Structures algébriques 2
Licence 3, UE 4TMF505U, 2019-2020
Université de Bordeaux

Qing Liu

Table des matières

Chapitre 1

Anneaux et idéaux

Beaucoup d'ensembles qu'on a rencontrés jusqu'à présent comme $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $M_n(\mathbb{R})$, $C^0(X, \mathbb{R})$ etc ont une propriété commune c'est qu'ils ont une structure d'anneaux. Une telle structure algébrique apporte des outils importants pour étudier les objets concernés.

Nous commençons par rappeler quelques notions déjà abordées dans l'UE Structures Algébriques 1.

1.1 Groupes

Définition 1.1.1 Un *groupe* est la donnée d'un ensemble G muni d'une loi de composition interne $*$ (souvent appelée multiplication) qui vérifie les propriétés suivantes :

(1) Associativité : $(a * b) * c = a * (b * c)$ pour tous $a, b, c \in G$.

(2) Élément unité : il existe $e \in G$ tel que $e * a = a * e = a$ pour tout $a \in G$.

(3) Inverse : pour tout $a \in G$, il existe $b \in G$ tel que $a * b = b * a = e$.

L'élement unité et l'inverse sont uniques. Le groupe G est *commutatif* si $a * b = b * a$ pour tous $a, b \in G$.

Dans la pratique, on écrira généralement ab à la place de $a * b$. Lorsque G est commutatif, on a tendance à noter la loi de composition par $+$, l'élément unité est alors noté 0.

Exemple 1.1.2 $\mathbb{Z}$; $n\mathbb{Z}$; $\mathbb{R}[X]$; l'ensemble des applications $X \to \mathbb{R}$ pour un ensemble non vide X fixé.

Définition 1.1.3 Sous-groupes. Homomorphismes (ou morphismes) de groupes. Noyau et image d'un homomorphisme de groupes.

Pour toute relation équivalence $\sim$ sur G, on peut considérer l'ensemble quotient $G/\sim$ et la surjection canonique $s : G \to G/\sim$ (qui envoie un élément de G sur sa classe d'équivalence modulo $\sim$). On voudrait que $G/\sim$ soit muni

d'une structure groupe et surtout que la surjection canonique soit alors un homomorphisme de groupes (ce qui veut dire que la structure de groupe sur le quotient est induite par celle de G). Pour cela, il faut et il suffit que la relation soit définie par un sous-groupe distingué.

Définition 1.1.4 Un sous-groupe H est G est dit *distingué* (ou normal) s'il est invariant par conjugaison : pour tout $h \in H$, on a $ghg^{-1} \in H$ pour tous $g \in G$.

Exemple 1.1.5
1. Dans un groupe commutatif, tout sous-groupe est distingué. Mais il existe des groupes non-commutatifs pour lesquels cette propriété est vraie.
2. Le noyau d'un noyau homomorphisme de groupes $G \to K$ est toujours un sous-groupe distingué de G (par contre l'image n'a aucune raison d'être un sous-groupe distingé dans K).
3. Ainsi, l'ensemble $\mathrm{Sl}_n(\mathbb{Q})$ des matrices carrées rationnelles d'ordre n de determinant 1 est un sous-groupe distingué du groupe des matrices inversibles $\mathrm{Gl}_n(\mathbb{Q})$.

Exemple 1.1.6 Un *commutateur* dans G est un élément de la forme $[a, b] := aba^{-1}b^{-1}$ avec $a, b \in G$. L'ensemble des commutateurs dans G contient l'élément neutre de G et est stable par inversion : $[a, b]^{-1} = [b, a]$ mais n'est pas stable par produit en général. Donc ce n'est pas un sous-groupe de G en général. Le sous-groupe engendré les commutateurs, c'est-à-dire l'ensemble des produits finis de commutateurs est noté $[G, G]$ est appelé le *groupe dérivé de* G.

Par définition, on a $ab = [a, b]ba$. Donc si $gcg^{-1} = [g, c]c$ pour tous $g, c \in G$. En particulier, si c est un produit de (disons n) commutateurs, alors gcg^{-1} est le produit de $n + 1$ commutateurs. Par conséquent $[G, G]$ est un sous-groupe distingué de G. On montre facilement que qu'il est contenu dans le noyau de tout homomorphisme de G dans un groupe commutatif.

Retournons aux quotients. Soit H un sous-groupe de G. On définit une relation d'équivalence sur G en posant $a \sim b$ si $ab^{-1} \in H$ (le fait que ce soit une relation d'équivalence vient de l'hypothèse que H est un sous-groupe). Notons par G/H l'ensemble quotient.

Proposition 1.1.7. *Soit $\sim$ une relation d'équivalence sur un groupe G. Il existe une structure de groupe sur $G/\sim$ telle que la surjection canonique $\pi : G \to G/\sim$ soit un homomorphisme de groupes si et seulement si $\sim$ est donnée comme ci-dessus par un sous-groupe de H distingué dans G.*

Démonstration. Supposons que $\sim$ soit donnée par un sous-groupe distingué H. Pour tous $x, y \in G/H$, on écrit $x = \pi(a), y = \pi(b)$ pour certains $a, b \in G$ et on pose

$$x * y = \pi(ab).$$

On vérifie que c'est bien défini (que le membre de droite ne dépend du choix de $a, b \in G$) grâce à l'hypothèse que H est un sous-groupe distingué. On vérifie

alors directement qu'on obtient une structure de groupe sur G/H et que π est un homomorphisme de groupes.

Réciproquement, si $G/\sim$ est un groupe et que π est un homomorphisme de groupes, alors on vérifie (exercice) que $\sim$ est donnée par le sous-groupe $\operatorname{Ker}\pi$ (donc nécessairement distingué). □

Définition 1.1.8 Un *groupe quotient* de G est un groupe de la forme G/H avec un sous-groupe distingué H de G.

Exemple 1.1.9 $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1.1.10 Trouver une condition nécessaire et suffisante, relative au groupe dérivé $[G,G]$, pour que G/H soit commutatif.

Théorème 1.1.11 (Théorème de factorisation)**.** *Soit $f : G \to K$ un homomorphisme de groupes. Soit $H \subseteq \operatorname{Ker} f$ un sous-groupe distingué de G et notons $\pi : G \to G/H$ la surjection canonique.*

(1) *Il existe une factorisation*
$$f = \tilde{f} \circ \pi$$
avec un homomorphisme de groupes $\tilde{f} : G/H \to K$. Un tel homomorphisme $\tilde{f}$ est unique.

(2) *On a $\operatorname{Im}(\tilde{f}) = \operatorname{Im}(f)$. En particulier $\tilde{f}$ est surjectif si et seulement si f est surjectif.*

(3) *L'homomorphisme $\tilde{f}$ est injectif si et seulement si $H = \operatorname{Ker} f$;*

Démonstration. On définit $\tilde{f}$ par
$$\tilde{f}(\pi(g)) = f(g), \quad \forall g \in G.$$
Le fait que $\tilde{f}$ soit bien définie, c'est-à-dire que $\pi(g) = \pi(g')$ implique que $f(g) = f(g')$ vient de la condition $H \subseteq \operatorname{Ker} f$. Il est alors aisé de vérifier le reste des propriétés. □

Corollaire 1.1.12. *Si $f : G \to K$ est un homomorphisme surjectif, alors f induit un isomorphisme de groupes $\tilde{f} : G/\operatorname{Ker} f \to K$.*

Corollaire 1.1.13. *Tout homomorphisme de groupes $f : G \to K$ se factorise en l'homomorphisme surjectif $s : G \to G/\operatorname{Ker} f$ suivi d'un homomorphisme injectif $G/\operatorname{Ker} f \to K$.*

Exemple 1.1.14 Soient $n, m \geq 1$ des entiers naturels. Alors la surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ se factorise en la surjection canonique canonique $\mathbb{Z} \to \mathbb{Z}/nm\mathbb{Z}$ suivie d'un homomorphisme surjectif $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

1.2 Anneaux

Définition 1.2.1 Un *anneau* est la donnée d'un ensemble A muni de deux lois de composition internes $+$ (addition) et $*$ (multiplication) qui vérifient les propriétés suivantes :

(1) $(A, +)$ est un groupe commutatif ;

(2) Associativité : $(a * b) * c = a * (b * c)$ pour tous $a, b, c \in A$.

(3) Distributivité : $a * (b + c) = a * b + a * c$, $(b + c) * a = b * a + c * a$ pour tous $a, b, c \in A$.

Dans la pratique, on écrira généralement ab à la place de $a * b$. L'élément neutre pour la loi de groupe est noté 0 (ou 0_A si la précision est nécessaire). On dit que A est *commutatif* si $ab = ba$ pour tous $a, b \in A$.

Définition 1.2.2 Un élément $e \in A$ tel que $e * a = a * e$ pour tout $a \in A$ est appelé l'*élément unité* de A et est noté 1 (ou 1_A si la précision est nécessaire). S'il existe un élément unité, il est alors unique (si e et e' sont des éléments unités, alors $e = e * e' = e'$). Un anneau possédant un élément unité est appelé un *anneau unitaire*.

Lemme 1.2.3. *Soit A un anneau. Pour tout $a \in A$, on a $0 * a = a * 0 = 0$, et, si A est unitaire, $(-1) * a = a * (-1) = -a$ (où $-a$ désigne l'opposé de a pour la loi de groupe sur $(A, +)$).*

Preuve: On a $0 * a + 0 * a = (0 + 0) * a = 0 * a$. Donc $0 * a = 0$. De même $a * 0 = 0$. Si A est unitaire, on a $(-1) * a + a = (-1) * a + 1 * a = (-1 + 1) * a = 0 * a = 0$, donc $(-1) * a = -a$. L'égalité $a * (-1) = -a$ se démontre de la même façon.

Exemple 1.2.4 Les $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$; $\mathbb{R}[X]$ sont des anneaux commutatifs unitaires ; $n\mathbb{Z}$ est un anneau non-unitaire si $n \geq 2$; les anneaux de matrices $M_n(\mathbb{R})$ sont unitaires, mais ne sont pas commutatifs si $n \geq 2$; D'autres exemples naturels sont les anneaux de fonctions continues d'un espace topologique dans $\mathbb{R}$;

Dans la suite, on ne considérera que des anneaux unitaires.

Remarque 1.2.5 L'ensemble $\{0\}$ réduit à un élément est muni d'une structure d'anneau unitaire. Par ailleurs, un anneau unitaire A est nul (c'est-à-dire réduit à un élément) si et seulement si $0_A = 1_A$. En effet, si l'égalité est vraie, alors pour tout $a \in A$, on a $a = 1 * a = 0 * a = 0$. L'implication dans l'autre sens est évidente.

Question 1.2.6 L'ensemble vide possède-il une structure d'anneau ?

Définition 1.2.7 Soient A, B des anneaux (unitaires). Une application $f : A \to B$ est appelé un *homomorphisme d'anneaux* si

(1) $f(a + a') = f(a) + f(a')$ pour tous $a, a' \in A$ (c'est-à-dire que f est un homomorphisme pour les structures de groupe sous-jaccentes),

(2) $f(aa') = f(a)f(a')$ pour tous $a, a' \in A$,

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

Noter qu'on a alors $f(0_A) = 0_B$, $f(-a) = -f(a)$ et $f(a - a') = f(a) - f(a')$.

On dit que f est un *isomorphisme d'anneaux* si c'est un homomorphisme d'anneaux et si c'est une application bijective. On voit alors facilement que l'application réciproque $f^{-1} : B \to A$ est aussi un homomorphisme d'anneaux. Un homomorphisme $A \to A$ est appelé un *endomorphisme de* A. Un isomorphisme $A \to A$ est appelé un *automorphisme* de A.

Exemple 1.2.8 L'application $\mathbb{R}[X] \to \mathbb{R}$ qui à tout $P(X)$ associe $P(0)$ est un homomorphisme d'anneaux.

Exemple 1.2.9 L'application identité $A \to A$ est un automorphisme. L'application constante $A \to B$, $a \mapsto 0$ n'est pas un homomorphisme si $B \neq 0$. La surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un homomorphisme.

Exemple 1.2.10 Soit $n \geq 2$. L'application det : $M_n(\mathbb{Q}) \to \mathbb{Q}$ qui à une matrice carrée d'ordre n associe son déterminant n'est pas un homomorphisme d'anneaux car il n'est pas compatible avec l'addition. L'application trace qui à une matrice carré associe la somme de ses éléments diagonaux est compatible avec l'addition mais pas avec la multiplication. Ce n'est donc pas un homomorphisme d'anneaux non plus.

Exercice 1.2.11 Soit A un anneau (unitaire). Montrer qu'il existe un et un seul homomorphisme d'anneaux $\mathbb{Z} \to A$.

Inversement, soit R un anneau tel que pour tout anneau A il existe un unique homomorphisme d'anneaux $R \to A$. Montrer qu'il existe un (unique) isomorphisme d'anneaux $\mathbb{Z} \to R$.

Dans la suite, on ne considérera que des anneaux unitaires et commutatifs.

Nous allons donner quelques procédés de construction d'anneaux.

Définition 1.2.12 Soient A, B deux anneaux. Le produit $A \times B$, muni de l'addition et de la multiplication termes à termes est un anneau appelé *le produit des anneaux* A, B. On définit similairement le produit d'un ensemble d'anneaux indexé par un ensemble quelconque. Si les anneaux en question sont commutatifs et unitaires, il en sera de même du produit.

Un cas particulier est l'ensemble A^X des applications d'un ensemble X vers un anneau donné A. L'addition et le produit se font sur les valeurs des applications. Quand $X = \mathbb{N}$, c'est l'ensemble des suites à valeurs dans A.

Remarque 1.2.13 La projection $A \times B \to A$, $(a, b) \mapsto a$ est un homomorphisme d'anneaux. Mais l'application naturelle $A \to A \times B$, $a \mapsto (a, 0)$ n'en est pas un si $B \neq \{0\}$ puisqu'il n'envoie pas 1 sur 1.

Définition 1.2.14 Un *sous-anneau* R d'un anneau A est un sous-groupe de A qui est stable par multiplication et qui contient l'unité 1_A. Cela revient à dire que :

1. $0_A, 1_A \in R$;
2. $x - y, xy \in R$ pour tous $x, y \in R$.

Par exemple, $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$. Mais $\mathbb{N}$ n'est pas un sous-anneau de $\mathbb{Z}$.

Exemple 1.2.15 Soit A l'ensemble des suites de Cauchy rationnelles $(r_n)_{n\geq 0}$. C'est un sous-anneau de $\mathbb{Q}^{\mathbb{N}}$. Soit $\varphi : A \to \mathbb{R}$ l'application qui à $(r_n)_n$ associe sa limite dans $\mathbb{R}$. Alors, parce que la limite commute avec la somme et le produit, φ est un homomorphisme d'anneaux. Il est surjectif car $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Cet exemple suppose l'existence du corps $\mathbb{R}$ comme un corps archimédien complet dans lequel $\mathbb{Q}$ est dense. On reviendra plus tard à cette question.

Exercice 1.2.16 Montrer que l'image d'un homomorphisme d'anneaux $A \to B$ est un sous-anneau de B.

Exercice 1.2.17 Soit I un intervalle ouvert de $\mathbb{R}$. Soit $A(I, \mathbb{R})$ l'anneau des fonctions de I dans $\mathbb{R}$. Montrer que $C^0(I, \mathbb{R})$, $C^1(I, \mathbb{R})$, $C^{+\infty}(I, \mathbb{R})$ sont des sous-anneaux de $A(I, \mathbb{R})$.

Nous connaissons bien les anneaux de polynômes à une variable à coefficients dans un corps. Nous allons maintenant aborder les polynômes à plusieurs variables. Une des applications importantes de la théorie des anneaux et corps commutatifs est la résolution d'équations polynômiales du type $x^5+y^5=z^5$ ou $y^2=x^3+1$ dans $\mathbb{Z}$ ou dans $\mathbb{Q}$.

Pour cela nous allons introduire la notion des polynômes à coefficients dans un anneau.

Définition 1.2.18 Soit A un anneau (commutatif unitaire). Soit $A[X]$ l'ensemble des suites finies à coefficients dans A (c'est-à-dire des suites $(a_0, a_1, ...)$ nulles à partir d'un certain rang). On note X la suite $(0,1,0,0....)$. C'est clairement un groupe commutatif pour l'addition des suites termes à termes. La multiplication est donnée par

$$(a_n)_{n\geq 0} \times (b_m)_{m\geq 0} = (c_k)_{k\geq 0}$$

avec

$$c_k = \sum_{n,m\geq 0, n+m=k} a_n b_m.$$

On vérifie que $(A[X], +, \times)$ est un anneau commutatif dont l'élément nul (pour l'addition) est la suite nulle et dont l'unité pour la multiplication est la suite $(1,0,...)$, et que l'application $A \to A[X]$, $a \mapsto (a,0,0,...)$ est un homomorphisme d'anneaux injectif, ce qui permet d'identifier A à un sous-anneau de $A[X]$. La suite $(a_0, a_1, \ldots, a_n, 0, ...)$ est alors égale à $a_0 + a_1 X + \cdots + a_n X^n$ si on identifie $a_k \in A$ à son image dans $A[X]$.

Les éléments de $A[X]$ sont appelés des *polynômes à coefficients dans A*. Les coefficients $a_0, a_1, ...$ sont les coefficients du polynôme $P(X) = a_0 + a_1 X + \cdots + a_n X^n$. Le *degré* d'un polynôme non nul $P(X)$ est le plus grand entier $d \geq 0$ tel que $a_d \neq 0$ et que $a_k = 0$ pour tous $k \geq d+1$. Le coefficient a_d est alors appelé le *coefficient dominant* de $P(X)$.

Par convention, le degré du polynôme nul est $-\infty$.

On vérifie immédiatement les inégalités pour $P(X), Q(X) \in A[X]$

$$\deg(P(X)+Q(X)) \leq \max\{\deg P(X), \deg Q(X)\},$$

$$\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X).$$

Ces inégalités sont strictes en général. Considérer par exemple $P(X) = X$ et $Q(X) = -X+1$ pour la première inégalité et $P(X) = Q(X) = \bar{2}X + 1$ dans $(\mathbb{Z}/4\mathbb{Z})[X]$ pour la seconde.

Définition 1.2.19 On dit que $a \in A$ est un *diviseur de zéro* dans A s'il existe $b \in A$ non nul (i.e. $\neq 0$) tel que $ab = 0$. On dit qu'un élément $a \in A$ est *régulier* si la relation $ax = ay$ ou dans A implique $x = y$. Il est immédiat de voir que $a \in A$ est régulier si et seulement s'il n'est pas diviseur de 0.

Définition 1.2.20 On dit qu'un anneau A est *intègre* si $A \neq \{0\}$ et s'il n'existe pas de diviseur de 0 non-nul. Autrement dit, si tout élément non-nul de A est régulier, ou encore que si $ab = 0$ avec $a, b \in A$, alors a ou b est nul.

Exemple 1.2.21 Les anneaux $\mathbb{Z}$, $\mathbb{R}[X]$ sont intègres. L'anneau de fonctions continues $\mathrm{C}^0(\mathbb{R}, \mathbb{R})$ n'est pas intègre. Les diviseurs de 0 dans $\mathbb{Z}/n\mathbb{Z}$ sont les classes $\bar{m}$ de $m \in \mathbb{Z}$ avec $\mathrm{pgcd}(m, n) > 1$. En particulier $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier. Quand $n = 1$ on obtient l'anneau nul qui n'est pas intègre par définition.

Exercice 1.2.22 Montrer que tout sous-anneau d'un anneau intègre est intègre. Donner un exemple d'un anneau non-intègre qui contient un sous-anneau intègre.

Proposition 1.2.23. *Si A est intègre, alors $A[X]$ est intègre et on a alors*

$$\deg(P(X)Q(X)) = \deg P(X) + \deg Q(X)$$

si $P(X), Q(X) \neq 0$.

Preuve: Soient $P(X), Q(X) \in A[X]$ non-nuls. Alors on peut écrire

$$P(X) = a_0 + a_1 X + \cdots + a_d X^d,\ Q(X) = b_0 + b_1 X + \cdots + b_e X^e,$$

avec $d, e \geq 0$ et $a_d, b_e \neq 0$. Il suit que $a_d b_e \neq 0$ puisque A est intègre, et

$$P(X)Q(X) = a_0 b_0 + (a_1 b_0 + a_0 b_1)X + \cdots + a_d b_e X^{d+e} \neq 0.$$

Enfin, $A[X] \neq \{0\}$ car $A \neq \{0\}$.

Exercice 1.2.24 Si $A = \{0\}$ est l'anneau nul. Quel est l'anneau $A[X]$?

Remarque 1.2.25 Un certain nombre de propriétés d'anneaux se transmettent de A à $A[X]$. On voit de voir c'est le cas de la propriété d'intégrité. Cependant, si A est un anneau principal, $A[X]$ ne sera jamais pas principal excepté si A est un corps (définition 1.4.10). L'objet du prochain chapitre sera d'introduire la notion d'anneaux factoriels et de montrer que cette propriété se transmet à $A[X]$.

Définition 1.2.26 Soit A un anneau (commutatif unitaire). L'anneau $A[X, Y]$ des polynômes à deux variables est défini comme étant

$$A[X, Y] = A[X][Y],$$

c'est-à-dire l'anneau des polynômes à une variable Y et à coefficients dans l'anneau $A[X]$. C'est un anneau commutatif unitaire. Concrètement les éléments de $A[X, Y]$ s'écrivent comme des sommes finies

$$P(X, Y) = \sum_{j \geq 0} a_j(X) Y^j$$

avec $a_j(X) \in A[X]$. Á leur tour, les $a_j(X)$ s'écrivent comme des sommes finies $a_j(X) = \sum_{i\geq 0} a_{ij}X^i$ avec $a_{ij} \in A$. On a donc

$$P(X,Y) = \sum_{i,j\geq 0} a_{ij}X^iY^j, \quad a_{ij} \in A$$

avec les a_{ij} tous nuls sauf un nombre fini. Du coup on a aussi

$$P(X,Y) = \sum_i (\sum_j a_{ij}Y^j)X^i \in A[Y][X].$$

On voit ainsi que $A[X,Y]$ est aussi égal à $A[Y][X]$.

Une troisième manière d'écrire les éléments de $A[X,Y]$ est la décomposition en "composantes homogènes" :

$$P(X,Y) = P_0(X,Y) + P_1(X,Y) + \cdots + P_d(X,Y) + \cdots,$$

où $P_r(X,Y) = \sum_{i+j=r} a_{ij}X^iY^j$. On définit le *degré total* de $P(X,Y) \neq 0$ comme étant le plus grand d tel qu'il existe $i,j \geq 0$ avec $i+j=d$ et $a_{ij} \neq 0$. Cela revient à dire que $P_d(X,Y) \neq 0$ et $P_m(X,Y) = 0$ pour tous $m \geq d+1$.

Il arrive aussi que l'on utilise la notion des degrés partiels. Le degré de $P(X,Y)$ en X, noté $\deg_X P(X,Y)$ est le degré de $P(X,Y) \in A[Y][X]$ vu comme un polynôme en X avec coefficients dans $A[Y]$. On définit symétriquement le degré en Y.

Considérons par exemple le polynôme

$$P(X,Y) = 1 + X + Y^2 + XY + 2X^4 + X^3Y^2 + Y^4 \in \mathbb{Q}[X,Y].$$

Il s'écrit

$$P(X,Y) = (1 + X + 2X^4) + XY + (1 + X^3)Y^2 + Y^4 \in \mathbb{Q}[X][Y]$$

mais aussi

$$P(X,Y) = (1 + Y^2 + Y^4) + (1 + Y)X + Y^2X^3 + 2X^4 \in \mathbb{Q}[Y][X],$$

ou en composantes homogènes :

$$P(X,Y) = 1 + X + (XY + Y^2) + (2X^4 + Y^4) + X^3Y^2.$$

Ainsi $\deg_Y P = 4 = \deg_X P$, et le degré total est 5.

On définit par récurrence l'anneau des polynômes à n-variables $A[X_1, \ldots, X_n]$. Par convention c'est l'anneau A si $n = 0$.

Théorème 1.2.27 (Propriété universelle)**.** *Soit $\phi : A \to B$ un homomorphisme d'anneaux. Fixons un élément $b_0 \in B$. Alors il existe un unique homomorphisme d'anneaux $\tilde{\phi} : A[X] \to B$ tel que $\tilde{\phi}(a) = \phi(a)$ pour tout $a \in A$ et que $\tilde{\phi}(X) = b_0$.*

Preuve: Si un tel homomorphisme $\tilde{\phi} : A[X] \to B$ existe, alors

$$\tilde{\phi}(\sum_i a_i X^i) = \sum_i \tilde{\phi}(a_i)\tilde{\phi}(X^i) = \sum_i \phi(a_i) b_0^i.$$

Ce qui implique l'unicité. Inversement, définissons une application f par

$$f(\sum_i a_i X^i) = \sum_i \phi(a_i) b_0^i.$$

(Par convention $b_0^0 = 1_B$). On vérifie aisément que c'est un homomorphisme d'anneaux.

Il faut voir ce théorème comme l'analogue de l'énoncé en algèbre linéaire qui dit qu'une application linéaire est uniquement déterminée par les images d'une base de l'espace de départ.

Corollaire 1.2.28. *Soit $t_0 \in A$. Alors il existe un unique homomorphisme d'anneaux $e_{t_0} : A[X] \to A$ tel que $e_{t_0}(a) = a$ pour tous $a \in A$ et que $e_{t_0}(X) = t_0$.*

Définition 1.2.29 Soient $t_0 \in A$ et $P(X) \in A[X]$. On pose $P(t_0)$ égale à l'image de $P(X)$ par l'homomorphisme e_{t_0} ci-dessus. C'est l'*homomorphisme d'évaluation* des polynômes en t_0. Concrètement, si $P(X) = \sum_i a_i X^i$, alors $P(t_0) = \sum_i a_i t_0^i$.

Corollaire 1.2.30 (Propriété universelle)**.** *Soit $\phi : A \to B$ un homomorphisme d'anneaux. Fixons deux éléments $b_0, b_1 \in B$. Alors il existe un unique homomorphisme d'anneaux $\tilde{\phi} : A[X,Y] \to B$ tel que $\tilde{\phi}(a) = \phi(a)$ pour tout $a \in A$ et que $\tilde{\phi}(X) = b_0$, $\tilde{\phi}(Y) = b_1$.*

Preuve: En utilisant le théorème on étend ϕ à $\psi : A[X] \to B$ tel que $\psi|_A = \phi$ et $\psi(X) = b_0$. Ensuite on applique de nouveau le théorème à $\psi : A[X] \to B$ pour obtenir $\tilde{\psi} : A[X][Y] \to B$. Comme $A[X,Y] = A[X][Y]$, le $\tilde{\psi}$ est exactement le $\tilde{\phi}$ recherché.

Définition 1.2.31 Soient $t_1, t_2 \in A$ et $P(X,Y) \in A[X,Y]$. On pose $P(t_1,t_2)$ égale à l'image de $P(X)$ par l'unique homomorphisme $f : A[X,Y] \to A$ tel que $f(a) = a$ pour tous $a \in A$ et $f(X) = t_1$, $f(Y) = t_2$. C'est l'évaluation de $P(X,Y)$ en $(t_1,t_2) \in A^2$. Concrètement, si $P(X,Y) = \sum_{i,j} a_{ij} X^i Y^j$, alors $P(t_1,t_2) = \sum_{i,j} a_{ij} t_1^i t_2^j$.

Exercice 1.2.32 (Division euclidienne dans $A[X]$) Soit $P(X) \in A[X]$ un polynôme unitaire.

1. Soit $Q(X) \in A[X]$. Montrer que $\deg(P(X)Q(X)) = \deg P(X) + \deg Q(X)$. En particulier, si $Q(X) \neq 0$, alors $P(X)Q(X) \neq 0$.
2. Soit $F(X) \in A[X]$. Montrer qu'il existe un couple $Q(X), R(X) \in A[X]$ tels que
$$F(X) = P(X)Q(X) + R(X), \quad \deg R(X) \leq \deg P(X) - 1.$$
3. Montrer que le couple $(Q(X), R(X))$ est unique quand $F(X)$ est fixé.
4. Soit $P(X) = 2X \in \mathbb{Z}[X]$. Montrer qu'il n'existe pas de division euclidienne de X par $P(X)$.

Exercice 1.2.33 (Automorphismes de $A[X]$). Soient A un anneau et $f : A[X] \to A[X]$ un automorphisme tel que sa restriction à A soit l'identité.

1. Soient $P(X), Q(X) \in A[X]$ non nuls. On suppose que A est réduit (par exemple intègre). Montrer que $\deg P(Q(X)) = \deg P(X) \deg Q(X)$.
2. Soit $F_0(X) = f(X)$. Montrer que $\deg F_0(X) = aX + b$ avec $a, b \in A$ et a inversible.
3. Soit $g : \mathbb{Q}[X] \to \mathbb{Q}[X]$ un automorphisme d'anneaux. Montrer que la restriction de g à $\mathbb{Q}$ est égal à l'identité et que $g(X) = aX + b$ pour certains $a, b \in \mathbb{Q}$ et $a \neq 0$.

Exercice 1.2.34 Soient $a, b, c, d \in \mathbb{C}$.

1. Montrer qu'il existe un homomorphisme d'anneaux $\tilde{\phi} : \mathbb{C}[X,Y] \to \mathbb{C}[X,Y]$ qui soit l'identité sur $\mathbb{C}$ et tel que $\tilde{\phi}(X) = aX + bY$, $\tilde{\phi}(Y) = cX + dY$.
2. Montrer que $\tilde{\phi}$ est un isomorphisme si et seulement si $ad - bc \neq 0$.
3. Montrer que le procédé ci-dessus induit un homomorphisme $\mathrm{Gl}_2(\mathbb{C}) \to \mathrm{Aut}(\mathbb{C}[X,Y])$ du groupe des matrices 2×2 inversibles vers le groupe des automorphismes de $\mathbb{C}[X,Y]$.

1.3 Idéaux, anneaux quotients

Définition 1.3.1 Soit A un anneau. Un *idéal* I de A est un sous-groupe de A, stable par multiplication par tout élément de A. Autrement dit, $0 \in I$ et, pour tous $a, b \in I$ et pour tout $x \in A$, on a $a + b \in I$ et $xa \in I$. Noter qu'un idéal est presque un sous-anneau de A, excepté qu'il ne contient pas 1_A en général.

Remarque 1.3.2 Dans un anneau non-commutatif, on définit un *idéal bilatère* de la même façon mais en demandant que xa *et* ax appartiennent à I.

Exemple 1.3.3 (1) L'ensemble $\{0\}$ est l'*idéal nul* de A ; A est l'*idéal unité* de A. Un idéal I est égal à l'idéal unité si et seulement s'il contient 1_A.

(2) L'ensemble $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$, mais $1 + 2\mathbb{Z}$ n'en est pas un.

(3) L'ensemble des polynômes $P(X,Y) = \sum_{i,j \geq 0} a_{ij} X^i Y^j \in A[X,Y]$ avec $a_{00} = 0$ est un idéal de $A[X,Y]$. Cela résulte d'une vérification directement. Mais on peut aussi le voir comme le noyau de l'homomorphisme $f : A[X,Y] \to A$ d'évaluation en $(0,0)$ (cf. définition 1.2.31) et utiliser l'exemple fondamental ci-dessous.

Exemple 1.3.4 Soit $f : A \to B$ un homomorphisme d'anneaux. Alors le noyau $\mathrm{Ker}\, f$ est un idéal de A (proposition 1.3.19 (1)). La proposition 1.3.16 plus bas dit que tout idéal est de cette forme.

Attention, l'image d'un idéal par un homomorphisme d'anneaux n'est en général pas un idéal de l'anneau d'arrivée. Cf. Proposition 1.3.19.

Exercice 1.3.5 Soient A un anneau et $\{I_i\}_i$ une famille d'idéaux de A. Montrer que $\cap_i I_i$ est un idéal de A.

Définition 1.3.6 Soient I_1, I_2 des idéaux de A. On note $I_1 + I_2$ l'idéal engendré par $I_1 \cup I_2$ et $I_1 I_2$ l'idéal engendré par les éléments de la forme $x_1 x_2$ avec $x_i \in I_i$. Cette construction est vue plus en détail en TD.

Pour tout idéal I de A et tout entier $n \geq 0$, I^n désigne l'idéal produit de I par lui-même n fois. Par convention $I^0 = A$.

Définition 1.3.7 Soit S une partie de A. L'*idéal de A engendré par S* est le plus petit (pour la relation d'inclusion) idéal de A contenant S. Il est égal à l'intersection de tous les idéaux de A contenant S.

Exemple 1.3.8 Soit $\alpha \in A$, alors l'idéal engendré par α est égal à αA. C'est un *idéal principal* ou *monogène* (en effet, certains auteurs réservent le mot principal aux idéaux nul ou engendrés par un élément régulier).

Soit S une partie de A. Alors l'idéal engendré par S est égal à l'ensemble des combinaisons

$$a = a_1x_1 + a_2x_2 + \cdots + a_mx_m$$

avec $m \geq 0$, $x_i \in S$ et $a_i \in A$. Lorsque $S = \{s_1, ..., s_n\}$ est une partie finie, alors l'idéal engendré par S est égal à l'ensemble des éléments de A de la forme

$$a = a_1s_1 + ... + a_ns_n, \quad a_1, ..., a_n \in A.$$

Cet idéal est noté $(s_1, \cdots, s_n)$ s'il n'y a pas d'ambiguïté possible.

Exemple 1.3.9
1. L'idéal dans l'exemple 1.3.3(4) est l'idéal de $A[X, Y]$ engendré par X et Y. Ce sont les polynômes qui s'annulent en $(0, 0)$.
2. L'idéal $(2, X)$ de $\mathbb{Z}[X]$ (engendré par 2 et X) : ce sont les polynômes à coefficients entiers de termes constants pairs.

Remarque 1.3.10 Rappelons qu'un *anneau principal* est un anneau intègre dont les idéaux sont principaux. Montrons que $\mathbb{Z}[X]$ n'est pas principal. Pour cela, il suffit de montrer que l'idéal $(2, X)$ n'est pas principal. Supposons le contraire : $(2, X) = P_0(X)\mathbb{Z}[X]$. Alors $2 = P_0(X)Q(X)$ pour un certain $Q(X) \in \mathbb{Z}[X]$. Cela implique que $\deg P_0(X) = \deg Q(X) = 0$, donc que $P_0(X) \in \mathbb{Z}$ est un entier divisant 2. On a alors deux possibilités :

(1) Soit $P_0(X) = \pm 1$. Mais il est claire $\pm 1 \notin (2, X)$ d'après la description donnée dans 1.3.9(2). Contradiction.

(2) Soit $P_0(X) = \pm 2$. Mais on doit avoir $X = P_0(X)Q_1(X)$ pour un certain $Q_1(X) \in \mathbb{Z}[X]$, ce qui impliquerait que 1 est divisible par 2 dans $\mathbb{Z}$, impossible.

Donc $\mathbb{Z}[X]$ **n'est pas principal**, alors que $\mathbb{Z}$ l'est.

Remarque 1.3.11 On peut montrer que pour tout $n \geq 1$, l'idéal

$$(2^n, 2^{n-1}X, \cdots, 2X^{n-1}, X^n) \subset \mathbb{Z}[X]$$

ne peut pas être engendré par n polynômes (cet idéal a besoin d'au moins $n+1$ générateurs). Mais ce n'est pas facile du tout !

Remarque 1.3.12 La propriété d'être intègre se transmet de A à $A[X]$. On vient de voir que celle d'être principal ne se transmet pas. Cependant, les anneaux principaux sont des anneaux "factoriels", et on verra au chapitre suivant que cette propriété se transmet à $A[X]$.

La remarque précédente dit qu'il existe des idéaux de $\mathbb{Z}[X]$ nécessitant autant de générateurs qu'on veut. Mais on peut quand même montrer que tout idéal de $\mathbb{Z}[X]$ peut être engendré par un nombre fini d'éléments (le théorème de base de Hilbert). C'est un exemple d'anneaux "noethériens".

Soit $A = C^0([0,1], \mathbb{R})$ l'anneau des fonctions continues de $[0,1]$ dans $\mathbb{R}$. Soit $I = \{f \in A \mid f(0) = 0\}$. C'est un idéal de A et on peut montrer qu'il ne peut pas être engendré par un nombre fini d'éléments. Cet anneau n'est donc pas noethérien.

Exercice 1.3.13 Soit $S = \{k_1, ..., k_n\}$ un ensemble d'entiers non-nuls. Alors l'idéal de $\mathbb{Z}$ engendré par S est égal à $k\mathbb{Z}$ où k est le pgcd des k_i.

Exercice 1.3.14 Soient $S_1 = \{X + Y, X - Y\}$ et $S_2 = \{X, Y\}$. Montrer que S_1, S_2 engendrent le même idéal dans $\mathbb{Q}[X, Y]$, mais que c'est faux dans $\mathbb{Z}[X, Y]$.

Exercice 1.3.15 Soit I un idéal de A. Montrer que l'idéal de $A[X]$ engendré par I (qui n'est pas un idéal de $A[X]$) est constitué des polynômes $\in A[X]$ dont tous les coefficients appartiennent à I.

Proposition 1.3.16. *Soient A un anneau, et I un idéal de A. Soit $s : A \to A/I$ la surjection canonique (A/I étant vu comme un groupe quotient). Alors il existe une (unique) structure d'anneau sur A/I telle que s soit un homomorphisme d'anneaux.*

Démonstration. Cf. cours L2. □

Définition 1.3.17 Soient A et I comme ci-dessus. On dit que A/I est l'*anneau quotient* de A par I.

Remarque 1.3.18 On a pu voir la notation $a + I$ pour un élément de l'anneau quotient A/I. Ce n'est pas incorrect, mais **il faut désormais l'oublier** ! Un élément de A/I se notera x ou $s(a)$ ou $\bar{a}$ avec $a \in A$.

Proposition 1.3.19. *Soit $f : A \to B$ un homomorphisme d'anneaux. Alors les propriétés suivantes sont vraies.*

(1) *Soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A contenant* $\mathrm{Ker}(f)$.

(2) *Supposons que f est surjectif. Pour tout idéal I de A, $f(I)$ est un idéal de B. C'est faux si f n'est pas surjectif.*

Preuve: Cf. cours L2.

Un des sujets principaux en algèbre est de classifier et de comparer les anneaux. Classifier c'est étudier les isomorphismes, comparer c'est étudier les homomorphismes. Beaucoup d'anneaux apparaissent naturellement ou par construction comme un anneau quotient A/I. Le théorème ci-dessous permet de construire des homomorphismes d'anneaux $A/I \to B$ à partir d'homomorphismes d'anneaux $A \to B$.

Théorème 1.3.20 (Théorème de factorisation)**.** *Soit $f : A \to B$ un homomorphisme d'anneaux. Soient I un idéal de A contenu dans* $\mathrm{Ker}(f)$, *$s : A \to A/I$ la surjection canonique.*

(1) *Il existe un unique homomorphisme d'anneaux $\tilde{f} : A/I \to B$ tel que $f = \tilde{f} \circ s$.*

(2) *Si* $\mathrm{Ker}\, f = I$*, alors* $\tilde{f}$ *est injectif.*

(3) *On a* $\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$*. En particulier,* $\tilde{f}$ *est surjectif si et seulement si* f *est surjectif.*

Preuve: Cf. cours L2.

Corollaire 1.3.21. *Tout homomorphisme d'anneaux surjectif* $f : A \to B$ *induit un isomorphisme* $\tilde{f} : A/\mathrm{Ker}\,(f) \to B$.

Exemple 1.3.22 Soit $\phi : \mathbb{R}[X] \to \mathbb{C}$ défini par $\phi(P(X)) = P(i)$ où $i = \sqrt{-1}$ (voir théorème 1.2.27). C'est un homomorphisme surjectif : tout nombre complexe z s'écrit $z = \lambda + \mu i$ avec $\lambda, \mu \in \mathbb{R}$. On a alors $z = \phi(\lambda + \mu X)$. Déterminons son noyau. Soit $P(X) \in \mathbb{R}[X]$. Alors $P(X) \in \ker \phi$ si et seulement si $P(i) = 0$. Par division euclidienne on peut écrire $P(X) = (X^2+1)Q(X) + \mu X + \lambda$ avec $\lambda, \mu \in \mathbb{R}$. Il suit que $\phi(P(X)) = \lambda + \mu i$ et $P(X) \in \ker(\phi)$ si et seulement si $\lambda = \mu = 0$, c'est-à-dire $P(X) \in (X^2+1)\mathbb{R}[X]$. Par conséquent $\ker(f)$ est l'idéal $(X^2+1)\mathbb{R}[X]$. D'où un isomorphisme $\tilde{\phi} : \mathbb{R}[X]/(X^2+1)\mathbb{R}[X] \to \mathbb{C}$.

Exercice 1.3.23 Soient K un corps et $\psi : K[X,Y] \to K[t]$ l'homomorphisme défini par $\psi(X) = t^2$, $\psi(Y) = t^3$ et $\psi|_K = \mathrm{Id}_K$. Montrer que ψ se factorise en un homomorphisme d'anneaux

$$\tilde{\psi} : K[X,Y] \to K[X,Y]/(Y^2 - X^3) \to K[t].$$

Montrer que $\tilde{\psi}$ est injectif et que son image est le sous-anneau

$$K + t^2K[t] := \{a_0 + t^2P(t) \mid P(t) \in K[t]\}.$$

Montrer que l'idéal de $K + t^2K[t]$ engendré par t^2, t^3 n'est pas principal.

Exercice 1.3.24 Soit I un idéal de A, soit $s : A \to A/I$ la surjection canonique. Alors s s'étend en un homomorphisme surjectif $s' : A[X] \to (A/I)[X]$, $\sum_i a_i X^i \mapsto \sum_i s(a_i)X^i$ (utiliser l'exercice 1.2.27). Montrer que le noyau de s' est égal à l'idéal $IA[X]$ de $A[X]$ engendré par $I \subset A[X]$. En déduire que s' induit un isomorphisme $A[X]/IA[X] \simeq (A/I)[X]$.

Exercice 1.3.25 Soient $I \subseteq J$ deux idéaux de A, soit $\bar{J}$ l'image de J dans l'anneau quotient A/I. Montrer que la surjection canonique $A \to A/I$ induit un isomorphisme $(A/I)/\bar{J} \simeq A/J$.

Exercice 1.3.26 Soit $s : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ la surjection canonique. Montrer qu'il existe un homomorphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ qui coincide avec s sur $\mathbb{Z}$ et qui envoie X sur 0.

En déduire que $\mathbb{Z}[X]/(2, X) \simeq \mathbb{Z}/2\mathbb{Z}$.

1.4 Idéaux premiers, idéaux maximaux

Rappelons qu'un anneau A est intègre (définition 1.2.20) si (1) $A \neq \{0\}$; (2) $ab \neq 0$ si $a, b \neq 0$ dans A.

Définition 1.4.1 Soient A un anneau et I un idéal de A. On dit que I est un *idéal premier* si (1) $I \neq A$ et si (2) $ab \notin I$ si $a, b \in A$ et $a \notin I$, $b \notin I$. (Autrement dit, le complémentaire $A \setminus I$ de I dans A est non vide et est stable par multiplication).

On sait par le cours de L2 que :

Proposition 1.4.2. *Soient A un anneau et I un idéal de A. Alors I est premier si et seulement si A/I est intègre.*

Exemple 1.4.3
1. Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et $p\mathbb{Z}$ avec p nombre premier.
2. Plus généralement les idéaux premiers non nuls d'un anneau principal sont exactement les idéaux engendrés par des éléments irréductibles.

Proposition 1.4.4. *Un anneau A est intègre si et seulement si l'idéal nul de A est premier.*

Proposition 1.4.5. *Soit $f : A \to B$ un homomorphisme d'anneaux. Soit $\mathfrak{q}$ un idéal premier de B. Alors $f^{-1}(\mathfrak{q})$ est un idéal premier de A. En particulier, si B est intègre, alors* $\mathrm{Ker}(f)$ *est un idéal premier.*

Preuve: Soit $\mathfrak{p} = f^{-1}(\mathfrak{q})$. C'est un idéal de A, différent de A car sinon $1_B = f(1_A) \in \mathfrak{q}$ contraire à l'hypothèse $\mathfrak{q}$ premier. Ensuite, si $a_1, a_2 \in A \setminus \mathfrak{p}$, alors $f(a_1), f(a_2) \notin \mathfrak{q}$, donc $f(a_1 a_2) \notin \mathfrak{q}$ et $a_1 a_2 \notin f^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Remarque 1.4.6 La proposition ci-dessus est fausse si l'on remplace "idéal premier" par "idéal maximal". Il suffit considérer l'inclusion $\mathbb{Z} \to \mathbb{Q}$.

Exemple 1.4.7 Considérons l'idéal $I = (X, Y) \subset \mathbb{Q}[X, Y]$ engendré par X et Y. Il est égal au noyau l'homomorphisme d'évaluation $e = e_{(0,0)} : \mathbb{Q}[X, Y] \to \mathbb{Q}$ en $(0, 0)$. Donc I est premier. Comme e est surjectif, on a même $\mathbb{Q}[X, Y]/I \simeq \mathbb{Q}$.

Proposition 1.4.8. *Soit $f : A \to B$ un homomorphisme d'anneaux* **surjectif**.

(1) *Soit $\mathfrak{p}$ un idéal premier de A contenant* $\mathrm{Ker}(f)$. *Alors $f(\mathfrak{p})$ est un idéal premier de B.*

(2) *La correspondance qui à tout idéal premier $\mathfrak{q}$ de B associe $f^{-1}(\mathfrak{q})$ est une bijection entre les idéaux premiers de B et les idéaux premiers de A contenant* $\mathrm{Ker}(f)$. *Autrement dit, pour tout idéal premier $\mathfrak{q}$ de B, il existe un unique idéal premier $\mathfrak{p}$ de A contenant* $\mathrm{Ker}(f)$ *tel que $\mathfrak{q} = f(\mathfrak{p})$.*

Preuve: (1) Vérification directe.

(2) Similaire à la preuve de la proposition 1.3.19. La correspondance réciproque est donnée par $\mathfrak{p} \mapsto f(\mathfrak{p})$.

Définition 1.4.9 On dit que I est un *idéal propre* de A si $I \neq A$. On dit que I est un *idéal maximal* si I est un idéal propre et s'il n'est contenu dans aucun autre idéal propre de A.

Définition 1.4.10 On dit qu'un anneau (commutatif) A est un *corps* si $A \neq \{0\}$ et si tout élément non-nul est inversible.

Exercice 1.4.11 Soit A un anneau fini. Montrer que A est un corps si et seulement s'il est intègre.

La proposition suivante a été vue dans Structures Algébriques 1.

Proposition 1.4.12. *Un idéal I est maximal si et seulement si A/I est un corps.*

Comme tout corps est intègre par définition, cela implique :

Corollaire 1.4.13. *Tout idéal maximal est premier.*

Exercice 1.4.14 Soit I un idéal propre dans un anneau A. Montrer que I est maximal si et seulement si pour tout $a \in A \setminus I$, il existe $b \in A$ tel que $1 - ab \in I$.

Exemple 1.4.15
1. On avons vu précédement que $\mathbb{Q}[X,Y]/(X,Y) \simeq \mathbb{Q}$, donc (X,Y) est un idéal maximal de $\mathbb{Q}[X,Y]$.
2. Dans $\mathbb{Q}[X,Y]$, l'idéal $X\mathbb{Q}[X,Y]$ est premier mais pas maximal. En effet, considérons l'homomorphisme d'évaluation $e_0 : A[X] \to A$ en 0 où $A = \mathbb{Q}[Y]$. Alors e_0 est surjectif de noyau $XA[X]$. Il suit que l'anneau quotient $\mathbb{Q}[X,Y]/X\mathbb{Q}[X,Y]$ est isomorphe à $A = \mathbb{Q}[Y]$ qui est un anneau intègre, mais qui n'est pas un corps.

Remarque 1.4.16 On sait que dans un anneau principal, tout idéal premier non nul est maximal. Le calcul ci-dessus implique en particulier que $\mathbb{Q}[X,Y]$ n'est pas principal.

La proposition suivante est un analogue de la proposition 1.4.8 et se démontre de la même façon.

Proposition 1.4.17. *Soit $f : A \to B$ un homomorphisme d'anneaux* **surjectif**.

(1) *Soit $\mathfrak{p}$ un idéal maximal de A contenant* $\mathrm{Ker}(f)$. *Alors $f(\mathfrak{p})$ est un idéal maximal de B.*

(2) *La correspondance qui à tout idéal maximal $\mathfrak{q}$ de B associe $f^{-1}(\mathfrak{q})$ est une bijection entre les idéaux maximaux de B et les idéaux maximaux de A contenant* $\mathrm{Ker}(f)$.

Exercice 1.4.18 Un anneau A est un corps si et seulement si $\{0\}$ est un idéal maximal dans A.

1.4.19 Construction de $\mathbb{R}$.

Un *corps totalement ordonné* est un corps K muni d'un ordre total tel que $x \geq y$ implique $x + z \geq y + z$ pour tous z, et $xz \geq yz$ pour tous $z \geq 0$. Un tel corps est dit *archimédien* si pour tous $x_0 > 0$, et $x \in K$ il existe un entier naturel n tel que $nx_0 \geq x$. On a une notion naturelle de suites de Cauchy dans un corps totalement ordonnée. On dit qu'un tel corps est *complet* si toute suite de Cauchy admet une limite dans ce corps.

Théorème 1.4.20. *Il existe un corps totalement ordonné archimédien complet, unique à isomorphisme unique près.*

Par définition ce corps est le corps $\mathbb{R}$ des nombres réels.

Voici une idée de la construction de ce corps. Soit A l'ensemble des suites de Cauchy à coefficients rationnels. C'est un anneau unitaire commutatif (l'addition et la multiplication se font termes à termes). Cf. 1.2.15. Soit $\mathfrak{m}$ le sous-ensemble des suites rationnelles qui convergent vers 0. On montre que $\mathfrak{m}$ est un idéal maximal à l'aide de l'exercice 1.4.14.

On définit l'ordre sur $A/\mathfrak{m}$ de la façon suivante. On pose

$$\overline{(a_n)_n} \geq \overline{(b_n)_n}$$

dans $A/\mathfrak{m}$ s'il y a égalité ou s'il existe $c \in \mathbb{Q}$ strictement positif tel que $a_n \geq b_n + c$ pour tout n à partir d'un certain rang n_0. On montre que c'est bien défini et que le corps $A/\mathfrak{m}$ muni de cet ordre est un corps totalement ordonné archimédien et complet.

Soit A un anneau, une question naturelle est de savoir s'il admet un idéal premier ou mieux, un idéal maximal. Si $A = \{0\}$, par définition il n'y pas d'idéal premier. Supposons donc $A \neq \{0\}$.

Théorème 1.4.21 (Krull)**.** *Soit A un anneau non trivial. Alors A admet un idéal maximal.*

Corollaire 1.4.22. *Tout idéal propre I de A est contenu dans un idéal maximal.*

Preuve: (du corollaire) L'anneau A/I est non trivial et admet donc un idéal maximal. L'image réciproque de ce dernier dans A est un idéal maximal de A contenant I (proposition 1.4.8(1)).

Discutons maintenant de la preuve du théorème de Krull.

Définition 1.4.23 On dit qu'un ensemble (partiellement) ordonné non-vide E est *inductif* si toute partie totalement ordonnée de E admet un majorant dans E.

Exemple 1.4.24 Soit A un anneau non trivial, soit E l'ensemble (non vide) des idéaux propres de A. On munit E de l'ordre partiel $I \leq J$ si $I \subseteq J$. Si $\{I_\alpha\}_\alpha$ est une famille totalement ordonnée dans E (c'est-à-dire que étant données deux indices α, α', on a forcément $I_\alpha \subseteq I_{\alpha'}$ ou l'inclusion inverse), alors $\cup_\alpha I_\alpha$ est un idéal propre de A (donc un élément de E) qui est évidemment un majorant de l'ensemble $\{I_\alpha\} \subseteq E$. On conclut que E est un ensemble ordonné inductif.

L'énoncé suivant est fondamental pour démontrer des résultats d'existence. On le rencontrera dans divers domaines de mathématiques.

Lemme 1.4.25. (Lemme de Zorn) *Tout ensemble inductif admet un élément maximal.*

On montre que le lemme de Zorn est équivalent à l'axiome du choix. Ce dernier est un des axiomes de la théorie des ensembles. Il s'énonce comme suit : pour tout ensemble $\{P_i \mid i \in I\}$ d'ensembles non-vides P_i, il est possible de choisir simultanément un élément dans chacun des P_i. Autrement dit, l'ensemble produit $\prod_{i\in I} P_i$ est non-vide. Il existe une quantité d'énoncés équivalents. Par exemple : toute application surjective $f : X \to Y$ possède une "section", c'est-à-dire une application $g : Y \to X$ telle que $f(g(y)) = y$ pour tout $y \in Y$.

Preuve du théorème 1.4.21. Il suffit d'appliquer le lemme de Zorn à l'ensemble E de l'exemple 1.4.24.

Exercice 1.4.26 Soit I un idéal propre de A. Soit P l'ensemble des idéaux premiers de A contenant I. On munit P de la relation d'ordre $J \leq J'$ si $J \supseteq J'$ (attention au sens de l'inclusion). Montrer que P est inductif. En déduire qu'il existe des idéaux premiers contenant I, et minimaux pour cette propriété (i.e. qui ne contiennent pas strictement d'autres idéaux premiers contenant I).

Exercice 1.4.27 Soit A un anneau intègre, montrer que $(A[X])^* = A^*$ (éléments inversibles).

Chapitre 2

Anneaux factoriels

On connaît l'importance dans les anneaux $\mathbb{Z}$ et $K[X]$ de pouvoir décomposer (de façon essentiellement unique) un élément en produit d'irréductibles. Les anneaux factoriels sont les anneaux intègres bénéficiant de cette propriété de décomposition. C'est une généralisation "en dimension supérieure" des anneaux principaux.

Dans tout ce chapitre, A sera un anneau (commutatif unitaire) intègre.

2.1 Généralités

2.1.1 Définitions et critères de factorialité

Définition 2.1.1 Soit A un anneau commutatif intègre. Soient $a, b \in A$ des éléments non nuls. On dit que a *divise* b (dans A), et on note $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. On dit aussi que a est un *diviseur* de b (si $a \neq 0$), et que b est un *multiple de* a.

Dans le cadre de l'étude des anneaux factoriels, on étend la terminologie au cas où a et b peuvent être nuls. Alors **tout élément** $a \in A$ **divise** 0**.**

Définition 2.1.2 Deux éléments non-nuls $a, b \in A$ sont dits *associés* s'il existe $u \in A^*$ tel que $a = ub$. Cela revient à dire que $aA = bA$, ou que a divise b et b divise a.

Un *élément irréductible* de A est un élément $a \in A$ non-nul et non-inversible tel que ses seuls diviseurs sont les éléments inversibles et ses associés. Cela revient à dire que si on décompose a en $a = bc$, alors b ou c est inversible.

On dit que $a \in A$ est *premier* si $a \neq 0$ et si aA est un idéal premier de A.

Proposition 2.1.3. *Soient* $a, b, c \in A$.

(1) *Les éléments inversibles divisent tout élément de* A.

(2) *On a* $\{a \mid b\} \iff \{b \in aA\} \iff \{bA \subseteq aA\}$.

(3) *Si* $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$.

(4) *Si $a \mid b$ et $b \mid a$, alors a et b sont associés. Ce qui équivaut à $aA = bA$.*

(5) *Les éléments premiers sont irréductibles.*

Preuve: Seule l'assertion (5) mérite une démonstration. Supposons $f \in A$ premier. Soit $f = ab$, alors $ab \in fA$, donc a ou b appartient à fA, c'est-à-dire divisible par f, donc associé à f par (4).

Remarque 2.1.4 Dans la réciproque de l'assertion (5) ci-dessus est fausse dans un anneau intègre en général. Un exemple (de type géométrique) sera traité en TD.

Exemple 2.1.5 (exemple arithmétique non exposé en détails en cours) Dans le sous-anneau intègre

$$A := \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

de $\mathbb{C}$, nous allons montrer que 2 est un élément irréductible de A mais n'est pas premier dans A.

Déterminons d'abord les éléments inversibles de A. Soit $z = a+b\sqrt{-5} \in A^*$, soit $z' = c + d\sqrt{-5} \in A$ son inverse. En prenant le carré des values absolues complexes dans l'égalité $1 = zz'$, on trouve $1 = (a^2 + 5b^2)(c^2 + 5d^2)$. Il suit que $b = d = 0$ et que $z = \pm 1$. Donc $A^* = \{\pm 1\}$.

Considérons maintenant l'élément $2 \in A$. Il est non nul et non inversible. Montrons qu'il est irréductible. Supposons que l'on a une décomposition

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

dans A. Alors on prend la valeur absolue comme précédemment et on obtient alors $4 = (a^2 + 5b^2)(c^2 + 5d^2)$, il suit que $b = d = 0$ et $a = \pm 1$ ou $c = \pm 1$. Donc $a + \sqrt{-5}b$ ou $c + \sqrt{-5}d$ est inversible.

Enfin 2 n'est pas un élément premier dans A. En effet $(1+\sqrt{-5})(1-\sqrt{-5}) \in 2A$, mais $1 \pm \sqrt{-5} \notin 2A = \{a + b\sqrt{-5} \mid a, b \in 2\mathbb{Z}\}$, donc $2A$ n'est pas un idéal premier de A.

Exercice 2.1.6 Soit $P(X) = aX + b \in A[X]$ avec $a, b \in A$. Supposons que (1) a est inversible ou bien (2) $a \neq 0$ est irreductible et ne divise pas b. Montrer que $P(X)$ est irréductible dans $A[X]$.

Définition 2.1.7 Soit A un anneau intègre. Soit $a \in A$ un élément non-nul. Une *factorisation de a en produit d'éléments irréductibles* est une écriture de a sous la forme

$$a = f_1 ... f_p$$

avec les f_i irréductibles. Par convention tout élément inversible est factorisable. On dit que a admet une *factorisation unique* s'il admet une factorisation en irréductibles $a = f_1 ... f_p$ et si pour toute autre factorisation en irréductibles $a = g_1 ... g_q$, on a $p = q$ et, quitte à renuméroter les indices, on a g_i associé à f_i pour tout $i \leq p$. Par convention, tout élément inversible est réputé avoir une factorisation unique.

On dit que A est *factoriel* si tout élément non-nul admet une factorsation unique.

Exemple 2.1.8 Il est bien connu que $\mathbb{Z}$ et $K[X]$, si K est un corps, sont factoriels.

Remarque 2.1.9 Soit A un anneau factoriel. Soit $a \in A$ non-nul. En regroupant les diviseurs irréductibles de a, on obtient une écriture

$$a = uf_1^{r_1}...f_n^{r_n}, \quad u \in A^*,\ r_i \geq 1$$

avec les f_i irréductibles et deux à deux non-associés. On montre par récurrence sur n que cette écriture est unique dans le sens suivant : si on a une autre décomposition (factorisation)

$$a = vg_1^{s_1}...f_m^{s_m}, \quad v \in A^*, g_j \text{ irréductible},\ s_j \geq 1,$$

alors $m = n$ et, quitte à renuméroter, f_i est associé à g_i, $r_i = s_i$ pour tout i.

Avec l'écriture ci-dessus, les f_i sont les *facteurs irréductibles* (ou diviseurs premiers) de A, et r_i est la *multiplicité* de a en f_i.

La réciproque de la proposition 2.1.3(5) est vraie dans les anneaux factoriels, comme affirme le lemme suivant :

Lemme 2.1.10. (Lemme de Gauss) *Soit A un anneau factoriel. Soient $a, b, c \in A$ avec a irréductible et $a \mid bc$. Alors $a \mid b$ ou $a \mid c$. Autrement dit, tout élément irréductible de A est premier.*

Preuve: Il existe $x \in A$ tel que $bc = xa$. En écrivant les factorisations en irréductibles de b et c et x, on voit que a est nécessairement un facteur irréductible de b ou de c par l'unicité de factorisation.

Remarque 2.1.11 L'anneau A de l'exemple 2.1.5 n'est pas factoriel puisqu'il admet un élément irréductible non premier. La proposition ci-dessous dit qu'on peut remplacer, dans la définition des anneaux factoriels, l'unicité de factorisation par "irréductible implique premier".

Proposition 2.1.12. *Un anneau intègre A est factoriel si et seulement si tout élément a une factorisation en irréductibles et si tout élément irréductible est premier.*

Preuve: La condition est nécessaire d'après le lemme 2.1.10. Montrons qu'elle est suffisante. Supposons que $a \in A \setminus \{0\}$ admet deux factorisations en irrductibles :

$$f_1...f_p = g_1...g_q.$$

Puisque g_1 est premier, un des f_i, disons f_1 appartient à g_1A, donc $g_1|f_1$. Comme ils sont premiers, donc irréductibles, il existe $u \in A^*$ tel que $g_1 = uf_1$. Il suit que

$$f_2...f_p = (ug_2)g_3...g_q.$$

On continue ainsi de suite et on voit que la factorisation est unique.

2.1.2 Anneaux principaux

Rappelons qu'un anneau principal est un anneau intègre dans lequel tout idéal est principal.

Proposition 2.1.13. *Soit A un anneau principal. Soit $f \in A$ non-nul. Alors f est irréductible $\iff$ fA est un idéal maximal $\iff$ f premier.*

Preuve: Supposons f irréductible. Alors fA est un idéal propre de A. Soit I un idéal propre contenant fA, on a $I = gA$ pour un certain $g \in A$. Donc $f \in gA$ et g divise f, et g non inversible (puisque $I \neq A$). Il suit que g est associé à f et $I = gA = fA$. Donc fA est maximal.

Si fA est maximal, il est premier (corollaire 1.4.13). Enfin si f est premier il est irréductible (2.1.3(5)).

Proposition 2.1.14. *Soit A un anneau principal. Alors A est factoriel.*

Preuve: Il suffit de montrer que tout élément non-nul et non inversible a possède une factorisation en produit d'éléments irréductibles (proposition 2.1.12).

Comme ci-dessus aA est contenu dans un idéal maximal f_1A, donc f_1 est premier et donc irréductible. On a $a = f_1a_1$. Si a_1 est inversible on a fini. Sinon, de la même façon on a $a_1 = f_2a_2$ avec f_2 irréductible. Si a_2 est inversible, on a fini, sinon on continue. Si le processus s'arrête au bout d'un nombre fini de fois, on a une factorisation de a en produit d'irréductible. Sinon, on a une suite infinie d'irréductibles $f_1, f_2, \ldots, f_n, \ldots$ et de $a_1, \ldots, a_n, \ldots \in A$ tels que $a = f_1f_2 \ldots f_na_n$ pour tout n (et donc $a_n = f_{n+1}a_{n+1}$). Cela se traduit par une suite strictement croissante infinie d'idéaux

$$a_1A \subsetneq a_2A \subsetneq \cdots \subsetneq a_nA \subsetneq \cdots$$

La réunion (croissante) $\cup_n a_nA$ est un idéal, donc égal à αA pour un certain $\alpha \in A$. Il existe $n_0 \geq 1$ tel que $\alpha \in a_{n_0}A$. Il suit que $\alpha A \subseteq a_{n_0}A$ et que $a_nA \subseteq \alpha A \subseteq a_{n_0}A$ (donc égalité) pour tout $n \geq n_0$. Contradiction puisque la suite est strictement croissante.

2.2 Irréductibilité de polynômes

Avant de poursuivre l'étude des anneaux factoriels, nous faisons une petite digression sur l'irréductibilité des polynômes, qui est en général une question difficile.

Définition 2.2.1 Soit A un anneau intègre. Un polynôme $P(X) \in A[X]$ est dit *irréductible* si c'est un élément irréductible de l'anneau $A[X]$.

Il est utile de rappeler, pour la question d'irréductibilité, que les éléments inversibles de $A[X]$ sont les polynômes constants inversibles A^* (exercice 1.4.27).

Si A_0 est un sous-anneau de A et si $P(X) \in A_0[X]$, on dira qu'il est irréductible dans $A_0[X]$ (ou simplement irréductible dans A_0) ou $A[X]$ suivant qu'il est irréductible dans $A_0[X]$ ou dans $A[X]$. Ces deux propriétés étant distinctes. En effet, si $P(X) \in A_0[X]$ est irréductible dans $A[X]$, il sera irréductible dans $A_0[X]$, mais la réciproque n'est pas vraie comme montre l'exemple simple suivant :

Exemple 2.2.2 Considérons $A_0 = \mathbb{R} \subset A = \mathbb{C}$. Alors $X^2 + 1 \in \mathbb{R}[X]$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Considérons d'abord un cas un peu trivial.

Proposition 2.2.3. *Soit K un corps. Soit $P(X) \in K[X]$.*

1. *Si $\deg P(X) = 1$, alors $P(X)$ est irréductible.*
2. *Supposons que $\deg P(X) = 2$ ou 3. Alors $P(X)$ est irréductible si et seulement s'il n'a pas de zéro dans K.*

Démonstration. (1) Immédiat. (2) En effet, si $P(X)$ est réductible, comme le degré du produit est égal à la somme des degrés, il a nécessairement un facteur de degré 1. Ce qui donne un zéro dans K. La réciproque est immédiate : si $P(\lambda) = 0$ pour un $\lambda \in K$, alors $X - \lambda \mid P(X)$. □

Attention : cet énoncé est **absolument faux** en degré ≥ 4. Par exemple, le polynôme $(X^2 + 1)^2 \in \mathbb{R}[X]$ n'a pas de racine dans $\mathbb{R}$, mais il est réductible dans $\mathbb{R}$.

Remarque 2.2.4 La proposition ci-dessus n'est pas valable sur un anneau. Par exemple $(2X + 1)^2 \in \mathbb{Z}[X]$ est de degré 2, n'a pas de racine dans $\mathbb{Z}$, mais n'est clairement pas irréductible.

Si A est un anneau intègre de corps des fractions K, il est parfois plus facile de prouver l'irréductibilité d'un polynôme dans $A[X]$ que dans $K[X]$. Lorsque A est factoriel, on verra plus tard que l'irréductibilité dans $A[X]$ implique l'irréductibilité dans $K[X]$. Ceci est particulièrement utile pour prouver l'irréductibilité de polynômes dans $\mathbb{Q}[X]$ par exemple.

Définition 2.2.5 Soit A un anneau intègre. Un polynôme

$$P(X) = a_0 + a_1X + \cdots + a_dX^d \in A[X]$$

non nul est dit *primitif* si les seuls diviseurs communs des a_i sont des éléments inversibles : si $a \mid a_i$ pour tout $i \leq d$, alors $a \in A^*$. Cela est équivalent à dire que si $P(X) = aQ(X)$ avec $a \in A$ et $Q(X) \in A[X]$, alors $a \in A^*$.

Rappelons (exercice 1.3.24) que pour tout idéal I de A, la surjection canonique $s : A \to A/I$ induit une surjection canonique $s' : A[X] \to (A/I)[X]$ dont le noyau est l'ensemble des polynômes à coefficients dans I. Il envoie un polynôme $\sum_i a_iX^i \in A[X]$ sur le polynôme $\sum_i s(a_i)X^i$ dans $(A/I)[X]$. C'est la réduction modulo I des polynômes $\in A[X]$.

Soit $P(X) \in A[X]$. L'image $s'(P(X))$ sera notée $\overline{P}(X)$ s'il n'y a pas d'ambiguïté. On a $\deg \overline{P}(X) \leq \deg P(X)$ et l'égalité a lieu si et seulement si le coefficient dominant de $P(X)$ n'appartient pas à I.

Proposition 2.2.6 (Critère d'irréductibilité par réduction)**.** *Soit A un anneau intègre. Soit*

$$P(X) = a_0 + a_1X + \cdots + a_dX^d \in A[X]$$

un polynôme primitif. On suppose qu'il existe un idéal premier $\mathfrak{p} \subset A$ tel que :

(1) $a_d \notin \mathfrak{p}$ *;*

(2) *l'image de $P(X)$ dans $(A/\mathfrak{p})[X]$ est irréductible.*

Alors $P(X)$ est irréductible dans $A[X]$.

Preuve: En effet, supposons que $P(X) = Q(X)R(X)$ est une décomposition dans $A[X]$. Par passage au quotient modulo $\mathfrak{p}$, on obtient une décomposition

$$\overline{P}(X) = \overline{Q}(X)\overline{R}(X).$$

Par hypothèse, l'un des facteurs à droite est inversible dans $(A/\mathfrak{p})[X]$. Supposons par exemple que $\overline{Q}(X) \in ((A/\mathfrak{p})[X])^* = (A/\mathfrak{p})^*$ (car $A/\mathfrak{p}$ est intègre), alors $\deg \overline{Q}(X) = 0$.

Or $\deg \overline{R}(X) \leq \deg R(X)$ et $\deg \overline{Q}(X) \leq \deg Q(X)$, et comme $a_d \notin \mathfrak{p}$, on a

$$\deg Q + \deg R = d = \deg(\overline{P}) = \deg \overline{Q} + \deg \overline{R}.$$

Il suit que $\deg Q = \deg \overline{Q} = 0$ et $Q(X) \in A$. Par l'hypothèse de primitivité de $P(X)$, on a $Q(X) \in A^*$ et donc $P(X)$ est bien irréductible dans $A[X]$.

Exemple 2.2.7 Le polynôme $X^3 + X + 1 \in \mathbb{F}_2[X]$ à coefficients dans le corps à 2 éléments $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ est irréductible car sans racine dans $\mathbb{F}_2$ et de degré 3. Le polynôme $5X^3 + 2X^2 + X + 3 \in \mathbb{Z}[X]$ est alors irréductible dans $\mathbb{Z}[X]$ puisque son image dans $\mathbb{F}_2[X]$ est $X^3 + X + 1$ qui est irréductible.

Considérons maintenant $X^4+X+1 \in \mathbb{F}_2[X]$ et montrons qu'il est irréductible. Sinon, il aurait un facteur irréductible de degré ≤ 2. Or les polynômes irréductibles de degré au plus 2 dans $\mathbb{F}_2[X]$ sont $X, X + 1$ et $X^2 + X + 1$ et on vérifie immédiatement (par division euclienne pour le dernier) que $X^4 + X + 1$ n'est divisible par aucun de ces polynômes. Donc il est bien irréductible. Cela implique par exemple que $5X^4 + 2X^3 + 6X^2 + X + 7 \in \mathbb{Z}[X]$ est irréductible.

Exercice 2.2.8 Le polynôme $(2X+1)X \in \mathbb{Z}[X]$ n'est pas irréductible, mais est irréductible modulo 2. Est-ce en contradiction avec la proposition 2.2.6 ?

Le critère précédent ne s'applique pas lorsque $\overline{P}(X)$ est "très réductible" comme par exemple X^4+7 modulo 7.

Theorem 2.2.9 (Critère d'Eisenstein)**.** *Soit A un anneau intègre. Soit*

$$P(X) = a_d X^d + a_{d-1}X^{d-1} + ... + a_0 \in A[X]$$

un polynôme primitif de degré $d \geq 1$. On suppose qu'il existe un élément premier $f \in A$ avec les propriétés suivantes :

(i) *f ne divise pas a_d ;*

(ii) *f divise $a_0, \cdots, a_{d-1}$;*

(iii) *f^2 ne divise pas a_0.*

Alors $P(X)$ est irréductible dans $A[X]$. Si de plus A est factoriel, alors $P(X)$ est irréductible dans $K[X]$ où K est le corps des fractions de A.

Démonstration. Supposons le contraire. On a alors une décomposition

$$P(X) = Q(X)R(X), \quad Q(X), R(X) \in A[X] \setminus A^*.$$

On a $\deg Q, \deg R > 0$ car $P(X)$ est primitif. Cette égalité induit une égalité dans $(A/fA)[X]$:

$$\bar{a}_d X^d = \overline{P}(X) = \overline{Q}(X)\overline{R}(X).$$

Comme dans la preuve de la proposition précédente, on a $\deg \overline{Q} = \deg Q > 0$ et $\deg \overline{R} = \deg R > 0$. On déduit immédiatement que $\overline{Q}(0) = \overline{R}(0) = 0$. En effet, si $\overline{Q}(0) \neq 0$, en écrivant $\overline{R}(X) = X^{d_1}(c_0 + c_1 X + ...)$ avec $c_0 \neq 0$ et $0 \leq d_1 < d$, alors le terme de degré d_1 dans $\bar{a}_d X^d = \overline{P} = \overline{Q}.\overline{R} = \overline{Q}(0)c_0 X^{d_1} + ...$ serait non nul, absurde. Il suit que $Q(0), R(0) \in fA$, donc $a_0 = P(0) = Q(0)R(0) \in f^2 A$, contradiction.

Si A est factoriel, le fait que l'irréductibilité dans $A[X]$ implique celle dans $K[X]$ sera prouvée ultérieurement (proposition 2.4.6). □

Exemple 2.2.10 (d'éléments premiers)

1. Soit p un nombre premier. Alors p est un élément premier dans $\mathbb{Z}$ et dans $\mathbb{Z}[X]$.
2. Soit K un corps. Alors tout polynôme de degré total 1 (donc de la forme $aX + bY + c$) est premier dans $K[X, Y]$.

Exemple 2.2.11

1. Les polynômes $2X^3 + 3, X^5 + 5X + 10 \in \mathbb{Z}[X]$ sont irréductibles dans $\mathbb{Z}[X]$ (donc dans $\mathbb{Q}[X]$).
2. Soit Ω un corps. Soit $\lambda \in \Omega$ différent de 0 et de 1. Alors le polynôme $Y^2 - X(X-1)(X-\lambda) \in \Omega[X, Y]$ est irréductible.

Remarque 2.2.12 Soit A un anneau intègre de corps de fractions K, soit $P(X) \in A[X]$. Si $P(X)$ est primitif et est irréductible dans $K[X]$, alors $P(X)$ est irréductible dans $A[X]$. Mais la réciproque est fausse en générale (sauf pour les anneaux factoriels) comme on le voit avec l'exemple qui suit.

Exemple 2.2.13 Soit $A = \mathbb{Z}[\sqrt{5}] \subset \mathbb{R}$. Considérons le polynôme $P(X) = X^2 - X - 2 \in A[X]$. Dans le corps des fractions $K = \mathbb{Q}[\sqrt{5}]$ de A, ce polynôme se décompose en

$$P(X) = (X - \frac{\sqrt{5}-1}{2})(X + \frac{\sqrt{5}+1}{2}).$$

Mais $P(X)$ est irréductible dans $A[X]$. En effet comme il est clairement primitif, s'il était réductible il serait produit de deux facteurs de degré 1 :

$$P(X) = (aX + b)(cX + d), \quad a, b, c, d \in A.$$

Il suit que $ac = 1$, donc $a \in A^*$ et on a

$$P(X) = (X + a^{-1}b)(X + a^{-1}d).$$

Il suit que $A \ni a^{-1}b \in \{(\sqrt{5}-1)/2, (-\sqrt{5}-1)/2\}$, ce qui est faux. En résumé, on obtient un élément irréductible de $A[X]$ qui n'est pas irréductible dans $K[X]$. Il faut noter qu'un tel exemple n'est pas très intéressant du fait que $\mathbb{Z}[\sqrt{5}][X]$ n'est pas factoriel et que dans un tel anneau, la notion d'éléments irréductibles n'est pas très pertinente.

2.3 Pgcd, ppcm et applications

Dans le reste de ce chapitre, les objets que nous allons aborder sont souvent définis à multiplication par un inversible près. Pour fixer les idées, on choisira une fois pour toute **un ensemble $\mathcal{P}$ d'éléments irréductibles** de A tel que tout élément irréductible de A soit associé avec un unique élément de $\mathcal{P}$. C'est un ensemble de représentants de l'ensemble des irréductibles de A modulo la relation d'équivalence d'association.

Pour $A = \mathbb{Z}$, on prend pour $\mathcal{P}$ l'ensemble des nombres premiers. Pour $A = K[X]$, on prend pour $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires. Dans le cas général, il n'y a pas de choix standard. Mais cela n'a pas d'importance vitale.

Définition 2.3.1 Soit A un anneau factoriel. Soient $a_1, ..., a_n \in A$. Un *pgcd* (plus grand commun diviseur) des a_i dans A est un diviseur commun des a_i, multiple de tout autre diviseur commun des a_i. Un tel élément, s'il existe, est unique à multiplication par un inversible près.

Similairement, on définit le *ppcm* (plus petit commun multiple) des a_i dans A comme étant un multiple commun des a_i, et qui divise tout autre multiple commun. Comme pour le pgcd, si un ppcm existe, il est alors unique à multiplication par une unité près.

Rappelons que si f est un diviseur irréductible de a, on appelle la *multiplicité de a en f* (ou *valuation de a en f*) l'exposant de f qui apparaît dans la décomposition de a (Remarque 2.1.9). C'est le plus grand entier $v \geq 0$ tel que f^v divise a. On la note $v_f(a)$. Si f ne divise pas a, on a $v_f(a) = 0$. Par convention $v_f(0) = +\infty$. On a $a = f^{v_f(a)}a'$ avec $f \not| \, a'$.

Avec le choix d'un système de représentants $\mathcal{P}$, tout élément $a \in A \setminus \{0\}$ s'écrit de manière (vraiment) unique sous la forme

$$a = u \prod_{f \in \mathcal{P}} f^{v_f(a)}$$

avec $u \in A^*$ et $v_f(a) = 0$ pour tous f sauf un nombre fini.

Lemme 2.3.2. *Soient $a, b \in A$.*

1. *$v_f(ab) = v_f(a) + v_f(b)$ (étant entendu que $k + (+\infty) = +\infty$).*
2. *On a $a \mid b$ si et seulement si $v_f(a) \leq v_f(b)$ pour tout irréductible $f \in \mathcal{P}$.*

Proposition 2.3.3. *Soit A un anneau factoriel. Soient $a_1, ..., a_n \in A$ non tous nuls avec $n \geq 1$. Alors* $\mathrm{pgcd}(a_1, ..., a_n)$ *et* $\mathrm{ppcm}(a_1, ..., a_n)$ *existent et sont uniques à association près.*

Preuve: Il suffit de considérer les produits (finis)

$$\prod_{f \in \mathcal{P}} f^{\min\{v_f(a_i)\}_{1 \leq i \leq n}} \quad \text{et} \quad \prod_{f \in \mathcal{P}} f^{\max\{v_f(a_i)\}_{1 \leq i \leq n}}$$

Ce sont respectivement un pgcd et un ppcm d'après le lemme précédent. Deux pgcd se divisent mutuellement par définition, et sont donc associés. Similairement, deux ppcm sont multiples mutuellement, et sont donc associés.

Remarque 2.3.4 Dans la suite, on prendra pour pgcd et ppcm ces produits. Ils dépendent bien sûr du choix de $\mathcal{P}$. Par convention, $f^0 = 1$ si $f \in \mathcal{P}$. En particulier, si ce pgcd est inversible, tous les exposants sont nuls et ce pgcd est alors égal à 1.

Définition 2.3.5 Soient $a_1, a_2 \in A$. On dit qu'ils sont *premiers entre eux* si les seuls diviseurs commons sont les éléments inversibles, autrement dit si $\text{pgcd}(a_1, ..., a_n) = 1$. Similairement $a_1, \ldots, a_n \in A$ (avec $n \geq 2$) sont ditss premiers entre eux si les seuls diviseurs commons sont les éléments inversibles. On dit qu'ils sont 2 à 2 premiers entre eux si pour tout couple $i \neq j$, a_i et a_j sont premiers entre eux. Cette propriété est plus forte que la précédente, cf. l'exemple des entiers $6, 15, 20$ dans $\mathbb{Z}$.

Remarque 2.3.6 Cas particuliers.

(1) Si un des $a_i = 0$, alors le ppcm des a_i est nul.

(2) $\text{pgcd}(a_1, ..., a_n)$ reste inchangé si l'on supprime les termes a_i qui sont nuls.

(3) $\text{pgcd}(a) = \text{ppcm}(1, a)$ est un élément associé à a.

Lemme 2.3.7. *Dans un anneau factoriel A avec un $\mathcal{P}$ fixé, on a*

$$\text{pgcd}(aa_1, aa_2, \ldots, aa_n) = \text{pgcd}(a)\text{pgcd}(a_1, \ldots, a_n).$$

Démonstration. On applique la définition 2.3.4 et le lemme 2.3.2. □

Proposition 2.3.8 (Lemme de Gauss)**.** *Soit A un anneau factoriel. Soient $a, b, c \in A$ non-nuls. On suppose que $a \mid bc$ et que a est premier à b. Alors $a \mid c$.*

Démonstration. On doit montrer que $v_f(a) \leq v_f(c)$ pour tout irréductible $f \in \mathcal{P}$. C'est automatique si $v_f(a) = 0$. Supposons $v_f(a) \geq 1$, alors $v_f(b) = 0$. Il suit que $v_f(a) \leq v_f(bc) = v_f(b) + v_f(c) = v_f(c)$. Donc $a \mid c$. □

Rappel. Si A est un anneau intègre, son corps des fractions, noté $\text{Frac}(A)$, est un corps contenant A comme sous-anneau et dont les éléments sont de la forme ab^{-1} ou a/b avec $a, b \in A$ et $b \neq 0$. Il existe et est unique à isomorphisme près.

Proposition 2.3.9. *Soit A un anneau factoriel de corps des fractions K. Tout élément $\alpha \in K^*$ s'écrit $\alpha = a/b$ avec $a, b \in A$ premiers entre eux. De plus, si $\alpha = a'/b'$ avec $a', b' \in A$, alors $a \mid a'$ et $b \mid b'$.*

Cette écriture est unique dans le sens suivant : si a', b' sont premiers entre eux et si $\alpha = a'/b'$, alors a' est associé à a et b' est associé à b.

Démonstration. À partir d'une écriture $\alpha = x/y$ avec $x, y \in A$ non-nuls, on pose $t = \text{pgcd}(x, y)$. Alors $a := x/t, b := y/t \in A$ et on a $t = \text{pgcd}(x, y) = \text{pgcd}(t)\text{pgcd}(a, b)$. Comme t et $\text{pgcd}(t)$ sont associés, on a $\text{pgcd}(a, b) = t/\text{pgcd}(t) \in A^*$ et $\alpha = a/b$.

Le reste de la proposition découle aisément du lemme de Gauss ci-dessus. □

Le théorème suivant a été vu dans Structures Algébriques 1 pour l'anneau $\mathbb{Z}$. Il est également valable pour tout anneau principal.

Theorem 2.3.10. (Identité de Bézout) *Soit A un anneau principal. Soient $a_1, ..., a_n \in A$ non tous nuls. Alors*

$$a_1A + \cdots + a_nA = \text{pgcd}(a_1, ..., a_n)A.$$

En particulier, si $a, b \in A$ sont premiers entre eux, alors il existe $u, v \in A$ tels que $au + bv = 1$.

Preuve: Comme A est principal, $a_1A + \cdots + a_nA = eA$ pour un certain $e \in A$. Comme $a_i \in a_iA \subseteq eA$, e divise tous les a_i. Par ailleurs, si a est un diviseur commun des a_i, alors $a_i \in aA$ pour tout $i \leq n$. Donc $e \in a_1A + \cdots + a_nA \subseteq aA$ et a divise e. Par conséquent, e est un pgcd des a_i et $eA = \text{pgcd}(a_1, ..., a_n)A$.

Remarque 2.3.11 On verra plus loin que l'anneau $\mathbb{Q}[X, Y]$ est factoriel. Dans l'anneau $\mathbb{Q}[X, Y]$, les éléments X, Y sont premiers entre eux, mais $XP(X, Y) + YQ(X, Y)$ n'est jamais égal au polynôme constant 1 (pas d'identité de Bézout), cela se voit en évaluant en $(0, 0)$. **Le théorème de Bézout est vrai pour les anneaux principaux, mais n'est pas vrai dans un anneau factoriel en général !**

Exercice 2.3.12 Soient $f \in A$ irréductible et $a, b \in A$. Montrer que $v_f(a+b) \geq \min\{v_f(a), v_f(b)\}$.

Exercice 2.3.13 Soient A factoriel et $a, b \in A$ non-nuls. Montrer que $abA = \text{pgcd}(a, b)\text{ppcm}(a, b)A$. Montrer que $\text{pgcd}(a, b, c) = \text{pgcd}(a, \text{pgcd}(b, c))$.

Exercice 2.3.14 Soient A factoriel, $a \in A$ non-nul. Décrire $\sqrt{aA}$ et montrer qu'il est égal à l'intersection des idéaux premiers de A contenant a.

Exercice 2.3.15 Soit A un anneau factoriel de corps de fractions K. Soit $\alpha \in K$. On suppose qu'α satisfait une relation

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$$

avec $a_i \in A$. Montrer que $\alpha \in A$. On dit que A est "intégralement clos".

Exercice 2.3.16 Soit A un anneau factoriel. Soient $a_1, ..., a_n \in A$. Montrer que $\text{ppcm}(a_1, ..., a_n)A = \cap_i a_iA$.

Exercice 2.3.17 Soit B un anneau principal. Soient A un sous-anneau principal de B (par exemple si L est un corps, K un sous-corps de L, $B = L[X]$ et $A = K[X]$) et $a, b \in A$ non-nuls. Montrer que $\text{pgcd}(a, b) \in A$ est égal (à association près) au pgcd de a, b calculé dans B.

Exercice 2.3.18 Trouver le pgcd des polynômes $X^5+5X^4+9X^3+7X^2+5X+3$ et $X^4 + 2X^3 + 2X^2 + X + 1$ dans $\mathbb{Q}[X]$.

Exercice 2.3.19 Soient $n, m \geq 1$. Déterminer $\text{pgcd}(X^n-1, X^m-1)$ dans $\mathbb{Q}[X]$.

Exercice 2.3.20 Soit K un corps. Soient $P(X), Q(X) \in K[X]$ deux polynômes premiers entre eux. Montrer qu'il existe $U(X), V(X) \in K[X]$ avec $\deg U(X) < \deg Q(X)$, $\deg V(X) < \deg P(X)$ et

$$1 = U(X)P(X) + V(X)Q(X).$$

2.4 Transfert de la factorialité

Soit A un anneau factoriel de corps de fractions K. Nous allons étudier les éléments irréductibles de $A[X]$ en relation avec ceux de $K[X]$.

On fixe un système de représentants $\mathcal{P}$ des éléments irréductibles de A, ce qui fixe le choix des pgcd et ppcm (cf. début du paragraphe §2.3).

Définition 2.4.1 Soit $P(X) = a_0 + a_1X + ... + a_dX^d \in A[X]$. On appelle le *contenu* de $P(X)$ le pgcd des coefficients de $P(X)$:

$$\text{cont}(P(X)) = \text{pgcd}(a_0, \ldots, a_d).$$

Il dépend du choix de $\mathcal{P}$, mais est uniquement déterminé à association près. Soit $a \in A \setminus \{0\}$. On a $\text{cont}(a) = 1$ si et seulement si $a \in A^*$. Par convention $\text{cont}(0) = 0$.

Rappelons que $P(X) \in A[X]$ est dit *primitif* si les coefficients de $P(X)$ sont premiers entre eux, autrement dit si $\text{cont}(P(X)) = 1$. C'est encore équivalent à dire que la classe de de $P(X)$ dans $(A/fA)[X]$ est non nulle pour tout élément irréductible f de A. Tout polynôme unitaire est primitif.

Exercice 2.4.2 Si $a, b \in A$, alors $\text{cont}(\text{cont}(a)) = \text{cont}(a)$, et $\text{cont}(ab) = \text{cont}(a)\text{cont}(b)$.

Lemme 2.4.3. *Soit A un anneau factoriel. Soient $P(X), Q(X) \in A[X]$ non nuls.*

(a) *Pour tout $a \in A$, on a* $\text{cont}(aP) = \text{cont}(a)\text{cont}(P)$.

(b) *On a $P(X) = \text{cont}(P)P_0(X)$ avec $P_0(X) \in A[X]$ primitif.*

(c) *On a* $\text{cont}(PQ) = \text{cont}(P)\text{cont}(Q)$.

Preuve: (a) Il s'agit de montrer que

$$\text{pgcd}(aa_0, ..., aa_d) = \text{cont}(a)\text{pgcd}(a_0, ..., a_d),$$

ce qui se voit aisément en comparant les multiciplités v_f des deux côtés :

$$\min_i\{v_f(a) + v_f(a_i)\} = v_f(a) + \min_i\{v_f(a_i)\}$$

pour tout $f \in \mathcal{P}$.

(b) On a $a_i = \mathrm{cont}(P)b_i$ avec $b_i \in A$. Donc $P(X) = \mathrm{cont}(P)P_0(X)$ avec $P_0(X) \in A[X]$. D'après (a), on a $\mathrm{cont}(P_0) = 1$.

(c) En utilisant (a) et (b), on se ramène au cas où $\mathrm{cont}(P) = \mathrm{cont}(Q) = 1$. Soit $f \in A$ irréductible. La classe $\overline{PQ}$ de PQ dans $(A/fA)[X]$ est égale à $\overline{PQ}$. Comme P, Q sont primitifs et que $(A/fA)[X]$ est intègre, on a $\overline{PQ} \neq 0$. Ceci étant vrai pour tout élément irréductible f, on conclut que PQ est primitif, donc $\mathrm{cont}(PQ) = 1$. □

Nous allons étendre la définition du contenu aux polynômes à coefficients dans K.

Définition 2.4.4 Soit $f(X) \in K[X]$. Alors il existe $a \in A$ non-nul (un dénominateur commun des coefficients de $f(X)$) tel que $af(X) \in A[X]$. On pose

$$\mathrm{cont}(f) = \mathrm{cont}(af)/\mathrm{cont}(a) \in K.$$

On vérifie sans peine (à l'aide du lemme précédent) que $\mathrm{cont}(f)$ ne dépend pas du choix d'un dénominateur commun a.

Lemme 2.4.5. *Soient A un anneau factoriel, K son corps de fractions et $f(X), g(X) \in K[X]$.*

(a) *Il existe $F_0(X) \in A[X]$ primitif tel que $f(X) = \mathrm{cont}(f)F_0(X)$. En particulier, $f(X) \in A[X]$ si et seulement si $\mathrm{cont}(f) \in A$.*

(b) *On a $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$.*

Preuve: (a) Ecrivons $f(X) = F(X)/a$ avec $a \in A$ non-nul et $F(X) \in A[X]$. On a $F(X) = \mathrm{cont}(F)F_1(X)$ avec $F_1(X) \in A[X]$ primitif (lemme 2.4.3). Il suit que $f(X) = \mathrm{cont}(f)F_0(X)$ avec $F_0(X) = (\mathrm{cont}(a)/a)F_1(X) \in A[X]$ primitif car $\mathrm{cont}(a)/a \in A^*$.

(b) C'est une conséquence immédiate du lemme 2.4.3(c).

Proposition 2.4.6. *Soit A un anneau factoriel, de corps de fractions K. Soit $P(X) \in A[X]$ de degré ≥ 1.*

(1) *Si $P(X)$ est irréductible dans $A[X]$, alors $P(X)$ est irréductible dans $K[X]$. (En particulier, si $P(X) \in \mathbb{Z}[X] \setminus \mathbb{Z}$ est irréductible dans $\mathbb{Z}[X]$, alors il est irréductible dans $\mathbb{Q}[X]$).*

(2) *Supposons $P(X)$ primitif. Alors la réciproque de (1) est vraie : si $P(X)$ est irréductible dans $K[X]$, alors il est irréductible dans $A[X]$.*

Preuve: (1) Montrons la contraposée. Supposons $P(X)$ réductible dans $K[X]$: $P(X) = f(X)g(X)$ avec $f(X), g(X) \in K[X]$ non-constants. On écrit

$$f(X) = \mathrm{cont}(f)F_0(X), \quad g(X) = \mathrm{cont}(g)G_0(X)$$

avec $F_0(X), G_0(X) \in A[X]$ primitifs de degré > 0. Il suit que

$$P(X) = (\mathrm{cont}(f)\mathrm{cont}(g))F_0(X)G_0(X)$$

et que $\mathrm{cont}(f)\mathrm{cont}(g) = \mathrm{cont}(P) \in A$. Par conséquent $P(X)$ se décompose en $(\mathrm{cont}(P)F_0(X))G_0(X)$ dans $A[X]$. Comme $\mathrm{cont}(P)F_0(X)$ et $G_0(X)$ sont de degré ≥ 1, donc non inversibles dans $A[X]$ (exercice 1.4.27), $P(X)$ est réductible dans $A[X]$.

(2) Supposons $P(X)$ réductible dans $A[X]$. Alors $P(X) = F(X)G(X)$ avec $F(X), G(X)$ non-inversibles dans $A[X]$. Comme $P(X)$ est primitif, on a nécessairement $\deg F(X) \geq 1$ et $\deg G(X) \geq 1$. Donc $P(X)$ est réductible dans $K[X]$.

Remarque 2.4.7 Noter que dans la propriété (2) ci-dessus, il est important de supposer $P(X)$ primitif. Par exemple $2X \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$, mais ne l'est pas dans $\mathbb{Z}[X]$ puisque c'est le produit de deux éléments non-inversibles 2 et X dans $\mathbb{Z}[X]$. Par ailleus (2) est valide pour tout anneau intègre A.

Exercice 2.4.8 Soit A un anneau factoriel de corps de fractions K. Soient $f(X), g(X) \in K[X]$ des polynômes unitaires. Montrer que si $f(X)g(X) \in A[X]$, alors $f(X), g(X) \in A[X]$.

Jusqu'à présent, les seuls exemples d'anneaux factoriels rencontrés sont les anneaux principaux. Le théorème suivant va nous en fournir bien d'autres.

Theorem 2.4.9 (Transfert de factorialité)**.** *Soit A un anneau factoriel de corps de fractions K. Alors on a les propriétées suivantes :*

(1) *Les éléments irréductibles de $A[X]$ sont les irréductibles de A, et les polynômes $F(X) \in A[X]$ primitifs non-constants qui sont irréductibles dans $K[X]$.*

(2) *L'anneau $A[X]$ est factoriel.*

Preuve: Les éléments de $A[X]$ listés dans (1) sont bien irréductibles : c'est évident pour les polynômes constants, et on utilise la proposition 2.4.6(b) pour les polynômes primitifs.

(2) Montrons que tout élément de $A[X]$ se décompose en produit d'éléments irréductibles listés dans (1). Cela impliquera en même temps que tout élément irréductible de $A[X]$ est de la forme ci-dessus.

On a $P(X) = f_1(X)...f_n(X)$ avec $f_i(X) \in K[X]$ irréductibles. On écrit $f_i(X) = \mathrm{cont}(f_i)F_i(X)$ avec $F_i(X) \in A[X]$ primitif. Alors

$$P(X) = \mathrm{cont}(P) \prod_{1 \leq i \leq n} F_i(X).$$

Comme cont(P) est un produit d'irréductibles de A, on a $P(X)$ comme produit d'irréductibles de $A[X]$ listés dans (1).

D'après la proposition 2.1.12, pour conclure que $A[X]$ est factoriel, il suffit de montrer que tout élément irréductible $P(X) \in A[X]$ est premier. Soient $F(X), G(X) \in A[X]$ tels que $F(X)G(X) \in P(X)A[X]$.

Supposons d'abord que $P(X) \in A$. On a cont$(P) \mid$ cont(F)cont(G). Comme cont(P) est irréductible dans A, on a par exemple cont$(P) \mid$ cont(F) et donc $P(X) \mid$ cont$(F) \mid F(X)$.

Supposons maintenant $\deg P(X) \geq 1$. Alors $P(X)$ est irréductible dans $K[X]$. Il suit que, par exemple, $P(X) \mid F(X)$ dans $K[X]$. Écrivons $F(X) = P(X)h(X)$ avec $h(X) \in K[X]$. On a $h(X) =$ cont$(h)H_0(X)$ avec $H_0(X) \in A[X]$ (lemme 2.4.5 (a)). Il suit que cont$(h) =$ cont$(F) \in A$, donc $H(X) \in A[X]$ et $F(X) \in P(X)A[X]$.

Corollaire 2.4.10. *Soit $n \geq 1$. Soit A un corps ou un anneau principal. Alors $A[X_1, ..., X_n]$ est factoriel.*

Preuve: On procède par récurrence sur n.

Exercice 2.4.11 Soit $f(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$ le déterminant de vandermonde.

$$\begin{vmatrix} 1 & X_1 & X_1^2 & ... & X_1^{n-1} \\ 1 & X_2 & X_2^2 & ... & X_2^{n-1} \\ \vdots & \vdots & \dots & & \vdots \\ 1 & X_n & X_n^2 & ... & X_n^{n-1} \end{vmatrix}$$

(1) Montrer que $X_i - X_j$ divise f pour tout couple $i \neq j$.

(2) En déduire que $D := \prod_{1 \leq i < j \leq n}(X_i - X_j)$ divise f.

(3) En comparant les degrés totaux de f et D, montrer qu'il existe $c \in \mathbb{Z}$ tel que $f = cD$.

(4) En calculant $f(0, X_2, ..., X_n)$ et $D(0, X_2, ..., X_n)$, montrer par récurrence sur n que $c = 1$.

(5) Soit K un corps. Soient $a_1, ..., a_n \in K$. Montrer que

$$\begin{vmatrix} 1 & a_1 & a_1^2 & ... & a_1^{n-1} \\ 1 & a_2 & a_2^2 & ... & a_2^{n-1} \\ \vdots & \vdots & \dots & & \vdots \\ 1 & a_n & a_n^2 & ... & a_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (a_j - a_i).$$

Chapitre 3

Extensions de corps

Tous les corps considérés sont commutatifs. On étudie dans cette partie du cours les relations entre les corps. Si K, L sont deux corps, tout homomorphisme $K \to L$ (si cela existe) est automatiquement injectif car le noyau est un idéal propre, donc nul dans K. Dans ce cas on peut identifier K à un sous-corps de L. Comme exemple on a $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Dans $\mathbb{C}$ on a des nombres irrationnels mais qui sont "presque" rationnels. Par exemple, $\sqrt{2}$ est irrationnel, mais une opération simple comme prendre le carré le rend rationnel. De même, $\alpha := \sqrt{2}+\sqrt{3}$ est devient rationnel par l'opération $\alpha^4 - 10\alpha^2$ qui vaut -1. Ce type de nombres sont dits "algébriques" (définition 3.3.6). Un outil de base pour étudier, comparer les nombres algébriques entre eux est la théorie des extensions de corps.

3.1 Rappel sur les espaces vectoriels

Ceci est un vade mecum basique d'algèbre linéaire. Il n'a pas été exposé en cours.

On fixe un corps (commutatif) K. Un *espace vectoriel* E sur K (ou un K-espace vectoriel) est un groupe commutatif muni d'une loi de produit externe $K \times E \to E, (\lambda, x) \mapsto \lambda.x$ (ou noté plus simplement λx) vérifiant les axiomes suivants :

(1) (Distributivité) $\lambda(x + y) = \lambda x + \lambda y$, $(\lambda + \mu)x = \lambda x + \mu x$.

(2) (Associativité) $\lambda(\mu x) = (\lambda\mu)x$.

(3) $1_K.x = x$.

Remarque 3.1.1 On a $0_K.x = 0_E$, $\lambda.0_E = 0_E$, $(-1_K).x = -x$ pour tous $\lambda \in K$ et $x \in E$.

Définition 3.1.2 Soient E, F des K-espaces vectoriels. Une *application linéaire* $f : E \to F$ est une application telle que $f(x+y) = f(x)+f(y)$ et $f(\lambda x) = \lambda f(x)$

pour tous $\lambda \in K$, $x, y \in E$. On dit que f est un *isomorphisme* si elle est de plus bijective (l'application réciproque f^{-1} est alors linéaire aussi).

On dit que deux K-espaces vectoriels sont *isomorphes* s'il existe un isomorphisme entre eux.

Définition 3.1.3 Soit E un espace vectoriel sur K. Un *sous-espace vectoriel* F de E est un sous-groupe de E stable par le produit externe : $\lambda x \in F$ pour tous $\lambda \in K, x \in F$. Une intersection de sous-espaces vectoriels de E est un sous-espace vectoriel de E.

Définition 3.1.4 Soit S une partie de E. Le *sous-espace vectoriel de E engendré par S* est le plus petit sous-espace vectoriel de E contenant S. C'est l'ensemble des combinaisons linéaires $\lambda_1 s_1 + ... + \lambda_n s_n$ avec $\lambda_i \in K$ et $s_i \in S$. On dit que S est une *partie génératrice* de E si elle engendre E tout entier.

On dit que S est *liée* s'il existe $s_1, ..., s_n \in S$ et des $\lambda_1, ..., \lambda_n \in K$ non tous nuls, tels que $\lambda_1 s_1 + ... + \lambda_n s_n = 0$. On dit que S est *libre* si elle n'est pas liée. On dit alors que les éléments de S sont *linéairement indépendants*. Un partie qui est à la fois génératrice et libre est appelée une *base*.

On dit que E est de *dimension finie* (ou de type fini) s'il est engendré par une partie finie.

Théorème 3.1.5. *Soit E un espace vectoriel de dimension finie.*

(1) *De toute partie génératrice de E on peut extraire une base de E.*

(2) (Théorème de la base incomplète) *Soient L une partie libre et G une partie génératrice de E. Alors on peut compléter L en une base de E, en rajoutant des éléments de G.*

(3) *Toutes les bases de E ont le même cardinal. Ce cardinal s'appelle la* dimension de E, *et on le note* $\dim E$.

(4) *Soit $n = \dim E$. Alors E est isomorphe à K^n.*

(5) *Soit F un sous-espace vectoriel de E. Alors F est de dimension finie,* $\dim F \leq \dim E$, *l'égalité ayant lieu si et seulement si $E = F$.*

Remarque 3.1.6 On peut montrer à l'aide du lemme de Zorn que tout espace vectoriel admet une base.

Corollaire 3.1.7. *Soit E un espace vectoriel de dimension n.*

(1) *Toute partie libre de E a au plus n éléments. Autrement dit, toute famille $\{x_1, ..., x_m\}$ de E avec $m > n$ est liée.*

(2) *Toute partie génératrice de E a au moins n éléments.*

Theorem 3.1.8. *Soit $f : E \to F$ une application linéaire.*

(1) *Les ensembles* $\mathrm{Ker}\, f$ *et* $\mathrm{Im} f$ *sont respectivement des sous-espaces vectoriels de E et de F.*

(2) *Supposons E de dimension finie. Alors il en est de même pour* $\mathrm{Im} f$. *De plus on a*

$$\dim E = \dim \mathrm{Ker}\, f + \dim(\mathrm{Im} f) \quad \text{(Théorème du rang)}.$$

La dimension $\dim \mathrm{Im} f$ s'appelle le *rang* de f.

Corollaire 3.1.9. *Soient E, F des espaces vectoriels de dimension finie, de même dimension. Soit $f : E \to F$ une application linéaire. Alors f est un isomorphisme $\iff$ f injective $\iff$ f surjective.*

Exemple 3.1.10 Soit $E = K[X]$. Alors c'est un K-espace vectoriel. L'ensemble $\{X^i \mid i \geq 0\}$ forme une base de E sur K. L'ensemble $K_n[X]$ des polynômes de degré $\leq n$ est un sous-espace vectoriel de $K[X]$, et $\{X^i \mid 0 \leq i \leq n\}$ en est une base. La dérivation $K[X] \to K[X]$ est linéaire, surjective (si K est de caractéristique nulle), mais pas injective.

3.2 Généralités sur les extensions

Définition 3.2.1 Soit K un corps. Une *extension* de K , ou une *K-extension* est un corps L contenant K comme sous-corps. On écrit souvent L/K pour désigner une extension L de K. Un *homomorphisme d'extensions* $L \to N$ de K est un homomorphisme d'anneaux $f : L \to N$ tel que $f(\lambda) = \lambda$ pour tout $\lambda \in K$. Un homomorphisme des extensions de K s'appelle aussi un *K-homomorphisme*.

Une *sous-extension* de L/K est un sous-corps de L contenant K.

Exemple 3.2.2 $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$, $K(T)/K$ sont des extensions. $\mathbb{R}[X]$ n'est pas une extension de $\mathbb{R}$ car ce n'est pas un corps.

Soit

$$\mathbb{Q}[\sqrt{2}] := \mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

C'est un sous-anneau de $\mathbb{C}$ contenant $\mathbb{Q}$. On vérifie directement que c'est aussi un corps. En effet, si $a + b\sqrt{2} \neq 0$, $a/(a^2 - 2b^2) + (-b/(a^2 - 2b^2)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ est son inverse (noter que $a^2 - 2b^2 \neq 0$). C'est donc une sous-extension de $\mathbb{C}/\mathbb{Q}$.

Remarque 3.2.3 Si L/N et N/K sont des extensions, alors L/K est une extension.

Définition 3.2.4 Les corps $\mathbb{Q}$ et $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, p nombres premiers, sont appelés des *corps premiers*.

Exercice 3.2.5 Dans un corps premier, le seul automorphisme de corps est l'identité.

Proposition 3.2.6. *Soit L un corps. Alors L contient un unique corps premier.*

Preuve: Soit $\phi : \mathbb{Z} \to L$ l'unique homomorphisme d'anneaux. Son noyau est un idéal premier de $\mathbb{Z}$, donc égal à $\{0\}$ ou $p\mathbb{Z}$ pour un nombre premier p. Dans le premier cas ϕ est alors injectif et induit donc un homomorphisme (automatiquement injectif) de corps $\mathbb{Q} \to L$ donné par $k/q \mapsto (q \cdot 1_L)^{-1}(k \cdot 1_L)$.

Si $\ker \phi = p\mathbb{Z}$, alors le théorème de factorisation donne un homomorphisme injectif canonique $\mathbb{F}_p \to L$.

Montrons l'unicité. Si L contient $\mathbb{Q}$, alors $p.1_L = p.1_{\mathbb{Q}} = p \neq 0$ pour tout p, donc L ne contient pas de $\mathbb{F}_p$. Si L contient $\mathbb{F}_p$, alors il ne contient pas $\mathbb{Q}$ car $p.1_L = p.1_{\mathbb{F}_p} = 0$. De même, si L contient $\mathbb{F}_p$ et si ℓ est un autre nombre premier, il existe par Bézout $u, v \in \mathbb{Z}$ tels que $u\ell + vp = 1$. Il suit que $u.(\ell.1_L) = -1_L \neq 0$, donc $\ell.1_L \neq 0$ et L ne peut pas contenir $\mathbb{F}_\ell$.

Définition 3.2.7 Si L contient $\mathbb{Q}$ on dit qu'il est de caractéristique nulle. S'il contient $\mathbb{F}_p$ on dit qu'il est de caractéristique p.

Si L/K est une extension, pour toute famille $\{E_i\}_i$ de sous-extensions, $\cap_i E_i$ est une sous-extension.

Définition 3.2.8 Soit L/K une extension. Soit S une partie de L. On appelle *sous-extension engendrée par* S et on note $K(S)$ la plus petite sous-extension de L/K contenant S.

L'extension $K(S)$ existe et est unique ; elle est égale à l'intersection des sous-extensions de L/K contenant S.

Remarque 3.2.9 Si $S = \{x_1, ..., x_n\}$, on note aussi $K(S)$ par $K(x_1, ..., x_n)$. On peut expliciter cette extension comme suit. Soit N l'ensemble des éléments de L de la forme $P(x_1, ..., x_n)/Q(x_1, ..., x_n)$ avec $P(X_1, ..., X_n), Q(X_1, ..., X_n) \in K[X_1, ..., X_n]$ et $Q(x_1, ..., x_n) \neq 0$. Alors on voit aisément que N est une sous-extensions de L/K. Montrons que $K(S) = N$. Comme N contient S, on a $K(S) \subseteq N$. Comme $K(S)$ est un corps qui contient K et les x_i, il contient les $P(x_1, ..., x_n)$, les $1/Q(x_1, ..., x_n)$ si $Q(x_1, ..., x_n) \neq 0$ et donc les fractions $P(x_1, ..., x_n)/Q(x_1, ..., x_n)$. Donc $N \subseteq K(S)$.

Exemple 3.2.10 Dans l'extension $\mathbb{C}/\mathbb{Q}$, considérons la sous-extension $\mathbb{Q}(\sqrt{2})$ engendrée par $\sqrt{2}$.Un calcul direct comme ci-dessus montre que $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2}$.

3.3 Extensions algébriques

3.3.1 Éléments algébriques

Notons d'abord un fait très util qui est le suivant. Si A est un anneau qui contient un corps K, alors A possède naturellement une structure de K-espace vectoriel, le produit externe étant défini par $\lambda.a = \lambda a$ si $\lambda \in K$ et $a \in A$. En particulier, pour toute extension L/K, L possède une structure naturelle de K-espace vectoriel.

Définition 3.3.1 On dit que L/K est une *extension finie* si L est de dimension finie sur K en tant qu'espace vectoriel.

Définition 3.3.2 Soit L/K une extension. Un élément $\alpha \in L$ est appelé un *élément algébrique (sur K)* s'il existe un polynôme $P(X) \in K[X]$ non-nul tel que $P(\alpha) = 0$. Autrement dit, α satisfait une relation polynomiale sur K. En divisant par le coefficient dominant, on peut toujours supposer $P(X)$ unitaire.

Exemple 3.3.3 Tout élément de K est algébrique sur K.

Exemple 3.3.4 Les nombres $\sqrt{2}, \sqrt{3}, i = \sqrt{-1} \in \mathbb{C}$ sont clairement algébriques sur $\mathbb{Q}$, racines des polynômes $X^2-2, X^2-3, X^2+1 \in \mathbb{Q}[X]$. La somme $\sqrt{2}+\sqrt{3}$ est racine du polynôme $X^4 - 10X^2 + 1$ obtenu comme le produit

$$(X - (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3}))(X - (-\sqrt{2} + \sqrt{3}))(X - (-\sqrt{2} - \sqrt{3})).$$

Il est donc algébrique sur $\mathbb{Q}$. On verra plus loin (remarque 3.3.21) une méthode qui permet de dire directement que $\sqrt{2} + \sqrt{3}$ est algébrique sur $\mathbb{Q}$ sans avoir à trouver un polynôme qui l'annule.

Exercice 3.3.5 Montrer que $X^4 - 10X^2 + 1$ est irréductible dans $\mathbb{Z}[X]$.

Définition 3.3.6 Un nombre complexe algébrique sur $\mathbb{Q}$ est appelé un *nombre algébrique*. Un nombre complexe qui n'est pas algébrique sur $\mathbb{Q}$ est appelé un *nombre transcendant*.

Exemple 3.3.7 Les nombres e (Hermite, 1873), π (Lindemann, 1882), $2^{\sqrt{2}}$ et e^{π} (Gelfond, 1934) sont transcendants. Les nombres de Liouville $\sum_{n\geq 1} a_n/10^{n!}$ avec $a_n \in \mathbb{N}$, compris entre 1 et 9, sont transcendants (voir TD).

Nous allons à présent donner un critère d'algébricité.

Lemme 3.3.8. *Soit A un anneau intègre contenant un corps K. On suppose que A est de dimension finie en tant que K-espace vectoriel. Alors A est un corps.*

Preuve: Soit $\alpha \in A$ non-nul. L'application $[\alpha] : A \to A$, $x \mapsto \alpha x$ est un endomorphisme K-linéaire injectif. Comme $\dim_K A$ est finie, il suit du corollaire 3.1.9 que $[\alpha]$ est surjectif. Soit $\beta \in A$ tel que $[\alpha](\beta) = 1$, alors $\alpha\beta = 1$, donc α est inversible et A est un corps.

Notation Soit L/K une extension. Soit $\alpha \in L$. On note $K[\alpha]$ l'ensemble des éléments de la forme $P(\alpha)$ avec les $P(X) \in K[X]$. C'est clairement un sous-anneau de L qui contient K. C'est aussi l'image de l'homomorphisme d'anneaux $\varphi : K[X] \to L$ défini par $\varphi(\sum_i \lambda_i X^i) = \sum_i \lambda_i \alpha^i$. C'est l'ensemble des combinaisons K-linéaires des puissances de α.

Il est aisé de voir que cette notation coïncide avec celle utilisée auparavant comme par exemple $\mathbb{Q}[\sqrt{2}]$.

Proposition 3.3.9. *Soient L/K une extension et $\alpha \in L$. Alors les propriétés suivantes sont équivalentes :*

(i) *α est algébrique sur K ;*

(ii) *$K[\alpha]$ est une extension finie de K ;*

(iii) *Il existe une sous-extension finie L'/K de L contenant α ;*

Preuve: (i) implique (ii) : Soit $P_0(X) \in K[X]$ un polynôme non nul qui annule α. Soit $d = \deg P_0(X) \geq 1$. Pour tout polynôme $P(X) \in K[X]$, il existe $Q(X), R(X) \in K[X]$ tels que $P(X) = P_0(X)Q(X)+R(X)$ et que $\deg R(X) < d$. Il suit que $P(\alpha) = R(\alpha)$ est une combinaire linéaire de $1, \alpha, ..., \alpha^{d-1}$ à coefficients dans K. Par conséquent $K[\alpha]$ est un anneau intègre, de dimension finie sur K. D'après le lemme 3.3.8, c'est un corps, donc une extension finie de K.

(ii) implique (iii) : On prend $L' = K[\alpha]$.

(iii) implique (i) : Soit $m = \dim L'$. Alors $\{1, \alpha, ..., \alpha^m\}$ est liée (corollaire 3.1.7) : il existe $\lambda_0, ..., \lambda_m \in K$, non tous nuls, tels que $\lambda_0.1+\lambda_1\alpha+...+\lambda_m\alpha^m = 0$. Soit $P_0(X) = \lambda_0 + \lambda_1 X + ... + \lambda_m X^m \in K[X]$. C'est un polynôme non nul et $P_0(\alpha) = 0$. Donc α est algébrique sur K.

Définition 3.3.10 On dit qu'une extension L/K est *algébrique* si tout élément de L est algébrique sur K.

Corollaire 3.3.11. *Toute extension finie L/K est algébrique.*

Preuve: Utiliser la propriété (iii) de la proposition ci-dessus avec $L' = L$.

Remarque 3.3.12 La réciproque est fausse : une extension algébrique n'est pas nécessairement finie. Voir l'exemple 3.3.22 plus loin.

Corollaire 3.3.13. *Soit $\alpha \in L$ algébrique sur K. Alors pour tout $P(X) \in K[X]$, $P(\alpha) \in L$ est algébrique sur K.*

Par exemple, le nombre réel $\sqrt[3]{2}$ est clairement un nombre algébrique. Ce corollaire implique que pour tous $a, b, c \in \mathbb{Q}$, $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ est un nombre algébrique, ce qui n'est pas complètement évident de prime abord.

Exercice 3.3.14 Soient L/K une extension et $\alpha \in L$. Montrer que α est algébrique sur K si et seulement si $K[\alpha] = K(\alpha)$ (voir la notation de la remarque 3.2.9).

3.3.2 Extensions finies

On a vu précédement que si α est algébrique sur K, alors toute combinaison K-linéaire des puissances de α est algébrique sur K. Plus généralement, si on prends deux éléments de L algébriques sur K, que peut-on dire de leurs somme et produit ? Sont-ils également algébriques sur K ?

Définition 3.3.15 Soit L/K une extension finie. Le *degré* de l'extension L/K, noté $[L : K]$, est la dimension de L en tant que K-espace vectoriel.

Théorème 3.3.16 (Théorème de la base téléscopique)**.** *Soient L/N et N/K des extensions. Alors l'extension L/K est finie si et seulement si L/N et N/K sont finies. Si ces conditions sont remplies, on aura la relation*

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

En particulier $[N : K] \mid [L : K]$. Autrement dit, dans une extension finie, le degré de toute sous-extension divise le degré de l'extension.

Preuve: Si L/K est finie, alors N/K est finie puisque N est un sous-K-espace vectoriel de L (théorème 3.1.5(f)). D'autre part, un système de générateurs de L comme K-espace vectoriel est *a fortiori* un système de générateurs de L comme N-espace vectoriel. Donc L/N est finie.

Inversement, supposons que L/N et N/K sont finies. Soient $e_1, ..., e_n$ une base de N sur K, et $f_1, ..., f_m$ une base de L/N. Alors tout élément $\alpha \in L$ s'écrit comme

$$\alpha = \sum_{1 \leq j \leq m} \lambda_j f_j, \quad \lambda_j \in N.$$

On a

$$\lambda_j = \sum_{1 \leq i \leq n} \mu_{ij} e_i, \quad \mu_{ij} \in K.$$

Donc

$$\alpha = \sum_{1\leq i\leq n, 1\leq j\leq m} \mu_{ij}(e_i f_j).$$

Par conséquent $\{e_i f_j\}_{1\leq i\leq n, 1\leq j\leq m}$ est une famille génératrice du K-espace vectoriel L. Montrons que c'est une base. Si

$$\sum_{1\leq i\leq n, 1\leq j\leq m} v_{ij}(e_i f_j) = 0, \quad v_{ij} \in K,$$

alors

$$\sum_{1\leq j\leq m} \delta_j f_j = 0, \quad \text{où} \;\; \delta_j = \sum_i v_{ij} e_j \in N.$$

Donc pour tout $j \leq m$, on a $\sum_{1\leq i\leq n} v_{ij} e_i = \delta_j = 0$. Il suit que $v_{ij} = 0$ pour tout i, j. Cela implique bien que L/K est une extension finie de degré $mn = [L : N][N : K]$.

Exercice 3.3.17 Soient L/K une extension finie et N/K une sous-extension. Montrer que $[N : K] = 1$ équivaut à $N = K$ et que $[N : K] = [L : K]$ équivaut à $N = L$.

Exercice 3.3.18 Soit L/K une extension de degré premier. Montrer que K et L sont les seules sous-extensions de L/K.

Notation Soit L/K une extension. Soient $\alpha_1, ..., \alpha_m \in L$. On note

$$K[\alpha_1, ..., \alpha_m] = \{F(\alpha_1, ..., \alpha_m) \mid F(X_1, ..., X_m) \in K[X_1, ..., X_m]\}.$$

C'est un sous-anneau (intègre) de L qui contient K. C'est l'ensemble des combinaisons K-linéaires des produits de puissances des α_i. Quand $m = 1$, on retrouve la notation qui précède la proposition 3.3.9.

Exercice 3.3.19 Soit L/K une extension finie. Montrer qu'il existe $\alpha_1, \ldots, \alpha_m$ dans L tels que $L = K[\alpha_1, \ldots, \alpha_m]$. Si K est de caractéristique nulle, on peut montrer que qu'il existe toujours un $\alpha \in L$ tel que $= K[\alpha]$.

Proposition 3.3.20. *Soit L/K une extension. Soient $\alpha_1, ..., \alpha_m \in L$ des éléments algébriques sur K. Alors $K[\alpha_1, ..., \alpha_m]$ est une extension finie de K. En particulier, pour tout $F(X_1, ..., X_m) \in K[X_1, ..., X_m]$, $F(\alpha_1, ..., \alpha_m)$ est algébrique sur K.*

Preuve: Procédons par récurrence sur m. Le cas $m = 1$ résulte de la proposition 3.3.9 (ii). Supposons avoir montré la proposition pour $m - 1$. Alors $N := K[\alpha_1, ..., \alpha_{m-1}]$ est une extension finie de K. Comme α_m est algébrique sur K, donc algébrique sur N, $N[\alpha_m]$ est une extension finie de N. Par le théorème 3.3.16, $N[\alpha_m]$ est finie sur K. Ce qui achève la démontration puisque $N[\alpha_m] = K[\alpha_1, ..., \alpha_m]$ (car $K[X_1, \ldots, X_m] = K[X_1, \ldots, X_{m-1}][X_m]$).

Corollaire 3.3.21. *Soit L/K une extension.*

(1) *Soient $\alpha, \beta \in L$ algébriques sur K. Alors $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur K. Si de plus $\alpha \neq 0$, alors α^{-1} est algébrique sur K.*

(2) *L'ensemble K^c des éléments $\gamma \in L$ algébriques sur K est une sous-extension algébrique de L.*

Preuve: (1) Comme $\alpha + \beta, \alpha\beta \in K[\alpha, \beta]$, ils sont algébriques sur K. Il en est de même pour $\alpha - \beta$. Si $\alpha \neq 0$, c'est un élément non nul du corps $K[\alpha]$, donc $\alpha^{-1} \in K[\alpha]$ et est donc algébrique sur K.

(2) C'est une conséquence immédiate de (1) et de la définition des extensions algébriques.

Exemple 3.3.22 L'ensemble $\overline{\mathbb{Q}}$ des nombres algébriques (nombres complexes algébriques sur $\mathbb{Q}$) est une extension algébrique infinie de $\mathbb{Q}$. En effet pour tout $d \geq 1$, le critère d'Eisenstein montre que $X^d - 2 \in \mathbb{Q}[X]$ est irréductible. Par des considérations du polynôme minimal (§3.3.4, proposition 3.3.39), on voit que $[\mathbb{Q}[\sqrt[d]{2}] : \mathbb{Q}] = d$. Si $\overline{\mathbb{Q}}$ était finie sur $\mathbb{Q}$, son degré serait $\geq d$ pour tout d, absurde.

Proposition 3.3.23 (Composition d'extensions algébriques)**.** *Soient L/N, N/K des extensions algébriques. Alors L/K est algébrique.*

Preuve: (Non présentée en cours) Soit $\alpha \in L$. Il existe $a_0, \ldots, a_{d-1} \in N$ tels que

$$a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} + \alpha^d = 0.$$

Donc α est algébrique sur la sous-K-extension finie $N_0 := K[a_0, \ldots, a_{d-1}]$ de L. Il suit que $N_0[\alpha]$ est finie sur N_0, donc finie sur K. Par conséquent $\alpha \in N_0[\alpha]$ est algébrique sur K.

Exercice 3.3.24 Montrer que toute extension algébrique est la réunion de ses sous-extensions finies.

3.3.3 Compositum de sous-extensions

Définition 3.3.25 Soient L_1, L_2 deux sous-extensions de L/K. On appelle *le compositum* de L_1, L_2 dans L la sous-extension de L engendrée par $L_1 \cup L_2$. On la note L_1L_2. Si $L_i = K(S_i)$, alors $L_1L_2 = K(S_1 \cup S_2)$.

Exemple 3.3.26 Soient $\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m \in L$ des éléments algébriques et soient $L_1 = K[\alpha_1, ..., \alpha_n]$, $L_2 = K[\beta_1, ..., \beta_m]$. Alors

$$L_1L_2 = K[\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m].$$

En effet le terme de droite est une sous-extension de L (proposition 3.3.20) contenant L_1 et L_2, et il est clairement contenu dans tout sous-corps de L contenant L_1 et L_2.

Lemme 3.3.27. *Soient L_1, L_2 deux sous-extensions finies de L/K. Alors on a $L_1L_2 = F$ où F est l'ensemble des sommes finies $\sum_k x_k y_k$ avec $x_k \in L_1$ et $y_k \in L_2$. De plus, si $\{e_1, ..., e_n\}$, $\{f_1, ..., f_m\}$ sont des familles génératrices (linéaires) respectives de L_1 et de L_2 sur K, alors $\{e_i f_j\}_{1 \leq i \leq n, 1 \leq j \leq m}$ est une famille génératrice de F sur K.*

Preuve: Comme L_1L_2 est un corps contenant $L_1 \cup L_2$, il est clair que L_1L_2 contient F.

L'ensemble F est clairement un sous-espace vectoriel de L contenant K. L'assertion sur la famille génératrice est immédiate. En particulier, F est de dimension finie sur K. Comme F est stable par multiplication, c'est un sous-anneau de L. Par conséquent F est un anneau intègre contenant K, de dimension finie sur K (comme espace vectoriel), c'est donc un corps (lemme 3.3.8), sous-extension de L contenant $L_1 \cup L_2$. Par définition on a alors $F \supseteq L_1L_2$. D'où $F = L_1L_2$.

Proposition 3.3.28. *Soient L_1, L_2 deux sous-extensions finies d'une extension L/K. Alors L_1L_2 est une extension finie de K. De plus, on a*

$$[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$$

et $[L_1L_2 : K]$ est divisible par $[L_1 : K]$ et par $[L_2 : K]$.

Preuve: La première partie résulte du lemme précédent. Le fait que $[L_1 : K]$ et $[L_2 : K]$ divisent $[L_1L_2 : K]$ suit de la proposition 3.3.20 puisque L_1 et L_2 sont des sous-extensions de L_1L_2/K.

Corollaire 3.3.29. *Si $[L_1 : K]$ et $[L_2 : K]$ sont premiers entre eux, alors*

$$[L_1L_2 : K] = [L_1 : K][L_2 : K].$$

Remarque 3.3.30 Attention, en général $[L_1L_2 : K] \neq [L_1 : K][L_2 : K]$. Par exemple si on prend $K = \mathbb{Q}$, $L = \mathbb{C}$ et $L_1 = L_2 \neq \mathbb{Q}$ une extension finie de $\mathbb{Q}$, alors $L_1L_2 = L_1$ et on a $[L_1L_2 : \mathbb{Q}] = [L_1 : \mathbb{Q}] < [L_1 : \mathbb{Q}][L_2 : \mathbb{Q}]$.

Exemple 3.3.31 On a $[\mathbb{Q}[\sqrt{2}, \sqrt[3]{5}] : \mathbb{Q}] = 6$. En effet, $\mathbb{Q}[\sqrt{2}, \sqrt[3]{5}]$ est le compositum des extensions $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt[3]{5}]$ dans $\mathbb{C}$ qui sont de degrés premiers entre eux.

Exercice 3.3.32 Calculer les degrés de $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ et de $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ sur $\mathbb{Q}$.

Exercice 3.3.33 Montrer que $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ et que $\mathbb{Q}[\sqrt{2}, \sqrt[3]{5}] = \mathbb{Q}[\sqrt{2} + \sqrt[3]{5}]$.

Exercice 3.3.34 Soit L/K une extension. Soient M, N des sous-extensions algébriques de L. Montrer que MN est algébrique sur K.

3.3.4 Polynôme minimal d'un élément algébrique

Soit L/K une extension. Si $\alpha \in L$ est algébrique sur K, on a envie de connaître les polynômes dans $K[X]$ qui s'annulent en α.

Lemme 3.3.35. *Soit $\alpha \in L$ un élément algébrique sur K. Alors l'ensemble*

$$\{F(X) \in K[X] \mid F(\alpha) = 0\}$$

est un idéal de $K[X]$, engendré par un unique polynôme unitaire irréductible $P(X)$.

Preuve: Cet ensemble est clairement un idéal premier, non-nul car α est algébrique sur K. D'où le lemme.

Définition 3.3.36 Soient L/K une extension et $\alpha \in L$ un élément algébrique sur K. On appelle *polynôme minimal (ou irréductible) de α sur K* et on le note $\mathrm{Irr}(\alpha, K, X) \in K[X]$ le générateur unitaire $P(X)$ ci-dessus. On appelle *degré de α sur K* le degré de ce polynôme.

La proposition suivante est immédiate.

Proposition 3.3.37. *Soit $\alpha \in L$ algébrique sur K.*

(1) *Si un polynôme irréductible unitaire dans $K[X]$ s'annule en α, alors c'est le polynôme minimal de α.*

(2) *Si un polynôme dans $K[X]$ de degré $< \deg \mathrm{Irr}(\alpha, K, X)$ s'annule en α, alors il est nul.*

(3) *Si $F(X) \in K[X]$ est unitaire, de même degré que α et s'annule en α, alors il est égal à $\mathrm{Irr}(\alpha, K, X)$.*

Exemple 3.3.38 Soit $d \geq 2$. Le polynôme $X^d - 2 \in \mathbb{Q}[X]$ est irréductible par le critère d'Eisenstein (théorème 2.2.9, prendre $A = \mathbb{Z}$ et $f = 2$). Donc $2^{1/d} \in \mathbb{R}$, qui est une des racines de ce polynôme, est de degré d sur $\mathbb{Q}$, et a pour polynôme minimal $X^d - 2$ sur $\mathbb{Q}$.

Nous allons maintenant relier le degré d'un élément algébrique au degré de la sous-extension qu'il engendre.

Proposition 3.3.39. *Soit $\alpha \in L$ un élément algébrique sur K. Soit $P(X) = \mathrm{Irr}(\alpha, K, X)$.*

(a) *On a un isomorphisme de corps $\tilde{\varphi} : K[X]/(P(X)) \simeq K[\alpha]$.*

(b) *On a $[K[\alpha] : K] = \deg P(X) = \deg_K \alpha$.*

Démonstration. (a) Soit $\varphi : K[X] \to L$ l'homomorphisme d'anneaux défini par

$$\varphi(\sum_i \lambda_i X^i) = \sum_i \lambda_i \alpha^i.$$

(voir la preuve du théorème 1.2.27). Alors $K[\alpha] = \mathrm{Im}\varphi$ et $P(X)$ est un générateur de l'idéal $\mathrm{Ker}\,\varphi$. Le théorème de factorisation dit alors que φ induit un isomorphisme d'anneaux

$$\tilde{\varphi} : K[X]/(P(X)) \simeq K[\alpha].$$

(b) Soit $d = \deg P(X)$. Soit $F(X) \in K[X]$. On va évaluer $F(\alpha)$. Par la division euclidienne on a

$$F(X) = Q(X)P(X) + R(X), \quad R(X) < d.$$

Donc $F(\alpha) = R(\alpha)$. On écrit $R(X) = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1} \in K[X]$, alors $R(\alpha) = a_0.1 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$. Donc $\{1, \alpha, ..., \alpha^{d-1}\}$ est une famille génératrice de $K[\alpha]$ sur K. Montrons qu'elle est libre. Soient $a_0, ..., a_{d-1} \in K$ tels que

$$a_0 + a_1\alpha + ... + a_{d-1}\alpha^{d-1} = 0.$$

Soit $R(X) = a_0 + a_1 X + ... + a_{d-1}X^{d-1} \in K[X]$. Alors $R(\alpha) = 0$, $\deg R(X) < d$, donc $R(X) = 0$ et $a_i = 0$ pour tout $i \leq d-1$. Par conséquent $[K[\alpha] : K] = d$. □

Exemple 3.3.40 La proposition ci-dessus permet de calculer le degré d'un élément algébrique sans connaître explicitement son polynôme irréductible.

Soit $n \geq 3$. On souhaite calculer le degré de $\cos(2\pi/n) \in \mathbb{R}$ sur $\mathbb{Q}$. Soit $\xi_n = e^{2i\pi/n} \in \mathbb{C}$. On a $\cos(2\pi/n) = (\xi_n + \xi_n^{-1})/2 \in \mathbb{Q}[\xi_n]$. Calculons d'abord le degré de ξ_n sur $\mathbb{Q}[\cos(2\pi/n)]$. On a

$$\xi_n^2 - 2\cos(2\pi/n)\xi_n + 1 = 0,$$

donc ξ_n est de degré au plus 2 sur $\mathbb{Q}[\cos(2\pi/n)]$. Mais $\xi_n \notin \mathbb{R}$, alors que l'extension $\mathbb{Q}[\cos(2\pi/n)]$ est contenue dans $\mathbb{R}$. Donc $\xi_n \notin \mathbb{Q}[\cos(2\pi/n)]$ et est de degré 2 sur $\mathbb{Q}[\cos(2\pi/n)]$.

On verra que ξ_n est de degré $\varphi(n)$, la fonction d'indicatrice d'Euler ($\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$). Comme

$$\big[\mathbb{Q}[\xi_n] : \mathbb{Q}\big] = \big[\mathbb{Q}[\xi_n] : \mathbb{Q}[\cos(2\pi/n)]\big]\,\big[\mathbb{Q}[\cos(2\pi/n)] : \mathbb{Q}\big] = 2\big[\mathbb{Q}[\cos(2\pi/n)] : \mathbb{Q}\big],$$

on obtient

$$\big[\mathbb{Q}[\cos(2\pi/n)] : \mathbb{Q}\big] = \varphi(n)/2.$$

Cela implique en particulier que $\cos(2\pi/n)$ est irrationnel si $n \geq 5$ (parce que $\varphi(n)$ est alors ≥ 3).

Exercice 3.3.41 Soit L/K une extension finie. Montrer que pour tout $\alpha \in L$, on a $\deg_K \alpha \mid [L : K]$.

Soit p un nombre premier. Montrer que pour tout $x \in \mathbb{Q}[\sqrt[p]{2}]$, on a $x \in \mathbb{Q}$ ou $\deg_{\mathbb{Q}} x = p$.

Exercice 3.3.42 Soit $\alpha \in L$ de degré d sur K. Montrer que $\lambda\alpha + \mu$ est de degré d sur K pour tout $\lambda \in K^*, \mu \in K$.

3.3.5 Corps de rupture, corps de décomposition

Soit $P(X) \in K[X]$ un polynôme irréductible. Si $\deg P(X) > 1$, alors $P(X)$ n'a pas de racine dans K. Cependant, en élargissant convenablement K, $P(X)$ admettra une racine.

Attention Quand on parle des racines d'un polynôme, toujours préciser dans quel corps !

Définition 3.3.43 Soit $P(X) \in K[X]$ un polynôme irréductible. Un *corps de rupture* de $P(X)$ est une extension E/K telle que $P(X)$ admette une racine $\alpha \in E$ et que $E = K[\alpha]$. Ainsi un corps de rupture est une extension de K engendrée par une racine de $P(X)$. C'est aussi une extension de K dans laquelle $P(X)$ admet une racine, et qui est minimale pour cette propriété.

Si $\deg P(X) \geq 2$, alors $P(X)$ n'est plus irréductible dans $E[X]$. On rompt ainsi l'irréductibilité de $P(X)$.

Proposition 3.3.44. *Soit $P(X) \in K[X]$ un polynôme irréductible. Alors $P(X)$ admet un corps de rupture, isomorphe à $K[X]/(P(X))$. De plus, les corps de rupture de $P(X)$ sont isomorphes comme extensions de K, et sont de degré* $\deg P(X)$ *sur K.*

Démonstration. On peut supposer $P(X)$ unitaire en le divisant par son coefficient dominant. Soit $L = K[X]/(P(X))$. Soit α l'image de X dans L. Alors $P(\alpha) = 0$ et $L = K[\alpha]$. Donc L est un corps de rupture de $P(X)$.

Soit E un corps de rupture de $P(X)$. Soit α une racine de $P(X)$ dans E. Alors $P(X) = \mathrm{Irr}(\alpha, K, X)$. On applique alors la proposition 3.3.39. □

Définition 3.3.45 Soit $F(X) \in K[X]$ un polynôme non-constant de degré d, non nécessairement irréductible. Un *corps de décomposition* de $F(X)$ est une extension L/K telle que $F(X)$ soit *scindé* (c'est-à-dire produit de facteurs de degré 1, **pas nécessairement distincts**) dans $L[X]$ et que $L = K[\alpha_1, ..., \alpha_d]$ où $\alpha_1, ..., \alpha_d$ sont les racines de $F(X)$ dans L.

Remarque 3.3.46 Soit $P(X) \in K[X]$ non constant.

1. Si $P(X)$ est irréductible, et si L/K est une extension dans la quelle $P(X)$ possède une racine $\alpha \in L$, alors $K[\alpha] \subseteq L$ est un corps de rupture de $P(X)$.
2. Si L/K est une extension dans laquelle $P(X)$ est scindée :

$$P(X) = a \prod_{1 \leq i \leq d} (X - \alpha_i), \quad a, \alpha_i \in L,$$

alors $K[\alpha_1, \ldots, \alpha_d] \subseteq L$ est un corps de décomposition de $P(X)$.

Proposition 3.3.47. *Tout polynôme non-constant $F(X) \in K[X]$ admet un corps de décomposition.*

Démonstration. Nous procédons par récurrence sur le degré d de $F(X)$. Si $d = 1$, il n'y a rien à montrer, $F(X)$ est déjà scindé dans $K[X]$. Supposons la propriété vraie pour tout polynôme de degré $\leq d - 1$ pour tout corps K. Soit $P(X)$ un facteur irréductible de $F(X)$. Soit E un corps de rupture de $P(X)$. Alors il existe $\alpha_d \in E$ tel que $X - \alpha_d \mid P(X)$ dans $E[X]$. Donc $F(X) = (X - \alpha_d)G(X)$ avec $G(X) \in E[X]$ et $\deg G(X) = d - 1$. Par hypothèse de récurrence, il existe un corps de décomposition L pour $G(X)$:

$$G(X) = c \prod_{1 \leq i \leq d-1} (X - \alpha_i), \quad c \in K^*, \alpha_i \in L.$$

Donc $F(X) = c \prod_{1 \leq i \leq d} (X - \alpha_i)$ est scindé dans $L[X]$. De plus,

$$L = E[\alpha_1, ..., \alpha_{d-1}] = K[\alpha_d][\alpha_1, ..., \alpha_{d-1}] = K[\alpha_1, ..., \alpha_d].$$

Donc L est bien un corps de décomposition de $F(X)$. □

Exemple 3.3.48 Soit $P(X) = X^3 - 5 \in \mathbb{Q}[X]$. Alors $\mathbb{Q}[\xi_3^k \sqrt[3]{5}]$ est un corps de rupture de $P(X)$ pour tout $k \in \mathbb{Z}$. On voit que $\mathbb{Q}[\sqrt[3]{5}]$ et $\mathbb{Q}[\xi_3 \sqrt[3]{5}]$ sont deux corps de rupture de $P(X)$, contenus dans $\mathbb{C}$, isomorphes entre eux, mais non égaux.

L'extension $\mathbb{Q}[\sqrt[3]{5}, \xi_3 \sqrt[3]{5}, \xi_3^2 \sqrt[3]{5}] = \mathbb{Q}[\sqrt[3]{5}, \xi_3]$ de $\mathbb{Q}$ est un corps de décomposition de $P(X)$.

Proposition 3.3.49. *Soit $F(X) \in K[X]$ un polynôme non-constant. Alors les corps de décomposition de $F(X)$ sont isomorphes entre eux comme extensions de K.*

Démonstration. Nous allons montrer une version plus forte de la proposition. Soit $\sigma : K_1 \to K_2$ un isomorphisme de corps. Il s'étend naturellement en un isomorphisme d'anneaux $\tau : K_1[X] \to K_2[X]$. Soient $F_1(X) \in K_1[X]$ non-constant et $F_2(X) = \tau(F_1(X))$. Soient L_1, L_2 des corps de décomposition respectifs de $F_1(X), F_2(X)$. Nous allons montrer par récurrence sur $d = \deg F_1(X)$ que σ se prolonge en un isomorphisme $L_1 \to L_2$.

Si $d = 1$ (ou plus généralement si $F_1(X)$ est scindé dans $K_1[X]$), alors $L_i = K_i$ et il n'y a rien à démontrer. Supposons $d \geq 2$ et la proposition démontrée pour tout polynôme de degré $\leq d - 1$.

On peut supposer que $F_1(X)$ n'est pas scindé. Soit $P_1(X) \in K_1[X]$ un facteur irréductible de degré ≥ 2 de $F_1(X)$. Alors $P_1(X)$ admet une racine $\alpha_1 \in L_1$, et $E_1 := K_1[\alpha_1]$ est un corps de rupture de $P_1(X)$, $F_1(X) = (X - \alpha_1)Q_1(X)$ avec $Q_1(X) \in E_1[X]$, et L_1 est un corps de décomposition de $Q_1(X) \in E_1[X]$.

Soit $P_2(X) = \tau(P_1(X))$. On définit similairement $\alpha_2 \in L_2$, E_2 et $Q_2(X)$. Alors σ se prolonge en un isomorphisme

$$\sigma' : E_1 \to K_1[X]/(P_1(X)) \to K_2[X]/(P_2(X)) \to E_2$$

tel que $\sigma'(\alpha_1) = \alpha_2$. Comme plus haut, σ' se prolonge de manière naturelle en un isomorphisme $\tau' : E_1[X] \to E_2[X]$ avec $\tau'(Q_1(X)) = Q_2(X)$.

On applique alors l'hypothèse de récurrence à $\sigma' : E_1 \to E_2$ et $Q_1(X) \in E_1[X]$, et on conclude que σ' se prolonge en un isomorphisme $L_1 \to L_2$. □

Les propositions 3.3.44, 3.3.47, 3.3.49 sont présentées sans démonstration en cours.

3.3.6 Clôture algébrique

Proposition 3.3.50. *Soit K un corps. Alors les propriétés suivantes sont équivalentes.*

(i) *Tout polynôme non-constant sur K est scindé sur K (cf. 3.3.45) ;*

(ii) *Tout polynôme non-constant sur K admet une racine dans K ;*

(iii) *Les polynômes irréductibles de K sont de degré 1 ;*

(iv) *Toute extension algébrique de K est égale à K.*

Démonstration. Il est clair que (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Montrons (iii) $\Longrightarrow$ (iv). Soient L/K une extension algébrique et $\alpha \in L$. Comme $\mathrm{Irr}(\alpha, K, X) \in K[X]$ est irréductible, donc de dégré 1, et s'annule en α, on a $\alpha \in K$. Donc $L = K$. Montrons enfin (iv) $\Longrightarrow$ (i). Soit $F(X) \in K[X]$ non-constant. Alors $F(X)$ est scindé sur un corps de décomposition L de $F(X)$. Comme L/K est algébrique, on a $L = K$, donc $F(X)$ est scindé sur K. □

Définition 3.3.51 Un corps K qui vérifie une des conditions équivalentes ci-dessus est dit *algébriquement clos.*

Définition 3.3.52 Soit K un corps. Une *clôture algébrique de K* est une extension algébrique K^c/K avec K^c algébriquement clos.

Le théorème suivant est admis.

Théorème 3.3.53. (Steinitz) *Soit K un corps. Alors K admet une clôture algébrique. Toutes les clôtures algébriques de K sont K-isomorphes entre elles.*

Théorème 3.3.54 (Théorème de d'Alembert-Gauss)**.** *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Démonstration. Soit $P(z) \in \mathbb{C}[z]$ un polynôme complexe non constant. La fonction $|P(z)| : \mathbb{C} \to \mathbb{R}$ tend vers $+\infty$ quand $|z| \to +\infty$. Il existe donc $d > 0$ tel que $|P(z)| > |P(0)|$ pour tous $|z| > d$. Il suit que

$$\inf_{z\in\mathbb{C}} |P(z)| = \inf_{|z|\leq d} |P(z)|.$$

Comme $\{z \in \mathbb{C} \mid |z| \leq d\}$ est compact et que $|P(z)|$ est continue, cette borne inférieure est en fait un minimum $|P(z_0)|$. Montrons par l'absurde que $|P(z_0)| = 0$. Supposons le contraire. Soit $F(z) = P(z+z_0)/P(z_0) \in \mathbb{C}[z]\backslash\mathbb{C}$. Alors $F(0) = 1$ et $|F(z)| \geq 1$ pour tout $z \in \mathbb{C}$. On peut écrire

$$F(z) = 1 + az^r(1 + zG(z)), \quad a \in \mathbb{C}^*, r \geq 1, G(z) \in \mathbb{C}[z].$$

Écrivons $a = \rho_0 e^{i\theta_0}$. Considérons les z de la forme $z = \epsilon e^{i(\theta_0+\pi)/r}$ avec $\epsilon \in \mathbb{R}$ positif et petit. Il suit que

$$F(z) = 1 - \rho_0\epsilon^r + o(z^r).$$

En prenant ϵ suffisamment petit on aura

$$|F(z)| \leq |1 - \rho_0\epsilon^r| + |o(\epsilon^r)| = 1 - \epsilon^r(\rho_0 - |o(\epsilon^r)|/\epsilon^r) < 1.$$

Contradiction. □

Corollaire 3.3.55. *Tout polynôme non-constant de $\mathbb{R}[X]$ se décompose en un produit de facteurs de degré 1 ou 2. Autrement dit, les polynômes irréductibles de $\mathbb{R}[X]$ sont de degré 1 ou 2. En particulier, tout polynôme $P(X) \in \mathbb{R}[X]$ non nul admet une unique décomposition sous la forme*

$$P(X) = c \prod_{1 \leq j \leq n} (X - x_j)^{r_j} \prod_{1 \leq k \leq m} (X^2 + a_k X + b_k)^{s_k}$$

avec $c, x_j, a_k, b_k \in \mathbb{R}$, les x_j deux à deux distincts et les $X^2 + a_k X + b_k$ deux à deux distincts.

Démonstration. Soit $F(X)$ un polynôme irréductible dans $\mathbb{R}[X]$. On peut supposer $F(X)$ unitaire. Soit $\alpha \in \mathbb{C}$ une racine complexe de $F(X)$. Alors $F(X) = \mathrm{Irr}(\alpha, \mathbb{R}, X)$ et $\deg F(X) = [\mathbb{R}[\alpha] : \mathbb{R}] \leq [\mathbb{C} : \mathbb{R}] = 2$ (propsition 3.3.39) puisque $\alpha \in \mathbb{C}$. □

Notons que les polynômes de degré 1 sont irréductibles. Un plynôme $X^2 + aX + b \in \mathbb{R}[X]$ de degré 2 est irréductible si et seulement si $a^2 - 4b < 0$, c'est-à-dire s'il n'a pas de racine réelle.

Proposition 3.3.56. *Soit Ω/K une extension (non nécessairement algébrique) avec Ω algébriquement clos. Soit $\bar{K}$ l'ensemble des éléments de Ω algébriques sur K. Alors $\bar{K}$ est une clôture algébrique de K.*

Démonstration. On sait que $\bar{K}$ est une extension algébrique de K (corollaire 3.3.21). Soit $P(X) \in \bar{K}[X]$ un polynôme non constant. Il admet une racine $\alpha \in \Omega$ puisque ce dernier est algébriquement clos. On a α algébrique sur K^c, donc algébrique sur K (proposition 3.3.23). Il suit que $\alpha \in K^c$. Donc $P(X)$ a une racine dans K^c et ce dernier est algébriquement clos. □

Ces résultats permettent de construire une clôture algébrique de $\mathbb{Q}$ sans utiliser le théorème de Steinitz.

Corollaire 3.3.57. *L'ensemble des nombres (complexes) algébriques $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.*

Proposition 3.3.58. *Soit L/K une extension algébrique, alors toute clôture algébrique L^c de L est aussi une clôture algébrique de K.*

Démonstration. En effet, L^c est algébriquement clos, algébrique sur L, donc algébrique sur K (corollaire 3.3.21), c'est donc une clôture algébrique de K. □

Exercice 3.3.59 Soit L/K une sous-extension de K^c/K. Montrer que K^c est une clôture algébrique de L.

3.4 Extensions remarquables

3.4.1 Extensions quadratiques

Une *extension quadratique* L/K est une extension de degré 2. Dans ce sous-paragraphe on suppose pour simplifier que K est de caractéristique nulle (donc K est une extension de $\mathbb{Q}$).

Proposition 3.4.1. *Soit K un corps de caractéristique nulle. Soit L une extension quadratique. Alors il existe $a \in K$ qui ne soit pas un carré dans K tel que $L = K[\alpha]$ avec $\alpha^2 = a$ (donc L/K est obtenue par extraction d'une racine carrée). De plus, si $L = K[\beta]$ avec $\beta^2 \in K$, alors il existe $c \in K^*$ tel que $\beta = c\alpha$.*

Démonstration. Soit $t \in L \setminus K$ avec polynôme minimal $X^2 + a_1X + a_0 \in K[X]$. Alors $(t + a_1/2)^2 = (a_1^2 - 4a_0)/4$. Notons $\alpha = t + a_1/2$, $a = (a_1^2 - 4a_0)/4 \in K$. Alors $\alpha^2 = a$. On a $\alpha \notin K$ car $t \notin K$. Si $L = K[\beta]$ avec $\beta^2 \in K$, on a $\alpha = c_0 + c_1\beta$ avec $c_i \in K$. Il suit que $2c_0c_1\beta = \alpha^2 - (c_0^2 + c_1\beta^2) \in K$. Donc $c_0 = 0$ ou $c_1 = 0$, mais le deuxième cas est impossible car $\alpha \notin K$. Par conséquent $c_0 = 0$ et $\beta \in \alpha K^*$. □

Remarque 3.4.2 Une extension finie L/K est dite *galoisienne* (du nom du mathématicien français Évariste Galois), s'il existe un polynôme irréductible $F(X) \in K[X]$ tel que : L/K soit un corps de décomposition de $F(X)$, et que $F(X)$ n'ait que des racines simples dans L.

Une extension quadratique en caractéristique nulle est automatiquement galoisienne.

3.4.2 Extensions cyclotomiques

Soit $n \geq 1$. On note μ_n l'ensemble des racines n-ièmes (non nécessairement primitives) de l'unité dans $\mathbb{C}$. Si $\xi_n = e^{2i\pi/n} \in \mathbb{C}$, alors

$$\mu_n = \{\xi_n^k \mid 0 \leq k \leq n-1\}.$$

Les *extensions cyclotomiques de* $\mathbb{Q}$ sont les extensions $\mathbb{Q}[\xi_n]/\mathbb{Q}$ pour $n \geq 1$. Elles ont été introduites par Kummer au 19ème siècle (et par Euler auparavant pour $n = 3$) dans le but de montrer le grand théorème de Fermat.

Dans ce qui suit, nous allons calculer les degrés de ces extensions. Rappelons que

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$$

est la fonction indicatrice d'Euler. On a facilement que $\varphi(p^r) = p^r - p^{r-1}$ si p est premier. Le théorème des restes chinois implique un isomorphisme d'anneaux

$$\mathbb{Z}/qr\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$$

si $\text{pgcd}(q, r) = 1$. D'où un isomorphisme de groupes

$$(\mathbb{Z}/qr\mathbb{Z})^* \simeq (\mathbb{Z}/q\mathbb{Z})^* \times (\mathbb{Z}/r\mathbb{Z})^*$$

et $\varphi(qr) = \varphi(q)\varphi(r)$ sous l'hypothèse $\text{pgcd}(q, r) = 1$. Par suite si on décompose $n = \prod_i p_i^{r_i}$ avec les p_i deux à deux distincts et $r_i \geq 1$, alors

$$\varphi(n) = \prod_i p_i^{ri-1}(p_i - 1).$$

L'ensemble μ_n^* des racines primitives n-ièmes de l'unité (c'est-à-dire les racines complexes d'ordre exactement n de 1) est égal à l'ensemble des ξ_n^k avec $1 \leq k \leq n$ et $\text{pgcd}(k, n) = 1$. Soit

$$\Phi_n(X) = \prod_{1 \leq k \leq n, (k,n)=1} (X - \xi_n^k) \in \mathbb{C}[X].$$

On l'appelle le **n-ième polynôme cyclotomique**. C'est un polynôme unitaire, de degré $\varphi(n)$, et ses zéros dans $\mathbb{C}$ sont des zéros simples.

Lemme 3.4.3. *Soit p un nombre premier. Alors pour tout $k = 1, 2, \ldots, p-1$, le coefficient binomial $\binom{p}{k}$ est divisible par p.*

Preuve: On sait que $k!(p-k)!$ divise $(p-1)!p = p!$ (le quotient étant précisément l'entier $\binom{p}{k}$) et est premier à p. Il suit du lemme de Gauss 2.1.10 que $k!(p-k)!$ divise $(p-1)!$. Par suite $\binom{p}{k} = p((p-1)!/(k!(p-k)!))$ est divisible par p.

Exemple 3.4.4 Calcul explicite de $\Phi_n(X)$ pour $n = 1, ..., 4$: $X - 1$, $X + 1$, $X^2 + X + 1$, $X^2 + 1$. Pour p premier,

$$\Phi_p(X) = (X^p - 1)/(X - 1) = X^{p-1} + \cdots + X + 1.$$

En effet, $X^p - 1$ est le produit des $X - \xi$ avec ξ parcourant les toutes les racines p-ième de l'unité. Parmi celles-ci, seule 1 n'est pas primitive. On constate que ces polynômes appartiennet en fait à $\mathbb{Z}[X]$. De plus $\Phi_p(X)$ est irréductible dans $\mathbb{Q}[X]$. En effet,

$$\Phi_p(X + 1) = ((X + 1)^p - 1)/X = X^{p-1} + a_{p-1}X^{p-2} + \cdots + a_2X + a_1$$

avec $a_k = \binom{p}{k}$ divisible par p pour tous $1 \leq k \leq p - 1$ (lemme 3.4.3), et $a_1 = p$ non divisible par p^2. Par le critère d'Eisenstein, on voit que $\Phi_p(X + 1)$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$. Cela implique le même résultat pour $\Phi_p(X)$.

La proposition 3.4.5 et le théorème 3.4.6 qui suivent sont admis. Les lecteurs intéressés peuvent lire la preuve détaillée ci-dessous.

Proposition 3.4.5. *Soit $n \geq 1$.*

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

(2) *$\Phi_n(X) \in \mathbb{Z}[X]$.*

Démonstration. (1) On partitionne l'ensemble des racines n-ièmes de 1 dans $\mathbb{C}$ en la réunion disjointe des racines primitives d-ièmes de 1, pour les diviseurs positifs d de n.

(2) On procède par récurrence sur n. On a déjà $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Supposons que $\Phi_m(X) \in \mathbb{Z}[X]$ pour tout $m < n$. Soit $F(X) = \prod_{d|n, d\neq n} \Phi_d(X)$. C'est alors un polynôme unitaire dans $\mathbb{Z}[X]$. On effectue la division euclidienne dans $\mathbb{Z}[X]$:

$$X^n - 1 = F(X)Q(X) + R(X)$$

avec $Q(X), R(X) \in \mathbb{Z}[X]$ et $\deg R(X) < \deg F(X)$. Cette égalité est aussi vraie dans $\mathbb{C}[X]$. Mais $F(X)$ divise $X^n - 1$ dans $\mathbb{C}[X]$, donc $F(X)$ divise $R(X)$ dans $\mathbb{C}[X]$, ce qui implique que $R(X) = 0$ en considérant les degrés. Par suite $\Phi_n(X) = Q(X) \in \mathbb{Z}[X]$. □

Theorem 3.4.6. *Pour tout $n \geq 1$, $\Phi_n(X)$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$. En particulier $[\mathbb{Q}[\xi_n] : \mathbb{Q}] = \varphi(n)$.*

Définition 3.4.7 Soit K un corps, soit $f(X) \in K[X] \setminus K$. On dit que $f(X)$ est *séparable* si dans une clôture algébrique de K, les racines de $f(X)$ sont toutes des racines simples. On voit facilement que cela équivaut à $\text{pgcd}(f(X), f'(X)) = 1$ dans $K[X]$ où $f'(X)$ est le polynôme dérivé de $f(X)$.

Exemple 3.4.8 Le polynôme $X^n - 1$ est séparable dans $K[X]$ si $n \in K^*$. En effet la dérivée nX^{n-1} est alors première à $X^n - 1$.

Si K est de caractéristique p, alors $X^{p^d} - X$ est séparable car sa dérivée est égala à $-1 \in K^*$, donc le pgcd concerné est 1.

Preuve: Comme $\Phi_n(X)$ est unitaire, donc primitif, son irréductibilité sur $\mathbb{Z}$ et sur $\mathbb{Q}$ sont équivalentes. Soit $F(X) \in \mathbb{Z}[X]$ un facteur irréductible de $\Phi_n(X) \in \mathbb{Z}[X]$. On peut le prendre unitaire. On va montrer que $F(X) = \Phi_n(X)$, ce qui impliquera que $\Phi_n(X)$ est irréductible. Admettons provisoirement l'assertion suivante :

(**A**) *Soit ξ une racine de $F(X)$ dans $\mathbb{C}$. Soit p un nombre premier ne divisant pas n. Alors ξ^p aussi racine de $F(X)$.*

Tout entier k premier à n est un produit de nombres premiers p ne divisant pas n, il suit que ξ^k est racine de $F(X)$. Or l'ensemble de ces puissances couvrent les racines primitives n-ièmes de l'unité, donc $F(X) = \Phi_n(X)$.

Il reste à montrer l'assertion (**A**). On a $\Phi_n(X) = F(X)G(X)$ avec $F, G \in \mathbb{Z}[X]$ unitaires et $\deg F(X) \geq 1$. Montrons d'abord deux résultats préliminaires.

Lemme 3.4.9. *Soit $g(X) \in \mathbb{F}_p[X]$. Alors $g(X^p) = (g(X))^p$.*

Preuve: Si $1 \leq k \leq p-1$ est un entier, alors le coefficient binômial $\binom{p}{k}$ est divisible par p dans $\mathbb{Z}$. Il suit de cela que si A est un anneau dans lequel $p.1_A = 0$, alors $(a_1 + a_2)^p = a_1^p + a_2^p$ pour tous $a_1, a_2 \in A$.

Soit $a \in \mathbb{F}_p$. Le petit théorème de Fermat dit que $a^p = a$ (c'est trivial si $a = 0$, sinon, $a \in (\mathbb{Z}/p\mathbb{Z})^*$ qui est un groupe d'ordre $p - 1$, et le théorème de

Legendre implique que $a^{p-1} = 1$, donc $a^p = a$). Comme on est dans un anneau de caractéristique p, on a

$$(\sum_i a_i X^i)^p = \sum_i a_i^p X^{ip} = \sum_i a_i X^{ip},$$

donc $g(X)^p = g(X^p)$.

Lemme 3.4.10. *Si $H(X) \in \mathbb{Z}[X]$ a une racine commune avec $F(X)$ dans $\mathbb{C}$, alors $F(X)$ divise $H(X)$ dans $\mathbb{Z}[X]$.*

Preuve: Montrons d'abord que F divise H dans $\mathbb{Q}[X]$. Sinon, comme F est irréductible dans $\mathbb{Q}[X]$, on aurait une identité de Bézout

$$1 = a(X)H(X) + b(X)F(X), \quad a(X), b(X) \in \mathbb{Q}[X].$$

En remplaçant X par une racine commune $\alpha \in \mathbb{C}$ de $F(X)$ et $H(X)$, on a $1 = 0$, absurde. D'où $H(X) = F(X)Q(X)$ avec $Q(X) \in \mathbb{Q}[X]$. Comme $\mathrm{cont}(Q) = \mathrm{cont}(H) \in \mathbb{Z}$, on a $Q(X) \in \mathbb{Z}[X]$ (proposition 2.4.5(a)).

Preuve de (**A**) : Pour tout

$$P(X) = a_d X^d + ... + a_0 \in \mathbb{Z}[X],$$

on note

$$\bar{P}(X) = \bar{a}_d X^d + ... + \bar{a}_0 \in \mathbb{F}_p[X],$$

où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $\bar{a}_k$ est l'image de a_k dans $\mathbb{F}_p$.

Supposons que ξ^p ne soit pas racine de $F(X)$. Comme ξ^p est aussi racine primitive n-ième de l'unité, elle est racine de $\Phi_n(X) = F(X)G(X)$. Il suit que ξ^p est racine de $G(X)$. Autrement dit, ξ est racine de $G(X^p)$. D'après le lemme ci-dessus,

$$F(X) \mid G(X^p) \quad \text{dans } \mathbb{Z}[X].$$

Soit $q(X)$ un facteur irréductible de $\bar{F}(X)$. Alors $q(X)$ divise $\bar{G}(X^p) = \bar{G}(X)^p$ (lemme 3.4.9), donc $q(X) \mid \bar{G}(X)$, et $q(X)^2$ divise $\bar{F}(X)\bar{G}(X) = \bar{\Phi}_n(X)$ qui divise $X^n - 1 \in \mathbb{F}_p[X]$. Cela implique que $X^n - 1 \in \mathbb{F}_p[X]$ n'a que des racines multiples dans une clôture algébrique de $\mathbb{F}_p$ et n'est donc pas séparable. Absurde (exemple 3.4.8). Donc ξ^p est bien une racine de $F(X)$. □

3.5 Corps finis

3.5.1 Structure des corps finis

On va classifier les corps commutatifs finis. Notons qu'en fait tout corps fini est commutatif (théorème de Wedderburn). Rappelons que pour tout nombre premier p, on note $\mathbb{F}_p$ le corps premier $\mathbb{Z}/p\mathbb{Z}$.

Proposition 3.5.1. *Soit F un corps fini. Alors sa caractéristique est un nombre premier p et F est une extension finie de $\mathbb{F}_p$. On a $|F| = p^{[F:\mathbb{F}_p]}$.*

Démonstration. L'homomorphisme canonique $\mathbb{Z} \to F$ ne peut pas être injectif, donc admet un noyau qui est un idéal maximal $p\mathbb{Z}$. Ce qui veut dire que F est de caractéristique p et que $\mathbb{F}_p \subseteq F$ (3.2.6). Comme F engendre lui-même comme espace vectoriel sur $\mathbb{F}_p$, il est de dimension finie. L'égalit $|F| = p^d$ où $d = [F : \mathbb{F}_p]$ résulte du fait que $F \simeq \mathbb{F}_p^d$ en tant que $\mathbb{F}_p$-espace vectoriel (théorème 3.1.5(4)). □

Soit K un corps. On a une opération de dérivation sur les polynômes définie par $(\sum_i a_i X^i)' = \sum_i i a_i X^{i-1}$. On vérifie immédiatement que pour tous $a \in K$, $P(X), Q(X) \in K[X]$, on a

1. $(P + Q)' = P' + Q'$, $(aP)' = aP'$.
2. $(PQ)' = P'Q + PQ'$.

Tout polynôme constant est de dérivé nul. La réciproque est vraie si K est de caractéristique nulle, mais fausse si K est de caractéristique positive p. En effet tout polynôme de la forme $\sum_i a_i X^{pi}$ est de dérivée nul.

Lemme 3.5.2. *Soit $P(X) \in K[X]$ un polynôme non constant à coefficients dans un corps K.*

1. *Si $a_1, \ldots, a_n \in K$ sont des racines 2 à 2 distinctes de $P(X)$, alors*

$$\prod_{1 \le i \le n} (X - a_i) \mid P(X).$$

   En particulier $n \le \deg P(X)$.

2. *Si a est une racine multiple de $P(X)$ (c'est-à-dire $(X-a)^2$ divise $P(X)$), alors c'est une racine commune de $P(X)$ et du polynôme dérivé $P'(X)$.*

Lemme 3.5.3. *Soit K un anneau de caractéristique p. Alors pour tout $a, b \in K$ et pour tout entier $d \ge 1$, on a $(a + b)^{p^d} = a^{p^d} + b^{p^d}$.*

Démonstration. Il suffit de prouver l'égalité quand $d = 1$. Le cas général suit d'une récurrence facile sur d. Par le lemme 3.4.3, Pour tout entier $1 \le k \le p-1$, le coefficient binômial $\binom{p}{k}$ est un multiple de p. En développant $(a + b)^p$ par la formule de Newton et en tenant compte du fait que $p.1_K = 0$, on obtient $(a + b)^p = a^p + b^p$. □

Dans toute la suite du paragraphe, pour nombre premier p, nous fixons une clôture algébrique $\bar{\mathbb{F}}_p$ de $\mathbb{F}_p$ (Définition 3.3.52).

Théorème 3.5.4. *Fixons p et $\bar{\mathbb{F}}_p$ comme ci-dessus.*

(a) *Soient $d \geq 1$ et $q = p^d$. Il existe une et une seule sous-extension $\mathbb{F}_q$ de degré d de $\bar{\mathbb{F}}_p/\mathbb{F}_p$, donnée par*

$$\mathbb{F}_q := \{x \in \bar{\mathbb{F}}_p \mid x^q = x\}.$$

(b) *Tout sous-corps fini de $\bar{\mathbb{F}}_p$ est égal à un $\mathbb{F}_q$.*

(c) *Soit $\ell \geq 1$. Alors $\mathbb{F}_{p^\ell} \subseteq \mathbb{F}_q$ si et seulement si $\ell \mid d$.*

Preuve: (a) On vérifie sans peine à l'aide du lemme 3.5.3 que l'ensemble $\mathbb{F}_q$ est un sous-corps de $\bar{\mathbb{F}}_p$. C'est l'ensemble des racines dans $\bar{\mathbb{F}}_p$ du polynôme $X^q - X \in \bar{\mathbb{F}}_p$. Celui-ci a pour dérivé -1, il n'a donc pas de racine multiple (lemme 3.5.2), et a donc exactement q racines dans $\bar{\mathbb{F}}_p$. Par conséquent, $\mathbb{F}_q$ est un sous-corps à q éléments de $\bar{\mathbb{F}}_p$, son degré sur $\mathbb{F}_p$ est d d'après la proposition 3.5.1.

Soit maintenant F une sous-extension de $\bar{\mathbb{F}}_p/\mathbb{F}_p$ de degré d. Pour tout $x \in F^*$, on a $x^{q-1} = 1$ puisque F^* est un groupe d'ordre $q-1$. Il suit que $x^q = x$ et cette égalité est vraie pour tout $x \in F$. Par conséquent $F \subseteq \mathbb{F}_q$. Comme ils ont le même cardinal, ils sont égaux.

(b) Soit F une sous-extension finie de $\bar{\mathbb{F}}_p/\mathbb{F}_p$, d'un certain degré d, alors $F = \mathbb{F}_{p^d}$ d'après (a).

(c) Soit $x \in \mathbb{F}_{p^\ell}$. D'après (a), on a $x^{p^\ell} = x$. Pour tout $k \geq 1$, on a

$$x^{p^{\ell k}} = x^{p^\ell p^{\ell(k-1)}} = (x^{p^\ell})^{p^{\ell(k-1)}} = x^{p^{\ell(k-1)}}.$$

On voit alors que $x^{p^{\ell k}} = x$ pour tout $k \geq 1$. Ainsi si $\ell \mid d$, $\mathbb{F}_{p^\ell} \subseteq \mathbb{F}_{p^{\ell \times (d/\ell)}} = \mathbb{F}_q$. Inversement, si $\mathbb{F}_{p^\ell} \subseteq \mathbb{F}_q$, alors $\ell = [\mathbb{F}_{p^\ell} : \mathbb{F}_p] \mid d = [\mathbb{F}_q : \mathbb{F}_p]$.

Corollaire 3.5.5. *Tout corps fini est isomorphe à un $\mathbb{F}_q$. Deux corps finis sont isomorphes si et seulement s'ils ont le même cardinal.*

Preuve: Soit F un corps fini. On a vu que F est une extension finie, d'un certain degré d, de $\mathbb{F}_p$, où p est la caractéristique de F. Soit F^c une clôture algébrique de F. Alors c'est une clôture algébrique de $\mathbb{F}_p$. Il existe donc un $\mathbb{F}_p$-isomorphisme $\sigma : F^c \to \bar{\mathbb{F}}_p$ (une clôture algébrique fixée de $\mathbb{F}_p$). L'image $\sigma(F)$ est un sous-corps de $\bar{\mathbb{F}}_p$ d'ordre $q = p^d$, donc $\sigma(F) = \mathbb{F}_q$ et F est isomorphe à $\mathbb{F}_q$.

Si F' est un corps de même cardinal q que F, alors $F' \simeq \mathbb{F}_q \simeq F$. La réciproque est triviale.

Corollaire 3.5.6. *Soient $d, k \geq 1$. Alors*

$$\mathbb{F}_{p^d} \cap \mathbb{F}_{p^k} = \mathbb{F}_{p^{\mathrm{pgcd}(d,k)}}.$$

Preuve: L'inclusion $\mathbb{F}_{p^{\mathrm{pgcd}(d,k)}} \subseteq \mathbb{F}_{p^d} \cap \mathbb{F}_{p^k}$ résulte du théorème 3.5.4 (c). Inversement, comme $\mathbb{F}_{p^d} \cap \mathbb{F}_{p^k}$ est une sous-extension de $\mathbb{F}_{p^d}$ et de $\mathbb{F}_{p^k}$, son degré sur $\mathbb{F}_p$ divise d et k, donc $\mathrm{pgcd}(d,k)$. Il suit que $\mathbb{F}_{p^d} \cap \mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^{\mathrm{pgcd}(d,k)}}$.

Remarque 3.5.7 Attention, le corps fini à p éléments est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, mais le corps fini à p^d éléments n'est **pas du tout** isomorphe à $\mathbb{Z}/p^d\mathbb{Z}$ si $d \geq 2$, même en tant en groupes. En effet, $\mathbb{F}_{p^d} \simeq \mathbb{F}_p^d$ en tant que $\mathbb{F}_p$-espace vectoriel, donc comme groupes $\mathbb{F}_{p^d} \simeq (\mathbb{Z}/p\mathbb{Z})^d$ qui n'est pas isomorphe à $\mathbb{Z}/p^d\mathbb{Z}$ (le dernier est cyclique mais pas le premier si $d \geq 2$). Une autre raison est que $\mathbb{Z}/p^d\mathbb{Z}$ n'est pas un anneau intègre si $d \geq 2$, et n'a donc aucune chance d'être un corps.

En tant que groupe, on vient de voir que $\mathbb{F}_{p^d} \simeq (\mathbb{Z}/p\mathbb{Z})^p$, mais c'est faux en tant qu'anneau dès que $d \geq 2$ car l'anneau produit à droite n'est alors pas intègre.

Exemple 3.5.8 On a $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$ (en particulier $\mathbb{F}_4$ n'est pas contenu dans $\mathbb{F}_8$) ; $\mathbb{F}_4\mathbb{F}_8 = \mathbb{F}_{64}$. Cela vient du fait que ce sont des extensions de $\mathbb{F}_2$ de degrés respectifs $2, 3$.

Exemple 3.5.9 On voudrait une représentation concrète des corps finis. Sur $\mathbb{F}_2$, on considère les polynômes $P_2(X) = X^2 + X + 1$, $P_3(X) = X^3 + X + 1$. Ils sont de degré ≤ 3 et sans racine dans $\mathbb{F}_2$ (on évalue $P_d(0)$ et $P_d(1)$), donc irréductibles (proposition 2.2.3). Un corps de ruputre de $P_d(X)$ est une extension de degré d de $\mathbb{F}_2$, donc isomorphe à $\mathbb{F}_{2^d}$. Ainsi

$$\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1); \quad \mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1).$$

Soit α l'image de X dans $\mathbb{F}_4$. Alors $\{1, \alpha\}$ est une base de $\mathbb{F}_4$ sur $\mathbb{F}_2$ (voir la preuve de la proposition 3.3.39(b)) et donc $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$.

Soit θ l'image de X dans $\mathbb{F}_8$. Alors $\{1, \theta, \theta^2\}$ est une base de $\mathbb{F}_8$ sur $\mathbb{F}_2$. Donc

$$\mathbb{F}_8 = \{0, 1, 1 + \theta, 1 + \theta^2, 1 + \theta + \theta^2, \theta, \theta + \theta^2, \theta^2\}.$$

On peut calculer les puissances θ^k, $1 \leq k \leq 6$ récursivement à l'aide de la relation $\theta^3 = \theta + 1$ (noter que $-x = x$ pour tout $x \in \mathbb{F}_8$ puisque c'est un corps de caractéristique 2), et on trouve

$$\theta, \theta^2, 1 + \theta, \theta + \theta^2, 1 + \theta + \theta^2, 1 + \theta^2.$$

On constate que θ engendre le groupe multiplicatif $\mathbb{F}_8^*$, de sorte que $\mathbb{F}_8^* \simeq \mathbb{Z}/7\mathbb{Z}$ est cyclique. On verra que c'est le cas général (théorème 3.5.12).

Remarque 3.5.10 Pour construire une extension de degré d de $\mathbb{F}_p$, il suffit de donner un polynôme irréductible $\in \mathbb{F}_p[X]$ de degré d. On peut montrer qu'un tel polynôme existe toujours : en effet, $F := \mathbb{F}_{p^d}$ est une extension de degré d. Soit $\alpha \in F^*$ un générateur du groupe F^* (théorème 3.5.12), alors $F = \{0, \alpha^k \mid k \in \mathbb{Z}\} \subseteq \mathbb{F}_p[\alpha]$. Donc $F = \mathbb{F}_p[\alpha]$. Le polynôme irréductible $\mathrm{Irr}(\alpha, \mathbb{F}_p, X) \in \mathbb{F}_p[X]$ est irréductible de degré $\deg \alpha = [\mathbb{F}_p[\alpha] : \mathbb{F}_p] = [F : \mathbb{F}_p] = d$ (proposition 3.3.39(b)). On peut même montrer que le nombre de polynômes irréductibles de degré d tends vers l'infini "rapidement" quand d tends vers l'infini.

Exercice 3.5.11 Montrer que $\sum_{a \in \mathbb{F}_q} a = 0$. Plus généralement calculer les fonctions symétriques élémentaires $s_1, ..., s_q$ en les q éléments de $\mathbb{F}_q$. Calculer la somme $\sum_{a \in \mathbb{F}_q} a^k$ pour tout $k \geq 1$.

3.5.2 Structure du groupe multiplicatif

Theorem 3.5.12. *Soit F un corps fini. Alors F^* est un groupe cyclique.*

C'est un cas particulier du résultat qui suit.

Proposition 3.5.13. *Soit K un corps commutatif. Soit G un sous-groupe fini du groupe multiplicatif K^*. Alors G est un groupe cyclique.*

Preuve: Soit $n = |G|$. Pour tout entier $d \geq 1$, notons $G_d = \{x \in G \mid x^d = 1\}$ et $H_d \subseteq G_d$ le sous-ensemble des éléments d'ordre exactement d. Alors $G = G_n$ est la réunion disjointe des H_d, $d \mid n$. Soit φ la fonction indicatrice d'Euler. Notons d'abord que $n = \sum_{d|n} \varphi(d)$ (utiliser la proposition 3.4.5(1)).

Soit $d \mid n$ tel que $H_d \neq \emptyset$. Montrons que $|H_d| = \varphi(d)$. Pour tout diviseur e de d, on a alors $H_e \neq \emptyset$. Donc $|H_e| \geq \varphi(e)$ car si $a \in H_e$ (donc d'ordre e), alors les a^r avec $1 \leq r \leq e-1$ premiers à e sont deux à deux distincts et d'ordre e. Comme le polynôme $X^d - 1 \in K[X]$ a au plus d racines dans K (lemme 3.5.2, c'est le seul endroit de la preuve où l'hypothèse G contenu dans K^* intervient), on a

$$d \geq |G_d| = \sum_{e|d} |H_e| \geq \sum_{e|d} \varphi(e) = d.$$

Donc $|H_e| = \varphi(e)$ pour tout $e \mid d$. En particulier $|H_d| = \varphi(d)$. Il suit que

$$\sum_{d|n} \varphi(d) = n = |G| = \sum_{d|n, H_d \neq \emptyset} \varphi(d).$$

Cela implique $H_d \neq \emptyset$ pour tout $d \mid n$. Par conséquent $H_n \neq \emptyset$, ce qui veut dire que G a un élément d'ordre n et est cyclique.