Gauss periods

January 16, 2014

Today we're going to more or less start over from the beginning, and get back into the historical root of cyclotomy: Gauss's study of the constructibility of regular n-gons by ruler and compass. This also involves finding explicit generators for subfields of cyclotomic fields. These generators will be the Gauss periods.

Let me start by recalling what is a ruler and compass construction. You start with the plane $\mathbb{R}^2$, and you give yourself the points $(0,0)$ and $(0,1)$. Starting from these points, you're allowed to generate more points by iterating the following rules:

1. If you have two distinct points P and Q, you're allowed to draw the line connecting P and Q, and you're allowed to draw the circle centered at P passing through Q.
2. Whenever you have an intersection of two figures, where a "figure" is either a line or circle, then you get the intersection points.

Then the question is, which points $P \in \mathbb{R}^2$ can you get? Or, in the usual terminology, which points P are "constructable"?

This question has a beautiful algebraic answer:

Proposition 0.1. *Think of $\mathbb{R}^2$ as $\mathbb{C}$, the complex numbers. Then for a point $z \in \mathbb{C}$, the following are equivalent:*

1. *z is constructible;*
2. *z can be expressed from 0 and 1 using only field operations and square roots;*
3. *z lies in a Galois extension $F/\mathbb{Q}$ of degree some power of 2.*

The appearance of the number "2" in the third criterion is an algebraic reflection of the fact that the intersection of a line and a circle, or the intersection of two circles, carries a two-fold ambiguity.

Let me briefly recall the proof of the above proposition. First one sees that 1 and 2 are equivalent. For 1 $\Rightarrow$ 2, one just sees that, algebraically, the intersection of two figures is described by either a linear equation or a quadratic equation. Thus, only field operations and square roots. For 2 $\Rightarrow$ 1, one needs to figure out how to geometrically realize the field operations and square roots by intersections of figures.

Then one sees that 2 and 3 are equivalent. For 2 $\Rightarrow$ 3, assuming 2 one has that z lies in an iterated quadratic extension of $\mathbb{Q}$. But then the same holds for all the conjugates of z; and hence also for the Galois closure of $\mathbb{Q}(z)$. By the "tower law", then, this Galois closure has degree a power of two, giving

3. For the last implication, 3 $\Rightarrow$ 2, one uses that for every inclusion of groups $H \subset G$ where G has order a power of two, one can "fill in" this inclusion by subgroups each of which is index two in the next. Applying this to $G = Gal(F/\mathbb{Q})$ and $H = Gal(F/\mathbb{Q}(z))$, by using the Galois corresopndence we deduce that $\mathbb{Q}(z)$ is an iterated quadratic extension of $\mathbb{Q}$, which gives us 2 via the quadratic equation.

Now let's use this to answer the question of when a regular n-gon can be constructed by ruler and compass. An equivalent question is whether a primitive n^{th} root of unity $\zeta_n \in \mathbb{C}$ is constructible. By the above proposition, this happens if and only if the cyclotomic field $\mathbb{Q}(\zeta_n)$ has degree a power of 2. But we know the degree of this field: it's $\varphi(n)$, the number of integers k relatively prime to n with $0 \leq k < n$. That's the irreducibility of the n^{th} cyclotomic polynomial.

As usual, for simplicity we'll focus on the case when n is a prime number p. Then $\varphi(p) = p - 1$, so the criterion is that a regular p-gon can be constructed by ruler and compass if and only if $p - 1$ is a power of 2.

That's a nice abstract result. But given such a prime p, how would one actually figure out how to construct the p-gon? Or, from the algebraic perspective, how can we explicitly write ζ_p in terms of field operations and square roots?

The idea for how comes from the proof of the above proposition. We know that the Galois group is $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$. This is cyclic of order $p - 1$, so for every divisor $d|(p-1)$ there is a unique subgroup H of order d. Assuming $p - 1$ is a power of 2, say $p - 1 = 2^n$, this means we can filter the Galois group as follows:

$$\{1\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_n = (\mathbb{Z}/p\mathbb{Z})^\times,$$

where H_k is the unique subgroup of order 2^k. Under the Galois correspondence, this corresponds to filtering $\mathbb{Q}(\zeta_p)$ by iterated quadratic extensions:

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n = \mathbb{Q}(\zeta_p),$$

where F_k is the fixed field of H_{n-k}. Then what we'll try to do is start with $\mathbb{Q}$ and work our way up this tower, successively finding explicit generators for the fields F_k in terms of square roots, until we get to the top and find a new expression for ζ_p.

To illustrate how this goes, let's look at a simple special case: $p = 5$. Here the Galois group has order 4, so there is just one intermediate field, call it F. So $\mathbb{Q} \subset F \subset \mathbb{Q}(\zeta_5)$, and both of these extensions have degree 2. So, how do we find a generator for F? So far all we know is ζ_5. That doesn't lie in F, because it's not fixed by the corresponding subgroup $\{1, 4\} \subset (\mathbb{Z}/5\mathbb{Z})^\times$ of order 2. But there's an easy trick for producing an element which is fixed: just take the sum of all the conjugates of ζ_5. That is, consider

$$\alpha = \zeta_5 + \zeta_5^4.$$

This is fixed by $\{1, 4\}$, because the summands are just swapped. So α lies in F. It also doesn't lie in $\mathbb{Q}$, because α is *not* fixed by the other Galois elements: the action by 2 or 3 in $(\mathbb{Z}/5\mathbb{Z})^\times$ on α gives

$$\alpha' = \zeta_5^2 + \zeta_5^3,$$

and we can't have $\alpha = \alpha'$, because that would imply the identity $1 - \zeta_5 - \zeta_5^2 + \zeta_5^3 = 0$ of degree 3, whereas we know that the minimal polynomial of ζ_5 has degree 4. So α must be a generator for the quadratic field F.

Now let's write α in terms of square roots. Or in other words, let's find a quadratic equation satisfied by α, with rational coefficients. We know this has to exist, because α lives in the quadratic field F. And actually, it's easy to write down such a quadratic equation: we know the other root should be the unique Galois conjugate of α, which is just the above α'. So the equation should be

$$(X - \alpha)(X - \alpha').$$

When we expand this out, it has to have $\mathbb{Q}$-coefficients, because it's fixed by Galois. Let's do it explicitly. We get

$$X^2 - (\zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4)X + (\zeta_5 + \zeta_5^4)(\zeta_5^2 + \zeta_5^3).$$

Now, the only algebraic relation we should need to use to see that this lies in $\mathbb{Q}$ is the equation $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$, coming from the minimal polynomial of ζ_5. And indeed, inputting this equation we find our polynomial is

$$X^2 + X - 1.$$

Thus,

$$\alpha, \alpha' = \frac{-1 \pm \sqrt{-5}}{2}.$$

(We could ask which is which if we take $\zeta_5 = exp(2\pi i/5)$. Then α would correspond to the $+\sqrt{-5}$, and α' to the $-\sqrt{-5}$, because we can see geometrically that $\zeta_5 + \zeta_5^4$ is positive. But let's stay in the algebraic realm, so ζ_5 is just some abstract primitive fifth root of unity, and the $\pm$ sign is indetermined.)

Thus we've solved F in terms of square roots. Now, using this, let's do the same for the full field $\mathbb{Q}(\zeta_5)$. We can play the same trick, just one level higher. We know $F \subset \mathbb{Q}(\zeta_5)$ is a quadratic extension. So ζ_5 must satisfy a quadratic polynomial with coefficients in F. To find it, we just make the polynomial whose roots are ζ and the conjugate of ζ by the Galois group $\{1, 4\}$. That is, we take

$$(X - \zeta_5)(X - \zeta_5^4).$$

When we expand this out, it must have coefficients in F, and therefore be expressible in terms of α. Indeed, expanding gives

$$X - \alpha X + 1.$$

Thus, we find

$$\zeta_5 = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2}.$$

If we plug in the above expression for α, we find an expression for ζ_5 in terms of square roots and field operations, which is exactly what we wanted. Note that in total there is a four-fold ambiguity coming from the two choices of $\pm$; this matches with the fact that the Galois group of $\mathbb{Q}(\zeta_5)$ is of order 4.

So if you didn't know how to construct a regular 5-gon by ruler and compass, now you do (modulo finding the algorithms for realizing field operations and square roots, which is a fun exercise). It should be clear that this method we just used works in general. Here's the abstract proposition:

Proposition 0.2. *Let p be a prime number, and let H be a subgroup of $G = (\mathbb{Z}/p\mathbb{Z})^\times$, considered as the Galois group of $\mathbb{Q}(\zeta_p)$. For every coset C of $H \subset G$, define the* Gauss period

$$P_C = \sum_{x \in C} \zeta_p^x.$$

Then for $g \in G$ we have $gP_C = P_{gC}$; thus all the P_C are Galois-conjugate. Moreover, each P_C generates the fixed field of H.

Proof. It's actually a trivial calculation to see that $g \cdot P_C = P_{gC}$. Thus all the P_C are Galois-conjugate. Moreover we see from the same formula that each P_C is fixed by H, and hence lies in the fixed field of H. By Galois theory, to see that P_C generates this fixed field, it's enough to see that P_C is not fixed by any $g \in G$ not in H. So, let $g \in G \setminus H$, and suppose

$$P_{gC} = P_C.$$

If we subtract P_C and divide by ζ_p, we find a polynomial of degree $< p-1$ satisfied by ζ_p, which is impossible, since we know that the minimal polynomial of ζ_p has degree $p-1$. □

A consequence of this proposition is that given a containment of two subgroups $H \subset H'$ of G, the minimal polynomial of P_H over the fixed field of H' is given by

$$\prod_{C \in H'/H} (X - P_C).$$

(This is the monic polynomial whose roots are the H'/H-orbits of P_H.) When one expands this out it must be possible to write the coefficients in terms of the $P_{H'}$, because $P_{H'}$ generates the fixed field of H'. In particular, when H is of index 2 in H' we get a quadratic equation satisfied P_H with coefficients in $\mathbb{Q}(P_{H'})$. Thus if $p-1$ is a power of 2, then by working your way down index-2-subgroups starting from G and ending at $\{1\}$, you end up with an expression for $P_{\{1\}} = \zeta_p$ in terms of iterated square roots. That's Gauss's algebraic construction of the regular p-gon.

If you ever put this into practice, then you really run into some interesting stuff. To illustrate this, let's focus on what would be just the very first step of using this idea to find an expression for ζ_p: finding the unique quadratic subextension of $\mathbb{Q}(\zeta_p)$. Here we don't really need to assume $p-1$ is a power of 2: we only need p to be odd. All the better.

The subgroup we need to think about is the subgroup $H \subset (\mathbb{Z}/p\mathbb{Z})^\times$ of index 2. There are two "dual" ways of describing this H: one is that H is the image of the squaring map on $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e. it is the subgroup of nonzero squares (mod p); the other is that H is the kernel of the "raising to the $\frac{p-1}{2}$-power" map on $(\mathbb{Z}/p\mathbb{Z})^\times$. The fact that these two descriptions agree and give the unique index two subgroup is an easily-verified fact about any cyclic group of even order.

By the above proposition, we know then that the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is generated by

$$P_H = \sum_{x \in H} \zeta_p^x,$$

and that the minimal polynomial of P_H is

$$(X - P_H)(X - P_{G-H}).$$

Let's calculate this minimal polynomial explicitly. Expanding, we get

$$X^2 - (P_H + P_{G-H})X + P_H \cdot P_{G-H}.$$

The coefficient of X is just the sum of ζ_p^x over all $x \in G$. We know that's -1, because $1 + \zeta_p + \ldots + \zeta_p^{p-1} = 0$. So our polynomial is

$$X^2 + X + P_H \cdot P_{G-H}.$$

As for $P_H \cdot P_{G-H}$, by distributing it is equal to

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} N_x \cdot \zeta_p^x,$$

where N_x denotes the number of ways of writing $x = y + z$ with $y \in H$ and $z \in G - H$. So we should figure out what this N_x is.

There are two cases to consider: $x = 0$, and $x \neq 0$.

Proposition 0.3. *Let p be an odd prime, and N_x for $x \in \mathbb{Z}/p\mathbb{Z}$ as defined above. Then:*

1. *$N_0 = 0$ if -1 is a square (mod p), and $N_0 = \frac{p-1}{2}$ if -1 is not a square (mod p).*
2. *For $x \neq 0$, we have $N_x = \frac{p-1}{4}$ if -1 is a square (mod p), and $N_x = \frac{p-3}{4}$ if -1 is not a square (mod p).*

Proof. The equation $0 = y + z$ is equivalent to $z = (-1) \cdot y$. Letting y run over H, we see that N_0 is the same as the number of elements $y \in H$ for which $(-1) \cdot y$ lies in $G - H$. If -1 is a square, then there are none of these, because $-1 \in H$ and $y \in H$ implies $(-1)y \in H$. Thus $N_0 = 0$ in that case. But if -1 is not a square, then $(-1) \cdot y \in G - H$ for every $y \in H$, because -1 lies in the nontrivial coset. So $N_0 = \frac{p-1}{2}$ in that case.

Now let's think about $x \neq 0$. The first remark to make is that the answer must be independent of x, i.e. $N_x = N_1$ for all x. That's because whether or not x is a square, multiplication by x gives a bijection between solutions to $1 = y + z$ and solutions to $x = y + z$. Indeed, multiplication by x either preserves H and $G - H$ (when x is a square) or swaps them (when x is not a square). In either case we get the desired conclusion. (We could also see why all the N_x must be equal by remembering where this problem came from: if the N_x were not all equal, then our constant coefficient $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} N_x \cdot \zeta_p^x \in \mathbb{Q}$ would give a polynomial equation satisfied by ζ_p which is not a multiple of the minimal polynomial of ζ_p, and that's impossible.)

Now, since the answer is independent of x, we may as well count the sum $\sum_{x \in \mathbb{Z}/p\mathbb{Z} - 0} N_x$ and then divide by $p - 1$. Well, if we threw N_0 into this sum, then we would get $\frac{p-1}{2} \cdot \frac{p-1}{2}$: there are $\frac{p-1}{2}$ choices for $y \in H$ and $\frac{p-1}{2}$ choices for $z \in G - H$, and who cares what the sum is, we're counting them all. Thus we find

$$N_x = \frac{1}{p-1}\left(\frac{p-1}{2} \cdot \frac{p-1}{2} - N_0\right),$$

which simplifies to the displayed result. □

Here we can make an interesting observation. If you didn't already know the criterion for when -1 is a square (mod p), you know it now. Indeed, N_x is obviously an integer. So the above implies that

when -1 is a square, p must be $1 \pmod 4$, and when -1 is not a square, p must be $3 \pmod 4$. Hence -1 is a square if and only if p is $1 \pmod 4$! That just fell out of the sky from our analysis of this minimal polynomial.

Speaking of which, we can now evaluate that minimal polynomial: it's

$$X^2 + X - \frac{p-1}{4}$$

when p is $1 \pmod 4$, and

$$X^2 + X + \frac{p+1}{4}$$

when p is $3 \pmod 4$.

So we find that the Gaussian period $\sum_{x \in H} \zeta_p^x$ is $\frac{-1 \pm \sqrt{p}}{2}$ in the first case, and $\frac{-1 \pm \sqrt{-p}}{2}$ in the second. Here's something else fantastic: these Gaussian periods "found" the most interesting quadratic fields, the ones where there are more integers than just the obvious $\mathbb{Z}[\sqrt{d}]$. See the "2's in the denominator"! Recall that the Gaussian period was a sum of roots of unity, so it is definitely an algebraic integer.

So the Gauss periods have already led us, without us even wanting it, to some interesting observations in number theory. In the next lecture we'll kick this up a notch, and use them to prove the quadratic reciprocity law.