125 - Fields extensions. Examples and applications.

1 On fields extensions

1.1 About extensions

Definition 1. Let K be a field, a field L is a field extension of K if $K \subset L$ and the field operations over K and L are the same. We say that K is a subfield of L and we denote L/K.

Example 2. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and then $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{R}$ are fields extensions.

Definition 3. Let L/KW be a field extension and $\mathcal{S}$ a subset of L, we define $K(\mathcal{S})$ as the smallest extension of K which contains $\mathcal{S}$.

Example 4. For example :

- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{R}\}$
- $\mathbb{C} = \mathbb{R}(i)$
- The nth cyclotomic field is the smallest extension of $\mathbb{Q}$ wich contains the set of the nth roots of unity : $\mathbb{Q}_n = \mathbb{Q}(\{e^{i2k\pi/n} \mid k \in 0, .., n\})$.

Proposition 5. If L is an extension of K then L is a K-vectorial space.

Definition 6. Let L/K be an extension field, the degree $[L : K]$ of this extension is the dimension of L as a K-vectorial space.

Example 7. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{C}, \mathbb{R}] = 2$

Lemma 8 (Telescopic basis). Let M/L and L/K two fields extensions. Then $[M : K] = [M : L][L : K]$.

Example 9. $X^3 + X + 1$ is irreducible over $\mathbb{F}_2$ and $\mathbb{F}_{16}$.

1.2 Linear algebra and fields extensions

Proposition 10. Let $M \in \mathcal{M}_{m,n}(K) \subset \mathcal{M}_{m,n}(L)$ where L/K is a field extension, the rank of M as an element of $\mathcal{M}_{m,n}(K)$ is the same as the rank of M as an element of $\mathcal{M}_{m,n}(L)$. If $m = n$, the characteristic and minimal polynomials of M are the same in K and L.

Corollary 11. Let u_K be the linear mapping associated with M over K and u_L over L then,

- u_K is injective if and only if u_L is injective
- u_K is surjective if and only if u_L is surjective.

Application 12. $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is diagonalizable over $\mathbb{C}$ but not over $\mathbb{R}$.

Proposition 13. The invariants of tensors are invariant by fields extension.

Application 14. Let L/K be a field extension and $M, N \in \mathcal{M}_n(K)$. M and N are similar over K if and only if they are similar over L.

1.3 Algebraic and transcendental elements

Definition 15. If L/K is a field extension, an element a of L is called an algebraic element over K if a is a root of a non-zero polynomial of $K[X]$. A non-algebraic element is called transcendental.

Example 16. $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ but π and e are not.

Definition 17. Let $a \in L$ be an algebraic element over K, the set of annulator polynomials of a is a non-zero ideal of $K[X]$. The unique monic generator of this ideal is called the minimal polynomial of a and is represented by $\mu_{K,a}$.

Example 18. $\mu_{\mathbb{R},i} = X^2 + 1$, $\mu_{\mathbb{R},j} = X^2 + X + 1$, $\mu_{\mathbb{Q},\sqrt{2}} = X^2 - 2$

Proposition 19. The minimal polynomial of $a \in L$ over K is irreducible over K.

Definition 20. Let L/K be a field extension and $a \in L$ algebraic over K. The degree of a as an algebraic element is the degree of $\mu_{K,a}$.

Theorem 21. Let L/K a field extension and $a \in L$. Then a is algebraic over K if and only if $K(a) = K[a]$ if and only if the K-vectorial space $K[a]$ has finite dimension.

Proposition 22. If the degree of a is $n \in \mathbb{N}$, then $[K(a) : K] = n$.

Theorem 23. Let L/K be a field extension, the set of algebraic elements of L over K is a field.

Theorem 24 (Primitive element theorem). If $\mathrm{char}(K) = 0$ and if L/K is a field extension of finite degree, then there exists $a \in L$ such that $L = K(a)$.

Definition 25. The extension L/K is algebraic if every element of L is algebraic over K.

Example 26. Extensions of finite degree are algebraic.

Proposition 27. Let L/K an extension. Then L is algebraic and finite if and only if there exist $a_1, .., a_n \in L$ algebraic over K such that $L = K(a_1, ..., a_n)$.

Proposition 28. Let L/K be a field extension, and $a, b \in L$ be two algebraic elements. If $\mu_{K,a} = \mu_{K,b}$, then there exists a field isomorphism $f : K(a) \to K(b)$ such that $f(a) = b$ and $\forall x \in K, f(x) = x$.

Example 29. Let p be a prime number and ω be a pth root of unity. Then for all $1 \leqslant k \leqslant p-1$, there exists a field isomorphism $\sigma_k : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega^k)$ such that $\sigma_k(\omega) = \omega^k$.

2 Building extensions

2.1 Rupture field and splitting field

Definition 30. Let K be a field and $P \in K[X]$ be a non constant (irreducible) polynomial. A rupture field of P over K is an extension L/K such that P has a root $\alpha \in L$ and $L = K(\alpha)$.

Example 31. For examples:

- $\mathbb{Q}_n$ is a rupture field over $\mathbb{Q}$ of Φ_n.
- $\mathbb{Q}(\sqrt[3]{2})$ is a rupture field of $X^3 - 2$ over $\mathbb{Q}$.
- $\mathbb{C}$ is a rupture field of $X^2 + 1$ over $\mathbb{R}$.

Theorem 32. There exists a rupture field and all rupture fields are isomorphic to $K[X]/(P)$ (P irreducible), especially: $[K(\alpha) : K] = \deg(P)$.

Application 33. Let L/K be an extension of degree m and $P \in K[X]$ of degree n such that $\gcd(n, m) = 1$. If P is irreducible over K then P is irreducible over L.

Example 34. The polynomial $X^3 - 2$ has two distincts, although isomorphic, rupture fields over $\mathbb{Q}$: $L_1 = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ and $L_2 = \mathbb{Q}(j\sqrt[3]{2}) \not\subset \mathbb{R}$.

Example 35. If K is finite and $P \in K[X]$ is irreducible, then the rupture field of P over K has $|K|^{\deg(P)}$ elements.

Definition 36. Let K be a field and $P \in K[X]$ be a non constant polynomial. A splitting field of P over K is an extension L/K such that P splits over L, i.e. $P = \prod_i (X - a_i)^{m_i}$ with $a_i \in L$, and such that $L = K(a_1, ..., a_n)$.

Example 37. For examples:

- $\mathbb{Q}_n$ is a splitting field over $\mathbb{Q}$ of Φ_n.
- $\mathbb{Q}(j, \sqrt[3]{2})$ is a splitting field of $X^3 - 2$ over $\mathbb{Q}$.

Remark 38. If $\deg(P) = 2$ and P is irreducible, then a rupture field is a splitting field.

Theorem 39. A splitting field (SF) exists and all splitting fields are K-isomorphic. Moreover, $[SF : K] \leqslant (\deg(P))!$.

Remark 40. A splitting field of P over K is the smallest extension L/K that contains all roots of P.

2.2 Application : the finite fields

Proposition 41. Let K be a finite field and $\mathrm{char}(K)$ be the characteristic of K. Then, $\mathrm{char}(K) = p$, where p is a prime, and there exists an integer n such that $|K| = p^n$.

Remark 42. There is no finite field with exactly 6 elements.

Proposition 43. Let K be a finite field, $\mathrm{char}(K) = p$. The map $\phi_p : K \to K$ defined by $\phi_p(x) = x^p$ is a field morphism called Frobenius morphism. As K is finite, ϕ_p is an automorphism.

Theorem 44. Let p be a prime, n be a positive integer. Let $q = p^n$. Then:

- A field K with q elements does exist. K is the splitting field of the polynomial $X^q - X$ over $\mathbb{F}_p$.
- K is unique up to isomorphism and called $\mathbb{F}_q$.

Example 45. Let $P = X^2 + 1$ and $Q = X^2 + X + 2$. $\mathbb{F}_9$ is isomorphic to the field defined by $\mathbb{F}_3[X]/(P)$ and also isomorphic to $\mathbb{F}_3[X]/(Q)$.

Proposition 46. $\mathbb{F}_{p^r}$ is a subfield of $\mathbb{F}_{p^d}$ if and only if r divides d.

Example 47. The subfields of $\mathbb{F}_{729}$ are $\mathbb{F}_3$, $\mathbb{F}_9$ and $\mathbb{F}_{27}$.

Counterexample 48. $\mathbb{F}_8$ is not a subfield of $\mathbb{F}_{16}$.

Proposition 49. $(\mathbb{F}_q^*, \times)$ is a cyclic group, isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$.

Remark 50. Every subgroup of $\mathbb{F}_q^*$ is also cyclic.

Example 51. Let $\alpha = \overline{X}^P$ and $\beta = \overline{X}^Q$ be the classes of X in $\mathbb{F}_3[X]/(P)$ and in $\mathbb{F}_3[X]/(Q)$. Then:

- $\alpha + 1$ is a generator of $\mathbb{F}_9^*$,
- β is a generator of $\mathbb{F}_9^*$,
- The isomorphism between $\mathbb{F}_3[X]/(P)$ and $\mathbb{F}_3[X]/(Q)$ is given by $\phi : \alpha + 1 \mapsto \beta$.

Remark 52. In general it is very hard to find a generator of $\mathbb{F}_q^*$. Besides, there is no canonical isomorphism between two finite fields of same cardinal.

2.3 Algebraic closure

Definition 53. Let K be a field, K is an algebraically closed field if every polynomial over K is splitted.

Proposition 54. There is equivalence between:

- K is algebraically closed,
- every irreducible polynomial has degree one,
- every non constant polynomial has at least one root,
- every algebraic extension of K is trivial.

Proposition 55. Let K be a field, the set of the algebraic elements over K is algebraically closed.

Example 56. $\mathbb{C}$ is algebraically closed.

Counterexample 57. $\mathbb{Q}$ and the set of the real algebraic elements over $\mathbb{Q}$ are not algebraically closed.

Counterexample 58. A finite field cannot be algebraically closed.

Definition 59. Let K be a field, an algebraic closure of K is an algebraically closed extension.

Example 60. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$, more generally the set of the algebraic elements over K is an algebraic closure of K.

Theorem 61 (Steinitz). Every field K has an algebraic closure, and it is unique up to isomorphism (admitted).

Application 62 (Dunford). Let K be a field, n a non zero integer and $M \in \mathcal{M}_n(K)$. There exist $D \in \mathcal{M}_n(K)$ diagonalizable over an extension of K and $N \in \mathcal{M}_n(K)$ nilpotent such that:

- $DN = ND$,
- $M = D + N$,
- $D, N \in K[M]$.

3 Two applications

3.1 Geometric constructions

Definition 63. Let $C \subset \mathbb{C}$ be a set of points. A line is constructible from C if it passes through two distinct points of C. A circle is constructible from C if its center is a point of C, and if its radius is the distance between two points of C.

Definition 64. Let $C_0 = \{0, 1\} \subset \mathbb{C}$. We define recursively C_{n+1} as the union of C_n with the set of all points that are intersection of either

- two constructible lines from C_n,
- a constructible line and a constructible circle from C_n,
- two constructible circles from C_n.

The set $C = \cup_{n\in\mathbb{N}} C_n$ is called the set of constructible points.

Definition 65. A complex number is constructible if it is the affix of a constructible point. We assimilate the set of constructible complex numbers with the set C of constructible points.
A real number is constructible if it is one of the coordinates of a constructible point. The set of constructible real numbers is denoted $C_\mathbb{R}$.

Remark 66.
- Given a constructible line D and a constructible point A, it is possible to draw the line that is parallel or perpendicular to D and that passes through A.
- Given two constructible points A and B, it is possible to draw the perpendicular bisector of the segment $[AB]$.
- A complex number $z = x + iy$ is constructible if and only if x and y are constructible real numbers.

Proposition 67. If $x \in \mathbb{R}_+$ is constructible, then $\sqrt{x}$ is constructible.

Theorem 68. The set $C_\mathbb{R}$ of constructible numbers is a subfield of $\mathbb{R}$.

Remark 69. As $\mathbb{Q}$ is the smallest subfield of $\mathbb{R}$, then $\mathbb{Q} \subset C_\mathbb{R}$.

Example 70. The numbers 7, $\frac{-2}{3}$, $\frac{1+\sqrt{5}}{2}$, $\sqrt[4]{13}$ are constructible.

Theorem 71 (Wantzel). Let $x \in \mathbb{R}$. Then x is constructible if and only if there exists $p \geqslant 1$ and a sequence of subfields $K_1 \subset ... \subset K_p$ of $\mathbb{R}$ such that

- $K_1 = \mathbb{Q}$,
- $[K_{i+1} : K_i] = 2$ for all $1 \leqslant i \leqslant p - 1$,
- $x \in K_p$.

Corollary 72. Every constructible number is algebraic over $\mathbb{Q}$. Moreover, there exists $p \in \mathbb{N}$ such that its degree is 2^p.

Application 73. The following constructions are impossible:

- squarring the circle because π is not a constructible number,
- doubling the cube because $\sqrt[3]{2}$ is not a constructible number.

Definition 74. An angle θ is constructible if $e^{i\theta}$ (or $\cos(\theta)$ or $\sin(\theta)$) is constructible. The n-sided regular polygon is constructible if $\frac{2\pi}{n}$ is constructible.

Lemma 75. If $\gcd(m, n) = 1$, then the mn-sided regular polygon is constructible if and only if the m-sided and the n-sided regular polygons are constructible.

Theorem 76 (Gauss-Wantzel). We have :

- For all $\alpha \in \mathbb{N}$, $\frac{2\pi}{2^\alpha}$ is constructible.
- Let $p \geqslant 3$ be a prime, and $\alpha \in \mathbb{N}$. Then $\frac{2\pi}{p^\alpha}$ is constructible if and only if $\alpha = 1$ and p is a Fermat prime number.

Example 77. The n-sided regular polygon is constructible for $n = 3, 4, 5, 6, 15, 17, 257$.
The n-sided regular polygon is not constructible for $n = 7, 9, 11, 100$.

Example 78. See the appendix for the construction of the regular pentagon.

3.2 Building error correcting codes

Definition 79. A binary cyclic code of block length n (odd) is the set of the polynomials $c \in \mathbb{F}_2[X]$ of degree lower than $n - 1$ such that $c(\zeta) = 0$ for all ζ in a set $\mathcal{S}$ of nth roots of unity over an extension of $\mathbb{F}_2$.

Proposition 80. Let $\mathcal{C}$ be a code defined by the set $\mathcal{S} = \{\zeta_1, ..., \zeta_k\}$ of nth roots of unity. If $P = \mathrm{lcm}(\mu_{\mathbb{F}_2,\zeta_1}, ..., \mu_{\mathbb{F}_2,\zeta_k})$ then $\mathcal{C} = P \times \mathbb{F}_2[X] \mod (X^n)$. Then P is called the generator polynomial of $\mathcal{C}$ and $P | X^n - 1$.

Example 81. Let $\zeta = \overline{X}$ in $\mathbb{F}_2[X]/(X^3 + X + 1)$. The code defined by the set $\mathcal{S} = \{\zeta\}$ is $\mathcal{C}_1 = P \times \mathbb{F}_2[X] \mod X^7$ where $P = X^3 + X + 1$.

Definition 82. Let s be a non-zero integer, $\delta > 1$ and $n = 2^s - 1$. Let $\zeta \in \mathbb{F}_{2^s}$ be a primitive root of unity. The BCH code of distance d and root ζ is the binary cyclic code defined by the set of roots $\mathcal{S} = \{\zeta, \zeta^2, ..., \zeta^{\delta-2}\}$.

Proposition 83. Let s be a non-zero integer and $n = 2^s - 1$.

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

and Φ_n is the product of irreducible polynomials of degree s over $\mathbb{F}_2$.

Application 84. In the same context, let P be a irreducible factor of Φ_n over $\mathbb{F}_2$ then $\overline{X} \in \mathbb{F}_2[X]/(P)$ is a primitive root of unity, its minimal polynomial is P : then BCH codes can be built.