Introduction to Galois Theory

November 7, 2016

Contents

Introduction

The document keeps lecture notes on Introduction to Galois theory that was provided by Ekaterina Amerik (Higher School of Economics) via Coursera.

Each chapter corresponds to one lecture (or one week on Coursera). The appendix keeps useful info for the course that is absent in it i.e. requirements that are necessary for the course understanding.

I also tried to make all my comments as footnotes or inside brackets '()' whenever it was possible.

All not clear (for me) or in-completed proofs are marked as ???

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

1.1.2 Field extension

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

and another definition

Definition 1.3 (Field extension). *Let K is a field then L is an extension of K if L is a K-algebra* [1]

Why the 2 definitions are equivalent?

Lemma 1.1 (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 1.2 (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

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

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

[1] L in the definition is not the same object with L from definition 1.2. Because L in the definition is a K-algebra i.e. a ring but L in the definition 1.2 is a field.

Example 1.3 (K-algebra is not a field)**.** *In the example [2] I will show that K algebra is not a field. Consider $K = \mathbb{R}$. Vector space $A = \mathbb{R}^2$ i.e. A consists of vectors of the following form*

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

where $x_1, x_2 \in \mathbb{R}$. I will define the multiplication for L (our K algebra) as follows

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 \cdot y_1 \\ x_2 \cdot y_2 \end{pmatrix}$$

It can be seen that all requirements of K-algebra are satisfied

$$(x + y) \cdot z = \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} =$$

$$= \begin{pmatrix} (x_1 + y_1)z_1 \\ (x_2 + y_2)z_2 \end{pmatrix} = \begin{pmatrix} x_1 z_1 + y_1 z_1 \\ x_2 z_2 + y_2 z_2 \end{pmatrix} = x \cdot z + y \cdot z$$

$$z \cdot (x + y) = z \cdot x + z \cdot y$$

$$(ax) \cdot (by) = \begin{pmatrix} ax_1 \\ ax_2 \end{pmatrix} \begin{pmatrix} by_1 \\ by_2 \end{pmatrix} = \begin{pmatrix} abx_1 y_1 \\ abx_2 y_2 \end{pmatrix} (ab)(x \cdot y)$$

The multiplication identity element of L is the following

$$1_L = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

The zero is the standard one from vector space

$$0_L = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

We can see that

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0_L$$

i.e. we have 2 divisor of zero which are not zero itself. The elements do not have invert ones and as result the L is not a field.

From other side if we define $L' \subset L$ as follows $L' = \left\{ \begin{pmatrix} r \\ r \end{pmatrix} \right\}$, where $r \in \mathbb{R}$, then we will have that L' is a field and $L' \cong \mathbb{R}$.

[2] the example was not present in the lectures

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 $char L = 0$
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 $char L = p$, where $p = \min m$ - 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 polynomial. (P) is an Ideal formed by the polynomial. [3] 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. [4] 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 $K[X]/(P)$.

Example 1.4. *The example is not a part of the lectures but it's very usefully in future lectures.*

Let K is a field and $a \in K$ then $K[X]/(X-a)$ is also a field and there exists an Isomorphism between the field and K i.e.

$$K[X]/(X-a) \cong K \tag{1.1}$$

The $K[X]/(X-a)$ is a field just because $X-a$ is Irreducible polynomial (see example A.15).

---

[3] I.e. $(P) = \{Q = GP\}$ where $G \in K[X]$

[4] As soon as P is irreducible in $K[X]$ then there is only one possibility for Q and P to have common divisors: if $Q = GP$ where $G \in K[X]$ but this is in contradiction with $Q \notin (P)$

For the proof the main statement (1.1) lets consider a polynomial $P \in K[X]$ *and define the following Homomorphism:*

$$\phi : K[X]/(X-a) \xrightarrow[P(X)\to P(a)]{} K \tag{1.2}$$

The ϕ *defined by (1.2) is Homomorphism. For the proof of the claim lets take* $P_1, P_2 \in K[X]/(X-a)$*. Clear that* $\phi(P_1+P_2) = P_1(a) + P_2(a) = \phi(P_1) + \phi(P_1)$*. The same holds with the multiplication. Division is more complex but also can be shown: if* $P_2 \neq 0$ *when there exists* P_2^{-1} *as soon as* $K[X]/(X-a)$ *is the field then with* $\phi\left(P_2^{-1}\right) = P_2^{-1}(a) = \frac{1}{\phi(P_2)}$ *one can get*

$$\phi\left(\frac{P_1}{P_2}\right) = \phi\left(P_1 P_2^{-1}\right) = \phi(P_1)\,\phi\left(P_2^{-1}\right) = \frac{\phi(P_1)}{\phi(P_2)}$$

We have $\ker\phi = (X-a)$ *because for any polynomial* P *that is in the ideal* $(X-a)$ *has* $P(a) = 0$ *i.e. in the kernel of* ϕ*.*

Next we should show that ϕ *is Surjection it's easy because* $\forall k \in K$ *we can consider constant polynomial* $P = k$ *from* $K[X]$*. For the polynomial we will have* $\phi(k) = k$*.*

Now (1.1) follows from the First isomorphism theorem.

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 [5] but a quotient by a Maximal ideal is a Field (see theorem About Quotient Ring and Maximal Ideal).

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

Example 1.5 ($K = \mathbb{F}_2/(X^2+X+1)$)**.** *Lets consider the following field* $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ *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:* $\{0, 1, \bar{X}, \overline{X+1}\}$*.*

[5] To prove that (P) is a Maximal ideal we have to use Bézout's lemma.

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

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

So this is the structure of a field of four elements. The cardinality of $K = \mathbb{F}_2/\left(X^2+X+1\right)$ is 4, one writes then $K = F_4$. Well, this might be strange at the first sight, because we only know that K has four elements and if you write F_4 you somehow mean that there is only one field of four elements. Well, it is true, there is only one field of four elements. In fact, all finite fields of the same cardinality are isomorphic, and we will see it very shortly (see theorem 3.1).

1.2.2 Algebraic elements

Definition 1.4 (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 1.3 (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* [6]

[6] see also theorem About irreducible polynomials

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.

Lets prove that P is irreducible. 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. □

Definition 1.5 (Minimal polynomial)**.** *If α is Algebraic element then the unitary polynomial P of minimal degree such that $P(\alpha) = 0$ is called minimal polynomial and denoted by $P_{min}(\alpha, K)$.*

1.3 Algebraic elements. Algebraic extensions

Definition 1.6. *Let $K \subset L$, $\alpha \in L$. The smallest sub-field contained K and α denoted by $K(\alpha)$. The smallest sub-ring (or K-algebra) contained K and α denoted by $K[\alpha]$.*

As soon as $K[\alpha]$ is a K-algebra it is a Vector space over K generated by

$$1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots.$$

Example 1.6 ($\mathbb{C}$)**.**

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

$\mathbb{C}$ 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 1.1. *The following assignment are equivalent*

1. *α is algebraic over K*
2. *$K[\alpha]$ is a finite dimensional Vector space over K*
3. *$K[\alpha] = K(\alpha)$* [7]

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

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

[7] Contrary to the example 1.3 we see that K-algebra is a field there.

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 $1, \alpha, \ldots, \alpha^{d-1}$ is a finite dimensional Vector space.

Lets proof that 2 implies 3. Its enough to prove that $K[\alpha]$ is a field because $K[\alpha] \subset K(\alpha)$.

Let $x \neq 0 \in K[\alpha]$ then lets look at an operation $x \cdot K[\alpha] \to K[\alpha]$. This is Injection. [8] But the $K[\alpha]$ is finite dimensional Vector space and a Homomorphism between 2 vector spaces with the same dimension is Surjection [9] 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 $i : K[X] \to K[\alpha] = K(\alpha)$ which sends $P(X)$ to $P(\alpha)$. [10] But $K[X]$ is not a field thus $K[\alpha]$ should not be a field too that is in contradiction with the initial conditions. [11] $\square$

Definition 1.7 (Algebraic extension)**.** *L an extension of K is called algebraic over K if* $\forall \alpha \in L$ - α *is algebraic over K.*

Proposition 1.2. *If L is algebraic over K then any K-subalgebra of L is a Field.*

Proof. Let $L' \subset L$ is 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. [12] $\square$

[8] If $y, z \in K[\alpha]$ and $\dim K[\alpha] = d < \infty$ where $d = \deg P_{min}(\alpha, K)$. Then $y = \sum_{i=0}^{d-1} y_i\alpha^i$ and $z = \sum_{i=0}^{d-1} z_i\alpha^i$ where $y_i, z_i \in K$. We have $y - z = \sum_{i=0}^{d-1}(y_i - z_i)\alpha^i \neq 0$ if $y \neq z$ (i.e. $\exists i : y_i \neq z_i$) because $y - z$ can be considered as a polynomial of degree $\leq d - 1 < \deg P_{min}(\alpha, K)$ and cannot be equal to 0 by minimal polynomial definition. Continue we have $x \cdot (y - z) \neq 0$ because it also can be considered as a product of 2 polynomial of degree $< d$. Thus

$$x \cdot y \neq x \cdot z$$

i.e. Injection property is satisfied.

[9] Two vector spaces with same dimension are isomorphic each other (see lemma A.2)

[10] And if $P(X) \neq 0$ then $P(\alpha) \neq 0$

[11] Alternative prove is the following. Let $x \neq 0 \in K[X]$ and $K[\alpha]$ is a field then $\exists y \in K[X] : i(x)i(y) = 1$ or $i(xy) = 1$ or finally x - is invertable and $K[X]$ is a field.

[12] As soon as $K[\alpha] = K(\alpha)$ is a field then its any element (especially α) is invertable.

Proposition 1.3. *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 $P_{min}(\alpha, K) \in L[X]$. [13] □

1.4 Finite extensions. Algebraicity and finiteness

Definition 1.8 (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 1.1 (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 $\{m_1, m_2, \dots, m_n\}$ 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

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

[13] 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 using lemma About minimal polynomial existence one can get that $P_{min}(\alpha, L)$ divides $P_{min}(\alpha, K)$.

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.

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

□

Definition 1.9 ($K(\alpha_1, \dots, \alpha_n)$)**.** *$K(\alpha_1, \dots, \alpha_n) \subset L$ generated by $\alpha_1, \dots, \alpha_n$ is the smallest sub field of L contained K and $\alpha_i \in L$.*

Theorem 1.2 (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 $\alpha_1, \dots, \alpha_d$ is a basis. In this case $L = K[\alpha_1, \dots, \alpha_d] = K(\alpha_1, \dots, \alpha_d)$. Moreover each $K[\alpha_i]$ is finite dimensional thus by proposition 1.1 α_i is algebraic.

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

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

Then using theorem 1.1 we can conclude that $K(\alpha_1, \dots, \alpha_d)$ has finite dimension. □

1.5 Algebraicity in towers. An example

Theorem 1.3. *$K \subset L \subset M$ 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) is finite over K thus α is algebraic over K. [14] □

Example 1.7 ($\mathbb{Q}$ 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 1.4 (On dimension of extension)**.**

$$[K(\alpha) : K] = \deg\left(P_{min}(\alpha, K)\right),$$

if α is algebraic.

---

[14] $P_{min}(\alpha, L) = \sum_{i=0}^{d-1} l_i \alpha^i$ where $l_i \in L$ and each l_i is algebraic over K by algebraic extension definition 1.7. By theorem 1.2 there are finite number of l_i and they forms an algebraic extension $E = K(l_0, l_1, \ldots, l_{d-1})$. The $E(\alpha)$ is finite over E and therefore finite over K. As soon as $E(\alpha)$ has a finite dimension over K thus there exists a relation for powers of α such that $\sum_{i=0}^{n} k_i \alpha^i = 0$ i.e. α is algebraic.

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

Proposition 1.5 (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

$$\alpha + \beta, \alpha \cdot \beta \in K[\alpha, \beta]$$

[15] □

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 1.2)
- $[K[\alpha] : K] = deg P_{min}(\alpha, K)$ (see proposition 1.4).

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 $x^{100} - 2$?

[15] We also have that $K[\alpha, \beta]$ is a field: $K[\alpha, \beta] = K(\alpha, \beta)$. Really $K[\alpha] = K(\alpha)$ (see proposition 1.1). β is algebraic over K and therefore over $K(\alpha)$ thus we can construct $K(\alpha)[\beta] = K(\alpha, \beta)$ by proposition 1.1

Lemma 1.4 (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

$$nmP = Q_1 R_1.$$

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

$$0 = \overline{Q_1 R_1}$$

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

$$P = Q_s R_t,$$

where $Q_s, R_t \in \mathbb{Z}[X]$. □

Example 1.8 (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*

$$x^{100} - 2 = QR \tag{1.3}$$

Lets consider (1.3) 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 1.5 (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 1.8. $\square$

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 $E = K[\alpha]$.* [1]

Such things exist, for instance we can take $K[X]/(P)$. It is a field because P is an Irreducible polynomial moreover the root of the P is in the field (see example 1.5).

We also can say that for any stem field E:

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

We can use the following Isomorphism: $f : \forall \mathcal{P} \in K[X]/(P) \to \mathcal{P}(\alpha)$, there α is a root of polynomial P. [2]

To summarize we have the following

[1] Comment from Marc Emmanuel: The stem field is more widely known as simple extensions [10]

[2] In the case we have $f(P) = P(\alpha) = 0$ as expected

Proposition 2.1 (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: [3]

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

thus

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

□

Remark 2.1 (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 $[E : K] = \deg P$

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 $[E : K] > degP$ [4]

[3] First of all if we have an isomorphism f between two K algebras $K[\alpha]$ and $K[\alpha']$ it should preserve the K-algebra structure, especially $\forall k \in K : k1_{K[\alpha]} \to_f k1_{K[\alpha']}$. As soon as $k \in K[\alpha]$ we can write the following

$$f\left(k1_{K[\alpha]}\right) = f(k) f\left(1_{K[\alpha]}\right) = f(k) 1_{K[\alpha']}.$$

But from other side

$$f\left(k1_{K[\alpha]}\right) = kf\left(1_{K[\alpha]}\right) = k1_{K[\alpha']}$$

i.e. $\forall k \in K : f = id$.

α forms a basis such that $\forall \beta \in E = K[\alpha]$ we have $\beta = \sum_i k_i \alpha^i$ where $k_i \in K$. We also have $f(\beta) = \sum_i k_i [f(\alpha)]^i = \sum_i k_i [\alpha']^i$. Thus if $\exists f'$ isomorphism such that $f'(\alpha) = \alpha'$ then $f'(\beta) = \sum_i k_i [\alpha']^i = f(\beta)$ i.e. the isomorphisms are the same.

[4] Let E' is a stem field of P. In the case we have $E' \subset E$ as soon as any element of E' is an element of E because E contains a root of P. From other side $E \neq E'$ as soon as E is not a stem field. Thus $\deg E > \deg E' = \deg P$.

2.1.2 Some irreducibility criteria

Corollary 2.1. *$P \in K[X]$ is irreducible over K if and only if it does not have a root in Field extension L of K 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 $degQ \leq \frac{n}{2}$. [5] The Stem field L for Q exists and it's degree is $degQ \leq \frac{n}{2}$. L should have a root of Q (as soon as a root of P) by definition.

$\Leftarrow$: If P has a root α in L then $\exists P_{min}(\alpha, K)$ with degree $\leq \frac{n}{2} < n$ [6] that divides P (see lemma 1.3) i.e. P become reducible. □

Corollary 2.2. *$P \in K[X]$ irreducible with $\deg P = n$. 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 of Q therefore $[M : L] = \deg Q = d < n$. Thus

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

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

$K(\alpha) \subseteq M$ and therefore $n \mid md$ [7] 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 2.2 (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 2.1 (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.*

---

[5] $P = RQ$ and if $degQ > \frac{n}{2}$ then we can take R as Q

[6] because $[L : K] \leq \frac{n}{2}$ (see remark 2.1)

[7] $K \subset K(\alpha) \subset M$ and with The multiplicativity formula for degrees we have

$$md = [M : L][L : K] = [M : K] = [M : K(\alpha)][K(\alpha) : K] = [M : K(\alpha)] \cdot n$$

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 (by induction) 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 2.1 says as that

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

i.e. $\exists \phi$ - isomorphism such that $\phi(\alpha) = \beta$.

Over M_1 we have $P = (x - \beta)S$, where $S = \phi(R)$. [8] M is a splitting field for S over $K[\beta]$ i.e. it is a $K[\beta]$-algebra but it's is also a $K[\alpha]$-algebra [9] and as result it's a splitting field for R over $K[\alpha]$ and by induction [10] we have $K[\alpha]$ isomorphism $L \cong M$ and as result K isomorphism $L \cong M$. [11] □

Remark 2.2. *The Isomorphism considered in theorem 2.1 is not unique. A splitting field can have many Automorphism and this is in fact the subject of Galois theory.*

[8] We have $\phi : K(\alpha) \to K(\beta)$. The $\phi : K \to K = id$ (see note 3). 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 $S = \phi(R)$.

[9] via the existent Isomorphism between $K[\alpha]$ and $K[\beta]$

[10] Induction steps are the following: we have a polynomial P with $\deg P = n$. For $n = 1$ the isomorphism exists by proposition 2.1. We suppose that the isomorphism is proved for polynomial with degree $n - 1$.

[11] Lukas Heger comment about the prove: We can consider another roots: α_2 for R and β_2 for S and there is an isomorphism between the 2 stem fields also. Continue in the way we will get the 2 following chains

$$K \subset L_1, \subset L_2 \subset \cdots \subset L_n \subset L$$
$$K \subset M_1, \subset M_2 \subset \cdots \subset M_n \subset M$$

On each step we have an isomorphism between L_i and M_i and as result the isomorphism between resulting fields L and M (via ϕ) as L_n algebras and therefore as K algebras.

2.3 An example. Algebraic closure

2.3.1 An example of automorphism

Example 2.1 ($x^3 - 2$ 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. $P_{min}(j, \mathbb{Q}) = X^2 + X + 1$ thus using remark 2.1 $[\mathbb{Q}(j) : \mathbb{Q}] = 2$. Using the same arguments one can get that $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$. As result the following picture can be got*

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

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* [12]

2. *$\mathbb{Q}(j)$ Automorphism. In this case the automorphism of exchanging $\sqrt[3]{2}$ and $j\sqrt[3]{2}$.* [13]*. 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 A.8):

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

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

---

[12] $j \to j^2$ thus $j^2 \to j^4 = j$. Therefore $j \leftrightarrow j^2$

[13] $\sqrt[3]{2} \to j\sqrt[3]{2}$ produces $j\sqrt[3]{2} \to j^2\sqrt[3]{2}$ and $j^2\sqrt[3]{2} \to -\sqrt[3]{2}$. This statement corresponds the fact that the minimal polynomial is $x^3 - 2$ there and thus we have 3 roots: $\sqrt[3]{2}$, $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$

- *σ: $\sqrt[3]{2} \to j\sqrt[3]{2} \to j^2\sqrt[3]{2} \to \sqrt[3]{2}$. This is a circle.*
- *τ - it keeps $\sqrt[3]{2}$ and exchanges j and j^2: $\sqrt[3]{2}j \leftrightarrow \sqrt[3]{2}j^2$ (see note 12). This is a transposition.*

2.3.2 Algebraic closure

Definition 2.3 (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 2.2 ($\mathbb{C}$)**.** *$\mathbb{C}$ is an Algebraically closed field. This will be proved later.*

Definition 2.4 (Algebraic closure)**.** *An algebraic closure of K is a field L that is Algebraically closed field and Algebraic extension over K.* [14]

Theorem 2.2 (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 a set $P(X_P)\ \forall P \in S$.[15] We claim that I is a Proper ideal i.e. $I \neq A$. If not then we can write (see theorem A.6)

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

[14] If L is algebraic closure of K then the following conditions are valid

- $\forall P \in L[X]\ \exists \alpha \in L$ such that $P(\alpha) = 0$ (see definition of Algebraically closed field)
- $\forall \alpha \in L\ \exists P \in K[X]$ such that $P(\alpha) = 0$ (see definition of Algebraic extension)

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

where $\lambda_i \in A$ and the sum is the finite (see definition A.27). 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 (see theorem 2.1).

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 $X_{P_i} \to \alpha_i$ [16] 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 (see proposition 2.2 below) and A/m is a field (see theorem A.9).

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

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 2.5 (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 2.1 (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.*

Proposition 2.2. *Any Proper ideal is in a Maximal ideal*

Proof. 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 $\mathcal{C} = \{I_\alpha\}$ [17] 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 $I \subset m$. □

[16] α_i is a root of P_i

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

If we take a Quotient ring by maximal ideal it's always a field [18] 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 [19].

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

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

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 2.3 (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 $\widetilde{\phi} : M \to \Omega$* [20]

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 $x \in N_\alpha$ $\psi(x) = \psi_\alpha(x)$.

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

[18] We refer to it as a theorem with definition provided in A.9. The comments can be considered as a simple prove of the fact.

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

[20] see also example 3.1.

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 $\tilde{\phi} = \psi_0$. □

Corollary 2.3 (About algebraic closure isomorphism). *If Δ and Δ' are 2 algebraic closures of K then they are isomorphic as K-algebras.*

Proof. Using theorem 2.3 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 $\Delta' \to \Delta$ □

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 embeds (see definition A.63) into the Algebraic closure* [2]

Example 3.1 (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. $\phi_1 : \alpha \to \sqrt{2}$

[1] There is a redefinition of corollary 2.3.

[2] i.e. $\forall E$ - algebraic extension of K, $\exists \phi : E \to \bar{K}$ - Homomorphism. The statement is a reformulation of theorem 2.3

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

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

   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 [4]
$$M = L[Y]/\left(Y^2 - \alpha\right)$$

3.1.1 Finite fields

Definition 3.1 (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 3.1 ($\mathbb{F}_{p^n}$)**.** *If K is a finite extension of $\mathbb{F}_p$* [5] *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: $\mathbb{F}_{p^n}$* [6]

Remark 3.2 (Frobenius homomorphism)**.** *If $\mathrm{char} K = p$, then exists a Homomorphism $F_p : K \to K$ such that $F_p(x) = x^p$. Really if we consider $(x+y)^p$ and $(xy)^p$ then we can get $(x+y)^p = x^p + y^p$* [7] *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.*

[4] I.e. in our case we have $\mathbb{Q} \subset L \subset M$. We have $\phi_{1,2} : L \to \overline{\mathbb{Q}}$ which can be extended (accordingly theorem 2.3) to $\psi_{1,2,3,4} : M \to \overline{\mathbb{Q}}$

[5] i.e. $[K : \mathbb{F}_p] < \infty$

[6] As we know $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. From other side $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$. For example $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$ because $\mathbb{Z}/4\mathbb{Z}$ is not a field ($2 \cdot 2 = 0$ i.e. zero divisors exist). You have to look at example 1.5 to see exact structure of $\mathbb{F}_4$.

[7]
$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p + p \cdot \left(\sum_{k=1}^{p-1} a_k x^k y^{p-k}\right),$$
where $a_k \in \mathbb{Z}$. I.e.
$$(x+y)^p \equiv (x^p + y^p) \mod p$$

Remark 3.3. *Also $F_{p^n}: K \to K$ such that $F_{p^n}(x) = x^{p^n}$ is also homomorphism (a power of Frobenius homomorphism.)*

3.2 Properties of finite fields

Theorem 3.1. *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 3.3) as result the following set $\{x \mid F_{p^n}(x) = x\}$ is a field containing $\mathbb{F}_p$ [8] i.e.

$$\mathbb{F}_p \subset \{x \mid F_{p^n}(x) = x\}$$

or, in other words, the considered set is a Field extension of $\mathbb{F}_p$.

If $Q_n(X) = X^{p^n} - X$ then the considered set consists of the root of the polynomial Q_n. The polynomial has no multiple roots because $gcd(Q_n, Q_n') = 1$. [9] This is because $Q_n' \equiv 1 \mod p$. [10] 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: $|K^\times| = p^n - 1$ [11] as result the multiplication of all the elements should give us 1: $\alpha^{p^n-1} = 1$ or $\alpha^{p^n} - \alpha = 0$

[8] For $x \in \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ we have that (see theorem A.4)

$$x^{|\mathbb{F}_p^\times|} = x^{p-1} = 1$$

and therefore $\forall x \in \mathbb{F}_p : x^p = x$ ($x = 0$ also satisfied the equation). We can continue as follows

$$\begin{aligned} x^{p^2} &= (x^p)^p = x^p = x, \\ x^{p^3} &= \left(x^{p^2}\right)^p = x^p = x \\ &\dots \\ x^{p^n} &= \left(x^{p^{n-1}}\right)^p = x^p = x \end{aligned}$$

and finally get $F_{p^n}(x) = x$. Thus $\forall x \in \mathbb{F}_p$ we also have $x \in \{x \mid F_{p^n}(x) = x\}$

[9] 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.

[10] Really we have the following one $Q_n' = p^n X^{p^n-1} - 1 \equiv -1 \mod p$ but the sign is not really matter because $\gcd(Q_n, -1) = \gcd(Q_n, 1) = 1$.

[11] $K^\times = K \setminus \{0\}$

(see theorem A.4). Therefore α is a root of Q_n. Thus the splitting field of Q_n consists of elements of K.

The uniqueness [12] of sub-extension of $\mathbb{F}_p$ with p^n elements is a result of uniqueness of the splitting field (see theorem 2.1). □

Theorem 3.2. *$\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ 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: $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. □

Theorem 3.3. *$\mathbb{F}_{p^n}$ 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. $[K : \mathbb{F}_p] = n$ (see remark 2.1) i.e. it should have p^n elements (see remark 3.1) and therefore $K = \mathbb{F}_{p^n}$ (see theorem 3.1).

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 [13] and as result P splits in $\mathbb{F}_{p^n}$. □

Corollary 3.3. *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*

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

[12] up to Isomorphism

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

Proof. As we just seen if $P \in \mathcal{P}_d$ and $d \mid n$ then $P \mid Q_n$. [14] Since all such polynomials are relatively prime of course [15] [16] and Q_n have no multiple roots (as result no multiple factors) then

$$\left(\prod_{d|n} \prod_{P \in \mathcal{P}_d} P\right) \mid Q_n$$

From other side let R is an irreducible factor of Q_n. α is a root of R then $Q_n(\alpha) = 0$ thus $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$. From remark 2.1 we have

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg R = d.$$

From remark 3.1 $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Theorem 3.2 says that $d \mid n$. As result $R \in \mathcal{P}_d$. Thus the polynomial should be in the product $\prod_{d|n} \prod_{P \in \mathcal{P}_d} P$. □

Example 3.2. *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 $x = -x$.

Just another example [2] [17]

Example 3.3. *In $\mathbb{F}_2[X]$, the irreducible factorization of $X^{2^n} - X$ for $n = 1, 2, 3, 4$ is as follows*

$$\begin{aligned} X^2 - X &= X(X-1), \\ X^4 - X &= X(X-1)\left(X^2+X+1\right), \\ X^8 - X &= X(X-1)\left(X^3+X+1\right)\left(X^3+X^2+1\right), \\ X^{16} - X &= X(X-1)\left(X^2+X+1\right) \\ \left(X^4+X+1\right)\left(X^4+X^3+1\right)&\left(X^4+X^3+X^2+X+1\right). \end{aligned}$$

You can compare the example with example 3.2 but you have to take into consideration the following fact $1 = -1 \mod 2$

[14] Since stem field is $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ (see theorem 3.2 and proof at the theorem 3.3)

[15] 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.

[16] 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 $0 = 1$.

[17] There is not a part of the video lectures

3.3 Multiplicative group and automorphism group of a finite field

Theorem 3.4. *Let K be a field and and G be a finite Subgroup of $K^\times$ (see definition A.25) then G is a Cyclic group*

Proof. Idea is to compare G and the Cyclic group $\mathbb{Z}/N\mathbb{Z}$ where $N = |G|$. [18]

Let $\psi(d)$ - is the number of elements of order d (see also Order of element in group) in G. We need $\psi(N) \neq 0$ [19] 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 $\mathbb{Z}/N\mathbb{Z}$. [20] As $\mathbb{Z}/N\mathbb{Z}$ contains a single (cyclic) subgroup of order d for each $d \mid N$. [21] $\phi(d)$ 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 $\psi(d) = \phi(d)$ [22] 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 (by Cyclic group definition). 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. [23]

If $\psi(d) \neq 0$ then exists such a subgroup and $\psi(d)$ is equal to the number of generators of that group or $\phi(d)$ [24] In particular $\psi(d) \leq \phi(d)$ [25] 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. □

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

[19] 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.

[20] 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

[21] 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.

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

[23] 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.

[24] 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.

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

Corollary 3.4. *If $\mathbb{F}_p \subset K$ 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 $\mathbb{F}_p$* [26]

Proof. We can take $\alpha =$ generator of $K^\times$ [27] □

Corollary 3.5. *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 3.2 where we showed that the Frobenius map is a field automorphism)*

Proof. As we know from theorem 3.1: $\forall x \in \mathbb{F}_{p^n} : x^{p^n} = x$ so [28] $F_p^n = id$. As result the order of $\langle F_p \rangle$ is no greater than n. Lets prove that the $ord F_p = n$. Really if $m < n$ then $x^{p^m} - x = 0$ has $p^m < p^n$ roots and [29] F_p^m cannot be identity. Finally (from corollary 3.4) we have $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ where α is a root of an irreducible polynomial of degree n. I.e. there cannot be more than n automorphism [30] so

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

and as we have n of them (Automorphisms) [31] then

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

and the group is cyclic generated by F_p. □

---

[26] The theorem 3.3 and remark 3.1 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.

[27] This is because from theorem 3.4 $K^\times = \langle \alpha \rangle$ i.e. any element of K except 0 can be got as a power of α. Moreover $\alpha \notin \mathbb{F}_p$ (in other case we will got $K = \mathbb{F}_p$) i.e. we really got $K = \mathbb{F}_p(\alpha)$. α is an Algebraic element because we can consider $1, \alpha, \dots, \alpha^{n-1}$ as a basis and α^n can be represented via the basis. I.e. $\exists P \in \mathbb{F}_p[X]$ such that $P(\alpha) = 0$. By lemma 1.3 there exists an irreducible polynomial $P_{min}(\alpha, \mathbb{F}_p)$.

[28] because

$$(F_p)^n(x) = (F_p)^{n-1}(F_p(x)) = (F_p)^{n-1}(x^p) = \cdots = x^{p^n} = x$$

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

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

[31] We have n different elements of cyclic group $\langle F_p \rangle$. The generator of the group is an automorphism and as result each of n elements is also an automorphism.

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 2.1) over K

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

that is also extended to an Automorphism on E (see theorem A.12).

There is one problem with it: is that truth that an irreducible polynomial of degree n has "many" i.e. exactly n (it cannot have more than n) 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. $gcd(P, P') \neq 1$.

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) [32]

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. it vanishes P is a polynomial in X^p. I.e. if $P = \sum a_i x^i$ and $p \mid i$ or $a_i = 0$. In that case ($P' = 0$) let $r = \max h$ such that P is a polynomial in X^{p^h} that is $a_i = 0$ whenever $p^h \nmid i$. See the following example [33]

Example 3.4. *Let $p = 2$. The polynomial $P(X) = X^{16} + 1$ has the required property ($P' = 0$). The polynomial can be present in the following form*

$$P(X) = X^{2^4} + 1 = Q(Y)$$

where $Y = X^{16}$ and $Q(Y) = Y + 1$. In the case $r = 4, p^r = 16 \mid 16$.

For polynomial $P(X) = X^{12} + 1$ we have

$$P(X) = \left(X^{2^2}\right)^3 + 1 = Q(Y)$$

where $Y = X^4$ and $Q(Y) = Y^3 + 1$. In the case $r = 2, p^2 = 4 \mid 12$ because $h = 3$ does not fit into the requirements: $p^h = 2^3 = 8 \nmid 12$.

Proposition 3.1. *Let $P(X) = Q\left(X^{p^r}\right)$ and $Q' \neq 0$ i.e. $gcd(Q, Q') = 1$ then Q does not have multiple roots but all roots of P have multiplicity p^r.*

[32] 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 lemma 1.3 (or theorem A.7) 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 $P' = 0$.

[33] The example is not a part of the video lectures.

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 [34] as result $Q(Y) = (Y - \lambda^{p^r})S(Y)$ 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 $S\left(X^{p^r}\right)$. [35] Thus we just got that multiplicity of λ is p^r. □

Definition 3.2 (Separable polynomial)**.** $P \in K[X]$ *irreducible polynomial is called separable if* $\gcd(P, P') = 1$

Definition 3.3 (Degree of separability)**.** $d_{sep}(P) = \deg Q$ *(as above)* [36]

Definition 3.4 (Degree of inseparability)**.** $d_i(P) = \frac{\deg P}{\deg Q}$ *($= p^r$ in proposition 3.1)*

Definition 3.5 (Pure inseparable polynomial)**.** *P is pure inseparable if $d_i = \deg P$. Then $P = X^{p^r} - a$* [37]

Definition 3.6 (Separable element)**.** *Let L be an Algebraic extension of K then $\alpha \in L$ is called separable(inseparable) if it's Minimal polynomial $P_{min}(\alpha, K)$ has the property. Note: the separable element is also Algebraic element because it has minimal polynomial.*

Proposition 3.2 (On number of homomorphisms)**.** *If α is separable on K then the number of Homomorphisms over K from K to $\bar{K}$*

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

in general

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

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

---

[34] $Q(\mu) = Q\left(\lambda^{p^r}\right) = P(\lambda) = 0$

[35] 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 $S\left(X^{p^r}\right)_{X=\lambda} \neq 0$

[36] 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 for which we will have $Q = q_r$ and $P(X) = Q\left(X^{p^r}\right)$. In the case $d_{sep}(P) = \deg Q$.

[37] In the case $\deg Q = 1$ i.e. $Q(Y) = Y - a$ or $P = X^{p^r} - a$.

3.5 Separable degree, separable extensions

We want to generalize the proposition 3.2 for any field extension (not necessary $K(\alpha)$). Let L be a finite extension of K

Definition 3.7 (Separable degree). $[L:K]_{sep} = \left|Hom_K\left(L, \bar{K}\right)\right|$

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

Definition 3.8 (Separable extension). *L is separable over K if* $[L:K]_{sep} = [L:K]$

Definition 3.9 (Inseparable degree).

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

Theorem 3.5 (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. $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, there α_i is separable over K

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

Remark 3.4. *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 2.3) it can be done with one way per each homomorphism from L to M i.e. it can be done by $\left|Hom_L\left(M, \bar{K}\right)\right|$ ways but we have

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

because $\bar{K}$ is also $\bar{L}$ (Algebraic closure over L) thus 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 have the following inequality [38]

$$[E:K]_{sep} \le [E:K]\,. \tag{3.1}$$

With the inequality (3.1) we also have

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

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. This finishes the proof of the first part.

About 2d part:

2a $\Rightarrow$ 2b: Part 1 implies that a separable sub extension $K(\alpha)$ or a separable extension L is separable. [39]

2b $\Rightarrow$ 2c: obvious [40]

2c $\Rightarrow$ 2d: We know that $P_{min}(\alpha_i, K(\alpha_1,\dots,\alpha_{i-1}))$ divides $P_{min}(\alpha_i, K)$. [41] Thus if $P_{min}(\alpha_i, K)$ is separable (i.e. have distinct roots) then it's divisor $P_{min}(\alpha_i, K(\alpha_1,\dots,\alpha_{i-1}))$ also should have distinct roots i.e. α_i is a Separable element over $K(\alpha_1,\dots,\alpha_{i-1})$

2d $\Rightarrow$ 2a: Induction as above [42] □

[38] The inequality can be proved by induction using the fact that it's true for $K(\alpha)$ because from general case of proposition 3.2

$$\left|Hom_K\left(K(\alpha),\bar{K}\right)\right| = d_{sep}P_{min}(\alpha,K) \le \deg P_{min}(\alpha,K) = [K(\alpha):K]$$

Then let it was proved for $E = K(\alpha_1,\dots,\alpha_{n-1})$ and we want to prove it for $K(\alpha_1,\dots,\alpha_{n-1},\alpha_n) = E(\alpha_n)$. It's easy because $\bar{E} = \bar{K}$ and we can use the same approach as for the first induction step.

[39] I.e. in the case we have $K \subset K(\alpha) \subset L$ and if L is separable then $K(\alpha)$ is separable and as result α is a Separable element because $P_{min}(\alpha, K)$ is separable.

[40] We consider finite extensions (see remark 3.1) i.e. which consists of finite number of elements

[41] Let $K(\alpha_1,\dots,\alpha_{i-1}) = L$ then $K \subset L$ and $P_{min}(\alpha_i, K) \in L[X]$ From other side $P_{min}(\alpha_i, L)$ is the minimal irreducible polynomial in $L[X]$ and any other polynomial with α_i as root has to by divisible by it. see also lemma 1.3

[42] The first induction step is trivial: $L = K(\alpha)$ where α is separable over K in this case $K(\alpha)$ is also separable. Now we have that $\forall k < n$: if $L = K(\alpha_1,\alpha_2,\dots,\alpha_k)$, there α_i is separable over $K(\alpha_1,\alpha_2,\dots,\alpha_{i-1})$ then L is separable over K. Thus we have $K(\alpha_1,\alpha_2,\dots,\alpha_{n-1})$ separable and α_n is separable over $K(\alpha_1,\alpha_2,\dots,\alpha_{n-1})$ thus using the first part of the theorem we can conclude that $K(\alpha_1,\alpha_2,\dots,\alpha_n)$ is also separable over K

What's about not finite extension? For that case we can define separable extension as follows.

Definition 3.10 (Separable closure). *If L over K not necessary finite (but algebraic over K) we can define*

$$L^{sep} = \{x | x \text{ separable over } K\}$$

L^{sep} is a sub extension [43] *called separable closure of K over L*

L is pure inseparable over L^{sep}.

Remark 3.5.

1. *If $\operatorname{char} K = 0$ then any extension of K is separable*
2. *If $\operatorname{char} K = p$ then pure inseparable extension has degree p^r and always degree of inseparability $[L : K]_i = p^r$*

3.6 Perfect fields

Definition 3.11 (Perfect field). *Let K is a field and $\operatorname{char} K = p > 0$. K is perfect if Frobenius homomorphism is a Surjection*

Example 3.5.

1. *Finite field is perfect because an Injection of a set into itself is always a Surjection*
2. *Algebraically closed fields are perfect because $X^p - a$ has a root α for any a particularly $a = F_p(\alpha)$* [44]
3. *Not perfect field example. Let $K = \mathbb{F}_p(X)$ be a field of rational fractions in 1 variable over $\mathbb{F}_p$. I.e. elements of the field are $\frac{f(X)}{g(X)}$ where $f, g \in \mathbb{F}_p[X]$. It's not perfect because $Im(F_p) = \mathbb{F}_p(X^p) \neq \mathbb{F}_p(X)$*

Theorem 3.6. *K is a Perfect field if and only if all irreducible polynomial over K are separable or in other words all Algebraic extensions of K are separable.*

Proof. Let K is perfect and $P \in K[X]$ is an irreducible polynomial. Let also

$$P(X) = Q\left(X^{p^r}\right) = \sum_i a_i \left(X^{p^r}\right)^i$$

[43] $K \subset L^{sep} \subset L$

[44] $\alpha^p - a = 0$ as soon as α is a root of $X^p - a$. Thus $a = \alpha^p = F_p(\alpha)$.

but as soon as my field is perfect then I can extract p-root of a_i [45] and do it repeatedly. I.e. $\exists b_i \in K$ such that $b_i^{p^r} = a_i$. Therefore

$$P(X) = \sum_i b_i^{p^r} \left(X^{p^r}\right)^i = \sum_i \left(b_i X^i\right)^{p^r} = \left(\sum_i b_i X^i\right)^{p^r}.$$

The polynomial is not irreducible unless $r = 0$ [46] so irreducible means separable.

If K is not perfect but all irreducible polynomial are separable. K is not perfect means that $\exists a \notin Im\left(F_p\right)$ and lets consider the following polynomial: $X^{p^r} - a$. It is irreducible and not separable.

About separability: in fact all roots are in $\bar{K}$ are the same x with $x^{p^r} = a$ [47] and of course $x^{p^{r-1}} \notin K$. [48]

About the polynomial is irreducible. We have already seen that in the case $[K(x) : K] = p^r$ so the polynomial is irreducible [49] and this finishes [50] the proof. $\square$

[45] The root b_i is a root of the following equation $X^p - a_i$ i.e. $b_i^p - a_i = 0$ or $a_i = F_p\left(b_i\right)$.

[46] In other case each root will have at least multiplicity p^r.

[47] We have $x^{p^r} = a$ thus polynomial $X^{p^r} - a$ can be written as $X^{p^r} - a = X^{p^r} - x^{p^r} = (X - x)^{p^r}$ thus x has multiplicity p^r

[48] as soon as any power of x (little x but not the big one X)

[49] Corollary 3.4 says that there exists an irreducible polynomial of degree p^r with x as the root. Theorem A.7 says that the polynomial should divide our polynomial $X^{p^r} - a$ as soon as they have the same root. The two polynomial have same degree and as result they are the same (up to a constant). Therefore the considered polynomial is irreducible.

[50] Because we found an irreducible polynomial that is not separable because has a root of multiplicity p^r

Chapter 4

Tensor product. Structure of finite K-algebras

This is a digression on commutative algebra. We introduce and study the notion of tensor product of modules over a ring. We prove a structure theorem for finite algebras over a field (a version of the well-known "Chinese remainder theorem").

4.1 Definition of tensor product

4.1.1 Summary for previous lectures

We considered finite Field extension L i.e $[L : K] < \infty$. We also saw that if L is generated by a finite number of Separable elements $\alpha_1, \ldots, \alpha_r$ then the number of Homomorphisms over K from L to $\bar{K}$ denoted by $\left|Hom_K\left(L, \bar{K}\right)\right|$ is equal to $[L : K]$. In general

$$[L : K]_{sep} = \left|Hom_K\left(L, \bar{K}\right)\right| \leq [L : K] \,.$$

For $L = K(\alpha)$ it is clear because the number of homomorphisms is equal to the number of roots of the Minimal polynomial $P_{min}(\alpha, K)$. In general one can use induction and multiplicativity of the degree $[L : K]$ and number of homomorphisms (see theorem About separable extensions). Thus separable extension was exactly an extension which had the right number of homomorphisms into the algebraic closure.

Our next goal is to characterize the separability in the terms of tensor product.

4.1.2 Tensor product

Definition 4.1 (Tensor product). *Let A is a ring, N, M are A-Modules. The tensor product $M \otimes_A N$ is another A-Module together with an A-bilinear map $\phi : M \times N \to M \otimes_A N$ which has "Universal property" defined below*

Definition 4.2 (Universal property). *A-bilinear map $\phi : M \times N \to M \otimes_A N$ has "universal property" if $\forall P$ - A-Module and for A-bilinear $f : M \times N \to P$ (i.e. $\forall m, f_m : N \xrightarrow[n \to f(m,n)]{} P$ and $\forall n, f_n : M \xrightarrow[m \to f(m,n)]{} P$ are Homomorphisms of A-modules), then $\exists! \tilde{f}$ - homomorphism of A-modules such that $f = \tilde{f} \circ \phi$* [1]

$$
\begin{tikzcd}
M \times N \arrow[rr, "f"] \arrow[dr, "\phi"'] & & P \\
& M \otimes_A N \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}
$$

The property characterize the pair $(\phi, M \otimes N)$. Really if have another pair $\left(\overline{\phi}, \overline{M \otimes N}\right)$ like this one then by definition we have mutually inverse homomorphisms of A-modules between them

Lemma 4.1 (About uniqueness of object defined by universal property). [2] *If we have two objects $(\phi, M \otimes N)$ and $\left(\overline{\phi}, \overline{M \otimes N}\right)$ which both satisfies Universal property than there is an unique Isomorphism between them:*

$$(\phi, M \otimes N) \cong \left(\overline{\phi}, \overline{M \otimes N}\right)$$

Proof. Let $P = \overline{M \otimes N}$ and $f = \overline{\phi}$. In the case we can consider the following diagram

$$
\begin{tikzcd}
& M \otimes_A N \arrow[d, "g = \tilde{\overline{\phi}}"] \\
M \times N \arrow[ur, "\phi"] \arrow[r, "\overline{\phi}"] \arrow[dr, "\phi"'] & \overline{M \otimes_A N} \arrow[d, "\bar{g} = \tilde{\phi}"] \\
& M \otimes_A N
\end{tikzcd}
$$

[1] That means that we have a Commutative diagram there

[2] It is out of the lecture video and can be considered as an explanation for the claim about having mutually inverse homomorphisms of A-modules. The proof was taken from [5].

As soon as we fixed $\overline{M \otimes_A N}$ we 2 unique homomorphisms (which are defined by the fixed $\overline{M \otimes_A N}$) - $g : M \otimes_A N \to \overline{M \otimes_A N}$ and $\bar{g} : \overline{M \otimes_A N} \to M \otimes_A N$. Both g and $\bar{g}$ are linear as mentioned above the pair is unique (if we fix g we will have only one $\bar{g}$ that corresponds to g). The composition $g \circ \bar{g}$ maps $M \otimes_A N$ to itself. Thus if we fix g and choose $\bar{g} = g^{-1}$ we will get $g \circ \bar{g} = id_{M \otimes_A N}$ that satisfied all requirements. The choice is final because we don't have a possibility to choose any other $\bar{g}$ (it should be unique).

Thus we have an Isomorphism and the isomorphism is unique as soon as the function g is unique due the Universal property.

We just prove an isomorphism existence between $M \otimes N$ and $\overline{M \otimes N}$ but the tensor product is characterized not only by the module $M \otimes N$ but also a bilinear map ϕ. Let $P = \overline{M \otimes N}$ thus we can get that $\bar{\phi} = \tilde{\bar{\phi}} \circ \phi$ is determined by the unique relation $\phi \to \bar{\phi}$ as soon as $\tilde{\bar{\phi}}$ is unique. Analogues one can get the unique relation $\bar{\phi} \to \phi$. □

The uniqueness does not mean existence and we should proof that such object exists.

Lemma 4.2 (About tensor product existence)**.** *Tensor product defined via Universal property exists*

Proof. Lets consider $\mathcal{E}$ the maps (functions) from $M \times N$ to A as sets which are 0 almost everywhere (i.e. outside of a finite set). For example we can consider delta functions:

$$\delta_{m,n} : M \times N \to A$$

such that

$$\delta_{m,n}(m, n) = 1,$$
$$\delta_{m,n}(m', n') = 0 \text{ if } (m, n) \neq (m', n')$$

Then $\mathcal{E}$ is a A-Free module with basis $\delta_{m,n}$. Thus we have a map of sets $M \times N \to \mathcal{E}$ such that $(m, n) \to \delta_{m,n}$ which is not bilinear but we can make it bilinear by means of changing $\mathcal{E}$.

Let $\mathcal{F} \subset \mathcal{E}$ a submodule generated by $\delta_{m+m',n} - \delta_{m,n} - \delta_{m',n}$, $\delta_{m,n+n'} - \delta_{m,n} - \delta_{m,n'}$, $\delta_{am,n} - a\delta_{m,n}$, $\delta_{m,an} - a\delta_{m,n}$. [3]

It can be shown that $M \times N \to \mathcal{E}/\mathcal{F}$ is bilinear [4] and has the desired Universal property.

[3] The basis is chosen to be a bilinear $\mod \mathcal{F}$, for instance $\delta_{m+m',n} = \delta_{m,n} + \delta_{m',n} \mod \mathcal{F}$

[4] Follows from the basis choice

Really lets we have the following bilinear map: $f : M \times N \to P$. Then we can consider the following linear map (Homomorphism) $f' : \mathcal{E} \to P$ that sends $\delta_{m,n}$ to $f(n, m)$. Using the fact that f is bilinear we can get

$$\begin{aligned} f'(\delta_{m+m',n}) = f(m+m',n) = f(m,n) + f(m',n) = \\ = f'(\delta_{m,n}) + f'(\delta_{m',n}). \end{aligned}$$

With the same approach one can get the following relations

$$\begin{aligned} f'(\delta_{m,n+n'}) = f'(\delta_{m,n}) + f'(\delta_{m,n'}), \\ f'(\delta_{am,n}) = af'(\delta_{m,n}), \\ f'(\delta_{m,an}) = af'(\delta_{m,n}) \end{aligned}$$

with the f' linearity we have

$$\begin{aligned} f'(\delta_{m+m',n}) = f'(\delta_{m,n} + \delta_{m',n}), \\ f'(\delta_{m,n+n'}) = f'(\delta_{m,n} + \delta_{m,n'}), \\ f'(\delta_{am,n}) = af'(\delta_{m,n}), \\ f'(\delta_{m,an}) = af'(\delta_{m,n}) \end{aligned}$$

The kernel $\ker f' = \mathcal{F}$ thus if we want to have a homomorphism to P we have to replace $\mathcal{E}$ with $\mathcal{E}/\mathcal{F}$ that is also denoted by $M \otimes_A N$. In the case we will replace f' with $\tilde{f}(\delta_{m,n} \mod \mathcal{F}) = f(m, n)$. As soon as the images for the basis is fixed the mapping is unique. $\square$

We will denote $\phi(m, n) = \delta_{m,n} \mod \mathcal{F}$ as $m \otimes n$. I.e our tensor product can be considered as the $(\otimes, M \otimes_A N)$ pair.

Remark 4.1. *Wrong idea is to define $M \otimes_A N$ as a set of $m \otimes n$. I.e. $M \otimes_A N \neq \{m \otimes n\}$. The $M \otimes_A N$ is generated by $m \otimes n$ i.e. $\forall x \in M \otimes_A N$ we have $x = \sum_{i=1}^{k} m_i \otimes n_i$ i.e. each element is a finite sum of $m \otimes n$ and I cannot reduce these further* [5].

4.2 Tensor product of modules

4.2.1 Advantages of the universal property

Now, you can ask why haven't I just defined the tensor product by this construction? Why am I talking of this universal property? And the answer is because it is easier to prove things this way. So advantages of the universal property is as follows: the proofs become easy.

[5] i.e. $\exists x \in M \otimes_A N$ such that $\exists! m \in M, n \in N : x = m \otimes n$ but $\exists m_1, \ldots, m_k \in M, n_1, \ldots, n_k \in N : x = \sum_{i=1}^{k} m_i \otimes n_i$

4.2.2 Several examples of universal property usage

Example 4.1 (Commutativity proof)**.** *We want to prove that*

$$M \otimes_A N \cong N \otimes_A M$$

We have the following bilinear map: $M \times N \to N \otimes_A M$ *for which the pair* (m, n) *is mapped to* $n \otimes m$*. Thus from Universal property we have that there is a linear map (homomorphism)* $\alpha : M \otimes_A N \to N \otimes_A M$*:*

$$\begin{tikzcd} M \times N \arrow[rr, "(m,n) \to n \otimes m"] \arrow[dr, "(m,n) \to m \otimes n"'] & & N \otimes_A M \\ & M \otimes_A N \arrow[ur, "\alpha"'] & \end{tikzcd}$$

With the same construction we can also get the inverse map a^{-1} *that sends* $N \otimes_A M$ *to* $M \otimes_A N$*:*

$$\begin{tikzcd} M \times N \arrow[rr, "(m,n) \to m \otimes n"] \arrow[dr, "(m,n) \to n \otimes m"'] & & M \otimes_A N \\ & N \otimes_A M \arrow[ur, "\alpha^{-1}"'] & \end{tikzcd}$$

Also

Corollary 4.1.

$$A \otimes_A M \cong M$$

Proof. For the proof [6] lets look at A. Really A can be considered as A-module because all requirements from definition A.42 are satisfied. The following diagrams shows that there exist 2 homomorphisms: $\alpha : A \otimes_A M \to M$ and $\alpha^{-1} : M \to A \otimes_A M$ as result there is a homomorphism $A \otimes_A M \cong M$:

$$\begin{tikzcd} A \times M \arrow[rr, "(a,m) \to a \cdot m"] \arrow[dr, "(a,m) \to a \otimes_A m"'] & & M \\ & A \otimes_A M \arrow[ur, "\alpha"'] & \end{tikzcd} \qquad \begin{tikzcd} A \times M \arrow[rr, "(a,m) \to a \otimes_A m"] \arrow[dr, "(a,m) \to a \cdot m"'] & & A \otimes_A M \\ & M \arrow[ur, "\alpha^{-1}"'] & \end{tikzcd}$$

In the diagrams $m \in M$, as usual, and $a \in A$.

□

[6] The proof is missed in the lectures

If we have that M is generated by $e_1, e_2, \dots$ and N is generated by $\epsilon_1, \epsilon_2, \dots$ than $M \otimes_A N$ is generated by pairs $e_i \otimes \epsilon_j$. It's obvious.

More complex fact is the following

Proposition 4.1. *Let M and N are Free modules with corresponding basises $e_1, e_2, \dots, e_n$ and $\epsilon_1, \epsilon_2, \dots, \epsilon_m$ than $M \otimes_A N$ is also free module with basis $e_i \otimes \epsilon_j$ where $1 \le i \le n$ and $1 \le j \le m$.*

Proof. Lets define $f_{i_0,j_0} : M \times N \to A$ as a map that sends $(\sum a_i e_i, \sum b_j \epsilon_j)$ to $a_{i_0} b_{j_0}$. It's bilinear [7] so it factors through the tensor product $\tilde{f}_{i_0,j_0} : M \otimes_A N \to A$. The map $\tilde{f}_{i_0,j_0}$ sends $e_{i_0} \otimes \epsilon_{j_0}$ to 1 and all others to 0. [8] So if

$$\sum \alpha_{ij} e_i \otimes \epsilon_j = 0$$

then applying $\tilde{f}_{i_0,j_0}$ for all indices one can get that $\forall i, j : \alpha_{ij} = 0$. [9] $\square$

In particular for the Vector space the tensor product is defined in the same way (as just proved in the proposition 4.1): the tensor product of 2 vector spaces with basises $e_1, e_2, \dots, e_n$ and $\epsilon_1, \epsilon_2, \dots, \epsilon_m$ is another vector space with the following basis $e_i \otimes \epsilon_j$ i.e. the definition does not take into consideration the Universal property.

Proposition 4.2 (Associative)**.**

$$(M_1 \otimes_A M_2) \otimes_A M_3 \cong M_1 \otimes_A (M_2 \otimes_A M_3)$$

Proof. There is just a scratch of the proof. Introduce $M_1 \otimes_A M_2 \otimes_A M_3$ as a universal object for 3-linear maps and show that 2 considered parts are isomorphic each other. $\square$

[7] for example $(\sum (a_i + a'_i) e_i, \sum b_j \epsilon_j)$ is sent to $(a_{j_0} + a'_{j_0}) b_{j_0}$.

[8] Because $f = \tilde{f}\phi$ i.e.

$$\begin{aligned} a_{i_0} b_{j_0} = f_{i_0,j_0}\left(\sum a_i e_i, \sum b_j \epsilon_j\right) = \\ = f_{i_0,j_0}\left(\phi\left(\sum a_i e_i, \sum b_j \epsilon_j\right)\right) = \\ = \tilde{f}_{i_0,j_0}\left(\sum a_i e_i \otimes \sum b_j \epsilon_j\right) = \sum_{i,j} a_i b_j \tilde{f}_{i_0,j_0}(e_i \otimes \epsilon_j). \end{aligned}$$

[9] because $\tilde{f}$ should be linear.

4.3 Base change

Let A is a Ring and B is A-algebra. Let also M is an A-Module and N is B-module.

I can of course make N into A-module (just forgetting the additional A-algebra structure). But we can also make B-module on M (that is not a trivial thing) by considering $B \otimes_A M$ [10] . We can introduce B-module structure on $B \otimes_A M$ by [11]

$$b \cdot (b' \otimes m) = (b \cdot b') \otimes m$$

Example 4.2 (The complexification of a real vector space)**.** *We can "make" $\mathbb{R}^{2n}$ from $\mathbb{C}^n$ by forgetting the complex structure.* [12] *The $\mathbb{C}^n$ has the following basis $e_1, \dots, e_n$. The $\mathbb{R}^{2n}$ has the following one $e_1, \dots, e_n, ie_1, \dots, ie_n$. Now we forgot about multiplication rules for $i = \sqrt{-1}$ and denote ie_i as v_i. In the case the basis for $\mathbb{R}^{2n}$ is the following one: $e_1, \dots, e_n, v_1, \dots, v_n$.*

But we can also do the following constructions

$$\mathbb{R}^n \to \mathbb{C}^n = \mathbb{C} \otimes \mathbb{R}^n \to \mathbb{R}^{2n}$$

for the $\mathbb{C}^n$ basis we have $1_\mathbb{C} \otimes e_1, \dots, 1_\mathbb{C} \otimes e_n$ and for $\mathbb{R}^{2n}$ - $1 \otimes e_1, \dots, 1 \otimes e_n, i \otimes e_1, \dots, i \otimes e_n$. [13]

Proposition 4.3. *In general we have the following. If M - free A - module with basis $e_1, \dots, e_n$ then $B \otimes_A M$ is a free B module with basis $1_B \otimes e_1, \dots, 1_B \otimes e_n$.*

---

[10] In other words we can make a B-module from A-module M

[11] I.e. we introduced B-algebra operations for objects from $B \otimes_A M$. See also definition 1.1.

[12] In the case we have ring $A = \mathbb{R}$ and $B = \mathbb{C}$ - A algebra. A - module is the following vector space $M = \mathbb{R}^{2n}$ and B - module is $N = \mathbb{C}^n$.

[13] some additional clarification: $\forall x \in \mathbb{C} \otimes \mathbb{R}^n$ we have

$$x = \sum_{i=1}^n c_i \otimes r_i e_i = \sum_{i=1}^n c_i r_i 1_\mathbb{C} \otimes e_i = \sum_{i=1}^n c'_i 1_\mathbb{C} \otimes e_i,$$

where $c_i, c'_i = c_i r_i \in \mathbb{C}, r_i \in \mathbb{R}$. Thus we just got $\mathbb{C}^n$. From other side we can write c_i as follows: $c_i = a_i + ib_i$, where $a_i, b_i \in \mathbb{R}$. Therefore

$$x = \sum_{i=1}^n a_i r_i 1 \otimes e_i + \sum_{i=1}^n b_i r_i i \otimes e_i.$$

I.e. $x \in \mathbb{R}^{2n}$ and the basis in $\mathbb{R}^{2n}$ is formed by $1 \otimes e_1, \dots, 1 \otimes e_n, i \otimes e_1, \dots, i \otimes e_n$.

Proof. The proof is the same as at proposition 4.1. Again we construct certain bilinear maps and say that those factor over the tensor product and this implies that certain families are linearly independent.

Really lets define bilinear map $f_{i_0} : B \times M \to A$ such that

$$f_{i_0}\left(b, \sum_{i=1}^{n} m_i e_i\right) = b m_{i_0} e_{i_0}$$

so there exists a linear map $\tilde{f}_{i_0}$ such that $f_{i_0} = \tilde{f}_{i_0}\phi$ or

$$f_{i_0}\left(b, \sum_{i=1}^{n} m_i e_i\right) = \tilde{f}_{i_0}\left(\phi\left(b, \sum_{i=1}^{n} m_i e_i\right)\right)$$
$$= \tilde{f}_{i_0}\left(b \otimes \sum_{i=1}^{n} m_i e_i\right) = b\tilde{f}_{i_0}\left(1_B \otimes \sum_{i=1}^{n} m_i e_i\right) = b m_{i_0}$$

i.e. it sends $1_B \otimes e_{i_0}$ to 1 and all others $1_B \otimes e_i$ to 0. Thus the following sum $\sum \alpha_i 1_B \otimes e_i$ is equal to 0 if and only if $\alpha_i = 0$ i.e. $\alpha_i 1_B \otimes e_i$ forms a basis. □

Remark 4.2. *We have the following maps.*

- *For A - modules: $\alpha : M \xrightarrow[m \to 1_B \otimes_A m]{} B \otimes_A M$ which makes a B-module from an A-module.*
- *For B - modules: $\mu : B \otimes_A N \xrightarrow[b \otimes n \to bn]{} N$.*

Theorem 4.1 (Base-change)**.** *Let A is a Ring and B is A-algebra. Let also M is an A-Module and N is B-module.*

$$Hom_A(M, N) \leftrightarrow Hom_B(B \otimes_A M, N)$$

I.e. the homomorphisms [14] *are the same or in other words the corresponding groups of homomorphisms are isomorphic:*

$$Hom_A(M, N) \cong Hom_B(B \otimes_A M, N)$$

[14] A-homomorphisms between A modules $Hom_A(M, N)$ are the same as B-homomorphisms between B modules $Hom_B(B \otimes_A M, N)$.

Proof. First of all we have [15] Homomorphism $f : B \otimes_A M \to N$. We also have the following map (see remark 4.2): $\alpha : M \to B \otimes_A M$. Thus $f \cdot \alpha : M \to N$ i.e. we can set the following relation

$$\hat{f} : Hom_B (B \otimes_A M, N) \to Hom_A (M, N)$$

such that $\hat{f}(f) = f\alpha$.

In other direction we have $g : M \to N$ thus $id_B \otimes g : B \otimes_A M \to B \otimes_A N$ but (see remark 4.2) we have $\mu : B \otimes_A N \to N$ i.e. we have the following relation

$$\hat{g} : Hom_A (M, N) \to Hom_B (B \otimes_A M, N)$$

such that

$$\hat{g}(g) = \mu \cdot (id_B \otimes g).$$

And we can check that those maps ($\hat{f}$ and $\hat{g}$) are mutually inverse. For the proof [16] the fact consider the following diagram

$$\begin{tikzcd}
M \arrow[rr, shift left, "f\alpha"] \arrow[rr, shift right, "g"'] \arrow[dr, "\alpha"'] & & N & \\
& B \otimes_A M \arrow[ur, "f"] \arrow[rr, "id_B \otimes g"] & & B \otimes_A N \arrow[ul, "\mu"']
\end{tikzcd}$$

One can conclude (as soon as the diagram commutes)

$$\hat{f}(\hat{g}(g)) = \mu \cdot (id_B \otimes g) \cdot \alpha = g.$$

I. e. $\hat{f} \circ \hat{g} = id$ [17] or in other words $\hat{f}$ and $\hat{g}$ are mutually inverse. $\square$

4.4 Examples. Tensor product of algebras

Proposition 4.4. *If $I \subset A$ - is an Ideal so my B - A algebra will be $B = A/I$ then*

$$A/I \otimes_A M \cong M/IM$$

Proof. We have map $\alpha : M \to B \otimes_A M = A/I \otimes_A M$ (see remark 4.2) which sends m to $\bar{1} \otimes m$. [18] The map sends IM to 0 because $\forall i \in I, m \in M : im \to$

[15] One homomorphism from $Hom_B (B \otimes_A M, N)$

[16] It's missed in the lectures

[17] Operation $\circ$ is defined as follows $(\hat{a} \circ \hat{b})(x) = \hat{a}(\hat{b}(x))$ where $\hat{a}, \hat{b}$ are 2 maps acting on a set X and $x \in X$.

[18] $\bar{1} = 1_A + I$

$\bar{1} \otimes im = \bar{i} \otimes m$ because the tensor product is over A and everything is A linear and as result $\bar{1} \otimes im = \bar{i} \otimes m$, but $\bar{i} \otimes m = \bar{0} \otimes m = 0$. [19] Thus α sends IM to 0. So α induces $\bar{\alpha} : M/IM \to A/I \otimes_A M$ such that $\bar{\alpha}(\bar{m}) = \bar{1} \otimes m$.

For other direction we apply Base-change theorem. The following map (projection) of A-modules

$$M \xrightarrow{m \to \bar{m}} M/IM$$

gives us the following map of B-modules [20]

$$\bar{\beta} : B \otimes_A M \to M/IM$$

i.e.

$$\bar{\beta} : A/I \otimes_A M \to M/IM$$

that sends $\bar{a} \otimes m$ to $a\bar{m}$ Ones check again that this inverse to $\bar{\alpha}$. [21] □

Several examples:

Example 4.3. *Let $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$ what will we obtain?*

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \cong^{\mathbb{Z}/3\mathbb{Z}} /_{(2)\cdot\mathbb{Z}/3\mathbb{Z}}$$

but 2 is invertible: $2^{-1} = -1 \mod 3$ [22] *thus* $(2)\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$ *and as result*

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \cong^{\mathbb{Z}/3\mathbb{Z}} /_{\mathbb{Z}/3\mathbb{Z}} = 0$$

Example 4.4. *Another obvious example* [23]

$$B \otimes_A A[X] \cong B[X]$$

and more interesting one

$$B \otimes_A A[X]/(P) \cong B[X]/(P),$$

there (P) becomes an ideal generated by P in $B[X]$.

[19] because $\bar{i} = 0 \mod I$

[20] just ignore B: $B \otimes_A M \to M \to M/IM$.

[21] For example $\bar{\beta}(\bar{\alpha}(\bar{m})) = \bar{\beta}(\bar{1} \otimes m) = \overline{1 \cdot m} = \bar{m}$

[22] I.e. there exist an invertible element $2^{-1} \in \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$ therefore $1_{\mathbb{F}_3} \in 2 \cdot \mathbb{F}_3$ or $2 \cdot \mathbb{F}_3 = \mathbb{F}_3$ and as result $(2) \cdot \mathbb{F}_3 = \mathbb{F}_3$

[23] $B \otimes_A A[X]$ has the following B-basis: $\{1_B \otimes X^i\}$ thus $\forall b \in B \otimes_A A[X]$ we can get

$$b = \sum b_i \cdot 1_B \otimes X^i$$

and there is an obvious isomorphism

$$f : B \otimes_A A[X] \xrightarrow[b \to \sum b_i X^i]{} B[X]$$

4.4.1 Tensor product of A-algebras

Let B, C are A-algebras. The following maps form an algebra structure on A:

$$\alpha : A \to B$$

$$\beta : A \to C$$

New A-algebra $B \otimes_A C$: is a ring with respect to the following operation [24]

$$(b \otimes c) \cdot (b' \otimes c') = (b \cdot b') \otimes (c \cdot c') \tag{4.1}$$

The tensor product has the following

Definition 4.3 (Universal property). *Let we have the following maps*

$$\begin{aligned} \alpha &: A \to B, \\ \beta &: A \to C, \\ \phi : B &\xrightarrow[b \to b \otimes 1_C]{} B \otimes_A C, \\ \psi : C &\xrightarrow[c \to 1_B \otimes c]{} B \otimes_A C \end{aligned}$$

Then for any A-algebra D one has

$$Hom_A (B \otimes_A C, D) \leftrightarrow Hom_A (B, D) \times Hom_A (C, D)$$

i.e. if I have some Homomorphism $h \in Hom_A (B \otimes_A C, D)$ this is the same as giving 2 homomorphisms $f \in Hom_A (B, D)$ and $g \in Hom_A (C, D)$ such that all maps in the following diagram commute (see Commutative diagram).

$$\begin{tikzcd}
D & & B \otimes C \arrow[ll, bend right, "h"'] & \\
& B \arrow[ul, dashed, "f"] \arrow[ur, "\phi"] & & C \arrow[ul, "\psi"'] \arrow[ulll, dashed, bend left, "g"] \\
& & A \arrow[ul, "\alpha"] \arrow[ur, "\beta"'] &
\end{tikzcd}$$

Thus if we have h then we can define $f = h \cdot \phi$ and $g = h \cdot \psi$. And conversely if I have f and g then I can define h by the following rule:

$$h (b \otimes c) = f(b) \cdot g(c)$$

[24] that makes it A-algebra (see K-algebra)

The main point for us is that the tensor product of the A-algebras is itself an A-algebra by this very simple rule, component-wise multiplication (see (4.1)).

Let consider next example. We will start with the following

$$\mathbb{C} \cong \mathbb{R}[X]/\left(X^2+1\right)$$

therefore with result from example 4.4 one can get

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X]/\left(X^2+1\right) \cong {}^{\mathbb{C}[X]}/_{(X^2+1)}$$

but by Chinese remainder theorem

$${}^{\mathbb{C}[X]}/_{(X^2+1)} \cong {}^{\mathbb{C}[X]}/_{(X+i)} \times {}^{\mathbb{C}[X]}/_{(X-i)} \cong \mathbb{C} \times \mathbb{C}$$

As result we have that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not a field because it has zero divisors. How we can get the zero divisors? The element $\overline{X+i}$ is a zero divisor in ${}^{\mathbb{C}[X]}/_{(X^2+1)}$ because

$$(X+i)(X-i) \equiv 0 \mod \left(X^2+1\right)$$

.

Another proof (not a part of the lecture) of the fact that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not a field consider the following one

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong {}^{\mathbb{C}[X]}/_{(X^2+1)}$$

but the polynomial $X^2+1 = (X+i)(X-i)$ is reducible in $\mathbb{C}[X]$ i.e. is not a Maximal ideal (see theorem A.8) and with the theorem A.9 the quotient by the polynomial is not a field (see also section 1.1.4).

4.5 Relatively prime ideals. Chinese remainder theorem

Definition 4.4 (Relatively prime ideals)**.** *Let A - Ring and I, J are Ideals. I and J are relatively prime if $I + J = A$.*

Lemma 4.3.

1. *If I, J are relatively prime then $IJ = I \cap J$*
2. *If $I_1, \dots, I_k$ relatively prime with J then $\prod_{i=1}^{k} I_i = I_1 \dots I_k$ is also relatively prime with J.*
3. *If I, J relatively prime then I^k and J^l are also relatively prime for any l and k.*

Proof. 1. The following one $IJ \subset I \cap J$ is clear [25] If I and J are relatively prime then $1_A = i + j$ for some $i \in I$ and $j \in J$. Thus $\forall x \in I \cap J$ we have the following ones: $xi \in IJ$ and $xj \in IJ$ and as result

$$x = xi + xj \in IJ$$

i.e. $I \cap J \subset IJ$.

2. Suppose for simplicity that $k = 2$. In the case we have $1_A = i_1 + j_1 = i_2 + j_2$ where $i_1 \in I_1, i_2 \in I_2$ and $j_1, j_2 \in J$. we also have

$$1_A = (i_1 + j_1)(i_2 + j_2) = i_1 i_2 + (j_1 i_2 + j_2 i_1 + j_1 j_2) \in I_1 I_2 + J$$

thus $\forall x \in A$ we have

$$x = 1_A x = i_1 i_2 x + (j_1 i_2 + j_2 i_1 + j_1 j_2)\, x \in I_1 I_2 + J,$$

i.e. $I_1 I_2 + J = A$ therefore $I_1 I_2$ and J are relatively prime.

3. is obvious [26]

□

Theorem 4.2 (Chinese remainder theorem)**.** *Let $I_1, \dots, I_n$ - ideals and map $\pi : A \to A/I_1 \times \cdots \times A/I_n$ defined as follows*

$$\pi(a) = (a \mod I_1, \dots, a \mod I_n)$$

The kernel $\ker \pi = I_1 \cap \cdots \cap I_n$.

The π is Surjection if and only if $I_1, \dots, I_n$ are pairwise relatively prime. In that case

$$A/\cap I_k \cong A/\prod I_k \cong \prod (A/I_k)$$

27

[25] Assuming that I and J commute we have if $x \in IJ$ then $x \in I$ and if $x \in JI$ then $x \in J$ i.e. $x \in I \cap J$.

[26] It follows from the 2 because we can assume $I_i = I$ and will get that $\forall k, I^k$ is relatively prime with J. From other side we can assume $I_i = J$ and $J = I^k$ and conclude that J^l is relatively prime with I^k.

[27] See First isomorphism theorem where $G = A$, $H = A/I_1 \times \cdots \times A/I_n$, $\phi = \pi$ and with lemma 4.3 (as soon as I_k pairwise relatively prime)

$$\ker \phi = \ker \pi = I_1 \cap \cdots \cap I_n = I_1 \dots I_n.$$

Proof. Let π is Surjection. In the case $\exists a_i \in A$ such that

$$\pi(a_i) = (0, \ldots, 1(\text{ in } i\text{-th place }), 0, \ldots, 0)$$

i.e. $a_i \mod I_j = 0$ or $a_i \in I_j$ for $i \neq j$. We also have $a_i \mod I_i = 1$ thus $1 - a_i = kI_i$ i.e. $1 - a_i \in I_i$. Thus $\forall j, \exists a_i \in I_j, a_k \in I_i$ such that $1 = a_i + a_k$ thus $A = I_j + I_i$ i.e. I_i relatively prime with any I_j.

Conversely if I_i is relatively prime with any I_j where $j \neq i$ then it also relatively prime with the product (see lemma 4.3) $\prod_{j \neq i} I_j$. In the case $\exists x_i \in I_i, y_i \in \prod_{j \neq i} I_j$ such that $1 = x_i + y_i$ in the case

$$\pi(y_i) = (0, \ldots, 1(\text{ in } i\text{-th place }), 0, \ldots, 0)$$

and $\forall b_i \in A/I_i$

$$\pi\left(\sum_{i=1}^{n} b_i y_i\right) = (b_1, \ldots, b_n)$$

i.e. π is surjective. $\square$

Let K is a field and A is a finite (finite dimensional vector space) K-algebra.

Proposition 4.5. *1. If A is an Integral domain then A is a field.*

2. (replacing the first one) Any Prime ideal of A is a Maximal ideal

Proof. Well, I shall prove only the first part, the second part is just a consequence of definitions. In fact, a factor over a prime ideal, a quotient over a prime ideal is an integral domain, and a quotient over a maximal ideal is a field. [28] If you don't know this, please look it up in any book.

Lets prove the first part. Integral domain means that there is no zero divisors i.e. $\forall a \in A$ [29] multiplication by a is Injection. A is finite dimensional Vector space (see above) that implies that $\times a$ is an Isomorphism, [30] in particular Surjection i.e. $\exists b \in A$ such that $b \times a = 1$ i.e. a is invertible therefore A is field. $\square$

[28] i.e. prime ideal is a maximal ideal

[29] $a \neq 0_A$

[30] $\times a$ sends a vector space into another vector space with the same dimension. But with lemma About vector space isomorphism one can get that the spaces are isomorphic each others and as result the operation $\times a$ is an Isomorphism.

4.6 Structure of finite algebras over a field. Examples

Remark 4.3. *The remark is not a part of the lectures but it is important to understand the below content.*

Let A is a K-algebra and m is a maximal ideal of A. Then A/m is also K-algebra.

Proof. Lemma 1.1 says that there is a ring homomorphism between K and A: $f_K : K \to A$. There is also a canonical homomorphism $f_A : A \underset{a \to \bar{a}}{\longrightarrow} A/m$. Therefore we can define $f = f_A f_K : K \to A/m$ and therefore with lemma1.1 can conclude that A/m is a K-algebra. [31]

Note that if A is a field then f_A is injection, $m = \{0_K\}$ and $A = A/m$. □

Theorem 4.3 (Structure of finite K-algebra)**.** *Let A be a finite K-algebra i.e. $\dim_K A < \infty$. Then*

1. *There are only finitely many Maximal ideals $m_1, \dots, m_r$ in A*
2. *Let $J = m_1 \cap \dots \cap m_r = m_1 \dots m_r$.* [32] *Then $J^n = 0$ for some n*
3. *$A \cong A/m_1^{n_1} \times \dots \times A/m_r^{n_r}$ for some $n_1, \dots, n_r$.*

Proof. 1. Let $m_1, \dots, m_i$ are maximal ideals. By Chinese remainder theorem we have [33]

$$A/m_1 \dots m_i \cong A/m_1 \times \dots \times A/m_i.$$

We know that A as well as $A/m_1 \dots m_i$ and A/m_k are finite dimensional K-Vector space [34] thus we have the following relations

$$\dim_K A \geq \dim_K A/m_1 \dots m_i = \sum_{j=1}^{i} dim_K A/m_j \geq i.$$

Therefore if N the number of maximal ideals then $\dim_K A \geq N$ i.e. the number of maximal ideal is limited by the vector space dimension.

[31] Thanks Zonglin Jiang for the proof.

[32] Since the ideals are relatively prime the intersection is the same as the product of the ideals

[33] Maximal ideals are relatively prime because in a commutative ring with unity, every Maximal ideal is a Prime ideal see also proposition 4.5.

[34] See remark 4.3 and take into consideration the theorem statement (see above) that says $\dim_K A < \infty$. A/m_1 is a projection i.e. $\dim_K A/m_1 < \dim_K A < \infty$.

2. $J = m_1 \cap \dots \cap m_r = m_1 \dots m_r$ is finite dimensional vector space over K as well as its powers J^k. We have the following sequence [35]

$$\dots \subseteq J^k \subseteq \dots \subseteq J^2 \subseteq J.$$

and the sequence should stop somewhere [36] i.e. $\exists n$ such that $J^n = J^{n+1}$. We claim that $J^n = 0$ in the case. Indeed if not we have the following basis of J^n: $e_1, \dots, e_s$. And as soon as $J^n = JJ^n$ we can write a vector $e_i \in J^n$ as a vector from J^n multiplied on an object from J i.e.

$$e_i = \sum \lambda_{ij} e_j,$$

there $e_j \in J^n, \lambda_{ij} \in J$. Thus if $M = id - \lambda_{ij}$

$$M \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_s \end{pmatrix} = 0.$$

It's possible over ring [37] to find a matrix $\tilde{M}$ such that

$$\tilde{M} M = \det M \cdot id,$$

i.e.

$$\det M \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_s \end{pmatrix} = 0.$$

But $\det M = 1 + \lambda$ where $\lambda \in J$. [38] Since $J = m_1 \cap \dots \cap m_r$ then $\forall i : \lambda \in m_i$ so $\nexists i$ such that $1 + \lambda \in m_i$ [39] thus $1 + \lambda$ is invertable [40] therefore $e_1 = \dots = e_s = 0$ [41]

[35] Let $j \in J \subset A$ and $x \in JJ$. Then $\exists j \in J$ such that $x = jj$ but $jj \in J$ because $\forall y \in J : jy \in J$. As result $J^2 \subseteq J$.

[36] On each step we should decrease the dimension if we don't stop. The dimension is limited and as result the sequence should stop.

[37] ???

[38] Because the det consists of the following items $\prod(1 - \lambda_{ii}) = 1 + (-1)^s \prod \lambda_{ii}$ and $\prod \lambda_{ij}$. The sum of the items (det) consists of 1 and another sum in which all items are from J. Thus the second sum is an element of J i.e. $\det M = 1 + \sum \prod \lambda_{ij} = 1 + \lambda$.

[39] We have that m_i is a Maximal ideal and therefore (by its definition) it is a Proper ideal i.e. $1 \notin m_i$. From other side if $1 + \lambda \in m_i$ then $1 + \lambda - \lambda \in m_i$ as soon as $\lambda \in m_i$. I.e. we have a contradiction.

[40] $0 \in m_i$ thus if $1 + \lambda \notin m_i$ then $1 + \lambda \neq 0$.

[41] Because $\det M = 1 + \lambda \neq 0$

3. Using part 2 $\exists n_1, \dots, n_r$ such that $m_1^{n_1} \dots m_r^{n_r} = 0$ (for example we can assume $n_i = n$). Then by Chinese remainder theorem

$$A \cong A/m_1^{n_1} \times \cdots \times A/m_r^{n_r}.$$

We used the following facts:

- $A = A/m_1^{n_1} \dots m_r^{n_r}$ [42]
- $m_i^{n_i}$ are pairwise relatively prime [43]

□

Remark 4.4. *The n_is are not uniquely defined. For example (see also example 5.1)*

$$A = {}^{K[X]} \big/ _{\left(X^2(X+1)^3\right)}.$$

We have 2 ideals there: $m_1 = (X)$ and $m_2 = (X+1)$. We of course have

$$A \cong A/m_1^2 \times A/m_2^3$$

but also we have

$$A \cong A/m_1^3 \times A/m_2^3$$

as soon as $m_1^2 = m_1^3$ in A: $(X)^2 \subset (X)^3$ but also $(X)^3 \subset (X)^2$ [44]

Several examples:

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \times \mathbb{C}.$$

Another example

$$\mathbb{Q}\left(\sqrt{2}\right) \otimes_{\mathbb{Q}} \mathbb{Q}\left(\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$$

---

[42] Because $A = A/\{0\}$. For example if $I = \{0\}$ and $x \in A$ then $\bar{x} \in A/I$ if $\bar{x} = x + I$. In our case $\bar{x} = x + \{0\} = x$ i.e. $\forall x \in A$ we have $x \in A/\{0\}$. (See also Quotient ring)

[43] As soon as $\{m_i\}$ - Maximal ideals and as result Prime ideals then with lemma 4.3 one can get that $\forall i \neq j$ $m_i^{n_i}$ is relatively prime with $m_j^{n_j}$.

[44] $(X)^3 \subset (X)^2$ - this is true for any polynomial $P(X)$ because if $P(X) \in (X)^3$ then $P(X) = X^3 P'(X) = X^2 \bar{P}(X) \in (X)^2$ where $\bar{P}(X) = X P'(X)$

$(X)^2 \subset (X)^3$ is the more complex one and it does not true for any polynomial ring but this is true for our A. Let $P(X) \in (X)^2 \subset K[X]$ then $P(X) = X^2 P'(X)$ but $X^2 P'(X) \equiv 0 \mod X^2$. From other side $X^4 P'(X) \equiv 0 \mod X^2$ therefore

$$P(X) \equiv X^3 X P'(X) \mod X^2$$

i.e. $P(X) \in (X)^3$.

And you see that those algebras are Cartesian products of fields. So all n_i's may be taken equal to 1 [45]. In other words, we don't have Nilpotent elements in our algebra [46]. So, it is a reduced algebras. Reduced, by definition, is without nilpotents. It's general phenomena because the presence of nilpotents is due to the inseparability of extensions come from inseparable extensions.

[45] Because A/m^n (where m is a maximal ideal) is a field if $n = 1$

[46] Cartesian products of fields has no nilpotent elements except 0 [7].

Chapter 5

Structure of finite K-algebras continued

We apply the discussion from the last lecture to the case of field extensions. We show that the separable extensions remain reduced after a base change: the inseparability is responsible for eventual nilpotents. As our next subject, we introduce normal and Galois extensions and prove Artin's theorem on invariants.

5.1 Structure of finite K-algebras, examples (cont'd)

Last time we have seen that a finite K-algebra A ($[A : K] < \infty$) has only finitely many maximal ideals $m_1, \dots, m_r$ and the following equation holds (see theorem 4.3):

$$A \cong A/m_1^{k_1} \times \cdots \times A/m_r^{k_r}$$

This is a general form of Chinese remainder theorem.

Example 5.1. *Let*

$$A = K\left[X\right] / \left(F\right)$$

And the polynomial F is not necessary irreducible so let's decompose into a product of irreducible factors: $F = P_1^{k_1} \dots P_r^{k_r}$. Then by the Chinese remainder theorem [1] one can get

$$A \cong K\left[X\right] / \left(P_1\right)^{k_1} \times \cdots \times K\left[X\right] / \left(P_r\right)^{k_r},$$

[1] See also remark 4.4 and theorem 4.3

where $K[X]/(P_i)^{k_i} = A/m_i^{k_i}$ *and* $m_i = (P_i \mod F)$ [2] *- an ideal.*

Definition 5.1 (Nilpotent element)**.** *Let A is a Ring than $x \in A$ is nilpotent if $x \neq 0$ but $\exists k : x^k = 0$.* [3]

Definition 5.2 (reduced)**.** *K-algebra A is reduced if it has no Nilpotent elements. Or in other words* [4] *if in the decomposition*

$$A \cong A/m_1^{k_1} \times \cdots \times A/m_r^{k_r}$$

$\forall i : k_i = 1$. Or [5] *if A is a product of fields.*

Definition 5.3 (local)**.** *Ring A is called local if it has only one Maximal ideal i.e. $A \cong A/m^k$.*

If A is local then all elements of A are nilpotents i.e. any element of A is a identity,zero or nilpotent [6] [7] .

Most of our last examples were examples of reduced K-algebras such as

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \times \mathbb{C}$$

---

[2] Using definition A.34 one can get that $P_i \in K[X]$ corresponds to $P_i \mod F$ in $A = K[X]/(F)$ therefore we have (P_i) is a Maximal ideal for $K[X]$ and

$$A/(P_i)^{k_i} = K[X]/(P_i \mod F)^{k_i}.$$

but $P_i \mod F = P_i$ and as result

$$K[X]/(F) \cong K[X]/(P_1)^{k_1} \times \cdots \times K[X]/(P_r)^{k_r}.$$

[3] Alternative definition from [32]: An element, x, of a ring, R, is called nilpotent if there exists some positive integer, n, such that $x^n = 0$.

[4] Let we have an i-th element of the product $\prod A/m_i^{k_i}$ with $k_i > 1$ and $m_i = (p)$ when $p \in A/m_i^{k_i}$ and $p \neq 0 = p^{k_i}$ i.e. p is a nilpotent.

[5] A/m_i is a field as soon as m_i is a Maximal ideal

[6] As it was mentioned in [29], a nonzero ring in which every element is either a unit or nilpotent is a local ring, but not reverse, as it was pointed on the lectures. There is also an example $A \cong A/\{0\}$ where A is a Field and $\{0\}$ is the only maximal ideal for the fields (see example A.14). In this case there are many non nilpotents different from identity and zero but the ring (K-algebra) is local.

[7] Comment from Staff on the issue: It looks confusing because Katya immediately applies this definition to the case of finite algebras without explicitly mentioning.

You are right that it is not true in general. For example, discrete valuation rings are local and have no zero divisors at all. (Also your counterexample is not quite correct, because a field is exactly the case when every element is either invertible or nilpotent).

But if a finite algebra has only one maximal ideal, then by the structural theorem it consists of nilpotents.

or

$$\mathbb{Q}\left(\sqrt{2}\right) \otimes_{\mathbb{Q}} \mathbb{Q}(i) = \mathbb{Q}\left(i, \sqrt{2}\right)$$

that is a field and if we start producing similar examples then mostly they are reduced. Well, why? Because in fact the presence of nilpotents has to do with inseparability. The presence of nilpotents reflects inseparability.

So let me give you one more example: tensor product of extensions which is not reduced. Let K be a field of characteristic p, for instance $\mathbb{F}_p$. Consider a field of rational functions over K [8] : $K(X)$. We will consider $K(X)$ as an extension of $K(X^p)$ (or with new variable $Y = X^p$ - $K(Y)$. We will be interested in $K(X) \otimes_{K(Y)} K(X)$ where X is a pth root of Y so [9]

$$\begin{aligned} K(X) \otimes_{K(Y)} K(X) &\cong \\ \cong K(X) \otimes_{K(Y)} K[T] / (T^p - Y) &\cong \\ \cong K(X)[T] / (T^p - Y) &= \\ = K(X)[T] / (T^p - X^p) = K(X)[T] / (T - X)^p & \end{aligned}$$

where T is another variable. As result we have got a ring with nilpotents for example $T - X$ and of course the reason is that our extension $K(X)$ is pure inseparable extension (see definition 3.9) of $K(Y)$.

5.2 Separability and base change

What is the reason for such a mysterious connection between presence of nilpotents and separability? If L is separable over K then the number of Homomorphisms $\left|Hom_K\left(L, \bar{K}\right)\right|$ is maximal and equal to degree $[L : K]$ but in general it is less or equal to the degree. This is of course clear, because if we have a polynomial with distinct roots, then it's stem field for instance has exactly this number of homomorphisms into the-algebraic closure and this number is equal to the number of roots. So if some roots coincide, then the number of homomorphisms diminishes.

Lets also recall Base-change. If L and E are extensions of K and L is finite over K then

$$Hom_K(L, E) \cong Hom_E(L \otimes_K E, E).$$

In the formula, $L \otimes_K E$ is a finite E-algebra denoted as A below.

[8] As it was shown in example 3.5 (part 3) it's not a Perfect field and as result of theorem 3.6 is not separable.

[9] as soon as $K(X) = K[T] / (T^p - Y)$

Remark 5.1. *The remark is not a part of the lectures but it is important to understand the below content.*

We have that $A = L \otimes_K E \cong E \otimes_K L$ *is a free* E *module as soon as* L *is a free* K *module and with proposition 4.3 we have that* $[A : E] < \infty$ *(as soon as* $[L : K] < \infty$*) and as result with theorem 4.3 one can get that there are finitely many maximal ideals* m_i *and*

$$A \cong A/m_1^{k_1} \times \cdots \times A/m_r^{k_r}$$

Definition 5.4. *With Chinese remainder theorem theorem we have*

$$A \cong A/m_1^{k_1} \times \cdots \times A/m_r^{k_r}$$

Reduced algebra A_{red} *is defined by the following equation*

$$A_{red} = A/m_1 \times \cdots \times A/m_r$$

We have that [10]

$$A_{red} = A/\eta\,(A)$$

where $\eta\,(A)$ is an Ideal of nilpotents in A.

It is clear that

$$Hom_E\,(A, E) = Hom_E\,(A_{red}, E)$$

because all homomorphism into a field must be zero on all nilpotents [11].

So again, we see that if there are nilpotents in the tensor product, then there is somehow fewer space for homomorphisms. Because if A is not reduced, then the dimension

$$[A_{red} : E] < [A : E]\,.$$

[10] i.e. nilpotents become zeros in the A_{red}.

[11] It requires some clarification. Consider a homomorphism $\phi \in Hom_E\,(A, E)$. $\forall x, y \in A, \phi(xy) = \phi(x)\phi(y)$. Let $x \in \eta\,(A)$ i.e. x is a nilpotent then $x \neq 0_A, x^k = 0_A$. We have

$$0_E = \phi(x^k) = \phi(x)^k$$

i.e. $\phi(x) = 0_E$. Therefore all nilpotents go to zero and, instead of A (as the set the ϕ acts on), we can consider A_{red}. As result, we will get that $\phi(0_{A_{red}}) = 0_E$ and all other properties of homomorphism are also hold, for instance $\forall \bar{x}, \bar{y} \in A_{red} : \phi(\bar{x} + \bar{y}) = \phi(\bar{x}) + \phi(\bar{y})$. Really $\bar{x} = x + \eta(A), \bar{x} = x + \eta(A)$ and

$$\phi(\bar{x} + \bar{y}) = \phi(x + y) = \phi(x) + \phi(y) = \phi(\bar{x}) + \phi(\bar{y})$$

as soon as $\phi(\eta(A)) = 0_E$.

So the maximal number of homomorphisms, so let's say the slogan "Maximal number of homomorphisms" is attained when A is reduced and all quotients

$$A/m_i \cong E \tag{5.1}$$

because those quotients are of course extensions of E. [12] In general, those quotients are extensions of E (see remark 4.3). We also have

$$A \cong A/m_1 \times \cdots \times A/m_r$$

but $Hom\,(A/m_i, E) = \{0\}$ if $[A/m_i : E] > 1$. This is because a field homomorphism is always injective. A field homomorphism a homomorphism of fields which are extensions of E an E-homomorphism is injective. So you cannot map an E-vector space of dimension greater than 1 into an E-vector space of dimension 1.

Lets take $E = \bar{K}$ then automatically we will get $A/m_i \cong E$ because an algebraically closed field does not have a non trivial finite extension.

So what have we had (see also example 5.2)?

$$A = L \otimes_K \bar{K},$$

$$A_{red} = \prod_{i=1}^{r} \bar{K}.$$

The following one $A = A_{red}$ is the same to r is maximal and equal to $[L : K] = \left[A : \bar{K}\right]$. [13] In the case

$$r = \left|Hom_{\bar{K}}\left(A, \bar{K}\right)\right| = \left|Hom_K\left(L, \bar{K}\right)\right|$$

[12] as it was mentioned above $A = L \otimes_K E$ is a finite E-algebra i.e. A is a E-extension. The A/m is also E-algebra (see remark 4.3) i.e. also E-extension.

From other hand we consider $Hom\,(A/m_i, E)$ i.e. there is a homomorphism (injection) from $A/m_i \to E$ and as result $A/m_i \cong E$. These arguments are also used in the text below for the fact explanation.

[13] It is because there are $[L : K] = r$ roots of a polynomial and all the roots are in $\bar{K}$. Each root α_i forms a polynomial $X - \alpha_i$ which creates an ideal $m_i = (X - \alpha_i)$. We also have $L = K\left(\alpha_1, \ldots, \alpha_r\right)$ and

$$A = L \otimes_K \bar{K} \cong \bar{K} \otimes_K L = \bar{K} \otimes_K K\left(\alpha_1, \ldots, \alpha_r\right).$$

It expands to (see example 4.4)

$$A \cong \bar{K} \otimes_K \frac{K\,[X]}{(X - \alpha_1)\ldots(X - \alpha_r)} \cong$$
$$\cong \frac{\bar{K}\,[X]}{(X - \alpha_1)} \times \cdots \times \frac{\bar{K}\,[X]}{(X - \alpha_r)} \cong \bar{K} \times \cdots \times \bar{K}.$$

So this explains why seperability is the same thing as the absence of nilpotents. So let me formulate it as a theorem.

Theorem 5.1. *Let L is a finite extension over K then*

1. *L is separable if and only if $L \otimes_K \bar{K}$ is reduced. L is pure inseparable if and only if $L \otimes_K \bar{K}$ is local*

2. *L is separable if and only if for all algebraic extension Ω, $L \otimes_K \Omega$ is reduced. L is pure inseparable if and only if for all algebraic extension Ω, $L \otimes_K \Omega$ is local.*

3. *If L is separable then the map*

$$\phi : L \otimes_K \bar{K} \to \bar{K}^n$$

which sends

$$\phi (l \otimes k) = (k\phi_1 (l), \ldots, k\phi_n (l))$$

where ϕ_i are distinct homomorphisms from L to $\bar{K}$, is an isomorphism.

Proof.

1. L separable is the same thing that the algebra $A = L \otimes_K \bar{K}$ has $[L : K]$ factors [14] $\bar{K}$ which is the same as A is reduced since $\dim_{\bar{K}} A = [L : K]$. [15]

   L is pure inseparable: this means that exists only one homomorphism of L into $\bar{K}$ i.e. A has only one $\bar{K}$-homomorphism into $\bar{K}$ thus only one factor and as result A is local.

2. If Ω is an algebraic extension then [16]

$$L \otimes_K \Omega \hookrightarrow L \otimes_K \bar{\Omega} = L \otimes_K \bar{K}.$$

   There is a sub-ring and so one easily checks, that a sub-ring of a reduced algebra is reduced and same for local.

[14] If we have $L = K(\alpha)$ (see theorem 3.5) then there exists a minimal polynomial $P_{min}(\alpha, K)$ of degree $r = [L : K]$. The polynomial splits and has r roots: $\alpha_1, \ldots, \alpha_r$. Thus we have r maximal ideals $m_1 = (X - \alpha_1), \ldots, m_r = (X - \alpha_r)$. For each maximal ideal we have $A/m_i \cong A$ (see example 1.4) thus with theorem 4.3 and (5.1) we have

$$A \cong \prod_{i=1}^{r} \bar{K}$$

[15] see example 1.4.

[16] see definition A.63

3. Leave as an excises [17]

$\square$

Remark 5.2. *In general for modules M, N and P over a ring R* ***not true*** *that if $M \hookrightarrow N$ (M is a sub module of N) then $M \otimes_R P \hookrightarrow N \otimes_R P$. But this become the truth if R is a field and as result M, N, P are Vector spaces. So, for my field extensions, I can say that if I have an extension and then I take a base change, then it remains an extension, but you should not think that the same thing is true for arbitrary modules over a ring.*

Example 5.2. *The example is not a part of lectures and was taken from [4]. Consider extension $\mathbb{Q}\left(\sqrt{2}\right)$ over $\mathbb{Q}$. Since*

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

tensoring with $\mathbb{Q}$ gives

$$\begin{aligned} \mathbb{Q}\left(\sqrt{2}\right) \otimes_{\mathbb{Q}} \bar{\mathbb{Q}} \cong \bar{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}\left(\sqrt{2}\right) \cong \\ \cong \bar{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}\left[X\right] / \left(X^2 - 2\right) \cong \\ \cong \bar{\mathbb{Q}}\left[X\right] / \left(\left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)\right) \cong \\ \cong \bar{\mathbb{Q}}\left[X\right] / \left(X - \sqrt{2}\right) \times \bar{\mathbb{Q}}\left[X\right] / \left(X - \sqrt{2}\right) \cong \bar{\mathbb{Q}} \times \bar{\mathbb{Q}} \end{aligned}$$

We used the following fact (see example 1.4)

$$\bar{\mathbb{Q}}\left[X\right] / \left(X \pm \sqrt{2}\right) \cong \bar{\mathbb{Q}}$$

5.3 Primitive element theorem

Definition 5.5 (Idempotent)**.** *The element x is called idempotent if $x \cdot x = x$*

[17] We have that $\forall l \otimes k \in L \otimes_K \bar{K}, \exists \bar{k}^n = \left(k\phi_1\left(l\right), \ldots, k\phi_n\left(l\right)\right) \in \bar{K}^n$.

From other side $\{\phi_i\}$ - distinct homomorphisms and can be considered as distinct Characters. Therefore by theorem A.10 the homomorphisms are linearly independent i.e. form a basis in $\bar{K}^n$. I.e. any $\bar{k}^n \in \bar{K}^n$ can be represented as

$$\bar{k}^n = k\left(\phi_1\left(l\right), \ldots, \phi_n\left(l\right)\right)$$

where $k \in \bar{K}$ and $l \in L$.

Theorem 5.2 (Primitive element). *Let L is a finite Separable extension of K then it has only finitely many sub extensions i.e. E such that $K \subset E \subset L$.*

Proof. So, let's base change to $\bar{K}$ [18] :

$$E \otimes_K \bar{K} \hookrightarrow L \otimes_K \bar{K}$$

. We also have (see also example 5.2)

$$E \otimes_K \bar{K} \cong \bar{K}^m$$

and

$$L \otimes_K \bar{K} \cong \bar{K}^n$$

are reduced $\bar{K}$ sub-algebras generated by Idempotents namely by $(0, 0, \dots, 1, \dots, 0)$ where 1 is in i-th place.

On the other hand $L \otimes_K \bar{K} \cong \bar{K}^n$ has only finitely many Idempotents because $(a_1, \dots, a_i, \dots, a_n)$ is an idempotent if and only if all a_i are 0 or 1 and therefore there are only finitely many ways to choose m idempotents out of them, so there is only finitely many ways to generate a subalgebra. □

Corollary 5.1 (Primitive element theorem). *$\exists \alpha \in L$ such that $L = K(\alpha)$ whenever L is finite and separable.*

Proof. And this is easy to see, of course, because if L and K are infinite, then L cannot be a union, a finite union of proper subextension. A vector space over an infinite field is not a finite union of proper subspaces. For instance a plane is not a finite union of lines. [19]

[18] see proof of theorem 5.1 (second part of it).

[19] It will require some additional explanations. Took $\alpha \in L$ such that $P_{min}(\alpha, K)$ has maximal degree. If $K(\alpha) = L$ we complete and found the primitive element. If not then let $\beta \in L \setminus K(\alpha)$. Consider the following element $\gamma_a = \alpha + a\beta$ where $a \in K$. For any $a \in K$ exists $K(\gamma_a)$ such that $K \subset K(\gamma_a) \subset L$. We have $|K| = \infty$ but the number of sub-extensions is limited by theorem 5.2 therefore $\exists a, b \in K$ such that $a \neq b$ and $K(\gamma_a) = K(\gamma_b) = K(\gamma)$ where $\gamma = \gamma_a$.

We have $\gamma_a - \gamma_b = (a - b)\beta \in K(\gamma)$, i.e. $\beta \in K(\gamma)$. Therefore $\alpha = \gamma_a - a\beta = \gamma - a\beta \in K(\gamma)$. We also have (as soon as $\beta \notin K(\alpha)$) $K \subset K(\alpha) \subsetneq K(\gamma) \subset L$. Thus $[K(\gamma) : K] > [K(\alpha) : K]$. Therefore (see proposition 1.4)

$$\deg(P_{min}(\gamma, K)) > \deg(P_{min}(\alpha, K))$$

that is in contradiction with α choose.

Note that [1] has another, more known, proof for the fact and prove that if $L = K(\alpha, \beta)$ then $\exists \lambda \in K$ such that $\gamma = \alpha + \lambda\beta$ is the primitive element i.e. $L = K(\gamma) = K(\alpha, \beta)$.

If L and K are Finite fields, then we have already described this situation completely. We have described all finite extensions and have seen that they are generated by one element. [20] $\square$

5.4 Examples. Normal extensions

5.4.1 Examples

Example 5.3 (Primitive element).

$$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right).$$

We have $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 4$ *so all sub-extensions are quadratic.* [21] *As no quadratic polynomial has* $\alpha = \sqrt{2} + \sqrt{3}$ *for a root* [22], α *generates* $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.

This must be a primitive element, generates our field. It is not contained in any proper subextension.

There is another proof (not part of the lectures) that shows that $\beta = \sqrt{2} + \sqrt{3}$ *is a primitive element i.e.* $\sqrt{2}, \sqrt{3}$ *are generated by* β. *Really* $\beta^2 = 5 + 2\sqrt{2}\sqrt{3}$ *i.e.*

$$\sqrt{2}\sqrt{3} = \frac{\beta^2 - 5}{2}.$$

From other side

$$\sqrt{2}\beta = \sqrt{2}\left(\sqrt{2} + \sqrt{3}\right) = 2 + \sqrt{2}\sqrt{3} = \frac{\beta^2 - 1}{2}.$$

Therefore

$$\sqrt{2} = \frac{\beta^2 - 1}{2\beta}$$

and

$$\sqrt{3} = \beta - \frac{\beta^2 - 1}{2\beta}.$$

---

[20] As it was mentioned in the proof of corollary 3.4 we can take $\alpha =$ generator of $K^{\times}$. For more info see corollary 3.4.

[21] As soon as extension has degree $4 = 2 \cdot 2$ then a sub-extension should have degree 2 and the minimal polynomial should be quadratic.

[22] Quadratic polynomials have very simple formula for roots with only one square (discriminant) and it is not possible to get 2 squares with it

Example 5.4 (Extension which cannot be generated by a single element). *So, take K equal to $\mathbb{F}_p$ and consider $K(x, y)$ as an extension of $K(x^p, y^p)$. It has degree p^2 [23] i.e.*

$$[K(x, y) : K(x^p, y^p)] = p^2.$$

We have $\forall \alpha \in K(x, y) \setminus K(x^p, y^p)$ is of degree p over $K(x^p, y^p)$. This is because $\alpha^p \in K(x^p, y^p)$ [24] . So, no element like these can generate our extension.

5.4.2 Normal extensions

Definition 5.6 (Normal extension). *A normal extension of K is a Splitting field of a family of polynomials [25] in $K[X]$. [26]*

Remark 5.3 (Normal extension). *So, take a bunch of polynomials in K and we adjoin all their roots to K, and this is what is called a normal extension. For instance, a Splitting field of one polynomial is also a normal extension.*

Theorem 5.3. *The following conditions are equivalent for an extension L of K:*

1. *$\forall x \in L$ $P_{min}(x, K)$ splits in L.*
2. *L is Normal extension*
3. *All Homomorphisms from L to $\bar{K}$ have the same image.*

---

[23] $K \subset K(x^p) \subset K(x^p, y^p)$ and $[K(x^p) : K] = p$ as well as $[K(x^p, y^p) : K(x^p)]$ thus with theorem 1.1

$$[K(x^p, y^p) : K] = p^2.$$

[24] $\alpha = k_1 x + k_2 y$, where $k_1, k_2 \in K = \mathbb{F}_p$. Using remark 3.2 we can get

$$\alpha^p = k_1^p x^p + k_2^p y^p \in K(x^p, y^p).$$

[25] There is a set of polynomials (can be only one polynomial in the set) and the polynomials not necessary to be irreducible. Example $\mathbb{Q}/\mathbb{Q}$ - is a normal extension because there is a set of polynomials split in it : $\{X - 1, X^2 - 1\}$. Note that any irreducible polynomial (another definition below) that has a root in it also splits, for instance $X - a$, where $a \in \mathbb{Q}$ is an irreducible, has a root $a \in \mathbb{Q}$ and splits in it. From other side an irreducible polynomial (for example $X^3 - 1$) can have a root in $\mathbb{Q}$ but does not necessary split in it.

[26] Another good definition of a normal extension [6] can also be used. Normal extension E/K is such algebraic extension in which every irreducible polynomial $P(X) \in K[X]$ that has a single root in E splits in E.

4. *The Group of Automorphisms $Aut\,(L/K)$ acts transitively (see definition A.16) on this set of homomorphisms $Hom_K\left(L, \bar{K}\right)$.*

Proof. 1 implies 2: Take $(P_i)_{i\in I} = \{P_{min}\,(x, K) \mid x \in L\}$ - the set of polynomials (i.e. the family of polynomials). L will be a splitting field of the set $(P_i)_{i\in I}$ and therefore (by definition) L is normal.

2 implies 3: Let $S = \{\text{roots of } P_i, i \in I \text{ in } L\}$ and $S' = \left\{\text{roots of } P_i, i \in I \text{ in } \bar{K}\right\}$ [27] then any homomorphism $\phi : L \to \bar{K}$ sends S to S', but S generates L over K, so $\phi\,(S)$ determines $\phi\,(L)$ [28] .

3 implies 4: Let $j, j' \in Hom_K\left(L, \bar{K}\right)$ (i.e. we took 2 homomorphisms) then they send L isomorphically to its image L'. So, these are isomorphisms from L to L'. So

$$\begin{tikzcd} & L' \arrow[dr, "j^{-1}"] & \\ L \arrow[ur, "j'"] \arrow[rr, "j^{-1}j'"] & & L \end{tikzcd}$$

take $j^{-1} \cdot j' \in Aut\,(L/K)$ and it sends j to j' [29].

4 implies 1: I have this Transitive group action and I have to prove that any minimal polynomial splits. Consider $P_{min}\,(x, K)$. $\alpha_1, \ldots, \alpha_n$ - roots in $\bar{K}$. Then I have map $K\,(x) \to K\,(\alpha_i)$ that extends to $j_i : L \xrightarrow[x\to\alpha_i]{} \bar{K}$. This is by theorem About extension of homomorphism. $\exists \theta_i \in Aut\,(L/K)$ such that $j_1\theta_i = j_i$ [30] thus $\alpha_i \in j_1\,(L)$ [31] or all roots are in $j_1\,(L)$ and the polynomial $P_{min}\left(x, \bar{K}\right)$ splits over $j_1\,(L)$ but this means that it splits over L [32] □

5.5 Galois extensions

Now we are ready to give a definition for central object of Galois theory

Definition 5.7 (Galois extension)**.** *A Galois extension is a Normal extension and Separable extension.*

[27] S and S' are 2 sets of roots

[28] As soon as $\phi(S) = S'$ then we have one set of roots and as result one image (that is generated by the set) for homomorphisms.

[29] We have got that $\forall j, j' \in Hom_K\left(L, \bar{K}\right), \exists g \in Aut\,(L/K)$ such that $g(j) = j'$, for instance $g = j^{-1}j'$ and

$$g(j) \equiv jg = jj^{-1}j' = j'. \tag{5.2}$$

Therefore group automorphisms acts transitively by the definition A.16

[30] as it was mentioned at the equation (5.2)

[31] $\theta_i : L \to L$ thus $j_1\theta_i : L \to j_1(L)$

[32] If $x = \alpha_1$ then $j_1 = id$ and $j_1(L) = L$

Theorem 5.4. *Let L be a finite over K then the number of automorphisms $Aut\,(L/K)$ is less or equal to degree $[L:K]$:*

$$|Aut\,(L/K)| \leq [L:K]\,.$$

The equality holds if and only if L is Galois extension.

Proof. We know that the group of automorphisms $Aut\,(L/K)$ acts freely (see definition A.17) on the set $Hom_K\left(L, \bar{K}\right)$, [33] so the number of automorphisms $|Aut\,(L/K)|$ is equal to the number of Orbit of this action which is less or equal [34] to the cardinality of the set it self: $\left|Hom_K\left(L, \bar{K}\right)\right|$. The equality holds whenever (if and only if) Action is Transitive group action. We just seen in theorem 5.3 that this means that L is normal over K. So we have

$$|Aut\,(L/K)| \leq \left|Hom_K\left(L, \bar{K}\right)\right| \leq [L:K]\,.$$

The first inequality become equality if L is normal and the second one if L is separable [35], thus

$$|Aut\,(L/K)| \leq [L:K]$$

and equality holds if L is both normal and separable i.e. if it's Galois extension. □

Definition 5.8 (Set of invariants)**.** *If group G acts on a set X then $X^G = \{x \in X \text{ such that } gx = x, \forall g \in G\}$ - the set of invariants.*

Remark 5.4 (on normal extensions)**.** *If L is normal over K then*

1. *If we have an Isomorphism of sub-extensions ($K \subset L_1, L_2 \subset L$) $\phi : L_1 \cong L_2$ then it extends to an Automorphism of L. To see this, we embed L into an algebraic closure $\bar{K}$. And remark that ϕ extends to a map from L_1 to $\bar{K}$, but all those maps have the same image (see theorem 5.3), namely L [36].*

[33] ??? Note that the number of distinct roots is equal to the number of distinct homomorphisms (see proposition 3.2). Thus we can set an association between roots and homomorphisms. Proposition 2.1 says that the stem field isomorphism (that translated to the considered automorphism) is unique determined by it's value on the roots that it exchanges. I.e. the the action of $Aut\,(L/K)$ on the set of roots (and as result on the set $Hom_K\left(L, \bar{K}\right)$) is exactly that one defined for Free group action.

See also first and second remarks at 5.4.

[34] in ideal case each element has an unique orbit and the number of elements and the number of orbits are equal.

[35] see definitions 3.7 and 3.8.

[36] Consider $L_1 \subset L_2 \subset \bar{K}$ we have a homomorphism $\phi : L_1 \to L_2$ (our isomorphism) it, accordingly theorem 2.3, can be extended to homomorphism $\tilde{\phi} : L_1 \to \bar{K}$. ??? using normality of L ??? we can conclude that all such homomorphisms have the same image. If the image is L then we have an Automorphism.

2. *The group of automorphisms $Aut\,(L/K)$ acts transitively on the roots of any irreducible polynomial $P \in K\,[X]$. Again, an isomorphism of stem fields extends to an automorphism of L* [37]*.*

3. *If the group $Aut\,(L/K)$ fixes (see definition A.14) some element $x \notin K$ then x is pure inseparable (see definitions 3.5 and 3.6) i.e. $P_{min}\,(x, K)$ has a single root x. Thus if L is Galois extension (i.e. is separable) then the set of elements which are fixed by the automorphisms of L over K is just K itself: $L^{Aut(L/K)} = L$ (see definition 5.8).* [38]

Definition 5.9 (Galois group)**.** *If L is Galois extension then Galois group $G = Gal\,(L/K)$ is the group of automorphisms $Aut\,(L/K)$.*

Thus we can write

$$L^{Gal(L/K)} = K. \tag{5.3}$$

5.6 Artin's theorem

Motivated by (5.3) let formulate and proof the important theorem

Theorem 5.5 (Artin)**.** *L is a field and $G \subset Aut\,(L)$*

1. *If G acts with finite orbits, so, I mean all orbits of G are finite (i.e. $\forall x \in L : |Orb(x)| < \infty$), then L is a Galois extension of L^G.*

2. *If $|G| = n < \infty$ then $\left[L : L^G\right] = n$ and G is a Galois group*

Remark 5.5. *Well notice, that acting with finite orbits and being finite is not the same thing. So, a short remark before giving a proof: notice that finite orbits does not mean finiteness because it's typical for Galois groups to act with finite orbits. If we have some G, which is Galois of L over K: $G = Gal\,(L/K)$, and $x \in L$, then x is a root of a polynomial of some finite degree and it's splitting field is finite over K, so, the orbit of x is also finite because it's always sent to another root of the same polynomial and so consists of roots of the $P_{min}\,(x, K)$. But of course the Galois group itself $Gal\,(L/K)$ can be infinite when L is not finite over K. For instance, if $K = \mathbb{F}_p$ and*

[37] ???

[38] Another explanation is the following. Let $x \in L \setminus K$ then $g \in Aut\,(L/K)$ such that $g \neq id$ permutes roots of irreducible $P_{min}\,(x, K)$ and $g(x) = x' \neq x$. The only thing that works for $\forall g \in Aut\,(L/K)$ is K i.e. $\forall k \in K$ and $\forall g \in Aut\,(L/K)$ we have $g(k) = k$. This is because $P_{min}\,(x, K) = X - k$ i.e. only one root possible.

$L = \overline{\mathbb{F}_p}$. It is very easy to compute all the Galois groups, and in fact we shall see shortly what is exactly this Galois group of L over K. [39]

Proof. 1. Let me take x, well say, $x_1 \in L$ which is not G-invariant: $x_1 \in L \setminus L^G$ and G-Orbit of x $Orb(x) = \{x_1, x_2, \dots, x_k\}$. The polynomial $P(X) = \prod_{i=1}^{k}(X - x_i)$ is G-invariant [40] . G just permutes the x_i, it permutes the factors of these polynomial, so the polynomial is G-invariant. Therefore its coefficients are G-invariant and as result $P \in L^G[X]$ by definition 5.8. L^G is a field of G invariants, and it is separable. P is separable, because all x_i are distinct (there are distinct elements of the orbit). And L is splitting field of P, therefore L is a Galois extension over L^G by the Galois extension definition.

2. We have $|G| = n$ then $\forall y \in L : |Orb(y)| \leq n$. Take x as above $(x \in L \setminus L^G)$ $\left[L^G(x) : L^G\right] \leq n$. Claim that this implies $\left[L : L^G\right] \leq n$. If I knew already, that L is finite over L^G, this would be very easy, this would be just a direct consequence of Primitive element theorem. I would say that L is generated by one element. I take this one element as my x and I see that L is of degree at most n over L^G. But I don't know yet that L is finite so I have to do some trick. So, proof of the claim: take x such that $\left[L^G(x) : L^G\right]$ is maximal then take $y \in L$. $L^G(x, y)$ is finite over L and I can apply Primitive element theorem. Therefore $L^G(x, y) = L^G(z)$. But

$$\left[L^G(x) : L^G\right] \geq \left[L^G(z) : L^G\right]$$

thus $L^G(x) = L^G(z)$ so $y \in L^G(x)$ and since I can do this for any y, I eventually conclude that $L = L^G(x)$, and in particular, $\left[L : L^G\right] \leq n$. Well, now if this is strictly less than n, then L cannot have n automorphisms over L^G but $G \subset Aut\left(L/L^G\right)$ so this is a contradiction. Therefore $\left[L : L^G\right] = n$ and $G = Aut\left(L/L^G\right)$

□

[39] Section 6.4.2 shows that $Gal\left(\bar{\mathbb{F}}_p/\mathbb{F}_p\right)$ is not cyclic, but theorem 3.4 says that if G is finite than it should be cyclic. Thus we can conclude that $Gal\left(\bar{\mathbb{F}}_p/\mathbb{F}_p\right)$ is not finite

[40] I.e. $\forall g \in G : g(P(X)) = P(X)$

Chapter 6

Galois correspondence and first examples

We state and prove the main theorem of these lectures: the Galois correspondence. Then we start doing examples (low degree, discriminant, finite fields, roots of unity).

6.1 Some further remarks on normal extension. Fixed field

Some definitions from previous lecture. L over K is Galois extension if and only if it is a Separable extension and Normal extension or in other words L is a Splitting field of a family of separable irreducible polynomials over K. We also seen (see theorem 5.4) that in the case of finite extension $[L : K] < \infty$ the number of automorphisms $|Aut\,(L/K)| = [L : K]$.

There are several remarks on Normal extensions which show that the extensions behave sometimes differently compare to other types of extensions. Especially we have seen for that an extension L over M over K was finite or algebraic or separable or purely inseparable if, and only if, it was true for L over M and M over K. So, for a normal extensions, this is not the case anymore.

Remark 6.1. *Let we have a tower of extensions $K \subset L \subset M$. If M is normal over K then of course the M is normal over L. It is clear because if M is a splitting field of a family of polynomials over K the one can just consider them as being polynomials over L and say that M is a splitting field of a family of polynomials over L.*

But L does not have to be normal over K (see example 6.1).

Example 6.1. *Consider*

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[4]{2}\right) \subset \mathbb{Q}\left(\sqrt[4]{2}, i\right)$$

We have $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$ to be a splitting field for polynomial $X^4 - 2$ but $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is just a Stem field (not Splitting field) for this polynomial. And as result $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is not a normal over $\mathbb{Q}$.

Remark 6.2. *A quadratic extension* [1] *is normal. This is by formula for roots of a quadratic equation.* [2]

If P quadratic over K has 1 root in L then its another root is also in L.

Remark 6.3. *One often has $K \subset L \subset M$ with L normal over K, M normal over L but M not normal over K (see example 6.2).*

Example 6.2. *Consider*

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\left(\sqrt[4]{2}\right)$$

We have $\mathbb{Q}\left(\sqrt{2}\right)$ normal over $\mathbb{Q}$ as well as $\mathbb{Q}\left(\sqrt[4]{2}\right)$ normal over $\mathbb{Q}\left(\sqrt{2}\right)$ because they both are quadratic extensions. But $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is not normal over $\mathbb{Q}$ (as it was mentioned in example 6.2)

We also seen at last lecture the following definition (see definition 5.8):

Definition 6.1 (Fixed field)**.** *If L is a field and $G \subset Aut(L)$ then*

$$L^G = \{x \in L \mid \forall g \in G : gx = x\}$$

is a fixed field

If we have a sub-field $K \subset L$ then we can consider the following group of automorphisms of L over K: $Aut(L/K)$ in the case if L is normal. Because otherwise the group will be too small to give information about L. But in the normal case it makes sense to consider the group of automorphisms of L over K.

We have seen (see (5.3)) that if L is separable over K then

$$L^{Aut(L/K)} = K$$

[1] Extensions with degree 2.

[2] Because a if we have 2 roots $x_1, x_2 \in L \supset K$ then there exists the following relation $x_2 = k_1 + k_2 x_1$ where $k_1, k_2 \in K$. I.e. if we know one root then the other is easy computed and located in the same extension as the first one.

This is because of the group of automorphisms was permuting the roots over the minimal polynomial of x over K (see item 3 in remark 5.4).

We also have seen (see theorem 5.5) that if G is finite the L is Galois extension over L^G and $\left[L : L^G\right] = |G|$.

And now we are going to summarize all these in a theorem which is in fact the main subject of this lecture course and this theorem is called the Galois correspondence.

6.2 The Galois correspondence

Let L over K be a Galois extension. By definition the group automorphisms $Aut\,(L/K)$ is called Galois group and denoted as $Gal\,(L/K)$

Theorem 6.1 (Galois correspondence)**.** *1. If L is finite over K then there is a Bijection between a sub-extension F (K ⊂ F ⊂ L) and a subgroup* $H \subset Gal\,(L/K)$. *The correspondence is the following*

$$\begin{aligned} F &\to Gal\,(L/F) \\ L^H &\leftarrow H \end{aligned}$$

2. The following statement are equivalent (if and only if)

(a) F is Galois over K

(b) $\forall g \in Gal\,(L/K)\, g\,(F) = F$

(c) $Gal\,(L/F)$ *is a Normal subgroup in* $Gal\,(L/K)$

In this case g goes to g restricted to F: $g \to g|_F$ *this is a Surjection* $Gal\,(L/K) \twoheadrightarrow Gal\,(F/K)$ *and the kernel is* $Gal\,(L/F)$. [3]

Proof. 1. Most work have been done before. What have we got by now? $L^{Gal(L/F)} = F$ (see (5.3)). By the theorem definition we have $H \subset Gal\,(L/K)$. Artin theorem gives us $\left[L : L^H\right] = |H|$ but with theorem 5.4 we also have $\left[L : L^H\right] = \left|Gal\left(L/L^H\right)\right|$ so one must have $H = Gal\left(L/L^H\right)$.

This means that the maps that we have in the theorem : $F \to Gal\,(L/F)$ and $L^H \leftarrow H$ are mutually inverse [4] and if a map is invertible then there is a Bijection.

---

[3] ??? is there an reformulation of First isomorphism theorem or just an application from [33] that the normality $N \triangleleft G$ is equivalent to the following statement. There is some homomorphism on G for which N is the kernel: $\exists \phi \in Hom(G) \mid \ker \phi = N$.

[4] We have the following maps:

$$F \to Gal\,(L/F) \to L^{Gal(L/F)} = F$$

2. We should proof equivalence of the following statements:

   (a) F is Galois over K

   (b) $\forall g \in Gal\left(L/K\right) g\left(F\right) = F$

   (c) $Gal\left(L/F\right) \triangleleft Gal\left(L/K\right)$

   Lets show that 2a implies 2b. Fix $x \in F$ the minimal polynomial $P_{min}\left(x, K\right)$ splits in L but it has a root in F thus it should have all roots in F by normality i.e. as soon as F is Normal extension $P_{min}\left(x, K\right)$ splits in F. This means, of course, that any map from Galois group preserves F since it premutes the roots: $\forall g \in Gal\left(L/K\right)$ g permutes the roots of $P_{min}\left(x, K\right)$ and that is the true for any $x \in F$ therefore $g\left(F\right) \subset F$ since F is generated (consists of) such roots.

   Lets show that 2b implies 2a. If $g\left(F\right) \subset F$ then all roots of $P_{min}\left(x, K\right)$, $x \in F$ are in F since g permutes those roots or, in other words, since Galois group acts transitively (??? see theorem 5.3) on roots of an irreducible polynomial therefore F is normal by definition.

   Lets show that 2a and 2b are equivalent to 2c i.e. let $g \in G$, $g\left(F\right) \subset L$ then if $h \in Gal\left(L/F\right)$ is such that $h|_F = id$ then $ghg^{-1}|_{g(F)} = id$. This means that $ghg^{-1} \in Gal\left(L/g\left(F\right)\right)$ so the statement $g\left(F\right) = F$ is the same to say

$$gGal\left(L/F\right)g^{-1} = Gal\left(L/F\right)$$

So apply this to all $g \in Gal\left(L/K\right)$ one can get that $Gal\left(L/F\right)$ is a Normal subgroup of $Gal\left(L/K\right)$

   Finally if all this statements (2a $\Longleftrightarrow$ 2b $\Longleftrightarrow$ 2c) are true then we can consider map (make sense by 2b)

$$\phi : Gal\left(L/K\right) \xrightarrow[g \to g|_F]{} Gal\left(L/F\right).$$

This is a Surjection by theorem 2.3 (???) and the kernel $\ker \phi = Gal\left(L/F\right)$ by definition because the kernel consists of things which are identity on F. □

Remark 6.4. *If L over K is not finite then Galois correspondence is not Bijection i.e. the maps which are in the theorem still make sense, but they will not be mutually inverse bijections and we shall see an example (see section 6.4.2).*

I.e. $\forall F$ such that $K \subset F \subset L$ we can construct $H = Gal\left(L/F\right)$ then we can construct L^H such that (by theorem 5.5) $K \subset L^H \subset L$.

6.3 First examples (polynomials of degree 2 and 3)

Example 6.3 (Degree 2)**.** *Let $[L : K] = 2$ and $\mathrm{char}K \neq 2$. The extension L is generated by a root of quadratic polynomial i.e. $x \in L \setminus K$ then $P_{min}(x, K)$ is quadratic and if we look at the formula for the root of the equation we will see that the extension is generated by a root of discriminant Δ: $L = K\left(\sqrt{\Delta}\right)$.*

What can we say about the $Gal(L/K)$. It consists of 2 elements and there is only one cyclic group of 2 elements: $\mathbb{Z}/2\mathbb{Z}$. Therefore

$$Gal(L/K) \cong \mathbb{Z}/2\mathbb{Z}$$

. The elements of the group is identity and an element that exchanges the 2 roots i.e. permutes $\sqrt{\Delta}$ and $-\sqrt{\Delta}$.

Example 6.4 (Degree 3)**.** *Let $[L : K] = 3$ and $\mathrm{char}K \neq 3$ (separable extensions) then L is generated by x - root of degree 3 polynomial P and there are 2 cases*

1. *P splits in L therefore L is a Galois group but the Galois group of 3 elements must be cyclic i.e. $Gal(L/K) \cong \mathbb{Z}/3\mathbb{Z}$ - cyclic group of order 3.*

2. *P does not split in L then there exists $M = K(x_1, x_2, x_3)$ - splitting field where $x_{1,2,3}$ are roots of P and $L = K(x_1)$. M is Galois and the Galois group is embeded into a group of permutation of 3 elements (because Galois group permutes the roots): $Gal(M/K) \hookrightarrow S_3$.*

   As soon $L \subsetneq M$ then $[M : K] > 3$ so $Gal(M/K) = S_3$. In particular $[M : K] = 6$

If you see a cubic polynomial how will you decide is its Galois group is cyclic or S_3? This is determined by a discriminant of polynomial which is a subject of next section (see example 6.5).

6.4 Discriminant. Degree 3 (cont'd). Finite fields

6.4.1 Discriminant

Definition 6.2 (discriminant)**.** *Let $P \in K[X]$. The polynomial has the following roots in $\bar{K}$: $x_1, x_2, \ldots, x_n$. The following product is called discrim-*

inant:

$$\Delta = \prod_{i<j} (x_i - x_j)^2$$

If we take group $G = Gal\,(P)$ then $G \subset S_n$ and any permutation preserves Δ and as result we have $\Delta \in K$ (see (5.3)).

Lets take a root of discriminant (we have to choose some roots order for this operation) then

$$\sqrt{\Delta} = \prod_{i<j} (x_i - x_j)$$

this quantity is preserved by even (and not by odd) permutations.

Proposition 6.1. *Let $G = Gal\,(P)$ - Galois group then $G \subset A_n$ [5] if and only if $\sqrt{\Delta} \in K$.*

Proof. Since if the Galois group is even then, this will be preserved by an element of Galois group and so will be in K and conversely, if it is an element of K, then it must be preserved by the Galois group, but we know it is preserved only by even permutations. $\square$

If we return to our example 6.4 we can get the following one

Example 6.5 (Discriminant of polynomial degree 3)**.** *Lets compute the discriminant for the following polynomial: $X^3 + pX + q$.* [6]

The discriminant easy to compute: [7] *$\Delta = -4p^3 - 27q^2$. So if Δ is a square in K then $Gal\,(P) \cong A_3$ (cyclic of order 3)* [8] *. If not then $Gal\,(P) \cong S_3$ (non commutative group of 6 elements).*

What can we say about sub-extensions for the two cases? If M is a splitting field of P over K then for the first case there is no any sub-extension. For the second case there are several sub-extensions (they are determined by sub-groups of the Galois group: S_3 for our case). Especially we have 3 sub-extension of degree 3: $K(x_1)$, $K(x_2)$ and $K(x_3)$ (fixed by non-normal sub-groups of order 2 - because M is degree 2 over $K(x_{1,2,3})$ - transpositions roots ???). And we have one quadratic sub-extension (of degree 2) fixed by $A_3 \subset S_3$ this is $K\left(\sqrt{\Delta}\right)$.

[5] A_n is a group of even permutations

[6] X^2 element can be always hidden via a variable change. Thus the polynomial can be considered as a common case for cubic polynomials.

[7] ??? compute it

[8] See example A.8 about groups S_3 and Alternating group A_3.

Galois correspondence says us that there are no other sub-extensions. Because those sub extensions correspond objectively to subgroups of the Galois group. And in this case, it does not have so many subgroups. These are just three subgroups of order 2 generated by transpositions, and one subgroup of order 3 generated by a three cycle.

6.4.2 Finite fields. An infinite degree example

We have seen that theory of finite fields is easy. Especially all Galois groups are cyclic (see corollary 3.5). I.e. we have the field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The Galois group is cyclic and generated by Frobenius map (see remark 3.2) which is $F_p : x \to x^q$.

More interesting are infinite extensions of a finite field, for instance the Algebraic closure. Thus consider $\bar{\mathbb{F}}_p$ as an extension of $\mathbb{F}_p$. If we take an invariant generated by Frobenius F_p [9] then

$$\bar{\mathbb{F}}_p^{\langle F_p \rangle} = \mathbb{F}_p$$

but

$$Gal\left(\bar{\mathbb{F}}_p / \mathbb{F}_p\right) \neq \langle F_p \rangle$$

therefore there is no bijective correspondence between sub-fields and subgroups. In particular the Galois correspondence is not Bijection (as it was mentioned at remark 6.4)

So how to see that the Galois group is not cyclic: $Gal\left(\bar{\mathbb{F}}_p / \mathbb{F}_p\right) \neq \langle F_p \rangle$?

Really a smaller group is not cyclic. Lets look at the following:

$$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \dots \mathbb{F}_{p^{2^n}} \subset \dots$$

and let

$$L = \cup \mathbb{F}_{p^{2^n}}$$

We claim that $Gal\left(L/\mathbb{F}_p\right)$ is not cyclic. Consider the following number $a_n = 1 + 2 + 4 + \cdots + 2^n$ then $\forall x \in \mathbb{F}_{p^{2^n}}$ $F_p^{a_n}(x) = F_p^{a_m}(x)$ for any $m > n$. This is because the Frobenius map F_p sends x to x^p is an identity on $\mathbb{F}_p$ therefore $F_p^{2^{n+l}}$ is identity on $\mathbb{F}_{p^{2^n}}$ $\forall l \geq 0$. This implies that there exists an automorphism $\phi : L \to L$ such that $\forall n \geq 0$

$$\phi|_{\mathbb{F}_{p^{2^n}}} = F^{a_n}$$

but $\forall k \in \mathbb{Z}$ $F_p^k \neq \phi$. One can look at ϕ as $\phi = F_p^{1+2+4+\cdots+2^n+\cdots}$ but this is, of course, very informal. The rigorous conclusions we can draw from this

[9] The group generated by one element F_p is denoted as $\langle F_p \rangle$.

is that our Galois group is not a cyclical group generated by the Frobenius map i.e. $Gal\left(\bar{\mathbb{F}}_p/\mathbb{F}_p\right) \neq \langle F_p \rangle$. And also, that we don't have a bijective Galois correspondents like we have for finite field extensions i.e no bijective correspondents between sub-groups of the Galois group and sub-extensions. Indeed the fixed field of the F_p and and the whole Galois group coincide.

6.5 Roots of unity: cyclotomic polynomials

Consider a number n that is prime to characteristic (see section 1.1.3) of K: $(n, char\,(K)) = 1$ and consider the polynomial $P_n = X^n - 1$ (if $(n, char\,(K)) = 1$ then the polynomial has no multiple roots). Thus the polynomial has exactly n roots which form a cyclic multiplicative subgroup of $\bar{K}^\times$ (see definition A.25) denoted by μ_n. So μ_n is just the group of n roots of unity in $\bar{K}^\times$.

Definition 6.3 (Primitive roots of unity)**.** *There are root of unity of degree n such that not root of unity of degree $d < n$.*

The set of Primitive roots of unity is denoted as μ_n^*. All elements of μ_n are powers of a single one: $\forall x \in \nu_n \exists a \in \mathbb{N} : x = \zeta^a$ for some $\zeta \in \mu_n$. And primitive roots of unity form the following set $\{\zeta^a\}$ where $(a, n) = 1$. The number of such primitive roots is determined by Euler's totient function: $|\mu_n^*| = \phi\,(n)$.

Definition 6.4 (n-th cyclotomic polynomial)**.** *The polynomial*

$$\Phi_n = \prod_{\alpha \in \mu_n^*} (X - \alpha) \in \bar{K}\,[X]$$

is called n-th cyclotomic polynomial.

Example 6.6 (n-th cyclotomic polynomial)**.**

$$\Phi_1 = X - 1$$

$$\Phi_2 = \frac{X^2 - 1}{X - 1} = X + 1$$

$$\Phi_3 = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$$

$$\Phi_4 = \frac{X^4 - 1}{(X - 1)(X + 1)} = X^2 + 1$$

$$\Phi_5 = X^4 + X^3 + X^2 + 1$$

Proposition 6.2. *1. $P_n = \prod_{d|n} \Phi_d$*

2. Φ_n has coefficients in prime fields (see section 1.1.3): $\mathbb{Q}$ if char$K = 0$ or $\mathbb{F}_p$ if char$K = p$

3. If char$K = 0$ then $\Phi_n \in \mathbb{Z}[X]$. If char$K = p$ then Φ_n is the reduction $\bmod p$ of the n-th cyclotomic polynomial over $\mathbb{Z}$.

Proof. (??? exercise) □

6.6 Irreducibility of cyclotomic polynomial.The Galois group

Theorem 6.2. *Φ_n is irreducible in $\mathbb{Q}[X]$.*

Proof. We have to prove that all Primitive roots of unity have the same minimal polynomial over $\mathbb{Q}$. It must be Φ_n by degree reason (minimal polynomial degree should be n).

Let fix one primitive root ζ and all others have the form ζ^a where a is prime to n: $(a, n) = 1$. We may assume that a is a prime number l and suppose

$$P_{min}(\zeta, \mathbb{Q}) \neq P_{min}\left(\zeta^l, \mathbb{Q}\right).$$

Then $\Phi_n = f \cdot g$ where f has ζ as a root and g has ζ^l as a root. This is true in $\mathbb{Q}[X]$ but also as we seen (??? add a link) in $\mathbb{Z}[X]$. So we have $g\left(\zeta^l\right) = 0$ thus we can define $g_l(X) = g\left(X^l\right)$ then g_l will have ζ as a root. But $g_l = g^l \mod l$ thus in modulo l Φ_n has ζ as a multiple root. This is impossible because Φ_n divides P_n and this does not have multiple roots whenever l prime to n. □

Remark 6.5. *Statements of theorem 6.2 are not true if char$K > 0$. I.e. over $\mathbb{F}_p$ Φ_n is not always irreducible.*

For instance $\Phi_8 = X^4 + 1$ is reducible over $\mathbb{F}_p$ for any p. [10] *In fact it splits in $\mathbb{F}_{p^2}$.* [11] *If p is odd then $8 \mid p^2 - 1$ so the Multiplicative group $\mathbb{F}_{p^2}^{\times}$ contains a cyclic subgroup of order 8 which is exactly the group of 8 roots of unity.*

[10] ??? explain proof provided below

[11] ???

Theorem 6.3. *The splitting field L of P_n over K is $K(\zeta)$, where ζ is a root of Φ_n.*

$\forall g \in Gal(L/K)$ acts by $g : \zeta \to \zeta^{a_g}$ where $(a_g, n) = 1$.

$Gal(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^{\times}$ and this is an isomorphism whenever Φ_n is irreducible over K (for example $K = \mathbb{Q}$).

Proof.

1. All n-th roots of unity are powers of ζ so the lie in $K(\zeta)$.
2. Thus any $g \in Gal(L/K)$ induces an automorphism of $\mu_n \subset L$ and all such automorphisms are raising a root to a power that is prime to n.
3. $Gal(L/K) \hookrightarrow Aut(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$. That is because (???) if is here one if g is identity on L since generates L over K (???)
4. If Φ_n is irreducible then there is an isomorphism because of cardinality: $[L : K] = \deg \Phi_n = \phi(n)$. But $\phi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right|$. So in the case the embedding must be isomorphism.

$\square$

Chapter 7

Galois correspondence and first examples. Examples continued

We continue to study the examples: cyclotomic extensions (roots of unity), cyclic extensions (Kummer and Artin-Schreier extensions). We introduce the notion of the composite extension and make remarks on its Galois group (when it is Galois), in the case when the composed extensions are in some sense independent and one or both of them is Galois. The notion of independence is also given a precise sense ("linearly disjoint extensions").

7.1 Cyclotomic extensions (cont'd). Examples over $\mathbb{Q}$

Last time we discussed cyclotomic extensions which are splitting fields of Φ_n (generated by n-th roots (Primitive roots of unity) of 1). And we got a very precise description of those extensions in the case when Phi_n was irreducible, for instance, over $\mathbb{Q}$.

We have seen (see theorem 6.3) that $\mathbb{Q}(\zeta_n)$ is a Galois extension of Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$ (see example A.11) where $\zeta_n = e^{\frac{2\pi i}{n}}$. So it acts as $g_a : \zeta_n \to \zeta_n^a$ where $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ that can be considered as a number relatively prime to n: $(a, n) = 1$.

Lets consider several examples

Example 7.1 ($n = 8$). *Lets consider $n = 8$. In the case*

$$\left|(\mathbb{Z}/8\mathbb{Z})^\times\right| = 4$$

i.e. the group has 4 elements there are

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}.$$

So our Galois group also has 4 elements:

$$Gal : \left\{id, \zeta_8 \to \zeta_8^3, \zeta_8 \to \zeta_8^5, \zeta_8 \to \zeta_8^7\right\} = \{id, \sigma_3, \sigma_5, \sigma_7\}.$$

We can note that $\sigma_7 = \zeta_8 \to \zeta_8^7$ *is something very simple - it is complex conjugation:* $\sigma_7 = \zeta_8 \to \bar{\zeta}_8$. *It's Fixed field* $\mathbb{Q}(\zeta_8)^{\sigma_7}$ *is determined by the following expression* [1]

$$\mathbb{Q}(\zeta_8)^{\sigma_7} = \mathbb{Q}(\zeta_8) \cap \mathbb{R} = \mathbb{Q}\left(\zeta_8 + \bar{\zeta}_8\right) = \mathbb{Q}\left(\sqrt{2}\right)$$

i.e. there is a quadratic extension.

Our Galois group has 3 subgroups of order 2 so we have 3 quadratic sub-extensions. One o them we have already found ($\mathbb{Q}\left(\sqrt{2}\right)$*) lets find 2 others.*

$$\mathbb{Q}(\zeta_8)^{\sigma_3} = \mathbb{Q}\left(\zeta_8 + \zeta_8^3\right) = \mathbb{Q}\left(i\sqrt{2}\right).$$

and finally (with note $\zeta_8^5 = -\zeta_8, \zeta_8^6 = -i$*)*

$$\mathbb{Q}(\zeta_8)^{\sigma_5} = \mathbb{Q}\left(\zeta_8 \cdot \zeta_8^5\right) = \mathbb{Q}\left(\zeta_8^6\right) = \mathbb{Q}(i).$$

Example 7.2 $(n = 5)$**.** $\mathbb{Q}(\zeta_5)$ *where* $\zeta_5 = e^{\frac{2\pi i}{5}}$. *The Galois group is the following:*

$$Gal \cong (\mathbb{Z}/5\mathbb{Z})^\times$$

that is a Cyclic group of order 4. It is generated by $\zeta_5 \to \zeta_5^2$ *and it has only one Proper subgroup* $\cong \mathbb{Z}/2\mathbb{Z}$ *so our field* $\mathbb{Q}(\zeta_5)$ *has only one sub-field different from* $\mathbb{Q}$ *of course and this going to be a real part all of the complex conjugation which are part of Galois group. Now this is the same as the real part* $\mathbb{Q}(\zeta_5) \cap \mathbb{R} = \mathbb{Q}\left(\zeta_5 + \bar{\zeta}_5\right) = \mathbb{Q}\left(cos\frac{2\pi}{5}\right)$.

So these were the examples of cyclotomic extensions of $\mathbb{Q}$ and of course the picture is exactly the same as long as the cyclotomic polynomial is irreducible. If it is not reducible, which can happen as we have seen, the Galois group becomes smaller.

7.2 Kummer extensions

Consider a field K such that the characteristics of K is prime to a certain number n: $(charK, n) = 1$ and such that $X^n - 1$ splits in K. So K contains all roots of unity. Consider an element a of K : $a \in K$ and let $\alpha = \sqrt[n]{a}$ (i.e. a root of $X^n - a$). Take $d = \min\{i \mid \alpha^i \in K\}$.

[1] ??? need a proof

Proposition 7.1. *$d \mid n$, minimal polynomial of α is $X^d - \alpha^d$ and $K(\alpha)$ is a Galois extension with cyclic Galois group of order d.*

Proof. It's clear that $K(\alpha)$ is Galois because all the n-th roots of unity are in K. So $K(\alpha)$ contains all roots of $X^n - a$. Therefore $K(\alpha)$ is a Splitting field of $X^n - a$. So it's normal and separable because it is a separable polynomial because $(char K, n) = 1$.

Lets define a Homomorphism $f : Gal(K(\alpha)/K) \xrightarrow[g \to \frac{g(\alpha)}{\alpha}]{} \mu_n$. This is correct because g sends α to another root of $X^n - a$ thus the quotient $\frac{g(\alpha)}{\alpha}$ is a root of unity:

$$\left(\frac{g(\alpha)}{\alpha}\right)^n = 1.$$

The homomorphism f is Injection because $g(\alpha)$ determines g. What's the image? It should be a Subgroup of a Cyclic group μ_n but the subgroup should be also cyclic. [2] Let δ is the order of the image and we want to show that $\delta = d$. Consider $g\left(\alpha^\delta\right) = f(g)^\delta \cdot \alpha^\delta = \alpha^\delta$ because $f(g)$ is a root of 1 ($f(g) = \sqrt[\delta]{1}$). Thus $\alpha^\delta \in K$. And $\alpha^i \notin K$ for $i < \delta$ since otherwise $\deg P_{min}(\alpha, K) = i < \delta$. But this is impossible because

$$[K(\alpha) : K] = |Gal(K(\alpha)/K)| = \delta.$$

Thus only possible option is $d = \delta$. Thus $P_{min}(\alpha, K) = X^d - \alpha^d$. □

Proposition 7.2. *And conversely (to 7.1) for all cyclic extension of degree n such that $(char K, n) = 1$ is generated by $\sqrt[n]{a}$ for some $a \in K$.*

Proof. Consider L is an extension of K. $Gal(L/K) = \langle\sigma\rangle$ then we have $\sigma^n = id$. We have that σ is diagonalisable. [3] Now, let us show that all eigenspaces have dimension 1. Indeed if x, y are in the same eigenspace then $\sigma\left(\frac{x}{y}\right) = \frac{x}{y}$ because x and y are multiplied by the same number. Therefore $\frac{x}{y} \in K$. And this is exactly means that dimension of the eigenspace is 1. [4] Thus all roots of 1 are eigenvalues of σ. Then take α such that $\sigma(\alpha) = \zeta\alpha$ where ζ is a Primitive roots of unity. Then $\langle\sigma\rangle$ - orbit of α has n elements therefore $[K(\alpha) : K] = n$ (see explanation below) and $\alpha^n \in K$ since $\sigma(\alpha^n) = \zeta^n \cdot \alpha^n = \alpha^n$. We see that α is a root of $X^n - a$. This is irreducible by degree reason.

[2] ??? add a ref
[3] ??? add a ref to linear algebra theorem
[4] ???

Maybe I should have said here, why it follows from the formula, $\langle\sigma\rangle$ - orbit of α has n elements that the degree of the extension is exactly n. While this is easy because either degree of the extension was less than n, then also, alpha would have to be fixed by some non-trivial subgroup of Galois group by Galois correspondence. And then its orbit would have less than n elements. $\square$

7.3 Artin-Schreier extensions

Let $n = char K$ this is called as Artin-Schreier extensions.

Definition 7.1 (Cyclic extension)**.** *The Galois extension is called cyclic extension if the corresponding Galois group is cyclic.*

Theorem 7.1. *Let $p - char K$ and let $P = X^p - X - a \in K[X]$. Then P is irreducible or splits over K. Let α be a root. If P is irreducible the $K(\alpha)$ is Cyclic extension of K of degree p.*

Conversely any cyclic extension of degree p is like this: $L/K, \exists\alpha \in K$ such that $L = K(\alpha)$, α - root of $X^p - X - a$ for some $a \in K$.

Proof. First of all notice that roots of P are $\alpha + k$ where $k \in \mathbb{F}_p$ (k is an element of prime field).

If P is irreducible then Galois group should be transitive on the roots (??? see theorem 5.3) then $\exists\sigma \in Gal(K(\alpha)/K)$ such that $\sigma(\alpha) = \alpha + 1$ (because roots of P are $\alpha + k$). The Order of element in group for σ is $p = [K(\alpha) : K]$ so the σ must generate the Galois group: $Gal(K(\alpha)/K) = \langle\sigma\rangle$.

We have to show that if P is not irreducible then P splits i.e. $\alpha \in K$. Leave it for an exercise [5]

Now we will prove the converse statement. Let L is a Cyclic extension of K of degree p. We want to find α such that $\sigma(\alpha) = \alpha + 1$ where σ is a generator of $Gal(L/K)$ (we know that the Galois group is cyclic i.e. must have the following form $Gal(L/K) = \langle\sigma\rangle$).

Set $f = \sigma - id$, $K = \ker f$ [6] and the Rank $rgf = p - 1$ [7] $(\sigma - id)^p = 0$ so the Kernel must be included into Image: $K = \ker f \subset \operatorname{Im} f$ because otherwise $L = \ker f \oplus \operatorname{Im} f$ (L is a Direct sum [8] of kernel and image) and f^k is never zero (but we have $f^p = 0$) [9].

[5] ??? proof

[6] this is because $\forall x \in K : \sigma(x) = x$ (see (5.3)).

[7] ??? in lectures we can hear about range (Image) not a Rank but by future content we spoke about the rank but not about range (image)

[8] see also definition A.46 and example A.19

[9] ??? $L = \ker f \oplus \operatorname{Im} f$ holds if f is projection i.e. $f^2 = f$ i.e. $f^k = f \neq 0$.

So as soon as K is an image of f then $\exists \alpha \in L$ such that $f(\alpha) = 1$ but this means that $\sigma(\alpha) = \alpha + 1$. Now consider $\sigma(\alpha^p - \alpha) = (\alpha+1)^p - (\alpha+1) = \alpha^p - \alpha$ (because we are in the field of characteristic p). This means that $\alpha^p - \alpha \in K$ because the field is fixed by Galois group (see (5.3)). So $\alpha^p - \alpha = a \in K$ and α is a root of $X^p - X - a$ and this finished the proof of the theorem. $\square$

7.4 Composite extensions. Properties

Definition 7.2 (Composite extension). *Let L_1 and L_2 are extensions of K both contained in some extension L (for instance the Algebraic closure $\bar{K}$). The composite extension L_1L_2 is the extension they generate: $L_1L_2 = L_2L_1 = K(L_1 \cup L_2)$.*

Another way to view this: consider the tensor product $L_1 \otimes_K L_2$ - there is a K-algebra. By Universal property there is a map from the tensor product to L:

$$j : L_1 \otimes_K L_2 \to L$$

such that $j(l_1 \otimes l_2) = l_1 l_2$ (??? can be considered as a bilinear map required for the universal property). The Image $\operatorname{Im} j$ is a sub-algebra of L. If L is algebraic then any sub algebra is a sub field (??? add a ref) and this is exactly the field generated by L_1L_2. In general we can take its fraction field (to obtain a field from a ring (an algebra)).

Property 7.1. *If L_1 is separable (pure inseparable, normal, finite of degree n) over K then L_1L_2 is also separable (pure inseparable, normal, finite of degree $\leq n$) over L_2*

Proof. Let $x \in L_1L_2$ (L_1L_2 is generated by L_1 over L_2) then it's minimal polynomial $P_{min}(x, L_2)$ is a divisor of $P_{min}(x, K)$ in $L_2[X]$. Therefore $P_{min}(x, L_2)$ has a degree $\leq n$ where n is degree of $P_{min}(x, K)$.

So if $P_{min}(x, K)$ is separable (pure inseparable, normal, finite of degree n) then $P_{min}(x, L_2)$ is separable (pure inseparable, normal, finite of degree $\leq n$).

The same is true for splitting so the normality is preserved.

About dimensions ("finite extension of degree" in the property formulation). By the Base-change:

$$\dim_K L_1 = \dim_{L_2}(L_1 \otimes_K L_2)$$

and as soon as L_1L_2 is the $\operatorname{Im} j$:

$$\dim_{L_2}(L_1 \otimes_K L_2) \geq \dim_{L_2}(L_1L_2)$$

i.e.

$$\dim_{L_2}(L_1L_2) \leq \dim_K L_1 = n.$$

□

Property 7.2. *If L_1, L_2 are separable (pure inseparable, normal, finite of degree n and m) over K then L_1L_2 is also separable (pure inseparable, normal, finite of degree $\leq nm$) over K*

Proof. We have the following towers:

$$K \hookrightarrow L_1 \hookrightarrow L_1L_2$$

and all properties except normality are preserved in the towers so follows from property 7.1.

Normality is obvious because if L_1 is a splitting field of the family polynomials $\{P_i\}_{i\in I}$ and L_2 is a splitting field of the family polynomials $\{Q_j\}_{j\in J}$ then L_1L_2 is a splitting field of the union of those families $\{P_i, Q_j\}_{i\in I, j\in J}$. So normality is obviously preserved. □

7.5 Linearly disjoint extensions. Examples

Theorem 7.2. *The following statements are equivalent (for algebraic extensions)*

1. *$L_1 \otimes_k L_2$ is a field*
2. *j is Injection*
3. *if we have $x_1, x_2, \ldots, x_n \in L_1$ linearly independent over K then they are linearly independent over L_2*
4. *if we have two families: $x_1, x_2, \ldots, x_n \in L_1$ linearly independent over K and $y_1, y_2, \ldots, y_m \in L_2$ linearly independent over K then x_iy_j linearly independent over K*

When L_1 finite over K then all the statements are equivalent to $[L_1L_2 : L_2] = [L_1 : K]$ or in other words $[L_1L_2 : K] = [L_1 : K]\,[L_2 : K]$

Definition 7.3 (Linearly disjoint extensions)**.** *In the case L_1 and L_2 are called linearly disjoint extensions*

Proof. Equivalence 1 and 2 is clear because we have that $L_1L_2 = \operatorname{Im} j$.

Then 2 implies 3: we have $x_1 \otimes 1, \dots, x_n \otimes 1$ are linearly independent over L_2 by Base-change property (??? is the link correct). If j is injective then their images $x_1, \dots, x_n$ are also linearly independent over L_2. This is because an injective map transforms a linearly independent set of vectors into a linearly independent set.

3 implies 4: if we have some relation $\sum a_{ij}x_iy_j = 0, a_{ij} \in K$ then since x_i linearly independent over K one can get $\sum a_{ij}y_j = 0$ but as soon as y_j linearly independent we will get $a_{ij} = 0$.

Next 4 implies 2 (remember that 2 is injectivity of j). Take $z \in L_1 \otimes_K L_2$ such that $j(z) = 0$. We have $z = \sum a_{ij}x_i \otimes y_j$ and $j(z) = \sum a_{ij}x_iy_j = 0$ i.e. $a_{ij} = 0$ and therefore $z = 0$. I.e. j is Injection.

The part about finite degrees follows from the 4 properties (??? need a proof) $\square$

Example 7.3. *First of all, the extensions which have relatively prime degrees are always linearly disjoint.*

I.e. if $[L_1 : K] = m$, $[L_2 : K] = n$ and $(m, n) = 1$ then L_1 and L_2 are linearly disjoint. Indeed m and n must divide $[L_1L_2 : K] \leq mn$. With our conditions $[L_1L_2 : K] = mn$ but this is one of definition of linearly disjoint extensions (see definition 7.3).

In particular $\mathbb{Q}\left(\sqrt[5]{2}\right)$ and $\mathbb{Q}\left(\sqrt[5]{1}\right)$ are linearly disjoint extensions because the degrees are $\left[\mathbb{Q}\left(\sqrt[5]{2}\right) : \mathbb{Q}\right] = 5$ and $\left[\mathbb{Q}\left(\sqrt[5]{1}\right) : \mathbb{Q}\right] = 4$.

From the other side with $\sqrt[5]{1} = e^{\frac{2\pi i}{5}}$ the following extensions are not linearly disjoint: $\mathbb{Q}\left(\sqrt[5]{2}\right)$ and $\mathbb{Q}\left(e^{\frac{2\pi i}{5}} \cdot \sqrt[5]{2}\right)$. Indeed in both cases L_1L_2 is a splitting field of $X^5 - 2$ and (for the first case) $[L_1L_2 : \mathbb{Q}] = 4 \cdot 5 = 20$. In the second case both $[L_{1,2} : \mathbb{Q}] = 5$ and $5 \cdot 5 \neq 20$.

So, you see that the difference is rather subtle. Well, the obvious reason in the second case is that those extensions are generated by rules of the same polynomial, but, still some effort is needed to formalize why this is not linearly disjoint case. In particular we see that $L_1 \cap L_2 = \mathbb{Q}$ does not imply that L_1 and L_2 are linearly disjoint over $\mathbb{Q}$. It's exactly what's happen in the second case.

7.6 Linearly disjoint extensions in the Galois case

Theorem 7.3. *Let $L_1, L_2 \subset \bar{K}$ - extensions of K. L_1 is Galois over K. Let $K' = L_1 \cap L_2$. Then $L_1 L_2$ is Galois over L_2. $Gal\left(L_1 L_2 / L_2\right)$ stabilizes L_1. $\phi : g \rightarrow g|_{L_1}$ is an injective map of $Gal\left(L_1 L_2 / L_2\right)$ to$Gal\left(L_1 / K\right)$ with image $Gal\left(L_1 / K'\right)$ and L_1, L_2 are linearly disjoint over K'.*

Proof. Let $x \in L_1$ and $g \in Gal\left(L_1 L_2 / L_2\right)$ then $g\left(x\right)$ is a root of $P_{min}\left(x, L_2\right)$. It is also a root of $P_{min}\left(x, K\right)$. But all such roots are in L_1 because L_1 is Galois. Thus the map ϕ is well defined. It's injective because if we have some σ such that $\sigma|_{L_1} = \sigma|_{L_2} = id$ then it should be $\sigma = id$. This is because our extension is generated by L_1 and L_2, so if it happened to be in identity on them both, it must be an identity.

So now lets find the image of ϕ. If $g\left(x\right) = x, \forall g \in Gal\left(L_1 L_2 / L_2\right)$ then $x \in L_2$ by Galois correspondence. So if also $x \in L_1$ then it should be $x \in K' = L_1 \cap Ł_2$. So if L_1 is finite over K then by Galois correspondence we can conclude that $\operatorname{Im} \phi = Gal\left(L / K'\right)$ because the Fixed field is K'.

In general (??? not finite L_1 over K) we have to find finite sub-extension of L_1: let denote it as L_1'. We also have a finite Galois sub extension of L_1 that contains L_1'. You can take the union of all images of L_1' by all automorphisms. And this will be a finite union since L_1' was finite, so there are finitely many possible roots of minimal polynomials so there are not really many possibilities for the images of this L_1'. So I shall leave it as an exercise (??? add proof), but the solution is more or less what I just have told you.

Lets denote the Galois sub-extension as L_1''. We have $\forall L_1''$ and L_2 are linearly disjoint over K' then it follows that L_1 and L_2 are also linearly disjoint over K' (see theorem 7.2 point 3).

Let $\gamma \in Gal\left(L_1 / K\right)$ then exists an element in $Gal\left(L_1 L_2 / L_2\right)$ which is sent by ϕ to γ. We have $j : L_1 \otimes_K L_2 \cong L_1 L_2$ and we can take $j \cdot \left(\gamma \otimes id\right) \cdot j^{-1}$ - this will be the element of Galois group (??? required element in $Gal\left(L_1 L_2 / L_2\right)$). $\square$

From the theorem 7.3 follows the following proposition

Proposition 7.3.

1. *L_1 and L_2 are both Galois over K and linearly disjoint then the following map $g \rightarrow \left(g|_{L_1}, g|_{L_2}\right)$ defines the isomorphism*

$$Gal\left(L_1 L_2 / K\right) \cong Gal\left(L_1 / K\right) \times Gal\left(L_2 / K\right)$$

2. *conversely to the first part: if $Gal\left(L / K\right) = G_1 \times G_2$ then $L = L^{G_1} L^{G_2}$ which are linearly disjoint over the intersection.*

Proof. The first part Is very sure because the interjectivity of this map is clear: if something is trivial both on L_1 and L_2, then it's trivial on the composite, so I only have to prove the subjectivity. I will use the same trick as before: $L_1 \otimes_K L_2 \cong_j L_1 L_2$ then $j \cdot (g_1 \otimes g_2) \cdot j^{-1}$ goes to (g_1, g_2).

The second part. L^{G_1} and L^{G_2} are both Galois because G_1 and G_2 are normal in the product: $G_1, G_2 \triangleleft G_1 \times G_2$. What I mean is G_1 embedded to the product by identifying it with $G_1 \times e$ where e is the neutral element of G_2.

The intersection $L^{G_1} \cap L^{G_2}$ is fixed by G so $L^{G_1} \cap L^{G_2} = K$. Linear disjoint follows from $L^{G_1} \cap L^{G_2} = K$ since we are in the Galois case (???). □

7.7 On the Galois group of the composite

Let me give you a small example:

Example 7.4. *We have a Composite extension $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n, \zeta_m)$ where $\zeta_n = e^{\frac{2\pi i}{n}}$. $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}\left(\zeta_{LCM(n,m)}\right)$ [10] therefore if $(n, m) = 1$ then $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)$ are linearly disjoint. It can be seen as follows: we can apply proposition 7.3 to our Galois groups then $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$ but by the Chinese remainder theorem*

$$(\mathbb{Z}/nm\mathbb{Z})^{\times} \cong (\mathbb{Z}/n\mathbb{Z})^{\times} \times (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

Thus $Gal(\mathbb{Q}(\zeta_{nm})) = Gal(\mathbb{Q}(\zeta_n)) \times Gal(\mathbb{Q}(\zeta_m))$. So the linear disjoint is just got from the proposition 7.3.

[10] LCM - least common multiple. For instance multiples for 4 are $4, 8, 12, \ldots$. Multiples for 6 are $6, 12, 18, \ldots$. Thus $LCM(4, 6) = 12$.

Chapter 8

Solvability by radicals, Abel's theorem. A few words on relation to representations and topology

We finally arrive to the source of Galois theory, the question which motivated Galois himself: which equation are solvable by radicals and which are not? We explain Galois' result: an equation is solvable by radicals if and only if its Galois group is solvable in the sense of group theory. In particular we see that the "general" equation of degree at least 5 is not solvable by radicals. We briefly discuss the relations to representation theory and to topological coverings.

8.1 Extensions solvable by radicals. Solvable groups. Example

8.1.1 Extensions solvable by radicals

Let K is a field of characteristic 0: $char K = 0$. It is embedded into its Algebraic closure.

Definition 8.1 (Extension solvable by radicals)**.** *A finite extension E of K is solvable by radicals if $\exists \alpha_1, \ldots, \alpha_r$ generating E such that $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ for some $n_i \in \mathbb{N}$.*

Example 8.1. *Let $K = \mathbb{Q}$, $E = \mathbb{Q}\left(\sqrt[3]{2+3\sqrt{7}}, \sqrt[5]{4+5\sqrt{11}}\right)$. We have $\alpha_1 = \sqrt{7}, \alpha_2 = \sqrt{11}, \alpha_3 = \sqrt[3]{2+3\sqrt{7}}, \alpha_4 = \sqrt[5]{4+5\sqrt{11}}$.*

Definition 8.2 (Polynomial solvable by radicals). *$P \in K[X]$ is called solvable by radicals if exists a E - Extension solvable by radicals and containing all roots of P.*

So more precisely, it would say that the equation, $P = 0$ is solvable by radicals.

Property 8.1. 1. *Composite extension of solvable by radicals is itself solvable by radicals*

2. *If L extension of K is solvable by radicals (by definition L should be finite extension of K) then exists a finite Galois extension E containing L and solvable by radicals.*

Proof. For the first property: ???

For the second property: Indeed take a composite of all images of L in $\bar{K}$. Or those are the same as images of L by $Gal\left(\bar{K}/K\right)$ □

8.1.2 Solvable groups

This shall be a brief reminder since this is not a course on group theory, you are supposed to know some group theory already. So I somehow I presume that you are familiar with this definition but I will recall the definition of basic properties.

Definition 8.3 (Solvable group). *G is called solvable if it has a filtration i. e. $G = G_0 \supset G_1 \supset \cdots \supset G_{r-1} \supset G_r = \{e\}$, such that G_i is a normal subgroup of G_{i-1} and the Quotient group G_{i-1}/G_i is abelian.*

Example 8.2 (Group of permutations S_3). *Consider S_3 - the group of permutations (see also example A.8). It's solvable because $S_3 \supset A_3 \supset \{e\}$.*

We have $|S_3/A_3| = 2$ (see example A.9) i.e. S_3/A_3 is cyclic of order 2. $|A_3|$ i.e. A_3 - cyclic of order 3.

Example 8.3 (Group of permutations S_4). *Consider S_4 - the group of permutations (see also example A.8). It's solvable because $S_4 \supset A_4 \supset K \supset \{e\}$, where K - is a subgroup of double transpositions (see example A.3 for permutation cycles notation):*

$$K = \{e, (12)(34), (13)(24), (14)(23)\}.$$

A double transposition is a product of two transpositions with distinct support, right, which permute the distinct elements.

$A_4 \triangleleft S_4$, $|S_4/A_4| = 2$, i.e. S_4/A_4 is cyclic of order 2.
$K \triangleleft A_4$, $|A_4/K| = 3$, i.e. A_4/K is cyclic of order 3.
K is Abelian group and $K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
So this shows that S_4 is solvable.

8.2 Properties of solvable groups. Symmetric group

Property 8.2. *If G is solvable and $H \subset G$ is a subgroup of G then H is solvable.*

Proof. Indeed $G_i \cap H$ gives a filtration with required property. □

Property 8.3. *If G is solvable and $H \triangleleft G$ is a normal subgroup of G then G/H is solvable.*

Proof. Indeed consider a projection map

$$\pi : G \to G/H \tag{8.1}$$

then $\pi\left(G_i\right)$ gives a filtration $\left(G/H\right)_i$ on G/H with required properties. □

Property 8.4. *If $H \triangleleft G$, H and G/H are solvable then G is solvable.*

Proof. Put togeter the filtration H_i and $\pi^{-1}\left(\left(G/H\right)_j\right)$ (see (8.1) for π definition). □

Property 8.5. *If G is finite than G is solvable (i.e. has a finite filtration with Abelian quotients) if and only if there exists a finite filtration with cyclic quotients.*

Proof. This is just because a finite Abelian group is just a product of cyclic groups. □

Lets also look at another definition of solvable group

Definition 8.4 (Solvable group)**.** *G is called solvable if the following sequence is finite:*

$$G \supseteq [G, G] = G^{(1)} \supseteq \left[G^{(1)}, G^{(1)}\right] = G^{(2)} \supseteq \cdots \supseteq \left[G^{(n-1)}, G^{(n-1)}\right] = G^{(n)} = \{e\}$$

where $G^{(i)} = \left[G^{(i-1)}, G^{(i-1)}\right]$ is the Commutator subgroup.

Remark 8.1. *Definitions of solvable group 8.4 and 8.3 are equivalent.*

Proof. Our filtration with Commutator subgroups $G \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(n)} = \{e\}$ is a filtration with abelian quotient because $G^{(i)} / \left[G^{(i)}, G^{(i)}\right] = G^{(i)}/G^{(i+1)}$ is an Abelian group.

From the other hand if G/H is an Abelian group then $H \supset [G, G]$. So if a finite filtration with abelian quotient exists then the filtration given by $G^{(i)}$ is also finite. It must terminate after a finite steps. So, this proves the equivalence. □

Theorem 8.1 (S_n solvability)**.** *S_n - the permutation of n elements (see example A.5) is not solvable for $n \geq 5$.*

Proof. It's easy to use definition 8.4. Main steps are the following

1. we know that $[S_n, S_n] = A_n$ - subgroup of even permutations (see definition A.23). It can be see from the fact that any 3-cycle is a Commutator subgroup and 3-cycles generate A_n [1]

2. If $n \geq 5$ then $[A_n, A_n] = A_n$ thus the filtration generated by commutators will never terminate i.e. will never reach the unity ($\{e\}$) and will stabilize on A_n. How we can see it? We can remember that $[A_4, A_4] = K$ (see example 8.3) - the subgroup of double transpositions. $A_4 \hookrightarrow A_n$ in many different ways. Because you can pick any 4 elements, our n elements and just consider the permutations of those 4 elements as a subgroup of permutations of n elements and then taking the commutators of those A_4, we see that all double transpositions are in the $[A_n, A_n]$ (Commutator subgroup of A_n). But if $n \geq 5$, they generate A_n.

□

8.3 Galois theorem on solvability by radicals

Theorem 8.2. *Let $P \in K[X]$. P is a Polynomial solvable by radicals if and only if $Gal(P)$ is solvable. There $Gal(P)$ is (by definition) $Gal(F/K)$ where F is a Splitting field of P over K.*

[1] 3-cycle are even permutations and result of their compositions is also even

Proof. First of all lets proof that if $Gal\left(P\right)$ is solvable then P is solvable. Let $n-\left[F:K\right]$ and consider $L=K\left(\zeta_n\right)$ where ζ_n - n-th root of 1. Let $M=FL$ - a Composite extension. So this is the splitting and field of P of which we have adjoined all the n-th roots of unity. Then M is a Galois extension and $Gal\left(M/K\right)\hookrightarrow Gal\left(F/K\right)$. $\forall g\in Gal\left(M/K\right)$ leaves F invariant. If $g\mid_F=id$ then $g=id$. Then the image in fact of this map is of the Galois group of F over the intersection of F and L. So $G=Gal\left(M/K\right)$ is solvable i.e.

$$G=G_0\supset G_1\supset\cdots\supset G_r=\{e\}$$

and G_i/G_{i+1} - cyclic of order $n_i\mid n$. And as soon as $n_i\mid n$ (very important), all n-th roots of 1 are in M (this is why we adjoin the L).

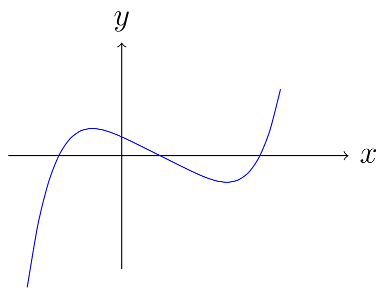
Let $M_i=M^{G_i}$. We know $M_i\hookrightarrow M_{i+1}$ is a cyclic Galois extension of order $n_i\mid n$ and roots of 1 are in it therefore there is Kummer extension (see section 7.2). So $M_{i+1}=M_i\left(\sqrt[n_i]{a_i}\right)$ (see proposition 7.2). So $M=K\left(\zeta_n,\alpha_1,\ldots,\alpha_r\right)$ where $\alpha_i=\sqrt[n_i]{a_i}$. Therefore M is solvable by radicals.

For another direction: if P is solvable then G is solvable. Let E is solvable extension containing F. We may suppose that this is Galois. Then write $E=K\left(\alpha_1,\ldots,\alpha_r\right)$ where $\alpha_i^{n_i}\in K\left(\alpha_1,\ldots,\alpha_{i-1}\right)$. Then let $L=K\left(\zeta_n\right)$ where $n=LCM\left(\{n_i\}\right)$ so $\forall n_i:n_i\mid n$. And take $M=LE$. We have $K\left(\alpha_1,\ldots,\alpha_{i-1}\right)\hookrightarrow K\left(\alpha_1,\ldots,\alpha_i\right)$ - cyclic extension of order n_i. We have $Gal\left(M/L\right)$ is solvable by this cyclic subgroups. $Gal\left(M/K\right)$ is also solvable since $Gal\left(M/L\right)$ subgroup and the quotient $\cong Gal\left(L/K\right)$ which is abelian. $Gal\left(F/K\right)$ is a quotient of $Gal\left(M/K\right)$ thus is solvable too. $\square$

8.4 Examples of equations not solvable by radicals."General equation"

As we can see there exist equations which are not solvable in radicals.

Example 8.4 (Not solvable polynomial of degree 5)**.** *Let $P\in\mathbb{Q}\left[X\right]$ is an irreducible polynomial with rational coefficients of degree 5. It has 3 real roots*



(and 2 complex conjugate roots) as it shown on the picture.

We claim that $Gal\left(P\right)=S_5$. This is because

1. *Gal* (P) *contains the complex conjugation (we have 2 complex conjugated roots but Galois group is the group of automorphisms which exchange roots and the complex conjugation will exchange the 2 complex roots). The complex conjugation is the transposition of roots*

2. *As soon as* P *is irreducible then Gal* (P) *should act transitively (see definition A.16) on roots. We have an irreducible polynomial. We can always send one of its roots to another of its roots. We have this isomorphism of stem fields which extends to an automorphism of the splitting field. But, what is the subgroup of* S_5*, which adds transitively?*

   Gal $(P) \subset S_5$ *acts transitively. This means that* $5 \mid |Gal\,(P)|$*. That is because (see Orbit-stabilizer theorem)* $|G| = |G(x)|\,|G_x|$ *(*$G(x)$ *- is the Orbit,* G_x *- Stabilizer subgroup) but the orbit has 5 elements and therefore 5 divides the cardinality of* G*. This means, by Sylow theorems, that our group contains something of order 5. But only 5-cycle has order 5. But a 5-cycle and transposition generate* S_5*. So Gal* $(P) = S_5$*.*

In fact, the same argument is valid for S_p *with every* p *- prime. I.e. applies to an arbitrary prime number* p *instead of 5.*

So Gal $(P) = S_5$ *- not solvable and therefore* P *is not solvable by radicals.*

Example 8.5 (General equation of degree n)**.** *What's the general equation. It is the following*

$$X^n - T_1 X^{n-1} + T_2 X^{n-2} + \cdots + (-1)^n T_n,$$

where T_i *is a variable. Where does it come from? Let* $X_1, \ldots, X_n$ *are roots of a polynomial of degree* n *when the polynomial itself is*

$$(X - X_1) \cdot \cdots \cdot (X - X_n) = X^n - \left(\sum_i X_i\right) X^{n-1} + \\ + \left(\sum_{i,j} X_i X_j\right) X^{n-2} + \cdots + (-1)^n \prod_i X_i,$$

i.e. $T_1 = \sum_i X_i, T_2 = \sum_{i,j} X_i X_j, \ldots, T_n = \prod_i X_i$.

One has $K[T_1, \ldots, T_n] \subset K[X_1, \ldots, X_n]$ *(multi-variable polynomial rings). We have the same also for field extensions:* $K(T_1, \ldots, T_n) \subset K(X_1, \ldots, X_n)$*. The* $K(X_1, \ldots, X_n)$ *is algebraic and a splitting field for our general polynomial. So it has degree at most* $n!$*. On the other hand* $K(T_1, \ldots, T_n) \subset K(X_1, \ldots, X_n)^{S_n}$ *so degree of the extension is* $n!$ *and*

$$K(T_1, \ldots, T_n) = K(X_1, \ldots, X_n)^{S_n}.$$

In particular the Galois group is S_n and our general polynomial is not solvable by radicals if $n \geq 5$. This is known as Abel theorem

8.5 Galois action as a representation. Normal base theorem

Connection with group representations.

Definition 8.5 (Group representation). *Let G is a finite group. V is a Vector space over K. Representation of G is a Homomorphism $\rho : G \to GL(V)$ (where $GL(V)$ is the General linear group of a vector space i.e. the group of Automorphisms of the vector space V).*

If L is a finite extension of K we can talk about it as about K-vector space. So we have a representation of G as Galois group $Gal(L/K)$: $\rho : G \to GL_K(L)$ - this is something that we have as the definition because we define the Galois group as the group of automorphisms of L over K.

We can ask the question: what's kind of representation is the ρ. We claim that ρ is something that is called as Regular representation.

Definition 8.6 (Regular representation). *Let a vector space V has a basis indexed by elements of group G: e_g where $g \in G$. $\rho_{reg}(h)$ acts by permutations:*

$$\rho_{reg}(h) e_g = e_{hg}.$$

We claim that the representation of Galois group is the regular representation. We have seen that (see proof of the theorem 5.2)

$$L \otimes_K \bar{K} \cong \bar{K}^n.$$

The sum $\bar{K}^n$ of n ($n = |G = Gal(L/K)|$) copies of $\bar{K}$ is indexed by the embeddings of L into $\bar{K}$. Pick one $j : L \hookrightarrow \bar{K}$ and all others can be obtained by group Action $j \circ g, g \in G$. So $\bar{K}^n$ has a basis indexed by G and the Action of G permutes the basis vectors. So $L \otimes_K \bar{K} \cong \bar{K}^n \cong$ Regular representation of G over $\bar{K}$. In particular $\exists x$ such that $gx \mid_{g \in G}$ form a basis of $L \otimes_K \bar{K}$ over $\bar{K}$.

Elements of G are linearly independent in in the space of Endomorphisms $End_{\bar{K}}\left(L \otimes_K \bar{K}\right)$

Theorem 8.3 (Normal base). *$\exists x \in L$ such that $\{gx \mid g \in G\}$ is a K basis of L.*

Proof. First of all consider a case when K is infinite. Let pick some basis $e_1, \ldots, e_n$ - K-basis in L. $g_1, \ldots, g_n \in G$. Let $x \in L$ then $g_1(x), \ldots, g_n(x)$ is a basis if and only if matrix formed by $g_i(x)$ in the basis e_j has non zero determinant. But this determinant is a polynomial in the coefficient, which is not identically zero. Well, why? Because if it was identically zero, it would remain identically zero also after the base changed to $\bar{K}$. Since it has a $\bar{K}$ point where it does not vanish.

There are many $x \in L \otimes_K \bar{K}$ such that $g_i(x)$ form a basis. And over an infinite field, a polynomial which is not identically zero cannot vanish identically. And over an infinite field, only a polynomial which is identically 0 can vanish at every point.

Let me to clarify the point: $P \in K[X]$ has at most $\deg P$ roots. So if K infinite and P has every element of K as a root then $P = 0$ (P is zero as an element of $K[X]$).

By induction we can get the same statement for a polynomial in several variables. so, our polynomial which is the determinant of the matrix, is non zero, as a polynomial of several variable because it has non rules over algebraic closure. And so, it also has to have rules, well non rules over K. So, there exists a point $x \in L$ (not anymore in $L \otimes_K \bar{K}$) such that $det(\ldots) \neq 0$ at x so $g_i(x)$ form a basis.

If K is finite then the argument with roots of a polynomial does not apply any more. But in the case Galois groups are cyclic i.e. $G = \langle \sigma \rangle$. We have $id, \sigma, \ldots, \sigma^{n-1}$ are linearly independent since this is the case over $\bar{K}$. Then the minimal polynomial of σ as an Endomorphism of L over K is $X^n - 1$. Thus

$$L \cong K[X] / (X^n - 1)$$

as a K-module with X acting by σ. This is a cyclic module and any generator x shall do i.e. $x, \sigma x, \ldots, \sigma^{n-1} x$ form a basis. $\square$

8.6 Relation with coverings

Remark 8.2. *If L is a finite Galois extension of K then $L \otimes_K L$ is a Direct sum of fields which are isomorphic to L. Sums are permuted by $G = Gal(L/k)$.*

Proof. So if $L = K(\alpha)$ is a splitting field of the polynomial $P = (X - \alpha_1) \cdot \cdots \cdot (X - \alpha_n)$ (where $\alpha \in \{\alpha_1, \ldots, \alpha_n\}$) that is isomorphic to $K[X]/(P)$. If we tensor it to L we will get

$$L[X] / (X - \alpha_1) \cdot \cdots \cdot (X - \alpha_n) \cong L[X] / (X - \alpha_1) \times \cdots \times L[X] / (X - \alpha_n)$$

that is a product of copies of L permuted by Galois action $\square$

In topology one has Galois covering $Y \to X$. G acts on Y, X quotient. The covering is characterized by the property that $Y \times_X Y = \sqcup_{g \in G} Y_g$, $Y_g = \{(y, gy)\}$. [2]

[2] ??? add an explanation

Chapter 9

Ring extensions, norms and traces, reduction bp

We build a tool for finding elements in Galois groups, learning to use the reduction modulo p. For this, we have to talk a little bit about integral ring extensions and also about norms and traces.

9.1 Integral elements over a ring

Let $P \in \mathbb{Z}[X]$. We want to know what is $Gal\,(P)$. Just a reminder that $Gal\,(P) = Gal\,(K/\mathbb{Q})$ where K is a Splitting field of P. We have already done the work for several types of polynomials: cyclotomic polynomial, Kummer extensions and so on.

Sometimes if, our polynomial is a kind of combination of then the explicit information about the roots helps to calculate the Galois group. For instance if we have polynomial $X^5 - 2$ we know it's roots: $\sqrt[5]{2}, j^k \sqrt[5]{2}$, where $j = e^{\frac{2\pi i}{5}}, 1 \leq k \leq 4$. Now we have a lot about Galois group. If K is the splitting field of the polynomial then we have the following towers:

$$\begin{tikzcd}
& \mathbb{Q}(j) \arrow[dr, "5"] & \\
\mathbb{Q} \arrow[ur, "4"] \arrow[dr, "5"'] & & \mathbb{Q}\left(\sqrt[5]{2}, j\right) = K \\
& \mathbb{Q}\left(\sqrt[5]{2}\right) \arrow[ur, "4"'] &
\end{tikzcd}$$

From that we know we can conclude that it follows that our Galois group, contains a normal cyclic subgroup of a order of five $\mathbb{Z}/5\mathbb{Z}$. And then the quotient is the Galois group of cyclotomic extension, so this is $(\mathbb{Z}/5\mathbb{Z})^{\times}$. So this is a group of order 20. You can show that this is noncommutative, and from this exact sequence, you have some information about it. But what will we do if we don't know the roots. One of the tool that we will use is the reduction of modulo prime and this will be the subject of the lecture.

9.1.1 Ring extensions

Definition 9.1 (Integral element)**.** *Let A be an Integral domain, i.e. a ring without zero divisors. And let B is an extension of A. The element $\alpha \in B$ is called integral over A if α is a root of a Monic polynomial $P \in A[X]$.*

So one can write the following relation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0, a_i \in A.$$

Example 9.1. $\frac{1}{2}$ *is not integral element over $\mathbb{Z}$ but $\sqrt{2}$ is an Integral element over $\mathbb{Z}$.*

This is because the polynomial in the definition 9.1 is monic i.e. the leading coefficient is 1.

Lemma 9.1. *The following conditions are equvivalent*

1. *α is integral over A.*
2. *$A[\alpha]$ is a finitely generated A-module (see definition A.47).*
3. *$A \subset C \subset B$ where C is a a finitely generated A-module (see definition A.47). I.e. A is contained in a finitely generated A-module.*

Proof. $1 \to 2 \to 3$ is easy [1] and we will concentrate on $3 \to 1$.

Let $x_1, \ldots, x_r$ generate C as A-module then we can write

$$\alpha x_i = \sum \lambda_{ij} x_j,$$

where $\lambda_{ij} \in A$. Consider the matrix $\Lambda = \{\lambda_{ij}\}$ and let $M = \alpha \cdot id - \Lambda$. Then

$$M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0.$$

[1] ??? provide an explanation

Thus

$$\det M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0.$$

Therefore $detM \cdot C = 0$ but $1 \in C$ thus $\det M = 0$. The equation $\det M = 0$ can be considered as a polynomial with α as a root. □

9.2 Integral extensions, integral closure, ring of integers of a number field

9.2.1 Integral extensions and integral closure

Definition 9.2 (Integral extension)**.** *Let $A \subset B$. B is integral over A if $\forall \alpha \in B$, α is an Integral element over A.*

Proposition 9.1. *Let $A \subset B \subset C$. B integral over A, C integral over B then C is an Integral extension over A.*

Proof. Proof is left as an exercise [2] □

Proposition 9.2. *Let B is a finitely generated over A as a module (see definition A.47) if and only if $B = A[\alpha_1, \ldots, \alpha_r]$ where each α_i is an Integral element over A.*

Proof. Proof is left as an exercise [3] □

Proposition 9.3. *Let $A \subset B$. I.e. B is an arbitrary extension of A. The elements of B which are integral over A form a subring of B (one calls it as the integral closure of A in B).*

Proof. Let α, β are integral over A then $A[\alpha, \beta]$ - finitely generated A-module (see definition A.47). This follows directly from lemma 9.1. It contains $\alpha + \beta$ and $\alpha\beta$ and by lemma 9.1 the $\alpha + \beta$ and $\alpha\beta$ are integral over A. But this is exactly we need to proof. □

[2] ??? provide the proof
[3] ??? provide the proof

Definition 9.3 (Integrally closed). *Let $A \subset B$. A is integrally closed in B if the integral closure of A in B equals to A.*

A is integrally closed (without mention of any B) if it is integrally closed in Fraction field $\mathrm{Frac}(A)$*.*

Example 9.2. *$\mathbb{Z}$ is Integrally closed.*

Remark 9.1. *More generally any Unique factorization domain is Integrally closed.*

Proof. Let A be a Unique factorization domain and $x \in \mathrm{Frac}(A)$ such that $x \neq 0$. So $x = \frac{p}{q}$ such that $p, q \in A, (p, q) = 1$ (this means no common prime divisor). If x integral over A then

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0.$$

Thus

$$\frac{p^n + qa_n p^{n-1} + q^2 a_{n-1} p^{n-2} + \cdots + q^{n-1}a_1 p + q^n a_0}{q^n} = 0$$

therefore $q \mid p^n$ which is in contradiction with $(p, q) = 1$. Unless q is invertable that is $x \in A$. □

9.2.2 Ring of integers in a number field

Definition 9.4 (Number field). *Let K is a finite extension of $\mathbb{Q}$ i.e. $[K : \mathbb{Q}] < \infty$. In the case K is a number field.*

Let K is a Number field and $[K : \mathbb{Q}] = N$.

Definition 9.5 (Ring of integers). *Let K is a Number field. The ring of integers $O_K \subset K$ is the integral closure of $\mathbb{Z}$ in K.*

Note: We know that integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$ but now we consider the closure in K but not in $\mathbb{Q}$.

Property 9.1. *1. $\forall \alpha \in K, \exists d \in \mathbb{Z} \setminus \{0\}$ such that $d\alpha \in O_K$.*

2. If $\alpha \in O_K$ then $P_{min}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$.

Proof. For the first part lets $P_{min}(\alpha, \mathbb{Q}) = X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}[X]$.

$\exists d \in \mathbb{Z}$ (the common denominator) such that $\forall i : da_i \in \mathbb{Z}$. So $b_i = d^{m-i}a_i \in \mathbb{Z}$ for any i. Therefore

$$(d\alpha)^m + b_{m-1}(d\alpha)^{m-1} + \cdots + b_0 = 0.$$

Thus $d\alpha \in O_K$.

The second part is also easy. If we have such $\alpha \in O_K$, it is a root of some Monic polynomial $Q \in \mathbb{Z}[X]$. Then the $P_{min} \mid Q$. So $Q = P_{min}R$. If we pick P_{min} to be monic, then by an argument very similar to that of the Gauss lemma, we conclude that both $P_{min}, R \in \mathbb{Z}[X]$. $\square$

9.3 Norm and trace

9.3.1 Finitely generated Abelian groups

(The material was given inside the proof of theorem 9.1 and can be considered as a recall) The Finitely generated abelian group is the same as finitely generated $\mathbb{Z}$-module. Any such group is isomorphic to (see theorem A.5)

$$\mathbb{Z}^n \oplus A,$$

where A is a finite group (torsion part). A subgroup of $\mathbb{Z}^n$ is itself a free ($\cong \mathbb{Z}^m$) of rank $m \leq n$.

9.3.2 Norms and traces

(The material was given inside the proof of theorem 9.1 and can be considered as a recall)

Definition 9.6 (Norm)**.** *Let $K \hookrightarrow E$ - finite separable field extension. Let $\alpha \in E$. Define the norm of alpha with respect to this extension as*

$$\mathrm{N}_{E/K}(\alpha) = \prod_{\sigma_i : E \hookrightarrow \bar{K}} \sigma_i(\alpha)$$

i.e. we took a product by all K embeddings of E into the algebraic closure of K. And we also assume that the product is finite i.e. $i = 1, \ldots, r$.

Definition 9.7 (Trace)**.** *Let $K \hookrightarrow E$ - finite separable field extension. Let $\alpha \in E$. Define the norm of alpha with respect to this extension as*

$$\mathrm{Tr}_{E/K}(\alpha) = \sum_{\sigma_i : E \hookrightarrow \bar{K}} \sigma_i(\alpha)$$

i.e. we took a sum by all K embeddings of E into the algebraic closure of K. And we also assume that the sum is finite i.e. $i = 1, \ldots, r$.

In the definitions 9.7 and 9.7 we assume that the extension E is Separable extension. If you're extension is not separable then you won't have to take it to the power equal to the pure inseparable degree of E/K, but for simplicity, we shall suppose that everything is separate.

Property 9.2. *1.* $\mathrm{N}_{E/K} : E^{\times} \to K^{\times}$ [4] *is multiplicative i.e. homomorphism of groups.* $\mathrm{Tr}_{E/K} : E \to K$ *is additive,* K*-linear i.e. homomorphism of* K*-vector spaces.* [5]

2. *If* $E = K(\alpha)$, $n = [E : K]$ *and* $P_{min}(\alpha, K) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$ *then* $\mathrm{N}_{E/K}(\alpha) = (-1)^n a_n$ *and* $\mathrm{Tr}_{E/K}(\alpha) = -a_1$.

3. *If we have the tower of extensions* $K \subset F \subset E$ *then*

$$\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_{F/K}(\alpha) \circ \mathrm{N}_{E/F}(\alpha)$$

and the same for trace

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}(\alpha) \circ \mathrm{Tr}_{E/F}(\alpha)$$

4. *Consider* $T : E \times E \xrightarrow[(x,y)\to \mathrm{Tr}_{E/K}(xy)]{} K$. *This is a non-degenerate* K*-bilinear form (see definition A.55)*

5. α *integral over* $\mathbb{Z}$, $K = \mathbb{Q}$. *Then* $\mathrm{N}_{E/\mathbb{Q}}(\alpha), \mathrm{Tr}_{E/\mathbb{Q}}(\alpha)$ *are integers.*

Proof. The first property is obvious from the definition.

The second one uses the following fact: $\sigma_i(\alpha)$ are roots of $P_{min}(\alpha, K)$. The Norm is a product and it's assigned to its constant term (a_n) and the sum is the first coefficient term (a_1) (see also example 8.5).

The third property is somewhat less trivial, so this follows from, the fact that if $\tau_1, \ldots, \tau_k$ are K embeddings of F into $\bar{K}$ and, $\mu_1, \ldots, \mu_s$ are F embeddings of E into $\bar{K}$ then the embedings of E into $\bar{K}$ are just the compositions $\{\tau_j \mu_i\}$.

For the 4th property. Indeed if $x \in \ker T$ then $\mathrm{Tr}_{E/K}(xy) = 0, \forall y \in E$ (see definition A.55). But this can't be a case when $xy \in K \setminus \{0\}$ by definition 9.7 $\mathrm{Tr}_{E/K}(xy) = [E : K]\, xy$.

For the 5th property we know that

$$\mathrm{Tr}_{E/\mathbb{Q}}(\alpha) = \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}\left(\mathrm{Tr}_{K/\mathbb{Q}(\alpha)}(\alpha)\right) = \\ = \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}\left([K : \mathbb{Q}(\alpha)]\, \alpha\right) = [K : \mathbb{Q}(\alpha)]\, \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$$

but $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ because $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$ is a coefficient of $P_{min}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$ (see property 9.1). ∎

[4] $E^{\times} = E \setminus \{0\}$ and $K^{\times} = K \setminus \{0\}$

[5] ??? May be there should be $\bar{K}$ instead of K.

Why such names are used? Consider the following map (multiplication by a)

$$f_a : E \xrightarrow[x \to ax]{} E$$

then the $\mathrm{Tr}_{E/K}(a)$ is exactly the trace of the linear map (i.e. sum of diagonal elements of the linear map matrix in a basis) and the $\mathrm{N}_{E/K}(a)$ is the determinant [6] . Now this f_a is a linear map, a K-linear map. It's an Endomorphism of a vector space you are working, and the trace of a is the trace of this endomorphism, and the norm of a is the determinant of this endomorphism.

9.3.3 Theorem about rings of integers

Theorem 9.1. *O_k is a finitely generated (see definition A.47) $\mathbb{Z}$-module that is a Free module of rank (see definition A.45) n, where $n = [K : \mathbb{Q}]$.*

Proof. If $e_1, \dots, e_n$ is a $\mathbb{Q}$-basis of K then $\forall i \exists d_i \in \mathbb{Z} \setminus \{0\}$ such that $d_i e_i \in O_K$ (see property 9.1). Therefore O_K contains a free $\mathbb{Z}$-submodule of rank n [7].

What is the $\mathbb{Z}$-module this is a finitely generated Finitely generated abelian group and we know a lot of things about such groups (see above).

We have to show that $O_K \subset A$ where A is a free $\mathbb{Z}$-submodule of rank $n = [K : \mathbb{Q}]$. Let $e_1, \dots, e_n$ is a $\mathbb{Q}$-basis of K (as above) contained in O_K. Consider the following map

$$(x, y) \to \mathrm{Tr}_{K/\mathbb{Q}}(xy)$$

this is Non-degenerate bilinear form (see 4th property 9.2) therefore $\exists v_1, \dots, v_n$ - Dual space basis ($\mathbb{Q}$-basis of K) and $\mathrm{Tr}_{K/\mathbb{Q}}(e_i v_j) = \delta_{ij}$.

We claim that $\mathbb{Z}$ submodule generated by $v_1, \dots, v_n$ contains O_K. Indeed let $\alpha \in O_K$ and write $\alpha = \sum \alpha_i v_i, \alpha_i \in \mathbb{Q}$. We can do it because $\{v_i\}$ is a $\mathbb{Q}$ basis of K. But one can see that $\alpha_i \in \mathbb{Z}$ because $\alpha_i = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha e_i)$ (by definition of v_j). Since α and e_i are elements of O_K then $\alpha e_i \in O_K$ too. Therefore $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha e_i) \in \mathbb{Z}$. So $\alpha_i \in \mathbb{Z}$ and this one is what we want to proof. We have expressed any element of O_K as a combination of v_i with integral coefficients. So O_K is contained in a $\mathbb{Z}$ submodule, generated by $\{v_i\}$. $\square$

---

[6] ??? add a proof

[7] This is because $d_1 e_1, \dots, d_n e_n$ are linearly independent and form a basis of a free $\mathbb{Z}$-module. The number of the cardinality of the basis n.

9.4 Reduction modulo a prime

Let $P \in \mathbb{Z}[X]$ - an irreducible polynomial with integer coefficients. K is a Splitting field of P over $\mathbb{Q}$ and $n = [K : \mathbb{Q}]$. Let $G = Gal(P) \stackrel{\text{def}}{=\!=} Gal(K/\mathbb{Q})$. We denote roots of P as $\alpha_1, \ldots, \alpha_n$ and they are elements of O_K. G acts on the set of roots, and on O_K. We will denote O_K as A. Let p is a prime number and we will consider A/pA. As we have seen

$$A/pA \cong A \otimes \mathbb{Z}/p\mathbb{Z}$$

there n-dimension vector space over $\mathbb{F}_p$. Maximal ideals of A/pA are in one-to-one correspondence with maximal ideals of A containing p. As we know (see theorem 4.3) there are only finitely many maximal ideal in a finite field. Therefore A also has finitly many maximal ideals $J_1, \ldots, J_r$ containing p. Our group G acting on A must permute these maximal ideals in some way.

Lets consider a subgroup $D_i \subset G$ which stabilizes J_i (see definition A.15) i.e.

$$D_i = \{g \in G \mid gJ_i = J_i\}.$$

Let also $k_i = A/J_i$ - this is a field and there is a finite extension of $\mathbb{F}_p$. Then there exists a natural homomorphism

$$D_i \to Gal(k_i/\mathbb{F}_p).$$

Since D_i stabilizes J_i and it acts on the residual classes of modulo J_i so there is a homomorphism of D_i into the Galois group.

Theorem 9.2. 1. *G acts transitively (see definition A.16) on $\{J_1, \ldots, J_r\}$ and the map $D_i \to Gal(k_i/\mathbb{F}_p)$ is a Surjection i. e. $D_i \twoheadrightarrow Gal(k_i/\mathbb{F}_p)$*

2. *If the reduction $\bar{P} = P \mod p$ has no multiple roots then the map $D_i \to Gal(k_i/\mathbb{F}_p)$ is bijection and k_i is a splitting field of the reduction $\bar{P}$.*

Proof. For the first part. Suppose that for some i and $\forall g \in G, g(J_1) \neq J_i$ i.e. suppose that there is not a Transitive group action. By Chinese remainder theorem theorem $\exists x \in A$ such that $x \equiv 0(\mod J_i), x \equiv 1(\mod g(J_1)) \forall g \in G$. Consider a product of all such things:

$$a = \prod_g gx$$

it's an integer $a \in \mathbb{Z}$. But since $x \in J_i$ then a is also in J_i (by ideal definition A.26): $a \in \mathbb{Z} \cap J_i = (p)$ - the ideal generated by the prime number p. So one has $a \in J_1$ since all J_i, and especially J_1, contains p. But this is impossible because J_1 is a Prime ideal. Because if we have $\prod_k x_k \in J_1$ then $\exists i$ such that $x_i \in J_1$ but there is not a case in our construction.

We still need to proof that $D_i \twoheadrightarrow Gal\left(k_i/\mathbb{F}_p\right)$ i.e. that there is a Surjection. We may assume that $i = 1$. By the Primitive element theorem $\exists z \in \mathbb{F}_p$ such that $k_1 = \mathbb{F}_p\left(z\right)$. By Chinese remainder theorem theorem $\exists y \in A$ such that $y \in J_i, i \neq 1, y \equiv z(\mod J_1)$. Consider polynomial $Q = \prod_{g \in G}\left(X - g\left(y\right)\right)$. There is a polynomial with integral coefficients i.e. $Q \in \mathbb{Z}\left[X\right]$. This is because we know that coefficients are G invariant i.e. in $\mathbb{Q}$ moreover they are integral over $\mathbb{Z}$ and are in $\mathbb{Z}$ as soon as $\mathbb{Z}$ is integrally closed.

Lets study $\bar{Q} = Q \mod J_1$. If $g \notin D_1$ then $\exists i$ such that $g\left(J_i\right) = J_1$ and particularly $g(y) \in J_1$. Therefore for such g we have

$$\overline{X - g\left(y\right)} = X - g\left(y\right) \mod J_1 = X.$$

So we have for $\bar{Q} \in \mathbb{F}_p\left[X\right]$

$$\bar{Q} = \prod_{g \in G \setminus D_1} X \prod_{g \in D_1}\left(X - \overline{g\left(y\right)}\right),$$

but $\prod_{g \in D_1}\left(X - \overline{g\left(y\right)}\right)$ has z as a root and D_1 acts transitively on its roots.

Now recall that z generates k_1. Thus an element of $Gal\left(k_1/\mathbb{F}_p\right)$ is determined by the image of z. And we have an element of D_1 which sends z to any possible image of it. But this means that $D_1 \twoheadrightarrow Gal\left(k_1/\mathbb{F}_p\right)$

For the second part of the theorem we assume that $\bar{P}$ has no multiple roots. So $\alpha_1, \ldots, \alpha_n$ -roots of P and $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ -roots of $\bar{P}$ where $\bar{\alpha}_i = \alpha_i \mod J_1$ (??? may be $\mod p$).

Lets $g \in D_1$ acts as id on k_1. Then, of course, $g\left(\bar{\alpha}_i\right) = \bar{\alpha}_i$. But $g\left(\alpha_i\right) \in \{\alpha_1, \ldots, \alpha_n\}$ and it can not be different from α_i since they will have diffeent reduction $\mod J_1$. So $\forall i, g\left(\alpha_i\right) = \alpha_i$ and therefore $g = id$. Thus conclusion that $D_1 \cong Gal\left(k_1/\mathbb{F}_p\right)$. By the same argument

$$Gal\left(k_1/\mathbb{F}_p\left[\bar{\alpha}_1, \ldots, \bar{\alpha}_n\right]\right) = id$$

therefore $k_1 = \mathbb{F}_p\left[\bar{\alpha}_1, \ldots, \bar{\alpha}_n\right]$. $\square$

9.5 Finding elements in Galois groups

How can we apply the above material to study Galois groups?

One uses this theorem to construct elements of a certain type in the Galois group to show that the Galois group is large.

So let $P \in \mathbb{Z}[X]$ be an irreducible polynomial and suppose that there is a prime $p \in \mathbb{Z}$ such that $\bar{P} = P \mod p$ is also irreducible. Then $Gal\,(P)$ contains a subgroup that is isomorphic to $Gal\left(\bar{P}\right)$ and both $Gal\,(P)$ and $Gal\left(\bar{P}\right)$ are irreducible of degree n. But we know Galois group of finite fields and we conclude that this Galois group contains an n cycle. This is because $Gal\left(\bar{P}\right)$ is cyclic generated by n cycle.

Sometimes, there is no such prime, but of course, a variant of this argument exists also in other cases.

Suppose, for instance that P is irreducible of degree 5 and that $\bar{P} = R_2R_3$ where R_i is irreducible of degree i.

Then the same argument, gives that $Gal\,(P)$ contains the permutation $(1,2)$ and then $(3,4,5)$ up to a numbering of roots.

And in this way one can construct elements of particular type in the Galois group and use this to show that those groups are very large.

Appendices

Appendix A

Course prerequisites

There are several prerequisites for the course there. They consists of definitions, theorems and examples mostly taken from Wikipedia.

A.1 Sets

Definition A.1 (Class). *A class is a collection of sets (or sometimes other mathematical objects) that can be unambiguously defined by a property that all its members share.*

A.2 Groups

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

Definition A.3 (Group). *Let we have a set of elements G with a defined binary operation $\circ$ that satisfied the following properties.*

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

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

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

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 A.1 (Group $\mathbb{Z}/2\mathbb{Z}$)**.** *Consider a set of 2 elements:* $G = \{0, 1\}$ *with the operation* $\circ$ *defined by the table A.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 A.4 (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.*

Definition A.5 (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.*

Theorem A.1 (Lagrange)**.** *For any finite group* G*, the order (number of elements) of every subgroup* H *of* G *divides the order of* G*.*

Definition A.6 (Subgroup)**.** *Let we have a Group* $(G, \circ)$*. The subset* $S \subset G$ *is called as subgroup if* $(S, \circ)$ *is a Group.*

Definition A.7 (Proper subgroup)**.** *A proper subgroup of a group* G *is a Subgroup* H *which is a proper subset of* G *(i.e.* $H \neq G$*) [37]*

Definition A.8 (Normal subgroup)**.** *A subgroup,* N*, of a group* G*, is called a normal subgroup if it is invariant under conjugation i.e.*

$$N \triangleleft G \Leftrightarrow \forall n \in N, \forall g \in G, gng^{-1} \in N$$

The definition taken from [33]

Definition A.9 (Quotient group)**.** *A quotient group or factor group is a mathematical group obtained by aggregating similar elements of a larger group using an equivalence relation that preserves the group structure. For example, the cyclic group of addition modulo n can be obtained from the integers by identifying elements that differ by a multiple of n and defining a group structure that operates on each such class (known as a congruence class) as a single entity. It is part of the mathematical field known as group theory [35].*

In a quotient of a group, the equivalence class of the identity element is always a normal subgroup of the original group, and the other equivalence classes are precisely the cosets of that normal subgroup. The resulting quotient is written G/N, where G is the original group and N is the normal subgroup.

Example A.2 (Quotient group)**.** *Consider [35] a group of integers $\mathbb{Z}$ (under addition) and the subgroup $2\mathbb{Z}$ of all even integers. This is a normal subgroup, because $\mathbb{Z}$ is Abelian group. There are only two Cosets: the set of even integers and the set of odd integers; therefore, the quotient group $\mathbb{Z}/2\mathbb{Z}$ is the cyclic group with two elements. This quotient group is isomorphic with the set $\{0,1\}$ with addition modulo 2; informally, it is sometimes said that $\mathbb{Z}/2\mathbb{Z}$ equals the set $\{0,1\}$ with addition modulo 2.*

Definition A.10 (Commutator)**.** *The commutator of two elements, g and h, of a group G, is the element [12]*

$$[g,h] = g^{-1}h^{-1}gh$$

Definition A.11 (Commutator subgroup)**.** *The commutator subgroup or derived subgroup of a group is the subgroup generated by all the Commutators of the group [13].*

Definition A.12 (Action)**.** *An action of a group is a way of interpreting the elements of the group as "acting" on some space in a way that preserves the structure of that space. See also [26].*

Definition A.13 (Orbit)**.** *Consider [26] a group G acting on a set X. The orbit of an element $x \in X$ is the set of elements in X to which x can be moved by the elements of G:*

$$Orb\,(x) = \{y \in X : \exists g \in G : y = g \cdot x\}$$

The orbit of element x is also denoted as $G\,(x)$.

Definition A.14 (Fixed point). *The set of points of X fixed by a group action are called the group's set of fixed points, defined by*

$$\{x : gx = x, \forall g \in G\}.$$

see also [8].

Definition A.15 (Stabilizer subgroup). *For every x in X, we define [26] the stabilizer subgroup of G with respect to x (also called the isotropy group) as the set of all elements in G that fix x:*

$$G_x = \{g \in G \mid g \cdot x = x\}$$

Theorem A.2 (Orbit-stabilizer theorem). *If group G and the set the group acting X are finite then*

$$|G| = |G(x)|\,|G_x|$$

where $x \in X$, $G(x)$ - is the Orbit, G_x - Stabilizer subgroup.

Note: the result was got from [26] as orbit-stabilizer theorem + Lagrange theorem

Definition A.16 (Transitive group action). *The action of G on X is called [26] transitive if X is non-empty and if for each pair $x, y \in X$ there exists a $g \in G$ such that $gx = y$.*

Definition A.17 (Free group action). *The action of G on X is called [26] free if, given $g, h \in G$, the existence of an $x \in X$ with $g(x) = h(x)$ implies $g = h$.*

A.2.1 Sylow theorems

Corollary A.1 (Sylow). *Given a finite group G and a prime number p dividing the order of G, then there exists an element (and hence a subgroup) of order p in G [38]*

A.2.2 Abelian group

Definition A.18 (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 $a \circ b = b \circ a$.*

Theorem A.3 (About order of element of an Abelian group)**.** *If G is a finite Abelian group and m is the maximal order of the elements of G then the order of every element of G divides m*

Theorem A.4. *Let G is an Abelian group and $n = |G|$ the group order (number of elements) then $\forall g \in G$ the following statement holds*

$$g^n = e,$$

there e is the group identity.

Proof. Let m is the maximal order of group G. In this case by Lagrange $m \mid n$ i. e. $n = k_1 m$ where $k_1 \in \mathbb{Z}$. Let l is the order of g i.e. $g^l = e$. By the theorem A.3 $l \mid m$ i.e. $m = k_2 l$. Thus

$$g^n = (g^m)^{k_1} = \left(g^l\right)^{k_2 k_1} = e.$$

□

Definition A.19 (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.

Definition A.20 (Direct sum)**.** *The direct sum of two abelian groups A and B is another abelian group $A \oplus B$ consisting of the ordered pairs (a, b) where $a \in A$ and $b \in B$ [15]*

Definition A.21 (Finitely generated abelian group)**.** *An Abelian group $(G, +)$ is called finitely generated [21] if there exist finitely many elements $x_1, \dots, x_s$ in G such that $\forall x \in G$:*

$$x = n_1 x_1 + \dots + n_s x_s \tag{A.1}$$

with $n_i \in \mathbb{Z}$. In this case we say that $\{x_1, \dots, x_s\}$ is a generating set of G.

In the (A.1) we have the following:

$$n_i x_i = \underbrace{x_i + \dots x_i}_{n_i \ times}$$

Theorem A.5 (The fundamental theorem of finitely generated abelian groups)**.** *Every Finitely generated abelian group G is isomorphic to a Direct sum of primary cyclic groups and infinite cyclic groups. A primary cyclic group is one whose order is a power of a prime. That is, every finitely generated abelian group is isomorphic to a group of the form*

$$\mathbb{Z}^n \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_t}$$

where the rank $n \geq 0$, and the numbers $q_1, \ldots, q_t$ are powers of (not necessarily distinct) prime numbers. In particular, G is finite if and only if $n = 0$. The values of $n, q_1, \ldots, q_t$ are (up to rearranging the indices) uniquely determined by G. The statement was took from [21].

A.3 Permutations

Example A.3 (Permutation)**.** *The following permutation*

$$\pi = \begin{array}{c} 1 \to 2 \\ 2 \to 5 \\ 3 \to 4 \\ 4 \to 3 \\ 5 \to 1 \end{array}$$

can be also written in different forms. The most common one is the following:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

In the permutation we can see 2 cycles: $1 \to 2 \to 5 \to 1$ and $3 \to 4 \to 3$. The first cycle can be written as $(1, 2, 5)$ (or $(5, 1, 2)$ or $(2, 5, 1)$) and the second one as $(3, 4)$ (or $(4, 3)$). The cycles gives us the shortest form of writing the permutation:

$$\pi = (1, 2, 5)(3, 4) = (3, 4)(5, 1, 2).$$

Definition A.22 (Parity of a permutation)**.** *When X is a finite set of at least two elements, the permutations of X (i.e. the bijective functions from X to X) fall into two classes of equal size: the even permutations and the odd permutations. If any total ordering of X is fixed, the parity (oddness or evenness) of a permutation σ of X can be defined as the parity of the number of inversions for σ, i.e., of pairs of elements x, y of X such that $x < y$ and $\sigma(x) > \sigma(y)$ [34].*

Table A.2: Cayley table for S_2

$\circ$	e	τ
e	e	τ
τ	τ	e

Example A.4 (Parity of a permutation). *For the following permutation* $(2,5,4,1,3)$ *we have the following inversions*

$$(2,5,4,1,3) \rightarrow_{(1,2)} (1,5,4,2,3) \rightarrow_{(5,2)}$$
$$(1,2,4,5,3) \rightarrow_{(3,4)} (1,2,3,5,4) \rightarrow_{(5,4)} (1,2,3,4,5)$$

We have made 4 inversions and as result the permutation is even.

Definition A.23 (Alternating group). *Alternating group [11] is the group of even permutations (see definition A.22) of a finite set. The alternating group on a set of* n *elements is called the alternating group of degree* n*, or the alternating group on* n *letters and denoted by* A_n*.*

Example A.5 (S_n group). *If we a have a permutation of* n *elements then it's possible to do by means of* $n!$ *ways.*

Example A.6 (S_1 group). S_1 *permutation of 1 element consists of only one element e - the simplest possible group*

Example A.7 (S_2 group). S_2 *permutation consists of 2 elements:*

1. *identity:* $e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

2. *transposition:* $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

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

Example A.8 (S_3 group). 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 can be obtained from this ones (see table A.3).*

1. *identity* $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

2. *transposition:* $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Table A.3: Cayley table for S_3 [9]

$\circ$	e	σ	σ_1	τ	τ_1	τ_2
e	e	σ	σ_1	τ	τ_1	τ_2
σ	σ	σ_1	e	τ_2	τ	τ_1
σ_1	σ_1	e	σ	τ_1	τ_2	τ
τ	τ	τ_1	τ_2	e	σ_1	σ
τ_1	τ_1	τ_2	τ	σ	e	σ_1
τ_2	τ_2	τ	τ_1	σ_1	σ	e

3. *circle:* $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Another elements of S_3*:* $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *and* $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

As we can see from the table A.3 the elements e, σ, σ_1 *forms a subgroup of* S_3 *moreover all the permutation (see definition A.22). I.e. there we will have Alternating group* A_3.

Example A.9 (S_3/A_3 quotient group)**.** *Lets consider the following Quotient group* S_3/A_3*. As we can see all elements of* S_3 *can be divided into 2 classes each of them with size* $3 = |A_3|$*:* $E = A_3 = \{e, \sigma, \sigma_1\}$ *and* $G = \{\tau, \tau_1, \tau_2\}$*. If we take an element* $x_1 \in E$ *and multiply it on another element of* $x_2 \in E$ *we will get* $x_1 x_2 \in E$ *(see table A.3) i.e.* $E \cdot E = E$*. For* G *we can get* $G \cdot G = E$ *and* $E \cdot G = G \cdot E = G$*. Therefore* $S_3/A_3 = \{E, G\}$ *forms a group of order 2. Thus*

$$S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$$

A.4 Rings and Fields

A.4.1 Rings

Definition A.24 (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 A.10 (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 A.25 (Multiplicative group)**.** *If* R *is a ring then the multiplicative group* $(R)^{\times}$ *is a group of invertible elements of* R *with the defined multiplication operation.*

Example A.11 (Multiplicative group of integers modulo n)**.** $(\mathbb{Z}/9\mathbb{Z})^{\times} = \{1, 2, 4, 5, 7, 8\}$ *[31]*

A.4.2 Ideals

Definition A.26 (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 A.12 (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 A.13 (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

$$\begin{aligned} \bar{k} \oplus \bar{l} &= \overline{k+l} \\ \bar{k} \odot \bar{l} &= \overline{k \cdot l} \end{aligned}$$

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

Definition A.27 (Ideal generated by a set)**.** *Let R be a Ring and S is a sub set of R. Consider the following set*

$$I = \{r_1 s_1 + \cdots + r_n s_n | n \in \mathbb{N}, r_i \in R, s_i \in S\}$$

I is called by an ideal generated by set S if $\forall r \in R, i \in I : r \cdot i \in I$.

The sum in the definition of the ideal should be finite. The ring is assumed commutative in the definition.

Definition A.28 (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 A.29 (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 A.30 (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 A.31 (Maximal ideal)**.** *A maximal ideal is an ideal that is maximal (with respect to set inclusion) amongst all Proper ideals i.e. I is a maximal ideal of a ring R if there are no other ideals contained between I and R [30].*

Example A.14 (Maximal ideal). *If F is a Field then the only maximal ideal is $\{0\}$ [30].*

Definition A.32 (Prime ideal). *An ideal I of a commutative ring R is prime if it has the following 2 properties* [1]

1. *If $a, b \in R$ such that $ab \in I$ then $a \in I$ or $b \in I$*

2. *I is not equal the whole ring R*

Definition A.33 (Proper ideal). *I is a proper ideal of a ring R if $I \subsetneq R$.*

Theorem A.6 (About proper ideal). *An ideal I of ring R is proper if and only if $1_R \notin I$.*

Definition A.34 (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

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

This equivalence class is also sometimes written as a mod I and called the "residue class of a modulo I" (see also example A.13).

The special $+$ and $\cdot$ operations are defined as follows

$$\forall \bar{x}, \bar{y} \in R/I : \bar{x} + \bar{y} = (x + I) + (y + I) = (x + y) + I = \overline{x + y}.$$

$$\forall \bar{x}, \bar{y} \in R/I : \bar{x} \cdot \bar{y} = (x + I) \cdot (y + I) = (x \cdot y) + I = \overline{x \cdot y}.$$

As result we will get the following ring $(R/I, +, \cdot)$ is called the quotient ring of R by I.

See also Quotient group

[1] There is a generalization of prime numbers in arithmetic

A.4.3 Polynomial ring $K[X]$

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

$$f = (f_0, f_1, \dots), \; f_i \in K, \tag{A.2}$$

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

We can define addition and multiplication on B as follows

$$\begin{aligned} f + g &= (f_0 + g_0, f_1 + g_1, \dots), \\ f \cdot g = h &= (h_0, h_1, \dots), \end{aligned} \tag{A.3}$$

where

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

The sequences (A.2) 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

$$\begin{aligned} X &= (0, 1, 0, \dots), \\ X^2 &= (0, 0, 1, \dots) \end{aligned}$$

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 (A.2), when one can get

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

Definition A.35 (Polynomial ring). *The Ring of sequences (A.2) with operations defined by (A.3) is called as polynomial ring $K[X]$.*

Lemma A.1 (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 A.36 (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*

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

Definition A.37 (Irreducible polynomial)**.** *An irreducible polynomial is, roughly speaking, a non-constant polynomial that cannot be factored into the product of two non-constant polynomials.*

Example A.15 (Irreducible polynomial)**.** *The following polynomial is irreducible in* $\mathbb{R}[X]$*:* $X^2 + 1$*. The following one is also irreducible despite it has a root:* $X + 1$*.*

Theorem A.7 (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. □

Theorem A.8 (About ideal generated by irreducible polynomial)**.** *Let* $P \in K[X]$ *is a polynomial and* $I = (P)$ *is an Ideal generated by the polynomial. The* I *is Maximal ideal if and only if* P *is irreducible in* $K[X]$

Proof. Let P is reducible i.e. $P = GF$. In the case $(P) \subset (G)$ and $(P) \subset (F)$ i.e. by definition it is not a maximal ideal.

If P is irreducible then $K[X]/(P)$ is a field (see section 1.1.4) and by theorem A.9 (P) is a maximal ideal. □

A.4.4 Fields

Definition A.38 (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 A.16 (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 A.39 (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.*

Theorem A.9 (About Quotient Ring and Maximal Ideal). *Let* $(R, +, \cdot)$ *is a commutative Ring with additive identity* 0_R *and multiplicative identity* 1_R*. Let* I *be an Ideal of* R *then* I *is Maximal ideal if and only if Quotient ring* R/I *is a Field*

Proof. See the end of section 2.3.3. □

Definition A.40 (Fraction field). *The field of fractions of an integral domain is the smallest field in which it can be embedded. The elements of the field of fractions of the integral domain* R *are equivalence classes (see the construction below) written as* $\frac{a}{b}$ *with* $a, b \in R$ *and* $b \neq 0$*. The field of fractions of* R *is sometimes denoted by* $\mathrm{Quot}(R)$ *or* $\mathrm{Frac}(R)$ *[20].*

A.4.5 Characters

Definition A.41 (Character). *For an abelian group* G*, finite or infinite, a character of* G *is a group homomorphism* $\phi : G \to F^\times$ *where* F *is a field.*

The definition was taken from [3]

Example A.17 (Character). *A field homomorphism* $K \to F$ *is a character by restricting it to the non- zero elements of* K *(that is, using* $G = K^\times$*) and ignoring the additive aspect of a field homomorphism.*

The example was taken from [3]

Theorem A.10 (Dedekind). *If we have* n *distinct Characters* $\phi_1, \dots, \phi_n : G \to F^\times$ *then they are linearly independent i.e. if* $c_1, \dots, c_n \in F$ *satisfy*

$$c_1\phi_1(g) + \dots + c_n\phi_n(g) = 0$$

for all $g \in G$ *then* $c_1 = \dots = c_n = 0$ *(see also [3]).*

A.5 Modules and Vector spaces

A.5.1 Modules

A module over a ring is a generalization of the notion of vector space over a field, wherein the corresponding scalars are the elements of an arbitrary given ring (with identity) and a multiplication (on the left and/or on the right) is defined between elements of the ring and elements of the module.

Definition A.42 (Module). *Let R is a Ring and 1_R is it's multiplicative identity. A left R-module M consists of an Abelian group $(M,+)$ and an operation $\cdot : R \times M \to M$ such that $\forall r,s \in R$ and $\forall x,y \in M$ the following relations are hold:*

1. $r \cdot (x+y) = r \cdot x + r \cdot y$
2. $(r+s) \cdot x = r \cdot x + s \cdot x$
3. $(rs) \cdot x = r \cdot (s \cdot x)$
4. $1_R \cdot x = x$

Example A.18 (Module). *If K is a Field then concepts of K-Vector space and K-module are the same*

Definition A.43 (Generating set of a module). *A generating set G of a module M over a ring R is a subset of M such that the smallest submodule of M containing G is M itself [25]*

Definition A.44 (Free module). *The Module that has a basis (i.e. linearly independent generating set) is called as free module [23].*

For a R-module M the set $E \subseteq M$ is a basic for M if

1. *E is a generating set (see definition A.43) for M i.e. $\forall m \in M\ \exists n < \infty$: $\exists e_i \in E, r_i \in R$: $m = \sum_{i=1}^{n} r_i e_i$*
2. *E is linearly independent, i.e. if $r_1 e_1 + \cdots + r_n e_n = 0_M$ for distinct elements $e_1, \ldots, e_n \in E$ then $r_1 = \cdots = r_n = 0_R$.*

Definition A.45 (Rank of free module). *The cardinality of any (and therefore every) basis is called the rank of the free module M [23].*

Definition A.46 (Direct sum of modules)**.** *In abstract algebra, the direct sum is a construction which combines several modules into a new, larger module. The direct sum of modules is the smallest module which contains the given modules as submodules with no "unnecessary" constraints, making it an example of a coproduct. Contrast with the direct product, which is the dual notion [16].*

Example A.19 (Direct sum of modules)**.** *If we have 2 Free modules M and N with bases $m_1, m_2, \ldots, m_m$ and $n_1, n_2, \ldots, n_n$. Then the Direct sum of modules $A = M \oplus N$ will also be a free module with composite basis: $m_1, m_2, \ldots, m_m, n_1, n_2, \ldots, n_n$*

Definition A.47 (Finitely generated module)**.** *Finitely generated module is a module that has a finite generating set (see also definition A.43) [22].*

A.5.2 Linear algebra

Definition A.48 (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 A.2 (About vector space isomorphism)**.** *2 vector spaces L and M with same dimension $dimL = dimM$ then there exists an Isomorphism between them*

Definition A.49 (Image). *The image or range of a linear map $f : V \to W$ is the following set [28]:*

$$\operatorname{Im} f = \{w \in W : w = f(v), v \in V\}$$

Definition A.50 (Kernel). *The kernel of a linear map $f : V \to W$ is the following set [27]:*

$$\ker f = \{v \in V : f(v) = 0\}$$

Definition A.51 (Rank). *The rank of a linear map $f : V \to W$ is dimension of Image: $rgf = \dim \operatorname{Im} f$ [36]:*

Definition A.52 (General linear group of a vector space). *If V is a Vector space over field K the general linear group of V, written $GL\,(V)$ or $Aut\,(V)$, is the group of all automorphisms of V, i.e. the set of all bijective linear transformations $V \to V$, together with functional composition as group operation [24].*

Definition A.53 (Dual space). *Given any vector space V over a field F, the dual space V^* is defined as the set of all linear maps $\phi : V \to F$ (linear functionals). The dual space V^* itself becomes a vector space over F when equipped with an addition and scalar multiplication satisfying:*

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x)$$
$$(a\varphi)(x) = a\,(\varphi(x))$$

for all $\phi, \psi \in V^*$, $x \in V$, and $a \in F$.

This is also named as algebraic dual space at [17].

Definition A.54 (Degenerate bilinear form). *A degenerate bilinear form $f(x, y)$ on a vector space V is a bilinear form such that the map from V to V^* (the Dual space of V) given by $v \to (x \to f(x, v))$ is not an isomorphism [14].*

An equivalent definition when V is finite-dimensional is that it has a non-trivial kernel: there exist some non-zero $x \in V$ such that $\forall y \in V f(x, y) = 0$

Definition A.55 (Non-degenerate bilinear form). *A nondegenerate or non-singular form is one that is not degenerate, meaning that the map from V to V^* (the Dual space of V) given by $v \to (x \to f(x, v))$ is an isomorphism [14] or equivalently when V is finite-dimensional if and only if $\forall y \in V f(x, y) = 0$ implies $x = 0$.*

A.6 Functions aka maps

A.6.1 Functions

Definition A.56 (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 A.57 (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 A.58 (Bijection). *The function $f : X \to Y$ is bijective (or one-to-one correspondence) if it is an Injection and a Surjection.*

Definition A.59 (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 A.60 (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 A.61 (Endomorphism). *An endomorphism is a morphism (or homomorphism) from a mathematical object to itself [18]*

Definition A.62 (Automorphism). *Automorphism is an isomorphism from a mathematical object to itself.*

Definition A.63 (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.

Theorem A.11 (First isomorphism theorem). *Let G is a group and $\phi : G \to H$ is a surjective Homomorphism. Then if $N = \ker \phi$ we have*

$$H \cong G/N$$

Theorem A.12 (Isomorphism extension theorem)**.** *Let F is a Field and E is an Algebraic extension of F. F' is another Field and E' the Algebraic extension of F'.*

If there exists an Isomorphism $\phi : F \to F'$ then it can be extended to an isomorphism $\tau : E \to E'$.

Proof. The proof of the isomorphism extension theorem depends on Zorn's lemma.

??? The theorem seems to be very close to the theorem 2.3. □

A.6.2 Category theory

Definition A.64 (Commutative diagram)**.** *A commutative diagram is a diagram of objects (also known as vertices) and morphisms (also known as arrows or edges) such that all directed paths in the diagram with the same start and endpoints lead to the same result by composition*

The following diagram commutes if $f_{AB} = f_{CB} f_{AC}$ or $f_{AB}(x) = f_{CB}(f_{AC}(x))$.

$$\begin{tikzcd} A \arrow[rr, "f_{AB}"] \arrow[dr, "f_{AC}"'] & & B \\ & C \arrow[ur, "f_{CB}"'] & \end{tikzcd}$$

A.7 Number theory

Definition A.65 (Euler's totient function)**.** *In number theory, Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter phi as $\phi(n)$, and may also be called Euler's phi function. It can be defined more formally as the number of integers k in the range $1 \leq k \leq n$ for which the greatest common divisor $gcd(n, k) = 1$. The integers k of this form are sometimes referred to as totatives of n.*

The definition was taken from [19]

Example A.20 (Euler's totient function)**.** *For example [19], the totatives of $n = 9$ are the six numbers 1, 2, 4, 5, 7 and 8. They are all relatively prime to 9, but the other three numbers in this range, 3, 6, and 9 are not, because $gcd(9, 3) = gcd(9, 6) = 3$ and $gcd(9, 9) = 9$. Therefore, $\phi(9) = 6$. As another example, $\phi(1) = 1$ since for $n = 1$ the only integer in the range from 1 to n is 1 itself, and $gcd(1, 1) = 1$.*

Bibliography

[1] Brown, K. The primitive element theorem / Ken Brown. — http://www.math.cornell.edu/~kbrown/6310/primitive.pdf.

[2] Conrad, K. Finite fields / Keith Conrad. — http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/finitefields.pdf.

[3] Conrad, K. Linear independence of characters / Keith Conrad. — http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/linearchar.pdf.

[4] Conrad, K. Separability ii / Keith Conrad. — http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/separable2.pdf.

[5] Conrad, K. Tensor poroducts / Keith Conrad. — http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/tensorprod.pdf.

[6] Normal extension (rus) — wikipedia, the free encyclopedia. — 2014. — http://ru.wikipedia.org/?oldid=65922374.

[7] Ribenboim, P. Classical Theory of Algebraic Numbers / P. Ribenboim. Universitext. — Springer New York, 2001. — https://books.google.ru/books?id=u5443xdaNZcC.

[8] Rowland, T. Group fixed point. — 2016. — From MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/GroupFixedPoint.html.

[9] Wikibooks. Abstract algebra/group theory/permutation groups — wikibooks, the free textbook project. — 2016. — [Online; accessed 27-September-2016]. https://en.wikibooks.org/w/index.php?title=Abstract_Algebra/Group_Theory/Permutation_groups&oldid=3070727.

[10] Wikipedia. Simple extension — wikipedia, the free encyclopedia. — 2014. — [Online; accessed 20-September-2016]. https://en.wikipedia.org/w/index.php?title=Simple_extension&oldid=595508851.

[11] Wikipedia. Alternating group — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 27-September-2016]. https://en.wikipedia.org/w/index.php?title=Alternating_group&oldid=736689793.

[12] Wikipedia. Commutator — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 30-September-2016]. https://en.wikipedia.org/w/index.php?title=Commutator&oldid=740207690.

[13] Wikipedia. Commutator subgroup — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 30-September-2016]. https://en.wikipedia.org/w/index.php?title=Commutator_subgroup&oldid=737371946.

[14] Wikipedia. Degenerate bilinear form — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 10-September-2016]. https://en.wikipedia.org/w/index.php?title=Degenerate_bilinear_form&oldid=738751020.

[15] Wikipedia. Direct sum — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 24-September-2016]. https://en.wikipedia.org/w/index.php?title=Direct_sum&oldid=738351383.

[16] Wikipedia. Direct sum of modules — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 25-September-2016]. https://en.wikipedia.org/w/index.php?title=Direct_sum_of_modules&oldid=730018916.

[17] Wikipedia. Dual space — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 6-October-2016]. https://en.wikipedia.org/w/index.php?title=Dual_space&oldid=742901318.

[18] Wikipedia. Endomorphism — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 2-October-2016]. https://en.wikipedia.org/w/index.php?title=Endomorphism&oldid=726230579.

[19] Wikipedia. Euler's totient function — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 14-September-2016].

https://en.wikipedia.org/w/index.php?title=Euler%27s_totient_function&oldid=736552571.

[20] Wikipedia. Field of fractions — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 5-October-2016]. https://en.wikipedia.org/w/index.php?title=Field_of_fractions&oldid=720271734.

[21] Wikipedia. Finitely generated abelian group — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 3-June-2016]. https://en.wikipedia.org/w/index.php?title=Finitely_generated_abelian_group&oldid=723506843.

[22] Wikipedia. Finitely generated module — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 5-October-2016]. https://en.wikipedia.org/w/index.php?title=Finitely_generated_module&oldid=735554374.

[23] Wikipedia. Free module — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 9-January-2016]. https://en.wikipedia.org/w/index.php?title=Free_module&oldid=699002213.

[24] Wikipedia. General linear group — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 2-October-2016]. https://en.wikipedia.org/w/index.php?title=General_linear_group&oldid=738480571.

[25] Wikipedia. Generating set of a module — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 5-October-2016]. https://en.wikipedia.org/w/index.php?title=Generating_set_of_a_module&oldid=732648521.

[26] Wikipedia. Group action — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 28-August-2016]. https://en.wikipedia.org/w/index.php?title=Group_action&oldid=735249701.

[27] Wikipedia. Kernel (linear algebra) — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 24-September-2016]. https://en.wikipedia.org/w/index.php?title=Kernel_(linear_algebra)&oldid=735290769.

[28] Wikipedia. Linear map — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 24-September-2016]. https://en.wikipedia.org/w/index.php?title=Linear_map&oldid=740065546.

[29] Wikipedia. Local ring — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 23-April-2016]. https://en.wikipedia.org/w/index.php?title=Local_ring&oldid=716779040.

[30] Wikipedia. Maximal ideal — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 29-July-2016]. https://en.wikipedia.org/w/index.php?title=Maximal_ideal&oldid=704326783.

[31] Wikipedia. Multiplicative group of integers modulo n — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 20-September-2016]. https://en.wikipedia.org/w/index.php?title=Multiplicative_group_of_integers_modulo_n&oldid=739054442.

[32] Wikipedia. Nilpotent — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 29-July-2016]. https://en.wikipedia.org/w/index.php?title=Nilpotent&oldid=727125150.

[33] Wikipedia. Normal subgroup — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 9-September-2016]. https://en.wikipedia.org/w/index.php?title=Normal_subgroup&oldid=737429252.

[34] Wikipedia. Parity of a permutation — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 28-September-2016]. https://en.wikipedia.org/w/index.php?title=Parity_of_a_permutation&oldid=736707840.

[35] Wikipedia. Quotient group — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 27-September-2016]. https://en.wikipedia.org/w/index.php?title=Quotient_group&oldid=726415849.

[36] Wikipedia. Rank (linear algebra) — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 24-September-2016]. https://en.wikipedia.org/w/index.php?title=Rank_(linear_algebra)&oldid=739885289.

[37] Wikipedia. Subgroup — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 23-September-2016]. https://en.wikipedia.org/w/index.php?title=Subgroup&oldid=737399477.

[38] Wikipedia. Sylow theorems — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 1-October-2016]. https://en.wikipedia.org/w/index.php?title=Sylow_theorems&oldid=735518140.