Algèbre III : Anneaux, polynômes et théorie de Galois

21 février 2020

Table des matières

Chapitre 1

Anneaux

1.1 Rappels sur les anneaux commutatifs

Définition 1.1. *Un anneau commutatif est un groupe abélien* $(A, +)$ *muni d'une application :*

$$A \times A \to A : (a, b) \to a.b = ab$$

tel que :

1. $\forall a, b, c \in A,\ (ab)c = a(bc)$.
2. $\exists 1_A \in A,\ \forall a \in A,\ 1_A a = a 1_A = a$.
3. $\forall a, b \in A,\ ab = ba$ *(commutativité).*
4. $\forall a, b, c \in A,\ a(b + c) = ab + ac$. *(distributivité).*

Exemple. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}[X]$, $\mathbb{R}[X]$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proposition 1.2. *Soit* A *un anneau commutatif. Alors* $A[X]$ *est un anneau commutatif.*

Démonstration. □

Remarque. $(A[X])[Y] = A[X, Y]$, *ie les polynomes à deux variables sont les polynomes construits sur un anneau de polynomes.*

Proposition 1.3. *Soient* A *et* B *deux anneaux commutatifs. Alors* $A \times B$ *est un anneau commutatif (avec la multiplication composante par composante).*

Démonstration. □

Proposition 1.4. *Soit* $(A_i)_{i \in I}$ *une famille d'anneaux commutatifs. Alors* $\prod_{i \in I} A_i$ *est un anneau commutatif.*

Démonstration. □

Exemple. *$\mathbb{Q}^{\mathbb{N}}$ est un anneau commutatif.*

Remarque.

1. *1_A est unique.*
2. *$\forall a \in A$, $0_A a = 0_A = a 0_A$.*
3. *$-1_A a = -a$.*
4. *$0_A = 1_A \Leftrightarrow A = \{0_A\}$.*
5. *Si on enlève la distributivité à gauche dans la définition, alors on obtient la définition d'un anneau. Exemple : $M_n(\mathbb{R})$, $M_n(\mathbb{C})$, $End(G)$ (G groupe abélien).*

Définition 1.5. *On définit $A^\times$ comme l'ensemble des inversibles de A, c'est-à-dire que :*

$$A^\times = \{a \in A \,|\, \exists b \in A, ab = ba = 1_A\}$$

Remarque. *Si $(A, .)$ est un monoïde, alors $(A^\times, .)$ est un groupe abélien.*

Exemple. *$\mathbb{Z}^\times = \{1, -1\}$, $\mathbb{Q}^\times = \mathbb{Q} \backslash \{0\}$, $\mathbb{R}^\times = \mathbb{R} \backslash \{0\}$, $\mathbb{R}[X]^\times = \mathbb{R}^\times$, $\mathbb{Z}[X]^\times = \mathbb{Z}^\times$.*

Définition 1.6. ***Un corps*** *est un anneau non nul tel que $A^\times = A \backslash \{0_A\}$.*

Définition 1.7. ***Un sous-anneau*** *B de A est un sous-groupe $(B, +)$ tel que $1_A \in B$ et $\forall a, b \in B$, $ab \in B$.*

Proposition 1.8. *Soient B et C deux sous-anneaux de A, alors $B \cap C$ est un sous-anneau de A. La propriété reste vraie pour une intersectionq quelconque.*

Démonstration. □

Proposition 1.9. *Soit B sous-anneau de A, alors $B^\times$ sous-anneau de $A^\times$.*

Démonstration. □

Définition 1.10. *$\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$ est l'ensemble des entiers de Gauss.*

Proposition 1.11. *$\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, dont les élements inversibles sont $1, -1, i, -i$.*

Démonstration. □

Proposition 1.12. *$\mathbb{Q}[i] = \{a + bi \,|\, a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$.*

Démonstration. $\square$

Définition 1.13. ***Un morphisme d'anneau*** *f entre deux anneaux A et B est un morphisme de groupe tel que $f(ab) = f(a)f(b)$ et $f(1_A) = 1_B$.*

De plus, c'est

1. ***un endormorphisme*** *si $A = B$.*
2. ***un isomorphisme*** *si f est bijectif.*
3. ***un automorphisme*** *si f est un isomorphisme et un endormorphisme.*
4. ***un morphisme de corps*** *si c'est un morphisme d'anneau entre deux corps.*

Remarque. *Si $f : A \to B$ est un morphisme d'anneau, alors $f(A^\times) \subseteq B^\times$, et*

$$f^* : (A^\times, .) \to (B^\times, .) \tag{1.1}$$

est un morphisme de groupe.

Proposition 1.14. *Il existe un unique morphisme d'anneau entre $\mathbb{Q}$ (resp $\mathbb{Z}$) et $\mathbb{C}$.*

Démonstration. Si on a un morphisme f, on a par récurrence $\forall n \in \mathbb{Z}, f(n) = n$. D'où, le seule morphisme est $(Id_{\mathbb{C}})_{|\mathbb{Z}}$.

La démonstration est la même pour $\mathbb{Q}$. $\square$

Proposition 1.15. *Il existe seulement deux morphismes d'anneaux entre $\mathbb{Q}[i]$ (resp $\mathbb{Z}[i]$) et $\mathbb{C}$.*

Démonstration. $\square$

Corollaire 1.16.

1. $Aut_{corps}(\mathbb{Q}) = Aut_{anneau}(\mathbb{Q}) = \{Id\}$
2. $Aut_{anneau}(\mathbb{Z}) = \{Id\}$

Démonstration. En effet, si d'autres automorphismes existeraient, on pourrait étendre l'ensemble d'arrivé en $\mathbb{C}$, et ils resteraient des morphismes. $\square$

Questions. *Combien il y a d'automorphismes de corps sur $\mathbb{C}$? Sur $\mathbb{R}$? Ici pour $\mathbb{C}$*

Pour $\mathbb{R}$, le seul automorphisme continu est l'identité. En effet, comme $\mathbb{Q}$ est dense dans $\mathbb{R}$, on a une suite d'élément de $\mathbb{Q}$ qui tend vers $x \in \mathbb{R}$. On a alors que $f(x)$ est la limite de la suite $f(x_n)$, où f maintenant est un morphisme de $\mathbb{Q}$ dans $\mathbb{R}$. Or, le seul morphisme est l'identité, donc $f(x) = x$ à la limite.

Pour $\mathbb{C}$, les seuls automorphismes sont l'identité et la conjugaison (même raisonnement que pour $\mathbb{R}$ en décomposant l'image de f en partie réelle et partie imaginaire).

Proposition 1.17. *Soient A, B, C trois anneaux. Soient $f : A \to B$ et $g : B \to C$ deux morphismes d'anneaux. Alors $g \circ f : A \to C$ est un morphisme d'anneau.*

Démonstration. □

Proposition 1.18.
1. *$f : A \to B$ isomorphisme d'anneau $\Rightarrow f^{-1} : B \to A$ isomorphisme d'anneau.*
2. *$Id_A : A \to A : a \to a$ est un isomorphisme d'anneau.*
3. *$(Aut_{anneau}(A), \circ)$ est un groupe.*
4. *Si A est un corps, $Aut_{anneau}(A) = Aut_{corps}(A)$.*
5. *Si $f : A \to B$ est un morphisme d'anneau, alors $Im(f)$ est un sous-anneau de B et $\ker(f)$ est un sous-groupe de A.*

Démonstration. □

Définition 1.19. *Soit A un anneau.* ***Un idéal de*** *A est un sous-groupe $(I, +)$ de $(A, +)$ tel que $\forall a \in I$, $\forall b \in A$, $ab \in I$.*

Exemple. – *$\{0_A\}$ et A sont des idéaux de A.*

Proposition 1.20. *Soit $f : A \to B$ où A et B sont deux anneaux commutatifs. Alors Im(f) est un sous-anneau de B, et ker(f) est un idéal de A.*

De plus on a :

1. *Si $Im(f)$ est un idéal, f est surjectif.*
2. *Si $Ker(f)$ est un sous-anneau, $B = \{0_B\}$.*

Démonstration. 1. On doit montrer que$Im(f) = B$. Comme f morphisme, $1 \in Im(f)$, on a donc que $Im(f) = B$ car $Im(f)$ est un idéal. 2. □

Proposition 1.21. *Les idéaux de $\mathbb{Z}$ sont les $\mathbb{Z}/n\mathbb{Z}$. Les idéaux de $\mathbb{Z}$ sont donc confondus avec les sous-groupes de $(\mathbb{Z}, +)$.*

Démonstration. □

Proposition 1.22. *Soit I et J deux idéaux d'un anneau commutatifs A tel que $I \subseteq J$. Alors J/I est un idéal de A/I.*

Démonstration. □

Définition 1.23 (Idéal principal)**.** *Un idéal I est un* ***idéal principal*** *si il est engendré par un seul élément. On note, si $a \in A$ engendre I, $I = (a)$.*

Définition 1.24 (Anneau principal)**.** *Un anneau A est un* ***anneau principal*** *si tout idéal est principal.*

Exemple. *1.* $\{0_A\} = (0_A)$, $A = (1_A)$

2. $(2)_{\mathbb{Z}} = 2\mathbb{Z} \neq \mathbb{Z}$.

3. $(2)_{\mathbb{Q}} = 2\mathbb{Q} = \mathbb{Q}$.

4. $I = \{2P(X) + XQ(X) \mid P, Q \in \mathbb{Z}[X]\}$ *est un idéal de* $\mathbb{Z}[X]$ *non principal.*

Définition 1.25. *Soit A un anneau. Soient $a, b \in A$. On dit que a* ***divise*** *b s'il existe $n \in \mathbb{Z}$ tel que $b = na$.*

Proposition 1.26. *a divise $b \Leftrightarrow (b) \subseteq (a)$.*

Démonstration. □

Exemple. *Soit $n, m \in \mathbb{Z}$. Alors $n|m \Leftrightarrow \mathbb{Z}/m\mathbb{Z} \subseteq \mathbb{Z}/n\mathbb{Z}$.*

Proposition 1.27. *Soient I, J deux idéaux d'un anneau A. alors*

1. *$I \cap J$ est le plus grand idéal de A contenu dans I et J*
2. *$I + J$ est le plus petit idéal contenant I et J (en particulier, c'est le plus petit sous-groupe contenant I et J).*

Nous pouvons généraliser à un nombre quelconque d'idéaux.

Démonstration. □

Proposition 1.28. *Si $n, m \in \mathbb{Z} \setminus \{0\}$, alors $n\mathbb{Z} \cap m\mathbb{Z} = ppcm(n, m)\mathbb{Z}$ et $n\mathbb{Z} + m\mathbb{Z} = pgcd(n, m)$*

Démonstration. □

Proposition 1.29. *Soit I un idéal de A. Alors, $I = A \Leftrightarrow I \cap A^\times \neq \emptyset \Leftrightarrow 1_A \in I$.*

Démonstration. □

Proposition 1.30. *Les seuls idéaux d'un corps $\mathbb{K}$ sont $(0_{\mathbb{K}})$ où $\mathbb{K}$.*

Démonstration. Soit I un idéal. S'il est nul, on a fini. Sinon on a un élément non nul $a \in I$. Comme K est un corps, $a^{-1} \in K$, et donc $a^{-1}a = 1 \in I$ car I idéal. Donc $I = K$. □

Corollaire 1.31. *Soit $\mathbb{K}$ un corps et L un anneau, et $f : \mathbb{K} \to L$ un morphisme d'anneau. Alors soit L est nul, soit f est injectif.*

Démonstration. $\square$

Exemple. *Soient* $\mathbb{K}$ *un corps et* E *un espace vectoriel non-nul sur* $\mathbb{K}$.

Alors l'application

$$f : \mathbb{K} \to End_{\mathbb{K}}(E) : \lambda \to f(\lambda) \tag{1.2}$$

où

$$f(\lambda) : E \to E : v \to \lambda v \tag{1.3}$$

est un morphisme d'anneau injectif.

1.2 Quotients

Proposition 1.32. *Soit* A *un anneau commutatif et soit* I *un idéal de* A. *La multiplication induit un sur* A *induit une structure d'anneau sur* $(A/I, +)$ *où*

$$(a + I)(b + I) = ab + I \tag{1.4}$$

et la projection

$$\pi_I : A \to A/I : a \to a + I \tag{1.5}$$

est un morphisme d'anneau surjectif.

De plus,

1. $\ker(\pi_I) = I$
2. $(A/I)^{\times} = \{a + I \in A/I \,|\, \exists b \in A \text{ tel que } ab^{-1} = I\}$

Démonstration. $\square$

Exemple.

1. $n \in \mathbb{Z}_0$, $A = \mathbb{Z}$, $I = n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ *anneau et*

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^{\times} &= \left\{a + n\mathbb{Z} \,|\, \exists b \in \mathbb{Z}, ab^{-1} \in n\mathbb{Z}\right\} &(1.6)\\ &= \{a + n\mathbb{Z} \,|\, \exists b, c \in \mathbb{Z} \text{ tel que } ab + nc = 1_A\} &(1.7)\\ &= \{a + n\mathbb{Z} \,|\, pgcd(a, n) = 1\} &(1.8)\end{aligned}$$

2. $(\mathbb{Z}/6\mathbb{Z})^{\times} = \{1 + 6\mathbb{Z} = 6\mathbb{Z}, -1 + 6\mathbb{Z} = 5 + 6\mathbb{Z}\}$

Proposition 1.33. *Soient* A *et* B *deux anneaux commutatifs et soit* $f : A \to B$ *un morphisme d'anneau. Soit* I *un idéal de* A.

Alors il existe un morphisme d'anneau

$$\overline{f} : A/I \to B \tag{1.9}$$

vérifiant

$$\overline{f} \circ \pi_I = f \Leftrightarrow I \subseteq \ker(f) \tag{1.10}$$

Dans ce cas, on a

1. $\mathrm{Im}(\overline{f}) = Im(f)$

2. $\ker(\overline{f}) = \ker(f)/I$

Démonstration. $\square$

Corollaire 1.34. *Soient A, B deux anneaux et soit $f : A \to B$ un morphisme d'anneaux.*

Alors

$$\overline{f} : A/\ker(f) \to \mathrm{Im}(f) : a + \ker(f) \to f(a) \tag{1.11}$$

est un isomorphisme d'anneaux

Démonstration. $\square$

1.3 Morphismes fondamentaux

1.3.1 Caractéristique d'un anneau

Proposition 1.35. *Soit A un anneau commutatif. Il existe un unique morphisme d'anneau $\mu_A : \mathbb{Z} \to A : n \to n1_A$ et $\exists c_A \in \mathbb{N}$ tel que $\ker \mu_A = c_A\mathbb{Z}$.*

Démonstration. $\square$

Définition 1.36. *c_A est appelé* ***la caractéristique de*** *A. En d'autres termes, la caractéristique d'un anneau est l'ordre de l'élément multiplicatif.*

Exemple. *La caractéristique de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ vaut 12.*

1.3.2 Anneaux de polynomes

Proposition 1.37. *Soit $f : A \to B$ un morphisme d'anneaux. Alors*

$$\tilde{f} : A[X] \to B[X] : P(X) = \sum_{i=1}^{k} a_k X^k \to \sum_{i=1}^{k} f(a_k) X^k \tag{1.12}$$

est un morphisme d'anneaux. De plus, $\tilde{f}_{|A} = f$. En d'autres termes, tout morphisme d'anneau peut être étendu dans l'anneau des polynômes.

Démonstration. $\square$

Exemple. *1. La conjugaison complexe étant un automorphisme d'anneaux de $\mathbb{C}$, la fonction*

$$\overline{f} : \mathbb{C}[X] \to \mathbb{C}[X] : \sum_{i=1}^{n} a_i X^i \to \overline{a_i} X^i \tag{1.13}$$

est un automorphisme d'anneaux.

2. *Soit* $n \in \mathbb{Z}$ *et soit* $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : a \to a + mod(n\mathbb{Z})$ *le morphisme surjectif de projection.*
   Alors

$$\tilde{\pi_n} : \mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}[X] \quad (1.14)$$

$$\sum_{i=1}^{n} a_i X^i \to \sum_{i=1}^{n} (a_i mod(n\mathbb{Z}))X^i \quad (1.15)$$

   est un morphisme d'anneau surjectif.
   Par factorisation, on obtient l'isomorphisme d'anneau

$$\mathbb{Z}[X]/n\mathbb{Z}[X] \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})[X] \quad (1.16)$$

1.3.3 Le corps des réels

Proposition 1.38. *Soit* $\mathcal{C}(\mathbb{Q}) = \{(a_n)_{n\in\mathbb{N}} \,|\, a_n$ *est une suite de Cauchy*$\}$. *Alors* $\mathcal{C}(\mathbb{Q})$ *est un sous-anneau de* $\mathbb{Q}^{\mathbb{N}}$

Démonstration. □

Définition 1.39. $\mathcal{C}_0(\mathbb{Q}) = \{(a_n)_{n\in\mathbb{N}} \,|\, lim a_n = 0\}$

Proposition 1.40. $\mathcal{C}_0(\mathbb{Q})$ *est un idéal de* $\mathbb{Q}^{\mathbb{N}}$.

Démonstration. □

Définition 1.41. $\mathbb{R} = \mathbb{Q}^{\mathbb{N}}/\mathcal{C}_0(\mathbb{Q})$

1.3.4 Evaluation interne

Proposition 1.42. *Soit* A *un anneau commutatif. Soit* $a \in A$.
Alors

$$eval_a : A[X] \to A : P(X) \to P(a) \quad (1.17)$$

est un morphisme d'anneau surjectif et $(eval_a)_{|A} = Id_A$.

Démonstration. □

Proposition 1.43. *Pour tout* $a \in A$,

$$\tau_a : A[X] \to A[X] : P(X) \to P(X-a) \quad (1.18)$$

est un automorphisme d'anneau avec $(\tau_a)^{-1} = \tau_{-a}$.

Démonstration. □

Proposition 1.44. *Pour tout $a \in A$,*

$$eval_a \circ \tau_a = eval_0 \tag{1.19}$$

Démonstration. $\square$

Corollaire 1.45. $\ker(eval_a) = \tau_a(\ker(eval_0)) = (X - a)$

Démonstration. $\square$

Proposition 1.46. *Pour tout $a \in A$, l'application*

$$A[X]/(X-a) \to A : P(X) \, mod(X-a) \to P(a) \tag{1.20}$$

est un isomorphisme d'anneaux.

On a donc $A[X]/(X-a) \xrightarrow{\sim} A$.

Démonstration. $\square$

1.3.5 Evaluation externe

Proposition 1.47. *Soient A et B deux anneaux commutatifs tel que A est un sous-anneau de B. Alors, pour tout $b \in B$, l'application d'évaluation en b*

$$eval_b : A[X] \to B : P(X) \to P(b) \tag{1.21}$$

est un morphisme d'anneau tel que $(eval_b)_{|A}$ est l'inclusion de A dans B.

De plus, $Im(eval_b) := A[b] :=$ le plus petit sous-anneau de B contenant A et b.

Démonstration. $\square$

1.4 Théorème chinois

1.4.1 Énoncé

Nous souhaitons, pour deux anneaux donnés, et sous certaines conditions, montrer que $A/(I \cap J)$ est isomorphe à $A/I \times A/J$.

Soient I, J deux idéaux de A. Alors, nous pouvons construire

$$f : A \to A/I \times A/J : a \to (a + I, a + J) \tag{1.22}$$

Nous avons $ker(f) = I \cap J$.

On a alors un morphisme injectif

$$\overline{f} : A/(I \cap J) \to A/I \times A/J \tag{1.23}$$

induit par f.

Il nous manque donc une condition, la surjectivité, pour avoir un isomorphisme entre ces deux anneaux. On en vient alors au théorème chinois :

Théorème 1.48. *Si $I + J = A$, alors $\overline{f}$ est surjectif, et donc $A/(I \cap J)$ est isomorphe à $A/I \times A/J$.*

Démonstration. □

On peut généraliser ce théorème à un nombre fini d'idéaux $I_1, \ldots, I_n$.

On construit comme précédemment f, et on déduit un morphisme injectif $\overline{f}$. Il suffit de trouver une condition pour que $\overline{f}$. Nous avons alors le résultat suivant, dit théorème chinois généralisé.

Théorème 1.49. *Si pour tout $1 \leq k \leq n$, on a*

$$I_k + \bigcap_{i=1, i\neq k}^{n} I_i = A \tag{1.24}$$

alors $\overline{f}$ est surjectif, et donc $\prod_{i=1}^{n} A/I_i$ est isomorphe à $A/\bigcap_{i=1}^{n} I_i$.

Démonstration. □

1.4.2 Interprétation et applications

Exemple.

1. *Soient $A = \mathbb{Z}$, $I = n\mathbb{Z}$, $J = m\mathbb{Z}$. On a $I \cap J = ppcm(n,m)\mathbb{Z}$, et $I + J = pgcd(n,m)\mathbb{Z}$. D'où $I + J = \mathbb{Z} \Leftrightarrow pgcd(n,m) = 1 \Leftrightarrow ppcm(n,m) = nm$.*

   Donc, si $pgcd(n,m) = 1$, on a un isomorphisme entre $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

   Celui-ci est donné par $a\ mod(nm\mathbb{Z}) \to (a\ mod(n\mathbb{Z}), a\ mod(m\mathbb{Z}))$.

2. *Soient K un anneau commutatif non nul, $A = K[X]$, $I = (X)$, $J = (X-1)$. On a $I + J = K[X]$ et $I \cap J = (X^2 - X)$.*

   Par le théorème chinois, on a

$$K[X]/(X^2 - X) \xrightarrow{\sim} K[X]/X \times K[X]/(X-1) \tag{1.25}$$

$$P(X)\, mod(X^2 - X) \xrightarrow{\sim} (P(X)\, mod(X), P(X),\ mod(X-1)) \tag{1.26}$$

De plus, on a vu que $K[X]/X$ est isomorphe à K grace à $eval_0$ et $K[X]/(X-1)$ est isomorphe à K grace à $eval_1$.
On en déduit que $K[X]/(X^2 - X)$ est isomorphe à $K \times K$.

Exemple. *Soient $A = \mathbb{Z}$ et $n \in \mathbb{Z}$. Posons $n = p_1^{m_1}. \cdots .p_l^{m_l}$ la décomposition de n en facteurs premiers.*

Posons $I_k = p_k^{m_k}\mathbb{Z}$ pour tout $1 \leq k \leq l$.

On a, pour tout $1 \leq j, k \leq l$, $j \neq k$

$$I_k + I_j = \mathbb{Z} \tag{1.27}$$

De plus,

$$ppcm(p_1^{m_1}, \cdots, p_l^{m_l}) = n \tag{1.28}$$

et

$$\bigcap_{1 \leq k \leq l} p_k^{m_k}\mathbb{Z} = n\mathbb{Z} \tag{1.29}$$

On en déduit que

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \prod_{1 \leq i \leq l} (\mathbb{Z}/p_i^{m_i}\mathbb{Z}) \tag{1.30}$$

et comme corollaire, on obtient

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \prod_{1 \leq i \leq l} (\mathbb{Z}/p_i^{m_i}\mathbb{Z})^\times \tag{1.31}$$

vu comme des groupes. On a alors

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = |\prod_{1 \leq i \leq l} (\mathbb{Z}/p_i^{m_i}\mathbb{Z})^\times| \tag{1.32}$$

Définition 1.50. *L'indicatrice d'Euler, noté souvent ϕ est la fonction*

$$\phi : \mathbb{N} \to \mathbb{N} : n \to |(\mathbb{Z}/n\mathbb{Z})^\times| \tag{1.33}$$

L'indicatrice d'Euler donne donc, pour chaque $n \in \mathbb{N}$, le nombre d'élément inversible de $\mathbb{Z}/n\mathbb{Z}$. On obtient directement une première propriété : $\phi(p) = p - 1$ où p est premier. En effet $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc tous les éléments non nuls sont inversibles.

Enonçons quelques propriétés de l'indicatrice d'Euler.

Proposition 1.51.

1. *Soit p un nombre premier. Alors $\phi(p) = p - 1$.*
2. *Soit $n, m \geq 1$. Alors, si m et n sont premiers entre eux, $\phi(nm) = \phi(n)\phi(m)$.*

3. *Soit $m \geq 1$ et soit p un nombre premier. Alors $\phi(p^m) = (p-1)p^{m-1}$*
4. *Soient $n \in \mathbb{N}$, et $n = p_1^{m_1} . \cdots . p_l^{m_k}$ sa décomposition en facteurs premiers. Alors $\phi(n) = \prod_{1 \leq i \leq l} (p_i - 1)p_i^{m_i - 1}$*
5. *Soit $n \geq 1$ un entier. Alors $\phi(n) = \sum_{d|n} \phi(d)$.*

Démonstration. □

1.5 Arithmétique des anneaux

Définition 1.52 (Anneau intègre)**.** *Soit A un anneau commutatif. On dit que A est **intègre** si*

1. *$A \neq \{0_A\}$*
2. *pour tout $a, b \in A$, $ab = 0 \Rightarrow (a = 0$ ou $b = 0)$.*

Exemple. 1. *$\mathbb{Z}$ est intègre.*

2. *Un corps est un anneau intègre.*
3. *$\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre (car $2.3 = 6 = 0$).*
4. *Soient A, B deux anneaux commutatifs tel que $A \subseteq B$. Si B est intègre, alors A est intègre.*
5. *$\mathbb{Z}[i]$ est intègre.*
6. *Soient A, B deux anneaux commutatifs non nuls. Alors $A \times B$ n'est pas intègre.*

Proposition 1.53. *Soit A un anneau intègre et soient $P(X), Q(X) \in A[X]$. Alors $deg(PQ) = deg(P) + deg(Q)$.*

Démonstration. □

Proposition 1.54. *Soit A un anneau intègre. Alors $A[X]$ est un anneau intègre.*

Démonstration. □

Corollaire 1.55. *Soit K un corps. Alors $K[X]$ est un anneau intègre.*

Démonstration. □

Proposition 1.56. *Soit A un anneau intègre. Alors $(A[X])^\times = A^\times$.*

Démonstration. $\square$

Exemple. 1. $(\mathbb{Z}[X])^\times = \{\pm 1\}$.

2. *Soit* K *un corps. Alors* $(K[X])^\times = K^\times = \{P(X) \in K[X] \mid deg(P) = 0\}$.

Proposition 1.57. *Soit* A *un anneau intègre.*
Alors, pour tout $a, b \in A$

$$(a) = (b) \Leftrightarrow \exists u \in A^\times \ a = ub \tag{1.34}$$

Démonstration. $\square$

Exemple. 1. $m\mathbb{Z} = n\mathbb{Z} \Leftrightarrow m = \pm n$

2. *Soit* K *un corps et soient* $P, Q \in K[X]$*. Alors,* $(P) = (Q)$ *ssi* $\exists u \in K^\times$*,* $P = uQ$*.*

Corollaire 1.58. *Soit* K *un corps et soit* $P \in K[X]$ *tel que* $P \neq 0$*. Alors* (P) *a un unique générateur monique.*

Démonstration. $\square$

Définition 1.59 (Idéal premier)**.** *Soit* A *un anneau commutatif et soit* I *un idéal de* A*. On dit que* I *est* ***un idéal premier*** *si*

1. $I \neq A$
2. *pour tout* $a, b \in A$*,* $ab \in I \Rightarrow a \in I$ *ou* $b \in I$*.*

Définition 1.60 (Idéal maximal)**.** *Soit* A *un anneau commutatif et soit* I *un idéal de* A*. On dit que* I *est* ***un idéal maximal*** *si*

1. $I \neq A$
2. *pour tout idéal* J *de* A*, si* $I \subseteq J$*, alors* $J = I$ *ou* $J = A$*.*

Proposition 1.61. *Soit* A *un anneau commutatif. Alors*

1. (0) *idéal premier ssi* A *intègre.*
2. (0) *idéal maximal ssi* A *corps.*
3. $n\mathbb{Z}$ *premier dans* $\mathbb{Z}$ *ssi* $n = 0$ *ou* $n = \pm p$ *où* p *est premier.*
4. $n\mathbb{Z}$ *maximal dans* $\mathbb{Z}$ *ssi* $n \pm p$ *où* p *premier.*

Démonstration. $\square$

Généralisons la proposition précédente.

Proposition 1.62. *Soit* A *un anneau commutatif et soit* I *un idéal de* A*. Alors*

1. *I premier ssi A/I principal.*
2. *I maximal ssi A/I corps.*

Démonstration. □

Exemple. 1. *$\mathbb{Z}/n\mathbb{Z}$ principal ssi $n = 0$ ou $n = \pm p$ où p est premier.*

2. *$\mathbb{Z}/n\mathbb{Z}$ corps ssi $n \pm p$ où p premier. On note alors $\mathbb{F}_p$ à la place de $\mathbb{Z}/p\mathbb{Z}$.*

Proposition 1.63. *Soit A un anneau commutatif et soit $a \in A$. Alors*

1. *A intègre ssi $(X - a)$ idéal premier de $A[X]$.*
2. *A corps ssi $(X - a)$ idéal maximal de $A[X]$.*

Démonstration. □

Proposition 1.64. *Tout idéal maximal est premier.*

Démonstration. □

Théorème 1.65. *Tout idéal est contenu dans un idéal maximal.*

Démonstration. □

1.5.1 Irréductibilité

Définition 1.66 (Élément irréductible)**.** *Soit $a \in A$. a est dit **irréductible** si pour tout $x, y \in A$*

$$a = xy \Rightarrow x \in A^\times \text{ ou } y \in A^\times. \tag{1.35}$$

Exemple. *Soit $n \in \mathbb{Z}$, n est irréductible dans $\mathbb{Z}$ ssi $n = \pm p$ où p premier.*

Proposition 1.67. *a est irréductible dans A ssi pour tout $u \in A^\times$, ua est irréductible dans A.*

Démonstration. □

Proposition 1.68. *Soit f un isomorphisme d'anneau. a est irréductible ssi $f(a)$ est irréductible.*

Démonstration. □

Exemple. *On a vu que la conjugaison est un automorphisme d'anneau, donc si z est irréductible, $\overline{z}$ l'est aussi.*

Une remarque importante est que l'irréductibilité d'un élément dépend de l'anneau dans lequel nous nous trouvons. On a par exemple 2 irréductible dans $\mathbb{Z}$ mais 2 est réductible dans $\mathbb{C}$ parce que $2 = (1+i)(1-i)$.

Donnons maintenant quelques équivalences en termes d'idéaux. La définition 1.66 date du XIXè siècle, la suivante, plus couramment utilisée actuellement, date du début du XXè siècle.

Proposition 1.69. *a est irréductible*
$\Leftrightarrow a \notin A^\times, a \neq 0$ $b|a \Rightarrow b \in A^\times$ *ou* $\exists u \in A^\times, b = ua$.
$\Leftrightarrow (a) \neq (0)$, $(a) \neq A$, $(a) \subseteq (b) \Rightarrow (b) = A$ *ou* $(a) = (b)$
$\Leftrightarrow (a) \neq (0)$, (a) *maximal parmi les idéaux principaux différents de* A.

Démonstration. Chaque équivalence est une réécriture. □

Proposition 1.70. *Soit K un corps. Alors $K[X]$ est principal.*

Démonstration. □

1.6 Anneau de polynômes

1.6.1 Généralités

Proposition 1.71. *1. A intègre $\Leftrightarrow (X)$ idéal premier de $A[X]$*

2. A corps $\Leftrightarrow (X)$ idéal maximal de $A[X]$

Démonstration. Si on prend la fonctions surjective $eval_0$, on a un isomorphisme induit entre A et $A[X]/(X)$. Comme (X) est un idéal premier, $A[X]/(X)$ est intègre. Par l'isomorphisme, A est intègre. □

Proposition 1.72. *Soit K un corps, alors $K[X]$ possède une division euclidienne. Par conséquent, $K[X]$ est principal.*

Démonstration. □

Proposition 1.73. *Soit K un corps, Pour tout idéal I non nul de $K[X]$, il existe un* ***unique*** *$P \in K[X]$* ***monique*** *tel que $I = (P)$. En d'autres termes, tout idéal est engengré par un unique polynome monique dans un anneau de polynome sur un corps.*

Démonstration. Commençons par l'existence.

Comme K est un corps, $K[X]$ est principal, et donc chaque idéal est engendré par un élément. Notons celui-ci $Q(X) = a_nX^n + \ldots + a_1X + a_0, a_n \neq 0$. On a donc $I = (Q)$. Comme K est un corps, on peut définir a_n^{-1}, et $P(X) =$

$a_n^{-1}Q(X) \in I$. Celui-ci est monique, et on a de plus que $(P) = (Q) = I$ car P et Q sont copremiers.

Supposons maintenant qu'il existe un autre polynôme monique $S(X)$ engendrant I. (A finir). □

Proposition 1.74. *Soit K un corps, $P \in K[X]$.*

1. *(P) est maximal $\Leftrightarrow$ P est irréductible.*
2. *(P) est premier $\Leftrightarrow$ $P = 0$ ou P irréductible.*

Démonstration. □

On a alors comme corollaire :

Corollaire 1.75.
1. *P est irréductible $\Leftrightarrow$ $K[X]/(P)$ est un corps.*
2. *$P = 0$ ou P est irréductible $\Leftrightarrow$ $K[X]/(P)$ est intègre.*

Démonstration. □

Proposition 1.76. *Soit $K[X]$ où K est un corps. Soit $P \in K[X]$.*

Si P est de degré 1, alors P est irréductible.

De plus, si K est algébriquement clos et P irréductible, alors P est de degré 1.

1.6.2 Irréductibilité dans $\mathbb{Q}[X]$

Définition 1.77. *Soit $P \in \mathbb{Q}[X]$. On définit*

$$\chi_P : \mathbb{Z} \to \mathbb{Q}[X]/n\mathbb{Z}[X] : n \to n\,P(X)\,mod(n\mathbb{Z}[X]) \tag{1.36}$$

Proposition 1.78. *Soit $P \in \mathbb{Q}[X]$. Alors χ_P est un morphisme de groupe. De plus, $\ker(\chi_P) = \{n \in \mathbb{Z} \,|\, nP(X) \in \mathbb{Z}[X]\} \neq 0$ est un sous-groupe de $\mathbb{Z}$.*

Démonstration. □

Définition 1.79. *Soit $P \in \mathbb{Q}[X]$. On définit $c(P)$ comme l'unique entier $n \geq 1$ tel que $\ker(\chi_P) = c(P)\mathbb{Z}$.*

Corollaire 1.80. *Soit $P \in \mathbb{Q}[X]$. Alors*

1. *$c(P) = \min\{n \geq 1 \,|\, nP(X) \in \mathbb{Z}[X]\}$*
2. *$(\forall n \geq 1,\ nP(X) \in \mathbb{Z}[X]) \Leftrightarrow c(P) = 1$. En particulier, $P(X) \in \mathbb{Z}[X] \Leftrightarrow c(P) = 1$.*

Démonstration. □

Définition 1.81 (Polynome primitif)**.** *Soit* $P(X) = \sum_{i=1}^{n} a_i X^i \in \mathbb{Z}[X]$*. On dit que* P *est* ***primitif*** *si*

1. $P(X) \neq 0$
2. $(a_0, \cdots, a_n) = \mathbb{Z}$ *où* $(a_0, \cdots, a_n)$ *est l'idéal engendré par* $a_0, \cdots, a_n$*.*

Proposition 1.82. *Soit* $P(X) = \sum_{i=1}^{n} a_i X^i \in \mathbb{Z}[X]$*. Alors les assertions suivantes sont équivalentes.*

1. *P est primitif.*
2. P *est non nul et pour tout* p *premier, il existe* $0 \leq i \leq n$ *tel que* p *ne divise pas* a_i*.*
3. P *est non nul et pgcd*$(a_0, \cdots, a_n) = 1$*.*

Démonstration. □

Exemple. $2X^2 + 3X + 1$ *est primitif.*

Proposition 1.83. *Soit* $P(X) \in \mathbb{Z}[X]$*. Alors, si* P *est monique, alors* P *est primitif.*

Démonstration. □

Lemme 1.84. *Soit* $P(X) \in \mathbb{Q}[X]$*. Si* P *est monique, alors* $c(P)P(X) \in \mathbb{Z}[X]$ *et* P *primitif.*

Démonstration. □

Remarque. *Soit* $R(X) \in \mathbb{Z}[X]$ *non nul. Alors* P *primitif ssi il existe* p *premier tel que* $R(X) \in \mathbb{F}[X]$ *ssi il existe* p *premier tel que* $\overline{R}(X) = 0$ *dans* $p\mathbb{F}_p[X]$*.*

Lemme 1.85. *Soient* $P, Q \in \mathbb{Z}[X]$*. Alors, les assertions suivantes sont équivalentes.*

1. PQ *primitif.*
2. P *primitif et* Q *primitif.*

Démonstration. □

Lemme 1.86. *Soit* $P \in \mathbb{Z}[X]$ *primitif et soit un entier* $m \geq 1$*. Alors* $c(\frac{1}{m}P) = m$*.*

Démonstration. □

Lemme 1.87 (Gauss)**.** *Soient* $P, Q \in \mathbb{Q}[X]$ *moniques. Alors* $c(PQ) = c(P)c(Q)$*.*

Démonstration. □

Corollaire 1.88. *Soient $P, Q \in \mathbb{Q}[X]$ moniques. Alors, les assertions suivantes sont équivalentes.*

1. $PQ \in \mathbb{Z}[X]$
2. $P \in \mathbb{Z}[X]$ *et* $Q \in \mathbb{Z}[X]$.

Démonstration. □

Corollaire 1.89. *Soient $P, Q \in \mathbb{Q}[X]$ non nuls. Alors, les assertions suivantes sont équivantes.*

1. $PQ \in \mathbb{Z}[X]$
2. *il existe* $P_0, Q_0 \in \mathbb{Z}[X]$ *tel que* $deg(P_0) = deg(P)$, $deg(Q_0) = deg(Q)$ *et* $P_0Q_0 = PQ$.

Démonstration. □

Remarque. *Soit $P \in \mathbb{Q}[X]$. Si $P \in \mathbb{Z}[X]$ et P réductible dans $\mathbb{Q}[X]$, alors P est réductible dans $\mathbb{Z}[X]$.*

1.6.3 Polynômes à coefficients dans $\mathbb{Z}[X]$

Dans cette partie nous allons étudier les propriétés que les polynômes à coefficients dans $\mathbb{Z}[X]$ possèdent dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.

Dans la suite, on considère que $P(X) = a_nX^n + \ldots + a_1X + a_0$ est un polynôme à coefficients dans $\mathbb{Z}$.

Rappelons d'abord la définition d'irréductibilité dans le cas de $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$.

Prenons $P(X)$ qui n'est pas inversible dans $\mathbb{Q}[X]$ (resp dans $\mathbb{Z}[X]$). Ce polynôme $P(X)$ est irréductible dans $\mathbb{Q}[X]$ (resp $\mathbb{Z}[X]$) si pour toute décomposition de $P(X)$ en deux polynômes $Q(X)$ et $R(X)$ ($P = QR$), on a $Q(X) \in \mathbb{Q}_0$ ou $R(X) \in \mathbb{Q}_0$ (resp $Q(X) = \pm 1$ ou $R(X) = \pm 1$ car les inversibles de $\mathbb{Z}[X]$ sont 1 et -1).

Prenons $P(X) = 2X - 2$. On a $P(X)$ qui est irréductible dans $\mathbb{Q}[X]$ mais celui-ci est réductible dans $\mathbb{Z}[X]$ car $P(X) = 2(X - 1)$. On n'a donc pas ($P(X)$ irréductible dans $\mathbb{Q}[X] \Rightarrow P(X)$ irréductible dans $\mathbb{Z}[X]$).

Nous avons tout de même, sous certaines hypothèses, que l'implication est vraie.

Proposition 1.90. *Si $pgcd(a_0, \ldots, a_n) = \pm 1$, alors :*

Si $P(X)$ est irréductible dans $\mathbb{Q}[X]$, alors $P(X)$ est irréductible dans $\mathbb{Z}[X]$.

Démonstration. □

Théorème 1.91 (Critère Eisenstein[1]). *Soit p premier tel que :*

1. *p ne divise pas a_n*
2. *$\forall i \in \{0, \dots, n-1\}$, p divise a_i.*
3. *p^2 ne divise pas a_0.*

Alors, $P(X)$ est irréductible dans $\mathbb{Q}[X]$.

Démonstration. □

Nous avons également un théorème qui permet de déterminer l'irréductibilité d'un polynôme. Celui-ci se sert du corps $\mathbb{Z}/p\mathbb{Z}$ où p est premier.

Théorème 1.92. *Si il existe un nombre premier p tel que le polynôme $\overline{P}(X) = \overline{a_n}X^n + \ldots + \overline{a_1}X + \overline{a_0}$ où $\overline{a_i} = a_i$ mod(p) est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors $P(X)$ est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. □

Corollaire 1.93. *Grace à ce dernier théorème, on en déduit que $X^{p-1} + \ldots + X + 1$ est irréductible dans $Q[X]$ (et dans $\mathbb{Z}[X]$) quand p est premier.*

De plus, $X^p - 1 = (X-1)(X^{p-1} + \cdots + X + 1)$.

Démonstration. □

1.6.4 Polynômes cyclotomiques

Nous allons maintenant étudier certains polynômes appelés **polynômes cyclotomiques.**

D'abord, rappelons que le polynôme $X^n - 1$ possèdent n racines complexes, appelées racines n-ième de l'unité, et qui sont $e^{\frac{2ki\pi}{n}}$, où k va de 0 à $n-1$. On peut de la même manière dire que $k \in \mathbb{Z}/n\mathbb{Z}$.

De plus, les racines n-ième de l'unité forment un groupe d'ordre n, qui est l'unique sous-groupe d'ordre n de $\mathbb{C}$, qui est cyclique, et isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Si on prend une de ces racines qui est d'ordre d, alors il engendre un unique sous-groupe d'ordre d. Ce d doit diviser n par le théorème de Lagrange. Notons cet unique sous-groupe d'ordre d par S_d.

Nous allons poser une notation pour les racines de l'unité.

1. Ferdinand **Gotthold** Max **Eisenstein** : 16 avril 1823 (Berlin) - 11 octobre 1862 (Berlin). Mathématicien allemand d'origine juive. Mort de tuberculose. Élève de Dirichlet à l'université de Berlin.

Notation. $\zeta_n^k := e^{\frac{2ik\pi}{n}}$

Proposition 1.94. *Dans* $\mathbb{C}[X]$, *on a*

$$X^n - 1 = \prod_{d|n} \prod_{k \in (\mathbb{Z}/d\mathbb{Z})^\times} (X - \zeta_d^k) \tag{1.37}$$

Démonstration. □

Définition 1.95 (Polynômes cyclotomiques)**.** *Soit* $n \geq 1$. *On définit* ***le n-ième polynome cyclotomique****, noté* $\Phi_n(X)$, *par le polynome complexe*

$$\Phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^k) \tag{1.38}$$

Proposition 1.96. *Soit* p *premier. On a* $\Phi_p(X) = X^{p-1} + \cdots + X + 1$.

Démonstration. □

Proposition 1.97. *Soit* $n \geq 1$. *On a* $deg(\Phi_n) = \phi(n)$.

Démonstration. □

Proposition 1.98. *Soit* $n \geq 1$. *On a*

$$\Phi_n(X) = \prod_{d|n} \Phi_d(X) \tag{1.39}$$

Démonstration. □

Proposition 1.99. *Soit* $n \geq 1$. *On a* $\Phi_n(X) \in \mathbb{Z}[X]$.

Démonstration. □

Théorème 1.100. *Soit* $n \geq 1$. *Alors* $\Phi_n(X)$ *est irréductible dans* $\mathbb{Q}[X]$.

Démonstration. □

Proposition 1.101. *Soit* $n \geq 1$. *Alors la décomposition de* $X^n - 1$ *en facteur irréductible dans* $\mathbb{Q}[X]$ *est donnée par*

$$\Phi_n(X) = \prod_{d|n} \Phi_d(X) \tag{1.40}$$

Chapitre 2

Théorie de Galois

2.1 Extension de corps

Rappelons qu'un **corps** est un anneau commutatif A tel que le seul élément non inversible est 0_A.

Définition 2.1 (Morphisme de corps)**.** *Soient K et F deux corps.* ***Un morphisme de corps entre*** *K* ***et*** *F est un morphisme d'anneau.*

Proposition 2.2. *Tout morphisme de corps est injectif*

Définition 2.3 (Extension de corps et sous corps)**.** *Soient K et L deux corps. On dit que L est* ***une extension de corps****, et K* ***un sous corps de*** *L si $K \subseteq L$ et on note L/K.*

Proposition 2.4. *Soit une extension de corps L/K. Alors L est un K-espace vectoriel.*

Définition 2.5 (Degré d'une extension)**.** *Soit L/K une extension de corps. On définit* ***le degré de l'extension*** *L/K par la dimension de L en tant que K-espace vectoriel, et on note $[L : K]$.*

Définition 2.6 (Extension finie)**.** *Soit L/K une extension de corps.*

On dit que L/K est ***une extension finie*** *si le degré de L/K ($[L : K]$) est fini.*

Remarque. *Soient $K \subseteq L \subseteq M$ trois corps.*

Alors :

1. $[L : K] \leq [M : K]$.
2. $[M : K]$ *fini* $\Rightarrow$ $[L : K]$ *fini.*

3. $[L : K] = 1 \Leftrightarrow L = K$.

Proposition 2.7 (Multiplicativité des degrés)**.** *Soient $K \subseteq L \subseteq M$ trois corps.*

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

Proposition 2.8 (Multiplicativité des degrés généralisée)**.** *Soient $L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n$.*

Alors $[L_n : L_1] = \prod_{i=1}^{n-1} [L_{i+1} : L_i]$.

Remarque. *Soit $K \subseteq L \subseteq M$.*

Alors $[L : K]$ divise $[M : K]$ et $[M : L]$ divise $[M : K]$.

En particulier, si $[M : K]$ est un nombre premier, alors il n'existe pas de corps strictement compris entre K et M.

Exercice 2.1. *Il n'y a pas de corps strictement compris entre $\mathbb{C}$ et $\mathbb{R}$.*

Définition 2.9. *Soient L/K et M/K deux extensions de corps tel que $L \subseteq E$ et $M \subseteq E$ où E est un corps. Alors on définit :*

1. *$LM = \bigcap_{\substack{F \subseteq E \text{ corps} \\ M \subseteq F \\ L \subseteq F}} F$. C'est la plus grande extension de K contenant L et M.*
2. *$L \cap M$ est la plus grande extension de K contenue dans L et M. De manière générale, on peut étudier une intersection quelconque d'extension.*

Exercice 2.2. *Si pgcd$([L : K], [M : K]) = 1$. Alors $L \cap M = K$.*

Définition 2.10. *Soit L/K une extension de corps. Soit S un sous-ensemble de L (il n'y a pas nécessairement de structures sur S).*

On définit $K(S)$ par :

$$K(S) = \bigcap_{\substack{K \subseteq F \subseteq L \text{ corps} \\ S \subseteq F}} F \tag{2.1}$$

En particulier, quand $S = \{\alpha_1, \cdots, \alpha_n\}$, on note $K(S)$ par $K(\alpha_1, \cdots, \alpha_n)$. C'est le plus petit corps contenant le corps K et le sous-ensemble S.

Proposition 2.11. *Soit L/K une extension de corps. Soient $\alpha, \beta \in L$.*

Alors $K(\alpha, \beta) = K(\alpha)K(\beta)$.

Démonstration. □

Soit L/K une extension de corps. Prenons $\alpha \in L$, et construisons le morphisme d'évaluation $eval_{\alpha,K} : K[X] \to L : P(X) \to P(\alpha)$ non nul. On pose $K[\alpha] = Im(eval_{\alpha,K})$.

Comme K est un corps, on a que $K[X]$ est euclidien, donc ses idéaux sont engendrés par un élément.

Comme $eval_{\alpha,K}$ morphisme, on a $\ker(ev_{\alpha,K}) = (P)$ car le noyau de tout morphisme d'anneau est un idéal.

Définition 2.12 (Algébrique / transcendant)**.** *Soit L/K et $\alpha \in L$.*

*On dit que α **est algébrique sur** K si $\ker(eval_{\alpha,K}) \neq \{0\}$. Sinon, α est dit **transcendant**.*

Proposition 2.13. *Soit $\alpha \in L$ algébrique sur K. Alors $K[\alpha]$ est un corps.*

En particulier, $K(\alpha) = K[\alpha]$.

Démonstration. □

Définition 2.14 (Polynome minimal)**.** *Soit $\alpha \in L$ algébrique sur K.*

***Le polynome minimal de** α **sur** K est l'unique $P_{\alpha,K} \in K[X]$ monique tel que $\ker(eval_{\alpha,K}) = (P_{\alpha,K})$. En particulier, $P_{\alpha,K}$ est irréductible sur K.*

Proposition 2.15. *Soient L/K une extension de corps, et $\alpha \in L$ algébrique sur K. Soit $n = deg(P_{\alpha,K})$.*

Alors $(1, \alpha, \alpha^2, \cdots, \alpha^{n-1})$ est une base de $K(\alpha)$ en tant que K espace vectoriel. En particulier, $[K(\alpha) : K] = deg(P_{\alpha,K})$.

Démonstration. □

Corollaire 2.16. *Soit L/K une extension de corps, et soit $\alpha \in L$.*

Alors, les assertions suivantes sont équivalentes.

1. *$K(\alpha)/K$ est finie.*
2. *α est algébrique sur K.*

Démonstration. □

2.2 Extension algébrique

Définition 2.17 (Extension algébrique)**.** *Soit L/K est une extension de corps.*

*On dit que l'extension L/K est **algébrique** si tout élément de L est algébrique sur K.*

De manière équivalente, grace à 2.16, $K(\alpha)/K$ est une extension finie pour tout α dans L.

Donnons une sous-classe des extensions algébriques.

Définition 2.18 (Extension séparable)**.** *Soit L/K une extension de corps. On dit que L/K est* ***une extention séparable*** *si*

1. *L/K est algébrique.*
2. *pour tout $\alpha \in L$, le polynome minimal de α sur K, $P_{\alpha,K}$, est scindé à racine simple.*

Exemple. *$\mathbb{C}/\mathbb{R}$ est une extension algébrique.*
$\mathbb{Q}(i)/\mathbb{Q}$ est une extension algébrique.
$\mathbb{R}/\mathbb{Q}$ n'est pas une extension algébrique.

Proposition 2.19. *Soient $K \subseteq L \subseteq M$ trois corps. Les assertions suivantes sont équivalentes.*

1. *M/K est une extension algébrique.*
2. *M/L et L/K sont des extensions algébriques.*

Démonstration. $\square$

Proposition 2.20. *Soit L/K une extension finie.*
Alors L/K est une extension algébrique.

Démonstration. $\square$

Remarque. *La réciproque est fausse.*

Proposition 2.21. *Soit L/K une extension finie.*
Alors il existe $n \geq 1$, et $\alpha_1, \ldots, \alpha_n$ algébriques sur K tel que $L = K(\alpha_1, \cdots, \alpha_n)$.

Démonstration. $\square$

Proposition 2.22. *Soit L/K une extension de corps. Soit F l'ensemble des éléments de L algébriques sur K.*
Alors F est un sous corps de L contenant K.

Démonstration. $\square$

Définition 2.23. *On appelle F, défini précédemment,* ***la cloture algébrique de K sur L****.*

Remarquons qu'a priori la cloture algébrique est dépendante d'une extension de corps. On montrera par après qu'en réalité, si on prend deux clotures algébriques, les théories sur celles-ci sont les mêmes. On pourra donc choisir notre cloture algébrique 'préférée'.

Théorème 2.24. *Soit K un corps. Alors il existe un corps algébriquement clos Ω contenant K.*

Démonstration. □

Lemme 2.25. *Soit L/K une extension de corps. Soient Ω algébriquement clos contenant K, et $\sigma : K \to \Omega$ un plongement de corps.*

Soit $\alpha \in L$ algébrique sur K.

Alors il existe un plongement $\tau : K(\alpha) \to \Omega$ tel que $\tau_{|K} = \sigma$.

Démonstration. □

Théorème 2.26 (Extension des plongements)**.** *Soit L/K algébrique. Soient Ω algébriquement clos contenant K et $\sigma : K \to \Omega$ un plongement de corps. Alors il existe $\tau : L \to \Omega$ plongement tel que $\tau_{|K} = \sigma$.*

Démonstration. □

Corollaire 2.27. *Soient K corps, Ω_1 et Ω_2 algébriquement clos contenant K.*

Soit F_1 (resp. F_2) la cloture algébrique de K dans Ω_1 (resp. dans Ω_2).

Alors il existe un isomorphisme K-linéaire entre F_1 et F_2. En d'autres termes, F_1 et F_2 sont isomorphes.

Démonstration. □

On en conclut que si on veut étudier les extensions algébriques de K, il suffit de choisir un corps algébriquement clos Ω contenant K, et d'étudier $\overline{K}$, la cloture algébrique de K dans Ω. Par la suite, nous dirons que nous prenons une cloture algébrique de K.

2.3 K-plongement

Soit K un corps de caractéristique nulle (voir 1.3.1).

Fixons une cloture algébrique $\overline{K}$ de K.

Définition 2.28. *Soit L/K algébrique.* ***Un K-plongement*** *est un morphisme de corps $\sigma : L \to \overline{K}$ K-linéaire.*

Remarquons que nous avons $L \subseteq \overline{K}$ car L algébrique, et $\overline{K}$ contient tous les éléments algébriques sur K.

Un K-plongement de corps $\sigma : L \to \overline{K}$ est un K-plongement ssi σ fixe tous les éléments a de K, ie $\sigma(a) = a$. D'où $\sigma_{|K} : K \to \overline{K}$ est le morphisme d'inclusion de K dans $\overline{K}$.

Rappelons que si α est algébrique, alors $K(\alpha)$ est un corps contenant K.

Proposition 2.29. *Soient $\alpha \in \overline{K}$, $\sigma : K(\alpha) \to \overline{K}$ un K-plongement et $P(X) \in K[X]$.*

Alors $\sigma(P(\alpha)) = P(\sigma(\alpha))$

Démonstration. □

En conclusion, l'image d'un polynome de $K[X]$ par un K-plongement de $K(\alpha)$ dans $\overline{K}$ est uniquement déterminé par l'image de α.

Par un même raisonnement, si on prend $\alpha_1, \cdots, \alpha_n$ et un K-plongement de $K(\alpha_1, \cdots, \alpha_n)$ dans $\overline{K}$, alors il suffit de connaitre les $\sigma(\alpha_i)$ pour $1 \leq i \leq n$.

Prenons maintenant le cas du polynome minimal $P_{\alpha,K}$. On a, par définition, $P_{\alpha,K}(\alpha) = 0$.

On obtient alors la proposition suivante.

Proposition 2.30. *Soit $P_{\alpha,K}$ le polynome minimal de α sur K.*

Soit $\sigma : K(\alpha) \to \overline{K}$ un K-plongement. Alors $\sigma(\alpha)$ est racine de $P_{\alpha,K}$.

En particulier, si on pose N le nombre de racines de $P_{\alpha,K}$, alors il y a au plus N K-plongements de $K(\alpha)$ dans $\overline{K}$.

Démonstration. □

Définition 2.31. *Soit L/K algébrique.*

On définit l'ensemble $Hom_K(L, \overline{K}) := \big\{\sigma : L \to \overline{K}, K\text{-plongement}\big\}$

Exemple. $|Hom_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})| \leq 3$

Proposition 2.32. *Soient F/K une extension algébrique, et $\alpha \in \overline{K}$. Soit $\sigma : F \to \overline{K}$ un K-plongement ($\sigma \in Hom_K(F, \overline{K})$).*

Alors l'application :

$$\big\{\tau \in Hom_K(F(\alpha), \overline{K}) \,|\, \tau_{|F} = \sigma\big\} \to \big\{\text{racines dans } \overline{K} \text{ de } \sigma(P_{\alpha,F})\big\} \tag{2.2}$$

$$\tau \to \tau(\alpha) \tag{2.3}$$

est bijective. Nous venons donc de faire le lien entre les plongements et les racines du polynome minimal.

Démonstration. □

Exemple. *On sait que $Hom_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}), \overline{\mathbb{Q}})$ comporte au plus 4 éléments distincts. Notons les σ_0, σ_1, σ_2 et σ_3, Nous avons $P_{\sqrt[4]{2},\mathbb{Q}}(X) = X^4 - 2$.*

$P_{\sqrt[4]{2},\mathbb{Q}}(X)$ possèdant 4 racines distinctes, la proposition nous dit alors que nous avons 4 K-plongements de $\mathbb{Q}(\sqrt[4]{2})$ dans $\overline{\mathbb{Q}}$, et ces plongements sont donnés par $\sigma_k : \mathbb{Q}(\sqrt[4]{2}) \to \overline{\mathbb{Q}} : \sqrt[4]{2} \to \zeta_4^k \sqrt[4]{2}$ pour $0 \leq k \leq 3$.

Proposition 2.33. *Rappelons que nous supposons que K est de caractéristique nulle.*

Soient F/K une extension algébrique et $P(X)$ irréductible dans $F[X]$. Alors toutes les racines de $P(X)$ dans $\overline{K}$ sont simples.

Démonstration. □

Corollaire 2.34. *Soient F/K algébrique et $\alpha \in \overline{K}$. Soit $\sigma \in Hom_K(F, \overline{K})$.*

Alors $\left| \left\{ \tau \in Hom_K(F(\alpha), \overline{K}) \,|\, \tau_{|K} = \sigma \right\} \right| = [F(\alpha) : F]$.

Démonstration. □

Proposition 2.35. *Soit L/K une extension finie.*

Alors $|Hom_K(L, \overline{K})| = [L : K]$. En d'autres termes, une extension finie est définie par les K-plongements, et le nombre de K-plongements est exactement le degré de l'extension.

Démonstration. □

Théorème 2.36 (de l'élément primitif)**.** *Soit K un corps de caractéristique nulle. Soit L/K une extension finie. Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Démonstration. □

Exercice 2.3. *Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ et que $\mathbb{Q}(\zeta_3, \zeta_2) = \mathbb{Q}(\zeta_3\zeta_2)$.*

Remarque. *Le théorème de l'élément primitif 2.36 est aussi valable pour les corps finis.*

2.4 Groupe de Galois en caractéristique nulle

Définition 2.37 (Groupe de Galois)**.** *Soit L/K une extension finie.*

*On définit **le groupe de Galois de l'extension** L/K :*

$$\begin{aligned} G(L, K) &:= Aut_K(L) && (2.4)\\ &= \{\tau : L \to L \,|\, \tau \text{ isomorphisme } K\text{-linéaire de corps}\} && (2.5) \end{aligned}$$

$(G(L, K), \circ)$ *est un groupe.*

Soit $i : L \to \overline{K}$ le morphisme d'injection de L dans $\overline{K}$.
Alors l'application

$$\begin{array}{rc} G(L, K) \to & Hom_K(L, \overline{K}) \\ \sigma \to & i \circ \sigma \end{array}$$

est injective. On a donc en particulier que $|G(L,K)| \leq |Hom_K(L,\overline{K})|$. Quels conditions nous faut-il sur les plongements pour obtenir une surjection ?

Soit $\tau : L \to \overline{K}$ un K-plongement tel que $\tau(L) \subseteq L$. Comme L/K est de dimension finie, on a par le théorème du rang que $\tau(L) = L$. D'où $\tau \in G(L,K)$.

On identifie donc, grace à cette injection,

$$G(L,K) \simeq \left\{\sigma \in Hom_K(L,\overline{K}) \,|\, \sigma(L) \subseteq L\right\} \tag{2.6}$$

Exemple. *Soit $L = K(\alpha)$, $\alpha \in \overline{K}$.*

Alors

$$\begin{aligned} G(K(\alpha),K) &= \left\{\sigma \in Hom_K(K(\alpha),\overline{K}) \,|\, \sigma(K(\alpha)) \subseteq K(\alpha)\right\} && (2.7)\\ &= \left\{\sigma \in Hom_K(K(\alpha),\overline{K}) \,|\, \sigma(\alpha) \in K(\alpha)\right\} && (2.8)\\ &\simeq Rac(P_{\alpha,K}) \cap K(\alpha) && (2.9)\end{aligned}$$

En particulier, $|G(L,K)| \leq |Hom_K(L,\overline{K})| = [L:K]$. La dernière égalité résultant de 2.35.

Exemple (Exercice)**.** *1. $G(K,K) = \{Id_K\}$.*

2. $G(\mathbb{Q}(\sqrt{2}),\mathbb{Q}) = \langle\sigma\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ où $\sigma(\sqrt{2}) = -\sqrt{2}$.

3. $G(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q}) = \{Id_{\mathbb{Q}}\}$

4. $G(\mathbb{Q}(\sqrt[4]{2}),\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ avec $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$

5. $G(\mathbb{Q}(\zeta_3,\sqrt[3]{2}),\mathbb{Q}) \simeq S_3$

6. $G(\mathbb{Q}(\zeta_4,\sqrt[4]{2}),\mathbb{Q}) \simeq D_4$

Nous en venons à la définition d'extension galoisienne.

Définition 2.38 (Extension finie galoisienne)**.** *Soit L/K une extension finie. L/K est **(une extension finie) galoisienne** si*

$$G(L,K) = Hom_K(L,\overline{K}) \tag{2.10}$$

C'est-à-dire que tout isomorphisme K-linéaire sur L est un K-plongement de L dans $\overline{K}$ et inversément.

C'est-à-dire que :

$$\begin{aligned} L/K \text{ galoisienne} &\Leftrightarrow \forall\sigma \in Hom_K(L,\overline{K}), \sigma(L) \subseteq L && (2.11)\\ &\Leftrightarrow Hom_K(L,\overline{K}) = G(L,K) && (2.12)\\ &\Leftrightarrow |G(L,K)| = [L:K] && (2.13)\end{aligned}$$

l'égalité $|G(L,K)| = [L:K]$ résultant de 2.35.

Proposition 2.39. *Prenons maintenant $L = K(\alpha)$ avec $\alpha \in \overline{K}$. Alors, les assertions suivantes sont équivalentes.*

1. *$K(\alpha)$ est galoisienne.*
2. *$Rac(P_{\alpha,K}) \subseteq K(\alpha)$.*

Démonstration. □

On peut alors généraliser la proposition précédente. Passons d'abord par une proposition.

Proposition 2.40. *Soit L/K une extension finie galoisienne et soit $\alpha \in L$. Notons $P_{\alpha,K}$ le polynome minimal de α sur K.*

Alors $Rac(P_{\alpha,K}) \subseteq L$.

Démonstration. □

Proposition 2.41. *Soit L/K une extension finie tel que $L = K(\alpha_1, \cdots, \alpha_n)$.*

Alors, les assertions suivantes sont équivalentes.

1. *L/K est galoisienne.*
2. *pour tout $1 \leq i \leq n$, $Rac(P_{\alpha_i,K}) \subseteq L$.*

Démonstration. □

Exemple (Exercice)**.**
1. *K/K est galoisienne.*
2. *$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est galoisienne.*
3. *$\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ galoisienne.*
4. *$\mathbb{Q}(\zeta_4, \sqrt[4]{2})/\mathbb{Q}$ galoisienne.*
5. *$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas galoisienne.*
6. *$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ n'est pas galoisienne.*

Remarquons que nous avons $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ avec $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ galoisiennes. **Or,** $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ **n'est pas galoisienne**. La propriété d'être galoisienne n'est pas transitive !

Définition 2.42. *Soit $P(X) \in K[X]$ tel que $n := deg(P) \geq 1$.*

Soit $Rac(P(X)) := \{\alpha_1, \cdots, \alpha_n\}$ l'ensemble des racines de $P(X)$ dans $\overline{K}$.

On appelle $K(\alpha_1, \cdots, \alpha_n) = K(Rac(P(X)))$ ***le corps de décomposition de*** *$P(X)$.*

Remarque. *Soit* $P(X) = \prod_{i=1}^{d}(X - \alpha_i)^{m_i}$ *et* $P_0(X) = \prod_{i=1}^{d}(X - \alpha_i)$. *Alors* $P(X)$ *et* $P_0(X)$ *ont le même corps de décomposition.*

Exemple. 1. $\mathbb{Q}(\sqrt{2})$ *est le corps de décomposition de* $X^2 - 2$.

2. $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ *est le corps de décomposition de* $X^3 - 2$.
3. $\mathbb{Q}(\sqrt[4]{2}, \zeta_4)$ *est le corps de décomposition de* $X^4 - 2$.
4. $\mathbb{Q}(\zeta_n)$ *est le corps de décomposition de* $X^n - 1$.

Nous allons maintenant donner une proposition essentielle.

Proposition 2.43. *Soit* L/K *finie. Alors les assertions suivantes sont équivalentes.*

1. L/K *est galoisienne.*
2. L *est le corps de décomposition d'un polynome de* $K[X]$.

Démonstration. □

Exemple. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ *est galoisienne, et son degré est donné par* $\phi(n)$ *où* ϕ *est l'indicatrice d'Euler.*

Maintenant, nous allons étudier les sous-groupes de $G(L, K)$. Commençons d'abord par définir des objets grace aux sous-ensembles du groupe de Galois de L/K.

Définition 2.44. *Soit* L/K *une extension de corps. Soit* $S \subseteq G(L, K)$ *un sous-ensemble fini.*

On pose $L^S := \{x \in L \,|\, \forall \sigma \in S, \sigma(x) = x\}$. L^S *comprend tous les éléments fixes par les éléments de* S.

Montrons maintenant quelques propriétés.

Proposition 2.45. 1. L^S *est un sous-corps de* L *contenant* K.

2. $S \subseteq T \Rightarrow L^T \subseteq L^S$ *(décroissance)*
3. $L^S = L^{\langle S \rangle}$ *où* $\langle S \rangle$ *est le sous-groupe engendré par* S.

Démonstration. □

La dernière proposition nous montre qu'il nous suffit d'étudier les sous-groupes de $G(L, K)$ pour déterminer tous les L^S où S est un sous-ensemble de $G(L, K)$.

Donnons alors des propriétés quand S est un sous-groupe. Nous utiliserons la notation H à la place de S pour rester cohérent avec les notations usuelles de la théorie des groupes.

Proposition 2.46. *Soient H et H' deux sous-groupes de $G(L, K)$. Alors :*

1. $L^{HH'} = L^H \cap L^{H'}$
2. $L^{H \cap H'} = L^H L^{H'}$

Démonstration. □

2.5 La correspondance de Galois

Soit L/K une extension finie galoisienne.
Soit $\alpha \in L$.
Soit $\sigma \in G(L, K)$.
Soit $\beta \in Rac(P_{\alpha,K})$, une racine du polynome minimal de α sur K.
Alors on a :

$$P_{\alpha,K}(\beta) = 0 \Rightarrow P_{\alpha,K}(\sigma(\beta)) = 0 \tag{2.14}$$

Donc, le groupe $G(L, K)$ agit sur tous les éléments de $Rac(P_{\alpha,K})$.
C'est-à-dire que l'application $\gamma : G(L, K) \to Rac(P_{\alpha,K})$ est bien définie et est une action de groupe.

Proposition 2.47. *L'action γ est transitive, c'est-à-dire que $Rac(P_{\alpha,K}) = \{\sigma(\alpha) \mid \sigma \in G(L, K)\}$.*

Démonstration. □

On obtient alors

$$P_{\alpha,K}(X) = \prod_{\sigma \in G(L,K)} (X - \sigma(\alpha)) \tag{2.15}$$

$$= \prod_{\sigma \in Hom_K(L,\overline{K})} (X - \sigma(\alpha)) \tag{2.16}$$

Théorème 2.48. *Soit L/K une extension finie galoisienne.*
Alors $L^{G(L,K)} = K$.
C'est-à-dire que les seules points fixes par chaque élément du groupe de Galois sont les éléments de K.

Démonstration. □

Proposition 2.49. *Soit L/K une extension finie. Soit F corps tel que $K \subseteq F \subseteq L$.*
Alors on a $G(L, F) < G(L, K)$ (décroissance entre sous-corps de L contenant K et sous-groupe de $G(L, K)$).

Démonstration. □

Proposition 2.50. *Soit L/K une extension galoisienne, et soit F corps tel que $K \subseteq F \subseteq L$.*

Alors L/F est une extension galoisienne.

Démonstration. □

Remarque. *F/K n'est pas nécessairement galoisienne si L/K est galoisienne. Un contre-exemple est donné par $\mathbb{Q}(\zeta_4, \sqrt[4]{2})$, $\mathbb{Q}(\sqrt[4]{2})$ et $\mathbb{Q}$.*

Nous avons alors montré que nous pouvons construire une fonction ϕ qui à chaque sous-corps de L contenant K associe un sous-groupe de $G(L, K)$ (2.49) et inversément, on peut construire une fonction ψ qui à chaque sous-groupe de $G(L, K)$, on peut associer un sous-corps de L contenant K (2.45)

Formellement, on a :

$$\begin{aligned} \phi : \{F \mid F \text{ corps et } K \subseteq F \subseteq L\} &\to \{H \mid H < G(L, K)\} \\ F &\to G(L, F) \\ \psi : \{H \mid H < G(L, K)\} &\to \{F \mid F \text{ corps et } K \subseteq F \subseteq L\} \\ H &\to L^H \end{aligned}$$

Quels sont les liens entre ϕ et ψ ? Cette étude va nous mener à la *correspondance de Galois.*

Théorème 2.51. *L'application décroissante ϕ est bijective et $\psi = \phi^{-1}$. C'est-à-dire $\phi \circ \psi = Id$ et $\psi \circ \phi = Id$.*

Démonstration. □

Nous venons donc de faire un lien entre les corps intermédiaires de L et K tel que L/K est galoisienne, et les sous-groupes du groupe de Galois $G(L, K)$.

Nous avons vu que si nous avons une extension galoisienne L/K et F corps tel que $K \subseteq F \subseteq L$, alors L/F est galoisienne, mais pas nécessairement F/K. Nous sommes prêts à donner une condition nécessaire et suffisante pour que F/K soit galoisienne.

Proposition 2.52. *Soit L/K une extension finie galoisienne. Soit F corps tel que $K \subseteq F \subseteq L$.*

Alors les assertions suivantes sont équivalentes.

1. *F/K est galoisienne.*
2. *$G(L, F) \lhd G(L, K)$*

Dans ce cas, le morphisme de restriction :

$$G(L, K) \to G(F, K) \tag{2.17}$$
$$\sigma \to \sigma_{|F} \tag{2.18}$$

induit un isomorphisme entre $G(L, K)/G(L, F)$ *et* $G(F, K)$.

Démonstration. $\square$

Annexe A

20 premiers polynomes cyclotomiques

$$\Phi_1(X) = X - 1 \tag{A.1}$$
$$\Phi_2(X) = X + 1 \tag{A.2}$$
$$\Phi_3(X) = X^2 + X + 1 \tag{A.3}$$
$$\Phi_4(X) = X^2 + 1 \tag{A.4}$$
$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1 \tag{A.5}$$
$$\Phi_6(X) = X^2 - X + 1 \tag{A.6}$$
$$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \tag{A.7}$$
$$\Phi_8(X) = X^4 + 1 \tag{A.8}$$
$$\Phi_9(X) = X^6 + X^3 + 1 \tag{A.9}$$
$$\Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1 \tag{A.10}$$
$$\Phi_{11}(X) = X^{10} + X^9 + X^8 + X^7 + X^6 \tag{A.11}$$
$$+ X^5 + X^4 + X^3 + X^2 + X + 1 \tag{A.12}$$
$$\Phi_{12}(X) = X^4 - X^2 + 1 \tag{A.13}$$
$$\Phi_{13}(X) = X^{12} + X^{11} + X^{10} + X^9 + X^8 + X^7 + X^6 \tag{A.14}$$
$$+ X^5 + X^4 + X^3 + X^2 + X + 1 \tag{A.15}$$
$$\Phi_{14}(X) = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1 \tag{A.16}$$
$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1 \tag{A.17}$$
$$\Phi_{16}(X) = X^8 + 1 \tag{A.18}$$

$$
\begin{aligned}
\Phi_{17}(X) &= X^{16} + X^{15} + X^{14} + X^{13} + X^{12} + X^{11} && \text{(A.19)}\\
&+ X^{10} + X^{9} + X^{8} + X^{7} + X^{6} && \text{(A.20)}\\
&+ X^{5} + X^{4} + X^{3} + X^{2} + X + 1 && \text{(A.21)}\\
\Phi_{18}(X) &= X^{6} - X^{3} + 1 && \text{(A.22)}\\
\Phi_{19}(X) &= X^{18} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} && \text{(A.23)}\\
&+ X^{12} + X^{11} + X^{10} + X^{9} + X^{8} + X^{7} + X^{6} && \text{(A.24)}\\
&+ X^{5} + X^{4} + X^{3} + X^{2} + X + 1 && \text{(A.25)}\\
\Phi_{20}(X) &= X^{8} - X^{6} + X^{4} - X^{2} + 1 && \text{(A.26)}
\end{aligned}
$$