

### 3/10 Cyclotomic Extensions §5.8

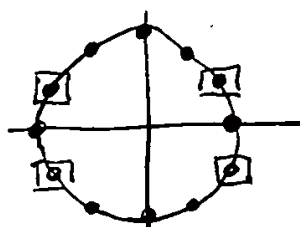
Our goal now is to study finite extensions of  $\mathbb{Q}$  of specific forms, leading up to a treatment of the problem which motivated the development of Galois theory: the solubility of polynomials by radicals.

Def'n Recall that a number  $u \in \mathbb{C}$  is called an  $n^{\text{th}}$  root of unity, for some  $n \geq 1$ , if  $u^n = 1$ , i.e., if  $u$  is a root of  $X^n - 1 \in \mathbb{Q}[X]$ . If  $u$  is an  $n^{\text{th}}$  root of unity, it is also a  $(mn)^{\text{th}}$  root of unity for any  $m \geq 1$ . We say  $u$  is a primitive  $n^{\text{th}}$  root of unity if it is an  $n^{\text{th}}$  root of unity but not a  $k^{\text{th}}$  root of unity for any  $k < n$ .

Prop. The  $n^{\text{th}}$  roots of unity are  $e^{\frac{2\pi i}{n}j}$  for  $j=0, 1, \dots, n-1$ .

The primitive  $n^{\text{th}}$  roots of unity are those  $e^{\frac{2\pi i}{n}j}$  with  $\gcd(j, n) = 1$ .

- (\*) E.g. We've seen before how the  $n^{\text{th}}$  roots of unity are equally spaced on the unit circle, for instance for  $n=12$  we get



$\Leftarrow$  the primitive  $12^{\text{th}}$  roots of unity are circled; they are  $e^{\frac{2\pi i}{12}j}$  for  $j=1, 5, 7, 11$ , the integers coprime to 12.

Pf sketch of prop: That the  $e^{\frac{2\pi i}{n}j}$  for  $j=0, 1, 2, \dots, n-1$  are the  $n^{\text{th}}$  roots of unity follows from the fact that  $e^{\frac{2\pi i}{n}j} \cdot e^{\frac{2\pi i}{n}k} = e^{\frac{2\pi i}{n}(j+k \bmod n)}$  (phases of complex #'s add when multiplied).

That the primitive ones are the coprime  $j$ 's then follows from  $e^{\frac{2\pi i}{n}j}$  is a primitive  $n^{\text{th}}$  root of unity  $\Leftrightarrow$

$j$  is a generator of  $(\mathbb{Z}/n\mathbb{Z}, +) \Leftrightarrow$

$j$  is a unit in the ring  $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow$

$j$  is coprime to  $n$ . You will flesh out this argument on your next HW assignment.  $\square$

Notice:  $\zeta_n = e^{\frac{2\pi i}{n}}$  is always a primitive  $n^{\text{th}}$  root of unity, and all  $n^{\text{th}}$  roots of unity are powers of this  $\zeta_n$ .

Def'n Let  $n \geq 1$ . The  $n^{\text{th}}$  cyclotomic polynomial  $\Phi_n(x) \in \mathbb{C}[x]$  is  $\Phi_n(x) = \prod_{\omega \text{ a primitive } n^{\text{th}} \text{ root of unity}} (x - \omega)$  (The book uses  $\varphi_n(x)$ .)

E.g.: The primitive 3rd roots of unity are  $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$  and  $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ ; so  $\Phi_3(x) = (x - \omega)(x - \omega^2) = x^2 + x + 1$ .

In fact, the first 6 cyclotomic polynomials are:

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1, \\ \Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \quad \Phi_6(x) = x^2 - x + 1.$$

Thm  $x^n - 1 = \prod_{d|n} \Phi_d(x)$

Pf: Every root of  $x^n - 1$  is an  $n^{\text{th}}$  root of unity, which is a primitive  $d^{\text{th}}$  root of unity for some  $d|n$ .  $\square$

Note: Even though  $\Phi_d(x)$  is a priori defined as an element of  $\mathbb{C}[x]$ , books give it belongs to  $\mathbb{Q}[x]$ . This is true and we'll prove it!

In fact the coefficients are integers, which can get arbitrarily big, but take a while ( $\Phi_{105}(x)$  is first with a coeff. not in  $\{1, -1\}$ ).

The way we will show cyclotomic polynomials are rational is by studying the extensions of  $\mathbb{Q}$  we get by adjoining their roots.

Def'n The  $n^{\text{th}}$  cyclotomic extension of  $\mathbb{Q}$  is the splitting field of  $x^n - 1$ . Equivalently, ...

Thm The  $n^{\text{th}}$  cyclotomic extension is  $\mathbb{Q}(\zeta_n)$ , where  $\zeta_n$  is a primitive  $n^{\text{th}}$  root of unity.

Pf: Since  $\zeta_n$  is an  $n^{\text{th}}$  root of unity, it belongs to splitting field of  $x^n - 1$ .  
But on other hand, every root of unity is a power of  $\zeta_n$ , hence in  $\mathbb{Q}(\zeta_n)$ .  $\square$

Thm Let  $\Psi_k: \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}(\zeta_n)$  be defined by  $\Psi_k(\zeta_n) = \zeta_n^k$ .

Then  $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \subseteq \{ \Psi_k : 1 \leq k \leq n, \gcd(n, k) = 1 \}$ .

Pf: Any  $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$  is determined by where it sends  $\zeta_n$ , which must be to some  $\zeta_n^k$  since these are roots of  $x^n - 1$ . But it cannot be sent to a non-primitive  $n^{\text{th}}$  root of unity, since it's not a root of any  $x^m - 1$  (with  $m < n$ ).  $\square$

Cor The cyclotomic polynomial  $\Phi_n(x) \in \mathbb{Q}[x]$ .

Pf:  $\mathbb{Q}(\zeta_n)$  is a Galois extension, since it's a splitting field, and every  $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$  fixes  $\Phi_n(x)$  since just permutes roots, so in fact coefficients of  $\Phi_n(x)$  are rational.  $\square$

Thm (Gauss)  $\Phi_n(x)$  is irreducible over  $\mathbb{Q}$ .

Pf: This is non-trivial but I skip it - see the book.  $\square$

Cor  $\Phi_n(x)$  is the minimal polynomial of  $\zeta_n$ , and every  $\Psi_k$  for  $\gcd(n, k) = 1$  is indeed an element of  $G = \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ .  
Hence  $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ , the multiplicative group mod  $n$ , via the isomorphism  $\Psi_k \mapsto k \in (\mathbb{Z}/n\mathbb{Z})^\times$ .

Remark: This shows  $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$  is an abelian group of order  $\varphi(n)$  where  $\varphi(n) = \# \{ 1 \leq k \leq n : \gcd(n, k) = 1 \}$

i) Euler's totient function. When  $n = p$  is prime we have seen that  $(\mathbb{Z}/p\mathbb{Z})^\times$  is in fact cyclic

(of order  $p-1$ ), but in general it need not be:

e.g.  $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ .

//

3/12

## Cyclic Extensions § 5.7

We are almost ready to study the solvability of polynomials by radicals. We just need one more preparatory result...

Def'n An <sup>algebraic, Galois</sup> extension  $L/K$  is called abelian if  $\text{Aut}_K(L)$  is abelian, it is called cyclic if  $\text{Aut}_K(L)$  is cyclic, and it is called cyclic of degree  $n$  if  $\text{Aut}_K(L) \cong \mathbb{Z}/n\mathbb{Z}$ .

Remark: We have seen that the cyclotomic extension  $\mathbb{Q}(\zeta_n)$  of  $\mathbb{Q}$  is always abelian, and sometimes cyclic (e.g. if  $n$  is prime) although not always.

In general it is hard to classify cyclic extensions, but there is a nice situation where we can do this.

Def'n For an arbitrary field  $K$ ,  $u \in K$  is called an  $n^{\text{th}}$  root of unity if  $u^n = 1 \in K$  and is called a primitive  $n^{\text{th}}$  root of unity if  $u, u^2, \dots, u^{n-1}$  are all distinct (hence all the  $n^{\text{th}}$  roots of unity).

For subfields of  $\mathbb{C}$ , this agrees with our previous definition.

Then let  $K$  be a field containing a primitive  $n^{\text{th}}$  root of unity  $\zeta_n$  for some  $n \geq 1$ . Then the following are equivalent for  $L/K$ :

- 1)  $L/K$  is cyclic of degree  $d$ , for some  $d \mid n$ .
- 2)  $L/K$  is the splitting field of a polynomial of form  $f(x) = x^n - a \in K[x]$ , in which case  $L = K(u)$  for  $u$  a root of  $f(x)$ .
- 3)  $L/K$  is splitting field of irreducible polynomial of form  $f(x) = x^d - a$  for some  $d \mid n$ , in which case  $L = K(u)$  for  $u$  root of  $f(x)$ .

E.g. Any degree 2 extension of  $\mathbb{Q}$  is the splitting field of a polynomial of the form  $x^2 - d$  where  $d$  is not a square in  $\mathbb{Q}$ , and this extension has Galois group  $\mathbb{Z}/2\mathbb{Z}$ .

E.g. On a previous homework you showed that if  $L = \mathbb{Q}(\omega, \sqrt[3]{2})$  is the splitting field of  $x^3 - 2$  over  $\mathbb{Q}$ , then  $\text{Aut}_K(L) \cong S_3$ , which is not cyclic (not even abelian!). But  $\mathbb{Q}$  does not have a prim. 3rd root of unity! If we instead take  $K = \mathbb{Q}(\omega)$ , then  $\text{Aut}_K(L) = \mathbb{Z}/3\mathbb{Z}$ .

In the theorem, 2) and 3) are easily seen to be equivalent, just having to do with whether  $x^n - a$  is irreducible, equivalently, whether  $a$  has a  $d$ th root in  $K$  for some  $d \mid n$ . The main point is showing  $3) \Leftrightarrow 1)$ . In fact we will mostly come about  $3) \Rightarrow 1)$ , which we will prove now ~~and~~ we just need:

Lemma If  $K$  is a field with a primitive  $n$ th root of unity  $\zeta$ , then for any  $d \mid n$ ,  $\eta = \zeta^{n/d}$  is a primitive  $d$ th root of 1.

And if  $L$  is an extension of  $K$  such that  $u \in L$  is a root of  $x^d - a \in K[x]$ , then all the roots of  $x^d - a$  are  $u, \eta u, \eta^2 u, \dots, \eta^{d-1} u$  (all distinct).

Pf. Straight forward exercise. P3

Pf of  $3) \Rightarrow 1)$  in thm: By the lemma, the roots of  $x^d - a$  in  $L$  are  $u, \eta u, \dots, \eta^{d-1} u$  where  $u$  is any root and  $\eta = \zeta^{n/d}$  as above. So any  $\sigma \in \text{Aut}_K(L)$  is determined by where it sends  $u$  (since  $\eta \in K$  is fixed by  $\sigma$ ). Since  $x^d - a$  is irreducible, there must be some  $\sigma$  with  $\sigma(u) = \eta u$ , and this  $\sigma$  generates all of  $\text{Aut}_K(L)$ . Since  $\sigma^k(u) = \eta^k u$ , which give all the possible automorphisms in the Galois group by the previous sentence. QED

We will only sketch the ideas that go into the pt of 1)  $\Rightarrow$  3):

Def'n Let  $L/K$  be a finite <sup>Galois</sup> extension, and suppose that  $\text{Aut}_K(L) = \{\sigma_1, \dots, \sigma_n\}$ . For any  $u \in L$ , the norm of  $u$  is  $N(u) = \sigma_1(u) \cdot \sigma_2(u) \cdot \dots \cdot \sigma_n(u)$ .

Eg. Let  $K = \mathbb{R}$  and  $L = \mathbb{C}$ . Recall that  $\text{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1, \sigma\}$  where  $\sigma: \mathbb{C} \mapsto \bar{\mathbb{C}}$  is complex conjugation. So the norm of  $z = a + bi \in \mathbb{C}$  is  $N(z) = z \cdot \bar{z} = a^2 + b^2$ , usual complex norm.

Eg. For  $K = \mathbb{Q}$  and  $L = \mathbb{Q}(i)$ , the same is true: the norm of  $a + bi$  is  $(a + bi)(a - bi) = a^2 + b^2 \in \mathbb{Q}$ .

Prop. If  $L/K$  is a finite Galois extension, then the norm  $N(u)$  of any  $u \in L$  is an element of the base field  $K$ .

Pf. For any  $\tau \in \text{Aut}_K(L)$ ,  $\tau(N(u)) = \tau(\sigma_1(u) \cdot \sigma_2(u) \cdot \dots \cdot \sigma_n(u))$   
 $= \tau(\sigma_1(u)) \cdot \tau(\sigma_2(u)) \cdot \dots \cdot \tau(\sigma_n(u))$   
 $= \sigma_{i_1}(u) \cdot \dots \cdot \sigma_{i_n}(u) = N(u)$

(where  $i_1, \dots, i_n$  is some permutation of  $1, \dots, n$ ), so because  $L/K$  is Galois,  $N(u) \in K$  as claimed.  $\square$

Remark: We can define the norm for non-Galois extensions too, and it remains true that it belongs to the ground field, but it's a little more technical.

Another important property of the norm is multiplicativity:

Prop. We have  $N(u) \cdot N(v) = N(uv)$  for  $u, v \in L$ .

Pf. Straight forward exercise.  $\square$

The norm is particularly useful for cyclic extensions...

Thm (Hilbert Theorem 90) Let  $L/K$  be a finite cyclic <sup>(Galois)</sup> extension and let  $\sigma \in \text{Aut}_K(L)$  be a generator of the Galois group. Then for  $u \in L$ ,  $N(u) = 1 \Leftrightarrow u = v/\sigma(v)$  for some  $v \in L$ .

Pf: One direction is easy: if  $u = \frac{v}{\sigma(v)}$  then  $N(u) = \frac{\sigma_1(v) \cdots \sigma_n(v)}{\sigma_1(v) \cdots \sigma_n(v)} = 1$

The other direction is nontrivial - see the book for a proof.  $\square$

Ex. Consider  $L = \mathbb{Q}(i)$  over  $K = \mathbb{Q}$ . The elements in  $\mathbb{Q}(i)$  of norm 1 are  $\frac{p}{r} + \frac{q}{r}i$  with  $\frac{p^2}{r^2} + \frac{q^2}{r^2} = 1$ , i.e.,  $p^2 + q^2 = r^2$ ,  $p, q, r \in \mathbb{Z}$ .

These are Pythagorean triples. Hilbert's Thm 90 says they can all be written in form  $\frac{a+bi}{a-bi} = \frac{a^2-b^2}{a^2+b^2} + \frac{2ab}{a^2+b^2}i$ ,  $a, b \in \mathbb{Z}$

It is a classic fact going back to Euclid that (primitive) Pythagorean triples can be parameterized in this way.

With Hilbert's thm 90 we can complete the pf of main thm.

Pf of 1)  $\Rightarrow$  3): Let  $\sigma \in \text{Aut}_K(L)$  be a generator, and let  $\eta = \zeta^{1/d}$  be a primitive  $d$ th root of unity.

Then  $N(\eta) = \eta \cdot \sigma(\eta) \cdots \sigma^{d-1}(\eta) = \eta^d$  (since  $\eta \in K$ )

so by Hilbert 90 we can write  $\eta = v/\sigma(v)$

for some  $v \in L$ . Notice  $\sigma(v^d) = (\sigma(v))^d = \left(\frac{v}{\eta}\right)^d = \frac{v^d}{\eta^d} = v^d$

(since  $\eta^d = 1$ ), so because the extension  $L/K$  is Galois,

this means that  $v^d \in K$ . Then  $v$  is a root of

the polynomial  $x^d - v^d \in K[x]$ , and it can be

shown that this polynomial is in fact irreducible

over  $K$  and that  $L = K(v)$  is the splitting field.  $\square$



3/17

## Radical Extensions & Solving Polynomials § 5.9

We come now to one of the major achievements of Galois theory: a precise understanding of when polynomial equations can be solved by expressing using radicals.

The famous quadratic formula  $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$  says that

the roots of any quadratic  $ax^2 + bx + c$  can be expressed in terms of the coefficients using the basic field operations  $(+, -, *, /)$  together with the square root  $\sqrt{\phantom{x}}$ .

Similarly, you saw on HW #4 how for any cubic equation  $ax^3 + bx^2 + cx + d = 0$ , we can express the solutions in terms of the coefficients using field operations together with square roots and cube roots.

In fact, there is also a "quartic formula" expressing the solutions to a degree 4 equation in terms of radicals (i.e.,  $n^{\text{th}}$  roots  $\sqrt[n]{\phantom{x}}$ ), but the pattern stops there: as we will see, there is no general "quintic formula."

Def'n Let  $K$  be a field. We say a finite (hence, algebraic) extension  $L = K(u_1, u_2, \dots, u_n)$  of  $K$  is a radical extension if for each  $i = 1, \dots, n$ , there is an  $m \geq 1$  such that  $u_i^m \in K(u_1, \dots, u_{i-1})$ , i.e.  $u_i$  is an " $m^{\text{th}}$  root" of an element in  $K(u_1, \dots, u_{i-1})$ .

Def'n Let  $f(x) \in K[x]$  be a polynomial. We say that  $f(x)$  is solvable by radicals if the splitting field of  $f(x)$  is a subfield of some radical extension of  $K$ .

This captures the notion of the roots of  $f(x)$  being expressible from  $K$  using the field operations & radicals.



Not only will we show that there is no general formula for equations of degree  $n \geq 5$  (using radicals), we will show that, for all degrees  $n \geq 5$ , there are specific polynomials  $f(x) \in \mathbb{Q}[x]$  for which  $f(x)$  is not solvable by radicals.

Remark: Notice that we take  $K = \mathbb{Q}$  here. If we took, e.g.,  $K = \mathbb{C}$ , then every  $f(x) \in \mathbb{C}[x]$  is "solvable by radicals" for the trivial reason that the roots of  $f(x)$  belong to the base field  $\mathbb{C}$ .

The key to showing that some polynomials are not solvable by radicals is to show that the Galois groups of polynomials that are solvable by radicals have a restricted form.

So we need to recall some notions from group theory.

Def'n Let  $G$  be a group. For  $x, y \in G$ ,  $[x, y] = xyx^{-1}y^{-1}$  is the commutator of  $x$  and  $y$  (measures extent to which  $x$  and  $y$  fail to commute) and for  $H_1, H_2 \leq G$  we use  $[H_1, H_2] = \langle [x, y] : x \in H_1, y \in H_2 \rangle$ . The derived subgroup of  $G$  is  $G' = [G, G]$ , it is  $\{e\}$  exactly when  $G$  is abelian. We say that  $G$  is solvable if the derived series  $G^{(0)} = G$ ,  $G^{(i)} = (G^{(i-1)})'$

eventually reaches the trivial subgroup:

$$\{e\} = G^{(k)} \trianglelefteq G^{(k-1)} \trianglelefteq \dots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G.$$

(That  $G'$  is normal in  $G$  is an easy exercise.)

Recall by comparison that  $G$  is nilpotent if its lower central series  $G^0 = G$ ,  $G^i = [G, G^{i-1}]$  eventually reaches the trivial subgroup:

$$\{e\} = G^k \trianglelefteq G^{k-1} \trianglelefteq \dots \trianglelefteq G^1 \trianglelefteq G^0 = G.$$

Every abelian group is nilpotent, and every nilpotent group is solvable (but not conversely).

E.g. The dihedral group  $D_4$  of order 8 is nilpotent but not abelian. The symmetric group  $S_3$  on 3 letters is solvable but not nilpotent. The alternating group  $A_5$  of order 60 is not solvable, since it is simple and non-abelian.

Prop. If  $G$  is solvable and  $H \subseteq G$  then  $H$  is solvable.

Pf: Derived series of  $H$  is "smaller" than that of  $G$ .

E.g. For any  $n \geq 5$ , the symmetric group  $S_n$  is not solvable, since  $A_n$ , a simple non-abelian group, is not solvable.

Thm A group  $G$  is solvable if and only if it has a

sub-normal series  $\{e\} = G_k \triangleleft G_{k-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$

such that the factor groups  $G_i/G_{i+1}$  are all abelian.

Pf: The derived series of a solvable group is such a series, since  $G/G'$  is always abelian. We proved the other direction last semester when discussing composition series and the Jordan-Hölder Theorem.

Explaining the name "Solvable," we have the following main result:

Thm A polynomial  $f(x) \in K[x]$  is solvable by radicals only if its Galois group, i.e. the group  $\text{Aut}_K(L)$  where  $L$  is its splitting field, is a solvable group.

A "generic" polynomial  $f(x) \in \mathbb{Q}[x]$  of degree  $n$  has  $S_n$  as its Galois group, hence by the previous theorem it does not have a solution in radicals for  $n \geq 5$  (this is the "Abel-Ruffini Theorem").