Introduction to Galois Theory

April 21, 2017

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 (Definition A.107) 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 1.2 (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 1.3 (Field extension)**.** Let K and L are fields. L is an extension of K if $L \supset K$

and another definition

Definition 1.4 (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 1.5 (K-algebra and homomorphism)**.** *Given a K-algebra is the same as having Homomorphism (Definition A.126) $f : K \to A$ of rings.*

Proof. Really if I have a K-algebra I can define the Homomorphism (Definition A.126) $f(k) = k \cdot 1_A$, where 1_A is an identity element of A. Thus $k \cdot 1_A \in A$.

And conversely if I have the Homomorphism (Definition A.126) $f : K \to A$ 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 1.6 (About homomorphism of fields)**.** *Any Homomorphism (Definition A.126) of fields is Injection (Definition A.124).* [2]

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 (Definition A.126) can be set between field K and its K-algebra. The Homomorphism (Definition A.126) is Injection (Definition A.124) therefore we can allocate a sub-field $A' \subset A$ for that we will have the Homomorphism (Definition A.126) is a Surjection (Definition A.123) and therefore we have an Isomorphism (Definition A.127) 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.

[1] L in the definition is not the same object with L from definition 1.3. Because L in the definition is a K-algebra i.e. a ring but L in the definition 1.3 is a field.

[2] But the statement is not valid for groups. In that case the homomorphism is injection if and only if the kernel is trivial and consists of only one element - identity. See theorem A.133.

Example 1.7 (Field extensions)**.** $\mathbb{C}$ *is a field extension for* $\mathbb{R}$*.* $\mathbb{R}$ *is a field extension for* $\mathbb{Q}$

Example 1.8 (K-algebra is not a field)**.** *In the example* [3] *I will show that* K *algebra is not a field. Consider* $K = \mathbb{R}$*. Vector space (Definition A.107)* $A = \mathbb{R}^2$ *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 (Definition 1.1) are satisfied

$$(x+y)\cdot z = \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right)\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} =$$
$$= \begin{pmatrix} (x_1+y_1)z_1 \\ (x_2+y_2)z_2 \end{pmatrix} = \begin{pmatrix} x_1z_1 + y_1z_1 \\ x_2z_2 + y_2z_2 \end{pmatrix} = x\cdot z + y\cdot z$$
$$z\cdot(x+y) = z\cdot x + z\cdot y$$
$$(ax)\cdot(by) = \begin{pmatrix} ax_1 \\ ax_2 \end{pmatrix}\begin{pmatrix} by_1 \\ by_2 \end{pmatrix} = \begin{pmatrix} abx_1y_1 \\ abx_2y_2 \end{pmatrix}(ab)(x\cdot y)$$

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* $L' \cong \mathbb{R}$*.*

[3] 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 $charL = 0$
2. $1+1+\cdots+1 = \sum_{i=1}^{m} 1 = 0$ for some $m \in \mathbb{Z}$. The first time when it happens is for a prime number i.e. minimal m with the property is prime. In this case $charL = p$, where $p = \min m$ - 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 (Definition A.63) of polynomials. The $P \in K[X]$ is an Irreducible polynomial (Definition A.85). (P) is an Ideal (Definition A.67) formed by the polynomial. [4] 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. [5] Then with Bézout's lemma (Lemma A.83) 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 1.9. *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 (Definition A.127) 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 (Definition A.85) (see example A.86).

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

[5] 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 (Definition A.126):*

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

The ϕ *defined by (1.2) is Homomorphism (Definition A.126). 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 (Definition A.123) 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 A.131) theorem.

1.2 Algebraic elements. Minimal polynomial

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

Alternative proof that $K[X]/(P)$ is the Field (Definition A.89). The (P) is a Maximal ideal (Definition A.74) [6] but a quotient by a Maximal ideal (Definition A.74) is a Field (Definition A.89) (see theorem About Quotient Ring and Maximal Ideal (Theorem A.92)).

$K[X]/(P)$ is an extension of K because it's K-algebra (Definition 1.1).

Example 1.10 ($K = \mathbb{F}_2/(X^2+X+1)$)**.** *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

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

[6] To prove that (P) is a Maximal ideal (Definition A.74) we have to use Bézout's lemma (Lemma A.83).

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

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

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

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

therefore

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

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

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

and thus

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

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 $K = \mathbb{F}_2/(X^2 + X + 1)$ *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 3.8).*

1.2.2 Algebraic elements

Definition 1.11 (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 1.12 (About minimal polynomial existence)**.** *If α is Algebraic element (Definition 1.11) 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* [7]

Proof. We know that $K[X]$ is a Principal ideal domain (Definition A.73) and a polynomial $Q(\alpha) = 0$ forms an Ideal (Definition A.67): $I\{Q \in K[X] \mid Q(\alpha) = 0\}$, 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 1.13 (Minimal polynomial)**.** If α is Algebraic element (Definition 1.11) 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 1.14. 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 (Definition 1.1)) contained K and α denoted by $K[\alpha]$.

As soon as $K[\alpha]$ is a K-algebra (Definition 1.1) it is a Vector space (Definition A.107) over K generated by

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

Example 1.15 ($\mathbb{C}$)**.**

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

$\mathbb{C}$ is also a Vector space (Definition A.107) generated by 1 and i: $\forall z \in \mathbb{Z}$ it holds $z = x + iy$ where $x, y \in \mathbb{R}$.

Proposition 1.16. *The following assignment are equivalent*

1. *α is algebraic over K*
2. *$K[\alpha]$ is a finite dimensional Vector space (Definition A.107) over K*

[7] see also theorem About irreducible polynomials (Theorem A.87)

3. $K[\alpha] = K(\alpha)$ [8]

Proof. Lets proof that 1 implies 2. If α is algebraic over K then using lemma Minimal polynomial (Definition 1.13) $\exists P_{min}(\alpha, K)$:

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

where $a_k \in K$. Then

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

this means that any α^n can be represented as a linear combination of finite number of powers of α i.e. $K[\alpha]$ generated by $1, \alpha, \ldots, \alpha^{d-1}$ is a finite dimensional Vector space (Definition A.107).

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 (Definition A.124). [9] But the $K[\alpha]$ is finite dimensional Vector space (Definition A.107) and a Homomorphism (Definition A.126) between 2 vector spaces with the same dimension is Surjection (Definition A.123) [10] thus $\exists y \in K[\alpha]$ such that $x \cdot y = 1_{K[\alpha]}$. Therefore x is invertable and $K[\alpha]$ is a Field (Definition A.89).

Lets proof that 3 implies 1. Let $K[\alpha]$ is a Field (Definition A.89) but α is not algebraic. Thus $\forall P \in K[X]\ P(\alpha) \neq 0$. The we have an Injection (Definition A.124) Homomorphism (Definition A.126) $i : K[X] \to K[\alpha] = K(\alpha)$ which sends $P(X)$ to $P(\alpha)$. [11] But $K[X]$ is not a field thus $K[\alpha]$ should not be a field too that is in contradiction with the initial conditions. [12] □

[8] Contrary to the example 1.8 we see that K-algebra is a field there.

[9] 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 (Definition A.124) property is satisfied.

[10] Two vector spaces with same dimension are isomorphic each other (see lemma A.108)

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

[12] Alternative prove is the following. Let $x \neq 0 \in K[X]$ and $K[\alpha]$ is a field then $i(x)$ is invertable i.e. $\exists y \in K[X] : i(x)i(y) = 1$ or $i(xy) = 1$ or finally x - is invertable and $K[X]$ is a field but $K[X]$ is a ring and therefore we just got a contradiction.

Definition 1.17 (Algebraic extension)**.** L an extension of K is called algebraic over K if $\forall \alpha \in L$ - α is algebraic over K.

Proposition 1.18. *If L is algebraic over K then any K-subalgebra of L is a Field (Definition A.89).*

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. [13] □

Proposition 1.19. *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. It is clear because $P_{min}(\alpha, K) \in L[X]$. [14] □

We can consider the following example (it is not a part of the lectures) as an illustration for proposition 1.19:

Example 1.20. *$K = \mathbb{R}, L = M = \mathbb{C}$. $\alpha = i \in M$ is algebraic over $K = \mathbb{R}$ and therefore using the proposition 1.19 it is algebraic over $L = \mathbb{C}$. Moreover $P_{min}(\alpha, L) = X - i$ and it divides $P_{min}(\alpha, K) = X^2 + 1$.*

1.4 Finite extensions. Algebraicity and finiteness

Definition 1.21 (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 1.22 (The multiplicativity formula for degrees)**.** *Let $K \subset L \subset M$. Then M is Finite extension (Definition 1.21) over K if and only if M is Finite extension (Definition 1.21) over L and L is Finite extension (Definition 1.21) over K. In this case*

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

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

[14] 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 (Lemma 1.12) one can get that $P_{min}(\alpha, L)$ divides $P_{min}(\alpha, K)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

then $\forall i$:

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

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

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

□

Definition 1.23 ($K(\alpha_1, \ldots, \alpha_n)$)**.** $K(\alpha_1, \ldots, \alpha_n) \subset L$ generated by $\alpha_1, \ldots, \alpha_n$ is the smallest sub field of L contained K and $\alpha_i \in L$.

Theorem 1.24 (About towers)**.** *L is finite over K if and only if L is generated by a finite number of algebraic elements over K.*

Proof. If L is finite then $\alpha_1, \ldots, \alpha_d$ is a basis. In this case $L = K[\alpha_1, \ldots, \alpha_d] = K(\alpha_1, \ldots, \alpha_d)$. Moreover each $K[\alpha_i]$ is finite dimensional thus by proposition 1.16 α_i is algebraic.

From other side if we have a finite set of algebraic elements $\alpha_1, \ldots, \alpha_d$ then $K[\alpha_1]$ is a finite dimensional Vector space (Definition A.107) over K, $K[\alpha_1, \alpha_2]$ is a finite dimensional Vector space (Definition A.107) over $K[\alpha_1]$ and so on $K[\alpha_1, \ldots, \alpha_d]$ is a finite dimensional Vector space (Definition A.107) over $K[\alpha_1, \ldots, \alpha_{d-1}]$. All elements are algebraic thus

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

Then using theorem 1.22 we can conclude that $K(\alpha_1, \ldots, \alpha_d)$ has finite dimension. □

1.5 Algebraicity in towers. An example

Theorem 1.25. *$K \subset L \subset M$ then M Algebraic extension (Definition 1.17) over K if and only if M algebraic over L and L algebraic over K.*

Proof. If $\alpha \in M$ is an Algebraic element (Definition 1.11) 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. [15] □

[15] $P_{min}(\alpha, L) = \sum_{i=0}^{d-1} l_i \alpha^i$ where $l_i \in L$ and each l_i is algebraic over K by algebraic extension definition 1.17. By theorem 1.24 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.

Example 1.26 ($\mathbb{Q}$ 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*

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

$$\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right):\mathbb{Q}\right]=3\cdot2=6.$$

Proposition 1.27 (On dimension of extension)**.**

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

if α *is algebraic.*

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

Proposition 1.28 (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

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

[16]

□

[16] We also have that $K[\alpha,\beta]$ is a field: $K[\alpha,\beta]=K(\alpha,\beta)$. Really $K[\alpha]=K(\alpha)$ (see proposition 1.16). β is algebraic over K and therefore over $K(\alpha)$ thus we can construct $K(\alpha)[\beta]=K(\alpha,\beta)$ by proposition 1.16

1.6 A digression: Gauss lemma, Eisenstein criterion

What we have seen so far:

- K is a field, α is an Algebraic element (Definition 1.11) over K if it is a root of a polynomial $P \in K[X]$.
- L is an Algebraic extension (Definition 1.17) over K if $\forall \alpha \in L$: α is an algebraic over K
- L is a Finite extension (Definition 1.21) 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 1.24)
- $[K[\alpha] : K] = degP_{min}(\alpha, K)$ (see proposition 1.27).

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

Lemma 1.29 (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 1.30 (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

$$\begin{aligned} Q &\equiv x^k \mod 2, \\ R &\equiv x^l \mod 2, \end{aligned}$$

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 1.31 (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 1.30. □

Note: that both: Gauss (Equation 1.29) and Eisenstein criterion (Lemma 1.31) are valid by replacing $\mathbb{Z}$ with an Unique factorization domain (Definition A.91) 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 (Definition A.84). Field extension (Definition 1.3) 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 (Definition A.85) moreover the root of the P is in the field (see example 1.10).

We also can say that for any stem field E:

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

We can use the following Isomorphism (Definition A.127): $f : \forall \mathcal{P} \in K[X]/(P) \to \mathcal{P}(\alpha)$, 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 [17]

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

Proposition 2.2 (About stem field existence)**.** *The stem field exist and if we have 2 stem fields E and E' which correspond 2 roots of P: $E = K[\alpha]$, $E' = K[\alpha']$ then $\exists! f : E \cong E'$ (Isomorphism (Definition A.127) of K-algebras) such that $f(\alpha) = \alpha'$.*

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

Uniquest of the Isomorphism (Definition A.127) 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 2.3 (About stem field).

1. In particular: If a stem field contains 2 roots of P then $\exists!$ Automorphism (Definition A.129) 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 2.4. *$P \in K[X]$ is irreducible over K if and only if it does not have a root in Field extension (Definition 1.3) 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 (Definition 2.1) 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 1.12) i.e. P become reducible. □

Corollary 2.5. *$P \in K[X]$ 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 (Definition 2.1) 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 2.6 (Splitting field)**.** Let $P \in K[X]$. The splitting field of P over K is an extension L where P is split (i.e. is a product of linear factors) and roots of P generate L

Theorem 2.7 (About splitting fields)**.** *1. Splitting field L exists and $[L:K] \leq d!$, where $d = degP$.*

[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 2.3)

[7] $K \subset K(\alpha) \subset M$ and with The multiplicativity formula for degrees (Theorem 1.22) we have

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

2. *If L and M are 2 splitting fields then $\exists\phi : L \cong M$ (an Isomorphism (Definition A.127)). But the Isomorphism (Definition A.127) is not necessary to be unique.*

Proof. Lets prove by induction on d. The first case ($d = 1$) is trivial the K itself is the splitting field. Now assume $d > 1$ and that the theorem is valid for any polynomial of degree $< d$ over any field K. Let Q be any irreducible factor of P. We can create a Stem field (Definition 2.1) $L_1 = K(\alpha)$ for Q that will be also a Stem field (Definition 2.1) 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 (Definition 2.6) 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 (Theorem 1.22)) is $\leq d \cdot (d-1)! = d!$.

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

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

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] □

[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 (Definition A.127) 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 2.2. 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

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

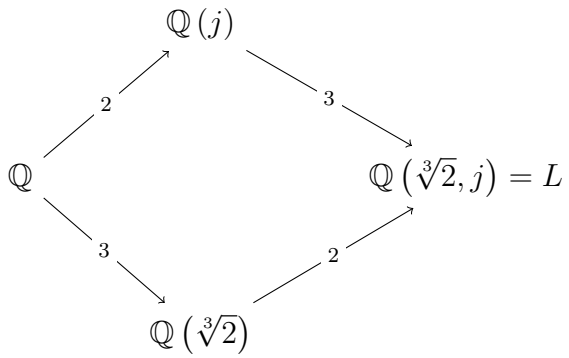
On each step we have an isomorphism between L_i and M_i and as result the isomorphism between resulting fields L and M (via ϕ) as L_n algebras and therefore as K algebras.

Remark 2.8. The Isomorphism (Definition A.127) considered in theorem 2.7 is not unique. A splitting field can have many Automorphism (Definition A.129) and this is in fact the subject of Galois theory.

2.3 An example. Algebraic closure

2.3.1 An example of automorphism

Example 2.9 (X^3-2 over $\mathbb{Q}$)**.** *Let we have the following polynomial* X^3-2 *over* $\mathbb{Q}$ *(see also example 6.10). 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 Automorphism (Definition A.129)s of the field.* $P_{min}\left(j, \mathbb{Q}\right) = X^2+X+1$ *thus using remark 2.3* $\left[\mathbb{Q}\left(j\right) : \mathbb{Q}\right] = 2$*. 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*



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

1. $\mathbb{Q}\left(\sqrt[3]{2}\right)$ *Automorphism (Definition A.129). 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 (Definition A.129) that exchanges the roots. Lets call it* τ [12]

2. $\mathbb{Q}\left(j\right)$ *Automorphism (Definition A.129). 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 $Aut\left(L/K\right)$ *is embedded into permutation*

[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 $j^2\sqrt[3]{2} \to j^3\sqrt[3]{2} = \sqrt[3]{2}$. 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 $j^2\sqrt[3]{2}$

group of 3 elements S_3 (see example A.54):

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

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

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

because σ and τ generates S_3 because

- *σ: $\sqrt[3]{2} \to j\sqrt[3]{2} \to j^2\sqrt[3]{2} \to \sqrt[3]{2}$. This is a circle.*
- *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 2.10 (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 2.11 ($\mathbb{C}$)**.** *$\mathbb{C}$ is an Algebraically closed field (Definition 2.10). This will be proved later.*

Definition 2.12 (Algebraic closure)**.** An algebraic closure of K is a field L that is Algebraically closed field (Definition 2.10) and Algebraic extension (Definition 1.17) over K. [14]

Theorem 2.13 (About Algebraic closure)**.** *Any field K has an Algebraic closure (Definition 2.12)*

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

$$K \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \ldots$$

[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 (Definition 2.10))
- $\forall \alpha \in L\ \exists P \in K[X]$ such that $P(\alpha) = 0$ (see definition of Algebraic extension (Definition 1.17))

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 (Definition A.70) $P(X_P)\ \forall P \in S$.[15] We claim that I is a Proper ideal (Definition A.79) i.e. $I \neq A$. If not then we can write (see theorem A.80)

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

where $\lambda_i \in A$ and the sum is the finite (see definition A.70). 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 (Definition 2.6) L for the polynomial P over K (see theorem 2.7).

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

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

that is impossible.

Fact: Any Proper ideal (Definition A.79) $I \subset A$ is contained in the Maximal ideal (Definition A.74) m (see proposition 2.16 below) and A/m is a field (see theorem A.92).

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 (Definition A.79) is in a Maximal ideal (Definition A.74). This is a consequence of what one calls Zorn's lemma

Definition 2.14 (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 $\beta \leq \alpha$.

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

[16] α_i is a root of P_i

Lemma 2.15 (Zorn). *If any non-empty Chain (Definition 2.14) $\mathcal{C}$ 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 2.16. *Any Proper ideal (Definition A.79) is in a Maximal ideal (Definition A.74)*

Proof. We can use Zorn (Lemma 2.15) lemma to prove that any proper ideal is in a Maximal ideal (Definition A.74).

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 (Definition 2.14) $\mathcal{C} = \{I_\alpha\}$ [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 $I \subset m$. □

If we take a Quotient ring (Definition A.81) 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

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

K_i is a field where each polynomial $P \in K_{i-1}$ has a root. The field K_i is Quotient ring (Definition A.81) of huge polynomial ring $K_{i-1}[X]$ by a suitable Maximal ideal (Definition A.74) that is got by means of Zorn (Lemma 2.15) lemma.

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

Theorem 2.17 (About extension of homomorphism). *Let $K \subset L \subset M$ - Algebraic extension (Definition 1.17). $K \subset \Omega$, where Ω - Algebraic closure (Definition 2.12) of K. $\forall \phi : L \to \Omega$ extends to $\widetilde{\phi} : M \to \Omega$* [20]

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

[18] We refer to it as a theorem with definition provided in A.92. 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 3.3.

Proof. Apply Zorn (Lemma 2.15) 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 (Definition 2.14) (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 (Definition 1.13) $P_{min}(x, N_0)$. It should have a root $\alpha \in \Omega$. Now we extend N_0 to $N_0(x)$ and define ψ' on $N_0(x)$ as follows: $\forall y \in N_0 : \psi'(y) = \psi_0(y)$ and $\psi'(x) = \alpha$. Thus we was able to find an element of the chain that is greater than maximal. Therefore our assumption about $N_0 \neq M$ was incorrect and we can conclude than $N_0 = M$ and therefore $\tilde{\phi} = \psi_0$. □

Corollary 2.18 (About algebraic closure isomorphism)**.** *If Δ and Δ' are 2 algebraic closures of K then they are isomorphic as K-algebras.*

Proof. Using theorem 2.17 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 (Definition A.124)) from Δ' to Δ.

If we assume $M = \Delta$ and $\Omega = \Delta$ then there exists a homomorphism (i.e. Injection (Definition A.124)) from Δ to Δ'. The Injection (Definition A.124) is also Surjection (Definition A.123) in another direction: $\Delta' \to \Delta$ and as result we have Isomorphism (Definition A.127) $\Delta' \to \Delta$ □

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 (Definition 2.12) of K is unique up to Isomorphism (Definition A.127) of K-algebras* [1]

Corollary 3.2. *Any Algebraic extension (Definition 1.17) of K embeds (see definition A.130) into the Algebraic closure (Definition 2.12)* [2]

Example 3.3 (Of extension of homomorphism)**.** *Let $K = \mathbb{Q}$ and $\overline{\mathbb{Q}}$ is the Algebraic closure (Definition 2.12) 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 (Definition A.1) of X in L. L has 2 Embedding (Definition A.130)s into $\overline{\mathbb{Q}}$

[1] There is a redefinition of corollary 2.18.

[2] i.e. $\forall E$ - algebraic extension of K, $\exists \phi : E \to \bar{K}$ - Homomorphism (Definition A.126). The statement is a reformulation of theorem 2.17

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

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

Let

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

β is a Class (Definition A.1) of Y in M. M has 4 Embedding (Definition A.130)s 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]

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

3.1.1 Finite fields

Definition 3.4 (Finite field)**.** K is a finite field if it's characteristic (see section 1.1.3) $charK = p$, where p - prime number

Remark 3.5 ($\mathbb{F}_{p^n}$). 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 3.6 (Frobenius homomorphism). If $charK = p$, then exists a Homomorphism (Definition A.126) $F_p : K \to K$ 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

[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 2.17) 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 1.10 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.

$$(x+y)^p \equiv (x^p + y^p) \mod p$$

$(xy)^p = x^p y^p$. The second property is the truth in the all fields (of course) but the first one is the special property of $\mathbb{F}_p$ fields.

Remark 3.7. Also $F_{p^n} : K \to K$ such that $F_{p^n}(x) = x^{p^n}$ is also homomorphism (a power of Frobenius homomorphism (Remark 3.6).)

3.2 Properties of finite fields

Theorem 3.8. *Lets fix $\mathbb{F}_p$ and it's Algebraic closure (Definition 2.12) $\overline{\mathbb{F}_p}$.*

The Splitting field (Definition 2.6) 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 (Definition A.126) (see remark 3.7) 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 (Definition 1.3) 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.

[8] For $x \in \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ we have that (see theorem A.40)

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

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 $\gcd(Q_n, -1) = \gcd(Q_n, 1) = 1$.

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 $\alpha^{p^n} - \alpha = 0$ (see theorem A.40). 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 2.7). □

Theorem 3.9. *$\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ 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

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

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 3.10. *$\mathbb{F}_{p^n}$ is a Stem field (Definition 2.1) and a Splitting field (Definition 2.6) of any Irreducible polynomial (Definition A.85) $P \in \mathbb{F}_p$ of degree n.*

Proof. Stem field (Definition 2.1) K has to have degree n over $\mathbb{F}_p$ i.e. $[K : \mathbb{F}_p] = n$ (see remark 2.3) i.e. it should have p^n elements (see remark 3.5) and therefore $K = \mathbb{F}_{p^n}$ (see theorem 3.8).

About Splitting field (Definition 2.6). 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 3.11. *Let $\mathcal{P}_d$ is the set of all irreducible, Monic polynomial (Definition A.84)s of degree d such that $\mathcal{P}_d \subset \mathbb{F}_p[X]$ then*

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

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

[12] up to Isomorphism (Definition A.127)

[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 2.3 we have

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

From remark 3.5 $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Theorem 3.9 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 3.12. *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 3.13. *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 3.12 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 3.9 and proof at the theorem 3.10)

[15] As soon as $\mathbb{F}_p[X]$ is Unique factorization domain (Definition A.91) 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 (Lemma A.83) one can get that $\exists Q, R \in \mathbb{F}_p[X]$ such that $P_1 Q + P_2 R = 1$ 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 3.14. *Let K be a field and and G be a finite Subgroup (Definition A.10) of $K^\times$ (see definition A.65) then G is a Cyclic group (Definition A.23)* [18]

Proof. Idea is to compare G and the Cyclic group (Definition A.23) $\mathbb{Z}/N\mathbb{Z}$ where $N = |G|$. [19]

Let $\psi(d)$ - is the number of elements of order d (see also Order of element in group (Definition A.7)) in G. We need $\psi(N) \neq 0$ [20] 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 (Definition A.7)) in $\mathbb{Z}/N\mathbb{Z}$. [21] As $\mathbb{Z}/N\mathbb{Z}$ contains a single (cyclic) subgroup of order d for each $d \mid N$. [22] $\phi(d)$ 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 $\psi(d) = \phi(d)$ [23] 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

[18] Not every finite group is cyclic. For instance the non-abelian group S_3 (see example A.54) consists of 6 elements but it is not cyclic.

If we want to have a cyclic group it should be Abelian group (Definition A.38) in the case it can be represented in the form of a cyclic group or a direct sum of cyclic groups accordingly The fundamental theorem of finitely generated abelian groups (Theorem A.45). Another important requirement is that the orders of the cyclic group have to be coprime.

For example there are 2 groups of order 4: the cyclic one - $\mathbb{Z}/4\mathbb{Z}$ and V_4 - Klein four group V_4 [61]. $V_4 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is non-cyclic because the orders are not coprime: $gcd(2,2) = 2 \neq 1$.

(From the staff) But a product of two cyclic groups is again cyclic, if their orders are coprime. For example, consider the element $(1,1) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It's order is 6, so it generates the whole group. Thus as it's mentioned $\mathbb{Z}/N\mathbb{Z}$ is a cyclic group.

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

[20] 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.

[21] The function $\phi(d)$ is also called as Euler's totient function (Definition A.135) and it counts the positive integers up to a given integer d that are relatively prime to d

[22] 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.

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

a cyclic subgroup of G (by Cyclic group (Definition A.23) 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. [24]

If $\psi(d) \neq 0$ then exists such a subgroup and $\psi(d)$ is equal to the number of generators of that group or $\phi(d)$ [25] In particular $\psi(d) \leq \phi(d)$ [26] 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. □

Corollary 3.15. *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 (Definition A.85) of degree n over $\mathbb{F}_p$* [27]

Proof. We can take $\alpha =$ generator of $K^\times$ [28] □

Corollary 3.16. *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 3.6 where we showed that the Frobenius map is a field automorphism)*

Proof. As we know from theorem 3.8: $\forall x \in \mathbb{F}_{p^n} : x^{p^n} = x$ so [29] $F_p^n = id$. 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 [30] F_p^m cannot be identity. Finally (from corollary 3.15) we have $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ where α is a

[24] 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.

[25] 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.

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

[27] The theorem 3.10 and remark 3.5 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.

[28] This is because from theorem 3.14 $K^\times = \langle \alpha \rangle$ 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 (Definition 1.11) because we can consider $1, \alpha, \ldots, \alpha^{n-1}$ 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 1.12 there exists an irreducible polynomial $P_{min}(\alpha, \mathbb{F}_p)$.

[29] because

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

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

root of an irreducible polynomial of degree n. I.e. there cannot be more than n automorphism [31] so

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

and as we have n of them (Automorphism (Definition A.129)s) [32] then

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

and the group is cyclic generated by F_p. □

3.4 Separable elements

Let E is a Splitting field (Definition 2.6) of an irreducible polynomial P. We would like to say that it "has many Automorphism (Definition A.129)s". What does this mean? This means the following thing: Let α and β be 2 roots of P then we have 2 extensions $K\left(\alpha\right) \subset E$ and $K\left(\beta\right) \subset E$.

There exists an Isomorphism (Definition A.127) (see proposition 2.2) over K

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

that is also extended to an Automorphism (Definition A.129) on E (see theorem A.132).

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 $charK = 0$, but not always if $charK = p$ (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 $charK = 0$ - it is because $\deg P' < \deg P$ and $P \nmid P'$ for $P' \neq 0$ (non constant polynomial) [33]

But for $charK = p$ 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 [34]

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

[32] 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.

[33] 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 1.12 (or theorem A.87) one can get that $P \mid P'$ in $K\left[X\right]$ but that is impossible because $\deg P' < \deg P$ and can be only possible if $P' = 0$.

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

Example 3.17. *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 $h = 3 > 2$ does not fit into the requirements: $p^h = 2^3 = 8 \nmid 12$.

Proposition 3.18. *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.*

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 [35] 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 $S\left(X^{p^r}\right)$. [36] Thus we just got that multiplicity of λ is p^r. □

Definition 3.19 (Separable polynomial)**.** $P \in K[X]$ irreducible polynomial is called separable if $\gcd(P, P') = 1$

Definition 3.20 (Degree of separability)**.** $d_{sep}(P) = \deg Q$ (as above) [37]

Definition 3.21 (Degree of inseparability)**.** $d_i(P) = \frac{\deg P}{\deg Q}$ ($= p^r$ in proposition 3.18)

Definition 3.22 (Pure inseparable polynomial)**.** P is pure inseparable if $d_i = \deg P$. Then $P = X^{p^r} - a$ [38]

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

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

[37] It requires some explanation compare to that one was got on the lecture video. If P is a Separable polynomial (Definition 3.19) 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 $d_{sep}(P) = \deg Q$.

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

Definition 3.23 (Separable element)**.** Let L be an Algebraic extension (Definition 1.17) of K then $\alpha \in L$ is called separable(inseparable) if it's Minimal polynomial (Definition 1.13) $P_{min}(\alpha, K)$ has the property. Note: the separable element is also Algebraic element (Definition 1.11) because it has minimal polynomial.

Proposition 3.24 (On number of homomorphisms)**.** *If α is separable on K then the number of Homomorphism (Definition A.126)s 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. □

3.5 Separable degree, separable extensions

We want to generalize the proposition 3.24 for any field extension (not necessary $K(\alpha)$). Let L be a finite extension of K

Definition 3.25 (Separable degree)**.** $[L:K]_{sep} = \left|Hom_K\left(L, \bar{K}\right)\right|$

As we know if $L = K(\alpha)$ then Separable degree (Definition 3.25) is a number of distinct roots of minimal polynomial $P_{min}(\alpha, K)$

Definition 3.26 (Separable extension)**.** L is separable over K if $[L:K]_{sep} = [L:K]$

Definition 3.27 (Inseparable degree)**.**

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

Theorem 3.28 (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 (Definition 3.26) 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 (Definition 3.23) over* K

(c) L *is generated over* K *by a finite number of Separable element (Definition 3.23)s 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 3.29. That holds if we replace separability with pure inseparability.

Proof. About 1st part: If we have a Homomorphism (Definition A.126) $\phi : L \to \bar{K}$ then it is extended to $\tilde{\phi} : M \to \bar{K}$ (by extension theorem 2.17) 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 (Definition 2.12) 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 [39]

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

With the inequality (3.1) we also have

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

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

About 2d part:

[39] The inequality can be proved by induction using the fact that it's true for $K(\alpha)$ because from general case of proposition 3.24

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

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

2a $\Rightarrow$ 2b: Part 1 implies that a separable sub extension $K(\alpha)$ or a separable extension L is separable. [40]

2b $\Rightarrow$ 2c: obvious [41]

2c $\Rightarrow$ 2d: We know that $P_{min}(\alpha_i, K(\alpha_1, \dots, \alpha_{i-1}))$ divides $P_{min}(\alpha_i, K)$. [42] 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 (Definition 3.23) over $K(\alpha_1, \dots, \alpha_{i-1})$

2d $\Rightarrow$ 2a: Induction as above [43] □

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

Definition 3.30 (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 [44] called separable closure of K over L

L is pure inseparable over L^{sep}.

Remark 3.31.

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

3.6 Perfect fields

Definition 3.32 (Perfect field)**.** Let K is a field and $charK = p > 0$. K is perfect if Frobenius homomorphism (Remark 3.6) is a Surjection (Definition A.123)

[40] 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 (Definition 3.23) because $P_{min}(\alpha, K)$ is separable.

[41] We consider finite extensions (see remark 3.5) i.e. which consists of finite number of elements

[42] 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 1.12).

[43] 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

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

Example 3.33. *1. Finite field is perfect because an Injection (Definition A.124) of a set into itself is always a Surjection (Definition A.123)*

2. Algebraically closed fields are perfect because $X^p - a$ has a root α for any a particularly $a = F_p(\alpha)$ [45]

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 3.34. *K is a Perfect field (Definition 3.32) if and only if all irreducible polynomial over K are separable or in other words all Algebraic extension (Definition 1.17)s of K are separable.*

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

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

but as soon as my field is perfect then I can extract p-root of a_i [46] 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 $r = 0$ [47] so irreducible means separable.

If K is not perfect but all irreducible polynomial are separable. K is not perfect means that $\exists a \notin Im(F_p)$ 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 $x^{p^r} = a$ [48] and of course $x^{p^{r-1}} \notin K$. [49]

About the polynomial is irreducible. We have already seen that in the case $[K(x) : K] = p^r$ so the polynomial is irreducible [50] and this finishes [51]

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

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

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

[48] 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

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

[50] Corollary 3.15 says that there exists an irreducible polynomial of degree p^r with x as the root. Theorem A.87 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.

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

the proof. □

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 (Definition 1.3) L i.e $[L:K]<\infty$. We also saw that if L is generated by a finite number of Separable element (Definition 3.23)s $\alpha_1,\ldots,\alpha_r$ then the number of Homomorphism (Definition A.126)s 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

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

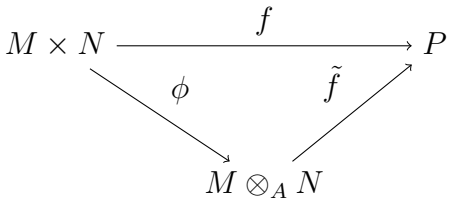
For $L=K(\alpha)$ it is clear because the number of homomorphisms is equal to the number of roots of the Minimal polynomial (Definition 1.13) $P_{min}(\alpha,K)$. In general one can use induction and multiplicativity of the degree $[L:K]$ and number of homomorphisms (see theorem About separable extensions (Remark 3.28)). 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-Module (Definition A.97)s. The tensor product $M \otimes_A N$ is another A-Module (Definition A.97) together with an A-bilinear map $\phi : M \times N \to M \otimes_A N$ which has "Universal property (Definition 4.2)" 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 (Definition A.97) 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 Homomorphism (Definition A.126)s of A-modules), then $\exists! \tilde{f}$ - homomorphism of A-modules such that $f = \tilde{f} \circ \phi$ [1]



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

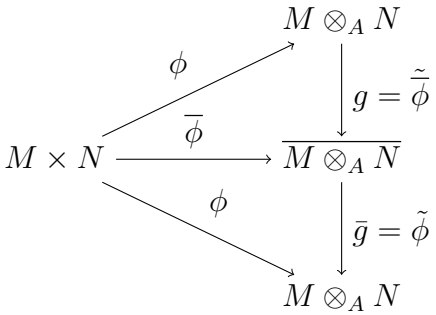
Lemma 4.3 (About uniqueness of object defined by universal property)**.** [2] *If we have two objects $(\phi, M \otimes N)$ and $\left(\overline{\phi}, \overline{M \otimes N}\right)$ which both satisfies Universal property (Definition 4.2) than there is an unique Isomorphism (Definition A.127) between 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

[1] That means that we have a Commutative diagram (Definition A.134) 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 and, 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. I.e. $\forall x \in M \times N$ we have $\bar{g}(g(\phi(x))) = \phi(x)$. If $y = \phi(x)$ then $\bar{g}(g(y)) = y$. The last equation holds $\forall y \in Im(\phi)$ i.e. $\forall y \in M \otimes_A N$. Therefore $\bar{g} = g^{-1}$. [3]

Thus we have an Isomorphism (Definition A.127) and the isomorphism is unique as soon as the function g is unique due the Universal property (Definition 4.2).

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 4.4 (About tensor product existence)**.** *Tensor product defined via Universal property (Definition 4.2) 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:

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

[3] Another explanation is the following: 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).

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 (Definition A.100) 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 $\delta_{m+m',n} - \delta_{m,n} - \delta_{m',n}$, $\delta_{m,n+n'} - \delta_{m,n} - \delta_{m,n'}$, $\delta_{am,n} - a\delta_{m,n}$, $\delta_{m,an} - a\delta_{m,n}$. [4]

It can be shown that $M \times N \to \mathcal{E}/\mathcal{F}$ is bilinear [5] and has the desired Universal property (Definition 4.2).

Really lets we have the following bilinear map: $f : M \times N \to P$. Then we can consider the following linear map (Homomorphism (Definition A.126)) $f' : \mathcal{E} \to P$ that sends $\delta_{m,n}$ to $f(n,m)$. Using the fact that f is bilinear we can get

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

With the same approach one can get the following relations

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

with the f' linearity we have

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

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. □

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

[5] Follows from the basis choice

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 4.5. 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 [6].

4.2 Tensor product of modules

4.2.1 Advantages of the universal property

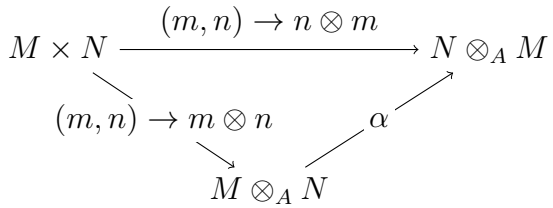
Now, you can ask why haven't I just defined the tensor product by this construction? Why am I talking of this universal property? And the answer is because it is easier to prove things this way. So advantages of the universal property is as follows: the proofs become easy.

4.2.2 Several examples of universal property usage

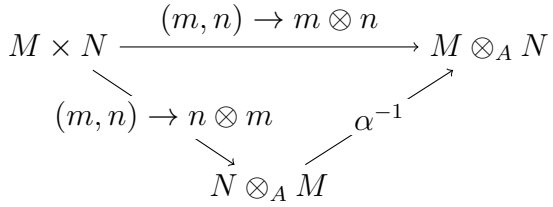
Example 4.6 (Commutativity proof)**.** *We want to prove that*

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

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 (Definition 4.2) we have that there is a linear map (homomorphism)* $\alpha : M \otimes_A N \to N \otimes_A M$*:*



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



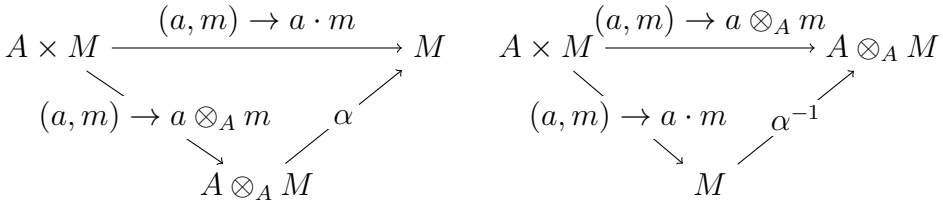
[6] i.e. $\exists x \in M \otimes_A N$ such that $\exists! m \in M, n \in N : x = m \otimes n$ but $\exists m_1, \ldots, m_k \in M, n_1, \ldots, n_k \in N : x = \sum_{i=1}^{k} m_i \otimes n_i$

Also

Corollary 4.7.

$$A \otimes_A M \cong M$$

Proof. For the proof [7] lets look at A. Really A can be considered as A-module because all requirements from definition A.97 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 $A \otimes_A M \cong M$:



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

□

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

More complex fact is the following

Proposition 4.8. *Let M and N are Free module (Definition A.100)s with corresponding basises $e_1, e_2, \ldots, e_n$ and $\epsilon_1, \epsilon_2, \ldots, \epsilon_m$ 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 [8] 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. [9] 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 $\forall i, j : \alpha_{ij} = 0$. [10] □

[7] The proof is missed in the lectures

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

[9] Because $f_{i_0,j_0} = \tilde{f}_{i_0,j_0} \phi$ i.e.

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

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

In particular for the Vector space (Definition A.107) the tensor product is defined in the same way (as just proved in the proposition 4.8): the tensor product of 2 vector spaces with basises $e_1, e_2, \ldots, e_n$ and $\epsilon_1, \epsilon_2, \ldots, \epsilon_m$ 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 (Definition 4.2).

Proposition 4.9 (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. □

4.3 Base change

Let A is a Ring (Definition A.63) and B is A-algebra. Let also M is an A-Module (Definition A.97) 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 $B \otimes_A M$ [11] . We can introduce B-module structure on $B \otimes_A M$ by [12]

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

Example 4.10 (The complexification of a real vector space)**.** *We can "make" $\mathbb{R}^{2n}$ from $\mathbb{C}^n$ by forgetting the complex structure.* [13] *The $\mathbb{C}^n$ has the following basis $e_1, \ldots, e_n$. The $\mathbb{R}^{2n}$ has the following one $e_1, \ldots, e_n, ie_1, \ldots, ie_n$. 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: $e_1, \ldots, e_n, v_1, \ldots, v_n$.*

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 $1_{\mathbb{C}} \otimes e_1, \ldots, 1_{\mathbb{C}} \otimes e_n$ and for $\mathbb{R}^{2n}$ - $1 \otimes e_1, \ldots, 1 \otimes e_n, i \otimes e_1, \ldots, i \otimes e_n$. [14]

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

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

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

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

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

Proposition 4.11. *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 $1_B \otimes e_1, \dots, 1_B \otimes e_n$.*

Proof. The proof is the same as at proposition 4.8. 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 $\tilde{f}_{i_0}$ (homomorphism) 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 4.12. 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 4.13 (Base-change)**.** *Let A is a Ring (Definition A.63) and B is A-algebra. Let also M is an A-Module (Definition A.97) and N is B-module.*

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

---

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: $c_i = a_i + i b_i$, 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 $1 \otimes e_1, \dots, 1 \otimes e_n, i \otimes e_1, \dots, i \otimes e_n$.

I.e. the homomorphisms [15] *are the same or in other words the corresponding groups of homomorphisms are isomorphic:*

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

Proof. First of all we have [16] Homomorphism (Definition A.126) $f : B \otimes_A M \to N$. We also have the following map (see remark 4.12): $\alpha : M \to B \otimes_A M$. 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 $\hat{f}(f) = f\alpha$.

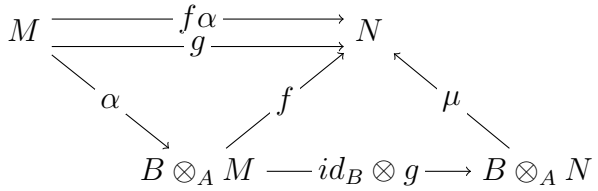
In other direction we have $g : M \to N$ thus $id_B \otimes g : B \otimes_A M \to B \otimes_A N$ but (see remark 4.12) we have $\mu : B \otimes_A N \to N$ i.e. we have the following relation

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

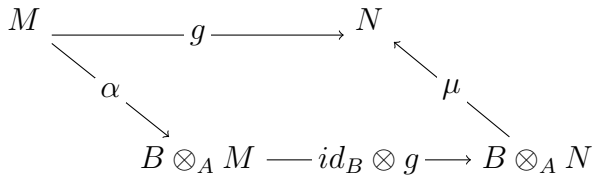
such that

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

And we can check that those maps ($\hat{f}$ and $\hat{g}$) are mutually inverse. For the proof [17] the fact consider the following diagram



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. $\hat{f} \circ \hat{g} = id$ [18] or in other words $\hat{f}$ and $\hat{g}$ are mutually inverse. □

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

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

[17] It's missed in the lectures

[18] 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 $x \in X$.

4.4 Examples. Tensor product of algebras

Proposition 4.14. *If $I \subset A$ - is an Ideal (Definition A.67) so my B - A algebra will be $B = A/I$ then*

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

where IM is a sub-module of M.

Proof. We have map $\alpha : M \to B \otimes_A M = A/I \otimes_A M$ (see remark 4.12) which sends m to $\bar{1} \otimes m$. [19] The map sends IM to 0 because $\forall i \in I, m \in M : im \to \bar{1} \otimes im = \bar{i} \otimes m$ because the tensor product is over A and everything is A linear and as result $\bar{1} \otimes im = \bar{i} \otimes m$, but $\bar{i} \otimes m = \bar{0} \otimes m = 0$. [20] 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 4.13) theorem. The following map (projection) of A-modules

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

gives us the following map of B-modules [21]

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

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 $\bar{\alpha}$. [22] □

Several examples:

Example 4.15. *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: $2^{-1} = -1 \mod 3$ [23] *thus $(2)\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$ and as result*

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

---

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

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

[21] the Base-change (Theorem 4.13) theorem says that homomorphism of A-modules $M \to N$ is isomorphic to homomorphism of B modules $B \otimes_A M \to N$. Using $N = M/IM$ we can get that $B \otimes_A M \to M/IM$ is isomorphic (i.e. the same) to $M \to M/IM$. We also can get the same result just ignore B: $B \otimes_A M \to M \to M/IM$.

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

[23] 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 $(2) \cdot \mathbb{F}_3 = \mathbb{F}_3$. I.e. (2) is not a Proper ideal (Definition A.79) in $\mathbb{F}_3$ because it is equal to $\mathbb{F}_3$.

Example 4.16. *Another obvious example* [24]

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

and more interesting one

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

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

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 [25]

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

The tensor product has the following

Definition 4.17 (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

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

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

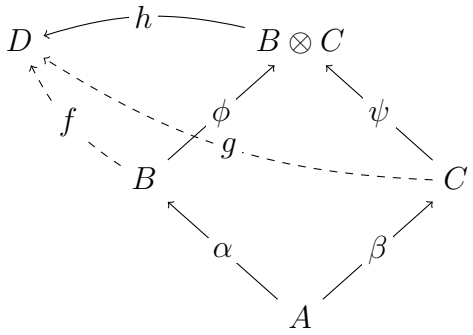
$$b = \sum b_i \cdot 1_B \otimes X^i$$

and there is an obvious isomorphism

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

[25] that makes it A-algebra (see K-algebra (Definition 1.1))

i.e. if I have some Homomorphism (Definition A.126) $h \in Hom_A(B \otimes_A C, D)$ 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 (Definition A.134)).



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:

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

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

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

therefore with result from example 4.16 one can get

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

but by Chinese remainder (Equation 4.20) 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

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

.

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 (Definition A.74) (see theorem A.88) and with the theorem A.92 the quotient by the polynomial is not a field (see also section 1.1.4).

4.5 Relatively prime ideals. Chinese remainder theorem

Definition 4.18 (Relatively prime ideals)**.** Let A - Ring (Definition A.63) and I, J are Ideal (Definition A.67)s. I and J are relatively prime if $I+J=A$.

Lemma 4.19. *1. If I, J are relatively prime then $IJ = I \cap J$*

2. *If $I_1, \ldots, I_k$ relatively prime with J then $\prod_{i=1}^{k} I_i = I_1 \ldots I_k$ 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 [26] 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 [27]

□

[26] 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. $x \in I \cap J$.

[27] 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.

Theorem 4.20 (Chinese remainder)**.** *Let $I_1, \dots, I_n$ - ideals and map $\pi : A \to A/I_1 \times \cdots \times A/I_n$ defined as follows*

$$\pi(a) = (a \mod I_1, \dots, a \mod I_n) \tag{4.2}$$

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

The π is Surjection (Definition A.123) if and only if $I_1, \dots, I_n$ are pairwise relatively prime.

In that case

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

[28]

Proof. Let π is Surjection (Definition A.123). In the case $\exists a_i \in A$ such that

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

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 4.19) $\prod_{j \neq i} I_j$. 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

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

and $\forall b_i \in A/I_i$

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

i.e. π is surjective. □

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

Proposition 4.21. *1. If A is an Integral domain (Definition A.72) then A is a field.*

[28] See First isomorphism (Theorem A.131) theorem where $G = A$, $H = A/I_1 \times \cdots \times A/I_n$, $\phi = \pi$ and with lemma 4.19 (as soon as I_k pairwise relatively prime)

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

2. *(replacing the first one) Any Prime ideal (Definition A.76) of A is a Maximal ideal (Definition A.74)*

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. [29] If you don't know this, please look it up in any book.

Lets prove the first part. Integral domain (Definition A.72) means that there is no zero divisors i.e. $\forall a \in A$ [30] multiplication by a is Injection (Definition A.124). A is finite dimensional Vector space (Definition A.107) (see above) that implies that $\times a$ is an Isomorphism (Definition A.127), [31] in particular Surjection (Definition A.123) i.e. $\exists b \in A$ such that $b \times a = 1$ i.e. a is invertible therefore A is field. □

4.6 Structure of finite algebras over a field. Examples

Remark 4.22. 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 1.5 says that there is a ring homomorphism between K and A: $f_K : K \to A$. There is also a canonical homomorphism $f_A : A \xrightarrow[a \to \bar{a}]{} A/m$. Therefore we can define $f = f_A f_K : K \to A/m$ and therefore with lemma1.5 can conclude that A/m is a K-algebra. [32]

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

Theorem 4.23 (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 ideal (Definition A.74)s $m_1, \ldots, m_r$ in A*

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

[30] $a \neq 0_A$

[31] $\times a$ sends a vector space into another vector space with the same dimension. But with lemma About vector space isomorphism (Lemma A.108) one can get that the spaces are isomorphic each others and as result the operation $\times a$ is an Isomorphism (Definition A.127).

[32] Thanks Zonglin Jiang for the proof.

2. *Let* $J = m_1 \cap \cdots \cap m_r = m_1 \dots m_r$. [33] *Then* $J^n = 0$ *for some* n

3. $A \cong A/m_1^{n_1} \times \cdots \times A/m_r^{n_r}$ *for some* $n_1, \dots, n_r$.

Proof. 1. Let $m_1, \dots, m_i$ are maximal ideals. By Chinese remainder (Equation 4.20) theorem we have [34]

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

We know that A as well as $A/m_1 \dots m_i$ and A/m_k are finite dimensional K-Vector space (Definition A.107) [35] 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.

2. $J = m_1 \cap \cdots \cap m_r = m_1 \dots m_r$ is finite dimensional vector space over K [36] as well as its powers J^k. We have the following sequence [37]

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

and the sequence should stop somewhere [38] 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.

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

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

[34] Maximal ideals are relatively prime because in a commutative ring with unity, every Maximal ideal (Definition A.74) is a Prime ideal (Definition A.76) see also proposition 4.21.

[35] See remark 4.22 and take into consideration the theorem statement (see above) that says $\dim_K A < \infty$. A/m_1 is a projection i.e. $\dim_K A/m_1 < \dim_K A < \infty$.

[36] We have $m_i \subset A$ i.e. $\dim_K m_i \leq \dim_K A < \infty$. From other side $J = m_1 \dots m_r = (m_1 \cap \cdots \cap m_r) \subset m_i, \forall i \in \{1, \dots, r\}$. Thus $\dim_K J \leq \dim_K m_i \leq \dim_K A < \infty \leq$

[37] 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 $J^2 \subseteq J$.

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

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 to find a matrix $\tilde{M}$ such that $\tilde{M}M = \det M \cdot id$, [39] i.e.

$$\det M \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_s \end{pmatrix} = 0. \tag{4.3}$$

But $\det M = 1 + \lambda$ where $\lambda \in J$. [40] Since $J = m_1 \cap \cdots \cap m_r$ then $\forall i : \lambda \in m_i$ so $\nexists i$ such that $1 + \lambda \in m_i$ [41] thus $1 + \lambda$ is invertable [42] therefore $e_1 = \cdots = e_s = 0$ [43]

3. Using part 2 $\exists n_1, \ldots, n_r$ such that $m_1^{n_1} \ldots m_r^{n_r} = 0$ (for example we can assume $n_i = n$). Then by Chinese remainder (Equation 4.20) theorem

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

We used the following facts:

- $A = A/m_1^{n_1} \ldots m_r^{n_r}$ [44]
- $m_i^{n_i}$ are pairwise relatively prime [45]

[39] If M is a matrix over a field we can consider the following 2 cases:

(a) $\det M = 0$: we can assume that $\tilde{M} = 0$

(b) $\det M \neq 0$: at the case $\exists M^{-1}$ and therefore $\tilde{M} = \det M \cdot M^{-1}$ will work.

For more common case we have to look at Adjugate matrix [56]

[40] 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. $\det M = 1 + \sum \prod \lambda_{ij} = 1 + \lambda$.

[41] We have that m_i is a Maximal ideal (Definition A.74) and therefore (by its definition) it is a Proper ideal (Definition A.79) 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.

[42] $0 \in m_i$ thus if $1 + \lambda \notin m_i$ then $1 + \lambda \neq 0$.

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

[44] 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 (Definition A.81))

[45] As soon as $\{m_i\}$ - Maximal ideal (Definition A.74)s and as result Prime ideal (Definition A.76)s then with lemma 4.19 one can get that $\forall i \neq j$ $m_i^{n_i}$ is relatively prime with $m_j^{n_j}$.

□

Remark 4.24. The n_is are not uniquely defined. For example (see also example 5.1)

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

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 $(X)^3 \subset (X)^2$ [46]

Several examples:

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

Another example

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

And you see that those algebras are Cartesian products of fields. So all n_i's may be taken equal to 1 [47]. In other words, we don't have Nilpotent element (Definition 5.2)s in our algebra [48]. 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.

[46] $(X)^3 \subset (X)^2$ - 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 $\bar{P}(X) = XP'(X)$

$(X)^2 \subset (X)^3$ 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. $P(X) \in (X)^3$.

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

[48] Cartesian products of fields has no nilpotent elements except 0 [13].

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 $m_1, \ldots, m_r$ and the following equation holds (see theorem 4.23):

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

This is a general form of Chinese remainder (Equation 4.20) theorem.

Example 5.1. *Let*

$$A = K[X]/(F)$$

And the polynomial F is not necessary irreducible so let's decompose into a product of irreducible factors: $F = P_1^{k_1} \ldots P_r^{k_r}$. Then by the Chinese remainder (Equation 4.20) theorem [1] *one can get*

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

[1] See also remark 4.24 and theorem 4.23

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

Definition 5.2 (Nilpotent element)**.** Let A is a Ring (Definition A.63) than $x \in A$ is nilpotent if $x \neq 0$ but $\exists k : x^k = 0$. [3]

Definition 5.3 (reduced)**.** K-algebra A is reduced if it has no Nilpotent element (Definition 5.2)s. 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 5.4 (local)**.** Ring (Definition A.63) A is called local if it has only one Maximal ideal (Definition A.74) 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.81 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 (Definition A.74) 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 [46]: 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 (Definition A.74)

[6] As it was mentioned in [43], 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 (Definition A.89) and $\{0\}$ is the only maximal ideal for the fields (see example A.75). 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 3.27) 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 Homomorphism (Definition A.126)s $\left|Hom_K\left(L, \bar{K}\right)\right|$ 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 (Theorem 4.13). 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 3.33 (part 3) it's not a Perfect field (Definition 3.32) and as result of theorem 3.34 is not separable.

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

Remark 5.5. 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 4.11 we have that $[A : E] < \infty$ (as soon as $[L : K] < \infty$) and as result with theorem 4.23 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 5.6. With Chinese remainder (Equation 4.20) 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 (Definition A.67) 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 4.22). We also have

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

but $Hom\left(A/m_i, E\right) = \{0\}$ 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 5.9)?

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

$$A_{red} = \prod_{i=1}^{r} \bar{K}. \tag{5.2}$$

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 4.22) i.e. also E-extension.

From other hand we consider $Hom\left(A/m_i, E\right)$ 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 4.16)

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

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

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

Theorem 5.7. *Let L is a finite extension over K then*

1. *L is separable if and only if $L \otimes_K \bar{K}$ is reduced (Definition 5.3). L is pure inseparable if and only if $L \otimes_K \bar{K}$ is local (Definition 5.4)*
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 (Definition 5.3) 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 (Definition 5.4).

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 3.28) 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 1.9) thus with theorem 4.23 and (5.1) we have

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

[15] From (5.2), if $A = A_{red}$, one can get $\dim_{\bar{K}} A = \dim_{\bar{K}} A_{red} = \dim_{\bar{K}} \prod_{i=1}^{r} \bar{K} = r = [L : K]$.

[16] i.e. we can setup an Injection (Definition A.124) and structure preserving map $f : L \otimes_K \Omega \to L \otimes_K \bar{\Omega}$ (see definition A.130)

3. Leave as an excises [17]

□

Remark 5.8. 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 space (Definition A.107)s. 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 5.9. *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*

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

[17] Accordingly [10] we have the following proof. Let $l_1, l_2, \ldots, l_n$ is a K basis in L. Then we can get the following elements of $\bar{K}^n$: $v_i = (\phi_1(l_i), \phi_2(l_i), \ldots, \phi_n(l_i))$. We can construct the following matrix if we put the v_i vectors as columns:

$$\begin{bmatrix} \phi_1(l_1) & \phi_1(l_2) & \cdots & \phi_1(l_n) \\ \phi_2(l_1) & \phi_2(l_2) & \cdots & \phi_2(l_n) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_n(l_1) & \phi_n(l_2) & \cdots & \phi_n(l_n) \end{bmatrix}$$

Linear dependence relation between rows looks like

$$\sum_{k=1} c_k \phi_k(l_i) = 0. \tag{5.3}$$

Thus $\forall l \in L^*, \exists \{k_i\} \subset K : l = \sum_{i=1}^{n} k_i l_i$ (as soon as $\{l_i\}$ is the K basis of L). Thus after multiplication (5.3) by k_i and summation we have

$$\sum_{i=1} k_i \sum_{k=1} c_k \phi_k(l_i) = \sum_{k=1} c_k \phi_k(l) = 0$$

that should hold for any k_i and as result for any l. By theorem A.96 we can conclude that $\forall k : c_k = 0$. As result we have the set $\{v_i\}$ as linear independent. The size of the set is $n = \dim \bar{K}^n$ i.e. $\{v_i\}$ is the $\bar{K}$ basis of $\bar{K}^n$.

We used the following fact (see example 1.9)

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

5.3 Primitive element theorem

Definition 5.10 (Idempotent)**.** The element x is called idempotent if $x \cdot x = x$

Theorem 5.11 (Primitive element)**.** *Let L is a finite Separable extension (Definition 3.26) 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] : $E \otimes_K \bar{K} \hookrightarrow L \otimes_K \bar{K}$ [19]. We also have (see also equation (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 Idempotent (Definition 5.10)s namely by

$$e_i = (0, 0, \ldots, 1, \ldots, 0),$$

where 1 is in i-th place [20].

On the other hand $L \otimes_K \bar{K} \cong \bar{K}^n$ has only finitely many Idempotent (Definition 5.10)s because $(a_1, \ldots, a_i, \ldots, a_n)$ 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, [21] so there is only finitely many ways to generate a subalgebra. □

[18] see proof of theorem 5.7 (second part of it).
[19] See also proof of theorem 5.7.
[20] this is because the typical element $k \in \bar{K}^n$ has the following form

$$k = (k_1, k_2, \ldots, k_n) = \sum_{i=1}^{n} k_i e_i,$$

where $k_i \in \bar{K}$.
[21] we have the following equation

$$\bar{K}^m \hookrightarrow \bar{K}^n$$

Corollary 5.12 (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. [22]

If L and K are Finite field (Definition 3.4)s, then we have already described this situation completely. We have described all finite extensions and have seen that they are generated by one element. [23] □

5.4 Examples. Normal extensions

5.4.1 Examples

Example 5.13 (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. [24] *As no quadratic polynomial has $\alpha = \sqrt{2}+\sqrt{3}$ for a root* [25]*, α generates $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$.*

[22] 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 5.11 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 1.27)

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

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. $L = K(\gamma) = K(\alpha, \beta)$.

[23] As it was mentioned in the proof of corollary 3.15 we can take $\alpha =$ generator of $K^\times$. For more info see corollary 3.15.

[24] 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.

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

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

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

Example 5.14 (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 [26] *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* $\alpha^p \in K(x^p, y^p)$ [27] *. So, no element like these can generate our extension.*

[26] $K \subset K(x^p) \subset K(x^p, y^p)$ and $[K(x^p) : K] = p$ as well as $[K(x^p, y^p) : K(x^p)]$ thus with theorem 1.22

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

[27] $\alpha = k_1 x + k_2 y$, where $k_1, k_2 \in K = \mathbb{F}_p$. Using remark 3.6 we can get

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

5.4.2 Normal extensions

Definition 5.15 (Normal extension)**.** A normal extension of K is a Splitting field (Definition 2.6) of a family of polynomials [28] in $K[X]$. [29]

Remark 5.16 (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 (Definition 2.6) of one polynomial is also a normal extension.

Theorem 5.17. *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 (Definition 5.15)*
3. *All Homomorphism (Definition A.126)s from* L *to* $\bar{K}$ *have the same image.* [30]
4. *The Group (Definition A.5) of Automorphism (Definition A.129)s* $Aut(L/K)$ *acts transitively (see definition A.31) on this set of homomorphisms* $Hom_K(L, \bar{K})$.

[28] 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 arbitrary polynomial (for example X^3-1) can have a root in $\mathbb{Q}$ but does not necessary split in it.

[29] Another good definition of a normal extension [18] 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.

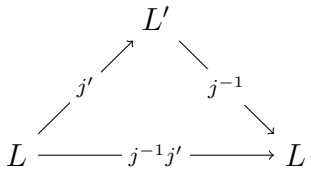
[30] And the image is L because id is also a Homomorphism (Definition A.126) ??? There are 2 staff's comments about the claim:

- You can't naturally identify L with a particular subfield of $\overline{K}$ (unless L is given as a subfield of $\overline{K}$ a priori). But from the lecture 2.5 we know, that there exists an embedding $L \hookrightarrow \overline{K}$ since L is algebraic over K. And the theorem says that images of all such embeddings are equal if L is normal over K.
- My previous answer was a little bit misleading. I meant, if you have an arbitrary algebraic extension of K, there is no canonical embedding into $\overline{K}$. Consider, for example, a field $\mathbb{Q}/(x^3-2)$. It has several embeddings into $\overline{\mathbb{Q}}$, namely, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$ and $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$. But if we consider the splitting field of x^3-2, then it's image in $\overline{\mathbb{Q}}$ is $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. So, yes, if we identify roots of polynomials which define L with some elements of $\overline{K}$ (up to a permutation for each polynomial), then the image is L itself.

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 5.15) L is normal.

2 implies 3: Let $S = \{\text{roots of } P_i, i \in I \text{ in } L\}$ and $S' = \left\{\text{roots of } P_i, i \in I \text{ in } \bar{K}\right\}$ [31] then any homomorphism $\phi : L \to \bar{K}$ sends S to S', but S generates L over K, so $\phi(S)$ determines $\phi(L)$ [32] .

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



take $j^{-1} \cdot j' \in Aut(L/K)$ and it sends j to j' [33].

4 implies 1: I have this Transitive group action (Definition A.31) 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 (Theorem 2.17). $\exists \theta_i \in Aut(L/K)$ such that $j_1\theta_i = j_i$ [34] thus $\alpha_i \in j_1(L)$ [35] 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 [36] □

5.5 Galois extensions

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

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

[32] 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. Or more concrete, let $l \in L, S = \{s_i\}, S' = \{s'_i\}$. We have $l = \sum l_{ik} s_i^k$ where $l_{ik} \in K$. For the homomorphism ϕ we have $\phi(l) = \sum l_{ik} s_i'^k$ i.e. the image $\phi(L)$ consists of elements of the following form: $\sum l_{ik} s_i'^k$. For any homomorphism we will have the same form for the image or in other words - any homomorphism has the same image.

[33] 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

$$g(j) \equiv jg = jj^{-1}j' = j'. \tag{5.4}$$

Therefore group automorphisms acts transitively by the definition A.31

[34] as it was mentioned at the equation (5.4)

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

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

Definition 5.18 (Galois extension)**.** A Galois extension is a Normal extension (Definition 5.15) and Separable extension (Definition 3.26).

Theorem 5.19. *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 (Definition 5.18).

Proof. We know that the group of automorphisms $Aut(L/K)$ acts freely (see definition A.32) on the set $Hom_K\left(L, \bar{K}\right)$, [37] so the number of automorphisms $|Aut(L/K)|$ is equal to the number of Orbit (Definition A.27) of this action which is less or equal [38] 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 (Definition A.26) is Transitive group action (Definition A.31). [39] We just seen in theorem 5.17 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 [40], 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 5.18). □

Definition 5.20 (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 5.21 (on normal extensions). If L is normal over K then

[37] Note that the number of distinct roots is equal to the number of distinct homomorphisms (see proposition 3.24). Thus we can set an association between roots and homomorphisms. Proposition 2.2 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 (Definition A.32).
See also first and second remarks at 5.21.

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

[39] This follows directly from the definition of Transitive group action (Definition A.31) i.e. $\forall h_1, h_2 \in Hom_K\left(L, \bar{K}\right)\ \exists a \in Aut(L/K)$ such that $a(h_1) = h_2$.

[40] see definitions 3.25 and 3.26.

1. If we have an Isomorphism (Definition A.127) of sub-extensions ($K \subset L_1, L_2 \subset L$) $\phi : L_1 \cong L_2$ then it extends to an Automorphism (Definition A.129) 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 $\bar{K}$, [41] but all those maps have the same image (see theorem 5.17), namely L [42].

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 [43].

3. If the group $Aut(L/K)$ fixes (see definition A.28) some element $x \notin K$ then x is pure inseparable (see definitions 3.22 and 3.23) i.e. $P_{min}(x, K)$ has a single root x. Thus if L is Galois extension (Definition 5.18) (i.e. is separable) then the set of elements which are fixed by the automorphisms of L over K is just K itself: $L^{Aut(L/K)} = K$ (see definition 5.20). [44]

Definition 5.22 (Galois group)**.** If L is Galois extension (Definition 5.18) then Galois group $G = Gal(L/K)$ is the group of automorphisms $Aut(L/K)$.

Thus we can write

$$L^{Gal(L/K)} = K. \tag{5.5}$$

5.6 Artin's theorem

Motivated by (5.5) let formulate and proof the important theorem

[41] Ekaterina really said that but may be more better to say that ϕ extends to a map from L to $\bar{K}$???

[42] Consider $L_1 \subset L_2 \subset L \subset \bar{K}$ we have a homomorphism $\phi_1 : L_1 \to L_2$ (our isomorphism) that accordingly theorem 2.17, can be extended to homomorphism $L_1 \to \bar{K}$ and the last one can be extended to $\tilde{\phi_1} : L \to \bar{K}$. We can also consider $L_2 \subset L_1 \subset L \subset \bar{K}$ and homomorphism $\phi_2 : L_2 \to L_1$ that can extended (using the same approach) to $\tilde{\phi_2} : L \to \bar{K}$. Both $\tilde{\phi_{1,2}}$ has the same image L as soon as L - normal extension (see theorem 5.17). Thus we have an Automorphism (Definition A.129).

[43] In the case we have Transitive group action (Definition A.31) i.e. for any roots x, y we have an isomorphism of stem fields ϕ such that $\phi(x) = y$ (see proposition 2.2). This isomorphism extends to an automorphism accordingly the prev. remark.

[44] 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.

Theorem 5.23 (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 (Definition 5.18) of L^G.*
2. *If $|G| = n < \infty$ then $\left[L : L^G\right] = n$ and G is a Galois group (Definition 5.22)*

Remark 5.24. 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 $L = \overline{\mathbb{F}_p}$. 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 is infinite. [45]

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 (Definition A.27) of x $Orb(x) = \{x_1, x_2, \ldots, x_k\}$. The polynomial $P(X) = \prod_{i=1}^{k}(X - x_i)$ is G-invariant [46] . 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 5.20. 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 (Definition 5.18) over L^G by the Galois extension (Definition 5.18) definition.
2. We have $|G| = n$ then $\forall y \in L : |Orb(y)| \leq n$. Take x as above ($x \in L \setminus L^G$) $\left[L^G(x) : L^G\right] \leq n$. [47] 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 5.11)

[45] Section 6.4.2 shows that $Gal\left(\bar{\mathbb{F}}_p/\mathbb{F}_p\right)$ is not cyclic, but theorem 3.14 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

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

[47] x is a root of the following polynomial $P(X) = \prod_{i=1}^{k}(X - x_i)$, where $x_i \in Orb(x)$. The polynomial has degree $\deg P = |Orb(x)| \leq n$ and $\deg P_{min}\left(x, L^G\right) \leq \deg P \leq n$ therefore $\left[L^G(x) : L^G\right] \leq n$.

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 [48] and I can apply Primitive element (Theorem 5.11) 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 $G = Aut\left(L/L^G\right)$ (see theorem 5.19).

□

[48] because x, y are algebraic elements and using theorem 1.24 and proposition 1.16 we can conclude that $L^G(x,y)$ is finite over L.

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 (Definition 5.18) if and only if it is a Separable extension (Definition 3.26) and Normal extension (Definition 5.15) or in other words L is a Splitting field (Definition 2.6) of a family of separable irreducible polynomials over K. We also seen (see theorem 5.19) 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 extension (Definition 5.15)s 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 6.2).

Example 6.2. *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 (Definition 2.1) (not Splitting field (Definition 2.6)) for this polynomial. And as result* $\mathbb{Q}\left(\sqrt[4]{2}\right)$ *is not a normal over* $\mathbb{Q}$.

Remark 6.3. 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 6.4. 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 6.5).

Example 6.5. *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 5.20):

Definition 6.6 (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 (5.5)) 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 5.21).

We also have seen (see theorem 5.23) that if G is finite the L is Galois extension (Definition 5.18) 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 (Definition 5.18). By definition the group automorphisms $Aut\left(L/K\right)$ is called Galois group (Definition 5.22) and denoted as $Gal\left(L/K\right)$

Theorem 6.7 (Galois correspondence). *1. If L is finite over K then there is a Bijection (Definition A.125) between a sub-extension F ($K \subset F \subset L$) and a subgroup $H \subset Gal\left(L/K\right)$. The correspondence is the following*

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

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

(a) F is Galois over K

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

(c) $Gal\left(L/F\right)$ is a Normal subgroup (Definition A.13) in $Gal\left(L/K\right)$

In this case g goes to g restricted to F: $g \to g|_F$ this is a Surjection (Definition A.123) $Gal\left(L/K\right) \twoheadrightarrow Gal\left(F/K\right)$ and the kernel is $Gal\left(L/F\right)$. [3]

Proof. 1. Most work have been done before. What have we got by now? $L^{Gal(L/F)} = F$ (see (5.5)). We also have $H \subset Gal\left(L/L^H\right)$. [4] Artin (Theorem 5.23) theorem gives us $\left[L : L^H\right] = |H|$ but with theorem 5.19 we also have $\left[L : L^H\right] = \left|Gal\left(L/L^H\right)\right|$ so one must have $H =$

[3] The fact is explained at the end of the proof of the theorem and is used in the claim 8.16 validation.

[4] Ekaterina called the fact obvious but let try to explain it. From (5.5) we have $L^{Gal\left(L/L^H\right)} = L^H$ thus $\forall h \in H$ it should also satisfy $h \in Gal\left(L/L^H\right)$ therefore $H \subset Gal\left(L/L^H\right)$.

$Gal\left(L/L^H\right)$ as soon as the subset H has the same cardinality as the set $Gal\left(L/L^H\right)$ itself.

This means that the maps that we have in the theorem : $F \to Gal\left(L/F\right)$ and $L^H \leftarrow H$ are mutually inverse [5] and if a map is invertible then there is a Bijection (Definition A.125).

2. We should proof equivalence of the following statements:

   (a) F is Galois over K

   (b) $\forall g \in Gal\left(L/K\right), g\left(F\right) = F$ [6]

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

Lets show that 2a implies 2b. Fix $x \in F$ then 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 a Normal extension (Definition 5.15), $P_{min}\left(x, K\right)$ splits in F (see theorem 5.17). 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. [7]

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 on roots of an irreducible polynomial [8] therefore F is normal by definition. [9]

Lets show that 2a and 2b are equivalent to 2c i.e. let $g \in G$, $g\left(F\right) \subset L$

[5] We have the following maps:

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

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 5.23) $K \subset L^H \subset L$.

[6] $g \in Gal\left(L/K\right)$ operates on $L \supset F$.

[7] We have the following fact: $x \in F$ then also $g(x) \in F$ i.e. $g(F) \subset F$. For equality $g\left(F\right) = F$ we have to proof that $\forall g \in Gal\left(L/K\right) : F \subset g\left(F\right)$. Really let $g \in Gal\left(L/K\right)$ then $g^{-1} \in Gal\left(L/K\right)$ and $g^{-1}(F) \subset F$ therefore $F = id(F) = g\left(g^{-1}(F)\right) \subset g(F)$ i.e. $F \subset g(F)$.

[8] see also 2d remark 5.21 that says that if F is normal then $Gal(L/F)$ acts transitively on the roots of any irreducible polynomial $P \in F\left[X\right]$.

[9] More clear explanation is below. We have to prove that F is normal and separable. Normality: $\forall P_{min}\left(x, K\right)$ splits in F thus the theorem 5.17 gives us the required normality. About separability. We have $K \subset F \subset L$. L is separable over K as soon as L is Galois extension. Thus theorem 3.28 gives us F separability.

then if $h \in Gal(L/F)$ is such that $h|_F = id$ then $ghg^{-1}|_{g(F)} = id$. [10] This means that $ghg^{-1} \in Gal(L/g(F))$ (see (5.5)) so the statement $g(F) = F$ is the same to say

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

So apply this to all $g \in Gal(L/K)$ one can get that $Gal(L/F)$ is a Normal subgroup (Definition A.13) of $Gal(L/K)$ by the definition of Normal subgroup (Definition A.13).

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

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

This is a Surjection (Definition A.123) by theorem 2.17 [11] and the kernel $\ker\phi = Gal(L/F)$ by definition because the kernel consists of things which are identity on F. □

Remark 6.8. If L over K is not finite then Galois correspondence is not Bijection (Definition A.125) 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 about it).

6.3 First examples (polynomials of degree 2 and 3)

Example 6.9 (Degree 2)**.** *Let* $[L : K] = 2$ *and* $charK \neq 2$*. 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*:* $L = K\left(\sqrt{\Delta}\right)$.

[10] The map g^{-1} acts as follows $g^{-1} : g(F) \to F$ i.e. h in $ghg^{-1}|_{g(F)}$ operates on F only therefore

$$ghg^{-1}|_{g(F)} = gh_Fg^{-1}|_{g(F)} = gg^{-1}|_{g(F)} = id$$

[11] We have that $\forall g_F \in Gal(L/F)$ g_F is a homomorphism that operates as follows $g_F : F \to \bar{K}$ (note that by the theorem 5.17 all homomorphisms on a normal extension F have the same image namely F) and therefore it can be extended (by theorem 2.17) to homomorphism $g : L \to \bar{K}$ i.e. $\forall g_F \in Gal(L/F), \exists g \in Gal(L/K)$ such that $\phi(g) = g_F$. Or in other words ϕ is a Surjection (Definition A.123).

What can we say about the $Gal\,(L/K)$*. It consists of 2 elements and there is only one cyclic group of 2 elements* [12] *:* $\mathbb{Z}/2\mathbb{Z}$*. 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 6.10 (Degree 3)**.** *Let* $[L:K] = 3$ *and* $charK \neq 3$ *(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 extension and $Gal\,(L/K)$ is the Galois group but the Galois group of 3 elements must be cyclic* [13] *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 extension 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 $[M:K] = |S_3| = 6$

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 (Definition 6.11) of polynomial which is a subject of next section (see example 6.13 and proposition 6.12).*

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

6.4.1 Discriminant

Definition 6.11 (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 discriminant:

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

[12] There is only one group of 2 elements [60]
[13] There is only one group of 3 elements and it is cyclic [60].

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 (5.5)).

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 only by even [14] (and not by odd) permutations.

Proposition 6.12. *Let $G = Gal(P)$ - Galois group (Definition 5.22) then $G \subset A_n$ [15] 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. □

If we return to our example 6.10 we can get the following one

Example 6.13 (Discriminant of polynomial degree 3)**.** *Lets compute the discriminant for the following polynomial: $X^3 + pX + q$.* [16]

The discriminant easy to compute: [17] $\Delta = -4p^3 - 27q^2$. *So if Δ is a*

[14] You can see from definition A.48 and example A.49 that for even permutations each insertion is equivalent to a root exchange. If the number of such exchange is even then we can return the changed root of a discriminant to its original form with event steps. Each step changes the sign and as result the even steps will not change the sign.

[15] A_n is a group of even permutations

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

[17] The below explanation was taken from [63]. The discriminant is a polynomial of degree 6. p can be represented as a polynomial of degree 2. $q = -X^3 - pX$ is a polynomial of degree 3. The discriminant therefore can be represented as follows $\Delta = ap^3 + bq^2$ where a, b are numbers. Let $p = -1, q = 0$ then the polynomial $X^3 - X$ has 3 roots: $-1, 0, 1$. It is easy to compute discriminant $\Delta = (0+1)^2(0-1)^2(1+1)^2 = 4$ therefore $a = -4$. For the case $p = 0, q = -1$ we will get the polynomial $X^3 - 1$ with roots $1, \zeta, \zeta^2$. We also have

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

therefore

$$(\zeta - 1)^2 = \zeta^2 - 2\zeta + 1 = -3\zeta$$

and

$$(\zeta + 1)^2 = \zeta^2 + 2\zeta + 1 = \zeta$$

square in K then $Gal(P) \cong A_3$ (cyclic of order 3) [18] *. 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? Let 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: [19] *$K(x_1)$, $K(x_2)$ and $K(x_3)$, fixed by non-normal sub-groups of order 2 - because M is degree 2 over $K(x_{1,2,3})$.* [20] *And we have one quadratic sub-extension (of degree 2) fixed by $A_3 \subset S_3$ this is $K\left(\sqrt{\Delta}\right)$.* [21]

Galois correspondence (Theorem 6.7) says us that there are no other sub-extensions. Because those sub extensions correspond objectively to subgroups of the Galois group (Definition 5.22). 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 group (Definition 5.22)s are cyclic (see corollary 3.16). I.e. we have the field $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. The Galois group is cyclic and generated by Frobenius map (see remark 3.6) which is $F_p : x \to x^p$.

More interesting are infinite extensions of a finite field, for instance the Algebraic closure (Definition 2.12). Thus consider $\bar{\mathbb{F}}_p$ as an extension of $\mathbb{F}_p$.

---

thus

$$\begin{aligned}\Delta = (\zeta-1)^2(\zeta^2-1)^2(\zeta^2-\zeta)^2 = \\ = (\zeta-1)^2(\zeta-1)^2(\zeta+1)^2\zeta^2(\zeta-1)^2 = \\ = (-3\zeta)^3\zeta^3 = -27.\end{aligned}$$

As result $b = -27$.

[18] See example A.54 about groups S_3 and Alternating group (Definition A.50) A_3.

[19] because x_1, x_2, x_3 are roots of a cubic polynomial

[20] $K(x_i) = M^{Gal(M/K(x_i))}$ and $Gal(M/K(x_i))$ has order 2, as soon as $[M : K(x_i)] = 2$, i.e. $Gal(M/K(x_i)) \cong \mathbb{Z}/2\mathbb{Z}$ - transposition of roots

[21] The extension should be $K(\alpha)$ where α is a root of a quadratic polynomial and $\alpha \notin K$ but $\alpha \in M$. $\sqrt{\Delta}$ is a good choice for the sub-extension generator because $\sqrt{\Delta} \notin K$ but $\sqrt{\Delta} \in M$ and $\sqrt{\Delta}$ - is a root of a quadratic polynomial i.e. it generates a quadratic extension. In the case $K\left(\sqrt{\Delta}\right) = M^{Gal\left(M/K\left(\sqrt{\Delta}\right)\right)} = M^{A_3}$ i.e. $Gal\left(M/K\left(\sqrt{\Delta}\right)\right) = A_3$.

If we take an invariant generated by Frobenius F_p [22] then [23]

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

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 sub-groups. In particular the Galois correspondence (Theorem 6.7) is not Bijection (Definition A.125) (as it was mentioned at remark 6.8)

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. [24] Lets look at the following:

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

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 $\forall x \in \mathbb{F}_{p^{2^n}}$

$$F_p^{a_n}(x) = F_p^{a_m}(x) \tag{6.1}$$

for any $m > n$. [25] 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 $\mathbb{F}_{p^{2^n}}$ $\forall l \geq 0$. [26] This implies

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

[23] It required some explanation. $\langle F_p \rangle$ consists of powers of Frobenius map: $F_p, F_{p^2}, \ldots, F_{p^n}, \ldots$, we also have that $\bar{\mathbb{F}}_p^{F_{p^n}} = \mathbb{F}_{p^n}$ (This is because $\forall x \in \mathbb{F}_{p^n} : F_{p^n}(x) = x^{p^n} = x$). Therefore

$$\bar{\mathbb{F}}_p^{\langle F_p \rangle} = \cap_n \mathbb{F}_{p^n} = \mathbb{F}_p$$

[24] We have a theorem that a subgroup of a cyclic group is cyclic (see Fundamental theorem of cyclic groups (Theorem A.24)). This means that if the whole group is cyclic then the smaller group has to be a cyclic too.

[25] If $F_p^{2^{n+l}} = id$ (see below in the text) then

$$F_p^{a_m}(x) = F_p^{a_n + 2^{n+1} + 2^{n+2} + \cdots + 2^m}(x) =$$
$$= F_p^{a_n}\left(F_p^{2^{n+1} + 2^{n+2} + \cdots + 2^m}(x)\right) = F_p^{a_n}(id(x)) = F_p^{a_n}(x).$$

[26] For example consider $F_p^{2^{n+1}}$ and let $x \in x \in \mathbb{F}_{p^{2^n}}$. We have

$$F_p^{2^{n+1}}(x) = F_p^{2^n \cdot 2}(x) = F_p^{2^n + 2^n}(x) =$$
$$= F_p^{2^n}\left(F_p^{2^n}(x)\right) = F_p^{2^n}\left(x^{2^n}\right) = F_p^{2^n}(x) = x^{2^n} = x.$$

that there exists an automorphism $\phi : L \to L$ such that $\forall n \geq 0$ [27]

$$\phi|_{\mathbb{F}_{p^{2^n}}} = F^{a_n} \tag{6.2}$$

but $\forall k \in \mathbb{Z}\ F_p^k \neq \phi$. [28] One can look at ϕ as $\phi = F_p^{1+2+4+\cdots+2^n+\cdots}$ but this is, of course, very informal. [29] The rigorous conclusions we can draw from this 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) [30] . Thus the polynomial has exactly n roots which form a cyclic (see definitionA.23) multiplicative sub-group of $\bar{K}^\times$ (see definition A.65) [31] denoted by μ_n. So μ_n is just the group of n roots of unity in $\bar{K}^\times$.

Definition 6.14 (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 (Definition 6.14) is denoted as μ_n^*. All elements of μ_n are powers of a single one: $\forall x \in \mu_n, \exists a \in \mathbb{N} : x = \zeta^a$ for some $\zeta \in \mu_n$. And primitive roots of unity form the following set $\{\zeta^a\}$ where $(a, n) = 1$. [32] The number of such primitive roots is determined by Euler's

[27] ??? We can say that ϕ maps L to L. If equation (6.2) holds for an arbitrary large N (i.e. informally $\mathbb{F}_{p^{2^N}}$ very close to L) then it also holds $\forall n < N$ because (6.1)

[28] i.e. $\phi \notin \langle F_p \rangle$

[29] Using (6.2) "informally" one can get

$$\phi = \phi|_L = \lim_{n\to\infty} \phi|_{\mathbb{F}_{p^{2^n}}} = \lim_{n\to\infty} F^{a_n} = F^{1+2+4+\cdots+2^n+\ldots}$$

[30] if $(n, char\,(K)) = 1$ then $P_n' = nX^{n-1} \not\equiv 0 \mod char\,(K)$ and as result $gcd\,(P_n, P_n') = 1$ i.e. P_n does not have multiple roots.

[31] $\exists x \in \mu_n$ such that $x^n = 1$ i.e. x is a root of P_n.

[32] The fact require a proof. Consider case $(a, n) = k > 1$. Thus $\frac{n}{k}, \frac{a}{k} \in \mathbb{Z}$ and we can get

$$(\zeta^a)^{\frac{n}{k}} = \left(\zeta^{\frac{a}{k}}\right)^n = 1$$

therefore ζ^a is a root of $X^{\frac{n}{k}} - 1$ and as soon as $\frac{n}{k} < n$ we conclude that $\zeta^a \notin \mu_n^*$ (but $\zeta^a \notin \mu_n$) i.e. ζ^a is not a Primitive roots of unity (Definition 6.14).

totient function (Definition A.135): $|\mu_n^*| = \phi(n)$. [33]

Definition 6.15 (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 6.16 (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 6.17. *1.* $P_n = \prod_{d|n} \Phi_d$

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

3. *If* $charK = 0$ *then* $\Phi_n \in \mathbb{Z}[X]$*. If* $charK = p$ *then* Φ_n *is the reduction* mod p *of the n-th cyclotomic polynomial (Definition 6.15) over* $\mathbb{Z}$*.*

Proof. The proof was marked as an exercise in the lectures

The first item proof is the following. The $X^n - 1$ has n roots and lets ζ is one of the root. Let $d = ord(\zeta)$ i.e. $\zeta^d = 1$ from other side $\zeta^n = 1$ i.e. $d \mid n$. Therefore $\zeta \in \mu_d^*$ i.e. ζ is a root of Φ_d. Thus any root $X^n - 1$ will also be a root of $\prod_{d|n} \Phi_d$. From other side for any root ζ' of $\prod_{d|n} \Phi_d$ exists d such that ζ' will be a root of Φ_d and as soon as $d \mid n$ then $\exists l \in \mathbb{Z} : n = d \cdot l$ therefore $(\zeta')^n = \left((\zeta')^d\right)^l = 1$ i.e. ζ' is also a root of $X^n - 1$. The both polynomial are Monic polynomial (Definition A.84)s and therefore are the same.

Lets consider case $char(K) = 0$ (for the second and third parts) and lets proof that in the case Φ_d has coefficients in $\mathbb{Z}$. Lets proof by induction. The

[33] That is by definition of Euler's totient function (Definition A.135) that counts the positive integers up to a given integer n that are relatively prime to n

case n is trivial because $\Phi_1 = X - 1$. Let for any $d < n$ we have that Φ_d has integer coefficients. Then using

$$P_n = \prod_{d|n} \Phi_d$$

we can get

$$\Phi_n = \frac{X^n - 1}{\prod_{d|n, d \neq n} \Phi_d}$$

using the fact that $\prod_{d|n,d\neq n} \Phi_d$ has integer coefficients (by induction hypothesis) we can conclude that Φ_n has coefficients in $\mathbb{Q}$. Then using Gauss (Equation 1.29) lemma we can conclude that $\Phi_n \in \mathbb{Z}[X]$.

Finally using

$$P_n = X^n - 1 = P_n \mod p = \prod_{d|n} (\Phi_d \mod p)$$

one can conclude that if $charK = p$ then Φ_n is the reduction $\mod p$ of the n-th cyclotomic polynomial (Definition 6.15) over $\mathbb{Z}$.

□

6.6 Irreducibility of cyclotomic polynomial.The Galois group

Theorem 6.18. *Let $char(K) = 0$, then Φ_n is irreducible in $\mathbb{Q}[X]$ (it amounts to the same to say that this is irreducible in $\mathbb{Z}[X]$ as we know).*

Proof. We have to prove that all Primitive roots of unity (Definition 6.14) have the same minimal polynomial over $\mathbb{Q}$. It must be Φ_n by degree reason.

Let fix one primitive root ζ and all others have the form ζ^a where a is prime to n: $(a, n) = 1$. [34] If we can show these for a prime then we can also show this for all a. [35] Thus we may assume that a is a prime number l and suppose

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

[34] as it was mentioned at the section 6.5.

[35] Let $a = l \cdot k$ where l and k are prime. We have (as it will be proved later) that $\nu = \zeta^l$ and ζ are roots of the same minimal polynomial. ν^k will also be a root of that minimal polynomial (if ν is a root and k is prime than ν^k will also be a root of the same polynomial), but $\nu^k = \zeta^{k \cdot l} = \zeta^a$.

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 [36] 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 $g_l \equiv g^l \mod l$. [37] 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 6.19. Statements of theorem 6.18 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. For instance $p = 2$ [38] In fact it splits in $\mathbb{F}_{p^2}$. This is because if p is odd then $8 \mid p^2 - 1$ so the Multiplicative group (Definition A.65) $\mathbb{F}_{p^2}^{\times}$ contains a cyclic subgroup of order 8 which is exactly the group of 8 roots of unity.

The main theorem about cyclotomic extensions is the following

Theorem 6.20. *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 they are 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. [39]

3. $Gal(L/K) \hookrightarrow Aut(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$. That [40] is because if a g is an identity on μ_n then it is also identity on L because μ_n generates L over

[36] $\Phi_n \in \mathbb{Z}[X]$ (see proposition 6.17). Gauss (Equation 1.29) lemma says that if Φ_n is reducible than they factors are also in $\mathbb{Z}[X]$.

[37] Using $g(X) = a_n X^n + \cdots + a_1 X + a_0$ we can get

$$g^l(X) = (a_n X^n + \cdots + a_1 X + a_0)^l =$$
$$= a_n X^{l^n} + \cdots + a_1 X^l + a_0 + l \cdot (\dots) \equiv g_l \mod l$$

[38] 1 is a root because $1^4 + 1 = 2 \equiv 0 \mod 2$. Therefore $\Phi_8 = X^4 + 1$ is reducible over $\mathbb{F}_2$

[39] This is because $\forall g \in Gal(L/K)$ g permutes roots of the irreducible polynomial Φ_n. The roots a generated by means of $\zeta \to \zeta^{a_g}$, where $(a_g, n) = 1$. Therefore we can associate a root permutation (i.e. g) with the following map $\zeta \to \zeta^{a_g}$, where $(a_g, n) = 1$.

[40] $Gal(L/K) \hookrightarrow Aut(\mu_n)$

K [41]

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.

□

[41] We have to proof there that $Gal(L/K) \hookrightarrow Aut(\mu_n)$ is an Embedding (Definition A.130) i.e. Injection (Definition A.124) that preserves the group structure. The injection was proved before because for $g_1, g_2 \in Gal(L/K)$ such that $g_1 \neq g_2$ we have two different root exchange $\zeta \to \zeta^{a_{g_1}}$ and $\zeta \to \zeta^{a_{g_2}}$. About structure preserving if $f : g \to (\zeta \to \zeta_a)$ then easy check that $f(g_1 g_2) = f(g_1) f(g_2)$ and that there is a homomorphism. By the way any embedding should preserve the identity element that was shown by Ekaterina.

Comments from staff about the identity preserving: The proof of injectivity in the lecture goes as follows: take arbitrary element $g \in Gal(L/K)$. We prove, that if the image of g is the identity in $(\mathbb{Z}/n)*$, then g is itself the identity in $Gal(L/K)$.

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 (Definition 6.14)) of 1). And we got a very precise description of those extensions in the case when Φ_n was irreducible, for instance, over $\mathbb{Q}$.

We have seen (see theorem 6.20) that $\mathbb{Q}(\zeta_n)$ is a Galois extension (Definition 5.18) of Galois group (Definition 5.22) $(\mathbb{Z}/n\mathbb{Z})^\times$ (see example A.66) 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: $(a, n) = 1$. [1]

Lets consider several examples

Example 7.1 ($n = 8$). *Lets consider $n = 8$. In the case*

$$\left|(\mathbb{Z}/8\mathbb{Z})^\times\right| = 4$$

[1] $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of elements which are invertible in $\mathbb{Z}/n\mathbb{Z}$. The numbers which are prime to n are invertible.

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 [2]*:*

$$Gal : \left\{id, \zeta_8 \to \zeta_8^3, \zeta_8 \to \zeta_8^5, \zeta_8 \to \zeta_8^7\right\} = \{id, \sigma_3, \sigma_5, \sigma_7\}.$$

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 (Definition 6.6)* $\mathbb{Q}(\zeta_8)^{\sigma_7}$ *is determined by the following expression* [3]

$$\mathbb{Q}(\zeta_8)^{\sigma_7} = \mathbb{Q}(\zeta_8) \cap \mathbb{R} = \mathbb{Q}\left(\zeta_8 + \bar{\zeta}_8\right) = \mathbb{Q}\left(\sqrt{2}\right)$$

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.* [4]

$$\mathbb{Q}(\zeta_8)^{\sigma_3} = \mathbb{Q}\left(\zeta_8 + \zeta_8^3\right) = \mathbb{Q}\left(i\sqrt{2}\right).$$

---

[2] There is a well known Klein four group V_4 [61] - the only non-cyclic group of order 4 (really there are 2 groups of order 4: the first one is the Klein four group, the second one is the cyclic group of order 4). We will also see the group when we will investigate the solvability of group S_4 at example 8.7.

[3] First of all by the Galois correspondence (Theorem 6.7) theorem for any normal subgroup of the Galois group (Definition 5.22) (V_4 in our case) there exists a sub-extension that is fixed by the normal sub-group. For our V_4 we have 3 normal subgroups: $\{id, \sigma_3\}, \{id, \sigma_5\}, \{id, \sigma_7\}$. Lets consider the last one i.e. lets find the extension that corresponds to $\{id, \sigma_7\}$. The extension has the following form (we are using triviality of id: $L^{id} = L$)

$$\mathbb{Q}(\zeta_8)^{\{id, \sigma_7\}} = \mathbb{Q}(\zeta_8)^{\sigma_7}$$

To calculate $\mathbb{Q}(\zeta_8)^{\sigma_7}$ we have to find a Primitive element (Example 5.13) ν such that $\nu \notin \mathbb{Q}$, $\nu \in \mathbb{Q}(\zeta_8)$ and $\sigma_7(\nu) = \nu$ (i.e. σ_7 fixes $\mathbb{Q}(\nu)$). Using the fact that $\bar{\zeta}_8 = \zeta_8^7$, it can be easy to check that

$$\sigma_7\left(\zeta_8 + \bar{\zeta}_8\right) = \sigma_7\left(\zeta_8 + \zeta_8^7\right) =$$
$$= \zeta_8^7 + \zeta_8^{49} = \zeta_8^7 + \zeta_8^{6 \cdot 8 + 1} = \zeta_8^7 + \zeta_8 = \bar{\zeta}_8 + \zeta_8,$$

i.e. we can take $\nu = \zeta_8 + \bar{\zeta}_8$ as an element that generates the required extension.

[4] The following equations were used

$$\sigma_3\left(\zeta_8 + \zeta_8^3\right) = \zeta_8^3 + \zeta_8^9 = \zeta_8^3 + \zeta_8$$

and

$$\sigma_5\left(\zeta_8 \cdot \zeta_8^5\right) = \zeta_8^5 \cdot \zeta_8^{25} = \zeta_8^5 \cdot \zeta_8^{3 \cdot 8 + 1} = \zeta_8^5 \cdot \zeta_8.$$

and finally (with note $\zeta_8^5 = -\zeta_8, \zeta_8^6 = -i$*)* [5]

$$\mathbb{Q}(\zeta_8)^{\sigma_5} = \mathbb{Q}\left(\zeta_8 \cdot \zeta_8^5\right) = \mathbb{Q}\left(\zeta_8^6\right) = \mathbb{Q}(i).$$

Example 7.2 ($n = 5$)**.** $\mathbb{Q}(\zeta_5)$ *where* $\zeta_5 = e^{\frac{2\pi i}{5}}$*. The Galois group (Definition 5.22) is the following:*

$$Gal \cong (\mathbb{Z}/5\mathbb{Z})^{\times}$$

that is a Cyclic group (Definition A.23) of order 4. [6] *It is generated by* $\zeta_5 \to \zeta_5^2$ [7] *and it has only one Proper subgroup (Definition A.11)* $\cong \mathbb{Z}/2\mathbb{Z}$ *(see theorem A.25) 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: $(char(K), n) = 1$ [8] 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

$$d = \min\left\{i \mid \alpha^i \in K\right\}. \tag{7.1}$$

[5] we cannot choose $\zeta_8 + \zeta_8^5 = 0$ and have chosen $\zeta_8 \cdot \zeta_8^5$ instead of it.

[6] As it was mentioned above there are only 2 finite group of order 4. The first one V_4 was considered at example 7.1. There is the second one that isomorphic to the cyclic group of order 4:

$$(\mathbb{Z}/5\mathbb{Z})^{\times} = \{1, 2, 3, 4\}$$

[7] $Gal = \langle\zeta_5\rangle$ and the group action on an element is just a multiplication by ζ_5 i.e. $id \to \zeta_5, \zeta_5 \to \zeta_5^2, \zeta_5^2 \to \zeta_5^3, \zeta_5^3 \to \zeta_5^4, \zeta_5^4 \to id$

[8] case $char(K) = 0$ is also included because it is used only one time to prove separability (see note 10)

Proposition 7.3. *$d \mid n$, minimal polynomial of α is $X^d - \alpha^d$ and $K(\alpha)$ is a Galois extension (Definition 5.18) with cyclic Galois group (Definition 5.22) 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 $X^n - a$. [9] Therefore $K(\alpha)$ is a splitting field of $X^n - a$ thus it's normal. The extension is also separable because $(char(K), n) = 1$. [10] Thus $K(\alpha)$ is Galois extension (Definition 5.18).

Lets define a Homomorphism (Definition A.126) $f : Gal(K(\alpha)/K) \xrightarrow[g \to \frac{g(\alpha)}{\alpha}]{} \mu_n$. 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: [11]

$$\left(\frac{g(\alpha)}{\alpha}\right)^n = 1.$$

The homomorphism f is Injection (Definition A.124) because $g(\alpha)$ determines g. [12] What's the image? It should be a Subgroup (Definition A.10) of a Cyclic group (Definition A.23) μ_n but the subgroup should be also cyclic. [13] Let δ is the order of the image and we want to show that $\delta = d$. Consider $g(\alpha^\delta) = f(g)^\delta \cdot \alpha^\delta = \alpha^\delta$ because $f(g)$ is a root of 1 ($f(g) = \sqrt[\delta]{1}$). [14] Thus $\alpha^\delta \in K$ (see (5.5)). And $\alpha^i \notin K$ for $i < \delta$ since otherwise $\deg P_{min}(\alpha, K) = i < \delta$. But this is impossible because

$$[K(\alpha) : K] = |Gal(K(\alpha)/K)| = \delta.$$

[9] Consider $\alpha_k = \alpha\zeta^k$ where $k = 0, 1, \ldots, n-1$. All such α_k are roots of $X^n - a$ because

$$\alpha_k^n - a = \alpha^n (\zeta^n)^k - a = a - a = 0.$$

We also have that $\forall k_1 \neq k_2 : \alpha_{k_1} \neq \alpha_{k_2}$ because $\zeta^{k_1} \neq \zeta^{k_2}$. Therefore we have n distinct roots i.e. all roots are in $K(\alpha)$

[10] If $P_n = X^n - a$ then $P_n' = nX^{n-1} \neq 0$ as soon as $(char(K), n) = 1$ and as result $(P_n, P_n') = 1$ and P_n does not have multiple roots and therefore it is separable. As result the extension $K(\alpha)$ is also separable.

The case $char(K) = 0$ is obvious because such extensions are always separable (see section 3.4).

[11] $g^n(\alpha) - \alpha^n = g^n(\alpha) - a = 0$

[12] If we have $g_1 \neq g_2$ then $g_1(\alpha) \neq g_2(\alpha)$ because in the case $g_1(\alpha)$ and $g_2(\alpha)$ are 2 different roots of $X^n - a$. As result the homomorphism f is Injection (Definition A.124).

[13] see Fundamental theorem of cyclic groups (Theorem A.24)

[14] Using $g(\alpha) g(\alpha) = g(\alpha \cdot \alpha) = g(\alpha^2)$:

$$f^\delta(g) = \frac{g^\delta(\alpha)}{\alpha^\delta} = \frac{g(\alpha^\delta)}{\alpha^\delta}.$$

Thus only possible option is $d = \delta$. [15] Thus $P_{min}(\alpha, K) = X^d - \alpha^d$. □

Proposition 7.4. *And conversely (to 7.3) 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 $\sigma^n = id$. Linear algebra says that σ is Diagonalizable map (Definition A.120). [16] Now, let us show that all eigenspaces have dimension 1. Indeed if x, y are in the same Eigenspace (Definition A.119) then $\sigma\left(\frac{x}{y}\right) = \frac{x}{y}$ [17] 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, x, y are proportional over K. [18] Thus all roots of 1 are eigenvalues of σ. [19] Then take α such that $\sigma(\alpha) = \zeta\alpha$ where ζ is a Primitive roots of unity (Definition 6.14). 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.

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, α 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. [20] □

7.3 Artin-Schreier extensions

Let $n = charK$ this is called as Artin-Schreier extensions.

[15] d was chosen accordingly (7.1) and therefore $\delta \geq d$.

[16] Apply theorem A.122 to the diagonalizable $\sigma^n = id$. Really a map is diagonalizable if it has n distinct eigenvalues (see theorem A.121). This fact will be proved below.

[17] $L^{\langle\sigma\rangle} = K$ i.e. $L^\sigma = K$.

[18] I.e. if $\mathcal{L}$ is the eigenspace then we have that $\exists x \in \mathcal{L}$ such that $\forall y \in \mathcal{L} : y = kx$, where $k \in K$. This exactly means that $\dim \mathcal{L} = 1$

[19] Let x - eigenvector of σ and ν is the eigenvalue. We have $\sigma(x) = \nu x$, using $\sigma^n = id$ and $\sigma \circ \sigma(x) = \sigma(\nu x) = \nu^2 x$, one can get $\sigma^n(x) = \nu^n x = id(x) = x$. Thus $\nu^n = 1$ i.e. ν is a root of unity.

[20] If we have $K \subset K(\alpha) \subset L$ and $\langle\sigma\rangle$ is a Galois group (Definition 5.22) L/K and $[K(\alpha) :] = d < n$ then by Galois correspondence (Theorem 6.7) there exists a subgroup $H \subset \langle\sigma\rangle$ (cyclic as soon as $\langle\sigma\rangle$) that fixes the $K(\alpha)$ and especially $\forall h \in H : h(\alpha) = \alpha$ therefore $\left|\sigma^k(\alpha)\right| < n$ i.e. the orbit contains less than n elements.

Another explanation as follows. If $[K(\alpha) :] = d < n$ then $P_{min}(\alpha, K)$ has d roots and the orbit $Orb(\alpha)$ consists of roots of $P_{min}(\alpha, K)$ and the number of roots is $d < n$.

Definition 7.5 (Cyclic extension)**.** The Galois extension is called cyclic extension if the corresponding Galois group (Definition 5.22) is cyclic.

Theorem 7.6. *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 then $K(\alpha)$ is Cyclic extension (Definition 7.5) 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). [21]

If P is irreducible then Galois group (Definition 5.22) should be transitive on the roots (see remark 5.21) 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 (Definition A.7) for σ is $p = [K(\alpha) : K]$ [22] so the σ must generate the Galois group (Definition 5.22): $Gal(K(\alpha)/K) = \langle\sigma\rangle$.

We have to show that if P is not irreducible then P splits i.e. $\alpha \in K$. Leave it for an exercise [23]

Now we will prove the converse statement. Let L is a Cyclic extension (Definition 7.5) 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 $Gal(L/K) = \langle\sigma\rangle$).

---

[21] In $\mathbb{F}_p$ we have $k^p = k$ and therefore

$$\begin{aligned}(\alpha + k)^p - (\alpha + k) - a = \\ = \alpha^p + k^p - \alpha - k - a = \alpha^p + k - \alpha - k - a = \\ = \alpha^p - \alpha - a = 0,\end{aligned}$$

as soon as α is a root of $X^p - X - a$.

[22]

$$\sigma^p = \sigma(\sigma(\sigma(\dots(\sigma(\alpha))\dots))) = \alpha + p = \alpha$$

i.e. $\sigma^p = id$ and order of $\langle\sigma\rangle$ is p.

[23] Let α is a root then we can get p different roots as $\alpha + k$ where $k \in \mathbb{F}_p$. Suppose that $\alpha \notin K$ and Q is a factor of P (it should exist as soon as P is reducible). Q splits in $K(\alpha)$ as soon as P splits there and its factors have the form $X - (\alpha - i)$. Let $d = \deg Q$, i.e.

$$Q = \prod_i (X - (\alpha - i)) = X^d + a_1 X^{d-1} + \dots + a_d.$$

Consider the coefficient a_1. It should have the form $a_1 = \sum_i (\alpha - i) = d\alpha - j$ (where i is taken from d factors of Q and $\sum_i i = j$ - another integer). $a_1 \in K$ (and as result $Q \in K[X]$) only if $d = 0 \mod p$. Therefore P has no nontrivial factors that is in the contradiction with statement that P is reducible.

Thanks Ben Petschel for the hint.

Set $f = \sigma - id$, $K = \ker f$ [24] and the Rank (Definition A.111) $rgf = p-1$. [25] We have $(\sigma - id)^p = 0$ [26] so the Kernel (Definition A.110) must be included into Image (Definition A.109): $K = \ker f \subset \operatorname{Im} f$ because otherwise $L = \ker f \oplus \operatorname{Im} f$ (L is a direct sum [27] of kernel and image) and f^k is never zero (but we have $f^p = 0$) [28].

So as soon as K is in the image of f then $\exists \alpha \in L$ such that $f(\alpha) = 1$ [29] 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 (5.5)). 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. □

---

[24] this is because $\forall x \in K : \sigma(x) = x$ (see (5.5)).

[25] In lectures we can hear about range (Image (Definition A.109)) not a Rank (Definition A.111) but by future content we spoke about the rank but not about range (image). In any way the equation $rgf = p-1$ requires some explanation. As soon as $f^{p-1} \neq 0$ $\exists x \in L$ such that $f^{p-1}(x) \neq 0$. Therefore $f^k(x) \neq 0$ for all $k < p-1$ because in other case

$$f^{p-1}(x) = f\left(\dots f\left(f^k(x)\right)\dots\right) = f(\dots f(0)\dots) = 0.$$

Lets show that $\left(f(x), f^2(x) \dots, f^{p-1}(x)\right)$ is linearly independent. For $k \in K, x \in L$ we can get

$$f(k \cdot x) = \sigma(k \cdot x) - k \cdot x = \sigma(k) \cdot \sigma(x) - k \cdot x = k \cdot \sigma(x) - k \cdot x = k \cdot f(x).$$

Thus for $k_i \in K$ such that:

$$\sum_{i=1}^{p-1} k_i f^i(x) = 0$$

applying f^{p-1} one can get that $k_1 = 0$, applying f^{p-2} gives us $k_2 = 0$. Continue the way we get that all $k_i = 0$. That proves the linear independence. Therefore $rg(f) \geq p-1$. The vector $y = \left(f^{p-1}(x), f^{p-1}(x) \dots, f^{p-1}(x)\right)$ is not zero but $f(y) = 0$ therefore $y \in \ker f$. This means that $\dim \ker f \geq 1$. Using Rank–nullity theorem (Theorem A.113) one can conclude that only possible choice there is $\dim \ker f = 1$ and $rg(f) = p-1$.

[26] In $\mathbb{F}_p$ we have

$$(\sigma - id)^p = \sigma^p - id = 0$$

as soon as $\langle \sigma \rangle$ has order p.

[27] see also definition A.102 and example A.103

[28] As soon as $f \neq 0$ exists $x \in L$ such that $y = f^{p-1}(x) \neq 0$ but $f(y) = f^p(x) = 0$, therefore $y \in \ker f$. Using the fact that $\dim \ker f = 1$ (follows from $rg(f) = p-1$ and Rank–nullity theorem (Theorem A.113)) and $y \in \operatorname{Im} f$ ($y = f\left(f^{p-2}(x)\right)$) one can conclude that the Kernel (Definition A.110) must be included into Image (Definition A.109).

[29] This is because $1 \in K$ but $K \subset \ker(f) \subset \operatorname{Im}(f)$ therefore $1 \in Im(f)$.

7.4 Composite extensions. Properties

Definition 7.7 (Composite extension)**.** Let L_1 and L_2 are extensions of K both contained in some extension L (for instance the Algebraic closure (Definition 2.12) $\bar{K}$). The composite extension L_1L_2 is the extension they generate: $L_1L_2 = L_2L_1 = K(L_1 \cup L_2)$. I.e. the composite extension is the smallest extension that contains both L_1 and 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 (Definition 4.2) there is a map from the tensor product to L: $j : L_1 \otimes_K L_2 \to L$ such that $j(l_1 \otimes l_2) = l_1 l_2$ [30]

$$\begin{array}{ccc} L_1 \times L_2 & \xrightarrow{f : (l_1, l_2) \to l_1 l_2} & L \\ & {\scriptstyle \phi} \searrow \quad \nearrow {\scriptstyle \tilde{f} = j} & \\ & L_1 \otimes_K L_2 & \end{array}$$

The Image (Definition A.109) $\operatorname{Im} j$ is a sub-algebra of L. If L is algebraic then any sub algebra is a sub field (see proposition 1.18) 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)) but in our case, as it was mentioned above, as soon as L is algebraic then $L_{1,2}$ are fields.

Property 7.8. *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 $x \in L_1$ (L_1L_2 is generated by L_1 over L_2) [31] then it's minimal polynomial $P_{min}(x, L_2)$ is a divisor of $P_{min}(x, K)$ in $L_2[X]$ (see proposition 1.19). 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) then $P_{min}(x, L_2)$ is separable (pure inseparable). [32]

The same is true for splitting so the normality is preserved. [33]

[30] By the Universal property (Definition 4.2) j is a Homomorphism (Definition A.126), but by lemma 1.6 the homomorphism is injection.

[31] We have $K \subset L_2 \subset L_1L_2$ as the case there

[32] From proposition 1.19) we know that $P_{min}(x, L_2)$ is a divisor of $P_{min}(x, K)$. Therefore if $P_{min}(x, K)$ does not have multiply roots then $P_{min}(x, L_2)$ (its divisor) will also have only non-multiply roots.

The inseparability is obvious because if the $P_{min}(x, K)$ has only one root the same will be the truth for $P_{min}(x, L)$.

[33] i.e. the polynomial splits in L_2 if it splits in $K \supset L_2$

About dimensions ("finite extension of degree" in the property formulation). By the Base-change (Theorem 4.13) [34]:

$$\dim_K L_1 = \dim_{L_2} (L_1 \otimes_K L_2)$$

and as soon as L_1L_2 is the $\operatorname{Im} j$: [35]

$$\dim_{L_2} (L_1 \otimes_K L_2) \geq \dim_{L_2} (L_1L_2)$$

i.e.

$$\dim_{L_2} (L_1L_2) \leq \dim_K L_1 = n.$$

□

Property 7.9. *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 7.8. [36]

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. □

[34] From Base-change (Theorem 4.13) one can get

$$\left|Hom_K (L_1, \bar{K})\right| = \left|Hom_{L_2} (L_2 \otimes_K L_1, \bar{K})\right|$$

But proposition 3.24 says that

$$\left|Hom_K (L_1, \bar{K})\right| = \deg (P_{min} (x, K)) = [L_1 : K] = \dim_K (L_1)$$

and

$$\left|Hom_{L_2} (L_2 \otimes_K L_1, \bar{K})\right| = [L_2 \otimes_K L_1 : L_2] = \dim_{L_2} (L_1 \otimes_K L_2)$$

[35] Using Rank–nullity theorem (Theorem A.113) one can conclude that for $j : L_1 \otimes_K L_2 \to L_1L_2$, $\dim \operatorname{Im} j \leq \dim L_1 \otimes_K L_2$ (the equal sign is when $\dim \ker j = 0$).

[36] From property 7.8 follows that if L_1 is separable over K then L_1L_2 is separable over L_2. If L_2 is separable over K then theorem 3.28 about separability says the L_1L_2 is separable over K as soon as $K \subset L_2 \subset L_1L_2$.

About degrees: if $n = [L_1 : K]$ and $m = [L_2 : K]$ then from property 7.8 follows that $[L_1L_2 : L_2] \leq n$. Using theorem 1.22 $[L_1L_2 : K] = [L_1L_2 : L_2]\,[L_2 : K] \leq nm$.

7.5 Linearly disjoint extensions. Examples

Theorem 7.10. *The following statements are equivalent (for algebraic extensions)*

1. $L_1 \otimes_K L_2$ *is a field*
2. j *is Injection (Definition A.124)*
3. *if we have* $x_1, x_2, \dots, x_n \in L_1$ *linearly independent over* K *then they are linearly independent over* L_2
4. *if we have two families:* $x_1, x_2, \dots, x_n \in L_1$ *linearly independent over* K *and* $y_1, y_2, \dots, y_m \in L_2$ *linearly independent over* K *then* $x_i y_j$ *are also 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* $[L_1L_2 : K] = [L_1 : K]\,[L_2 : K]$ [37]

Definition 7.11 (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 $L_1L_2 = \operatorname{Im} j$. [38]

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 (see proposition 4.11). 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. [39]

3 implies 4: if we have some relation $\sum_{i,j} a_{ij} x_i y_j = 0, a_{ij} \in K$ then since x_i linearly independent over K one can get $\sum_j a_{ij} y_j = 0$ but as soon as y_j linearly independent we will get $a_{ij} = 0$.

---

[37] Using theorem 1.22 we have $[L_1L_2 : K] = [L_1L_2 : L_2]\,[L_2 : K]$.

[38] By the Universal property (Definition 4.2) j is a Homomorphism (Definition A.126), but by lemma 1.6 the homomorphism is injection if $L_1 \otimes_K L_2$ is a field.

If j is injection then from the fact $L_1L_2 = \operatorname{Im} j$ we can conclude that for any $x \in L_1 \otimes_K L_2$ such that $x \neq 0$ there exists $y \in L_1 \otimes_K L_2$ such that $j(x)j(y) = 1$ as soon as $L_1L_2 = K(L_1 \cup L_2)$ is a field (both L_1 and L_2 are algebraic). Therefore $xy = 1$ and for any non zero element of $L_1 \otimes_K L_2$ we can the the inverse one. This means that $L_1 \otimes_K L_2$ is a field.

[39] Let $x_1, \dots, x_n$ are not linearly independent over L_2 then there exists $\alpha_1, \dots, \alpha_n \in L_2$ such that $\exists \alpha_k \neq 0$ but $\sum_{i=1}^n \alpha_i x_i = 0$. From other side $x_i = j(x_i \otimes 1)$ therefore $j(\sum_{i=1}^n \alpha_i x_i \otimes 1) = 0$ but $\sum_{i=1}^n \alpha_i x_i \otimes 1 \neq 0$ as soon as $x_1 \otimes 1, \dots, x_n \otimes 1$ are linearly independent over L_2. Therefore we just got a contradiction: j cannot be injection.

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 $j(z) = \sum a_{ij} x_i y_j = 0$ i.e. $a_{ij} = 0$ and therefore $z = 0$. I.e. j is Injection (Definition A.124).

The part about finite degrees follows from the 4 properties. [40] □

Example 7.12. *First of all, the extensions which have relatively prime degrees are always linearly disjoint.*

I.e. if $[L_1 : K] = n$, $[L_2 : K] = m$ *and* $(m, n) = 1$ *then* L_1 *and* L_2 *are linearly disjoint. Indeed* m *and* n *must divide* $[L_1 L_2 : K] \leq mn$. *With our conditions* $[L_1 L_2 : K] = mn$ *but this is one of definition of linearly disjoint extensions (see definition 7.11).* [41]

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* $\left[\mathbb{Q}\left(\sqrt[5]{1}\right) : \mathbb{Q}\right] = 4$. [42]

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* $L_1 L_2$ *is a splitting field of* $X^5 - 2$ *and (for the first case)* $[L_1 L_2 : \mathbb{Q}] = 4 \cdot 5 = 20$. *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 7.13. *Let* $L_1, L_2 \subset \bar{K}$ *- extensions of* K. L_1 *is Galois extension (Definition 5.18) over* K. *Let* $K' = L_1 \cap L_2$. *Then* $L_1 L_2$ *is Galois*

[40] Let L_1 and L_2 are linearly disjoint extensions over K with finite degree: $[L_1 : K] = n, [L_2 : K] = m$. From 3 we can conclude that $[L_1 L_2 : L_2] = n$ and using theorem 1.22 we will obtain $[L_1 L_2 : K] = [L_1 L_2 : L_2]\,[L_2 : K] = nm$.

[41] The claim is the following: if $(m, n) = 1$ then L_1 and L_2 are linearly disjoint. From property 7.9 $[L_1 L_2 : K] \leq mn$. But from theorem 1.22 $n \mid [L_1 L_2 : K]$, as soon as $K \subset L_1 \subset L_1 L_2$, and $m \mid [L_1 L_2 : K]$, as soon as $K \subset L_2 \subset L_1 L_2$ and therefore using $(m, n) = 1$ one can conclude that $[L_1 L_2 : K] = nm$ and thus L_1 and L_2 are linearly disjoint by last statement of theorem 7.10.

[42] $P_{min}\left(\sqrt[5]{2}, \mathbb{Q}\right) = X^5 - 2$ and $\deg\left(P_{min}\left(\sqrt[5]{2}, \mathbb{Q}\right)\right) = 5$.
$P_{min}\left(\sqrt[5]{1}, \mathbb{Q}\right) = X^4 + X^3 + X^2 + X + 1$ and $\deg\left(P_{min}\left(\sqrt[5]{1}, \mathbb{Q}\right)\right) = 4$.

over L_2. $Gal\left(L_1L_2/L_2\right)$ *stabilizes* L_1. $\phi : g \to g|_{L_1}$ *is an injective map of* $Gal\left(L_1L_2/L_2\right) \to Gal\left(L_1/K\right)$ *with image* $Gal\left(L_1/K'\right)$ *and* L_1, L_2 *are linearly disjoint over* K'.

Proof. The proof that L_1L_2 is Galois over L_2 is obvious. [43]

The next statement is that $Gal\left(L_1L_2/L_2\right)$ stabilizes L_1. [44] Let $x \in L_1$ and $g \in Gal\left(L_1L_2/L_2\right)$ then $g\left(x\right)$ is a root of $P_{min}\left(x, L_2\right)$. [45] It is also a root of $P_{min}\left(x, K\right)$. [46] But all such roots are in L_1 because L_1 is a Galois extension (Definition 5.18).

Therefore the map ϕ is well defined. The map is 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. [47]

So now lets find the image of ϕ. If $g\left(x\right) = x, \forall g \in Gal\left(L_1L_2/L_2\right)$ then $x \in L_2$ by Galois correspondence (Theorem 6.7). So if also $x \in L_1$ then it should be $x \in K' = L_1 \cap L_2$. So if L_1 is finite over K then by Galois correspondence (Theorem 6.7) we can conclude that $\operatorname{Im}\phi = Gal\left(L_1/K'\right)$ [48] because the Fixed field (Definition 6.6) is K'.

In general [49] we have to find finite sub-extension of L_1: let denote it as

[43] We have L_1 is Galois extension (Definition 5.18) and therefore normal and separable over K. By property 7.8 this means that L_1L_2 is normal and separable over L_2 or in other words L_1L_2 is Galois over L_2.

[44] I.e. $\forall g \in Gal\left(L_1L_2/L_2\right)$ and for any $x \in L_1$ we have $g(x) \in L_1$ or in other words $g(L_1) = L_1$ (see also definition A.29).

[45] This is because g permutes roots and the image of the permutation is the set of roots of the following polynomial $P_{min}\left(x, L_2\right)$. Note that x is also one of the roots.

[46] This is because proposition 1.19 i.e. because $P_{min}\left(x, L_2\right)$ divides $P_{min}\left(x, K\right)$ i.e. all roots of $P_{min}\left(x, L_2\right)$ are also roots of $P_{min}\left(x, K\right)$.

[47] We have that $\phi(id) = id$ i.e. ϕ is Injection (Definition A.124). Because if $g_1, g_2 \neq id$ then the equality $\phi(g_1) = \phi(g_2)$ holds if $g_1 g_2^{-1} = id$ i.e. if $g_1 = g_2$ that is accordingly with the injectivity definition.

Another proof is the following. Accordingly the staff comment on last section of lecture 6 (see note 41). We have to take an arbitrary element $g \in L$ then if its image is identity ($\phi(g) = id$) then $g = id$. We got the required property if we assume

$$\begin{cases} \phi(g)\left(x\right) = g\left(x\right), & \text{if } x \in L_1 \\ \phi(g)\left(x\right) = id\left(x\right) = x, & \text{if } x \in L_2. \end{cases}$$

In the case if $\phi(g) = id$ then $g|_{L_1} = id$ and $g|_{L_2} = id$ or as it was mentioned in the lectures $g = id$. This finishes the proof that ϕ is injective.

See also theorem A.133.

[48] In the lectures Ekaterina marked it as $\operatorname{Im}\phi = Gal\left(L/K'\right)$ but really we should have L_1 instead of L there.

[49] not finite L_1 over K

L_1'. We also have a finite Galois sub extension of L_1 that contains L_1'. We denote this Galois sub-extension as L_1''. [50]

We have L_1'' and L_2 are linearly disjoint over K' [51] then it follows that L_1 and L_2 are also linearly disjoint over K' (see theorem 7.10 point 3).

Several additional comments about the $\operatorname{Im}\phi$. Let $\gamma \in Gal\,(L_1/K')$ then exists an element in $Gal\,(L_1L_2/L_2)$ which is sent by ϕ to γ. [52] We have $j : L_1 \otimes_K L_2 \cong L_1L_2$ and we can take $j \cdot (\gamma \otimes id_{L_2}) \cdot j^{-1}$ - this will be the element of the required Galois group. [53] □

7.7 On the Galois group of the composite

From the theorem 7.13 follows the following proposition

Proposition 7.14. *1. L_1 and L_2 are both Galois over K and linearly disjoint then the following map $g \to \left(g|_{L_1}, g|_{L_2}\right)$ defines the isomorphism* [54]

$$Gal\,(L_1L_2/K) \cong Gal\,(L_1/K) \times Gal\,(L_2/K)$$

2. conversely to the first part: if $Gal\,(L/K) = G_1 \times G_2$ then $L = L^{G_1}L^{G_2}$ which are linearly disjoint over the intersection. [55]

---

[50] ??? The claim require a proof. Ekaterina provided only initial ideas about how the proof can look like: 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 , but the solution is more or less what I just have told you.

[51] As soon as j is injection, the theorem 7.10 gives us that L_1'' and L_2 are linearly disjoint over K'.

[52] The element exists if $\operatorname{Im}\phi = Gal\,(L_1/K')$.

[53] I.e. there is an element $g \in Gal\,(L_1L_2/L_2)$ such that $\phi(g) = \gamma$. Let $x \in L_1$ (but $x \notin L_2$ i.e. $x \notin K'$ because for such x and $\forall g \in Gal\,(L_1L_2/L_2)$ it will be $g(x) = x$ as well as $\gamma(x) = x$ i.e. obviously the required property is satisfied) then, using equality $x = x \cdot 1_{L_2}$, one can get

$$j^{-1}(x) = x \otimes 1_{L_2}$$

and therefore

$$\phi(g)(x) = j \cdot (\gamma \otimes id_{L_2}) \cdot j^{-1}(x) =$$
$$= j \cdot (\gamma(x) \otimes id_{L_2}(1)) = \gamma(x) \cdot 1 = \gamma(x).$$

I.e. $\phi(g) = \gamma$.

[54] $Gal\,(L_1/K) \times Gal\,(L_2/K)$ is a Direct product (Definition A.34) of 2 groups $Gal\,(L_1/K)$ and $Gal\,(L_2/K)$.

[55] i.e. L^{G_1} and L^{G_2} are linearly disjoint over $L^{G_1} \cap L^{G_2}$

Proof. The first part is very sure because the injectivity of this map is clear: if something is trivial both on L_1 and L_2, then it's trivial on the composite, [56] so I only have to prove the surjectivity. I will use the same trick as before: $L_1 \otimes_K L_2 \cong_j L_1L_2$ then $j \cdot (g_1 \otimes g_2) \cdot j^{-1}$ goes to (g_1, g_2). [57]

The second part. L^{G_1} and L^{G_2} are both Galois [58] because G_1 and G_2 are normal in the product (see property A.35): $G_1, G_2 \triangleleft G_1 \times G_2$. 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 $L^{G_1} \cap L^{G_2} = K$. [59] Linear disjoint follows from $L^{G_1} \cap L^{G_2} = K$ since we are in the Galois case. [60] □

---

[56] If we take an arbitrary element $g \in Gal(L_1L_2/K)$ and the image of the element is: $\left(id|_{L_1}, id|_{L_2}\right) \in Gal(L_1/K) \times Gal(L_2/K)$ then the taken element is the identity too: $g = id$. This proves the injectivity i.e. the proof is the same as in the note 47.
See also theorem A.133.

[57] Let $x \in L_1$ then using equality $x = x \cdot 1_{L_2}$, one can get

$$j^{-1}(x) = x \otimes 1_{L_2}$$

and therefore

$$\left(j \cdot \left(g|_{L_1} \otimes g|_{L_2}\right) \cdot j^{-1}\right)(x) = j \cdot \left(g|_{L_1}(x) \otimes g|_{L_2}(1)\right) = \\ = g|_{L_1}(x) \cdot 1 = g_1(x).$$

If $x \in L_2$ then using equality $x = 1_{L_1} \cdot x$, one can get

$$j^{-1}(x) = 1_{L_1} \otimes x$$

and therefore

$$\left(j \cdot \left(g|_{L_1} \otimes g|_{L_2}\right) \cdot j^{-1}\right)(x) = j \cdot \left(g|_{L_1}(1) \otimes g|_{L_2}(x)\right) = \\ = 1 \cdot g|_{L_2}(x) = g_2(x).$$

Thus we have the following construction

$$\begin{cases} j \cdot (g_1 \otimes g_2) \cdot j^{-1} \to g_1 = g_{L_1}, & \forall x \in L_1 \\ j \cdot (g_1 \otimes g_2) \cdot j^{-1} \to g_2 = g_{L_2}, & \forall x \in L_2 \end{cases}$$

In the obvious case $x \in L_1 \cap L_2$ we have $g_1 = g_2$. Thus we can write $j \cdot (g_1 \otimes g_2) \cdot j^{-1} \to (g_1, g_2)$.

[58] see theorem 6.7 point 2a

[59] ??? Let $x \in L^{G_1} \cap L^{G_2}$ then $\forall g_1 \in G_1, g_2 \in G_2 : g_1(x) = x, g_2(x) = x$. Or in other words $\forall g \in G : g = (g_1, g_2)$ we have $g(x) = x$. Therefore G fixes $L^{G_1} \cap L^{G_2}$, but $G = Gal(L/K)$ thus $L^{G_1} \cap L^{G_2} = K$.

[60] We can use theorem 7.13 as soon as L^{G_1} and L^{G_2} are both Galois (see theorem 6.7

Let me give you a small example:

Example 7.15. *We have a Composite extension (Definition 7.7)* $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n, \zeta_m)$ [61] *where* $\zeta_n = e^{\frac{2\pi i}{n}}$. $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}\left(\zeta_{LCM(n,m)}\right)$ [62] *therefore if* $(n, m) = 1$ *then* $\mathbb{Q}(\zeta_n)$ *and* $\mathbb{Q}(\zeta_m)$ *are linearly disjoint.* [63] *It can be seen as follows: we can apply proposition 7.14 to our Galois groups then* $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$ *but by the Chinese remainder (Equation 4.20) theorem* [64]

$$(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times .$$

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 7.14.*

---

point 2a).

[61] We can consider $L_1 = \mathbb{Q}(\zeta_n)$, $L_2 = \mathbb{Q}(\zeta_m)$ and $L_1L_2 = \mathbb{Q}(\zeta_n, \zeta_m)$.

[62] LCM - least common multiple. For instance multiples for 4 are $4, 8, 12, \ldots$. Multiples for 6 are $6, 12, 18, \ldots$. Thus $LCM(4, 6) = 12$.

[63] See example 7.12 where we got if $([L_1 : K], [L_2 : K]) = (n, m) = 1$ then L_1 and L_2 are linearly disjoint.

[64] and also by Fundamental theorem of cyclic groups (Theorem A.24)

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 2.12).

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 8.2. *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 8.3 (Polynomial solvable by radicals)**.** $P \in K[X]$ is called solvable by radicals if exists a E - Extension solvable by radicals (Definition 8.1) and containing all roots of P.

So more precisely, it would say that the equation, $P = 0$ is solvable by radicals.

Property 8.4. *1. Composite extension (Definition 7.7) 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 (Definition 5.18) E containing L and solvable by radicals.

Proof. For the first property (the proof is missing in the lectures): let $L = L_1L_2$ where L_1 and L_2 are solvable i.e. $L_1 = K(\alpha_1, \dots, \alpha_n), L_2 = K(\beta_1, \dots, \beta_m)$ with α_i, β_j which satisfies properties from definition 8.1. In the case we can assume $L = L_1L_2 = K(L_1 \cup L_2) = K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ and all properties from definition 8.1 will also be satisfied. Therefore the composite extension $L = L_1L_2$ is also solvable.

For the second property: Indeed take a composite of all images of L in $\bar{K}$ or, in other words, images of L by $Gal\left(\bar{K}/K\right)$. [1] □

[1] Lets prove by induction. For the first step we have that $K(\alpha)$ is solvable therefore $\exists d = \min\{j \mid \alpha^j \in K\}$. Let ζ_d is a root of unity i.e. root of $X^d - 1$ then by proposition 7.3, the $K(\zeta_d, \alpha) \supset K(\alpha)$ is a Galois extension and it has a finite degree ($\leq d \cdot d$).

Using induction hypothesis we have that if $K(\alpha_1, \dots, \alpha_i)$ is solvable then there exists a Galois extension of finite degree $F = K(\beta_1, \dots, \beta_k)$ that is solvable and $K(\alpha_1, \dots, \alpha_i) \subset F$. By Galois correspondence (Theorem 6.7) (item 2b) we have that $\forall g \in G = Gal\left(\bar{K}/K\right)$:

$$g(F) = F.$$

Lets consider $F(\alpha_{i+1})$. As we know (by induction hypothesis) $K(\alpha_1, \dots, \alpha_i, \alpha_{i+1})$ is solvable i.e. $\exists d = \min\{k \mid \alpha_{i+1}^k \in K(\alpha_1, \dots, \alpha_i)\}$ therefore α_{i+1} is a root of the following irreducible polynomial $X^d - a$ where $a = \alpha_{i+1}^d$. The Galois group $G = Gal\left(\bar{K}/K\right)$ permutes the roots of the polynomial and as result $\forall g \in G$

$$L_g = g(F(\alpha_{i+1})) = F(\beta_g),$$

where $\beta_g = g(\alpha_{i+1})$ is a root of $X^d - a$. I.e. L_g is solvable. If we take a composite extension $L \cup_{g \in G} L_g$ then by first property of 8.4 it will be solvable but as soon as L is the image of all $g \in G$ then $\forall g \in G : g(L) = L$ and by Galois correspondence (Theorem 6.7) (item 2b) the extension L is Galois. L is a splitting field of $X^d - a$ (because it contains all its roots) but by theorem 2.7 it has finite degree: $[L : F] \leq d!$.

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 8.5 (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 (Definition A.13) of G_{i-1} and the Quotient group (Definition A.15) G_{i-1}/G_i is an Abelian group (Definition A.38).

Example 8.6 (Group of permutations S_3)**.** *Consider S_3 - the group of permutations (see also example A.54). It's solvable because $S_3 \supset A_3 \supset \{e\}$.*

We have $|S_3/A_3| = 2$ (see example A.55) i.e. S_3/A_3 is cyclic of order 2. $|A_3| = 3$ i.e. A_3 - cyclic of order 3. [2]

Example 8.7 (Group of permutations S_4)**.** *Consider S_4 - the group of permutations (see also example A.54). It's solvable because $S_4 \supset A_4 \supset K \supset \{e\}$, where K - is a subgroup* [3] *of double transpositions (see example A.47 for permutation cycles notation):*

$$K = \{e, (12)(34), (13)(24), (14)(23)\}.$$

A double transposition is a product of two Transposition (Definition A.58)s 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. [4]

$K \triangleleft A_4$, $|A_4/K| = 3$, i.e. A_4/K is cyclic of order 3. [5]

K is Abelian group (Definition A.38) 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 8.8. *If G is solvable and $H \subset G$ is a subgroup of G then H is solvable.*

[2] As it was mentioned at [60] there is only one group of order 3. We also have (with theorem A.41) that A_3 is Abelian group (Definition A.38)

[3] There is a well known Klein four group V_4 [61] - the only non-cyclic group of order 4. It also denoted as K_4. We have already seen it at example 7.1.

[4] i.e. theorem A.41 gives us that S_4/A_4 is Abelian group (Definition A.38)

[5] i.e. theorem A.41 gives us that A_4/K is Abelian group (Definition A.38)

Proof. Indeed $G_i \cap H$ gives a filtration with required property. [6] □

Property 8.9. *If G is solvable and $H \lhd G$ 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 $\pi(G_i)$ gives a filtration $(G/H)_i$ on G/H with required properties. [7] □

Property 8.10. *If $H \lhd G$, H and G/H are solvable then G is solvable.*

[6] We have $H_i = G_i \cap H$ and as soon as $G_i \lhd G_{i-1}$ we also get $H_i \lhd H_{i-1}$. Really $\forall h \in H_{i-1}$ we have $h \in G_{i-1} \cap H \subset G_{i-1}$. Thus, using normality (see definition A.13) $G_i \lhd G_{i-1}$,

$$hG_i = G_i h.$$

The last equation also holds for any subset of G_{i-1} and especially for $H_i = G_i \cap H \subset G_i$. I.e. $\forall h \in H_{i-1} : hH_i = H_i h$ or in other words, $H_i \lhd H_{i-1}$.

We have that G_{i-1}/G_i is an Abelian group (Definition A.38) and now we have to prove that the Quotient group (Definition A.15) H_{i-1}/H_i is abelian. $\forall h' \in H_{i-1}/H_i, \exists h_{i-1} \in H_{i-1}$ such that $h' = \{h_{i-1}, H_i\}$. From other hand $h_{i-1} \in G_{i-1}$ and $H_i \subset G_i$ therefore we can associate with h' the $g' = \{h_{i-1}, G_i\} \in G_{i-1}/G_i$. I.e. we just got an injection $f : H_{i-1}/H_i \xrightarrow[h' \to g']{} G_{i-1}/G_i$. Obviously we have $\forall h', h'' \in H_{i-1}/H_i$ the following relation

$$f(h'h'') = g'g'' = f(h')\, f(h''),$$

where $g'' = \{h'', G_i\}$ and $g'g'' = \{h'h'', G_i\}$. Therefore f is Homomorphism (Definition A.126). Thus $\forall a, b \in H_{i-1}/H_i$ we have $f(ab) = f(a)f(b)$, but as soon as G_{i-1}/G_i is abelian, $f(a)f(b) = f(b)f(a) = f(ba)$, or, using property of homomorphism, one can get that $ab = ba$ i.e. H_{i-1}/H_i is an Abelian group (Definition A.38) and as result H is solvable.

[7] We can associate each element $g \in G$ with $\bar{g} \in G/H$ via the following map: $\pi : G \xrightarrow[g \to \bar{g}]{} G/H$. I.e. $\pi(g) = \bar{g} = gH$. Thus we also have $\pi(G_i) = \bar{G}_i = G_i H$. Lets prove that $\bar{G}_i$ forms the required filtration i.e. that $\bar{G}_i \lhd \bar{G}_{i-1}$ and $\bar{G}_{i-1}/\bar{G}_i$ is Abelian group (Definition A.38).

For normality (see definition A.13) prove we have that $G_i \lhd G_{i-1}$ i.e. $\forall g \in G_{i-1} : gG_i = G_i g$ but $\forall \bar{g} \in \bar{G}_{i-1}$ we have

$$\bar{g}\bar{G}_i = gHG_iH$$

but $H \lhd G$ i.e. $\forall g' \in G_i \subset G : g'H = Hg'$ therefore

$$\bar{g}\bar{G}_i = gG_iH = G_igH = G_igHH = G_iHgH = \bar{G}_i\bar{g}$$

that finished the normality proof.

For the abelian quotient proof we have that G_{i-1}/G_i is Abelian group (Definition A.38) therefore $\forall a, b \in G_{i-1} : abG_i = baG_i$. Using the fact that H is a Normal subgroup

Proof. Put togeter the filtration H_i and $\pi^{-1}\left((G/H)_j\right)$ (see (8.1) for π definition). [8] □

The following property is not a part of the lectures but it's required for the property 8.12 proof

Property 8.11. *If G is finite Abelian group (Definition A.38) than G is solvable and there exists a finite filtration with cyclic quotients for G.*

Proof. Accordingly theorem A.45) each finite Abelian group (Definition A.38) G can be represented as

$$G = K_1 \oplus K_2 \oplus \cdots \oplus K_{n-1} \oplus K_n,$$

(Definition A.13) one can get

$$\begin{aligned} \bar{a}\bar{b}\bar{G}_i = aHbHG_iH = abG_iH = baG_iH = \\ = baG_iHH = baHG_iH = baHHG_iH = bHaHG_iH = \\ = \bar{b}\bar{a}\bar{G}_i, \end{aligned}$$

i.e. $\bar{G}_{i-1}/\bar{G}_i$ is Abelian group (Definition A.38).

[8] $\forall \bar{g} \in \bar{G} = G/H$ we can consider it as a set of elements: $\bar{g} = \{\forall h \in H : hg\}$ where $g \in G$. If we combine then we will get the following: $\cup_g \bar{g} = G$. We also have

$$GH = \cup_g \bar{g}H = \cup_g gHH = \cup_g gH = \cup_g \bar{g} = G. \tag{8.2}$$

Thus from $\bar{G}_i \lhd \bar{G}_{i-1}$ one can get $\forall \bar{g} \in \bar{G}_{i-1} : \bar{g}\bar{G}_i = \bar{G}_i\bar{g}$ or in other words (with $G_{i-1} = \cup_{\bar{g}\in\bar{G}_{i-1}}\bar{g}$) $\forall g \in G_{i-1}$ we have the following

$$gG_{i-1} = gHG_{i-1}H = \bar{g}\bar{G}_{i-1} = \bar{G}_{i-1}\bar{g} = G_{i-1}HgH = G_{i-1}HHg = G_{i-1}g,$$

i.e. $G_i \lhd G_{i-1}$. As result the filtration

$$\{e\} = \bar{H} \lhd \cdots \lhd \bar{G}_i \lhd \bar{G}_{i-1} \lhd \cdots \lhd \bar{G}_0 = \bar{G}$$

produces the following one

$$H \lhd \cdots \lhd G_i \lhd G_{i-1} \lhd \cdots \lhd G_0 = G. \tag{8.3}$$

If $\bar{G}_{i-1}/\bar{G}_i$ is abelian, i.e. $\forall \bar{a}, \bar{b} \in \bar{G}_{i-1}$: $\bar{a}\bar{b}\bar{G}_i = \bar{b}\bar{a}\bar{G}_i$, we can get the following $\forall a, b \in G_{i-1}$ (as soon as (8.2) gives us $G_i = G_iH$)

$$\begin{aligned} abG_i = abG_iH = abG_iHH = abHG_iH = abHHG_iH = aHbHG_iH = \\ = \bar{a}\bar{b}\bar{G}_i = \bar{b}\bar{a}\bar{G}_i = bHaHG_iH = baHG_iH = baG_iH = baG_i \end{aligned}$$

i.e. the Quotient group (Definition A.15) G_{i-1}/G_i is an Abelian group.

Finally combining (8.3) with H solvability one can get

$$\{e\} \lhd \cdots \lhd H_j \lhd H_{j-1} \lhd \cdots \lhd H \lhd \cdots \lhd G_i \lhd G_{i-1} \lhd \cdots \lhd G_0 = G$$

i.e. G is solvable.

where K_i is a Cyclic group (Definition A.23). If we denote

$$G_i = K_1 \oplus K_2 \oplus \cdots \oplus K_i$$

when, by property A.35, we can get

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G.$$

The gotten filtration has cyclic quotients because (see property A.36) $G_i/G_{i-1} = K_i$, where K_i is a cyclic group. □

Property 8.12. *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 (Definition A.38) is just a product of cyclic groups (see see The fundamental theorem of finitely generated abelian groups (Theorem A.45)). [9] □

Lets also look at another definition of solvable group

Definition 8.13 (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 (Definition A.20).

Remark 8.14. Definitions of solvable group 8.13 and 8.5 are equivalent.

[9] If exists a finite filtration of G with cyclic quotient then the G is solvable because Cyclic group (Definition A.23) is abelian (see theorem A.41).

The other direction is not so simple. Lets G is solvable then $G_i \triangleleft G_{i-1}$ and $G_{i-1}/G_i = K$ - abelian. The property 8.11 (that follows from The fundamental theorem of finitely generated abelian groups (Theorem A.45)) says us that there exists a finite filtration with cyclic quotients for K i.e.

$$\{e\} = K^{(n)} \triangleleft \cdots \triangleleft K^{(j)} \triangleleft K^{(j-1)} \triangleleft \cdots \triangleleft K_0 = K$$

where $K^{(j-1)}/K^{(j)}$ is cyclic. The Correspondence theorem (Theorem A.18) says us that $\forall K^{(j)}, \exists G_i^{(j)} \subset G_{i-1}$ with the same properties i.e. $G_i^{(j)} \triangleleft G_i^{(j-1)}$ and $G_i^{(j-1)}/G_i^{(j)}$ is cyclic. As result we can complete each $G_i \triangleleft G_{i-1}$ with

$$G_i = G_i^{(n)} \triangleleft \cdots \triangleleft G_i^{(j)} \triangleleft G_i^{(j-1)} \triangleleft \cdots \triangleleft G_i^{(0)} = G_{i-1}$$

and the result filtration will have cyclic quotients.

Proof. Our filtration with Commutator subgroup (Definition A.20)s $G \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(n)} = \{e\}$ is a filtration with abelian quotient because $G/[G,G]$ as well as $G^{(i)}/\left[G^{(i)},G^{(i)}\right] = G^{(i)}/G^{(i+1)}$ are Abelian group (Definition A.38)s. [10]

From the other hand if G/H is an Abelian group (Definition A.38) then $H \supset [G,G]$. [11] 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 8.15 (S_n solvability)**.** *S_n - the permutation of n elements (see example A.51) is not solvable for $n \geq 5$.*

Proof. It's easy to use definition 8.13. Main steps are the following

1. we know that $[S_n, S_n] = A_n$ - subgroup of even permutations (see definition A.50). It can be seen from the fact that any 3-cycle is a Commutator subgroup (Definition A.20) [12] and 3-cycles generate A_n [13]

[10] See definition A.22 and theorem A.21

[11] See theorem A.21

[12] Let $n \geq 3$ and $(a,b,c) \in S_n$ is a 3-cycle then (see example A.60)

$$\begin{aligned}(a,b,c) = (a,b,c)^2 = ((a,c)(a,b))^2 = \\ = (a,c)(a,b)(a,c)(a,b) = (c,a)^{-1}(b,a)^{-1}(a,c)(a,b) = \\ = (a,c)^{-1}(a,b)^{-1}(a,c)(a,b) = \\ = [(a,c),(a,b)] \subset [S_n,S_n]\,.\end{aligned}$$

[13] Any even permutation can be represented in a form of product of transpositions (see theorem A.61). The number of transpositions should be even. We have several cases there:

(a) The transpositions with different elements produces 2 3-cycles

$$(a,b)(c,d) = (a,b,c)(b,c,d).$$

Really

$$(a,b,c)(b,c,d) = \begin{array}{c} c \to d \\ d \to b \to c \\ b \to c \to a \\ a \to b \end{array} = (a,b)(c,d)$$

(b) The transpositions that have a same element produces a 3-cycle (see example A.60)

$$(a,c)(a,b) = (a,b,c)$$

As soon as we have even number of transposition then we will always have a translation to a product of 3-cycles for any product of transposition pairs.

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 8.7) - the subgroup of double transpositions. $A_4 \hookrightarrow A_n$ in many different ways. Because you can pick any 4 elements among 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 (Definition A.20) of A_n). [14] But if $n \geq 5$, they generate A_n. [15]

□

8.3 Galois theorem on solvability by radicals

The following claim missing in the lectures but it's important for the theorem 8.17 proof.

Claim 8.16. *Let $K \subset L \subset M$ and both M and L are Galois extension (Definition 5.18)s over K then*

$$\frac{Gal\,(M/K)}{Gal\,(M/L)} \cong Gal\,(L/K)\,.$$

[14] The double transposition consists of 4 elements. We can consider all permutations of the 4 elements only and ignore all others. For instance if $n = 6$ and we are interested in all double transpositions of $1, 2, 4, 5$. In the case we have to look at the following permutations:

$$\pi_{1,2,4,5} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ i_1 & i_2 & 3 & i_3 & i_4 & 6 \end{pmatrix}.$$

Note that we consider the even permutations only i.e. $\pi_{1,2,4,5} \in A_6$. From example 8.7 we know that the commutator of such permutations contains all double transpositions for $1, 2, 4, 5$: $\{e, (12)(45), (14)(25), (15)(24)\}$ (the elements $3, 6$ are not changed and disappeared in the commutator). Continue such way we can conclude that for any double transposition:

$$(i_1, i_2)(i_3, i_4) \in [A_n, A_n]$$

[15] Really if $n \geq 5$ then for any 3 elements a, b, c (which form a 3-cycle (a, b, c)) exist 2 elements e, d such that all elements a, b, c, d, e are different. Using the $(e, d)(e, d) = id$ one can get that 2 double transpositions $(a, b)(d, e)$ and $(d, e)(b, c)$ generate the 3-cycle (a, b, c):

$$(a, b)(d, e)(d, e)(b, c) = (a, b)(b, c) = (a, b, c).$$

I.e. any 3-cycle can be generated by 2 double transpositions. Therefore (see note 13) the whole A_n is generated by the double transpositions.

Thanks Arnur Nigmetov for the hint.

Proof. Consider the following group Homomorphism (Definition A.126)

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

The Galois correspondence (Theorem 6.7) theorem says that ϕ is a Surjection (Definition A.123) with kernel $Gal\left(L/F\right)$. Therefore by First isomorphism (Theorem A.131) theorem one can get the required statement. □

Theorem 8.17. *Let $P \in K[X]$. P is a Polynomial solvable by radicals (Definition 8.3) if and only if $Gal\left(P\right)$ is solvable. There $Gal\left(P\right)$ is (by definition) $Gal\left(F/K\right)$ where F is a Splitting field (Definition 2.6) of P over K.*

Proof. First of all lets proof that if $Gal\left(P\right)$ is solvable then P is solvable. Let $n = [F : K]$ and consider $L = K\left(\zeta_n\right)$ where ζ_n - n-th root of 1. Let $M = FL$ is a Composite extension (Definition 7.7). 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 (Definition 5.18) [16] and $Gal\left(M/L\right) \hookrightarrow Gal\left(F/K\right)$. [17] $\forall g \in Gal\left(M/L\right)$ leaves F invariant. [18] If $g\mid_F = id$ then $g = id$. Then the image in fact of this map is $Gal\left(F/F \cap L\right)$. [19] So $G = Gal\left(M/L\right)$ is solvable [20] i.e.

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$$

and G_i/G_{i+1} - cyclic [21] of order $n_i \mid n$. [22] 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, thus there is Kummer extension. [23] and

[16] Accordingly property 7.9 the composition of two Galois extensions will also be Galois.
[17] See theorem 7.13 where $L_1 = F, L_2 = L, L_1L_2 = M = FL$.
[18] $g(F) = F$ see Galois correspondence (Theorem 6.7) (point 2b)
[19] See theorem 7.13 where $L_1 = F, L_2 = L, L_1L_2 = M$.
[20] Using property 8.8 G is solvable as soon as $G \subset Gal\left(F/K\right)$ and $Gal\left(F/K\right)$ is solvable
[21] see property 8.12
[22] As soon as $G_i, G_{i+1} \subset G$ then using Lagrange (Theorem A.8) theorem one can get that $|G_i| \mid |G|$ as well as $|G_{i+1}| \mid |G|$ and therefore $|G_i/G_{i+1}| \mid |G|$. But $G \subset Gal\left(F/K\right)$, thus $|G| \mid |Gal\left(F/K\right)| = n$ and, as result, $|G_i/G_{i+1}|$ divides n.
[23] We have $M_i = M^{G_i}$ where

$$M_0 = M^{G_0} = M^G = M^{Gal(M/L)} = L$$

and

$$M_r = M^{G_r} = M^{\{e\}} = M.$$

Thus by Galois correspondence (Theorem 6.7), as soon as $G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$,

therefore $M_{i+1} = M_i\left(\sqrt[n_i]{a_i}\right)$ (see proposition 7.4). So $M = K(\zeta_n, \alpha_1, \ldots, \alpha_r)$ 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 (using property 8.4) that this is Galois. Then write $E = K(\alpha_1, \ldots, \alpha_r)$ where $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$. Then let $L = K(\zeta_n)$ where $n = LCM(\{n_i\})$ so $\forall n_i : n_i \mid n$. And take $M = LE$. We have $K(\alpha_1, \ldots, \alpha_{i-1}) \hookrightarrow K(\alpha_1, \ldots, \alpha_i)$ - cyclic extension of order n_i. We have $Gal(M/L)$ is solvable by this cyclic subgroups. $Gal(M/K)$ is also solvable since

$$Gal(M/L) \subset Gal(M/K)$$

and the quotient (see claim 8.16)

$$\frac{Gal(M/K)}{Gal(M/L)} \cong Gal(L/K)$$

which is abelian. [24] $Gal(F/K)$ is a quotient [25] of $Gal(M/K)$ thus it is solvable too. [26] □

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 8.18 (Not solvable polynomial of degree 5)**.** *Let $P \in \mathbb{Q}[X]$ 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 have the following "tower":

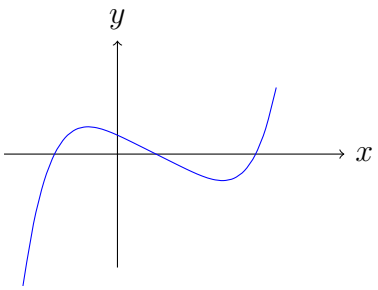
$$L = M_0 \subset M_1 \subset \cdots \subset M_{r-1} \subset M_r = M.$$

If we consider $M_i \subset M_{i+1}$ then we can get the following: M_i contains all n-th roots of unity as soon as $K(\zeta_n) = L \subset M_i$; M_{i+1} is Galois extension (Definition 5.18) over M_i with Galois group (Definition 5.22) G_i/G_{i+1} (we have $G_i = Gal(M/M_i)$, $G_{i+1} = Gal(M/M_{i+1})$ and therefore, by claim 8.16, $G_i/G_{i+1} = Gal(M_{i+1}/M_i)$) which is cyclic of order $n_i \mid n$ and as result M_{i+1} will be also be cyclic of the same order $n_i \mid n$. Therefore M_{i+1} is a Kummer extension (see section 7.2) over M_i,

[24] as result the property 8.10 gives us the solvability of $Gal(M/K)$

[25] ??? subset

[26] by the property 8.8



We claim that $Gal(P) = S_5$. *This is because*

1. $Gal(P)$ *contains the complex conjugation (we have 2 complex conjugated roots but Galois group (Definition 5.22) 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* [27]

2. *As soon as* P *is irreducible then* $Gal(P)$ *should act transitively (see definition A.31) on roots (see theorem 5.17). 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 (Theorem A.30))* $|G| = |Orb(x)|\,|G_x|$ *(*$Orb(x)$ *- is the Orbit (Definition A.27),* G_x *- Stabilizer subgroup (Definition A.29)) but the orbit has 5 elements* [28] *and therefore 5 divides the cardinality of* G. *This means, by Sylow (Theorem A.37) theorems, that our group contains something of order 5. But only 5-cycle has order 5 (see theorem A.9). But a 5-cycle and transposition generate* S_5 *(see corollary A.62). 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 8.19 (General equation of degree n)**.** *What's the general equation. It is the following*

$$X^n - T_1 X^{n-1} + T_2 X^{n-2} + \cdots + (-1)^n T_n,$$

[27] $(1,2) = 1 \to 2 \to 1$

[28] $|Orb(x)| = 5$ because there are 5 different roots that can be permuted by the Galois group.

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 $n!$, i.e. $[K(X_1, \ldots, X_n) : K] \leq n!$ (see theorem 2.7). On the other hand $K(T_1, \ldots, T_n) \subset K(X_1, \ldots, X_n)^{S_n}$ [29] so degree of the extension is $n!$ [30] 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 8.20 (Group representation)**.** Let G is a finite group. V is a Vector space (Definition A.107) over K. Representation of G is a Homomorphism (Definition A.126) $\rho : G \to GL(V)$ (where $GL(V)$ is the General linear group of a vector space (Definition A.114) i.e. the group of Automorphism (Definition A.129)s of the vector space V).

[29] This is because S_n permutes the roots, for instance $X_k \to X_l \to X_k$, but the equations for T_i are not changed during the transformation.

[30] We have that $S_n \subset Gal(K(X_1, \ldots, X_n)/K(T_1, \ldots, T_n))$ and therefore

$$[K(X_1, \ldots, X_n) : K(T_1, \ldots, T_n)] \geq |S_n| = n!.$$

Thus with $[K(X_1, \ldots, X_n) : K] \leq n!$ one can get that $[K(X_1, \ldots, X_n) : K(T_1, \ldots, T_n)] = n!$ and $[K(X_1, \ldots, X_n) : K] = n!$.

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 (Definition 5.22) $Gal\left(L/K\right)$: $\rho : G \to GL_K\left(L\right)$ - 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 8.21).

Definition 8.21 (Regular representation)**.** Let a vector space V has a basis indexed by elements of group G: e_g where $g \in G$. $\rho_{reg}\left(h\right)$ [31] acts by permutations: [32]

$$\rho_{reg}\left(h\right) e_g = e_{hg}.$$

We claim that the representation of Galois group is the regular representation. We have seen that (see proof of the theorem 5.11)

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

The $\bar{K}^n$ is a Direct sum (Definition A.43) of n ($n = |G = Gal\left(L/K\right)|$) copies of $\bar{K}$. The sum is indexed by the embeddings of L into $\bar{K}$. [33] Pick one $j : L \hookrightarrow \bar{K}$ and all others can be obtained by group Action (Definition A.26) $j \circ g, g \in G$. [34] So $\bar{K}^n$ has a basis indexed by G and the Action (Definition A.26) of G permutes the basis vectors. [35] So $L \otimes_K \bar{K} \cong \bar{K}^n \cong R$, where R is a Regular representation (Definition 8.21) of G over $\bar{K}$. In particular $\exists x \in L \otimes_K \bar{K}$ such that $gx \mid_{g \in G}$ forms a basis of $L \otimes_K \bar{K}$ over $\bar{K}$.

[31] where $h \in G$.

[32] $\rho_{reg}\left(h\right)$ is an Automorphism (Definition A.129) of V i.e.

$$\rho_{reg}\left(h\right) : V \xrightarrow[e_g \to e_{gh}]{} V.$$

[33] The embeddings are also noticed as the set of homomorphisms $Hom_K\left(L, \bar{K}\right)$. And $\bar{K}^n = \prod_{i=1}^{n} \bar{K}$ where $n = \left|Hom_K\left(L, \bar{K}\right)\right|$ (accordingly (5.2)).

[34] This is because the Galois group (Definition 5.22) acts transitively on the set of homomorphisms from L to $\bar{K}$ ($Hom_K\left(L, \bar{K}\right)$), see theorem 5.17.

[35] We have L is a Galois extension (Definition 5.18) i.e. (via Primitive element (Theorem 5.11) theorem) $\exists \alpha \in L$ such that $L = K\left(\alpha\right)$, where α is a root of a polynomial $P_{min}\left(\alpha, K\right)$ of degree $[L : K] = n$. The consider the set of the following vectors in $\bar{K}^n$:

$$e_i = \left(\phi_1(\alpha^{i-1}), \phi_2(\alpha^{i-1}), \ldots, \phi_n(\alpha^{i-1})\right),$$

where ϕ_j -distinct homomorphisms such that $\phi_j(\alpha) = \alpha_j$ - is another root of $P_{min}\left(\alpha, K\right)$.

[36] And, as result, the elements of G are linearly independent in the space of Endomorphism (Definition A.128)s $End_{\bar{K}}\left(L \otimes_K \bar{K}\right)$ [37]

Theorem 8.22 (Normal base)**.** *$\exists x \in L$ such that $\{gx \mid g \in G\}$ is a K basis of L.*

G are linearly independent in the space of Endomorphism (Definition A.128)s $End_K(L)$

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. [38] But this determinant is a polynomial in the coefficient,

---

The set is linearly independent:

$$\sum_{i=1}^{n} c_i e_i = \left(\sum_{i=1}^{n} c_i \alpha_1^{i-1}, \sum_{i=1}^{n} c_i \alpha_2^{i-1}, \ldots, \sum_{i=1}^{n} c_i \alpha_n^{i-1}\right) = \\ = (P(\alpha_1), P(\alpha_2), \ldots, P(\alpha_n)),$$

where $P(X) = \sum_{i=1}^{n} c_i X^{i-1}$. It can have $\alpha_1, \alpha_2, \ldots, \alpha_n$ as roots only if all $c_i = 0$ because the minimal polynomial $\forall \alpha_i$ has degree $n > n-1$. As result $\{e_i\}$ are linearly independent.

If we put the vectors into a matrix as rows we can get

$$A = \begin{bmatrix} \phi_1(1) & \phi_2(1) & \phi_3(1) & \ldots & \phi_n(1) \\ \phi_1(\alpha) & \phi_2(\alpha) & \phi_3(\alpha) & \ldots & \phi_n(\alpha) \\ \phi_1(\alpha^2) & \phi_2(\alpha^2) & \phi_3(\alpha^2) & \ldots & \phi_n(\alpha^2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \phi_1(\alpha^{n-1}) & \phi_2(\alpha^{n-1}) & \phi_2(\alpha^{n-1}) & \ldots & \phi_n(\alpha^{n-1}) \end{bmatrix}.$$

The columns are also linearly independent (as rows) and therefore

$$v_i = \left(\phi_i(1), \phi_i(\alpha), \ldots, \phi_i(\alpha^{n-1})\right) \tag{8.4}$$

is a basis of $\bar{K}^n$. If $g \in G$ such that $g(\alpha_i) = \alpha_j$ then

$$g(v_i) = g\left(1, \alpha_i, \ldots, \alpha_i^{n-1}\right) = \\ = \left(1, \alpha_j, \ldots, \alpha_j^{n-1}\right) = \left(\phi_j(1), \phi_j(\alpha), \ldots, \phi_j(\alpha^{n-1})\right) = v_j$$

[36] you can take one basis vector from (8.4): $x = v_i$

[37] See also theorem A.96 about linearly independents of elements of a group G

[38] We have $x = X_1 e_1 + \ldots X_n e_n$ where $X_i \in K$. $\forall g_l \in G : g_l(x) = \sum_i X_i g_l(e_i)$ because $g_l(X_i) = X_i$ (remember that $L^G = K$). For each $g_l(e_i)$ we can write

$$g_l(e_i) = \sum_j k_{ij}^{(l)} e_j \tag{8.5}$$

We have $k_{ij}^{(l)}$ are predefined (because $\{g_l\}$ and $\{e_i\}$ are predefined) elements of L and

which is not identically zero. [39] Well, why? Because if it was identically zero, it would remain identically zero also after the base changed to $\bar{K}$. [40] 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 ($P \neq 0$). And over an infinite field, only a polynomial which is identically 0 can vanish at every point. [41]

---

therefore X_i can only be changed.

We want $\{g_j(x)\}$ to be linearly independent set of elements from L. Therefore the equation

$$c_1 g_1(x) + \dots c_n g_n(x) = 0,$$

where $c_i \in K$, should holds only for $c_1 = c_2 = \dots = c_n = 0$. We also can write

$$c_1 \sum_j \left(\sum_i X_i k_{ij}^{(1)} \right) e_j + c_2 \sum_j \left(\sum_i X_i k_{ij}^{(2)} \right) e_j + \dots + \\ + c_n \sum_j \left(\sum_i X_i k_{ij}^{(n)} \right) e_j = \sum_j 0 e_j = 0$$

The equation can also be rewritten in the matrix form

$$\begin{bmatrix} \sum_i X_i k_{i1}^{(1)} & \sum_i X_i k_{i1}^{(2)} & \cdots & \sum_i X_i k_{i1}^{(n)} \\ \sum_i X_i k_{i2}^{(1)} & \sum_i X_i k_{i2}^{(2)} & \cdots & \sum_i X_i k_{i2}^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_i X_i k_{in}^{(1)} & \sum_i X_i k_{in}^{(2)} & \cdots & \sum_i X_i k_{in}^{(n)} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

The equation has non-trivial solutions only if

$$\det \left(\begin{bmatrix} \sum_i X_i k_{i1}^{(1)} & \sum_i X_i k_{i1}^{(2)} & \cdots & \sum_i X_i k_{i1}^{(n)} \\ \sum_i X_i k_{i2}^{(1)} & \sum_i X_i k_{i2}^{(2)} & \cdots & \sum_i X_i k_{i2}^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_i X_i k_{in}^{(1)} & \sum_i X_i k_{in}^{(2)} & \cdots & \sum_i X_i k_{in}^{(n)} \end{bmatrix} \right) \neq 0. \tag{8.6}$$

[39] The determinant(8.6) can always be written in the form of multi-variable polynomial $P \in L[X_1, \dots, X_n]$ i.e. the polynomial coefficients are from L.

[40] The element $g \in G$ acts on $l \otimes k \in L \otimes_K \bar{K}$ as follows $g(l \otimes k) = g(l) \otimes k$ (see proof for the theorem 4.13). Using proposition 4.11 we have $x = X_1 e_1 \otimes 1_{\bar{K}} + \dots X_n e_n \otimes 1_{\bar{K}}$ and $X_i \in \bar{K}$. With equation (8.5) we have

$$g_l(e_i \otimes 1_{\bar{K}}) = g_l(e_i) \otimes 1_{\bar{K}} = \sum_j k_{ij}^{(l)} e_j \otimes 1_{\bar{K}}$$

i.e. all $k_{ij}^{(l)}$ are the same as in the (8.6) and as result the polynomial coefficients will be the same (i.e. the polynomial will be identically zero).

[41] I.e. polynomial of the following polynomial ring $P \in L[X_1, \dots, X_n]$ can vanish at

Let me to clarify the point. $P \in K[X]$ has at most $\deg P$ roots. [42] 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. [43] So, our polynomial which is the determinant of the matrix, is non zero, as a polynomial of several variable because it does not have roots over algebraic closure $\bar{K}$. And so, it also does not have roots over K. So, there exists a point $x \in L$ (not anymore in $L \otimes_K \bar{K}$) such that $\det(\dots) \neq 0$ 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 the Galois group (Definition 5.22) is cyclic i.e. $G = \langle\sigma\rangle$ (see corollary 3.16). We have $id, \sigma, \dots, \sigma^{n-1}$ are linearly independent because they are linearly independent over $\bar{K}$. [44] Then the minimal polynomial of σ as an Endomorphism (Definition A.128) of L over K is $X^n - 1$. This is because a lower degree polynomial cannot vanish at σ since, the lower power of σ are linearly independent. [45] Therefore, as a $K[X]$-module with X acting by σ, [46] L is isomorphic to

$$L \cong K[X] / (X^n - 1).$$

This is a Cyclic module (Definition A.105) [47] and any generator x shall do i.e. $x, \sigma x, \dots, \sigma^{n-1}x$ form a basis. [48] □

---

every point only if it is identically zero $P = 0$.

[42] Therefore it is impossible to have each $k \in K$ as a root of the polynomial because in the case the number of roots $|K| = \infty > \deg P$.

[43] Let $P_n \in K_n = K[X_1, X_2, \dots, X_{n-1}, X_n]$ and we proved the statement for any $P_{n-1} \in K_{n-1} = K[X_1, X_2, \dots, X_{n-1}]$ i.e. if $\forall k_1, k_2, \dots, k_{n-1} \in K$ we have $P_{n-1}(k_1, k_2, \dots, k_{n-1}) = 0$ then $P_{n-1} = 0_K$.

We want to proof that if P_n vanishes for any choice of $k_1, \dots, k_n \in K$ then it is identically 0. Consider P_n as a polynomial of single variable X_n with coefficients from K_{n-1}. If the polynomial is 0 for every $k_n \in K$ then its coefficients are 0. But by the induction hypothesis they are identically 0 (as soon as they stays zero for any k_i choice). Thus the result polynomial is also identically zero: $P_n = 0_K$

[44] See theorem A.96.

[45] $\sigma^n = 1$ as soon as $G = \langle\sigma\rangle$ (cyclic group of order n). If $\exists m < n$ such that $\sum_{i=0}^{m} c_i \sigma^i = 0$ and $c_i \neq 0$ then the set $1, \sigma, \dots, \sigma^m$ is not linearly independent that is in contradiction with Dedekind (Theorem A.96) theorem. Thus the minimal polynomial for σ is $X^n - 1$.

[46] We consider L as a module over $K[X]$ where X acts on L as σ i.e. if $f(X) \in K[X]$ then $f(X) : L \xrightarrow[\alpha \to f(\sigma)(\alpha)]{} L$ [3], for instance $f(X) = X^2 + X + 1$ acts on $\alpha \in L$ as follows: $\sigma^2(\alpha) + \sigma(\alpha) + \alpha$.

[47] By claim A.106 there is a cyclic $K[X]$-module. I.e. if $x \in L$ is the generator then $L = K[X]x$.

[48] As soon as X acts as σ on L and $\sigma^n - 1 = 0$ then any element from $K[X]$ can be represented as follows $k_0 + k_1 X + \dots + k_{n-1} X^{n-1}$, where $k_i \in K$. Let $x \in L$ is the

8.6 Relation with coverings

Remark 8.23. If L is a finite Galois extension (Definition 5.18) of K then $L \otimes_K L$ is a direct sum of fields [49] 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 (see examples 4.16 and 5.1)

$$\begin{aligned} L \otimes_K L \cong L \otimes_K K[X]/(X - \alpha_1) \cdot \cdots \cdot (X - \alpha_n) \cong \\ \cong L[X]/(X - \alpha_1) \cdot \cdots \cdot (X - \alpha_n) \cong \\ \cong L[X]/(X - \alpha_1) \times \cdots \times L[X]/(X - \alpha_n) \cong \\ \cong L \times \cdots \times L \end{aligned}$$

that is a product of copies of L permuted by Galois action □

In topology one has Galois covering $Y \to X$. G acts on Y, X is a Quotient of the group action (Definition A.33). The covering is characterized by the property that $Y \times_X Y = \sqcup_{g \in G} Y_g$ (is a Disjoint union (Definition A.2)), $Y_g = \{(y, gy)\}$. [50]

---

generator of L as $K[X]$-module thus one can get

$$\begin{aligned} L = \left(k_0 + k_1 X + \cdots + k_{n-1} X^{n-1}\right)\Big|_{X=\sigma} x = \\ = k_0 x + k_1 \sigma(x) + \cdots + k_{n-1} \sigma^{n-1}(x) \end{aligned}$$

i.e. $x, \sigma x, \ldots, \sigma^{n-1} x$ is a K basis of L.

[49] see also definition A.102

[50] ??? add an explanation

Chapter 9

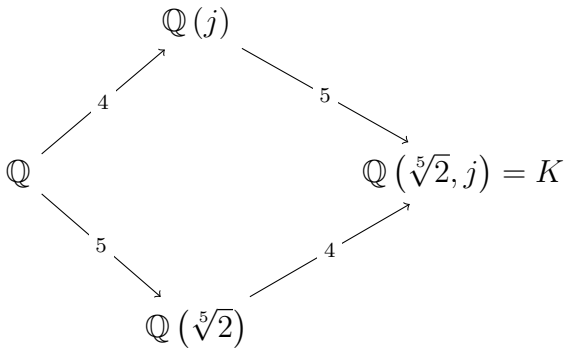
Ring extensions, norms and traces, reduction modulo p

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 (Definition 2.6) of P. We have already done the work for several types of polynomials: n-th cyclotomic polynomial (Definition 6.15)s, Kummer extensions (section 7.2) and so on.

Sometimes, if our polynomial is a kind of combination of them, 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 the Galois group (Definition 5.22). If K is the splitting field of the polynomial then we have the following towers:



From that we know we can conclude that it follows that our Galois group, contains a normal cyclic subgroup of a order 5: $\mathbb{Z}/5\mathbb{Z}$. [1] And then the quotient is the Galois group of cyclotomic extension [2] , so this is $(\mathbb{Z}/5\mathbb{Z})^{\times}$. So this is a group of order 20. [3] 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 (Definition A.72), 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 (Definition A.84) $P \in A[X]$.

So one can write the following relation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0, a_i \in A.$$

---

[1] We have the following towers: $\mathbb{Q} \subset \mathbb{Q}(j) \subset \mathbb{Q}\left(j, \sqrt[5]{2}\right) = K$, where $\mathbb{Q}(j)$ and $\mathbb{Q}\left(j, \sqrt[5]{2}\right)$ are Galois extension (Definition 5.18)s. By Galois correspondence (Theorem 6.7) one can get that

$$Gal\left(K/\mathbb{Q}(j)\right) \triangleleft Gal\left(K/\mathbb{Q}\right) = Gal\left(P\right).$$

As soon as (see theorem 5.19),

$$|Gal\left(K/\mathbb{Q}(j)\right)| = [K : \mathbb{Q}(j)] = 5,$$

the $Gal(P)$ has a normal subgroup of order 5.

[2] The quotient is

$$Gal\left(K/\mathbb{Q}\right)/Gal\left(K/\mathbb{Q}(j)\right).$$

It has order $20/5 = 4$ and therefore it is $(\mathbb{Z}/5\mathbb{Z})^{\times}$. It is also (see claim 8.16) $Gal\left(\mathbb{Q}(j)/\mathbb{Q}\right)$

[3] There is a General affine group: $Gal(P) \cong GA(1,5) \triangleleft S_5$ [8, 7]

Example 9.2. *$\frac{1}{2}$ is not integral element over $\mathbb{Z}$ but $\sqrt{2}$ is an Integral element (Definition 9.1) over $\mathbb{Z}$.*

This is because the polynomial in the definition 9.1 is monic i.e. the leading coefficient is 1.

Lemma 9.3. *The following conditions are equvivalent*

1. *α is integral over A.*
2. *$A[\alpha]$ is a finitely generated A-module (see definition A.104).*
3. *$A[\alpha] \subset C \subset B$ where C is a a finitely generated A-module (see definition A.104). I.e. $A[\alpha]$ is contained in a finitely generated A-module.*

Proof. $1 \to 2 \to 3$ is easy [4] and we will concentrate on $3 \to 1$.

Let $x_1, \dots, x_r$ generate C as A-module then we can write [5]

$$\alpha x_i = \sum \lambda_{ij} x_j,$$

where $\lambda_{ij} \in A$. Consider the matrix $\Lambda = \{\lambda_{ij}\}$ and let $M = \alpha \cdot id - \Lambda$. Then

$$M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0.$$

Thus (see (4.3) at theorem 4.23 proof)

$$\det M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0.$$

Therefore $\det M \cdot C = 0$ but $1 \in C$ thus $\det M = 0$. [6] The equation $\det M = 0$ can be considered as a polynomial with α as a root. [7] □

[4] $1 \to 2$ is really easy because the finite set $\{1, \alpha, \dots, \alpha^{n-1}\}$ generates $A[\alpha]$ i.e. $\forall x \in A[\alpha], \exists \{x_i\} \subset A$ such that $x = \sum_{i=0}^{n-1} x_i \alpha^i$.

$2 \to 3$ is even more easy because $C = A[\alpha]$ will work.

[5] As soon as $\alpha x_i \in C$ is an element of C that can be written as a linear combination of $x_1, \dots, x_r$ with coefficients from A.

[6] There is a question why do we need $\det M \cdot C = 0$, may be we can directly write $\det M = 0$? Staff provided a good example why it's necessary: Sending generators to zero is not sufficient for having zero determinant. For example, consider a ring A, its ideal $I \subset A$ and A/I as a A-Cyclic module (Definition A.105) i.e. module with one generator. If $x \in A$ is the generator then we can just say that $\det Mx \in I$ and as result $\det M$ not necessary to be zero.

[7] The polynomial will be a Monic polynomial (Definition A.84) because the matrix element can have α with coefficient equal 1.

9.2 Integral extensions, integral closure, ring of integers of a number field

9.2.1 Integral extensions and integral closure

Definition 9.4 (Integral extension)**.** Let $A \subset B$. B is integral over A if $\forall \alpha \in B$, α is an Integral element (Definition 9.1) over A.

The following proposition is not a part of the lectures but it is required for propositions 9.6 and 9.7 proof.

Proposition 9.5. *Let A is a sub-ring of C and $\alpha_1, \alpha_2, \ldots, \alpha_n \in C$, α_1 is an integral over A, α_2 is an integral over $A[\alpha_1]$, and so on, α_n is an integral over $A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}]$ then $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is a finitely generated A module.*

Proof. Lets proof by induction. The case $n = 1$ follows directly from lemma 9.3.

Induction hypothesis gives us that $B = A[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}]$ is a finitely generated A module and we have to prove that $S = A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is a finitely generated A module.

For B as a finitely generated A module we have

$$B = \sum_i Ab_i,$$

but $S = B[\alpha_n]$ is a finitely generated B module (thanks lemma 9.3) and therefore

$$S = \sum_j Bs_j$$

and as result

$$S = \sum_{ij} Ab_i s_j = \sum_{ij} Ak_{ij}$$

where $b_i s_j = k_{ij} \in S$ form a finite set of generators for S. □

Proposition 9.6. *Let $A \subset B \subset C$. B integral over A, C integral over B then C is an Integral extension (Definition 9.4) over A.*

Proof. Proof is left as an exercise. [8] □

[8] Let $x \in C$ then

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0,$$

where $b_i \in B$. Thus x is an integral element over $A[b_0, b_1, \ldots, b_{n-1}]$. We also have that B is integral over A therefore b_i is an integral over A. As result we have b_0 is integral over A, b_1 is integral over $A[b_0]$, and so on x is integral over $A[b_0, b_1, \ldots, b_{n-1}]$. As result with proposition 9.5 we have that $A[b_0, b_1, \ldots, b_{n-1}, x]$ is a finitely generated A module and as $A[x] \subset A[b_0, b_1, \ldots, b_{n-1}, x]$, the lemma 9.3 gives us that x is an integral element over A.

Proposition 9.7. *B is a finitely generated over A as a module (see definition A.104) if and only if $B = A[\alpha_1, \dots, \alpha_r]$ where each α_i is an Integral element (Definition 9.1) over A.*

Proof. Proof is left as an exercise [9] □

Proposition 9.8. *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.104). This follows directly from lemma 9.3. It contains $\alpha+\beta$ and $\alpha\beta$ and by lemma 9.3 the $\alpha + \beta$ and $\alpha\beta$ are integral over A. But this is exactly we need to proof. [10] □

Definition 9.9 (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 (Definition A.93) $\mathrm{Frac}(A)$.

Example 9.10. *$\mathbb{Z}$ is Integrally closed (Definition 9.9).* [11]

Remark 9.11. More generally any Unique factorization domain (Definition A.91) is Integrally closed (Definition 9.9).

Proof. Let A be a Unique factorization domain (Definition A.91) 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

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + a_1\frac{p}{q} + a_0 = 0.$$

[9] If α_i is an integral over A then it also an integral over $A[\alpha_1, \alpha_2, \dots, \alpha_{i-1}]$ and therefore by proposition 9.5, $A[\alpha_1, \alpha_2, \dots, \alpha_r] = B$ is finitely generated A-module.

Let B is finitely generated A module i.e. $B = \sum_{i=1}^{r} \alpha_i x_i$, where $\alpha_i \in B$ - the module generators and $x_i \in A$. If we look at any α_i we can notice that $A[\alpha_i] \subset B$ - finitely generated A module and therefore by lemma 9.3, α_i is an integral element. We also have (from definition A.104) that $\forall b \in B, \exists\{x_i\} \in A$ such that $b = \sum_{i=1}^{r} \alpha_i x_i$. Therefore $B = A[\alpha_1, \alpha_2, \dots, \alpha_r]$.

[10] $A[\alpha + \beta] \subset A[\alpha, \beta]$ and as soon as $A[\alpha, \beta]$ - finetely generated A module then $\alpha + \beta$ is an integral element by lemma 9.3.

Same result can be got for $\alpha\beta$ from the following inclusion: $A[\alpha\beta] \subset A[\alpha, \beta]$

[11] $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. An arbitrary element $q \in \mathbb{Q}$ is an integral element over $\mathbb{Z}$ if and only if $q \in \mathbb{Z}$. For example $5 \in \mathbb{Z} \subset \mathbb{Q}$ is integral over $\mathbb{Z}$ as a root of a monic polynomial $P = X - 5$. But $\frac{5}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$ because it is a root of a non-monic polynomial $P = 2X - 5$.

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 $q \mid p^n$ [12] which is in contradiction with $(p, q) = 1$. As result we have that q is invertible and therefore $x \in A$. [13] □

9.2.2 Ring of integers in a number field

Definition 9.12 (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 (Definition 9.12) and $[K : \mathbb{Q}] = N$.

Definition 9.13 (Ring of integers)**.** Let K is a Number field (Definition 9.12). 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 9.14. *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 (Definition A.84) $Q \in \mathbb{Z}[X]$. 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 (Equation 1.29) lemma, we conclude that both $P_{min}, R \in \mathbb{Z}[X]$. [14] □

---

[12] This is because we have

$$p^n = q\left(-a_n p^{n-1} - qa_{n-1} p^{n-2} - \cdots - q^{n-2} a_1 p - q^{n-1} a_0\right)$$

and

$$\left(-a_n p^{n-1} - qa_{n-1} p^{n-2} - \cdots - q^{n-2} a_1 p - q^{n-1} a_0\right) \in A$$

[13] $q^{-1} \in A$ and $x = \frac{p}{q} = pq^{-1} \in A$.

[14] I.e. we can always write

$$Q = mnP_1 R_1$$

9.3 Norm and trace

9.3.1 Norms and traces

(The material was given inside the proof of theorem 9.20 and can be considered as a recall. The remarks 9.15 and 9.18 are not parts of the lectures and were given for better understanding the material)

Remark 9.15 (K embedding of E into the algebraic closure $\bar{K}$). Let $K \subset E \subset \bar{K}$. When we say about K embedding of E into the algebraic closure $\bar{K}$ we assume $\sigma \in Hom_K\left(E, \bar{K}\right)$ i.e. σ is a Homomorphism (Definition A.126) of K-algebra (Definition 1.1)s i.e. the map that preserves the structure and especially $\sigma(K) = K$ i.e. $\forall k \in K : \sigma(k) = k$.

If E is a normal extension then all such homomorphisms have the same image accordingly theorem 5.17. The image is E and therefore the homomorphisms can be considered as automorphisms i.e. $Gal\left(E/K\right) = Hom_K\left(E, \bar{K}\right)$.

Definition 9.16 (Norm)**.** Let $K \hookrightarrow E$ - finite separable field extension. Let $\alpha \in E$. Define the norm of alpha with respect to this extension as

$$\mathrm{N}_{E/K}\left(\alpha\right) = \prod_{\sigma_i : E \hookrightarrow \bar{K}} \sigma_i\left(\alpha\right)$$

i.e. we took a product by all K embeddings of E into the algebraic closure of K (see remark 9.15). And we also assume that E is finite and as result $i = 1, \ldots, r$.

---

where $P_1, R_1 \in \mathbb{Z}\left[X\right]$. Choose p is a prime divisor of mn we can write

$$\bar{P}_1 \bar{R}_1 = \bar{Q} = 0$$

where $\bar{Q} = Q \mod p$, $\bar{P}_1 = P_1 \mod p$, $\bar{R}_1 = R_1 \mod p$ thus $\bar{P}_1$ or $\bar{R}_1$ are equal to 0. Let $\bar{R}_1 = 0$ thus all coefficients of R_1 are divided by p i.e. $R_1 = \frac{R_2}{p}$ where $R_2 \in \mathbb{Z}\left[X\right]$. Therefore

$$Q = \frac{mn}{p} P_1 R_2$$

Continue this way we can conclude that

$$Q = P_s R_t,$$

where $P_s, R_t \in \mathbb{Z}\left[X\right]$. As soon as Q is monic then both P_s and R_t are monic. Using the fact that $P_s = z P_{min}$ where $z \in \mathbb{Z}$ we have $P_s\left(\alpha\right) = 0$ and therefore we can conclude that P_s is the minimal polynomial.

Definition 9.17 (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 (see remark 9.15). And we also assume that E is finite and as result $i = 1, \ldots, r$.

In the definitions 9.16 and 9.17 we assume that the extension E is Separable extension (Definition 3.26). If the extension is not separable then you have to take it to the power equal to the pure inseparable degree of E/K, [15] but for simplicity, we shall suppose that everything is separate.

Remark 9.18. We have $\mathrm{N}_{E/K}(\alpha) \in K$ and $\mathrm{Tr}_{E/K}(\alpha) \in K$

Proof. Let $g \in Gal(E/K)$. We have to prove that $g\left(\mathrm{N}_{E/K}(\alpha)\right) = \mathrm{N}_{E/K}(\alpha)$. In the case $\mathrm{N}_{E/K}(\alpha) \in K$ because $E^{Gal(E/K)} = K$.

The g just permutes the homomorphisms $Hom_K\left(E, \bar{K}\right)$ i.e. $\left|gHom_K\left(E, \bar{K}\right)\right| = \left|Hom_K\left(E, \bar{K}\right)\right|$. If this is not the truth then $\exists \sigma_i, \sigma_j, \sigma_k \in Hom_K\left(E, \bar{K}\right)$ such that $g\sigma_i = \sigma_k, g\sigma_j = \sigma_k$ and $\sigma_i \neq \sigma_j$. Therefore

$$\sigma_j = g^{-1}\sigma_k = g^{-1}g\sigma_i = \sigma_i$$

that is contradiction. By the field definition (A.89) the product in Norm (Definition 9.16) does not depend on the order and the result become the same after the permutation.

The same result is for Trace (Definition 9.17). □

Property 9.19. *1.* $\mathrm{N}_{E/K} : E^\times \to K^\times$ [16] *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.* [17]

[15] [11] p. 284 gives the following definitions for norm and trace in not separable case:

$$\mathrm{N}_{E/K}(\alpha) = \left(\prod_{\sigma_i : E \hookrightarrow \bar{K}} \sigma_i(\alpha)\right)^{[E:K]_i},$$
$$\mathrm{Tr}_{E/K}(\alpha) = [E:K]_i \sum_{\sigma_i : E \hookrightarrow \bar{K}} \sigma_i(\alpha),$$

where $[E:K]_i$ is Inseparable degree (Definition 3.27).

[16] $E^\times = E \setminus \{0\}$ and $K^\times = K \setminus \{0\}$

[17] The property statement is the truth i.e. there really should be K (not $\bar{K}$)(see remark 9.18).

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*

$$\mathrm{N}_{E/K} = \mathrm{N}_{F/K} \circ \mathrm{N}_{E/F}$$

and the same for trace

$$\mathrm{Tr}_{E/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{E/F}$$

[18]

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.118)*

5. α *integral over* $\mathbb{Z}$. *Then* $\mathrm{N}_{E/\mathbb{Q}}(\alpha), \mathrm{Tr}_{E/\mathbb{Q}}(\alpha)$ *are integers.* [19]

Proof. The first property is obvious from the definition. [20]

[18] Or in other words

$$\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_{F/K}\left(\mathrm{N}_{E/F}(\alpha)\right)$$

and

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right).$$

Lets also note [6] that the following expression does not make sense:

$$\mathrm{Tr}_{E/F}\left(\mathrm{Tr}_{F/K}(\alpha)\right)$$

because $\mathrm{Tr}_{E/F} : E \to F$ and $\mathrm{Tr}_{F/K} : F \to K$ (see remark 9.18). The same is valid for Norm (Definition 9.16).

[19] We have $K = \mathbb{Q}$ in the property.

[20] Let $\alpha, \beta \in E$ then

$$\mathrm{N}_{E/K}(\alpha\beta) = \prod_{\sigma_i : E \hookrightarrow \bar{K}} \sigma_i(\alpha\beta) =$$

$$= \prod_{\sigma_i : E \hookrightarrow \bar{K}} \sigma_i(\alpha)\sigma_i(\beta) = \mathrm{N}_{E/K}(\alpha)\mathrm{N}_{E/K}(\beta).$$

With remark 9.18 we can get that

$$\mathrm{N}_{E/K} : E^\times \to K^\times$$

If we take $a, b \in K, \sigma \in Hom_K\left(E, \bar{K}\right)$ then one can get that $\sigma(a\alpha) = a\sigma(\alpha)$. This is because a is fixed under every embedding of E over K ([11] page 286), see also remark 9.15.

Therefore one can get

$$\mathrm{Tr}_{E/K}(a\alpha + b\beta) = a\mathrm{Tr}_{E/K}(\alpha) + b\mathrm{Tr}_{E/K}(\beta)$$

I.e. there is a K-linear map of E to K (see remark 9.18).

The second one uses the following fact: $\sigma_i(\alpha)$ are roots of $P_{min}(\alpha, K)$. The Norm (Definition 9.16) 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 8.19).

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 $\{\tau_j \mu_i\}$. [21]

For the 4th property. Indeed if $x \in \ker T$, [22] that means $\mathrm{Tr}_{E/K}(xy) = 0, \forall y \in E$ (see definition A.118), but this can't be a case when $xy \in K \setminus \{0\}$ by definition 9.17 [23] $\mathrm{Tr}_{E/K}(xy) = [E : K]\, xy$. [24]

For the 5th property we know that

$$\mathrm{Tr}_{E/\mathbb{Q}}(\alpha) = \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}\left(\mathrm{Tr}_{E/\mathbb{Q}(\alpha)}(\alpha)\right) =$$
$$= \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}([E : \mathbb{Q}(\alpha)]\,\alpha) = [E : \mathbb{Q}(\alpha)]\,\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$$

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 $P_{min}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$. [25] □

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 [26] . Now this f_a is a a K-linear map. It's an Endomorphism (Definition A.128) of a vector space E/K, and the $\mathrm{Tr}_{E/K}(a)$ is the trace of

[21] We have $K \subset F \subset \bar{K}$, and (see remark 9.15):

$$\begin{cases} \tau_j : F \to \bar{K} \text{ such that } \forall k \in K : \tau_j(k) = k, \\ \mu_i : E \to \bar{K} \text{ such that } \forall f \in F : \mu_i(f) = f. \end{cases}$$

Lets extend homomorphism $\tau_j : F \to \bar{K}$ to the automorphism $\bar{K} \to \bar{K}$ and denote the result with the same τ_j ([11] p. 285). As result we have $\tau_j \mu_i : E \to \bar{K}$. We also have $\forall k \in K \subset F\ \mu_i(k) = k$ (as soon as $k \in F$) and therefore $\tau_j(\mu_i(k)) = \tau_j(k) = k$. Thus $\tau_j \mu_i \in Hom_K(E, \bar{K})$.

[22] $T : E \times E \to K$

[23] and by taking into consideration the following fact (see remark 9.15): if $xy \in K$ then $\sigma_i(xy) = xy$

[24] we proved that T has a trivial kernel i.e. only $x = 0$ is in the $\ker T$. There is one of definitions of the non-degenerate K-bilinear form (see definition A.118)

[25] Property 9.14 says that $P_{min}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$. But 2d item of the property 9.19 says that the Trace (Definition 9.17) is a coefficient of the polynomial i.e. $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \in \mathbb{Z}$

[26] Consider an easy case when $E = K(a)$. In the case a is a root of $P_{min}(a, K) = a_n + a_{n-1}X + \cdots + a_1 X^{n-1} + X^n$. We have the following basis $1, a, \ldots, a^{n-1}$. The basis

this endomorphism, and the $\mathrm{N}_{E/K}(a)$ is the determinant of this endomorphism.

9.3.2 Theorem about rings of integers

Theorem 9.20. *O_k is a finitely generated (see definition A.104) $\mathbb{Z}$-module that is a Free module (Definition A.100) of rank (see definition A.101) n, where $n = [K : \mathbb{Q}]$.*

Proof. If $e_1, \ldots, e_n$ 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 9.14). Therefore O_K contains a free $\mathbb{Z}$-submodule of rank n [27].

---

is transformed by multiplication via the following rules

$$\begin{cases} 1 \to a, \\ a \to a^2, \\ \vdots \\ a^{n-1} \to a^n = -a_n - a_{n-1}a - \cdots - a_1 a^{n-1}. \end{cases}$$

Therefore the Endomorphism (Definition A.128) matrix can be written as follows:

$$M = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & \cdots & -a_2 & -a_1 \end{bmatrix}$$

It can be easy seen (with 2d item of the property 9.19) that

$$\mathrm{Tr}(M) = -a_1 = \mathrm{Tr}_{E/K}(a)$$

and

$$\det(M) = (-1)^n a_n = \mathrm{N}_{E/K}(a).$$

[27] This is because $d_1 e_1, \ldots, d_n e_n$ are linearly independent and form a basis of a free $\mathbb{Z}$-module. The number n is the cardinality of the basis.

It can be proved by contradiction i.e. let there exists a set $\{c_i\}$ such that $\exists j : c_j \neq 0$ and

$$\sum_{i=1}^{n} c_i d_i e_i = 0,$$

as soon as $d_j \neq 0$ then $k_j = c_j d_j \neq 0$ and

$$\sum_{i=1}^{n} k_i e_i = 0,$$

i.e. $\{e_i\}$ are not linearly independent. This is in contradiction with the initial conditions.

What is the $\mathbb{Z}$-module this is a finitely generated Finitely generated abelian group (Equation A.44) and we know a lot of things about such groups. The Finitely generated abelian group (Equation A.44) is the same as finitely generated $\mathbb{Z}$-module. Any such group is isomorphic to (see theorem A.45)

$$\mathbb{Z}^n \oplus A,$$

where A is a finite group (torsion part). A subgroup $B \subset \mathbb{Z}^n$ is itself a free module ($B \cong \mathbb{Z}^m$) of rank $m \leq n$.

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 ($T : K \times K \to \mathbb{Q}$):

$$(x, y) \to \mathrm{Tr}_{K/\mathbb{Q}}(xy)$$

this is Non-degenerate bilinear form (Definition A.118) (see 4th property 9.19) therefore $\exists v_1, \dots, v_n$ - Dual basis (Definition A.116) ($\mathbb{Q}$-basis of K) and we have the property that $\mathrm{Tr}_{K/\mathbb{Q}}(e_i v_j) = \delta_{ij}$. [28]

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). [29] 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 $\{v_i\}$. □

[28] Lets consider the following map $T : K \times K \to \mathbb{Q}$. We can use it to construct a linear map by the following rule: $\forall x \in K$ we have $f_x(y) = T(x, y) : K \to \mathbb{Q}$. We have $f_{x+y} = f_x + f_y$ and $f_{ax} = a f_x$ i.e. the set $\{f_x\} = K^*$ is the linear space. The map $K \xrightarrow[x \to f_x]{} K^*$ is Surjection (Definition A.123) by the f_x construction. The map is also Injection (Definition A.124) as soon as the map $T : K \times K \to \mathbb{Q}$ is Non-degenerate bilinear form (Definition A.118) and as result the $f_x(y) = T(x, y)$ has a trivial kernel (if $x \neq 0$): $\ker f = \{0\}$. Therefore we can conclude that K^* is Dual space (Equation A.115). I.e. exists a set of elements $\{f_{v_j}\} \subset K^*$ which form the Dual basis (Definition A.116) to $\{e_i\}$ i.e. $f_{v_j}(e_i) = \delta_{ij}$. Each element f_{v_j} of dual space corresponds to $v_j \in K$. For such v_j we have:

$$\delta_{ij} = f_{v_j}(e_i) = T(v_j, e_i) = \mathrm{Tr}_{K/\mathbb{Q}}(v_j e_i).$$

[29]

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha e_i) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{j=1}^{n} \alpha_j v_j e_i\right) =$$

$$= \sum_{j=1}^{n} \alpha_j \mathrm{Tr}_{K/\mathbb{Q}}(v_j e_i) = \sum_{j=1}^{n} \alpha_j \delta_{ij} = \alpha_i$$

9.4 Reduction modulo a prime

Let $P \in \mathbb{Z}[X]$ is an irreducible polynomial with integer coefficients. K is a Splitting field (Definition 2.6) 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 [30]

$$A/pA \cong A \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} = A \otimes_{\mathbb{Z}} \mathbb{F}_p$$

there $A \otimes_{\mathbb{Z}} \mathbb{F}_p$ is a n-dimension vector space over $\mathbb{F}_p$ [31]. Maximal ideals of A/pA are in one-to-one correspondence with maximal ideals of A containing p. As we know (see theorem 4.23) there are only finitely many maximal ideal in a finite algebra over a 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. [32]

Lets consider a subgroup $D_i \subset G$ which stabilizes J_i (see definition A.29) i.e.

$$D_i = \{g \in G \mid gJ_i = J_i\}.$$

Let also $k_i = A/J_i$ - this is a field [33] and there is a finite extension of $\mathbb{F}_p$. [34] 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 (Definition 5.22). [35]

Theorem 9.21. *1. G acts transitively (see definition A.31) on $\{J_1, \ldots, J_r\}$ and the map $D_i \to Gal(k_i/\mathbb{F}_p)$ is a Surjection (Definition A.123) i. e.*

[30] see proposition 4.14 where $M = A, A = \mathbb{Z}$ and $I = p\mathbb{Z}$.

[31] As soon as $A = O_K$ is a free $\mathbb{Z}$-module of rank n (see theorem 9.20) then proposition 4.11 gives us that $A \otimes_{\mathbb{Z}} \mathbb{F}_p$ is a free $\mathbb{F}_p$-module with rank equal to n.

[32] Let J is an Ideal (Definition A.67) of A, then $AJ = J$ (i.e. $\forall a \in A, j \in J : aj \in J$). Let also $g \in G$ then $g(A) = A$ (see [11] p. 341) and

$$Ag(J) = g(A)\,g(J) = g(AJ) = g(J)$$

i.e. $g(J)$ is also an ideal of A.

[33] see theorem A.92

[34] We have that A is a $\mathbb{F}_p$-algebra. J_i is a Maximal ideal (Definition A.74) of A then by remark 4.22 we have that $k_i = A/J_i$ is also $\mathbb{F}_p$-algebra i.e. k_i is a field extension of $\mathbb{F}_p$ (see definition 1.4). The extension is finite as soon as A is finite.

[35] We can notice that both k_i and D_i are related to J_i because any $g^{(k)} \in Gal(k_i/\mathbb{F}_p)$ is an automorphism of k_i i.e. it should preserve $O_{k_i} = J_i$ (as soon as it is an injection). Or in other words any element of $Gal(k_i/\mathbb{F}_p)$ acts in the same way as elements of D_i (preserves J_i). See also theorem 9.21 about the map structure (it's surjection and in several situations is also bijection).

$D_i \twoheadrightarrow Gal\left(k_i/\mathbb{F}_p\right)$

2. *If the reduction* $\bar{P} = P \mod p$ *has no multiple roots then the map* $D_i \to Gal\left(k_i/\mathbb{F}_p\right)$ *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 $\forall g \in G, g\left(J_1\right) \neq J_i$ i.e. suppose that there is not a Transitive group action (Definition A.31). By Chinese remainder (Equation 4.20) theorem $\exists x \in A$ such that $x \equiv 0(\mod J_i), x \equiv 1(\mod g\left(J_1\right))\forall g \in G$. [36] Consider a product of all such things:

$$a = \prod_g gx$$

it's an integer $a \in \mathbb{Z}$. [37] But since $x \in J_i$ (remember that $\equiv 0 \mod J_i$) then a is also in J_i: [38] $a \in \mathbb{Z} \cap J_i = (p)$ [39] - 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 as soon as J_1 is a Prime ideal (Definition A.76) (see note 39). That is because if we have $\prod_k x_k \in J_1$ $(x_k = g_k(x))$ then $\exists i$ such that $x_i \in J_1$ but there is not a case in our construction. [40]

We still need to proof that $D_i \twoheadrightarrow Gal\left(k_i/\mathbb{F}_p\right)$. [41] We may assume that $i = 1$. By the Primitive element (Theorem 5.11) theorem $\exists z \in \mathbb{F}_p$ such that $k_1 = \mathbb{F}_p\left(z\right)$ i.e. z generates $k_i/\mathbb{F}_p$. By Chinese remainder (Equation 4.20) theorem $\exists y \in A$ such that $y \in J_i, i \neq 1, y \equiv z(\mod J_1)$. [42] 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.

[36] We have that all J_i are relatively prime (see note 39 below) and as result the map $\pi\left(a\right)$ from (4.2) is Surjection (Definition A.123) i.e. for any residuals and therefore for the chosen ones ($\equiv 0 \mod J_i$ and $\equiv 1 \mod J_1$) exists x that produces the residuals.

[37] This is because $\prod_g gx = \mathrm{N}_{A/\mathbb{Q}}\left(x\right)$, but by 5th item of property 9.19 one can get that such Norm (Definition 9.16) (in the definition of norm we have homomorphism but not automorphism but accordingly remark 9.15 it is not important as soon as A is a normal extension of $\mathbb{Q}$) is an integer.

[38] $a = \prod_g gx = x\prod_{g \neq id} gx$ and by ideal definition A.67 we can conclude that $a \in J_i$.

[39] We have J_i is a Maximal ideal (Definition A.74) and A is a Principal ideal domain (Definition A.73). Therefore by lemma A.78, J_i is a Prime ideal (Definition A.76) that contains $p \in \mathbb{Z}$, but the prime ideal in $\mathbb{Z}$ that contains p is (p) (see lemma A.77).

[40] We have $x \in J_i$ and $x_i \in J_1$ but x_i is obtained from x by applying an element from G i.e. $\exists g_i \in G$ such that $x_i = g_i(x)$. But if we consider a reverse element: $g = g_i^{-1}$ then $g(x_i) = x \in J_i$ that is in contradiction with $g(J_1) \neq J_i$.

[41] i.e. that there is a Surjection (Definition A.123) or in other words that $\forall \bar{g}_i \in Gal\left(k_i/\mathbb{F}_p\right), \exists d_i \in D_i$ such that $d_i \to \bar{g}_i$.

[42] I.e. using the same argument as in note 36 one can conclude that $\exists y \in A$ such that its residual are the following $\forall i \neq 1$: $\equiv 0 \mod J_i$ and $\equiv z \mod J_1$.

$Q \in \mathbb{Q}[X]$ [43] moreover the roots are Integral element (Definition 9.1)s over $\mathbb{Z}$ [44] and therefore the polynomial arguments are in $\mathbb{Z}$. [45]

Lets study $\bar{Q} = Q \mod J_1$. If $g \notin D_1$ then $\exists i$ such that $g(J_i) = J_1$ [46] and particularly $g(y) \in J_1$. Therefore for such g we have

$$\overline{X - g(y)} = X - g(y) \mod J_1 = X.$$

So we have for $\bar{Q} \in \mathbb{F}_p[X]$

$$\bar{Q} = \prod_{g \in G \setminus D_1} X \prod_{g \in D_1} \left(X - \overline{g(y)} \right),$$

but $\prod_{g \in D_1} \left(X - \overline{g(y)} \right)$ has z as a root [47] and D_1 acts transitively on its roots.

Now recall that z generates k_1 (i.e. $k_1 = \mathbb{F}_p(z)$). Thus an element of $Gal(k_1/\mathbb{F}_p)$ is determined by the image of z. [48] And we have an element of D_1 which sends z to any possible image of it. But this means that $D_1 \twoheadrightarrow Gal(k_1/\mathbb{F}_p)$

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 $\bar{\alpha}_i = \alpha_i \mod J_1$.

Lets $g \in D_1$ acts as id on k_1. Then, of course, $g(\bar{\alpha}_i) = \bar{\alpha}_i$. But $g(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\}$ and it can not be different from α_i since they will have diffeent reduction $\mod J_1$. So $\forall i, g(\alpha_i) = \alpha_i$ and therefore $g = id$. [49] Thus conclusion that $D_1 \cong Gal(k_1/\mathbb{F}_p)$.

By the same argument [50]

$$Gal(k_1/\mathbb{F}_p[\bar{\alpha}_1, \ldots, \bar{\alpha}_n]) = id$$

therefore $k_1 = \mathbb{F}_p[\bar{\alpha}_1, \ldots, \bar{\alpha}_n]$ i.e. k_1 is a splitting field. □

---

[43] $Q = P_{min}(y, \mathbb{Q})$.

[44] as soon as $y \in A = O_K$.

[45] Ekaterina also said that ??? as soon as $\mathbb{Z}$ is Integrally closed (Definition 9.9).

[46] If $g \notin D_1$ then $g^{-1} \notin D_1$ i.e. $g^{-1}(J_1) \neq J_1$ i.e. as soon as $g \in G$ permutes the ideals (see note 32) then $\exists i$ such that $g^{-1}(J_1) = J_i$ i.e. $g(J_i) = J_1$.

[47] Let $g = id \in D_1$ then $\overline{g(y)} = y \mod J_1 = z$

[48] Because we have bijection $g \to g(z)$.

[49] This proves injection of the map $D_1 \to Gal(k_1/\mathbb{F}_p)$ (see lecture 6 note 41).

[50] i.e. $\forall g \in Gal(k_1/\mathbb{F}_p[\bar{\alpha}_1, \ldots, \bar{\alpha}_n])$ and $\forall x \in \mathbb{F}_p[\bar{\alpha}_1, \ldots, \bar{\alpha}_n]$ we have $g(x) = x$ i.e. $g = id$.

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 $Gal\left(\bar{P}\right)$. [51] 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 (see corollary 3.16).

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 $\bar{P} = R_2 R_3$ where R_i is irreducible of degree i. Then the same argument, gives that $Gal(P)$ contains the permutation $(1,2)(3,4,5)$. [52]

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.

[51] See theorem 9.21 there $D_i \cong Gal(k_i/\mathbb{F}_p)$

[52] The $Gal(P)$ contains a subgroup of 2-cycle (associated with the first 2 roots) and a subgroup of 3-cycle (associated with the last 3 roots).

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.

Definition A.2 (Disjoint union)**.** Let [58] $\{A_i : i \in I\}$ be a family of sets indexed by I. The disjoint union of this family is the set

$$\sqcup_{i\in I} A_i = \cup_{i\in I} \{(x, i) : x \in A_i\}.$$

The elements of the disjoint union are ordered pairs (x, i). Here i serves as an auxiliary index that indicates which Ai the element x came from.

Example A.3 (Disjoint union)**.** *Let [58] we have 2 sets* $A_0 = \{1, 2, 3\}$ *and* $A_1 = \{1, 2\}$*. We can construct the following sets of pairs*

$$A_0^* = \{(1, 0), (2, 0), (3, 0)\},$$
$$A_1^* = \{(1, 1), (2, 1)\}$$

so

$$A_0 \sqcup A_1 = A_0^* \cup A_1^* = \{(1, 0), (2, 0), (3, 0), (1, 1), (2, 1)\}$$

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

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

A.2 Groups

Definition A.4 (Monoid)**.** The set of elements M with defined binary operation $\circ$ we will call as a monoid if the following conditions are satisfied.

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

Definition A.5 (Group)**.** Let we have a set of elements G with a defined binary operation $\circ$ that satisfied the following properties.

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

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

Therefore the group is a Monoid (Definition A.4) with inverse element property.

Example A.6 (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* $\forall a \in G$*:* $a \circ a = 0 = e$*.*

See also example A.17

Definition A.7 (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.8 (Lagrange). *For any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.*

Theorem A.9 (Finite group of prime order). *Let G is a finite group of prime order i.e. $|G| = p$, where p is prime number. Then G is a Cyclic group (Definition A.23).*

Proof. Let $g \in G$ such that $g \neq e$ then, by theorem A.8, we have $|\langle g \rangle| \mid |G|$. Thus $|\langle g \rangle| = p$ because $|G| = p$ and p is a prime number. As result we have $G = \langle g \rangle$ and therefore G is a cyclic group. □

Definition A.10 (Subgroup). Let we have a Group (Definition A.5) $(G, \circ)$. The subset $S \subset G$ is called as subgroup if $(S, \circ)$ is a Group (Definition A.5).

Definition A.11 (Proper subgroup). A proper subgroup of a group G is a Subgroup (Definition A.10) H which is a proper subset of G (i.e. $H \neq G$) [53]

Definition A.12 (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.13 (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 [47]

We also can write normality in the Coset (Definition A.12) notation as follows. $N \triangleleft G$ if $\forall g \in G : gN = Ng$.

Definition A.14 (Simple group). A simple group is a nontrivial group whose only Normal subgroup (Definition A.13)s are the trivial group and the group itself.

The definition taken from [52]

Definition A.15 (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 (Definition A.23) 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 [49].

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.

In other words the quotient group can be defined as a set of all left Coset (Definition A.12)s (they also equal to the right cosets as soon as N is a Normal subgroup (Definition A.13)):

$$G/N = \{aN : a \in G\}$$

See also example S_3/A_3 quotient group (Example A.55).

Theorem A.16 (Quotient group)**.** *If G is a group and $H \triangleleft G$ then the operation $aH \cdot bH = a \cdot H$ makes G/H a group with identity H and inverse element $(aH)^{-1} = a^{-1}H$.*

Proof. See [64] p. 33. □

Example A.17 (Quotient group)**.** *Consider [49] 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 (Definition A.38). There are only two Coset (Definition A.12)s: the set of even integers and the set of odd integers; therefore, the quotient group $\mathbb{Z}/2\mathbb{Z}$ is the Cyclic group (Definition A.23) 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.*

See also example A.6.

Theorem A.18 (Correspondence theorem)**.** *The correspondence theorem, sometimes referred to as the fourth isomorphism theorem or the lattice theorem, states that if N is a Normal subgroup (Definition A.13) of a group G, then there exists a bijection from the set of all subgroups A of G containing N, onto the set of all subgroups of the quotient group G/N. The structure of the subgroups of G/N is exactly the same as the structure of the subgroups of G containing N, with N collapsed to the identity element [22].*

Definition A.19 (Commutator)**.** The commutator of two elements, g and h, of a group G, is the element [20]

$$[g, h] = g^{-1}h^{-1}gh$$

Definition A.20 (Commutator subgroup)**.** The commutator subgroup or derived subgroup of a group is the subgroup generated by all the Commutator (Definition A.19)s of the group [21].

Theorem A.21 (About quotient group and commutator subgroup)**.** *Given a group G a Quotient group (Definition A.15) G/N is an Abelian group (Definition A.38) if and only if $N \supseteq [G, G]$ [21]*

Definition A.22 (Abelianization)**.** The quotient $G/[G, G]$ is an abelian group (as it follows from theorem A.21) called the abelianization of G or G made abelian. [21]

A.2.1 Cyclic group

Definition A.23 (Cyclic group)**.** A cyclic group or monogenous group is a group that is generated by a single element. Note that Group $\mathbb{Z}/2\mathbb{Z}$ (Table A.6) is a cyclic group. See example A.66.

Theorem A.24 (Fundamental theorem of cyclic groups)**.** *In abstract algebra, every subgroup of a Cyclic group (Definition A.23) is cyclic. Moreover, for a finite cyclic group of order n, every Subgroup (Definition A.10)'s order is a divisor of n, and there is exactly one subgroup for each divisor.This result has been called the fundamental theorem of cyclic groups [54]*

Theorem A.25 (About subgroups of a cyclic group)**.** *Let [15] $G = \langle a \rangle$ be a cyclic group.*

1. *Every subgroup S of G is cyclic*
2. *If $|G| = n$, then G has a unique subgroup of order d for each divisor d of n*

See example A.66

A.2.2 Group action

Definition A.26 (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 [39].

Definition A.27 (Orbit)**.** Consider [39] 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.28 (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 [14].

Definition A.29 (Stabilizer subgroup)**.** For every x in X, we define [39] 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.30 (Orbit-stabilizer theorem)**.** *If group G and the set the group acting X are finite then*

$$|G| = |Orb\,(x)|\,|G_x|$$

where $x \in X$, $G\,(x)$ - is the Orbit (Definition A.27), G_x - Stabilizer subgroup (Definition A.29).

Note: the result was got from [39] as orbit-stabilizer theorem + Lagrange (Theorem A.8) theorem

Definition A.31 (Transitive group action)**.** The action of G on X is called [39] 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.32 (Free group action)**.** The action of G on X is called [39] free if, given $g, h \in G$, the existence of an $x \in X$ with $g(x) = h(x)$ implies $g = h$.

Definition A.33 (Quotient of the group action)**.** Consider [39] a group G acting on a set X. The set of all Orbit (Definition A.27)s of X under the action of G is written as X/G, and is called the quotient of the action.

A.2.3 Direct product

Definition A.34 (Direct product)**.** Given groups G and H, the direct product $G \times H$ is defined as follows:

The underlying set is the Cartesian product, $G \times H$. That is, the ordered pairs (g, h), where $g \in G$ and $h \in H$. The binary operation on $G \times H$ is defined component-wise:

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2)$$

The resulting algebraic object satisfies the axioms for a group. See [26].

The direct product of 2 Abelian group (Definition A.38)s is also called Direct sum (Definition A.43)

Property A.35 (Direct product of groups)**.** *Let G_1, G_2 - Group (Definition A.5)s and $G = G_1 \times G_2$ - Direct product (Definition A.34) of the groups. Then*

1. *$G_1 \cong (G_1, 1_{G_2})$ and $G_2 \cong (1_{G_1}, G_2)$*
2. *G_1 and G_2 are Normal subgroup (Definition A.13)s in G*

See [26].

Property A.36 (Quotient of direct product)**.** *Let G_1, G_2 - Group (Definition A.5)s and $G = G_1 \times G_2$ - Direct product (Definition A.34) of the groups. Then*

$$G/G_1 \cong G_2$$

and

$$G/G_2 \cong G_1$$

Proof. Lets prove the first claim: $G/G_1 \cong G_2$ (the second one is analogous). Consider projection $\pi : G \xrightarrow[(g_1,g_2)\to(1_{G_1},g_2)]{} G_2$. The π is Homomorphism (Definition A.126). Really let $a = (a_1, a_2), b = (b_1, b_2) \in G$ where $a_1, b_1 \in G_1$, $a_2, b_2 \in G_2$:

$$\pi(a \cdot b) = \pi((a_1, a_2) \cdot (b_1, b_2)) =$$
$$= \pi((a_1 b_1, a_2 b_2)) = a_2 b_2 = \pi(a)\pi(b)$$

As result π is a Homomorphism (Definition A.126).

The π is also a Surjection (Definition A.123) because $\forall a_2 \in G_2\ \exists a \in G$ such that $\pi(a) = a_2$. Really we can use $a = (1_{G_1}, a_2)$.

Therefore by First isomorphism (Theorem A.131) theorem one can get

$$G/\ker\pi \cong G_2,$$

but $\forall g_1 \in G_1$ we have $(g_1, 1_{G_2}) \in \ker\pi$. And conversely $\forall k \in \ker\pi$ we have $k = (k_1, k_2)$ where $k_1 \in G_1$ and $k_2 = 1_{G_2}$. As result (see property A.35)

$$\ker\pi = (G_1, 1_{G_2}) \cong G_1.$$

Therefore

$$G/G_1 \cong G_2.$$

□

A.2.4 Sylow theorems

Corollary A.37 (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 [55]*

A.2.5 Abelian group

Definition A.38 (Abelian group)**.** Let we have a Group (Definition A.5) $(G, \circ)$. The group is called an Abelian or commutative if $\forall a, b \in G$ it holds $a \circ b = b \circ a$.

Theorem A.39 (About order of element of an Abelian group)**.** *If G is a finite Abelian group (Definition A.38) and m is the maximal order of the elements of G then the order of every element of G divides m*

Theorem A.40. *Let G is an Abelian group (Definition A.38) 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 (Theorem A.8) $m \mid n$ 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.39 $l \mid m$ i.e. $m = k_2 l$. Thus

$$g^n = (g^m)^{k_1} = \left(g^l\right)^{k_2 k_1} = e.$$

□

Theorem A.41 (Cyclic Group is Abelian)**.** *Let G be a Cyclic group (Definition A.23) then G is Abelian group (Definition A.38)*

Proof. As soon as $G = \langle g \rangle$ then $\forall x, y \in G, \exists n, m \in \mathbb{N}$ such that $x = g^n, y = g^m$. In the case

$$xy = g^n g^m = g^{n+m} = g^m g^n = yx,$$

i.e. G is abelian. □

Remark A.42 (Not every Abelian group is cyclic). The theorem statement cannot be reversed i.e. there exist abelian group that are not cyclic. For example well known Klein four group V_4 [61] that is an Abelian group (Definition A.38) but not Cyclic group (Definition A.23)

Definition A.43 (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 $b \in B$. [27] See also Direct product (Definition A.34).

Definition A.44 (Finitely generated abelian group)**.** An Abelian group (Definition A.38) $(G, +)$ is called finitely generated [34] if there exist finitely many elements $x_1, \ldots, x_s$ in G such that $\forall x \in G$:

$$x = n_1 x_1 + \cdots + n_s x_s \tag{A.1}$$

with $n_i \in \mathbb{Z}$. In this case we say that $\{x_1, \ldots, x_s\}$ is a generating set of G.

In the (A.1) we have the following:

$$n_i x_i = \underbrace{x_i + \ldots x_i}_{n_i \text{ times}}$$

Theorem A.45 (The fundamental theorem of finitely generated abelian groups)**.** *Every Finitely generated abelian group (Equation A.44) G is isomorphic to a Direct sum (Definition A.43) 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 [34].

Theorem A.46 (Simple subgroup of an abelian group)**.** *Every non-simple abelian group has a simple normal subgroup. ??? add link ???*

A.3 Permutations

Example A.47 (Permutation)**.** *The following permutation*

$$\pi = \begin{array}{l} 1 \to 2 \\ 2 \to 5 \\ 3 \to 4 \\ 4 \to 3 \\ 5 \to 1 \end{array}$$

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:*

$$\pi = (1, 2, 5)(3, 4) = (3, 4)(5, 1, 2).$$

If we have 2 permutations

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}.$$

and

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

then we can combine them into the new one (via a multiplication)

$$\pi = \pi_1\pi_2 = \begin{array}{l} 1 \to 2 \to 1 \\ 2 \to 5 \to 4 \\ 3 \to 4 \to 2 \\ 4 \to 3 \to 5 \\ 5 \to 1 \to 3 \end{array} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix} = (1)(2, 4, 5, 3) = (2, 4, 5, 3)$$

We have identity element

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

such that $\forall \pi : \pi e = e\pi = \pi$*.*

For every π *we can define* π^{-1} *such that* $\pi\pi^{-1} = \pi^{-1}\pi = e$*.*

For our example

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (1,2,5)(3,4)$$

we have

$$\pi^{-1} = \begin{pmatrix} 2 & 5 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix} = (1,5,2)(3,4)$$

As result we have a Group (Definition A.5) of permutations.

Definition A.48 (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 $\sigma(x) > \sigma(y)$ [48].

Example A.49 (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.

The same result can be got if we use the following equation $l - 1$ *where* l *is the circle length (5 in our case)*

Definition A.50 (Alternating group)**.** Alternating group [19] is the group of even permutations (see definition A.48) 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.51 (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.52 (S_1 group)**.** S_1 *permutation of 1 element consists of only one element* e *- the simplest possible group*

Example A.53 (S_2 group)**.** S_2 *permutation consists of 2 elements:*

1. *identity:* $e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

Table A.2: Cayley table for S_2

$\circ$	e	τ
e	e	τ
τ	τ	e

Table A.3: Cayley table for S_3 [16]

$\circ$	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

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.54 (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:* $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

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.48). I.e. there we will have Alternating group (Definition A.50) A_3.

Example A.55 (S_3/A_3 quotient group)**.** *Lets consider the following Quotient group (Definition A.15)* 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*

$$S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$$

Definition A.56 (Cycle)**.** A cyclic permutation (or cycle) is a permutation of the elements of some set X which maps the elements of some subset S of X to each other in a cyclic fashion, while fixing (that is, mapping to themselves) all other elements of X. If S has k elements, the cycle is called a k-cycle [24].

Example A.57 (Cycle)**.** *The following permutation is a 3-cycle:*

$$(1,2,3) = \begin{array}{l} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{array}$$

Definition A.58 (Transposition)**.** A cycle with only two elements is called a transposition. [24]

Example A.59 (Transposition)**.** *The following permutation is a transposition:*

$$(1,2) = \begin{array}{l} 1 \to 2 \\ 2 \to 1 \end{array}$$

See also example A.60

Example A.60 (Transposition product)**.** *The example shows a product of 2 Transposition (Definition A.58)s with a same element:*

$$(a,c)(a,b) = \begin{array}{l} a \to b \\ b \to a \to c \\ c \to a \end{array} = (a,b,c)$$

Theorem A.61. *Every permutation can be represented as a product of Transposition (Definition A.58)s*

Proof. This is because any cycle $(a_1, a_2, a_3, \ldots, a_{n-1}, a_n)$ can be represented as a product of transpositions as follows

$$(a_1, a_2, a_3, \ldots, a_{n-1}, a_n) = (a_1, a_n)(a_1, a_{n-1}) \ldots (a_1, a_3)(a_1, a_2)$$

□

Corollary A.62. *S_n is generated by any combination of a Transposition (Definition A.58) and n-cycle if and only if n is prime*

Proof. See [9] □

A.4 Rings and Fields

A.4.1 Rings

Definition A.63 (Ring)**.** Consider a set R with 2 binary operations defined. The first one $\oplus$ (addition) and elements of R forms an Abelian group (Definition A.38) under this operation. The second one is $\odot$ (multiplication) and the elements of R forms a Monoid (Definition A.4) 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 (Definition A.63) is a generalization of integer numbers conception.

Example A.64 (Ring of integers $\mathbb{Z}$)**.** *The set of integer numbers $\mathbb{Z}$ forms a Ring (Definition A.63) under $+$ and $\cdot$ operations i.e. addition $\oplus$ is $+$ and multiplication $\odot$ is $\cdot$. Thus for integer numbers we have the following Ring (Definition A.63):* $(\mathbb{Z}, +, \cdot)$

Definition A.65 (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.66 (Multiplicative group of integers modulo n)**.** *Lets consider the following group* $(\mathbb{Z}/9\mathbb{Z})^{\times} = \{1, 2, 4, 5, 7, 8\}$ *[45]*

The group has order 6. The group generator is 2*:* $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 7, 2^5 = 5, 2^6 = 1$.

Accordingly theorem A.25, there are only 2 Proper subgroup (Definition A.11) not equal to id.

One of them is a cyclic group of order 2: $\{1, 8\} \cong \mathbb{Z}/2\mathbb{Z}$.

Another one is also cyclic and has order 3: $\{1, 4, 7\} \cong \mathbb{Z}/3\mathbb{Z}$.

A.4.2 Ideals

Definition A.67 (Ideal)**.** Lets we have the Ring (Definition A.63) $(R, \oplus, \odot)$. Subset $I \subset R$ will be an ideal if it satisfied the following conditions

1. $(I, \oplus)$ is Subgroup (Definition A.10) 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.68 (Ideal $2\mathbb{Z}$)**.** *Consider even numbers. They forms an Ideal (Definition A.67) 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.69 (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 (Definition A.67).*

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

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

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

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

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

, thus

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

Very often use the following notation

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

We can define the following operations

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

The Ring (Definition A.63) where the objects are defined is called as $\mathbb{Z}/n\mathbb{Z}$.

Definition A.70 (Ideal generated by a set)**.** Let R be a Ring (Definition A.63) 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.71 (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.72 (Integral domain)**.** In mathematics, and specifically in abstract algebra, an integral domain is a nonzero commutative Ring (Definition A.63) in which the product of any two nonzero elements is nonzero.

Definition A.73 (Principal ideal domain)**.** In abstract algebra, a principal ideal domain, or PID, is an Integral domain (Definition A.72) in which every ideal is principal, i.e., can be generated by a single element.

Definition A.74 (Maximal ideal)**.** A maximal ideal is an ideal that is maximal (with respect to set inclusion) amongst all Proper ideal (Definition A.79)s i.e. I is a maximal ideal of a ring R if there are no other ideals contained between I and R [44].

Example A.75 (Maximal ideal)**.** *If F is a Field (Definition A.89) then the only maximal ideal is $\{0\}$ [44].*

Definition A.76 (Prime ideal)**.** An ideal I of a commutative ring R is prime if it has the following 2 properties [62] [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

Lemma A.77 ($n\mathbb{Z}$ prime ideal)**.** *A positive integer n is a prime if and only if $n\mathbb{Z}$ is a Prime ideal (Definition A.76) in $\mathbb{Z}$ [62]*

Lemma A.78. *All nonzero Prime ideal (Definition A.76)s are maximal in a principal ideal domain [44]*

Definition A.79 (Proper ideal)**.** I is a proper ideal of a ring R if $I \subsetneq R$.

[1] There is a generalization of prime numbers in arithmetic

Theorem A.80 (About proper ideal)**.** *An ideal I of ring R is proper if and only if $1_R \notin I$.*

Definition A.81 (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 Coset (Definition A.12)s 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.69).

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 (Definition A.15)

A.4.3 Polynomial ring $K[X]$

Let we have a commutative Ring (Definition A.63) K. Lets create a new Ring (Definition A.63) 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 (Definition A.63) 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 (Definition A.63) K. Thus K is sub-ring of the new ring B.

Let

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

thus if we have

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

where f_n is the last non-zero element of (A.2), when one can get

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

Definition A.82 (Polynomial ring)**.** The Ring (Definition A.63) of sequences (A.2) with operations defined by (A.3) is called as polynomial ring $K[X]$.

Lemma A.83 (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.84 (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.85 (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.86 (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.87 (About irreducible polynomials). *Let $\pi(X)$ is an Irreducible polynomial (Definition A.85) 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 (Lemma A.83) 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.88 (About ideal generated by irreducible polynomial). *Let $P \in K[X]$ is a polynomial and $I = (P)$ is an Ideal (Definition A.67) generated by the polynomial. The I is Maximal ideal (Definition A.74) 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.92 (P) is a maximal ideal. □

A.4.4 Fields

Definition A.89 (Field). The ring $(R, \oplus, \odot)$ is called as a field if $(R \setminus \{0\}, \odot)$ is an Abelian group (Definition A.38).

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

Example A.90 (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.91 (Unique factorization domain). Unique factorization domain (UFD) is a commutative ring, which is an Integral domain (Definition A.72), 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.92 (About Quotient Ring and Maximal Ideal). *Let $(R, +, \cdot)$ is a commutative Ring (Definition A.63) with additive identity 0_R and multiplicative identity 1_R. Let I be an Ideal (Definition A.67) of R then I is Maximal ideal (Definition A.74) if and only if Quotient ring (Definition A.81) R/I is a Field (Definition A.89)*

Proof. See the end of section 2.3.3. □

Definition A.93 (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 $\text{Quot}(R)$ or $\text{Frac}(R)$ [33].

A.4.5 Characters

Definition A.94 (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.95 (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.96 (Dedekind). *If we have n distinct Character (Definition A.94)s $\phi_1, \ldots, \phi_n : G \to F^\times$ then they are linearly independent i.e. if $c_1, \ldots, c_n \in F$ satisfy*

$$c_1\phi_1(g) + \cdots + c_n\phi_n(g) = 0$$

for all $g \in G$ then $c_1 = \cdots = c_n = 0$ (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.97 (Module)**.** Let R is a Ring (Definition A.63) and 1_R is it's multiplicative identity. A left R-module M consists of an Abelian group (Definition A.38) $(M, +)$ 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.98 (Module)**.** *If K is a Field (Definition A.89) then concepts of K-Vector space (Definition A.107) and K-module are the same*

Definition A.99 (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 [38]

Definition A.100 (Free module)**.** The Module (Definition A.97) that has a basis (i.e. linearly independent generating set) is called as free module [36].

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.99) 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.101 (Rank of free module)**.** The cardinality of any (and therefore every) basis is called the rank of the free module M [36].

Definition A.102 (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 [28].

Example A.103 (Direct sum of modules)**.** *If we have 2 Free module (Definition A.100)s 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 (Definition A.102) $A = M \oplus N$ 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.104 (Finitely generated module)**.** Finitely generated module is a module that has a finite generating set (see also definition A.99) [35].

Definition A.105 (Cyclic module)**.** A (left) R-Module (Definition A.97) M is called cyclic if M can be generated by a single element i.e.

$$M = \langle x \rangle = Rx = \{rx \mid r \in R\}$$

for some $x \in M$ [23].

Claim A.106. *M is a cyclic R module if and only if exists left ideal $I \subset R$ such that $M \cong R/I$*

Proof. See [12]. Note that [11] p. 149 has the claim as a definition of the Cyclic module (Definition A.105). □

A.5.2 Linear algebra

Definition A.107 (Vector space)**.** Let F is a Field (Definition A.89). 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.108 (About vector space isomorphism)**.** *2 vector spaces L and M with same dimension $dimL = dimM$ then there exists an Isomorphism (Definition A.127) between them*

Definition A.109 (Image)**.** The image or range of a linear map $f : V \to W$ is the following set [42]:

$$\operatorname{Im} f = \{w \in W : w = f(v), v \in V\}$$

Definition A.110 (Kernel)**.** The kernel of a linear map $f : V \to W$ is the following set [41]:

$$\ker f = \{v \in V : f(v) = 0\}$$

Definition A.111 (Rank)**.** The rank of a linear map $f : V \to W$ is dimension of Image (Definition A.109): $rgf = \dim \operatorname{Im} f$ [50]:

Definition A.112 (Nullity)**.** The nullity of a linear map $f : V \to W$ is dimension of Kernel (Definition A.110): $nulf = \dim \ker f$ [41]:

Theorem A.113 (Rank–nullity theorem)**.** *Let V and W be vector spaces over some field and let $T : V \to W$ be a linear map. Then the Rank (Definition A.111) of T is the dimension of the image of T and the Nullity (Definition A.112) of T is the dimension of the kernel of T, so we have*

$$\dim(\operatorname{Im} T) + \dim(\ker T) = \dim V$$

or, equivalently

$$rg(T) + nul(T) = \dim(V)$$

Proof. See [51] □

Definition A.114 (General linear group of a vector space)**.** If V is a Vector space (Definition A.107) 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 [37].

Definition A.115 (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 [30].

Definition A.116 (Dual basis)**.** If $\{e_i\}$ is a basis of V then exists a basis $\{v_j\}$ of Dual space (Equation A.115) such that $v_j(e_i) = \delta_{ij}$ and is called as dual basis. [29]

Definition A.117 (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 (Equation A.115) of V) given by $v \to (x \to f(x, v))$ is not an isomorphism [25].

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.118 (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 (Equation A.115) of V) given by $v \to (x \to f(x, v))$ is an isomorphism [25] or equivalently when V is finite-dimensional if and only if $\forall y \in V f(x, y) = 0$ implies $x = 0$, i.e. the map f has a trivial kernel.

Definition A.119 (Eigenspace)**.** Consider a linear map $T : V \to V$. The set of all eigenvectors of T corresponding to the same eigenvalue, together with the zero vector, is called an eigenspace or characteristic space of T [59]

Definition A.120 (Diagonalizable map)**.** If V is a finite-dimensional vector space, then a linear map $T : V \to V$ is called diagonalizable if there exists an ordered basis of V with respect to which T is represented by a diagonal matrix.

A linear map $T : V \to V$ is diagonalizable if and only if the sum of the dimensions of its eigenspaces is equal to $n = dim(V)$, which is the case if and only if there exists a basis of V consisting of eigenvectors of T. With respect to such a basis, T will be represented by a diagonal matrix. The diagonal entries of this matrix are the eigenvalues of T [57].

Theorem A.121 (About eigenvalues of a diagonalizable linear map)**.** *A linear map $T : V \to V$ with $n = dim(V)$ is diagonalizable if it has n distinct eigenvalues [57].*

Theorem A.122 (About invertible matrix)**.** *Let A be a matrix over F. If A is diagonalizable, then so is any power of it. Conversely, if A is invertible, F is algebraically closed, and A^n is diagonalizable for some n that is not an integer multiple of the characteristic of F, then A is diagonalizable.*

Proof. See [57] □

A.6 Functions aka maps

A.6.1 Functions

Definition A.123 (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.124 (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.125 (Bijection)**.** The function $f : X \to Y$ is bijective (or one-to-one correspondence) if it is an Injection (Definition A.124) and a Surjection (Definition A.123).

Definition A.126 (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.127 (Isomorphism)**.** If a map is Bijection (Definition A.125) as well as Homomorphism (Definition A.126) when it is called as isomorphism.

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

Definition A.128 (Endomorphism)**.** An endomorphism is a morphism (or homomorphism) from a mathematical object to itself [31]

Definition A.129 (Automorphism)**.** Automorphism is an isomorphism from a mathematical object to itself.

Definition A.130 (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.131 (First isomorphism)**.** *Let G is a group and $\phi : G \to H$ is a surjective Homomorphism (Definition A.126). Then if $N = \ker \phi$ we have*

$$H \cong G/N$$

Theorem A.132 (Isomorphism extension theorem). *Let F is a Field (Definition A.89) and E is an Algebraic extension (Definition 1.17) of F. F' is another Field (Definition A.89) and E' the Algebraic extension (Definition 1.17) of F'.*

If there exists an Isomorphism (Definition A.127) $\phi : F \to F'$ then it can be extended to an isomorphism $\tau : E \to E'$.

Proof. The proof of the isomorphism extension theorem depends on Zorn (Lemma 2.15)'s lemma.

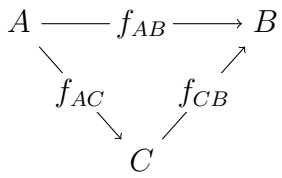
??? The theorem seems to be very close to the theorem 2.17. □

Theorem A.133 (About group homomorphism). *A group homomorphism is Injection (Definition A.124) iff the kernel is trivial [40]*

A.6.2 Category theory

Definition A.134 (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 $f_{AB}(x) = f_{CB}(f_{AC}(x))$.



A.7 Number theory

Definition A.135 (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 [32]

Example A.136 (Euler's totient function). *For example [32], 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* $gcd\,(1,1) = 1$.

Index

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] Conrad, K. Trace and norm ii / Keith Conrad. — http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/tracenorm2.pdf.

[7] Groupwiki. "general affine group: $ga(1,5)$". — 2017. — [Online; accessed 15-March-2017]. https://groupprops.subwiki.org/w/index.php?title=General_affine_group:GA(1,5)&oldid=45747.

[8] Groupwiki. "subgroup structure of symmetric group:s_5". — 2017. — [Online; accessed 15-March-2017]. https://groupprops.subwiki.org/w/index.php?title=Subgroup_structure_of_symmetric_group:S5&oldid=49180.

[9] Gruber, A. Why is s_5 generated by any combination of a transposition and a 5-cycle? — Mathematics Stack Exchange. — URL:http://math.stackexchange.com/q/357673 (version: 2013-05-11). http://math.stackexchange.com/q/357673.

[10] (http://math.stackexchange.com/users/326053/starfall), S. Tensor product of galois extension and algebraic closure. — Mathematics Stack Exchange. — URL:http://math.stackexchange.com/q/2217402 (version: 2017-04-04). http://math.stackexchange.com/q/2217402.

[11] Lang, S. Algebra / Serge Lang. Graduate Texts in Mathematics. — 3 edition. — Springer Science and Business Media, 2002. — https://books.google.ru/books?id=eOUlBQAAQBAJ.

[12] Miller, K. Isomorphism and cyclic modules. — Mathematics Stack Exchange. — URL:http://math.stackexchange.com/q/1003598 (version: 2014-11-03). http://math.stackexchange.com/q/1003598.

[13] Ribenboim, P. Classical Theory of Algebraic Numbers / P. Ribenboim. Universitext. — Springer New York, 2001. — https://books.google.ru/books?id=u5443xdaNZcC.

[14] Rowland, T. Group fixed point. — 2016. — From MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/GroupFixedPoint.html.

[15] user58289. Subgroups of a cyclic group and their order. — Mathematics Stack Exchange. — URL:https://math.stackexchange.com/q/410389 (version: 2013-07-27). https://math.stackexchange.com/q/410389.

[16] 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.

[17] 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.

[18] Wikipedia. "Нормальное расширение — Википедия, свободная энциклопедия". — 2014. — http://ru.wikipedia.org/?oldid=65922374.

[19] 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.

[20] Wikipedia. Commutator — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 30-September-2016]. https://en.wikipedia.org/w/index.php?title=Commutator&oldid=740207690.

[21] 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.

[22] Wikipedia. Correspondence theorem (group theory) — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 2-March-2017]. https://en.wikipedia.org/w/index.php?title=Correspondence_theorem_(group_theory)&oldid=744531320.

[23] Wikipedia. Cyclic module — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 13-March-2017]. https://en.wikipedia.org/w/index.php?title=Cyclic_module&oldid=752351296.

[24] Wikipedia. Cyclic permutation — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 6-March-2017]. https://en.wikipedia.org/w/index.php?title=Cyclic_permutation&oldid=755419947.

[25] 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.

[26] Wikipedia. Direct product of groups — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 19-February-2017]. https://en.wikipedia.org/w/index.php?title=Direct_product_of_groups&oldid=723991376.

[27] 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.

[28] 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.

[29] Wikipedia. Dual basis — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 1-April-2017]. https://en.wikipedia.org/w/index.php?title=Dual_basis&oldid=748729591.

[30] 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.

[31] Wikipedia. Endomorphism — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 2-October-2016]. https://en.wikipedia.org/w/index.php?title=Endomorphism&oldid=726230579.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] Wikipedia. Group homomorphism — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 4-March-2017]. https://en.wikipedia.org/w/index.php?title=Group_homomorphism&oldid=737886552.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] Wikipedia. Nilpotent — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 29-July-2016]. https://en.wikipedia.org/w/index.php?title=Nilpotent&oldid=727125150.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] Wikipedia. Rank–nullity theorem — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 15-February-2017]. https://en.wikipedia.org/w/index.php?title=Rank%E2%80%93nullity_theorem&oldid=730054227.

[52] Wikipedia. Simple group — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 1-March-2017]. https://en.wikipedia.org/w/index.php?title=Simple_group&oldid=709515196.

[53] Wikipedia. Subgroup — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 23-September-2016]. https://en.wikipedia.org/w/index.php?title=Subgroup&oldid=737399477.

[54] Wikipedia. Subgroups of cyclic groups — wikipedia, the free encyclopedia. — 2016. — [Online; accessed 10-February-2017]. https://en.wikipedia.org/w/index.php?title=Subgroups_of_cyclic_groups&oldid=744131880.

[55] 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.

[56] Wikipedia. Adjugate matrix — wikipedia, the free encyclopedia. — 2017. — [Online; accessed 3-April-2017]. https://en.wikipedia.org/w/index.php?title=Adjugate_matrix&oldid=765833302.

[57] Wikipedia. Diagonalizable matrix — wikipedia, the free encyclopedia. — 2017. — [Online; accessed 10-February-2017]. https://en.wikipedia.org/w/index.php?title=Diagonalizable_matrix&oldid=764159566.

[58] Wikipedia. Disjoint union — wikipedia, the free encyclopedia. — 2017. — [Online; accessed 13-April-2017]. https://en.wikipedia.org/w/index.php?title=Disjoint_union&oldid=774047863.

[59] Wikipedia. Eigenvalues and eigenvectors — wikipedia, the free encyclopedia. — 2017. — [Online; accessed 10-February-2017]. https://en.wikipedia.org/w/index.php?title=Eigenvalues_and_eigenvectors&oldid=764288456.

[60] Wikipedia. Finite group — wikipedia, the free encyclopedia. — 2017. — [Online; accessed 5-February-2017]. https://en.wikipedia.org/w/index.php?title=Finite_group&oldid=759713845.

[61] Wikipedia. Klein four-group — wikipedia, the free encyclopedia. — 2017. — [Online; accessed 9-February-2017]. https://en.wikipedia.org/w/index.php?title=Klein_four-group&oldid=759017274.

[62] Wikipedia. Prime ideal — wikipedia, the free encyclopedia. — 2017. — [Online; accessed 29-March-2017]. https://en.wikipedia.org/w/index.php?title=Prime_ideal&oldid=763442154.

[63] Yuan, Q. Using vieta's theorem for cubic equations to derive the cubic discriminant. — Mathematics Stack Exchange. — URL:http://math.stackexchange.com/q/103504 (version: 2012-01-29). http://math.stackexchange.com/q/103504.

[64] Кострикин А. И. Введение в алгебру. ч. 3. Основные структуры алгебры / Кострикин А. И. — МЦНМО, Москва, 2012.