unity. We can argue for this exactly as in the second paragraph of the above proof. Assuming otherwise, we have $\overline{\alpha}/\alpha = \overline{\pi}/\pi$, so $\alpha\overline{\pi}$ lies in $\mathcal{O}_{K^+}$. But we know that the ideal generated by α comes from $\mathcal{O}_{K^+}$ too, so this would mean that $(\overline{\pi})$ comes from $\mathcal{O}_{K^+}$. But that can't be, because it's an odd power of (π).

Thus $\overline{\alpha}/\alpha$ is a p^{th} root of unity; in particular it equals $\overline{u}/u$ for some $u \in U_K$ (by the surjectivity of the last map in the above exact sequence). Then we see that $\alpha\overline{u}$ lies in $\mathcal{O}_{K^+}$. Then the ideal $(\alpha\overline{u})$ has the same extension to $\mathcal{O}_K$ as I does since u is a unit; thus we must have $I = (\alpha\overline{u})$, so I is principal, as desired.

I should say, I found these clever arguments in Lang's book on cyclotomic fields. He credits them to Iwasawa.