Algèbre 2

Cours de Greg McShane
Notes de Alexis Marchand

ENS de Lyon
S2 2017-2018
Niveau L3

Table des matières

1 Anneaux – définitions et exemples de base

1.1 Définition

Définition 1.1.1 (Anneau). *Un anneau est un triplet* $(A, +, \times)$*, où* A *est un ensemble et* $+$ *et* $\times$ *sont des lois de composition interne sur* A *vérifiant :*

(i) $(A, +)$ *est un groupe abélien, de neutre noté* 0_A*.*

(ii) $\times$ *est associative et admet un neutre noté* 1_A*.*

(iii) $\times$ *est distributive à gauche et à droite sur* $+$*.*

Si de plus $\times$ *est commutative, on dit que* $(A, +, \times)$ *est un anneau commutatif.*

Exemple 1.1.2. $\mathbb{Z}$, $\mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}[X]$, $\mathbb{Z}/n\mathbb{Z}[X]$ *sont des anneaux.*

1.2 Divisibilité

Définition 1.2.1 (Divisibilité). *Soit* A *un anneau,* $(a, b) \in A^2$*. On dit que* a divise b*, et on note* $a \mid b$*, lorsqu'il existe un* $c \in A$ *t.q.* $b = ac$*.*

Notation 1.2.2. *Soit* A *un anneau. Étant donné* $a \in A$*, on note* $\mathrm{Div}(a)$ *l'ensemble des diviseurs de* a *dans* A*.*

Définition 1.2.3 (Éléments associés). *Soit* A *un anneau,* $(a, b) \in A^2$*. S'équivalent :*

(i) $a \mid b$ et $b \mid a$.

(ii) $\mathrm{Div}(a) = \mathrm{Div}(b)$.

On dit alors que a *et* b *sont* associés.

Définition 1.2.4 (Éléments inversibles). *Soit* A *un anneau et* $a \in A$*. On dit que* a *est* inversible *dans* A *lorsqu'il existe* $b \in A$ *t.q.* $1_A = ab = ba$*. On écrit alors* $b = a^{-1}$*. On note* $A^\times$ *l'ensemble des éléments inversibles de* A*.*

Proposition 1.2.5. *Soit* A *un anneau. Alors* $(A^\times, \times)$ *est un groupe de neutre* 1_A*.*

Définition 1.2.6 (Corps). *Soit* A *un anneau commutatif. On dit que* A *est un* corps *lorsque* $A^\times = A \backslash \{0\}$*.*

Remarque 1.2.7. *Soit* A *un anneau. Alors* $\forall a \in A,\ A^\times \subset \mathrm{Div}(a)$*.*

Définition 1.2.8 (Éléments premiers entre eux). *Soit* A *un anneau,* $(a, b) \in A^2$*. On dit que* a *et* b *sont* premiers entre eux *lorsque* $\mathrm{Div}(a) \cap \mathrm{Div}(b) = A^\times$*.*

1.3 Éléments premiers et irréductibles

Définition 1.3.1 (Éléments premiers et irréductibles)**.** *Soit A un anneau commutatif et $a \in A$. On suppose que $a \neq 0_A$ et $a \notin A^\times$.*

(i) *On dit que a est* irréductible *lorsque :*

$$\forall (b,c) \in A^2,\ a = bc \Longrightarrow b \in A^\times \text{ ou } c \in A^\times.$$

(ii) *On dit que a est* premier *lorsque :*

$$\forall (b,c) \in A^2,\ a \mid bc \Longrightarrow a \mid b \text{ ou } a \mid c.$$

1.4 Diviseurs de zéro

Définition 1.4.1 (Diviseur de zéro)**.** *Soit A un anneau. Un élément $a \in A$ est appelé* diviseur de zéro *lorsque* $\exists b \in A \backslash \{0_A\},\ 0_A = ab = ba$.

Définition 1.4.2 (Anneau intègre)**.** *Un anneau commutatif est dit* intègre *lorsqu'il n'admet aucun diviseur de zéro non nul.*

Proposition 1.4.3. *Tout corps est un anneau intègre.*

Exemple 1.4.4. $\mathbb{Z}/n\mathbb{Z}$ *est intègre* ssi n *est premier.*

1.5 Factorisation et équations diophantiennes

Lemme 1.5.1 (Lemme de Gauß)**.** *Soit $\pi \in \mathbb{Z}$. Alors π est irréductible dans $\mathbb{Z}$* ssi *π est premier dans $\mathbb{Z}$.*

Théorème 1.5.2. *Soit $\pi \in \mathbb{Z}[i]$. Alors π est irréductible dans $\mathbb{Z}[i]$* ssi *π est premier dans $\mathbb{Z}[i]$.*

Démonstration. Admis temporairement. □

Remarque 1.5.3. 2 *est premier dans $\mathbb{Z}$ mais pas dans $\mathbb{Z}[i]$ (car $2 = (1+i)(1-i)$).*

Théorème 1.5.4. *Soit $a \in \mathbb{Z}[i] \backslash \{0\}$. Alors il existe $u \in \mathbb{Z}[i]^\times$, $\pi_1, \ldots, \pi_r$ des irréductibles deux à deux non associés de $\mathbb{Z}[i]$ et $(n_1, \ldots, n_r) \in (\mathbb{N}^*)^r$ t.q. $a = u\pi_1^{n_1} \cdots \pi_r^{n_r}$. De plus, l'écriture est unique à permutation près, en s'autorisant à remplacer les π_i par des irréductibles associés.*

Démonstration. Admis temporairement. □

Lemme 1.5.5. *Soit $x, y, z \in \mathbb{Z}$ premiers entre eux dans leur ensemble t.q. $z^2 = x^2 + y^2$. Alors :*

(i) *$(x+iy)$ et $(x-iy)$ sont premiers entre eux dans $\mathbb{Z}[i]$.*

(ii) *Il existe $u \in \mathbb{Z}[i]^\times$ et $(\alpha, \beta) \in \mathbb{Z}^2$ t.q. $x + iy = u(\alpha + i\beta)^2$ et $x - iy = \overline{u}(\alpha - i\beta)^2$.*

Proposition 1.5.6. *Soit $x, y, z \in \mathbb{Z}$ premiers entre eux dans leur ensemble t.q. $z^2 = x^2 + y^2$. Alors il existe $(\alpha, \beta) \in \mathbb{Z}^2$ t.q. $(x, y, z) = (\alpha^2 - \beta^2, 2\alpha\beta, \alpha^2 + \beta^2)$.*

2 Anneaux – Sous-anneaux, idéaux, morphismes et quotients

2.1 Sous-anneaux

Définition 2.1.1 (Sous-anneau)**.** *Soit A un anneau. On appelle* sous-anneau *de A tout sous-ensemble $B \subset A$ vérifiant les trois propriétés suivantes :*

(i) *B est un sous-groupe de $(A,+)$.*

(ii) *B est stable par $\times$: $\forall (x,y) \in B^2$, $xy \in B$.*

(iii) *$1_A \in B$.*

Définition 2.1.2 (Sous-anneau engendré par une partie)**.** *Soit A un anneau. Si $E \subset A$, on appelle* sous-anneau engendré *par E le plus petit sous-anneau de A contenant E.*

Exemple 2.1.3. *Soit K un corps. On appelle* corps premier *de K, et on note K_0, le plus petit sous-corps de K. K_0 contient le sous-anneau de K engendré par $\{1_K\}$.*

2.2 Idéaux

Définition 2.2.1 (Idéal)**.** *Soit A un anneau. On appelle* idéal à gauche *(resp.* à droite*) de A tout sous-ensemble $I \subset A$ vérifiant les deux propriétés suivantes :*

(i) *I est un sous-groupe de $(A,+)$.*

(ii) *$\forall x \in A$, $xI \subset I$ (resp. $\forall x \in A$, $Ix \subset I$).*

Lorsque A est commutatif, la notion d'idéal à gauche est équivalente à celle d'idéal à droite ; on dit alors simplement "idéal".

Exemple 2.2.2. *Soit A un anneau commutatif non nul. Alors A admet au moins deux idéaux : $\{0_A\}$ et A. Et A est un corps* ssi *ces deux idéaux sont les seuls idéaux de A.*

Définition 2.2.3 (Idéal engendré par une partie)**.** *Soit A un anneau commutatif. Si $E \subset A$, on appelle* idéal engendré *par E, noté (E), le plus petit idéal de A contenant E.*

Définition 2.2.4 (Idéal principal)**.** *Soit A un anneau commutatif. Pour $x \in A$, l'idéal $(\{x\})$ est noté (x) et appelé* idéal principal *engendré par x.*

Exemple 2.2.5. *Tout idéal de $\mathbb{Z}$ est principal.*

2.3 Morphismes

Définition 2.3.1 (Morphisme d'anneaux)**.** *Soit A et B deux anneaux. On appelle* morphisme d'anneaux *de A vers B toute application $\phi : A \to B$ vérifiant :*

(i) *$\forall (x,y) \in A^2$, $\phi(x+y) = \phi(x) + \phi(y)$,*

(ii) *$\forall (x,y) \in A^2$, $\phi(xy) = \phi(x)\phi(y)$,*

(iii) *$\phi(1_A) = 1_B$.*

Remarque 2.3.2. *Si l'anneau B est intègre et l'application ϕ est non nulle, la condition* (iii) *dans la définition d'un morphisme d'anneaux est une conséquence des deux autres.*

Notation 2.3.3. *Si A et B sont deux anneaux et $\phi : A \to B$ et un morphisme d'anneaux, on note* $\operatorname{Ker}\phi = \phi^{-1}(\{0_B\})$ *et* $\operatorname{Im}\phi = \phi(A)$.

Proposition 2.3.4. *Soit A et B deux anneaux commutatifs et $\phi : A \to B$ un morphisme. Alors :*

(i) *Pour tout J idéal de B, $\phi^{-1}(J)$ est un idéal de A.*

(ii) $\operatorname{Ker}\phi$ *est un idéal de A.*

(iii) $\operatorname{Im}\phi$ *est un sous-anneau de B.*

(iv) *$\phi(A^\times) \subset B^\times$.*

(v) *Si ϕ est surjective et $x \in A$ est irréductible, alors $\phi(x)$ est irréductible.*

Exemple 2.3.5. *Il n'existe aucun morphisme d'anneaux $\phi : \mathbb{Z}[i] \to \mathbb{Z}$ (sinon on aurait $0 = \phi(i^2+1) = \phi(i)^2 + 1$).*

2.4 Quotients

Définition 2.4.1 (Anneau quotient)**.** *Soit A un anneau commutatif et I un idéal de A. On définit une relation d'équivalence $\mathcal{R}$ sur A par :*

$$\forall (x,y) \in A^2,\ x\mathcal{R}y \Longleftrightarrow (x-y) \in I.$$

Le quotient $A/\mathcal{R}$ est noté A/I. Alors il existe une unique structure d'anneau sur A/I t.q. la projection canonique $\pi : A \to A/I$ est un morphisme d'anneaux. Si $a \in A$, l'élément $\pi(a)$ pourra être noté $\overline{a}$ ou bien $a+I$.

Définition 2.4.2 (Idéal premier, idéal maximal)**.** *Soit A un anneau commutatif et I un idéal de A.*

(i) *On dit que I est premier lorsque $\forall (a,b) \in A^2,\ ab \in I \Longrightarrow a \in I$ ou $b \in I$.*

(ii) *On dit que I est maximal lorsque $I \subsetneq A$ et pour tout idéal J de A, si $I \subset J \subsetneq A$, alors $I = J$.*

Proposition 2.4.3. *Soit A un anneau commutatif et I un idéal de A.*

(i) *I est premier* ssi *A/I est intègre.*

(ii) *I est maximal* ssi *A/I est un corps.*

Corollaire 2.4.4. *Tout idéal maximal est premier.*

2.5 Divisibilité et idéaux

Proposition 2.5.1. *Soit A un anneau commutatif et $(a,b) \in A^2$. Alors :*

$$a \mid b \Longleftrightarrow (b) \subset (a).$$

Proposition 2.5.2. *Soit A un anneau commutatif et $a \in A$. Alors :*

(i) *a est premier* ssi *(a) est premier.*

(ii) *a est irréductible* ssi *(a) est maximal parmi les idéaux principaux propres de A.*

Définition 2.5.3 (Anneau principal)**.** *Un anneau commutatif intègre A est dit* principal *lorsque tout idéal de A est principal.*

Exemple 2.5.4. *$\mathbb{Z}$ est principal.*

Proposition 2.5.5. *Soit A un anneau principal. Alors un élément $p \in A$ est irréductible* ssi *il est premier.*

2.6 Exemple – critère d'Eisenstein

Proposition 2.6.1. *Soit K un corps. Alors pour tout $S \in K[X]$ et pour tout $P \in K[X]$ avec $\deg P \geqslant 1$, il existe un unique couple $(Q,R) \in K[X]^2$ t.q.*

$$S = PQ + R \qquad \text{et} \qquad \deg R < \deg P.$$

Lemme 2.6.2. *Soit K un corps. Soit $n \in \mathbb{N}^*$ et $(A,B) \in K[X]^2$ t.q. $X^n = AB$. Alors il existe $u \in K^*$, $0 \leqslant n_0 \leqslant n$ t.q. $A = uX^{n_0}$ et $B = u^{-1}X^{n-n_0}$.*

Théorème 2.6.3 (Critère d'Eisenstein)**.** *Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, avec $n \in \mathbb{N}^*$. On suppose qu'il existe un nombre premier p t.q.*

(i) *$p \nmid a_n$.*

(ii) *$\forall k \in \{0,\dots,n-1\}$, $p \mid a_k$.*

(iii) *$p^2 \nmid a_0$.*

Alors P est irréductible dans $\mathbb{Z}[X]$.

Démonstration. Supposons par l'absurde $P = AB$, avec $(A,B) \in (\mathbb{Z}[X] \backslash \mathbb{Z}_0[X])^2$. La réduction de P modulo p s'écrit : $\overline{A} \times \overline{B} = \overline{P} = \overline{a_n} X^n$. D'après le lemme 2.6.2, $\overline{A}$ et $\overline{B}$ sont des monômes dans $\mathbb{Z}/p\mathbb{Z}[X]$. Donc p divise les coefficients constants respectifs de A et B ; donc p^2 divise a_0. C'est absurde. $\square$

2.7 Opérations sur les idéaux

Proposition 2.7.1. *Soit A un anneau commutatif, I et J deux idéaux de A. Alors $I \cap J$ et $I + J$ sont des idéaux de A.*

Définition 2.7.2 (Idéal produit)**.** *Soit A un anneau commutatif, I et J deux idéaux de A. On définit l'idéal IJ par :*

$$IJ = (\{xy,\ (x, y) \in I \times J\}) = \left\{ \sum_{k=1}^{r} x_k y_k,\ r \in \mathbb{N},\ (x_1, \ldots, x_r) \in I^r,\ (y_1, \ldots, y_r) \in J^r \right\}.$$

On définit de plus l'idéal I^n par récurrence sur n en posant $I^0 = A$ et $I^{n+1} = I^n I$.

Définition 2.7.3 (PGCD et PPCM)**.** *Soit A un anneau principal, $(a_1, \ldots, a_n) \in A^n$.*

(i) *On appelle* PGCD *de $a_1, \ldots, a_n$ tout élément $d \in A$ t.q. $(d) = (a_1) + \cdots + (a_n)$.*

(ii) *On appelle* PPCM *de $a_1, \ldots, a_n$ tout élément $m \in A$ t.q. $(m) = (a_1) \cap \cdots \cap (a_n)$.*

Définition 2.7.4 (Idéaux premiers entre eux)**.** *Deux idéaux I et J d'un anneau commutatif A sont dits* premiers entre eux *lorsque $A = I + J$.*

Théorème 2.7.5 (Théorème des restes chinois)**.** *Soit A un anneau commutatif.*

(i) *Soit I et J deux idéaux premiers entre eux de A. Alors $I_1 I_2 = I_1 \cap I_2$ et on a un isomorphisme canonique :*
$$A/\left(I \cap J\right) \simeq \left(A/I\right) \times \left(A/J\right).$$

(ii) *Soit $I_1, \ldots, I_n$ n idéaux premiers entre eux deux à deux de A. Alors $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$ et on a un isomorphisme canonique :*
$$A/\left(I_1 \cap \cdots \cap I_n\right) \simeq \left(A/I_1\right) \times \cdots \times \left(A/I_n\right).$$

3 Anneaux noethériens

3.1 Anneaux noethériens

Définition 3.1.1 (Idéal principal, idéal de type fini)**.** *Soit A un anneau commutatif, I un idéal de A.*

(i) *On dit que I est* principal *lorsqu'il existe $x \in A$ t.q. $I = (x)$.*

(ii) *On dit que I est* de type fini *lorsqu'il existe $(x_1, \ldots, x_n) \in A^n$ t.q. $I = (x_1) + \cdots + (x_n)$.*

Définition 3.1.2 (Anneau principal, anneau noethérien)**.** *Soit A un anneau commutatif.*

(i) *On dit que A est* principal *lorsque A est intègre et tout idéal de A est principal.*

(ii) *On dit que A est* noethérien *lorsque tout idéal de A est de type fini.*

Remarque 3.1.3. *Un anneau noethérien n'est pas nécessairement intègre.*

Proposition 3.1.4. *L'image par un morphisme d'anneaux d'un anneau noethérien est noethérien.*

Corollaire 3.1.5. *Soit A un anneau noethérien et I un idéal de A. Alors A/I est noethérien.*

3.2 Théorème de Krull

Proposition 3.2.1. *Soit A un anneau commutatif. Soit $(I_\lambda)_{\lambda\in\Lambda}$ une chaîne d'idéaux de A (i.e. $\forall(\lambda,\mu)\in\Lambda^2$, $I_\lambda\subset I_\mu$ ou $I_\mu\subset I_\lambda$). Alors :*

(i) *$\bigcup_{\lambda\in\Lambda} I_\lambda$ est un idéal de A.*

(ii) *Si $\forall\lambda\in\Lambda$, $I_\lambda\subsetneq A$, alors $\bigcup_{\lambda\in\Lambda} I_\lambda\subsetneq A$.*

Définition 3.2.2 (Ensemble inductif)**.** *Un ensemble ordonné est dit inductif lorsque toute chaîne (i.e. toute partie totalement ordonnée) admet un majorant.*

Théorème 3.2.3 (Lemme de Zorn)**.** *Tout ensemble inductif admet un élément maximal.*

Théorème 3.2.4 (Théorème de Krull)**.** *Soit A un anneau commutatif et I un idéal propre de A. Alors il existe un idéal maximal J t.q.*

$$I\subset J\subsetneq A.$$

Démonstration. On considère $\mathcal{F}=\{J \text{ idéal de } A,\ I\subset J\subsetneq A\}$. Selon la proposition 3.2.1, $\mathcal{F}$ est inductif. Selon le lemme de Zorn, $\mathcal{F}$ admet donc un élément maximal J, ce qui fournit le résultat. □

3.3 Anneaux noethériens (suite)

Théorème 3.3.1. *Soit A un anneau commutatif. S'équivalent :*

(i) *A est noethérien.*

(ii) *Toute suite d'idéaux de A croissante pour l'inclusion est stationnaire.*

(iii) *Toute famille non vide d'idéaux de A admet un élément maximal.*

Démonstration. (i) $\Rightarrow$ (ii) Soit $(I_n)_{n\in\mathbb{N}}$ une suite d'idéaux croissante pour l'inclusion. On note $I_\infty=\bigcup_{n\in\mathbb{N}} I_n$. Selon la proposition 3.2.1, I_∞ est un idéal de A. Comme A est noethérien, il existe des éléments $a_1,\dots,a_k$ t.q. $I_\infty=(a_1)+\cdots+(a_k)$. Pour $j\in\{1,\dots,k\}$, on a $a_j\in I_\infty=\bigcup_{n\in\mathbb{N}} I_n$, donc il existe $n_j\in\mathbb{N}$ t.q. $a_j\in I_{n_j}$. Si $N=\max_{1\leqslant j\leqslant k} n_j$, alors $\forall j\in\{1,\dots,k\}$, $a_j\in I_N$, d'où $I_\infty=(a_1)+\cdots+(a_k)=I_N$. Ainsi $\forall n\geqslant N$, $I_n=I_N$. (ii) $\Rightarrow$ (iii) Par contraposée, supposons qu'il existe une famille $\mathcal{F}$ non vide d'idéaux de A sans élément maximal. On choisit alors $I_0\in\mathcal{F}$, puis, après avoir construit $I_0\subsetneq\cdots\subsetneq I_n$, comme I_n n'est pas un élément maximal de $\mathcal{F}$, il existe $I_{n+1}\in\mathcal{F}$ t.q. $I_n\subsetneq I_{n+1}$. On construit ainsi une suite strictement croissante (donc non stationnaire) d'idéaux de A. (iii) $\Rightarrow$ (i) Soit I un idéal de A. On considère $\mathcal{F}=\{J \text{ idéal de } A \text{ de type fini},\ J\subset I\}$. On a $\mathcal{F}\neq\varnothing$ car $\{0\}\in\mathcal{F}$. Donc $\mathcal{F}$ admet un élément maximal J_m. Si $J_m\subsetneq I$, alors il existe $x\in I\backslash J_m$, et $(J_m+(x))\in\mathcal{F}$, ce qui contredit la maximalité de J_m. Donc $J_m=I$, et I est de type fini. □

3.4 Anneaux de polynômes

Définition 3.4.1 (Polynômes à coefficients dans un anneau)**.** *Si A est un anneau commutatif, on note $A[X]$ l'anneau des polynômes à coefficients dans A. On définit de plus par récurrence les anneaux des polynômes à plusieurs indéterminées en posant $A[X_1,\dots,X_{n+1}]=A[X_1,\dots,X_n][X_{n+1}]$.*

Remarque 3.4.2. *Soit A un anneau commutatif. Alors l'application $j:a\in A\longmapsto aX^0\in A[X]$ est un morphisme injectif d'anneaux, ce qui permet d'identifier A au sous-anneau $j(A)$ de $A[X]$.*

Proposition 3.4.3. *Soit A un anneau commutatif intègre.*

(i) $\forall P\in A[X]$, $\deg P<0\Longleftrightarrow P=0$.

(ii) $\forall(P,Q)\in A[X]^2$, $\deg(PQ)=\deg P+\deg Q$.

Corollaire 3.4.4. *Soit A un anneau commutatif.*

(i) *A est intègre* ssi *$A[X]$ est intègre.*

(ii) *Si A est intègre, alors $A[X]^\times = A^\times$.*

Théorème 3.4.5 (Division euclidienne)**.** *Soit A un anneau commutatif intègre. Alors pour tout $S \in A[X]$ et pour tout $P \in A[X]$ avec P unitaire (i.e. de coefficient dominant 1_A), il existe un unique couple $(Q, R) \in A[X]^2$ t.q.*

$$S = PQ + R \qquad \text{et} \qquad \deg R < \deg P.$$

Proposition 3.4.6. *Soit A un anneau commutatif, $P \in A[X]$ et $\alpha \in A$. S'équivalent :*

(i) $P(\alpha) = 0$.

(ii) *$X - \alpha$ divise P.*

On dit alors que α est racine de P.

Démonstration. (ii) $\Rightarrow$ (i) Clair. (i) $\Rightarrow$ (ii) Noter que $\forall k \in \mathbb{N}$, $X^k - \alpha^k = (X - \alpha)Q_k$, avec $Q_k = \sum_{j=0}^{k-1} \alpha^{k-1-j} X^j$. Comme $P(\alpha) = 0$, il vient, en écrivant $P = \sum_{k=0}^{d} p_k X^k$:

$$P = P - P(\alpha) = \sum_{k=0}^{d} p_k \left(X^k - \alpha^k\right) = (X - \alpha) \sum_{k=0}^{d} p_k Q_k.$$

□

Corollaire 3.4.7. *Soit A un anneau commutatif intègre. Alors tout polynôme $P \in A[X]$ admet au plus* $\deg P$ *racines.*

Lemme 3.4.8. *Soit G un groupe abélien fini. Alors G admet un élément dont l'ordre est le* PPCM *des ordres des éléments de G.*

Proposition 3.4.9. *Si A est un anneau commutatif intègre, alors tout sous-groupe fini de $A^\times$ est cyclique.*

3.5 Théorème de Hilbert

Lemme 3.5.1. *Soit A un anneau commutatif. Pour I idéal de $A[X]$ est $n \in \mathbb{N}$, on définit :*

$$\mathfrak{d}_n(I) = \{0\} \cup \{\textit{coefficients dominants des éléments de } I \textit{ qui sont de degré } n\}.$$

Alors $\mathfrak{d}_n(I)$ est un idéal de A et on a les propriétés suivantes :

(i) *Si $I \subset J$ sont des idéaux de A, alors $\forall n \in \mathbb{N}$, $\mathfrak{d}_n(I) \subset \mathfrak{d}_n(J)$.*

(ii) *Si I est un idéal de A, alors $\forall n \in \mathbb{N}$, $\mathfrak{d}_n(I) \subset \mathfrak{d}_{n+1}(I)$.*

(iii) *Si $I \subset J$ sont des idéaux de A, alors $I = J \iff \forall n \in \mathbb{N}$, $\mathfrak{d}_n(I) = \mathfrak{d}_n(J)$.*

Démonstration. (iii) Si $I = J$, alors $\forall n \in \mathbb{N}$, $\mathfrak{d}_n(I) = \mathfrak{d}_n(J)$. Si $I \subsetneq J$ supposons par l'absurde que $\forall n \in \mathbb{N}$, $\mathfrak{d}_n(I) = \mathfrak{d}_n(J)$. Soit $P \in J \backslash I$ t.q.

$$\deg P = \min_{Q \in J \backslash I} \deg Q.$$

Si $k = \deg P$, alors le coefficient dominant de P est dans $\mathfrak{d}_k(J) = \mathfrak{d}_k(I)$, donc il existe $Q \in I \subset J$ de même degré et de même coefficient dominant que P. Ainsi, $(P - Q) \in J$, et $\deg(P - Q) < \deg P$. Par construction de P, il vient $(P - Q) \in I$, d'où $P \in I$, ce qui est faux. □

Théorème 3.5.2 (Théorème de Hilbert)**.** *Si A est un anneau noethérien, alors $A[X]$ est noethérien.*

Démonstration. Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de $A[X]$. Avec les notations du lemme 3.5.1, et d'après le théorème 3.3.1, la famille $(\mathfrak{d}_k(I_n))_{(k,n)\in\mathbb{N}^2}$ admet un élément maximal $\mathfrak{d}_\ell(I_m)$, car A est noethérien. Pour $k\in\{0,\ldots,\ell\}$, la suite $(\mathfrak{d}_k(I_n))_{n\in\mathbb{N}}$ est une suite croissante d'idéaux, donc il existe $n_k\in\mathbb{N}$ t.q.

$$\forall n\geqslant n_k,\ \mathfrak{d}_k(I_n)=\mathfrak{d}_k(I_{n_k}).$$

On pose maintenant $N=\max\{m,n_0,\ldots,n_\ell\}$. Soit maintenant $n\geqslant N$. Montrons que $I_n=I_N$. On a $I_N\subset I_n$. Selon le lemme 3.5.1, il suffit de prouver que $\forall k\in\mathbb{N},\ \mathfrak{d}_k(I_N)=\mathfrak{d}_k(I_n)$. Soit donc $k\in\mathbb{N}$. Si $k\leqslant\ell$, alors $\mathfrak{d}_k(I_N)=\mathfrak{d}_k(I_{n_k})=\mathfrak{d}_k(I_n)$. Si $k>\ell$, alors :

$$\mathfrak{d}_k(I_N)\supset\mathfrak{d}_k(I_m)\supset\mathfrak{d}_\ell(I_m)\qquad\text{et}\qquad\mathfrak{d}_k(I_n)\supset\mathfrak{d}_k(I_m)\supset\mathfrak{d}_\ell(I_m).$$

Par maximalité de $\mathfrak{d}_\ell(I_m)$, on a $\mathfrak{d}_k(I_N)=\mathfrak{d}_\ell(I_m)=\mathfrak{d}_k(I_n)$. D'où $I_N=I_n$. □

4 Anneaux euclidiens et anneaux factoriels

4.1 Anneaux euclidiens

Définition 4.1.1 (Anneau euclidien)**.** *Soit A un anneau commutatif intègre. On dit que A est* euclidien *lorsqu'il existe une application $\nu : A\setminus\{0_A\}\to\mathbb{N}$ t.q.*

$$\forall(a,b)\in A\times(A\setminus\{0_A\}),\ \exists(q,r)\in A^2,\ a=qb+r\ \text{ et }\ (r=0\ \text{ ou }\ \nu(r)<\nu(b)).$$

On dit alors que ν est un stathme euclidien

Exemple 4.1.2. *$\mathbb{Z}$ et $\mathbb{Z}[i]$ sont euclidiens. $K[X]$ est euclidien si K est un corps.*

Proposition 4.1.3. *Tout anneau euclidien est principal.*

4.2 Anneaux factoriels

Définition 4.2.1 (Système de représentants des classes d'irréductibles)**.** *Soit A un anneau commutatif intègre. Soit P l'ensemble des irréductibles de A. On appelle* système de représentants des classes d'irréductibles pour la relation d'association *(SRCI) de A toute partie $\mathcal{P}\subset P$ t.q. pour tout $\pi\in P$, il existe un unique $\pi'\in\mathcal{P}$ qui est associé à π.*

Définition 4.2.2 (Anneau factoriel)**.** *Un anneau commutatif intègre A est dit* factoriel *lorsque pour tout $a\in A\setminus\{0_A\}$, il existe un unique $u\in A^\times$ et une unique famille presque nulle $(n_\pi)_{\pi\in\mathcal{P}}\in\mathbb{N}^{\mathcal{P}}$ t.q. $a=u\prod_{\pi\in\mathcal{P}}\pi^{n_\pi}$, où $\mathcal{P}$ est un SRCI de A.*

Proposition 4.2.3. *Soit A un anneau noethérien intègre. Alors tout élément de A se décompose en produit d'irréductibles.*

Démonstration. Soit F l'ensemble des éléments non nuls et non inversibles de A ne se décomposant pas en produit d'irréductibles. Poser $\mathcal{F}=\{(a),\ a\in F\}$; supposer par l'absurde $\mathcal{F}\neq\varnothing$ et considérer un élément maximal de $\mathcal{F}$. □

Définition 4.2.4 (Valuation π-adique)**.** *Soit A un anneau commutatif intègre, π un irréductible de A. Pour $a\in A$, on définit la* valuation π-adique *de a par :*

$$v_\pi(a)=\sup\{n\in\mathbb{N},\ \pi^n\mid a\}.$$

On a $\pi\mid a\iff v_\pi(a)>0$.

Proposition 4.2.5. *Soit A un anneau factoriel. Soit π un irréductible de A. Alors :*

(i) $\forall(a,b)\in A^2,\ v_\pi(ab)=v_\pi(a)+v_\pi(b)$.

(ii) $\forall (a,b) \in A^2,\ v_\pi(a+b) \geqslant \min(v_\pi(a), v_\pi(b))$, *avec égalité dès que* $v_\pi(a) \neq v_\pi(b)$.

Définition 4.2.6 (PGCD)**.** *Soit A un anneau factoriel muni d'un SRCI $\mathcal{P}$. Si $(a,b) \in A^2$, on définit le* PGCD *de a et b par :*

$$a \wedge b = \prod_{\pi \in \mathcal{P}} \pi^{\min(v_\pi(a), v_\pi(b))}.$$

Proposition 4.2.7. *Soit A un anneau commutatif intègre vérifiant les deux hypothèses suivantes :*

(i) *Tout élément de A se décompose en produit d'irréductibles.*

(ii) *Tout élément irréductible de A est premier.*

Alors A est factoriel.

Corollaire 4.2.8. *Tout anneau principal est factoriel.*

4.3 Corps des fractions d'un anneau intègre

Théorème 4.3.1. *Soit A un anneau intègre. Alors il existe un corps K_A, appelé* corps des fractions *de A, t.q.*

(i) *Il existe un morphisme injectif d'anneaux $j : A \to K_A$.*

(ii) *Pour tout corps F, et pour tout morphisme injectif d'anneaux $\varphi : A \to F$, il existe un morphisme de corps $\psi : K_A \to F$ t.q. $\varphi = \psi \circ j$ (i.e. ψ prolonge φ, en identifiant A et $j(A)$).*

K_A est unique à isomorphisme près. On identifiera toujours A à $j(A)$ et on considérera que $A \subset K_A$.

Définition 4.3.2 (Élément normalisé)**.** *Soit A un anneau factoriel muni d'un SRCI $\mathcal{P}$ et soit K_A le corps des fractions de A. On dit qu'un élément $x \in K_A \setminus \{0_A\}$ est* normalisé *par rapport à $\mathcal{P}$ lorsqu'il existe une famille presque nulle $(n_\pi)_{\pi \in \mathcal{P}} \in \mathbb{Z}^{\mathcal{P}}$ t.q.*

$$x = \prod_{\pi \in \mathcal{P}} \pi^{n_\pi}.$$

4.4 Contenu d'un polynôme sur un anneau factoriel

Définition 4.4.1 (Polynôme primitif)**.** *Soit A un anneau factoriel et $P \in A[X] \setminus \{0_A\}$. On dit que P est* primitif *lorsque le* PGCD *des coefficients de P est égal à 1_A (dans n'importe quel SRCI).*

Proposition 4.4.2. *Soit A un anneau factoriel muni d'un SRCI $\mathcal{P}$ et soit K_A le corps des fractions de A. Pour tout $P \in K_A[X] \setminus \{0_A\}$, il existe un unique $c(P) \in K_A \setminus \{0_A\}$ normalisé t.q. $P = c(P)P_1$, où $P_1 \in A[X]$ est un polynôme primitif. On dit que $c(P)$ est le* contenu *de P (dans le SRCI $\mathcal{P}$).*

Proposition 4.4.3. *Soit A un anneau factoriel muni d'un SRCI $\mathcal{P}$ et soit K_A le corps des fractions de A.*

(i) $\forall P \in K_A[X] \setminus \{0_A\},\ \forall \alpha \in K_A \setminus \{0_A\}$ *normalisé,* $c(\alpha P) = \alpha c(P)$.

(ii) $\forall P \in K_A[X] \setminus \{0_A\},\ P \in A[X] \iff c(P) \in A$.

(iii) $\forall P \in A[X] \setminus \{0_A\},\ P$ *primitif* $\iff c(P) = 1_A$.

Notation 4.4.4. *Soit A un anneau commutatif intègre et $\pi \in A$ un élément premier. Alors la projection canonique $A \to A/(\pi)$ induit un morphisme d'anneaux $P \in A[X] \longmapsto \overline{P} \in A/(\pi)[X]$. Ce morphisme est appelé* morphisme de réduction modulo (π)*. De plus, comme π est premier, $A/(\pi)$ est intègre donc $A/(\pi)[X]$ aussi.*

Lemme 4.4.5. *Soit A un anneau factoriel. Alors tout élément irréductible de A est premier.*

Démonstration. Soit π un irréductible de A. Soit $(a,b) \in A^2$ t.q. $\pi \mid ab$. Alors $v_\pi(a) + v_\pi(b) = v_\pi(ab) > 0$ donc $v_\pi(a) > 0$ ou $v_\pi(b) > 0$. $\square$

Proposition 4.4.6. *Soit A un anneau factoriel muni d'un SRCI $\mathcal{P}$. Alors :*

$$\forall (P,Q) \in A[X] \setminus \{0_A\}^2 \,,\ c(PQ) = c(P)c(Q).$$

Démonstration. Soit P_1 et Q_1 des polynômes primitifs t.q. $P = c(P)P_1$ et $Q = c(Q)Q_1$. On a $PQ = c(P)c(Q)P_1Q_1$. Il suffit alors de prouver que P_1Q_1 est primitif. En effet, si P_1Q_1 n'est pas primitif, soit π un irréductible de A divisant $c\left(P_1Q_1\right)$. On réduit modulo (π) :

$$\overline{P_1} \cdot \overline{Q_1} = \overline{P_1Q_1} = 0_{A/(\pi)[X]}.$$

Comme $A/(\pi)[X]$ est intègre, $\overline{P_1} = 0_{A/(\pi)[X]}$ ou $\overline{Q_1} = 0_{A/(\pi)[X]}$. Donc P_1 ou Q_1 n'est pas primitif. C'est absurde. □

4.5 Théorème de Gauß

Proposition 4.5.1. *Soit A un anneau factoriel dont on note K_A le corps des fractions. Alors les irréductibles de $A[X]$ sont les irréductibles de A et les polynômes non constants, irréductibles dans $K_A[X]$, et primitifs.*

Théorème 4.5.2 (Théorème de Gauß)**.** *Si A est un anneau factoriel, alors $A[X]$ est factoriel.*

Démonstration. On va montrer que $A[X]$ est factoriel à l'aide de la proposition 4.2.7. Montrons que les hypothèses (i) et (ii) sont vérifiées. (i) Si $P \in A[X] \setminus \{0_A\}$, on décompose P en produit d'irréductibles de $K_A[X]$, où K_A est le corps des fractions de A, et on en déduit une décomposition de P en produit d'irréductibles de $A[X]$. (ii) Soit $P \in A[X]$ un élément irréductible. On veut prouver que P est premier, i.e. $A[X]/(P)$ est intègre. Si $P \in A$, alors $A[X]/(P) \simeq A/(P)[X]$, donc $A[X]/(P)$ est intègre. Sinon, P est primitif et irréductible dans $K_A[X]$. On considère alors le morphisme d'anneaux suivant :

$$\phi : A[X]/(P) \longrightarrow K_A[X]/(P).$$

Montrons que ϕ est injectif. Pour cela, soit $\Gamma \in \operatorname{Ker}\phi$ et $H \in \Gamma$. Alors il existe $D \in K_A[X]$ t.q. $H = DP$. Si $D = 0$, alors $D \in A[X]$. Sinon, $c(D) = c(D)c(P) = c(DP) = c(H) \in A$ car $H \in A[X]$, donc $D \in A[X]$. Donc $H \in (P)$ (dans $A[X]$), i.e. $\Gamma = 0_{A[X]/(P)}$. Donc ϕ est injectif et $A[X]/(P)$ est isomorphe à un sous-anneau de $K_A[X]/(P)$ (qui est intègre), donc $A[X]/(P)$ est intègre. □

5 Extensions de corps

5.1 Plongements et extensions de corps

Définition 5.1.1 (Plongement)**.** *On appelle* plongement *tout morphisme injectif d'anneaux.*

Définition 5.1.2 (Extension de corps)**.** *Soit K et L deux corps. S'il existe un plongement $\rho : K \to L$, on dit que L est une* extension *de K, ou encore que L/K est une* extension de corps*.*

Exemple 5.1.3. *$\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$ et $\mathbb{Q}\left[\sqrt{2}\right]/\mathbb{Q}$ sont des extensions de corps.*

Définition 5.1.4 (Corps algébriquement clos)**.** *Un corps K est dit* algébriquement clos *lorsque tout polynôme non constant de $K[X]$ admet une racine dans K.*

Théorème 5.1.5 (Théorème de d'Alembert-Gauß)**.** *$\mathbb{C}$ est algébriquement clos.*

5.2 Point de vue de l'algèbre linéaire

Définition 5.2.1 (Extension finie)**.** *Une extension de corps L/K est dite* finie *lorsque L est de dimension finie en tant que K-espace vectoriel. Sa dimension est alors appelée* degré *de l'extension L/K et notée $[L:K]$.*

Remarque 5.2.2. *Si L/K est une extension finie, où K est un corps fini, alors L est un corps fini et $|L| = |K|^{[L:K]}$.*

Théorème 5.2.3 (Théorème de la base télescopique)**.** *Soit M/L et L/K deux extensions finies. Alors M/K est une extension finie et :*

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

Plus précisément, si $(e_i)_{i\in I}$ est une K-base de L et $(f_j)_{j\in J}$ est une L-base de M, alors $(e_i f_j)_{(i,j)\in I\times J}$ est une K-base de M.

5.3 Éléments algébriques et transcendants

Notation 5.3.1. *Si B est un anneau, A un sous-anneau de B et $\alpha \in B$, on note $A[\alpha]$ le plus petit sous-anneau de B contenant A et α.*

Lemme 5.3.2. *Soit B un anneau, A un sous-anneau de B et $\alpha \in B$. Alors il existe un unique morphisme d'anneau $\delta_\alpha : A[X] \to B$ t.q.*

(i) *$\forall a \in A$, $\delta_\alpha(a) = a$.*

(ii) *$\delta_\alpha(X) = \alpha$.*

On a alors $A[\alpha] = \operatorname{Im}\delta_\alpha$.

Définition 5.3.3 (Élément algébrique ou transcendant)**.** *Soit L/K une extension de corps et $\alpha \in L$.*

(i) *On dit que α est* transcendant *sur K lorsque* $\operatorname{Ker}\delta_\alpha = \{0_A\}$.

(ii) *On dit que α est* algébrique *sur K lorsque* $\operatorname{Ker}\delta_\alpha \neq \{0_A\}$. *Comme $K[X]$ est principal, on note alors $P_\alpha \in K[X]$ l'unique polynôme unitaire t.q.* $\operatorname{Ker}\delta_\alpha = (P_\alpha)$. *$P_\alpha$ est appelé le* polynôme minimal *de α ; son degré est appelé* degré *de α.*

Notation 5.3.4. *Si L est un corps, K un sous-corps de L et $\alpha \in L$, on note $K(\alpha)$ le plus petit sous-corps de L contenant K et α.*

Théorème 5.3.5. *Soit L/K une extension de corps et $\alpha \in L$. Sont équivalentes :*

(i) *α est algébrique sur K.*

(ii) *$K[\alpha] = K(\alpha)$.*

(iii) *L'extension $K(\alpha)/K$ est finie.*

Définition 5.3.6 (Extension algébrique)**.** *Une extension de corps L/K est dite* algébrique *lorsque tout élément de L est algébrique sur K.*

Corollaire 5.3.7. *Toute extension finie est algébrique.*

Corollaire 5.3.8. *Soit L/K une extension de corps. On note L_{alg} l'ensemble des éléments de L algébriques sur K. Alors L_{alg} est un sous-corps de L, et l'extension L_{alg}/K est algébrique.*

5.4 Corps de rupture, corps de décomposition

Définition 5.4.1 (Corps de rupture)**.** *Soit K un corps et P un irréductible de $K[X]$. On appelle* corps de rupture *de P sur K tout corps L t.q. il existe $\alpha \in L$ t.q. $L = K[\alpha]$ et $P(\alpha) = 0$.*

Définition 5.4.2 (Corps de décomposition)**.** *Soit K un corps et $P \in K[X]$ un polynôme non constant. On dit que L est un* corps de décomposition *de P sur K lorsqu'il existe $(\alpha_1, \ldots, \alpha_s) \in L^s$, $u \in K^\times$ t.q. $L = K[\alpha_1, \ldots, \alpha_s]$ et $P = u \prod_{i=1}^{s} (X - \alpha_i)$.*

Définition 5.4.3 (K-morphisme)**.** *Soit $i : K \to L$ et $i' : K \to L'$ deux extensions de corps. On appelle K-*morphisme *tout morphisme de corps $\sigma : L \to L'$ t.q. $\sigma \circ i = i'$.*

Proposition 5.4.4. *Soit $j : K \to K'$ un isomorphisme de corps. On note $j : K[X] \to K'[X]$ le morphisme induit par j. Soit P un irréductible de $K[X]$. On note L et L' des corps de rupture respectifs de P sur K et de $j(P)$ sur K' ; et on note α et α' des racines respectives de P et $j(P)$ dans L et L'. Alors il existe un unique isomorphisme $\widetilde{j} : L \to L'$ prolongeant j et t.q. $j(\alpha) = \alpha'$.*

Théorème 5.4.5. *Soit K un corps et P un irréductible de $K[X]$. Alors il existe un corps de rupture de P sur K. De plus, le corps de rupture est unique à K-isomorphisme près.*

Théorème 5.4.6. *Soit K un corps et $P \in K[X]$ non constant. Alors il existe un corps de décomposition de P sur K. De plus, le corps de décomposition est unique à K-isomorphisme près. Il est noté $D_K(P)$.*

5.5 Corps finis

5.5.1 Caractéristique et sous-corps premier

Définition 5.5.1 (Caractéristique)**.** *Soit K un corps. On considère le morphisme d'anneaux :*

$$\vartheta : \left| \begin{array}{l} \mathbb{Z} \longrightarrow K \\ n \longmapsto n \cdot 1_K \end{array} \right. .$$

Si ϑ est injectif, on dit que K est de caractéristique nulle *et on note* $\operatorname{car} K = 0$*. Sinon, il existe un nombre premier p t.q.* $\operatorname{Ker} \vartheta = p\mathbb{Z}$*. Le nombre premier p est appelé* caractéristique *de K et noté* $\operatorname{car} K$*.*

Définition 5.5.2 (Sous-corps premier)**.** *Soit K un corps. On appelle* sous-corps premier *de K le plus petit sous-corps de K.*

Notation 5.5.3. *Si p est un nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.*

Proposition 5.5.4. *Soit K un corps.*

(i) *Si* $\operatorname{car} K = 0$*, alors le sous-corps premier de K est isomorphe à $\mathbb{Q}$.*

(ii) *Si* $\operatorname{car} K = p > 0$*, alors le sous-corps premier de K est isomorphe à $\mathbb{F}_p$.*

Proposition 5.5.5. *Soit K un corps de caractéristique $p > 0$. Alors l'application :*

$$F : x \in K \longmapsto x^p \in K$$

est un endomorphisme de corps, appelé endomorphisme de Frobenius *de K. Si K est fini, c'est un automorphisme induisant l'identité sur le corps premier.*

5.5.2 Classification des corps finis

Proposition 5.5.6. *Le cardinal d'un corps fini est toujours un* nombre primaire*, c'est-à-dire une puissance d'un nombre premier.*

Lemme 5.5.7. *Soit L un corps et $\phi : L \to L$ un endomorphisme de corps. Alors* $\mathrm{Ker}\,(\phi - id_L)$ *est un sous-corps de L.*

Théorème 5.5.8. *Soit p un nombre premier et $n \in \mathbb{N}^*$. Alors il existe un corps de cardinal p^n (donc de caractéristique p). Il est unique à $\mathbb{F}_p$-isomorphisme près. On le note $\mathbb{F}_{p^n}$.*

Démonstration. Considérer un corps de décomposition L de $X^{p^n} - X$ sur $\mathbb{F}_p$. En notant F l'endomorphisme de Frobenius de L, noter que les racines de $X^{p^n} - X$ sur L sont les éléments de $\mathrm{Ker}\,(F^n - id_L)$. D'après le lemme 5.5.7, $\mathrm{Ker}\,(F^n - id_L)$ est un sous-corps de L et contient toutes les racines de $X^{p^n} - X$, donc $L = \mathrm{Ker}\,(F^n - id_L)$. Ainsi, L est l'ensemble des racines de $X^{p^n} - X$, donc $|L| = p^n$. □

5.5.3 Groupe multiplicatif d'un corps fini

Lemme 5.5.9. *Soit A un anneau intègre et G un sous-groupe fini de $A^\times$. Alors G est cyclique.*

Proposition 5.5.10. *Soit q un nombre primaire. Alors $\mathbb{F}_q^\times$ est cyclique.*

5.5.4 Polynômes irréductibles d'un corps fini

Proposition 5.5.11. *Soit K un corps et soit $P \in K[X]$ un polynôme de degré $n \geqslant 1$. S'équivalent :*

(i) *P est irréductible sur K.*

(ii) *Pour toute extension L/K de degré inférieur ou égal à $\frac{n}{2}$, P n'a pas de racine dans L.*

Corollaire 5.5.12. *Soit p un nombre premier et $d \in \mathbb{N}^*$. Alors il existe un polynôme de $\mathbb{F}_p[X]$ irréductible unitaire de degré d.*

5.6 Clôture algébrique

Définition 5.6.1 (Clôture algébrique)**.** *Soit K un corps. On dit qu'un corps L est une* clôture algébrique *de K lorsque L est algébriquement clos et l'extension L/K est algébrique.*

Proposition 5.6.2. *Soit L/K une extension algébrique et soit Ω un corps algébriquement clos. Alors tout morphisme de corps $j : K \to \Omega$ se prolonge en un morphisme de corps $\widetilde{j} : L \to \Omega$.*

Démonstration. On considère :

$$\mathcal{F} = \left\{(F, \tau),\ F \text{ est un corps t.q. } K \subset F \subset L, \tau : F \to \Omega \text{ est un morphisme de corps t.q. } \tau_{|K} = j\right\}.$$

On munit $\mathcal{F}$ de l'ordre $\preccurlyeq$ défini par $(F, \tau) \preccurlyeq (F', \tau')$ ssi $F \subset F'$ et $\tau'_{|F} = \tau$. Alors l'ensemble ordonné $(\mathcal{F}, \preccurlyeq)$ est inductif ; selon le lemme de Zorn (théorème 3.2.3), il admet un élément maximal (F, τ). Supposons par l'absurde que $F \subsetneq L$ et soit $\alpha \in L \backslash F$. Alors α est algébrique sur K donc sur F (car l'extension L/K est supposée algébrique), soit donc P_α le polynôme minimal de α sur F. Soit $Q = \tau(P_\alpha) \in \Omega[X]$. Comme Ω est algébriquement clos, soit β une racine de Q dans Ω. D'après le lemme 5.4.4, on peut prolonger $\tau : F \to \Omega$ en un morphisme $\widetilde{\tau} : F[\alpha] \to \Omega$ t.q. $\widetilde{\tau}(\alpha) = \beta$. Ainsi, $(F, \tau) \preccurlyeq (F[\alpha], \widetilde{\tau})$ et $F \neq F[\alpha]$. Cela contredit la maximalité de (F, τ). Donc $F = L$. □

Lemme 5.6.3. *Soit L/K une extension algébrique et M/L une extension quelconque. Soit $x \in M$ un élément algébrique sur L. Alors x est algébrique sur K.*

Démonstration. Comme x est algébrique sur L, soit $P = \sum_{i=0}^{d} \lambda_i X^i \in L[X]\backslash\{0\}$ t.q. $P(x) = 0$. Pour $i \in \{0, \dots, d+1\}$, on pose $K_i = K[\lambda_0, \dots, \lambda_{i-1}]$. Alors, pour tout $i \in \{0, \dots, d\}$, $K_{i+1}/K_i = K_i[\lambda_i]/K_i$, et λ_i est dans L, donc λ_i est algébrique sur K donc sur K_i. Ainsi, l'extension K_{i+1}/K_i est finie. On en déduit que l'extension K_{d+1}/K est finie. Et l'extension $K_{d+1}[x]/K_{d+1}$ est finie car $P(x) = 0$ et $P \in K_{d+1}[X]\backslash\{0\}$. Donc $K_{d+1}[x]/K$ est finie, donc $K[x]/K$ est finie : x est algébrique sur K. □

Proposition 5.6.4. *Soit L/K une extension, avec L algébriquement clos. On note L_{alg} l'ensemble des éléments de L algébriques sur K. Alors L_{alg} est algébriquement clos ; c'est donc une clôture algébrique de K.*

Lemme 5.6.5. *Soit K un corps. Alors il existe une extension L/K t.q. tout polynôme non constant de $K[X]$ possède une racine dans L.*

Démonstration. On pose :

$$\mathcal{S} = \{X_P,\ P \in K[X]\backslash K\}.$$

Et on considère $K[\mathcal{S}]$ l'anneau des polynômes à indéterminées dans $\mathcal{S}$. On considère de plus :

$$I = (\{P(X_P),\ P \in K[X]\backslash K\}) \subset K[\mathcal{S}].$$

I est un idéal de $K[\mathcal{S}]$. Et $I \subsetneq K[\mathcal{S}]$ car $1 \notin I$. D'après le théorème de Krull (théorème 3.2.4), il existe un idéal maximal $\mathfrak{m}$ t.q. $I \subset \mathfrak{m} \subsetneq K[\mathcal{S}]$. On vérifie alors que, dans $K[\mathcal{S}]/\mathfrak{m}$ (qui est un corps), tout polynôme non constant de $K[X]$ admet une racine. □

Théorème 5.6.6 (Théorème de Steinitz)**.** *Soit K un corps. Alors K admet une clôture algébrique, et elle est unique à K-isomorphisme près.*

Démonstration. *Unicité.* Soit L_1 et L_2 deux clôtures algébriques de K. D'après la proposition 5.6.2, le plongement $\iota : K \to L_2$ se prolonge en un morphisme $j : L_1 \to L_2$. Alors j est injectif (car c'est un morphisme de corps). Reste à prouver que j est surjectif. Pour cela, soit $y \in L_2$. Comme L_2/K est une extension algébrique, soit $P \in K[X]\backslash\{0\}$ unitaire t.q. $P(y) = 0$. Comme L_1 est algébriquement clos, on décompose $P = \prod_{k=1}^{d} (X - x_i)$, avec $(x_1, \dots, x_d) \in L_1^d$. On note $K' = K[x_1, \dots, x_d]$, $K'' = K[j(x_1), \dots, j(x_d)]$. Notons que y est racine de P, donc $y \in K''$. De plus, $j(K') \subset K''$, j est injectif, et K' et K'' sont de même dimension sur K, donc $j(K') = K''$. Donc $y \in K'' = j(K') \subset j(L_1)$. Donc j est un isomorphisme. *Existence.* D'après la proposition 5.6.4, il suffit de prouver que K admet une extension L/K, avec L algébriquement clos. Pour cela, on construit une suite de corps $(L_k)_{k\in\mathbb{N}}$ en posant $L_0 = K$, puis $L_{k+1} \supset L_k$ t.q. tout polynôme non constant de $L_k[X]$ possède une racine dans L_{k+1} (selon le lemme 5.6.5). On pose alors $L = \bigcup_{k\in\mathbb{N}} L_k$ et on vérifie que L est un corps algébriquement clos contenant K. □

5.7 Polynômes symétriques

Définition 5.7.1 (Polynôme symétrique)**.** *Soit A un anneau commutatif et $n \in \mathbb{N}^*$. Un polynôme $P \in A[X_1, \dots, X_n]$ est dit* symétrique *lorsque :*

$$\forall \tau \in \mathfrak{S}_n,\ P\left(X_{\tau(1)}, \dots, X_{\tau(n)}\right) = P(X_1, \dots, X_n).$$

L'ensemble des polynômes symétriques de $A[X_1, \dots, X_n]$ forme un sous-anneau de $A[X_1, \dots, X_n]$.

Notation 5.7.2 (Polynômes symétriques élémentaires)**.** *Soit A un anneau commutatif et $n \in \mathbb{N}^*$. Pour $p \in \{1, \dots, n\}$, on pose :*

$$\sigma_p = \sum_{1 \leqslant i_1 < \dots < i_p \leqslant n} X_{i_1} \cdots X_{i_p} \in A[X_1, \dots, X_n].$$

Le polynôme σ_p est symétrique.

Proposition 5.7.3. *Soit A un anneau commutatif et $n \in \mathbb{N}^*$. On a :*

$$\prod_{j=1}^{n}(T - X_j) = T^n + \sum_{p=1}^{n}(-1)^p \sigma_p T^{n-p} \in (A[X_1, \dots, X_n])[T].$$

Corollaire 5.7.4. *Soit K un corps. Soit $P = \sum_{j=0}^{n} a_j X^j \in K[X]$, avec $a_n \neq 0$, $n \geqslant 1$. Soit $\alpha_1, \dots, \alpha_n$ les racines de P dans une extension L/K dans laquelle P est scindé. Alors :*

$$\forall p \in \{1, \dots, n\}, \ \sigma_p(\alpha_1, \dots, \alpha_n) = (-1)^p \frac{a_{n-p}}{a_n}.$$

Théorème 5.7.5. *Soit A un anneau commutatif et $n \in \mathbb{N}^*$. Si $P \in A[X_1, \dots, X_n]$ est un polynôme symétrique, alors il existe un unique polynôme $Q \in A[T_1, \dots, T_n]$ t.q.*

$$P = Q(\sigma_1, \dots, \sigma_n).$$

6 Théorie de Galois

6.1 K-morphismes et séparabilité

6.1.1 Morphismes d'une extension monogène

Définition 6.1.1 (Extension monogène)**.** *Une extension L/K est dite monogène lorsqu'il existe $\alpha \in L$ t.q. $L = K[\alpha]$.*

Proposition 6.1.2. *Soit L/K une extension monogène, $\alpha \in L$ t.q. $L = K[\alpha]$, P_α le polynôme minimal de α sur K. Si Ω est une clôture algébrique de K, alors l'application :*

$$\left| \begin{array}{rcl} \mathrm{Hom}_K(L, \Omega) & \longrightarrow & \mathcal{R}_\Omega(P_\alpha) \\ f & \longmapsto & f(x) \end{array} \right.$$

est une bijection entre l'ensemble $\mathrm{Hom}_K(L, \Omega)$ *des K-morphismes $L \to \Omega$ et l'ensemble $\mathcal{R}_\Omega(P_\alpha)$ des racines de P_α sur Ω.*

6.1.2 Séparabilité

Définition 6.1.3 (Polynôme séparable)**.** *Soit K un corps et $P \in K[X]$. S'équivalent :*

(i) *Les racines de P dans une clôture algébrique de K sont simples.*

(ii) *P et P' sont premiers entre eux dans $K[X]$.*

Si ces propriétés sont vérifiées, on dit que P est séparable*.*

Définition 6.1.4 (Élément séparable et extension séparable)**.** *Si L/K est une extension algébrique, un élément $\alpha \in L$ est dit* séparable *sur K si son polynôme minimal sur K est séparable. On dit de plus que l'extension L/K est* séparable *lorsque tout élément de L est séparable sur K.*

Lemme 6.1.5. *Soit L/K une extension algébrique et Ω une clôture algébrique de L. Si $\alpha \in \Omega$ est séparable sur K, alors α est séparable sur L.*

Démonstration. Le polynôme minimal de α sur L divise le polynôme minimal de α sur K. $\square$

Théorème 6.1.6. *Soit L/K une extension finie et Ω une clôture algébrique de K. Soit $N = |\mathrm{Hom}_K(L, \Omega)|$ le nombre de K-morphismes distincts $L \to \Omega$. Alors on a :*

$$1 \leqslant N \leqslant [L : K].$$

De plus, les assertions suivantes sont équivalentes :

(i) *$N = [L : K]$.*

(ii) *Il existe des éléments $x_1, \dots, x_n$ de L séparables sur K t.q. $L = K[x_1, \dots, x_n]$.*

(iii) *L'extension L/K est séparable.*

Démonstration. Par récurrence à l'aide de la proposition 6.1.2. $\square$

6.1.3 Corps parfaits

Définition 6.1.7 (Corps parfait)**.** *Soit K un corps. Sont équivalentes :*

(i) *Tout polynôme irréductible de $K[X]$ est séparable.*

(ii) *Tout élément d'une clôture algébrique de K est séparable sur K.*

(iii) *Toute extension algébrique de K est séparable.*

(iv) *Pour toute extension finie L/K, le nombre de K-morphismes distincts de L dans une extension algébriquement close de K est égal à $[L : K]$.*

On dit alors que K est un corps parfait.

Proposition 6.1.8. *Toute extension algébrique d'un corps parfait est un corps parfait.*

Proposition 6.1.9. *Un corps est parfait* ssi *il est de caractéristique nulle* ou *son* endomorphisme de Frobenius *(c.f. proposition 5.5.5) est bijectif.*

Corollaire 6.1.10. *Les corps finis sont parfaits.*

6.2 Groupe d'automorphismes d'une extension

Définition 6.2.1 (K-automorphisme)**.** *Soit L/K une extension de corps. Un* K-automorphisme *de L est un K-morphisme bijectif $L \to L$. On note* $\mathrm{Aut}(L/K)$ *le groupe des K-automorphismes de L.*

Remarque 6.2.2. *Soit L/K une extension de corps et $\sigma \in \mathrm{Aut}(L/K)$. Si $P \in K[X]$, alors :*

$$\forall x \in L,\ \sigma\left(P(x)\right) = P\left(\sigma(x)\right).$$

Par conséquent, σ agit par permutation sur l'ensemble des racines de P dans L.

Remarque 6.2.3. *Si L/K est une extension finie, alors tout K-morphisme $L \to L$ est un K-automorphisme de L.*

Proposition 6.2.4. *Soit L/K une extension finie. Alors le groupe* $\mathrm{Aut}(L/K)$ *est fini et :*

$$\left|\mathrm{Aut}\left(L/K\right)\right| \leqslant [L : K].$$

En cas d'égalité, l'extension L/K est séparable.

Définition 6.2.5 (Extension normale)**.** *Soit L/K une extension finie. On dit que L/K est une* extension normale *lorsque tout polynôme irréductible de $K[X]$ qui a une racine dans L est scindé sur L.*

Définition 6.2.6 (Extension galoisienne)**.** *Soit L/K une extension finie. Sont équivalentes :*

(i) $\left|\mathrm{Aut}\left(L/K\right)\right| = [L : K]$.

(ii) *L'extension L/K est séparable et tout K-morphisme de L dans une clôture algébrique de L a pour image L.*

(iii) *L'extension L/K est normale et séparable.*

(iv) *Il existe un polynôme $P \in K[X]$ séparable dont L/K est une extension de décomposition.*

On dit alors que l'extension L/K est galoisienne. *Le groupe* $\mathrm{Aut}(L/K)$ *est alors appelé* groupe de Galois *de L/K et noté* $\mathrm{Gal}(L/K)$.

6.3 Lemme d'Artin

Notation 6.3.1. *Si L est un corps et G est un groupe d'automorphismes de L, on pose :*

$$L^G = \{x \in L,\ \forall \sigma \in G,\ \sigma(x) = x\}.$$

Théorème 6.3.2 (Lemme d'Artin)**.** *Soit L un corps et G un groupe fini d'automorphismes de L. Alors L^G est un sous-corps de L, l'extension L/L^G est finie et :*

$$\left[L : L^G\right] = |G|.$$

En particulier, l'extension L/L^G est galoisienne de groupe de Galois G.

Démonstration. On a $L^G = \bigcap_{\sigma \in G} \mathrm{Ker}\,(\sigma - id_L)$, donc L^G est un sous-corps de L selon le lemme 5.5.7. Supposons par l'absurde que $|G| < \left[L : L^G\right] \leqslant +\infty$. Soit $n = |G|$. On note $G = \{\sigma_1, \dots, \sigma_n\}$. Par hypothèse, il existe un $(n+1)$-uplet $(a_1, \dots, a_{n+1}) \in L^{n+1}$ qui est L^G-libre. On considère l'application linéaire :

$$f : \left| \begin{array}{rcl} L^{n+1} & \longrightarrow & L^n \\ (x_1, \dots, x_{n+1}) & \longmapsto & \left(\displaystyle\sum_{j=1}^{n+1} \sigma_i(a_j)\, x_j\right)_{1 \leqslant i \leqslant n} \end{array} \right. .$$

Alors f admet un noyau non trivial ; soit $(x_1, \dots, x_{n+1}) \in \mathrm{Ker}\, f \backslash \{0\}$ dont le nombre m de coefficients non nuls est minimal. On peut supposer que les coefficients non nuls de $(x_1, \dots, x_n)$ sont les m premiers, et que $x_m = 1$. On a alors :

$$\forall \sigma \in G,\ \sum_{j=1}^{m-1} \sigma(a_j)\, x_j + \sigma(a_m) = 0. \tag{$*$}$$

Montrons que $(x_1, \dots, x_{n+1}) \in \left(L^G\right)^{n+1}$. En effet, si $\tau \in G$, la relation $(*)$ appliquée à $\tau^{-1} \circ \sigma$ fournit $\sum_{j=1}^{m-1} \sigma(a_j)\, \tau(x_j) + \sigma(a_m) = 0$ pour tout $\sigma \in G$. Par différence :

$$\forall \tau \in G,\ \forall \sigma \in G,\ \sum_{j=1}^{m-1} \sigma(a_j)\left(\tau(x_j) - x_j\right) = 0.$$

Donc $\forall \tau \in G,\ \left(\tau(x_j) - x_j\right)_{1 \leqslant j \leqslant n+1} \in \mathrm{Ker}\, f$. Par minimalité de m :

$$\forall j \in \{1, \dots, n+1\},\ \forall \tau \in G,\ \tau(x_j) = x_j.$$

Donc $(x_1, \dots, x_{n+1}) \in \left(L^G\right)^{n+1} \backslash \{0\}$. Comme $\sum_{j=1}^{n+1} a_j x_j = 0$, la famille $(a_1, \dots, a_{n+1})$ est L^G-liée, ce qui est absurde. Ainsi, l'extension L/L^G est finie et $\left[L : L^G\right] \leqslant |G|$. De plus $|G| \leqslant \left|\mathrm{Aut}\left(L/L^G\right)\right| \leqslant \left[L : L^G\right]$, d'où le résultat. □

6.4 Correspondance de Galois

Théorème 6.4.1 (Correspondance de Galois)**.** *Soit L/K une extension finie galoisienne.*

(i) *Pour tout sous-groupe $H \subset \mathrm{Gal}\,(L/K)$, l'ensemble L^H est un sous-corps de L contenant K, et $\left[L^H : K\right]$ est égal à l'indice de H dans* $\mathrm{Gal}\,(L/K)$.

(ii) *Pour tout sous-corps F de L contenant K, l'extension L/F est galoisienne et* $\mathrm{Gal}\,(L/F) = \{\sigma \in \mathrm{Gal}\,(L/K),\ \forall x \in F,\ \sigma(x) = x\}$.

(iii) *Les applications $H \longmapsto L^H$ et $F \longmapsto \mathrm{Gal}\,(L/F)$ sont des bijections décroissantes, réciproques l'une de l'autre, entre l'ensemble des sous-groupes de* $\mathrm{Gal}\,(L/K)$ *et l'ensemble des sous-corps de L contenant K.*

Définition 6.4.2. *Si G est un groupe et H est un sous-groupe de G, on définit le* normalisateur *de H dans G par :*

$$N_G(H) = \left\{ g \in G,\ gHg^{-1} = H \right\}.$$

Proposition 6.4.3. *Soit L/K une extension finie galoisienne et soit H un sous-groupe de* $\mathrm{Gal}\,(L/K)$.

(i) *Pour tout $\sigma \in \mathrm{Gal}\,(L/K)$, on a :*

$$\sigma\left(L^H\right) = L^{\sigma H \sigma^{-1}}.$$

Ainsi, le normalisateur de H dans $\mathrm{Gal}\,(L/K)$ *est* $\left\{\sigma \in \mathrm{Gal}\,(L/K)\,,\ \sigma\left(L^H\right) \subset L^H\right\}$.

(ii) *L'application :*

$$\left|\begin{aligned} N_{\mathrm{Gal}(L/K)}(H) &\longrightarrow \mathrm{Aut}\left(L^H/K\right) \\ \sigma &\longmapsto \sigma_{|L^H} \end{aligned}\right.$$

est un morphisme surjectif de groupes de noyau H. En particulier, l'extension L^H/K est galoisienne ssi *H est distingué dans* $\mathrm{Gal}\,(L/K)$. *Si tel est le cas, alors :*

$$\mathrm{Gal}\left(L^H/K\right) \simeq \mathrm{Gal}\,(L/K)\,/H.$$

Proposition 6.4.4. *Soit K un corps, Ω une clôture algébrique de K, et L une extension finie séparable de K contenue dans Ω. Il existe alors une plus petite extension L^{g}/L contenue dans Ω t.q. l'extension L^{g}/K soit galoisienne. On dit que L^{g} est une* clôture galoisienne *de l'extension L/K.*

Corollaire 6.4.5. *Si L/K est une extension finie séparable, alors L n'admet qu'un nombre fini de sous-corps contenant K.*

Démonstration. Soit L^{g} une clôture galoisienne de L/K. La correspondance de Galois montre que l'ensemble des sous-corps de L contenant K est en bijection avec l'ensemble des sous-groupes de $\mathrm{Gal}\,(L^{\mathrm{g}}/K)$ contenant $\mathrm{Gal}\,(L^{\mathrm{g}}/L)$. Le résultat découle alors du fait qu'un groupe fini n'a qu'un nombre fini de sous-groupes. □

6.5 Action du groupe de Galois sur les racines

Proposition 6.5.1. *Soit K un corps, $P \in K[X]$ un polynôme séparable et L une extension de décomposition de P sur K.*

(i) $\mathrm{Gal}(L/K)$ *agit par permutation sur l'ensemble $\mathcal{R}_L(P)$ des racines de P dans L.*

(ii) *L'action de* $\mathrm{Gal}(L/K)$ *sur $\mathcal{R}_L(P)$ est fidèle.*

(iii) *L'action de* $\mathrm{Gal}(L/K)$ *sur $\mathcal{R}_L(P)$ est transitive* ssi *P est irréductible.*

6.6 Théorème de l'élément primitif

Lemme 6.6.1. *Soit K un corps infini, V un K-espace vectoriel de dimension finie, $V_1, \ldots, V_n$ une famille finie de sous-espaces vectoriels stricts de V. Alors $\bigcup_{i=1}^n V_i \subsetneq V$.*

Théorème 6.6.2 (Théorème de l'élément primitif)**.** *Soit L/K une extension finie séparable. Alors l'extension L/K est monogène, i.e. il existe $x \in L$ t.q. $L = K[x]$.*

Démonstration (Première méthode)**.** *Premier cas* : K est fini. Alors L est fini, donc $L^\times$ est un groupe cyclique engendré par $x \in L^\times$ (c.f. proposition 5.5.10). Ainsi, $L = K^\times$. *Second cas* : K est infini. Selon le corollaire 6.4.5, l'ensemble $\mathcal{H} = \{K[x],\ x \in L\}$ est fini. De plus, on a $\bigcup_{M\in\mathcal{H}} M = L$ car $\forall x \in L,\ x \in K[x]$. D'après le lemme 6.6.1, il existe $M \in \mathcal{H}$ t.q. $L = M$. Autrement dit, il existe $x \in L$ t.q. $L = K[x]$. □

Démonstration (Deuxième méthode)**.** Par récurrence, on se ramène au cas où $L = K[x, y]$, et on cherche à montrer que $\exists z \in L,\ L = K[z]$. Si K est fini, alors $L^\times$ est cyclique et L/K est monogène ; on peut donc supposer K infini. Soit P_x et P_y les polynômes minimaux respectifs de x et y sur K. On pose Ω une clôture algébrique de L et on écrit dans Ω :

$$P_x = \prod_{i=1}^{r} (X - x_i) \qquad \text{et} \qquad P_y = \prod_{j=1}^{s} (X - y_j)\,,$$

avec $x = x_1$ et $y = y_1$, et les $(x_i)_{1 \leqslant i \leqslant r} \in \Omega^r$ deux à deux distincts et les $(y_j)_{1 \leqslant j \leqslant s} \in \Omega^s$ aussi car l'extension L/K est séparable. Comme K est infini, il existe $c \in K$ t.q. $\forall (i, j) \neq (1, 1),\ x_i + cy_j \neq x_1 + cy_1$. Posons $z = x + cy$ et montrons que $L = K[z]$. Pour cela, posons :

$$R = P_x\,(z - cX) \in (K[z])\,[X].$$

On a $R(y) = 0$. De plus, $\forall j \neq 1,\ R\,(y_j) \neq 0$ par choix de c. On en déduit que $R \wedge P_y = X - y$. Or $R \in (K[z])\,[X],\ P_y \in K[X] \subset (K[z])\,[X]$, donc $R \wedge P_y \in (K[z])\,[X]$, d'où $y \in K[z]$, puis $x \in K[z]$, d'où $L = K[x, y] \subset K[z]$. $\square$

Remarque 6.6.3. *Une autre approche de la théorie de Galois consisterait à démontrer d'abord le théorème de l'élément primitif (avec la deuxième démonstration ci-dessus, donc sans utiliser de théorie de Galois), puis en déduire les théorèmes de théorie de Galois. Ceci permet de ne considérer que des extensions monogènes.*

Références

[1] N. Bourbaki. *Algèbre.*

[2] N. Jacobson. *Basic algebra.*

[3] S. Lang. *Algebra.*