Introduction to Galois Theory

June 22, 2016

Contents

Requirements

0.1 Groups

Definition 0.1 (Monoid). *The set of elements M with defined binary operation $\circ$ we will call as a monoid if the following conditions are satisfied.*

1. *Closure:* $\forall a, b \in M$: $a \circ b \in G$
2. *Associativity:* $\forall a, b, c \in M$: $a \circ (b \circ c) = (a \circ b) \circ c$
3. *Identity element:* $\exists e \in M$ *such that* $\forall a \in G$: $e \circ a = a \circ e = a$

Definition 0.2 (Group). *Let we have a set of elements G with a defined binary operation $\circ$ that satisfied the following properties.*

1. *Closure:* $\forall a, b \in G$: $a \circ b \in G$
2. *Associativity:* $\forall a, b, c \in G$: $a \circ (b \circ c) = (a \circ b) \circ c$
3. *Identity element:* $\exists e \in G$ *such that* $\forall a \in G$: $e \circ a = a \circ e = a$
4. *Inverse element:* $\forall a \in G$ $\exists a^{-1} \in G$ *such that* $a \circ a^{-1} = e$

In this case $(G, \circ)$ is called as group.

Therefore the group is a Monoid with inverse element property.

Example 0.1.1 (Group $\mathbb{Z}/2\mathbb{Z}$). *Consider a set of 2 elements:* $G = \{0, 1\}$ *with the operation $\circ$ defined by the table 1.*

The identity element is 0 *i.e.* $e = 0$. *Inverse element is the element itself because* $\forall a \in G$: $a \circ a = 0 = e$.

Definition 0.3 (Cyclic group). *A cyclic group or monogenous group is a group that is generated by a single element. Note that Group $\mathbb{Z}/2\mathbb{Z}$ is a cyclic group.*

Table 1: Cayley table for $\mathbb{Z}/2\mathbb{Z}$

$\circ$	0	1
0	0	1
1	1	0

Definition 0.4 (Order of element in group)**.** *Order, sometimes period, of an element a of a group is the smallest positive integer m such that $a^m = e$ (where e denotes the identity element of the group, and am denotes the product of m copies of a). If no such m exists, a is said to have infinite order.*

Definition 0.5 (Subgroup)**.** *Let we have a Group $(G, \circ)$. The subset $S \subset G$ is called as subgroup if $(S, \circ)$ is a Group.*

Definition 0.6 (Abelian group)**.** *Let we have a Group $(G, \circ)$. The group is called an Abelian or commutative if $\forall a, b \in G$ it holds $a \circ b = b \circ a$.*

Definition 0.7 (Coset)**.** *If G is a group, and H is a subgroup of G, and g is an element of G, then*

$$gH = \{gh|h \in H\}$$

is the left coset of H in G with respect to g, and

$$Hg = \{hg|h \in H\}$$

is the right coset of H in G with respect to g.

0.1.1 Permutations

Example 0.1.2 (S_n group)**.** *If we a have a permutation of n elements then it's possible to do by means of $n!$ ways.*

S_1 permutation of 1 element consists of only one element e - the simplest possible group

S_2 permutation consists of 2 elements:

1. *identity e:*
$$\begin{array}{c} 1 \to 1 \\ 2 \to 2 \end{array}$$

2. *transposition τ:*
$$\begin{array}{c} 1 \to 2 \\ 2 \to 1 \end{array}$$

Table 2: Cayley table for S_2

$\circ$	e	τ
e	e	τ
τ	τ	e

It's easy to see that the Cayley table has the form 2

S_3 permutation consists of 6 elements: $e, \tau, \tau_1, \tau_2, \sigma, \sigma_1$. The most important are e, τ and σ and all others are represented via them.

1. *identity e:*
$$\begin{aligned} 1 &\to 1 \\ 2 &\to 2 \\ 3 &\to 3 \end{aligned}$$

2. *transposition τ:*
$$\begin{aligned} 1 &\to 2 \\ 2 &\to 1 \\ 3 &\to 3 \end{aligned}$$

3. *circle σ:*
$$\begin{aligned} 1 &\to 2 \\ 2 &\to 3 \\ 3 &\to 1 \end{aligned}$$

0.2 Rings, Ideals and Fields

Definition 0.8 (Ring). *Consider a set R with 2 binary operations defined. The first one $\oplus$ (addition) and elements of R forms an Abelian group under this operation. The second one is $\odot$ (multiplication) and the elements of R forms a Monoid under the operation. The two binary operations are connected each other via the following distributive law*

- *Left distributivity: $\forall a, b, c \in R$: $a \odot (b \oplus c) = a \odot b \oplus a \odot c$*
- *Right distributivity: $\forall a, b, c \in R$: $(a \oplus b) \odot c = a \odot c \oplus b \odot c$*

  The identity element for $(R, \oplus)$ is denoted as 0 (additive identity). The identity element for $(R, \odot)$ is denoted as 1 (multiplicative identity).

  The inverse element to a in $(R, \oplus)$ is denoted as $-a$

In this case $(R, \oplus, \odot)$ is called as ring.

The Ring is a generalization of integer numbers conception.

Example 0.2.1 (Ring of integers $\mathbb{Z}$)**.** *The set of integer numbers $\mathbb{Z}$ forms a Ring under $+$ and $\cdot$ operations i.e. addition $\oplus$ is $+$ and multiplication $\odot$ is $\cdot$. Thus for integer numbers we have the following Ring: $(\mathbb{Z}, +, \cdot)$*

Definition 0.9 (Ideal)**.** *Lets we have the Ring $(R, \oplus, \odot)$. Subset $I \subset R$ will be an ideal if it satisfied the following conditions*

1. *$(I, \oplus)$ is Subgroup of $(R, \oplus)$*
2. *$\forall i \in I$ and $\forall r \in R$: $i \odot r \in I$ and $r \odot i \in I$*

Example 0.2.2 (Ideal $2\mathbb{Z}$)**.** *Consider even numbers. They forms an Ideal in $\mathbb{Z}$. Because multiplication of any even number to any integer is an even. The ideal's symbolic name is $2\mathbb{Z}$.*

Example 0.2.3 (Ring of integers modulo n: $\mathbb{Z}/n\mathbb{Z}$)**.** *Let $n \in \mathbb{Z}$ and $n > 1$. Then $n\mathbb{Z}$ is an Ideal.*

Two integer $a, b \in \mathbb{Z}$ are said to be congruent modulo n, written

$$a \equiv b(\mod n)$$

if their difference $a - b$ is an integer multiple of n.

Thus we have a separation of set $\mathbb{Z}$ into subsets of numbers that are congruent. Each subset has the following form

$$\{r\}_n = r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}$$

, thus

$$\mathbb{Z} = \{0\}_n \cup \{1\}_n \cup \cdots \cup \{n-1\}_n .$$

Very often use the following notation

$$\bar{r} = \{r\}_n .$$

We can define the following operations

$$\bar{k} \oplus \bar{l} = \overline{k + l}$$
$$\bar{k} \odot \bar{l} = \overline{k \cdot l}$$

The Ring where the objects are defined is called as $\mathbb{Z}/n\mathbb{Z}$.

Definition 0.10 (Principal ideal)**.** *The ideal that is generated by one element a is called as principal ideal and is denoted as (a) i.e. left principal ideal: $(a) = \{ra \mid \forall r \in R\}$ and right principal ideal: $(a) = \{ar \mid \forall r \in R\}$*

Definition 0.11 (Integral domain). *In mathematics, and specifically in abstract algebra, an integral domain is a nonzero commutative Ring in which the product of any two nonzero elements is nonzero.*

Definition 0.12 (Principal ideal domain). *In abstract algebra, a principal ideal domain, or PID, is an Integral domain in which every ideal is principal, i.e., can be generated by a single element.*

Definition 0.13 (Maximal ideal). *I is a maximal ideal of a ring R if there are no other ideals contained between I and R.*

Definition 0.14 (Proper ideal). *I is a proper ideal of a ring R if $I \subsetneq R$.*

Definition 0.15 (Quotient ring). *Quotient ring is a construction where one starts with a ring R and a two-sided ideal I in R, and constructs a new ring, the quotient ring R/I, whose elements are the Cosets of I in R subject to special $+$ and $\cdot$ operations.*

Given a ring R and a two-sided ideal $I \subset R$, we may define an equivalence relation $\sim$ on R as follows: $a \sim b$ if and only if $a - b \in I$. The equivalence class of the element a in R is given by

$$[a] = a + I := \{a + r : r \in I\}.$$

This equivalence class is also sometimes written as a mod I and called the "residue class of a modulo I".

Definition 0.16 (Field). *The ring $(R, \oplus, \odot)$ is called as a field if $(R \setminus \{0\}, \odot)$ is an Abelian group.*

The inverse element to a in $(R \setminus \{0\}, \odot)$ is denoted as a^{-1}

Example 0.2.4 (Field $\mathbb{Q}$). *Note that $\mathbb{Z}$ is not a field because not for every integer number an inverse exists. But if we consider a set of fractions $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\}$ when it will be a field.*

The inverse element to a/b in $(\mathbb{Q} \setminus \{0\}, \cdot)$ will be b/a.

Definition 0.17 (Unique factorization domain). *Unique factorization domain (UFD) is a commutative ring, which is an Integral domain, and in which every non-zero non-unit element can be written as a product of prime elements (or irreducible elements), uniquely up to order and units, analogous to the fundamental theorem of arithmetic for the integers.*

0.3 Linear algebra

Definition 0.18 (Vector space). *Let F is a Field. The set V is called as vector space under F if the following conditions are satisfied*

1. *We have a binary operation $V \times V \to V$ (addition): $(x, y) \to x + y$ with the following properties:*
   (a) $x + y = y + x$
   (b) $(x + y) + z = x + (y + z)$
   (c) $\exists 0 \in V$ *such that* $\forall x \in V : x + 0 = x$
   (d) $\forall x \in V \exists - x \in V$ *such that* $x + (-x) = x - x = 0$
2. *We have a binary operation $F \times V \to V$ (scalar multiplication) with the following properties*
   (a) $1_F \cdot x = x$
   (b) $\forall a, b \in F, x \in V$: $a \cdot (b \cdot x) = (ab) \cdot x$.
   (c) $\forall a, b \in F, x \in V$: $(a + b) \cdot x = a \cdot x + b \cdot x$
   (d) $\forall a \in F, x, y \in V$: $a \cdot (x + y) = a \cdot x + a \cdot y$

Lemma 0.19 (About vector space isomorphism). *2 vector spaces L and M with same dimension $dimL = dimM$ then there exists an Isomorphism between them*

0.4 Functions

Definition 0.20 (Surjection). *The function $f : X \to Y$ is surjective (or onto) if $\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$.*

Definition 0.21 (Injection). *The function $f : X \to Y$ is injective (or one-to-one function) if $\forall x_1, x_2 \in X$, such that $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$.*

Definition 0.22 (Bijection). *The function $f : X \to Y$ is bijective (or one-to-one correspondence) if it is an Injection and a Surjection.*

Definition 0.23 (Homomorphism). *The homomorphism is a function (map) between two sets that preserves its algebraic structure. For the case of groups $(X, \circ)$ and $(Y, \odot)$ the function $f : X \to Y$ is called homomorphism if $\forall x_1, x_2 \in X$ it holds $f(x_1 \circ x_2) = f(x_1) \odot f(x_2)$.*

Definition 0.24 (Isomorphism)**.** *If a map is Bijection as well as Homomorphism when it is called as isomorphism.*

We use the following symbolic notation for isomorphism between X and Y: $X \cong Y$.

Definition 0.25 (Automorphism)**.** *Automorphism is an isomorphism from a mathematical object to itself.*

Definition 0.26 (Embedding)**.** *When some object X is said to be embedded in another object Y, the embedding is given by some injective and structure-preserving map $f : X \to Y$. The precise meaning of "structure-preserving" depends on the kind of mathematical structure of which X and Y are instances.*

The fact that a map $f : X \to Y$ is an embedding is often indicated by the use of a "hooked arrow", thus: $f : X \hookrightarrow Y$. On the other hand, this notation is sometimes reserved for inclusion maps.

0.5 Polynomial ring $K[X]$

Let we have a commutative Ring K. Lets create a new Ring B with the following infinite sets as elements:

$$f = (f_0, f_1, \dots), \; f_i \in K, \tag{1}$$

such that only finite number of elements of the sets are non zero.

We can define addition and multiplication on B as follows

$$\begin{aligned} f + g &= (f_0 + g_0, f_1 + g_1, \dots), \\ f \cdot g &= h = (h_0, h_1, \dots), \end{aligned} \tag{2}$$

where

$$h_k = \sum_{i+j=k} f_i g_j.$$

The sequences (1) forms a Ring with the following identities:

- Additive identity: $(0, 0, \dots)$
- Multiplicative identity: $(1, 0, \dots)$

The sequences $k = (k, 0, \dots)$ added and multiplied as elements of K this allows say that such elements are elements of original Ring K. Thus K is sub-ring of the new ring B.

Let

$$X = (0, 1, 0, \dots),$$
$$X^2 = (0, 0, 1, \dots)$$

thus if we have

$$f = (f_0, f_1, f_2, \dots, f_n, 0, \dots),$$

where f_n is the last non-zero element of (1), when one can get

$$f = f_0 + f_1 X + f_2 X^2 + \dots + f_n X^n.$$

Definition 0.27 (Polynomial ring). *The Ring of sequences (1) with operations defined by (2) is called as polynomial ring* $K[X]$*.*

Lemma 0.28 (Bézout's lemma). *Let a and b be nonzero integers and let d be their greatest common divisor. Then there exist integers x and y such that*

$$ax + by = d.$$

Definition 0.29 (Monic polynomial). *Monic polynomial is a univariate polynomial in which the leading coefficient (the nonzero coefficient of highest degree) is equal to 1. Therefore, a monic polynomial has the form*

$$x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$$

Theorem 0.30 (About irreducible polynomials). *Let $\pi(X)$ is an irreducible polynomial in $K[X]$ and let α be a root of $\pi(X)$ in a some larger field. $\forall h(x) \in K(X)$ if have the following statement: $h(\alpha) = 0$ if and only if $\pi(X) \mid h(X)$ in $K[X]$.*

Proof. If $h(X) = \pi(X)g(X)$ then $h(\alpha) = 0$

From other side let $\pi \nmid h$ in $K[X]$ this means that they are relatively prime in $K[X]$ and by Bézout's lemma we can get $Q, R \in K[X]$ such that

$$\pi(X)R(X) + h(X)Q(X) = 1,$$

and especially for $X = \alpha$ we will get that $0 = 1$ that is impossible. $\square$

Chapter 1

Generalities on algebraic extensions

We introduce the basic notions such as a field extension, algebraic element, minimal polynomial, finite extension, and study their very basic properties such as the multiplicativity of degree in towers.

1.1 Field extensions: examples

1.1.1 K-algebra

Definition 1.1 (K-algebra). *Let K be a field and A be a Vector space over K equipped with an additional binary operation $A \times A \to A$ that we denote as $\cdot$ here. The the A is an algebra over K if the following identities hold $\forall x, y, z \in A$ and for every elements (often called as scalar) $a, b \in K$*

- *Right distributivity:* $(x + y) \cdot z = x \cdot z + y \cdot z$
- *Left distributivity:* $z \cdot (x + y) = z \cdot x + z \cdot y$
- *Compatibility with scalars:* $(ax) \cdot (by) = (ab)(x \cdot y)$

Example 1.1.1 (Field of complex numbers $\mathbb{C}$). *The field of complex numbers $\mathbb{C}$ can be considered as a K-algebra over field of real numbers $\mathbb{R}$.*

1.1.2 Field extension

Let K and L are fields.

Definition 1.2 (Field extension). *L is an extension of K if $L \supset K$*

and another definition

Definition 1.3 (Field extension). *L is an extension of K if L is a K-algebra*

Why the 2 definitions are equivalent?

Lemma 1.4 (K-algebra and Homomorphism). *Given a K-algebra is the same as having Homomorphism $f : K \to A$ of rings.*

Proof. Really if I have a K-algebra I can define the Homomorphism $f(k) = k \cdot 1_A$, where 1_A is an identity element of A. Thus $k \cdot 1_A \in A$.

And conversely if I have the Homomorphism $f : K \to A$ I can define the K-algebra structure by setting $ka = f(k)a$ because $f(k), a \in A$ and there is a multiplication defined on A. As result I have a rule for multiplication a scalar ($k \in K$) on a vector ($a \in A$). □

Lemma 1.5 (About Homomorphism of fields). *Any Homomorphism of fields is Injection.*

Proof. Lets proof by contradiction. Really if $f(x) = f(y)$ and $x \neq y$ then

$$f(x) - f(y) = 0_A,$$
$$f(x - y) = 0_A,$$
$$f(x - y)f((x - y)^{-1}) = f\left(\frac{x - y}{x - y}\right) = f(1_K) = 1_A = 0_A$$

that is impossible. □

There are some comments on the results. We have got that a Homomorphism can be set between field K and its K-algebra. This means that K-algebra is a field. The Homomorphism is Injection therefore we can allocate a sub-field $A' \subset A$ for that we will have the Homomorphism is a Surjection and therefore we have an Isomorphism between original field K and a sub-field A'. This means that we can say that the original field K is a sub-field for the K-algebra.

Example 1.1.2 (Field extensions). *$\mathbb{C}$ is a field extension for $\mathbb{R}$. $\mathbb{R}$ is a field extension for $\mathbb{Q}$*

1.1.3 Field characteristic

If L is a field there are 2 possibilities

1. $1 + 1 + \cdots \neq 0$. In this case $\mathbb{Z} \subset L$ but $\mathbb{Z}$ is not a field therefore L is an extension of $\mathbb{Q}$. In the case $charL = 0$

2. $1 + 1 + \cdots + 1 = \sum_{i=1}^{m} 1 = 0$ for some $m \in \mathbb{Z}$. The first time when it happens is for a prime number i.e. minimal m with the property is prime. In this case $charL = p$, where $p = minm$ - the minimal m (prime) with the property. In this case $\mathbb{Z}/p\mathbb{Z} \subset L$. The $\mathbb{Z}/p\mathbb{Z}$ is a field denoted by $\mathbb{F}_p$. The L is an extension of $\mathbb{F}_p$.

No other possibilities exist. The $\mathbb{Q}$ and $\mathbb{F}_p$ are the prime fields. Any field is an extension of one of those.

1.1.4 Field $K[X]/(P)$

Let $K[X]$ Ring of polynomials. The $P \in K[X]$ is an irreducible. (P) is an Ideal formed by the polynomial. The set of residues by the polynomial forms a field that denoted by $K[X]/(P)$. How we can see it? If $Q \in K[X]$ is a polynomial that $Q \notin (P)$ when Q is prime to P. Then with Bézout's lemma we can get $\exists A, B \in K[X]$ such that

$$AP + BQ = 1,$$

or

$$BQ \equiv 1 \mod P,$$

thus B is Q^{-1} in $K[X]/(P)$.

1.2 Algebraic elements. Minimal polynomial

1.2.1 $K[X]/(P)$ field

Alternative proof that $K[X]/(P)$ is the Field. The (P) is a Maximal ideal but a quotient by a Maximal ideal is a Field.

$K[X]/(P)$ is an extension of K because it's K-algebra.

Example 1.2.1 ($\mathbb{F}_2/(x^2+x+1)$)**.** *Lets consider the following field $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ in the field polynomial $x^2 + x + 1$ is irreducible. It's very easy to verify it because $\mathbb{F}_2$ has only 2 elements that can be (possible) a root:*

$$0^2 + 0 + 1 = 1 \neq 0$$

and

$$1^2 + 1 + 1 = 1 \neq 0$$

The polynomial has the following residues: $\bar{x} = x + (x^2 + x + 1)$ *and* $\overline{x+1} = x + 1 + (x^2 + x + 1)$. *Thus the field* $\mathbb{F}_2/(x^2 + x + 1)$ *consists of 4 elements:* $\{0, 1, \bar{x}, \overline{x+1}\}$.

It's easy to see that the third element ($\bar{x}$) *is a root of* $P(x) = x^2 + x + 1$*:*

$$\bar{x}^2 + \bar{x} + 1 = P(x) + (P(x)) = (P(x)) \equiv 0 \mod P.$$

$$\bar{x}^2 + \bar{x} + 1 = \bar{0},$$

therefore

$$\bar{x}^2 = -\bar{x} - 1 = \bar{x} + 1 = \overline{x+1}.$$

This is because we are in field $\mathbb{F}_2$ *where*

$$2(x+1) \mod 2 = 0$$

and thus

$$-\bar{x} - 1 = \bar{x} + 1$$

Also

$$\overline{x+1}^2 = \bar{x},$$

and they are inverse each other

$$\overline{x+1}\bar{x} = 1,$$

1.2.2 Algebraic elements

Definition 1.6 (Algebraic element). *Let* $K \subset L$ *and* $\alpha \in L$. α *is an algebraic element if* $\exists P \in K[X]$ *such that* $P(\alpha) = 0$. *Otherwise the* α *is called transcendental.*

1.2.3 Minimal polynomial

Lemma 1.7 (About minimal polynomial existence). *If* α *is Algebraic element then* $\exists!$ *unitary polynomial* P *of minimal degree such that* $P(\alpha) = 0$. *It is irreducible.* $\forall Q$ *such that* $Q(\alpha) = 0$ *is divisible by* P

Definition 1.8 (Minimal polynomial). *Such polynomial is called minimal polynomial and denoted by* $P_{min}(\alpha, K)$.

Proof. We know that $K[X]$ is a Principal ideal domain and a polynomial $Q(\alpha) = 0$ forms an Ideal: $I\{Q \in K[X] \mid Q(\alpha) = 0\}$, so the ideal is generated by one element: $I = (P)$. This is an unique (up to constant) polynomial minimal degree in I. If P is not irreducible then $\exists Q, R \in I$ such that $P = QR$, $Q(\alpha) = 0$ or $R(\alpha) = 0$ and $degR, Q < degP$ that is in contradiction with the definition that P is a polynomial of minimal degree. □

1.3 Algebraic elements. Algebraic extensions

Definition 1.9. *Let $K \subset L$, $\alpha \in L$. The smallest sub-field contained K and α denoted by $K(\alpha)$. The smallest sub-ring contained K and α denoted by $K[\alpha]$.*

As soon as $K[\alpha]$ is a K-algebra it is a Vector space generated by $1, \alpha, \alpha^2, \dots, \alpha^n, \dots$.

Example 1.3.1 ($\mathbb{C}$)**.**

$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$$

$\mathbb{C}$ is also a Vector space generated by 1 and i: $\forall z \in \mathbb{Z}$ it holds $z = x + iy$ where $x, y \in \mathbb{R}$.

Proposition 1.10. *The following assignment are equivalent*

1. *α is algebraic over K*
2. *$K[\alpha]$ is a finite dimensional Vector space over K*
3. *$K[\alpha] = K(\alpha)$*

Proof. Lets proof that 1 implies 2. If α is algebraic over K then using lemma Minimal polynomial $\exists P_{min}(\alpha, K)$:

$$P_{min}(\alpha, K) = \alpha^d + a_{d-1}\alpha^{d-1} + a_1\alpha + a_0 = 0,$$

where $a_k \in K$. Then

$$\alpha^d = -a_{d-1}\alpha^{d-1} - a_1\alpha - a_0$$

this means that any α^n can be represented as a linear combination of finite number of powers of α i.e. $K[\alpha]$ generated by $1, \alpha, \dots, \alpha^{d-1}$ is a finite dimensional Vector space.

Lets proof that 2 implies 3. Its enough proof that $K[\alpha]$ is a field. Let $x \neq 0 \in K[\alpha]$ then lets look at an operation $x \cdot K[\alpha] \to K[\alpha]$. This is Injection because if $y, z \in K[\alpha]$ and $z \neq y$ then $x \cdot y \neq x \cdot z$. But the $K[\alpha]$

is finite dimensional Vector space and a Homomorphism between 2 vector spaces with the same dimension is Surjection thus $\exists y \in K[\alpha]$ such that $x \cdot y = 1_{K[\alpha]}$. Therefore x is invertable and $K[\alpha]$ is a Field.

Lets proof that 3 implies 1. Let $K[\alpha]$ is a Field but α is not algebraic. Thus $\forall P \in K[X]$ $P(\alpha) \neq 0$. The we have an Injection Homomorphism $f : K[X] \to K[\alpha]$ but $K[X]$ is not a field thus $K[\alpha]$ should not be a field too that is in contradiction with the initial conditions. □

Definition 1.11 (Algebraic extension). *L an extension of K is called algebraic if $\forall \alpha \in L$ - α is algebraic over K.*

Proposition 1.12. *If L is algebraic over K then any K-subalgebra of L is a Field.*

Proof. Let $L' \subset L$ a subalgebra and let $\alpha \in L'$. We want to show that α is invertable. α is algebraic therefore $\alpha \in K[\alpha] \subset L' \subset L$ and it's invertable. □

Proposition 1.13. *Let $K \subset L \subset M$. $\alpha \in M$ - algebraic over K then α algebraic over L and $P_{min}(\alpha, L)$ divides $P_{min}(\alpha, K)$.*

Proof. Its clear because $P_{min}(\alpha, K) \in L[X]$ thus $\exists P_L \in L[X]$ such that $P_L(\alpha) = 0$ i.e. α is algebraic over L.

As soon as $P_{min}(\alpha, K) \in L[X]$ then $deg P_{min}(\alpha, L) \leq P_{min}(\alpha, K)$ and as soon as $P_{min}(\alpha, K) \in (P_{min}(\alpha, L))$ then $P_{min}(\alpha, L)$ divides $P_{min}(\alpha, K)$. □

1.4 Finite extensions. Algebraicity and finiteness

Definition 1.14 (Finite extension). *L is a finite extension of K if $dim_k L < \infty$. $dim_k L$ is called as degree of L over K and is denoted by $[L : K]$*

Theorem 1.15 (The multiplicativity formula for degrees). *Let $K \subset L \subset M$. Then M is Finite extension over K if and only if M is Finite extension over L and L is Finite extension over K. In this case*

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

Proof. Let $[M : K] < \infty$ but any linear independent set of vectors $\{m_1, m_2, \ldots, m_n\}$ over L is also linear independent over K thus

$$[M : K] < \infty \Rightarrow [M : L] < \infty$$

also L is a vector sub space of M thus if $[M : K] < \infty$ then $[L : K] < \infty$.

Let $[M : L] < \infty$ and $[L : K] < \infty$ then we have the following basises

- L-basis over M: $(e_1, e_2, \dots, e_n)$
- K-basis over L: $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_d)$

Lets proof that $e_i\varepsilon_j$ forms a K-basis over M. $\forall x \in M$:

$$x = \sum_{i=1}^{n} a_i e_i,$$

where $a_i \in L$ and can be also written as

$$a_i = \sum_{j=1}^{d} b_{ij}\varepsilon_j,$$

where $b_{ij} \in K$. Thus

$$x = \sum_{i=1}^{n}\sum_{j=1}^{d} b_{ij}\varepsilon_j e_i,$$

therefore $\varepsilon_j e_i = e_i\varepsilon_j$ generates M over K. From the other side we should check that $\varepsilon_j e_i$ linear independent system of vectors. Lets

$$\sum_{i,j} c_{ij}\varepsilon_j e_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{d} c_{ij}\varepsilon_j\right) e_i,$$

then $\forall i$:

$$\sum_{j=1}^{d} c_{ij}\varepsilon_j = 0.$$

Thus $\forall i, j : c_{ik} = 0$ that finishes the proof the linear independence. The number of linear independent vectors is $n \times d$ i.e.

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

$\square$

Definition 1.16 ($K(\alpha_1, \dots, \alpha_n)$)**.** *$K(\alpha_1, \dots, \alpha_n) \subset L$ generated by $\alpha_1, \dots, \alpha_n$ is the smallest sub field of L contained K and $\alpha_i \in L$.*

Theorem 1.17 (About towers)**.** *L is finite over K if and only if L is generated by a finite number of algebraic elements over K.*

Proof. If L is finite then $\alpha_1, \ldots, \alpha_d$ is a basis. In this case $L = K[\alpha_1, \ldots, \alpha_d] = K(\alpha_1, \ldots, \alpha_d)$. Moreover each $K[\alpha_i]$ is finite dimensional thus by proposition 1.10 α_i is algebraic.

From other side if we have a finite set of algebraic elements $\alpha_1, \ldots, \alpha_d$ then $K[\alpha_1]$ is a finite dimensional Vector space over K, $K[\alpha_1, \alpha_2]$ is a finite dimensional Vector space over $K[\alpha_1]$ and so on $K[\alpha_1, \ldots, \alpha_d]$ is a finite dimensional Vector space over $K[\alpha_1, \ldots, \alpha_{d-1}]$. All elements are algebraic thus

$$K[\alpha_1, \ldots, \alpha_i] = K(\alpha_1, \ldots, \alpha_i)$$

Then using theorem 1.15 we can conclude that $K(\alpha_1, \ldots, \alpha_d)$ has finite dimension. $\square$

1.5 Algebraicity in towers. An example

Theorem 1.18. *$K \subset L \subset M$ then M Algebraic extension over K if and only if M algebraic over L and L algebraic over K.*

Proof. If $\alpha \in M$ is an Algebraic element over K then $\exists P \in K[X]$ such that $P(\alpha) = 0$ but the polynomial $P \in K[X] \subset L[X]$ thus α is algebraic over L. If $\alpha \in L \subset M$ then α is algebraic over K thus L is algebraic over K.

Let M algebraic over L and L algebraic over K and let $\alpha \in M$. We want to prove that α is algebraic over K. Lets consider $P_{min}(\alpha, L)$ the polynomial coefficients are from L and they (as soon as they count is a finite) generate a finite extension E over K thus $E(\alpha)$ is finite over E (exists a relation between powers of α) and by theorem 1.17 is finite over K thus α is algebraic over K. $\square$

Example 1.5.1 ($\mathbb{Q}$ extension)**.** *$\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$ algebraic and finite over $\mathbb{Q}$:*

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$$

Minimal polynomial

$$P_{min}\left(\sqrt[3]{2}, \mathbb{Q}\right) = x^3 - 2.$$

$\mathbb{Q}\left(\sqrt[3]{2}\right)$ is generated over $\mathbb{Q}$ by $1, \sqrt[3]{2}, \sqrt[3]{4}$ thus $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$.

But $\sqrt{3} \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$ because otherwise $\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2$ must devide $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$ that is impossible.

Therefore $x^2 - 3$ is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$ and

$$P_{min}\left(\sqrt{3}, \mathbb{Q}\left(\sqrt[3]{2}\right)\right) = x^2 - 3.$$

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 3 \cdot 2 = 6.$$

Proposition 1.19 (On dimension of extension)**.**

$$[K(\alpha) : K] = degP_{min}(\alpha, K),$$

if α is algebraic.

Proof. If $degP_{min}(\alpha, K) = d$ then $1, \alpha, \cdots, \alpha^{d-1}$ - d independent vectors and dimension $K(\alpha)$ is d. □

Proposition 1.20 (About algebraic closure)**.** *If $K \subset L$ (L extension of K). Consider*

$$L' = \{\alpha \in L \mid \alpha \text{ algebraic over } K\},$$

then L' sub-field of L and is called as algebraic closure of K in L.

Proof. We have to prove that if α, β are algebraic then $\alpha + \beta$ and $\alpha \cdot \beta$ are also algebraic. This is trivial because

$$\alpha + \beta, \alpha \cdot \beta \in K[\alpha, \beta] = K(\alpha, \beta)$$

□

1.6 A digression: Gauss lemma, Eisenstein criterion

What we have seen so far:

- K is a field, α is an Algebraic element over K if it is a root of a polynomial $P \in K[X]$.
- L is an Algebraic extension over K if $\forall \alpha \in L$: α is an algebraic over K
- L is a Finite extension over K if $dim_K L < \infty$.
- If an extension is finite then it is algebraic

- An extension is finite if and only if it is algebraic and generated by a finite number of algebraic elements (see theorem 1.17)
- $[K[\alpha] : K] = degP_{min}(\alpha, K)$ (see proposition 1.19).

How to decide that a polynomial P is irreducible over K? About polynomial $x^3 - 2$ it is easy to decide that it's irreducible over $\mathbb{Q}$, but what's about $x^{100} - 2$?

Lemma 1.21 (Gauss)**.** *Let $P \in \mathbb{Z}[X]$, i.e. a polynomial with integer coefficients, then if P decomposes over $\mathbb{Q}$ ($P = Q \cdot R, degQ, R < degP$) then it also decomposes over $\mathbb{Z}$.*

Proof. Let $P = QR$ over $\mathbb{Q}$. Then

$$Q = mQ_1, Q_1 \in \mathbb{Z}[X],$$
$$R = nR_1, R_1 \in \mathbb{Z}[X],$$

thus

$$nmP = Q_1R_1.$$

There exists p that divides mn: $p \mid mn$ thus in modulo p we have

$$0 = \overline{Q_1R_1}$$

but p is prime and the equation is in the field $\mathbb{F}_p$ thus either $\overline{Q_1} = 0$ or $\overline{R_1} = 0$. Let $\overline{Q_1} = 0$ thus p divides all coefficients in Q_1 and we can take $\frac{Q_1}{p} = Q_2 \in \mathbb{Z}[X]$. Continue for all primes in mn we can get that

$$P = Q_sR_t,$$

where $Q_s, R_t \in \mathbb{Z}[X]$. □

Example 1.6.1 (Eisenstein criterion)**.** *Lets consider the following polynomial $x^{100}-2$. It's irreducible. Lets prove it. If it reducible then $\exists Q, R \in \mathbb{Z}[X]$ such that*

$$x^{100} - 2 = QR \tag{1.1}$$

Lets consider (1.1) modulo 2. In the case we will have

$$QR \equiv x^{100} \mod 2,$$

therefore

$$Q \equiv x^k \mod 2,$$
$$R \equiv x^l \mod 2,$$

or

$$Q = x^k + \cdots + 2 \cdot m$$

and

$$R = x^l + \cdots + 2 \cdot n$$

thus

$$QR = x^{100} + 4 \cdot nm$$

that is impossible because $n, m \in \mathbb{Z}$ *and* $nm \neq -\frac{1}{2}$.

Lemma 1.22 (Eisenstein criterion)**.** *Lets* $P \in \mathbb{Z}[X]$ *and* $P = a_n X^n + a_{n-1}X^{n-1} + a_1 X + a_0$. *If* $\exists p$ *- prime such that* $p \nmid a_n$, $p \mid a_i \forall i < n$ *and* $p^2 \nmid a_0$, *then* $P \in \mathbb{Z}[X]$ *is irreducible.*

Proof. the same as for example 1.6.1. $\square$

Note: that both: Gauss and Eisenstein criterion are valid by replacing $\mathbb{Z}$ with an Unique factorization domain R and $\mathbb{Q}$ by its factorization field.

Chapter 2

Stem field, splitting field, algebraic closure

We introduce the notion of a stem field and a splitting field (of a polynomial). Using Zorn's lemma, we construct the algebraic closure of a field and deduce its unicity (up to an isomorphism) from the theorem on extension of homomorphisms.

2.1 Stem field. Some irreducibility criteria

2.1.1 Stem field

Definition 2.1 (Stem field). *Let $P \in K[X]$ is an irreducible Monic polynomial. Field extension E is a stem field of P if $\exists \alpha \in E$ - the root of polynomial P and $E = K[\alpha]$.*

Such things exist, for instance we can take $K[X]/(P)$. It is a field because P is irreducible moreover the root of the P is in the field (see example 1.2.1).

We also can say that for any stem field E:

$$K[X]/(P) \cong E.$$

We can use the following Isomorphism: $f : \forall p \in K[X]/(P) \to p(\alpha)$, there α is a root of polynomial P. To summarize we have the following

Proposition 2.2 (About stem field existence). *The stem field exist and if we have 2 stem fields E and E' which correspond 2 roots of P: $E = K[\alpha]$, $E' = K[\alpha']$ then $\exists! f : E \cong E'$ (Isomorphism of K-algebras) such that $f(\alpha) = \alpha'$.*

Proof. Existence: $K[X]/(P)$ can be took as the stem field.

Uniquest of the Isomorphism is easy because it is defined by it's value on argument α:

$$\phi : K[X]/(P) \cong_{x\to\alpha} E,$$
$$\psi : K[X]/(P) \cong_{x\to\alpha'} E',$$

thus

$$\phi^{-1} \circ \psi : E \cong_{\alpha\to\alpha'} E'.$$

□

Remark 2.3 (About stem field). *1. In particular: If a stem field contains 2 roots of P then $\exists!$ Automorphism taking one root into another.*

2. If E stem field then $[E : K] = degP$

3. If $[E : K] = degP$ and E contains a root of P then E is a stem field

4. If E is not a stem field but contains root of P then $[E : K] > degP$ (???)

2.1.2 Some irreducibility criteria

Corollary 2.4. *$P \in K[X]$ is irreducible over K if and only if it does not have a root in Field extension L of K of such that $[L : K] \leq \frac{n}{2}$, where $n = degP$.*

Proof. $\Rightarrow$: If P is not irreducible then it has a polynomial Q that divides P and $degQ \leq \frac{n}{2}$ ($P = RQ$ and if $degQ > \frac{n}{2}$ then we can take R as Q). The Stem field L for Q exists and it's degree is $degQ \leq \frac{n}{2}$. L should have root of Q (as soon as root of P) by definition.

$\Leftarrow$: If P has a root α in L then $\exists P_{min}(\alpha, K)$ with degree $\leq \frac{n}{2} < n$ (because $[L : K] \leq \frac{n}{2}$) that divides P i.e. P become reducible. □

Corollary 2.5. *$P \in K[X]$ irreducible with $degP = n$. Let L be an extension of K such that $[L : K] = m$. If $gcd(n, m) = 1$ then P is irreducible over L.*

Proof. If it is not a case and $\exists Q$ such that $Q \mid P$ in $L[X]$. Let M be a Stem field of Q over L.

So we have $K \subset L \subset M = L(\alpha)$. M is a stem field that $[M : L] = degQ = d < n$. Thus $[M : L] = md$

Lets $K(\alpha)$ is a stem field of P over K then $[K(\alpha) : K] = degP = n$.

$K(\alpha) \subseteq M$ and therefore $n \mid md$ thus using $gcd(m, n) = 1$ one can get that $n \mid d$ but this is impossible because $d < n$. □

2.2 Splitting field

Definition 2.6 (Splitting field)**.** *Let $P \in K[X]$. The splitting field of P over K is an extension L where P is split (i.e. is a product of linear factors) and roots of P generate L*

Theorem 2.7 (About splitting fields)**.**

1. *Splitting field L exists and $[L : K] \leq d!$, where $d = degP$.*

2. *If L and M are 2 splitting fields then $\exists \phi : L \cong M$ (an Isomorphism). But the Isomorphism is not necessary to be unique.*

Proof. Lets prove by induction on d. The first case ($d = 1$) is trivial the K itself is the splitting field. Now assume $d > 1$ and that the theorem is valid for any polynomial of degree $< d$ over any field K. Let Q be any irreducible factor of P. We can create a Stem field $L_1 = K(\alpha)$ for Q that will be also a Stem field for P.

Over L_1 we have $P = (x - \alpha)R$, where R is a polynomial with $degR = d - 1$. We know (see remark 2.3) that there exists a Splitting field L for R over L_1 and its degree: $[L : L_1] \leq (d-1)!$ We have $K \subset L_1 \subset L$. The L will be a splitting field for original polynomial P. Its degree (by The multiplicativity formula for degrees) is $\leq d \cdot (d-1)! = d!$.

Uniqueness: Let L and M are 2 splitting fields. Let β is a root of Q (irreducible factor of P) in M. We have 2 stem fields: $L_1 = K(\alpha)$ and $M_1 = K(\beta)$. Proposition 2.2 says as that

$$\exists \phi : L_1 = K(\alpha) \cong K(\beta) = M_1,$$

such that $\phi(\alpha) = \beta$.

Over M_1 we have $P = (x - \beta)S$, where $S = \phi(R)$ [1]

M is splitting field for S over $K(\beta) = M_1$. M is also L_1-algebra (via the Isomorphism ϕ) and as such it's a splitting field for R over L_1. As soon as $[L : L_1] = [M : M_1]$ the $M/L_1 \cong L/L_1$ because the L_1-algebras with the same dimension are isomorphic (see lemma 0.19). Therefore we have an $L_1 = K(\alpha)$ Isomorphism $L \cong M$ and therefore K Isomorphism $L \cong M$. □

Remark 2.8. *The Isomorphism is not unique. A splitting field can have many Automorphism and this is in fact the subject of Galois theory.*

[1] We have $\phi : K(\alpha) \to K(\beta)$. The $\phi : K \to K$ because $K \subset K(\alpha)$ as well as $K \subset K(\beta)$. Therefore $\phi(P) = P$ because $P \in K[X]$. Thus

$$P = (x - \beta)S = \phi(P) = \phi((x - \alpha)R) = (x - \beta)\phi(R)$$

and $S = \phi(R)$.

2.3 An example. Algebraic closure

2.3.1 An example of automorphism

Example 2.3.1 ($x^3 - 2$ over $\mathbb{Q}$)**.** *Let we have the following polynomial $x^3 - 2$ over $\mathbb{Q}$. It has the following roots: $\sqrt[3]{2}, j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$, where $j = e^{\frac{2\pi i}{3}}$. Splitting field is the following $L = \mathbb{Q}\left(\sqrt[3]{2}, j\right)$. Lets find Automorphisms of the field.*

$$\begin{tikzcd}
& \mathbb{Q}(j) \arrow[dr, "3"] & \\
\mathbb{Q} \arrow[ur, "2"] \arrow[dr, "3"'] & & \mathbb{Q}\left(\sqrt[3]{2}, j\right) = L \\
& \mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[ur, "2"'] &
\end{tikzcd}$$

As soon as L is a stem field for $\mathbb{Q}(j)$ and for $\mathbb{Q}\left(\sqrt[3]{2}\right)$ then 2 types of automorphism exist:

1. *$\mathbb{Q}\left(\sqrt[3]{2}\right)$ Automorphism. We have $x^2 + x + 1$ as $P_{min}\left(j, \mathbb{Q}\left(\sqrt[3]{2}\right)\right)$. The polynomial has 2 roots: j and j^2 and there is an Automorphism that exchanges the root. Lets call it τ*

2. *$\mathbb{Q}(j)$ Automorphism. In this case the automorphism of exchanging $\sqrt[3]{2}$ and $j\sqrt[3]{2}$. [2]. Lets call it σ*

The group of automorphism of L $Aut(L/K)$ is embedded into permutation group of 3 elements S_3 (see example 0.1.2):

$$Aut(L/K) \hookrightarrow S_3.$$

It's embedded because the automorphism exchanges the roots of $x^3 - 2$. Moreover

$$Aut(L/K) = S_3,$$

because σ and τ generates S_3 because

- *σ: $\sqrt[3]{2} \to j\sqrt[3]{2} \to j^2\sqrt[3]{2} \to \sqrt[3]{2}$. This is a circle.*

[2] ??? The minimal polynomial is $x^3 - 2$ there and thus we have 3 roots: $\sqrt[3]{2}$, $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$

- τ - *it keeps* $\sqrt[3]{2}$ *and exchanges* j *and* j^2: $\sqrt[3]{2}j \leftrightarrow \sqrt[3]{2}j^2$ *(???). This is a transposition.*

Lets also look at $\mathbb{Q}\left(\sqrt[3]{2}\right)$*. The question is the following: how many Homomorphisms to* $L = \mathbb{Q}\left(\sqrt[3]{2}, j\right)$ *do we have. As we know*

$$L = \mathbb{Q}\left(\sqrt[3]{2}, j\right) = \mathbb{Q}\left(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\right),$$

i.e. $\sqrt[3]{2}$ *can be switched with one of the roots:* $\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$ *and each permutation is a homomorphism. To demonstrate it lets look at the following permutation* $\sqrt[3]{2} \leftrightarrow j\sqrt[3]{2}$*. We have a unique Isomorphism*

$$\mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(j\sqrt[3]{2}\right) \subset L.$$

i.e. we have a homomorphism $\mathbb{Q}\left(\sqrt[3]{2}\right) \to L$ *associated with the following permutation:* $\sqrt[3]{2} \leftrightarrow j\sqrt[3]{2}$

2.3.2 Algebraic closure

Definition 2.9 (Algebraically closed field)**.** *K is algebraically closed if any non constant polynomial $P \in K[X]$ has a root in K or in other words if any $P \in K[X]$ splits*

Example 2.3.2 ($\mathbb{C}$)**.** *$\mathbb{C}$ is an Algebraically closed field. This will be proved later.*

Definition 2.10 (Algebraic closure)**.** *An algebraic closure of K is a field L that is Algebraically closed field and Algebraic extension over K.*

Theorem 2.11 (About Algebraic closure)**.** *Any field K has an Algebraic closure*

Proof. Lets discuss the strategy of the prove. First construct K_1 such that $\forall P \in K[X]$ has a root in K_1. There is not a victory because K_1 can introduce new coefficients and polynomials that can be irreducible over K_1. Then construct K_2 such that $\forall P \in K_1[X]$ has a root in K_2 and so forth. As result we will have

$$K \subset K_1 \subset K_2 \subset \dots \subset K_n \subset \dots$$

Take $\bar{K} = \cup_i K_i$ and we claim that $\bar{K}$ is algebraically closed. Really $\forall P \in \bar{K}[X]\ \exists j : P \in K_j[X]$ thus it has a root in K_{j+1} and as result in $\bar{K}$.

Now how can we construct K_1. Let S be a set of all irreducible $P \in K[X]$. Let $A = K\left[(X_p)_{p\in S}\right]$ - multi-variable (one variable X_p for each $p \in S$) polynomial ring.

Let $I \subset A$ is an Ideal generated by $P(X_p)\ \forall p \in S$.[3] We claim that I is a Proper ideal i.e. $I \neq A$. If not then we can write

$$1_A = \sum_i^n \lambda_i P_i\left(X_{p_i}\right), \tag{2.1}$$

where $\lambda_i \in A$ and the sum is the finite. As soon as the sum is finite then I can take the product of the polynomials in the sum: $P = \prod_i^n P_i$ and I can create a Splitting field L for the polynomial P over K. [4].

A is a polynomial ring and it's very easy produce a homomorphism between polynomial algebra and any other algebra. Therefore there is a homomorphism between rings A and L such that $\phi : A \to L$ where $X_{p_i} \to \alpha_i$ if $P = P_i$ and $X_{p_i} \to 0$ otherwise. From (2.1) we have

$$\phi(1_A) = \sum_i^n \lambda_i \phi\left(P_i\left(X_{p_i}\right)\right) = \sum_i^n \lambda_i P_i\left(\alpha_i\right) = 0$$

that is impossible.

Fact: Any Proper ideal $I \subset A$ is contained in the Maximal ideal m and A/m is a field.

Thus I can take $K_1 = A/m$ and continue in the same way to construct $K_2, K_3, \dots, K_n, \dots$. □

2.3.3 Ideals in a ring

The ring is commutative, associative with unity. Any Proper ideal is in a Maximal ideal. This is a consequence of what one calls Zorn's lemma

Definition 2.12 (Chain). *Let $\mathcal{P}$ is a partially ordered set ($\leq$ is the order relation). $\mathcal{C} \subset \mathcal{P}$ is a chain if $\forall \alpha, \beta \in \mathcal{C}$ exists a relation between α and β i.e. $\alpha \leq \beta$ or $\beta \leq \alpha$.*

Lemma 2.13 (Zorn). *If any non-empty Chain $\mathcal{C}$ in a non-empty set $\mathcal{P}$ has an upper bound (that is $M \in \mathcal{P}$ such that $M \geq x, \forall x \in \mathcal{C}$) then $\mathcal{P}$ has a maximal element.*

[3] $I = \sum_i \lambda_i P_i\left(X_{p_i}\right)$, where $\lambda_i \in A$

[4] α_i is a root of P_i

We can use Zorn lemma to prove that any proper ideal is in a Maximal ideal.

Let $\mathcal{P}$ is the set of proper ideals in A containing I. The set is not empty because it has at least one element I. Any Chain $\mathcal{C} = \{I_\alpha\}$ [5] has an upper bound: it's $\cup_\alpha I_\alpha$ (exercise that the union is an ideal). So $\mathcal{P}$ has a maximal element m and $I \subset m$.

If we take a Quotient ring by maximal ideal it's always a field otherwise it will have a proper ideal: $\exists a \in A/m$ such that (a) is a proper ideal and it pre-image in $\pi : A \to A/m$ should strictly contain m [6].

2.4 Extension of homomorphisms. Uniqueness of algebraic closure

Some summary about just proved existence of algebraic closure. There exists $\bar{K} = \cup_{i=1}^{\infty} K_i$ - algebraic closure of K, where

$$K \subset K_1 \subset K_2 \subset \dots \subset K_{i-1} \subset K_i \subset \dots$$

K_i is a field where each polynomial $P \in K_{i-1}$ has a root. The field K_i is Quotient ring of huge polynomial ring $K_{i-1}[X]$ by a suitable Maximal ideal that is got by means of Zorn lemma.

Another question is the closure unique? The answer is yes. We start the proof with the following theorem

Theorem 2.14 (About extension of homomorphism)**.** *Let $K \subset L \subset M$ - Algebraic extension. $K \subset \Omega$, where Ω - Algebraic closure of K. $\forall \phi : L \to \Omega$ extends to $\widetilde{\phi} : M \to \Omega$*

Proof. Apply Zorn lemma to the following set (of pairs)

$$\mathcal{E} = \{(N, \psi) : L \subset N \subset M, \psi \text{ extends } \phi\}$$

$\mathcal{E}$ is non empty because $(L, \phi) \in \mathcal{E}$.

The set $\mathcal{E}$ is partially ordered by the following relation $(\leq)$:

$$(N, \psi) \leq (N', \psi'),$$

if $N \subseteq N'$ and $\psi'/N = \psi$ (ψ' extends ψ). Any Chain (N_α, ψ_α) has an upper bound (N, ψ), where $N = \cup_\alpha N_\alpha$ - field, sub extension of M. ψ defined in the following way: for $x \in N_\alpha$ $\psi(x) = \psi_\alpha(x)$.

---

[5] The order is the following $I_\alpha \leq I_\beta$ if $I_\alpha \subset I_\beta$

[6] ??? i.e. m is not a maximal ideal in the case.

Thus $\mathcal{E}$ has a maximal element that we denote by (N_0, ψ_0).

Lets suppose that $N_0 \neq M$, i.e. $N_0 \subsetneq M$. Now it's very easy to get a contradiction. Lets take $x \in M \setminus N_0$ and consider Minimal polynomial $P_{min}(x, N_0)$. It should have a root $\alpha \in \Omega$. Now we extend N_0 to $N_0(x)$ and define ψ' on $N_0(x)$ as follows: $\forall y \in N_0 : \psi'(y) = \psi_0(y)$ and $\psi'(x) = \alpha$. Thus we was able to find an element of the chain that is greater than maximal. Therefore our assumption about $N_0 \neq M$ was incorrect and we can conclude than $N_0 = M$ and therefore $\tilde{\phi} = \psi_0$. $\square$

Corollary 2.15 (About algebraic closure isomorphism)**.** *If Δ and Δ' are 2 algebraic closures of K then they are isomorphic as K-algebras.*

Proof. Using theorem 2.14 one can assume $L = K$, $M = \Delta'$ and $\Omega = \Delta$ i.e. we have

$$K \subset K \subset \Delta'$$

in this case homomorphism $K \to \Delta$ can be extended to $\Delta' \to \Delta$ i.e. there exists a homomorphism (i.e. Injection) from Δ' to Δ.

If we assume $M = \Delta$ and $\Omega = \Delta$ then there exists a homomorphism (i.e. Injection) from Δ to Δ'. The Injection is also Surjection in another direction: $\Delta' \to \Delta$ and as result we have Isomorphism $\Delta' \to \Delta$ $\square$

Chapter 3

Finite fields. Separability, perfect fields

We recall the construction and basic properties of finite fields. We prove that the multiplicative group of a finite field is cyclic, and that the automorphism group of a finite field is cyclic generated by the Frobenius map. We introduce the notions of separable (resp. purely inseparable) elements, extensions, degree. We briefly discuss perfect fields.

3.1 An example (of extension)s. Finite fields

Corollary 3.1. *Algebraic closure of K is unique up to Isomorphism of K-algebras* [1]

Corollary 3.2. *Any Algebraic extension of K is embedded into the Algebraic closure* [2]

Example 3.1.1 (Of extension of homomorphism)**.** *Let $K = \mathbb{Q}$ and $\overline{\mathbb{Q}}$ is the Algebraic closure of K. For instance we can consider $\overline{\mathbb{Q}} \subset \mathbb{C}$.* [3]

Let

$$L = \mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}[X] / \left(X^2 - 2\right),$$

α is a class of X in L. L has 2 Embeddings into $\overline{\mathbb{Q}}$

1. $\phi_1 : \alpha \to \sqrt{2}$
2. $\phi_2 : \alpha \to -\sqrt{2}$

[1] There is a redefinition of corollary 2.15.

[2] seems to be a reformulation of theorem 2.14

[3] Really $\overline{\mathbb{Q}} = \mathbb{A}$ - the set of all algebraic numbers, i.e. roots of polynomials $P \in \mathbb{Q}[X]$.

Let

$$M = \mathbb{Q}\left(\sqrt[4]{2}\right) = \mathbb{Q}[Y] / \left(Y^4 - 2\right),$$

β is a class of Y in M. M has 4 Embeddings into $\overline{\mathbb{Q}}$

1. $\psi_1 : \beta \to \sqrt[4]{2}$ *(extends ϕ_1)*
2. $\psi_2 : \beta \to -\sqrt[4]{2}$ *(extends ϕ_1)*
3. $\psi_3 : \beta \to i\sqrt[4]{2}$ *(extends ϕ_2)*
4. $\psi_4 : \beta \to -i\sqrt[4]{2}$ *(extends ϕ_2)*

This ("extends") is because

$$M = L[Y] / \left(Y^2 - \alpha\right)$$

3.1.1 Finite fields

Definition 3.3 (Finite field)**.** *K is a finite field if it's characteristic (see section 1.1.3) $\mathrm{char} K = p$, where p - prime number*

Remark 3.4 ($\mathbb{F}_{p^n}$)**.** *If K is a finite extension of $\mathbb{F}_p$ and $n = [K : \mathbb{F}_p]$ then number of elements of K: $|K| = p^n$. The following notation is also used for a finite extension of a finite field: $\mathbb{F}_{p^n}$*

Remark 3.5 (Frobenius homomorphism)**.** *If $\mathrm{char} K = p$, then exists a Homomorphism $F_p : K \to K$ such that $x \in K \to x^p \to K$. Really if we consider $(x+y)^p$ and $(xy)^p$ then we can get $(x+y)^p = x^p + y^p$ and $(xy)^p = x^p y^p$. The second property is the truth in the all fields (of course) but the first one is the special property of $\mathbb{F}_p$ fields.*

Remark 3.6. *Also $F_{p^n} : x \in K \to x^{p^n} \in K$ is also homomorphism (a power of Frobenius homomorphism.*

3.2 Properties of finite fields

Theorem 3.7. *Lets fix $\mathbb{F}_P$ and it's Algebraic closure $\overline{\mathbb{F}_P}$.*

The Splitting field of $x^{p^n} - x$ has p^n elements. Conversely any field of p^n elements is a splitting field of $x^{p^n} - x$. Moreover there is an unique sub extension of $\overline{\mathbb{F}_P}$ with p^n elements.

Proof. Note that $F_{p^n} : x \to x^{p^n}$ is a Homomorphism (see remark 3.6) as result the following set $\{x \mid F_{p^n}(x) = x\}$ is a sub-field containing $\mathbb{F}_p$ [4] Lets $Q_n(X) = X^{p^n} - X$ thus the considered set consists of the root of the polynomial Q_n. The polynomial has no multiple roots because $gcd(Q_n, Q_n') = 1$. [5] This is because $Q_n' \equiv 1 \mod p$. [6] As soon as Q_n has no multiple roots then there are p^n different roots and therefore the splitting field is the field with p^n elements.

Conversely lets $|K| = p^n$ and $\alpha \neq 0 \in K$. Using the fact that the multiplication group of K has $p^n - 1$ elements: $|K^*| = p^n - 1$ [7] as result the multiplication of all the elements should give us 1: $\alpha^{p^n-1} = 1$ or $\alpha^{p^n} - \alpha = 0$. Therefore α is a root of Q_n. Thus the splitting field of Q_n consists of elements of K.

The uniqueness of sub-extension of $\mathbb{F}_p$ with p^n elements is a result of uniqueness of the splitting field (see theorem 2.7). $\square$

Theorem 3.8. $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ *if and only if* $d \mid n$.

Proof. Let $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ in this case $\mathbb{F}_p \subset \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ and

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = \left[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}\right]\left[\mathbb{F}_{p^d} : \mathbb{F}_p\right]$$

or $n = x \cdot d$ i.e. $d \mid n$

Conversely if $d \mid n$ then $n = x \cdot d$ or $p^n = \prod_{i=1}^{x} p^d$ thus if $x^{p^d} = x$ then

$$x^{p^n} = x^{\prod_{i=1}^{x} p^d} \left(x^{p^d}\right)^{\prod_{i=2}^{x} p^d} = x^{\prod_{i=2}^{x} p^d} = \cdots = x^{p^d} = x,$$

i.e. $\forall \alpha \in \mathbb{F}_{p^d}$ we also have $\alpha \in \mathbb{F}_{p^n}$ or in other notation: $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. $\square$

Theorem 3.9. $\mathbb{F}_{p^n}$ *is a Stem field and a Splitting field of any irreducible polynomial* $P \in \mathbb{F}_p$ *of degree* n.

Proof. Stem field K has to have degree n over $\mathbb{F}_p$ i.e. $[K : \mathbb{F}_|] = n$ i.e. it should have p^n elements and therefore $K = \mathbb{F}_{p^n}$ (see also remark 3.4).

About Splitting field. Using the just proved result we can say that if α is a root of P then $\alpha \in \mathbb{F}_{p^n}$ thus $Q_n(\alpha) = 0$. Therefore P divides Q_n [8] and as result P splits in $\mathbb{F}_{p^n}$. $\square$

---

[4] For $x \in \mathbb{F}_p$ we have that $x^{p-1} = 1$ (the field with fixed number of elements) and therefore $\forall x \in \mathbb{F}_p : x^p = x$ i. e. $F_{p^n}(x) = x$.

[5] If Q_n has a multiple root β then it is divisible by $(X - \beta)^2$ and the Q_n' is divisible by (at least) $(X - \beta)$ thus the $(X - \beta)$ should be a part of gcd.

[6] ??? $Q_n' = p^n X^{p^n-1} - 1 \equiv -1 \mod p$

[7] $K^* = K \setminus \{0\}$

[8] as soon as any root of P also a root of Q_n

Corollary 3.10. *Let $\mathcal{P}_d$ is the set of all irreducible, Monic polynomials of degree d such that $\mathcal{P}_d \subset \mathbb{F}_p[X]$ then*

$$Q_n = \prod_{d|n} \prod_{P \in \mathcal{P}_d} P$$

Proof. As we just seen if $P \in \mathcal{P}_d$ and $d \mid n$ then $P \mid Q_n$. [9] Since all such polynomials are relatively prime of course [10] [11] and Q_n have no multiple roots (as result no multiple factors) then

$$\prod_{d|n} \prod_{P \in \mathcal{P}_d} P \mid Q_n$$

From other side let R is an irreducible factor of Q_n. α is a root of R then $Q_n(\alpha) = 0$ thus $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$ therefore $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$ where $d \mid n$ and as result, $degR \mid n$. Thus the polynomial should be in the product $\prod_{d|n} \prod_{P \in \mathcal{P}_d} P$. □

Example 3.2.1. *Let $p = n = 2$. The monic irreducible polynomials in $\mathbb{F}_2$ whose degree divides 2 are: x, $x + 1$ and $x^2 + x + 1$. As you can see*

$$x(x+1)\left(x^2 + x + 1\right) = x^4 + x = x^4 - x$$

because $2x = 0 \mod 2$ *or* $x = -x$.

3.3 Multiplicative group and automorphism group of a finite field

Theorem 3.11. *Let K be a field and and G be a finite Subgroup of K^* then G is a Cyclic group*

Proof. Idea is to compare G and the Cyclic group $\mathbb{Z}/N\mathbb{Z}$ where $N = |G|$. [12]

[9] Since stem field is $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$

[10] As soon as $\mathbb{F}_p[X]$ is Unique factorization domain then any polynomial can be written as a product of irreducible elements, uniquely up to order and units this means that each $P \in \mathcal{P}_d$ (where $d \mid n$) should be in the factorization of Q_n. It should be only one time because there is no multiply roots.

[11] We also can say that 2 irreducible polynomial $P_1, P_2 \in \mathbb{F}_p[X]$ should not have same roots. For example if α is the same root - it cannot be in $\mathbb{F}_p$ because in the case the polynomials will be reducible. Thus it can be only in an extension of $\mathbb{F}_p$ from other side $gcd(P_1, P_2) = 1$ and therefore with Bézout's lemma one can get that $\exists Q, R \in \mathbb{F}_p[X]$ such that $P_1Q + P_2R = 1$ and setting α into the equation leads to fail statement that $0 = 1$.

[12] We also will use the fact that any cyclic group of order N is isomorphic to $\mathbb{Z}/N\mathbb{Z}$

Let $\psi(d)$ - is the number of elements of order d (see also Order of element in group) in G. We need $\psi(N) \neq 0$ [13] and we know that $N = \sum \psi(d)$.

Let also $\phi(d)$ - is the number of elements of order d (see also Order of element in group) in $\mathbb{Z}/N\mathbb{Z}$. [14] As $\mathbb{Z}/N\mathbb{Z}$ contains a single (cyclic) subgroup of order d for each $d \mid N$. [15] $\phi(d)$ is the number of generators of $\mathbb{Z}/d\mathbb{Z}$ i.e. the number of elements between 1 and $d-1$ that are prime to d. We know that $\phi(N) \neq 0$.

We claim that either $\psi(d) = 0$ or $\psi(d) = \phi(d)$ [16] If no element of order d in G then $\psi(d) = 0$ otherwise if $x \in G$ has order d then $x^d = 1$ or x is a root of the following polynomial $x^d - 1$. The roots of the polynomial forms a cyclic subgroup of G. So G as well as $\mathbb{Z}/N\mathbb{Z}$ has a single cyclic subgroup of order d (which is cyclic) or no such group at all. [17]

If $\psi(d) \neq 0$ then exists such a subgroup and $\psi(d)$ is equal to the number of generators of that group or $\phi(d)$ [18] In particular $\psi(d) \leq \phi(d)$ [19] but there should be equality because the sum of both $\sum \psi(d) = \sum \phi(d) = N$. In particular $\psi(N) \neq 0$ and we proved the theorem. $\square$

Corollary 3.12. *If $K \subset \mathbb{F}_p$ and $[K : \mathbb{F}_p] = n$ then $\exists \alpha$ such that $K = \mathbb{F}_p(\alpha)$. In particular $\exists$ an irreducible polynomial of degree n over $\mathbb{F}_p$* [20]

Proof. We can take $\alpha =$ generator of K^* [21] $\square$

---

[13] In this case we will have at least one element x of order N i.e. N different elements of G is generated by the x i.e. the G is cyclic.

[14] The function $\phi(d)$ is also called as Euler's totient function and it counts the positive integers up to a given integer d that are relatively prime to d

[15] The one generated by N/d. Let $N = r \cdot d$ in the case $x^N = 1$ there x is a $\mathbb{Z}/N\mathbb{Z}$ group generator. From other side

$$x^N = x^{r \cdot d} = \prod_{i=1}^{r} x^d$$

thus $x^d = 1$ i.e. there is a cyclic subgroup of order d.

[16] suffices since $\sum \psi(d) = \sum \phi(d) = N$

[17] Several comments about the subgroup. There is a group because multiplication of any elements is in the set. It's cyclic because it's generated by one element. All x^i where $i \leq d$ are different (in other case the group should have an order less than d). Each element of the group x^i is a root of $x^d - 1$ because $(x^i)^d = (x^d)^i = 1^i = 1$. And the group is unique as well as we have d different roots of $x^d - 1$ in the group.

[18] Because the group is cyclic and any cyclic group is isomorphic to $\mathbb{Z}/d\mathbb{Z}$ and as result has the same number of generators.

[19] because $\psi(d) = 0$ or $\psi(d) = \phi(d)$

[20] The theorem 3.9 and remark 3.4 says that the stem field for any polynomial of degree n over $\mathbb{F}_p$ exists and there is $\mathbb{F}_{p^n}$ and $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ i.e. $K = \mathbb{F}_{p^n}$. But we had not proved yet that an irreducible polynomial of degree n exists.

[21] This is because $K^* = \langle \alpha \rangle$ i.e. any element of K except 0 can be got as a power of α

Corollary 3.13. *The group of automorphism of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is cyclic and generated by Frobenius map: $F_p : x \to x^p$ (see remark 3.5)*

Proof. As we know from theorem 3.7: $\forall x \in \mathbb{F}_{p^n} : x^{p^n} = x$ so $F_p^n = Id$ [22]. From other side if $m < n$ then $x^{p^m} - x = 0$ has $p^m < p^n$ roots and cannot be identity [23] Finally (from corollary 3.12) we have $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ where α is a root of an irreducible polynomial of degree n. Thus there exists exactly n automorphisms of $\mathbb{F}_{p^n}$. [24] So

$$|Aut(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq n$$

and as we have n of them (Automorphisms) then

$$|Aut(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$$

□

3.4 Separable elements

Let E is a Splitting field of an irreducible polynomial P. We would like to say that it "has many Automorphisms". What does this mean? This means the following thing: Let α and β be 2 roots of P then we have 2 extensions $K(\alpha) \subset E$ and $K(\beta) \subset E$.

There exists an Isomorphism (see proposition 2.2) over K

$$\phi : K(\alpha) \to K(\beta)$$

that is also extended to an Automorphism on E (see theorem 2.14).

There is one problem with it: is that truth that an irreducible polynomial of degree n has "many" (no more than n and not single) roots.

The answer is yes if $char K = 0$, but not always if $char K = p$ (where p is a prime number). P can have multiple roots in the case i.e. $gcd(P, P') \neq 1$.

i.e. we really got $K = \mathbb{F}_p(\alpha)$.

??? The irreducible polynomial we can get if consider $1, \alpha, \ldots, \alpha^{n-1}$ as a basis and α^n can be represented via the basis.

[22] because $F_p^n : x \to x^{p^n} = x$.

[23] because operates only with p^m elements i.e. not of all elements of $\mathbb{F}_{p^n}$.

[24] Each automorphism converts the root α into another one of n roots of the irreducible polynomial

Why it's not a case for $char K = 0$ - it is because $\deg P' < \deg P$ and $P \nmid P'$ for $P' \neq 0$ (non constant polynomial) [25]

But for $char K = p$ there can be a case when $P' = 0$ for a non constant polynomial thus $P \mid P'$ and as result $gcd(P, P') = P$. The $P' = 0$ i.e. is vanish if $P = \sum a_i x^i$ and $p \mid i$ or $a_i = 0$.

Let $r = \max h$ such that P is a polynomial in x^{p^h} that is $a_i = 0$ whenever $p^h \nmid i$

Proposition 3.14. *Let $P(X) = Q\left(x^{p^r}\right)$ and $Q' \neq 0$ i.e. $gcd(Q, Q') = 1$ and Q does not have multiple roots but all roots of P have multiplicity p^r.*

Proof. If λ is a root of P then λ: $P(X) = (X - \lambda)R$ Thus $\mu = \lambda^{p^r}$ is the root of Q: $Q(Y) = (Y - \lambda^{p^r})S(Y)$ therefore

$$P(X) = \left(X^{p^r} - \lambda^{p^r}\right) S\left(X^{p^r}\right) = (X - \lambda)^{p^r} S\left(X^{p^r}\right)$$

and λ is not a root of $S\left(X^{p^r}\right)$. [26] Thus we just got that multiplicity of λ is p^r. □

Definition 3.15 (Separable polynomial)**.** *$P \in K[X]$ irreducible polynomial is called separable if* $\gcd(P, P') = 1$

Definition 3.16 (Degree of separability)**.** *$d_{sep}(P) = \deg Q$ (as above)* [27]

Definition 3.17 (Degree of inseparability)**.** *$d_i(P) = \frac{\deg P}{\deg Q}$ ($= p^r$ in definition 3.16)*

Definition 3.18 (Pure inseparable polynomial)**.** *P is pure inseparable if $d_i = \deg P$. Then $P = X^{p^r} - a$* [28]

Definition 3.19 (Separable element)**.** *Let L be an Algebraic extension of K then $\alpha \in K$ is called separable(inseparable) if it's Minimal polynomial $P_{min}(\alpha, K)$ has the property*

[25] Let P has multiply roots. As soon as it's irreducible a multiply root is in an extension of K. In this case the root should be also a root for P' thus by theorem 0.30 one can get that $P \mid P'$ in $K[X]$ but that is impossible because $\deg P' < \deg P$ and can be only possible if $P' = 0$.

[26] This is because Q does not have multiply roots and as result $\mu = \lambda^{p^r}$ is not a root of S or in other words $S\left(X^{p^r}\right)_{X=\lambda} \neq 0$

[27] It requires some explanation compare to that one was got on the lecture video. If P is a Separable polynomial then $d_{sep}(P) = \deg P$. In other case P should be represented as $P(X) = q_1(X^p)$. If $q_1(Y)$ is separable than $Q = q_1$ otherwise we continue and represent $q_1(X) = q_2(X^p)$. We should stop on some q_r in this case $Q = q_r$ and $P(X) = Q\left(X^{p^r}\right)$. In the case $d_{sep}(P) = \deg Q$.

[28] ??? For example but not then

Proposition 3.20 (On number of homomorphisms). *If α is separable on K then the number of Homomorphisms*

$$\left|Hom_k\left(K\left(\alpha\right), \bar{K}\right)\right| = \deg P_{min}\left(\alpha, K\right)$$

in general

$$\left|Hom_k\left(K\left(\alpha\right), \bar{K}\right)\right| = d_{sep} P_{min}\left(\alpha, K\right)$$

Proof. It's obvious because d_{sep} is the number of distinct roots. $\square$

3.5 Separable degree, separable extensions

We want to generalize the proposition 3.20 for any field extension (not necessary $K\left(\alpha\right)$). Let L be a finite extension of K

Definition 3.21 (Separable degree). $[L : K]_{sep} = \left|Hom_k\left(L, \bar{K}\right)\right|$

As we know if $L = K\left(\alpha\right)$ then Separable degree is a number of distinct roots of minimal polynomial $P_{min}\left(\alpha, K\right)$

Definition 3.22 (Separable extension). *L is separable over K if $[L : K]_{sep} = [L : K]$*

Definition 3.23 (Inseparable degree).

$$[L : K]_i = \frac{[L : K]}{[L : K]_{sep}}$$

Theorem 3.24 (About separable extensions). *1. If $K \subset L \subset M$ then $[M : K]_{sep} = [M : L]_{sep} [L : K]_{sep}$ and M is Separable extension over K if and only if M is separable over L and L is separable over K*

2. The following things are equivalent

(a) L is separable over K

(b) $\forall \alpha \in L$ α Separable element over K

(c) L is generated over K by a finite number of Separable elements i.e. $L = K\left(\alpha_1, \alpha_2, \ldots, \alpha_n\right)$, there α_i is separable over K

(d) $L = K\left(\alpha_1, \alpha_2, \ldots, \alpha_n\right)$, there α_i is separable over $K\left(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}\right)$

Remark 3.25. *That holds if we replace separability with pure inseparability.*

Proof. About 1st part: If we have a Homomorphism $\phi : L \to \bar{K}$ then it is extended to $\tilde{\phi} : M \to \bar{K}$ (by extension theorem 2.14) it can be done with one way per each homomorphism from L to M i.e. it can be done by $[M : L]_{sep}$ ways. From other side $\bar{K}$ is also $\bar{L}$ (Algebraic closure over L) thus ???

$$[M : L]_{sep} = \left|Hom_L\left(M, \bar{L}\right)\right| = \left|Hom_L\left(M, \bar{K}\right)\right|$$

For the total number of homomorphisms one can get the following equations ???

$$[M : K]_{sep} = \left|Hom_k\left(M, \bar{K}\right)\right| = \left|Hom_k\left(L, \bar{K}\right)\right| \left|Hom_L\left(M, \bar{K}\right)\right| = \\ \left|Hom_k\left(L, \bar{K}\right)\right| \left|Hom_L\left(M, \bar{L}\right)\right| = [M : L]_{sep} [L : K]_{sep}$$

We also have

$$[M : K]_{sep} = [M : L]_{sep} [L : K]_{sep} \leq [M : L] [L : K] = [M : K]$$

The equality is possible if $[M : L]_{sep} = [M : L]$ and $[L : K]_{sep} = [L : K]$ i.e. if M is separable over L and L is separable over K. [29] This finishes the proof of the first part.

About 2d part: □

3.6 Perfect fields

[29] In video EA suggested to use induction. How???