

## Math 505, 1/11

We now look at a particularly important example of a Galois extension of  $\mathbf{Q}$ , namely a *cyclotomic extension*  $C_n = \mathbf{Q}(e^{2\pi i/n})$  for some  $n$ . This is the splitting field of the polynomial  $x^n - 1$  over  $\mathbf{Q}$ , since the roots of  $x^n - 1$  are clearly the powers of  $\alpha_n = e^{2\pi i/n}$ . We begin by recalling that  $x^n - 1$  is the product of the *cyclotomic polynomials*  $\Phi_d(x)$  as  $d$  runs over the positive divisors of  $n$ , where  $\Phi_d(x)$  the unique monic polynomial whose roots are exactly the primitive  $d$ th roots of 1 in  $\mathbf{C}$ . It follows easily by (strong) induction on  $n$  that  $\Phi_n(x)$  is a monic polynomial with integer coefficients; its degree is  $\phi(n)$ , the number of positive integers less than  $n$  and relatively prime to it, or equivalently the order of the multiplicative group  $\mathbf{Z}_n^*$  of units in  $\mathbf{Z}_n$ . The main result is that  $\Phi_n(x)$  is irreducible in  $\mathbf{Z}[x]$  for any  $n$ . To prove this suppose for a contradiction that  $\Phi_n(x)$  factors as  $f(x)g(x)$  where  $f(x), g(x)$  are monic with integer coefficients,  $g(x) \neq 1$ , and  $f(x)$  is irreducible. Then every one of the  $\phi(n)$  primitive  $n$ th roots of 1 in  $\mathbf{C}$  is a root of  $f(x)$  or  $g(x)$  but not both, whence there is a prime number  $p$  no dividing  $n$  and a primitive  $n$ th root  $\alpha$  of 1 such that  $\alpha$  is a root of  $f(x)$  while  $\alpha^p$  is a root of  $g(x)$ . By irreducibility  $f(x)$  must then divide  $g(x^p)$  in  $\mathbf{Z}[x]$ , since both of these polynomials have  $\alpha$  as a root; denoting by  $\bar{f}(x), \bar{g}(x)$  the respective reductions of  $f(x), g(x)$  modulo  $p$ , we get that  $\bar{f}(x)$  divides  $\bar{g}(x^p) = (\bar{g}(x))^p$  in  $\mathbf{Z}_p[x]$ . But then  $x^n - 1$  would have to have a repeated root in its splitting field over  $\mathbf{Z}_p$  (since both  $\bar{f}(x), \bar{g}(x)$  divide  $x^n - 1$  in  $\mathbf{Z}_p[x]$ ); this is a contradiction, since the derivative  $nx^{n-1}$  of  $x^n - 1$  clearly has no roots in common with  $x^n - 1$  over any field. Now we know that all the powers  $e^{2\pi im/n}$  of  $e^{2\pi i/n}$  are roots of the same irreducible polynomial  $\Phi_n(x)$  over  $\mathbf{Z}$  or  $\mathbf{Q}$ , as  $m$  runs over the elements of  $\mathbf{Z}_n^*$ ; it follows for any such  $m$  that there is a unique automorphism of  $C_n$  sending  $\alpha_n$  to  $\alpha_n^m$ , so that the Galois group of  $C_n$  over  $\mathbf{Q}$  is exactly  $U_n = \mathbf{Z}_n^*$ ; in particular, it is abelian (and cyclic if  $n$  is prime, or a power of an odd prime). More generally, the splitting field of  $x^n - 1$  over any field of characteristic not dividing  $n$  is a subgroup (possibly proper) of  $U_n$  and so is abelian.

It follows for any  $n$  that any field  $K$  between  $\mathbf{Q}$  and  $C_n$  that is Galois over  $\mathbf{Q}$  has an abelian Galois group (being a quotient of  $U_n$ ). It is a remarkable fact that the converse holds: *any finite abelian extension of  $\mathbf{Q}$ , that is any finite Galois extension of  $\mathbf{Q}$  with abelian Galois group, lies in  $C_n$  for some  $n$* . This result, called the Kronecker-Weber Theorem, at first sight seems flatly impossible: if for example  $p$  is a prime number, how can the quadratic extension  $\mathbf{Q}(\sqrt{p})$  of  $\mathbf{Q}$ , with Galois group  $\mathbf{Z}_2$ , lie in any  $C_n$ ? In fact, a fairly simple direct calculation shows that it lies in  $C_{4p}$ ; extending this, it is not difficult to show directly that any quadratic extension of  $\mathbf{Q}$  indeed lies in a cyclotomic extension. Now suppose that  $p$  is an odd prime number of the form  $2^m + 1$  for some  $m$ ; it then turns out that  $m$  must itself be a power of 2, and in fact there are only five known examples, corresponding to the values  $m = 1, 2, 4, 8, 16$ . Then the cyclotomic extension  $C_p$  has degree  $\phi(p) = p - 1 = 2^m$  over  $\mathbf{Q}$  and its Galois group is cyclic of this order. There is an obvious descending chain of subgroups starting from  $U_p$  and ending at 1, each having index 2 in its predecessor; applying the Galois correspondence we get an increasing chain of fields starting at  $\mathbf{Q}$  and ending at

$C_p$  with each a quadratic extension of its predecessor. The quadratic formula then guarantees that each field can be obtained from its predecessor by adjoining a single square root. But now there is a simple geometric construction which starts from a line segment of a specified length  $a$  and constructs one of length  $\sqrt{a}$  using only straightedge and compass; in a similar manner, starting with a given point  $a + bi$  in the complex plane (together with the origin  $0 = 0 + 0i$ ) and using only straightedge and compass, one can construct a second point  $c + di$  with  $(c + di)^2 = a + bi$ . The upshot is that *the complex number  $e^{2\pi i/p}$ , or equivalently a regular  $p$ -gon inscribed in a unit circle, can be constructed using only compass and straightedge for any such  $p$* . It was Gauss's discovery of this fact (for  $p = 17$ ) that convinced him to go into mathematics as a profession. More recently a rather anal-retentive German professor by the name of Hermes wrote a manuscript for how this could be done explicitly for  $p = 65537$ , the largest known prime of the form  $2^m + 1$ . This took ten years to produce and the manuscript is carefully preserved under glass in Göttingen today.

More generally (and more interestingly) one could ask for which  $n$  is there a formula for the roots of any polynomial over  $\mathbf{Q}$  of degree  $n$  using only rational numbers,  $m$ th roots (for any  $m$ , not just  $m \leq n$ ), and field operations. We will see that such a formula exists for  $n = 3$  or  $4$ , but not any higher  $n$ ; the proof will use the simplicity of the alternating group  $A_n$  for any  $n \geq 5$ .