

# Math 250A Lecture 23 Notes

Daniel Raban

November 16, 2017

## 1 Cyclic Extensions and Cyclotomic Polynomials

### 1.1 Cyclic extensions

**Definition 1.1.** A *cyclic extension* is a Galois extension with a cyclic Galois group.

Last time, we determined that a cyclic extension  $L/K$  is  $K[\sqrt[n]{a}]$  if the characteristic does not divide  $n$  and  $K[\alpha]$  otherwise, where  $\alpha^n - \alpha - b = 0$ ; also note that the former element is the solution to  $\alpha^n - a = 0$ . The nice thing about this is that if we know one root,  $\alpha$ , then we know other roots ( $\alpha\zeta^i$  and  $\alpha + i$ , respectively).

Which polynomials can be “solved by radicals”? What we means is that roots can be written using addition, subtraction, multiplication, and  $k$ -th roots. For example, the roots to a quadratic equation  $ax^2 + bx + c$  are  $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ .<sup>1</sup>

**Theorem 1.1.** *The Galois group is solvable iff roots can be given using radicals and Artin-Schrier equations ( $\text{char} > 0$ ).*

*Proof.* Suppose an equation is solvable by radicals. Assume that the base field  $K$  contains all roots of 1 we need. Look at  $K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq L$ , where  $L$  is the splitting field of the polynomial.  $K_1 = K_0(\sqrt[n]{a_1})$ . Look at the Galois groups:

$$G \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq 1.$$

$G_2$  is normal in  $G_1$ , and  $G_1/G_2$  is cyclic.  $G$  has a chain of subgroups, each normal in the next, and all quotients are cyclic. So  $G$  is solvable.

Suppose  $G$  is solvable (and  $K$  contains all roots of 1). We have

$$G \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq 1,$$

---

<sup>1</sup>Mathematicians used to duel for money and prestige, presenting each other with difficult problems to solve. Cardano came up with a general solution for finding roots of degree 4 polynomials, which became a valuable asset for him in these duels.

where  $G_i$  is normal in  $G_{i-1}$ , and  $G_{i-1}/G_i$  is cyclic of prime order. Look at the fields

$$K \subseteq \underbrace{K_1}_{=L^{G_1}} \subseteq \underbrace{K_2}_{=L^{G_2}} \subseteq \cdots \subseteq L.$$

$K_{i+1}/K_i$  is a cyclic Galois extension, so  $K_{i+1} = K_i(\sqrt[n]{\alpha_n})$  or Artin-Schrier.  $\square$

**Example 1.1.** Consider  $x^5 - 4x + 2$ . The Galois group is  $S_5$ , which has order 120. The only normal subgroups are 1,  $A_5$ , and  $S_5$ . This polynomial is not solvable by radicals.

**Example 1.2.**  $x^5 - 2$  is irreducible and of degree 5, but it can be solve by radicals. The Galois group is solvable. The field extensions look like  $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\zeta, \sqrt[5]{2})$ . The corresponding groups of the wuotients of the Galois groups are  $\mathbb{Z}/4\mathbb{Z}$  and  $\mathbb{Z}/5\mathbb{Z}$ , which are cyclic.

**Example 1.3.** All polynomials of degree  $\leq 4$  can be solved by radicals (in characteristic 0), the Galois groups is a subgroup of  $S_4$ , so it is solvable. We have

$$S_4 \supseteq A_4 \supseteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \supseteq 1.$$

## 1.2 Cyclotomic polynomials

Over  $\mathbb{Q}$ , the roots of unity are the roots of  $x^n - 1 = 0$ . How does this factor into irreducibles? Look at  $x^{12} - 1$ . This is divisible by  $x^6 - 1$ ,  $x^4 - 1$ ,  $x^3 - 1$ , etc., but these have factors in common.

**Definition 1.2.** The  $n$ -th *cyclotomic polynomial*  $\Phi_n(x)$  is the polynomial with roots the primitive  $n$ -th roots of unity (order exactly  $n$ ).

**Example 1.4.** Let's compute some examples:

| $n$ | $\Phi_n(x)$   |
|-----|---|
| 1   | $x - 1$   |
| 2   | $x + 1$   |
| 3   | $x^3 + x + 1 = \frac{x^3 - 1}{x - 1}$                       |
| 4   | $x^2 + 1 = \frac{x^4 - 1}{x^2 - 1}$                         |
| 5   | $x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1}$           |
| 6   | $x^2 - x + 1 = \frac{(x^6 - 1)(x - 1)}{(x^3 - 1)(x^2 - 1)}$ |

**Example 1.5.** We have to make sure we're not dividing by factors multiple times, so we must put an  $x - 1$  in the numerator:

$$\Phi_{12}(x) = \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = x^4 - x^2 + 1$$

$$x^{12} - 1 = \Phi_{12}(x)\Phi_6(x)\Phi_4(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).$$

**Example 1.6.** Again, we make sure we don't divide by factors multiple times.

$$\Phi_{15}(x) = \frac{(x^{15} - 1)(x - 1)}{(x^5 - 1)(x^3 - 1)} = x^8 - x^7 + x^5 - x^4 + x^2 - x + 1.$$

If you want to really understand cyclotomic polynomials, try out the following exercise: Find the smallest  $n$  such that  $\Phi_n(x)$  has a coefficient not 0 or  $\pm 1$ .<sup>2</sup>

**Theorem 1.2.**  $\Phi_n(x)$  is irreducible over  $\mathbb{Q}$ . Its Galois group is  $(\mathbb{Z}/n\mathbb{Z})^*$ .

*Proof.* If  $b$  is prime, we have proved this using Eisenstein's criterion. A similar proof works for prime powers. For general  $n$ , we use a different argument. The first key idea is to reduce (mod  $p$ ) for primes  $p$ . The second key idea is to use the Frobenius map,  $F(t) = t^p$ , where the field has characteristic  $p$ ;  $F$  is an automorphism.

Suppose  $f$  is an irreducible factor of  $\Phi_n(x)$  (over  $\mathbb{Q}$ ). Form  $\mathbb{Z}[\zeta] = \mathbb{Z}[x]/f(x)$ . This is an integral domain, and the quotient field  $\mathbb{Q}(\zeta)$  is generated by a primitive  $n$ -th root  $\zeta$  of 1. Use  $\mathbb{Z}$ , not  $\mathbb{Q}$  to reduce mod  $p$ .  $\mathbb{Z}[\zeta]$  contains  $n$  distinct roots of  $x^n - 1$ :  $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ . Now choose an irreducible factor  $g(x)$  of  $f(x)$  in  $F_p(x)$  (factor  $f \pmod{p}$ ). In general,  $\deg g < \deg f$ . The key point is that since  $x^n - 1$  has  $n$  distinct roots,  $nx^{n-1} = \frac{d}{dx}(x^n - 1)$  and  $x^n - 1$  are coprime.

Since  $\zeta$  is a root of  $g$  (which is irreducible),  $\zeta^p$  is also a root of  $g$  as  $t \mapsto t^p$  is an automorphism of  $F_p(\zeta)$ . So in  $\mathbb{Z}[\zeta]$ ,  $\zeta^p$  is also a root of  $f$ . Then the map from roots of unity in  $\mathbb{Z}[s]$  to roots of unity in  $F_p[\zeta]$  is bijective. So if  $p$  does not divide  $n$ , then the roots of  $f$  are closed under the map  $\zeta \mapsto \zeta^p$ .

Now look at the Galois group of  $\mathbb{Z}[\zeta]$ . Automorphisms take  $\zeta \mapsto \zeta^k$  for  $k, n$  coprime, so the Galois group is a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^*$ . The Galois group contains  $\zeta \mapsto \zeta^p$  for  $p, n$  coprime, which generate  $(\mathbb{Z}/n\mathbb{Z})^*$ . So the Galois group equals  $(\mathbb{Z}/n\mathbb{Z})^*$ , so  $f = \Phi_n(x)$ .  $\square$

**Definition 1.3.** A cyclotomic<sup>3</sup> field is a field generated by roots of unity.

## 1.3 Applications of cyclotomic polynomials

### 1.3.1 Primes modulo $n$

**Theorem 1.3.** Suppose  $n \in \mathbb{Z}$ . There are infinitely many primes  $p > 0$  with  $p \equiv 1 \pmod{n}$ .<sup>4</sup>

*Proof.* The idea is to look at the primes  $P$  dividing  $\Phi_n(a)$  for some  $a$ . Suppose  $p, n$  are coprime. Then all roots of  $\Phi_n(x)$  are distinct mod  $p$ . So  $\Phi_n(x)$  is coprime to  $\Phi_m(x)$  in

<sup>2</sup>You may have to check  $n > 100$ , but do not just do this brute force. You should do small cases and notice some kind of pattern.

<sup>3</sup>"Cyclo" means "circle," and "tomic" means "cut."

<sup>4</sup>Dirichlet proved this for  $p \equiv a \pmod{n}$  for any  $a$  coprime to  $n$ , but the proof is not as nice. There seems to be no known way to extend the nice proof to this more general case, which frustrates some people.

$F_p(x)$  for  $m$  dividing  $n$ . So if  $p \mid \Phi_n(a)$ ,  $p$  does not divide  $\Phi_m(a)$  for  $m \mid n$ . This says that if  $\Phi_n(a) \equiv 0 \pmod{p}$ , then  $\Phi_m(a) \not\equiv 0 \pmod{p}$  when  $m \mid n$ . So if  $a^n \equiv 1 \pmod{p}$ , then  $a^m \not\equiv 1 \pmod{p}$  for  $m \mid n$ . So  $a$  has order exactly  $n \pmod{p}$ , so  $n$  divides  $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$ , so  $p \equiv 1 \pmod{n}$ .

So if  $p \mid \Phi_n(a)$ , then either  $p \mid n$  or  $p \equiv 1 \pmod{n}$ . Suppose  $p_1, \dots, p_k$  are  $1 \pmod{n}$ . Choose  $p$  dividing  $\Phi_n(np_1 \cdots p_k)$ .  $\Phi_n(x) = 1 + x + \cdots$ , so this is  $1 \pmod{n} p_1 \cdots p_k$ , so  $p$  does not divide  $p_1 \cdots p_k$ . Then  $p$  does not divide  $n$ . So we have found  $p$ , a new prime  $\equiv 1 \pmod{n}$ .  $\square$

**Example 1.7.** Let  $n = 8$ . Then  $\Phi_8(a) = a^4 + 1$ . if  $a = 1$ , we get 2, which divides 8. If  $a = 2$ , we get 9, which is  $1 \pmod{8}$ . If  $a = 3$ , we get  $82 = 41 \times 2$ ;  $41 \equiv 1 \pmod{8}$ , and  $2 \mid 8$ .

### 1.3.2 Galois extensions over $\mathbb{Q}$

Recall the hard problem: given finite  $G$ , is  $G$  a Galois group of  $K/\mathbb{Q}$  for some  $K$ ?

**Theorem 1.4.** *If  $G$  is abelian, there exists some  $K/\mathbb{Q}$ , such that  $G$  is the Galois group of  $K/\mathbb{Q}$ .*

*Proof.* Write  $G$  as a product of cyclic groups:

$$G = (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots .$$

Choose distinct primes  $p_1 \equiv 1 \pmod{n_1}, p_2 \equiv 1 \pmod{n_2}, \dots$ .  $(\mathbb{Z}/n_1\mathbb{Z})$  is a quotient of  $(\mathbb{Z}/p_1 + 1\mathbb{Z})^*$ . So  $G$  is a quotient of  $\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots)^* = (\mathbb{Z}/p_1 p_2 \cdots \mathbb{Z})^*$ , which is the Galois group of  $x^{p_1 \cdots p_n} - 1$ . So any quotient  $G/H$  is the Galois group of some extension  $K/\mathbb{Q}$ .  $\square$

Here is a type of converse, which we will not prove.

**Theorem 1.5** (Kronecker-Weber-Hilbert). *If  $K$  is a Galois extension of  $\mathbb{Q}$  with abelian Galois group, then  $K \subseteq \mathbb{Q}(\zeta)$  for some root of unity  $\zeta$ .*

### 1.3.3 Finite division algebras

Can we find finite analogues of the quaternions  $\mathbb{H}$ ? This is a division algebra that is a “non-commutative field.”

**Theorem 1.6** (Wedderburn). *Any finite division algebra is a field (commutative).*

*Proof.* Recall that any group  $G$  is the union of its conjugacy classes, which have sizes  $|G|/|H|$ , where  $H$  is a subgroup centralizing a representative element of a conjugacy class.

Let  $L$  be a finite division algebra, and let  $K$  be its center, a field  $F_q$  of order  $q$  for some prime power  $q$ . Look at the group  $G = L^*$ , which has order  $q-1$ . Suppose  $a \in G$ . The

centralizer of  $a$  in  $L$  is a subfield of order  $q^k$  for some  $k$ , so the centralizer of  $a$  in  $G$  is a subfield of order  $q^k - 1$  ( $0 \notin G$ ). So

$$q^{n-1} = q - 1 + \sum_i \frac{q^n - 1}{q^{k_i - 1}},$$

where the sum is over conjugacy classes of orders  $> 1$ . Note that  $k_1 < n$ .

Now note that  $q^{n-1}$  is divisible by  $\Phi_n(q)$ . Also note that so is  $(q^n - 1)/(q^{k_i - 1})$ , as  $k_1 < n$ . So  $q - 1$  is divisible by  $\Phi_n(x) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} (q - \zeta^i)$ . But observe that  $|q - \zeta^i| > q - 1$  unless  $\zeta^i = 1$ . So  $n = 1$ . So  $L = K$ , which makes  $L$  commutative.  $\square$

**Definition 1.4.** The *Brauer group* is the group of isomorphism classes of a finite dimensional division algebras over a field  $K$  with center  $K$ .

**Example 1.8.** The Brauer group of  $\mathbb{R}$  has 2 elements:  $\mathbb{R}$ , and  $\mathbb{H}$ .

If  $D_1, D_2$  are division algebras,  $D_1 \otimes_K D_2 \cong M_n(D_3)$  for some  $n, D_3$ , where  $D_3$  is the product of  $D_1, D_2$  in the Brauer group.

**Remark 1.1.** Wedderburn's theorem shows that the Brauer group of a finite field is trivial.

## 1.4 Norm and trace in finite extensions

Let  $L/K$  be a finite extension, and choose  $a \in L$ . Multiplication by  $a$  is a linear transformation from  $L \rightarrow L$ , where  $L$  is viewed as a vector space over  $K$ .

**Definition 1.5.** The *trace* of  $a$  is defined as the trace of  $a$  as a linear transformation. The norm of  $a$  is the determinant of  $a$  as a linear transformation.

**Definition 1.6.** The *norm* of  $a$  is the determinant of  $a$  as a linear transformation.<sup>5</sup>

**Example 1.9.** Take  $\mathbb{C}/\mathbb{R}$  and  $a = x + iy \in \mathbb{C}$ . A basis for  $\mathbb{C}/\mathbb{R}$  is  $\{1, i\}$ .  $a \cdot 1 = x + iy$ , and  $a \cdot i = -y + ix$ . So  $a$  is given by the matrix

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix}.$$

So the trace of  $a$  is  $2x$ , and the norm is  $x^2 + y^2$ .

---

<sup>5</sup>Ignore Lang's definition. Professor Borchers thinks it is "silly."