B3.1 Galois Theory

Damian Rössler

Oxford, Michaelmas Term 2020

Introduction

The basic idea of Galois Theory is the following.

Let $P(x) \in \mathbb{Q}[x]$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be the roots of $P(x)$.

Let $F := \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{C}$ be the smallest subfield of $\mathbb{C}$, which contains $\alpha_1, \ldots, \alpha_n$.

Then we may consider the group

$$G := \{\text{field automorphisms of } F\}.$$

By construction, the elements of G permute the α_i, and if an element of G fixes all the roots, then it must be the identity. Thus there is a natural injection $\iota : G \hookrightarrow S_n$, such that $\alpha_{\iota(g)(i)} = \alpha_{g(\alpha_i)}$, for $i \in \{1, \ldots, n\}$. In particular, G is finite.

The fundamental insight of É. Galois was that the group theoretic properties of G provide crucial information on $P(x)$.

For example, the structure of G alone determines whether it is possible to express the roots of $P(x)$ from its coefficients using a closed formula containing only polynomial expressions and extractions of k-th roots (for $k \geq 1$). A polynomial with the latter property is called *solvable by radicals*.

Using his theory, Galois was then able to answer in the negative the following age-old question: are there polynomials, which are not solvable by radicals?

Galois Theory was vastly generalised in the 1950s and 1960s by A. Grothendieck, who saw it as a special case of what is now called *faithfully flat descent*.

Prerequisites and bibliography

A basic reference for this course is the book *Galois Theory* (Springer) by J. Rotman.

Another excellent textbook on the topic is *Galois Theory* (Routledge, fourth edition) by I.-N. Stewart.

The reader might also want to consult E. Artin's lectures on Galois Theory, which are available here:

https://projecteuclid.org/euclid.ndml/1175197041

Prerequisites of the course. Part A course Rings and Modules. If this course was not attended, the relevant material can be studied alongside this course.

Rings and domains

A (unitary) *ring* is a quadruple $(R, +, \cdot, 1, 0)$, where R is a set, 0 and 1 are elements of R, and $+$ and $\cdot$ are maps

$$+ : R \times R \to R$$

and

$$\cdot : R \times R \to R$$

st

- $(R, +, 0)$ is an abelian group;

- (associativity) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$;

- (distributivity) $a \cdot (b + c) = a \cdot b + a \cdot c, \ (b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$;

- $1 \cdot a = a = a \cdot 1$ for all $a \in R$.

A ring is *commutative*, if $a \cdot b = b \cdot a$ for all $a, b \in R$.

If $(R, +, \cdot, 1, 0)$ and $(S, +, \cdot, 1, 0)$ are rings, a

ring homomorphism (or ring map)

from $(R, +, \cdot, 1, 0)$ to $(S, +, \cdot, 1, 0)$ is a map $\phi : R \to S$, such that $\phi(1) = 1$ and for all $a, b \in R$,

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

and

$$\phi(a + b) = \phi(a) + \phi(b).$$

There is an obvious notion of subring of a ring $(R, +, \cdot, 1, 0)$.

From now on, unless explicitly stated otherwise, a ring will be a commutative ring.

If $(R, +, \cdot, 1, 0)$ is a ring, we shall mostly use the shorthand R for $(R, +, \cdot, 1, 0)$. Also, if $r, t \in R$, we shall often write rt for $r \cdot t$.

If $a \in R$ is an element of a ring, we shall write $a^{-1} \in R$ for the element st $a \cdot a^{-1} = 1$, *if it exists* (in which case it is unique).

This element is called the *inverse* of a (if it exists). If a has inverse, then we say that a is *invertible*, or is a *unit.*

A ring is *integral (or a domain, or an integral domain)* if, for any $a, b \in R$, the equation $a \cdot b = 0$ implies that either $a = 0$ or $b = 0$.

If R is a domain, an element $r \in R \backslash \{0\}$ is called *irreducible*, if whenever $r = r_1 r_2$, then either r_1 or r_2 is a unit.

Example. $\mathbb{Z}$ and $\mathbb{C}[x]$ are integral domains.

An additive subgroup $I \subseteq R$ of R is called an *ideal*, if for all $a \in R$ and $b \in I$, we have $a \cdot b \in I$.

If H is a subset of R, then set

$$(H) := \{\text{finite } R\text{-linear combinations of elements of } H\}$$

is an ideal (exercise), the *ideal generated by H*.

An ideal, which has the form (r) for some $r \in R$, is called *principal*.

If $r, t \in R$, the notation $r|t$ mean $t \in (r)$.

If $f : R \to S$ is a ring map, then the subset of R

$$\ker(f) := \{r \in R \,|\, f(r) = 0\}$$

is an ideal of R (exercise).

This ideal is called the *kernel* of f.

Example. Any ideal of $\mathbb{Z}$ is principal.

If $I \subseteq R$ is an ideal, the relation $\bullet \equiv \bullet \pmod{I}$ on R, st

$$a \equiv b \pmod{I} \text{ iff } a - b \in I$$

is an equivalence relation (verify).

The set of equivalence classes of $\bullet \equiv \bullet (\text{mod } I)$ is denoted R/I.

There is a natural map $[\bullet]_I : R \to R/I$ sending an element r to its equivalence class $[r]_I \in R/I$, and there is a unique ring structure on R/I, such that this map is a ring homomorphism.

We shall always implicitly endow R/I with this ring structure.

If $f : R \to S$ is a ring map, then there a unique ring map $f' : R/\ker(f) \to S$, such that $f(r) = f'([r]_{\ker(f)})$ for all $r \in R$. Furthermore, f' is injective.

An ideal I in a ring R is said to be *prime* if R/I is a domain.

An ideal I in a ring R is said to be *maximal* if R/I is a field.

For any ring R, there a unique ring map $\phi : \mathbb{Z} \to R$, st

$$\phi(n) = 1 + \cdots + 1 \, (n\text{-times})$$

The *characteristic* $\mathrm{char}(R)$ of R is the unique $r \geq 0$, such that $(r) = \ker(\phi)$.

If R is a domain, then $\mathrm{char}(R)$ is either 0 or a prime number.

Fields

A ring R is a *field* if $(R\backslash\{0\}, \cdot, 1)$ is a commutative group and if $0 \neq 1$.

Note that the ring R is a field iff all the elements of $R\backslash\{0\}$ are invertible.

Proposition-Definition

Let R be a domain. Then there is a field F and an injective ring map $\phi : R \to F$ with the following property.
If $\phi_1 : R \to F_1$ is a ring map into a field F_1, then there is a unique ring map $\lambda : F \to F_1$ st $\phi_1 = \lambda \circ \phi$.

The field F is thus uniquely determined, up to unique isomorphism. It is called the *field of fractions* of F.

One often writes $F := \operatorname{Frac}(R)$.

Lemma

(i) Let K be a field and let $I \subseteq K$ be an ideal. Then either $I = (0)$ or $I = K$.
(ii) Let K, L be fields and let $\phi : K \to L$ be a ring map. Then ϕ is injective.

Proof. (i) If $I \neq (0)$, then let $k \in I \backslash \{0\}$. By definition, k^{-1} exists and since I is an ideal $x^{-1} \cdot x = 1 \in I$. But $K = (1) \subseteq I$ and thus $I = K$.

(ii) Consider $\ker(\phi)$. If $\ker(\phi) = K$ then $\phi(1) = 1 = 0$, which is a contradiction to the fact that L is a field. Thus $\ker(\phi) = (0)$ by (i). In particular, ϕ is injective by the first isomorphism theorem (see above). $\square$

end of lecture 1

Rings of polynomials

Let R be a ring. We shall write $R[x]$ for the ring of polynomials in the variable x and with coefficients in R.

Let $P(x) = a_d x^d + \cdots + a_1 x + a_0 \in R[x]$, where $a_d \neq 0$.

We shall say that $P(x)$ is *monic* if $a_d = 1$.

The natural number $\deg(P) := d$ is called the *degree* of $P(x)$.

An element $t \in R$ is a *root* of $P(x)$ if $a_d t^d + \cdots + a_1 t + a_0 = 0$.

By convention, we set the degree of the 0 polynomial to be $-\infty$.

Notation. If K is a field, then we shall write $K(x)$ for the field of fractions of $K[x]$.

Lemma

If R is a domain, then so is $R[x]$.

Proof. Let $P(x), Q(x) \in R[x]$ and suppose that $P(x), Q(x) \neq 0$. Write

$$P(x) = a_d x^d + \cdots + a_1 x + a_0 \in R[x]$$

and

$$Q(x) = b_l x^d + \cdots + b_1 x + b_0 \in R[x]$$

with $a_d, b_l \neq 0$. Then

$$P(x) \cdot Q(x) = (a_d \cdot b_l) x^{d+l} + \ldots$$

and thus, if $P(x) \cdot Q(x) = 0$, then $a_d \cdot b_l = 0$ and thus either $a_d = 0$ or $b_l = 0$, a contradiction. $\square$

Proposition (Euclidean division)

Let K be a field. Let $f, g \in K[x]$ and suppose that $g \neq 0$. Then there are two polynomials $q, r \in K[x]$ st

$$f = gq + r$$

and $\deg(r) < \deg(g)$.

The polynomials q and r are uniquely determined by these properties.

Recall that a Principal Ideal Domain (PID) is a domain, which has the property, that all its ideals are principal.

A Unique Factorisation Domain (UFD) is a domain R, which has the following property.

For any $r \in R \backslash \{0\}$, there is a sequence $r_1, \ldots, r_k \in R$ (for some $k \geq 1$), st

(1) all the r_i are irreducible;

(2) $(r) = (r_1 \cdots r_k)$;

(3) if $r'_1, \ldots, r'_{k'}$ is another sequence with properties (1) and (2), then $k = k'$ and there is a permutation $\sigma \in S_n$ st $(r_i) = (r'_{\sigma(i)})$ for all $i \in \{1, \ldots, k\}$.

Corollary

$K[x]$ is a PID, and in particular a UFD.

Note that if R is a domain and $r, r' \in R$, then $(r) = (r')$ iff $r = ur'$, where u is a unit (exercise).

Applying this to $R = K[x]$, when K is a field, we see that if $f, g \in K[x]$ are two monic polynomials, then $(f) = (g)$ iff $f = g$.

We conclude from the corollary that for any monic polynomial $f \in K[x]$, there is a sequence of irreducible monic polynomials $f_1, \ldots, f_k$, st $f = f_1 \cdots f_k$.

Moreover, this sequence is unique up to permutation.

Another consequence of Euclidean division is the following.

Corollary

Let K be a field and let $f \in K[x]$ and $a \in K$. Then
(i) a is a root of f iff $(x-a)|f$;
(ii) there is a polynomial $g \in K[x]$, which has no roots, and a decomposition

$$f(x) = g(x) \prod_{i=1}^{k} (x - a_i)^{m_i}$$

where $k \geq 0$, $m_i \geq 1$ and $a_i \in K[x]$.

We end this section with two useful criteria for irreducibility (for the proofs, see Rings and Modules).

Lemma (Gauss lemma)

Let $f \in \mathbb{Z}[x]$. Suppose that f is monic.
Then f is irreducible in $\mathbb{Z}[x]$ iff f is irreducible in $\mathbb{Q}[x]$.

Proposition (Eisenstein criterion)

Let

$$f = x^d + \sum_{i=0}^{d-1} a_i x^i \in \mathbb{Z}[x]$$

Let $p > 0$ be a prime number.
Suppose that $p | a_i$ for all $i \in \{1, \ldots, d-1\}$ and that $p^2 \nmid a_0$.

Then f is irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$).

Actions of groups on rings

Let R be a ring and let G be a group.

Write $\mathrm{Aut}_{\mathrm{Rings}}(R)$ for the group of bijective ring maps $a : R \to R$.

An *action* of G on R is group homomorphism

$$\phi : G \to \mathrm{Aut}_{\mathrm{Rings}}(R)$$

Notation. If $\gamma \in G$ and $r \in R$, we write

$$\gamma(r) := \phi(\gamma)(r).$$

We also sometimes write γr for $\gamma(r)$. We write R^G for the set of invariants of R under the action of G, ie

$$R^G := \{r \in R \,|\, \gamma(r) = r \ \forall \gamma \in G\}.$$

Lemma

Let G act on the ring R.

(i) R^G is a subring of R.

(ii) If R is a field, then R^G is a field.

Proof. (i) Clearly $\gamma(1) = 1$ for all $\gamma \in G$. Also, if $\gamma(a) = a$ and $\gamma(b) = b$ for some $\gamma \in G$, then $\gamma(ab) = \gamma(a)\gamma(b) = ab$ and $\gamma(a + b) = \gamma(a) + \gamma(b) = a + b$. This proves (i).

(ii) Suppose that $a \neq 0$ and that $\gamma(a) = a$ for some $\gamma \in G$. Then $\gamma(aa^{-1}) = \gamma(a)\gamma(a^{-1}) = \gamma(1) = 1 = a\gamma(a^{-1})$. Thus $\gamma(a^{-1})$ is an inverse of a and must thus coincide with a^{-1}. Since γ was arbitrary, $a^{-1} \in R^G$. Thus every element of R^G has an inverse, and R^G is thus a field. $\square$

Let K be a field and let $n \geq 1$.

There is a natural action of S_n on $K[x_1, \ldots, x_n]$, given by the formula

$$\sigma(P(x_1, \ldots, x_n)) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Definition

A symmetric polynomial is an element of $K[x_1, \ldots, x_n]^{S_n}$.

Examples. For any $k \in \{1, \ldots, n\}$, the polynomial

$$s_k := \sum_{i_1 < i_2 < \cdots < i_k} \prod_{j=1}^{k} x_{i_j}$$

is symmetric. For instance, we have

$$s_1 = x_1 + \cdots + x_n$$

and

$$s_n = x_1 \cdots x_n.$$

Theorem (Fundamental theorem of the theory of symmetric functions)

$$K[x_1, \ldots, x_n]^{S_n} = K[s_1, \ldots, s_n].$$

Here is a more precise formulation.

Let $\phi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ be the map of rings, which sends x_k to s_k and which sends constant polynomials to themselves.

Then

(i) the ring $K[x_1, \ldots, x_n]^{S_n}$ is the image of ϕ;

(ii) ϕ is injective.

Proof. We shall sketch the proof of (i). We first introduce the lexicographic ordering on monomials. We shall write

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \overset{\text{DEF}}{\leq} x_1^{\beta_1} \cdots x_n^{\beta_n}$$

if either

- $\alpha_1 < \beta_1$

or

- $\alpha_1 = \beta_1$ and $x_2^{\alpha_2} \cdots x_n^{\alpha_n} \leq x_2^{\beta_2} \cdots x_n^{\beta_n}$.

The lexicographic ordering is similar to the alphabetic ordering on words.

Now let f be a symmetric polynomial. Let $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be the largest monomial in f, for the lexicographic ordering. We must have $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$.

To see this, note that, by definition, for any $\sigma \in S_n$, the monomial $x_1^{\alpha_{\sigma(1)}} \cdots x_n^{\alpha_{\sigma(n)}}$ must also appear in f.

Now suppose for contradiction that $\alpha_1 < \alpha_2$.

Apply the permutation σ, which swaps 1 and 2 to $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

We obtain the monomial $x_1^{\alpha_2} x_2^{\alpha_1} \cdots x_n^{\alpha_n}$.

By the above, this polynomial also appears in f and by definition

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \leq x_1^{\alpha_2} x_2^{\alpha_1} \cdots x_n^{\alpha_n},$$

which is a contradiction.

Hence $\alpha_1 \geq \alpha_2$.

Now repeat this reasoning for α_2 and α_3, α_3 and α_4, etc.

Now one may compute that the largest monomial in the polynomial

$$s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \cdots s_n^{\alpha_n}$$

is also $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Thus we see that for some $c \in K$, all the monomials in the polynomial

$$f - c \cdot s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \cdots s_n^{\alpha_n}$$

are strictly smaller than $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for the lexicographic ordering.

We now repeat all the above reasoning, with

$$f - c \cdot s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \cdots s_n^{\alpha_n}$$

in place of f, and apply induction. $\square$

Example. $\sum_{i=1}^{n} x_i^2 = s_1^2 - 2s_2$.

Proposition-Definition

(i) $\Delta(x_1, \ldots, x_n) := \prod_{i<j}(x_i - x_j)^2 \in \mathbb{Q}[x_1, \ldots, x_n]^{S_n}$;

(ii) $\delta(x_1, \ldots, x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Q}[x_1, \ldots, x_n]^{A_n}$.

Here $A_n \subseteq S_n$ is the alternating group. This is the subgroup of permutations with even sign.

The polynomial $\Delta(x_1, \ldots, x_n)$ is called the *discriminant*.

Proof. Clear. $\square$

$\boxed{\text{end of lecture 2}}$

Field extensions: definitions

Let K be a field.

A *field extension* of K, or K-extension, is an injection

$$K \hookrightarrow M$$

of fields. This gives M the structure of a K-vector space.

Alternate notation: $M - K$, $M|K$, $M : K$. We shall mostly use the notation $M|K$.

$[M : K] := \dim_K(M)$.

$[M : K]$ is called the *degree* of the extension $M|K$.

$M|K$ is *finite* if $[M : K] < \infty$.

A map from the K-extension $M|K$ to the K-extension $M'|K$ is a ring map $M \to M'$ (which is necessarily injective), which is compatible with the injections $K \hookrightarrow M$ and $K \hookrightarrow M'$.

$\mathrm{Aut}_K(M) :=$ group of bijective maps of K-extensions $M \to M$

Proposition (tower law)

If $L|M$ and $M|K$ are finite field extensions, then we have

$$[M : K] \cdot [L : M] = [L : K].$$

Proof. See Rings and Modules. $\square$

Let $M|K$ be a field extension and let $a \in M$. We define

$$\mathrm{Ann}(a) := \{P(x) \in K[x] \,|\, P(a) = 0\}$$

$\mathrm{Ann}(a) \subseteq K[x]$ is called the *annihilator* of x. It is an ideal of $K[x]$ (easy).

We say that a is *transcendental* over K if $\mathrm{Ann}(a) = (0)$.

We say that a is *algebraic* over K if $\mathrm{Ann}(a) \neq (0)$.

If a is algebraic over K, then the *minimal polynomial* m_a is by definition the unique monic polynomial, which generates $\mathrm{Ann}(a)$.

Note. If a is algebraic over K, the $\mathrm{Ann}(a)$ is a maximal ideal and m_a is irreducible.

$M|K$ is *algebraic* if for all $a \in M$, the element a is algebraic over K.

$M|K$ is *transcendental* if it is not algebraic over K.

Lemma

If $M|K$ is finite, then $M|K$ is algebraic.

Proof.

We prove the contraposition.

Let $m \in M$. Suppose that m is transcendental over K.

Then there is an injection of K-vector spaces $K[x] \hookrightarrow M$.

Since $K[x]$ is infinite dimensional, the tower law implies that $[M : K] = \infty$. $\square$

Separability

Let K be a field. Let

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0 \in K[x].$$

We define

$$P'(x) = \frac{\mathrm{d}}{\mathrm{d}x} P(x) := d a_d x^{d-1} + (d-1) a_{d-1} x^{d-2} + \cdots + a_1.$$

Here $d - i$ is understood as $1_K + \cdots + 1_K$ $((d-i)$ - times).

The operation $P(x) \mapsto P'(x)$ is a K-linear map from $K[x]$ to $K[x]$ and it satisfies the "Leibniz rule":

$$\frac{\mathrm{d}}{\mathrm{d}x}(P(x)Q(x)) = \frac{\mathrm{d}}{\mathrm{d}x}(P(x))Q(x) + P(x)\frac{\mathrm{d}}{\mathrm{d}x}Q(x)$$

(see exercises).

We say that $P(x)$ *has no multiple roots* if $(P(x), P'(x)) = (1)$.

Otherwise, we say that $P(x)$ *has multiple roots*.

Note the following fact, which justifies the terminology.

If

$$P(x) = (x - \rho_1)(x - \rho_2) \cdots (x - \rho_d)$$

then $P(x)$ has multiple roots iff there are $i, j \in \{1, \ldots, d\}$ such that $i \neq j$ and $\rho_i = \rho_j$.

See the exercises for this (use the Leibniz rule).

Let $L|K$ be a field extension. Let $P(x), Q(x) \in K[x]$.

Write $\gcd_L(P(x), Q(x))$ for the greatest common divisor of $P(x)$ and $Q(x)$ viewed as polynomials with coefficients in L.

Lemma

$$\gcd(P(x), Q(x)) = \gcd_L(P(x), Q(x)).$$

Proof. This follows from the fact that a generator of $(P(x), Q(x))$ can be computed using Euclidean division. See the notes. $\square$

Corollary (of Lemma 2)

$P(x)$ has multiple roots as a polynomial with coefficients in K

$$\Leftrightarrow$$

$P(x)$ has multiple roots as a polynomial with coefficients in L.

Proof. Apply the lemma to $Q(x) = P'(x)$. $\square$

Lemma

Let $P(x), Q(x) \in K[x]$ and suppose that $Q(x)|P(x)$. Suppose that $P(x)$ has no multiple roots. Then $Q(x)$ has no multiple roots.

Proof. Let $T(x) \in K[x]$ be st $Q(x)T(x) = P(x)$. Then by the Leibniz rule, we have

$$(P, P') = (Q'T + QT', QT) = (1)$$

If now Q and Q' were both divisible by a polynomial $W(x)$ with positive degree, then so would be $Q'T + QT'$ and QT, a contradiction. $\square$

Let K be a field.

Lemma

Suppose that $P(x) \in K[x] \backslash \{0\}$. Suppose that $\mathrm{char}(K)$ does not divide $\deg(P)$ and that $P(x)$ is irreducible. Then $(P, P') = (1)$.

Proof. Let

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$$

where $a_d \neq 0$. By definition, we have

$$P'(x) = d a_d x^{d-1} + (d-1) a_{d-1} x^{d-2} + \cdots + a_1.$$

By assumption $(d, \mathrm{char}(K)) = (1)$ and so $d \neq 0_K$ in K. Thus $P'(x) \neq 0$.

Since P is irreducible and $\deg(P') < \deg(P)$ we have $(P, P') = (1)$. $\square$

$P(x) \in K[x] \backslash \{0\}$ is *separable* if all the irreducible factors of $P(x)$ have no multiple roots.

From the above, we see that this notion is invariant under field extension.

Note that according to the last Lemma, an irreducible polynomial with coefficients in K, whose degree is prime to the characteristic of K, is separable.

In particular, if $\mathrm{char}(K) = 0$, then any irreducible polynomial with coefficients in K is separable.

Definition
Let $L|K$ be an algebraic field extension.
$L|K$ is said to be separable if the minimal polynomial over K of any element of L is separable.

Note that if K is a field and $\mathrm{char}(K) = 0$, then all the algebraic extensions of K are separable. This follows from the last remark.

Lemma
Let $M|L$ and $L|K$ be algebraic field extensions. Suppose $M|K$ is separable. Then $M|L$ are $L|K$ and both separable.

Proof. See the notes. $\square$

Example of a finite extension, which is not separable.

Let $K := \mathbb{F}_2(t)$, where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ is the field with two elements.

Let $P(x) := x^2 - t$. Since $P(x)$ is of degree 2 and has no roots in K (show this), it is irreducible.

Let $L := K[x]/(P(x))$. Since $P(x)$ is irreducible, L is a field.

On the other hand, $P'(x) = 0$ so $(P', P) = (P) \neq (1)$.

Now $P(x)$ is the minimal polynomial of

$$x \pmod{P(x)} \in K[x]/(P(x)) = L.$$

Hence the extension $L|K$ is not separable.

$\boxed{\text{end of lecture 3}}$

Simple extensions

Let $\iota : K \hookrightarrow M$ be a field extension and let $S \subseteq M$ be a subset.

We define

$$K(S) := \bigcap_{L \text{ a field}, L \subseteq M, L \supseteq S, L \supseteq \iota(K)} L$$

$K(S)$ is the *field generated by* S *over* K and the elements of S are called *generators* of $K(S)$ over K.

The field extension $M|K$ is the composition of the natural field extensions $K(S)|K$ and $M|K(S)$.

Note the following elementary fact. If $S = \{s_1, \ldots, s_k\}$, then

$$K(S) = K(s_1)(s_2)\ldots(s_k)$$

We say that $M|K$ is a *simple extension* if there is $m \in M$, such that $M = K(m)$.

Examples.

• Let $K = \mathbb{Q}$ and let $M = \mathbb{Q}(i, \sqrt{2})$ be the field generated by i and $\sqrt{2}$ in $\mathbb{C}$.

Then M is a simple algebraic extension of $K = \mathbb{Q}$, generated by $i + \sqrt{2}$.

• Let $M = \mathbb{Q}(x) = \mathrm{Frac}(\mathbb{Q}[x])$ and let $K = \mathbb{Q}$.

Then M is a simple transcendental extension of K, generated by x (note that x is transcendental over $\mathbb{Q}$).

Proposition

Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $P(x)$ be the minimal polynomial of α over K. Then there is a natural isomorphism of K-extensions

$$K[x]/(P(x)) \simeq M$$

sending x to α.

Proof. The existence of the map follows from the definitions.

Since $P(x) \neq 0$, $(P(x))$ is a maximal ideal.

Thus the image of $K[x]/(P(x))$ in M is a field.

By the definition of M, this field must be all of M. $\square$

Note. We have $[M : K] = \deg(P)$.

The proposition also shows that a finitely generated algebraic extension is finite.

The last proposition also implies the following.

Let $M = K(\alpha)|K$ be a simple algebraic extension.

Let $P(x)$ be the minimal polynomial of α over K.

Let $K \hookrightarrow L$ be an extension of fields.

Let $P(x)$ be the minimal polynomial of α over K.

Then the maps of K-extensions $M \hookrightarrow L$ are in $1-1$-correspondence with the roots of $P(x)$ in L.

Example.

Let $M := \mathbb{Q}(i) \subseteq \mathbb{C}$ and let $K = \mathbb{Q}$.

Let $L := \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$. Then there is no map of K-extensions $M \hookrightarrow L$, because the roots of $x^2 + 1$ are $\pm i$, which do not lie in $L \subseteq \mathbb{R}$.

If $L = \mathbb{C}$, and M and K are as above, then there are two maps of K-extensions $M \hookrightarrow L$, which correspond to the two roots of $x^2 + 1$ in $\mathbb{C}$.

Splitting fields

Let K be a field and let $P(x) \in K[x]$.

We say that $P(x)$ *splits* in K, if for some $c \in K$, and some sequence $\{a_i \in K\}_{i \in \{1,\dots,k\}}$, we have

$$P(x) = c \cdot \prod_{i=1}^{k} (x - a_i)$$

Example. $x^2 + 1 = (x - i)(x + i)$ splits in $\mathbb{C}$ but (famously!) not in $\mathbb{R}$.

Note. If $P(x) \in K[x]$ is irreducible and $\deg(P) > 1$ then $P(x)$ has no roots in K, and in particular $P(x)$ does not split in K.

A field extension $M|K$ is a *splitting extension* (or, less precisely, a splitting field) for $P \in K[x]$, if

(i) $P(x)$ splits in M;

(ii) M is generated over K by the roots of $P(x)$ in M.

Theorem

Let $P(x) \in K[x]$. Then

(i) There exists a field extension $M|K$, which is a splitting extension for $P(x)$.

(ii) If $L|K$ is a splitting extension for $P(x)$, then L and M are isomorphic as K-extensions.

(iii) Let $L|K$ be a splitting extension for $P(x)$ and let $J|K$ be any K-extension. Then the images of all the maps of K-extensions $L \hookrightarrow J$ coincide.

See the notes for the proof.

Note that the isomorphism announced in (ii) is not canonical.

$\boxed{\text{end of lecture 4}}$

An algebraic extension $L|K$ is *normal* if the minimal polynomial over K of any element of L splits in L.

Examples.

(1) The extension $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not normal.

Indeed, the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$. On the other hand $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ and $x^3 - 2$ has non real roots, so it does not split $\mathbb{Q}(\sqrt[3]{2})$.

(2) The extension $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is normal.

Let $a \in \mathbb{Q}(\sqrt{2})$ and let $m_a(x) \in \mathbb{Q}[x]$ be its minimal polynomial. Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, we have $\deg(m_a(x)) \leq 2$. On the other hand $m_a(x)$ has a root in $\mathbb{Q}(\sqrt{2})$, and any polynomial of degree ≤ 2, which has a root, splits. Hence $m_a(x)$ splits in $\mathbb{Q}(\sqrt{2})$.

Let $M = K(\alpha_1, \ldots, \alpha_k)|K$ be an algebraic field extension.

Let $J|K$ be an extension in which the polynomial

$$\prod_{i=1}^{k} m_{\alpha_i}(x) \in K[x]$$

splits.

Lemma (crucial!)

There is a map of K-extensions $M \to J$. Furthermore, the number of maps of K-extensions $M \to J$ is finite. Finally, if the polynomials m_{α_i} are all separable, then there are $[M : K]$ such maps.

In other words: the set of extensions of the map $K \hookrightarrow J$ to a ring map $M \hookrightarrow J$ is finite and non empty, and if all the m_{α_i} are separable, then this set has cardinality $[M : K]$.

Proof. We shall only prove the first assertion here.

By the properties of simple extensions, there is an extension of the map $K \hookrightarrow J$ to $K(\alpha_1)$.

Now note that the minimal polynomial of α_2 over $K(\alpha_1)$ divides $m_{\alpha_2}(x)$; it thus has a root in J, since $m_{\alpha_2}(x)$ splits in J.

Thus we conclude again that for any ring map $K(\alpha_1) \hookrightarrow J$, there is an extension of this map to a map

$$K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2) \hookrightarrow J.$$

Continuing this way, we see that there is an extension of the map $K \hookrightarrow J$ to a ring map $K(\alpha_1, \dots, \alpha_k) = M \hookrightarrow J$. $\square$

Theorem

A finite field extension $L|K$ is normal iff it is a splitting extension for a polynomial with coefficients in K.

Proof. Suppose that $L|K$ is finite and normal. Let $\alpha_1, \ldots, \alpha_k$ be generators for L over K (eg a K-basis). Let

$$P(x) := \prod_{i=1}^{k} m_{\alpha_i}(x)$$

where $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K.

Then, by assumption, $P(x)$ splits in L and the roots of $P(x)$ generate L, so L is a splitting field of $P(x)$.

Suppose now that L is a splitting field of a polynomial in $K[x]$.

Let $\alpha \in L$ and let $\beta_1, \dots, \beta_k \in L$ be st $L = K(\alpha, \beta_1, \dots, \beta_k)$.

Let J be a splitting field of the product of the minimal polynomials over K over the elements $\alpha, \beta_1, \dots, \beta_k$.

Now choose a root ρ in J of the minimal polynomial $Q(x)$ of α over K. By the properties of simple extensions, there is an extension of the map $K \hookrightarrow J$ to a ring map $\mu : K(\alpha) \hookrightarrow J$ such that $\mu(\alpha) = \rho$.

Notice that by the crucial Lemma there is an extension of μ to a ring map $\lambda : L \hookrightarrow J$. Now note that by the properties of splitting extensions, the image by λ of L in J is independent of λ, and thus of μ.

Hence the image by λ of L in J contains all the roots of $Q(x)$, ie $Q(x)$ splits in the image of λ. Since $Q(x)$ has coefficients in K and λ gives an isomorphism between L and the image of λ, we see that $Q(x)$ splits in L, which is what wanted to prove. $\square$

Theorem

Let $L|K$ be the splitting field of a separable polynomial over K. Then we have $\#\mathrm{Aut}_K(L) = [L : K]$.

Proof. Apply the crucial Lemma with $L = M = J$. $\square$

Theorem

Let $\iota : K \hookrightarrow L$ *be a finite field extension.*

Then $\mathrm{Aut}_K(L)$ *is finite.*

Furthermore, the following statements are equivalent:

(i) $\iota(K) = L^{\mathrm{Aut}_K(L))}$*;*

(ii) $L|K$ *is normal and separable;*

(iii) $L|K$ *is a splitting extension for a separable polynomial with coefficients in* K*.*

Proof. We shall only prove (i)⇒(ii) .

The fact that $\mathrm{Aut}_K(L)$ is finite is a consequence of the second assertion in the crucial Lemma.

Let $P(x)$ be the minimal polynomial of the element $\alpha \in L$.

We have to show that $P(x)$ splits and is separable.

Let

$$Q(x) := \prod_{\beta \in \mathrm{Orb}(\alpha, \mathrm{Aut}_K(L))} (x - \beta)$$

By construction, $Q(x)$ is separable. Let

$$d := \#\mathrm{Orb}(\alpha, \mathrm{Aut}_K(L)).$$

Let $\beta_1, \dots, \beta_d$ be the elements of $\mathrm{Orb}(\alpha, \mathrm{Aut}_K(L))$.

We have

$$Q(x) = x^d - s_1(\beta_1, \dots, \beta_d)x^{d-1} + \cdots + (-1)^d s_d(\beta_1, \dots, \beta_d)$$

Now note that for any $\gamma \in \mathrm{Aut}_K(L))$ and any $i \in \{1, \dots, d\}$, we have

$$\gamma(s_i(\beta_1, \dots, \beta_d)) = s_i(\gamma(\beta_1), \dots, \gamma(\beta_d))$$

Since s_i is a symmetric function, we have

$$s_i(\gamma(\beta_1), \dots, \gamma(\beta_d)) = s_i(\beta_1, \dots, \beta_d).$$

Since γ was arbitrary, we see that $s_i(\beta_1, \dots, \beta_d) \in L^G = \iota(K)$.

Thus $Q(x) \in \iota(K)[x]$ and (abusing language), we identify with a polynomial in $K[x]$ via ι.

On the other hand $\alpha \in \mathrm{Orb}(\alpha, \mathrm{Aut}_K(L))$ so that $Q(\alpha) = 0$.

Thus, by the definition of $P(x)$, we see that $P(x)$ divides $Q(x)$.

Hence $P(x)$ splits in L and has no multiple roots.

In particular, $P(x)$ is separable. $\square$

Corollary

Let $L|K$ be an algebraic field extension.

Suppose that L is generated by $\alpha_1, \dots, \alpha_k \in M$ and that the minimal polynomial of each α_i is separable.

Then the extension $L|K$ is separable.

Proof. According to the crucial Lemma and the existence of splitting fields, there is an extension $M|L$ st the extension $M|K$ is the splitting field of a separable polynomial.

According to the previous theorem, the extension $M|K$ is separable.

Thus the extension $L|K$ is also separable. $\square$

end of lecture 5

Galois extensions - overview

A field extension $\iota : K \hookrightarrow L$ is called a *Galois extension*, if

$$L^{\mathrm{Aut}_K(L)} = \iota(K).$$

Note. By the above, a finite field extension $L|K$ is a Galois extension iff L is the splitting field of a separable polynomial over K and iff it is normal and separable.

If $L|K$ is a Galois extension, we write

$$\mathrm{Gal}(L|K) = \Gamma(L|K) := \mathrm{Aut}_K(L)$$

and we call $\mathrm{Gal}(L|K)$ the *Galois group* of $L|K$. If $L|K$ is a finite, then this is a finite group.

Fundamental theorem of Galois theory (to be proven later in a more detailed form).

The map

$$\{\text{subfields of } L \text{ containing } \iota(K)\} \mapsto \{\text{subgroups of } \mathrm{Gal}(L|K)\}$$

given by

$$M \mapsto \mathrm{Gal}(L|M)$$

is a bijection.

Example. We shall compute the Galois group of the extension $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$.

Note that $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field of the polynomial $(x^2 - 2)(x^2 + 1)$, whose roots are $\pm\sqrt{2}, \pm i$.

Thus $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ is the splitting field of a separable polynomial, and is thus Galois.

We have successive extensions $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})|\mathbb{Q}$.

The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.

Similarly, the polynomial $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$.

Thus we conclude that

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

By the theorem above, we thus have

$$\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}) = 4.$$

Let $G := \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q})$.

From the classification of finite groups, we conclude that G is abelian.

Thus we either have $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G = \mathbb{Z}/4\mathbb{Z}$.

Now note that we have $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i)) = 2$.

Similarly, $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})) = 2$.

Thus

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i)) \simeq \mathbb{Z}/2\mathbb{Z}$$

and

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})) \simeq \mathbb{Z}/2\mathbb{Z}.$$

By the fundamental theorem of Galois theory, the subgroups $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})) \subseteq G$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i)) \subseteq G$ cannot coincide, because they correspond to different subfields of $\mathbb{Q}(\sqrt{2}, i)$.

Thus we conclude that G has two distinct subgroups of order 2, and hence we must have $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Examples of field extensions, which are not Galois.

(i) We saw that $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not a normal extension. Thus it is not Galois.

(ii) Consider the extension $\mathbb{F}_2(t)[x]/(x^2 - t)|\mathbb{F}_2(t)$. We saw that this extension is not separable. Thus it is not Galois.

$\boxed{\text{end of lecture 6}}$

The following basic statement is the linchpin of the whole theory.

Theorem (Artin's lemma)

Let K be a field and let $G \subseteq \mathrm{Aut}_{\mathrm{Rings}}(K)$ be a finite subgroup.

Then the extension $K|K^G$ is a finite Galois extension, and the inclusion $G \hookrightarrow \mathrm{Aut}_{K^G}(K)$ is an isomorphism of groups.

We will sketch the proof. We will need the

Lemma

Let K be a field and let $G \subseteq \mathrm{Aut}_{\mathrm{Rings}}(K)$ be a finite subgroup. Then $[K : K^G] \leq \#G$.

Proof. See the notes. The proof is by linear algebra. $\square$

We are now in a position to prove Artin's lemma. We shall first prove that
$$K^G = (K)^{\mathrm{Aut}_{K^G}(K)}.$$
By definition, we have
$$K^G \subseteq (K)^{\mathrm{Aut}_{K^G}(K)}$$
and
$$G \subseteq \mathrm{Aut}_{K^G}(K),$$
so that $K^G \supseteq (K)^{\mathrm{Aut}_{K^G}(K)}$.

We conclude that $K^G = (K)^{\mathrm{Aut}_{K^G}(K)}$, as required.

Now, *since* $K|K^G$ *is a finite extension* by the last lemma, we conclude that $K|K^G$ is a splitting extension of a separable polynomial with coefficients in K^G.

We may thus conclude that

$$[K : K^G] = \#\mathrm{Aut}_{K^G}(K).$$

On the other hand, we know from the last lemma that $[K : K^G] \leq \#G$, so that $\#\mathrm{Aut}_{K^G}(K) \leq \#G$.

Since $G \subseteq \mathrm{Aut}_{K^G}(K)$, we also have $\#G \leq \#\mathrm{Aut}_{K^G}(K)$, and we conclude that $\#G = \#\mathrm{Aut}_{K^G}(K)$.

This implies that $G = \mathrm{Aut}_{K^G}(K)$.

We conclude that $K|K^G$ is a finite Galois extension with Galois group G. $\square$

end of lecture 7

The fundamental theorem of Galois theory

Let $\iota : K \hookrightarrow L$ be a field extension.

We shall call a subfield of L containing $\iota(K)$ an *intermediate field*.

(i) The map

$$\{\text{subfields of } L \text{ containing } \iota(K)\} \mapsto \{\text{subgroups of } \mathrm{Gal}(L|K)\}$$

given by

$$M \mapsto \mathrm{Gal}(L|M)$$

is a bijection. Its inverse is given by the map

$$H \mapsto L^H.$$

(where H is a subgroup of $\mathrm{Gal}(L|K)$).

We shall write $G_M := \mathrm{Gal}(L|M)$.

(ii) Let M be a subfield of L containing $\iota(K)$. We have

$$[L : M] = \#G_M$$

and

$$[M : K] = \frac{\#\mathrm{Gal}(L|K)}{\#G_M}.$$

(iii) Let M be a subfield of L containing $\iota(K)$.

Then $M|K$ is a Galois extension iff the group G_M is a normal subgroup of $\mathrm{Gal}(L|K)$.

If that is the case, there is an isomorphism

$$I_M : \mathrm{Gal}(L|K)/G_M \simeq \mathrm{Gal}(M|K),$$

which is uniquely determined by the fact that

$$I_M(\gamma \pmod{G_M}) = \gamma|_M$$

for any $\gamma \in \mathrm{Gal}(L|K)$.

Here $\gamma|_M$ is the restriction of γ to M and it is part of the statement that $\gamma(M) = M$.

For the proof of the fundamental theorem of Galois theory, see the notes.

Corollary

Let $\iota : K \hookrightarrow L$ be a finite separable extension.

Then there are only finitely many intermediate fields between L and $\iota(K)$.

Proof. We may wrog replace L by one of its extensions.

By the crucial lemma, we may thus suppose that the extension $L|K$ is a Galois extension.

In that case, the statement is a consequence of (i) above and the fact that $\mathrm{Gal}(L|M)$ is finite (and thus has finitely many subgroups).

$\boxed{\text{end of lecture 8}}$

We record the following important lemma.

Lemma

Let $L|K$ be a finite Galois extension. Let $\alpha \in L$.

Then the minimal polynomial of α over K is the polynomial

$$\prod_{\beta \in \mathrm{Orb}(\alpha, \mathrm{Gal}(L|K))} (x - \beta)$$

We shall go through the proof in the next slides.

Let $P(x) = \prod_{\beta \in \mathrm{Orb}(\alpha, \mathrm{Gal}(L|K))} (x - \beta)$.

Let $m_\alpha(x) \in K$ be the minimal polynomials of α over K. We saw above that $P(x) \in K[x]$.

Thus, by the definition of the minimal polynomial, we have

$$m_\alpha(x) | P(x).$$

So we only need to prove that $P(x)$ is irreducible over K.

Suppose for contradiction that $P(x)$ is not irreducible and let

$$P(x) = Q(x)T(x),$$

where $Q(x), T(x) \in K[x]$ and $\deg(Q), \deg(T) > 1$.

Note that if $\rho \in L$ and $Q(\rho) = 0$, then for any $\gamma \in \mathrm{Gal}(L|K)$, we have

$$\gamma(Q(\rho)) = Q(\gamma(\rho)) = \gamma(0) = 0$$

and thus the roots of $Q(x)$ in L are stable under the action of $\mathrm{Gal}(L|K)$.

Now note that $Q(x)$ has a root in L, since $P(x)$ splits in L and $Q(x)|P(x)$.

Thus the set of the roots of $P(x)$ contains a subset, which is stable under $\mathrm{Gal}(L|K)$ and has cardinality strictly smaller than $\deg(P(x)) = \#\mathrm{Orb}(\alpha, \mathrm{Gal}(L|K))$.

This contradicts the fact that the set of roots of $P(x)$ is the orbit of α under $\mathrm{Gal}(L|K)$.

Let $n \geq 1$. A finite subgroup G of S_n is called *transitive* if it has only one orbit in $\{1, \dots, n\}$.

Lemma (proven in the notes)

Let K be a field and let $P(x) \in K[x]$. Let $L|K$ be a splitting extension of $P(x)$ and let $\alpha_1, \dots, \alpha_n \in L$ be the roots of $P(x)$, with multiplicities.

(1) Suppose that $P(x)$ has no repeated roots. Let $\phi : \mathrm{Aut}_K(L) \to S_n$ be the map st $\gamma(\alpha_i) = \alpha_{\phi(\gamma)(i)}$ for all $i \in \{1, \dots, n\}$. Then ϕ is an injective group homomorphism.

(2) If $P(x)$ is irreducible over K and has no repeated roots, then the image of ϕ is a transitive subgroup of S_n.

(3) The element $\Delta_P := \Delta(\alpha_1, \dots, \alpha_n)$ lies in K and depends only on $P(x)$.

(4) Suppose that $\mathrm{char}(K) \neq 2$. Suppose that $P(x)$ has no repeated roots. Then the image of ϕ lies inside $A_n \subseteq S_n$ iff $\Delta_P \in (K^*)^2$.

Example. In the first exercise sheet, it is shown that

$$\Delta(x_1, x_2, x_3) = -4s_1^3 s_3 + s_1^2 s_2^2 + 18 s_1 s_2 s_3 - 4s_2^3 - 27 s_3^2$$

(where the s_i are the symmetric functions in 3 variables).

Now let $P(x) = x^3 - x - \frac{1}{3} \in \mathbb{Q}[x]$.

The polynomial $P(x)$ has no roots in $\mathbb{Q}$ (exercise) and it thus irreducible over $\mathbb{Q}$.

In particular, it has no multiple roots, since $\mathrm{char}(\mathbb{Q}) = 0$.

Let $L|\mathbb{Q}$ be a splitting field for $P(x)$ and let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $P(x)$ in L.

We have

$$s_3(\alpha_1, \alpha_2, \alpha_3) = -1/3,$$

$$s_2(\alpha_1, \alpha_2, \alpha_3) = -1$$

and

$$s_1(\alpha_1, \alpha_2, \alpha_3) = 0.$$

In particular,

$$\Delta_P = -4s_2(\alpha_1, \alpha_2, \alpha_3)^3 - 27s_3(\alpha_1, \alpha_2, \alpha_3)^2 = 4 - \frac{27}{9} = 1$$

Thus $\Delta_P \in (\mathbb{Q}^*)^2$.

We conclude from the lemma above that $\mathrm{Gal}(L|\mathbb{Q})$ can be realised as a subgroup of A_3.

We know that $\mathrm{Gal}(L|\mathbb{Q})$ has at least order 3 because the extension $K(\alpha_i)|\mathbb{Q}$ has degree 3 for any α_i.

Since $\# A_3 = 3$, we conclude that $\mathrm{Gal}(L|\mathbb{Q}) \simeq A_3$.

Theorem

Let $L|K$ be a finite separable extension of fields. Then there is an element $\alpha \in L$ st $L = K(\alpha)$.

Proof. We suppose that K is an infinite field.

The case of a finite field is treated in the exercises.

Since L is a finite extension of K, L is generated over K by a finite number of elements.

By induction on the number of generators, it will be sufficient to prove that L is generated by one element if it is generated by two elements.

So suppose that $L = K(\beta, \gamma)$.

For $d \in K$, we consider the intermediate field $K(\beta + d\gamma)$.

By the corollary above, there are only finitely many intermediate fields.

Since K is infinite, we may thus find $d_1, d_2 \in K$ such that $d_1 \neq d_2$ and $K(\beta + d_1\gamma) = K(\beta + d_2\gamma)$.

There is thus $P(x) \in K[x]$ st $\beta + d_1\gamma = P(\beta + d_2\gamma)$.

Thus we have

$$\gamma = \frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}$$

and

$$\beta = (\beta + d_2\gamma) - d_2 \frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}$$

and in particular

$$K(\beta, \gamma) = K(\beta + d_2\gamma).$$

□

end of lecture 9

Cyclotomic extensions

Let $n \geq 1$. For any field E, define

$$\mu_n(E) := \{\rho \in E \mid \rho^n = 1\}.$$

Note that the set $\mu_n(E)$ inherits a group structure from E^*.

The elements of $\mu_n(E)$ are called the *n-th roots of unity* (in E).

Lemma

The group $\mu_n(E)$ is a finite cyclic group.

Proof. Exercise. $\square$

We shall call an element $\omega \in \mu_n(E)$ a *primitive* n-th root of unity if it is a generator of $\mu_n(E)$.

Note that if ω is a primitive n-th root of unity, then all the other primitive n-th roots of unity are of the form ω^k, where k is an integer prime to $\#\mu_n(E)$.

We will also need the

Lemma

Let G be a finite cyclic group.

Write the group law of G multiplicatively.

Let $k := \#G$.

Let $I : (\mathbb{Z}/k\mathbb{Z})^* \to \mathrm{Aut}_{\mathrm{Groups}}(G)$ be the map given by the formula

$$I(a \pmod k)(\gamma) = \gamma^a$$

for any $a \in \mathbb{Z}$ and $\gamma \in G$.

Then I is an isomorphism.

Proof. Exercise. $\square$

Let now K be a field and suppose that $(n, \mathrm{char}(K)) = (1)$.

Let L be a splitting field for the polynomial $x^n - 1 \in K[x]$.

Note that $x^n - 1$ has no repeated roots, because

$$\frac{\mathrm{d}}{\mathrm{d}x}(x^n - 1) = nx^{n-1} \neq 0.$$

Thus $\#\mu_n(L) = n$ and $L|K$ is a Galois extension.

In particular, since $\mu_n(L) \simeq \mathbb{Z}/n\mathbb{Z}$ by the lemma above, we see that there are $\#(\mathbb{Z}/n\mathbb{Z})^* = \Phi(n)$ primitive n-th roots of unity in L.

Here $\Phi(\bullet)$ is Euler's totient function.

Let

$$\Phi_{n,K}(x) := \prod_{\omega \in \mu_n(E),\, \omega \text{ primitive}} (x - \omega)$$

Note that $\deg(\Phi_{n,K}(x)) = \Phi(n)$.

Lemma

The polynomial $\Phi_{n,K}(x)$ has coefficients in K and depends only on n and K.

Proof. The coefficients of $\Phi_{n,K}(x)$ are symmetric functions in the primitive $n-$th roots.

Since the primitive n-roots are permuted by $\mathrm{Gal}(L|K)$, the coefficients are thus invariant under $\mathrm{Gal}(L|K)$, and thus lies in K.

The polynomial $\Phi_{n,K}(x) \in K[x]$ only depends on n and K, because all the splitting K-extensions for $x^n - 1$ are isomorphic. $\square$

Proposition

(i) There is a natural injection of groups

$$\phi : \mathrm{Gal}(L|K) \hookrightarrow \mathrm{Aut}_{\mathrm{Groups}}(\mu_n(L)).$$

(ii) The map ϕ is surjective iff $\Phi_{n,K}(x)$ is irreducible over K.

Proof. (i) is clear, since $\mu_n(L)$ generates L and $\mathrm{Gal}(L|K)$ acts on L by ring automorphisms.

(ii) Let $\omega \in \mu_n(L)$ be a primitive n-th root of unity.

Suppose that $\Phi_{n,K}(x)$ is irreducible over K.

Since $\Phi_{n,K}(x)$ annihilates ω, it must be the minimal polynomial of ω.

Hence $[L : K] \geq \Phi(n)$, and thus we have $\#\mathrm{Gal}(L|K) \geq \Phi(n)$.

On the other hand $\#\mathrm{Gal}(L|K) \leq \Phi(n)$ by (i) and the lemma above.

Hence $\#\mathrm{Gal}(L|K) = \Phi(n)$ and we may conclude from (i) that ϕ is surjective.

Now suppose that ϕ is surjective.

Then the minimal polynomial of ω is $\Phi_{n,K}(x)$ by the lemma above and the lemma after the fundamental theorem. $\square$

We also record the following important result.

Proposition

The polynomial $\Phi_{n,\mathbb{Q}}(x)$ *is irreducible and has coefficients in* $\mathbb{Z}$.

Proof. See the notes. Uses reduction modulo p. $\square$

$\boxed{\text{end of lecture 10}}$

Kummer extensions

Let K be a field and let n be a positive integer with $(n, \mathrm{char}(K)) = (1)$. Suppose that $x^n - 1$ splits in K.

Let $a \in K$ and let $M|K$ be a splitting extension for the polynomial $x^n - a$.

Note that $\frac{\mathrm{d}}{\mathrm{d}x}(x^n - a) = nx^{n-1}$. Since $(x^n - a, nx^{n-1}) = (1)$, we see that $x^n - a$ is a separable polynomial.

Hence $M|K$ is a Galois extension.

Such an extension is called a *Kummer* extension.

Lemma

Let $\rho \in L$ be st that $\rho^n = a$.

There is a unique group homomorphism

$$\phi : \mathrm{Gal}(M|K) \to \mu_n(K)$$

st that

$$\phi(\gamma) = \gamma(\rho)/\rho.$$

This map does not depend on the choice of ρ and it is injective.

Proof. Elementary. See the notes. $\square$

Note also that a Kummer extension $M|K$ as above is a simple extension, generated by any root of $x^n - a$.

The following theorem is a kind of converse to the previous Lemma.

Theorem. *Let K be a field and let n be a positive integer with $(n, \mathrm{char}(K)) = (1)$.*

Suppose that $x^n - 1$ splits in K.

Suppose that $L|K$ is a Galois extension and that $\mathrm{Gal}(L|K)$ is a cyclic group of order n.

Let $\sigma \in \mathrm{Gal}(L|K)$ be a generator of $\mathrm{Gal}(L|K)$ and let $\omega \in K$ is a primitive n-th root of unity in K.

For any $\alpha \in L$ let

$$\beta(\alpha) := \alpha + \omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) + \cdots + \omega^{n-1}\sigma^{n-1}(\alpha).$$

Then:

- *for any $\alpha \in L$, we have $\beta(\alpha)^n \in K$;*
- *if $\beta(\alpha) \neq 0$, then $L = K(\beta)$ (so that L is the splitting field of $x^n - \beta(\alpha)^n$);*
- *there is an $\alpha \in L$, such that $\beta(\alpha) \neq 0$.*

For the proof, we shall need a general result on characters of groups with values in multiplicative groups of fields.

Let E be a field. Let H be a group (not necessarily finite). A *character* of H is a group homomorphism $H \to E^*$.

Proposition (Dedekind)

Let $\chi_1, \ldots, \chi_k$ be distinct characters of H with values in E^*.

Let $a_1, \ldots, a_k \in E$ and suppose that

$$a_1\chi_1(h) + \cdots + a_k\chi_k(h) = 0$$

for all $h \in H$. Then $a_1 = a_2 = \cdots = a_k = 0$.

Proof. By induction on k. See the notes. $\square$

Proof. (of the Theorem). Let $\alpha \in L$. We compute

$$\begin{aligned} & \sigma(\beta(\alpha)) \\ = \;& \sigma(\alpha) + \omega\sigma^2(\alpha) + \omega^2\sigma^3(\alpha) + \cdots + \omega^{n-1}\alpha \\ = \;& \omega^{n-1}\beta(\alpha) = \omega^{-1}\beta(\alpha). \end{aligned}$$

We deduce from this that for any integer i, we have

$$\sigma^i(\beta(\alpha)) = \omega^{-i}\beta(\alpha).$$

Furthermore, we then have

$$\sigma(\beta(\alpha)^n) = \sigma(\beta(\alpha))^n = \omega^{-n}\beta(\alpha)^n = \beta(\alpha)^n$$

and thus $\beta(\alpha)^n \in K$.

Now note that any element of $\mathrm{Gal}(L|K)$ defines a character on L^* with values in L^*.

We conclude from Dedekind's lemma that that there is $\alpha \in L^*$ st $\beta(\alpha) \neq 0$.

Suppose that $\alpha \in L^*$ and that $\beta(\alpha) \neq 0$ from now on.

Let $a := \beta^n$. Since the $\omega^{-i}\beta$ are all roots of $x^n - a$, we have shown that $x^n - a$ splits in L.

Furthermore, we have shown above that $\mathrm{Gal}(L|K)$ acts faithfully and transitively on the roots of $x^n - a$.

Thus $x^n - a$ is irreducible over K.

Hence $[K(\beta) : K] = n = [L : K]$.

Thus $L = K(\beta)$ and L is a splitting field for $x^n - a$. $\square$

end of lecture 11

Definition. *Let G be a group.*

A finite filtration of G is finite ascending sequence $G_\bullet$ of subgroups

$$0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that G_i is normal in G_{i+1} for all $i \in \{0, \ldots, n-1\}$.

The number n is called the length of the finite filtration.

The finite filtration $G_\bullet$ is said to have no redundancies if $G_i \neq G_{i+1}$ for all $i \in \{0, \ldots, n-1\}$.

The finite filtration $G_\bullet$ is said to have abelian quotients if the quotient group G_{i+1}/G_i is an abelian group for all $i \in \{0, \ldots, n-1\}$.

Finally, the finite filtration $G_\bullet$ is said to be trivial if $n = 1$.

Note that that (trivially...) the trivial filtration always exists and is unique.

Definition

A group is said to be solvable if there exists a finite filtration with abelian quotients on G.

Recall also that a group G is *simple* if it has no non trivial normal subgroups.

Lemma

Let G be a solvable group and let H be a subgroup. Then H is solvable. If H is normal in G, then the quotient group G/H is also solvable.

Proof. See the notes. $\square$

Definition

The length $\mathrm{length}(G)$ *of a finite group* G *is the quantity*

$$\sup\{n \in \mathbb{N} \mid n \textit{ is the length of a finite filtration with no redundancies of } G\}$$

Note that the length of a finite group is necessarily finite, because the length cannot be larger than $\#G$.

Lemma

Suppose that G *is a finite solvable group and let* $G_\bullet$ *be finite filtration with no redundancies of length* $\mathrm{length}(G)$ *on* G.

Then for all $i \in \{0, \ldots, \mathrm{length}(G) - 1\}$, *the group* G_{i+1}/G_i *is a cyclic group of prime order.*

Proof. See the notes. $\square$

Examples.

- abelian groups are solvable (by definition);

- the group S_3 is solvable. The ascending sequence

$$0 \subseteq A_3 \subseteq S_3$$

is a finite filtration of S_3, with quotients $A_3/0 \simeq A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$.

- the group S_4 is also solvable but the groups A_5 and S_5 are not solvable. The group A_5 is in fact simple and non abelian (and thus only has a trivial finite filtration). By the above, this implies that S_n is not solvable for all $n \geq 5$.

$\boxed{\text{end of lecture 12}}$

Solvability by radicals

Let $L|K$ be a finite field extension.

Definition

The extension $L|K$ is said to be radical if $L = K(\alpha_1, \ldots, \alpha_k)$ and there are natural numbers $n_1, \ldots, n_k$ such that $\alpha_1^{n_1} \in K$, $\alpha_2^{n_2} \in K(\alpha_1)$, $\alpha_3^{n_3} \in K(\alpha_1, \alpha_2)$, $\ldots$, $\alpha_k^{n_k} \in K(\alpha_1, \ldots, \alpha_{k-1})$.

We see from the definition that if $L|K$ and $M|L$ are radical extensions, then $M|K$ is a radical extension.

Example. Kummer extensions are radical. This fact will play an essential role below.

Theorem. *Suppose that* $\mathrm{char}(K) = 0$.

Let $L|K$ *be a finite Galois extension.*

(a) *If* $\mathrm{Gal}(L|K)$ *is solvable then there exists a finite extension* $M|L$ *with the following properties.*

(1) The composed extension $M|K$ *is Galois.*

(2) There is a map of K*-extensions* $K(\mu_{[L:K]}) \hookrightarrow M$.

(3) M *is generated by the images of* L *and* $K(\mu_{[L:K]})$ *in* M.

(4) The extension $M|K(\mu_{[L:K]})$ *is a composition of Kummer extensions. In particular* $M|K$ *is a radical extension.*

(b) *Conversely, if there exists a finite extension* $M|L$ *such that the composed extension* $M|K$ *is radical, then* $\mathrm{Gal}(L|K)$ *is solvable.*

Proof. We shall outline the proof of (a). For the proof of (b), see the notes. Let $d := [L : K]$.

First note that there exists a Galois extension of K and maps of K-extensions $K(\mu_d) \hookrightarrow J$ and $L \hookrightarrow J$.

This follows from the existence of splitting extensions and the crucial Lemma.

Let P be the field generated by L and $K(\mu_d)$ in J.

By construction, we then have the following diagram of field extensions:

$$\begin{tikzcd}
 & P & \\
L \arrow[ur] & & K(\mu_d) \arrow[ul] \\
 & K \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Now note that the extension $P|K(\mu_d)$ is Galois and that the restriction map $\mathrm{Gal}(P|K(\mu_d)) \to \mathrm{Gal}(L|K)$ is injective.

Indeed if $\sigma \in \mathrm{Gal}(P|K(\mu_d))$ restricts to Id_L on L, then σ fixes $K(\mu_d)$ and L. Thus σ must fix all of P, since P is generated by L and $K(\mu_d)$ over K.

We now prove (a). Suppose that $\mathrm{Gal}(L|K)$ is solvable. We conclude from the above that $\mathrm{Gal}(P|K(\mu_d))$ is solvable.

In other words, there is a finite filtration with abelian quotients

$$0 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = \mathrm{Gal}(P|K(\mu_d)).$$

By the above, we may assume that the quotients of this filtration are cyclic.

By the fundamental theorem of Galois theory, the subgroups H_i correspond to a decreasing sequence of subfields of P

$$P = P_n \supseteq P_{n-1} \supseteq \cdots \supseteq P_1 \supseteq P_0 = K(\mu_d)$$

such that $P_{i+1}|P_i$ is a Galois extension for any $i \in \{0, \dots, n-1\}$.

Furthermore, we then have $\mathrm{Gal}(P_{i+1}|P_i) \simeq H_{i+1}/H_i$ so that $\mathrm{Gal}(P_{i+1}|P_i)$ is cyclic.

Now note that by Lagrange's theorem, $\#(H_{i+1}/H_i)$ is a divisor of $\#\mathrm{Gal}(P|K(\mu_d))$, and thus of $\#\mathrm{Gal}(L|K) = d$.

Thus the polynomial $x^{\#\mathrm{Gal}(P_{i+1}|P_i)} - 1$ splits in $K(\mu_d)$.

By Kummer theory, this implies that $P_{i+1}|P_i$ is a Kummer extension, and so in particular a radical extension.

We conclude from this that $P|K(\mu_d)$ is a radical extension.

Also, note that $K(\mu_d)|K$ is clearly a radical extension.

Thus $P|K$ is a radical extension, being a composition of radical extensions. $\square$

Corollary

Let $n \geq 5$ and let K is a field. The extension

$$K(x_1 \dots, x_n)|K(x_1 \dots, x_n)^{S_n}$$

is not radical.

Here we consider the action of S_n on $K(x_1 \dots, x_n)$, which is the action induced by the action of S_n on $K[x_1 \dots, x_n]$.

Proof. Note that the extension $K(x_1 \dots, x_n)|K(x_1 \dots, x_n)^{S_n}$ is a Galois extension by Artin's lemma.

On the other hand, we saw that the group S_n is not solvable for $n \geq 5$.

By the previous theorem, the extension cannot be radical. $\square$

$\boxed{\text{end of lecture 13}}$

The solution of the general cubical equation

We shall now illustrate the previous Theorem in a specific situation.

Let K be a field and suppose that $\mathrm{char}(K) = 0$. We wish to solve the cubical equation

$$y^3 + ay^2 + by + c = 0$$

where $a, b, c \in K$. Letting $x = y + \frac{a}{3}$, we obtain the equivalent equation

$$x^3 + px + q = 0 \tag{1}$$

where

$$p = -\frac{1}{3}a^2 + b$$

and

$$q = \frac{2}{27}a^3 - \frac{1}{3}ab + c.$$

Let $P(x) := x^3 + px + q$.

We want to find a formula for the roots of $P(x)$ in terms of the elements p, q, which arises as an iteration of the following operations:

- multiplication by an element of K

- multiplication, addition

- extraction of 2nd and 3rd roots (ie $\sqrt{\bullet}$ and $\sqrt[3]{\bullet}$).

Let $L|K$ be a splitting extension for $P(x)$.

Let $\omega \in K(\mu_3)$ be a primitive 3rd root of unity.

By the crucial lemma and the existence of splitting extensions there is a finite Galois extension $J|K$ and maps of K-extensions $L \hookrightarrow J$ and $K(\mu_3) = K(\omega) \hookrightarrow J$.

Let $M = L(\omega)$ be the field generated in J by the images of L and $K(\omega)$ in J.

The situation is summarised by the following commutative diagram of field extensions

$$\begin{tikzcd} & M & \\ L \arrow[ur] & & K(\mu_3) \arrow[ul] \\ & K \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Now $\mathrm{Gal}(L|K)$ is a solvable (because it can be realised as a subgroup of S_3) and as before we see that $M|K$ is radical.

The calculations below exploit (and reprove) precisely this fact.

Consider the sequence of extensions

$$K \hookrightarrow K(\omega) \hookrightarrow K(\omega, \sqrt{\Delta_P}) \hookrightarrow M.$$

Note that $[K(\omega) : K] \leq 2$ and that $[K(\omega, \sqrt{\Delta_P}) : K(\omega)] \leq 2$.

Note also that M is a splitting field of $P(x)$ over $K(\omega, \sqrt{\Delta_P})$.

Thus we see that $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P}))$ can be realised as a subgroup of $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$.

We conclude that either $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P}))$ is the trivial group or

$$\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P})) \simeq \mathbb{Z}/3\mathbb{Z}.$$

Let now $\alpha_1, \alpha_2, \alpha_3 \in L$ be the three roots of $P(x)$, with multiplicities. Let

$$\beta := \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \in M$$

and

$$\gamma := \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 \in M.$$

Note that

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

In particular, we have

$$\alpha_1 := \frac{1}{3}(\beta + \gamma),$$

$$\alpha_2 = \frac{1}{3}(\omega^2\beta + \omega\gamma)$$

and

$$\alpha_3 = \frac{1}{3}(\omega\beta + \omega^2\gamma).$$

Now we claim that β^3 and γ^3 lie in $K(\omega, \sqrt{\Delta_P})$.

If $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P}))$ is the trivial group, then $M = K(\omega, \sqrt{\Delta_P})$ and then the claim holds tautologically.

If $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P})) \simeq \mathbb{Z}/3\mathbb{Z}$, then the claim follows from Kummer theory.

So we see that the minimal polynomials of β^3 and γ^3 over $K(\omega)$ are of degree ≤ 2.

We may thus express α_1, α_2 and α_3 by a formula involving only multiplications, additions and extractions of 2nd and 3rd roots.

We make this explicit.

Using the fact that $1 + \omega + \omega^2 = 0$, we compute

$$\begin{aligned} \beta\gamma &= (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3) \\ &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3. \end{aligned}$$

Note also that

$$0 = (\alpha_1 + \alpha_2 + \alpha_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2\alpha_1\alpha_2 + 2\alpha_1\alpha_3 + 2\alpha_2\alpha_3.$$

Thus

$$\beta\gamma = \beta\gamma - (\alpha_1 + \alpha_2 + \alpha_3)^2 = -3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -3p.$$

Similarly, we compute

$$\beta^3 + \gamma^3 = -27q = 27\alpha_1\alpha_2\alpha_3.$$

Thus β^3 and γ^3 are the roots of the quadratic equation

$$x^2 + 27qX - 27p^3 = 0.$$

Putting everything together, we see that the solutions of the equation

$$y^3 + ay^2 + by + c = 0$$

are (see next slide)

$$\beta_1 = \frac{1}{3}\sqrt[3]{-\frac{27}{2}q + \frac{1}{2}\sqrt{729q^2 + 108p^3}} + \frac{1}{3}\sqrt[3]{-\frac{27}{2}q - \frac{1}{2}\sqrt{729q^2 + 108p^3}} - \frac{1}{3}a$$

$$\beta_2 = \frac{\omega^2}{3}\sqrt[3]{-\frac{27}{2}q + \frac{1}{2}\sqrt{729q^2 + 108p^3}} + \frac{\omega}{3}\sqrt[3]{-\frac{27}{2}q - \frac{1}{2}\sqrt{729q^2 + 108p^3}} - \frac{1}{3}a$$

$$\beta_3 = \frac{\omega}{3}\sqrt[3]{-\frac{27}{2}q + \frac{1}{2}\sqrt{729q^2 + 108p^3}} + \frac{\omega^2}{3}\sqrt[3]{-\frac{27}{2}q - \frac{1}{2}\sqrt{729q^2 + 108p^3}} - \frac{1}{3}a$$

for <u>some</u> choices of 3rd roots of

$$-\frac{27}{2}q + \frac{1}{2}\sqrt{729q^2 + 108p^3}$$

and

$$-\frac{27}{2}q - \frac{1}{2}\sqrt{729q^2 + 108p^3}$$

(not all of them will give solutions).

$\boxed{\text{end of lecture 14}}$

Let G be a finite group.

Theorem (Sylow)

Suppose that $\#G = p^n a$, where $(a,p) = 1$, p is prime and $n \geq 0$.

Then there is a subgroup $H \subseteq G$ such that $\#H = p^n$.

Furthermore, if $H, H' \subseteq G$ are two subgroups such that $\#H = \#H' = p^n$ then there is $g \in G$ such that $g^{-1}Hg = H'$.

Corollary (Cauchy)

If p is prime and $p|\#G$, then there is an element of order p in G.

Proof. Exercise. $\square$

Let $n, k \geq 0$. Let $\sigma \in S_n$ and write $[\sigma]$ for the subgroup of σ generated by σ.

Recall that σ is is said to be a k-*cycle*, if

- $[\sigma]$ has one orbit of cardinality k in $\{1, \dots, n\}$;

- all the other orbits of $[\sigma]$ have cardinality 1.

Lemma

Let p be a prime number and let $\sigma \in S_p$.

Suppose that the order of σ is p.

Then σ is a p-cycle.

Proof. See the notes. $\square$

Proposition

Let p be a prime number.

Let $\sigma, \tau \in S_p$ and suppose that σ is a transposition and that τ is a p-cycle.

Then σ and τ generate S_p.

Proposition

Let p be a prime number and let $P(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p.

Suppose that $P(x)$ has precisely $p-2$ real roots in $\mathbb{C}$.

Then $\mathrm{Gal}(P) \simeq S_p$.

Proof. See the notes. Notice that complex conjugation provides a transposition, and apply Cauchy's theorem and the last propostion. $\square$

Corollary

The polynomial $x^5 - 6x + 3 \in \mathbb{Q}[x]$ *is not solvable by radicals.*

Proof. See the notes. This polynomial is irreducible by Eisenstein and can easily be see to have precisely three real roots. $\square$

$\boxed{\text{end of lecture 15}}$

We will now prove that $\mathbb{C}$ is algebraically closed using Galois theory and basic real analysis.

We shall need the following well-known fact.

Lemma

Let $P(x) \in \mathbb{R}[x]$ be a monic polynomial of odd degree. Then $P(x)$ has a root in $\mathbb{R}$.

Proof. well-known (or see the notes). $\square$

Theorem. *The field $\mathbb{C}$ is algebraically closed.*

Proof. Let $P(x) \in \mathbb{C}[x]$. We need to show that $P(x)$ splits.

Replacing $P(x)$ by $P(x)\bar{P}(x)$, we may even assume that the degree of $P(x)$ is even and has coefficients in $\mathbb{R}$.

Let $L|\mathbb{R}$ be a splitting field of $P(x)$. Let $G := \mathrm{Gal}(L|\mathbb{R})$. Let $G_2 \subseteq G$ be a 2-Sylow subgroup of G. Let $M = L^{G_2}$. Then $[M : \mathbb{R}]$ is odd by the definition of Sylow subgroups.

Suppose that there is $\alpha \in M \backslash \mathbb{R}$ and let $m_\alpha(x) \in \mathbb{R}[x]$ be the minimal polynomial of α.

Then $\deg(m_\alpha(x)) | [M : \mathbb{R}]$ by the tower law and thus $\deg(m_\alpha(x))$ is odd.

Thus, by the previous lemma, $m_\alpha(x)$ has a root in $\mathbb{R}$.

Since $m_\alpha(x)$ is irreducible, this means that $\deg(m_\alpha(x)) = 1$.

This contradicts the fact that $\alpha \in M \backslash \mathbb{R}$. We conclude that $M|\mathbb{R}$ is the trivial extension.

In particular $G = G_2$ is a 2-Sylow group.

Suppose that $\#G = 2^k$ for some $k \geq 0$. We may suppose wrog that $k > 0$.

Any group, whose order is a power of a prime number is solvable (see the notes). Thus there is a filtration on G, which has cyclic quotients of order 2.

As before, this gives rise to a sequence of subfields

$$L = L_n \supseteq L_{n-1} \supseteq \cdots \supseteq L_0 = \mathbb{R}$$

such that L_{i+1} is Galois over L_i for all $i \in \{0, \ldots, n-1\}$, and $\mathrm{Gal}(L_{i+1}|L_i) \simeq \mathbb{Z}/2\mathbb{Z}$.

By Kummer theory, there exists $\beta \in L_1$ such that $\beta^2 \in L_0 = \mathbb{R}$ and such that $L_1 = \mathbb{R}(\beta)$.

Since any positive element of $\mathbb{R}$ has a square root in $\mathbb{R}$, we see that $\beta^2 < 0$. Now we may compute

$$(\beta/\sqrt{|\beta^2|})^2 = \beta^2/|\beta^2| = -1.$$

Thus the polynomial $x^2 + 1 \in \mathbb{R}[x]$ has a root in L_1.

In particular, $x^2 + 1$ splits in L_1.

We conclude that L_1 is a splitting field for $x^2 + 1$.

In other words $L_1 \simeq \mathbb{C}$ as a $\mathbb{R}$-extension.

Now suppose that $k > 1$.

By a similar reasoning, there is a $\rho \in L_2$, such that $\rho^2 \in L_1 \simeq \mathbb{C}$ and such that $L_2 = L_1(\rho)$.

Furthermore $L_2 | L_1$ is a non trivial extension by assumption.

This is a contradiction, because any element of $L_1 \simeq \mathbb{C}$ has a square root (if $z = re^{i\theta}$, then $\sqrt{r}e^{i\theta/2}$ is a square root of z).

We conclude that $k = 1$ and thus $L = L_1 \simeq \mathbb{C}$. In particular, $P(x)$ splits in $\mathbb{C}$. $\square$

end of lecture 16