Introduction to Galois Theory

July 27, 2016

Contents

Introduction

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

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

I also tried to make all my comments as footnotes whenever it was possible.

Chapter 1

Generalities on algebraic extensions

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

1.1 Field extensions: examples

1.1.1 K-algebra

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

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

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

1.1.2 Field extension

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

and another definition

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

Why the 2 definitions are equivalent?

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

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

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

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

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

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

that is impossible. □

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

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

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

Example 1.1.3 (K-algebra is not a field)**.** *In the example* [2] *I will show that K algebra is not a field. Consider $K = \mathbb{R}$. Vector space $A = \mathbb{R}^2$ i.e. A consists of vectors of the following form*

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

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

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

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

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

The multiplication identity element of L is the following

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

The zero is the standard one from vector space

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

We can see that

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

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

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

[2] the example was not present in the lectures

1.1.3 Field characteristic

If L is a field there are 2 possibilities

1. $1+1+\cdots \neq 0$. In this case $\mathbb{Z} \subset L$ but $\mathbb{Z}$ is not a field therefore L is an extension of $\mathbb{Q}$. In the case $charL = 0$
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 of polynomials. The $P \in K[X]$ is an Irreducible polynomial. (P) is an Ideal formed by the polynomial. [3] The set of residues by the polynomial forms a field that denoted by $K[X]/(P)$. How we can see it? If $Q \in K[X]$ is a polynomial that $Q \notin (P)$ when Q is prime to P. [4] Then with Bézout's lemma we can get $\exists A, B \in K[X]$ such that

$$AP + BQ = 1,$$

or

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

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

1.2 Algebraic elements. Minimal polynomial

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

Alternative proof that $K[X]/(P)$ is the Field. The (P) is a Maximal ideal [5] but a quotient by a Maximal ideal is a Field (see theorem About Quotient Ring and Maximal Ideal).

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

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

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

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

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

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

and

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

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

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

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

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

therefore

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

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

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

and thus

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

Also

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

and they are inverse each other

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

So this is the structure of a field of four elements. The cardinality of $K = \mathbb{F}_2/(X^2+X+1)$ *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 3.7).*

1.2.2 Algebraic elements

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

1.2.3 Minimal polynomial

Lemma 1.7 (About minimal polynomial existence)**.** *If α is Algebraic element then $\exists!$ unitary polynomial P of minimal degree such that $P(\alpha) = 0$. It is irreducible. $\forall Q$ such that $Q(\alpha) = 0$ is divisible by P* [6]

Proof. We know that $K[X]$ is a Principal ideal domain and a polynomial $Q(\alpha) = 0$ forms an Ideal: $I\{Q \in K[X] \mid Q(\alpha) = 0\}$, so the ideal is generated by one element: $I = (P)$. This is an unique (up to constant) polynomial minimal degree in I.

Lets prove that P is irreducible. If P is not irreducible then $\exists Q, R \in I$ such that $P = QR$, $Q(\alpha) = 0$ or $R(\alpha) = 0$ and $degR, Q < degP$ that is in contradiction with the definition that P is a polynomial of minimal degree. □

Definition 1.8 (Minimal polynomial)**.** *If α is Algebraic element then the unitary polynomial P of minimal degree such that $P(\alpha) = 0$ is called minimal polynomial and denoted by $P_{min}(\alpha, K)$.*

1.3 Algebraic elements. Algebraic extensions

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

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

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

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

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

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

[6] see also theorem About irreducible polynomials

Proposition 1.10. *The following assignment are equivalent*

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

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

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

where $a_k \in K$. Then

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

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

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

Let $x \neq 0 \in K[\alpha]$ then lets look at an operation $x \cdot K[\alpha] \to K[\alpha]$. This is Injection. [8] But the $K[\alpha]$ is finite dimensional Vector space and a Homomorphism between 2 vector spaces with the same dimension is Surjection [9] thus $\exists y \in K[\alpha]$ such that $x \cdot y = 1_{K[\alpha]}$. Therefore x is invertable and $K[\alpha]$ is a Field.

Lets proof that 3 implies 1. Let $K[\alpha]$ is a Field but α is not algebraic. Thus $\forall P \in K[X]\ P(\alpha) \neq 0$. The we have an Injection Homomorphism $i : K[X] \to K[\alpha] = K(\alpha)$ which sends $P(X)$ to $P(\alpha)$. [10] But $K[X]$ is not a field thus $K[\alpha]$ should not be a field too that is in contradiction with the initial conditions. [11] □

[7] Contrary to the example 1.1.3 we see that K-algebra is a field there.

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

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

i.e. Injection property is satisfied.

[9] Two vector spaces with same dimension are isomorphic each other (see lemma A.35)

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

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

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

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

Proof. Let $L' \subset L$ is a subalgebra and let $\alpha \in L'$. We want to show that α is invertable. α is algebraic therefore $\alpha \in K[\alpha] \subset L' \subset L$ and it's invertable. [12] □

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

Proof. Its clear because $P_{min}(\alpha, K) \in L[X]$. [13] □

1.4 Finite extensions. Algebraicity and finiteness

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

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

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

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

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

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

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

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

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

[13] Thus $\exists P_L \in L[X]$ such that $P_L(\alpha) = 0$ i.e. α is algebraic over L.

As soon as $P_{min}(\alpha, K) \in L[X]$ then using lemma About minimal polynomial existence one can get that $P_{min}(\alpha, L)$ divides $P_{min}(\alpha, K)$.

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

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

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

From other side if we have a finite set of algebraic elements $\alpha_1, \ldots, \alpha_d$ then $K[\alpha_1]$ is a finite dimensional Vector space over K, $K[\alpha_1, \alpha_2]$ is a finite

dimensional Vector space over $K[\alpha_1]$ and so on $K[\alpha_1, \ldots, \alpha_d]$ is a finite dimensional Vector space over $K[\alpha_1, \ldots, \alpha_{d-1}]$. All elements are algebraic thus

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

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

1.5 Algebraicity in towers. An example

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

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

Let M algebraic over L and L algebraic over K and let $\alpha \in M$. We want to prove that α is algebraic over K. Lets consider $P_{min}(\alpha, L)$ the polynomial coefficients are from L and they (as soon as they count is a finite) generate a finite extension E over K thus $E(\alpha)$ is finite over E (exists a relation between powers of α) is finite over K thus α is algebraic over K. [14] □

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

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

Minimal polynomial

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

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

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

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

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

[14] $P_{min}(\alpha, L) = \sum_{i=0}^{d-1} l_i \alpha^i$ where $l_i \in L$ and each l_i is algebraic over K by algebraic extension definition 1.11. By theorem 1.17 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.

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

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

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

if α is algebraic.

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

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

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

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

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

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

[15]

□

1.6 A digression: Gauss lemma, Eisenstein criterion

What we have seen so far:

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

[15] We also have that $K[\alpha,\beta]$ is a field: $K[\alpha,\beta]=K(\alpha,\beta)$. Really $K[\alpha]=K(\alpha)$ (see proposition 1.10). β is algebraic over K and therefore over $K(\alpha)$ thus we can construct $K(\alpha)[\beta]=K(\alpha,\beta)$ by proposition 1.10

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

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

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

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

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

thus

$$nmP = Q_1R_1.$$

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

$$0 = \overline{Q_1R_1}$$

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

$$P = Q_sR_t,$$

where $Q_s, R_t \in \mathbb{Z}[X]$. □

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

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

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

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

therefore

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

or

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

and

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

thus

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

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

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

Proof. the same as for example 1.6.1. □

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

Chapter 2

Stem field, splitting field, algebraic closure

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

2.1 Stem field. Some irreducibility criteria

2.1.1 Stem field

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

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

We also can say that for any stem field E:

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

We can use the following Isomorphism: $f : \forall \mathcal{P} \in K[X]/(P) \to \mathcal{P}(\alpha)$, there α is a root of polynomial P. [1]

To summarize we have the following

Proposition 2.2 (About stem field existence)**.** *The stem field exist and if we have 2 stem fields E and E' which correspond 2 roots of P: $E = K[\alpha]$,*

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

$E' = K[\alpha']$ then $\exists! f : E \cong E'$ (Isomorphism of K-algebras) such that $f(\alpha) = \alpha'$.

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

Uniquest of the Isomorphism is easy because it is defined by it's value on argument α: [2]

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

thus

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

□

Remark 2.3 (About stem field)**.**
1. *In particular: If a stem field contains 2 roots of P then $\exists!$ Automorphism taking one root into another.*
2. *If E stem field then $[E : K] = \deg P$*
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 $[E : K] > degP$* [3]

2.1.2 Some irreducibility criteria

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

---

[2] 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.

[3] 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 $\deg E > \deg E' = \deg P$.

Proof. $\Rightarrow$: If P is not irreducible then it has a polynomial Q that divides P and $degQ \leq \frac{n}{2}$. [4] The Stem field L for Q exists and it's degree is $degQ \leq \frac{n}{2}$. L should have a root of Q (as soon as a root of P) by definition.

$\Leftarrow$: If P has a root α in L then $\exists P_{min}(\alpha, K)$ with degree $\leq \frac{n}{2} < n$ [5] that divides P (see lemma 1.7) 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 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 $n \mid md$ [6] thus using $gcd(m, n) = 1$ one can get that $n \mid d$ but this is impossible because $d < n$. □

2.2 Splitting field

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

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

1. *Splitting field L exists and $[L : K] \leq d!$, where $d = degP$.*
2. *If L and M are 2 splitting fields then $\exists \phi : L \cong M$ (an Isomorphism). But the Isomorphism is not necessary to be unique.*

Proof. Lets prove by induction on d. The first case ($d = 1$) is trivial the K itself is the splitting field. Now assume $d > 1$ and that the theorem is valid for any polynomial of degree $< d$ over any field K. Let Q be any irreducible

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

[5] because $[L : K] \leq \frac{n}{2}$ (see remark 2.3)

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

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

factor of P. We can create a Stem field $L_1 = K(\alpha)$ for Q that will be also a Stem field for P.

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

Uniqueness: Let L and M are 2 splitting fields. Let β is a root of Q (irreducible factor of P) in M. We have 2 stem fields: $L_1 = K(\alpha)$ and $M_1 = K(\beta)$. Proposition 2.2 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 $S = \phi(R)$. [7] 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 [8] and as result it's a splitting field for R over $K[\alpha]$ and by induction [9] we have $K[\alpha]$ isomorphism $L \cong M$ and as result K isomorphism $L \cong M$. [10] $\square$

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

---

[7] We have $\phi : K(\alpha) \to K(\beta)$. The $\phi : K \to K = id$ (see note 2). 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 $S = \phi(R)$.

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

[9] 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 $n-1$.

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

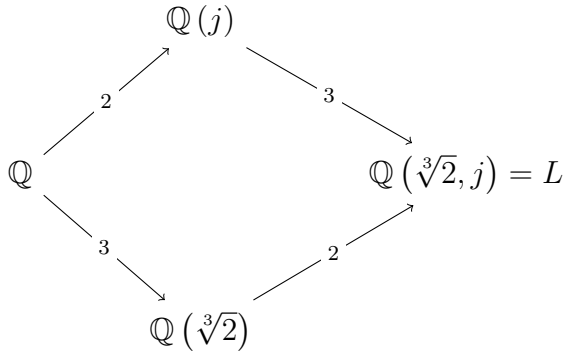
$$K \subset L_1, \subset L_2 \subset \cdots \subset L_n \subset L$$
$$K \subset M_1, \subset M_2 \subset \cdots \subset M_n \subset M$$

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

2.3 An example. Algebraic closure

2.3.1 An example of automorphism

Example 2.3.1 (x^3-2 over $\mathbb{Q}$)**.** *Let we have the following polynomial x^3-2 over $\mathbb{Q}$. It has the following roots: $\sqrt[3]{2}, j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$, where $j = e^{\frac{2\pi i}{3}}$. Splitting field is the following $L = \mathbb{Q}\left(\sqrt[3]{2}, j\right)$. Lets find Automorphisms of the field. $P_{min}(j, \mathbb{Q}) = X^2 + X + 1$ thus using remark 2.3 $[\mathbb{Q}(j) : \mathbb{Q}] = 2$. Using the same arguments one can get that $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$. As result the following picture can be got*



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

1. *$\mathbb{Q}\left(\sqrt[3]{2}\right)$ Automorphism. We have $x^2 + x + 1$ as $P_{min}\left(j, \mathbb{Q}\left(\sqrt[3]{2}\right)\right)$. The polynomial has 2 roots: j and j^2 and there is an Automorphism that exchanges the root. Lets call it τ* [11]

2. *$\mathbb{Q}(j)$ Automorphism. In this case the automorphism of exchanging $\sqrt[3]{2}$ and $j\sqrt[3]{2}$.* [12]*. Lets call it σ*

The group of automorphism of L $Aut(L/K)$ is embedded into permutation group of 3 elements S_3 (see example A.3.1):

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

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

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

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

- σ: $\sqrt[3]{2} \to j\sqrt[3]{2} \to j^2\sqrt[3]{2} \to \sqrt[3]{2}$. *This is a circle.*
- τ - *it keeps* $\sqrt[3]{2}$ *and exchanges* j *and* j^2: $\sqrt[3]{2}j \leftrightarrow \sqrt[3]{2}j^2$ *(see note 11). This is a transposition.*

2.3.2 Algebraic closure

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

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

Definition 2.10 (Algebraic closure)**.** *An algebraic closure of K is a field L that is Algebraically closed field and Algebraic extension over K.* [13]

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

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

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

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

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

Let $I \subset A$ is an Ideal generated by a set $P(X_P)$ $\forall P \in S$.[14] We claim that I is a Proper ideal i.e. $I \neq A$. If not then we can write (see theorem A.22)

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

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

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

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

where $\lambda_i \in A$ and the sum is the finite (see definition A.15). As soon as the sum is finite then I can take the product of the polynomials in the sum: $P = \prod_i^n P_i$ and I can create a Splitting field L for the polynomial P over K (see theorem 2.7).

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 $X_{P_i} \to \alpha_i$ [15] if $P = P_i$ and $X_{P_i} \to 0$ otherwise. From (2.1) we have

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

that is impossible.

Fact: Any Proper ideal $I \subset A$ is contained in the Maximal ideal m (see proposition 2.14 below) and A/m is a field (see theorem A.31).

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

2.3.3 Ideals in a ring

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

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

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

Proposition 2.14. *Any Proper ideal is in a Maximal ideal*

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

Let $\mathcal{P}$ is the set of proper ideals in A containing I. The set is not empty because it has at least one element I. Any Chain $\mathcal{C} = \{I_\alpha\}$ [16] 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 $I \subset m$. □

[15] α_i is a root of P_i

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

If we take a Quotient ring by maximal ideal it's always a field [17] 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 [18].

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 of huge polynomial ring $K_{i-1}[X]$ by a suitable Maximal ideal that is got by means of Zorn lemma.

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

Theorem 2.15 (About extension of homomorphism)**.** *Let $K \subset L \subset M$ - Algebraic extension. $K \subset \Omega$, where Ω - Algebraic closure of K. $\forall \phi : L \to \Omega$ extends to $\widetilde{\phi} : M \to \Omega$* [19]

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

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

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

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

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

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

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

Lets suppose that $N_0 \neq M$, i.e. $N_0 \subsetneq M$. Now it's very easy to get a contradiction. Lets take $x \in M \setminus N_0$ and consider Minimal polynomial $P_{min}(x, N_0)$. It should have a root $\alpha \in \Omega$. Now we extend N_0 to $N_0(x)$ and

[17] We refer to it as a theorem with definition provided in A.31. The comments can be considered as a simple prove of the fact.

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

[19] see also example 3.1.1.

define ψ' on $N_0(x)$ as follows: $\forall y \in N_0 : \psi'(y) = \psi_0(y)$ and $\psi'(x) = \alpha$. Thus we was able to find an element of the chain that is greater than maximal. Therefore our assumption about $N_0 \neq M$ was incorrect and we can conclude than $N_0 = M$ and therefore $\tilde{\phi} = \psi_0$. □

Corollary 2.16 (About algebraic closure isomorphism)**.** *If Δ and Δ' are 2 algebraic closures of K then they are isomorphic as K-algebras.*

Proof. Using theorem 2.15 one can assume $L = K$, $M = \Delta'$ and $\Omega = \Delta$ i.e. we have

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

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

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

Chapter 3

Finite fields. Separability, perfect fields

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

3.1 An example (of extension)s. Finite fields

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

Corollary 3.2. *Any Algebraic extension of K embeds (see definition A.42) into the Algebraic closure* [2]

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

Let

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

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

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

[1] There is a redefinition of corollary 2.16.

[2] i.e. $\forall E$ - algebraic extension of K, $\exists \phi : E \to \bar{K}$ - Homomorphism. The statement is a reformulation of theorem 2.15

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

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

Let

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

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

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

This ("extends") is because [4]

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

3.1.1 Finite fields

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

Remark 3.4 ($\mathbb{F}_{p^n}$)**.** *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 3.5 (Frobenius homomorphism)**.** *If $charK = p$, then exists a Homomorphism $F_p : K \to K$ such that $F_p(x) = x^p$. Really if we consider $(x+y)^p$ and $(xy)^p$ then we can get $(x+y)^p = x^p + y^p$* [7] *and $(xy)^p = x^p y^p$. The second property is the truth in the all fields (of course) but the first one is the special property of $\mathbb{F}_p$ fields.*

[4] I.e. in our case we have $\mathbb{Q} \subset L \subset M$. We have $\phi_{1,2} : L \to \overline{\mathbb{Q}}$ which can be extended (accordingly theorem 2.15) 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 1.2.1 to see exact structure of $\mathbb{F}_4$.

[7]

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p + p \cdot \left(\sum_{k=1}^{p-1} a_k x^k y^{p-k}\right),$$

where $a_k \in \mathbb{Z}$. I.e.

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

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

3.2 Properties of finite fields

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

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

Proof. Note that $F_{p^n} : x \to x^{p^n}$ is a Homomorphism (see remark 3.6) as result the following set $\{x \mid F_{p^n}(x) = x\}$ is a field containing $\mathbb{F}_p$ [8] i.e.

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

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

If $Q_n(X) = X^{p^n} - X$ then the considered set consists of the root of the polynomial Q_n. The polynomial has no multiple roots because $gcd(Q_n, Q_n') = 1$. [9] This is because $Q_n' \equiv 1 \mod p$. [10] As soon as Q_n has no multiple roots then there are p^n different roots and therefore the splitting field is the field with p^n elements.

Conversely lets $|K| = p^n$ and $\alpha \neq 0 \in K$. Using the fact that the multiplication group of K has $p^n - 1$ elements: $|K^*| = p^n - 1$ [11] as result the multiplication of all the elements should give us 1: $\alpha^{p^n - 1} = 1$ or $\alpha^{p^n} - \alpha = 0$

[8] For $x \in \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ we have that (see theorem A.10)

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

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

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

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

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

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

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

(see theorem A.10). 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 3.8. *$\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ if and only if $d \mid n$.*

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

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

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

Proof. Stem field K has to have degree n over $\mathbb{F}_p$ i.e. $[K : \mathbb{F}_p] = n$ (see remark 2.3) i.e. it should have p^n elements (see remark 3.4) and therefore $K = \mathbb{F}_{p^n}$ (see theorem 3.7).

About Splitting field. Using the just proved result we can say that if α is a root of P then $\alpha \in \mathbb{F}_{p^n}$ thus $Q_n(\alpha) = 0$. Therefore P divides Q_n [13] and as result P splits in $\mathbb{F}_{p^n}$. □

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

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

[12] up to Isomorphism

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

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

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

From other side let R is an irreducible factor of Q_n. α is a root of R then $Q_n(\alpha) = 0$ thus $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$. From remark 2.3 we have

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

From remark 3.4 $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Theorem 3.8 says that $d \mid n$. As result $R \in \mathcal{P}_d$. Thus the polynomial should be in the product $\prod_{d|n} \prod_{P \in \mathcal{P}_d} P$. □

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

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

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

Just another example [1] [17]

Example 3.2.2. *In $\mathbb{F}_2[X]$, the irreducible factorization of $X^{2^n} - X$ for $n = 1, 2, 3, 4$ is as follows*

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

[14] Since stem field is $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ (see theorem 3.8 and proof at the theorem 3.9)

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

[16] We also can say that 2 irreducible polynomial $P_1, P_2 \in \mathbb{F}_p[X]$ should not have same roots. For example if α is the same root - it cannot be in $\mathbb{F}_p$ because in the case the polynomials will be reducible. Thus it can be only in an extension of $\mathbb{F}_p$ from other side $gcd(P_1, P_2) = 1$ and therefore with Bézout's lemma one can get that $\exists Q, R \in \mathbb{F}_p[X]$ such that $P_1 Q + P_2 R = 1$ 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 3.11. *Let K be a field and and G be a finite Subgroup of K^* then G is a Cyclic group*

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

Let $\psi(d)$ - is the number of elements of order d (see also Order of element in group) in G. We need $\psi(N) \neq 0$ [19] and we know that $N = \sum \psi(d)$.

Let also $\phi(d)$ - is the number of elements of order d (see also Order of element in group) in $\mathbb{Z}/N\mathbb{Z}$. [20] As $\mathbb{Z}/N\mathbb{Z}$ contains a single (cyclic) subgroup of order d for each $d \mid N$. [21] $\phi(d)$ is the number of generators of $\mathbb{Z}/d\mathbb{Z}$ i.e. the number of elements between 1 and $d-1$ that are prime to d. We know that $\phi(N) \neq 0$.

We claim that either $\psi(d) = 0$ or $\psi(d) = \phi(d)$ [22] If no element of order d in G then $\psi(d) = 0$ otherwise if $x \in G$ has order d then $x^d = 1$ or x is a root of the following polynomial $x^d - 1$. The roots of the polynomial forms a cyclic subgroup of G (by Cyclic group definition). So G as well as $\mathbb{Z}/N\mathbb{Z}$ has a single cyclic subgroup of order d (which is cyclic) or no such group at all. [23]

If $\psi(d) \neq 0$ then exists such a subgroup and $\psi(d)$ is equal to the number of generators of that group or $\phi(d)$ [24] In particular $\psi(d) \leq \phi(d)$ [25] but there should be equality because the sum of both $\sum \psi(d) = \sum \phi(d) = N$. In particular $\psi(N) \neq 0$ and we proved the theorem. □

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

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

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

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

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

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

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

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

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

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

Corollary 3.12. *If $\mathbb{F}_p \subset K$ and $[K:\mathbb{F}_p] = n$ then $\exists\alpha$ such that $K = \mathbb{F}_p(\alpha)$. In particular $\exists$ an Irreducible polynomial of degree n over $\mathbb{F}_p$* [26]

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

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

Proof. As we know from theorem 3.7: $\forall x \in \mathbb{F}_{p^n} : x^{p^n} = x$ so [28] $F_p^n = Id$. As result the order of $\langle F_p\rangle$ is no greater than n. Lets prove that the $ordF_p = n$. Really if $m < n$ then $x^{p^m} - x = 0$ has $p^m < p^n$ roots and [29] F_p^m cannot be identity. Finally (from corollary 3.12) we have $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ where α is a root of an irreducible polynomial of degree n. I.e. there cannot be more than n automorphism [30] so

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

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

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

and the group is cyclic generated by F_p. □

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

[27] This is because from theorem 3.11 $K^* = \langle\alpha\rangle$ i.e. any element of K except 0 can be got as a power of α. Moreover $\alpha \notin \mathbb{F}_p$ (in other case we will got $K = \mathbb{F}_p$) i.e. we really got $K = \mathbb{F}_p(\alpha)$. α is an Algebraic element because we can consider $1, \alpha, \ldots, \alpha^{n-1}$ 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 1.7 there exists an irreducible polynomial $P_{min}(\alpha, \mathbb{F}_p)$.

[28] because

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

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

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

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

3.4 Separable elements

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

There exists an Isomorphism (see proposition 2.2) over K

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

that is also extended to an Automorphism on E (see theorem A.44).

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) [32]

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 [33]

Example 3.4.1. *Let $p = 2$. The polynomial $P(X) = X^{16}+1$ has the required property ($P' = 0$). The polynomial can be present in the following form*

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

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

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

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

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

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

[32] Let P has multiply roots. As soon as it's irreducible a multiply root is in an extension of K. In this case the root should be also a root for P' thus by lemma 1.7 (or theorem A.28) one can get that $P \mid P'$ in $K[X]$ but that is impossible because $\deg P' < \deg P$ and can be only possible if $P' = 0$.

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

Proof. If λ is a root of P then λ: $P(X) = (X - \lambda)R$ Thus $\mu = \lambda^{p^r}$ is the root of Q [34] as result $Q(Y) = (Y - \lambda^{p^r})S(Y)$ therefore

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

and λ is not a root of $S\left(X^{p^r}\right)$. [35] Thus we just got that multiplicity of λ is p^r. □

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

Definition 3.16 (Degree of separability)**.** $d_{sep}(P) = \deg Q$ *(as above)* [36]

Definition 3.17 (Degree of inseparability)**.** $d_i(P) = \frac{\deg P}{\deg Q}$ *(* $= p^r$ *in proposition 3.14)*

Definition 3.18 (Pure inseparable polynomial)**.** P *is pure inseparable if* $d_i = \deg P$*. Then* $P = X^{p^r} - a$ [37]

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

Proposition 3.20 (On number of homomorphisms)**.** *If* α *is separable on* K *then the number of Homomorphisms over* K *from* K *to* $\bar{K}$

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

in general

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

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

---

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

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

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

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

3.5 Separable degree, separable extensions

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

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

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

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

Definition 3.23 (Inseparable degree)**.**

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

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

2. The following things are equivalent

(a) L is separable over K

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

(c) L is generated over K by a finite number of Separable elements i.e. $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, 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 3.25. *That holds if we replace separability with pure inseparability.*

Proof. About 1st part: If we have a Homomorphism $\phi : L \to \bar{K}$ then it is extended to $\tilde{\phi} : M \to \bar{K}$ (by extension theorem 2.15) it can be done with one way per each homomorphism from L to M i.e. it can be done by $\left|Hom_L\left(M, \bar{K}\right)\right|$ ways but we have

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

because $\bar{K}$ is also $\bar{L}$ (Algebraic closure over L) thus for the total number of homomorphisms one can get the following equations

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

We have the following inequality [38]

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

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:

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

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

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

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

[38] The inequality can be proved by induction using the fact that it's true for $K(\alpha)$ because from general case of proposition 3.20

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

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.

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

[40] We consider finite extensions (see remark 3.4) i.e. which consists of finite number of elements

[41] Let $K(\alpha_1,\ldots,\alpha_{i-1}) = L$ 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 1.7

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

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

Definition 3.26 (Separable closure)**.** *If L over K not necessary finite (but algebraic over K) we can define*

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

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

L is pure inseparable over L^{sep}.

Remark 3.27. *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 3.28 (Perfect field)**.** *Let K is a field and $charK = p > 0$. K is perfect if Frobenius homomorphism is a Surjection*

Example 3.6.1. *1. Finite field is perfect because an Injection of a set into itself is always a Surjection*

2. Algebraically closed fields are perfect because $X^p - a$ has a root α for any a particularly $a = F_p(\alpha)$ [44]

3. Not perfect field example. Let $K = \mathbb{F}_p(X)$ be a field of rational fractions in 1 variable over $\mathbb{F}_p$. I.e. elements of the field are $\frac{f(X)}{g(X)}$ where $f, g \in \mathbb{F}_p[X]$. It's not perfect because $Im(F_p) = \mathbb{F}_p(X^p) \neq \mathbb{F}_p(X)$

Theorem 3.29. *K is a Perfect field if and only if all irreducible polynomial over K are separable or in other words all Algebraic extensions of K are separable.*

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

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

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

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

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

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

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

If K is not perfect but all irreducible polynomial are separable. K is not perfect means that $\exists a \notin Im(F_p)$ 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 $x^{p^r} = a$ [47] and of course $x^{p^{r-1}} \notin K$. [48]

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

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

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

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

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

[49] Corollary 3.12 says that there exists an irreducible polynomial of degree p^r with x as the root. Theorem A.28 says that the polynomial should divide our polynomial $X^{p^r} - a$ as soon as they have the same root. The two polynomial have same degree and as result they are the same (up to a constant). Therefore the considered polynomial is irreducible.

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

Chapter 4

Tensor product. Structure of finite K-algebras

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

4.1 Definition of tensor product

4.1.1 Summary for previous lectures

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

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

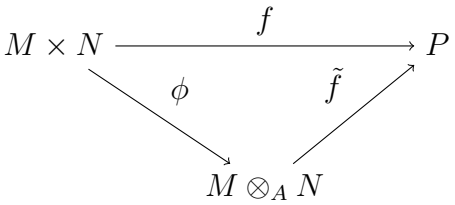
For $L=K(\alpha)$ it is clear because the number of homomorphisms is equal to the number of roots of the Minimal polynomial $P_{min}(\alpha,K)$. In general one can use induction and multiplicativity of the degree $[L:K]$ and number of homomorphisms (see theorem About separable extensions). Thus separable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

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

4.1.2 Tensor product

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

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

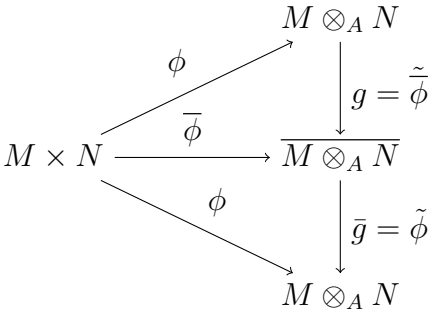


The property characterize the pair $(\phi, M \otimes N)$. Really if have another pair $\left(\overline{\phi}, \overline{M \otimes N}\right)$ like this one then by definition we have mutually inverse homomorphisms of A-modules between them

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 than there is an unique Isomorphism between them:*

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

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



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

[2] It is out of the lecture video and can be considered as an explanation for the claim about having mutually inverse homomorphisms of A-modules

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

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

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

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

Lemma 4.4 (About tensor product existence)**.** *Tensor product defined via Universal property exists*

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

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

such that

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

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

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

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

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

[4] Follows from the basis choice

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

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

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. □

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* [5].

4.2 Tensor product of modules

4.2.1 Advantages of the universal property

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

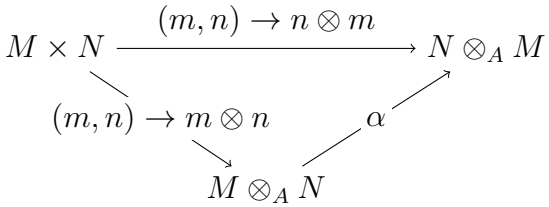
[5] i.e. $\exists x \in M \otimes_A N$ such that $\exists! m \in M, n \in N : x = m \otimes n$ but $\exists m_1, \ldots, m_k \in M, n_1, \ldots, n_k \in N : x = \sum_{i=1}^{k} m_i \otimes n_i$

4.2.2 Several examples of universal property usage

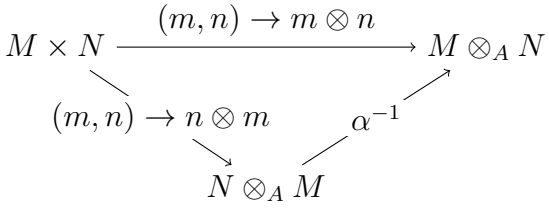
Example 4.2.1 (Commutativity proof)**.** *We want to prove that*

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

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



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

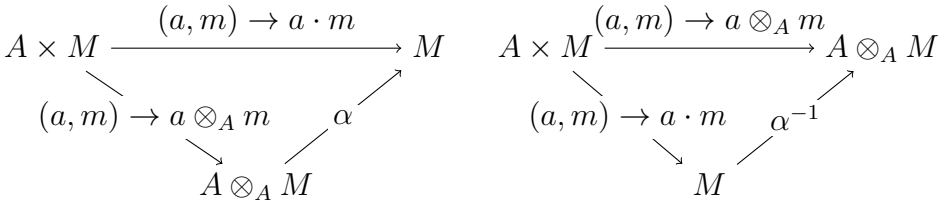


Also

Corollary 4.6.

$$A \otimes_A M \cong M$$

Proof. For the proof [6] lets look at A. Really A can be considered as A-module because all requirements from definition A.32 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 $a \in A$.

□

[6] The proof is missed in the lectures

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

More complex fact is the following

Proposition 4.7. *Let M and N are Free modules with corresponding basises $e_1, e_2, \dots, e_n$ and $\epsilon_1, \epsilon_2, \dots, \epsilon_m$ than $M \otimes_A N$ is also free module with basis $e_i \otimes \epsilon_j$ where $1 \leq i \leq n$ and $1 \leq j \leq m$.*

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 $a_{j_0} b_{j_0}$. It's bilinear [7] so it factors through the tensor product $\tilde{f}_{i_0,j_0} : M \otimes_A N \to A$. The map $\tilde{f}_{i_0,j_0}$ sends $e_{i_0} \otimes \epsilon_{j_0}$ to 1 and all others to 0. [8] So if

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

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

In particular for the Vector space the tensor product is defined in the same way (as just proved in the proposition 4.7): the tensor product of 2 vector spaces with basises $e_1, e_2, \dots, e_n$ and $\epsilon_1, \epsilon_2, \dots, \epsilon_m$ is another vector space with the following basis $e_i \otimes \epsilon_j$ i.e. the definition does not take into consideration the Universal property.

Proposition 4.8 (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. □

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

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

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

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

4.3 Base change

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

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

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

Example 4.3.1 (The complexification of a real vector space)**.** *We can "make" $\mathbb{R}^{2n}$ from $\mathbb{C}^n$ by forgetting the complex structure.* [11] *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 $1 \otimes e_1, \ldots, 1 \otimes e_n$ and for $\mathbb{R}^{2n}$ - $1 \otimes e_1, \ldots, 1 \otimes e_n, i \otimes e_1, \ldots, i \otimes e_n$.

Proposition 4.9. *In general we have the following. If M - free A - module with basis $e_1, \ldots, e_n$ then $B \otimes_A M$ is a free B module with basis $1_B \otimes e_1, \ldots, 1_B \otimes e_n$.*

Proof. The proof is the same as at proposition 4.7. Again we construct certain bilinear maps and say that those factor over the tensor product and this implies that certain families are linearly independent.

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

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

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

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

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 all $\alpha_i = 0$ i.e. $\alpha_i 1_B \otimes e_i$ forms a basis. □

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

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

Remark 4.10. *We have the following maps.*

- *For A - modules: $\alpha : M \to B \otimes_A M$ such that $m \to 1_B \otimes_A m$*
- *For B - modules: $\mu : B \otimes_A N \to N$ such that $b \otimes n \to bn$.*

Theorem 4.11 (Base-change)**.** *Let A is a Ring and B is A-algebra. Let also M is an A-Module and N is B-module.*

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

I.e. the homomorphisms are the same or in other words the corresponding groups of homomorphisms are isomorphic.

Proof. First of all we have [12] Homomorphism $f : B \otimes_A M \to N$. We also have the following map (see remark 4.10): $\alpha : M \to B \otimes_A M$. 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 4.10) 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. [13] □

4.4 Examples. Tensor product of algebras

Proposition 4.12. *If $I \subset A$ - an Ideal so my B - A algebra will be $B = A/I$ then*

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

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

[13] ???

Proof. We have map $\alpha : M \to B \otimes_A M = A/I \otimes_A M$ (see remark 4.10) which sends m to $\bar{1} \otimes m$. [14] 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 $\bar{i} \otimes m = \bar{0} \otimes m = 0$. [15] Thus α sends IM to 0. So α induces $\bar{\alpha} : M/IM \to A/I \otimes_A M$ such that $\bar{\alpha}(\bar{m}) = \bar{1} \otimes m$.

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

$$M \to M/IM$$

gives us the following map of B-modules

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

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 $\bar{\alpha}$. [16] □

Several examples:

Example 4.4.1. *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: $2^{-1} = -1 \mod 3$ *thus* $(2)\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$ *and as result*

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

Example 4.4.2.

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

and more interesting one

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

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

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

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

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

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 [17]

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

The tensor product has the following

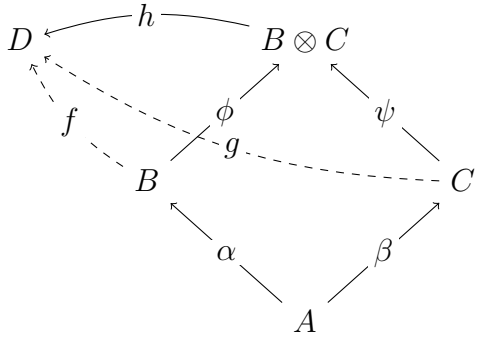
Definition 4.13 (Universal property)**.** *Let we have the following maps*

$$\begin{aligned} \alpha : A \to B, \\ \beta : A \to C, \\ \phi : b \in B \to b \otimes 1 \in B \otimes_A C, \\ \psi : c \in C \to 1 \otimes c \in B \otimes_A C \end{aligned}$$

Then for any A-algebra D one has

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

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



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:

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

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

Let consider the following example

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

but by Chinese remainder theorem

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

As result we have that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not a field because it has zero divisors.

4.5 Relatively prime ideals. Chinese remainder theorem

Definition 4.14 (Relatively prime ideals)**.** *Let A - Ring and I, J are Ideals. I and J are relatively prime if $I + J = A$.*

Lemma 4.15. *1. If I, J are relatively prime then $IJ = I \cap J$*

2. *If $I_1, \ldots, I_k$ relatively prime with J then $\prod_{i=1}^{k} I_i = I_1 \cdot \cdots \cdot I_k$ 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 [18] 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 $1 = i_1 + j_1 = i_2 + j_2$ where $i_1 \in I_1, i_2 \in I_2$ and $j_1, j_2 \in J$. we also have

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

thus $\forall x \in A$ we have

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

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

3. is obvious [19]

□

Theorem 4.16 (Chinese remainder theorem)**.** *Let $I_1, \dots, I_n$ - ideals and map $\pi : A \to A/I_1 \times \cdots \times A/I_n$ defined as follows*

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

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

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

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

[20]

Proof. Let π is Surjection. 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 that $1 - a_i \in I_i$. 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 4.15) $\prod_{j \neq i} I_j$. 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 4.17. *1. If A is an Integral domain then A is a field.*

[19] 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.

[20] see First isomorphism theorem

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

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

Lets prove the first part. Integral domain means that there is no zero divisors i.e. $\forall a \in A$ [21] multiplication by a is Injection. A is finite dimensional Vector space that implies that $\times a$ is an Isomorphism, [22] in particular Surjection 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

Theorem 4.18 (Structure of finite K-algebra)**.** *Let A be a finite K-algebra i.e.* $\dim_K A < \infty$*. Then*

1. *There are only finitely many Maximal ideals $m_1, \ldots, m_r$ in A*
2. *Let $J = m_1 \cap \cdots \cap m_r = m_1 \ldots m_r$.* [23] *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 $n_1, \ldots, n_r$.*

Proof. 1. Let $m_1, \ldots, m_i$ be a several maximal ideals. By Chinese remainder theorem we have [24]

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

We know that A as well as $A/m_1 \ldots m_i$ and A/m_k are finite dimensional K-Vector space. Thus we have the following relations

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

[21] $a \neq 0_A$

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

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

[24] Maximal ideals are relatively prime because in a commutative ring with unity, every Maximal ideal is a Prime ideal see also proposition 4.17.

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 as well as its powers J^k. We have the following sequence [25]

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

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

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

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

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

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

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

i.e.

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

But $\det M = 1 + \lambda$ where $\lambda \in J$. [26] Since $J = m_1 \cap \cdots \cap m_r$ then $\forall i : \lambda \in m_i$ so $\nexists i$ such that $1 + \lambda \in m_i$ [27] thus $1 + \lambda$ is invertable [28] therefore $e_1 = \cdots = e_s = 0$ [29]

[25] Let $j \in J \subset A$ then $\forall y \in A : jy \in J$. But if $x \in JJ$ then $x = jj = jy$ there $y = i \in A$. and as soon as $j \in J$ then $x = jj$ is also an element of J. As result $J^2 \subseteq J$.

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

[27] ???

[28] ???

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

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

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

We used the following facts:

- $A = A/m_1^{n_1} \dots m_r^{n_r}$ [30]
- $m_i^{n_i}$ are pairwise relatively prime [31]

□

Remark 4.19. *The n_is are not uniquely defined. For example*

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

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 $(X)^3 \subset (X)^2$ [32]

Several examples:

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

Another example

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

And you see that those algebras are products of fields. So all n_i's may be taken equal to 1. In other words, we don't have Nilpotent elements in our algebra. 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 ome from inseparable extensions.

[30] 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)

[31] As soon as $\{m_i\}$ - Maximal ideals and as result Prime ideals then with lemma 4.15 one can get that $\forall i \neq j$ $m_i^{n_i}$ is relatively prime with $m_j^{n_j}$.

[32] ??? exercise

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)

5.2 Separability and base change

5.3 Separability and base change (cont'd). Primitive element theorem

5.4 Examples. Normal extensions

5.5 Galois extensions

5.6 Artin's theorem

Appendices

Appendix A

Course prerequisites

There are several prerequisites for the course there. They consists of definitions, theorems and examples mostly taken from Wikipedia.

A.1 Sets

Definition A.1 (Class)**.** *A class is a collection of sets (or sometimes other mathematical objects) that can be unambiguously defined by a property that all its members share.*

A.2 Gropus

Definition A.2 (Monoid)**.** *The set of elements M with defined binary operation $\circ$ we will call as a monoid if the following conditions are satisfied.*

1. *Closure:* $\forall a, b \in M$*:* $a \circ b \in M$
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.3 (Group)**.** *Let we have a set of elements G with a defined binary operation $\circ$ that satisfied the following properties.*

1. *Closure:* $\forall a, b \in G$*:* $a \circ b \in G$
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* $\forall a \in G$*:* $e \circ a = a \circ e = a$

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

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

4. Inverse element: $\forall a \in G\ \exists a^{-1} \in G$ *such that* $a \circ a^{-1} = e$

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

Therefore the group is a Monoid with inverse element property.

Example A.2.1 (Group $\mathbb{Z}/2\mathbb{Z}$)**.** *Consider a set of 2 elements:* $G = \{0, 1\}$ *with the operation* $\circ$ *defined by the table A.1.*

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

Definition A.4 (Cyclic group)**.** *A cyclic group or monogenous group is a group that is generated by a single element. Note that Group* $\mathbb{Z}/2\mathbb{Z}$ *is a cyclic group.*

Definition A.5 (Order of element in group)**.** *Order, sometimes period, of an element a of a group is the smallest positive integer m such that* $a^m = e$ *(where e denotes the identity element of the group, and am denotes the product of m copies of a). If no such m exists, a is said to have infinite order.*

Theorem A.6 (Lagrange)**.** *For any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.*

Definition A.7 (Subgroup)**.** *Let we have a Group* $(G, \circ)$*. The subset* $S \subset G$ *is called as subgroup if* $(S, \circ)$ *is a Group.*

A.2.1 Abelian group

Definition A.8 (Abelian group)**.** *Let we have a Group* $(G, \circ)$*. The group is called an Abelian or commutative if* $\forall a, b \in G$ *it holds* $a \circ b = b \circ a$*.*

Theorem A.9 (About order of element of an Abelian group)**.** *If G is a finite Abelian group and m is the maximal order of the elements of G then the order of every element of G divides m*

Theorem A.10. *Let G is an Abelian group and $n = |G|$ the group order (number of elements) then $\forall g \in G$ the following statement holds*

$$g^n = e,$$

there e is the group identity.

Proof. Let m is the maximal order of group G. In this case by Lagrange $m \mid n$ i. e. $n = k_1 m$ where $k_1 \in \mathbb{Z}$. Let l is the order of g i.e. $g^l = e$. By the theorem A.9 $l \mid m$ i.e. $m = k_2 l$. Thus

$$g^n = (g^m)^{k_1} = \left(g^l\right)^{k_2 k_1} = e.$$

□

Definition A.11 (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.

A.3 Permutations

Example A.3.1 (S_n group)**.** *If we a have a permutation of n elements then it's possible to do by means of $n!$ ways.*

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

S_2 permutation consists of 2 elements:

1. *identity e:*

$$1 \to 1$$
$$2 \to 2$$

2. *transposition τ:*

$$1 \to 2$$
$$2 \to 1$$

Table A.2: Cayley table for S_2

$\circ$	e	τ
e	e	τ
τ	τ	e

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

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

1. *identity e:*
$$1 \to 1$$
$$2 \to 2$$
$$3 \to 3$$

2. *transposition τ:*
$$1 \to 2$$
$$2 \to 1$$
$$3 \to 3$$

3. *circle σ:*
$$1 \to 2$$
$$2 \to 3$$
$$3 \to 1$$

A.4 Rings and Fields

A.4.1 Rings

Definition A.12 (Ring)**.** *Consider a set R with 2 binary operations defined. The first one $\oplus$ (addition) and elements of R forms an Abelian group under this operation. The second one is $\odot$ (multiplication) and the elements of R forms a Monoid under the operation. The two binary operations are connected each other via the following distributive law*

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

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

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

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

The Ring is a generalization of integer numbers conception.

Example A.4.1 (Ring of integers $\mathbb{Z}$)**.** *The set of integer numbers* $\mathbb{Z}$ *forms a Ring under* $+$ *and* $\cdot$ *operations i.e. addition* $\oplus$ *is* $+$ *and multiplication* $\odot$ *is* $\cdot$*. Thus for integer numbers we have the following Ring:* $(\mathbb{Z}, +, \cdot)$

Definition A.13 (Nilpotent element)**.** *An element,* x*, of a ring,* R*, is called nilpotent if there exists some positive integer,* n*, such that* $x^n = 0$*.*

A.4.2 Ideals

Definition A.14 (Ideal)**.** *Lets we have the Ring* $(R, \oplus, \odot)$*. Subset* $I \subset R$ *will be an ideal if it satisfied the following conditions*

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

Example A.4.2 (Ideal $2\mathbb{Z}$)**.** *Consider even numbers. They forms an Ideal in* $\mathbb{Z}$*. Because multiplication of any even number to any integer is an even. The ideal's symbolic name is* $2\mathbb{Z}$*.*

Example A.4.3 (Ring of integers modulo n: $\mathbb{Z}/n\mathbb{Z}$)**.** *Let* $n \in \mathbb{Z}$ *and* $n > 1$*. Then* $n\mathbb{Z}$ *is an Ideal.*

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

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

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

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

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

, thus

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

Very often use the following notation

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

We can define the following operations

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

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

Definition A.15 (Ideal generated by a set)**.** *Let R be a Ring and S is a sub set of R. Consider the following set*

$$I = \{r_1 s_1 + \cdots + r_n s_n | n \in \mathbb{N}, r_i \in R, s_i \in S\}$$

I is called by an ideal generated by set S if $\forall r \in R, i \in I : r \cdot i \in I$.

The sum in the definition of the ideal should be finite. The ring is assumed commutative in the definition.

Definition A.16 (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.17 (Integral domain)**.** *In mathematics, and specifically in abstract algebra, an integral domain is a nonzero commutative Ring in which the product of any two nonzero elements is nonzero.*

Definition A.18 (Principal ideal domain)**.** *In abstract algebra, a principal ideal domain, or PID, is an Integral domain in which every ideal is principal, i.e., can be generated by a single element.*

Definition A.19 (Maximal ideal)**.** *I is a maximal ideal of a ring R if there are no other ideals contained between I and R.*

Definition A.20 (Prime ideal)**.** *An ideal I of a commutative ring R is prime if it has the following 2 properties* [1]

1. *If $a, b \in R$ such that $ab \in I$ then $a \in I$ or $b \in I$*
2. *I is not equal the whole ring R*

Definition A.21 (Proper ideal)**.** *I is a proper ideal of a ring R if $I \subsetneq R$.*

Theorem A.22 (About proper ideal)**.** *An ideal I of ring R is proper if and only if $1_R \notin I$.*

Definition A.23 (Quotient ring)**.** *Quotient ring is a construction where one starts with a ring R and a two-sided ideal I in R, and constructs a new ring, the quotient ring R/I, whose elements are the Cosets of I in R subject to special $+$ and $\cdot$ operations.*

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

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

[1] There is a generalization of prime numbers in arithmetic

This equivalence class is also sometimes written as a mod I and called the "residue class of a modulo I" (see also example A.4.3).

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.

A.4.3 Polynomial ring $K[X]$

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

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

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

We can define addition and multiplication on B as follows

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

where

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

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

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

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

Let

$$\begin{aligned} X &= (0, 1, 0, \dots), \\ X^2 &= (0, 0, 1, \dots) \end{aligned}$$

thus if we have

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

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

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

Definition A.24 (Polynomial ring)**.** *The Ring of sequences (A.1) with operations defined by (A.2) is called as polynomial ring $K[X]$.*

Lemma A.25 (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.26 (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*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

Definition A.27 (Irreducible polynomial)**.** *An irreducible polynomial is, roughly speaking, a non-constant polynomial that cannot be factored into the product of two non-constant polynomials.*

Theorem A.28 (About irreducible polynomials)**.** *Let $\pi(X)$ is an Irreducible polynomial in $K[X]$ and let α be a root of $\pi(X)$ in a some larger field. $\forall h(x) \in K(X)$ if have the following statement: $h(\alpha) = 0$ if and only if $\pi(X) \mid h(X)$ in $K[X]$.*

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

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

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

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

A.4.4 Fields

Definition A.29 (Field)**.** *The ring $(R, \oplus, \odot)$ is called as a field if $(R \setminus \{0\}, \odot)$ is an Abelian group.*

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

Example A.4.4 (Field $\mathbb{Q}$)**.** *Note that $\mathbb{Z}$ is not a field because not for every integer number an inverse exists. But if we consider a set of fractions $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\}$ when it will be a field.*

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

Definition A.30 (Unique factorization domain)**.** *Unique factorization domain (UFD) is a commutative ring, which is an Integral domain, and in which every non-zero non-unit element can be written as a product of prime elements (or irreducible elements), uniquely up to order and units, analogous to the fundamental theorem of arithmetic for the integers.*

Theorem A.31 (About Quotient Ring and Maximal Ideal)**.** *Let $(R, +, \cdot)$ is a commutative Ring with additive identity 0_R and multiplicative identity 1_R. Let I be an Ideal of R then I is Maximal ideal if and only if Quotient ring R/I is a Field*

Proof. See the end of section 2.3.3. □

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.32 (Module)**.** *Let R is a Ring and 1_R is it's multiplicative identity. A left R-module M consists of an Abelian group $(M, +)$ and an operation $\cdot : R \times M \to M$ such that $\forall r, s \in R$ and $\forall x, y \in M$ the following relations are hold:*

1. $r \cdot (x + y) = r \cdot x + r \cdot y$
2. $(r + s) \cdot x = r \cdot x + s \cdot x$
3. $(rs) \cdot x = r \cdot (s \cdot x)$
4. $1_R \cdot x = x$

Example A.5.1 (Module)**.** *If K is a Field then concepts of K-Vector space and K-module are the same*

Definition A.33 (Free module)**.** *The Module that has a basic (i.e. linearly independent generating set) is called as free module.*

For a R-module M the set $E \subseteq M$ is a basic for M if

1. *E is a generating set 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* $r_1 = \cdots = r_n = 0_R$.

A.5.2 Linear algebra

Definition A.34 (Vector space)**.** *Let F is a Field. The set V is called as vector space under F if the following conditions are satisfied*

1. *We have a binary operation* $V \times V \to V$ *(addition):* $(x, y) \to x + y$ *with the following properties:*

   (a) $x + y = y + x$

   (b) $(x + y) + z = x + (y + z)$

   (c) $\exists 0 \in V$ *such that* $\forall x \in V : x + 0 = x$

   (d) $\forall x \in V \exists -x \in V$ *such that* $x + (-x) = x - x = 0$

2. *We have a binary operation* $F \times V \to V$ *(scalar multiplication) with the following properties*

   (a) $1_F \cdot x = x$

   (b) $\forall a, b \in F, x \in V$*:* $a \cdot (b \cdot x) = (ab) \cdot x$.

   (c) $\forall a, b \in F, x \in V$*:* $(a + b) \cdot x = a \cdot x + b \cdot x$

   (d) $\forall a \in F, x, y \in V$*:* $a \cdot (x + y) = a \cdot x + a \cdot y$

Lemma A.35 (About vector space isomorphism)**.** *2 vector spaces L and M with same dimension* $dimL = dimM$ *then there exists an Isomorphism between them*

A.6 Functions aka maps

A.6.1 Functions

Definition A.36 (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.37 (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.38 (Bijection)**.** *The function $f : X \to Y$ is bijective (or one-to-one correspondence) if it is an Injection and a Surjection.*

Definition A.39 (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.40 (Isomorphism)**.** *If a map is Bijection as well as Homomorphism when it is called as isomorphism.*

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

Definition A.41 (Automorphism)**.** *Automorphism is an isomorphism from a mathematical object to itself.*

Definition A.42 (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.43 (First isomorphism theorem)**.** *Let G is a group and $\phi : G \to H$ is a surjective Homomorphism. Then if $N = \ker \phi$ we have*

$$H \cong G/N$$

Theorem A.44 (Isomorphism extension theorem)**.** *Let F is a Field and E is an Algebraic extension of F. F' is another Field and E' the Algebraic extension of F'.*

If there exists an Isomorphism $\phi : F \to F'$ then it can be extended to an isomorphism $\tau : E \to E'$.

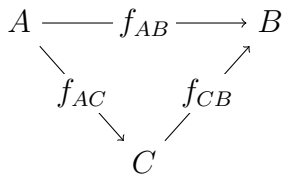
Proof. The proof of the isomorphism extension theorem depends on lem:zorn's lemma.

??? The theorem seems to be very close to the theorem 2.15. □

A.6.2 Category theory

Definition A.45 (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* $f_{AB}(x) = f_{CB}(f_{AC}(x))$.



Bibliography

[1] Conrad, K. Finite fields / Keith Conrad. — http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/finitefields.pdf.