Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Equations and Groups
   - Solution by Radicals
   - Cyclotomic Polynomials
   - Cyclic Extensions

Subsection 1

Solution by Radicals

Linear and Quadratic Equations

- The roots of a polynomial equation
$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$$
with rational coefficients are functions of those coefficients.
- For the linear equation $X + a_0 = 0$, the unique solution $-a_0$ is a rational function of the coefficients.
- In the case of a quadratic equation $X^2 + a_1X + a_0 = 0$
$$\alpha = \frac{1}{2}(-a_1 + \sqrt{\Delta}), \qquad \beta = \frac{1}{2}(-a_1 - \sqrt{\Delta}),$$
where $\Delta = a_1^2 - 4a_0$.

  The number Δ is called the **discriminant** of the equation.

  The roots, in general, belong not to $\mathbb{Q}$, but to the extension $\mathbb{Q}(\sqrt{\Delta})$.

  The sum and product of the roots are $\alpha + \beta = -a_1$ and $\alpha\beta = a_0$.

The Cubic Equation

- Consider the cubic equation $X^3 + a_2X^2 + a_1X + a_0 = 0$.
  If we make the substitution $X = Y - \frac{1}{3}a_2$, we obtain
  $$Y^3 - a_2Y^2 + \frac{1}{3}a_2^2Y - \frac{1}{27}a_2^3 + a_2Y^2 - \frac{2}{3}a_2^2Y + \frac{1}{9}a_2^3 + a_1Y - \frac{1}{3}a_1a_2 + a_0 = 0.$$
  We can rewrite as $Y^3 + aY + b = 0$. We may thus confine our attention to cubic equations in which there is no quadratic term.
  To avoid some fractions we write the standard cubic equation as
  $$X^3 + 3aX + b = 0.$$
  Let p be a root. Find q and r, such that $q + r = p$ and $qr = -a$.
  These are the roots of the quadratic equation $X^2 - pX - a = 0$ (and will in general be complex numbers). Then
  $$(q+r)^3 = q^3 + r^3 + 3(q^2r + qr^2) = q^3 + r^3 + 3pqr$$
  $$0 = p^3 + 3ap + b = q^3 + r^3 + 3p(a + qr) + b = q^3 + r^3 + b.$$

The Cubic Equation (Cont'd)

- From $q^3 + r^3 = -b$ and $q^3 r^3 = -a^3$, we deduce that q^3 and r^3 are the roots of the equation $Z^2 + bZ - a^3 = 0$. Hence we may write
$$q^3 = \frac{1}{2}(-b + \sqrt{\Delta}), \quad r^3 = \frac{1}{2}(-b - \sqrt{\Delta}), \quad \Delta = b^2 + 4a^3.$$
We find q and r, and hence p, by taking cube roots:
Let q_1, r_1 be cube roots (respectively) of q^3, r^3, such that $q_1 r_1 = -a$.
If $\omega = e^{2\pi i/3}$ and $\omega^2 = e^{4\pi i/3}$ are the complex cube roots of unity, we also have $(q_1\omega)(r_1\omega^2) = -a$ and $(q_1\omega^2)(r_1\omega) = -a$.
Hence we have three possible values for p:
$$q_1 + r_1, \quad q_1\omega + r_1\omega^2, \quad q_1\omega^2 + r_1\omega,$$
where
$$q_1 = \left[\frac{1}{2}(-b + \sqrt{b^2 + 4a^3})\right]^{1/3}, \quad r_1 = \left[\frac{1}{2}(-b - \sqrt{b^2 + 4a^3})\right]^{1/3}.$$

Example

- Find the three roots of $X^3+6X+2=0$.

  Here $a=b=2$.

  q^3 and r^3 satisfy $q^3+r^3=-b=-2$ and $q^3r^3=-a^3=-8$.

  So they are solutions of $Z^2+2Z-8=0$.

  We find $q^3=-4$ and $r^3=2$.

  So $q=2^{1/3}$ and $r=-4^{1/3}=-2^{2/3}$ (with $qr=-a=-2$).

  Now the three solutions of the cubic are

$$q+r \quad q\omega+r\omega^2, \quad q\omega^2+r\omega.$$

- That example, in which the discriminant of $Z^2+2Z-8=0$ has a rational square root, is perhaps a little contrived, for the discriminant may well be a complex number.

Example

- Find the three roots of $X^3-6X+2=0$.

  Here $a=-2$ and $b=2$.

  q^3 and r^3 satisfy $q^3+r^3=-b=-2$ and $q^3r^3=-a^3=8$.

  So they are solutions of $Z^2+2Z+8=0$.

  We find $q^3=-1-\sqrt{7}i=\sqrt{8}e^{-i\theta}$ and $r^3=-1+\sqrt{7}i=\sqrt{8}e^{i\theta}$.

  Here θ is such that $\cos\theta=-\frac{1}{\sqrt{8}}$, $\sin\theta=\frac{\sqrt{7}}{\sqrt{8}}$.

  So $q=\sqrt{2}e^{-i\theta/3}$ and $r=\sqrt{2}e^{i\theta/3}$ (with $qr=-a=2$).

  Now the three solutions of the cubic are

$$q+r=2\sqrt{2}\cos\left(\frac{\theta}{3}\right) \quad q\omega+r\omega^2, \quad q\omega^2+r\omega.$$

Solution By Radicals

- The solution of the cubic is what is called a **solution by radicals**.
- This means that the function

$$(a,b) \mapsto \left[\frac{1}{2}(-b+\sqrt{b^2+4a^3})\right]^{1/3} + \left[\frac{1}{2}(-b-\sqrt{b^2+4a^3})\right]^{1/3}$$

from the coefficients to the solution involves, in addition to rational operations, only the taking of square roots and cube roots.

The Quartic Equation

- Consider, next the quartic equation

$$X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = 0.$$

Again substituting $X = Y - \frac{a_3}{4}$ means that we may consider only equations $X^4 + aX^2 + bX + c = 0$ in which the cubic term is absent. Suppose that, over some extension of $\mathbb{Q}$, the polynomial factorizes into quadratic factors (which, due to the absence of X^3, should be)

$$X^4 + aX^2 + bX + c = (X^2 + pX + q)(X^2 - pX + r).$$

Multiplying out, we get

$$X^4 + aX^2 + bX + c = X^4 + (q + r - p^2)X^2 + (pr - pq)X + qr.$$

Equating coefficients, we get

$$q + r - p^2 = a, \quad p(r - q) = b, \quad qr = c.$$

The Quartic Equation (Cont'd)

- We got
$$q+r-p^2=a, \quad p(r-q)=b, \quad qr=c.$$
Now we have
$$\left\{\begin{array}{rcl} q+r-p^2 & = & a \\ pr-pq & = & b \end{array}\right\} \Rightarrow \left\{\begin{array}{rcl} pq+pr & = & p^3+ap \\ pr-pq & = & b \end{array}\right\}$$
$$\Rightarrow \left\{\begin{array}{rcl} 2pr & = & p^3+ap+b \\ 2pq & = & p^3+ap-b \end{array}\right\}$$
$$4p^2c=4p^2qr=(2pr)(2pq)=(p^3+ap+b)(p^3+ap-b)$$
$$=p^6+2ap^4+a^2p^2-b^2$$
$$p^6+2ap^4+(a^2-4c)p^2-b^2=0.$$
This is a cubic in p^2.
So it can be solved by taking square and cube roots.
Then p can be found by taking square roots.

The Quartic Equation (Conclusion)

- We determine p^2 (and hence p) using the procedure of a cubic on $p^6+2ap^4+(a^2-4c)p^2-b^2=0$.

  Then, we determine q and r, using

  $$q+r-p^2=a, \quad p(r-q)=b, \quad qr=c.$$

  Finally we solve the two quadratic equations

  $$X^2+pX+q=0 \quad \text{and} \quad X^2-pX+r=0.$$

  Again this is a solution by radicals:

  - The determination of p involves square and cube roots;
  - The finding of q and r involves only rational operations;
  - The solving of the quadratic equations involves square roots.

Radical Extensions

- All fields will be of characteristic 0.
- Let K be a field.
- A field L containing K is called an **extension by radicals**, or a **radical extension**, if there is a sequence

$$K = L_0,\ L_1,\ \ldots,\ L_m = L,$$

  with the property that, for all $j = 0, 1, \ldots, m-1$,

  $L_{j+1} = L_j(\alpha_j)$, where α_j is a root of an irreducible polynomial in $L_j[X]$ of the form $X^{n_j} - c_j$.
- This formalizes the notion that the elements of L can be obtained from those of K by means of rational operations together with the taking of n_j-th roots ($j = 1, 2, \ldots, m$).

Solvability by Radicals

- Example: If $K = \mathbb{Q}$, the element
$$(3+\sqrt{2})^{1/7} + 5\sqrt[5]{2}(8-\sqrt[3]{4})^{1/11}$$
lies in a field L_5, where:
$$\begin{array}{ll} L_1 = \mathbb{Q}(\alpha_0), & \alpha_0^2 = 2 \in \mathbb{Q}, \\ L_2 = L_1(\alpha_1), & \alpha_1^7 = 3+\sqrt{2} \in L_1, \\ L_3 = L_2(\alpha_2), & \alpha_2^3 = 4 \in L_2, \\ L_4 = L_3(\alpha_3), & \alpha_3^{11} = 8-\sqrt[3]{4} \in L_3, \\ L_5 = L_4(\alpha_4), & \alpha_4^5 = 2 \in L_4. \end{array}$$
- A polynomial f in $K[X]$ is said to be **soluble by radicals** if there is a splitting field for f contained in a radical extension of K.
- We saw that all linear, quadratic, cubic and quartic equations are soluble by radicals.

Normal Closure of Radical Extensions

Theorem

Let L be a radical extension of K, and let M be a normal closure of L. Then M is also a radical extension of K.

- By a preceding theorem, $M = L_1 \vee L_2 \vee \cdots \vee L_k$, where the extensions $L_1, L_2, \ldots, L_k$ are all isomorphic to L, and so all radical.

  It suffices to show the join of two radical extensions is radical.

  Let $M_1 = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$, $M_2 = K(\beta_1, \beta_2, \ldots, \beta_n)$, where:
  - $\alpha_i^{k_i} \in K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$, $i = 1, \ldots, m$;
  - $\beta_j^{\ell_j} \in K(\beta_1, \beta_2, \ldots, \beta_{j-1})$, $j = 1, \ldots, n$.

  Then $M_1 \vee M_2 = K(\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n)$, with:
  - $\alpha_i^{k_i} \in K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$, $i = 1, \ldots, m$;
  - $\beta_j^{\ell_j} \in K(\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_{j-1})$, $j = 1, \ldots, n$.

  Thus, $M_1 \vee M_2$ is a radical extension.

Subsection 2

Cyclotomic Polynomials

The Roots of the Polynomial $X^m - 1$

- Consider the polynomial $f = X^m - 1$.
- Since we are working in fields K of characteristic 0, the splitting field L of f over K is both normal and separable.
- The set R consisting of the roots in L of $X^m - 1$ is easily seen to be an (abelian) multiplicative subgroup of L.

Lemma

$(R, \cdot)$ is a cyclic group.

- Denote the exponent of R by e. Then $a^e = 1$, for all a in R.
  - Now $X^e - 1$ has at most e roots. So we must have $|R| \leq e$.
  - However, the exponent of a group can never exceed the order of the group. So $e \leq |R|$.

Thus, $e = |R| = m$. So R is cyclic.

Primitive Roots of Unity and Cyclotomic Polynomials

- A **primitive m-th root of unity** ω is a generator of the cyclic group R of the roots of $X^m - 1$.
- Then $R = \{1, \omega, \omega^2, \ldots, \omega^{m-1}\}$.
- ω^j is a primitive m-th root of unity if and only if j and m are coprime.
- Let P_m be the set of primitive m-th roots of unity.
- The **cyclotomic polynomial** Φ_m is defined by

$$\Phi_m = \prod_{\epsilon \in P_m} (X - \epsilon).$$

Example

- Let K be a field of characteristic 0.

  Let $L \subseteq \mathbb{C}$ be the splitting field for $X^p - 1$, where p is prime.

  Then, except for 1, all of the roots of $X^p - 1$ are primitive.

  So
  $$\Phi_p = \frac{X^p - 1}{X - 1} = X^p + X^{p-1} + \cdots + X + 1.$$

Example

- Let $K = \mathbb{Q}$ and let $L \subseteq \mathbb{C}$ be the splitting field of $X^{12} - 1$.
  One of the primitive 12-th roots of unity is $\omega = e^{\pi i/6}$.
  The elements of R are

$$1, \omega, \omega^2 = e^{\pi i/3}, \omega^3 = i, \omega^4 = e^{2\pi i/3}, \omega^5 = e^{5\pi i/6}, \omega^6 = -1,$$
$$\omega^7 = e^{7\pi i/6}, \omega^8 = e^{4\pi i/3}, \omega^9 = -i, \omega^{10} = e^{5\pi i/3}, \omega^{11} = e^{11\pi i/6}.$$

  The group R contains the set P_d of primitive d-th roots of unity, for each of the divisors $d = 12, 6, 4, 3, 2, 1$ of 12. Let $\Phi_d = \prod_{\epsilon \in P_d} (X - \epsilon)$.
  The set P_{12} is $\{\omega, \omega^5, \omega^7 = \overline{\omega}^5, \omega^{11} = \overline{\omega}\}$. So we have

$$\begin{array}{rcl}
\Phi_{12} & = & (X - e^{\pi i/6})(X - e^{-\pi i/6})(X - e^{5\pi i/6})(X - e^{-5\pi i/6}) \\
& = & (X^2 - 2\cos\frac{\pi}{6} + 1)(X^2 - 2\cos\frac{5\pi}{6} + 1) \\
& = & (X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1) \\
& = & X^4 - X^2 + 1.
\end{array}$$

Example (Cont'd)

- The set P_6 is $\{\omega^2, \omega^{10} = \overline{\omega}^2\}$, and $\Phi_6 = X^2 - X + 1$.

  The set P_4 is $\{i, -i\}$, and $\Phi_4 = X^2 + 1$.

  The set P_3 is $\{\omega^4, \omega^8 = \overline{\omega}^4\}$, and $\Phi_3 = X^2 + X + 1$.

  The set P_2 is $\{\omega^6\}$, and $\Phi_2 = X + 1$.

  Finally, $P_1 = \{1\}$, and $\Phi_1 = X - 1$.

  Observe that, for $d \mid 12$, Φ_d has rational coefficients.

  Moreover

$$\begin{aligned} X^{12} - 1 &= \prod_{d \mid 12} \Phi_d \\ &= (X-1)(X+1)(X^2+X+1)(X^2+1)(X^2-X+1)(X^4-X^2+1). \end{aligned}$$

Generalizing

- Let K be a field of characteristic 0.
- Let $m \geq 1$.
- Let L a splitting field over K for $X^m - 1$.
- Then
$$X^m - 1 = \prod_{d|m} \Phi_d,$$
where we are including both 1 and m among the divisors of m.
- Note that, for $0 \leq k < m$, $X - \omega^k$ is a factor of Φ_d, where
  - $(k, d) = 1$;
  - $d = \frac{m}{\mathrm{GCD}(k,m)}$.

  Therefore, we have
$$\begin{aligned} X^m - 1 &= \prod_{0 \leq k < m} (X - \omega^k) = \prod_{d = \frac{m}{\mathrm{GCD}(k,m)}} \prod_{(k,d)=1} (X - \omega^k) \\ &= \prod_{d|m} \prod_{(k,d)=1} (X - \omega^k) = \prod_{d|m} \Phi_d. \end{aligned}$$

The Coefficient Lemma

Lemma

Let K, L be fields, with $K \subseteq L$. Let f, g be polynomials in $L[X]$, such that $f, fg \in K[X]$. Then $g \in K[X]$.

- Let $f = a_0 + a_1X + \cdots + a_mX^m$, $g = b_0 + b_1X + \cdots + b_nX^n$, where $a_0, a_1, \ldots, a_m \in K$, $b_0, b_1, \ldots, b_n \in L$, $a_m \neq 0$ and $b_n \neq 0$. Suppose that
$$fg = c_0 + c_1X + \cdots + c_{m+n}X^{m+n} \in K[X].$$
Then $b_n = \frac{c_{m+n}}{a_m} \in K$. Suppose inductively that $b_j \in K$, for all $j > r$. Then
$$c_{m+r} = a_m b_r + a_{m-1} b_{r+1} + \cdots + a_{m-n+r} b_n,$$
where $a_i = 0$ if $i < 0$. Hence,
$$b_r = \frac{c_{m+r} - a_{m-1} b_{r+1} - \cdots - a_{m-n+r} b_n}{a_m} \in K.$$
It follows that $b_j \in K$, for all j. So $g \in K[X]$.

Home of the Cyclotomic Polynomials

Theorem

Let K be a field of characteristic 0, containing m-th roots of unity for each m, and let $K_0 (\cong \mathbb{Q})$ be the prime subfield of K. Then, for every divisor d of m (including m itself), the cyclotomic polynomial Φ_d lies in $K_0[X]$.

- It is clear that $\Phi_1 = X - 1$ belongs to $K_0[X]$.

  Let $d (\neq 1)$ be a divisor of m, and suppose inductively that $\Phi_r \in K_0[X]$, for all proper divisors r of d.

  Then, if Δ_d is the set of all divisors of d,

  $$X^d - 1 = \left(\prod_{r \in \Delta_d \setminus \{d\}} \Phi_r \right) \Phi_d.$$

  It follows from the lemma that $\Phi_d \in K_0[X]$.

Example

- We consider Φ_{14}, and show that $\cos\frac{\pi}{7}+\cos\frac{3\pi}{7}+\cos\frac{5\pi}{7}=\frac{1}{2}$.
  Let $\omega=e^{\pi i/7}$. Then the primitive roots of $X^{14}-1$ are $\omega,\omega^3,\omega^5,\omega^9,\omega^{11},\omega^{13}$. So $\partial(\Phi_{14})=6$. We have

$$\begin{array}{rcl} X^{14}-1 & = & (X^7-1)(X^7+1) \\ & = & (X-1)(X^6+X^5+X^4+X^3+X^2+X+1) \\ & & \cdot(X+1)(X^6-X^5+X^4-X^3+X^2-X+1). \end{array}$$

  By the preceding example, the second factor is Φ_7. Hence, we get

$$\Phi_{14}=X^6-X^5+X^4-X^3+X^2-X+1.$$

  The primitive roots are conjugate in pairs. So Φ_{14} factorizes in $\mathbb{R}[X]$ as

$$\left(X^2-2X\cos\frac{\pi}{7}+1\right)\left(X^2-2X\cos\frac{3\pi}{7}+1\right)\left(X^2-2X\cos\frac{5\pi}{7}+1\right).$$

  Comparing the coefficients of X, gives the required identity.

Irreducibility of the Cyclotomic Polynomial

Theorem

For all $m \geq 1$, the cyclotomic polynomial Φ_m is irreducible over $\mathbb{Q}$.

- Suppose, for a contradiction, that Φ_m is not irreducible over $\mathbb{Q}$. We know that $\Phi_m \in \mathbb{Z}[X]$. By Gauss's Lemma, we may suppose that $\Phi_m = fg$, where $f, g \in \mathbb{Z}[X]$ and f is an irreducible monic polynomial such that $1 \leq \partial f < \partial \Phi_m$.

  Let K be a splitting field for Φ_m over $\mathbb{Q}$. At least one of the primitive m-th roots of unity ϵ in K must be a root of f. Now f is monic and irreducible and $f(\epsilon) = 0$. So f is the minimum polynomial of ϵ over $\mathbb{Q}$.

  If p is a prime, $p \nmid m$, then ϵ^p is also a primitive m-th root of unity.

  We show that ϵ^p is a root of f.

ϵ^p is a Root of f

- Suppose not. Then $g(\epsilon^p)=0$. Define $h(X)\in\mathbb{Z}[X]$ by $h(X)=g(X^p)$. Then $h(\epsilon)=g(\epsilon^p)=0$. But f is the minimum polynomial of ϵ over $\mathbb{Q}$. So $f\mid h$, i.e., $h=fu$, where $u\in\mathbb{Z}[X]$.

  Consider the map $n\mapsto\overline{n}$ from $\mathbb{Z}$ onto $\mathbb{Z}_p$, where $\overline{n}$ is the residue class $\{m\in\mathbb{Z}:m\equiv n \pmod{p}\}$. This map extends to a map $v\mapsto v^\dagger$ from $\mathbb{Z}[X]$ onto $\mathbb{Z}_p[X]$, in the obvious way:

  $$(a_0+a_1X+\cdots+a_nX^n)^\dagger=\overline{a}_0+\overline{a}_1X+\cdots+\overline{a}_nX^n.$$

  It is clear that $f^\dagger u^\dagger=h^\dagger$. Note in $\mathbb{Z}_p[X]$, $(ax+by)^p=a^px^p+b^py^p=ax^p+by^p$. So $[h(X)]^\dagger=[g(X^p)]^\dagger=[(g(X))^\dagger]^p$. Thus, $f^\dagger u^\dagger=(g^\dagger)^p$. Let $q^\dagger$ be an arbitrarily chosen irreducible factor of $f^\dagger$ in $\mathbb{Z}_p[X]$. Then $q^\dagger\mid(g^\dagger)^p$. So $q^\dagger\mid g^\dagger$. Thus, $q^\dagger$ divides both $f^\dagger$ and $g^\dagger$. Hence, $(q^\dagger)^2\mid\Phi_m^\dagger$. It follows that $\Phi_m^\dagger$ and hence also X^m-1, has a repeated root in a splitting field over $\mathbb{Z}_p$. By a previous theorem, this cannot happen, since p does not divide m. Thus, ϵ^p is a root of f.

Irreducibility of the Cyclotomic Polynomial (Conclusion)

- Let ζ be a root of f and η a root of g.

  Then both ζ and η are primitive m-th roots of unity.

  So $\eta = \zeta^r$, for some r, such that r and m are coprime.

  Let $r = p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are (not necessarily distinct) primes not dividing m.

  By what was proven in the preceding slide,

  $$\zeta^{p_1}, (\zeta^{p_1})^{p_2} = \zeta^{p_1 p_2}, \ldots, \zeta^{p_1 p_2 \cdots p_k} = \zeta^r$$

  are all roots of f.

  Thus η is a root of f as well as g.

  It follows that η is a repeated root of Φ_m.

  So η is also a repeated root of $X^m - 1$.

  This contradiction proves that Φ_m is irreducible.

The Galois group of $X^m - 1$

Theorem

Let K be a field of characteristic zero, and let L be a splitting field over K of the polynomial $X^m - 1$. Then $\mathrm{Gal}(L:K)$ is isomorphic to R_m, the multiplicative group of residue classes $\overline{r} \pmod{m}$, such that $(r,m) = 1$.

- Let ω be a primitive m-th root of unity in L. Let $\sigma \in \mathrm{Gal}(L:K)$. Then $L = K(\omega)$. We know that $\sigma(\omega)$ must also be a primitive m-th root of unity. So $\sigma \in \mathrm{Gal}(L:K)$ if and only if $\sigma(\omega) = \omega^{r_\sigma}$, where $(r_\sigma, m) = 1$. Now

  $$\omega^r = \omega^s \quad \text{if and only if} \quad r \equiv s \pmod{m}.$$

  So we have a one-to-one mapping

  $$\sigma \mapsto \overline{r}_\sigma$$

  from $\mathrm{Gal}(L:K)$ onto R_m, the multiplicative group of residue classes $\overline{r}$ mod m, such that $(r,m) = 1$.

The Galois group of $X^m - 1$ (Cont'd)

- We defined
$$\mathrm{Gal}(L:K) \to R_m; \quad \sigma \mapsto \overline{r}_\sigma.$$
Let $\sigma, \tau \in \mathrm{Gal}(L:K)$. Then
$$(\sigma\tau)(\omega) = \sigma(\omega^{r_\tau}) = (\omega^{r_\tau})^{r_\sigma} = \omega^{r_\sigma r_\tau} = (\omega^{r_\sigma})^{r_\tau} = (\tau\sigma)(\omega).$$
So $\mathrm{Gal}(L:K)$ is abelian.
The other consequence is that the map $\sigma \mapsto \overline{r}_\sigma$ is a homomorphism, since $\sigma\tau$ maps to $\overline{r}_\sigma \overline{r}_\tau$.
It is clear that the map is one-one.
The irreducibility of $X^m - 1$ gives that the map is also onto.

Consequence and Example

Corollary

Let K be a field of characteristic zero, and let L be a splitting field over K of the polynomial $X^p - 1$, where p is prime. Then $\text{Gal}(L:K)$ is cyclic.

- Suppose the exponent is prime. Then, the Galois group is isomorphic to the multiplicative group $\mathbb{Z}_p^*$ of non-zero integers modulo p. We know this is a cyclic group.

  Example: The splitting field in $\mathbb{C}$ of $X^8 - 1$ contains the primitive root $\omega = e^{\pi i/4}$. The Galois group has four elements

  $$\omega \mapsto \omega,\ \omega \mapsto \omega^3,\ \omega \mapsto \omega^5,\ \omega \mapsto \omega^7.$$

  It is isomorphic to $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, with multiplication table shown on the right.

$\times$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

Subsection 3

Cyclic Extensions

Cyclic Extensions

- Let K be a field of characteristic 0.
- Let $L:K$ be a field extension.
- We say that L is a **cyclic extension** of K if:
  - It is normal (and separable);
  - $\mathrm{Gal}(L:K)$ is a cyclic group.

  Example: By the preceding theorem, if p is prime, the splitting field over K of X^p-1 is a cyclic extension of K.

Norm and Trace

- Let K be a field of characteristic 0.
- Let L be an extension of K of finite degree n.
- Let N be a normal closure of L.
- By a previous theorem, there are exactly n distinct K-monomorphisms $\tau_1, \tau_2, \ldots, \tau_n$ from L into N.
- For each element x of L, we define the **norm** $\mathrm{N}_{L/K}(x)$ **of** x by
$$\mathrm{N}_{L/K}(x) = \prod_{i=1}^{n} \tau_i(x).$$
- For each element x of L, we define the **trace** $\mathrm{Tr}_{L/K}(x)$ **of** x by
$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \tau_i(x).$$

Properties of Norm and Trace

Theorem

The mapping $\mathrm{N}_{L/K}$ is a group homomorphism from $(L^*,\cdot)$ into $(K^*,\cdot)$. The mapping $\mathrm{Tr}_{L/K}$ is a non-zero group homomorphism from $(L,+)$ into $(K,+)$.

- It is clear that, for all x,y in L^*,

$$\begin{array}{rcl}\mathrm{N}_{L/K}(xy) & = & \prod_{i=1}^n \tau_i(xy) \\ & = & \prod_{i=1}^n \tau_i(x)\tau_i(y) \\ & = & (\prod_{i=1}^n \tau_i(x))(\prod_{i=1}^n \tau_i(y)) \\ & = & \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y).\end{array}$$

  Similarly, $\mathrm{Tr}_{L/K}(x+y)=\mathrm{Tr}_{L/K}(x)+\mathrm{Tr}_{L/K}(y)$.

  Thus, $\mathrm{N}_{L/K}$ and $\mathrm{Tr}_{L/K}$ are homomorphisms into $(L^*,\cdot)$ and $(L,+)$.

  It remains to show that the images are contained in K.

Properties of Norm and Trace (Cont'd)

- Let τ be a K-automorphism of N. Then $\tau\tau_1$, $\tau\tau_2$, ..., $\tau\tau_n$ are n distinct K-monomorphisms from L into N. So the list is simply the list $\tau_1, \tau_2, \ldots, \tau_n$ in a different order. Hence, for all x in L and all τ in $\mathrm{Gal}(N:K)$,

$$\tau(\mathrm{N}_{L/K}(x)) = \tau\left(\prod_{i=1}^{n}\tau_i(x)\right) = \prod_{i=1}^{n}\tau(\tau_i(x)) = \prod_{i=1}^{n}\tau_i(x) = \mathrm{N}_{L/K}(x).$$

  Similarly, $\tau(\mathrm{Tr}_{L/K}(x)) = \mathrm{Tr}_{L/K}(x)$.

  Hence, both $\mathrm{N}_{L/K}(x)$ and $\mathrm{Tr}_{L/K}(x)$ lie in $\Phi(\mathrm{Gal}(N:K)) = K$.

  It remains to show that $\mathrm{Tr}_{L/K}$ is not the zero homomorphism.

  Suppose, for all x in L, $\mathrm{Tr}_{L/K}(x) = \tau_1(x) + \tau_2(x) + \cdots + \tau_n(x) = 0$.

  It follows that the set $\{\tau_1, \tau_2, \ldots, \tau_n\}$ is linearly dependent over L.

  This contradicts a preceding result.

Hilbert's Theorem

Theorem (Hilbert)

Let L be a cyclic extension of a field K, and let τ be a generator of the (cyclic) group $\mathrm{Gal}(L:K)$. Suppose $x \in L$.

- $\mathrm{N}_{L/K}(x) = 1$ if and only if, there exists y in L, such that $x = \frac{y}{\tau(y)}$.
- $\mathrm{Tr}_{L/K}(x) = 0$ if and only if, there exists z in L, such that $x = z - \tau(z)$.

- Let $[L:K] = n$. Then $\tau^n = \iota$. Suppose that $x = \frac{y}{\tau(y)}$. Then

$$\mathrm{N}_{L/K}(x) = \iota(x)\tau(x)\cdots\tau^{n-1}(x) = \frac{y}{\tau(y)}\frac{\tau(y)}{\tau^2(y)}\frac{\tau^2(y)}{\tau^3(y)}\cdots\frac{\tau^{n-1}(y)}{\tau^n(y)} = 1.$$

  Conversely, suppose $\mathrm{N}_{L/K}(x) = 1$. Then $x^{-1} = \tau(x)\tau^2(x)\cdots\tau^{n-1}(x)$. The set $\{\iota, \tau, \tau^2, \ldots, \tau^{n-1}\}$ is linearly independent over L. So the map

$$\iota + x\tau + x\tau(x)\tau^2 + \cdots + x\tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}$$

  is non-zero.

Hilbert's Theorem (Cont'd)

- Thus, for some t in L, the element
$$y = t + x\tau(t) + x\tau(x)\tau^2(t) + \cdots + x\tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t) \neq 0.$$
Applying the automorphism τ gives
$$\begin{aligned}\tau(y) &= \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots \\ &\quad \cdots + \tau(x)\tau^2(x)\tau^3(x)\cdots\tau^{n-1}(x)\tau^n(t).\end{aligned}$$
Now note that
$$\begin{aligned}x^{-1}y &= x^{-1}t + \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots \\ &\quad \cdots + \tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t) \\ &= \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \cdots \\ &\quad \cdots + \tau(x)\tau^2(x)\cdots\tau^{n-2}(x)\tau^{n-1}(t) + x^{-1}\tau^n(t).\end{aligned}$$
Comparing the two equations, we get
$$\tau(y) = \tau(x)\tau^2(x)\cdots\tau^{n-1}(x)\tau^n(t) + x^{-1}y - x^{-1}\tau^n(t) = x^{-1}y.$$
The proof concerning $\mathrm{Tr}_{L/K}$ is similar.

The Intermediate Field $K(\omega)$

Theorem

Let $f = X^m - a \in K[X]$, where K is a field of characteristic 0. Let L be a splitting field of f over K.

- L contains an element ω, a primitive m-th root of unity.
- The group $\mathrm{Gal}(L : K(\omega))$ is cyclic, with order dividing m.
- $|\mathrm{Gal}(L : K(\omega))| = m$ if and only if f is irreducible over $K(\omega)$.

- Let K be a field of characteristic 0 and let $X^m - a \in K[X]$.

  Let L be a splitting field for $f = X^m - a$ over K.

  Then, f has distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_m$ in L.

  So L contains the distinct roots $\alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, \ldots, \alpha_m\alpha_1^{-1}$ of the polynomial $X^m - 1$.

  In particular, it contains a primitive m-th root of unity ω.

The Intermediate Field $K(\omega)$ (Cont'd)

- Suppose, without loss of generality, that $\alpha_2\alpha_1^{-1} = \omega$ is a primitive m-th root of unity.

  Then, in some order, the elements

  $$\alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, \ldots, \alpha_m\alpha_1^{-1}$$

  are $1, \omega, \ldots, \omega^{m-1}$.

  So we can re-label the roots of $X^m - a$ in L as

  $$\alpha_1, \omega\alpha_1, \ldots, \omega^{m-1}\alpha_1.$$

  Hence, over L,

  $$X^m - a = (X - \alpha_1)(X - \omega\alpha_1)\cdots(X - \omega^{m-1}\alpha_1).$$

  We have that $K \subseteq K(\omega) \subseteq L$.

  Moreover, the intermediate field $K(\omega)$ contains all the roots of unity.

The Intermediate Field $K(\omega)$ (Cont'd)

- We have seen that, if α is a root of f, then, over L,
$$f=(x-\alpha)(x-\omega\alpha)\cdots(x-\omega^{m-1}\alpha),$$
where ω is a primitive m-th root of unity. Thus $L=K(\omega,\alpha)$.
An automorphism σ in $\mathrm{Gal}(L:K(\omega))$ is determined by its action on α. The image must be a root of f. So $\sigma(\alpha)=\omega^{r_\sigma}\alpha$, for some r_σ in $\{0,1,\ldots,m-1\}$. For τ another element of $\mathrm{Gal}(L:K(\omega))$,
$$(\sigma\tau)(\alpha)=\sigma(\omega^{r_\tau}\alpha)=\omega^{r_\tau}\omega^{r_\sigma}\alpha=\omega^{r_\tau+r_\sigma}\alpha.$$
So $\sigma\mapsto\overline{r}_\sigma$ is a homomorphism onto the additive group $\mathbb{Z}_m$.
$\overline{r}_\sigma=\overline{0}$ if and only if m divides r_σ if and only if $\sigma(\alpha)=\alpha$.
The kernel of $\sigma\mapsto\overline{r}_\sigma$ is the identity in $\mathrm{Gal}(L:K(\omega))$.
So $\mathrm{Gal}(L:K(\omega))$ is isomorphic to a subgroup of the additive group $\mathbb{Z}_m$.
We may now deduce that the group is cyclic.

The Intermediate Field $K(\omega)$ (Conclusion)

- Suppose that $f = X^m - a$ is irreducible over $K(\omega)$. Then,
$$|\mathrm{Gal}(L:K(\omega))| = [L:K(\omega)] = \partial f = m.$$
So $\mathrm{Gal}(L:K(\omega)) \cong \mathbb{Z}_m$.
Conversely, suppose f is not irreducible over $K(\omega)$.
Then it has a monic irreducible proper factor g, with $\partial g < m$.
Let ρ be a root of g in L. Then
$$X^m - a = (X-\rho)(X-\omega\rho)\cdots(X-\omega^{m-1}\rho).$$
So $L = K(\omega,\rho)$ is a splitting field for f over $K(\omega)$. Hence,
$$|\mathrm{Gal}(L:K(\omega))| = [L:K(\omega)] = \partial g < m.$$
So $\mathrm{Gal}(L:K(\omega))$ is isomorphic to a proper subgroup of $\mathbb{Z}_m$.
- In the notation of the theorem, although the Galois groups $\mathrm{Gal}(K(\omega):K)$ and $\mathrm{Gal}(L:K(\omega))$ are both abelian, the group $\mathrm{Gal}(L:K)$ will usually be non-abelian.

Cyclic Extension of Degree m

Theorem

Let K be a field of characteristic zero, let m be a positive integer. Suppose that $X^m - 1$ splits completely over K. Let L be a cyclic extension of K such that $[L:K] = m$.

- There exists a in K, such that $X^m - a$ is irreducible over K and L is a splitting field for $X^m - a$.
- Moreover, L is generated over K by a single root of $X^m - a$.

- Let τ be a generator of the cyclic group $G = \mathrm{Gal}(L:K)$. Let ω be a primitive m-th root of unity in K. Every m-th root of unity is left fixed by every automorphism in G. Hence, $\mathrm{N}_{L/K}(\omega) = \omega^m = 1$. By Hilbert's Theorem, there exists z in L, such that $\omega = \frac{z}{\tau(z)}$. Hence, $\tau(z) = \omega^{-1} z$. So $\tau^k(z) = \omega^{-k} z \neq z$, $k = 1, 2, \ldots, m-1$. Thus, $\Gamma[K(z)] = \{\iota\}$. Now L, being cyclic, is normal. By the Fundamental Theorem, $K(z) = \Phi(\Gamma[K(z)]) = \Phi(\{\iota\}) = L$.

Cyclic Extension of Degree m (Cont'd)

- By $\tau(z) = \omega^{-1}z$, we get
$$\tau(z^m) = [\tau(z)]^m = \omega^{-m}z^m = z^m.$$
It immediately follows that $\tau^k(z^m) = z^m$, for $k = 0, 1, \ldots, m-1$.
Thus, $z^m \in \Phi(G) = K$. Denote z^m by a.
z is a root of the polynomial $X^m - a$ in $K[X]$.
So the minimum polynomial g of z over K is a factor of $X^m - a$.
But $[K(z) : K] = [L : K] = m$. So $g = X^m - a$.
It follows that $X^m - a$ is irreducible over K.
Moreover, the roots of $X^m - a$ are $\omega^{-k}z$ $k = 0, 1, \ldots, m-1$, all in L.
So L is a splitting field for $X^m - a$ over K.
- The theorem tells us that, provided the base field K has "enough" roots of unity, a cyclic extension of K is a radical extension.

Abel's Theorem

- Abel's Theorem helps us determine whether the polynomial $X^m - a$ is irreducible over $\mathbb{Q}(\omega)$ when m is prime.

Theorem (Abel's Theorem)

Let K be a field of characteristic 0, p be a prime and $a \in K$. If $X^p - a$ is reducible over K, then it has a linear factor $X - c$ in $K[X]$.

- Suppose that $f = X^p - a$ is reducible over K.

  Let $g \in K[X]$ be a monic irreducible factor of f of degree d.

  If $d = 1$, there is nothing to prove.

  Suppose that $1 < d < p$. Let L be a splitting field for f over K.

  Let β be a root of f in L. Then g factorizes in $L[X]$ as

$$g = (X - \omega^{n_1}\beta)(X - \omega^{n_2}\beta)\cdots(X - \omega^{n_d}\beta),$$

  where ω is a primitive p-th root of unity and $0 \le n_1 < n_2 < \cdots < n_d < p$.

Abel's Theorem (Cont'd)

- We have $g = (X - \omega^{n_1}\beta)(X - \omega^{n_2}\beta)\cdots(X - \omega^{n_d}\beta)$.
  Suppose that
  $$g = X^d - b_{d-1}X^{d-1} + \cdots + (-1)^d b_0.$$
  Comparing and setting $n = n_1 + \cdots + n_d$, we get
  $$b_0 = \omega^{n_1+n_2+\cdots+n_d}\beta^d = \omega^n \beta^d.$$
  Hence, since $\beta^p = a$,
  $$b_0^p = \omega^{np}\beta^{dp} = \beta^{dp} = a^d.$$
  Since p is prime, d and p have greatest common divisor 1.
  So there exist integers s and t, such that $sd + tp = 1$. Hence,
  $$a = a^{sd}a^{tp} = b_0^{sp}a^{tp} = (b_0^s a^t)^p.$$
  So $X - c$, where $c = b_0^s a^t \in K$, is a linear factor of f.

Example

- We determine the Galois group over $\mathbb{Q}$ of $X^5 - 7$.
  By the Eisenstein criterion, $X^5 - 7$ is irreducible over $\mathbb{Q}$.
  The primitive root $\omega = e^{2\pi i/5}$ has minimum polynomial $X^4 + X^3 + X^2 + X + 1$. So $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$.
  The polynomial $X^5 - 7$ is irreducible even over $\mathbb{Q}(\omega)$.
  If not, by Abel's Theorem, there exists b in $\mathbb{Q}(\omega)$, with $b = 7^{1/5}$.
  But $[\mathbb{Q}(b) : \mathbb{Q}] \leq [\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(7^{1/5}) : \mathbb{Q}] \geq 5$.
  So no such b can exist.
  The roots of $X^5 - 7$ in $\mathbb{C}$ are $v, v\omega, v\omega^2, v\omega^3, v\omega^4$, where $v = 7^{1/5}$ and $\omega = e^{2\pi i/5}$. The Galois group consists of elements $\sigma_{p,q}$ ($p = 0, 1, 2, 3, 4$, $q = 1, 2, 3, 4$), where

$$\begin{array}{rccl} \sigma_{p,q}: & v & \mapsto & v\omega^p, \\ & \omega & \mapsto & \omega^q. \end{array}$$

  The identity of the group is $\sigma_{0,1}$.

Example (Cont'd)

- Also,

$$\sigma_{p,q}\sigma_{r,s}(v) = \sigma_{p,q}(v\omega^r) = (v\omega^p)\omega^{qr} = v\omega^{p+qr};$$
$$\sigma_{p,q}\sigma_{r,s}(\omega) = \sigma_{p,q}(\omega^s) = \omega^{qs}.$$

So $\sigma_{p,q}\sigma_{r,s} = \sigma_{p+qr,qs}$, with addition and multiplication mod 5. If $p \in \{1,2,3,4,5\}$ and $q \in \{1,2,3,4\}$, then

$$\sigma_{1,1}^p = \sigma_{p,1}, \quad \sigma_{0,2}^q = \sigma_{0,2^q}, \quad \sigma_{p,1}\sigma_{0,2^q} = \sigma_{p,2^q}.$$

Hence, the Galois group is generated by $\beta = \sigma_{1,1}$ and $\gamma = \sigma_{0,2}$, where $\beta^5 = 1$, $\gamma^4 = 1$, and

$$\gamma\beta = \sigma_{0,2}\sigma_{1,1} = \sigma_{0+2\cdot 1,2\cdot 1} = \sigma_{2,2} = \sigma_{2+1\cdot 0,1\cdot 2} = \sigma_{2,1}\sigma_{0,2} = (\sigma_{1,1})^2\sigma_{0,2} = \beta^2\gamma.$$

The group, with presentation

$$\langle \beta,\gamma : \beta^5 = \gamma^4 = \beta^2\gamma\beta^{-1}\gamma^{-1} = 1\rangle$$

is of order 20.