Introduction to Galois Theory

Ekaterina Amerik

Table of contents

About This Document

This document contains lecture notes on Introduction to Galois theory provided by Ekaterina Amerik (Higher School of Economics) via Coursera. Each chapter corresponds to one lecture (or one week on Coursera). The appendix contains useful information for the course that may be absent in the main content.
The notes were actually taken by a fellow student who had published them in LaTeX ,I have converted them to quarto here. My orginal notes were handwritten but realised this conversion is far easier and a good revision.

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 element (often called scalar) $a, b \in K$:

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

Example 1.2 (Field of complex numbers $\mathbb{C}$): The field of complex numbers $\mathbb{C}$ can be considered as a K-algebra over the field of real numbers $\mathbb{R}$.

1.1.2 Field Extension

Definition 1.3 (Field extension)

Let K and L be fields. L is an extension of K if $L \supset K$.
Alternative definition: Let K be a field then L is an extension of K if L is a K-algebra.

Why are the 2 definitions equivalent?

Lemma 1.5 (K-algebra and homomorphism)

Given a K-algebra is the same as having a homomorphism $f : K \to A$ of rings.
Proof: 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 $k \cdot 1_A \in A$.
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 1.6 (About homomorphism of fields)

Any field homomorphism is an injection.
Proof: Let's prove by contradiction. If $f(x) = f(y)$ and $x \neq y$ then

$$f(x) - f(y) = 0_A$$

$$f(x - y) = 0_A$$

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

that is impossible.

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

Example 1.8 (K-algebra is not a field)

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:

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

The multiplication identity element of L is $1_L = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

We can see that $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0_L$ i.e. we have 2 divisors of zero which are not zero itself. The elements do not have inverse ones and as result the L is not a field.

Definition 1.9 (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 $\text{char} L = 0$.
2. $1 + 1 + \cdots + 1 = \sum_{i=1}^{m} 1 = 0$ for some $m \in \mathbb{Z}$. The first time when it happens is for a prime number i.e. minimal m with the property is prime. In this case $\text{char} L = p$, where $p = \min m$ - the minimal m (prime) with the property. In this case $\mathbb{Z}/p\mathbb{Z} \subset L$. The $\mathbb{Z}/p\mathbb{Z}$ is a field denoted by $\mathbb{F}_p$. The L is an extension of $\mathbb{F}_p$.

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

Definition 1.10 (Prime field)

If L is a field $\mathbb{Q} \subset L$, i.e. $\text{char} L = 0$ then $\mathbb{Q}$ is the prime field for L. Otherwise, if $\text{char} L = p > 0$ then $\mathbb{F}_p$ is the prime field.

! Claim 1.11

Let $K[X]$ be the ring of polynomials. The $P \in K[X]$ is an irreducible polynomial. (P) is an ideal formed by the polynomial. The set of residues by the polynomial forms a field that is denoted by $K[X]/(P)$.

Proof of Claim 1.11

If $Q \in K[X]$ is a polynomial that $Q \notin (P)$ then Q is prime to P. Then with Bézout's identity we can get $\exists A, B \in K[X]$ such that

$$AP + BQ = 1$$

or

$$BQ \equiv 1 \bmod P$$

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

1.2 Algebraic Elements. Minimal Polynomial

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

! Claim 1.12

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

$$K[X]/(X-a) \cong K$$

Proof of Claim 1.12

The $K[X]/(X-a)$ is a field because $X-a$ is an irreducible polynomial.
For the proof of the isomorphism, let's consider a polynomial $P \in K[X]$ and define the following field homomorphism:

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

The ϕ is a field homomorphism and by Lemma 1.6, any field homomorphism is injection, i.e. ϕ is an injection.
Next we should show that ϕ is surjection. It's easy because $\forall k \in K$ we can consider constant polynomial $P = k$ from $K[X]$. For the polynomial we will have $\phi(k) = k$.
As result ϕ is bijection and homomorphism, therefore ϕ is isomorphism.

1.2.2 Algebraic elements

Definition 1.15 (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 1.16 (About minimal polynomial existence)

If α is an 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.

Proof of Lemma 1.16

We know that $K[X]$ is a principal ideal domain and a polynomial $Q(\alpha) = 0$ forms an ideal: $I = \{Q \in K[X] | Q(\alpha) = 0\}$, so the ideal is generated by one element: $I = (P)$. This is a unique (up to constant) polynomial of minimal degree in I.
Let's 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 $\deg R, Q < \deg P$ that is in contradiction with the definition that P is a polynomial of minimal degree.

Definition 1.17 (Minimal polynomial)

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

Example 1.18 (Minimal polynomial): Consider the following minimal polynomial $P_{\min}(\alpha, \mathbb{Q})$, where $\alpha = \sqrt{2}$. In GAP we have:

```
gap> x:=Indeterminate(Rationals,"x");;
gap> alpha:=Sqrt(2);;
gap> MinimalPolynomial(Rationals, alpha);
x^2-2
```

I.e. $P_{\min}(\alpha, \mathbb{Q}) = X^2 - 2$.

1.3 Algebraic Elements. Algebraic Extensions

Definition 1.19

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

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

Example 1.20 (C):

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

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

Proposition 1.21

The following statements are equivalent:

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

Proof of Proposition 1.21

1 2: If α is algebraic over K then using the minimal polynomial lemma there exists $P_{\min}(\alpha, K)$:

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

where $a_k \in K$. Then

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

this means that any α^n can be represented as a linear combination of finite number of powers of α i.e. $K[\alpha]$ generated by $1, \alpha, \dots, \alpha^{d-1}$ is a finite dimensional vector space.
2 3: It's enough to prove that $K[\alpha]$ is a field because $K[\alpha] \subset K(\alpha)$.
Let $x \neq 0 \in K[\alpha]$ then let's look at an operation $x \cdot K[\alpha] \to K[\alpha]$. This is injection. But the $K[\alpha]$ is finite dimensional vector space and a homomorphism between 2 vector spaces with the same dimension is surjection, thus $\exists y \in K[\alpha]$ such that $x \cdot y = 1_{K[\alpha]}$. Therefore x is invertible and $K[\alpha]$ is a field.
3 1: Let $K[\alpha]$ be a field but α is not algebraic. Thus $\forall P \in K[X]$, $P(\alpha) \neq 0$. Then we have an injection homomorphism $i : K[X] \to K[\alpha] = K(\alpha)$ which sends $P(X)$ to $P(\alpha)$. But $K[X]$ is not a field thus $K[\alpha]$ should not be a field too that is in contradiction with the initial conditions.

Definition 1.22 (Algebraic extension)

L an extension of K is called algebraic over K if $\forall \alpha \in L$ - α is algebraic over K.

Proposition 1.23

If L is algebraic over K then any K-subalgebra of L is a field.

Proof of Proposition 1.23

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

Proposition 1.24

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

Proof of Proposition 1.24

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

We can consider the following example as an illustration for proposition 1.24:

Example 1.25: $K = \mathbb{R}$, $L = M = \mathbb{C}$. $\alpha = i \in M$ is algebraic over $K = \mathbb{R}$ and therefore using the proposition 1.24 it is algebraic over $L = \mathbb{C}$. Moreover $P_{\min}(\alpha, L) = X - i$ and it divides $P_{\min}(\alpha, K) = X^2 + 1$.

1.4 Finite Extensions. Algebraicity and Finiteness

Definition 1.26 (Finite extension)

L is a finite extension of K if $\dim_K L < \infty$. $\dim_K L$ is called the degree of L over K and is denoted by $[L : K]$.

Theorem 1.27 (The multiplicativity formula for degrees)

Let $K \subset L \subset M$. Then M is a finite extension over K if and only if M is a finite extension over L and L is a finite extension over K. In this case

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

Proof of Theorem 1.27

Let $[M : K] < \infty$ but any linear independent set of vectors $\{m_1, m_2, \dots, m_n\}$ over L is also linear independent over K thus $[M : K] < \infty \Rightarrow [M : L] < \infty$. Also L is a vector subspace of M thus if $[M : K] < \infty$ then $[L : K] < \infty$.
Let $[M : L] < \infty$ and $[L : K] < \infty$ then we have the following bases: - L-basis over M: $(e_1, e_2, \dots, e_n)$ - K-basis over L: $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_d)$

Let's prove 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

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

The number of linear independent vectors is $n \times d$ i.e.

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

Definition 1.28 ($K(\alpha_1, \dots, \alpha_n)$)

$K(\alpha_1, \dots, \alpha_n) \subset L$ generated by $\alpha_1, \dots, \alpha_n$ is the smallest subfield of L containing K and $\alpha_i \in L$.

Theorem 1.29 (About towers)

L is finite over K if and only if L is generated by a finite number of algebraic elements over K.

Proof of Theorem 1.29

If L is finite then $\alpha_1, \dots, \alpha_d$ is a basis. In this case $L = K[\alpha_1, \dots, \alpha_d] = K(\alpha_1, \dots, \alpha_d)$. Moreover each $K[\alpha_i]$ is finite dimensional thus by proposition 1.21 α_i is algebraic.
From other side if we have a finite set of algebraic elements $\alpha_1, \dots, \alpha_d$ then $K[\alpha_1]$ is a finite dimensional vector space over K, $K[\alpha_1, \alpha_2]$ is a finite dimensional vector space over $K[\alpha_1]$ and so on $K[\alpha_1, \dots, \alpha_d]$ is a finite dimensional vector space over $K[\alpha_1, \dots, \alpha_{d-1}]$. All elements are algebraic thus $K[\alpha_1, \dots, \alpha_i] = K(\alpha_1, \dots, \alpha_i)$. Then using theorem 1.27 we can conclude that $K(\alpha_1, \dots, \alpha_d)$ has finite dimension.

1.5 Algebraicity in Towers. An Example

Theorem 1.30

$K \subset L \subset M$ then M is an algebraic extension over K if and only if M is algebraic over L and L is algebraic over K.

Proof of Theorem 1.30

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 be algebraic over L and L be algebraic over K and let $\alpha \in M$. We want to prove that α is algebraic over K. Let's consider $P_{\min}(\alpha, L)$ - the polynomial coefficients are from L and they (as soon as their count is 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.

Example 1.31 ($\mathbb{Q}$ extension): $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ is algebraic and finite over $\mathbb{Q}$:

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

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

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

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

Therefore $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$ and $P_{\min}(\sqrt{3}, \mathbb{Q}(\sqrt[3]{2})) = x^2 - 3$.

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

Proposition 1.32 (On dimension of extension)

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

if α is algebraic.

Proof of Proposition 1.32

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

Proposition 1.33 (About algebraic closure)

If $K \subset L$ (L extension of K). Consider

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

then L' is a subfield of L and is called the algebraic closure of K in L.

Proof of Proposition 1.33

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

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 algebraic over K. - L is a finite extension over K if $\dim_K L < \infty$. - If an extension is finite then it is algebraic. - An extension is finite if and only if it is algebraic and generated by a finite number of algebraic elements. - $[K[\alpha] : K] = \deg P_{\min}(\alpha, K)$.

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 about $x^{100} - 2$?

! Lemma 1.34 (Gauss)

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

Proof of Lemma 1.34

Let $P = QR$ over $\mathbb{Q}$. Then $Q = mQ_1$, $Q_1 \in \mathbb{Z}[X]$, $R = nR_1$, $R_1 \in \mathbb{Z}[X]$, thus $nmP = Q_1 R_1$. There exists p that divides mn: $p|mn$ thus in modulo p we have $0 = \overline{Q_1 R_1}$ but p is prime and the equation is in the field $\mathbb{F}_p$ thus either $\overline{Q_1} = 0$ or $\overline{R_1} = 0$. Let $\overline{Q_1} = 0$ thus p divides all coefficients in Q_1 and we can take $\frac{Q_1}{p} = Q_2 \in \mathbb{Z}[X]$. Continue for all primes in mn we can get that $P = Q_s R_t$, where $Q_s, R_t \in \mathbb{Z}[X]$.

Example 1.35 (Eisenstein criterion): Let's consider the following polynomial $x^{100} - 2$. It's irreducible. Let's prove it. If it's reducible then $\exists Q, R \in \mathbb{Z}[X]$ such that $x^{100} - 2 = QR$.

Let's consider this equation modulo 2. In the case we will have $QR \equiv x^{100} \bmod 2$, therefore $Q \equiv x^k \bmod 2$, $R \equiv x^l \bmod 2$, 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 1.36 (Eisenstein criterion)

Let $P \in \mathbb{Z}[X]$ and $P = a_n X^n + a_{n-1} X^{n-1} + a_1 X + a_0$. If $\exists p$ - prime such that $p \nmid a_n$, $p|a_i$ $\forall i < n$ and $p^2 \nmid a_0$, then $P \in \mathbb{Z}[X]$ is irreducible.

Proof of Lemma 1.36

The proof is the same as for example 1.35.

Note: Both Gauss (Lemma 1.34) and Eisenstein criterion (Lemma 1.36) are valid by replacing $\mathbb{Z}$ with a unique factorization domain R and $\mathbb{Q}$ by its factorization field.

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 uniqueness (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 $P \in K[X]$ be 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.

We also can say that for any stem field E: $K[X]/(P) \cong E$.

We can use the following isomorphism: $f : \forall P \in K[X]/(P) \to P(\alpha)$, where α is a root of polynomial P.

Proposition 2.2 (About stem field existence)

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

Proof of Proposition 2.2

Existence: $K[X]/(P)$ can be taken as the stem field.
Uniqueness of the isomorphism: It is easy because it is defined by its value on argument α: $\phi : K[X]/(P) \xrightarrow{x \mapsto \alpha} E$ $\psi : K[X]/(P) \xrightarrow{x \mapsto \alpha'} E'$ thus $\psi \circ \phi^{-1} : E \xrightarrow{\alpha \mapsto x \mapsto \alpha'} E'$

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 is a stem field then $[E : K] = \deg P$. 3. If $[E : K] = \deg P$ 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 $[E : K] > \deg P$.

2.1.2 Some Irreducibility Criteria

Corollary 2.4

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

Proof of Corollary 2.4

$\Rightarrow$: If P is not irreducible then it has a polynomial Q that divides P and $\deg Q \leq \frac{n}{2}$. The stem field L for Q exists and its degree is $\deg Q \leq \frac{n}{2}$. 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 $\leq \frac{n}{2} < n$ that divides P, i.e. P becomes 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 of Corollary 2.5

If it is not the case and $\exists Q$ such that $Q|P$ 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 $[M : K] = [M : L][L : K] = md$.
Let $K(\alpha)$ be a stem field of P over K then $[K(\alpha) : K] = \deg P = n$. $K(\alpha) \subseteq M$ and therefore $n|md$ thus using $\gcd(m, n) = 1$ one can get that $n|d$ 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 $d = \deg P$.
2. If L and M are 2 splitting fields then $\exists \phi : L \cong M$ (an isomorphism). But the isomorphism is not necessarily unique.

Proof of Theorem 2.7

Let's prove by induction on d. The first case ($d = 1$) is trivial - the K itself is the splitting field. Now assume $d > 1$ and that the theorem is valid for any polynomial of degree $< d$ over any field K. Let Q be any irreducible factor of P. We can create a stem field $L_1 = K(\alpha)$ for Q that will be also a stem field for P.
Over L_1 we have $P = (x - \alpha)R$, where R is a polynomial with $\deg R = d - 1$. 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 is $\leq d \cdot (d-1)! = d!$.

Uniqueness: Let L and M be 2 splitting fields. Let β be 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 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 $S = \phi(R)$. M is a splitting field for S over $K[\beta]$ and by induction we have $K[\alpha]$ isomorphism $L \cong M$ and as result K isomorphism $L \cong M$.

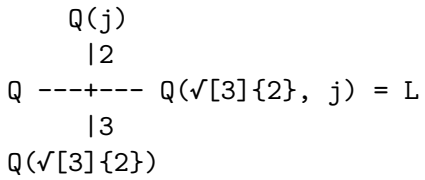
Remark 2.8: The isomorphism considered in theorem 2.7 is not unique. A splitting field can have many automorphisms and this is in fact the subject of Galois theory.

2.3 An Example. Algebraic Closure

2.3.1 An Example of Automorphism

Example 2.9 ($X^3 - 2$ over $\mathbb{Q}$): Let we have the following polynomial $X^3 - 2$ over $\mathbb{Q}$. It has the following roots: $\sqrt[3]{2}$, $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$, where $j = e^{2\pi i/3}$. Splitting field is the following $L = \mathbb{Q}(\sqrt[3]{2}, j)$.

Let's find automorphisms of the field. $P_{\min}(j, \mathbb{Q}) = X^2 + X + 1$ thus $[\mathbb{Q}(j) : \mathbb{Q}] = 2$. Using the same arguments one can get that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. As result the following picture can be obtained:



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

1. $\mathbb{Q}(\sqrt[3]{2})$ automorphism. We have $X^2 + X + 1$ as $P_{\min}(j, \mathbb{Q}(\sqrt[3]{2}))$. The polynomial has 2 roots: j and j^2 and there is an automorphism that exchanges the roots. Let's call it τ.
2. $\mathbb{Q}(j)$ automorphism. In this case the automorphism exchanges $\sqrt[3]{2}$ and $j\sqrt[3]{2}$. Let's call it σ.

The group of automorphisms of L, $\mathrm{Aut}(L/K)$, is embedded into the permutation group of 3 elements S_3: $\mathrm{Aut}(L/K) \hookrightarrow S_3$.

It's embedded because the automorphism exchanges the roots of $X^3 - 2$. Moreover $\mathrm{Aut}(L/K) = S_3$, because σ and τ generate S_3.

2.3.2 Algebraic Closure

Definition 2.10 (Algebraically closed field)

K is algebraically closed if any non-constant polynomial $P \in K[X]$ has a root in K or in other words if any $P \in K[X]$ splits.

Example 2.11 ($\mathbb{C}$): $\mathbb{C}$ is an algebraically closed field. This will be proved later.

Definition 2.12 (Algebraic closure)

An algebraic closure of K is a field L that is an algebraically closed field and an algebraic extension over K.

Theorem 2.13 (About algebraic closure)

Any field K has an algebraic closure.

Proof of Theorem 2.13

Let's discuss the strategy of the proof. 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 $K \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset ...$
Take $\overline{K} = \bigcup_i K_i$ and we claim that $\overline{K}$ is algebraically closed. Really $\forall P \in \overline{K}[X]\ \exists j : P \in K_j[X]$ thus it has a root in K_{j+1} and as result in $\overline{K}$.
Now how can we construct K_1. Let S be a set of all irreducible $P \in K[X]$. Let $A = K[(X_P)_{P \in S}]$ - multi-variable (one variable X_P for each $P \in S$) polynomial ring.
Let $I \subset A$ be an ideal generated by a set $P(X_P)\ \forall P \in S$. We claim that I is a proper ideal i.e. $I \neq A$. If not then we can write $1_A = \sum_i \lambda_i P_i(X_{P_i})$ where $\lambda_i \in A$ and the sum is finite. As soon as the sum is finite then I can take the product of the polynomials in the sum: $P = \prod_i P_i$ and I can create a splitting field L for the polynomial P over K.
A is a polynomial ring and it's very easy to produce a homomorphism between polynomial algebra and any other algebra. Therefore there is a homomorphism between rings A and L such that $\phi : A \to L$ where $X_{P_i} \to \alpha_i$ if $P = P_i$ and $X_{P_i} \to 0$ otherwise. From the equation above we have $\phi(1_A) = \sum_i \lambda_i \phi(P_i(X_{P_i})) = \sum_i \lambda_i P_i(\alpha_i) = 0$ that is impossible.
Fact: Any proper ideal $I \subset A$ is contained in the maximal ideal m and A/m is a field.
Thus I can take $K_1 = A/m$ and continue in the same way to construct $K_2, K_3, \dots, K_n, ...$

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 2.14 (Chain)

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

Lemma 2.15 (Zorn)

If any non-empty chain C in a non-empty set P has an upper bound (that is $M \in P$ such that $M \geq x$, $\forall x \in C$) then P has a maximal element.

Proposition 2.16

Any proper ideal is in a maximal ideal.

Proof of Proposition 2.16

We can use Zorn's lemma to prove that any proper ideal is in a maximal ideal.
Let P be the set of proper ideals in A containing I. The set is not empty because it has at least one element I. Any chain $C = \{I_\alpha\}$ has an upper bound: it's $\bigcup_\alpha I_\alpha$ (exercise that the union is an ideal). So P has a maximal element m and $I \subset m$.

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

2.4 Extension of Homomorphisms. Uniqueness of Algebraic Closure

Some summary about just proved existence of algebraic closure. There exists $\overline{K} = \bigcup_{i=1}^{\infty} K_i$ - 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's lemma.

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

Theorem 2.17 (About extension of homomorphism)

Let $K \subset L \subset M$ - algebraic extension. $K \subset \Omega$, where Ω - algebraic closure of K. $\forall \phi : L \to \Omega$ extends to $\tilde{\phi} : M \to \Omega$.

Proof of Theorem 2.17

Apply Zorn's lemma to the following set (of pairs) $E = \{(N, \psi) : L \subset N \subset M, \psi \text{ extends } \phi\}$
E is non-empty because $(L, \phi) \in E$.
The set 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 $N = \bigcup_\alpha N_\alpha$ - field, sub extension of M. ψ defined in the following way: for $x \in N_\alpha$, $\psi(x) = \psi_\alpha(x)$.
Thus E has a maximal element that we denote by (N_0, ψ_0).
Let's suppose that $N_0 \neq M$, i.e. $N_0 \subsetneq M$. Now it's very easy to get a contradiction. Let's take $x \in M \setminus N_0$ and consider minimal polynomial $P_{\min}(x, N_0)$. It should have a root $\alpha \in \Omega$. Now we extend N_0 to $N_0(x)$ and define ψ' on $N_0(x)$ as follows: $\forall y \in N_0 : \psi'(y) = \psi_0(y)$ and $\psi'(x) = \alpha$. Thus we were 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 that $N_0 = M$ and therefore $\tilde{\phi} = \psi_0$.

Corollary 2.18 (About algebraic closure isomorphism)

If Δ and Δ' are 2 algebraic closures of K then they are isomorphic as K-algebras.

Proof of Corollary 2.18

Using theorem 2.17 one can assume $L = K$, $M = \Delta'$ and $\Omega = \Delta$ i.e. we have $K \subset K \subset \Delta'$. In this case homomorphism $K \to \Delta$ can be extended to $\Delta' \to \Delta$ i.e. there exists a homomorphism (i.e. injection) 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 $\Delta' \to \Delta$.

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 Extensions. Finite Fields

Corollary 3.1

Algebraic closure of K is unique up to isomorphism of K-algebras.

Corollary 3.2

Any algebraic extension of K embeds into the algebraic closure.

Example 3.3 (Of extension of homomorphism): Let $K = \mathbb{Q}$ and $\overline{\mathbb{Q}}$ be t# Finite fields. Separability, perfect fields {#sec-ch3}

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.

3.2 An example (of extension)s. Finite fields

Corollary 3.1 Algebraic closure of K is unique up to Isomorphism of K-algebras.

Corollary 3.2 Any Algebraic extension of K embeds into the Algebraic closure.
i.e. $\forall E$ - algebraic extension of K, $\exists \phi : E \to \bar{K}$ - Homomorphism. The statement is a reformulation of Theorem 2.17.

Example 3.1. Example 3.3 (Of extension of homomorphism). Let $K = \mathbb{Q}$ and $\bar{\mathbb{Q}}$ is the Algebraic closure of K. For instance we can consider $\mathbb{Q} \subset \mathbb{C}$.

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

Let

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

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

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

Let

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

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

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

This ("extends") is because $M = L[Y]/(Y^2 - \alpha)$.

3.2.1 Finite fields

Definition 3.4 (Finite field). K is a finite field if its Characteristic $\mathrm{char}K = p$, where p is a prime number.

Tip

Remark 3.5 ($\mathbb{F}_{p^n}$). If K is a finite extension of $\mathbb{F}_p$ and $n = [K : \mathbb{F}_p]$ then number of elements of K: $|K| = p^n$. The following notation is also used for a finite extension of a finite field: $\mathbb{F}_{p^n}$. Note that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. 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).

Tip

Remark 3.6 (Frobenius homomorphism). If $\mathrm{char}K = p$, then exists a Homomorphism $F_p : K \to K$ such that $F_p(x) = x^p$. Really if we consider $(x+y)^p$ and $(xy)^p$ then we can get $(x+y)^p = x^p + y^p$ and $(xy)^p = x^p y^p$.
The second property is the truth in all fields (of course) but the first one is the special property of $\mathbb{F}_p$ fields.

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

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

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

Tip

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

3.3 Properties of finite fields

Important

Theorem 3.8 Lets fix $\mathbb{F}_p$ and its Algebraic closure $\bar{\mathbb{F}}_p$.
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 a unique sub extension of $\bar{\mathbb{F}}_p$ with p^n elements.

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

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

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 $\gcd(Q_n, Q_n') = 1$. This is because $Q_n' \equiv 1 \bmod p$. As soon as Q_n has no multiple roots then there are p^n different roots and therefore the splitting field is the field with p^n elements.

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

The uniqueness of sub-extension of $\bar{\mathbb{F}}_p$ with p^n elements is a result of uniqueness of the splitting field.

□

> **!** Important
>
> **Theorem 3.9** $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ if and only if $d|n$.

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

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

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

Conversely if $d|n$ 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: $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$.

□

> **!** Important
>
> **Theorem 3.10** $\mathbb{F}_{p^n}$ 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. $[K : \mathbb{F}_p] = n$ i.e. it should have p^n elements and therefore $K = \mathbb{F}_{p^n}$.

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

□

> **i** **Corollary 3.11** Let $\mathcal{P}_d$ is the set of all irreducible, Monic polynomials of degree d such that $\mathcal{P}_d \subset \mathbb{F}_p[X]$ then
>
> $$Q_n = \prod_{d|n} \prod_{P \in \mathcal{P}_d} P$$

Proof. As we just seen if $P \in \mathcal{P}_d$ and $d|n$ then $P|Q_n$. Since all such polynomials are relatively prime and Q_n has no multiple roots (as result no multiple factors) then

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

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

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

From Remark 3.5 $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Theorem 3.9 says that $d|n$. 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. Example 3.12 Let $p = n = 2$. The monic irreducible polynomials in $\mathbb{F}_2$ whose degree divides 2 are: X, $X+1$ and X^2+X+1. As you can see

$$X(X+1)(X^2+X+1) = X^4+X = X^4-X$$

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

3.4 Multiplicative group and automorphism group of a finite field

> ! Important
>
> **Theorem 3.15** Let K be a field and G be a finite Subgroup of $K^\times$ then G is a Cyclic group. Not every finite group is cyclic. For instance the non-abelian group S_3 consists of 6 elements but it is not cyclic.

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

Let $\psi(d)$ - is the number of elements of order d in G. We need $\psi(N) \neq 0$ and we know that $N = \sum \psi(d)$.

Let also $\phi(d)$ - is the number of elements of order d in $\mathbb{Z}/N\mathbb{Z}$. As $\mathbb{Z}/N\mathbb{Z}$ contains a single (cyclic) subgroup of order d for each $d|N$. $\phi(d)$ 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 $\psi(d) = \phi(d)$. If no element of order d in G then $\psi(d) = 0$ otherwise if $x \in G$ has order d then $x^d = 1$ or x is a root of the following polynomial $x^d - 1$. The roots of the polynomial forms a cyclic subgroup of G. So G as well as $\mathbb{Z}/N\mathbb{Z}$ has a single cyclic subgroup of order d (which is cyclic) or no such group at all.

If $\psi(d) \neq 0$ then exists such a subgroup and $\psi(d)$ is equal to the number of generators of that group or $\phi(d)$.

In particular $\psi(d) \leq \phi(d)$ 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.

□

> i **Corollary 3.16** 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 $\mathbb{F}_p$.

Proof. We can take $\alpha =$ generator of $K^\times$.

□

> i **Corollary 3.17** The group of automorphism of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is cyclic and generated by Frobenius map: $F_p : x \to x^p$.

Proof. As we know from Theorem 3.8: $\forall x \in \mathbb{F}_{p^n} : x^{p^n} = x$ so $F_p^n = \mathrm{id}$. As result the order of $\langle F_p \rangle$ is no greater than n. Lets prove that the $\mathrm{ord} F_p = n$.

Really if $m < n$ then $x^{p^m} - x = 0$ has $p^m < p^n$ roots and F_p^m cannot be identity. Finally 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 so

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

and as we have n of them (Automorphisms) then

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

and the group is cyclic generated by F_p.

□

3.5 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 over K

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

that is also extended to an Automorphism on E.

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

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

But for $\mathrm{char} K = p$ there can be a case when $P' = 0$ for a non constant polynomial thus $P | P'$ 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 $p | i$ 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 $p^h \nmid i$.

> **Proposition 3.19** Let $P(X) = Q(X^{p^r})$ and $Q' \neq 0$ i.e. $\gcd(Q, Q') = 1$ then Q does not have multiple roots but all roots of P have multiplicity p^r.

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

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

and λ is not a root of $S(X^{p^r})$. Thus we just got that multiplicity of λ is p^r.

□

Definition 3.20 (Separable polynomial). $P \in K[X]$ irreducible polynomial is called separable if $\gcd(P, P') = 1$.

Definition 3.21 (Degree of separability). $d_{\text{sep}}(P) = \deg Q$ (as above).

Definition 3.22 (Degree of inseparability). $d_i(P) = \frac{\deg P}{\deg Q}$ $(= p^r$ in Proposition 3.19).

Definition 3.23 (Pure inseparable polynomial). P is pure inseparable if $d_i = \deg P$. Then $P = X^{p^r} - a$.

Definition 3.24 (Separable element). Let L be an Algebraic extension of K then $\alpha \in L$ is called separable(inseparable) if its Minimal polynomial $P_{\min}(\alpha, K)$ has the property. Note: the separable element is also Algebraic element because it has minimal polynomial.

Proposition 3.25 (On number of homomorphisms). If α is separable on K then the number of Homomorphisms over K from K to $\bar{K}$

$$|\text{Hom}_K(K(\alpha), \bar{K})| = \deg P_{\min}(\alpha, K)$$

in general

$$|\text{Hom}_K(K(\alpha), \bar{K})| = d_{\text{sep}} P_{\min}(\alpha, K)$$

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

□

3.6 Separable degree, separable extensions

We want to generalize Proposition 3.25 for any field extension (not necessary $K(\alpha)$). Let L be a finite extension of K.

Definition 3.26 (Separable degree). $[L : K]_{\text{sep}} = |\text{Hom}_K(L, \bar{K})|$
As we know if $L = K(\alpha)$ then Separable degree is a number of distinct roots of minimal polynomial $P_{\min}(\alpha, K)$.

Definition 3.27 (Separable extension). L is separable over K if $[L : K]_{\text{sep}} = [L : K]$.

Definition 3.28 (Inseparable degree).

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

Important

Theorem 3.29 (About separable extensions).

1. If $K \subset L \subset M$ then $[M : K]_{\text{sep}} = [M : L]_{\text{sep}}[L : K]_{\text{sep}}$ 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. $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, where α_i is separable over K
   d) $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, where α_i is separable over $K(\alpha_1, \alpha_2, \dots, \alpha_{i-1})$

Tip

Remark 3.30 That holds if we replace separability with pure inseparability.

3.7 Perfect fields

Definition 3.33 (Perfect field). Let K is a field and char$K = p > 0$. K is perfect if Frobenius homomorphism is a Surjection.

Example 3.3. Example 3.34

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 $a = F_p(\alpha)$
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 $\text{Im}(F_p) = \mathbb{F}_p(X^p) \neq \mathbb{F}_p(X)$

Important

Theorem 3.35 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 $P(X) = Q(X^{p^r}) = \sum_i a_i (X^{p^r})^i$ but as soon as my field is perfect then I can extract p-root of a_i and do it repeatedly. I.e. $\exists b_i \in K$ such that $b_i^{p^r} = a_i$. Therefore

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

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

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

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

□

---

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 $\alpha_1, \dots, \alpha_r$ then the number of Homomorphisms over K from L to $\bar{K}$ denoted by $|\mathrm{Hom}_K(L, \bar{K})|$ is equal to $[L : K]$. In general

$$[L : K]_{\mathrm{sep}} = |\mathrm{Hom}_K(L, \bar{K})| \leq [L : K].$$

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.

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 $f : M \times N \to P$, then $\exists!$ $\tilde{f}$ - homomorphism of A-modules such that $f = \tilde{f} \circ \phi$.
The property characterize the pair $(\phi, M \otimes N)$. Really if have another pair $(\phi', M \otimes' N)$ 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). If we have two objects $(\phi, M \otimes N)$ and $(\phi', M \otimes' N)$ which both satisfies Universal property than there is an unique Isomorphism between them:

$$(\phi, M \otimes N) \cong (\phi', M \otimes' N)$$

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

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

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

It can be shown that $M \times N \to E/F$ is bilinear and has the desired Universal property.

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

□

Tip

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.

4.2 Tensor product of modules

4.2.1 Advantages of the universal property

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

4.2.2 Several examples of universal property usage

Example 4.1. Example 4.6 (Commutativity proof). We want to prove that $M \otimes_A N \cong N \otimes_A M$

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

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

> **Corollary 4.7** $A \otimes_A M \cong M$

If we have that M is generated by $e_1, e_2, \dots$ and N is generated by $\varepsilon_1, \varepsilon_2, \dots$ than $M \otimes_A N$ is generated by pairs $e_i \otimes \varepsilon_j$. It's obvious.

More complex fact is the following:

> **Proposition 4.8** Let M and N are Free modules with corresponding basises $e_1, e_2, \dots, e_n$ and $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m$ than $M \otimes_A N$ is also free module with basis $e_i \otimes \varepsilon_j$ 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 $(\sum a_i e_i, \sum b_j \varepsilon_j)$ to $a_{i_0} b_{j_0}$. It's bilinear 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 $e_{i_0} \otimes \varepsilon_{j_0}$ to 1 and all others to 0. So if $\sum \alpha_{ij} e_i \otimes \varepsilon_j = 0$ then applying $\tilde{f}_{i_0,j_0}$ for all indices one can get that $\forall i, j : \alpha_{ij} = 0$.

□

In particular for the Vector space the tensor product is defined in the same way: the tensor product of 2 vector spaces with basises $e_1, e_2, \dots, e_n$ and $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m$ is another vector space with the following basis $e_i \otimes \varepsilon_j$ i.e. the definition does not take into consideration the Universal property.

> **Proposition 4.9** (Associative). $(M_1 \otimes_A M_2) \otimes_A M_3 \cong M_1 \otimes_A (M_2 \otimes_A M_3)$

4.3 Base change

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

I can of course make N into A-module (just forgetting the additional A-algebra structure). But we can also make B-module on M (that is not a trivial thing) by considering $B \otimes_A M$. We can introduce B-module structure on $B \otimes_A M$ by $b \cdot (b' \otimes m) = (b \cdot b') \otimes m$

Example 4.2. Example 4.10 (The complexification of a real vector space). We can "make" $\mathbb{R}^{2n}$ from $\mathbb{C}^n$ by forgetting the complex structure. The $\mathbb{C}^n$ has the following basis $e_1, \dots, e_n$. The $\mathbb{R}^{2n}$

has the following one $e_1, \dots, e_n, ie_1, \dots, ie_n$. Now we forgot about multiplication rules for $i = \sqrt{-1}$ and denote ie_i as v_i. In the case the basis for $\mathbb{R}^{2n}$ is the following one: $e_1, \dots, e_n, v_1, \dots, v_n$.

But we can also do the following constructions $\mathbb{R}^n \to \mathbb{C}^n = \mathbb{C} \otimes \mathbb{R}^n \to \mathbb{R}^{2n}$

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

Proposition 4.11 In general we have the following. If M - free A-module with basis $e_1, \dots, e_n$ then $B \otimes_A M$ is a free B module with basis $1_B \otimes e_1, \dots, 1_B \otimes e_n$.

Tip

Remark 4.12 We have the following maps.

- For A-modules: $\alpha : M \to B \otimes_A M$ which makes a B-module from an A-module.
- For B-modules: $\mu : B \otimes_A N \to N$.

Important

Theorem 4.13 (Base-change). Let A is a Ring and B is A-algebra. Let also M is an A-Module and N is B-module.
$\mathrm{Hom}_A(M, N) \leftrightarrow \mathrm{Hom}_B(B \otimes_A M, N)$
I.e. the homomorphisms are the same or in other words the corresponding groups of homomorphisms are isomorphic: $\mathrm{Hom}_A(M, N) \cong \mathrm{Hom}_B(B \otimes_A M, N)$

4.4 Examples. Tensor product of algebras

Proposition 4.14 If $I \subset A$ - is an Ideal so my B - A algebra will be $B = A/I$ then $A/I \otimes_A M \cong M/IM$ where IM is a sub-module of M.

Several examples:

Example 4.3. Example 4.15 Let $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$ what will we obtain? $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}/(2) \cdot \mathbb{Z}/3\mathbb{Z}$

but 2 is invertible: $2^{-1} = -1 \bmod 3$ thus $(2)\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$ and as result $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}/\mathbb{Z}/3\mathbb{Z} = 0$

Example 4.4. Example 4.16 Another obvious example $B \otimes_A A[X] \cong B[X]$ and more interesting one $B \otimes_A A[X]/(P) \cong B[X]/(P)$, where (P) becomes an ideal generated by P in $B[X]$.

4.4.1 Tensor product of A-algebras

Let B, C are A-algebras. The following maps form an algebra structure on A: $\alpha : A \to B, \quad \beta : A \to C$

New A-algebra $B \otimes_A C$: is a ring with respect to the following operation $(b \otimes c) \cdot (b' \otimes c') = (b \cdot b') \otimes (c \cdot c')$

The tensor product has the following:

Definition 4.17 (Universal property). Let we have the following maps $\alpha : A \to B, \quad \beta : A \to C$, $\phi : B \to B \otimes_A C, \quad \psi : C \to B \otimes_A C$
Then for any A-algebra D one has $\mathrm{Hom}_A(B \otimes_A C, D) \leftrightarrow \mathrm{Hom}_A(B, D) \times \mathrm{Hom}_A(C, D)$
i.e. if I have some Homomorphism $h \in \mathrm{Hom}_A(B \otimes_A C, D)$ this is the same as giving 2 homomorphisms $f \in \mathrm{Hom}_A(B, D)$ and $g \in \mathrm{Hom}_A(C, D)$.

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

Let consider next example. We will start with the following $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$ therefore $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X]/(X^2+1) \cong \mathbb{C}[X]/(X^2+1)$

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

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

How we can get the zero divisors? The element $X + i$ is a zero divisor in $\mathbb{C}[X]/(X^2+1)$ because $(X+i)(X-i) \equiv 0 \bmod (X^2+1)$.

4.5 Relatively prime ideals. Chinese remainder theorem

Definition 4.18 (Relatively prime ideals). Let A - Ring and I, J are Ideals. I and J are relatively prime if $I + J = A$.

Lemma 4.19

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

Important

Theorem 4.20 (Chinese remainder). Let $I_1, \dots, I_n$ - ideals and map $\pi : A \to A/I_1 \times \cdots \times A/I_n$ defined as follows $\pi(a) = (a \bmod I_1, \dots, a \bmod I_n)$
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 $A/\cap I_k \cong A/\prod I_k \cong \prod(A/I_k)$

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

Proposition 4.21

1. If A is an Integral domain then A is a field.
2. (replacing the first one) Any Prime ideal of A is a Maximal ideal

Proof. Well, I shall prove only the first part, the second part is just a consequence of definitions. In fact, a factor over a prime ideal, a quotient over a prime ideal is an integral domain, and a quotient over a maximal ideal is a field.

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

Tip

Remark 4.22 Let A is a K-algebra and m is a maximal ideal of A. Then A/m is also K-algebra.

Important

Theorem 4.23 (Structure of finite K-algebra). Let A be a finite K-algebra i.e. $\dim_K A < \infty$. Then

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

Several examples: $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \times \mathbb{C}$

Another example $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

And you see that those algebras are Cartesian products of fields. So all \$n_is 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 come from inseparable extensions.