Math 552: Abstract Algebra II

Wolmer V. Vasconcelos

Set 1

Spring 2009

Outline

- Pre-requisites: One previous algebra course, e.g. Math 551
- Textbook: See Syllabus
- webpage:www.math.rutgers.edu/(tilde)vasconce
- email : vasconce AT math.rutgers.edu
- Office hours [H228]: T 12:4, or by arrangement

General Syllabus

- Fields: Galois Theory
- Solving Algebraic Equations
- Finitely Generated Algebras
- Rings in Linear Algebra
- Chain Conditions
- Noetherian Rings
- Structure of Artinian Rings
- The X-Topic

Outline

Syllabus

Math 552 Course description. It follows the same organization as the current Math 551.

- Text: Jacobson, ”Basic Algebra”, Volumes 1 and 2, second edition. Note: These volumes are out of print. Students may be able to obtain used copies online (be sure it is the second edition) through addall.com or other websites. In the fall, photocopies will be available for purchase.
- Prerequisites: Any standard course in abstract algebra for undergraduates and/or Math 551.
- Topics: This is the continuation of Math 551, aimed at an exploration of many fundamental algebraic structures.

Topics

1. Galois Theory: Finite algebraic extensions, resolutions of equations by radicals (and without radicals).
2. Noetherian rings: Rings of polynomials, Hilbert basis theorem, Dedekind domains, Finitely generated algebras over fields, Noether normalization, Nullstellensatz.
3. Basic Module Theory: Projective and injective modules, resolutions, baby homological algebra, Hilbert syzygy theorem.
4. Artin Rings: Radical of a ring, semisimple rings, division rings, Artin-Wedderburn theorem.

Outline

Evariste Galois (1811-1832)

Galois Portraits

Evariste Galois

A drawing done in 1848 from memory by Evariste's brother

Fields

F: field

Keep in mind basic examples: $\mathbf{Q}$, $\mathbb{Z}_2$, $\mathbf{Q}(i)$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}(\mathbf{x})$, and 17 zillion others...

Fields: How to study them?

Two basic strategies:

- Look for relationships
- Enrich the environment with new structures

Let **F** be a field. Its nature is sometimes revealed when we attempt to enlarge it, or seek its subfields:

$$\mathbf{K} \subset \mathbf{F} \subset \mathbf{L}$$

We must treat ways to find **K**'s [Groups] and **L**'s [Equations], and mix them up [Galois Theory].

Definition

Let $\mathbf{K} \subset \mathbf{F}$ be fields. The degree of $\mathbf{F}$ over $\mathbf{K}$ is the vector space dimension $\dim_{\mathbf{K}} \mathbf{F}$. It is denoted

$$[\mathbf{F} : \mathbf{K}].$$

If $\mathbf{K} \subset \mathbf{F}$ are fields, we say that $\mathbf{F}$ is an **extension** of $\mathbf{K}$. More precisely, if $[\mathbf{F} : \mathbf{K}]$ is finite, we speak of a **finite extension**–otherwise we say the extension is **infinite.**

This is the vector space dimension: $[\mathbb{C} : \mathbb{R}] = 2$

- $u \in \mathbf{L}$: Algebraic/Transcendental?

$\mathbf{F}(u)$ is the smallest subfield of $\mathbf{L}$ containing $\mathbf{F}$ and u e.g. $\mathbb{Q}(\pi)$ or $\mathbb{C}(x)$, x an indeterminate or how about $\mathbb{Q}(\pi + \exp 1)$?

Like Lagrange...

Theorem

If $\mathbf{K} \subset \mathbf{F} \subset \mathbf{L}$ *is a tower of fields then*

$$[\mathbf{L} : \mathbf{K}] = [\mathbf{L} : \mathbf{F}] \cdot [\mathbf{F} : \mathbf{K}]$$

.

Reminds you of Lagrange's Theorem? Even same notation.

It will be enough to prove:

Lemma

If $\{u_i, i \in I\}, \{v_j, j \in J\}$ *are vector spaces bases of* $\mathbf{F}/\mathbf{K}$ *and* $\mathbf{L}/\mathbf{F}$*, then*

$$\{u_i v_j, i \in I, j \in J\}$$

is a basis of $\mathbf{L}/\mathbf{K}$*.*

Proof.

Note that every element of $\mathbf{L}$ is uniquely written (finite sum) $w = \sum_j b_j v_j, \quad b_j \in \mathbf{F}$. Expanding each b_j in the basis $\{u_i\}$, $b_j = \sum_i a_{ij} u_i, \quad a_{ij} \in \mathbf{K}$, and substituting

$$w = \sum_{ij} a_{ij} u_i v_j.$$

This shows the $u_i v_j$ span $\mathbf{L}$ over $\mathbf{K}$, while reversing the expansions show they are linearly independent. □

Suppose $[\mathbf{F} : \mathbf{K}] = n < \infty$

- Very few subspaces $\mathbf{K} \subset \mathbf{V} \subset \mathbf{F}$ can be fields
- If $u \in \mathbf{F}$ the elements

$$1, u, u^2, \ldots, u^n$$

must be linearly dependent

$$a_0 + a_1 u + \cdots + a_n u^n = 0,$$

$a_i \in \mathbf{K}$, some nonzero, that is, u is algebraic.

$\dim \mathbf{V_K} < \infty$

- If V is an integral domain then it is a field: If $0 \neq u \in \mathbf{V}$ pick lowest degree equation

  $$a_0 + a_1 u + \cdots + a_m u^m = 0, 0 \neq a_0,$$

  gives

  $$u^{-1} = -{a_0}^{-1}(a_1 + a_2 u + \cdots + a_m u^{m-1}) \in \mathbf{V}.$$

  Alternatively, $0 \neq u \in \mathbf{V}$ defines an injective linear transformation of a finite dimensional vector space

  $$v \in \mathbf{V} \mapsto u \cdot v \in \mathbf{V},$$

  which must be surjective, so for some $v_0 \in \mathbf{V}$, we must have $u \cdot v_0 = 1$.
- $\mathbf{K} \subset \mathbf{F}$ is an algebraic extension if every $u \in \mathbf{F}$ is algebraic over $\mathbf{K}$

Towers of Algebraic Extensions

Theorem

If $\mathbf{K} \subset \mathbf{F} \subset \mathbf{L}$ *is a tower of algebraic extensions then* $\mathbf{L}$ *is algebraic over* $\mathbf{K}$

Proof. Let $u \in \mathbf{L}$ be algebraic over $\mathbf{F}$:

$$u^n = \sum_{i=0}^{n-1} a_i u^i, \quad a_i \in \mathbf{F}$$

Each a_i is algebraic over $\mathbf{K}$ so we have equations of the form

$$a_i^{d_i} = \sum_{j=0}^{d_i-1} c_{ij} a_i^j, \quad c_{ij} \in \mathbf{K}$$

Let **V** be the **K**–subspace of **L** spanned by all ‘monomials’ in $u, a_0, a_1, \ldots, a_{n-1}$.

We make two claims about **V**:

• **V** is a ring: clear

• **V** is a finite dimensional vector space over **K**: just use the relations above to reduce number of required monomials

By a previous observation **V** is an algebraic extension. □

Algebraic Closure

Corollary

If $\mathbf{K} \subset \mathbf{F}$ is a field extension, the set of all elements of $\mathbf{F}$ which are algebraic over $\mathbf{K}$ is a field.

Proof. If u and v are elements of $\mathbf{F}$ which are algebraic over $\mathbf{K}$, then the set

$$\mathbf{V} = \mathbf{K}[u^i v^j]$$

is an integral domain which is a finite dimensional vector space over $\mathbf{K}$. □

Definition

The set of all elements of $\mathbf{F}$ which are algebraic over $\mathbf{K}$ is a field called the algebraic closure of $\mathbf{K}$ in $\mathbf{F}$.

Doing arithmetic in a field

The proof above hints at how to carry arithmetic in a field. Let us illustrate more. Suppose **F** is an extension of **K** and there is $u \in \mathbf{F}$ so that every other element v is a linear combination over **K** of powers of u. [Right off this implies that only a bounded number of powers are needed: why?] We can also frame this using a representation

$$\varphi : \mathbf{K}[x] \longrightarrow \mathbf{F}, \quad x \mapsto u$$

This is a surjective ring morphism so its kernel must be generated by an irreducible polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad n > 0 \quad a_i \in \mathbf{K}$$

As a consequence every element of **F** is represented by $g(u)$, for a unique polynomial $g(x)$ of degree $< n$. The addition $g(u) + h(u)$ is cheap, but the multiplication

$$g(u) \cdot h(u) = r(u),$$

may require long division [which is not always cheap]

$$g(x)h(x) = q(x)f(x) + r(x), \deg r(x) < \deg f(x)$$

Reciprocals also use long division: If $g(u) \neq 0$,

$$\gcd(f(x), g(x)) = 1,$$

so there is

$$a(x)g(x) + b(x)f(x) = 1, \quad \deg a(x) < n$$

$$(g(u))^{-1} = a(u)$$

Exercises

Exercise 1: How would you 'rationalize'

$$(\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7})^{-1}$$

Exercise 2: Let $\mathbf{K}$ be a field, x an indeterminate over it and $u = \frac{f(x)}{g(x)}$ a rational fraction with $\gcd(f(x), g(x)) = 1$. Then

$$[\mathbf{K}(x) : \mathbf{K}(u)] = \max\{\deg f(x), \deg g(x)\}.$$

x is a root of the polynomial (with coefficients in $\mathbf{K}(u)$)

$$f(T) - ug(T),$$

so the extension is finite. Show that this polynomial is irreducible.

Exercise 3: Is it possible to find a subfield $\mathbf{K} \subset \mathbb{R}$ with $[\mathbb{R} : \mathbf{K}] < \infty$?

Existence of roots

Theorem

If

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{K}[x]$$

is an irreducible polynomial there is an extension **F** *of* **K** *with a root of it.*

Proof. Set $\mathbf{F} = \mathbf{K}[t]/(f(t))$, t some fresh indeterminate. Set u for the residue class of t. The elements of **F** are $g(u)$, $\deg g(x) < n$. Note $f(u) = 0$. □

Remarks

- If $[\mathbf{F} : \mathbf{K}]$ is prime, there are no intermediate extensions
- If $\mathbf{F} = \mathbb{Q}(\sqrt[3]{5})$, $[\mathbf{F} : \mathbb{Q}] = 3$ and $\mathbb{Q}(\sqrt[3]{5}) = \mathbb{Q}(\sqrt[3]{25})$
- Usually difficult to find the degree of a finite extension. Very hard to decide whether an extension is algebraic. For example, consider $\mathbb{R}$ over $\mathbb{Q}$: The algebraic real numbers are roots of the irreducible polynomials of $\mathbb{Q}[x]$, which can be ‘listed’ along with their roots, in particular they are countable. Thus almost all real numbers are **transcendental.**

Outline

Ruler and Compass Constructions

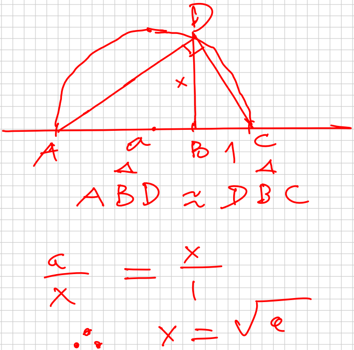
The set of all complex numbers that are algebraic over $\mathbb{Q}$ are called the **algebraic numbers**: $\overline{\mathbb{Q}}$. Since $\mathbb{C}$ is **algebraically closed**, $\overline{\mathbb{Q}}$ is the **algebraic closure** of $\mathbb{Q}$.

$\overline{\mathbb{Q}}$ has many interesting subfields (and subrings). One of these is the set **L** of the coordinates of all points in the plane obtained from any **construction** with ruler and compass. These numbers are said to be **constructible**.

Theorem

Let $\mathbf{L}$ *be a field. That is if* $c, d \in \mathbf{L}$, *then* $c \pm d, cd \in \mathbf{L}$ *and if* $0 \neq d$, $c/d \in \mathbf{L}$. *Moreover* $\sqrt{c} \in \mathbf{L}$.

Square roots



The Delphic Problems

What is a constructible algebraic number?

1. Trisection of the Angle: Trisect, say, the angle of 60°
2. Duplication of the Unit Cube: Construct $\sqrt[3]{2}$
3. Quadrature of the Unit Circle: Construct π

Constructability Criterion

Theorem

If c is a constructible number then

$$[\mathbb{Q}(c) : \mathbb{Q}] = 2^n.$$

- If two lines $a_1 x + b_1 y = c_1$ and $a_2 x + b_2 y = c_2$ have coefficients in the field **K**, their intersection [if there is one] (x, y) have $x, y \in \mathbf{K}$.
- If the line $ax + by = c$ and the circle $(x - x_0)^2 + (y - y_0)^2 = r^2$ have coefficients in the field **K**, their intersection [if there is one] (x, y) have $x, y \in \mathbf{K}(\sqrt{c})$, $c \in \mathbf{K}$.
- If the circles $(x - x_1)^2 + (y - y_1)^2 = r_1^2$ and $(x - x_2)^2 + (y - y_2)^2 = r_2^2$ have coefficients in the field **K**, their intersection [if there is one] (x, y) have $x, y \in \mathbf{K}(\sqrt{c})$, $c \in \mathbf{K}$.

There is a converse, which we will see when we discuss Galois Theory.

• **Duplication of the Cube:** $z = \sqrt[3]{2}$ is not constructible since the polynomial $x^3 - 2$ is irreducible by Eisenstein's.

• **Trisection of the Angle:** Let $z = \cos 20^\circ$. Finding z amounts to trisecting 60°.

From the trigonometric formula,

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$$

we have the equation of z

$$8z^3 - 6z - 1 = 0, \quad \text{or} \quad x^3 - 3x - 1 = 0, \quad x = z/2.$$

This is an irreducible polynomial since any rational root had to be ± 1, which is not the case.

Regular Polygons

Let $n \geq 3$. Which n-regular polygons can be constructed with ruler and compass? That is, which complex number z, with

$$z^n = 1 \quad z^i \neq 1, \quad i < n$$

can be constructed?

According to the theorem, the minimal polynomial of such z must satisfy

$$[\mathbf{Q}(z) : \mathbf{Q}] = 2^r.$$

Theorem (Gauss)

z is constructible if and only if $n = 2^m p_1 \cdots p_s$, where p_i are Fermat primes, that is, $p = 2^{2^r} + 1$ for some r.

Proof

The minimal polynomials of elements such as $\epsilon = e^{2\pi i/n}$ are called cyclotomic polynomial $q_n(x)$. If $n = p$ prime,

$$q_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Since $\{z \in \mathbb{C} : z^n = 1\}$ is a cyclic group of order n, its generators are $P_n = \{\epsilon^i : \gcd(i, n) = 1\}$. If $n = p_1^{r_1} \cdots p_s^{r_s}$, the cardinality of P_n is given by the value of the Möbius function,

$$\psi(n) = \prod_1^s (p_i^{r_i} - p^{r_i - 1}).$$

Similarly, we can collect for each $d|n$, the set P_d of roots of order d.

The assertion of the theorem follows from the fact that

$$\begin{aligned} \psi(n) &= 2^c \Rightarrow \\ n &= 2^m p_1 \cdots p_r, \quad p_i = 2^{s_i} + 1, \end{aligned}$$

and as p_i is prime, $s_i = 2^{m_i}$.

Remark about cyclotomic polynomial

Proposition

For each natural number n,

$$q_n(x) = \prod_{\sigma \in P_n} (x - \sigma)$$

is an irreducible polynomial of $\mathbf{Q}[x]$.

Proof. We prove this by induction on n. Note that $q_1(x) = x - 1$, $q_2(x) = x + 1$, $q_3(x) = x^2 + x + 1$. From

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

it follows (by induction) the product of the $q_d(x)$, $d < n$, is a monic polynomial of $\mathbf{Q}[x]$. $q_n(x)$ being a quotient of two monic polynomials of $\mathbf{Q}[x]$, by long division $q_n(x) \in \mathbf{Q}[x]$.

To prove that $q_n(x)$ is irreducible over $\mathbb{Q}$, since it is a monic polynomial of $\mathbb{Z}[x]$, ETS that it is irreducible over $\mathbb{Z}$.

The case $n = p$ prime,

$$q_p(x) \;=\; \frac{x^p - 1}{x - 1}$$

so that by changing variables, $x = t + 1$

$$q_p(t+1) \;=\; \frac{(t+1)^p - 1}{t} = t^{p-1} + pt^{p-2} + \cdots + p,$$

where are the other coeficients, $\binom{p}{i}$, are divisible by p. Applying Eisenstein's, it follows that $q_p(x)$ is irreducible.
We send you to look up the proof in your favorite source for factorization.

Outline

Galois Theory

Let $\mathbf{F}, \mathbf{L}$ be two extensions of $\mathbf{K}$. The structure we are going to examine are the $\mathbf{K}$–morphisms

$$\varphi : \mathbf{F} \longrightarrow \mathbf{L}$$

Of interest is when φ is an isomorphism and of particular interest is when further $\mathbf{F} = \mathbf{L}$: The set of all φ form a group, the **Galois group of F over K.** It is written as $\mathbf{Aut_K}(\mathbf{F})$ or $\mathbf{Gal_K}(\mathbf{F})$. Galois Theory is the study of the relationships between $\mathbf{Gal_K}(\mathbf{F})$ and the set of intermediate subextensions of $\mathbf{F}/\mathbf{K}$.

Building Field Isomorphisms

It is rooted [sorry for the joke] on the following observation: Let

$$\varphi : \mathbf{F} \to \mathbf{L}$$

be a field isomorphism and let $f(x) = \sum_i a_i x^i$ be a polynomial with coefficients in **F**. If $\alpha \in \mathbf{F}$ is a root of $f(x)$ then $\varphi(\alpha)$ is a root of the polynomial $\sum_i \varphi(a_i) x^i$.

Suppose $f(x)$ is an irreducible polynomial over the field **F** and α and β are roots of $f(x)$ in two field extensions $\mathbf{L}_1$ and $\mathbf{L}_2$. (Contrary to popular belief, a polynomial of degree n may have lots of roots–what is not allowed is more than n roots in a same field.) We then have an isomorphism

$$\varphi : \mathbf{F}(\alpha) \to \mathbf{F}(\beta), \quad \varphi(\alpha) = \beta.$$

This is because both extensions are isomorphic to

$$\mathbf{F}[x]/(f(x))$$

Galois Correspondence

Let $\mathbf{F}/\mathbf{K}$ be a field extension of Galois group $G = \mathrm{Gal}_{\mathbf{K}}(\mathbf{F})$.

1. If H is a subgroup of G the elements

$$H' = \{r \in \mathbf{F} \mid \sigma(r) = r \quad \forall \sigma \in H\}$$

   is a subextension

$$\mathbf{K} \subset H' \subset \mathbf{F}$$

2. Conversely, if $\mathbf{L}$ is an intermediate subextension of $\mathbf{F}/\mathbf{K}$, the elements

$$L' = \{\sigma \in G \mid \sigma(s) = s \quad \forall s \in \mathbf{L}\}$$

   is a subgroup of G.

These 'priming' operations are called 'Galois correspondence'.

Properties

$$
\begin{aligned}
1' &= \mathbf{F} \\
\mathbf{F}' &= 1 \\
\mathbf{K}' &= G \\
G' &= ? \\
H &< J \Rightarrow J' \subset H' \\
L &\subset M \Rightarrow M' < L' \\
H &< H'' \quad ?= \\
L &\subset L'' \quad ?=
\end{aligned}
$$

To clarify ?:

Galois Extension

Definition

$\mathbf{L}/\mathbf{K}$ is a *Galois extension* if

$$G' = \mathbf{K}.$$

If $H = H''$, we say that H is a closed subgroup. Similarly, if $L = L''$, L is a closed extension. (Observe that 'priming' is order-reversing.)

What is this all about?

Big Theorem

Theorem

If **F** *is a finite dimensional Galois extension of* **K**, *priming gives a one-one correspondence. More precisely:*

1. $[H : J] = [J' : H']$ *and* $[M : L] = [L' : M']$, *in particular* $|G| = [\mathbf{F} : \mathbf{K}]$.
2. **F** *is Galois over any intermediate extension* E *of Galois group* E', *but* E *is Galois over* **K** *iff* E' *is normal; in this case* $G/E' = \mathrm{Gal}_{\mathbf{K}}(E)$.

How good is this? It already tells us many things, but it would be better if we *knew* what are Galois extensions! (Meaning: How they occur.) We will come to this soon, let us get started with the proof. It can be organized as two technical lemmas.

Lemma 1

Lemma

Let $\mathbf{F}/\mathbf{K}$ be a field extension and $L \subset M$ be intermediate fields. If $M : L$ is finite, then

$$[L' : M'] \leq [M : L].$$

In particular, if $[\mathbf{F} : \mathbf{K}] < \infty$ then $|\mathrm{Gal}_{\mathbf{K}}(\mathbf{F})| \leq [\mathbf{F} : \mathbf{K}]$.

Proof. Set $n = [M : L]$ (will argue by induction, ok if $n = 1$.) If $L \subset N \subset M$ are distinct subextensions, we make use of

$$[M : L] \quad = \quad [M : N] \cdot [N : L]$$

$$[L' : M'] \quad = \quad [N' : M'] \cdot [L' : N']$$

We may assume that $M = L(u)$, where u the root of a polynomial $f(x)$ of degree n. Note that if $\sigma M'$ is a coset of L', for any of its elements $\sigma\alpha$,

$$\sigma\alpha(u) = \sigma(u).$$

Since $\sigma(u)$ is a root of $f(x)$ (in $\mathbf{F}$), we have at most n values for it. In particular, if $\sigma_1(u) = \sigma_2(u)$, $\sigma_1, \sigma_2 \in L'$, then they lie in the same coset relative to M'.

Lemma 2

Lemma

Let $\mathbf{F}/\mathbf{K}$ *be a field extension and* $H < J$ *be subgroups of* $\mathrm{Gal}_{\mathbf{K}}(\mathbf{F})$*. If* $[J : H]$ *is finite, then*

$$[H' : J'] \leq [J : H].$$

Proof. Set $[J : H] = n$ and assume $[H' : J'] > n$. Let $u_1, \ldots, u_{n+1} \in H'$ be linearly independent over J'. Let $\tau_1, \ldots, \tau_n \in J$ be a complete set of representatives of cosets of H in J. Consider the system of n homogeneous linear equations in $n + 1$ unknowns (in $\mathbf{F}$):

$$\begin{aligned}
\tau_1(u_1)x_1 + \tau_1(u_2)x_2 + \cdots + \tau_1(u_{n+1})x_{n+1} &= 0\\
\tau_2(u_1)x_1 + \tau_2(u_2)x_2 + \cdots + \tau_2(u_{n+1})x_{n+1} &= 0\\
&\vdots\\
\tau_n(u_1)x_1 + \tau_n(u_2)x_2 + \cdots + \tau_n(u_{n+1})x_{n+1} &= 0
\end{aligned}$$

There exists in **F** a nonzero solution. Among all such pick one with as many zeros as possible; change the notation (order of the τ_i) so that this solution has the form

$$(a_1, \ldots, a_r, 0, \ldots, 0), \quad a_i \neq 0 \quad a_1 = 1.$$

If all $a_i \in H'$, since one of the coset representatives $\tau_i \in J$, we would have a nontrivial linear relation among the u_i with coefficients in H' (when the u_i are linearly independent over H'). Say then $a_2 \notin H'$ and so for some $\tau = \tau_j$, $\tau_j(a_2) \neq a_2$. Apply τ to the system of equations and note that $\tau\tau_1, \ldots, \tau\tau_n$ is just a permutation of the cosets and the new equations are a permutation of the old equations and thus

$$(1, \tau(a_2), \ldots, \tau(a_r), 0, \ldots, 0)$$

is also a solution. Subtracting we get a 'shorter' nontrivial solution, contradiction. □

Proof of the Theorem

1. $[H : J] = [J' : H']$ and $[M : L] = [L' : M']$, in particular $|G| = [\mathbf{F} : \mathbf{K}]$.
2. **F** is Galois over any intermediate extension E of Galois group E', but E is Galois over **K** iff E' is normal; in this case $G/E' = \mathrm{Gal}_{\mathbf{K}}(E)$.

Proof. Let $\mathbf{K} \subset L \subset \mathbf{F}$ be an intermediate extension. By the first and then by the second lemma,

$$[L : \mathbf{K}] \geq [\mathbf{K}' : L'] \geq [L'' : \mathbf{K}'']$$

Since $\mathbf{F}/\mathbf{K}$ is a Galois extension, $\mathbf{K} = \mathbf{K}''$. As $L \subset L''$, the inequality of the degrees forces $L = L''$–thus every intermediate extension is closed.

We also have $[\mathbf{F} : \mathbf{K}] \geq [\mathbf{K}' : \mathbf{F}'] = [G : 1]$, so G is a finite group and we can now use the second lemma followed by the first to get $H = H''$, that is, every subgroup is closed.

Note that

$$E' = \mathrm{Gal}_E(\mathbf{F})$$

The second assertion follows since $E'' = E$ for every subextension: so $\mathbf{F}$ is Galois over E.
For the final assertion, we need a new notion, that of a *stable* subextension $\mathbf{K} \subset E \subset \mathbf{F}$: If $\sigma \in G = \mathrm{Gal}_{\mathbf{K}}(\mathbf{F})$, then $\sigma(E) \subset E$.
This means that if E is stable, the restriction is well defined and therefore we get a group homomorphism (and therefore E' is a normal subgroup)

$$E' \triangleleft G = \mathrm{Gal}_{\mathbf{K}}(\mathbf{F}) \to H = \mathrm{Gal}_{\mathbf{K}}(E).$$

Also

$$[G : E'] \leq [H : 1] \leq [E : \mathbf{K}] = [\mathbf{K}' : E'] = [G' : E'],$$

and we have actually have a surjective isomorphism. Thus $E/\mathbf{K}$ is a Galois extension.

Conversely: $E' \triangleleft G$ means that if $\sigma \in G$, $\alpha \in H$ for $v \in E$

$$\sigma^{-1}\alpha\sigma(v) = v,$$

and thus

$$\alpha(\sigma(v)) = \sigma(v) \quad \forall \alpha \in H$$

and

$$\alpha(v) \in E$$

and thus E is stable. □

Outline

Assignment #1

- (Just warm-up, don't hand in.) Let $k \subset F$ be a field extension. Show that if $u \in F$ is algebraic of odd degree over k, then so is u^2 and $k(u) = k(u^2)$.
- Let F be the extension of $\mathbb{Q}$ obtained by adjoining $u = \sqrt{2}$ and $\sqrt{5}$, $F = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$. What is $[F : \mathbb{Q}]$ and what is the inverse of $1 + \sqrt{2} + \sqrt{5}$ (rationalized)?
- Let $\mathbf{K}$ be a field and let x be an indeterminate over $\mathbf{K}$. Describe $\mathrm{Gal}_{\mathbf{K}}(\mathbf{K}(x))$.
- (Challenge to class: show in class if someone succeeds.) Find a method (by any method) to join any two points in a plane using exclusively a *short* ruler. (Say the two points are further away than the length of the ruler.)

Outline

Last Class ... and Today

Let $\mathbf{L}/\mathbf{K}$ be a field extension and the group $\mathbf{G} = \mathrm{Gal}_{\mathbf{K}}(\mathbf{L})$ of $\mathbf{K}$-automorphisms of $\mathbf{L}$ (called the Galois group of $\mathbf{L}/\mathbf{K}$).

We consider the relationship between the subextensions $\mathbf{K} \subset \mathbf{F} \subset \mathbf{L}$ and subgroups $H \subset \mathbf{G}$:

$$\begin{aligned} \mathbf{F} &\longrightarrow \mathbf{F}' = \{s \in \mathbf{G} : s(x) = x, \quad \forall x \in \mathbf{F}\} \\ H &\longrightarrow H' = \{x \in \mathbf{L} : s(x) = x, \quad s \in H\} \end{aligned}$$

The key technical facts about this operation (priming) are:

- If $\mathbf{F}_1 \subset \mathbf{F}_2$ is finite, $[\mathbf{F}_1' : \mathbf{F}_2'] \leq [\mathbf{F}_2 : \mathbf{F}_1]$
- If $H_1 \subset H_2$ are subgroups and $[H_2 : H_1]$ is finite, then $[H_1' : H_2'] \leq [H_2 : H_1]$

Galois Extension

Definition

$\mathbf{L}/\mathbf{K}$ is a *Galois extension* if

$$\mathbf{G}' = \mathbf{K}.$$

This means: If $x \in \mathbf{L} \setminus \mathbf{K}$, there is $s \in \mathbf{G}$ such that $s(x) \neq x$.

If $\mathbf{L}$ is (finite) Galois over $\mathbf{K}$, lots of things happen:

- Priming is involutive in both directions, $H'' = H$ and $\mathbf{F}'' = \mathbf{F}$. In particular $\mathbf{L}$ is Galois over $\mathbf{F}$.
- $\mathbf{F}$ however is only Galois over $\mathbf{K}$ if $\mathbf{F}'$ is (iff) a normal subgroup of $\mathbf{G}$.
- $\mathbf{L}$ is Galois over $\mathbf{K}$ iff $|\mathbf{G}| = [\mathbf{L} : \mathbf{K}]$

Proving an extension is Galois

Let **L** be a finite extension of **K**, of Galois group **G**. To check **L** is Galois over **K**:

- It is obviously difficult to apply the definition: for $u \in \mathbf{L} \setminus \mathbf{K}$ find $s \in \mathbf{G}$ such that $s(u) \neq u$.
- Instead, given u we try to build s in stages: first find an intermediate extension $\mathbf{K} \subset \mathbf{K}(u)$ and a homomorphism

$$s_1 \quad : \quad \mathbf{K}(u) \longrightarrow \mathbf{L}, \quad s_1(u) \neq u$$

- Extend s_1 to a homomorphism $s : \mathbf{L} \longrightarrow \mathbf{L}$

Recognizing a Galois Extension

1. $\mathbf{F}/\mathbf{K}$ is Galois iff $|\mathrm{Gal}_{\mathbf{K}}(\mathbf{F})| = [\mathbf{F} : \mathbf{K}]$
2. If $\mathbf{F}/\mathbf{K}$ is Galois and $u \in \mathbf{F}$ with (monic) minimal polynomial $f(x)$, then all the roots of $f(x)$ are distinct and lie in $\mathbf{F}$: If $\sigma \in G = \mathrm{Gal}_{\mathbf{K}}(\mathbf{F})$ then $\sigma(u)$ is also a root of $f(x)$. Let $u_1, \ldots, u_n$ be these distinct images of u and consider the polynomial with coefficients in $\mathbf{F}$

$$g(x) = (x - u_1)(x - u_2)\cdots(x - u_n).$$

   Note that any $\sigma \in G$ acting on the coefficients of $g(x)$ leaves them fixed–and therefore they all lie in $\mathbf{K}$. Thus $g(x) \mid f(x)$ and $g(x) = f(x)$.
3. If $\mathbf{F}/\mathbf{K}$ is Galois then there is a polynomial $f(x) \in \mathbf{K}[x]$ whose roots $u_1, \ldots, u_n$ in some extension field of $\mathbf{K}$ are distinct and $\mathbf{F} = \mathbf{K}[u_1, \ldots, u_n]$.

Outline

Splitting Fields & Separable Extensions

What are Galois extensions really like?

Definition

Let **K** be a field and let $\mathbf{f}(x)$ be a (monic) polynomial over **K**. A splitting field of $\mathbf{f}(x)$ is a minimal extension **F** of **K** in which $\mathbf{f}(x)$ decomposes completely

$$\mathbf{f}(x) = (x - u_1)(x - u_2) \cdots (x - u_n), \quad u_i \in \mathbf{F}.$$

Minimal means that the u_i generate **F**:

$$\mathbf{F} = \mathbf{K}[u_1, \ldots, u_n]$$

Note that there may be several.

Theorem

Splitting fields of polynomials over a field exist and are unique up to isomorphism.

Proof.

- Given a field $\mathbf{K}$ and polynomial $\mathbf{f}(x)$, we have already described how to find a root for $\mathbf{f}(x)$: If $\mathbf{g}(x)$ is an irreducible factor of $\mathbf{f}(x)$ over $\mathbf{K}$, in $\mathbf{F} = \mathbf{K}[t]/(\mathbf{g}(t))$, u the residue class of t is a root of $\mathbf{g}(x)$, $\mathbf{g}(u) = 0$, and therefore of $\mathbf{f}(x)$.
- $\mathbf{f}(x) = (x - u)\mathbf{h}(x)$.
- We go on until all irreducible factors of $\mathbf{f}(x)$ (in the new fields) have degree 1. If we ensure not to add anything extra, we get a splitting field.

This can be more controlled as follows.

Suppose $\mathbf{L}$ is another splitting field. Let $\mathbf{g}(x)$ be an irreducible factor of $\mathbf{f}(x)$ in $\mathbf{K}[x]$.
Let u_1 (resp. v_1) be a root of $\mathbf{g}(x)$ in $\mathbf{F}$ (resp. in $\mathbf{L}$). We have isomorphisms

$$\mathbf{F} \supset \mathbf{K}[u_1] \simeq \mathbf{K}[x]/(\mathbf{g}(x)) \simeq \mathbf{K}[v_1] \subset \mathbf{L}$$

which we aim to extend $\mathbf{K}[u_1] \overset{\sigma}{\simeq} \mathbf{K}[v_1]$ to an isomorphism $\mathbf{L} \simeq \mathbf{F}$.

Let $\mathbf{h}(x)$ be an irreducible factor of $\mathbf{g}(x)$ over $\mathbf{K}[u_1]$. Applying σ to $\mathbf{h}(x)$ gives an irreducible factor of $\mathbf{g}(x)$ over $\mathbf{K}[v_1]$.

Iterating leads to the isomorphism of the towers:

$$\begin{array}{rcl} \mathbf{K} & \simeq & \mathbf{K} \\ \mathbf{K}[u_1] & \simeq & \mathbf{K}[v_1] \\ \mathbf{K}[u_1, u_2] & \simeq & \mathbf{K}[v_1, v_2] \\ & \vdots & \\ \mathbf{K}[u_1, \ldots, u_n] & \simeq & \mathbf{K}[v_1, \ldots, v_n] \\ \mathbf{F} & \simeq & \mathbf{L} \end{array}$$

Separable Polynomial

Let $\mathbf{k} = \mathbb{Z}/(p)$, let x, y be indeterminates over $\mathbf{k}$ and set

$$\mathbf{K} = \mathbf{k}(x^p, y^p) \subset \mathbf{k}(x, y) = \mathbf{F}$$

Then $[\mathbf{F} : \mathbf{K}] = p^2$ and $t^p - x^p \in \mathbf{K}[t]$ is an irreducible polynomial with a root $u = x$ of multiplicity p.

If $\mathbf{g}(x) \in \mathbf{K}[x]$ is a polynomial with a double root u in an extension $\mathbf{K} \subset \mathbf{F}$,

$$\mathbf{g}(x) = (x - u)^2 \mathbf{h}(x)$$

Thus u is a root of $\mathbf{g}(x)$ and $\mathbf{g}'(x)$.

Separable Extension

Definition

A polynomial $\mathbf{f}(x) \in \mathbf{K}[x]$ is separable if it does not have multiple roots. An extension $\mathbf{K} \subset \mathbf{F}$ is separable if for all $u \in \mathbf{F}$ its minimal polynomial is separable.

Characterization of Galois Extensions

Theorem

Let $\mathbf{K} \subset \mathbf{F}$ *be a finite extension. The following conditions are equivalent:*

1. $\mathbf{F}$ *is a Galois extension of* $\mathbf{K}$*.*
2. $\mathbf{F}$ *is separable over* $\mathbf{K}$ *and a splitting field over* $\mathbf{K}$*.*
3. $\mathbf{F}$ *is the splitting field of a separable polynomial over* $\mathbf{K}$*.*

Proof(s)

- **F** Galois over **K** $\Rightarrow$ **F** separable over **K** and a splitting field.

Let $G = \mathrm{Gal}_{\mathbf{K}}(\mathbf{F})$. For $u \in \mathbf{F}$, let $\{\sigma_1(u), \ldots, \sigma_r(u)\}$ be the distinct images of u under the action of G. Set

$$\begin{aligned}\mathbf{g}(x) &= (x - \sigma_1(u)) \cdots (x - \sigma_r(u)) \\ &= x^r - (\sigma_1(u) + \cdots + \sigma_r(u))x^{r-1} + \cdots \\ &+ (-1)^r(\sigma_1(u) \cdots \sigma_r(u))\end{aligned}$$

This polynomial is invariant under G: $\sigma(\mathbf{g}(x)) = \mathbf{g}(x)$. Thus its coefficients lie in **K** (Galois hypothesis). This proves that every element of **F** satisfies a polynomial equation with distinct roots, all lying in **F**.

• **F** is the splitting field of a separable polynomial over **K** $\Rightarrow$ **F** is Galois over **K**.

Let $\mathbf{F} = \mathbf{K}[u_1, \ldots, u_r]$, $\mathbf{f}_i(x)$ minimal polynomial of u_i, separable. Let $\mathbf{f}(x) = \mathbf{f}_1(x) \cdots \mathbf{f}_r(x)$.

Will show that

$$|\mathrm{Gal}_{\mathbf{K}}(\mathbf{F})| = [\mathbf{F} : \mathbf{K}],$$

which is enough to assure that **F** is Galois over **K**.

If $\mathbf{f}(x)$ factors completely over $\mathbf{K}$, $\mathbf{F} = \mathbf{K}$, and we are done.

Let $\mathbf{g}(x)$ be an irreducible factor of $\mathbf{f}(x)$, with $\deg \mathbf{g}(x) = r \geq 2$. Let u be a root of $\mathbf{g}(x)$ in $\mathbf{F}$ and set $\mathbf{L} = \mathbf{K}[u]$, $[\mathbf{L} : \mathbf{K}] = r$.

Let $H = \mathbf{L}' \subset G = \mathrm{Gal}_{\mathbf{K}}(\mathbf{F})$. Note that $[G : H]$ is the number of images of u under automorphisms of $\mathbf{F}/\mathbf{K}$. But every one of the r distinct roots of $\mathbf{g}(x)$ is such an image by our discussion of splitting fields on how to building its automorphisms.

We have then

$$[G : H] = r = [\mathbf{L} : \mathbf{K}]$$

Since $H = \mathrm{Gal}_{\mathbf{L}}(\mathbf{F})$, by induction we have that $|H| = [\mathbf{F} : \mathbf{L}]$.
Finally, by Lagrange's we have

$$|G| = [G : H] \cdot |H| = [\mathbf{F} : \mathbf{L}] \cdot [\mathbf{L} : \mathbf{K}] = [\mathbf{F} : \mathbf{K}].$$

$\mathbb{C}$ is algebraically closed

Theorem

$\mathbb{C}$ is algebraically closed.

Proof. Let u be an element algebraic over $\mathbb{C}$; u is also algebraic over $\mathbb{R}$. Let $\mathbf{f}(x)$ be its minimal polynomial over $\mathbb{R}$ and let $\mathbf{F}$ be a splitting field

$$\mathbb{R} \subset \mathbb{C} \subset \mathbf{F}.$$

We are going to argue that $\mathbf{f}$ is a quadratic polynomial. It will suffice to prove the theorem.

F is Galois over $\mathbb{R}$. Let $G = \mathrm{Gal}_{\mathbb{R}}(\mathbf{F})$ and denote by H its 2-Sylow subgroup.

$$\begin{array}{rcl} \mathbf{F} & \leftrightarrow & 1 \\ H' & \leftrightarrow & H \\ \mathbb{R} & \leftrightarrow & G \end{array}$$

Recall:

- $[\mathbf{F} : H'] = [H : 1] = 2^n$
- $[H' : \mathbb{R}]$ is odd

- $\mathbb{R}$ has no extension of degree odd (by the intermediate value theorem of Calculus).
- Thus $G = H$, $|G| = 2^n$. Since G is solvable, there exists a tower of subgroups

$$(1) \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_n = G,$$

$$[H_i : H_{i-1}] = 2$$

and a corresponding tower of quadratic extensions

$$\mathbb{R} \subset \mathbf{F}_1 \subset \cdots \subset \mathbf{F}_n = \mathbf{F},$$

and therefore $n = 1$, that is $\mathbf{F} \simeq \mathbb{C}$.

Outline

Assignment #2

1. (Hand in) If $c \in \mathbb{C}$ and $[\mathbb{Q}(c) : \mathbb{Q}] = 2^r$, prove that c can be constructed with ruler and compass. [This is a bit of reverse engineering.] (You may have to assume more, like what?)
2. (Done in classs) Determine the Galois group of $\mathbb{R}$ over $\mathbb{Q}$.
3. (For thinking) Guess what is the Galois group of all the constructible numbers is.

Outline

Finite Fields

Let $\mathbb{F}$ be a finite field. Its prime field is $\mathbb{F}_p = \mathbb{Z}/(p)$ for some prime p. Let $[\mathbb{F} : \mathbb{F}_p] = n$. Then

$$|\mathbb{F}| = p^n.$$

The set $\mathbb{F} \setminus \{0\} = \mathbb{F}^\bullet$ is the multiplicative group of $\mathbb{F}$, $|\mathbb{F}^\bullet| = p^n - 1$.

This numerical data will determine $\mathbb{F}$.

Proposition

If $|\mathbb{F}| = p^n$*, then* $\mathbb{F}$ *consists of the roots of* $x^{p^n} - x$*.*

Proof.

Since the group $\mathbb{F}^\bullet$ has order $p^n - 1$, its elements satisfy $u^{p^n-1} = 1$. □

Construction of Finite Fields

Corollary

For every prime p and natural number n there is a (unique) field $\mathbb{F}$ of cardinality p^n.

Proof.

Let $\mathbb{F}$ be the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Let S be the set of roots of this polynomial in $\mathbb{F}$. We claim that $\mathbb{F} = S$. It suffices to note that S is a ring: for α and β in S,

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$$

and similarly for the product. The uniqueness comes for the uniqueness (up to isos) of the splitting field. □

Finite groups

Proposition

For a field **F***, if G is a finite subgroup of the multiplicative group* $\mathbf{F}^\bullet$ *then G is cyclic.*

Proof.

By the FTAG, G is a direct product of cyclic groups,

$$G = C_1 \times \cdots \times C_n,$$

where the order of C_i divides the order of C_{i+1}.

This means that if $d = |C_n|$, $u^d = 1$ for all $u \in G$.

But the equation $x^d = 1$ in **F** has at most d roots. This implies $n = 1$, that is G is cyclic.

□

Representation

One important issue is how to represent the elements of a field in terms of simpler data. In the case of a finite field $\mathbb{F}$ of cardinality p^n one approach is the following: Since $\mathbb{F}^\bullet$ is a cyclic group of order $p^n - 1$, for each choice of a generator u we have

$$\begin{aligned} u^r \cdot u^s &= u^{r+s} \\ u^r + u^s &= u^{\mathbf{f}(r,s)} \end{aligned}$$

where $\mathbf{f}(r, s) \leq p^n - 1$ if $u^r + u^s \neq 0$. In other terms, it is easy to build the multiplication table of $\mathbb{F}$, but difficult to build its addition table.

Knowing such a function, which depends on the choice of u, would make arithmetic amenable.

Galois Group

Since $\mathbb{F}$ is entirely determined by its order $q = p^n$, we denote it by $\mathbb{F}_q$. Let us determine its Galois group.

The mapping

$$\mathbf{f} : \mathbb{F} \to \mathbb{F}, \quad \mathbf{f}(a) = a^p$$

has the properties

$$\mathbf{f}(a+b) = \mathbf{f}(a) + \mathbf{f}(b), \quad \mathbf{f}(ab) = \mathbf{f}(a)\mathbf{f}(b).$$

Since it is injective and $\mathbb{F}$ is finite, $\mathbf{f}$ is an isomorphism of $\mathbf{f}$ that is the identity on $\mathbb{F}_p = \mathbb{Z}/(p)$.

Theorem

$\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}) \simeq \mathbb{Z}/(n)$ *and is generated by* $\mathbf{f}$. *(This isomorphism is called the Frobenius mapping.)*

Proof.

Note that **f** has order n, since this is the smallest integer s such that $\mathbf{f}^s(a) = a^{p^s} = a$ for all $a \in \mathbb{F}$.

Thus

$$|\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F})| \geq n = [\mathbb{F} : \mathbb{F}_p].$$

But one always has $\leq$, so $=$ holds. In particular $\mathbb{F}$ is a Galois extension of $\mathbb{F}_p$. □

Simple Extensions

Definition

The extension $\mathbf{K} \subset \mathbf{F}$ is simple if $\mathbf{F} = \mathbf{K}(u)$.

An example is a transcendental extension $\mathbf{K}(x)$.

Theorem

A finite extension $\mathbf{K} \subset \mathbf{F}$ *is simple if and only if the number of intermediate extensions*

$$\mathbf{K} \subset \mathbf{L} \subset \mathbf{F}$$

is finite.

Proof. Suppose the number of intermediate extensions is finite. Pick an element $u \in \mathbf{F}$ so that $[\mathbf{K}(u) : \mathbf{K}]$ is largest.

If $\mathbf{K}$ is a finite field, $\mathbf{F}$ is also finite and we have seen that they are simple. So assume $\mathbf{K}$ is infinite.

If $v \in \mathbf{F} \setminus \mathbf{K}(u)$, consider the set of extensions

$$\{\mathbf{K}(u + av), \quad a \in \mathbf{K}\}.$$

By the Pigeonhole Principle, two of these extensions coincide

$$\mathbf{L} = \mathbf{K}(u + av) = \mathbf{K}(u + bv), \quad a \neq b.$$

This means that $(u + av) - (u + bv) = (a - b)v \in \mathbf{L}$, and $u, v \in \mathbf{L}$, which is a contradiction.

Conversely, if $\mathbf{F} = \mathbf{K}(u)$, let $\mathbf{f}(x)$ be the minimal polynomial of u over $\mathbf{K}$. For every intermediate field $\mathbf{K} \subset \mathbf{L} \subset \mathbf{F}$, the minimal polynomial of u over $\mathbf{L}$ is a factor $\mathbf{g}(x)$ of $\mathbf{f}(x)$.

$$\mathbf{g}(x) = a_r x^r + \cdots + a_0, \quad a_i \in \mathbf{L}.$$

Let $\mathbf{L}_0 = \mathbf{K}[a_r, \ldots, a_0]$. Note that

$$[\mathbf{F} : \mathbf{L}_0] \leq r = [\mathbf{F} : \mathbf{L}],$$

so $\mathbf{L} = \mathbf{L}_0$.

In other words, $\mathbf{L}$ is completely determined by $\mathbf{g}(x)$ and vice-versa.

Thus the irreducible factors of $\mathbf{f}(x) \in \mathbf{F}[x]$ are in 1-1 correspondence with the intermediate extensions.

Corollary

If $\mathbf{F}$ *is a Galois extension of* $\mathbf{K}$*, then* $\mathbf{F} = \mathbf{K}(u)$*.*

Proof.

By Galois correspondence, the intermediate fields are uniquely coded by the (finitely many) subgroups of $\mathrm{Gal}_{\mathbf{K}}(\mathbf{F})$. □

Corollary

If $\mathbf{K} \subset \mathbf{F}$ *is an algebraic extension and* $\mathbf{F} = \mathbf{K}(u)$ *then any intermediate extension* $\mathbf{K} \subset \mathbf{L} \subset \mathbf{F}$ *is simple.*

Purely Transcendental Extensions

These are the extensions of a field **K** of the form $\mathbf{F} = \mathbf{K}(x_1, \ldots, x_n)$ where the x_i are independent indeterminates over **K**. They are full of difficult questions, except when $n = 1$, that we discuss now. Set $\mathbf{F} = \mathbf{K}(t)$.

If $u \in \mathbf{F} \setminus \mathbf{K}$, $u = \mathbf{f}(t)/\mathbf{g}(t)$, $\mathbf{f}(t), \mathbf{g}(t) \in \mathbf{K}[t]$, with $\gcd(\mathbf{f}(x), \mathbf{g}(x)) = 1$. If $\max\{\deg \mathbf{f}(x), \mathbf{g}(x)\} = n$,

$$\begin{aligned} \mathbf{f}(t) &= a_0 + a_1 t + \cdots + a_n t^n \\ \mathbf{g}(t) &= b_0 + b_1 t + \cdots + b_n t^n \end{aligned}$$

$a_n - u b_n \neq 0$ shows that $\mathbf{K}(t)$ is algebraic over $\mathbf{K}(u)$, $[\mathbf{K}(t) : \mathbf{K}(u)] \leq n$.

Proposition

With these notations, $[\mathbf{K}(t):\mathbf{K}(u)] = n$ *and the minimal polynomial of* t *over* $\mathbf{K}(u)$ *divides* $\mathbf{f}(x,u) = \mathbf{f}(x) - u\mathbf{g}(x)$*.*

Proof. Set $\mathbf{f}(x,y) = \mathbf{f}(x) - y\mathbf{g}(x) \in \mathbf{K}[x,y]$.

1. This is a linear polynomial over $\mathbf{K}[x]$ and since $\gcd(\mathbf{f}(x),\mathbf{g}(x)) = 1$, it is irreducible.
2. Since t is algebraic over $\mathbf{K}(u)$, u must be transcendental over $\mathbf{K}$. Then $\mathbf{K}[x,y] \simeq \mathbf{K}[x,u]$ under the $\mathbf{K}[x]$-homomorphism that maps y to u. Therefore $\mathbf{f}(x,u)$ is irreducible in $\mathbf{K}[x,u]$ and thus $\mathbf{f}(x,u)$ is irreducible over $\mathbf{K}(u)$.
3. Since $\mathbf{f}(t,u) = \mathbf{f}(t) - u\mathbf{g}(t) = 0$, $\mathbf{f}(x,u)$ is a multiple over $KK(u)$ of the minimal polynomial of t over $\mathbf{K}(u)$. Hence $[\mathbf{K}(t):\mathbf{K}(u)]$ is the degree in x of $\mathbf{f}(x,u)$, that is n.

Galois group of $\mathbf{K}(t)$ over K

1. Any automorphism σ of $\mathbf{K}(t)$ over $\mathbf{K}$, according to the Proposition, must be defined by

$$\sigma(t) = \frac{at+b}{ct+d}, \quad ad - bc \neq 0$$

2. $\sigma(t) = t$ iff $a = d$, and $b = c = 0$.
3. It follows that

$$\mathrm{Gal}_{\mathbf{K}}(\mathbf{K}(t)) = GL_2(\mathbf{K})/H, \quad H = \{aI, a \neq 0\}$$

Luroth Theorem

Theorem

If $\mathbf{F} = \mathbf{K}(t)$ *is a transcendental extension, then any intermediate extension* $\mathbf{L}$ *is transcendental,* $\mathbf{L} = \mathbf{K}(u)$*.*

Proof. Let $v \in \mathbf{L} \setminus \mathbf{K}$. Then t is algebraic over $\mathbf{K}(v)$ and thus over $\mathbf{L}$.

1. Let $\mathbf{f}(x)$ be the minimal polynomial of t over $\mathbf{L}$, $\mathbf{f}(x) = x^n + k_1 x^{n-1} + \cdots + k_n$, $k_i \in \mathbf{L}$
2. Since t is not algebraic over $\mathbf{K}$, some $k_i \in \mathbf{L} \setminus \mathbf{K}$. We claim that $\mathbf{L} = \mathbf{K}(u)$, $u = k_i$.
3. We write $u = \mathbf{g}(t)\mathbf{h}(t)^{-1}$, $\gcd(\mathbf{g}(t), \mathbf{h}(t)) = 1$, $\max\{\deg(\mathbf{g}(t)), \deg(\mathbf{h}(t))\} = m$. We know that $[\mathbf{K}(t) : \mathbf{K}(u)] = m \geq n$.
4. t is a root of $\mathbf{g}(x) - u\mathbf{h}(x)$ and therefore we have $q(x) \in \mathbf{L}[x]$ such that

Cont'd

1. Write $k_i = c_i(t)/c_0(t)^{-1}$, $c_i(t) \in \mathbf{K}[t]$, $\gcd(c_0(t), c_1(t), \ldots, c_n(t)0 = 1$, and clear the denominators of $\mathbf{f}(x)$ to write it as a primitive polynomial

$$\mathbf{f}(x,t) = c_0(t)x^n + c_1(t)x^{n-1} + \cdots + c_n(t) \in \mathbf{K}[x,t]$$

2. The x-degree of $\mathbf{f}(x,t)$ is n, while its t–degree is $\geq m$ (because of the choice of $u = k_i$).
3. If we replace $u = \mathbf{g}(t)\mathbf{h}(t)^{-1}$ in $\mathbf{g}(x) - u\mathbf{h}(x) = q(x)\mathbf{f}(x)$, we see that $\mathbf{f}(x,t)$ divides $\mathbf{g}(t)\mathbf{h}(x) - \mathbf{g}(t)\mathbf{h}(x)$ in $\mathbf{K}(t)[x]$.
4. Since $\mathbf{f}(x,t)$ and $\mathbf{g}(x)\mathbf{h}(t) - \mathbf{g}(t)\mathbf{h}(x)$ are in $\mathbf{K}[x,t]$ and $\mathbf{f}(x,t)$ is primitive, there is $q(x,t) \in \mathbf{K}[x,t]$ such that

$$\mathbf{g}(x)\mathbf{h}(t) - \mathbf{g}(t)\mathbf{h}(x) = q(x,t)\mathbf{f}(x,t).$$

$$\mathbf{g}(x)\mathbf{h}(t) - \mathbf{g}(t)\mathbf{h}(x) = q(x,t)\mathbf{f}(x,t).$$

Now we check that the t-degree of LHS is $\leq m$, while the t-degree of $\mathbf{f}(x,t)$ is $\geq m$. Thus $q(x,t) \in \mathbf{K}[x]$.

Then the RHS is primitive as a polynomial in x, and so is the LHS.

By symmetry the LHS is primitive as a polynomial in t, thus $q \in \mathbf{K}$.

Then $\mathbf{f}(x,t)$ has the same x-degree and t-degree, so $m = n$.

Outline

Galois Group of an Equation

Let $\mathbf{f}(x) \in \mathbf{K}[x]$, and let $U = \{u_1, \ldots, u_n\}$ a full set of roots of $\mathbf{f}(x)$ in some field. Consider the splitting field $\mathbf{F} = \mathbf{K}[u_1, \ldots, u_n]$.

Definition

$\mathrm{Gal}_{\mathbf{K}}(\mathbf{L})$ is the Galois group of $\mathbf{f}(x)$ over $\mathbf{K}$. Notation: $\mathrm{Gal}_{\mathbf{K}}(\mathbf{f}(x))$.

For each $\sigma \in G$,

$$U \mapsto \{\sigma(u_1), \ldots, \sigma(u_n)\}$$

defines a permutation of U. The construction gives an injective homomorphism of G into S_n.

Remark: If $\mathbf{f}(x)$ is irreducible and separable, for any two roots u_1 and u_2, there is an isomorphism $\sigma \in g = \mathrm{Gal}_{\mathbf{K}}(\mathbf{f}(x))$ such that

$$\sigma(u_1) = u_2.$$

This means that G is a transitive subgroup of S_n.

Let $\mathbf{f}(x)$ be an irreducible, separable polynomial over $\mathbf{K}$ and let $\{u_1, \ldots, u_n\}$ be its roots, $\mathbf{F} = \mathbf{K}[u_1, \ldots, u_n]$. Let

$$\Delta = \prod_{i<j} (u_i - u_j).$$

Definition

$D = \Delta^2$ is the discriminant of $\mathbf{f}(x)$ over $\mathbf{F}$.

If $\mathbf{f}(x) = x^2 + bx + c$,

$$D = (u_1 - u_2)^2 = (u_1 + u_2)^2 - 4u_1 u_2 = b^2 - 4c$$

Proposition

Let $G \hookrightarrow S_n$ be the embedding above. Then

1. *With $\Delta = \prod_{i<j}(u_i - u_j)$, for $\sigma \in G$, $\sigma(\Delta) = \pm\Delta$ according whether σ is an even/odd permutation.*
2. $D = \Delta^2 \in \mathbf{K}$.

Proof. Note that $\sigma(\Delta) = \pm\Delta$, so $\sigma(D) = D$.Since G is Galois, $D \in \mathbf{K}$.

Corollary

$G \subset A_n \Leftrightarrow \Delta \in \mathbf{K}$, that is D is a square in $\mathbf{K}$.

Cubics

Let us apply these observations to polynomials of low degree.

Let $\mathbf{f}(x) \in \mathbf{K}[x]$ be a separable, irreducible cubic polynomial and let G be its Galois group. Then:

$$G = \begin{cases} S_3, & \Delta \notin \mathbf{K} \\ A_3, & \text{otherwise} \end{cases}$$

Quartics

Let $\mathbf{f}(x) \in \mathbf{K}[x]$ be a separable, irreducible quartic polynomial, let $\mathbf{F}$ be its splitting field and let G be its Galois group. Now there are several more choices for G since S_4 has several transitive subgroups:

$$G = \begin{cases} S_4 \\ A_4 \\ V \\ 2\text{-Sylow subgroup, there are } 3 \simeq D_4 \\ \mathbb{Z}_4 \end{cases}$$

The key subgroup is
$V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

Let u_1, u_2, u_3, u_4 be the roots of $\mathbf{f}(x)$. Set

$$\begin{aligned} \alpha &= u_1 u_2 + u_3 u_4 \\ \beta &= u_1 u_3 + u_2 u_4 \\ \gamma &= u_1 u_4 + u_2 u_3 \end{aligned}$$

These elements are fixed exactly by $G \cap V$ and we have **[this is a Lemma]** that $\mathrm{Gal}_{\mathbf{K}}(\mathbf{K}(\alpha, \beta, \gamma)) = G/G \cap V$.

Let us argue that if $s \in G \setminus V$, then s moves one of the α, β, γ. For instance if $s = (12)$, and

$$\begin{aligned} s(u_1 u_3 + u_2 u_4) &= u_1 u_3 + u_2 u_4 = u_2 u_3 + u_1 u_4 \quad \Rightarrow \\ u_2(u_3 - u_4) &= u_1(u_3 - u_4) \quad \Rightarrow \quad u_2 = u_1 \quad \text{or} \quad u_3 = u_4 \end{aligned}$$

which is a contradiction.

The other possibilities are handled similarly: it suffices to check coset representatives of V, still takes time.

If $\mathbf{f}(x) = x^4 + bx^3 + cx^2 + dx + e$, the polynomial

$$\mathbf{g}(y) = (y-\alpha)(y-\beta)(y-\gamma) = y^3 - cy^2 - (bd-4e)y - b^2e + 4ce - d^2$$

is called the **resolvent cubic** of $\mathbf{f}(x)$.

It may help first changing variables: $x \to x = t - b/4$ (char $\neq 2$), $\mathbf{f}(t) = t^4 + c't^2 + d't + e'$ (write $\mathbf{f}(x) = x^4 + cx^2 + dx + e$

$$\begin{aligned} 0 &= u_1 + u_2 + u_3 + u_4 \\ c &= u_1u_2 + u_1u_3 + u_1u_4 + u_2u_3 + u_2u_4 + u_3u_4 \\ -d &= u_1u_2u_3 + u_1u_2u_4 + u_2u_3u_4 + u_1u_3u_4 \\ e &= u_1u_2u_3u_4 \end{aligned}$$

Write $\alpha + \beta + \gamma$, $\alpha\beta + \alpha\gamma + \beta\gamma$ and $\alpha\beta\gamma$ in terms of c, d, e.

Theorem

Let $[\mathbf{K}(\alpha, \beta, \gamma) : \mathbf{K}] = m$. *Then*

1. $m = 6 \Leftrightarrow G = S_4$.
2. $m = 3 \Leftrightarrow G = A_4$.
3. $m = 1 \Leftrightarrow G = V$.
4. $m = 2$ *(Suppose* $\mathbf{f}(x)$ *is irreducible). Since* $\mathbf{K}(\alpha, \beta, \gamma)$ *is the splitting field of a cubic,* $m = 1, 2, 3, 6$. *We also have* $m = [\mathbf{K}(\alpha, \beta, \gamma) : \mathbf{K}] = |G/G \cap V|$.

Consider the Galois correspondence diagram

$$\begin{array}{ccc} \mathbf{F} & \longrightarrow & (1) \\ \downarrow & & \\ \mathbf{K}(\alpha, \beta, \gamma) & \longrightarrow & V \cap G \\ \Big\downarrow{\scriptstyle m} & & \\ \mathbf{K} & \longrightarrow & G \end{array}$$

- The implications $\Rightarrow$ will follow from the next calculations.
- If $G = A_4$, $G \cap V = V$ and $m = |A_4/V| = 3$.
- If $G = S_4$, $G \cap V = V$ and $m = |S_4/V| = 6$.
- If $G = V$, $G \cap V = V$ and $m = |V/V| = 1$.
- If $G = D_4$, $G \cap V = V$ and $m = |D_4/V| = 2$.
- If $G = \mathbb{Z}_4$, G is generated by a 4-cycle, so its square is in V. Thus $|G \cap V| = 2$ and therefore $m = |\mathbb{Z}_4/\mathbb{Z}_4 \cap V| = 2$.

Quintics

Let $\mathbf{f}(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$.This polynomial has the following properties:

1. $\mathbf{f}(x)$ is irreducible over $\mathbb{Q}$: by Eisenstein's
2. $\mathbf{f}'(x) = 5x^4 - 6$ has two roots.
3. Examining graph gives that $\mathbf{f}(x)$ has 3 real roots and a pair of complex conjugate roots.
4. As a subgroup of S_5, G has order divisible by 5 because of item (1), and therefore by Sylow contains a cycle σ of order 5. In view of (3), G has a cycle τ of order 2.

Proposition

If p is prime and a subgroup of H of S_p contains a cycle of order p and another of order 2, then $H = S_p$.

Applying to our case,

$$\mathrm{Gal}_{\mathbb{Q}}(x^5 - 6x + 3) = S_5.$$

Tschirnhaus Transformation

Given a quintic

$$\mathbf{f}(x) = x^5 + \underbrace{ax^4 + bx^3 + cx^2} + dx + e,$$

there are transformations, some linear, which we used to get rid of *a*, some quadratic, that permit to study an equivalent quintic without the terms indicated. This is a theorem of Bring-Jerrand.

Outline

Assignment #3

1. Prove that over any field **K**, $x^3 - 3x + 1$ is either irreducible or splits over **K**.
2. Prove that in a finite field **F**, every element is a sum of two squares.
3. Give the addition and multiplication tables for the field $\mathbb{F}_4$.

Outline

Radical Extensions

Let

$$\mathbf{f}(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_0 = 0, \quad a_i \in \mathbf{K},$$

and let u be a root in some extension field. By an explicit solution by radical we mean

$$u = \mathbf{h}(a_0, a_1, \ldots, a_n)$$

where $\mathbf{h}$ is a rational function over $\mathbf{K}$ involving root extractions.

For $n = 1, 2$ is classical, for $n = 3, 4$ the solution is due to Tartaglia, Cardano and Ferrari. For $n = 5$, Abel proved the impossibility and the explanation for $n \geq 5$ is a crowning achievement of Galois.

Cardano's Formula

$y^3 + ay^2 + by + c = 0$. If char $\neq 3$, the substitution $y = x - a/3$ gives the equivalent equation

$$x^3 + px + q = 0, \quad p = b - a^3/3, \quad q = c + (2a^3 - 9ab)/27$$

Now substitute $x = u + v$:

$$(u+v)^3 + p(u+v) + q = (u^3 + v^3 + q) + (u+v)(3uv + p) = 0$$

Cardano's trick: Choosing $3uv + p = 0$ gives two equations

$$\begin{aligned} u^3 + v^3 &= -q \\ u^3 v^3 &= -p^3/27 \end{aligned}$$

Thus u^3 and v^3 are roots of the quadratic

$$t^2 + qt - p^3/27 = 0$$

If char $\neq 2$, we use the quadratic formula to get

$$x = u + v = \sqrt[3]{-q + \sqrt{q^2/4 + p^3/27}} + \sqrt[3]{-q - \sqrt{q^2/4 + p^3/27}}$$

There seems to be too many roots with the various choices of the cubic roots.

Radical Extensions

Definition

Let **F** be a finite extension. **F** is a radical extension of **K** if there exist $u_1, \ldots, u_n \in \mathbf{F}$ such that $\mathbf{F} = \mathbf{K}[u_1, \ldots u_n]$ and a set of positive integers $r_1, \ldots, r_n$ such that

$$\begin{aligned} u_1^{r_1} &\in \mathbf{K} \\ u_2^{r_2} &\in \mathbf{K}[u_1] \\ &\vdots \\ u_n^{r_n} &\in \mathbf{K}[u_1, \ldots, u_{n-1}] \end{aligned}$$

Remark: If one of these exponents r_i is a composite number, $r_i = r \cdot s$, we can write $u_i^{r_i} = ((u_i)^r)^s$, and therefore replace the u_i by another set of elements in which all the exponents are prime. We assume this from now on.

Main Theorem for Radical Extensions

Theorem

Let $\mathbf{F}$ *be a radical extension of a field* $\mathbf{K}$*. For any intermediate extension*

$$\mathbf{K} \subset \mathbf{M} \subset \mathbf{F}$$

$$\mathrm{Gal}_{\mathbf{K}}(\mathbf{M})$$

is solvable.

See how powerful this is: If $\mathbf{L}$ is an algebraic extension of $\mathbf{K}$, and $u \in \mathbf{L}$ is to be obtained by a sequence of rational operations plus root extractions, then $\mathrm{Gal}_{\mathbf{K}}(\mathbf{K}(u))$ must be solvable.

Recall

For a group G, the commutator subgroup $G^{(1)}$ is the subgroup generated by all $aba^{-1}b^{-1}$, $a, b \in G$.

G is solvable if some iterate

$$G^{(n)} = (G^{n-1})^{(1)} = (1)$$

This is equivalent to the existence of a chain of subgroups

$$(1) \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_m \triangleleft G,$$

such that G_{i+1}/G_i is abelian.

Facts

1. If $H \subset G$ and G is solvable, then H is solvable.
2. The alternating group A_n is solvable for $n \leq 4$, but simple (therefore not solvable) for $n \geq 5$.
3. $H \triangleleft G$, then G is solvable iff H and G/H are solvable.

Proof: Preparatory Steps

1. $\mathbf{K} \subset \mathbf{M} \subset \mathbf{F}$ radical: Let $G = \mathrm{Gal}_{\mathbf{K}}(\mathbf{M})$ and set $\mathbf{K} \subset \mathbf{K}_0 = G'$.
2. Then $G = \mathrm{Gal}_{\mathbf{K}_0}(\mathbf{M})$, so we may assume that **M** is Galois over **K**–after we replace **K** by $\mathbf{K}_0$ as

$$\mathbf{F} = \mathbf{K}_0[u_1, \ldots, u_n]$$

3. Replace **F** by $\mathbf{F}_0$ the splitting field of all of the minimal polynomials of all the u_i. $\mathbf{F}_0$ is also a radical extension.
4. We are going to assume char zero although the theorem holds in all chars.

Proof: Change of Setting

Set $\overline{G} = \mathrm{Gal}_{\mathbf{K}_0}(\mathbf{F}_0)$ and $G = \mathrm{Gal}_{\mathbf{K}_0}(\mathbf{M})$. Note that

$$\mathbf{M}' \triangleleft \overline{G}, \quad G = \overline{G}/\mathbf{M}'$$

so ETS $\overline{G}$ is solvable.

- $\mathbf{M} = \mathbf{K}[u_1, \ldots, u_n]$, all r_i prime, char 0.
- $\mathbf{M}$ splitting field.

Lemma 1

Lemma

Let p be a prime number and $\mathbf{L}$ the splitting field of $x^p - 1$ over $\mathbf{K}$. Then $\mathrm{Gal}_{\mathbf{K}}(\mathbf{L})$ is abelian.

Proof. If char $= p$, $x^p - 1 = (x-1)^p$ and $\mathbf{L} = \mathbf{K}$.

1. If char $\neq p$, $x^p - 1$ is a separable polynomial.
2. If $\epsilon \neq 1$ is one of its roots, it must have order p, so the other roots $\neq 1$ are ϵ^i, $0 < i < p$.
3. $\mathbf{L} = \mathbf{K}[\epsilon]$ and any two automorphisms $\sigma(\epsilon) = \epsilon^i$, $\tau(\epsilon) = \epsilon^j$, so that

$$\tau(\sigma(\epsilon)) = \epsilon^{ij}$$

from which it follows that they commute.

Lemma 2

Lemma

Suppose $x^n - 1$ factors completely over **K** *and let* **L** *be the splitting field of $x^n - a$, $a \in \mathbf{K}$. Then $\mathrm{Gal}_{\mathbf{K}}(\mathbf{L})$ is abelian.*

Proof. If u is a root of $x^n - a$, the other roots are $u\epsilon$, where $\epsilon^n = 1$. Thus $\mathbf{L} = \mathbf{K}[u]$.

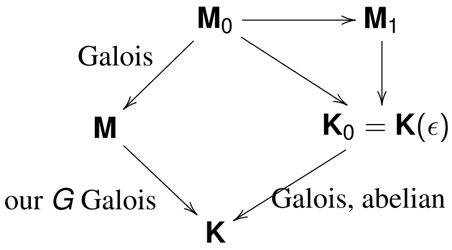
Two elements of Galois group are specified by $\sigma(u) = u\epsilon$, $\epsilon^n = 1$, and $\tau(u) = u\eta$, $\eta^n = 1$.

Therefore $\tau(\sigma(u)) = u\epsilon\eta = \sigma(\tau(u))$. □

Proof by Diagramming

Set $\mathbf{M} = \mathbf{K}[u_1, \ldots, u_n]$. If $u_1^p \in \mathbf{K}$, let $\mathbf{K}_0$ be the splitting field of $x^p - 1$, and set $\mathbf{M}_1 = \mathbf{K}_0[u_1] = \mathbf{K}[\epsilon, u_1]$ and

$$\mathbf{M}_0 = \mathbf{M}[\epsilon] = \mathbf{K}[\epsilon, u_1, \ldots, u_n] = \mathbf{M}_1[u_2, \ldots, u_n]$$



End of Proof of Galois Theorem

1. It is enough to prove that $\mathrm{Gal}_{\mathbf{K}}(\mathbf{M}_0)$ is solvable since **M** is Galois over **K**.

   Let $\widetilde{G} = \mathrm{Gal}_{\mathbf{K}(\epsilon)}(\mathbf{M}_0)$

2. $\mathbf{M}_0$ is radical over $\mathbf{M}_1 = \mathbf{K}_0[u_1]$ and therefore the Galois group H is solvable by induction on n.

3. Since $\mathbf{M}_1$ is Galois and abelian over $\mathbf{K}_0$, and $\mathbf{K}_0$ is Galois and abelian over **K**.

4. Thus $\mathrm{Gal}_{\mathbf{K}}(\mathbf{M}_1)$ is solvable. Therefore $\widetilde{G}$ and G along with it are solvable.

Outline

Assignment #4

- Let **K** be a subfield of $\mathbb{R}$ and $\mathbf{f} \in \mathbf{K}[x]$ an irreducible quartic. If **f** has exactly two real roots, show that the Galois group of **f** is S_4 or D_4.
- Determine the Galois group of $x^4 + 3x^3 + 3x - 2$ over $\mathbb{Q}$, or more simply $x^4 + 1$ over $\mathbb{Q}$.

Outline

Assignment #5

Pick two problems.

1. Show that if $n \geq 3$, then $x^{2^n} + x + 1$ is reducible over $\mathbb{Z}_2$.
2. Let **F** be a field extension of **K**. Prove the statement: If $u \in \mathbf{F}$ is separable over **K** and $v \in \mathbf{F}$ is purely inseparable over **K** then $\mathbf{K}(u, v) = \mathbf{K}(u + v)$ and if $uv \neq 0$, then $\mathbf{K}(u, v) = \mathbf{K}(uv)$.
3. Prove: If **F** is a finite extension of $\mathbb{Q}$ then it contains only a finite number of roots of 1.
4. Prove that if **F** is a radical extension of **K** and **L** is an intermediate extension then **F** is a radical extension of **L**.

Outline

Trace and Norm

Definition

Let $\mathbf{K} \subset \mathbf{L}$ be a finite extension of Galois group $\mathbf{G}$.

1. The **trace of L over K** is the function $u \in \mathbf{L} \to \mathbf{T}(u) = \sum_{\sigma \in \mathbf{G}} \sigma(u)$.
2. The **norm of L over K** is the function $u \in \mathbf{L} \to N(u) = \prod_{\sigma \in \mathbf{G}} \sigma(u)$.

Both $\mathbf{T}(u)$ and $N(u)$ are fixed elements. These functions play many roles, from the study of the structure of cyclic extensions to ring theory in general.

Linear Independence of Automorphisms

We are going to examine some properties of the **K**-linear transformations of **L** of the form

$$\mathbf{h} = a_1\sigma_1 + \cdots + a_n\sigma_n, \quad a_i \in \mathbf{L},\ \sigma_i \in \mathbf{G}.$$

Definition

The set **L**[**G**] of all linear transformations as **h** is a ring, called the twisted group ring of **G** over **L**.

- Note the action:
  $(a\sigma)(b\tau)(x) = (a\sigma)(b\tau(x)) = a\sigma(b)(\sigma\tau)(x)$
- The ring **L**[**G**] is a left **L**-vector space. It is also a left **K**-vector space

Dedekind Theorem

Theorem (Dedekind)

The elements $\sigma_1, \ldots, \sigma_n$ are linearly independent over $\mathbf{L}$.

Proof. Suppose there is a nontrivial dependence relation in distinct σ_i

$$a_1\sigma_1 + \cdots + a_n\sigma_n = 0,$$

with n as small as possible.

Note that $n > 1$ and $a_i \neq 0$.

Since $n > 1$, there is $a \in \mathbf{L}$ such that $\sigma_1(a) \neq \sigma_2(a)$. Applying the relation to ax, x an arbitrary element of $\mathbf{L}$, gives rise to another relation

$$a_1\sigma_1 + \cdots + a_n\sigma_n = 0,$$
$$a_1\sigma_1(a)\sigma_1 + \cdots + a_n\sigma_n(a)\sigma_n = 0.$$

Multiplying the first relation (on the left) by $\sigma_1(a)$ and subtracting from the second relation gives

$$a_2(\sigma_2(a) - \sigma_1(a))\sigma_2 + \cdots + a_n(\sigma_n(a) - \sigma_1(a))\sigma_n = 0,$$

which is a nontrivial relation of shorter length, a contradiction.

Structure of L[G]

It is an immediate consequence that if x_i is a basis of **L** over **K**, then the elements $x_i\sigma_j$ are linearly independent over **K**.

Proof.

Suppose

$$\sum_{ij} c_{ij} x_i \sigma_j = 0, \quad c_{ij} \in \mathbf{K}$$

Then

$$\sum_j \left(\sum_i c_{ij} x_i\right)\sigma_j = 0 \quad \Rightarrow \quad \text{by Previous theorem}$$

$$\sum_i c_{ij} x_i = 0 \quad \forall j \quad \Rightarrow c_{ij} = 0.$$

□

Theorem

If $\mathbf{L}$ *is a Galois extension over* $\mathbf{K}$*, there is an isomorphism* $\mathbf{L}[\mathbf{G}] \approx \mathrm{Hom}_{\mathbf{K}}(\mathbf{L}, \mathbf{L})$*.*

Proof.

Since $|\mathbf{G}| = [\mathbf{L} : \mathbf{K}]$, the ring of matrices $\mathrm{Hom}_{\mathbf{K}}(\mathbf{L}, \mathbf{L})$, and its subring (subspace) $\mathbf{L}[\mathbf{G}]$ have the same dimension as vector spaces over $\mathbf{K}$. □

Cyclic Extensions

Definition

An extension $\mathbf{L}$ of a field $\mathbf{K}$ is called **cyclic** [resp. **abelian**] if $\mathbf{L}$ is a Galois extension and $\mathbf{G}(\mathbf{L}/\mathbf{K})$ is cyclic [resp. abelian].

A basic tool to study these extensions is:

Theorem

Let $\mathbf{L}$ be a cyclic extension field of $\mathbf{K}$ of degree n, σ a generator of $\mathbf{G}$ and $u \in \mathbf{L}$. Then

1. $\mathbf{T}(u) = 0$ *if and only if* $u = v - \sigma(v)$ *for some* $v \in \mathbf{L}$.
2. *(**Hilbert's 90**)* $N(u) = 1$ *if and only if* $u = v\sigma(v)^{-1}$ *for some* $v \in \mathbf{L}$.

Proof. The forward assertions follow directly from the definition of trace and norm.

Proof

- Suppose $\mathbf{T}(u) = 0$. Now we choose $w \in \mathbf{L}$ such that $\mathbf{T}(w) = 1$ as follows. By the linear independence of automorphisms, there exists $z \in \mathbf{L}$ such that

$$0 \neq 1z + \sigma z + \sigma^2 z + \cdots + \sigma^{n-1} z = \mathbf{T}(z).$$

- As $\mathbf{T}(z) \in \mathbf{K}$, setting $w = z\mathbf{T}(z)^{-1}$, we have $\mathbf{T}(w) = 1$.

Proof Cont'd

- Set

$$\begin{aligned} v &= uw + (u + \sigma u)(\sigma w) + (u + \sigma u + \sigma^2 u)(\sigma^2 w) + \\ \cdots &\quad + (u + \sigma u + \cdots + \sigma^{n-2} u)(\sigma^{n-2} w) \end{aligned}$$

- Since $\mathbf{T}(u) = 0$, setting $u = -\sigma u - \sigma^2 u - \cdots - \sigma^{n-1} u$ in the last equation, shows that

$$\begin{aligned} v - \sigma v &= uw + u\sigma(uw) + \cdots + u\sigma^{n-1} w \\ &= u\mathbf{T}(w) = u1 = u. \end{aligned}$$

Proof of Hilbert's 90th

- Suppose $N(u) = 1$. By the linear independence of automorphisms, there exists $y \in \mathbf{L}$ such that

$$\begin{aligned} 0 \neq v &= uy + (u\sigma u)\sigma y + (u\sigma u\sigma^2 u)\sigma^2 y + \\ \cdots &+ (u\sigma u \cdots \sigma^{n-1} u)\sigma^{n-1} y. \end{aligned}$$

- The last summand is $N(u)\sigma^{n-1}y = \sigma^{n-1}y$, making it easy to verify that $u^{-1}v = \sigma v$, hence

$$u = v(\sigma v)^{-1}$$

Cyclic Extension

Theorem

Let $\mathbf{K}$ *be a field of characteristic* $p \neq 0$. $\mathbf{L}$ *is a cyclic extension of degree p iff* $\mathbf{L}$ *is a splitting field over* $\mathbf{K}$ *of a polynomial* $\mathbf{x}^p - \mathbf{x} - a \in \mathbf{K}[\mathbf{x}]$. *In this case* $\mathbf{L} = \mathbf{K}(u)$ *where u is a root of* $\mathbf{x}^p - \mathbf{x} - a$.

Proof. If σ is the generator of the cyclic group $\mathbf{G}(\mathbf{L}/\mathbf{K})$,

$$\mathbf{T}(1) = \sum_i \sigma^i(1) = p.1 = 0$$

By part (1), of the theorem, there exists $v \in \mathbf{L}$ such that $1 = v - \sigma v$. Setting $u = -v$, we have $\sigma u = u + 1$, and thus $u \notin \mathbf{K}$. Since there are no intermediate extensions, $\mathbf{L} = \mathbf{K}(u)$.

Finally, $u = \sigma^p u = (u+1)^p = u^p + 1$. This implies that $\sigma(u^p - u) = u^p - u$, which shows that $u^p - u = a \in \mathbf{K}$. Thus u satisfies the equation $\mathbf{x}^p - \mathbf{x} - a = 0$.

Cyclic Extension

Corollary

If $\mathbf{K}$ is a field of characteristic $p \neq 0$ and $\mathbf{x}^p - \mathbf{x} - a \in \mathbf{K}[\mathbf{x}]$, then $\mathbf{x}^p - \mathbf{x} - a$ is either irreducible or splits in $\mathbf{k}[\mathbf{x}]$.