Université Mohammed Premier

Faculté des Sciences
Oujda

Département de Mathématiques

Master de Théorie des Nombres

Semestre: 1

Théorie des corps

Mohammed TALBI et Abdelkader ZEKHNINI

2019–2020

Table des matières

Rappels

0.1 Anneaux et corps

Définition 0.1. Soit A un ensemble, "$+$" et "$\cdot$" deux lois internes sur A. On dit que $(A, +, \cdot)$ est un anneau si

1) $(A, +)$ est un groupe abélien,

2) la loi "$\cdot$" est associative et distributive,

3) la loi "$\cdot$" admet un élément neutre.

On note souvent :

- A l'anneau $(A, +, \cdot)$.
- 0_A et 1_A (ou 0 et 1) les éléments neutres respectives de "$+$" et "$\cdot$".
- A^* l'ensemble des éléments non-nuls pour la loi "$+$" ($A^* = A - \{0\}$).
- $A^\times$ l'ensemble des éléments inversibles pour la loi "$\cdot$".
- $\forall\ x \in A,\ \forall\ n \in \mathbb{Z},\ nx$ est la puissance n-ème de x dans $(A, +)$.
- $\forall\ x \in A,\ \forall\ n \in \mathbb{N},\ x^n$ est la puissance n-ème de x dans $(A, \cdot)$.
- $\forall\ x \in A^\times,\ \forall\ n \in \mathbb{Z},\ x^n$ est la puissance n-ème de x dans $(A, \cdot)$.
- Un anneau $(A, +, \cdot)$ est dit commutatif, si la loi "$\cdot$" est commutative.

Exemples.

1) $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif et on a $\mathbb{Z}^\times = \{-1;\ 1\}$.

2) $(\mathbb{N}, +, \cdot)$ n'est pas un anneau.

3) $(\mathbb{Z}[\sqrt{-5}], +, \cdot)$ est un anneau commutatif et on a $\mathbb{Z}[\sqrt{-5}]^\times = \{-1;\ 1\}$.

4) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sont des anneaux commutatifs et on a $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$, $\mathbb{C}^\times = \mathbb{C}^*$.

Définition 0.2. On appelle corps, tout anneau $(A, +, \cdot)$ dans lequel les éléments inversibles pour la loi "$\cdot$" sont les éléments non nuls ($\neq 0$). Autrement dit, si $A^\times = A^* = A - \{0\}$.
Un corps est dit commutatif, si l'anneau sous-jacent est commutatif.

Remarque. Cette définition exclue que l'anneau trivial $\{0\}$ soit un corps ($A^* = A - \{0\} = \emptyset$).

Exemples.

1) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sont des corps commutatifs.

2) $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ est un corps commutatif.

0.2 Sous-anneaux

Définition 0.3. Soient $(A, +, \cdot)$ et $(B, +', \cdot')$ deux anneaux (resp. deux corps), on dit que $(A, +, \cdot)$ est un sous-anneau (resp. sous-corps) de $(B, +', \cdot')$, si :

1) $A \subseteq B$,

2) $\forall\ x, y \in A,\ x + y = x +' y,\ x \cdot y = x \cdot' y,$

3) $1_A = 1_B$.

Par abus de langage, on dit que A est un sous-anneau (resp. sous-corps) de B.

Remarque.

- La condition 3 est inutile pour les sous-corps, elle résulte des autres conditions.
- Les relations "être sous-anneau" et "être sous-corps" sont transitives.

Définition 0.4. Soient $A,\ B,\ C$ des anneaux (resp. des corps). On dit que B est un anneau (resp. un corps) intermédiaire à A et C, si A est un sous-anneau (resp. un sous-corps) de B et B est un sous-anneau (resp. un sous-corps) de C.

Proposition 0.1. *Soient $(A, +, \cdot)$ un anneau (resp. un corps) et S une partie de A. S est un sous-anneau (resp. un sous-corps) de A si et seulement si*

1) $1_A \in S$,

2) $\forall\ x,\ y \in S,\ x - y \in S$ *et* $xy \in S$ *(resp.* $\forall\ x,\ y \in S$ *avec* $y \neq 0,\ x - y \in S$ *et* $xy^{-1} \in S$*).*

Proposition 0.2. *Soient A un anneau (resp. un corps) et $(S_i)_{i\in I}$ une famille de sous-anneaux (resp. de sous-corps) de A, alors $\cap_{i\in I} S_i$ est un sous-anneau (resp. un sous-corps) de A.*

Définition 0.5. Soient A un anneau (resp. un corps) et S une partie de A. On appel sous-anneau (resp. sous-corps) de A engendré par S, l'intersection des sous-anneaux (resp. des sous-corps) de A contenant S.

Il résulte immédiatement de cette définition que le sous-anneau (resp. le sous-corps) B de A engendré par S est caractérisé par :

1) B est un sous-anneau (resp. un sous-corps) de A contenant S.

2) Tout sous-anneau (resp. sous-corps) de A contenant S contient B.

Notations :
Soient B un anneau (resp. un corps), A un sous-anneau de B et S une partie de B. On note

- $A[S]$ le sous-anneau de B engendré par $A \cup S$ (resp. $A(S)$ le sous-corps de B engendré par $A \cup S$).
- Si $S = \{a_1, a_2, \ldots, a_n\}$, $A[S]$ se note $A[a_1, a_2, \ldots, a_n]$ (resp. $A(S)$ se note $A(a_1, a_2, \ldots, a_n)$).
- On vérifie immédiatement que

$$A[S_1][S_2] = A[S_2][S_1] = A[S_1 \cup S_2] \text{ (resp. } A(S_1)(S_2) = A(S_2)(S_1) = A(S_1 \cup S_2)).$$

- Si B est commutatif et $S = \{a_1, a_2, \ldots, a_n\}$ est fini, on a

$$A[a_1, \ldots, a_n] = \{P(a_1, \ldots, a_n) \mid P \in A[X_1, \ldots, X_n]\}$$

$$\text{(resp. } A(a_1, \ldots, a_n) = \{\frac{P(a_1, \ldots, a_n)}{Q(a_1, \ldots, a_n)} \mid P,\ Q \in A[X_1, \ldots, X_n],\ Q(a_1, \ldots, a_n) \neq 0\}.)$$

Exemples.

1) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

2) $\mathbb{Z}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Z}\}$.

3) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{x + y\sqrt{2} + z\sqrt{3} + t\sqrt{6} \mid x, y, z, t \in \mathbb{Q}\}$.

Définition 0.6. Un anneau (resp. un corps) est dit premier s'il n'admet pas de sous anneau (resp. sous-corps) autre que lui même.

Nous expliciterons plus loin les anneaux et les corps premiers.

Proposition 0.3. *Soit A un anneau (resp. un corps), il existe parmi les sous-anneaux (resp. sous-corps) de A un et un seul anneau (resp. corps) premier P, ainsi tout sous-anneau (resp. sous-corps) de A contient P.*
Donc P est le plus petit sous-anneau (resp. sous-corps) de A.

Preuve. Soit P le sous-anneau de A engendré par $\{1_A\}$,tout sous-anneau de A contient 1_A, donc contient P. P est premier car si P_1 est un sous-anneau de P, alors P_1 est un sous-anneau de A, donc $P \subseteq P_1$ et $P_1 \subseteq P$, ce qui donne que $P = P_1$.
Soit P' un autre sous-anneau de A qui est premier. Comme $P \subseteq P'$, alors $P = P'$ (car on a aussi $P' \subseteq P$). □

0.3 Idéaux

Définition 0.7. Soient $(A, +, \cdot)$ un anneau et I une partie de A. On dit que I est un idéal de A, si

1) I est un sous-groupe de $(A, +)$;

2) $\forall\ a \in A,\ \forall\ x \in I,\ a \cdot x$ et $x \cdot a \in I$.

Exemples.

1) Les idéaux de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$ où $n \in \mathbb{Z}$.

2) Un corps K a exactement deux idéaux $\{0\}$ et K.

Proposition 0.4. *Soient $(A, +, \cdot)$ un anneau et $\mathcal{R}$ une relation binaire sur A. Pour que $\mathcal{R}$ soit une relation d'équivalence compatible avec les deux lois "$+$" et "$\cdot$", il faut et il suffit qu'il existe un idéal I de A tel que*

$$\forall\ x, y \in A,\ x\mathcal{R}y \Leftrightarrow x - y \in I.$$

Preuve. Supposons que $\mathcal{R}$ est une relation d'équivalence compatible avec "$+$" et "$\cdot$", soit $I = \{x \in A \mid x\mathcal{R}0\}$, on vérifie facilement que I est un idéal de A, et on a

$$\forall\ x, y \in A,\ x\mathcal{R}y \Leftrightarrow (x-y)\mathcal{R}(y-y) \Leftrightarrow (x-y)\mathcal{R}0 \Leftrightarrow x - y \in I.$$

Inversement si I est un idéal de A, on vérifie que la relation $\mathcal{R}$ définit par

$$\forall\ x, y \in A,\ x\mathcal{R}y \Leftrightarrow x - y \in I$$

est une relation d'équivalence compatible avec les deux lois "$+$" et "$\cdot$". □

Remarque. L'idéal I associé à la relation $\mathcal{R}$ par la proposition ci-dessus est unique, on note alors A/I l'ensemble quotient $A/\mathcal{R}$.

Proposition 0.5. *Soient A un anneau et I un idéal de A. La relation "$x - y \in I$" étant une relation d'équivalence compatible avec les deux lois "$+$" et "$\cdot$", cela induit sur A/I les deux lois internes*

$$(\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} = \overline{x + y} \text{ et } (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

pour lesquels $(A/I, +, \cdot)$ est un anneau.

Définition 0.8. L'anneau $(A/I, +, \cdot)$ s'appelle anneau quotient de l'anneau $(A, +, \cdot)$ par son idéal I.

Exemple. Soit I un idéal de $\mathbb{Z}$, alors il existe un et un seul n dans $\mathbb{N}$ tel que $I = n\mathbb{Z}$. L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ s'appelle anneau des classes résiduelles modulo n. Si $n = 0$, $\mathbb{Z}/n\mathbb{Z}$ s'identifie à $\mathbb{Z}$, si $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ est fini et a n éléments.

Proposition 0.6. *Soient A un anneau et I un idéal de A. Les idéaux de A/I sont les ensembles J/I tel que J est un idéal de A contenant I.*

Définition 0.9. Soit A un anneau commutatif, un idéal I de A est dit maximal si $I \neq A$ et si pour tout idéal J de A tel que $I \subseteq J$, alors $J = I$ ou $J = A$.

Remarque. Pour $n \in \mathbb{N}$, $n\mathbb{Z}$ est maximal si et seulement si n est premier.

Proposition 0.7. *Soient A un anneau commutatif et I un idéal de A, alors I est maximal si et seulement si A/I est un corps.*

Preuve.

$$\begin{aligned} A/I \text{ est un corps } &\Leftrightarrow A/I \text{ a exactement deux idéaux } A/I \text{ et } I/I \\ &\Leftrightarrow \text{ exactement deux idéaux de } A \text{ contient } I \\ &\Leftrightarrow I \text{ est maximal.} \end{aligned}$$

□

Proposition 0.8. *Soit A un anneau commutatif, alors tout idéal de A, distinct de A est contenu dans un idéal maximal.*

Preuve. Soit I un idéal de A tel que $I \neq A$ et soit $\mathcal{E} = \{J \mid J \text{ idéal de } A,\ J \neq A \text{ et } I \subseteq J\}$.

- $\mathcal{E} \neq \emptyset$ $(I \in \mathcal{E})$.
- $\mathcal{E}$ est inductif par inclusion, ainsi $\mathcal{E}$ contient un élément maximal $\hat{I}$. On vérifie immédiatement que $\hat{I}$ est maximal et on a $I \subseteq \hat{I}$.

□

Remarque. Tout anneau commutatif qui contient au moins deux éléments admet un idéal maximal.
En effet, d'après la proposition précédente il suffit de prendre $I = \{0\}$.

Proposition 0.9. *Soient A un anneau et $(I_\alpha)_{\alpha\in\Lambda}$ une famille d'idéaux de A, alors $\cap_{\alpha\in\Lambda} I_\alpha$ est un idéal de A.*

Définition 0.10. Soient A un anneau et S une partie de A, on appel idéal de A engendré pa S l'intersection des idéaux de A contenant S et qu'on le note par (S). Ainsi l'idéal (S) est caractérisé par

1) (S) est un idéal de A contenant S.

2) Tout idéal de A contenant S contient l'idéal (S).

Remarque. On vérifie immédiatement que si A est un anneau commutatif, alors on a

$$(S) = \{\sum_{s\in S} a_s \cdot s \mid a_s \in A \text{ et les } a_s \text{ sont presque tous nuls }\}.$$

Et si $S = \{s_1,\ s_2,\ \ldots,\ s_n\}$, alors

$$(S) = \{\sum_{i=1}^{n} a_i \cdot s_i \mid a_i \in A\},\ \text{en particulier } (x) = \{a \cdot x \mid a \in A\}.$$

0.4 Morphismes d'anneaux

Définition 0.11. Soient $(A, +, \cdot)$ et $(B, +', \cdot')$ deux anneaux (resp. deux corps). Un homomorphisme d'anneaux (resp. de corps) de A dans B est une application de A dans B qui vérifient

1) $\forall\ x, y \in A,\ f(x + y) = f(x) +' f(y)$.

2) $\forall\ x, y \in A,\ f(x \cdot y) = f(x) \cdot' f(y)$.

3) $f(1_A) = 1_B$.

Soient A et B deux anneaux (resp. deux corps) et f un homomorphisme de A dans B. On vérifie immédiatement que

- $\forall\ x \in A,\ \forall\ n \in \mathbb{Z},\ f(nx) = nf(x)$.
- $\forall\ x \in A,\ \ (\text{resp. } x \in A^*),\ \forall\ n \in \mathbb{N},\ (\text{resp. } \forall\ n \in \mathbb{Z}),\ f(x^n) = f(x)^n$.
- L'image d'un sous-anneau (resp. sous-corps) de A est un sous-anneau (resp. sous-corps) de B.
- L'image réciproque d'un sous-anneau (resp. sous-corps) de B est un sous-anneau (resp. sous-corps) de A.
- L'image d'un idéal de A est un idéal de B.
- L'image réciproque d'un idéal de B est un idéal de A.

Exemple. Soient A un anneau et I un idéal de A, alors l'application

$$\begin{array}{rccc} p: & A & \longrightarrow & A/I \\ & a & \longmapsto & a+I \end{array}$$

est homomorphisme surjectif, appelé la projection canonique.

Proposition 0.10. *Soient A, B, C des anneaux (resp. des corps), f un homomorphisme de A dans B et g un homomorphisme de B dans C, alors gof est un homomorphisme d'anneaux (resp. de corps) de A dans C.*

Définition 0.12.

- Un isomorphisme d'anneaux (resp. de corps) est un homomorphisme d'anneaux (resp. de corps) bijectif.
- Un endomorphisme d'anneaux (resp. de corps) est un homomorphisme d'un anneau (resp. un corps) dans lui même.
- Un endomorphisme bijectif de A s'appelle un automorphisme de A. L'ensemble des automorphismes de A est un sous-groupe du groupe des bijections de A.

Soit f un homomorphisme d'anneau de A dans B, on note

$$\mathrm{Ker}(f) = \{x \in A \mid f(x) = 0\} \text{ et } \mathrm{Im}(f) = \{f(x) \mid x \in A\}.$$

Proposition 0.11. *Soit f un homomorphisme d'anneau de A dans B, alors*

1) *f est injectif si et seulement si* $\mathrm{Ker}(f) = \{0\}$.
2) *Si A est un corps et $B \neq \{0\}$, alors f est injectif. En particulier tout homomorphisme de corps est injectif.*

Preuve.

1) Trivial.
2) Soit $x \in \mathrm{Ker}(f)$ et supposons que $x \neq 0$.
   On a
   $$1 = f(1) = f(xx^{-1}) = f(x) \cdot f(x^{-1}) = 0 \cdot f(x^{-1}) = 0,$$
   ce qui donne que $1 = 0$ (dans B), donc $B = \{0\}$, contradiction, ainsi $\mathrm{Ker}(f) = \{0\}$, par suite f est injectif.

□

Théorème 0.12. *Soit f un homomorphisme d'anneaux de A dans B, alors* $\mathrm{Ker}(f)$ *est un idéal de A,* $\mathrm{Im}(f)$ *est un sous-anneau de B et on a un isomorphisme canonique de* $A/\mathrm{Ker}(f)$ *dans* $\mathrm{Im}(f)$ *qui associe $\overline{x}$ par $f(x)$.*

0.5 Caractéristiques

Soient $(A,+,\cdot)$ un anneau, $x \in A,\ n \in \mathbb{Z}$, on note nx la puissance $n^{\text{ème}}$ (additive) de x dans $(A,+)$, on a

1) $\forall\ n,m \in \mathbb{Z},\ \forall\ x \in A,\ (n+m)x = nx + mx$.

2) $\forall\ n,m \in \mathbb{Z},\ \forall\ x \in A,\ n(mx) = (nm)x = m(nx)$.

3) $\forall\ n \in \mathbb{Z},\ \forall\ x,y \in A,\ n(x+y) = nx + ny$.

4) $\forall\ n \in \mathbb{Z},\ \forall\ x,y \in A,\ n(xy) = (nx)y = x(ny)$.

Plus généralement $\forall\ n,m \in \mathbb{Z},\ \forall\ x,y \in A,\ (nx)(my) = (nm)(xy) = (mx)(ny)$.

Remarque. Soit h une application de $\mathbb{Z}$ dans A qui associe n par $n \cdot 1_A$.
Il résulte des propriétés précédentes que h est un homomorphisme d'anneaux, donc $\text{Ker}(h)$ est un idéal de $\mathbb{Z}$, ainsi $\exists!\ m \in \mathbb{N},\ \text{Ker}(h) = m\mathbb{Z}$.

- Si h est injectif, alors $m = 0$ ($\text{Ker}(h) = \{0\}$).
- Si h n'est pas injectif, alors $m > 0$ et on a $\forall\ n \in \mathbb{Z}$

$$n \cdot 1_A = 0 \Leftrightarrow \forall\ x \in A,\ n \cdot x = 0 \Leftrightarrow m \mid n.$$

Définition 0.13. L'entier m définit ci-dessus ($\text{Ker}(h) = m\mathbb{Z}$) s'appelle caractéristique de l'anneau A qu'on note par $\text{car}(A) = m$.

Remarque. Soient A un anneau et B un sous-anneau de A, alors $\text{car}(B) = \text{car}(A)$.
En effet, comme $1_B = 1_A$, on a $n \cdot 1_B = n \cdot 1_A,\ \forall\ n \in \mathbb{Z}$, d'où le résultat.

Exemples.

- $\text{car}(\mathbb{Z}) = 0$ (car $\text{Ker}(h) = \{0\}$ avec $h : \mathbb{Z} \longrightarrow \mathbb{Z},\ n \longmapsto n \cdot 1 = n$).
- $\text{car}(\mathbb{Z}/4\mathbb{Z}) = 4$ (car $\text{Ker}(h) = 4\mathbb{Z}$ avec $h : \mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z},\ n \longmapsto n \cdot \bar{1} = \bar{n}$).
- Soit A un sous-anneau de $\mathbb{C}$, alors $\text{car}(A) = 0$.

Reprenons l'homomorphisme $h : \mathbb{Z} \longrightarrow A,\ n \longmapsto n \cdot 1_A$, alors $\text{Im}(h) = \{n \cdot 1_A \mid n \in \mathbb{Z}\}$ est un sous-anneau de A, or tout sous-anneau de A contient 1_A, donc contient $\text{Im}(h)$, ainsi $\text{Im}(h)$ est le sous-anneau premier de A, on a donc

Proposition 0.13. *Soit A un anneau, $m = \text{car}(A)$, P le sous-anneau premier de A, alors on a un isomorphisme canonique entre P est $\mathbb{Z}/m\mathbb{Z}$.*

Inversement on vérifie que tout anneau $\mathbb{Z}/m\mathbb{Z}$ est premier, on a donc

Proposition 0.14. *Un anneau est premier si et seulement si il est isomorphe à un anneau $\mathbb{Z}/m\mathbb{Z}$ avec $m \in \mathbb{N}$.*

Proposition 0.15. *Soit K un corps, $p = \text{car}(K)$ et P le sous-corps premier de K, alors $p = 0$ ou p est un nombre premier, dans le premier cas P est isomorphe au corps $\mathbb{Q}$ et dans le second cas P est isomorphe au corps $\mathbb{Z}/p\mathbb{Z}$.*

Preuve. Soit P_1 le sous-anneau premier de l'anneau K, on a $P_1 \simeq \mathbb{Z}/p\mathbb{Z}$ et comme P_1 est intègre, alors $\mathbb{Z}/p\mathbb{Z}$ aussi, par suite p est un nombre premier ou $p = 0$.
Dans le cas où p est premier, on aura $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc P_1 l'est aussi, comme $P_1 \subseteq P$ et comme P est un sous-corps premier de K, donc $P \subseteq P_1$, ainsi on a $P = P_1 \simeq \mathbb{Z}/p\mathbb{Z}$.
Dans le cas où $p = 0$, on aura $\forall\ n \in \mathbb{Z},\ n \cdot 1_K = 0 \Leftrightarrow n = 0$. Soit donc $\hat{h}$ de $\mathbb{Q}$ dans K qui associe $r = \frac{a}{b}$ $(a,b \in \mathbb{Z},\ b \neq 0)$ par $(a \cdot 1_K) \cdot (b \cdot 1_K)^{-1}$. On vérifie que $\hat{h}$ est bien définit et que c'est un homomorphisme de corps et on a $\text{Im}(\hat{h}) = \{(a \cdot 1_K) \cdot (b \cdot 1_K)^{-1} \mid a,b \in \mathbb{Z},\ b \neq 0\}$.
$\text{Im}(\hat{h})$ est un sous-corps de K, tout sous-corps de K contient 1_K, donc contient $(a \cdot 1_K) \cdot (b \cdot 1_K)^{-1}\ \forall\ a,b \in \mathbb{Z},\ b \neq 0$, donc contient $\text{Im}(\hat{h})$, ainsi $\text{Im}(\hat{h}) = P$, par suite $P \simeq \mathbb{Q}$. □

Exemples.

- $\text{car}(\mathbb{Q}) = 0$ ($\text{car Ker}(h) = \{0\}$ avec $h : \mathbb{Z} \longrightarrow \mathbb{Q},\ n \longmapsto n \cdot 1 = n$).
- $\text{car}(\mathbb{Z}/3\mathbb{Z}) = 3$ ($\text{car Ker}(h) = 3\mathbb{Z}$ avec $h : \mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z},\ n \longmapsto n \cdot \bar{1} = \bar{n}$).

Inversement, on vérifie que les corps $\mathbb{Z}/p\mathbb{Z}$ avec p premier et $\mathbb{Q}$ sont des corps premiers. On a donc

Proposition 0.16. *Un corps est premier si et seulement si il est isomorphe au corps $\mathbb{Q}$ ou à un corps $\mathbb{Z}/p\mathbb{Z}$.*

Notation : Soit K un corps de caractéristique 0, $x \in K$, $r = \frac{a}{b}$ $(a, b \in \mathbb{Z},\ b \neq 0) \in \mathbb{Q}$, on note $rx = r1_K \cdot x$ avec $r1_K = (a \cdot 1_K) \cdot (b \cdot 1_K)^{-1}$ et on vérifie

1) $\forall\ r, r' \in \mathbb{Q},\ \forall\ x \in K,\ (r + r')x = rx + r'x$.

2) $\forall\ r, r' \in \mathbb{Q},\ \forall\ x \in K,\ r(r'x) = (rr')x (= r'(rx))$.

3) $\forall\ r \in \mathbb{Q},\ \forall\ x, y \in K,\ r(x + y) = rx + ry$.

4) $\forall\ r \in \mathbb{Q},\ \forall\ x, y \in K,\ r(xy) = (rx)y = x(ry)$.

Proposition 0.17. *Soit K un corps commutatif, alors*

1) *K admet un sous-corps P qui est le plus petit parmi les sous-corps de K.*

2) *Si A est un sous-anneau de K, alors $L = \{ab^{-1} \mid a, b \in A, b \neq 0\}$ est le plus petit sous-corps de K contenant A.*

Preuve.

1) Soient $\{K_\lambda \mid \lambda \in \Lambda\}$ l'ensemble des sous-corps de K et $P = \cap_{\lambda \in \Lambda} K_\lambda$. On a $\forall\ \lambda \in \Lambda,\ 1 \in K_\lambda$, donc $1 \in P$, soient $a, b \in P$, alors $a, b \in K_\lambda,\ \forall\ \lambda \in \Lambda$, donc $a - b,\ ab,\ a^{-1} \in K_\lambda,\ \forall\ \lambda \in \Lambda$ $(a \neq 0)$, ainsi $a - b,\ ab,\ a^{-1} \in P$ $(a \neq 0)$, ce qui donne que P est un sous-corps de K et on a évidement que c'est le plus petit sous-corps de K.

2) On a $1 \in A$, donc $1 = 1 \cdot 1^{-1} \in L$. Si $ab^{-1},\ cd^{-1} \in L$, alors

$$ab^{-1} - cd^{-1} = (ad - bc) \cdot (bd)^{-1},\ (ab^{-1}) \cdot (cd^{-1}) = (ac) \cdot (bd)^{-1},\ (ab^{-1})^{-1} = ba^{-1} \in L,$$

ainsi L est un sous-corps de K et L contient A car $\forall\ a \in A$, $a = a \cdot 1^{-1} \in L$. Comme tout sous-corps est fermé pour les inverses, alors L est le plus petit sous-corps de K contenant A.

□

Remarque. Il est évident que P est un corps premier et c'est le corps premier de K.

Proposition 0.18 (Dedekind)**.**
Soient k et K des corps et $\varphi_i : k \longrightarrow K,\ i = 1, \ldots, n$, des homomorphismes non nuls deux à deux distincts. Si $a_1, \ldots, a_n \in K$ sont non tous nuls, alors il existe $b \in k$ tel que

$$a_1\varphi_1(b) + a_2\varphi_2(b) + \ldots + a_n\varphi_n(b) \neq 0.$$

Preuve. Comme K est un corps, le résultat est vrai pour $n = 1$. Supposons que $n > 1$ et que le résultat est vrai pour $n - 1$. Supposons au contraire que

$$a_1\varphi_1(x) + a_2\varphi_2(x) + \ldots + a_n\varphi_n(x) = 0, \forall\ x \in k \quad (1).$$

Il suit de l'hypothèse de récurrence que $a_1 \neq 0$. Comme $\varphi_1 \neq \varphi_n$, il existe $c \in k$ tel que $\varphi_1(c) \neq \varphi_n(c)$. D'après (1),

$$a_1\varphi_1(cx) + a_2\varphi_2(cx) + \ldots + a_{n-1}\varphi_{n-1}(cx) + a_n\varphi_n(cx) = 0, \forall\ x \in k,$$

c'est-à-dire

$$a_1\varphi_1(c)\varphi_1(x) + \ldots + a_{n-1}\varphi_{n-1}(c)\varphi_{n-1}(x) + a_n\varphi_n(c)\varphi_n(x) = 0, \forall\ x \in k \quad (2).$$

En soustrayant le produit de (1) par $\varphi_n(c)$ de (2), on trouve

$$a_1(\varphi_1(c) - \varphi_n(c))\varphi_1(x) + \ldots + a_{n-1}(\varphi_{n-1}(c) - \varphi_n(c))\varphi_{n-1}(x) = 0, \forall\ x \in k,$$

qui est une contradiction à l'hypothèse de récurrence car $a_1(\varphi_1(c) - \varphi_n(c)) \neq 0$. Ceci achève la démonstration. □

Proposition 0.19. *Soit A un anneau commutatif de caractéristique p (premier), alors l'application définie de A dans A et qui associe x par x^p est un endomorphisme de A.*

Preuve. Il suffit de montrer que $\forall\ a, b \in A,\ (a+b)^p = a^p + b^p$.
On a

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k\ b^{p-k} + b^p.$$

Pour $1 \leq k \leq p-1$ on a

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \ldots k} = \frac{p}{k}\binom{p-1}{k-1},$$

donc

$$k\binom{p}{k} = p\binom{p-1}{k-1} \Rightarrow p \mid k\binom{p}{k},$$

or p et k sont premiers entre eux, donc $p \mid \binom{p}{k}$, ainsi $\binom{p}{k}a^k\ b^{p-k} = 0$, donc $(a+b)^p = a^p + b^p$. □

Remarque. Soit A un anneau commutatif de caractéristique p (premier) et $n \in \mathbb{N}$, alors l'application définie de A dans A et qui associe x par x^{p^n} est un endomorphisme de A.

0.6 Polynômes irréductibles

Partout dans cette section, on se fixe A un anneau commutatif et K un corps commutatif.

Définition 0.14. Soit $f(X) = a_0 + a_1X + \ldots + a_nX^n$ un polynôme sur A, où $a_n \neq 0_A$ si f est non nul.

1) Le constant a_0 s'appelle terme constant de f, et a_n le coefficient directeur lorsque f est non nul.
2) Le degré $\deg(f)$ de f est défini par $\deg(f) = n$ si f est non nul, et $\deg(f) = -\infty$ sinon.
3) $f(X)$ est dit monique (ou unitaire) si $a_n = 1_A$.

Remarque. On voit que $f(x) \in A$ si, et seulement si, $\deg(f) \leqslant 0$. Dans ce cas, on dit que f est un polynôme constant.

Proposition 0.20. *L'ensemble $A[X]$ des polynômes sur A est un anneau commutatif pour l'addition et la multiplication de polynômes. En outre, A est un sous-anneau de $A[X]$.*

Lemme 0.21. *Soient $f, g \in A[X]$ non nuls. Alors*

1) $\deg(f+g) \leqslant \max\{\deg(f), \deg(g)\}$.
2) $\deg(fg) \leqslant \deg(f) + \deg(g)$. *L'égalité a lieu si, et seulement si, le produit des coefficients directeurs est non nul. C'est le cas lorsque f ou g a coefficient directeur inversible.*

Exemple. Sur $\mathbb{Z}/4\mathbb{Z}$, on a $(2x+1)(2x+2) = 2x+2$, donc

$$\deg((2x+1)(2x+2)) < \deg(2x+1) + \deg(2x+2).$$

Soit $f(x) = \sum_{i=0}^{n} a_iX^i \in A[X]$. Pour $a \in A$, on pose $f(a) = \sum_{i=0}^{n} a_ia^i \in A$.

Proposition 0.22. *Soit $a \in A$. Alors l'application*

$$\begin{array}{rccc} \rho_a : & A[X] & \longrightarrow & A \\ & f(X) & \longmapsto & f(a) \end{array}$$

est un homomorphisme d'anneaux, appelée l'évaluation en a.

Le résultat suivant est évident.

Proposition 0.23. *Un homomorphisme $\phi : A \longrightarrow B$ d'anneaux commutatifs induit un homomorphisme*

$$\begin{array}{rccc} \psi : & A[X] & \longrightarrow & B[X] \\ & \sum_{i=0}^{n} a_i X^i & \longmapsto & \sum_{i=0}^{n} \phi(a_i) X^i \end{array}$$

d'anneaux commutatifs.

Théorème 0.24. *Soit $g(X)$ un polynôme sur A dont le coefficient directeur est inversible. Pour tout $f(X) \in A[X]$, il existe des polynômes uniques $q(X),\ r(X)$ sur A tels que*

$$f(X) = g(X)q(X) + r(X),\ \deg(r) < \deg(g).$$

Preuve. Posons $g = b_0 + \ldots + b_{m-1}X_{m-1} + b_m X^m$ avec $m \geqslant 0$ et b_m inversible.
Si $m = 0$, alors

$$f(X) = g(X)(b_m^{-1} f(X)) + 0,\ \forall\ f(x) \in A[X].$$

Supposons que $m > 0$. Soit $f = a_0 + a_1 X + \ldots + a_n X^n$ avec $a_n \neq 0$.
Si $n = 0$, on a $f(X) = 0g(X) + f(X)$ avec $\deg(f) < \deg(g)$.
Supposons maintenant que $n > 0$ et l'énoncé est vrai pour tout polynôme de degré $< n$. Si $n < m$, alors $f(X) = 0g(X) + f(X)$ avec $\deg(f) < \deg(g)$. Si $n \geqslant m$, alors f et $a_n b_m^{-1} X^{n-m} g$ ont même coefficient directeur. Ainsi

$$h(X) = f(X) - a_n b_m^{-1} X^{n-m} g(X) \text{ est de degré } < n.$$

D'après l'hypothèse de récurrence, $h = gq_1 + r$ avec $\deg(r) < \deg(g)$. Or

$$f(X) = \left(a_n b_m^{-1} X^{n-m} + q_1(X)\right) g(X) + r(X).$$

D'où l'existence de q et r.
Soient $q_0(X),\ r_0(X) \in A[X]$ tels que $f = q_0 g + r_0$ avec $\deg(r_0) < \deg(g)$. Alors $(q - q_0)g = r - r_0$. Supposons au contraire que $q - q_0 \neq 0_A$, c'est-à-dire , $\deg(q - q_0) \geqslant 0$. Comme le coefficient directeur de g est inversible, alors

$$\deg(q - q_0) + \deg(g) = \deg((q - q_0)g) = \deg(r - r_0) < \deg(g) \Rightarrow \deg(g) < \deg(g),$$

ce qui est absurde. Ainsi $q = q_0$, et donc $r = r_0$. □

Remarque. Si A est un corps, alors le théorème 0.24 est vrai pour tout polynôme non nul $g(X)$ sur A.

Exemple.

1) Considérons les polynômes rationnels $f(X) = X^7 + 1$ et $g(X) = -x^4 + 3X + 2$. Alors

$$f = qg + r,\ \text{où } q(X) = -X^3 - 3,\ r(X) = 2X^3 + 9X + 7.$$

2) Considérons les polynômes $X^3 + 1$ et $2X + 2$ sur $\mathbb{Z}/4\mathbb{Z}$. Alors il n'existe pas de polynômes $q(X),\ r(X)$ tels que $X^3 + 1 = (2X + 2)q(X) + r(X)$ avec $\deg(r) < \deg(2X + 2)$. En effet, si oui, on a alors que $2X^3 + 2 = 2r(X)$ est degré < 1, une contradiction. (On ne peut pas appliquer le théorème dans cet exemple car 2 **n'est pas inversible** dans $\mathbb{Z}/4\mathbb{Z}$).

Définition 0.15. Soit $f \in A[X]$ non constant. On dit que $a \in A$ est une racine de f si $f(a) = 0_A$.

Remarque.

1) Si A est fini, alors on peut trouver les racines de f en calculant $f(a)$ pour tout $a \in A$.
2) Si K est un corps, alors tout polynôme de degré 1 admet une racine dans K. Mais c'est pas nécessairement le cas sur un anneau. Par exemple, le polynôme $2X + 1$ sur $\mathbb{Z}/4\mathbb{Z}$ n'a pas de racine dans $\mathbb{Z}/4\mathbb{Z}$.

Proposition 0.25. *Soit $f(X) \in A[X]$ non constant. Alors $a \in A$ est racine de $f(X)$ si, et seulement si, $f(X) = (X - a)q(X)$ avec $q(X) \in A[X]$.*

Définition 0.16. Soit $f(X) \in A[X]$ non constant. On dit que f est réductible sur A s'il existe $g, h \in A[X]$ avec $\deg(g), \deg(h) > 0$ tels que $f = gh$; et irréductible sur A sinon.

Exemples.

1) Le polynôme $X^2 - 2$ est irréductible sur $\mathbb{Q}$, mais réductible sur $\mathbb{R}$.
2) Le polynôme X sur $\mathbb{Z}/4\mathbb{Z}$ est réductible. En effet, $X = (2X^2 + X)(2X + 1)$.

Remarque. Soient K un corps et $f \in K[X]$. Alors f est réductible sur K si, et seulement si, $f = gh$ avec $0 < \deg(g), \deg(h) < \deg(f)$. Par conséquent, si K est un corps fini, on peut déterminer si f est irréductible sur K ou non en calculant les produits des polynômes sur K de degré $< \deg(f)$.

Proposition 0.26. *Soit $f \in A[X]$ avec $\deg(f) \geqslant 2$. Si f admet une racine dans A, alors f est réductible sur A.*

Preuve. Soit $a \in A$ tel que $f(a) = 0$. D'après la proposition 0.25, il existe $q(X) \in A[X]$ tel que $f(X) = (X - a)q(X)$. Donc $\deg(f) = \deg(q) + 1$ car $X - a$ est monique. D'où $\deg(q) > 0$. Ceci achève la démonstration. □

Remarque. La réciproque de la proposition 0.26 n'est pas vraie. Par exemple, sur $\mathbb{Z}/6\mathbb{Z}$, on a $4X^2 - 1 = (2X + 1)(2X - 1)$, mais $4X^2 - 1$ n'a pas de racine dans $\mathbb{Z}/6\mathbb{Z}$.

Remarque. Si un polynôme irréductible f sur A admet une racine dans A, alors $\deg(f) = 1$.

Proposition 0.27. *Soit K un corps et soit $f(X) \in K[X]$avec $2 \leqslant \deg(f) \leqslant 3$. Alors f est irréductible sur K si, et seulement si, f n'a pas de racine dans K.*

Preuve. Si f a racine dans K, alors f est réductible puisque $\deg(f) \geqslant 2$. Réciproquement, si f est réductible, alors $f = gh$ avec $g, h \in K[X]$ non constants. Comme $\deg(g) + \deg(h) = \deg(f) \leqslant 3$, on a $\deg(g) = 1$ ou $\deg(h) = 1$. Comme K est un corps, g ou h admet une racine dans K, et donc f en a une. □

Théorème 0.28. *Soient K un corps et I un idéal de $K[X]$.*

1) *Il existe $p(X) \in K[X]$ tel que $I = (p(X)) = \{p(X)f(X) \mid f(X) \in K[X]\}$.*
2) *Le quotient $K[X]/I$ est un corps si, et seulement si, $p(X)$ est irréductible sur K.*

Preuve.

1) Si $I = 0$, prenons $p(X) = 0$. Sinon, prenons $p(X) \in I$ non nul de degré minimal. Alors pour tout $f(X) \in I$, il existe $q(X), r(X) \in K[X]$ avec $\deg(r) < \deg(p)$ tels que $f(X) = p(X)q(X) + r(X)$. Comme $r(X) \in I$, on a $r(X) = 0$ par la minimalité de degré de $p(X)$.
2) Si $p(X)$ est réductible sur K, alors $p = gh$, où $g, h \in K[X]$ avec $0 < \deg(g), \deg(h) < \deg(p)$. Donc $\bar{g}, \bar{h} \in K[X]/I$ sont tous non nuls tels que $\bar{g}\bar{h} = \bar{g}\bar{h} = \bar{p} = \bar{0}$, ce qui donne que $K[X]/I$ n'est pas un corps. Supposons réciproquement que $p(X)$ est premier. Si $\bar{f} \neq \bar{0}$, alors $p(X)$ ne divise pas $f(X)$. Ainsi f est co-premier à p. D'après le théorème de Bézout, il existe $g, h \in K[X]$ tels que $fg + ph = 1$. D'où, $\bar{f}\bar{g} = \bar{1}$, c'est-à-dire , f est inversible. Ainsi $K[X]/I$ est un corps.

□

0.7 Polynômes irréductibles rationnels

Dans cette section on considère le problème de déterminer si un polynôme sur $\mathbb{Q}$ est irréductible ou non.

Définition 0.17. Un polynôme non nul sur $\mathbb{Z}$ est dit primitif si le plus grand commun facteur de ses coefficients est 1.

Exemple. Le polynôme $2X^3 + 2X + 3$ est primitif et $2X^2 + 4X + 10$ ne l'est pas.

Remarque. Si $f(X) \in \mathbb{Q}[X]$, alors il existe $a \in \mathbb{Q}$ et un polynôme primitif $g(X) \in \mathbb{Z}[X]$ tels que $f(X) = ag(X)$. Par exemple,

$$\frac{2}{3}X^3 + \frac{6}{5}X + 4 = \frac{2}{15}(5X^3 + 9X + 30).$$

Lemme 0.29. *Si $f, g \in \mathbb{Z}[X]$ sont primitifs, alors fg l'est.*

Preuve. Posons

$$f(x) = \sum_{i=0}^{n} a_i X^i \text{ et } g(X) = \sum_{j=0}^{m} b_j X^j,$$

alors

$$f(X)g(X) = \sum_{k=0}^{n+m} c_k X^k \text{ avec } c_k = \sum_{i+j=k} a_i b_j.$$

Si fg n'est pas primitif, alors il existe un entier premier p tel que $p \mid c_k$, pour tout $0 \leqslant k \leqslant n+m$. Comme $f,\ g$ sont primitifs, il existe un indice minimal $r \geqslant 0$ tel que $p \nmid a_r$ et un indice minimal $s \geqslant 0$ tel que $p \nmid b_s$. En particulier, $p \nmid a_r b_s$. Si $r + s = 0$, alors $r = s = 0$. Donc $p \nmid a_0 b_0 = c_0$, une contradiction. Si $r + s \geqslant 0$, alors

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = a_r b_s + \sum_{i+j=r+s,(i,j)\neq(r,s)} a_i b_j.$$

Remarquons que si $(i, j) \neq (r, s)$, alors $i < r$ ou $j < s$, et donc $p \mid a_i b_j$. On en déduit que $p \nmid c_{r+s}$, une contradiction. Donc fg est primitif. Ceci achève la démonstration. □

Théorème 0.30 (Théorème de Gauss)**.**
Soit $f(X) \in \mathbb{Z}[X]$ non constant. Alors f est irréductible sur $\mathbb{Q}$ si, et seulement si, f est irréductible sur $\mathbb{Z}$.

Preuve. Il suffit de montrer la suffisance. Supposons que f est réductible sur $\mathbb{Q}$. Alors il existe $g, h \in Q[X]$ avec $\deg(g), \deg(h) > 0$ tels que $f = gh$. Or on peut écrire

$$g = \alpha g_1, h = \beta h_1 \text{ avec } \alpha, \beta \in \mathbb{Q} \text{ et } g_1, h_1 \in \mathbb{Z}[X] \text{ primitifs.}$$

Donc $f = \gamma g_1 h_1$, où $\gamma = \alpha\beta \in \mathbb{Q}$ et $g_1 h_1 \in \mathbb{Z}[X]$ est primitif d'après le lemme 0.29. Posons $g_1 h_1 = a_0 + a_1 X + \ldots + a_n X^n$ avec $a_i \in \mathbb{Z}$. Alors $\gamma a_i \in \mathbb{Z}$, pour tout $0 \leqslant i \leqslant n$, car $f \in \mathbb{Z}[X]$. En outre, comme le plus grand commun facteur de $a_0, a_1, \ldots, a_n$ est 1, il existe $s_i \in \mathbb{Z}$ tel que $\sum_{i=0}^{n} a_i s_i = 1$. Ceci nous donne

$$\gamma = \gamma(\sum_{i=0}^{n} a_i s_i) = \sum_{i=0}^{n} (\gamma a_i) s_i \in \mathbb{Z}.$$

Par conséquent, $f = (\gamma g_1(X))h_1(X)$ est réductible sur $\mathbb{Z}$. Ceci achève la démonstration. □

Le résultat ci-dessus nous dit que le problème de déterminer un polynôme rationnel est irréductible ou non sur $\mathbb{Q}$ se ramène à déterminer un polynôme entier est irréductible ou non sur $\mathbb{Z}$. On donne deux méthodes pour ce faire.
D'abord, pour un entier $q > 1$, la projection canonique $\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$ induit un homomorphisme

$$\begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}/q\mathbb{Z}. \\ f(X) = \sum_{i=0}^{n} a_i X^i & \longmapsto & \bar{f}(X) = \sum_{i=0}^{n} \bar{a}_i X^i \end{array}$$

Remarquons $\deg(\bar{f}) \leqslant \deg(f)$ et l'égalité a lieu si, et seulement si $q \nmid a_n$.

Proposition 0.31. *Soient $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ et $q > 0$ un entier avec $q \nmid a_n$. Si $\bar{f}$ est irréductible sur $\mathbb{Z}/q\mathbb{Z}$, alors f est irréductible sur $\mathbb{Z}$.*

Preuve. Supposons que f est réductible sur $\mathbb{Z}$ et montrons que $\overline{f}$ est réductible sur $\mathbb{Z}/q\mathbb{Z}$.
Si f est réductible sur $\mathbb{Z}$, alors il existe $g, h \in \mathbb{Z}[X]$ tel que $f = gh$ et $0 < \deg(g), \deg(h) < \deg(f)$.
On a $\overline{f} = \overline{gh} = \overline{g}\overline{h}$. Donc si $\overline{f}$ est irréductible sur $\mathbb{Z}/q\mathbb{Z}$, alors $\deg(\overline{g}) = 0$ ou $\deg(\overline{h}) = 0$, ainsi

$$\deg(\overline{f}) \leqslant \max\{\deg(\overline{g}), \deg(\overline{h})\} \leqslant \max\{\deg(g), \deg(h)\} < \deg(f).$$

D'où, $q \mid a_n$, une contradiction. Donc $\overline{f}$ est réductible sur $\mathbb{Z}/q\mathbb{Z}$. Ceci achève la démonstration. □

Remarques.

1) La réciproque n'est pas vraie. Par exemple, $X^2 - 2$ est irréductible sur $\mathbb{Z}$, mais sur $\mathbb{Z}/2\mathbb{Z}$, on voit que $X^2 - 2 = X^2$ est réductible.
2) La condition $q \nmid a_n$ est importante. Par exemple, sur $\mathbb{Z}/2\mathbb{Z}$, le polynôme $2X^2 + X - 1 = X - 1$ est irréductible, mais $2X^2 + X - 1 = (2X - 1)(X + 1)$ est réductible sur $\mathbb{Z}$.
3) On choisit souvent q un nombre premier pour contrôler les degrés dans $\mathbb{Z}/q\mathbb{Z}$.

Exemple. Considérons le polynôme rationnel $f(x) = \frac{5}{2}X^3 + 2X^2 + \frac{3}{2}X + 1$.

f est irréductible sur $\mathbb{Q}$ si et seulement si $g = 2f = 5X^3 + 4X^2 + 3X + 2$ est irréductible sur $\mathbb{Q}$.

Sur le corps $\mathbb{Z}/2\mathbb{Z}$, on a $\bar{g}(x) = X^3 + X$ est réductible, donc on en déduit aucune conclusion.
Sur $\mathbb{Z}/3\mathbb{Z}$, on a $\bar{g} = -X^3 + X - 1$ est un polynôme de degré 3, qui n'a pas de racine dans $\mathbb{Z}/3\mathbb{Z}$, et donc irréductible sur $\mathbb{Z}/3\mathbb{Z}$, d'après la proposition 0.27. Par conséquent, g est irréductible sur $\mathbb{Z}$, et donc irréductible sur $\mathbb{Q}$ d'après le théorème de Gauss. Ceci montre que f est irréductible sur $\mathbb{Q}$.

Théorème 0.32 (Critère d'Eisenstein)**.**
Soit $f(X) = a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{Z}[X]$ avec $n > 0$. Alors $f(X)$ est irréductible sur $\mathbb{Q}$ s'il existe un nombre premier p tel que

1) *$p \mid a_i,\ i = 0, 1, \ldots, n-1$, mais $p \nmid a_n$;*
2) *$p^2 \nmid a_0$.*

Preuve. Supposons au contraire que f soit réductible sur $\mathbb{Q}$. D'après le théorème de Gauss,

$$f = (b_0 + b_1 X + \ldots + b_r X^r)(c_0 + c_1 X + \ldots + c_s X^s),\ b_i, c_j \in \mathbb{Z};\ b_r \neq 0,\ c_s \neq 0,\ r, s > 0.$$

Comme $b_r c_s \neq 0$, on a $0 < r, s < n$. Comme $p \mid a_0 = b_0 c_0$, on a $p \mid b_0$ ou $p \mid c_0$. On peut supposer $p \mid b_0$. Comme $p \nmid a_n = b_r c_s$, on a $p \nmid b_r$. Ainsi il existe un $0 < t \leqslant r$ tel que $p \mid b_i$, pour tout $0 \leqslant i < t$ et $p \nmid b_t$. Remarquons

$$a_t = \sum_{i+j=t} b_i c_j = b_t c_0 + \sum_{i+j=t, i<t} b_i c_j.$$

Comme $t \leqslant r < n$, on a $p \mid a_t$ par l'hypothèse et $p \mid b_i c_j$ pour tout $0 \leqslant i < t$. Ceci implique $p | b_t c_0$. Comme $p \nmid b_t$, on a $p \mid c_0$. Ainsi $p^2 \mid b_0 c_0 = a_0$, une contradiction. Donc f est irréductible sur $\mathbb{Q}$. Ceci achève la démonstration. □

Exemples.

1) Soit p premier. Pour tout $n > 1$, d'après le critère d'Eisenstein, le polynôme $X^n - p$ est irréductible sur $\mathbb{Q}$. Donc $X^n - p$ n'a pas de racine dans $\mathbb{Q}$. Par conséquent, $\sqrt[n]{p}$ est irrationnel.
2) Considérons le polynôme rationnel $f(X) = \frac{2}{9}X^5 + \frac{5}{3}X^4 + X^3 + \frac{1}{3}$.
Posons $g(X) = 9f(X) = 2X^5 + 15X^4 + 9X^3 + 3$. Appliquant le critère d'Eisenstein pour $p = 3$, on voit que g est irréductible sur $\mathbb{Q}$. Donc f l'est également.

Lemme 0.33. *Soit $f(X) \in \mathbb{Q}[X]$ non constant et soient $a, b \in \mathbb{Q}$ avec a non nul. Alors $f(X)$ est irréductible sur $\mathbb{Q}$ si, et seulement si, $g(X) = f(aX + b)$ est irréductible sur $\mathbb{Q}$.*

Preuve. Si $f(X) = f_1(X)f_2(X), f_1, f_2 \in \mathbb{Q}[X]$ avec $\deg(f1), \deg(f2) > 0$, alors

$$g(X) = f(aX + b) = f_1(aX + b)f_2(aX + b) = g_1(X)g_2(X) \text{ avec } g_i(X) = f_i(aX + b).$$

Comme $a \neq 0$, on a $\deg(g_i) = \deg(f_i) > 0$. Ainsi $g(X)$ est réductible sur $\mathbb{Q}$. D'autre part, si $g(X)$ est réductible sur $\mathbb{Q}$, alors $f(X) = g(\frac{1}{a}X - \frac{b}{a})$ est réductible sur $\mathbb{Q}$. Ceci achève la démonstration. □

Corollaire 0.34. *Soit p un nombre premier. Alors $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$, appelé polynôme cyclotomique, est irréductible sur $\mathbb{Q}$.*

Preuve. Posons $g(X) = \Phi_p(X + 1)$. Comme $(X - 1)\Phi_p(X) = X^p - 1$, on a

$$Xg(X) = (X + 1)^p - 1 = X^p + \binom{p}{1}X^{p-1} + \ldots + \binom{p}{p-2}X^2 + \binom{p}{p-1}X.$$

D'où,

$$g(X) = X^{p-1} + \binom{p}{1}X^{p-2} + \ldots + \binom{p}{p-2}X + \binom{p}{p-1}.$$

Comme p est premier, on a $p \mid \binom{p}{i}$, pour tout $1 \leqslant i \leqslant p - 1$ et $p^2 \nmid \binom{p}{p-1} = p$. D'après le critère d'Eisenstein, $g(X)$ est irréductible sur $\mathbb{Q}$. Il suit du lemme 0.33 que $\Phi_p(X)$ est irréductible sur $\mathbb{Q}$. □

Chapitre 1

Extensions algébriques

1.1 Extensions d'anneaux

Définition 1.1. Soient B un anneau et A un sous-anneau de B. On dit que B est une extension de A ou B/A est une extension d'anneaux.
Si C et D sont deux anneaux intermédiaires à A et B avec $C \subset D$, alors on dit que D/C est une sous-extension de B/A. Par abus de langage on appelle aussi sous-extension de B/A tout anneau intermédiaire C (en fait C/A) à A et B.

Dans la suite, le terme extension signifiera extension d'anneau B/A avec (sauf mention contraire) A et B **des corps commutatifs**.

Remarque. Soit K/k une extension (de corps commutatifs), alors K est muni canoniquement d'une structure d'espace vectoriel sur k, ses lois sont celle qui associe tout couple (x, y) de $K \times K$ par $x + y \in K$ et celle qui associe tout couple (λ, x) de $k \times K$ par $\lambda \cdot x \in K$.
Par abus de langage les termes : système, partie libre, partie génératrice, base se rapportent à une extension K/k sont ceux de l'espace vectoriel K sur k.

Définition 1.2. Soit K/k une extension, la dimension de l'espace vectoriel K sur k s'appelle le degré de l'extension K/k qu'on note par $[K : k]$.

Exemples.

1) $[\mathbb{C} : \mathbb{R}] = 2$, car $\dim_{\mathbb{R}} \mathbb{C} = 2$.
2) Pour tout corps K, on a $[K(X) : K] = +\infty$. En effet, $\{1, X, \ldots, X^n, \ldots\}$ est une famille libre infinie de vecteurs de $K(X)$. Par conséquent, $K(X)$ est de dimension infinie sur K.

$$K(X) = \{\frac{f(X)}{g(X)} \mid f, g \in K(X), g \neq 0\} \text{ appelé le corps des fractions rationnelles sur } K.$$

Remarque. Soit K/k une extension de corps. Alors $[K : k] = 1$ si, et seulement si, $K = k$.

Proposition 1.1. *Soit L une sous-extension de K/k, alors* $[K : k] = [K : L] \cdot [L : k]$.

Preuve. Soient $(e_i)_{i \in I}$ une base de K/L et $(\varepsilon_j)_{j \in J}$ une base de L/k. Soit $\mathcal{S} = (e_i \varepsilon_j)_{(i,j) \in I \times J}$ et montrons que $\mathcal{S}$ est une base de K/k.
La partie $\mathcal{S}$ est génératrice. En effet, soit $x \in K$, alors $x = \sum\limits_{i \in I} \lambda_i e_i$ avec $\lambda_i \in L,\ \forall\ i \in I$, chaque λ_i s'écrit alors $\lambda_i = \sum\limits_{j \in J} \lambda_{i,j} \varepsilon_j$ avec $\lambda_{i,j} \in k,\ \forall\ j \in J$, ainsi

$$x = \sum_{i \in I} (\sum_{j \in J} \lambda_{i,j} \varepsilon_j) e_i = \sum_{i \in I} \sum_{j \in J} \lambda_{i,j} \varepsilon_j e_i,$$

ce qui donne que $\mathcal{S}$ est une partie génératrice de K/k.

La partie $\mathcal{S}$ est libre (sur k). En effet, si $\sum_{(i,j)\in I\times J} \lambda_{i,j}\varepsilon_j e_i = 0$ avec $\lambda_{i,j} \in k$, alors

$$\sum_{i\in I}\left(\sum_{j\in J}\lambda_{i,j}\varepsilon_j\right)e_i = 0 \Rightarrow \sum_{j\in J}\lambda_{i,j}\varepsilon_j = 0,\ \forall\, i \in I \Rightarrow \lambda_{i,j} = 0,\ \forall\, j \in J,$$

ce qui donne que $\lambda_{i,j} = 0,\ \forall\, (i,j) \in I \times J$, par suite $\mathcal{S}$ est libre. □

Définition 1.3. Une extension K/k est dite finie, si $[K : k]$ est fini.

Corollaire 1.2. *Soit L une sous-extension d'une extension K/k, alors K/k est finie si et seulement si K/L et L/k sont finies.*

1.2 Éléments algébriques

Définition 1.4. Soient K/k une extension et α un élément de K. On dit que α est algébrique sur k si α est une racine d'un polynôme non nul P dans $k[X]$. Dans le cas contraire on dit que α est transcendant sur k.

On a donc :

- α est algébrique sur $k \Leftrightarrow \exists P \in k[X],\ P \neq 0,\ P(\alpha) = 0$.
- α est transcendant sur $k \Leftrightarrow (\forall P \in k[X],\ P(\alpha) = 0 \Rightarrow P = 0)$.

Exemples.

1) Soit k un corps, alors $\forall\ \alpha \in k$, α est toujours algébrique sur k. En effet, α est racine de $X - \alpha \in k[X]$.
2) $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. En effet, $\sqrt{2}$ est racine de $X^2 - 2 \in \mathbb{Q}[X]$.
3) Soit $z \in \mathbb{C}$, alors z est algébrique sur $\mathbb{R}$. En effet, on a $z = a + bi$ avec $a, b \in \mathbb{R}$ est une racine du polynôme réel $X^2 - 2aX + a^2 + b^2$.
4) Le nombre réel π est transcendant sur $\mathbb{Q}$ (Lindemann).

Remarque. Soit L une sous-extension d'une extension K/k et $\alpha \in K$, alors

- α est algébrique sur $k \Rightarrow \alpha$ est algébrique sur L.
- α est transcendant sur $L \Rightarrow \alpha$ est transcendant sur k.

Remarque. Soient K/k une extension, α un élément de K et h une application de $k[X]$ dans K qui associe chaque polynôme P par $P(\alpha)$, alors h est homomorphisme d'anneaux et on a

- α est algébrique sur $k \Leftrightarrow \mathrm{Ker}(h) \neq \{0\} \Leftrightarrow h$ n'est pas injectif.
- α est transcendant sur $k \Leftrightarrow \mathrm{Ker}(h) = \{0\} \Leftrightarrow h$ est injectif.

Proposition 1.3. *Soient K/k une extension, α un élément de K algébrique sur k, alors il existe un polynôme unitaire unique Q dans $k[X]$ tel que $\forall\ P \in k[X],\ P(\alpha) = 0 \Leftrightarrow Q \mid P$.*

Preuve. Reprenons l'homomorphisme h définit ci-dessus. On a $\mathrm{Ker}(h)$ est un idéal de $k[X]$ et $k[X]$ est un anneau principal, donc il existe un polynôme Q_1 dans $k[X]$ tel que $\mathrm{Ker}(h) = (Q_1)$ et comme $\mathrm{Ker}(h) \neq \{0\}$, alors $Q_1 \neq 0$.
Écrivons $Q_1 = a_nX^n + \ldots + a_1X + a_0$ avec les a_i dans k et $a_n \neq 0$ et soit $Q = \frac{Q_1}{a_n}$, alors $(Q) = (Q_1)$, Q est unitaire et $\forall\ P \in k[X],\ P(\alpha) = 0 \Leftrightarrow P \in \mathrm{Ker}(h) \Leftrightarrow P \in (Q) \Leftrightarrow Q \mid P$.
Soit $\tilde{Q}$ un polynôme unitaire de $k[X]$ qui possède la propriété $\forall\ P \in k[X],\ P(\alpha) = 0 \Leftrightarrow \tilde{Q} \mid P$. On a $Q(\alpha) = 0$, alors $\tilde{Q} \mid Q$ et on a $\tilde{Q}(\alpha) = 0$, donc $Q \mid \tilde{Q}$, ainsi $\tilde{Q} = \lambda Q$ avec $\lambda \in k^*$ et comme Q et $\tilde{Q}$ sont unitaires, alors $\lambda = 1$ et $Q = \tilde{Q}$. □

Proposition 1.4. *Avec les notations de la proposition 1.3, le polynôme Q est irréductible (sur k). Soit $\tilde{Q}$ un polynôme irréductible dans $k[X]$ qui vérifie $\tilde{Q}(\alpha) = 0$, alors $\tilde{Q} = \lambda Q$ avec $\lambda \in k^*$.*

Preuve. Supposons que $Q = A \cdot B$ avec $A, B \in k[X]$, alors $Q(\alpha) = A(\alpha) \cdot B(\alpha) = 0$, donc $A(\alpha) = 0$ ou $B(\alpha) = 0$, supposons que $A(\alpha) = 0$, alors $Q \mid A$ et comme $A \mid Q$, alors B est un polynôme constant, ce qui donne que Q est irréductible.
Soit $\tilde{Q}$ un polynôme irréductible dans $k[X]$ tel que $\tilde{Q}(\alpha) = 0$, alors $Q \mid \tilde{Q}$, or $\tilde{Q}$ est irréductible, alors $\exists\ \lambda \in k^*$ tel que $\tilde{Q} = \lambda Q$. □

Définition 1.5. Avec les notations de la proposition 1.3, le polynôme Q s'appelle le polynôme irréductible de α sur k et son degré s'appelle le degré de α sur k. On note $Q = \mathrm{Irr}(\alpha/k)$ et $\deg(Q) = \deg(\alpha/k)$.

Exemple. On a $\mathrm{Irr}(\sqrt{2}/\mathbb{Q}) = X^2 - 2$ et $\deg(\sqrt{2}/\mathbb{Q}) = 2$.

Proposition 1.5. *Soient K/k une extension, α un élément de K algébrique sur k et $Q = \mathrm{Irr}(\alpha/k)$, alors on a un isomorphisme canonique de $k[X]/(Q)$ dans $k[\alpha]$ qui associe $\overline{P}$ par $P(\alpha)$. En particulier $k[\alpha]$ est un corps et $k[\alpha] = k(\alpha)$.*

Preuve. Reprenons l'homomorphisme h de $k[X]$ dans K qui associe P par $P(\alpha)$, alors h induit un isomorphisme canonique de $k[X]/\mathrm{Ker}(h)$ dans $\mathrm{Im}(h)$ qui associe $\overline{P}$ par $h(P) = P(\alpha)$, or $\mathrm{Ker}(h) = (Q)$ et $\mathrm{Im}(h) = \{P(\alpha) \mid P \in k[X]\} = k[\alpha]$.
Comme Q est irréductible, alors (Q) est maximal, ainsi $k[X]/(Q)$ est un corps, ce qui donne que $k[\alpha]$ est un corps, par suite $k(\alpha) \subseteq k[\alpha]$ et comme on a toujours $k[\alpha] \subseteq k(\alpha)$, alors $k[\alpha] = k(\alpha)$. □

Proposition 1.6. *Soient K/k une extension et α un élément de K, alors α est algébrique sur k si et seulement si $k[\alpha] = k(\alpha)$.*

Preuve. Si α est algébrique sur k, alors, d'après la proposition précédente, $k[\alpha] = k(\alpha)$.
Si $k[\alpha] = k(\alpha)$, supposons que $\alpha \neq 0$, alors $\frac{1}{\alpha} \in k[\alpha]$, ainsi il existe un polynôme P dans $k[X]$ tel que $P(\alpha) = \frac{1}{\alpha}$, ce qui donne $\exists\ P \in k[X],\ \alpha P(\alpha) = 1$, soit $\tilde{P} = XP - 1$, alors $\tilde{P}(\alpha) = 0$ et $\tilde{P}(0) = -1 \neq 0$, ainsi α est algébrique sur k (car $\tilde{P} \in k[X]$). □

Proposition 1.7. *Soient K/k une extension, α un élément de K algébrique sur k et $n = \deg(\alpha/k)$, alors $B = (1, \alpha, \ldots, \alpha^{n-1})$ est une base de $k(\alpha)/k$. En particulier, $k(\alpha)/k$ est finie et $[k(\alpha) : k] = n$.*

Preuve. La partie B est génératrice, en effet soit $x \in k(\alpha) = k[\alpha]$, alors $x = P(\alpha)$ avec $P \in k[X]$. Effectuons la division euclidienne de P par $Q = \mathrm{Irr}(\alpha/\mathbb{Q})$, alors $P = Q_1 Q + R$ avec $Q_1, R \in k[X]$ et $\deg(R) < n$, ainsi $x = P(\alpha) = Q_1(\alpha)Q(\alpha) + R(\alpha) = R(\alpha)$. Comme $\deg(R) < n$, alors on peut écrire $R = r_{n-1}X^{n-1} + \ldots + r_1 X + r_0$ avec les r_i dans k, ainsi $x = r_{n-1}\alpha^{n-1} + \ldots + r_1\alpha + r_0$ et la partie B est génératrice.
La partie B est libre, car si $r_{n-1}\alpha^{n-1} + \ldots + r_1\alpha + r_0 = 0$ avec les r_i dans k, alors il existe un polynôme $R = r_{n-1}X^{n-1} + \ldots + r_1 X + r_0$ de $k[X]$ de degré inférieur strictement à n et tel que $R(\alpha) = 0$, alors $R = 0$ c'est-à-dire $r_i = 0,\ \forall\ i$ et ainsi la partie B est libre. □

Lemme 1.8. *Soit K/k une extension de corps. Alors $\alpha \in K$ est algébrique sur k si, et seulement si, il existe $n > 0$ tel que la famille $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur k.*

Preuve. Supposons premièrement que α est algébrique sur k. Alors il existe $f(X) = a_0 + a_1 X + \ldots + a_n X^n \in k[X]$ non nul tel que $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Donc $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur k.
Supposons réciproquement que $\{1, \alpha, \ldots, \alpha^n\}$ avec $n > 0$ est liée sur k. Alors il existe $a_0, a_1, \ldots, a_n \in k$ non tous nuls tels que $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Cela veut dire que $a_0 + a_1 X + \ldots + a_n X^n$ est un polynôme non nul sur k dont α est une racine. Donc α est algébrique sur k. □

Exemple. Soit $k(X)$ le corps des fractions rationnelles sur k. Alors $X \in k(X)$ est transcendant sur k. En effet, pour tout $n > 0$, la famille $\{1, X, \ldots, X^n\}$ est libre sur k. Donc X est transcendant sur k.

Proposition 1.9. *Soient K/k une extension et α un élément de K, alors α est algébrique sur k si et seulement si l'extension $k(\alpha)/k$ est finie.*

Preuve. Si α est algébrique sur k, alors, d'après la proposition précédente, l'extension $k(\alpha)/k$ est finie.
Inversement, si l'extension $k(\alpha)/k$ est finie. Posons $[k(\alpha) : k] = n$, le système $(1, \alpha, \ldots, \alpha^n)$ contient $n+1$ éléments, donc il lié (sur k), donc $\exists\ \lambda_0, \lambda_1, \ldots, \lambda_n \in k$ non tous nuls tel que $\lambda_0 + \lambda_1\alpha + \ldots + \lambda_n\alpha^n = 0$. Posons $P = \lambda_0 + \lambda_1 X + \ldots + \lambda_n X^n$, on a donc $P \in k[X],\ P \neq 0$ et $P(\alpha) = 0$, ainsi α est algébrique sur k. □

Remarque. L'isomorphisme de $k[X]/(Q)$ dans $k(\alpha)$ et qui associe $\overline{P}$ par $P(\alpha)$ suggère comment inversement étant donné un polynôme irréductible Q de $k[X]$ on peut construire une extension de k de la forme $k(\alpha)$ avec $Q(\alpha) = 0$.
Par exemple pour $Q = X^2 + 1$ qui est un polynôme irréductible de $\mathbb{R}[X]$ et i est une racine de ce polynôme, donc $\mathbb{R}[X]/(Q) \simeq \mathbb{R}(i)$ qui est par définition le corps $\mathbb{C}$.

Proposition 1.10. *Soient k un corps commutatif, $P \in k[X] \setminus k$, alors il existe une extension K de k de la forme $k(\alpha)$ avec $P(\alpha) = 0$.*

Preuve. Comme $P \in k[X]\setminus k$, alors P admet un diviseur irréductible Q. Posons $K = k[X]/(Q)$, comme Q est irréductible, alors K est un corps. L'application qui fait correspondre α dans k par $\overline{\alpha}$ dans K est un homomorphisme (injectif) de corps identifiant $\overline{\alpha}$ avec α, donc k s'identifie à un sous-corps de K.
Soit $x \in K$, donc $x = \overline{P_1},\ P_1 \in k[X]$ et écrivons $P_1 = a_n X^n + \ldots + a_1 X + a_0$, on a

$$x = \overline{P_1} = \overline{a_n}\,\overline{X}^n + \ldots + \overline{a_1}\,\overline{X} + \overline{a_0},$$

donc si on pose $\alpha = \overline{X}$, alors x s'identifie à $P_1(\alpha)$, donc K s'identifie à $k[\alpha](= k(\alpha))$.
Prenons $P = P_1$, on a $\overline{P} = \overline{0}$ car $Q \mid P$, or $\overline{P}$ s'identifie à $P(\alpha)$ donc $P(\alpha) = 0$. □

Cette proposition sera considérablement généralisée au chapitre 4.

1.3 Extensions algébriques

Définition 1.6. Une extension K/k est dite algébrique si tout élément de K est algébrique sur k, dans le cas contraire K/k est dite transcendante.

Exemples.

1) Soit k un corps, alors k est algébrique sur lui-même.
2) L'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est algébrique.
3) L'extension $\mathbb{C}/\mathbb{R}$ est algébrique.
4) L'extension $\mathbb{R}/\mathbb{Q}$ n'est pas algébrique.

Remarque. Soit L une sous-extension d'une extension K/k. Si l'extension K/k est algébrique, alors l'extension K/L est algébrique.

Proposition 1.11. *Toute extension finie est algébrique.*

Preuve. Soient K/k une extension finie et α un élément de K. On a $k(\alpha)$ est un sous-espace vectoriel de K sur k, donc comme K/k est finie, alors l'extension $k(\alpha)/k$ est finie, ainsi α est algébrique sur k, par suite K/k est algébrique. □

Proposition 1.12 (Transitivité de l'algébricité)**.**
Soit L une sous-extension d'une extension K/k, alors l'extension K/k est algébriques si et seulement si les extensions K/L et L/k sont algébriques.

Preuve. Si K/k est algébriques, alors, d'après la remarque au dessus, l'extension K/L est algébrique et comme $L \subseteq K$, alors L/k est algébrique.
Inversement, Supposons que les extensions K/L et L/k sont algébriques et soit $\alpha \in K$, alors α est algébrique sur L, donc posons $\mathrm{Irr}(\alpha/L) = X^n + \ldots + a_1X + a_0$. Comme les a_i sont dans L et L/k est algébrique, alors pour $i \in \{0, \ldots, n-1\}$, il existe $P_i \in k[X],\ P_i \neq 0$ et $P_i(a_i) = 0$, ainsi il existe $P \in k[X],\ P \neq 0$ et $P(\alpha) = 0$, ce qui veut dire que α est algébrique sur k, par suite K/k est algébrique.
On peut montrer ceci aussi en utilisant la transitivité de la finitude. □

Proposition 1.13. *Soit K/k une extension, alors l'ensemble des éléments de K algébriques sur k est une sous-extension de l'extension K/k.*

Preuve. Soient $\alpha,\ \beta$ deux éléments de K algébriques sur k. On a α est algébrique sur k, donc l'extension $k(\alpha)/k$ est algébrique. On a β est algébrique sur k, donc algébrique sur $k(\alpha)$, ainsi l'extension $k(\alpha)(\beta)/k(\alpha)$ est algébrique et par transitivité l'extension $k(\alpha, \beta)/k$ sera algébrique. Ce qui donne que $\alpha + \beta,\ \alpha - \beta,\ \alpha\beta,\ \alpha/\beta$ (pour $\beta \neq 0$) sont algébriques sur k, ainsi l'ensemble des éléments de K algébriques sur k est une sous-extension de l'extension K/k. □

Définition 1.7. Soit K/k une extension. L'ensemble des éléments de K algébriques sur k s'appelle clôture algébrique de k dans K.

Il résulte immédiatement de cette définition que la clôture algébrique L de k dans K est caractérisée par :

$$\forall\ L' \text{ sous-extension de } K/k,\ L'/k \text{ est algébrique } \Leftrightarrow L' \subset L.$$

Ou encore par :

1) L/k est algébrique,

2) $\forall\ x \in K \setminus L,\ x$ est transcendant sur k.

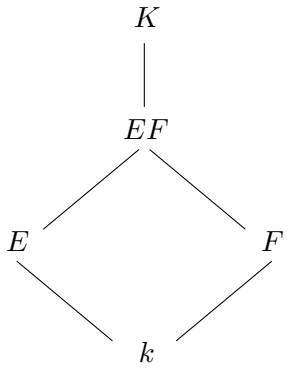
Ce qui est, par transitivité, équivaut à

1) L/k est algébrique,

2) $\forall\ x \in K \setminus L,\ x$ est transcendant sur L.

1.4 Extensions produits

Définition 1.8. Soient E et F des sous-extensions d'une extension K/k. On appelle produit des sous-corps E et F, le sous-corps de K engendré par $E \cup F$, c'est-à-dire $k(E \cup F)$, et qu'on note par $E \vee F$ (ou souvent par EF).



Exemple. On a $E = \mathbb{Q}(\sqrt{2})$ et $F = \mathbb{Q}(\sqrt{3})$ sont des sous-extensions de l'extension $\mathbb{R}/\mathbb{Q}$ et $EF = \mathbb{Q}(\sqrt{2},\ \sqrt{3})$.

Proposition 1.14. *Soient E_1/F_1 et E_2/F_2 des sous-extensions d'une extension K/k. Si E_1/F_1 et E_2/F_2 sont algébriques, alors $(E_1E_2)/(F_1F_2)$ est algébrique.*

Preuve. La clôture algébrique de F_1F_2 dans K contient E_1 et E_2, donc contient E_1E_2, d'où le résultat. □

Proposition 1.15. *Soient E et F des sous-extensions d'une extension K/k, alors il est équivalent de dire*

1) Tout système de E k-libre est F-libre.

2) Tout système de F k-libre est E-libre.

3) Si $(e_i)_{i\in I}$ et $(\varepsilon_j)_{j\in J}$ sont des systèmes respectivement de E et de F k-libres, alors $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est k-libre.

Preuve. Il suffit de montrer que (1) $\Leftrightarrow$ (3).
Supposons qu'on a (1) et soient $(e_i)_{i\in I}$ et $(\varepsilon_j)_{j\in J}$ des systèmes respectivement de E et de F k-libres. Soit $(\lambda_{i,j})_{(i,j)\in I\times J}$ une famille d'éléments de k tel que $\sum\limits_{(i,j)\in I\times J}\lambda_{i,j}e_i\varepsilon_j = 0$, alors $\sum\limits_{i\in I}\left(\sum\limits_{j\in J}\lambda_{i,j}\varepsilon_j\right)e_i = 0$. Comme $\sum\limits_{j\in J}\lambda_{i,j}\varepsilon_j \in F$ et comme $(e_i)_{i\in I}$ est un système de E k-libre, alors il est F-libre par (1), ce qui donne que $\sum\limits_{j\in J}\lambda_{i,j}\varepsilon_j = 0,\ \forall\ i \in I$. Comme $(\varepsilon_j)_{j\in J}$ est un système de F k-libre, alors $\lambda_{i,j} = 0,\ \forall\ (i,j) \in I \times J$, par suite $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est k-libre.
Supposons qu'on a (3) et soit $(e_i)_{i\in I}$ un système de E k-libre. Soit $(\lambda_i)_{i\in I}$ une famille d'éléments de F tel que $\sum\limits_{i\in I}\lambda_i e_i = 0$, soit $(\varepsilon_j)_{j\in J}$ une base de F/k, alors chaque λ_i s'écrit $\lambda_i = \sum\limits_{j\in J}\lambda_{i,j}\varepsilon_j$, ainsi $\sum\limits_{i\in I}\left(\sum\limits_{j\in J}\lambda_{i,j}\varepsilon_j\right)e_i = 0$, et comme $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est k-libre, alors $\lambda_{i,j} = 0,\ \forall\ (i,j) \in I \times J$, ce qui donne que $\lambda_i = 0,\ \forall\ i \in I$, par suite $(e_i)_{i\in I}$ est F-libre. □

1.5 Extensions linéairement disjointes

Définition 1.9. Soient E et F des sous-extensions d'une extension K/k. On dit que E et F sont k-linéairement disjoints s'ils vérifient l'une des conditions équivalentes de la proposition 1.15.

Remarque. Soient E et F des sous-extensions d'une extension K/k. Si E et F sont k-linéairement disjoints, alors $E \cap F = k$.

En effet, soit $x \in E \cap F$, alors le système $(1, x)$ est F-lié, donc $(1, x)$ est k-lié, ce qui donne que $x \in k$, par suite $E \cap F \subset k$, d'où le résultat.

Remarque. Soient E/k et F/k deux extensions, M une sous-extension de E/k et N une sous-extension de F/k. Si E et F sont k-linéairement disjoints, alors M et N sont k-linéairement disjoints.

En effet, soit S un système de M, k-libre, alors S est un système de E, k-libre (car $M \subset E$). Comme E et F sont k-linéairement disjoints, alors S est F-libre, ainsi S est N-libre (car $N \subset F$), ce qui donne que M et N sont k-linéairement disjoints.

Exemples.

1) Dans l'extension $\mathbb{C}/\mathbb{Q}$, les sous-extensions $\mathbb{R}$ et $\mathbb{Q}[i]$ sont $\mathbb{Q}$-linéairement disjointes.

2) Dans l'extension $\mathbb{C}/\mathbb{Q}$, les sous-extensions $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $F = \mathbb{Q}(\sqrt[4]{2})$ ne sont pas $\mathbb{Q}$-linéairement disjointes.

   En effet, si E et F sont $\mathbb{Q}$-linéairement disjointes, alors $E \cap F = \mathbb{Q}$, ce qui n'est pas le cas. Donc E et F ne sont pas $\mathbb{Q}$-linéairement disjointes.

Remarque. Soient E et F des sous-extensions d'une extension K/k. Si $E \cap F = k$, alors on a pas nécessairement que E et F sont k-linéairement disjoints.

Contre exemple. Pour $k = \mathbb{Q}$, $K = \mathbb{C}$, $E = \mathbb{Q}(\sqrt[3]{2})$ et $F = \mathbb{Q}(j\sqrt[3]{2})$, on a $E \cap F = k$ mais E et F ne sont pas linéairement disjoints sur k.
En effet, $B = \left\{1,\ j\ \sqrt[3]{2},\ \left(j\ \sqrt[3]{2}\right)^2\right\}$ est une base de F/k (avec $j = e^{i\frac{2\pi}{3}}$), donc B est un système de F, k-libre. Mais le système B n'est pas E-libre (B est E-lié) car B vérifie la relation linéaire

$$\left(j\ \sqrt[3]{2}\right)^2 + \sqrt[3]{2}\cdot(j\ \sqrt[3]{2}) + \sqrt[3]{2}^2 \cdot 1 = \sqrt[3]{2}^2\left(j^2 + j + 1\right) = 0,$$

et les coefficients sont dans E.

Proposition 1.16. *Soient E et F deux sous-extensions d'une extensions K/k avec E/k ou F/k est algébrique, $(e_i)_{i\in I}$ une base de E/k, $(\varepsilon_j)_{j\in J}$ une base de F/k, alors*

1) *$(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est un générateur de $(EF)/k$.*
2) *$(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est une base de EF sur k si et seulement si E et F sont k-linéairement disjoints.*

Corollaire 1.17. *Soient E et F deux sous-extensions d'une extensions K/k avec E/k ou F/k est algébrique, alors*

1) *$[EF : k] \leq [E : k] \times [F : k]$.*
2) *Si E et F sont k-linéairement disjoints, alors $[EF : k] = [E : k] \times [F : k]$.*
3) *Si E/k et F/k sont finies, alors E et F sont k-linéairement disjoints si et seulement si $[EF : k] = [E : k] \times [F : k]$*

Preuve.

1) Soient $(e_i)_{i\in I}$ une base de E/k, $(\varepsilon_j)_{j\in J}$ une base de F/k, alors, d'après la proposition 1.16, $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est un générateur de EF/k, donc de cette partie on peut extraire une base de EF/k, ainsi
$$[EF : k] \leq [E : k] \times [F : k].$$
2) Supposons que E et F sont k-linéairement disjoints, alors si $(e_i)_{i\in I}$ est une base de E/k et $(\varepsilon_j)_{j\in J}$ est une base de F/k, alors $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est une base de EF/k, ce qui donne que
$$[EF : k] = [E : k] \times [F : k].$$
3) Supposons que E/k et F/k sont finies et montrons que : E et F sont k-linéairement disjoints si et seulement si $[EF : k] = [E : k] \times [F : k]$.
Si E et F sont k-linéairement disjoints, alors, d'après (2),
$$[EF : k] = [E : k] \times [F : k].$$
Supposons maintenant que $[EF : k] = [E : k] \times [F : k]$, or on sait que
$$[EF : k] = [EF : F] \times [F : k] \Rightarrow [EF : F] = [E : k].$$
Soit $\{e_1, \ldots, e_n\}$ un système de E, k-libre et soient $\lambda_1, \ldots, \lambda_n \in F$ tel que $\lambda_1 e_1 + \ldots + \lambda_n e_n = 0$, or cette dernière combinaison linéaire et dans EF et on a $[EF : F] = [E : k]$, donc $\lambda_1 = \ldots = \lambda_n = 0$, ainsi $\{e_1, \ldots, e_n\}$ est F-libre, par suite E et F sont k-linéairement disjoints.

□

Proposition 1.18. *Soient E et F deux sous-extensions d'une extension K/k avec E/k ou F/k est algébrique, $(e_i)_{i\in I}$ une base de E/k, alors*

1) *$(e_i)_{i\in I}$ est un générateur de EF/F.*
2) *$(e_i)_{i\in I}$ est une base de EF/F si et seulement si E et F sont k-linéairement disjoints.*

Corollaire 1.19. *Soient E et F deux sous-extensions d'une extension K/k avec E/k ou F/k est algébrique, alors*

1) $[EF : F] \leq [E : k]$.

2) *Si E et F sont k-linéairement disjoints, alors $[EF : F] = [E : k]$.*

3) *Si E/k est finie, alors E et F sont k-linéairement disjoints si et seulement si $[EF : F] = [E : k]$.*

Remarque. La proposition 1.16 est équivalente à la proposition 1.18.

Car si L est une sous-extension d'une extension K/k, $(e_i)_{i\in I}$ un système de K et $(\varepsilon_j)_{j\in J}$ une base de L/k, alors on a :

- $(e_i)_{i\in I}$ est L-libre $\Leftrightarrow$ $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est k-libre.
- $(e_i)_{i\in I}$ est générateur de $K/L \Leftrightarrow$ $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est générateur de K/k.
- $(e_i)_{i\in I}$ est une base de $K/L \Leftrightarrow$ $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est une base de K/k.

De même, Soient $(e_i)_{i\in I}$ une base de K/L et $(\varepsilon_j)_{j\in J}$ un système de L, alors on a :

- $(\varepsilon_j)_{j\in J}$ est k-libre $\Leftrightarrow$ $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est k-libre.
- $(\varepsilon_j)_{j\in J}$ est générateur de $L/k \Leftrightarrow$ $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est générateur de K/k.
- $(\varepsilon_j)_{j\in J}$ est une base de $L/k \Leftrightarrow$ $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est une base de K/k.

Lemme 1.20. *Soient E et F deux sous-extensions d'une extension K/k avec E/k ou F/k est algébrique, alors*

$$EF = \{\sum_{n\in\mathbb{N}} a_n b_n \mid a_n \in E,\ b_n \in F \text{ presque tous nuls }\} = \{\sum_{\text{finie}} a_n b_n \mid a_n \in E,\ b_n \in F\}.$$

Preuve. Soit $B = \{\sum_{n\in\mathbb{N}} a_n b_n \mid a_n \in E,\ b_n \in F$ presque tous nuls $\}$, alors $B \subset EF$.
Aussi, on a B est un sous-anneau de EF, E et F sont inclus dans B. Pour montrer que $EF \subset B$, il suffit de montrer que B est un corps. Pour ceci, soit $x \in B$ tel que $x \neq 0$, supposons que E/k est algébrique, donc EF/F est algébrique, ainsi x est algébrique sur F, donc $F[x]$ est un corps, ce qui donne que $x^{-1} \in F[x]$, or $F[x] \subset B$, donc $x^{-1} \in B$, par suite B est un corps et on a $EF \subset B$. □

Preuve de la proposition 1.18.
Proposition 1.18. Soient E et F deux sous-extensions d'une extension K/k avec E/k ou F/k est **algébrique**, $(e_i)_{i\in I}$ une base de E/k, alors

1) $(e_i)_{i\in I}$ est un générateur de EF/F.

2) $(e_i)_{i\in I}$ est une base de EF/F si et seulement si E et F sont k-linéairement disjoints.

1) Soient $(e_i)_{i\in I}$ une base de E/k et $x \in EF$, alors $x = \sum_{s=0}^{n} a_s b_s, a_s \in E,\ b_s \in F$, chaque a_s peut s'écrire $a_s = \sum_{i\in I} a_{s,i} e_i,\ a_{s,i} \in k$, donc $x = \sum_{i\in I} \left(\sum_{s=0}^{n} a_{s,i} b_s\right) e_i$, or $\sum_{s=0}^{n} a_{s,i} b_s \in F$, ainsi $(e_i)_{i\in I}$ est un générateur de EF/F.

2) Si E et F sont k-linéairement disjoints, $(e_i)_{i\in I}$ est F-libre, donc c'est une base de EF/F.
Inversement, supposons que $(e_i)_{i\in I}$ est une base de EF/F. Soit $(\varepsilon_j)_{j\in J}$ un système de F, k-libre, comme $(e_i)_{i\in I}$ est une base de EF/F, alors $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est k-libre. Comme $(e_i)_{i\in I}$ est une base de E/k et que $(e_i\varepsilon_j)_{(i,j)\in I\times J}$ est k-libre, alors $(\varepsilon_j)_{j\in J}$ est k-libre, $(\varepsilon_j)_{j\in J}$ est E-libre, ainsi E et F sont k-linéairement disjoints.

□

Cas particuliers de la proposition 1.14.

▷ Soient E et F des sous-extensions d'une extension K/k.
Si E/k et F/k sont algébriques, alors EF/k est algébrique.

▷ Soient E/F et L des sous-extensions d'une extension K/k.
Si E/F est algébrique, alors EL/FL est algébrique.

▷ Soient E/F une sous-extension d'une extension K/k et $A \subset K$.
Si E/F est algébrique, alors $E(A)/F(A)$ est algébrique.

Remarque. Soient $E = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}(j\sqrt[3]{2})$, $k = \mathbb{Q}$ et $K = \mathbb{C}$.
On a $E \cap F = k$, mais E et F ne sont pas k-linéairement disjoints car

$$\begin{aligned}[EF : k] &= [\mathbb{Q}(j, \sqrt[3]{2}) : \mathbb{Q}] \\ &= [\mathbb{Q}(j, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \\ &= 2 \times 3 \\ &= 6 \\ &< [E : k][F : k] = 3 \times 3 = 9.\end{aligned}$$

Remarque. Le corollaire 1.19 n'est pas vrai sans l'hypothèse que E/k ou F/k est algébrique.

En effet, pour $k = \mathbb{Q},\ E = \mathbb{Q}(X),\ F = \mathbb{C}$ et $K = \mathbb{C}(X)$, on a

$$[EF : F] = [\mathbb{C}(X) : \mathbb{C}] = |\mathbb{C}| > [E : k] = [\mathbb{Q}(X) : \mathbb{Q}] = |\mathbb{N}|.$$

$\left(X^n, \frac{1}{(X-\alpha)^m}\right),\ n, m \in \mathbb{N},\ n \geq 1,\ \alpha \in \mathbb{C}$ est une base de $\mathbb{C}[X]/\mathbb{C}$.

Proposition 1.21. *Soient E_1/F_1 et E_2/F_2 deux sous-extensions algébriques d'une extension K/k, alors*

$$[E_1E_2 :\ F_1F_2] \leq [E_1 :\ F_1] \times [E_2 :\ F_2].$$

Preuve. On a

$$[E_1E_2 : F_1F_2] = [E_1E_2 : E_1F_2] \times [E_1F_2 : F_1F_2].$$

et

$$[E_1E_2 : E_1F_2] = [(E_1F_2)E_2 : E_1F_2] \leq [E_2 : F_2].$$

De même

$$[E_1F_2 : F_1F_2] \leq [E_1 : F_2].$$

Ainsi

$$[E_1E_2 : F_1F_2] \leq [E_1 : F_1] \times [E_2 : F_2].$$

□

Corollaire 1.22. *Soient E_1/F_1 et E_2/F_2 des sous-extensions d'une extension K/k. Si les extensions E_1/F_1 et E_2/F_2 sont finies, alors l'extension E_1E_2/F_1F_2 est finie.*

Chapitre 2

Extensions transcendantes

2.1 Indépendance algébrique

Rappelons qu'un élément α d'un corps K est dit transcendant sur un sous-corps k de K s'il n'est pas algébrique sur ce corps. Cela équivaut à dire que la famille $(\alpha^n)_{n\geq 0}$ est linéairement indépendante sur k.
La transcendance de α sur k traduit aussi l'isomorphisme entre $k(\alpha)$ et le corps $k(X)$ des fractions rationnelles à coefficients dans k.
Une extension non algébrique d'un corps k est dite une extension transcendante de k.

Définition 2.1. Soient K/k une extension. Une famille $(\alpha_1, \ldots, \alpha_n)$ d'éléments de K est dite algébriquement libre (ou les α_i sont algébriquement indépendants) sur k si les monômes $\prod_{i=1}^{n} \alpha^{n_i}$ forment une famille linéairement indépendante sur k, cela équivaut à

$$\forall\ P \in k[X_1, \ldots, X_n],\ P(\alpha_1, \ldots, \alpha_n) = 0 \Rightarrow P = 0.$$

Dans le cas contraire, on dit que la famille $(\alpha_1, \ldots, \alpha_n)$ est algébriquement lié (ou les α_i sont algébriquement dépendants) sur k.
Une famille quelconque $\mathcal{S}$ d'éléments de K est dite algébriquement libre sur k si toutes ses sous-familles finies le sont.

Exemple.

1) Dans $\mathbb{R}/\mathbb{Q}$, $\{\pi\}$ est algébriquement libre sur $\mathbb{Q}$.
2) Dans $\mathbb{R}/\mathbb{Q}$, $\{\pi,\ e\}$ est algébriquement libre sur $\mathbb{Q}$.
3) Soit k un corps commutatif et $k(X, Y)$ le corps des fractions rationnelles sur k à 2 indéterminés, identifié à une extension de k, alors la famille (X, Y) est algébriquement libre sur k.

Proposition 2.1. *Soient K/k une extension et $(\alpha_1, \ldots, \alpha_n)$ une famille d'éléments de K. L'unique k-homomorphisme de $k[X_1, \ldots, X_n]$ dans K, qui envoie X_i sur α_i est injectif si et seulement si $(\alpha_1, \ldots, \alpha_n)$ est algébriquement libre sur k, au quel cas on a un k-isomorphisme*

$$\begin{array}{ccc} k(X_1, \ldots, X_n) & \to & k(\alpha_1, \ldots, \alpha_n). \\ \frac{P}{Q} & \mapsto & \frac{P(\alpha_1, \ldots, \alpha_n)}{Q(\alpha_1, \ldots, \alpha_n)} \end{array}$$

Remarque. Soient L une sous-extension d'une extension K/k et $(\alpha_1, \ldots, \alpha_n)$ une famille d'éléments de K.

1) Si la famille $(\alpha_1, \ldots, \alpha_n)$ est algébriquement liée sur k, alors $(\alpha_1, \ldots, \alpha_n)$ est algébriquement liée sur L.
2) Si la famille $(\alpha_1, \ldots, \alpha_n)$ est algébriquement libre sur L, alors $(\alpha_1, \ldots, \alpha_n)$ est algébriquement libre sur k.

Propriétés immédiates :

1) Soient K/k une extension et α un élément de K, alors $\{\alpha\}$ est algébriquement libre sur k si et seulement si α est transcendant sur k.
2) Soient K/k une extension et $L \subset K$. Si L est algébriquement libre sur k et $L' \subset L$, alors L' est algébriquement libre sur k.
   En particulier, si L est algébriquement libre sur k, alors $\forall\ \alpha \in L,\ \alpha$ est transcendant sur k.
3) Soient K/k une extension et $L \subset K$, alors L est algébriquement libre sur k si et seulement si toute partie finie de L est algébriquement libre sur k.

Proposition 2.2 (**Associativité de l'indépendance algébrique**).
Soient K/k une extension, A et B deux parties de K. Il est équivalent de dire :

1) *$A \cup B$ est algébriquement libre sur k avec $A \cap B = \emptyset$.*
2) *A est algébriquement libre sur k et B est algébriquement libre sur $k(A)$.*
3) *B est algébriquement libre sur k et A est algébriquement libre sur $k(B)$.*

Preuve. Il suffit de montrer que (1) $\Leftrightarrow$ (2).
Considérons le diagramme des k-homomorphismes canoniques suivant :

$$\begin{array}{ccc} k[X_a]_{a\in A}[Y_b]_{b\in B} & \xrightarrow{\ f\ } & k[A][Z_b]_{b\in B} \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle g} \\ k[T_c]_{c\in A\cup B} & \xrightarrow{\ h\ } & k[A\cup B] \end{array}$$

$A \cup B$ est algébriquement libre sur k avec $A \cap B = \emptyset \Leftrightarrow h$ et s sont injectifs
$\Leftrightarrow h \circ s$ est injectif car s est surjectif
$\Leftrightarrow g \circ f$ est injectif
$\Leftrightarrow f$ et g sont injectifs car f est surjectif
$$\Leftrightarrow \begin{cases} A \text{ est algébriquement libre sur } k \\ B \text{ est algébriquement libre sur } k(A). \end{cases}$$

□

Corollaire 2.3. *Soient K/k une extension, α et β deux éléments distincts de K, alors $\{\alpha, \beta\}$ est algébriquement libre sur k si et seulement si α est transcendant sur k et β est transcendant sur $k(\alpha)$.*

Proposition 2.4 (**Transitivité de la dépendance algébrique**).
Soient L une sous-extension d'une extension K/k et A une partie de K.

1) *Si A est algébriquement liée sur L et L/k est algébrique, alors A est algébriquement liée sur k.*
2) *Si A est algébriquement libre sur k est L/k est algébrique, alors A est algébriquement libre sur L.*

Pour la démonstration de cette proposition on est besoin du lemme suivant.

Lemme 2.5. *Soient K/k une extension et A une partie de K, alors A est algébriquement libre sur k si et seulement si $\forall\ x \in A,\ x$ est transcendant sur $k(A \setminus \{x\})$.*

Preuve. Supposons que A est algébriquement libre sur k, alors, en utilisant la proposition 2.2 (associativité de l'indépendance algébrique), on trouve que $\forall\ x \in A,\ x$ est transcendant sur $k(A \setminus \{x\})$.
Réciproquement, supposons que $\forall\ x \in A,\ x$ est transcendant sur $k(A \setminus \{x\})$ et montrons que A est algébriquement libre sur k.

Supposons que A est algébriquement liée sur k, alors il existe une partie finie non vide A_0 de A tel que A_0 est algébriquement liée sur k et choisissons $|A_0|$ minimum. Soit $x \in A_0$, alors $A_0 \setminus \{x\}$ est algébriquement libre sur k.
Comme $A_0 = (A_0 \setminus \{x\}) \cup \{x\}$ est algébriquement liée sur k, alors, par la proposition 2.2, x sera algébrique sur $k(A_0 \setminus \{x\})$, donc algébrique sur $k(A \setminus \{x\})$, ce qui n'est pas le cas, ainsi A est algébriquement libre sur k. □

Preuve. (Preuve de la proposition 2.4)

1) Supposons que A est algébriquement liée sur L, alors, par le lemme 2.5, $\exists\ x \in A$ tel que x est algébrique sur $L(A \setminus \{x\})$. Comme L/k est algébrique, alors $L(A \setminus \{x\})/k(A \setminus \{x\})$ est algébrique, donc x est algébrique sur $k(A \setminus \{x\})$, par le lemme 2.5, A est algébriquement liée sur k.
2) Supposons que A est algébriquement libre sur k et soit $x \in A$, alors, par le lemme 2.5, x est transcendant sur $k(A \setminus \{x\})$. Comme L/k est algébrique, alors $L(A \setminus \{x\})/k(A \setminus \{x\})$ est algébrique, donc x est transcendant sur $L(A \setminus \{x\})$ (car sinon, x est algébrique sur $L(A \setminus \{x\})$ et $L(A \setminus \{x\})/k(A \setminus \{x\})$ est algébrique, nous donne que x est algébrique sur $k(A \setminus \{x\})$, ce qui n'est pas le cas), ainsi, par le lemme 2.5, A est algébriquement libre sur L.

□

2.2 Générateurs algébriques

Définition 2.2. Soit K/k une extension, on dit que k est algébriquement clos dans K si tout élément de K algébrique sur k est dans k.

Exemple. Soit K/k une extension, L la clôture algébrique de k dans K, alors L est algébriquement clos dans K.

Proposition 2.6. *Soient K un corps commutatif et $(K_i)_{i\in I}$ une famille de sous-corps de K algébriquement clos dans K, alors $\bigcap_{i\in I} K_i$ est algébriquement clos dans K.*

Preuve. Soit x un élément de K algébrique sur $\bigcap_{i\in I} K_i$, alors x est algébrique sur chaque K_i, donc $x \in K_i,\ \forall\ i \in I$, ainsi $x \in \bigcap_{i\in I} K_i$. □

Définition 2.3. Soient K un corps commutatif et G une partie de K. On appelle sous-corps de K algébriquement engendré par G l'intersection des sous-corps de K algébriquement clos dans K contenant G.

Proposition 2.7. *Soient K un corps commutatif, G une partie de K, K_0 le sous-corps de K engendré par G et K_c le sous-corps de K algébriquement engendré par G, alors K_c est la clôture algébrique de K_0 dans K.*

Preuve. Soit L la clôture algébrique de K_0 dans K. On a $G \subset K_0 \subset L$, comme L est algébriquement clos dans K, alors $K_c \subset L$. Soit $\alpha \in L$, α est algébrique sur K_0, et comme $K_0 \subset K_c$, α est algébrique sur K_c, or K_c est algébriquement clos dans K, donc $\alpha \in K_c$, ainsi $L = K_c$. □

Remarque. Soient K un corps commutatif, G une partie de K, K_0 le sous-corps de K engendré par G et P le sous-corps premier de K, alors $K_0 = P(G)$.

En effet, On a K_0 est le plus petit sous-corps de K contenant G, donc $K_0 \subset P(G)$. d'autre part on a P est le plus petit sous-corps de K, donc $P \subset K_0$, et comme $G \subset K_0$, alors $P(G) \subset K_0$, d'où le résultat.

Définition 2.4. Soient K/k une extension et $(\alpha_1, \ldots, \alpha_n)$ une famille d'éléments de K. On dit que $(\alpha_1, \ldots, \alpha_n)$ est un générateur algébrique de K/k si tout élément de K est algébrique sur $k(\alpha_1, \ldots, \alpha_n)$.
On peut étendre cette définition à une famille quelconque $\mathcal{S} = (s_i)_{i\in I}$ d'éléments de K.

Remarque. Soient K/k une extension et G une partie de K. G est un générateur algébrique de K/k si $K/k(G)$ est algébrique.

Remarque. Soient K/k une extension et G une partie de K, alors G est un générateur algébrique de K/k si et seulement si K est le sous-corps de K algébriquement engendré par $k \cup G$.

En effet, soit K_c le sous-corps de K algébriquement engendré par $k \cup G$, alors $k(G) \to K_c \to K$. Si G est un générateur algébrique de K/k, alors $K/k(G)$ est algébrique, donc K/K_c est algébrique, or K_c est algébriquement clos dans K, donc $K = K_c$.
Inversement, si $K = K_c$, alors $K/k(G)$ est algébrique, ce qui veut dire que G est un générateur algébrique de K/k.

Remarque. Soient L une sous-extension d'une extension K/k et G une partie de K. Si G est un générateur algébrique de K/k, alors G est un générateur algébrique de K/L.

Propriétés immédiates :

1) Soient K/k une extension, G et G' deux parties de K avec $G \subset G'$. Si G est un générateur algébrique de K/k, alors G' est un générateur algébrique de K/k.
   En effet, on a $k(G) \to k(G') \to K$, donc si G est un générateur algébrique de K/k, alors $K/k(G)$ est algébrique, donc $K/k(G')$ est algébrique, ainsi G' est un générateur algébrique de K/k.
2) Soient K/k une extension et G une partie de K, alors G est un générateur algébrique de K/k si et seulement si $\forall\ x \in K,\ \exists\ G_0 \subset G$ tel que G_0 est finie et x est algébrique sur $k(G_0)$.

2.3 Base et dimension algébrique

Définition 2.5. Soient K/k une extension et $\mathcal{S} = (s_i)_{i\in I}$ un système de K. On dit que $\mathcal{S}$ est une base algébrique (ou base de transcendance) de K/k si $\mathcal{S}$ est à la fois algébriquement libre sur k et un générateur algébrique de K/k.

Exemple. Soit $k(X, Y)$ le corps des fractions rationnelles sur k à 2 indéterminés, identifié à une extension de k, le système (X, Y) est une base algébrique de $k(X, Y)/k$.

Définition 2.6. Soit K/k une extension de corps. Une famille $(x_i)_{i\in I}$ d'éléments de K est appelée **une base pure** de K/k si elle est algébriquement libre et si l'on a $K = k(x_i)_{i\in I}$.
On dit que K/k est une extension pure si K possède une base pure.

La famille vide est algébriquement libre, donc k est une extension pure de lui- même. Avec les notations de la définition 2.6, chaque élément x_i est transcendant sur k ; si I n'est pas vide, K est donc une extension transcendante de k.

Théorème 2.8 (**Théorème de la base incomplète**).
Soient K/k une extension, $L \subset K$ algébriquement libre sur k et G un un générateur algébrique de K/k, alors il existe $G_0 \subset G$ tel que $L \cup G_0$ soit une base algébrique de K/k. (On peut compléter L par des éléments de G pour obtenir une base algébrique de K/k).

Preuve. On va utiliser le lemme de Zorn, donc soit

$$\mathcal{E} = \{L' \mid L \subset L' \subset L \cup G,\ L' \text{ algébriquement libre sur } k\}.$$

- $\mathcal{E} \neq \emptyset$ (car $L \in \xi$).
- $\mathcal{E}$ est inductif pour l'inclusion.
  Soit $(L_i)_{i\in I}$ une famille totalement ordonnée de $\mathcal{E}$. Posons $M = \bigcup_{i\in I} L_i$, on a immédiatement que $L \subset M \subset L \cup G$. Soit $M_0 \subset M$, M_0 est finie, $\exists\ j$ tel que $M_0 \subset Lj$. Comme L_j est algébriquement libre sur k, M_0 aussi, donc $M \in \mathcal{E}$ et M majore la famille $(L_i)_{i\in I}$.

Soit $\hat{L}$ un élément maximal de $\mathcal{E}$. Comme $L \subset \hat{L} \subset L \cup G$, on a $\hat{L} = L \cup G',\ G' \subset G$. Montrons que $\hat{L}$ est une base algébrique de K/k.

- $\hat{L}$ est algébriquement libre, car $\hat{L} \in \mathcal{E}$.
- $\hat{L}$ est un générateur algébrique de K/k.
  En effet, soit $g \in G$, si g est transcendant sur $k(\hat{L})$, comme $\hat{L}$ est algébriquement libre sur k, $\hat{L} \cup \{g\}$ est algébriquement libre sur k et $g \notin \hat{L}$, donc $\hat{L} \subsetneq \hat{L} \cup \{g\}$ et $\hat{L} \cup \{g\} \in \mathcal{E}$, ce qui contredit que $\hat{L}$ est maximal. Donc $\forall\ g \in G$, g est algébrique sur $k(\hat{L})$, donc $k(\hat{L})(G)/k(\hat{L})$ est algébrique. Comme $K/k(G)$ est algébrique, $K/k(\hat{L})(G)$ est algébrique, donc $K/k(\hat{L})$ est algébrique (autrement, le sous-corps algébriquement engendré par $k \cup \hat{L}$ contient G (et k), donc contient le sous-corps algébriquement engendré par $k \cup G$ qui est K).

□

Cas particulier du Théorème 2.8 :

⋆) Toute partie algébriquement libre sur k de K/k se complète à une base algébrique ($G = K$).

⋆) Tout générateur algébrique de K/k contient une base algébrique ($L = \emptyset$).

⋆) Toute extension K/k admet une base algébrique ($L = \emptyset$ et $G = K$).

Remarque. Soient K/k une extension et B une base algébrique de K/k, on voit que K/k est composé de l'extension $k(B)/k$ qui est la plus simple extension transcendante (puisque k-isomorphe à $k(X_b)_{b\in B}$), et de l'extension $K/k(B)$ qui est algébrique ($k \longrightarrow k(B) \longrightarrow K$ la première est pure et la deuxième est algébrique).

Remarque. Soit K/k une extension. Toute base algébrique de K est un élément maximal de l'ensemble (ordonné par inclusion) des parties de K algébriquement libres sur k.
Inversement, si S est une partie de K telle que K soit algébrique sur $k(S)$, alors toute partie algébriquement libre maximale de S est une base algébrique de K.

En effet, soient B une base algébrique de K sur k, et $x \in K - B$. Alors x est algébrique sur $k(B)$ et la partie $B \cup \{x\}$ de K n'est pas algébriquement libre sur k, d'où la première partie de la remarque.
D'autre part, si K est algébrique sur $k(S)$, et B est une partie algébriquement libre maximale de S, alors $\forall\ x \in S$, x est algébrique sur $k(B)$; donc $k(S)$ est algébrique sur $k(B)$, et par suite K est algébrique sur $k(B)$.

Théorème 2.9 (**Théorème de la dimension**).
Soient K/k une extension, B et B' des bases algébriques de K/k, alors $\mathrm{card}(B) = \mathrm{card}(B')$.

Lemme 2.10 (**Lemme d'échange**).
Soient K/k une extension, B et B' des bases algébriques de K/k, alors pour $x \in B$, $\exists\ x' \in B'$ tel que $(B' \setminus \{x'\}) \cup \{x\}$ soit une base algébrique de K/k.

Preuve. Comme x est algébrique sur $k(B')$ et B' algébriquement libre sur k et x transcendant sur k, B' est algébriquement lié sur $k(x)$, donc $\exists\ x' \in B'$ tel que x' algébrique sur $k(x)(B' \setminus \{x'\})$, donc x' est algébrique sur $k((B' \setminus \{x'\}) \cup \{x\})$.
Soit $\tilde{B'} = (B' \setminus \{x'\}) \cup \{x\}$ et montrons que $\tilde{B'}$ est une base algébrique de K/k.

- $\tilde{B'}$ est un un générateur algébrique de K/k, car $\forall\ y \in B'$, y est algébrique sur $k(\tilde{B'})$ (car $y = x'$ ou $y \neq x' \Rightarrow y \in \tilde{B'}$).
- $\tilde{B'}$ est un algébriquement libre sur k, car sinon $B' \setminus \{x'\}$ est algébriquement libre sur k et on a x est algébrique sur $k(B' \setminus \{x'\})$, donc $k(B' \setminus \{x'\})(x)/k(B' \setminus \{x'\})$ est algébrique, comme x' est algébrique sur $k(B' \setminus \{x'\})(x)$, alors x' est algébrique sur $k(B' \setminus \{x'\})$. Or B' est algébriquement libre sur k, donc on a une contradiction avec l'associativité de l'indépendance algébrique. Ainsi $\tilde{B'}$ est un algébriquement libre sur k.

□

Preuve. (Preuve du Théorème 2.9).
Premier cas : l'une des base algébriques est finies.
Supposons que B est finie et soit $n = \text{card}(B)$, donc on va utiliser la récurrence sur $\text{card}(B)$. Pour $n = 0$, rien à démontrer car l'extension K/K sera algébrique, $\text{card}(B') = 0$. Si $n = 1$, alors nécessairement $\text{card}(B') = 1$, car sinon on aura une contradiction avec l'associativité de l'indépendance algébrique. Supposons que la propriété est vraie à l'ordre $n \geq 1$. Étant donné $x \in B$, le lemme d'échange fournit $x' \in B'$ tel que $(B' \setminus \{x'\}) \cup \{x\}$ soit une base algébrique de K/k, or $B \setminus \{x\}$ est une base algébrique de $K/k(x)$, de même $((B' \setminus \{x'\}) \cup \{x\}) \setminus \{x\} = B' \setminus \{x'\}$ est une base algébrique de $K/k(x)$ et $\text{card}(B \setminus \{x\}) < \text{card}(B)$, donc l'hypothèse de récurrence

$$\text{card}(B \setminus \{x\}) = \text{card}(B' \setminus \{x'\}) \Rightarrow \text{card}(B \setminus \{x\}) + 1 = \text{card}(B' \setminus \{x'\}) + 1 \Rightarrow \text{card}(B') = \text{card}(B).$$

Deuxième cas : les deux base algébriques sont infinies.
Soit $x \in B$, alors x est algébrique sur $k(B')$ et il existe une partie finie D_x de B' telle que x est algébrique sur $k(D_x)$. Posons $D = \bigcup_{x \in B} D_x$ d'où $D \subset B'$; comme B est infini, alors $\text{card}(D) \leq \text{card}(B)$. Mais tout élément de B étant algébrique sur $k(D)$, et K est algébrique sur $k(B)$, on conclut que K est algébrique sur $K(D)$, ce qui donne que $D = B'$, ce qui donne que $\text{card}(B') \leq \text{card}(B)$. De même $\text{card}(B) \leq \text{card}(B')$, ainsi $\text{card}(B) = \text{card}(B')$. □

Définition 2.7. Soit K/k une extension, le cardinal d'une base algébrique (quelconque) s'appelle degré de transcendance (ou dimension algébrique) de K/k et qu'on note par $\text{d°tr}(K/k)$.

Remarque. $\text{d°tr}(K/k) = 0 \Leftrightarrow K/k$ est algébrique.

Conséquences des théorèmes 2.8 et 2.9 :
Soit K/k une extension, supposons $\text{d°tr}(K/k) = n$ est fini, alors

⋆) Tout système algébriquement libre de K/k contient au plus n éléments.

⋆) Tout système algébriquement libre de K/k ayant n éléments est une base algébrique.

⋆) Tout système générateur algébrique de K/k contient au moins n éléments.

⋆) Tout système générateur algébrique de K/k ayant n éléments est une base algébrique.

Proposition 2.11. *Soient L une sous-extension d'une extension K/k, A une base algébrique de L/k et B une base algébrique de K/L, alors $A \cup B$ est une base algébrique de K/k avec $A \cap B = \emptyset$.*

Preuve. On a B est algébriquement libre sur L, donc sur $k(A) \subset L$. Comme A est algébriquement libre sur k, alors $A \cup B$ est algébriquement libre sur k et $A \cap B = \emptyset$.
Aussi on a $L/k(A)$ est algébrique, donc $L(B)/k(A)(B)$ est algébrique et comme $K/L(B)$ est algébrique, alors $K/k(A \cup B)$ est algébrique, ainsi $A \cup B$ est un générateur algébrique. D'où $A \cup B$ est une base algébrique de K/k et $A \cap B = \emptyset$. □

Corollaire 2.12. *Soit L une sous-extension d'une extension K/k, alors*

$$\text{d°tr}(K/k) = \text{d°tr}(K/L) + \text{d°tr}(L/k).$$

Proposition 2.13 (**Transitivité de la finitude du degré de transcendance**).
Soit L une sous-extension d'une extension K/k, alors

$$\text{d°tr}(K/k) \text{ est fini } \Leftrightarrow \text{d°tr}(K/L) \text{ est fini et } \text{d°tr}(L/k) \text{ est fini .}$$

2.4 Extensions algébriquement disjointes

Proposition 2.14. *Soient E et F deux sous-extension d'une extension K/k, il est équivalent de dire*

1) *Tout système algébriquement libre sur k de E est algébriquement libre sur F.*

2) *Tout système algébriquement libre sur k de F est algébriquement libre sur E.*

3) *Si A et B sont des parties respectivement de E et F algébriquement libres sur k, alors $A \cup B$ est algébriquement libre sur k et $A \cap B = \emptyset$.*

Preuve. Il suffit de montrer que (1) et (3) sont équivalentes.
Supposons qu'on a (1) et soient A et B deux parties respectivement de E et F algébriquement libre sur k, par (1) A est algébriquement libre sur F donc sur $k(B)$ ($\subset F$), comme B est algébriquement libre sur k, $A \cup B$ est algébriquement libre sur k et $A \cap B = \emptyset$.
Supposons qu'on a (3) et soit $A \subset E$ algébriquement libre sur k. Soit B une base algébrique de F sur k, par (3) $A \cup B$ est algébriquement libre sur k et $A \cap B = \emptyset$, donc A est algébriquement libre sur $k(B)$, comme $F/k(B)$ est algébrique, A est algébriquement libre sur F. □

Définition 2.8. Soient E et F deux sous-extensions d'une extension K/k. On dit que E et F sont algébriquement disjoints (sur k) si, pour toute partie A (resp. B) de E (resp. F) algébriquement libre sur k, alors $A \cap B = \emptyset$ et $A \cup B$ est algébriquement libre sur k .

Donc E et F sont algébriquement disjoints (sur k) si ils vérifient l'une des conditions équivalente de la proposition 2.14.

Proposition 2.15. *Soient E et F deux sous-extension d'une extension K/k, A une base algébrique de E/k et B une base algébrique de F/k, alors*

1) *$A \cup B$ est un générateur algébrique de EF/k.*

2) *$A \cup B$ est une base algébrique de EF/k si et seulement si E et F sont k-algébriquement disjoints ($A \cap B = \emptyset$).*

Corollaire 2.16. *Soient E et F des sous-extension d'une extension K/k, alors*

$$\mathrm{d^\circ tr}(EF/k) \leq \mathrm{d^\circ tr}(E/k) + \mathrm{d^\circ tr}(F/k).$$

De plus,

1) *si E et F sont k-algébriquement disjoints, alors* $\mathrm{d^\circ tr}(EF/k) = \mathrm{d^\circ tr}(E/k) + \mathrm{d^\circ tr}(F/k)$.

2) *si* $\mathrm{d^\circ tr}(E/k)$ *et* $\mathrm{d^\circ tr}(F/k)$ *sont finis, alors E et F sont k-algébriquement disjoints si et seulement si* $\mathrm{d^\circ tr}(EF/k) = \mathrm{d^\circ tr}(E/k) + \mathrm{d^\circ tr}(F/k)$.

Proposition 2.17. *Soient E et F des sous-extension d'une extension K/k et A une base algébrique de E/k, alors*

1) *A est un générateur algébrique de EF/F.*

2) *A est une base algébrique de EF/F si et seulement si E et F sont k-algébriquement disjoints.*

Corollaire 2.18. *Soient E et F des sous-extension d'une extension K/k, alors*

$$\mathrm{d^\circ tr}(EF/F) \leq \mathrm{d^\circ tr}(E/k).$$

De plus,

1) *si E et F sont k-algébriquement disjoints, alors* $\mathrm{d^\circ tr}(EF/F) = \mathrm{d^\circ tr}(E/k)$.

2) *si* $\mathrm{d^\circ tr}(E/k)$ *est fini, alors E et F sont k-algébriquement disjoints si et seulement si* $\mathrm{d^\circ tr}(EF/F) = \mathrm{d^\circ tr}(E/k)$.

Remarque. Les deux propositions 2.15 et 2.17 sont équivalentes.
En effet, soit L une sous-extension d'une extension K/k, A une base algébrique de L/k et B une partie de K, alors

- B est algébriquement libre sur $L \Leftrightarrow A \cup B$ est algébriquement libre sur k et $A \cap B = \emptyset$.
- B est un générateur algébrique de $K/L \Leftrightarrow A \cup B$ est un générateur algébrique de K/k.
- B est une base algébrique de $K/L \Leftrightarrow A \cup B$ est base algébrique de K/k et $A \cap B = \emptyset$.

De même si B une base algébrique de K/L et A une partie de L, alors

- A est algébriquement libre sur $k \Leftrightarrow A \cup B$ est algébriquement libre sur k et $A \cap B = \emptyset$.
- A est un générateur algébrique de $L/k \Leftrightarrow A \cup B$ est un générateur algébrique de K/k.
- A est une base algébrique de $L/k \Leftrightarrow A \cup B$ est une base algébrique de K/k et $A \cap B = \emptyset$.

Preuve. (Preuve de la proposition 2.17).
Soit A une base algébrique de E/k, donc $E/k(A)$ est algébrique, donc $EF/F(A)$ est algébrique, ainsi A est un un générateur algébrique de EF/F.
Si E et F sont algébriquement disjoints sur k, alors A est algébriquement libre sur F, ainsi A est une base algébrique de EF/F.
Inversement, soient C (resp. D) une partie de E (resp. F) algébriquement libre sur k et montrons que $C \cap D = \emptyset$ et $C \cup D$ est algébriquement libre sur k.
Complétons C on une base algébrique A' de E sur k, alors A' est une base algébrique de EF/F.
Comme $D \subset F$ est algébriquement libre sur k, alors $A' \cup D$ est algébriquement libre sur k et $A' \cap D = \emptyset$, ainsi $C \cup D$ est algébriquement libre sur k et $C \cap D = \emptyset$, par suite E et F sont algébriquement disjoints sur k. □

Proposition 2.19. *Soient E_1/F_1 et E_2/F_2 deux sous-extensions d'une extension K/k, alors*

$$\mathrm{d^\circ tr}(E_1E_2/F_1F_2) \leq \mathrm{d^\circ tr}(E_1/F_1) + \mathrm{d^\circ tr}(E_2/F_2).$$

Preuve. Analogue au cas linéaire. □

Proposition 2.20. *Soient E_1/F_1 et E_2/F_2 deux sous-extensions d'une extension K/k, alors*

$$\mathrm{d^\circ tr}(E_1/F_1) \text{ et } \mathrm{d^\circ tr}(E_2/F_2) \text{ sont finis } \Leftrightarrow \mathrm{d^\circ tr}(E_1E_2/F_1F_2) \text{ est fini.}$$

Chapitre 3

Corps finis

3.1 Groupe additif d'un corps fini

Proposition 3.1. *L'ordre de tout corps fini k est une puissance p^n, avec $n \in \mathbb{N}^*$, d'un nombre premier p et où $p = \mathrm{car}(k)$.*

Preuve. Soit P le sous-corps premier de k. Comme P est fini, alors $P \simeq \mathbb{Z}/p\mathbb{Z}$ avec $p = \mathrm{car}(k)$ (> 0). Comme P est commutatif, alors k est muni d'une structure d'espace vectoriel canonique sur P. Comme k est fini, alors sa dimension (comme P-espace vectoriel) est finie, donc soit n cette dimension, alors on a un isomorphisme d'espace vectoriel $k \simeq P^n$, ainsi $\mathrm{card}(k) = \mathrm{card}(P^n) = \mathrm{card}(P)^n = p^n$. □

Proposition 3.2. *Soit k un corps fini d'ordre p^n (p premier), alors le groupe additif de k est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$.*

Preuve. Reprenons la preuve de la proposition 3.1, l'isomorphisme $k \simeq P^n$ est en particulier un isomorphisme de groupes. Comme $P \simeq \mathbb{Z}/p\mathbb{Z}$, alors $k \simeq P^n \simeq (\mathbb{Z}/p\mathbb{Z})^n$. □

Remarque. La proposition 3.2 donne la liste des exposants $((p, p, \ldots, p))$ du groupe additif de k, donc classifie complètement ce groupe parmi les groupes abéliens finis.

3.2 Groupe multiplicatif d'un corps fini

Proposition 3.3. *Soit k un corps fini d'ordre p^n (p premier), alors l'ordre de tous sous-corps de k est de la forme p^d, où d est un diviseur de n.*

Preuve. Soit k' un sous-corps de k, alors $\mathrm{car}(k') = \mathrm{car}(k) = p$, ainsi, d'après la proposition 3.1, $\mathrm{card}(k') = p^d$. Comme k'^* est un sous-groupe du groupe multiplicatif k^*, alors

$$\mathrm{card}(k'^*) \mid \mathrm{card}(k^*) \Rightarrow p^d - 1 \mid p^n - 1.$$

Montrons que $d \mid n$, effectuons la division euclidienne de n par d, alors $n = qd + r$ avec $0 \leq r < d$, donc

$$\begin{aligned} p^n - 1 &= p^{qd+r} - 1 \\ &= (p^{qd+r} - p^r) + (p^r - 1) \\ &= p^r(p^{qd} - 1) + (p^r - 1) \\ &= p^r(p^d - 1)(p^{d(q-1)} + \ldots + p^d + 1) + (p^r - 1). \end{aligned}$$

On a $p^d - 1 \mid p^n - 1$ et $p^d - 1 \mid p^r(p^d - 1)(p^{d(q-1)} + \ldots + p^d + 1)$, donc $p^d - 1 \mid p^r - 1$, or $r < d$, donc $r = 0$, ainsi $d \mid n$. □

Théorème 3.4 (**Théorème de Wedderburn**)**.**
Tout corps fini est commutatif.

Définition 3.1. Soient $n \in \mathbb{N}^*$ et $\xi = e^{2i\pi/n} \in \mathbb{C}$. On appelle n-ème polynôme cyclotomique, le polynôme

$$\Phi_n(X) = \prod_{\substack{k \leq n \\ \text{pgcd}(k,n)=1}} (X - \xi^k) \qquad (\in \mathbb{C}[X]).$$

Proposition 3.5. *Soit $n \in \mathbb{N}^*$, alors $X^n - 1 = \prod_{d|n} \Phi_d(X)$.*

Preuve. Le polynôme $X^n - 1$ à n racines distincts dans $\mathbb{C}$ qui sont $1, \xi, \xi^2, \ldots, \xi^{n-1}$, donc

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \xi^k) = \prod_{k=0}^{n-1} (X - e^{2i\pi \frac{k}{n}}).$$

Chaque fraction $\frac{k}{n}$ s'écrit de façon unique sous forme irréductible $\frac{k'}{d}$ avec d un diviseur de n, k' premier à d et $k' < d$, donc

$$\{\frac{k}{n} \mid 0 \leq k \leq n-1\} = \bigcup_{d|n} \{\frac{k'}{d} \mid 0 \leq k' < d,\ \text{pgcd}(k', d) = 1\} \text{ (union disjointe)},$$

ainsi

$$X^n - 1 = \prod_{d|n} \prod_{\substack{k' < d \\ \text{pgcd}(k',d)=1}} (X - e^{2i\pi \frac{k'}{d}}) = \prod_{d|n} \Phi_d(X).$$

□

Corollaire 3.6. *Soit $n \in \mathbb{N}^*$, alors $\Phi_n(X) \in \mathbb{Z}[X]$.*

Preuve. Par récurrence sur n.
Pour $n = 1$, on a $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.
Supposons que pour $n \in \mathbb{N}^*$, $\Phi_n(X) \in \mathbb{Z}[X]$ et montrons que $\Phi_{n+1}(X) \in \mathbb{Z}[X]$.
Posons

$$Q = \prod_{\substack{d \mid n+1 \\ d \neq n+1}} \Phi_d(X),$$

par hypothèse de récurrence, on a $Q \in \mathbb{Z}[X]$ et comme Q est unitaire, la division euclidienne de $X^{n+1} - 1$ par Q est possible dans $\mathbb{Z}[X]$, ainsi

$X^{n+1} - 1 = Q\tilde{Q} + R$, $deg(R) < deg(Q)$, $\tilde{Q}$, $R \in \mathbb{Z}[X]$ et on a que $X^{n+1} - 1 = Q\Phi_{n+1}(X)$ dans $\mathbb{C}[X]$.

L'unicité de la division euclidienne dans $\mathbb{C}[X]$, donne que $\Phi_{n+1}(X) = \tilde{Q} \in \mathbb{Z}[X]$ (et $R = 0$).
Ainsi $\forall\ n \in \mathbb{N}^*$, $\Phi_n(X) \in \mathbb{Z}[X]$. □

Exemples.

$\Phi_1(X) = X - 1$ et $\zeta_1 = e^{i\frac{2\pi}{1}} = 1$.

$\Phi_2(X) = X + 1$ et $\zeta_2 = e^{i\frac{2\pi}{2}} = -1$.

$\Phi_3(X) = X^2 + X + 1$ et $\zeta_3 = e^{i\frac{2\pi}{3}} = j = \dfrac{-1 + i\sqrt{3}}{2}$.

$\Phi_4(X) = X^2 + 1$ et $\zeta_4 = e^{i\frac{2\pi}{4}} = i$.

$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ et $\zeta_5 = e^{i\frac{2\pi}{5}} = \dfrac{\sqrt{5} - 1}{4} + i\dfrac{\sqrt{2(5 + \sqrt{5})}}{4}$.

$\Phi_6(X) = \Phi_3(-X) = X^2 - X + 1$ et $\zeta_6 = e^{i\frac{2\pi}{6}} = \dfrac{1 + i\sqrt{3}}{2}$.

$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ et $\zeta_7 = e^{i\frac{2\pi}{7}}$.

$\Phi_8(X) = X^4 + 1$ et $\zeta_8 = e^{i\frac{2\pi}{8}} = \dfrac{\sqrt{2} + i\sqrt{2}}{2}$.

$\Phi_p(X) = \dfrac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1$ et $\zeta_p = e^{i\frac{2\pi}{p}}$ (p premier).

$\Phi_{p^m}(X) = \dfrac{X^{p^m} - 1}{X^{p^{m-1}} - 1} = X^{p^{m-1}(p-1)} + X^{p^{m-1}(p-2)} + \ldots + X^{p^{m-1}} + 1$ (p premier et $m \geq 1$).

Remarque. Soient A un anneau et P le sous-anneau premier de A, alors l'homomorphisme canonique

$$\begin{array}{rccc} h: & \mathbb{Z} & \longrightarrow & A \\ & n & \longmapsto & n \cdot 1_A \end{array}$$

induit un homomorphisme canonique

$$\begin{array}{rccc} \tilde{h}: & \mathbb{Z}[X] & \longrightarrow & P[X]. \\ & \sum\limits_i n_i X^i & \longmapsto & \sum\limits_i (n_i \cdot 1_A) X^i \end{array}$$

Définition 3.2. Soient A un anneau et P le sous-anneau premier de A, alors l'image de $\Phi_n(X)$ par l'homomorphisme canonique $\tilde{h}$ de $\mathbb{Z}[X]$ dans $P[X]$ s'appelle le n-ième polynôme cyclotomique de A.
On note toujours $\Phi_n(X)$ le n-ième polynôme cyclotomique de A et on a $X^n - 1_A = \prod\limits_{d|n} \Phi_d(X)$.

Preuve du Théorème 3.4 : Théorème de Wedderburn.
Soit k un corps fini et on suppose par l'absurde que k est non commutatif.
Le groupe multiplicatif k^* opère sur k^* par la loi

$$\begin{array}{ccc} k^* \times k^* & \longrightarrow & k^* \\ (g, x) & \longmapsto & gxg^{-1} \end{array}$$

L'équation aux classes s'écrit

$$|k^*| = |Z(k^*)| + \sum_{x \notin Z(k^*)} [k^* : \ Z(x)],$$

avec pour $x \in k^*$,

$$Z(x) = \{y \in k^* \mid xy = yx\} \text{ et } Z(k^*) = \{x \in k^* \mid xy = yx, \ \forall \ y \in k^*\} = \bigcap_{x \in k^*} Z(x).$$

Pour $x \in k^*$, posons

$$C(x) = Z(x) \cup \{0\}, \ C(k) = Z(k^*) \cup \{0\}.$$

On vérifie immédiatement que $C(x)$ et $C(k)$ sont des sous-corps de k.

On a $C(x)$ est commutatif et $C(k) \subset C(x),\ \forall\ x \in k^*$, donc $C(k)$ est commutatif.
Le corps k est muni d'une structure d'espace vectoriel canonique sur $C(k)$, si n est la dimension de cet espace et $q = \text{card}(C(k))$, alors $\text{card}(k) = q^n$ (preuve analogue à la proposition 3.1).
Pour $x \in k^*$, $C(x)$ est un sous-espace vectoriel de k sur $C(k)$, donc $\text{card}(C(x)) = q^{d_x}$ avec d_x est un diviseur de n (preuve analogue à la proposition 3.3), donc l'équation au classe s'écrit

$$q^n - 1 = q - 1 + \sum_{x \notin Z(k^*)} \frac{q^n - 1}{q^{d_x} - 1} \qquad (1).$$

Dans $\mathbb{Z}$, par une propriété classique des polynômes cyclotomiques :

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

De même

$$q^{d_x} - 1 = \prod_{d|d_x} \Phi_d(q).$$

Donc

$$\frac{q^n - 1}{q^{d_x} - 1} = \prod_{d|n,\ d\nmid d_x} \Phi_d(q).$$

Pour $d_x < n$, on voit donc en particulier que

$$\Phi_n(q) \mid \frac{q^n - 1}{q^{d_x} - 1} \qquad (2).$$

On a

$$\Phi_n(q) \mid q^n - 1 \qquad (3).$$

Soit donc $x \in k^*$ tel que $x \notin Z(k^*)$, alors $d_x < n$, ainsi, de $(1), (2)$ et (3) on trouve que

$$\Phi_n(q) \mid q - 1 \Rightarrow \Phi_n(q) \leq q - 1 \qquad (*).$$

Or

$$\Phi_n(q) = (q - \xi_1) \dots (q - \xi_l),\ (\xi_1, \dots, \xi_l \text{ sont les racines primitives } n\text{-èmes de l'unité.})$$

En particulier, $|\xi_i| = 1$ et $\xi_i \neq 1$. Et on a $|q - \xi_i| > q - 1$. Ainsi,

$$|\Phi_n(q)| > (q-1)^l \geq q - 1,$$

ce qui contredit $(*)$. Par suite $k = C(k)$ est commutatif. □

Proposition 3.7. *Soit k un corps fini, alors le groupe multiplicatif de k est cyclique.*

Preuve. Posons $\text{card}(k) = q$, alors

$$\begin{aligned} \forall\ x \in k^*,\ x^{q-1} = 1 &\Rightarrow X^{q-1} - 1\ \in k[X],\ \text{est scindé sur } k \\ &\Rightarrow\ \text{toutes les racines de } X^{q-1} - 1 \text{ sont simples dans } k. \end{aligned}$$

Comme $\Phi_{q-1}(X)$ divise $X^{q-1} - 1$, alors $\Phi_{q-1}(X)$ est scindé sur k, et comme $\Phi_{q-1}(X)$ n'est pas constant, alors elle a une racine $\xi \in k^*$. Soit d l'ordre de ξ dans k^* et montrons que $d = q - 1$. On a $d \mid q - 1 = |k^*|$. Supposons que $d < q - 1$, on a

$$\begin{aligned} 0 = \xi^d - 1 = \prod_{d'|d} \Phi_{d'}(\xi) &\Rightarrow \exists\ d' \mid d \text{ tel que } \Phi_{d'}(\xi) = 0 \text{ et } d' < q - 1 \\ &\Rightarrow \xi \text{ est une racine double de } X^{q-1} - 1 = \prod_{d|q-1} \Phi_d(X) \\ &\Rightarrow \xi \text{ est une racine de } (X^{q-1} - 1)' = (q-1)X^{q-2} \\ &\Rightarrow (q-1)\xi^{q-2} = 0 \\ &\Rightarrow \xi^{q-2} = 0\ \ (q - 1 \neq 0) \\ &\Rightarrow \xi = 0. \end{aligned}$$

Ce qui est absurde, car $\xi \in k^*$. Ainsi $d = q - 1$, ce qui donne $k^* = \langle \xi \rangle$ est cyclique. □

3.3 Classification des corps finis

Proposition 3.8. *Soit k un corps fini d'ordre p^n (p premier), alors pour chaque diviseur d de n, k admet un et un seul sous-corps d'ordre p^d.*

Preuve. Soit d un diviseur de n et posons $k_d = \{x \in k \mid x^{p^d} = x\}$. On a k_d est un sous-corps de k. Comme $X^{p^n} - X$ est scindé sur k et a tous ces racines simples et comme $X^{p^d} - X \mid X^{p^n} - X$ (car $p^d - 1 \mid p^n - 1$), alors $X^{p^d} - X$ est aussi scindé sur k et à tous ces racines simples, donc $\text{card}(k_d) = p^d$. Si k' est un sous-corps de k d'ordre p^d, alors $\forall\ x \in k',\ x^{p^d} = x$, donc $k' \subset k_d$, et comme $\text{card}(k') = \text{card}(k_d)$, alors $k' = k_d$. □

Théorème 3.9 (**Classification des corps fini, suite de la proposition 3.1**).
Soit p un nombre premier. Pour toute puissance $q = p^n$ ($n \geq 1$) de p, il existe un corps unique à isomorphisme près d'ordre q.

On note $\mathbb{F}_q$ le corps fini à q élément.

Preuve. Posons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Soient $\Phi_{q-1}(X) \in \mathbb{F}_p[X]$ et ξ tel que $\Phi_{q-1}(\xi) = 0$, ainsi on peut construire une extension $\mathbb{F}_p(\xi)/\mathbb{F}_p$.

- On vérifie que ξ est d'ordre $q-1$ (preuve analogue à la proposition 3.7), donc $\text{card}(\mathbb{F}_p(\xi)) \geq q$.
- On vérifie que $\text{card}(\mathbb{F}_p(\xi)) \leq q$. En effet, soit $x \in \mathbb{F}_p(\xi)$, donc $x = P(\xi)$ avec $P \in \mathbb{F}_p[X]$, ainsi

$$x^q = (P(\xi))^{p^n} = P(\xi^{p^n}) = P(\xi) = x.$$

Soit k' un autre corps d'ordre q, $\mathbb{P}$ le sous-corps premier de k', on a $\mathbb{P} \simeq \mathbb{Z}/p\mathbb{Z}$ (car $\text{car}(k') = p$. Soit $h : \mathbb{F}_p \longrightarrow \mathbb{P}$ un isomorphisme de corps, $f = \text{Irr}(\xi/\mathbb{F}_p)$, alors h induit un homomorphisme d'anneaux de $\mathbb{F}_p[X]$ dans $\mathbb{P}[X]$. Comme $f \mid X^{q-1} - 1$, alors $h(f) \mid h(X^{q-1} - 1) = X^{q-1} - 1$. Comme $X^{q-1} - 1$ est scindé sur k', alors $h(f)$ l'est aussi, et on a $h(f)$ est non constant, il admet une racine $\xi' \in k'$.
Soit

$$\begin{array}{rccc} \tilde{h}: & \mathbb{F}_p(\xi) & \longrightarrow & k' \\ & P(\xi) & \longmapsto & h(P)(\xi') \end{array}$$

$\tilde{h}$ est bien définie, car si

$$\begin{aligned} P_1(\xi) = P_2(\xi) &\Rightarrow (P_1 - P_2)(\xi) = 0 \\ &\Rightarrow f \mid (P_1 - P_2) \\ &\Rightarrow h(f) \mid h(P_1 - P_2) = h(P_1) - h(P_2) \\ &\Rightarrow (h(P_1) - h(P_2))(\xi') = 0 \\ &\Rightarrow h(P_1)(\xi') = h(P_2)(\xi'). \end{aligned}$$

$\tilde{h}$ est trivialement un homomorphisme de corps, donc injectif. Comme $\text{card}(\mathbb{F}_p(\xi)) = \text{card}(k')$ est fini, alors $\tilde{h}$ est bijectif, ainsi $\mathbb{F}_p(\xi) \simeq k'$. □

Chapitre 4

Clôture algébrique

4.1 k-plongements

Définition 4.1. Soient K et K' deux extensions d'un corps k. Un k-plongement σ de K dans K' est un plongement (morphisme de corps) de K dans K' fixant k, ce qui veut dire que σ est un morphisme de corps qui vérifie

$$\forall\ \lambda \in k,\ \forall\ x \in K,\ \sigma(\lambda x) = \lambda\ \sigma(x).$$

Propriétés : Soient K, K' deux extensions d'un corps k et σ un k-plongement de K dans K', alors

$\star$) $\forall\ P \in k[X_i]_{i\in I},\ \forall\ s = (s_i)_{i\in I}$ un système de K, alors $\sigma(P(s_i)_{i\in I}) = P(\sigma(s_i))_{i\in I}$.

$\star$) $\forall\ P \in k[X],\ \forall\ \alpha \in K$, alors $\sigma(P(\alpha)) = P(\sigma(\alpha))$.

$\star$) $\forall\ P \in k[X],\ \forall\ \alpha \in K$, alors $P(\alpha) = 0 \Rightarrow P(\sigma(\alpha)) = 0$.

Exemples.

1) Soit K/k une extension de corps, alors id_K est un k-plongement de K dans K.
2) Soient $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$, $K' = \mathbb{Q}(\zeta_3\sqrt[3]{2})$ avec $\zeta_3 = e^{i2\pi/3}$ et $\sigma : K \longrightarrow K',\ \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}$, alors σ est un k-plongement de K dans K'.

Proposition 4.1. *Soient K, K' et K'' des extensions d'un corps k.*

1) *Si $\sigma : K \longrightarrow K'$ et $\tau : K' \longrightarrow K''$ sont deux k-plongements, alors $\tau \circ \sigma : K \longrightarrow K''$ est un k-plongement.*
2) *Si $\sigma : K \longrightarrow K'$ est un k-plongement bijectif, alors $\sigma^{-1} : K' \longrightarrow K$ est un k-plongement.*

Définition 4.2. Soient K et K' deux extensions d'un corps k.

- Un k-isomorphisme de K dans K' est un k-plongement bijectif de K dans K'. Dans ce cas on dit que K et K' sont k-isomorphes.
- Un k-endomorphisme de K est un k-plongement de K dans K.
- Un k-automorphisme de K est un k-endomorphisme bijectif de K.

Remarque. La proposition 4.1 montre que :

- la relation "être k-isomorphe" est une relation d'équivalence sur la classe des extensions de k.
- l'ensemble des k-automorphismes de K est un sous-groupe du groupe des bijections de K.

Proposition 4.2. *Soient K et K' deux extensions algébriques d'un corps k. S'il existe un k-plongement $\sigma : K \longrightarrow K'$ et un k-plongement $\tau : K' \longrightarrow K$, alors K et K' sont k-isomorphes et σ et τ sont des k-isomorphismes.*

Preuve. Soit $h = \tau \circ \sigma : K \longrightarrow K$ et soient $\alpha \in K$, $Q = \mathrm{Irr}(\alpha/k)$ et $E = \{\alpha, h^2(\alpha), h^3(\alpha), \ldots\}$. On a E est fini car ses éléments sont des racines de Q, E est stable par h, h/E est injectif (car h l'est), donc h/E est injectif sur un ensemble fini E, ainsi h/E est bijectif, par suite $\exists\ \alpha' \in E$ tel que $\alpha = h(\alpha') = \tau \circ \sigma(\alpha')$, donc τ est surjectif et puisque τ est injectif on trouve que τ est bijectif. Ainsi τ est un k-isomorphisme et K et K' sont k-isomorphes. □

Corollaire 4.3. *Soit L une sous-extension d'une extension algébrique K/k. S'il existe un k-plongement $\sigma : K \longrightarrow L$, alors $K = L$ et σ est un k-automorphisme de K.*

Preuve. On applique la proposition 4.2 avec $\sigma : K \longrightarrow L$ et $i : L \longrightarrow K$ l'injection canonique. □

4.2 Corps algébriquement clos

Définition 4.3. Un polynôme est dit scindé sur un corps commutatif K s'il est décomposable en facteurs de premier degré sur K.

Exemples.

1) Le polynôme $X^2 + 1$ est scindé sur $\mathbb{C}$ car $X^2 + 1 = (X - i)(X + i)$ sur $\mathbb{C}$.

2) Le polynôme $X^2 + 1$ n'est pas scindé sur $\mathbb{Q}$.

3) Pour p premier, le polynôme $X^p + 1$ est scindé sur $\mathbb{F}_p$ car $X^p + 1 = (X + 1)^p$ sur $\mathbb{F}_p$.

Définition 4.4. Un corps commutatif C est dit algébriquement clos si tout polynôme non constant de $C[X]$ a une racine dans C.

Proposition 4.4. *Soit C un corps commutatif, alors les conditions suivantes sont équivalentes.*

1) *Toute extension algébrique C'/C vérifie $C' = C$.*

2) *$\forall\ P \in C[X]$ non constant, P a une racine dans C.*

3) *$\forall\ P \in C[X]$ non constant, P est scindé sur C.*

Preuve.
1) $\Rightarrow$ 2) Supposons qu'on a (1) et soit $P \in C[X]$ non constant, alors il existe α tel que $P(\alpha) = 0$. Posons $C' = C(\alpha)$, alors C'/C est une extension algébrique, ainsi, par (1), $C' = C$, par suite $\alpha \in C$ et P a une racine dans C.
2) $\Rightarrow$ 3) Supposons qu'on a (2) et soit $P \in C[X]$ non constant, montrons par récurrence sur $n = \deg(P)$ que P est scindé sur C.
Pour $n = 1$, c'est évident que P est scindé (car C est un corps), supposons que la propriété est vraie pour $n \geq 1$, et montrons qu'elle est vraie pour $n+1$. Soit $P \in C[X]$ tel que $\deg(P) = n+1$, par (2), P a une racine $\alpha \in C$, donc $P = (X - \alpha)P_1,\ P_1 \in C[X]$ et $\deg(P_1) < \deg(P)$, donc P_1 est scindé sur C, par suite P est scindé sur C.
3) $\Rightarrow$ 1) Supposons qu'on a (2) et soit C' une extension algébrique de C et montrons que $C' = C$. Soit $\alpha \in C'$ et $Q = \mathrm{Irr}(\alpha/C)$, alors Q est scindé sur C, donc $\alpha \in C$, par suite $C' = C$. □

Remarque. Un corps commutatif C est dit algébriquement clos s'il vérifie l'une des conditions équivalentes de la proposition 4.4.

Exemples.

1) Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.

2) Un corps fini k n'est jamais algébriquement clos ($\prod_{\alpha \in k} (X - \alpha) + 1$ n'a pas de racine dans k).

Théorème 4.5 (**Théorème de prolongement**).
Soit $\sigma : k \longrightarrow C$ un plongement de corps commutatif, avec C algébriquement clos. Soit K/k une extension algébrique, alors il existe $\hat{\sigma} : K \longrightarrow C$ un plongement prolongeant σ.

Preuve. Soit $\mathcal{E} = \{(L, \sigma_L) \mid L$ une sous-extension de K/k et σ_L un plongement prolongeant $\sigma\}$. On a $\mathcal{E} \neq \emptyset$, car $(k, \sigma) \in \mathcal{E}$.
$\mathcal{E}$ est inductif pour la relation d'ordre : $(L, \sigma_L) \leq (L', \sigma_{L'}) \Leftrightarrow L \subseteq L'$ et $\sigma_{L'}/L = \sigma_L$.
Soit $(\hat{L}, \hat{\sigma})$ un élément maximal de $\mathcal{E}$, on a $\hat{L} = K$, sinon, soit $\alpha \in K \setminus \hat{L}$ et $Q = \mathrm{Irr}(\alpha/\hat{L})$, $\hat{\sigma}$ induit un homomorphisme

$$\begin{array}{rccc} \hat{\sigma}: & \hat{L}[X] & \longrightarrow & C[X] \\ & \sum\limits_i a_i X^i & \longmapsto & \sum\limits_i \hat{\sigma}(a_i) X^i \end{array}$$

C est algébriquement clos, donc $\hat{\sigma}(Q)$ a une racine $\alpha' \in C$, soit donc

$$\begin{array}{rccc} \hat{\sigma}_1: & \hat{L}(\alpha) & \longrightarrow & C. \\ & P(\alpha) & \longmapsto & \hat{\sigma}(P)(\alpha') \end{array}$$

On a $\hat{\sigma}_1$ est bien définie, car

$$P_1(\alpha) = P_2(\alpha) \Rightarrow Q \mid P_1 - P_2 \Rightarrow \hat{\sigma}(Q) \mid \hat{\sigma}(P_1) - \hat{\sigma}(P_2) \Rightarrow \hat{\sigma}(P_1)(\alpha') = \hat{\sigma}(P_2)(\alpha').$$

$\hat{\sigma}_1$ est un plongement de corps prolongeant $\hat{\sigma}$, donc σ, ainsi $(\hat{L}(\alpha), \hat{\sigma}_1) \in \mathcal{E}$ et $(\hat{L}, \hat{\sigma}) < (\hat{L}(\alpha), \hat{\sigma}_1)$, ce qui contredit $(\hat{L}, \hat{\sigma})$ est maximal. Par suite $\hat{L} = K$. □

4.3 Clôture algébrique

Définition 4.5. Soit k un corps commutatif. Une extension Ω de k est appelé clôture algébrique de k si :

1) Ω/k est algébrique ;

2) Ω est algébriquement clos.

Remarque. Si K/k est algébrique, alors toute clôture algébrique de K est une clôture algébrique de k.

Proposition 4.6. *Soit k un corps commutatif et Ω une extension de k, alors Ω est une clôture algébrique de k si et seulement si*

1) *Ω/k est algébrique ;*

2) *Toute extension algébrique de k se k-plonge dans Ω.*

Preuve. Supposons que Ω vérifie (1) et (2) et soit Ω' une extension algébrique de Ω. On a Ω'/Ω et Ω/k sont algébriques, donc Ω'/k est algébrique, ainsi, d'après (2), Ω' se k-plonge dans Ω, par suite, d'après le corollaire 4.3, $\Omega' = \Omega$.
Inversement, supposons que Ω est une clôture algébrique de k, alors on a (1) par définition. Soit K une extension algébrique de k, alors, d'après le Théorème de prolongement, l'injection canonique $i : k \longrightarrow \Omega$, se prolonge en un k-plongement $\sigma : K \longrightarrow \Omega$, ce qui vérifie (2). □

Théorème 4.7 (**Théorème de Steinitz**).
Tout corps commutatif k admet une clôture algébrique et deux clôtures algébriques de k sont k-isomorphe.

Chapitre 5

Extensions séparables

5.1 Éléments k-conjugués

Définition 5.1. Soient L et L' des sous-extensions algébriques d'une extension K/k. On dit que L et L' sont k-conjugués s'il existe un k-isomorphisme $\sigma : L \longrightarrow L'$.

Remarque. La relation "être k-conjugué" est une relation d'équivalence sur l'ensemble des sous-extensions algébriques de K/k.

Proposition 5.1. *Soient L et L' des sous-extensions d'une extension algébrique K/k et Ω une clôture algébrique de K, alors les deux propriétés suivantes sont équivalentes.*

1) *L et L' sont k-conjugués.*

2) *Il existe un k-automorphisme σ de Ω tel que $\sigma(L) = L'$.*

Preuve. Supposons qu'on a (1). Soit $\sigma : L \longrightarrow L'$ un k-isomorphisme et $\sigma_1 : L \longrightarrow \Omega$ qui associe x par $\sigma(x)$. Comme Ω/L est algébrique et Ω est algébriquement clos, alors, par le théorème de prolongement, il existe $\hat{\sigma_1} : \Omega \longrightarrow \Omega$ un k-plongement prolongeant σ_1. Comme Ω/k est algébrique, alors, d'après le corollaire 4.3 du chapitre 3, $\hat{\sigma_1}$ est un k-automorphisme de Ω et on a $\hat{\sigma_1}(L) = \sigma_1(L) = \sigma(L) = L'$.
Pour l'autre implication c'est immédiate. □

Définition 5.2. Soient K/k une extension, α et β deux éléments de K algébriques sur k. On dit que α et β sont k-conjugués s'il existe un k-isomorphisme σ de $k(\alpha)$ dans $k(\beta)$ vérifiant $\sigma(\alpha) = \beta$.

Remarque. La relation "être k-conjugués" est une relation d'équivalence sur la clôture algébrique de k dans K.

Proposition 5.2. *Soit K/k une extension algébrique, α, β deux éléments de K et Ω une clôture algébrique de K, il est équivalent de dire*

1) *α et β sont k-conjugués.*

2) *Il existe un k-automorphisme σ de Ω tel que $\sigma(\alpha) = \beta$.*

3) $\forall\ P \in k[X],\ P(\alpha) = 0 \Rightarrow P(\beta) = 0$.

4) *β est racine de* $\mathrm{Irr}(\alpha/k)$.

5) $\mathrm{Irr}(\alpha/k) = \mathrm{Irr}(\beta/k)$.

Preuve.
1) $\Rightarrow$ 2) On utilise la même méthode comme dans la proposition 5.1.
2) $\Rightarrow$ 3) Supposons qu'on a (2) et soit σ un k-automorphisme de Ω tel que $\sigma(\alpha) = \beta$, soit $P \in k[X]$ tel que $P(\alpha) = 0$, alors

$$P(\alpha) = 0 \Rightarrow \sigma(P(\alpha)) = 0 \Rightarrow P(\sigma(\alpha)) = 0 \Rightarrow P(\beta) = 0.$$

3) ⇒ 4) On a $\mathrm{Irr}(\alpha/k) \in k[X]$ et $\mathrm{Irr}(\alpha/k)(\alpha) = 0$, donc $\mathrm{Irr}(\alpha/k)(\beta) = 0$, ainsi β est racine de $\mathrm{Irr}(\alpha/k)$.
4) ⇒ 5) Supposons qu'on a (4), alors $\mathrm{Irr}(\beta/k) \mid \mathrm{Irr}(\alpha/k)$, donc $\mathrm{Irr}(\alpha/k) \sim \mathrm{Irr}(\beta/k)$, et comme $\mathrm{Irr}(\alpha/k)$ et $\mathrm{Irr}(\beta/k)$sont unitaires, alors $\mathrm{Irr}(\alpha/k) = \mathrm{Irr}(\beta/k)$.
5) ⇒ 1) Supposons qu'on a (5) et soit

$$\begin{array}{rccc} \sigma: & k(\alpha) & \longrightarrow & k(\beta). \\ & P(\alpha) & \longmapsto & P(\beta) \end{array}$$

On a σ est bien définie, en effet,

$$\begin{aligned} P_1(\alpha) = P_2(\alpha) \Rightarrow (P_1 - P_2)(\alpha) = 0 &\Rightarrow \mathrm{Irr}(\alpha/k) \mid P_1 - P_2 \Rightarrow \mathrm{Irr}(\beta/k) \mid P_1 - P_2 \\ &\Rightarrow (P_1 - P_2)(\beta) = P_1(\beta) - P_2(\beta) = 0 \\ &\Rightarrow P_1(\beta) = P_2(\beta). \end{aligned}$$

σ est un k-isomorphisme de $k(\alpha)$ dans $k(\beta)$ vérifiant $\sigma(\alpha) = \beta$, d'où (1). □

Exemple. $\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}$ sont les racines de $X^3 - 2 = \mathrm{Irr}(\sqrt[3]{2}/\mathbb{Q})$, donc ils sont $\mathbb{Q}$-conjugués dans $\mathbb{C}$ et on a

$$\forall\ P \in \mathbb{Q}[X],\ P(\sqrt[3]{2}) = 0 \Leftrightarrow P(\zeta_3\sqrt[3]{2}) = 0 \Leftrightarrow P(\zeta_3^2\sqrt[3]{2}) = 0.$$

5.2 Degré de séparabilité

Définition 5.3. Soit K/k une extension algébrique et Ω une clôture algébrique de k. Le cardinal de l'ensemble de k-plongement de K dans Ω s'appelle le degré de séparabilité de K/k et on le note par $[K : k]_s$.

Remarque. Soit K/k une extension algébrique et Ω une clôture algébrique de k, alors $[K : k]_s \geq 1$.

Remarque. Soit K/k une extension algébrique et Ω une clôture algébrique de K (Ω est aussi une clôture algébrique de k).
Supposons que $[K : k]_s = 1$, alors le seul k-plongement de K dans Ω est l'injection canonique. Si K' est une extension de K et σ est un k-plongement de K' dans Ω, alors σ/K est un k-plongement de K dans Ω, par suite $\sigma/K = i$, ainsi σ est un K-plongement c'est-à-dire que $[K' : k]_s = [K' : K]_s$, "K et k sont inséparables".

Proposition 5.3. *Soit L une sous-extension d'une extension algébrique K/k, alors*

$$[K : k]_s = [K : L]_s \cdot [L : k]_s.$$

Preuve. Soient Ω une clôture de K (donc de k et de L) et

$$\begin{aligned} \mathcal{E}_1 &= \{k\text{-plongement de } L \text{ dans } \Omega\}, \\ \mathcal{E}_2 &= \{L\text{-plongement de } K \text{ dans } \Omega\}, \\ \mathcal{E} &= \{k\text{-plongement de } K \text{ dans } \Omega\}. \end{aligned}$$

Pour $\sigma \in \mathcal{E}_1$, on note $\hat{\sigma}$ un k-automorphisme de Ω prolongeant σ et soit

$$\begin{array}{rccc} \phi: & \mathcal{E}_1 \times \mathcal{E}_2 & \longrightarrow & \mathcal{E} \\ & (\sigma,\ \tau) & \longmapsto & \hat{\sigma} \circ \tau \end{array}$$

$\star$) ϕ est bien définie.

$\star$) ϕ est injective car

$$\begin{aligned}\phi(\sigma_1,\tau_1)=\phi(\sigma_2,\tau_2) &\Rightarrow \hat{\sigma}_1\circ\tau_1=\hat{\sigma}_2\circ\tau_2\\ &\Rightarrow \forall\ \alpha\in L, \hat{\sigma}_1\circ\tau_1(\alpha)=\hat{\sigma}_2\circ\tau_2(\alpha)\\ &\Rightarrow \forall\ \alpha\in L, \hat{\sigma}_1(\tau_1(\alpha))=\hat{\sigma}_2(\tau_2(\alpha)),\end{aligned}$$

donc $\hat{\sigma}_1(\alpha)=\hat{\sigma}_2(\alpha)$ (car $\tau_i(\alpha)=\alpha, \forall\alpha\in L$), donc $\sigma_1(\alpha)=\sigma_2(\alpha)$, donc $\sigma_1=\sigma_2$, ainsi $\hat{\sigma}_1=\hat{\sigma}_2$, donc

$$\forall\ \alpha\in K,\ \hat{\sigma}_1(\tau_1(\alpha))=\hat{\sigma}_2(\tau_2(\alpha))=\hat{\sigma}_1(\tau_2(\alpha)),$$

et on a que $\hat{\sigma}_1$ est injectif, donc $\tau_1(\alpha)=\tau_2(\alpha), \forall\ \alpha\in K$, ainsi $\tau_1=\tau_2$. Par suite ϕ est injectif.

$\star$) ϕ est surjectif. En effet, soit $\sigma\in\mathcal{E},\ \sigma_1=\sigma/L$ et $\tau=\hat{\sigma}_1^{-1}\circ\sigma$, alors

$$\forall\alpha\in L,\ \tau(\alpha)=\hat{\sigma}_1^{-1}(\sigma(\alpha))=\hat{\sigma}_1^{-1}(\sigma_1(\alpha))=\hat{\sigma}_1^{-1}(\hat{\sigma}_1(\alpha))=\alpha,$$

donc $\tau\in\mathcal{E}_2$ et on a $\sigma=\hat{\sigma}_1\circ\tau=\phi(\sigma_1,\ \tau)$.

Ainsi ϕ est une bijection, ce qui donne que

$$\text{card}(\mathcal{E})=\text{card}(\mathcal{E}_1)\times\text{card}(\mathcal{E}_2)\Leftrightarrow[K:k]_s=[K:L]_s\times[L:k]_s.$$

□

Définition 5.4. Soient K/k une extension et α un élément de K, algébrique sur k. On appelle degré de séparabilité de α sur k, celui de $k(\alpha)/k$ qu'on le note par $d_s^\circ(\alpha/k)=[k(\alpha):k]_s$.

Proposition 5.4. *Soient K/k une extension, α un élément de K, algébrique sur k, $Q=\text{Irr}(\alpha/k)$ et Ω une clôture algébrique de k, alors le degré de séparabilité de α sur k, $d_s^\circ(\alpha/k)$ est le nombre de racines de Q dans Ω, en particulier on a $d_s^\circ(\alpha/k)\leq d^\circ(\alpha/k)$.*

Preuve. Un k-plongement σ de $k(\alpha)$ dans Ω est déterminé par la donnée de $\sigma(\alpha)$ qui est racine de Q dans Ω, en particulier $d_s^\circ(\alpha/k)$ est le nombre de racines de Q dans Ω qui est inférieur ou égal au $\deg(Q)$. □

5.3 Éléments séparables

Définition 5.5. Soient K/k une extension, α un élément de K, algébrique sur k. On dit que α est séparable sur k si $d_s^\circ(\alpha/k)=d^\circ(\alpha/k)$ (maximum), dans le cas contraire α est dit non séparable sur k.

Remarque. Supposons que $d_s^\circ(\alpha/k)=1$ (minimum) et K/k est algébrique, soit Ω la clôture algébrique de $k(\alpha)$, donc tout k-plongement $\sigma: K\longrightarrow\Omega$ vérifie $\sigma(\alpha)=\alpha$, "α est inséparable sur k".

Proposition 5.5 (**Caractérisation des éléments séparables**).
Soient K/k une extension, α un élément de K, algébrique sur k, $Q=\text{Irr}(\alpha/k)$ et Ω une clôture algébrique de k. Il est équivalent de dire :

1) *α est non séparable sur k.*
2) *Q a des racines multiples dans Ω.*
3) *$Q'=0$.*
4) *$Q\in k[X^p]$ avec $p=\text{car}(k)$ $(p>0)$.*

Preuve.
1) $\Rightarrow$ 2) Supposons qu'on a (1), alors $d_s^\circ(\alpha/k)=$ nombre de racines de Q dans $\Omega<\deg(Q)$. Comme Q est scindé sur Ω, alors on (2).

2) ⇒ 3) Si on a (2), soit $\alpha \in \Omega$ une racine multiple de Q, alors $Q = \mathrm{Irr}(\alpha/k) = (X-\alpha)^n P(X)$ avec $n \geq 2$ et $P \in \Omega[X]$, donc $Q'(\alpha) = 0$, or $Q(\alpha) = 0$, donc $Q = \mathrm{Irr}(\alpha/k) \mid Q'$ et comme $\deg(Q') < \deg(Q)$, alors $Q' = 0$.
3) ⇒ 4) Si on a (3), écrivons $Q = \sum_i a_i X^i$, donc $Q' = \sum_{i\geq 1} i a_i X^{i-1} = 0$, ainsi $ia_i = 0,\ \forall\ i \geq 1$, donc $a_i = 0$ ou $p \mid i$ (avec $p = \mathrm{car}(k)$), par suite on a (4).
4) ⇒ 1) Si on a (4), écrivons $Q = Q_1(X^p)$, dans $\Omega[X]$ on a $Q_1 = (X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_s)$, soit $\beta_i^p = \alpha_i$, on a donc

$$Q(X) = Q_1(X^p) = (X^p-\beta_1^p)(X^p-\beta_2^p)\dots(X^p-\beta_s^p) = ((X-\beta_1)(X-\beta_2)\dots(X-\beta_s))^p\,,$$

donc $d_s^\circ(\alpha/k) \leq s = \frac{\deg(Q)}{p} < \deg(Q)$ $(p > 1)$. □

Remarque. Soient L une sous-extension d'une extension K/k, α un élément de K, algébrique sur k. Si α est séparable sur k, alors α est séparable sur L.

En effet, si α est séparable sur k, alors $\mathrm{Irr}(\alpha/k)$ n'a pas de racine multiple dans Ω et comme $\mathrm{Irr}(\alpha/L)$ divise $\mathrm{Irr}(\alpha/k)$, alors $\mathrm{Irr}(\alpha/L)$ n'a pas de racine multiple dans Ω, ainsi α est séparable sur L.

Définition 5.6. Soit k un corps commutatif et P un polynôme de $k[X]$. On dit que P est séparable si toutes ses racines sont simples dans une clôture algébrique de k. Dans le cas contraire on dit que P est non séparable.

Proposition 5.6. *Soient K/k une extension et α un élément de K. α est séparable sur k si et seulement si il existe $P \in k[X]$ séparable tel que $P(\alpha) = 0$.*

Preuve. Soient K/k une extension, α un élément de K et Ω une clôture algébrique de K.
Si α est séparable sur k, alors toutes les racines de $\mathrm{Irr}(\alpha/k)$ sont simples dans Ω, donc $\mathrm{Irr}(\alpha/k) \in k[X]$ est séparable et $\mathrm{Irr}(\alpha/k)(\alpha) = 0$.
Inversement supposons qu'il existe $P \in k[X]$ séparable tel que $P(\alpha) = 0$, alors $\mathrm{Irr}(\alpha/k)$ est séparable, par suite α est séparable sur k. □

5.4 Extensions séparables

Définition 5.7. Une extension K/k est dite séparable, si tout élément de K est séparable sur k. Dans le cas contraire K/k est dite non séparable.

Remarque. Soient L une sous-extension d'une extension K/k. Si K/k est séparable, alors K/L est séparable (de même pour L/k).

Proposition 5.7. *Toute sous-extension d'une extension séparable est séparable.*

Preuve. Soit L/L' une sous-extension de K/k, alors K/k séparable ⇒ L/k séparable ⇒ L/L' séparable. □

Proposition 5.8. *Soit K/k une extension finie, alors $[K:k]_s \leq [K:k]$, avec l'égalité si et seulement si K/k est séparable.*

Preuve. Récurrence sur $n = [K:k]$. Pour $n = 1$, on a $[K:k]_s \leq [K:k]$ ($[K:k]_s = [K:k]$).
Supposons que la propriété est vraie pour $[K:k] = n \geq 1$ et soit $\alpha \in K \setminus k$. On a

$$\begin{cases} [k(\alpha):k]_s \leq [k(\alpha):k] \quad \text{(Proposition 5.4)} \quad (1). \\ [K:k(\alpha)]_s \leq [K:k(\alpha)] \quad \text{(H. R.)} \quad (2). \end{cases}$$

De (1) et (2), on trouve que

$$[K:k]_s = [K:k(\alpha)]_s \cdot [k(\alpha):k]_s \leq [K:k(\alpha)] \cdot [k(\alpha):k] = [K:k] \quad (3).$$

Si K/k est séparable, alors (1) est une égalité par définition de l'élément séparable et (2) est une égalité par l'hypothèse de récurrence (car si K/k est séparable finie, alors $K/k(\alpha)$ l'est aussi), donc (3) est une égalité.
Inversement, si (3) est une égalité, alors (1) et (2) sont des égalités, donc x est séparable sur k. Ceci $\forall\ \alpha \in K \setminus k$, donc K/k est séparable. □

Remarque. Si α est séparable sur k, on a $[k(\alpha) : k]_s = [k(\alpha) : k]$, donc $k(\alpha)/k$ est séparable.

Théorème 5.9. *Soit K/k une extension séparable finie, alors il existe un élément θ de K tel que $K = k(\theta)$.*

Lemme 5.10. *Soient A un espace vectoriel sur k, $V, A_1, \ldots, A_n$ des sous-espaces de A.*
Si $\mathrm{card}(k) \geq n$, *et si V n'est contenu dans aucun des A_i, alors V n'est pas contenu dans* $\bigcup_{i=1}^{n} A_i$.

Preuve. Raisonnant par récurrence sur n. Si $n = 1$, alors si $V \not\subset A_1$, alors $V \not\subset A_1$. Supposons que la propriété est vraie à l'ordre $n-1$ et soient $V, A_1, \ldots, A_n$ des sous-espaces de A tel que $\mathrm{card}(k) \geq n$, et supposons que V n'est contenu dans aucun des $A_i, \forall i \in \{1, \ldots, n\}$, alors $V \not\subset A_n$ et supposons que $V \subset \bigcup_{i=1}^{n} A_i$ et montrons que $V \subset \bigcup_{i=1}^{n-1} A_i$.

Soit $x \in V$ tel que $x \notin A_n$, et soit y quelconque dans V. Si y appartient à kx, alors $y \in \bigcup_{i=1}^{n-1} A_i$. Sinon, les éléments x et $y + \lambda x, \lambda \in k$, sont en nombre strictement supérieur à n (car $\mathrm{card}(k) \geq n$) et appartiennent à $\bigcup_{i=1}^{n} A_i$; deux d'entre eux appartiennent donc au même A_i. Il existe donc $i, 1 \leq i \leq n$, avec, soit $x \in A_i$ et $y + \lambda x \in A_i$ pour un $\lambda \in k$, soit $y + \lambda x \in A_i$ et $y + \mu x \in A_i$ pour deux scalaires distincts $\lambda, \mu \in k$. Dans les deux cas, on en conclut que $x \in A_i$ et $y \in A_i$: mais cela implique $i \neq n$, donc $y \in \bigcup_{i=1}^{n-1} A_i$, ainsi $V \subset \bigcup_{i=1}^{n-1} A_i$, ce qui n'est pas le cas d'après l'hypothèse de récurrence, ce qui achève la démonstration. □

Remarque. Dans le lemme 5.10, l'hypothèse de $\mathrm{card}(k) \geq n$ est indispensable.

Contre exemple. Soient $k = \mathbb{F}_2$, $E = k^2 = \{0, a, b, c\}$, $F_1 = ka = \{0, a\}$, $F_2 = kb = \{0, b\}$, $F_3 = kc = \{0, c\}$, on a $E \not\subset F_1$, $E \not\subset F_2$ et $E \not\subset F_3$, mais $E \subset F_1 \cup F_2 \cup F_3 = E$.

Preuve. (Preuve du théorème 5.9).

- Si k est fini, alors K est fini, donc K^* est cyclique, ainsi $K = k(\theta)$ où θ est un générateur de K^*.
- Si k est fini. Soit Ω une clôture algébrique de K, $i : k \longrightarrow \Omega$ l'injection canonique, alors pour chaque $\sigma : K \longrightarrow \Omega$ un k-plongement on note

$$K_\sigma = \{x \in K \mid \sigma(x) = x\}.$$

  Les K_σ $(\sigma \neq i)$ et K sont des sous-espaces vectoriels de K/k, et K n'est contenu dans aucun des K_σ, alors, par le lemme 5.10, K n'est pas contenu dans $\bigcup_{\sigma \neq i} K_\sigma$ c'est-à-dire que $\bigcup_{\sigma \neq i} K_\sigma \subsetneq K$. Soit donc $\theta \in K \setminus \bigcup_{\sigma \neq i} K_\sigma$, alors $k(\theta) = K$, car sinon on aura $[K : k(\theta)] > 1$ et comme $K/k(\theta)$ est séparable, alors $[K : k(\theta)]_s > 1$, donc il existe $\tau \neq i$ un $k(\theta)$-plongement, et comme $K/k(\theta)$ est algébrique, alors τ se prolonge en un k-plongement $\sigma \neq i$ de K dans Ω, et comme $\sigma(\theta) = \tau(\theta) = \theta$, alors $\theta \in K_\sigma$, or $\theta \in K \setminus \bigcup_{\sigma \neq i} K_\sigma$, ce qui est impossible, par suite $K = k(\theta)$.

□

Proposition 5.11 (**Transitivité de la séparabilité**).
Soit L une sous-extension d'une extension K/k, alors K/k est séparable si et seulement si K/L et L/k sont séparables.

Preuve. On sait que si K/k est séparable, alors K/L et L/k sont séparables.
Inversement, supposons que K/L et L/k sont séparables et soit $\alpha \in K$, alors α est séparable sur L. Soit donc

$$\mathrm{Irr}(\alpha/L) = a_0 + \ldots + a_d X^d,\ L' = k(a_0, \ldots, a_d),\ K' = L'(\alpha).$$

On a L/k est séparable et $L' \subset L$, donc L'/k est séparable et on a L'/k est finie. Aussi on a $\mathrm{Irr}(\alpha/L') = \mathrm{Irr}(\alpha/L)$, $d_s^\circ(\alpha/L') = d_s^\circ(\alpha/L)$, ainsi α est séparable sur L', donc K'/L' est finie et séparable, ainsi

$$[K' : k]_s = [K' : L']_s \cdot [L' : k]_s = [K' : L'] \cdot [L' : k] = [K' : k],$$

comme K'/k est finie, alors, par la proposition 5.8, K'/k est séparable, donc α est séparable sur k, par suite K/k est séparable. □

Proposition 5.12. *Soit K/k une extension, alors l'ensemble des éléments de K séparables sur k est un corps intermédiaire à k et K.*

Preuve. Soient α et β deux éléments de K séparables sur k, donc $k(\alpha)/k$ est séparable et $k(\alpha)(\beta)/k(\alpha)$ est séparable (car β est séparable sur k, donc sur $k(\alpha)$), ainsi par transitivité on aura $k(\alpha, \beta)/k$ est séparable, donc $\alpha + \beta$, $\alpha - \beta$ et α/β (si $\beta \neq 0$) sont séparables sur k, ce qui donne que l'ensemble des éléments de K séparables sur k est un corps (intermédiaire à k et K). □

Définition 5.8. Soit K/k une extension. L'ensemble des éléments de K séparables sur k s'appelle la clôture séparable de k dans K.

Il résulte immédiatement de cette définition que la clôture séparable S de k dans K est caractérisé par l'une des trois caractérisations suivantes.

- Soit L une sous-extension de K/k, alors L/k est séparable si et seulement si $L \subset S$.
- (a) S/k est séparable ;
  (b) $\forall\ \alpha \in K \setminus S$, α est non séparable sur k.
- (a) S/k est séparable ;
  (b) $\forall\ \alpha \in K \setminus S$, α est non séparable sur S.

Proposition 5.13. *Soient E_1/F_1 et E_2/F_2 des sous-extensions de K/k. Si E_1/F_1 et E_2/F_2 sont séparables, alors E_1E_2/F_1F_2 est séparable.*

Preuve. La clôture séparable de F_1F_2 dans K contient E_1 et E_2, donc elle contient E_1E_2. □

Cas particuliers :

- Soient E et F des sous-extensions de K/k. Si E/k et F/k sont séparables, alors EF/k est séparable.
- Soient E/F une sous-extension de K/k. Si E/F est séparable, alors EL/FL est séparable pour toute sous-extension L de K/k.
- Soient E/F une sous-extension de K/k et A une partie de K. Si E/F est séparable, alors $E(A)/F(A)$ est séparable.

5.5 Clôture séparable

Définition 5.9. On dit qu'un corps commutatif C est séparablement clos si toute extension algébrique séparable de C est triviale (toute extension séparable algébrique C'/C vérifie $C' = C$).

Remarques.

1) Un corps algébriquement clos est séparablement clos.

2) Si un corps parfait C est séparablement clos, il est algébriquement clos, car toute extension algébrique de C est séparable.

Proposition 5.14. *Soit C un corps commutatif, alors il est équivalent de dire*

1) *C est un corps séparablement clos.*

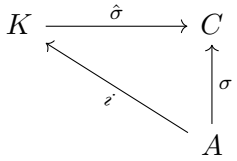
2) *Tout polynôme $P \in C[X]$ séparable non constant a une racine dans C.*

3) *Tout polynôme $P \in C[X]$ séparable est scindé sur C.*

Preuve. Analogue au cas algébrique. □

Remarque. Un corps commutatif est dit séparablement clos si il vérifie les conditions équivalentes de la proposition 5.14.

Théorème 5.15 (**Théorème de prolongement séparable**).
Soient k et C deux corps commutatifs avec C étant séparablement clos, $\sigma : k \longrightarrow C$ un plongement de corps, et soit K une extension séparable de k, alors il existe un plongement $\hat{\sigma} : K \longrightarrow C$ prolongeant σ.
Autrement dit on a un diagramme commutatif :



Preuve. Analogue au cas algébrique. □

Définition 5.10. Soit k un corps commutatif et Ω une extension de k. Si Ω/k est séparable et Ω est séparablement clos, alors Ω est appelée clôture séparable de k.

Proposition 5.16. *Soient k un corps commutatif et Ω une extension de k. Ω est une clôture séparable de k si et seulement si*

1) *Ω/k est séparable.*

2) *Toute extension séparable de k se k-plonge dans Ω.*

Preuve. Analogue au cas algébrique. □

Remarque. Soient k un corps commutatif et Ω une extension de k, alors Ω est une clôture séparable de k si Ω vérifie la propriété suivante :

$$\text{pour toute extension } K/k,\ K/k \text{ est séparable } \Leftrightarrow K \text{ se } k\text{- plonge dans } \Omega.$$

Théorème 5.17 (**Théorème de Steinitz séparable**).
Tout corps commutatif k admet une clôture séparable, et deux clôtures séparables de k sont k-isomorphes.

5.6 Corps inséparablement disjoints

Définition 5.11. Soient E, F deux sous-extensions algébriques d'une extension K/k et Ω une clôture algébrique de k. On dit que E et F sont k-inséparablement disjoints si pour tous k-plongements $\sigma_1 : E \longrightarrow \Omega$ et $\sigma_2 : F \longrightarrow \Omega$, il existe un k-plongement $\sigma : EF \longrightarrow \Omega$ prolongeant σ_1 et σ_2.

Proposition 5.18. *Soient E, F des sous-extensions algébriques d'une extension K/k et Ω (resp. Ω_1, Ω_2) une clôture algébrique de k (resp. E, F), alors les conditions suivantes sont équivalentes.*

1) *Tout k-plongement $\sigma : E \longrightarrow \Omega_2$ se prolonge en un F-plongement $\hat{\sigma} : EF \longrightarrow \Omega_2$.*

2) *Tout k-plongement $\sigma : F \longrightarrow \Omega_1$ se prolonge en un E-plongement $\hat{\sigma} : EF \longrightarrow \Omega_1$.*

3) *Si $\sigma_1 : E \longrightarrow \Omega$ et $\sigma_2 : F \longrightarrow \Omega$ sont des k-plongements, alors il existe $\sigma : EF \longrightarrow \Omega$ un k-plongement prolongeant σ_1 et σ_2.*

Preuve. Il suffit de montrer que (1) $\Leftrightarrow$ (3).
Supposons qu'on a (1). Soient $\sigma_1 : E \longrightarrow \Omega$ et $\sigma_2 : F \longrightarrow \Omega$ des k-plongements, comme F/k est algébrique et Ω est une clôture algébrique de k, alors Ω est une clôture algébrique de F. Par le théorème de prolongement, il existe $\hat{\sigma}_2$ un k-automorphisme de Ω prolongeant σ_2. Soit donc $\tilde{\sigma} = \hat{\sigma}_2 \circ \sigma_1 : E \longrightarrow \Omega$, donc, par (1), il existe $\hat{\sigma} : EF \longrightarrow \Omega$ un F-plongement prolongeant $\tilde{\sigma}$.
Soit $\sigma = \hat{\sigma}_2 \circ \hat{\sigma} : EF \longrightarrow \Omega$, alors on a :

- si $x \in E$, $\sigma(x) = \hat{\sigma}_2(\hat{\sigma}(x)) = \hat{\sigma}_2(\tilde{\sigma}(x)) = \hat{\sigma}_2(\hat{\sigma}_2^{-1} \circ \sigma_1(x)) = \sigma_1(x)$.
- si $x \in F$, $\sigma(x) = \hat{\sigma}_2(\hat{\sigma}(x)) = \hat{\sigma}_2(x) = \sigma_2(x)$.

Supposons qu'on a (3), soient $\sigma_1 : E \longrightarrow \Omega_2$ un k-plongement et $i : F \longrightarrow \Omega_2$ l'injection canonique, alors, par (3) il existe $\sigma : EF \longrightarrow \Omega$ un k-plongement prolongeant i et σ_1. σ est un F-plongement car c'est un k-plongement prolongeant i. □

Remarques.

- Soient E, F des sous-extensions algébriques d'une extension K/k, alors E et F sont k-inséparablement disjoints si et seulement si E et F vérifient les conditions équivalentes de la proposition 5.18.
- Soient E, F des sous-extensions algébriques d'une extension K/k et soient M et N des sous-extensions de E/k et F/k respectivement. Si E et F sont k-inséparablement disjoints, alors M et N sont k-inséparablement disjoints.
- Soient E, F des sous-extensions algébriques d'une extension K/k. Si E et F sont k-inséparablement disjoints, alors on n'a pas nécessairement que $E \cap F = k$ (cf. Chap. 6).
- La propriété k-inséparablement disjoints n'implique pas la propriété k-linéairement disjoints.

Proposition 5.19. *Soient E et F des sous-extensions algébriques d'une extension K/k. Si E et F sont k-linéairement disjoints, alors ils sont k-inséparablement disjoints.*

Preuve. Soient Ω_2 une clôture algébrique de F, $\sigma : E \longrightarrow \Omega_2$ un k-plongement et montrons que σ se prolonge en un F-plongement $\hat{\sigma} : EF \longrightarrow \Omega_2$.
Soit $(e_i)_{i\in I}$ une base de E/k, alors comme E et F sont k-linéairement disjoints, $(e_i)_{i\in I}$ est une base de EF/F, ainsi pour $z \in EF$, $z = \sum_{i\in I} \lambda_i e_i$ avec $\lambda_i \in F$ et soit $\hat{\sigma} : EF \longrightarrow \Omega_2$ défini par $\hat{\sigma}(z) = \sum_{i\in I} \lambda_i \sigma(e_i)$.

- $\hat{\sigma}$ est F-linéaire par construction.
- $\hat{\sigma}$ prolonge σ, car si $z \in E$, alors $z = \sum_{i\in I} \lambda_i e_i$ avec $\lambda_i \in k \subset F$, ainsi

$$\hat{\sigma}(z) = \sum_{i\in I} \lambda_i \sigma(e_i) = \sigma(\sum_{i\in I} \lambda_i e_i) = \sigma(z).$$

• Soient $z, z' \in EF$, alors $z = \sum_{i\in I} \lambda_i e_i$ et $z' = \sum_{i\in I} \lambda'_i e_i$ avec $\lambda_i, \lambda'_i \in F$, donc

$$\begin{aligned}
\hat{\sigma}(zz') &= \hat{\sigma}(\sum_{(i,j)} \lambda_i \lambda'_j e_i e_j) \\
&= \sum_{(i,j)} \lambda_i \lambda'_j \hat{\sigma}(e_i e_j) \quad \text{(F-linéaire)} \\
&= \sum_{(i,j)} \lambda_i \lambda'_j \sigma(e_i e_j) \quad (\hat{\sigma} \text{ prolonge } \sigma) \\
&= \sum_{(i,j)} \lambda_i \lambda'_j \sigma(e_i)\sigma(e_j) \\
&= \sum_{i} \lambda_i \sigma(e_i) \sum_{j} \lambda'_j \sigma(e_j) \\
&= \hat{\sigma}(z)\hat{\sigma}(z').
\end{aligned}$$

Ainsi on a un F-plongement $\hat{\sigma} : EF \longrightarrow \Omega_2$ et E et F sont k-inséparablement disjoints. □

Proposition 5.20. *Soient E, F des sous-extensions algébriques d'une extension K/k et Ω une clôture algébrique de k. Soient*

$$\begin{aligned}
\mathcal{E}_1 &= \{k\text{-plongement de } E \text{ dans } \Omega\}, \\
\mathcal{E}_2 &= \{k\text{-plongement de } F \text{ dans } \Omega\}, \\
\mathcal{E} &= \{k\text{-plongement de } EF \text{ dans } \Omega\},
\end{aligned}$$

et l'application

$$\begin{array}{rccc} \phi : & \mathcal{E} & \longrightarrow & \mathcal{E}_1 \times \mathcal{E}_2 \\ & \sigma & \longmapsto & (\sigma/E,\ \sigma/F) \end{array}$$

alors

1) *ϕ est injective ;*
2) *ϕ et surjective si et seulement si F et F sont k-inséparablement disjoints.*

Preuve.

1) Soient $\sigma,\ tau \in \mathcal{E}$ tel que $\phi(\sigma) = \phi(\tau)$ et soit $L = \{x \in EF \mid \sigma(x) = \tau(x)\}$. On a L est un sous-corps de EF, comme $E \subset L$ et $F \subset L$, alors $EF \subset L$, ainsi $EF = L$, ainsi ϕ est injective ;
2) Trivial.

□

Corollaire 5.21. *Soient E et F deux sous-extensions algébriques d'une extension K/k, alors*

1) $[EF : k]_s \leq [E : k]_s \cdot [F : k]_s$.
2) *Si E et F sont k-inséparablement disjoints, alors $[EF : k]_s = [E : k]_s \cdot [F : k]_s$.*
3) *Si $[E : k]_s$ et $[F : k]_s$ sont finis, alors E et F sont k-inséparablement disjoints si et seulement si $[EF : k]_s = [E : k]_s \cdot [F : k]_s$.*

Proposition 5.22. *Soient E, F des sous-extensions algébriques d'une extension K/k et Ω une clôture algébrique de k. Soient*

$$\begin{aligned}
\mathcal{E} &= \{F\text{-plongement de } EF \text{ dans } \Omega\}, \\
\mathcal{E}_1 &= \{k\text{-plongement de } E \text{ dans } \Omega\},
\end{aligned}$$

et l'application

$$\begin{array}{rccc} \phi : & \mathcal{E} & \longrightarrow & \mathcal{E}_1 \\ & \sigma & \longmapsto & \sigma/E \end{array}$$

alors

1) *ϕ est injective ;*

2) *ϕ et surjective si et seulement si F et F sont k-inséparablement disjoints.*

Corollaire 5.23. *Soient E et F des sous-extensions algébriques d'une extension K/k, alors*

1) $[EF : F]_s \leq [E : k]_s$.

2) *Si E et F sont k-inséparablement disjoints, alors $[EF : F]_s = [E : k]_s$.*

3) *Si $[E : k]_s$ est fini, alors E et F sont k-inséparablement disjoints si et seulement si $[EF : F]_s = [E : k]_s$.*

Proposition 5.24. *Soient E_1/F_1 et E_2/F_2 deux sous-extensions algébriques d'une extension K/k, alors*

$$[E_1E_2 : F_1F_2]_s \leq [E_1 : F_1]_s \times [E_2 : F_2]_s.$$

Preuve. Analogue au cas linéaire et au cas transcendant. □

Chapitre 6

Extensions purement inséparables

6.1 Exposant caractéristique d'un corps. Corps parfaits

Soit k un corps. On appelle exposant caractéristique de k l'entier égal à 1 si $\text{car}(k) = 0$, et à $\text{car}(k) = p$ si $\text{car}(k) \neq 0$.

Proposition 6.1. *Soit k un corps d'exposant caractéristique q. Pour tout entier $n \geq 0$, l'application $x \longmapsto x^{q^n}$ est un isomorphisme de k sur un de ses sous-corps (noté k^{q^n}) .*

Preuve.

1) Si $q = 1$ ($\text{car}(k) = 0$), on a $i : k \longrightarrow k,\ x \longmapsto x$ est un isomorphisme.
2) Si $q > 1$ ($q = \text{car}(k) = p$), on a $f : k \longrightarrow k^{q^n},\ x \longmapsto x^{q^n}$ est un isomorphisme.

$$\forall\ a, b \in k,\ (a+b)^{q^n} = a^{q^n} + b^{q^n},\ (ab)^{q^n} = a^{q^n} b^{q^n}.$$

□

Définition 6.1. On dit qu'un corps k d'exposant caractéristique q est parfait si l'on a $k^q = k$.

Proposition 6.2. *Si k est un corps de caractéristique 0, ou fini, ou algébriquement clos, alors k est parfait.*

Preuve.

1) Si $\text{car}(k) = 0$, alors k est parfait.
2) Si $\text{car}(k) = p$ et k est fini, alors le sous-groupe multiplicatif k^* est d'ordre $p-1$, ainsi $\forall\ \alpha \in k, \alpha^p = \alpha$, donc le sous-corps k^p de k a même cardinal que k, d'où $k^p = k$ et k est parfait.
3) Si k est algébriquement clos. Soit $a \in k$, alors le polynôme $X^p - a$ a une racine α dans k, donc $\exists\ \alpha \in k$ tel que $\alpha^p = a$, ainsi $k \subset k^p$, d'où $k^p = k$ et k est parfait.

□

Remarques.

1) Tout corps premier est parfait.
2) Soient k_0 un corps de caractéristique $p \neq 0$ et $k = k_0(X)$, le corps des fractions rationnelles à une indéterminée X sur k_0, alors k est imparfait.

En effet, il n'existe aucun élément $u(X)/v(X)$ de k (u et v des polynômes de $k_0[X]$) tel que

$$\left(\frac{u(X)}{v(X)}\right)^p = X.$$

Car sinon, on aura $u(X)^p = X \cdot v(X)^p$, et en comparant les degrés des deux membres on trouve une contradiction.

6.2 Éléments purement inséparables

Définition 6.2. Soient K/k une extension et α un élément de K, **algébrique** sur k. On dit que α est purement inséparable (ou radiciel) sur k si $d_s^\circ(\alpha/k) = 1$ (minimum).

Proposition 6.3 (**Caractérisation des éléments purement inséparables**).
Soient K/k une extension, q l'exposant caractéristique de k, α un élément de K, algébrique sur k, $Q = \mathrm{Irr}(\alpha/k)$ et Ω une clôture algébrique de k, il est équivalent de dire :

1) *α est purement inséparable sur k.*

2) *Q a une seule racine dans Ω.*

3) *$Q = X^{q^n} - a$ avec $n \in \mathbb{N}$, $a \in k$.*

4) *Il existe une puissance q^n de q tel que $\alpha^{q^n} \in k$.*

Preuve.
1) $\Rightarrow$ 2) Immédiat.
2) $\Rightarrow$ 3) Supposons qu'on a (2) et soit q^n la plus grande puissance de q tel que $Q \in k[X^{q^n}]$, alors $Q = Q_1(X^{q^n})$, comme Q est irréductible, alors Q_1 est irréductible, et on $Q_1 \notin k[X^q]$, sinon $Q \in k[X^{q^{n+1}}]$, ce qui n'est pas le cas. Q_1 est donc séparable dans $\Omega[X]$ et on a

$$Q_1 = (X - \alpha_1) \dots (X - \alpha_s) \text{ avec les } \alpha_i \text{ distincts,}$$

Soit $\beta_i \in \Omega$ tel que $\beta_i^{q^n} = \alpha_i$, donc

$$Q = Q_1(X^{q^n}) = (X^{q^n} - \beta_1^{q^n}) \dots (X^{q^n} - \beta_s^{q^n}) = ((X - \beta_1) \dots (X - \beta_s))^{q^n},$$

par (2) on a que $s = 1$, ainsi $Q = (X - \beta_1)^{q^n} = X^{q^n} - a$ avec $a \in k$.
3) $\Rightarrow$ 4) Immédiat.
4) $\Rightarrow$ 1) Supposons qu'on a (4) et choisissons Ω une clôture algébrique de $k(\alpha)$. Soit $\sigma : k(\alpha) \longrightarrow \Omega$ un k-plongement, comme $\alpha^{q^n} \in k$, alors $\sigma(\alpha^{q^n}) = \alpha^{q^n}$, ainsi $\sigma(\alpha)^{q^n} = \alpha^{q^n}$, ce qui donne que $\sigma(\alpha) = \alpha$, par suite σ est l'injection canonique de $k(\alpha)$ dans Ω, ainsi $d_s^\circ(\alpha/k) = 1$, d'où (1). □

Remarques.

- α est séparable et purement inséparable sur k si et seulement si $\alpha \in k$.
- Soient L une sous-extension de K/k, α un élément de K, algébrique sur k. Si α est purement inséparable sur k, alors α est purement inséparable sur L.

En effet, si α est purement inséparable sur k, alors, par (4), il existe une puissance q^n de q tel que $\alpha^{q^n} \in k$ et on a $k \subset L$, d'où α est purement inséparable sur L.

Proposition 6.4. *Soient K/k une extension, q l'exposant caractéristique de k, α un élément de K purement inséparable sur k et n le plus petit entier tel que $a = \alpha^{q^n} \in k$, alors*

$$\mathrm{Irr}(\alpha/k) = X^{q^n} - a, \ [k(\alpha) : k] = q^n.$$

Preuve. On a α est purement inséparable sur k, donc $\mathrm{Irr}(\alpha/k) = X^{q^n} - a$ et soit $m \in \mathbb{N}$ tel que $\alpha^{q^m} \in k$, donc $n \leq m$, en effet, si $q = 1$, alors $n = 0$ et donc $n \leq m$ et si $q > 1$, on a $X^{q^n} - a \mid X^{q^m} - \alpha^{q^m}$, ainsi $q^n \leq q^m$, ainsi $n \leq m$. □

Définition 6.3. Soient k un corps commutatif et P un polynôme de $k[X]$. On dit que P est purement inséparable si P n'admet qu'une seule racine dans une clôture algébrique de k.

Proposition 6.5. *Soient K/k une extension et α un élément de K. α est purement inséparable sur k si et seulement si il existe un polynôme P de $k[X]$ purement inséparable tel que $P(\alpha) = 0$.*

Preuve. Si α est purement inséparable sur k, alors $\mathrm{Irr}(\alpha/k)$ est purement inséparable et on prend $P(X) = \mathrm{Irr}(\alpha/k)$.
S'il existe un polynôme $P \in k[X]$ purement inséparable tel que $P(\alpha) = 0$, alors on a $\mathrm{Irr}(\alpha/k)$ est purement inséparable (car $\mathrm{Irr}(\alpha/k) \mid P(X)$). □

6.3 Extensions purement inséparables

Définition 6.4. Soient K/k une extension **algébrique**, on dit que K/k est purement inséparable (ou radicielle) si et seulement si tout élément de K est purement inséparable sur k.

Remarque. Soit L une sous-extension de K/k. Si K/k est purement inséparable, alors K/L et L/k sont purement inséparables.

En effet, soit $\alpha \in K$, on a $\mathrm{Irr}(\alpha/L) \mid \mathrm{Irr}(\alpha/k)$, alors comme α est purement inséparable sur k, α est purement inséparables sur L.
Soit $\beta \in L$, alors $\beta \in K$, donc β est purement inséparable sur k.

Proposition 6.6. *Toute sous-extension d'une extension purement inséparable est purement inséparable.*

Preuve. Soient K/k une extension purement inséparable et E/F une sous-extension de K/k. Soit $\alpha \in E$, alors $\alpha \in K$, ainsi α est purement inséparable sur F (remarque), par suite E/F est purement inséparable. □

Proposition 6.7. *Soit K/k une extension algébrique, alors $[K : k]_s \geq 1$, avec l'égalité si et seulement si K/k est purement inséparable.*

Preuve. Soit $\alpha \in K$, alors $[K : k]_s = [K : k(\alpha)]_s \cdot [k(\alpha) : k]_s$. Si $[K : k]_s = 1$, alors $[K : k(\alpha)]_s = 1$ et $[k(\alpha) : k]_s = 1$, donc α est purement inséparable, ainsi K/k est purement inséparable.
Inversement, supposons que K/k est purement inséparable, alors $\forall \alpha \in K$, α est purement inséparable sur k, ainsi $\forall \alpha \in K, [k(\alpha) : k]_s = 1$. Soit Ω une clôture algébrique de K et $\sigma : K \longrightarrow \Omega$ un k-plongement, alors pour tout $\alpha \in K$ on a $\sigma/k(\alpha)$ est l'injection canonique (car $[k(\alpha) : k]_s = 1$), ainsi $\sigma(\alpha) = \alpha, \forall \alpha \in K$, ce qui donne que σ est l'injection canonique de K dans Ω, par suite $[K : k]_s = 1$. □

Remarques. Soit K/k une extension algébrique et $\alpha \in K$.

- Si α est purement inséparable sur k, alors $[k(\alpha) : k]_s = 1$, par suite $k(\alpha)/k$ est purement inséparable.
- K/k est séparable et purement inséparable si et seulement si $K = k$.

Proposition 6.8. *Soient K/k une extension algébrique et S une sous-extension de K/k. S est la clôture séparable de k dans K si et seulement si*

1) *S/k est séparable.*
2) *K/S est purement inséparable.*

Preuve. Si S est la clôture séparable de k dans K, alors

1) S/k est séparable.
2) Soit $\alpha \in K$, $Q = \mathrm{Irr}(\alpha/k)$, q^n la plus grande puissance de q tel que $Q \in k[X^{q^n}]$ (q l'exposant caractéristique de k), alors $Q(X) = Q_1(X^{q^n})$ avec Q_1 est irréductible et séparable. Comme $Q_1(\alpha^{q^n}) = Q(\alpha) = 0$, alors α^{q^n} est séparable sur k, donc $\alpha^{q^n} \in S$, ainsi α est purement inséparable sur S.

Inversement, Soit $\alpha \in K$ séparable sur k et supposons que $\alpha \notin S$. Comme K/S est purement inséparable et $\alpha \in K \setminus S$, alors α est purement inséparable sur S. Or on a α séparable sur k, donc $k(\alpha)/k$ est séparable et on a S/k est séparable, ce qui donne que $S(\alpha)/k$ est séparable, par suite $S(\alpha)/S$ est séparable, ce qui est en contradiction, ainsi $\alpha \in S$, par suite S est la clôture séparable de k dans K. □

Remarque. Soient K/k une extension algébrique et S la clôture séparable de k dans K, alors on a

$$k \xrightarrow{\text{sép.}} S \xrightarrow{\text{pur. insép.}} K,$$

donc si K/k est quelconque, alors on a la suite

$$k \xrightarrow{\text{pure}} k(B) \xrightarrow{\text{sép.}} S \xrightarrow{\text{pur. insép.}} K.$$

Proposition 6.9. *Soient K/k une extension finie et S la clôture séparable de k dans K, alors on a $[K : k]_s = [S : k]$, en particulier on a $[K : k]_s$ divise $[K : k]$.*

Preuve. On a $[K : k]_s = [K : S]_s \cdot [S : k]_s = 1 \cdot [S : k]$. □

Proposition 6.10 (**Transitivité de la pure inséparabilité**).
Soit L une sous-extension d'une extension K/k, alors K/k est purement inséparable si et seulement si K/L et L/k sont purement inséparables.

Preuve. On a $[K : k]_s = [K : L]_s \cdot [L : k]_s$, donc $[K : k]_s = 1 \Leftrightarrow [K : L]_s = [L : k]_s = 1$. □

Proposition 6.11. *Soit K/k une extension, alors l'ensemble des éléments de K purement inséparables sur k est un corps intermédiaire à k et K.*

Preuve. Soient $\alpha,\ \beta \in K$ purement inséparables sur k. α est purement inséparable sur k, donc $k(\alpha)/k$ est purement inséparable, β est purement inséparable sur k, donc β est purement inséparable sur $k(\alpha)$, ainsi $k(\alpha)(\beta)/k$ est purement inséparable c'est-à-dire que $k(\alpha, \beta)/k$ est purement inséparable, ce qui donne que $\alpha+\beta,\ \alpha-\beta,\ \alpha\beta$ et α/β (lorsque $\beta \neq 0$) sont purement inséparables sur k. □

Définition 6.5. Soit K/k une extension, on appelle clôture purement inséparable de k dans K, l'ensemble des éléments de K purement inséparables sur k.

Il résulte immédiatement de cette définition que le clôture purement inséparable P de k dans K est caractérisé par l'une des trois caractérisation :

- ▶ Pour toute sous-extension L de K/k, L/k est purement inséparable si et seulement si $L \subset P$.
- ▶ (a) P/k est purement inséparable.
  (b) $\forall\ \alpha \in K \setminus P$, α est non purement inséparable sur k.
- ▶ (a) P/k est purement inséparable.
  (b) $\forall\ \alpha \in K \setminus P$, α est non purement inséparable sur P.

Proposition 6.12. *Soient E_1/F_1 et E_2/F_2 deux sous-extensions d'une extension K/k. Si E_1/F_1 et E_2/F_2 sont purement inséparables, alors E_1E_2/F_1F_2 est purement inséparable.*

Preuve. La clôture purement inséparable de F_1F_2 dans K contient E_1 et E_2, donc contient E_1E_2. □

Cas particuliers :

- Soient E et F deux sous-extensions d'une extension K/k. Si E/k et F/k sont purement inséparables, alors EF/k est purement inséparable.
- Soient E/F et L deux sous-extensions d'une extension K/k. Si E/F est purement inséparable, alors EL/FL est purement inséparable.
- Soient E/F une sous-extension d'une extension K/k et A une partie de K. Si E/F est purement inséparable, alors $E(A)/F(A)$ est purement inséparable.

6.4 Clôtures purement inséparables

Proposition 6.13. *Soit C un corps commutatif, alors il est équivalent de dire*

1) *Toute extension purement inséparable C'/C vérifie $C' = C$.*
2) *Tout polynôme P de $C[X]$, purement inséparable à une racine dans C.*
3) *Tout polynôme P de $C[X]$, purement inséparable est scindé sur C.*

Preuve. Analogue au cas algébrique et au cas séparable. □

Définition 6.6. Un corps commutatif C est dit inséparablement clos (ou parfait) si il vérifie les conditions équivalentes de la proposition 6.13.

Proposition 6.14. *Soit C un corps commutatif et et q l'exposant caractéristique de C ($q = 1$ si $\mathrm{car}(C) = 0$ et $q = p$ si $\mathrm{car}(C) = p > 0$). Le corps C est parfait si et seulement si l'homomorphisme $x \in C \longmapsto x^q \in C$ est surjectif (bijectif).*

Preuve. Supposons que C est parfait, alors pour $\beta \in C$, on peut construire une extension de C de la forme $C(\alpha)$ avec $\alpha^q = \beta$, donc $C(\alpha)/C$ est purement inséparable, donc $C(\alpha) = C$, ainsi $\alpha \in C$ et $\alpha^q = \beta$, donc l'homomorphisme $x \in C \longmapsto x^q \in C$ est surjectif.
Inversement, supposons que l'homomorphisme $f : C \longmapsto C, x \longmapsto x^q$ est surjectif. Soit C' une extension purement inséparable de C, alors tout élément de C' est purement inséparable sur C, ainsi $\forall\ x \in C', \exists\ n \in \mathbb{N}$ tel que $x^{q^n} \in C$, donc si $n \leq 1$, alors $x \in C$, et si $n > 1$, on aura par surjectivité de f, est surjectif, $x^{q^{n-1}} \in C$, par suite $x \in C$, et ainsi $C' = C$, donc C est purement inséparable. □

Proposition 6.15. *Un corps commutatif C est parfait si et seulement si toute extension algébrique de C est séparable.*

Preuve. Si $\mathrm{car}(C) = 0$, alors rien à démontrer.
Si $\mathrm{car}(C) = p > 0$. Supposons que C est parfait et soit C'/C une extension algébrique. Supposons que C'/C est non séparable, donc $\exists\ x \in C'$ tel que x est non séparable sur C, donc $\mathrm{Irr}(x/C) \in C[X^p]$, écrivons

$$\mathrm{Irr}(x/C) = a_0 + a_1X^p + a_2X^{2p} + \ldots + a_dX^{dp}.$$

Puisque $x \in C \longmapsto x^p \in C$ est surjectif, chaque $a_i = b_i^p$ avec $b_i \in C$, ainsi

$$\mathrm{Irr}(x/C) = b_0^p + b_1^pX^p + b_2^pX^{2p} + \ldots + b_d^pX^{dp} = (b_0 + b_1X + b_2X^2 + \ldots + b_dX^d)^p,$$

ce qui contredit le fait que $\mathrm{Irr}(x/C)$ est irréductible, par suite C'/C est séparable.
Inversement, supposons que toute extension algébrique de C est séparable. Soit C'/C une extension purement inséparable, or elle est aussi séparable par supposition, donc $C = C'$, donc C est parfait. □

Proposition 6.16 (**Théorème de prolongement purement inséparable**).
Soient C un corps parfait, $\sigma : k \longrightarrow C$ un plongement de corps et K/k une extension purement inséparable, alors il existe $\hat{\sigma} : K \longrightarrow C$ un plongement prolongeant σ.

Preuve. Analogue au cas algébrique et séparable. □

Définition 6.7. Soit k un corps commutatif, une extension Ω de k est appelé clôture purement inséparable (ou parfaite) de k si

1) Ω/k est purement inséparable.

2) Ω est parfait.

Proposition 6.17. *Soit k un corps commutatif, Ω une extension de k. Ω est une clôture parfaite de k si et seulement si*

1) *Ω/k est purement inséparable.*

2) *Toute extension purement inséparable de k se k-plonge dans Ω.*

Preuve. Analogue au cas algébrique et séparable. □

Proposition 6.18 (**Théorème de Steinitz purement inséparable**).
Tout corps commutatif k admet une clôture parfaite et deux clôtures parfaites de k sont k-isomorphes.

Preuve. Soit Ω_1 une clôture algébrique de k, Ω la clôture purement inséparable de k dans Ω_1, alors :

1) Ω/k est purement inséparable.
2) Soit K une extension purement inséparable de k, alors il existe $\hat{\sigma}$ un k-plongement de K dans Ω_1 (clôture algébrique). Posons $\sigma = \hat{\sigma}/k$, alors σ est un plongement de k dans Ω, ainsi, par le théorème de prolongement, il existe un plongement de K dans Ω prolongeant σ. Ainsi, toute extension purement inséparable de k se k-plonge dans Ω.

Ω est donc une clôture parfaite de k. □

6.5 Degré d'inséparabilités

Définition 6.8. Soit K/k une extension, S la clôture purement séparable de k dans K, le degré $[K : S]$ s'appelle degré d'inséparabilité de l'extension K/k, on note $[K : k]_i = [K : S]$.

Remarques.

- Si K/k est finie, alors $[K : k]_i \leq [K : k]$, avec l'égalité si et seulement si K/k est purement inséparable.
- Si K/k est algébrique, alors $1 \leq [K : k]_i$, avec l'égalité si et seulement si K/k est séparable.
- Si K/k est finie, alors
$$[K : k]_i = [K : S] = \frac{[K : k]}{[S : k]} = \frac{[K : k]}{[K : k]_s}.$$
Donc si L est une sous-extension d'une extension K/k, alors $[K : k]_i = [K : L]_i \cdot [L : k]_i$, cependant cette relation est vraie pour toute extension algébrique K/k.

Proposition 6.19. *Soient E_1/F_1 et E_2/F_2 deux sous-extensions algébriques d'une extension K/k, alors*
$$[E_1E_2 : F_1F_2]_i \leq [E_1 : F_1] \times [E_2 : F_2].$$

Preuve. Soit S_r la clôture séparable de F_r dans E_r $(r = 1, 2)$, alors la clôture séparable de F_1F_2 dans E_1E_2 est S_1S_2, en effet

1) S_1S_2/F_1F_2 est séparable car S_r/F_r l'est.
2) E_1E_2/S_1S_2 est purement inséparable car E_r/S_r l'est.

Et on a :

$$[E_1E_2 : F_1F_2]_i = [E_1E_2 : S_1S_2]_i \leq [E_1 : S_1] \times [E_2 : S_2] \leq [E_1 : F_1] \times [E_2 : F_2].$$

□

Remarques.

1) Soient E et F des sous-extensions algébriques de K/k. Si E/k est purement inséparable, alors E et F sont k-inséparablement disjoints.
2) Soient E et F des sous-extensions algébriques de K/k. Si E et F sont k-inséparablement disjoints, alors $(E \cap F)/k$ est purement inséparable.

   $\sigma : E \cap F \longrightarrow \Omega$, $\hat{\sigma} : E \longrightarrow \Omega$, $\hat{\sigma} : EF \longrightarrow \Omega$ un F-plongement $\rightarrow \sigma$ est l'injection canonique.

Chapitre 7

Extensions normales

7.1 Corps de rupture

Définition 7.1. Soient k un corps commutatif et P un polynôme irréductible de $k[X]$. Un corps de rupture de P sur k est une extension simple $k(\alpha)$ de k avec α une racine de P.

Exemples.
1) $\mathbb{Q}(\sqrt{2})$ est un corps de rupture de X^2-2 sur $\mathbb{Q}$.
2) $\mathbb{Q}(\sqrt[4]{2})$ est un corps de rupture de X^4-2 sur $\mathbb{Q}$.
3) $\mathbb{C}$ est un corps de rupture de X^2+1 sur $\mathbb{R}$.

Théorème 7.1. *Soient k un corps commutatif et P un polynôme irréductible de $k[X]$. Alors P admet un corps de rupture, unique à k-isomorphisme près.*

Preuve. Soit $K = k[X]/(P)$, alors K est une extension de k car la restriction de $s : k[X] \longrightarrow k[X]/(P)$ à k est injective. Si on identifie k à son image dans K, on a $K = k(\alpha)$ où $\alpha = \bar{X}$ dans K, il est évident par ailleurs que $P(\alpha) = 0$.
Si $K' = k(\alpha')$ est un corps de rupture de P sur k, alors K et K' sont k-isomorphes par un isomorphisme laissant fixes les éléments de k et échangeant α en α'. □

Définition 7.2. Soient k un corps commutatif et P un polynôme de $k[X]$, de degré supérieur ou égal à 1. Un corps de rupture de P sur k est une extension simple $k(\alpha)$ de k avec α racine de P.

Un tel corps existe toujours, il suffit de prendre f un facteur irréductible de P et le corps $K = k[X]/(f)$, alors $K = k(\alpha)$ où $\alpha = \bar{X}$ dans Ket il est évident par ailleurs que $f(\alpha) = 0$, donc $P(\alpha) = 0$.

Remarque. Si P n'est pas irréductible, deux corps de rupture ne sont pas toujours isomorphes.

Contre exemple. Soit $P(X) = X(X^2-2) \in \mathbb{Q}[X]$, $\mathbb{Q} = \mathbb{Q}(0)$ et $\mathbb{Q}(\sqrt{2})$ sont deux corps de rupture de P non isomorphes (2 n'étant pas un carré dans $\mathbb{Q}$ et il est dans $\mathbb{Q}(\sqrt{2})$).

Plus généralement, si $\varphi : k_1 \longrightarrow k_2$ est un isomorphisme, $f(X)$ un polynôme irréductible de $k_1[X]$, K_1 et K_2 deux corps de rupture de f et $\varphi(f)$ sur k_1 et k_2 respectivement, avec

$$f = \sum_{i=0}^{n} a_i X^i \longmapsto \varphi(f) = \sum_{i=0}^{n} \varphi(a_i) X^i,$$

alors il existe un isomorphisme $\overline{\varphi} : K_1 \longrightarrow K_2$ qui prolonge φ.
En effet, $K_1 = k_1(\alpha_1), K_2 = k_2(\alpha_2)$ où α_1, α_2 sont deux racines de f et $\varphi(f)$ respectivement.
Posons $n = \deg(f)$, alors $(1, \alpha_1, \ldots, \alpha_1^{n-1})$ est une k_1-base de $k_1(\alpha_1)$, donc tout élément de $k_1(\alpha_1)$ s'écrit de façon unique $\sum_{i=0}^{n} a_i \alpha_1^i$ où $a_i \in k_1$, alors on voit que $\overline{\varphi}$ définie par

$$\overline{\varphi}(\sum_{i=0}^{n} a_i \alpha_1^i) = \sum_{i=0}^{n} \varphi(a_i) \alpha_2^i$$

convient.

Définition 7.3. Soient k un corps commutatif et P un polynôme de $k[X]$, de degré supérieur ou égal à 1. Un corps de décomposition de P sur k (qu'on note par $D_k(P)$) est une extension (minimale) K de k telle que :

1) P est scindé sur K ;
2) les racines de P dans K engendrent K sur k, c'est-à-dire que $K = k(\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n$ sont les racines de P.

Proposition 7.2. *Soient k un corps commutatif et P un polynôme de $k[X]$, de degré supérieur ou égal à 1. Alors P possède un corps de décomposition, unique à isomorphisme près. Celui-ci est une extension finie de k, et c'est une sous-extension de toute extension sur laquelle P est scindé.*

Exemples.

1) $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$.
2) $\mathbb{Q}(\sqrt[4]{2})$ n'est pas un corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$.
3) $\mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$ est un corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$.
4) $\mathbb{C}$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.

7.2 Extensions normales

Définition 7.4. Soient k un corps commutatif et N une extension algébrique de k. On dit que N est une extension normale (ou quasi-galoisienne) de k si et seulement si à chaque fois qu'un polynôme $f(X)$ irréductible de $k[X]$ a une racine dans N, $f(X)$ a toutes ses racines dans N (c'est-à-dire $f(X)$ est scindé sur N).

Exemples.

1) Le corps k est normal sur lui-même ;
2) Toute clôture algébrique de k est normale sur k.

Proposition 7.3. *Toute extension quadratique d'un corps k est normale.*

Preuve. Soit K une extension quadratique de k et soit $P(X)$ un polynôme irréductible de $k[X]$, ayant une racine $\alpha \in K$.
On a $\mathrm{Irr}(\alpha/k)$ divise $P(X)$ dans $K[X]$, or $P(X)$ est irréductible sur k, donc

$$\exists\ \lambda \in k^* : P = \lambda \cdot \mathrm{Irr}(\alpha/k).$$

Si $\alpha \in k$, alors

$$\mathrm{Irr}(\alpha/k) = X - \alpha \text{ est de degré } 1 \Rightarrow P \text{ est scindé sur } k \Rightarrow P \text{ est scindé sur } K.$$

Si $\alpha \notin k$, alors

$$\begin{aligned}\mathrm{Irr}(\alpha/k) = X^2 + bX + c,\ b, c \in k,\ \text{est de degré } 2 &\Rightarrow \mathrm{Irr}(\alpha/k) = (X - \alpha)(X + b + \alpha)\\ &\Rightarrow P(X) = \lambda(X - \alpha)(X + b + \alpha)\\ &\Rightarrow P \text{ est scindé sur } K.\end{aligned}$$

Par suite K/k est normale. □

Remarques.

1) Soient K/k une extension normale et E une sous-extension de K/k, alors l'extension K/E est normale.

   En effet, soit $P(X)$ un polynôme irréductible sur E et qui a une racine dans K. Comme $k \subset E$, alors $P(X)$ est irréductible sur k et qui a une racine dans K, et comme K/k est normale, alors $P(X)$ a toutes ses racines dans K, ainsi K/E est normale.

2) Soient K/k une extension normale et E une sous-extension de K/k, alors on a pas nécessairement que l'extension E/k est normale.

Contre exemple. Soient $k = \mathbb{Q}, E = \mathbb{Q}(\sqrt[3]{2}), K = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(j, \sqrt[3]{2})$. On a K/k est normale mais E/k ne l'est pas.

3) Soient E/k et K/E deux extensions normales, alors on a pas nécessairement que l'extension K/k est normale.

Contre exemple. Soient $k = \mathbb{Q}, E = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}(\sqrt[4]{2})$. On a E/k et K/E sont deux extensions normales mais K/k ne l'est pas.

Théorème 7.4. *Soient K/k une extension algébrique et Ω une clôture algébrique de K. Les conditions suivantes sont équivalentes :*

1) *K est une une extension normale de k.*
2) *Pour tout $\alpha \in K$, les conjugués de α dans Ω par rapport à k appartiennent tous à K.*
3) *Pour toute extension L de k contenant K et pour tout k-plongement $\sigma : K \longrightarrow L$, on a $\sigma(K) \subset K$.*
4) *Pour tout k-plongement $\sigma : K \longrightarrow \Omega$, on a $\sigma(K) \subset K$.*
5) *Pour toute extension L de k contenant K. Tout k-plongement $\sigma : K \longrightarrow L$ est un k-automorphisme de K.*
6) *Tout k-plongement $\sigma : K \longrightarrow \Omega$ est un k-automorphisme de K.*

Preuve.
3) $\Rightarrow$ 4), 5) $\Rightarrow$ 6), 5) $\Rightarrow$ 3) et 6) $\Rightarrow$ 4) sont triviaux.
1) $\Rightarrow$ 3) Supposons qu'on a (1), soient $\alpha \in K$, $Q = \mathrm{Irr}(\alpha/k)$ et soit $\sigma : K \longrightarrow L$ un k-plongement. On a $Q(\sigma(\alpha)) = \sigma(Q(\alpha)) = \sigma(0) = 0$, donc $\sigma(\alpha)$ est une racine de Q or K/k est normale, donc $\sigma(\alpha) \in K$, ainsi $\sigma(K) \subset K$.
3) $\Rightarrow$ 5) Soit L une extension de k contenant K et soit $\sigma : K \longrightarrow L$ un k-plongement, alors, par (3) on a $\sigma(K) \subset K$, donc pour montrer que σ est un k-automorphisme de K, il suffit de prouver que $K \subset \sigma(K)$.

- Si $[K : k]$ est fini, comme σ est une application k-linéaire injective de K dans $\sigma(K)$, alors

$$[\sigma(K) : k] = [K : k].$$

Comme $k \subset \sigma(K) \subset K$, on a :

$$[K : k] = [K : \sigma(K)] \times [\sigma(K) : k] \Rightarrow [K : \sigma(K)] = 1 \Rightarrow \sigma(K) = K.$$

- Si $[K : k]$ est infini, soient $\alpha \in K$, $Q = \mathrm{Irr}(\alpha/k)$ et $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ les racines distinctes de $Q(X)$ dans L qui appartiennent à K, alors,d'après (3), $\sigma(\alpha_i) \in K, \forall\ i = 1, \ldots, s$, et on a $\sigma(\alpha_i)$ est une racine de $Q(X)$, donc $\exists\ j$ tel que $\sigma(\alpha_i) = \alpha_j$. Ainsi σ induit une application, nécessairement injective, de l'ensemble fini $\{\alpha_1, \ldots, \alpha_s\}$ dans lui-même. Cette application est aussi surjective, ainsi $\exists\ p$ tel que $\sigma(\alpha_p) = \alpha$, par suite $\alpha \in \sigma(K)$, ainsi $K \subset \sigma(K)$.

4) $\Rightarrow$ 2) Soient $\alpha \in K$ et $\beta \in \Omega$ un conjugué de α sur k, alors il existe un k-isomorphisme $\sigma : k(\alpha) \longrightarrow k(\beta)$ tel que $\sigma(\alpha) = \beta$. Or on peut prolonger σ en un k-plongement $\hat{\sigma} : K \longrightarrow \Omega$ et on a

$$\beta = \sigma(\alpha) = \hat{\sigma}(\alpha) \in \hat{\sigma}(K) \subset K.$$

2) $\Rightarrow$ 1) Soit $P(X) \in k[X]$ un polynôme irréductible, ayant une racine α dans K. Soit $\beta \in \Omega$ une racine de $P(X)$, alors β est un conjugué de α sur k, donc $\beta \in K$ d'après (2). Ainsi toutes les racines de $P(X)$ sont dans K, ce qui donne que K/k est normale. □

7.3 Extensions normales finies et corps de décomposition

Théorème 7.5. *Soient k un corps commutatif et K une extension de degré fini de k, alors l'extension K/k est normale si et seulement si K est le corps de décomposition d'un polynôme de $k[X]$ sur k.*

Preuve. Supposons que K est le corps de décomposition d'un polynôme $P(X) \in k[X]$ sur k, alors

$$P(X) = \lambda(X - \alpha_1)\dots(X - \alpha_n), \lambda \in K \text{ et } K = k(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Soient Ω une clôture algébrique de K et $\sigma : K \longrightarrow \Omega$ un k-plongement. Soit $x \in K$, alors $x = \sum_{i=0}^{n} \lambda_i \alpha_i, \lambda_i \in k$. Comme $P(X) \in k[X]$, alors $\sigma(P(x)) = P(\sigma(x))$ et on a $P(\sigma(\alpha_i)) = \sigma(P(\alpha_i)) = \sigma(0) = 0$, ainsi $\sigma(\alpha_i)$ est une racine α_j de $P(X)$, par suite $\sigma(x) \in K$, ainsi $\sigma(K) \subset K$, ce qui donne que K/k est normale.
Inversement, on a K est une extension de type fini de K, donc $K = k(\alpha_1, \alpha_2, \dots, \alpha_n)$. Soit $Q_i = \mathrm{Irr}(\alpha_i/k)$, alors Q_i est un polynôme irréductible de $k[X]$ et a une racine α_i dans K et K/k est normale, donc Q_i est scindé sur K. Soit $P(X)$ le produit des facteurs distincts du premier degré dans les décompositions des Q_i, alors $P(X) \in k[X]$ et est scindé sur K. Soient U l'ensemble des racines de P et $D = k(U)$ le corps de décomposition de P sur K. Comme P est scindé sur K, alors $U \subset K$, ainsi $D = k(U) \subset K$, et comme $\alpha_1, \alpha_2, \dots, \alpha_n \in U$, alors $K \subset k(U) = D$, par suite $K = D$ est le corps de décomposition de $P(X)$ sur k. □

Exemples.

1) Soient $k = \mathbb{Q}, K = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$, alors K/k est normale car $K = D_k(X^3 - 2)$.
2) Soient $k = \mathbb{Q}, K = \mathbb{Q}(i, \sqrt[4]{2})$, alors K/k est normale car $K = D_k(X^4 - 2)$.
3) Soient $n \in \mathbb{N}^*, \omega$ une racine primitive n-ième de l'unité, alors $\mathbb{Q}(\omega)/\mathbb{Q}$ est normale, car

$$\mathbb{Q}(\omega) = \mathbb{Q}(1, \omega, \dots, \omega^{n-1}) = D_{\mathbb{Q}}(X^n - 1).$$

Corollaire 7.6. *Soient k un corps commutatif et K une extension de degré fini de k. Si l'extension K/k est normale et séparable, alors K est le corps de décomposition d'un polynôme séparable de $k[X]$ sur k.*

Proposition 7.7. *Soient k un corps commutatif et K une extension de degré fini de k. Si l'extension K/k est normale et séparable, alors K est le corps de décomposition d'un polynôme irréductible séparable de $k[X]$ sur k.*

Proposition 7.8. *Toute extension algébrique d'un corps fini est normale.*

Preuve. Soient k un corps fini et K/k une extension algébrique. Soit $\alpha \in K$, alors $\mathrm{card}(k(\alpha)) = q$, donc $k(\alpha)$ est le corps de décomposition de $X^q - X$, donc $k(\alpha)/k$ est normale, ainsi $\mathrm{Irr}(\alpha/k)$ est scindé sur $k(\alpha)$, donc sur K, par suite tous les conjugués de α sur k sont dans K, ce qui donne que K/k est normale. □

Proposition 7.9. *Soient E_1/F_1 et E_2/F_2 deux sous-extensions algébriques d'une extension K/k. Si E_1/F_1 et E_2/F_2 sont normales, alors E_1E_2/F_1F_2 est normale.*

Preuve. Soient Ω une clôture algébrique de E_1E_2 et $\sigma : E_1E_2 \longrightarrow \Omega$ un F_1F_2-plongement, donc σ/E_i est un k-plongement dans Ω ($\sigma/E_i : E_i \longrightarrow \Omega$), soit Ω_i la clôture algébrique de F_i dans Ω (donc Ω_i est la clôture algébrique de E_i dans Ω), σ/E_i est un F_i-plongement, comme E_i/F_i est algébrique, alors $\sigma(E_i)/F_i$ est algébrique, donc $\sigma(E_i) \subset \Omega_i$, donc $\sigma/E_i : E_i \longrightarrow \Omega_i$, donc $\sigma(E_i) = E_i$, ainsi $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2) = E_1E_2$.

□

7.4 Clôture normale d'une extension algébrique

Proposition 7.10. *Soient K/k une extension et $(N_i)_{i\in I}$ une famille de sous-extensions de K/k normales sur k, alors $\bigcap_{i\in I} N_i$ est normale sur k.*

Preuve. Soit Q un polynôme irréductible de $k[X]$, ayant une racine dans $\bigcap_{i\in I} N_i$, alors Q est scindé sur chaque N_i, donc Q est scindé sur $\bigcap_{i\in I} N_i$. □

Définition 7.5. Soient N/k une extension normale et G une partie de N. On appelle sous-extension normale sur k engendré par G l'intersection des sous-extensions de N/k normales sur k et contenant G.

Proposition 7.11. *Soit K/k une extension algébrique, il existe une extension N de K, normale sur k, unique à K-isomorphisme près tel que pour toute extension K' de K, on a si K'/k est normale, alors N se K-plonge dans K'.*

Preuve. Soient Ω une clôture algébrique de K et N l'extension normale sur k engendré par K. Soient K' une extension algébrique de K, normale sur k et $\sigma : K' \longrightarrow \Omega$ un K-plongement, alors $\sigma(K')/k$ est normale, donc $N \subset \sigma(K')$, donc N se K-plonge dans K'. Si $\tilde{N}$ possède aussi la propriété de N, alors N se K-plonge dans N' et N' se K-plonge dans N, donc N et N' sont K-isomorphes. □

Définition 7.6. Avec les notations de la proposition 7.11, l'extension N/k s'appelle extension normale engendré par l'extension K/k (ou clôture normale de K/k).

Définition 7.7. Soit K/k une extension algébrique. On dit que N est une clôture normale de K/k si et seulement si :

1) N est une extension algébrique de K ;

2) N/k est normale ;

3) Si N' est une sous-extension de N/K avec N'/k est normale, alors $N' = N$.

Ainsi une clôture normale de K/k est un élément minimal de l'ensemble des extensions de K qui sont normales sur k.

Théorème 7.12. *Soit K/k une extension de degré fini, alors :*

1) *K/k admet une clôture normale N.*

2) *N/k est de degré fini.*

3) *Si M est une clôture normale de K/k, alors M et N sont K-isomorphe.*

Preuve. On a K/k est de degré fini, alors K est une extension de type fini de k, ainsi $K = k(\alpha_1, \ldots, \alpha_n)$.
Pour chaque $i \in [\![1\ ;\ n]\!]$, notons $Q_i = \mathrm{Irr}(\alpha_i/k)$ et posons

$$P(X) = Q_1(X) \ldots Q_n(X) \in k[X].$$

Soit N un corps de décomposition de $P(X)$ sur K, alors $N = K(\beta_1, \ldots, \beta_m)$ où :
(1) $P(X) = (X - \beta_1) \ldots (X - \beta_m) \in N[X]$, les $\beta_j \in N$, ainsi

$$N = k(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) \Rightarrow N = k(\beta_1, \ldots, \beta_m)$$

(car les α_i sont des racines de $P(X)$ dans K, donc dans N, ainsi $\alpha_i = \beta_j$). Donc N est un corps de décomposition de $P(X)$ sur k, ainsi N est une extension normale de k et $[N : k]$ est fini.

Soit N' est une sous-extension de N/K avec N'/k est normale, Pour chaque $i \in [\![1\ ;\ n]\!]$, $Q_i(X)$ est un polynôme irréductible de $k[X]$ et admet au moins une racine α_i dans N' ; donc, comme N'/k est normale, $Q_i(X)$ est scindé sur N'. Donc $P(X) = Q_1(X) \ldots Q_n(X)$ est scindé sur N' :

(2) $P(X) = (X-\gamma_1)\dots(X-\gamma_m) \in N'[X]$, les $\gamma_j \in N'$.

(1) et (2) sont deux décompositions de $P(X)$ en produit de facteurs irréductibles dans $N[X]$, donc il existe σ dans S_n tel que $\forall\, i, \beta_i = \gamma_{\sigma(i)}$. Donc les β_i appartiennent à N'. Ainsi $N = k(\beta_1, \dots, \beta_m) \subset N'$. Par suite $N' = N$.

Soit M une clôture normale de K/k. Pour chaque $i \in [\![1\,;\, n]\!]$, $Q_i(X)$ est un polynôme irréductible de $k[X]$ et admet au moins une racine α_i dans M ; donc, comme M/k est normale, $Q_i(X)$ est scindé sur M. Donc $P(X) = Q_1(X)\dots Q_n(X)$ est scindé sur M :

$$P(X) = (X-\delta_1)\dots(X-\delta_m) \in M[X], \text{ les } \delta_j \in M.$$

$D = k(\delta_1, \dots, \delta_m)$ est un corps de décomposition de $P(X)$ sur k. Comme chaque α_i est une racine de $P(X)$ dans $K \subset M$, chaque α_i est un δ_j, donc $K = k(\alpha_1, \dots, \alpha_n) \subset D$, ainsi $K \subset D \subset M$, avec D/k est normale.
Comme M est une clôture normale de K/k, alors $M = D$. $D = K(\delta_1, \dots, \delta_m)$ est aussi un corps de décomposition de $P(X)$ sur K. N étant lui aussi un corps de décomposition de $P(X)$ sur K, donc il existe un K-isomorphisme de M dans N. □

Proposition 7.13. *Soient K/k une extension algébrique avec $K = k(G)$, Ω une clôture algébrique de K et $\hat{G} = \{x \in \Omega \mid \exists\, x' \in G,\ x \text{ et } x' \text{ sont } k\text{-conjugués}\}$, alors $k(\hat{G})/k$ est l'extension normale engendré par K/k.*

Exemples.

1) Soient $\Omega = \mathbb{C}$, $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[5]{2})$, alors $G = \{\sqrt[5]{2}\}$, donc

$$\hat{G} = \{x \in \Omega \mid x \text{ et } \sqrt[5]{2} \text{ sont } k\text{-conjugués}\} = \{\sqrt[5]{2}, \zeta_5\sqrt[5]{2}, \zeta_5^2\sqrt[5]{2}, \zeta_5^3\sqrt[5]{2}, \zeta_5^4\sqrt[5]{2}\},$$

ainsi $k(\hat{G})/k$ est l'extension normale engendré par K/k (ou clôture normale de K/k), avec

$$k(\hat{G}) = \mathbb{Q}(\sqrt[5]{2}, \zeta_5\sqrt[5]{2}, \zeta_5^2\sqrt[5]{2}, \zeta_5^3\sqrt[5]{2}, \zeta_5^4\sqrt[5]{2}) = \mathbb{Q}(\zeta_5,\ \sqrt[5]{2}).$$

2) Soient $\Omega = \mathbb{C}$, $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$, alors $G = \{\sqrt[3]{2}\}$, donc

$$\hat{G} = \{x \in \Omega \mid x \text{ et } \sqrt[3]{2} \text{ sont } k\text{-conjugués}\} = \{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\},$$

ainsi $k(\hat{G})/k$ est la clôture normale de K/k, avec

$$k(\hat{G}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) = \mathbb{Q}(\zeta_3,\ \sqrt[3]{2}).$$

Proposition 7.14. *Soient K/k une extension algébrique, Ω une clôture algébrique de K et $K_1, \dots, K_n$ les k-conjugués de K dans Ω, alors $(K_1K_2\dots K_n)/k$ est l'extension normale engendré par K/k.*

Exemple. Soient $\Omega = \mathbb{C}$, $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[5]{2})$, alors

$$K_1 = \mathbb{Q}(\sqrt[5]{2}), K_2 = \mathbb{Q}(\zeta_5\sqrt[5]{2}), K_3 = \mathbb{Q}(\zeta_5^2\sqrt[5]{2}), K_4 = \mathbb{Q}(\zeta_5^3\sqrt[5]{2}), K_5 = \mathbb{Q}(\zeta_5^4\sqrt[5]{2}).$$

On a $N = K_1K_2\dots K_5 = \mathbb{Q}(\zeta_5,\ \sqrt[5]{2})$, ainsi N/k est l'extension normale engendré par K/k (ou clôture normale de K/k).

Remarque. Les proposition 7.13 et 7.14 restent vraies si on change Ω par une extension algébrique N de K normale sur k.

Proposition 7.15. *Soit K/k une extension algébrique et soit N une clôture normale de K/k.*

1) *Si K/k est de degré fini, alors N/k est de degré fini.*

2) *Si K/k est séparable, alors N/k est séparable.*

Preuve. Soient Ω une clôture algébrique de K et H l'ensemble des k-plongement de K dans Ω.

1) Si K/k est de degré fini, alors $K = k(\alpha_1, \ldots, \alpha_n)$, où les α_i sont algébriques sur k, ainsi

$$N = k(\bigcup_{\sigma \in H} \sigma(K)) = k(R), \text{ avec } R = \bigcup_{\sigma \in H} \bigcup_{i=1}^{n} \sigma(\alpha_i).$$

R est l'ensemble de toutes les racines dans Ω des polynômes minimaux de tous les α_i avec $i \in [\![1 \ ; \ n]\!]$. R est un ensemble fini dont tous les éléments sont algébriques sur k, donc $N = k(R)$ est une extension de degré fini de k.

2) Supposons que K/k est séparable. Pour montrer que N/k est séparable, il suffit de prouver que tout élément β de $\bigcup_{\sigma \in H} \sigma(K)$ est séparable. Soit donc $\beta = \sigma(\alpha)$, où $\sigma \in H$ et $\alpha \in K$. Comme K/k est séparable, $\mathrm{Irr}(\alpha/k)(X)$ est séparable. On a

$$\mathrm{Irr}(\alpha/k)(\beta) = \mathrm{Irr}(\alpha/k)(\sigma(\alpha)) = \sigma(\mathrm{Irr}(\alpha/k)(\alpha)) = \sigma(0) = 0,$$

donc $\mathrm{Irr}(\alpha/k)(X) = \mathrm{Irr}(\beta/k)(X)$. Ainsi $\mathrm{Irr}(\beta/k)(X)$ est séparable, ce qui donne que β est séparable.

□

Chapitre 8

Extension Galoisienne

8.1 Groupe de Galois et Corps des invariants

Définition 8.1. Soient K un corps commutatif, $A \subset K$ et $H \subset \mathrm{Aut}(K)$.

1) On appelle groupe de Galois de K sur A, qu'on note par $\mathrm{Gal}(K/A)$ l'ensemble

$$\mathrm{Gal}(K/A) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(x) = x,\ \forall\ x \in A\}.$$

2) On appelle corps des invariants de H, qu'on note par $\mathrm{Inv}(H)$ l'ensemble

$$\mathrm{Inv}(H) = \{x \in K \mid \sigma(x) = x,\ \forall\ \sigma \in H\}.$$

On vérifie immédiatement que $\mathrm{Gal}(K/A)$ est un sous-groupe de $\mathrm{Aut}(K)$ et que $\mathrm{Inv}(H)$ est un sous-corps de K.

Propriétés. Soient K un corps commutatif.

- Soient H_1 et H_2 deux parties de $\mathrm{Aut}(K)$ tel que $H_1 \subset H_2$, alors $\mathrm{Inv}(H_2) \subset \mathrm{Inv}(H_1)$.
- Soient A_1 et A_2 deux parties de K tel que $A_1 \subset A_2$, alors $\mathrm{Gal}(K/A_2) \subset \mathrm{Gal}(K/A_1)$.
- Soit H une partie de $\mathrm{Aut}(K)$, alors $H \subset \mathrm{Gal}(K/\mathrm{Inv}(H))$.
- Soit A une partie de K, alors $A \subset \mathrm{Inv}(\mathrm{Gal}(K/A))$.

Exemples.

1) On a $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.
   En effet, soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, alors σ est entièrement déterminé par $\sigma(\sqrt{2})$. On a

$$\sigma(\sqrt{2})^2 = \sigma(\sqrt{2}^2) = \sigma(2) = 2 \Rightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}.$$

   Ainsi $\sigma(\sqrt{2}) = \sqrt{2} \Rightarrow \sigma = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$ ou $\sigma(\sqrt{2}) = -\sqrt{2}$, et il est clair que $\sigma \circ \sigma = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$.
   Par suite $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$.

2) On a $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$.
   En effet, soit $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, alors σ est entièrement déterminé par $\sigma(i)$. On a

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1 \Rightarrow \sigma(i) = \pm i.$$

   Ainsi $\sigma(i) = i \Rightarrow \sigma = \mathrm{id}_{\mathbb{C}}$ ou $\sigma(i) = -i$, et il est clair que $\sigma \circ \sigma = \mathrm{id}_{\mathbb{C}}$.
   Par suite $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$.

3) Déterminons maintenant $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. Soit σ un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\sqrt[3]{2})$. Alors σ est entièrement déterminé par $\sigma(\sqrt[3]{2})$. On a

$$\sigma(\sqrt[3]{2})^3 = \sigma(\sqrt[3]{2}^3) = \sigma(2) = 2 \Rightarrow \sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}.$$

   Comme $j \notin \mathbb{Q}(\sqrt[3]{2})$, alors $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, ainsi $\sigma = \mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}$.
   Par suite $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\}$.

On note souvent id par 1.

Remarques. Soit K/k une extension algébrique.

- $|\operatorname{Gal}(K/k)| \leq [K:k]_s$.
- Si K/k est finie, alors $|\operatorname{Gal}(K/k)| \leq [K:k]$.
- Si K/k est normale, alors $|\operatorname{Gal}(K/k)| = [K:k]$.
- Si K/k est finie, alors K/k est normale si et seulement si $|\operatorname{Gal}(K/k)| = [K:k]$.

8.2 Extensions galoisiennes

Définition 8.2. Soit K/k une extension de corps commutatifs, on dit que l'extension K/k est galoisienne (finie) [1] si

1) $\operatorname{Gal}(K/k)$ est fini ;

2) $k = \operatorname{Inv}(\operatorname{Gal}(K/k))$.

Proposition 8.1. *Soit K/k une extension de corps commutatifs. Les conditions suivantes sont équivalentes.*

1) *L'extension K/k est galoisienne (finie).*

2) *L'extension K/k est finie, séparable et normale.*

Preuve.
1) $\Rightarrow$ 2) Supposons que l'extension K/k est galoisienne. soient $x \in K$,

$$E = \{\sigma(x) \mid \sigma \in \operatorname{Gal}(K/k)\} \text{ et } Q = \prod_{\alpha \in E} (X - \alpha).$$

Chaque $\sigma \in \operatorname{Gal}(K/k)$ induit un k-automorphisme de

$$\begin{array}{ccc} K[X] & \longrightarrow & K[X] \\ P = \sum\limits_i a_i X^i & \longmapsto & \sigma(P) = \sum\limits_i \sigma(a_i) X^i \end{array}$$

On a E est stable par $\operatorname{Gal}(K/k)$, donc

$$\sigma(Q) = \prod_{\alpha \in E} (X - \sigma(\alpha)) = \prod_{\alpha \in E} (X - \alpha) = Q,$$

Écrivons $Q = \sum\limits_i a_i X^i$, alors

$$\begin{aligned} \sigma(Q) = \sum_i \sigma(a_i) X^i) = \sum_i a_i X^i, \forall\ \sigma \in \operatorname{Gal}(K/k) &\Rightarrow \sigma(a_i) = a_i,\ \forall\ i \in \mathbb{N},\ \forall \sigma \in \operatorname{Gal}(K/k) \\ &\Rightarrow a_i \in k,\ \forall\ i \in \mathbb{N} \\ &\Rightarrow Q \in k[X]. \end{aligned}$$

Comme $x \in E$, alors $Q(x) = 0$, donc x est algébrique sur k, ainsi $\operatorname{Irr}(x/k) \mid Q$. Comme Q est séparable, alors x est séparable sur k. Comme Q est scindé sur $k[X]$, alors $\operatorname{Irr}(x/k)$ l'est aussi. Ceci $\forall\ x \in K$, donc K/k est normale, K/k est séparable et $|\operatorname{Gal}(K/k)| = [K:k]_s$. Comme $\operatorname{Gal}(K/k)$ est finie, alors $[K:k]_s$ l'est aussi. $[K:k]_s$ finie et K/k séparable nous donnent nécessairement que K/k est finie.
2) $\Rightarrow$ 1) Supposons que l'extension K/k est finie, séparable et normale.
On a $[K:k]_s$ est fini, donc $|\operatorname{Gal}(K/k)| = [K:k]_s$ est fini.

1. La définition d'une extension galoisienne diffère d'un auteur à autre. Certains définissent une extension galoisienne entant qu'une extension finie, séparable et normale (comme notre cas ici). Autres définissent une extension galoisienne entant qu'une extension séparable et normale (finie ou infinie).

Soit $x \in \mathrm{Inv}(\mathrm{Gal}(K/k))$, soit Ω une clôture algébrique de K et $\sigma : K \longrightarrow \Omega$ un k-plongement. Comme K/k est normale, alors $\sigma(K) = K$, donc σ est un k-automorphisme de K, ainsi $\sigma \in \mathrm{Gal}(K/k)$. Comme $x \in \mathrm{Inv}(\mathrm{Gal}(K/k))$, alors $\sigma(x) = x$, par suite $\sigma(x) = x$ pour tout $\sigma : K \longrightarrow \Omega$ un k-plongement, ce qui donne que x est purement inséparable sur k. Or K/k est séparable, donc $x \in k$. Ainsi on a $\mathrm{Inv}(\mathrm{Gal}(K/k)) \subset k$ et on a $k \subset \mathrm{Inv}(\mathrm{Gal}(K/k))$, d'où $k = \mathrm{Inv}(\mathrm{Gal}(K/k))$. Donc on a $|\mathrm{Gal}(K/k)|$ est fini et $k = \mathrm{Inv}(\mathrm{Gal}(K/k))$, ce qui veut dire que l'extension K/k est galoisienne. □

Remarques. Soit L une sous-extension d'une extension K/k.

- Si l'extension K/k est galoisienne, alors l'extension K/L est galoisienne.
- Si l'extension K/k est galoisienne, alors on n'a pas nécessairement que l'extension L/k est galoisienne.

  Contre exemple. Soient $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}), K = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(j, \sqrt[3]{2})$. On a K/k est galoisienne mais L/k ne l'est pas.
- Si les deux extensions K/L et L/k sont galoisiennes, alors on n'a pas nécessairement que l'extension K/k est galoisienne.

  Contre exemple. Soient $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}(\sqrt[4]{2})$. On a L/k et K/L sont deux extensions normales mais K/k ne l'est pas.

Proposition 8.2. *Soit K/k une extension finie. Les conditions suivantes sont équivalentes.*

1) *L'extension K/k est galoisienne.*
2) $|\mathrm{Gal}(K/k)| = [K : k]$.

Preuve. On a toujours $|\mathrm{Gal}(K/k)| \leq [K : k]_s \leq [K : k]$. Ainsi

$$|\mathrm{Gal}(K/k)| = [K : k] \Leftrightarrow \begin{cases} |\mathrm{Gal}(K/k)| = [K : k]_s \\ [K : k]_s = [K : k] \end{cases}$$
$$\Leftrightarrow \begin{cases} K/k \text{ est normale} \\ K/k \text{ est séparable} \end{cases}$$

□

Proposition 8.3. *Toute extension finie d'un corps fini k est galoisienne de groupe de Galois cyclique engendré par l'automorphisme $X \longmapsto X^q$ avec $q = \mathrm{card}(k)$.*

Preuve. Soient k un corps fini, $q = \mathrm{card}(k)$ et K/k une extension finie. Alors K/k est séparable et K/k est normale, ainsi K/k est galoisienne.
Soit

$$\sigma : \begin{array}{ccc} K & \longrightarrow & K \\ X & \longmapsto & X^q \end{array} \Rightarrow \sigma^2 :\longmapsto (X^q)^q = X^{q^2}, \ldots, \sigma^m : X \longmapsto X^{q^m}.$$

Si $[K : k] = n$, alors $\mathrm{card}(K) = q^n$, donc $\sigma^n : X \longmapsto X^{q^n} = X$, ainsi $\sigma^n = \mathrm{id}_K$. Soit d l'ordre de σ dans $\mathrm{Gal}(K/k)$, alors $\sigma^d = \mathrm{id}_K$, donc $d \mid n$, or on a

$$\sigma^d = \mathrm{id}_K \Rightarrow \forall\ x \in K,\ x^{q^d} = x \Rightarrow \mathrm{card}(K) \leq q^d \Rightarrow q^n \leq q^d \Rightarrow n \leq d.$$

Par suite $n = d$. □

Proposition 8.4. *Soit K/k une extension fine, alors il existe une plus grande extension parmi les sous-extensions galoisiennes de K/k de la forme N/k.*

Preuve. Soit S la clôture séparable de k dans K et N/k la plus grande sous-extension normale de S/k. On a N/k est galoisienne car elle est finie, séparable et normale. Soit G/k une sous-extension galoisienne de K/k, on a $G \subset S$ car G/k est séparable et $G \subset N$ car G/k est normale. Donc N/k est la plus grande extension parmi les sous-extensions galoisiennes de K/k. □

Proposition 8.5. *Soient E_1/F_1 et E_2/F_2 des sous-extensions d'une extension K/k. Si E_1/F_1 et E_2/F_2 sont galoisiennes, alors l'extension E_1E_2/F_1F_2 est galoisienne.*

8.3 Théorème fondamental de Galois

Théorème 8.6 (**Théorème de préparation**).
Soient K un corps commutatif, G un groupe fini d'automorphisme de K et $k = \mathrm{Inv}(G)$, alors l'extension K/k est galoisienne et $\mathrm{Gal}(K/k) = G$.

Lemme 8.7 (**Lemme de Dedekind**).
Soient K et L deux corps commutatifs, $\sigma_1, \sigma_2, \ldots, \sigma_n$ n plongements deux à deux distincts de K dans L, alors $\sigma_1, \sigma_2, \ldots, \sigma_n$ sont linéairement indépendant sur L.

Remarque.

1) Ce lemme est une autre version de la proposition 0.18.
2) L'indépendance linéaire dans ce cas à lieu au sens de l'espace vectoriel L^K (des applications de $K \longrightarrow L$) sur L.

Preuve. (Preuve du lemme).
Par récurrence sur n. Pour $n = 1$, la propriété est vraie. Supposons que $n > 1$ et que la propriété est vraie pour $n - 1$. Supposons qu'il existe $\alpha_1, \ldots, \alpha_n$ dans L tel que

$$\begin{gathered}
\alpha_1\sigma_1 + \alpha_2\sigma_2 + \ldots + \alpha_n\sigma_n = 0 \qquad (1) \\
\Updownarrow \\
\alpha_1\sigma_1(x) + \alpha_2\sigma_2(x) + \ldots + \alpha_n\sigma_n(x) = 0,\ \forall\ x \in K \\
\Updownarrow \\
\alpha_1\sigma_1(ax) + \alpha_2\sigma_2(ax) + \ldots + \alpha_n\sigma_n(ax) = 0,\ \forall\ x, a \in K \\
\Updownarrow \\
\alpha_1\sigma_1(a)\sigma_1 + \alpha_2\sigma_2(a)\sigma_2 + \ldots + \alpha_n\sigma_n(a)\sigma_n = 0,\ \forall\ a \in K \qquad (2).
\end{gathered}$$

Donc $(2) - \sigma_1(a) \times (1) = 0 \Rightarrow \sum_{i=2}^{n} \alpha_i(\sigma_i(a) - \sigma_1(a))\sigma_i = 0$.
Par hypothèse de récurrence on a $\alpha_i(\sigma_i(a) - \sigma_1(a)) = 0$ pour $i = 2, \ldots, n$.
Pour i fixé dans $[\![2\ ;\ n]\!]$, on a $\sigma_i \neq \sigma_1$, donc il existe $a \in K$ tel que $\sigma_i(a) - \sigma_1(a) \neq 0$, donc $\alpha_i = 0$. Ainsi $\alpha_i = 0, \forall\ i \in [\![2\ ;\ n]\!]$. Il reste donc $\alpha_1\sigma_1 = 0$, ainsi $\alpha_1\sigma_1(1) = \alpha_1 = 0$. Par suite $\alpha_i = 0,\ \forall\ i \in [\![1\ ;\ n]\!]$, ce qui donne que $\sigma_1, \sigma_2, \ldots, \sigma_n$ sont linéairement indépendant sur L. □

Preuve. (Preuve du théorème 8.6).
On a G est fini et $k = \mathrm{Inv}(G)$, donc pour montrer que K/k est galoisienne il suffit de montrer que $G = \mathrm{Gal}(K/k)$.
On sait que $G \subset \mathrm{Gal}(K/k)$. Soient $x \in K$ et $y = \sum_{h \in G} h(x)$. Pour $\tau \in G$ on a

$$\tau(y) = \sum_{h \in G} (\tau h)(x) = y \Rightarrow y \in \mathrm{Inv}(G) = k \Rightarrow \sigma(y) = y,\ \forall\ \sigma \in \mathrm{Gal}(K/k).$$

Or

$$\sigma(y) = \sum_{h \in G} (\sigma h)(x) = \sum_{h \in G} h(x) \Rightarrow \left(\sum_{h \in G} \sigma h - \sum_{h \in G} h \right)(x) = 0,\ (\forall\ x \in K) \Rightarrow \sum_{h \in G} \sigma h - \sum_{h \in G} h = 0.$$

Supposons que G est d'ordre n et écrivons $G = \{h_1, \ldots, h_n\}$, alors $\sigma G = \{h_{n+1}, \ldots, h_{2n}\}$.
Si $\sigma \in \mathrm{Gal}(K/k) \setminus G$, alors $(\sigma G) \cap G = \emptyset$, donc les h_i sont deux à deux distincts et

$$-h_1 - h_2 - \ldots - h_n + h_{n+1} + \ldots + h_{2n} = 0,$$

ce qui contredit le lemme de Dedekind. Ainsi $G = \mathrm{Gal}(K/k)$. □

Théorème 8.8 (**Théorème fondamental de Galois**).
Soient K/k une extension galoisienne finie, $\mathcal{L}$ l'ensemble des corps intermédiaires de K/k et $\mathcal{H}$ l'ensemble des sous-groupes de $\mathrm{Gal}(K/k)$*, alors les applications*

$$\begin{array}{rccc} \varphi: & \mathcal{L} & \longrightarrow & \mathcal{H} \\ & L & \longmapsto & \mathrm{Gal}(K/L) \end{array} \quad et \quad \begin{array}{rccc} \psi: & \mathcal{H} & \longrightarrow & \mathcal{L} \\ & H & \longmapsto & \mathrm{Inv}(H) \end{array}$$

sont décroissantes (pour l'inclusion), bijectives et réciproques l'une à l'autre.
De plus pour $L \in \mathcal{L}$, L/k est galoisienne si et seulement si $\mathrm{Gal}(K/L)$ *est distingué dans* $\mathrm{Gal}(K/k)$*, auquel cas on a un isomorphisme*

$$\begin{array}{ccccc} \mathrm{Gal}(K/k)/\mathrm{Gal}(K/L) & \longrightarrow & \mathrm{Gal}(L/k) & & \\ \overline{\sigma} & \longmapsto & \tilde{\sigma} & & (x \mapsto \sigma(x)) \end{array}$$

Preuve. Soient $L \in \mathcal{L}$ et $H \in \mathcal{H}$, alors, par le théorème 8.6,

$$\psi(\varphi(L)) = \mathrm{Inv}(\mathrm{Gal}(K/L)) = L \text{ et } \varphi(\psi(H)) = \mathrm{Gal}(K/\mathrm{Inv}(H)) = H,$$

donc ψ et φ sont bijectives et réciproques l'une de l'autre.
Soit $L \in \mathcal{L}$, si $\mathrm{Gal}(K/L) \lhd \mathrm{Gal}(K/k)$, montrons que L/k est galoisienne, pour ceci, il suffit de montrer que L/k est normale.
Soit Ω une clôture algébrique de K, $\sigma : L \longrightarrow \Omega$ un k-plongement, $\hat{\sigma} : K \longrightarrow \Omega$ un k-plongement prolongeant σ. Comme K/k est normale, alors $\hat{\sigma}(K) = K$, donc $\hat{\sigma}$ induit $\tilde{\sigma} \in \mathrm{Gal}(K/k)$ ($\tilde{\sigma} : x \mapsto \sigma(x)$). Soit $x \in L$, alors

$$\begin{aligned} \sigma(x) \in L &\Leftrightarrow \forall\ \tau \in \mathrm{Gal}(K/L),\ \tau(\sigma(x)) = \sigma(x) \\ &\Leftrightarrow \forall\ \tau \in \mathrm{Gal}(K/L),\ \tau(\tilde{\sigma}(x)) = \tilde{\sigma}(x) \\ &\Leftrightarrow \forall\ \tau \in \mathrm{Gal}(K/L),\ \tilde{\sigma}^{-1} \circ \tau \circ \tilde{\sigma}(x) = x. \end{aligned}$$

Comme $\mathrm{Gal}(K/L) \lhd \mathrm{Gal}(K/k)$, alors $\forall\ \tau \in \mathrm{Gal}(K/L),\ \tilde{\sigma}^{-1} \circ \tau \circ \tilde{\sigma} \in \mathrm{Gal}(K/L)$, donc

$$\forall\ \tau \in \mathrm{Gal}(K/L),\ \tilde{\sigma}^{-1} \circ \tau \circ \tilde{\sigma}(x) = x \Rightarrow \sigma(x) \in L,$$

par suite $\sigma(L) = L$, donc L/k est normale, ainsi L/k est galoisienne.
Inversement, supposons que L/k est galoisienne et soit

$$\begin{array}{rccccc} h: & \mathrm{Gal}(K/k) & \longrightarrow & \mathrm{Gal}(L/k) & & \\ & \sigma & \longmapsto & \tilde{\sigma} & & (\tilde{\sigma} : x \mapsto \sigma(x)). \end{array}$$

- h est bien définie (car L/k est normale).
- h est un homomorphisme de groupe. En effet, soient $\sigma, \tau \in \mathrm{Gal}(K/k)$, donc pour $x \in L$, on a

  $$\widetilde{\sigma \circ \tau}(x) = \sigma \circ \tau(x) = \sigma(\tau(x)) = \sigma(\hat{\tau}(x)) = \tilde{\sigma}(\hat{\tau}(x)) \text{ (car } \tilde{\tau}(x) \in L) = \tilde{\sigma} \circ \tilde{\tau}(x),$$

  ainsi $\widetilde{\sigma \circ \tau} = \tilde{\sigma} \circ \tilde{\tau}$.
- $\mathrm{Im}(h) = \mathrm{Gal}(L/k)$ (Théorème de prolongement).
- $\ker(h) = \{\sigma \in \mathrm{Gal}(K/k) \mid \tilde{\sigma} = \mathrm{id}_L\} = \{\sigma \in \mathrm{Gal}(K/k) \mid \sigma \in \mathrm{Gal}(K/L)\} = \mathrm{Gal}(K/L)$, donc $\mathrm{Gal}(K/L) \lhd \mathrm{Gal}(K/k)$ (Le noyau d'un homomorphisme de groupes est un sous-groupe distingué du groupe de départ), et on a un isomorphisme canonique

  $$\begin{array}{ccccc} \mathrm{Gal}(K/k)/\mathrm{Gal}(K/L) & \longrightarrow & \mathrm{Gal}(L/k). & & \\ \overline{\sigma} & \longmapsto & \tilde{\sigma} & & \end{array}$$

□

Remarques.

- Dans la preuve du théorème 8.8, si on suppose que K/k est seulement normale, on a toujours si L/k est normale, alors $\mathrm{Gal}(K/L) \lhd \mathrm{Gal}(K/k)$, et on a un isomorphisme canonique $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L) \simeq \mathrm{Gal}(L/k)$.
- Lorsque K/k est une extension galoisienne infinie, la correspondance de Galois se fait avec les sous-groupes fermés de $\mathrm{Gal}(K/k)$, pour une certaine topologie, qui est la topologie triviale lorsque l'extension est finie. Le lecteur curieux pourra consulter par exemple [1, Chapitre 5].

8.4 Groupe de Galois et extension produit

Proposition 8.9. *Soient E et F des sous-extensions galoisiennes finies d'une extension K/k, alors l'application*

$$\begin{array}{rccccc} f: & \mathrm{Gal}(EF/k) & \longrightarrow & \mathrm{Gal}(E/k)\times\mathrm{Gal}(F/k) & & \\ & \sigma & \longmapsto & (\tilde{\sigma}_1,\ \tilde{\sigma}_2) & & (\tilde{\sigma}_i : x\mapsto\sigma(x)) \end{array}$$

est un homomorphisme injectif de groupes. C'est un isomorphisme si et seulement si E et F sont k-linéairement disjoints.

Preuve.

- f est bien définie (Théorème 8.8)
- f est un homomorphisme de groupe (car chaque application $\sigma\mapsto\tilde{\sigma}_i$ $(i=1,2)$ l'est (Théorème 8.8)).
- f est injective. En effet, soit $\sigma\in\mathrm{Gal}(EF/k)$ tel que

  $$f(\sigma)=(\tilde{\sigma}_1,\ \tilde{\sigma}_2)=(\mathrm{id}_E,\mathrm{id}_F),\ L=\{x\in EF\mid\sigma(x)=x\},$$

  alors L est un sous-corps de EF. Or $E,F\subset L$, donc $EF\subset L$, ainsi $L=EF$, donc $\sigma=\mathrm{id}_{EF}$, par suite l'application est injective.
- Comme $\mathrm{Gal}(E/k)\times\mathrm{Gal}(F/k)$ est fini, alors

  $$\begin{aligned} f \text{ est bijective} &\Leftrightarrow |\mathrm{Gal}(EF/k)| = |\mathrm{Gal}(E/k)|\times|\mathrm{Gal}(F/k)| \\ &\Leftrightarrow [EF:k]=[E:k]\times[F:k] \\ &\Leftrightarrow E \text{ et } F \text{ sont } k\text{-linéairement disjoints.} \end{aligned}$$

□

Remarque. La proposition 8.9 donne des informations sur le groupe $\mathrm{Gal}(EF/k)$ connaissant $\mathrm{Gal}(E/k)$ et $\mathrm{Gal}(F/k)$.

Exemple. Si $\mathrm{Gal}(E/k)$ et $\mathrm{Gal}(F/k)$ sont abéliens, alors $\mathrm{Gal}(EF/k)$ est abélien.

Proposition 8.10. *Soient E et F des sous-extensions d'une extension K/k avec l'extension E/k est galoisienne finie, alors l'application*

$$\begin{array}{rccccc} & \mathrm{Gal}(EF/F) & \longrightarrow & \mathrm{Gal}(E/k) & & \\ & \sigma & \longmapsto & \tilde{\sigma} & & (\tilde{\sigma} : x\mapsto\sigma(x)) \end{array}$$

est un homomorphisme injectif de groupes. C'est un isomorphisme si et seulement si E et F sont k-linéairement disjoints.

Preuve. Analogue à la preuve de la proposition 8.9. □

Remarque. La proposition 8.9 donne des informations sur le groupe $\mathrm{Gal}(EF/F)$ connaissant $\mathrm{Gal}(E/k)$.

Proposition 8.11. *Soient E_1/F_1 et E_2/F_2 des sous-extensions galoisiennes finies d'une extension K/k, alors l'application*

$$\begin{array}{rccccc} & \mathrm{Gal}(E_1E_2/F_1F_2) & \longrightarrow & \mathrm{Gal}(E_1/F_1)\times\mathrm{Gal}(E_2/F_2) & & \\ & \sigma & \longmapsto & (\tilde{\sigma}_1,\tilde{\sigma}_2) & & (\tilde{\sigma}_i : x\mapsto\sigma(x)) \end{array}$$

est un homomorphisme injectif de groupe.

Chapitre 9

Équations résolubles par radicaux

9.1 Extensions cyclotomiques

Définition 9.1. Soient k un corps, $n \in \mathbb{N}^*$ et $\zeta \in k$. On dit que

- ζ est une racine n-ième de l'unité si $\zeta^n = 1$.
- ζ est une racine primitive n-ième de l'unité si ζ est d'ordre n dans le groupe multiplicatif k^* de k.

Remarque. Soient k un corps commutatif et $n \in \mathbb{N}^*$. Si k contient une racine primitive n-ième de l'unité ζ, alors k contient toutes les racines n-ièmes de l'unité.

Proposition 9.1. *Soient k un corps, $p = \mathrm{car}(k)$, $n \in \mathbb{N}^*$, $\Phi_n(X)$ le n-ième polynôme cyclotomique de k et $\zeta \in k$, alors il est équivalent de dire*

1) *ζ est une racine primitive n-ième de l'unité.*

2) *$\Phi_n(\zeta) = 0$ et $p \nmid n$.*

Preuve.
1) $\Rightarrow$ 2) Supposons qu'on a (1), alors

$$\zeta^n - 1 = \prod_{d|n} \Phi_d(\zeta) = 0 \Rightarrow \exists\ d \mid n \text{ tel que } \Phi_d(\zeta) = 0 \Rightarrow \zeta^d - 1 = \prod_{d'|d} \Phi_{d'}(\zeta) = 0 \Rightarrow n \mid d,$$

ainsi $n = d$ et $\Phi_n(\zeta) = 0$.
Et $p \nmid n$, car sinon $\zeta^n = (\zeta^{n/p})^p = 1 \Rightarrow (\zeta^{n/p} - 1)^p = 0 \Rightarrow \zeta^{n/p} = 1 \Rightarrow n \mid \frac{n}{p}$, ce qui impossible.
2) $\Rightarrow$ 1) Supposons qu'on a (2), on a $\zeta^n - 1 = \prod_{d|n} \Phi_d(\zeta) = 0$, soit d l'ordre de ζ dans k^*, en utilisant l'implication 1) $\Rightarrow$ 2), on a $\Phi_d(\zeta) = 0$, $p \nmid d$ et $d \mid n$ car $\zeta^n = 1$. Si on suppose que $d < n$, alors ζ est une racine double de $X^n - 1 = \prod_{d|n} \Phi_d(X)$, donc $(X^n - 1)'(\zeta) = n\zeta^{n-1} = 0$, puisque $n \neq 0$ (car $p \nmid n$), donc $\zeta^{n-1} = 0$, ainsi $\zeta = 0$, ce qui n'est pas le cas car $\zeta^n = 1$, ainsi $n = d$. □

Remarque. Supposons que $n = mp^s$ avec $p = \mathrm{car}(k)$ et $p \nmid m$, alors

$$\zeta^n = (\zeta^m)^{p^s} = 1 \Leftrightarrow \zeta^m = 1 \ (\text{car } p = \mathrm{car}(k),\ \text{donc } x^p = 1 \Leftrightarrow x = 1).$$

On peut convenir d'appeler racine primitive n-ième de l'unité tout $\zeta \in k$ d'ordre m dans k^* et on a toujours ζ est une racine primitive de l'unité si et seulement si $\Phi_n(\zeta) = 0$.

$$\Phi_{mp^s}(X) = \frac{\Phi_m(X^{p^s})}{\Phi_m(X^{p^{s-1}})} = (\Phi_m(X))^{p^s - p^{s-1}}.$$

Proposition 9.2. *Soient k un corps commutatif, $n \in \mathbb{N}^*$, l'ensemble des racines n-ième de l'unité de k est un sous-groupe cyclique de k^* d'ordre un diviseur de n.*

Preuve. Posons $\mathcal{U} = \{x \in k \mid x^n = 1\}$, on a $\forall\ x \in \mathcal{U},\ x^n = 1$, ainsi $|\mathcal{U}| \leqslant n$. Soit $d = |\mathcal{U}|$, alors $\forall\ x \in \mathcal{U},\ x^d = 1$, ainsi $P = X^d - 1$ est scindé sur $\mathcal{U}$, par suite $\Phi_d(X)$ est aussi scindé sur $\mathcal{U}$. Soit $\zeta \in \mathcal{U}$ tel que $\Phi_d(\zeta) = 0$, on a si $p = \mathrm{car}(k)$, alors $p \nmid d$, sinon $\forall\ x \in \mathcal{U},\ x^{d/p} = 1 \Rightarrow |\mathcal{U}| \leqslant \frac{d}{p} \Rightarrow d \leqslant \frac{d}{p}$, ce qui est impossible, ainsi ζ est d'ordre d, par suite $\mathcal{U} = \langle\zeta\rangle$ est cyclique d'ordre d et $d \mid n$ (car $\zeta^n = 1$). □

Remarque. La proposition 9.2 n'est pas vraie sans l'hypothèse que k est commutatif.

Contre exemple. Soit $\mathbb{H}$ le corps des quaternions :

$$\mathbb{H} = \mathbb{R}(i, j, k) \text{ tel que } i^2 = j^2 = k^2 = -1,\ ij = k = -ji,\ jk = i = -kj,\ ki = j = -ik.$$

Soit $\theta \in \mathbb{R},\ \varphi_\theta = \cos(\theta)i + \sin(\theta)j$, on a $\varphi_\theta^2 = -1$, donc $\varphi_\theta^4 = 1$, par suite $\{\varphi \in \mathbb{H} \mid \varphi^4 = 1\}$ est infini.

Définition 9.2. Une extension K/k est dite cyclotomique, s'il existe $n \in \mathbb{N}^*$ et $\zeta \in K$ tel que $K = k(\zeta)$ et $\zeta^n = 1$.

Remarque. On peut toujours prendre ζ une racine primitive n-ième de l'unité.

Proposition 9.3. *Soit K/k une extension cyclotomique, $K = k(\zeta)$ avec ζ une racine primitive n-ième de l'unité. Alors, l'extension K/k est galoisienne de groupe de Galois abélien et canoniquement isomorphe à un sous-groupe du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{m} \mid \mathrm{pgcd}(m, n) = 1\}$.*

Preuve. Soit $P = X^n - 1$. Comme ζ est d'ordre n, alors $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ sont des racines distinctes de P, donc P est scindé, et donc séparable, ainsi K/k est séparable. L'extension K/k est normale car K est un corps de décomposition de P. Comme K/k est finie, alors c'est une extension galoisienne.
Soit $\sigma \in \mathrm{Gal}(K/k)$, alors $\sigma(\zeta)$ est d'ordre n et est une racine de P, par suite $\sigma(\zeta) \in \langle\zeta\rangle$ et $\sigma(\zeta) = \zeta^{n_\sigma}$ avec $\mathrm{pgcd}(n\sigma, n) = 1$.
Soit

$$\begin{array}{rccc} \varphi : & \mathrm{Gal}(K/k) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ & \sigma & \longmapsto & \overline{n}_\sigma \end{array}$$

- φ est bien définie (car $\sigma(\zeta) = \zeta^{n_\sigma} = \zeta^m \Rightarrow \overline{n}_\sigma = \overline{m}$).
- φ est un homomorphisme de groupe. En effet, pour $\sigma,\ \tau \in \mathrm{Gal}(K/k)$ on a

  $$\sigma \circ \tau(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{n_\tau}) = (\zeta^{n_\tau})^{n_\sigma} = \zeta^{n_\sigma n_\tau},$$

  donc $\overline{n}_{\sigma\circ\tau} = \overline{n}_\sigma \cdot \overline{n}_\tau$.
- φ est injectif. En effet, soit $\sigma \in \mathrm{Gal}(K/k)$ tel que $\varphi(\sigma) = \overline{1}$, alors

  $$\varphi(\sigma) = \overline{1} \Rightarrow \overline{n}_\sigma = \overline{1} \Rightarrow \sigma(\zeta) = \zeta \Rightarrow \sigma(P(\zeta)) = P(\zeta), \forall\ P \in k[X] \Rightarrow \sigma = \mathrm{id}_K\,.$$

  Ainsi $\mathrm{Gal}(K/k)$ est isomorphe à un sous-groupe du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

□

Proposition 9.4. *Soit K/k une extension cyclotomique, $K = k(\zeta)$ avec ζ une racine primitive n-ième de l'unité. Alors, pour que $\mathrm{Gal}(K/k)$ soit isomorphe au groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ il faut et il suffit que le n-ième polynôme cyclotomique $\Phi_n(X)$ de k soit irréductible dans $k[X]$.*

Preuve.

$$\begin{aligned} \text{L'homomorphisme } \varphi \text{ est bijectif} &\Leftrightarrow |\mathrm{Gal}(K/k)| = |(\mathbb{Z}/n\mathbb{Z})^*| \\ &\Leftrightarrow [K : k] = \deg(\Phi_n) \\ &\Leftrightarrow \deg(\zeta/k) = \deg(\Phi_n) \\ &\Leftrightarrow \mathrm{Irr}(\zeta/k) = \Phi_n. \end{aligned}$$

□

Proposition 9.5. *Soit $n \in \mathbb{N}^*$, alors le n-ième polynôme cyclotomique Φ_n est irréductible dans $\mathbb{Z}[X]$.*

Preuve. Soit ζ une racine primitive n-ième de l'unité dans $\mathbb{C}$. Notons $f(X) = \mathrm{Irr}(\zeta/\mathbb{Q})(X)$. Clairement $f(X)$ divise $X^n - 1$ dans $\mathbb{Q}[X]$:

$$X^n - 1 = f(X)h(X),\ h(X) \in \mathbb{Q}[X].$$

$X^n - 1 \in \mathbb{Z}[X]$ et $f(X)$ étant unitaires, donc $h(X) \in \mathbb{Z}[X]$.

- Montrons que si u est une racine de f, et p un nombre premier ne divisant pas n, alors u^p est aussi racine de f.

  Comme $f(X)$ divise $X^n - 1$ dans $\mathbb{Q}[X]$, on a $u^n - 1 = 0$. u est une racine n-ième de l'unité dans $\mathbb{C}$, donc u^p aussi :

  $$0 = (u^p)^n - 1 = f(u^p)h(u^p).$$

  Supposons $f(u^p) \neq 0$, alors $h(u^p) = 0$. Or u est racine de f irréductible dans $\mathbb{Q}[X]$, donc $f = \mathrm{Irr}(u/\mathbb{Q})$. Donc $f(X)$ divise $h(X^p)$ dans $\mathbb{Q}[X]$:

  $$h(X^p) = f(X)g(X),\ g(X) \in \mathbb{Q}[X].$$

  Comme $h(X^p) \in \mathbb{Z}[X]$ et $f(X)$ étant unitaires, alors $g(X) \in \mathbb{Z}[X]$. Réduisons modulo p l'égalité : $h(X^p) = f(X)g(X)$. Il vient :

  $$(\overline{h}(X))^p = \overline{h(X^p)} = \overline{f}(X)\overline{g}(X) \text{ dans } \mathbb{F}_p[X].$$

  Soit $\theta \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{f}$. Alors θ divise $\overline{h}^p$, donc divise $\overline{h}$ dans $\mathbb{F}_p[X]$, donc θ^2 divise $\overline{fh} = X^n - \overline{1}$ dans $\mathbb{F}_p[X]$. Par-conséquent $X^n - \overline{1} \in \mathbb{F}_p[X]$ possède une racine double dans une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$, ce qui est absurde. Ainsi $f(u^p) = 0$.
- Comme ζ est racine de f, et comme toute racine primitive n-ième de l'unité dans $\mathbb{C}$, c'est-à-dire toute ζ^k où k premier avec n, peut être obtenue par élévations successives de ζ à des puissances p, où p premier ne divise pas n ; le résultat précédent montre que toute racine primitive n-ième de l'unité dans $\mathbb{C}$ est racine de f. Donc $\deg(f) \geq \varphi(n)$. Or $f(X)$ divise $\Phi_n(X)$ dans $\mathbb{Q}[X]$, $\deg(\Phi_n) = \varphi(n)$, et f et Φ_n sont tous deux unitaires. Donc $\Phi_n(X) = f(X) = \mathrm{Irr}(\zeta/\mathbb{Q})(X)$. Donc $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

□

Remarques. La dérivée de $X^n - 1$ est nX^{n-1}.

- Si $\mathrm{car}(K) = 0$, alors la seule racine de nX^{n-1} est 0, qui n'annule pas $X^n - 1$, donc $X^n - 1$ est séparable.
- Si $\mathrm{car}(K) = p$ (premier), alors
  - ▷ ou bien $p \nmid n$ et alors $X^n - 1$ est séparable ;
  - ▷ ou bien $p \mid n$ et alors notant $n = p^k n'$ avec n' premier à p, on a par la formule du binôme $X^n - 1 = (X^{n'} - l)^{p^k}$, et $X^n - 1$ n'est pas séparable.
- Si $p \nmid n$, alors $X^n - \overline{1}$ est premier avec sa dérivée nX^{n-1} dans $\mathbb{F}_p[X]$ car

$$\frac{1}{\overline{n}} X \overline{n} X^{n-1} - (X^n - \overline{1}) = 1. \text{(théorème de Bezout)}$$

Théorème 9.6 (Théorème 90 de Hilbert)**.**
Soit L/K une extension galoisienne de degré n, avec $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ est cyclique. Pour $x \in L$, les conditions suivantes sont équivalentes :

1) $N_{L/K}(x) = 1$;

2) *Il existe $y \in L^*$ tel que $x = \frac{y}{\sigma(y)}$.*

Preuve. L/K est séparable et normale de degré n, donc $\forall\ \ell \in L,\ N_{L/K}(\ell) = \prod_{i=0}^{n-1} \sigma^i(\ell)$.
2) $\Rightarrow$ 1) Trivial.
2) $\Rightarrow$ 1) Soit $x \in L$ tel que $N_{L/K}(x) = 1$. Considérons la suite $(e_i)_{i\in\mathbb{N}}$ d'éléments de L définie par :

$$\forall\ i \in \mathbb{N}, e_i = \prod_{q=0}^{i} \sigma^q(x) = x\sigma(x)\dots\sigma^i(x).$$

Posons

$$t = e_0\,\mathrm{id}_L + e_1\sigma + ... + e_{n-1}\sigma^{n-1}.$$

Comme σ est d'ordre n, les K-automorphismes $\mathrm{id}_L, \sigma, \dots, \sigma^{n-1}$ sont distincts. Donc $(\mathrm{id}_L, \sigma, \dots, \sigma^{n-1})$ est une famille L-linéairement indépendante. Comme $e_0 = x \neq 0$, on a donc $t \neq 0$. Donc il existe $z \in L^*$ tel que $t(z) \neq 0$. Posons $y = t(z)$. Clairement $(\forall\ i \in \mathbb{N}, x\sigma(e_i) = e_{i+1})$, par conséquent :

$$\begin{aligned} x\sigma(y) = x\sigma(t(z)) &= x\sigma(\sum_{i=0}^{n-1} e_i\sigma^i(z)) \\ &= \sum_{i=0}^{n-1} x\sigma(e_i)\sigma^{i+1}(z) \\ &= \sum_{i=0}^{n-1} e_{i+1}\sigma^{i+1}(z) \\ &= \sum_{i=1}^{n} e_i\sigma^i(z) \\ &= t(z) - e_0z + e_n\sigma^n(z) = y - e_0z + e_n\sigma^n(z). \end{aligned}$$

Or $e_{n-1} = N_{L/K}(x) = 1$ et $\sigma^n = \mathrm{id}_L$, donc $e_n = e_{n-1}\sigma^n(x) = x = e_0$, et $\sigma^n(z) = z$, donc $x\sigma(y) = y$. Or on a $y \neq 0$ et $\sigma \in \mathrm{Gal}(L/K)$ est injectif, donc $\sigma(y) \neq 0$. Ainsi $x = \frac{y}{\sigma(y)}$. □

Théorème 9.7 (Artin-Schreier (première partie))**.**
Soient K un corps de caractéristique p (premier) et $a \in K$. Alors, ou bien le polynôme $P(X) = X^p - X - a$ a une racine dans K, et alors il est scindé sur K ; ou bien il est irréductible sur K. Dans ce dernier cas, notant c une racine dans K de ce polynôme, $K(c)/K$ est une extension galoisienne de groupe de Galois $\mathrm{Gal}(K(c)/K)$ cyclique d'ordre p.

Remarque. Si $K = \mathbb{F}_p$ et $a \neq 0$, on a $\forall\ x \in K, P(x) = -a \neq 0$, donc nous sommes dans le cas où le polynôme $P(X)$ est irréductible sur K. On peut donc énoncer : $X^p - X - 1$ est irréductible dans $\mathbb{Z}[X]$ pour tout premier p.

Preuve.

- Soit c une racine de $P(X)$. Comme $\mathrm{car}(K) = p$, on voit que les $c + i, 0 \leq i \leq p-1$, sont distincts, et qu'ils sont aussi racines de $P(X)$. Donc $P(X)$ a p racines distinctes, et si l'une est dans K, elles sont toutes dans K.
- Supposons que $P(X)$ n'a pas de racine dans K.
  ▷ Supposons que $P(X)$ est réductible sur K :

  $$P(X) = Q(X)R(X), 1 \leq \deg(Q), \deg(R) \leq p.$$

  Soit Ω une clôture algébrique K, alors

  $$P(X) = \prod_{i=0}^{p-1}(X-c-i) \text{ et } Q(X) = \prod_{j=0}^{d-1}(X-c-\alpha_j) \text{ dans } \Omega[X] \text{ avec } d = \deg(Q),\ 0 \leq \alpha_j \leq p-1.$$

  Le coefficient de degré $d-1$ de $Q(X)$ est donc

  $$-(dc + \alpha_0 + \ldots + \alpha_{d-1}) = -(dc + z) \in K,\ \text{où } z \in \mathbb{Z},$$

donc $dc \in K$. Comme $1 \leq d \leq p$, il vient $c = d^{-1}dc \in K$, contradiction. Ainsi $P(X)$ est irréductible dans $K[X]$.

▷ $K(c)$ est le corps des racines sur K de $P(X)$, qui est séparable, donc $K(c)/K$ est galoisienne. Comme $P(X)$ est irréductible sur K, $P = \mathrm{Irr}(c/K)$, donc $[K(c) : K] = \deg(P) = p$, ainsi $|\operatorname{Gal}(K(c)/K)| = p$, par suite, $\operatorname{Gal}(K(c)/K)$ est cyclique.

□

Théorème 9.8 (Théorème 90 de Hilbert, forme additive)**.**
Soit L/K une extension galoisienne de degré n, avec $\operatorname{Gal}(L/K) = \langle\sigma\rangle$ est cyclique. Pour $x \in L$, les conditions suivantes sont équivalentes :

1) $tr_{L/K}(x) = 0$;

2) Il existe $y \in L$ tel que $x = y - \sigma(y)$.

Preuve. L/K est séparable et normale de degré n, donc $\forall\ \ell \in L,\ tr_{L/K}(\ell) = \sum_{i=0}^{n-1} \sigma^i(\ell)$.
2) $\Rightarrow$ 1) Trivial.
2) $\Rightarrow$ 1) Soit $x \in L$ tel que $tr_{L/K}(x) = 0$. Considérons la suite $(d_i)_{i\in\mathbb{N}}$ d'éléments de L définie par :

$$\forall\ i \in \mathbb{N}, d_i = \sum_{q=0}^{i} \sigma^q(x) = x + \sigma(x) + \ldots + \sigma^i(x).$$

Posons

$$u = d_0\sigma + d_1\sigma^2 + ... + d_{n-2}\sigma^{n-1}.$$

Comme σ est d'ordre n, les K-automorphismes $\mathrm{id}_L, \sigma, \ldots, \sigma^{n-1}$ sont distincts, donc est une famille L-linéairement indépendante. Donc $tr_{L/K} = \sum_{q=0}^{n-1} \sigma^q \neq 0$. Donc il existe $z \in L^*$ tel que $tr_{L/K}(z) \neq 0$. Posons $y = \frac{t(z)}{tr_{L/K}(z)}$.

$$\begin{aligned} y - \sigma(y) &= \frac{1}{tr_{L/K}(z)}(u(z) - \sigma(u(z))) \\ &= \frac{1}{tr_{L/K}(z)}\left(d_0\sigma(z) + \sum_{i=1}^{n-2}(d_i - \sigma(d_{i-1}))\sigma^{i+1}(z) - \sigma(d_{n-2})\sigma(z)\right). \end{aligned}$$

Comme $\sigma(d_i) = d_{i+1} - x, \forall\ i \in \mathbb{N}$, alors

$$y - \sigma(y) = \frac{1}{tr_{L/K}(z)}\left(x\sum_{j=1}^{n}\sigma^j(z) - d_{n-1}\sigma^n(z)\right).$$

Or $d_{n-1} = tr_{L/K}(x) = 0$ et $\sigma^n = \mathrm{id}_L$, donc

$$y - \sigma(y) = \frac{1}{tr_{L/K}(z)}x\sum_{j=0}^{n-1}\sigma^j(z) = x.$$

□

Théorème 9.9 (Artin-Schreier (seconde partie))**.**
Soit K un corps de caractéristique p (premier). Soit L une extension galoisienne de degré p de K. Alors il existe $c \in L$ tel que $L = K(c)$ et $c^p - c \in K$.

Preuve. Soit σ un générateur du groupe cyclique $\operatorname{Gal}(L/K)$. On a

$$1 \in K \Rightarrow tr_{L/K}(1) = [L : K]1 = pl = 0.$$

Par conséquent, d'après le théorème 90 de Hilbert, $\exists c \in L : \sigma(c) - c = 1$. Alors, $\forall\, i \in \mathbb{N}, \sigma^i(c) = c + i1$, donc les $\sigma^j(c), 0 \leq j \leq p-1$, sont tous distincts. Par conséquent, comme il les a tous pour racines, le polynôme minimal de c est de degré $\geq p$, soit $[K(c) : K] = \deg(\mathrm{Irr}(c/K)) \geq p$. Comme $[L : K] = p$, i1 vient $K(c) = L$. Et

$$\sigma(c^p - c) = (\sigma(c))^p - \sigma(c) = (c+1)^p - (c+1) = c^p - c \Rightarrow c^p - c \in \mathrm{Inv}(\mathrm{Gal}(L/K)) = K.$$

□

9.2 Extension par radical

Définition 9.3. Une extension K/k est dit par radical s'il existe $n \in \mathbb{N}^*$ et $\theta \in K$ tel que $K = k(\theta)$ et $\theta^n \in k$.

Proposition 9.10. *Soient K/k une extension et $n \in \mathbb{N}^*$. On suppose que k contient les racines n-ièmes de l'unité. Alors, les propriétés suivantes sont équivalentes.*

1) K/k est galoisienne à groupe de Galois cyclique d'ordre divisant n.

2) $K = k(\theta)$ avec $\mathrm{Irr}(\theta/k) = X^d - a$ et d un diviseur de n.

3) $K = k(\theta)$ avec $\theta^n \in k$.

Preuve.
1) $\Rightarrow$ 2) Supposons qu'on a (1). Soient $d = |\mathrm{Gal}(K/k)|$ et σ un générateur de $\mathrm{Gal}(K/k)$. Comme k contient les racines n-ièmes de l'unité, il contient les racines d-ièmes de l'unité. Soit ζ une racine primitive d-ième de l'unité, par le lemme de Dedekind, il existe $x \in K$ tel que $\theta = \sum_{i=0}^{d-1} \zeta^{-i}\sigma^i(x) \neq 0$. On a

$$\sigma(\theta) = \sum_{i=0}^{d-1} \zeta^{-i}\sigma^{i+1}(x) \Rightarrow \sigma(\theta) = \zeta\theta \Rightarrow \sigma^2(\theta) = \zeta^2\theta \ldots \Rightarrow \sigma^{d-1}(\theta) = \zeta^{d-1}\theta.$$

Comme θ a d conjugués deux à deux distincts, alors $\deg(\theta/k) \geq d$. Or $[K : k] = d$ et $\theta \in K$, alors $\deg(\theta/k) = d$, ainsi $K = k(\theta)$. Comme $\sigma(\theta^d) = (\zeta\theta)^d = \theta^d$, alors $\theta \in \mathrm{Inv}(\mathrm{Gal}(K/k)) = k$. Posons $\theta^d = a \in k$, $K = k(\theta)$ avec $\mathrm{Irr}(\theta/k) = X^d - a$ et d un diviseur de n.
2) $\Rightarrow$ 3) Trivial.
3) $\Rightarrow$ 1) Supposons qu'on a (3). Soient $P = X^n - \theta^n$ et $\zeta \in k$ une racine primitive n-ième de l'unité. On a

$$P = X^n - \theta^n = \prod_{i=0}^{n-1}(X - \zeta^i\theta),$$

donc P est scindé sur K et P est séparable (car P a que des racines simples). On a $K = k(\theta) = k(\theta, \zeta\theta, \zeta^2\theta, \ldots)$ est un corps de décomposition de P, donc K/k est normale. L'extension K/k est séparable car P l'est. Comme K/k est finie, alors K/k est galoisienne. Soit $\sigma \in \mathrm{Gal}(K/k)$, alors $\sigma(\theta)$ est aussi racine de P, donc $\sigma(\theta) = \zeta^i\theta$. Soit

$$\begin{array}{rccc} \varphi : & \mathrm{Gal}(K/k) & \longrightarrow & \{x \in k \mid x^n = 1\} \\ & \sigma & \longmapsto & \frac{\sigma(\theta)}{\theta} \end{array}$$

- φ est un homomorphisme de groupe. En effet, soient $\sigma, \tau \in \mathrm{Gal}(K/k)$, alors

$$\varphi(\sigma \circ \tau) = \frac{\sigma \circ \tau(\theta)}{\theta} = \frac{\sigma(\tau(\theta))}{\sigma(\theta)} \cdot \frac{\sigma(\theta)}{\theta} = \sigma(\frac{\tau(\theta)}{\theta}) \cdot \frac{\sigma(\theta)}{\theta} = \frac{\tau(\theta)}{\theta} \cdot \frac{\sigma(\theta)}{\theta} = \varphi(\tau) \cdot \varphi(\sigma).$$

- φ est injectif. En effet, soient $\sigma \in \mathrm{Gal}(K/k)$ tel que $\varphi(\sigma) = 1$, alors

$$\frac{\sigma(\theta)}{\theta} \Rightarrow \sigma(\theta) = \theta \Rightarrow \sigma(P(\theta)) = P(\theta), \forall\, P \in k[X] \Rightarrow \sigma = \mathrm{id}_K\,.$$

Donc $\mathrm{Gal}(K/k)$ est isomorphe à un sous-groupe du groupe cyclique $\langle\zeta\rangle$, ainsi $\mathrm{Gal}(K/k)$ est un groupe cyclique d'ordre divisant n. □

Proposition 9.11. *Soient k un corps commutatif, $a \in k$ et p un nombre premier, alors le polynôme $X^p - a$ est soit irréductible sur k soit a une racine dans k.*

Preuve. Soient Ω une clôture algébrique de k, $\theta \in \Omega$ tel que $\theta^p = a$ et ζ une racine de l'unité d'ordre p dans Ω.
Dans $\Omega[X]$, on a $P = X^p - \theta^p = \prod_{i=0}^{p-1}(X - \zeta^i\theta)$. Supposons que le polynôme P est réductible dans $k[X]$, alors $P = AB,\ A, B \in k[X] \setminus k$. Soit $n = \deg(A)$. On a $1 \leq n \leq p$ (donc n est premier à p). Dans $\Omega[X]$, on a $A = \prod_{i\in E}(X - \zeta^i\theta)$ avec $|E| = n$, soit $a_o = A(0)$, alors $a_0 = \pm\zeta^n\theta^n \in k$, donc $a_0^p = \pm a^n$. Le théorème de Bezout nous donne l'existence de $u, v \in \mathbb{Z}$ tel que $un + vp = 1$, donc

$$\pm a^{un} = a_0^{up} = \pm a^{1-vp} = \pm a a^{-vp} \Rightarrow a = \pm a_0^{up} a^{vp} = (\pm a_0^u a^v)^p = b^p \in k.$$

Ainsi P a une racine b dans k. □

Corollaire 9.12. *Soit K/k une extension tel que $K = k(\theta)$ où $\theta^p \in k$ avec p est un nombre premier. Si k contient les racines p-ième de l'unité, alors $[K : k] = p$ ou $K = k$.*

Preuve. On a θ est une racine de $X^p - \theta^p \in k[X]$. Supposons que $[K : k] < p$, alors $X^p - \theta^p$ n'est pas irréductible sur k, donc il admet une racine $\alpha \in k$. On a $\theta^p = \alpha^p$, donc $\theta = \zeta\alpha$ avec ζ est une racine p-ième de l'unité dans k, donc $\theta \in k$, ainsi $K = k$. □

Corollaire 9.13. *Soit K/k une extension réelle tel que $K = k(\theta)$ où $\theta^p \in k$ avec p est un nombre premier. Alors $[K : k] = p$ ou $K = k$.*

Preuve. On a θ est une racine de $X^p - \theta^p \in k[X]$. Supposons que $[K : k] < p$, alors $X^p - \theta^p$ n'est pas irréductible sur k, donc il admet une racine $\alpha \in k$. On a $\theta^p = \alpha^p$, donc $\theta = \pm\alpha$, donc $\theta \in k$, ainsi $K = k$. □

9.3 Extensions par radicaux

Définition 9.4. Une extension K/k est dite une extension par radicaux s'il existe une suite finie de corps intermédiaire à K/k : $K_0 = k \subset K_1 \subset \ldots \subset K_n = K$ tel que K_{i+1}/K_i est une extension par radical. Autrement, $K = k(\theta_1, \ldots, \theta_n)$ tel que $\theta_i^{n_i} \in k(\theta_1, \ldots, \theta_{i-1})$ avec $n_i \in \mathbb{N}^*$.

Exemple. Soient K un corps et ζ une racine primitive n-ième de l'unité sur K, alors $K(\zeta)$ est une extension par radicaux de K.

Remarques.

- Une extension par radicaux est finie.
- On peut supposer que les n_i sont des nombres premiers.
- Si K' est une extension de k, k-isomorphe à une extension par radicaux de k, alors K' est une extension par radicaux de k.
- La notion d'extension par radicaux est transitive : Soit $k \subset K \subset L$ une tour d'extensions. Si L est une extension par radicaux de K, et K une extension par radicaux de k, alors L est une extension par radicaux de k.

Proposition 9.14. *Soient F_1/E_1 et F_2/E_2 des sous-extensions d'une extension K/k. Si F_1/E_1 et F_2/E_2 sont des extensions par radicaux, alors F_1F_2/E_1E_2 est une extension par radicaux.*

Preuve. On a

$$\begin{cases} F_1 = E_1(\theta_1, \ldots, \theta_n),\ \theta_i^{n_i} \in E_1(\theta_1, \ldots, \theta_{i-1}) \\ F_2 = E_2(\theta'_1, \ldots, \theta'_m),\ \theta_i^{n'_i} \in E_1(\theta'_1, \ldots, \theta'_{i-1}). \end{cases}$$

Donc $F_1F_2 = E_1E_2(\theta_1, \ldots, \theta_n, \theta'_1, \ldots, \theta'_m)$. Posons $\theta_{i+n} = \theta'_i$ et $n_{i+n} = n'_i$, donc

$$F_1F_2 = E_1E_2(\theta_1, \ldots, \theta_n, \theta_{n+1}, \ldots, \theta_{n+m}),\ \theta_i^{n_i} \in E_1E_2(\theta_1, \ldots, \theta_{i-1}),$$

ainsi F_1F_2/E_1E_2 est une extension par radicaux. □

Proposition 9.15. *Soit K/k une extension par radicaux, alors l'extension normale engendré par K/k est une extension par radicaux.*

Preuve. Soit Ω une clôture algébrique de K, $K_1, \ldots, K_n$ les k-conjugués de K dans Ω. On a $K_i = \sigma_i(K)$ avec σ_i un k-plongement de K dans Ω. On a $K_1 \ldots K_n/k$ est l'extension normale engendré par K/k. Or, on a

$$K = k(\theta_1, \ldots, \theta_m),\ \theta_j^{m_j} \in k(\theta_1, \ldots, \theta_{j-1}),$$

donc

$$K_i = \sigma_i(K) = k(\sigma_i(\theta_1), \ldots, \sigma_i(\theta_m)),\ \sigma_i(theta_j)^{m_i} = \sigma_i(theta_j^{m_i}) \in k(\sigma_i(\theta_1), \ldots, \sigma_i(\theta_{i-1})),$$

donc K_i/k est une extension par radicaux, ainsi $K_1 \ldots K_n/k$, l'extension normale engendré par K/k, est une extension par radicaux. □

9.4 Équations algébriques résolubles par radicaux

Définition 9.5. Soient k un corps commutatif et P un polynôme dans $k[X]$. On dit que P (ou que l'équation $P = 0$) est résoluble par radicaux s'il existe une extension par radicaux de k contenant un corps de décomposition de P. (Autrement, s'il existe une extension par radicaux de k dans laquelle P est scindé).

Exemples.

1) Soient K un corps tel que $\text{car}(K) \neq 2$ et $P(X) = X^2 + bX + c \in K[X]$.
   On a $P(X)$ est résoluble par radicaux. (II suffit de considérer la tour $K_0 = K \subset K_1 = K(\delta)$, où $\delta^2 = b^2 - 4c$).
2) Le polynôme $X^2 + X + 1 \in \mathbb{F}_2[X]$ est résoluble par radicaux sur $\mathbb{F}_2$. En effet, on a

$$D_{\mathbb{F}_2}(X^2 + X + 1) = \mathbb{F}_4 = \mathbb{F}_2(j) \text{ avec } j^3 = 1.$$

Soit G un groupe. Une suite finie de sous-groupes de G,

$$G = H_0 \supset H_1 \supset \ldots \supset H_n = \{e\},$$

est dite sous normale si

$$H_{i+1} \lhd H_i, \forall\ i = 0, \ldots, n.$$

L'entier n s'appelle la longueur de la suite (H_i) et les groupes H_i/H_{i+1} les facteurs de la suite (H_i).

- Un groupe est dit résoluble s'il admet une suite sous normale à facteurs abéliens.
- Un groupe fini est résoluble si et seulement si il admet une suite sous normale à facteurs cycliques.
- Soit G un groupe et H un sous-groupe distingué de G. Alors le groupe G est résoluble si et seulement si les groupes H et G/H sont résolubles.

Définition 9.6. Soient k un corps commutatif et P un polynôme dans $k[X]$. On appelle groupe de Galois de P (ou de l'équation $P = 0$) le groupe de Galois d'une extension D_P/k où D_P est un corps de décomposition de P. On note $\mathrm{Gal}(P)$ le groupe de Galois de P et on a $\mathrm{Gal}(P)$ ne dépend pas du choix du corps de décomposition de P.

Théorème 9.16. *Soient k un corps commutatif de caractéristique 0 et P un polynôme dans $k[X]$ de degré ≥ 1. P est résoluble par radicaux si et seulement si $\mathrm{Gal}(P)$ est résoluble.*

Preuve. Notons D_P un corps de décomposition de P sur k. On a D_P/k est de degré fini, normale, et séparable ($\mathrm{car}(k) = 0$). Ainsi D_P/k est galoisienne finie.

- Supposons que P est résoluble par radicaux sur k : il existe R extension de k par radicaux telle que $D_P \subset R$. Notons L la clôture normale de R/k. Alors $R \subset L$, L/K est normale, L/K est de degré fini, donc L est une extension de k par radicaux. Comme k est parfait, L/k est séparable. Ainsi L/k est galoisienne finie. Comme D_P/k est normale, on a $\mathrm{Gal}(D_P/k)$ est isomorphe au groupe-quotient $\mathrm{Gal}(L/k)/\mathrm{Gal}(L/D_P)$. Or $\mathrm{Gal}(L/k)$ est résoluble. Donc $\mathrm{Gal}(D_P/k)$ est résoluble.
- Supposons $\mathrm{Gal}(D_P/k)$ est résoluble. Notons $n = [D_P : k]$. Soit ζ une racine primitive n-ième de l'unité dans la clôture algébrique Ω de D_P, et $F = k(\zeta)$. On a D_PF est une extension galoisienne finie de F, et $\mathrm{Gal}(D_PF/F)$ est résoluble. Posons

$$m = [D_PF : F] = |\,\mathrm{Gal}(D_PF/F)|.$$

Comme $\mathrm{Gal}(D_PF/F)$ est isomorphe à un sous-groupe de $\mathrm{Gal}(D_P/k)$, m divise n. Donc pour tout diviseur premier p de m, F contient toutes les racines p-ièmes de l'unité. Comme $\mathrm{Gal}(D_PF/F)$ est résoluble, il existe une suite

$$\{1\} = G_r \lhd G_{r-1} \lhd \ldots \lhd G_0 = \mathrm{Gal}(D_PF/F)$$

de sous-groupes de $\mathrm{Gal}(D_PF/F)$ telle que $\forall\ i, G_{i+1} \lhd G_i$ et G_i/G_{i+1} est un groupe cyclique d'ordre premier p_i divisant m.

La correspondance de Galois fournit une tour d'extensions

$$F = F_0 \subset F_1 \subset \ldots \subset F_{r-1} \subset F_r = D_PF, \text{ où } F_i = \mathrm{Inv}(G_i),$$

chaque F_{i+1}/F_i est galoisienne finie et $\mathrm{Gal}(F_{i+1}/F_i) \simeq G_i/G_{i+1}$, donc $\mathrm{Gal}(F_{i+1}/F_i)$ est cyclique d'ordre p_i. On a donc : $\forall\ i, F_{i+1} = F_i(\alpha_i)$ où $\alpha_i \in F_i$. Ainsi D_PF est une extension par radicaux de F, donc D_PF est une extension par radicaux de k. Donc puisque $D_P \subset D_PF$, le polynôme P est résoluble par radicaux sur k.

□

Bibliographie

[1] N. Bourbaki (1959), *Algèbre. Chapitres 4 et 5*, Hermann Ed.

[2] M. Chellali (1995–1996), *Théorie des corps*, Cours Maths 4, Faculté des sciences, Oujda.

[3] I. Gozard (1997), *Théorie de Galois*, Ellipses, Édition Marketing S. A.

[4] A. Jebli (1996), *Théorie de Galois*, Les éditions Toubkal.

[5] P. Samuel (1971), *Théorie algébrique des nombres*, Hermann Ed.